governmentattic.org
"Rummaging in the government's attic"

Description of document:	National Security Agency (NSA) CRYPTOLOG internal newsletter/journals, 1997-1974
Requested date:	18-February-2008
Released date:	12-March-2013
Posted date:	18-March-2013
Source of document:	Mandatory Declassification Review Request National Security Agency Declassification Services (DJ5) Suite 6884, Bldg. SAB2 9800 Savage Road Ft. George G. Meade, MD, 20755-6884

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

-- Web site design Copyright 2007 governmentattic.org --

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

Serial: MDR-54847
12 March 2013

This responds to your request of 18 February 2008 to have all issues of *Cryptolog* reviewed for declassification. NSA/CSS periodically conducts "Special Topical Reviews" of categories of records that may be of wide public interest and posts those records to the www.NSA.gov website. In choosing Special Topics, NSA attempts to respond to subjects for which there have been numerous requests for review for declassification, as is the case with the release of the 135 issues of *Cryptolog*.

Therefore, we are directing you to the aforementioned website, where you will find copies of all 135 issues of *Cryptolog*. Some portions were redacted from the documents, as they were found to be currently and properly classified in accordance with E. O. 13526. The information denied meets the criteria for classification set forth in Section 1.4 subparagraphs (c) and (d), and remains classified TOP SECRET, SECRET, and CONFIDENTIAL as provided in Section 1.2 of E.O. 13526. The withheld information is exempt from automatic declassification in accordance with Section 3.3 (b) 3 of the Executive Order.

Section 3.5 (c) of E.O. 13526, allows for the protection afforded to information under the provisions of law. Therefore, the names of NSA/CSS employees and information that would reveal NSA/CSS functions and activities have been protected in accordance with Section 6, Public Law 86-36 (50 U.S. Code 402 note).

As your request was one of those that prompted NSA to undertake this release, which is monumental not only in terms of its size but also in the broad spectrum of NSA functions and activities the release reveals, we trust you will be pleased with the release of this collection.

Sincerely,

BLAKE C. BARNES
Chief
Declassification Services

DOCID: 4036133

~~TOP SECRET UMBRA~~

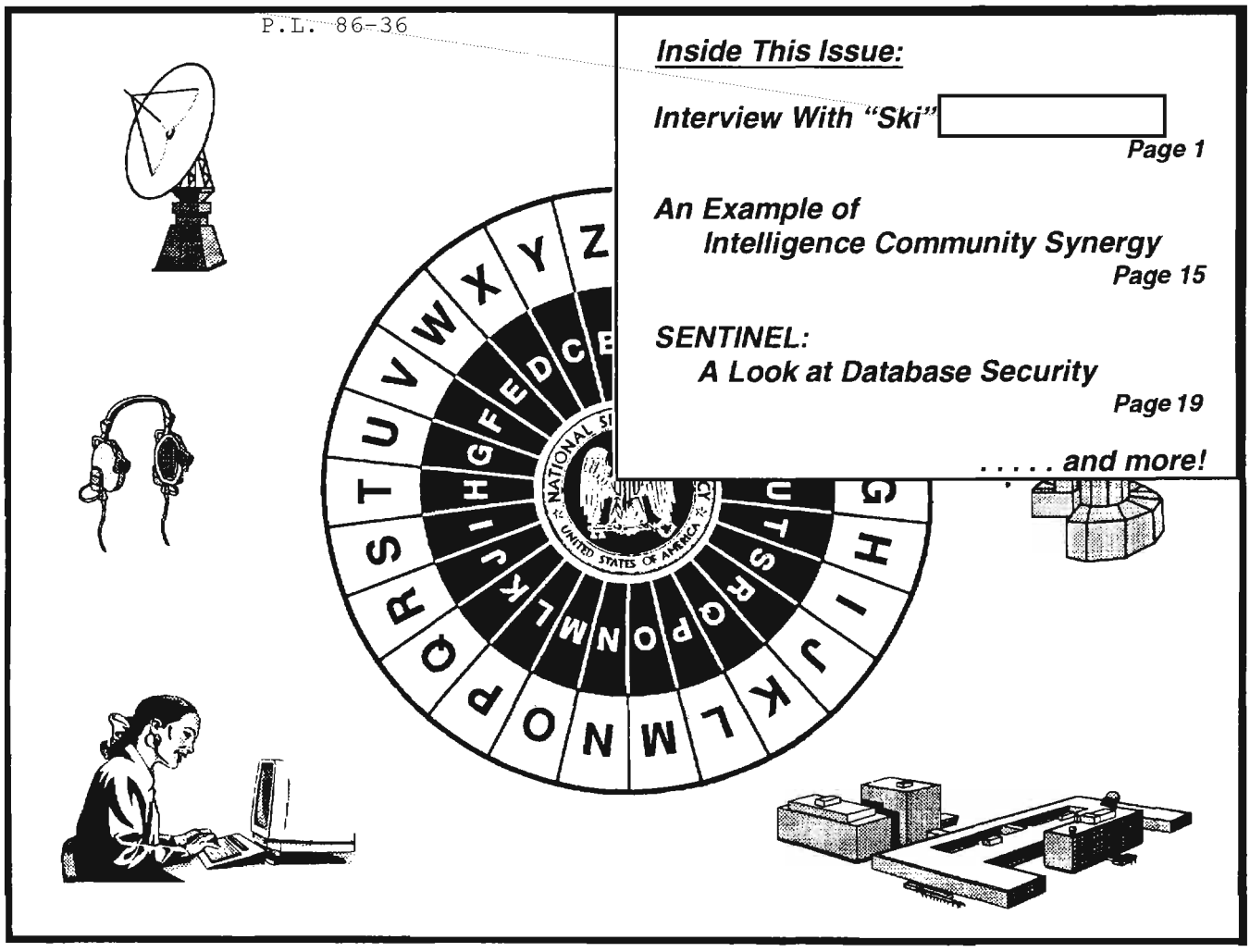
NATIONAL SECURITY AGENCY

CRYPTOLOG

The Journal of Technical Health

Vol. XXIII, No. 2 SUMMER 1997

P.L. 86-36



Inside This Issue:

Interview With "Ski" [redacted]
Page 1

An Example of Intelligence Community Synergy
Page 15

SENTINEL: A Look at Database Security
Page 19

. . . . . and more!

~~Derived From: NSA/CSSM 123-2~~
~~Dated 3 September 1991~~
~~Declassify On: Source Marked "OADR"~~
~~Date of source: 3 Sep 91~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

~~TOP SECRET UMBRA~~

DOCID: 4036133

CRYPTOLOG

Summer 1997
Vol. XXIII, No. 2

Published by P02, Operations Directorate Intelligence Staff

Publisher ..... William Nolte (963-5283)

Editor ..... [redacted] (963-5283)

P.L. 86-36

Board of Advisors

Chairman ..... [redacted] (963-7712)
Computer Systems ..... [redacted] (961-1051)
Cryptanalysis ..... [redacted] (963-7243)
Intelligence Analysis ..... William Nolte, P02 (963-5283)
Language ..... [redacted] (963-7667)
Mathematics ..... [redacted] (963-1363)
Signals Collection ..... [redacted] (963-5717)
Telecommunications ..... [redacted] (996-7847)
Member at Large ..... [redacted] (968-4010)
Member at Large ..... [redacted] (961-8214)

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

To submit articles and letters, please see last page.

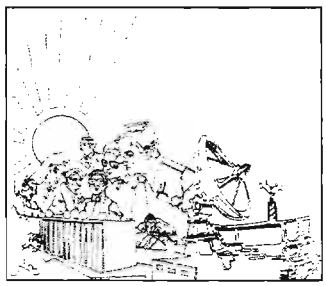


Table of Contents

Interview with "Ski" [redacted] *(U), by Bill Nolte* *1*

Signals Analysis:
The Untold Success Story (U), by [redacted] *10*

Adventure in the Attic:
An Example of IC Synergy (U), by [redacted] *15*

SENTINEL: A Look at Database Security (U), by [redacted] *19*

[redacted] *by* [redacted] *22*

Book Review:
Rapid Development: Taming Wild Software Schedules (U) *32*

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Perspective:

Lessons Learned

Interview with [redacted]

P.L. 86-36

One of the pioneers of signals analysis reflects on a fifty-year career in cryptologic service

(U) An important theme in Twentieth Century Cryptology is its expansion beyond the classic "code making and code breaking" endeavors that stretch back as long, or so it seems, as humankind has been attempting to communicate.

(U) The development of traffic analysis remains one of the most significant of those expansions. The analytic effort to derive useful information from the externals of message traffic, in addition to or apart from success in reaching the underlying plaintext of the message contents, ranks as a defining event in cryptologic history Beyond its intelligence value, traffic analysis pointed to something fundamental about the cryptology of our time: the fundamental importance of understanding not just the content of communications and the means to hide those contents but of the systems and technologies that carried those communications.

(U) An obvious point? In retrospect, possibly. But the history of cryptology and of the agencies that practice it are largely told in the gap between the retrospective obvious and earlier conventional wisdoms. After the Second World War, signals analysis represented yet another potential extension of cryptologic activity. But was it truly cryptologic in nature? Or was it more simply a matter of communications research, with, it might be granted, some intelligence implications.

P.L. 86-36

(U) [redacted] (any number of NSA personnel might hesitate for a second on the full name before reaching recognition with "Oh, you mean 'Ski.'") has spent a career, a half-century at the center of the evolution of signals analysis. In December 1996, shortly before his retirement, Ski discussed his career with *Cryptolog*.

(U) **Let's start chronologically. You went into the Navy in 1946, when you were 18 years old.**

(U) I was still 17.

(U) **Were you drafted?**

(U) No. The draft was still on, but the Navy had a program—I guess all the services had something like this—called the Kiddy Cruise. If you enlisted in the Navy at 17 and stayed until you were 21, you got credit for four years of service plus all your GI Bill benefits for schooling, housing, and all those other things. So I enlisted in

August, I was 18 in October, stayed for three years and two months or whatever it was; I would have received credit for four years of federal service had I stayed in.

(U) **How did you get into cryptologic service? Was that just a decision by the guy at the recruit depot?**

(U) No. It happened somewhere between the time I enlisted and the time I got out of boot camp. I was one of fifteen selected to be sent from Great Lakes, Illinois, to Washington, D.C., for this strange training that nobody knew anything about. George Rocawich was another in that group. He became one of our premier traffic analysts and just retired a few years ago. There was another group that came from the San Diego recruiting center, and they lorded it over the rest of us that they had come by ship to the East Coast. We had come by train from Chicago, so they had sea duty, and we didn't.

(U) We arrived in D.C., reported to the Navy Department, and they said we were to take off for a few days and then to report to Nebraska Avenue, the Naval Security Station or U.S. Navy Communications Station Washington (CSAW) as it was known then.

(U) **What did you do after reporting there?**

(U) The first thing, while we waited for our clearances, we were assigned in an LIC area in the attic studying electricity, math, typing, and cryptography. Our CO was CDR John Quincy Adams III, a direct descendant of President Adams.

(U) Jim Bates was part of that group and we always went to him with our crypt problems because he always had the solution first. From there, my first assignment after being cleared was in the personnel office. Then I was assigned to R&D, and I was a yeoman for a while and then communications technician or CT. From there I was reassigned to what became the R&D signals analysis lab. It wasn't called that then, but that's basically what it was. The Navy organization was N33 (later to become AFSA 334).

(U) In fact, though, the basic mission of the lab was for support to engineers building equipment; the use of signals analytic results for intelligence production was really a secondary mission. But we did have different kinds of signals coming in and the types of questions that were being asked—what kind of signals were they? How did they look? What did we have to cope with them? Who was the user? I took a real interest in that, so in addition to doing the administrative duties for the office, I also began working on the signals and found that more interesting.

(U) **We've been in a period of downsizing the last few years. But that period immediately after the war must have been a tremendously difficult period.**

(U) When I transferred from the Navy to civilian life in 1949, it was only through intervention of the folks inside the building that I got on board. They were not hiring—certainly not clerks. I wasn't exactly in a critical skill.

(U) But the fact that I had learned something about signals analysis and was interested in pursuing that made the difference. The chief of the research element needed someone who fit my qualifications, and he hired me. The Lord was smiling at me all the way on that one.

(U) **You were hired as a clerk?**

(U) Yes. "Clerk, General" is what they called it at the time.

(U) **At what grade?**

(U) Then it was called CAF-4, at about $2700 per year. Which was only slightly more than I was making in the Navy.

(U) **Were you at Nebraska Avenue when AFSA was formed?**

(U) Yes. They called us all together, the whole complex, to the back of the loading dock of what I think was Building 4A, while they announced that we were now the Armed Forces Security Agency. It didn't mean a whole lot, and of course the ser-

vices weren't too keen on the idea.

(U) **How much did things change after that? Did the Army people start to show up at Nebraska Avenue and so on?**

(U) Oh yes. There was a big exchange of people. I left Nebraska Avenue and went over to Arlington Hall. Because of the new structure new opportunities were available. That's where we started signals analysis in the production organization. The first organization was AFSA 204. The research folks were, as I said, more interested in the subject from the point of view of building equipment. The production element was very small: an Army captain named Ron Schmidt, myself, and two maintenance technicians. And me.

(U) But that was the start of what became NSA W34, T16, and A5? The latter two were evolved from the processing efforts whereas W34 stayed with signals analysis.

(U) **When you look at that fact on your résumé "started the first signals analysis effort in the production organization," that's a rather striking statement. It's hard to realize there was ever a point where we didn't have a signals analysis effort.**

(U) Well, there was the effort in R/D, but not in operations.

(U) **Was that controversial? Were there people who fought that?**

~~(S-CCO)~~ Signals analysis was not well understood at that time. At first there was no duplication of effort since our mission was so totally different from that of R/D. It did cause some problems later until the two efforts were joined in 1972. To answer your question directly, it wasn't something we set out to do with some elaborate plan. In fact,

[redacted]

(U) When I was in R&D we were using wire recorders, and it almost forced you to take up smoking. The only way to splice the wire was to tie the two ends of the wire—which was always breaking—in a square knot, pull it tight, and fuse it with some kind of heat. Well with one hand on each end of the wire, there was no way to hold a soldering iron or a match, so we soon learned how to touch the wire with the end of a lighted cigarette.

~~(S-CCO)~~ We worked at this for several years, but the idea of signals analysis in PROD did not really catch [redacted] Every job I had, and every time I either got promoted or we reorganized, my job was described as either an engineering aide or communications specialist or something. It wasn't until about 1954 that we came up with signals analyst to describe what we did.

EO 1.4.(c)
P.L. 86-36

~~(S-CCO)~~ In 1958 we became a division. Admiral Tommy R. Kurtz, USN, was the Director for Production (PROD) when we started to work

[redacted]

[redacted]

[redacted]

EO 1.4.(c)
P.L. 86-36

(U) I didn't realize this at the time, because when you're a GS-12 working in the basement you don't get too involved in the politics of *any*thing. But the Navy was very jealous, but Adm. Kurtz was convinced this was a SIGINT challenge and NSA was going to handle it. and we did.

(U) **Did you ever think you were going to be transferred back to the Navy or something like that?**

(U) Not really. Of course, AFSA had its problems. But then we became NSA and things seemed to settle down a little. But we still had—beyond my pay grade and my interest—politics of one sort or another. At my level, we had work to do, and signals to analyze, so we didn't get involved in it.

P.L. 86-36

~~(S-CCO)~~ And we were able to get things done. With NSA's help, the Navy was able to build the [redacted] That was built and in place in about a year. It was one of the fastest projects I've ever seen. I'm almost positive that Charlie Gandy in R/D built the recognizer that went to the field to recognized this specific signal. The real secret part of the whole project wasn't that we could intercept the signal so much as it was the ability to DF it. And that was built into the system.

(U) **You mentioned politics. What about the politics within the building. Were the signals analysts accepted as part of the process?**

~~(S-CCO)~~ No. In fact, what was then GENS 2 was not too keen that we were working on the [redacted] and we weren't part of GENS. So we were more or less tolerated. It helped tremendously that we had Admiral Kurtz as chief of PROD supporting us. Not that he ignored GENS 2, but he paid a lot of attention to us. He'd come down into the basement, take off the jacket with all those ribbons on it and hang it on a chair, and say, "What do you have today, Ski?" He was a strong believer in teamwork and saw to it that it worked for us.

(U) We had a terrific team. There was about five of us. Vernon Franks was in the Navy. Bruce Russell was a civilian analyst. Another who made

chief later on was CT1 James Killeron, USN. Leroy Spiess was our contact in GENS. But what a team!

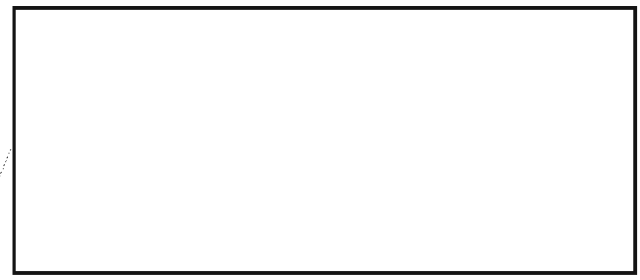
(U) I received the largest Special Act Award the agency had ever given to that time. Admiral Kurtz came down one day and told me he'd put me in for an award, and I told him I was going to have to buy him a coffee. "Coffee, hell," was his response. "You're going to have to buy me a car." That was a lot of money in 1960. But that wasn't the point. It was such a hard project, and so many people worked *so* hard on it. Not just at NSA, but the Navy, and the other services. It was a terrific effort. ADM Kurtz signed my picture of the presentation with 'team work with competence can't be beat.' That is still so true to this day.

(U) **Beyond cryptanalysis, beyond traffic analysis, the development of signals analysis could be thought of as almost another concentric circle of cryptology, couldn't it.**

(U) One thing that was different was that we didn't always pass things on from one stage of the process to another the way we do now. I had my job, which was signals analysis, and there was a sense that I didn't need to know whether the cryptanalysts were reading the system or not. We were much more inclined to say to the engineers, "Here are the parameters on which you need to work. Don't ask about anything beyond that." And we did the same with every other stage of the process. It was fairly segmented.

(U) **Talk about that. We are doing things differently, and there are very clear tradeoffs involved in that.**

(U) I think the way we're going now is a little better. I really do. I don't think everyone in the chain needs to know everything, but there were things we didn't know in the signals arena that folks watching the traffic did know. As it turned out, sometimes we found out things by accident that we had to know, such as the length of standard messages. We had to know that, and we have to be able to share information.

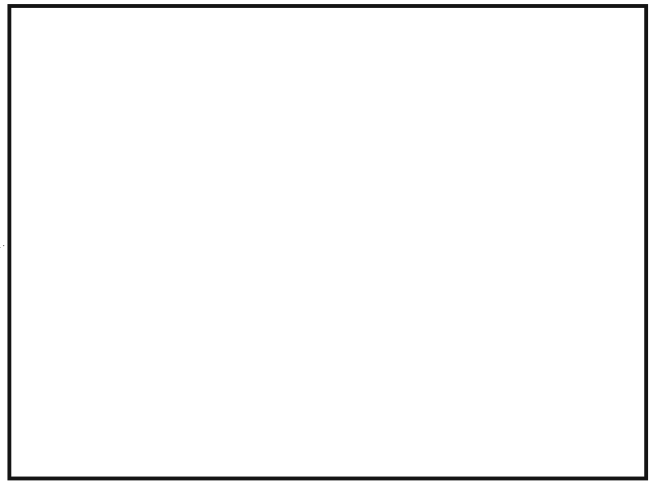


(U) It really helped to know schedules and things of that sort, so we would know where to look. We didn't have to know every detail.

(U) **Let's talk for a moment about career issues. Were you one of the early group to come out to NSA?**

(U) Not the first group, but early on. Some things haven't changed. We reorganized a lot, and people moved back and forth between Nebraska Avenue and Arlington Hall, and then we got ordered out here. It never failed. Every time I moved my residence to get closer to work, I got reassigned.

(U) **What was it like working for NSA in the 1950s?**



P.L. 86-36
EO 1.4.(c)

(U) It was just the best place to be. I guess that's what kept me here for fifty years.

(U) **But you get the sense—greater secrecy and all—that this was a much tighter community of people.**

(U) I was talking about this just the other day. You kept such a close hold on what your did and where you worked. You took your badge off when you cleared the gate. You told people you worked for the government or the Defense Department. If anyone asked what you did, you said you were an analyst, or an engineer, or whatever. A good example is that my Navy records do not reflect my assignment to CSAW, but merely to Navy Barracks Washington D.C.

(U) When I first saw the terms signals analysis and COMINT in the newspaper I nearly had a heart attack. ELINT was one thing, because the services had their own ELINT operations, and so on. But COMINT! That was enough to send shivers up my spine.

(U) **You really had an extraordinary group of folks at the top of the place, didn't you?**

~~(S-CCO)~~ The nice part of my job was it took me through all the different components of NSA. Dr. Tordella was actually the Chief of C at the time

[redacted]

~~(S-CCO)~~ Dr. Tordella had that ability to see the whole SIGINT process. And he was such a human person. I was standing out in front of the building one day when Dr. Tordella was escorting a senior DOD official out to his car. They walked past me, stopped, and turned around. Now, it was around 5:00 in the afternoon, so I didn't think I was leaving early. And even if I had, I didn't think Dr. Tordella would chew me out in front of a visitor. But he came over and told the visitor that I was the gentleman responsible for all the requests NSA was putting on the department of research and development as a result of all the new signals we were finding, [redacted] I was glad that was over, because I didn't know what he was going to do.

(U) His heart was really in the technical end of the business. He'd come down to the basement, look around, and ask questions. From time to time, he'd stick his head behind the racks to see how everything was wired up. And he didn't like to see wires just tossed around carelessly back there. He wanted them neat and laced together. He was one of the finest people this agency ever produced. Of course there are many others, but I think of him as certainly one of the best.

(U) **Like a lot of the people from that era, you had come in from the service, without a college degree and then ended up going to school at night.**

(U) That was very common in those days. And you'd go down to someplace like George Washington, and you'd find Dr. Tordella and people like that teaching a course and a number of your fellow workers in class with you.

(U) Working full time, going to school, sometimes holding a second job. It was tough. But those were good times, and I wouldn't trade them for anything.

(U) **You stayed in the signals analysis effort for a long time and then went off to field operations. What was that all about?**

(U) I went to the Air War College, graduating in 1968, and they wouldn't let me have my old job back. At the time, that was probably one of the bigger disappointments of my career. So I went to work in field operations. At that time, anything that involved feedback to the sites, making sure

they were properly equipped and informed went through there. We were basically responsible for seeing that they had what they needed to do their jobs.

(U) One of the problems we had was that all the group chiefs at that time, people like Art Levenson and Frank Raven, were going in to Gen. John Morrison, the DDO, and trying to get top priority for processing. So the folks in the processing area got a little tired of three and four people asking for some sort of change in priorities, all based on the idea they should have first shot.

(U) So, General Morrison decided he was tired of hearing all of this and decided we needed a plan. So, the Signals Processing Requirements Panel was born, in order to sort out some of this. It was staff work, pure and simple, which I wasn't too keen on, but it had to be done. I only spent a couple or three years there.

(U) Followed by a tour in the office of ELINT?

[redacted]

(U) So you've been a manager but always with signals analysis roots. How do you feel about the relationship between technical skills and managerial skills?

(U) From a personal standpoint, I had the best of both worlds. I knew enough from the technical side to hold my own in signals analysis and collection. I was not an engineer nor a mathematician, so if I tried to go back to signals analysis these days I wouldn't stand a chance. Somehow, along the way, I'd acquired enough managerial ability—I think I was good with people and good at pulling teams together. I don't know really how it happened. I went from being a section chief to a branch chief, to division and ended up being the deputy of W3. But because of my early background I was viewed by some folks as technical; others saw me as managerial. To this day, I still don't know how the decision was made to make me an SLE but I am certainly glad it was done!

(U) The fact is that in those days you didn't get ahead unless you were a manager. If I hadn't become a branch chief and a division chief, who knows where I would have ended up.

(U) And that's a continuing issue.

(U) I think at least through branch management, you have to have technical roots in this business. You have to have some sense of what your people are doing. You have to be able to mentor them and help them solve their technical problems.

(U) We're going to have to leave some details of your career to the oral history program. You've spent so long as Technical Director of B Group, I want to spend some time on that. How did you wind up there?

(U) I had spent seven years as Deputy of W3, the Office of Search. It was time for me to move. I was transferred and at the request of [redacted] was assigned to R5 to do a study of the signals analysis effort and to work on development of a system for moving technology out of the R labs into the operational areas. The signals analysis work force was aging and there were no people in the pipeline. P.L. 86-36

(U) I was disappointed in leaving W3, and I was planning to make R5 my swan song. But when [redacted] announced he was going to private industry, I was determined to finish the study before he left. I finished the study and it became the basis of an R/D and DO implementation plan. And with that done, I was returned to DO, with a note from [redacted] saying they were sending me back unharmed. One day, [redacted] approached me and asked me to come back to B as tech advisor. During my first ten years in B Group I

had eight different chiefs. I've told people my job wasn't technical, my job was to train group chiefs and in fact had a sign that said, "Honk if you have been the chief of B!"

P.L. 86-36

(U) When [redacted] came in, he wanted to do what we would now call SRTD work, in one division for all of B. He wanted me to head the division. It was there that I was promoted to SLE. At the time the rules about how many people SLEs could supervise applied. And one day, Dick Lord asked [redacted] where I had been assigned, and when [redacted] told him, Lord said maybe they should take the promotion back. I quickly requested a vote in that, so I went back to being the tech advisor.

(U) Every one of the chiefs has used me differently, depending on what their strengths were. And where they felt there was work to be done.

[redacted]

EO 1.4.(c)
P.L. 86-36

~~(S-CCO)~~ So I was always able to stay close to the signals and have fun with that. My job was to keep management informed of the trends and new signals appearing. I often believe that I had two

[redacted]

(U) How did the change to the new B affect you?

(U) I had build up a good rapport with a lot of people in the old B, so I had that base. And I knew many of the people coming in as part of the new B. So that was a help.

(U) Beyond that, the chief, [redacted] was very interested in two projects: SRTD and the development of the technical track. Those duties became paramount, so I never got involved with the signals folks in the new organization the way I had before the reorganization. Most of my chores were involved in making the structure work, and working on details, and going to any number of working group, panel etc. meetings.

(U) One big part of my job has been convincing people that there is more to the tech track than books and trips. There is more to getting a title than just getting a title. There is a payback associated with this effort—payback to the mission as well as to the people you work with.

(U) We've gotten so big. Managers have gotten farther and farther away from their technical people. And here we have a chance—as signals analysts judging signals analysts or IA judging IAs—to say to management, "When you start thinking about promotions, here are our best people." It's not a hoop you jump through.

(U) Think about the professionalization program. I know people have mixed views about it now, but you have to recall its origins. In signals analysis, most of our people had come in from the military, without degrees, and we had very little with which to motivate them to continue their development. Professionalization forced them to keep up with things, to learn about things they might otherwise have neglected. And the technical track offers us the same opportunity.

(U) Too often we think of the technical track as something you need to get promoted. And it's not that. It's you as a person. It's what does Bill bring here, and what value do we put on his talents, and what training and experience do we give him to make him better. That's very important.

(U) Professionalization developed our specialties; the tech track seems to offer the prospect of integrating those specialties. Is that a fair way to put it?

(U) The pendulum swings back and forth on that. When I came in, signals analysts were to learn signals analysis, traffic analysts were to learn traffic analysis, and so on.

P.L. 86-36

(U) Then we seemed to want to spread out a bit more. But that can go too far as well. The Army has that slogan "Be all you can be" and I like that as a way of saying develop a skill that you can excel in. Not to the exclusion of everything else, but from a base in a skill that you can truly master. Of the three possibilities, that's the one I like best. I hope that's where we're heading.

(U) **As you look back over the last fifty years, what's your proudest accomplishment?**

(U) There's no question that I'm proudest of the signals analysis lab and getting to the point where its survival was assured. I still meet people who go back to that era and who are now long gone from here, but who see me and come up to say that the lab was the best part of their career. From a personal view, that's my biggest accomplishment. For the mission, I think that had a real impact. Without signals analysis, I don't know where we'd be. Today the skill fields are a bit less defined and signals analysis overlaps a number of others, such as cryptanalysis and engineering for example. But the signals analysis function remains a corner stone of the cryptologic family. Another area I am proud of is the SRTD effort, but the success of that effort remains to be graded.

(U) **You came in at a time of downsizing and transition. And here we are again, with a fair amount of concern expressed all around. But the lesson is you can do good work in those times.**

(U) Somehow you manage. Sure, you have things going on, you have things to worry about. But whenever there's been a crisis, this agency has turned to. Nobody raises the question of overtime or all that; nobody even thinks about being here all night in a crisis. Our people respond. They always have.

(U) **Any last thoughts?**

(U) It's going to be tough to leave. When I took my last polygraph, the operator was astonished to find I had been here fifty years. So, when he asked that sneaky question they always ask at the end, it turned out to be "In your fifty years here, have you ever been unhappy?" And I said no. I don't what the response was on the machine, but I owe this agency an awful lot. I really do. I'll always remember the people here. We have our ups and downs, but as far as the mission is concerned, as far as the sense of having contributed to what General Minihan described as avoiding "the war we didn't have," I feel like I did make a contribution.

(U) **At the Navy Memorial on Pennsylvania Avenue, there's a quote from President Kennedy to the effect that no man should have a prouder boast than that of having served in the United States Navy. You could make the same case, I think, for the Cold War American Intelligence Community.**

(U) I'm a plank owner of that memorial, and could never be prouder of my long association with both the U.S. Navy and the NSA. My thanks to both for a most rewarding opportunity.

KA

DOCID: 4036133

CRYPTOLOG
Summer 1997

P.L. 86-36

Signals Analysis: The Untold Success Story

by [redacted]

The Background:

(U) After World War II, both the Army and Navy conducted SIGINT activities as independent efforts. The Army's effort was headquartered at Arlington Hall Station (AHS) in Virginia and the Navy on Nebraska Avenue in Washington, D.C., (CSAW). In 1946 the Navy's headquarters was also known as the Naval Security Station (NSS) and as Communications Station Activity (Washington). Captain Harper was the commanding officer.

EO 1.4.(c)
P.L. 86-36

~~(FOUO)~~ The Research and Development department was headed by Mr. E. N. Dingley, Jr., a captain in the U.S. Naval Reserve. A number of R&D positions were located both in the continental U.S. and overseas. [redacted] were charged with search and collection of new signals and the testing of new equipment to cope with the growing technology of the time.

(U) Signals from these collectors were sent to CSAW (I believe the designator at the time was N33). LCDR Fred W. Hitz, USN, was in charge of a number of senior civilian analysts/reporters who reported the findings, verified the analysis and did the tasking. Mr. James Cochrane, and Ms. Nancy Swann were assigned along with several other navy and civilian personnel. CTC Jack Ciska, USN, was the yeoman.

(U) The actual analysis of these signals was performed in N33 under the supervision of Mr. Russell L. Hoepner. The personnel either all Navy veterans or active-duty officers. Among the best were Mr. Edward J. Malone, Mr. Henry Stamps and CWO "Poochie" Jones, USN. I became a member of this team in October 1949.

(U) In late 1949 the military intelligence services (ASA, NSS and now the Air Force's AFSS) joined to become the Armed Forces Security Agency, at which time my organization was renumbered AFSA 334. By this time the volume of material requiring analysis was growing along with the need to process not only printer and time-multiplex systems but a very large input of facsimile. The volume processing of these signals from wire and disc recordings was fast becoming a problem for an organization more concerned with new technology.

(U) In mid-1951 a new organization, under the auspices of Captain Ronald Schmidt, USA,was being initiated at Arlington Hall Station as AFSA 204. The primary function was to do the processing and analysis from SIGINT stations worldwide. I transferred from AFSA 334 to AFSA 204 and, along with Mr. Schmidt and two Army sergeants (one of whose name was Arsenault), began the first signals analysis effort in the Production organization.

~~(S-CCO)~~ Beginning in 1951 the organization withstood a number of reorganizations caused by the increasing number of Soviet signals, processing demands and attempts to find the right fit for this still-misunderstood element. These growing demands also resulted in increased manning. Cap-

DOCID: 4036133
EO 1.4.(c)
P.L. 86-36

tain Schmidt became the civilian chief, Sergeant Richard Gibson, USA, and Mr. Joseph Marenick were added to the group. By this time the increase [redacted] Mr. Hoepner was added to the management team as we built a rather large processing facility in the basement of the cafeteria at AHS. As we grew out of our spaces it was decided to move us to NSS. By this time we had added additional people to perform signals analysis, the master being a retired Navy radioman named William Skinner. We had also divided the functions into processing and analysis, with Skinner the chief by virtue of his experience and talents.

(U) In May 1956 the signals analysis effort returned to AHS, but the processing remained at NSS. We were now COLL-331, soon changed to COLL-221. Eugene E. Embry was the chief of COLL-22 and Bill Skinner of COLL-221. We were assigned to COLL-2 because this was the technical arm of Production, much along the lines of the original Navy organization 334. In late 1956 we returned to NSS from whence we moved to Ft. George G. Meade in 1957. It was not until early 1957 that we were recognized as Signals Analysts by the Civil Service job descriptions. Until then we were Clerks (General), Engineering Aides (Electronic and/or General), Communications Analysts/Specialists and finally Signals Analysts.

~~(FOUO)~~ In February 1958, the signals analysis effort had grown to division size and I was named its first chief. In 1959, since COLL did more than Collection, the title was changed to COSA to reflect the Collection *and* Signals Analysis efforts. It was during this time frame that the extension of the signals analysis effort to the "front end" of the SIGINT system was made. [redacted] was established with Mr. Joseph Sausnock, Jr. assigned as the chief. Mr. Russell "Jose" Rogers performed the same function at the [redacted] Both of these men were ex-Navy personnel who had excellent training and were experienced signals analysts, and who had been section chiefs in COSA-34. From its humble beginnings at AHS, the Signals Analysis career field had taken its place among the best of the best in the intelligence business; J45, Z15 and W34 all trace their roots to AHS.

(U) I remained the chief until August 1967 when I was assigned to the Air War College, at which time Mr. George Jelen replaced me.

EO 1.4.(c)
P.L. 86-36

The Challenge: (U)

~~(S-CCO)~~ The fledging effort in Production (PROD) faced a number of technical challenges in the fifties: a growing number of technology changes on the part of the targets, [redacted]

I became a member of this team in October 1949 [but] it was not until early 1957 that we were recognized as Signals Analysts. Until then we were Clerks (General), Engineering Aides (Electronic and/or General), or Communications Analysts/Specialists.

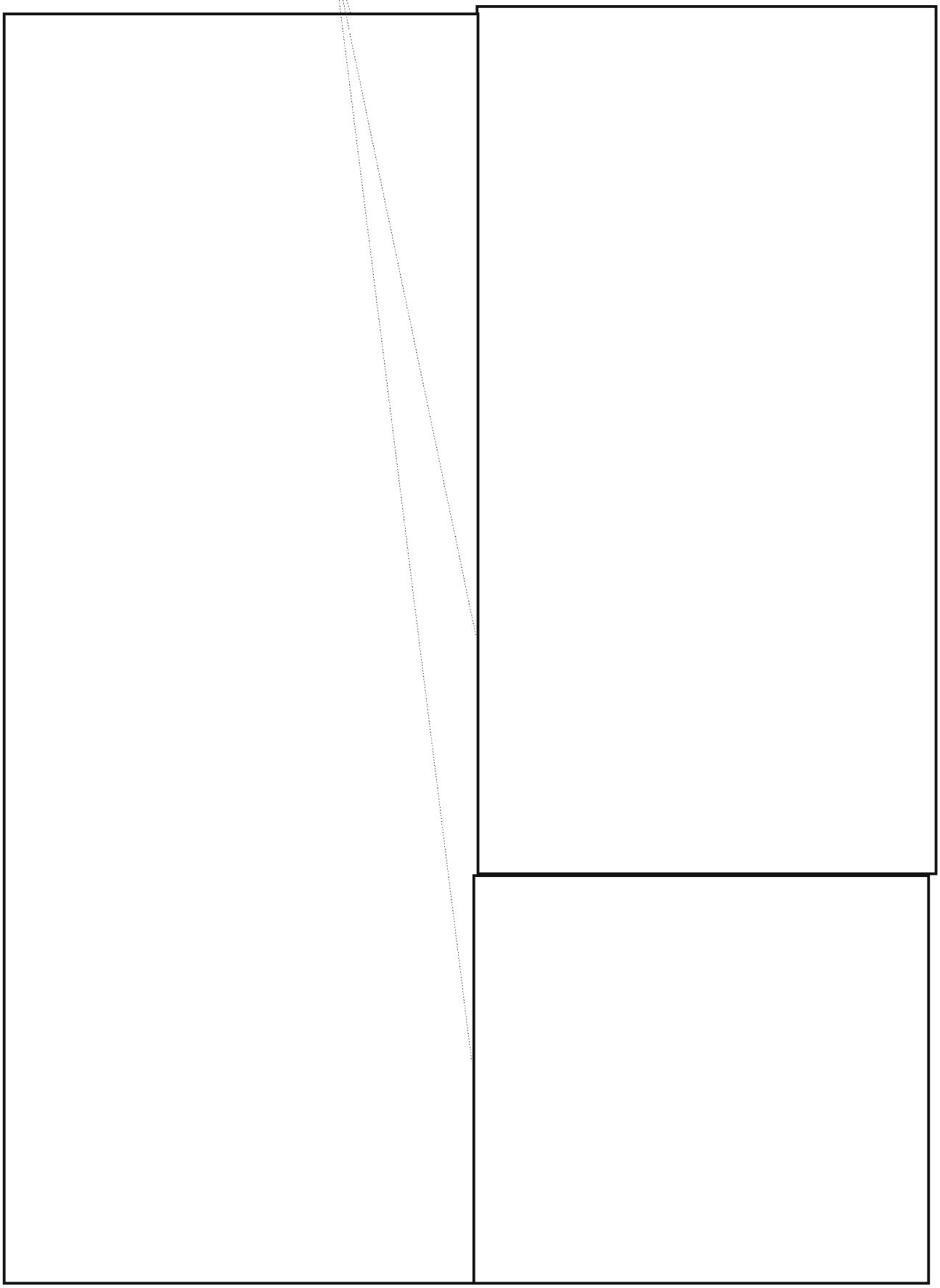
~~(S-CCO)~~ [redacted] this task was levied by the Deputy Director for Operations, Rear Admiral T. R. Kurtz, Jr., USN.

[redacted]

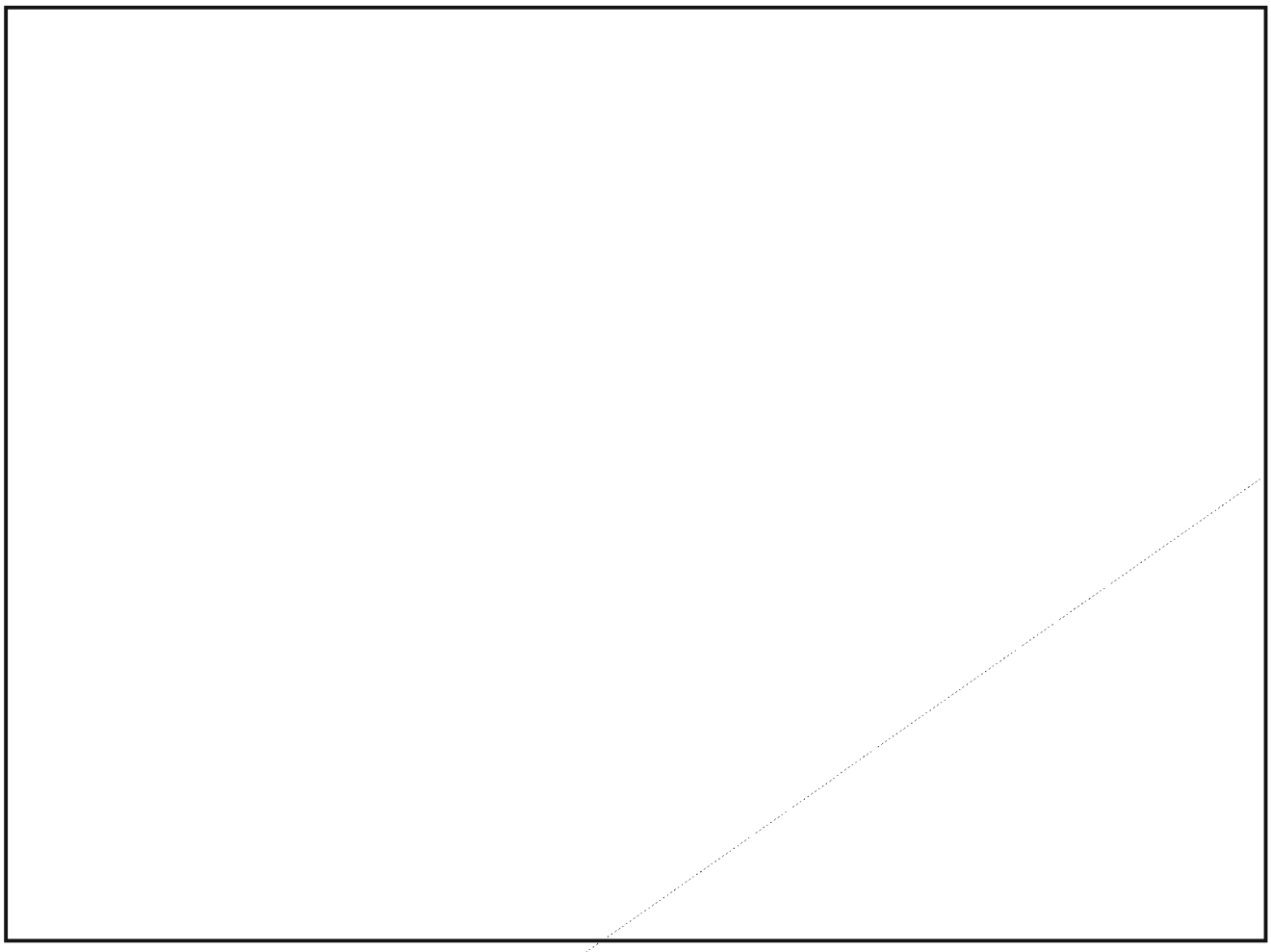
EO 1.4.(c)
P.L. 86-36

DOCID: 4036133

EO 1.4.(c)
P.L. 86-36



DOCID: 4036133

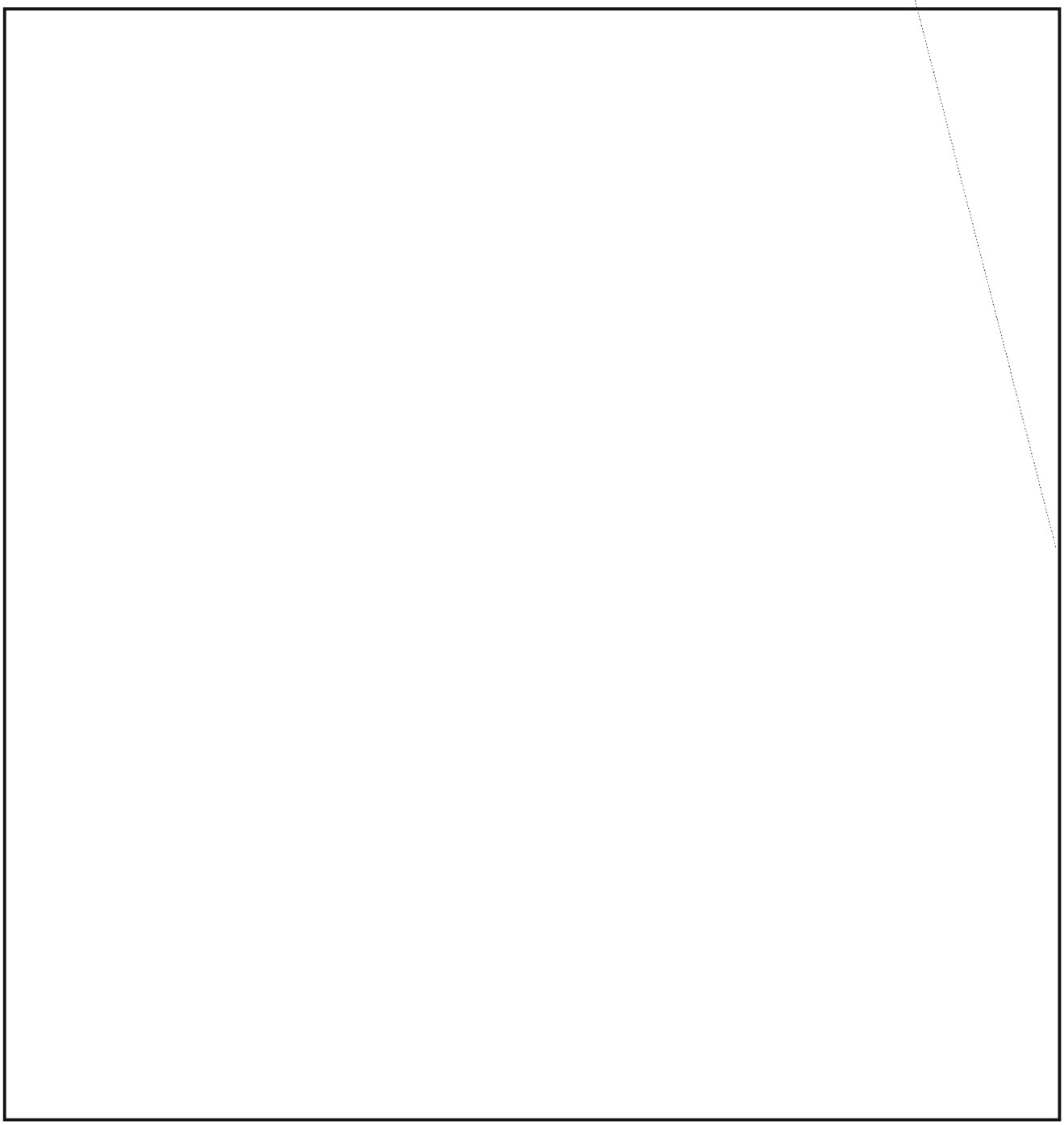


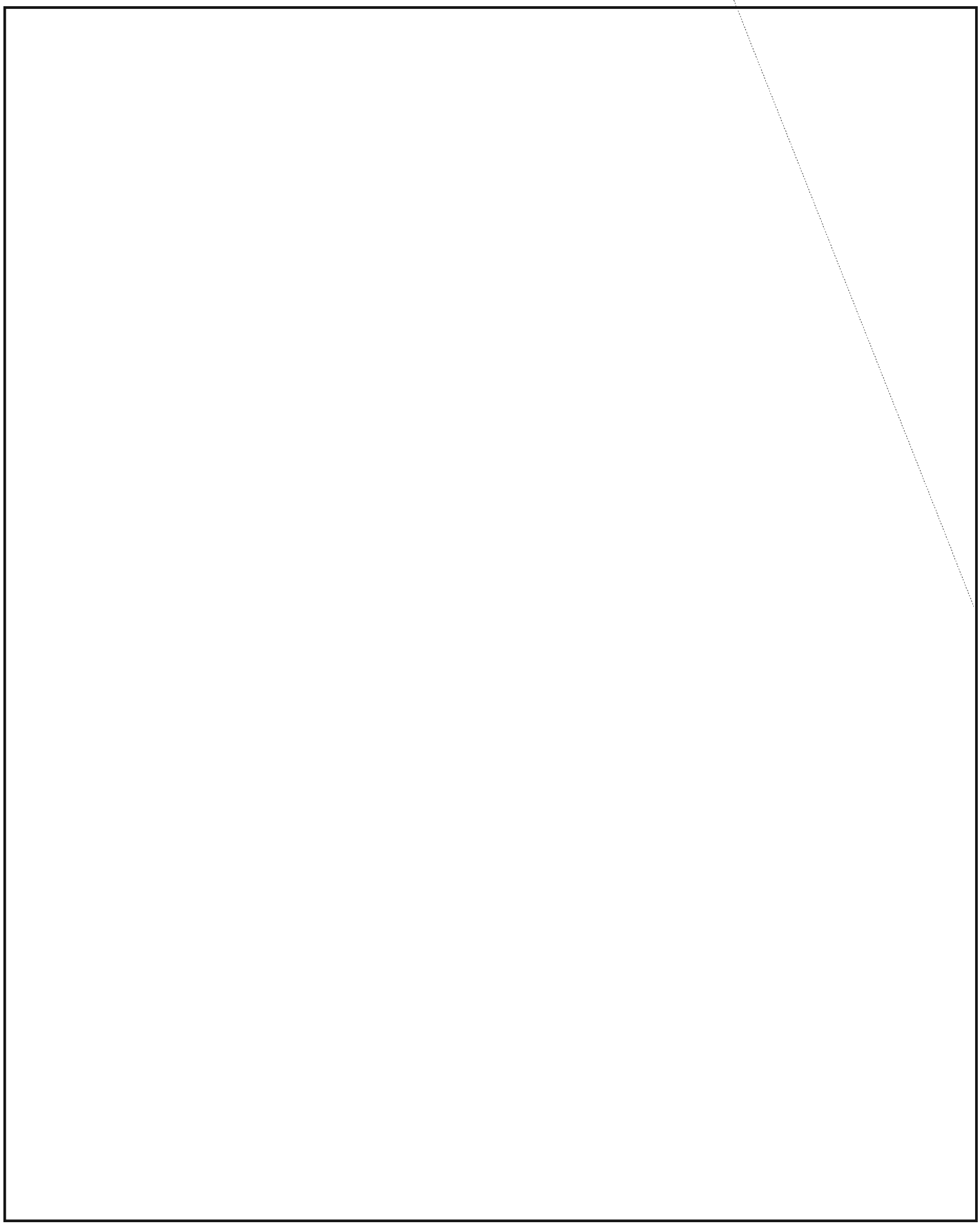
EO 1.4.(c)
P.L. 86-36

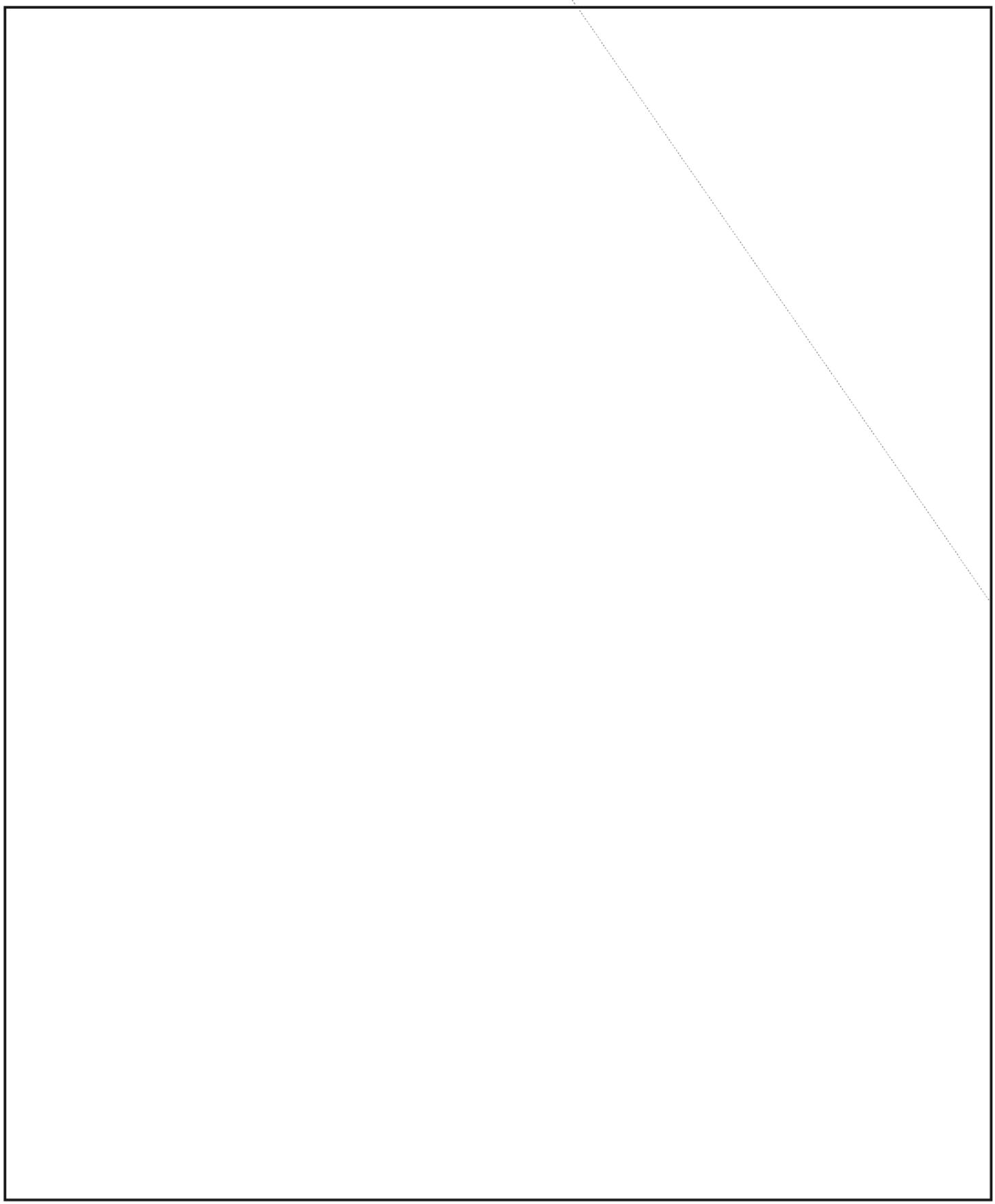
An Example of Intelligence Community Synergy

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

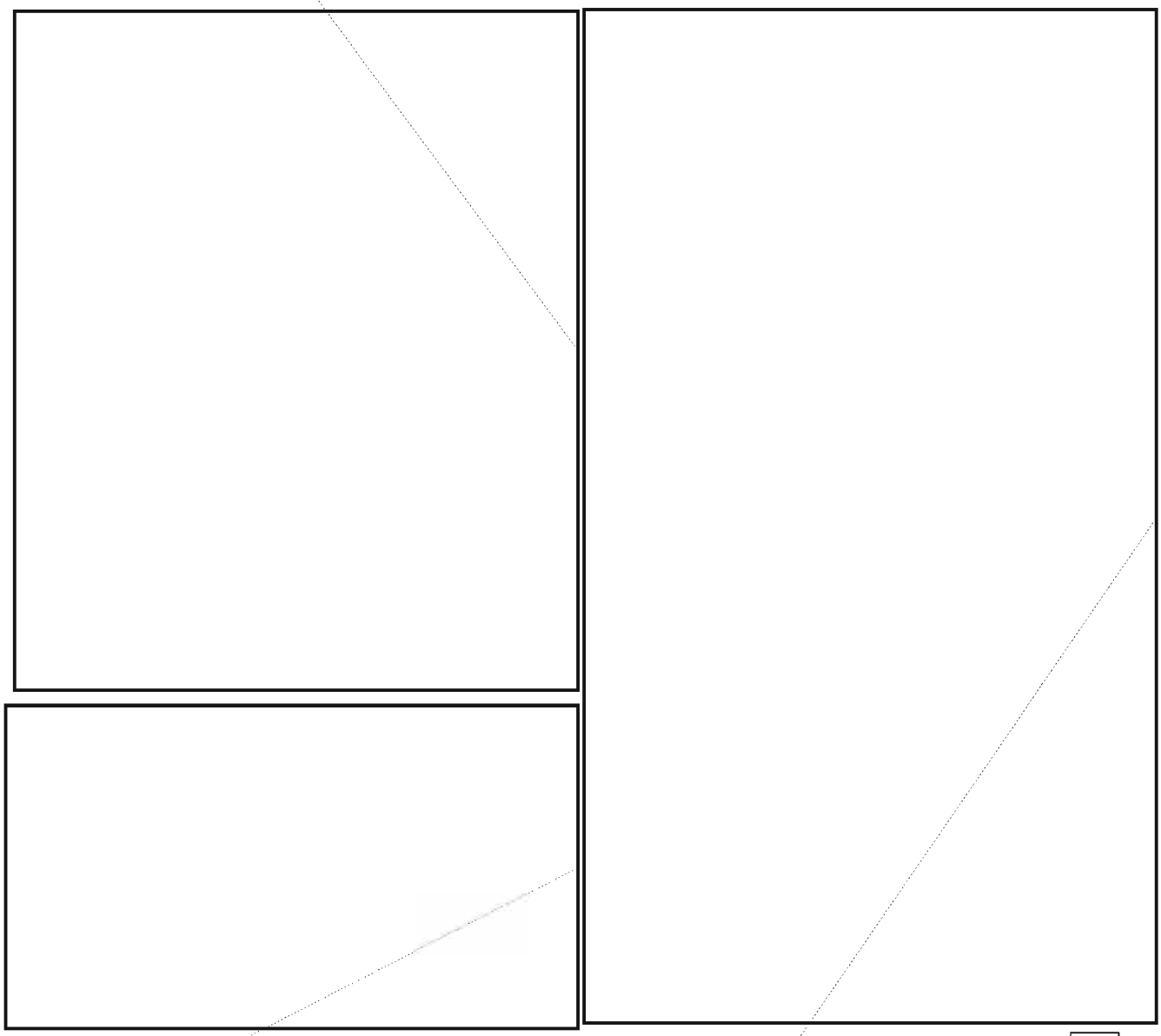






~~TOP SECRET~~

EO 1.4.(c)
P.L. 86-36



Κλ

P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)

DOCID: 4036133

SENTINEL: A Look at Database Security ~~(FOUO)~~

by [redacted]

P.L. 86-36

(U) The need to store data classified at many different levels in one database prompted the creation of the SENTINEL database security filter. Managers, analysts and collectors at NSA need to make decisions based on data from many different sources and classification levels. With shrinking budgets and personnel cuts, individuals are expected to manage more information and make broader decisions than in the past.

Approaches to security (U)

(U) The most secure solution to the database security issue is to start at the ground level. Acquire a secure operating system, such as Trusted Solaris, as the foundation. Next place a secure relational database management system on top of this to form a completely secure system. Unfortunately, this solution is more expensive, harder to use, and more difficult to administer than a traditional operating system and database management system. In addition to cost and usability, this solution requires you to supply all the users of your system with the same configuration, which incurs further cost.

(U) Another solution, and the one taken by SENTINEL, is to take a traditional operating system such as SunOS, Solaris, or AIX and use a traditional database management system such as SYBASE. This solution is not as secure as the one mentioned above but fits into the existing computer architecture, which does not include trusted operating systems and database management systems. SENTINEL was created to prevent accidental data disclosure but not a malicious attack.

What is SENTINEL? (U)

(U) SENTINEL is a security filter for SYBASE databases which provides multi-level security down to the row level. SYBASE alone provides security at the table level, but this is not good enough for SENTINEL's users, who demand finer granularity down to the row level. For those not familiar with relational database management systems, the composition of today's relational database management systems consist of application databases at the top. Databases are composed of tables and tables are composed of rows. SENTINEL insures a user will only see the rows of data for which he/she is cleared to access.

(U) The SENTINEL security filter is an integral part of project PLUS. PLUS has 1600 users worldwide located at the CSGs, RSOCs, field sites, other Key Components and DO. PLUS gives users feedback about SIGINT production as a whole and where they fit into the SIGINT production system. SENTINEL is used in [redacted] and a Second Party project called [redacted].

(U) SENTINEL has been certified by J06 at the C2 level for in-house use. The C2 criteria can be found in the Orange Book. For the full criteria, go to **http://nectarine.q.nsa/REGS/rainbow/**

orange on the NSA network. For those not familiar with the Orange Book criteria, D is the lowest or least secure level and A is the highest or most secure level with C and B in between.

How it works (U)

(U) SENTINEL is a SYBASE Open Server application program that runs between the user application, or client, and the backend SYBASE server program. It acts like a watchdog in front of the user's application database preventing unauthorized access to data. SENTINEL intercepts each Structured Query Language (SQL) request sent to the SYBASE server, modifies the request by adding the appropriate security information and forwards the modified request to the SYBASE server for processing. Once SYBASE receives this modified SQL request, it processes the request and sends the results back through SENTINEL, in pass through mode, to the user process. Pass through mode means the data is unaltered.

(U) The SENTINEL database is used to store all the pertinent security information about users, what databases they have access to and the clearance level of the databases. Storing the user classification in a separate location from the data classification is a characteristic of secure systems. Again, consult the Orange Book for more information. The SENTINEL database can be updated manually or automatically. An example of the automatic mode can be found in Project PLUS which has written a program to query the SPECLR clearance database nightly and transfer that information to the SENTINEL database. In this mode, SENTINEL will have current security information about its users. It will know, for instance, if a user has lost the TK clearance from one day to the next.

(U) SENTINEL will have current security information about its users. It will know, for instance, if a user has lost the TK clearance from one day to the next

(U) SENTINEL expects a security label to be attached to every row in a database and to every database user. This label contains three components: a hierarchical component for storing clearance information such as Top Secret, Confidential, etc.; a privacy component which restricts releasability privileges; and a compartment component which stores need to know items such as TK, VRK, BYEMAN, etc. The clearance component can store 16 different combinations of mnemonics. The privacy component supports a maximum of 32 privacy labels. The compartment component supports a maximum of 1024 compartments. These components are stored as bit mapped fields where each bit or pattern of bits corresponds to a mnemonic such as TK, VRK, SECRET etc. The decision to store this information as bits was developed in the interest of space and speed. Since a bit, which can either be a 1 or a 0, is the smallest unit in a computer, it does not take up much space. Manipulation of bits in a computer is also very fast.

(U) At the heart of SENTINEL is the SQL parser. It breaks SQL statements down into separate components which are then passed to the processing module of SENTINEL. This processing module inserts limiting information, derived from the SENTINEL database, about the user into the user's SQL and then forwards the modified SQL on to the SYBASE server for processing. For instance, a user query might say something like, "I want to see all rows in the employee table." SENTINEL modifies that query to say "I want to see all rows in the employee table that are at my clearance level," or, more specifically, "I want to see all rows in the employee table that are Top Secret or below, TK and VRK." The information used to modify the query comes from the SENTINEL database.

(U) In addition to the row level security provided by SENTINEL, other security features are in place. The first restriction SENTINEL imposes is no user accounts on the backend SYBASE server. We don't want an ordinary user to bypass SENTINEL by logging on to the backend database to access information. Users log in to SENTINEL using their unsecured Agency SID and password. SENTINEL uses this account to retrieve the sid and password of the user's secured account. Using this information, a secured connection is established, the unsecured connection is terminated and

DOCID: 4036133

the password to the secured account is changed. This level of security differentiates between a user's access to a database in secured mode versus access to a database in an unsecured mode. Access to secured databases is granted to a user through the secured sid. Attempts to use a secured database under an unsecured SID will be prevented by the SYBASE server's database level access control mechanism.

(U) One of the main reasons SENTINEL only works with the SYBASE relational database management system is that it is the only widespread database management system at the Agency that supports bit manipulation. There are other products on the market that perform database security such as ORACLE's Row Level Security product, but this requires developers to purchase ORACLE whereas SYBASE is essentially "free" since NSA has a site license for SYBASE.

SENTINEL Operation (U)

(U) SENTINEL runs in the background, which means there is nothing to see. It has no user interface, so you will never see a SENTINEL icon on your computer screen. SENTINEL operates in two modes. In the first mode, developers can include SENTINEL library "C" language modules in their "C" programs to create their own custom applications that are secure. This is what project PLUS has done. The last method to access SENTINEL is through the use of stored procedures. Stored procedures are collections of SQL statements used to perform a task or set of tasks designated by the user. These stored procedure calls can be sent to SENTINEL through a "C" language program or an ISQL session. An ISQL session allows its user to type and send SQL without having to know a programming language such as "C". This last mode provides the greatest flexibility because it allows a user to send any allowable SQL and receive results instantly while still being assured they will receive only the data for which they are cleared. In addition to the standard SYBASE stored procedures, the SENTINEL developers have added many security specific stored procedures. These stored procedures allow the user to set and retrieve their clearance, privacy and compartment levels within allowable bounds. A user is allowed to downgrade their clearance level to give a demo, for instance, but is never allowed to raise their clearance level beyond that which is set by the SENTINEL administrator.

Conclusion (U)

P.L. 86-36

(U) The long-range goal of database security is to have a product that can access many different types of databases, not just SYBASE. This product would not greatly hinder the performance of database retrievals and updates. It would also require minimal updates to the user's application to take advantage of the security aspects. Until such an application is found, SENTINEL is here to fulfil the database security requirement.

~~(FOUO)~~ Mr. [redacted] started his Agency career twelve years ago as a computer analyst in the R directorate. Since then, he has worked in a variety of areas from contracting officer's representative (COR) to software development and system support. He currently works in E223 as the SENTINEL project leader. When the weather is nice, Mr. [redacted] can be found riding his bicycle. He would like to thank [redacted] and [redacted] for their enhancements to this article.

Kλ

~~FOR OFFICIAL USE ONLY~~

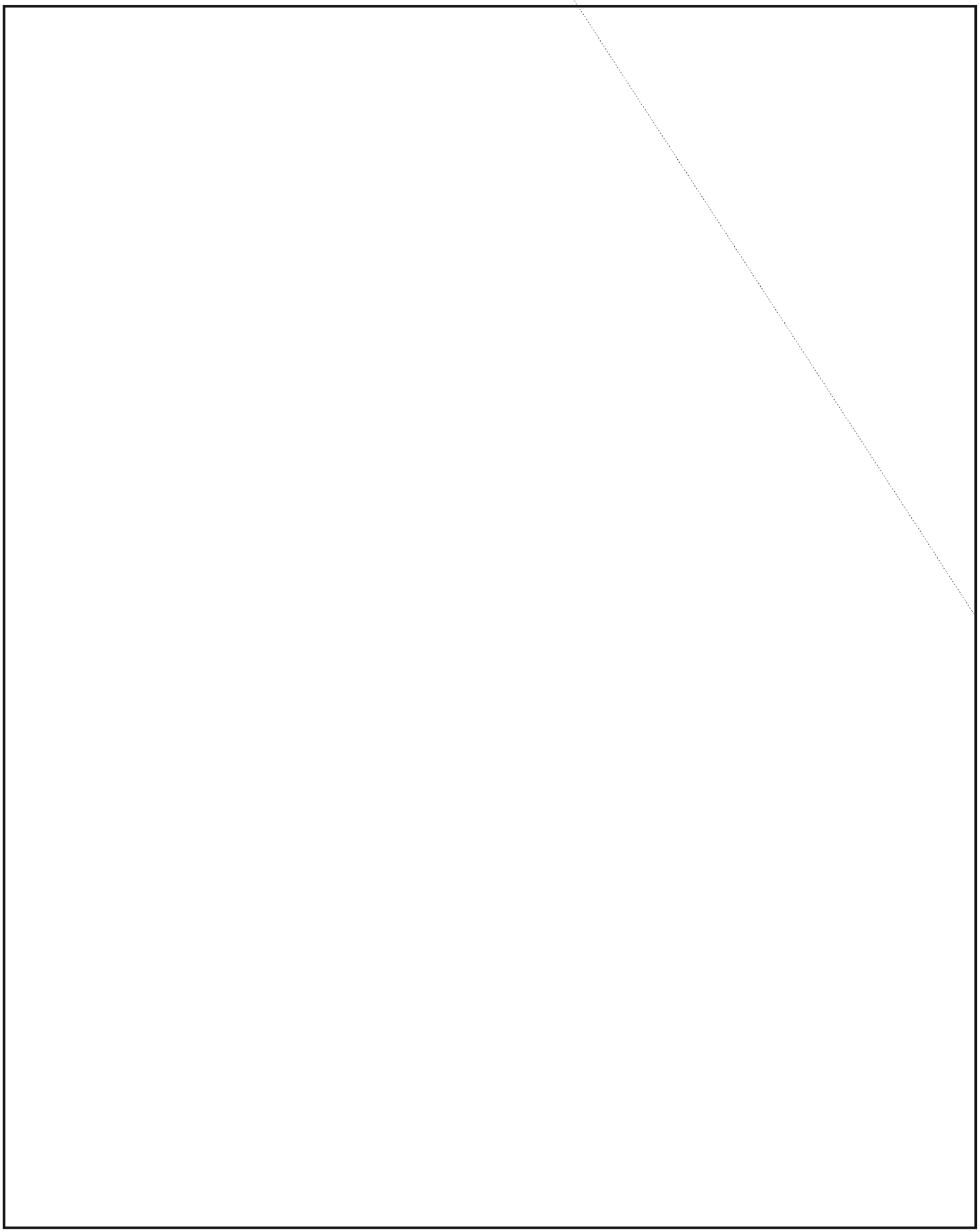
~~TOP SECRET UMBRA~~

EO 1.4.(c)
P.L. 86-36

by [redacted] P.L. 86-36

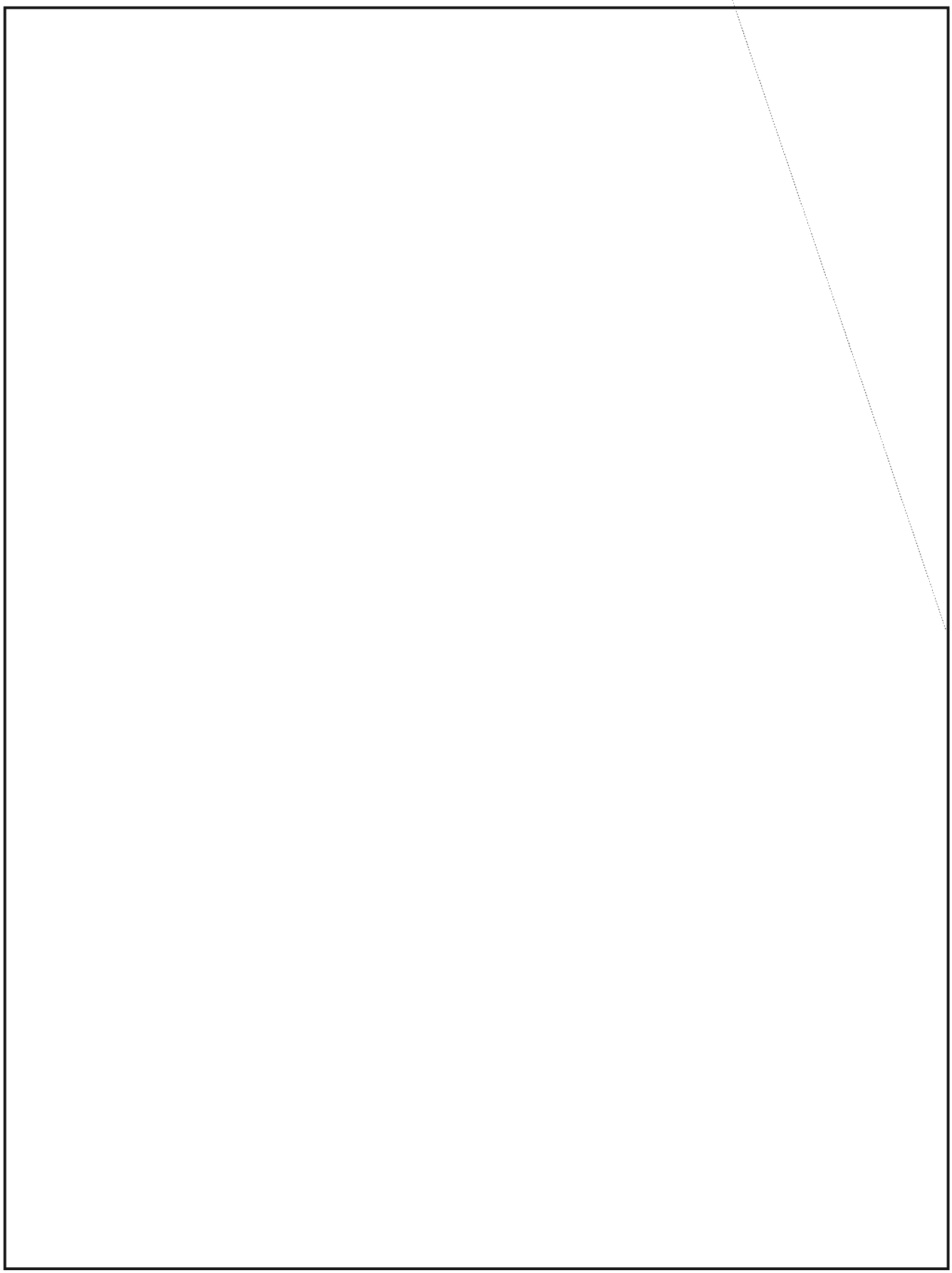
[redacted]

EO 1.4.(c)
P.L. 86-36

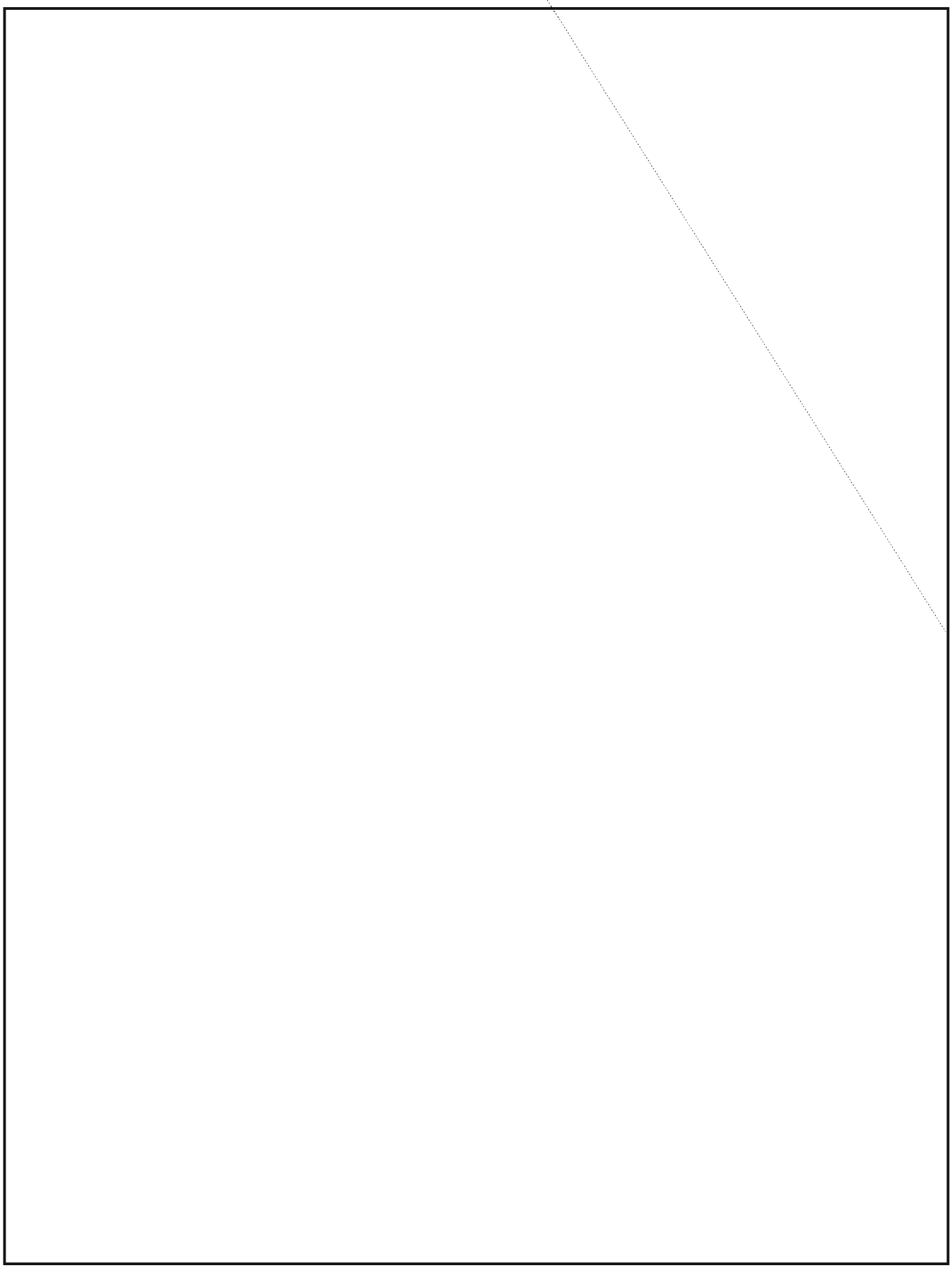


~~TOP SECRET UMBRA~~

EO 1.4.(c)
P.L. 86-36

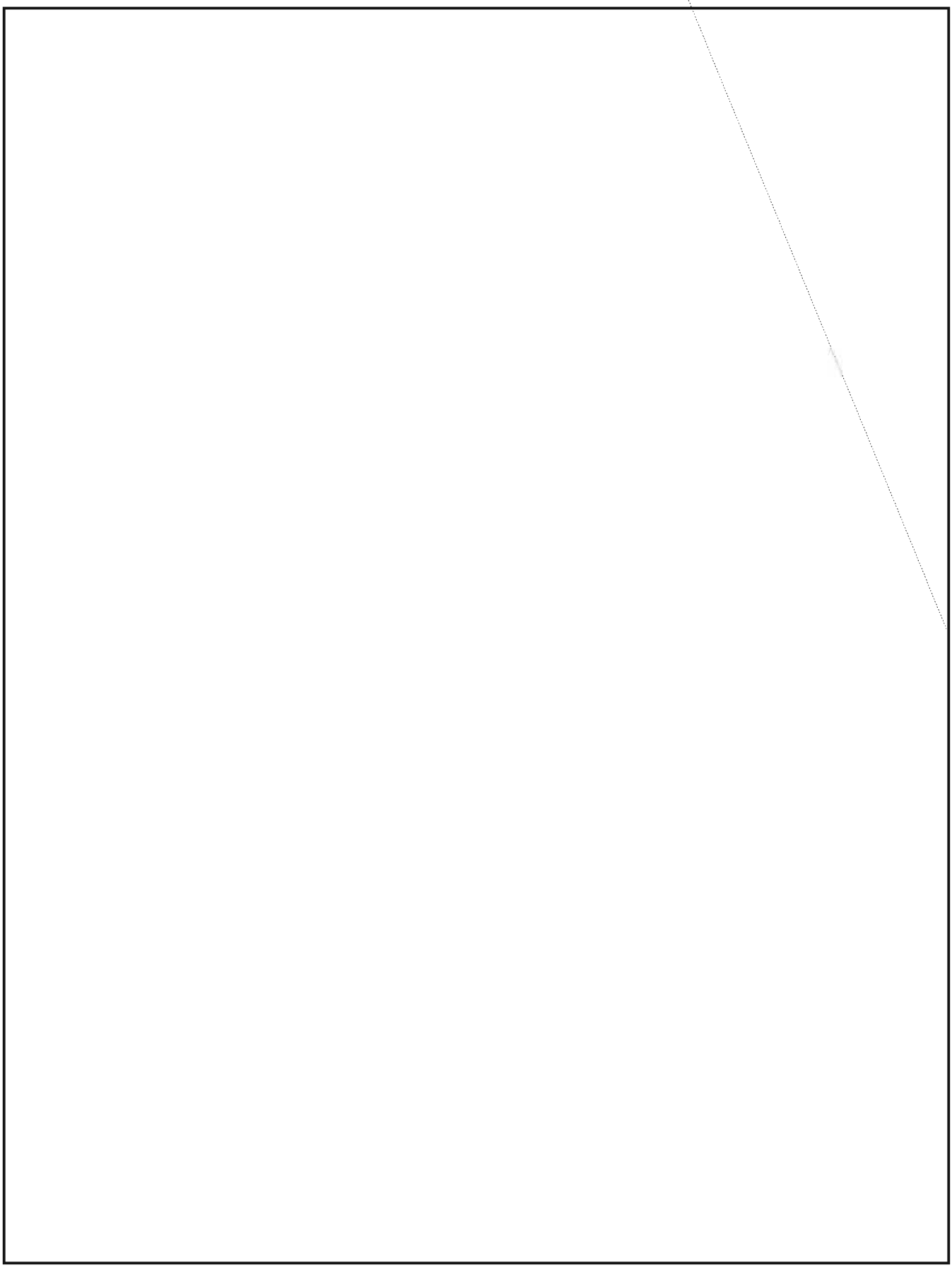


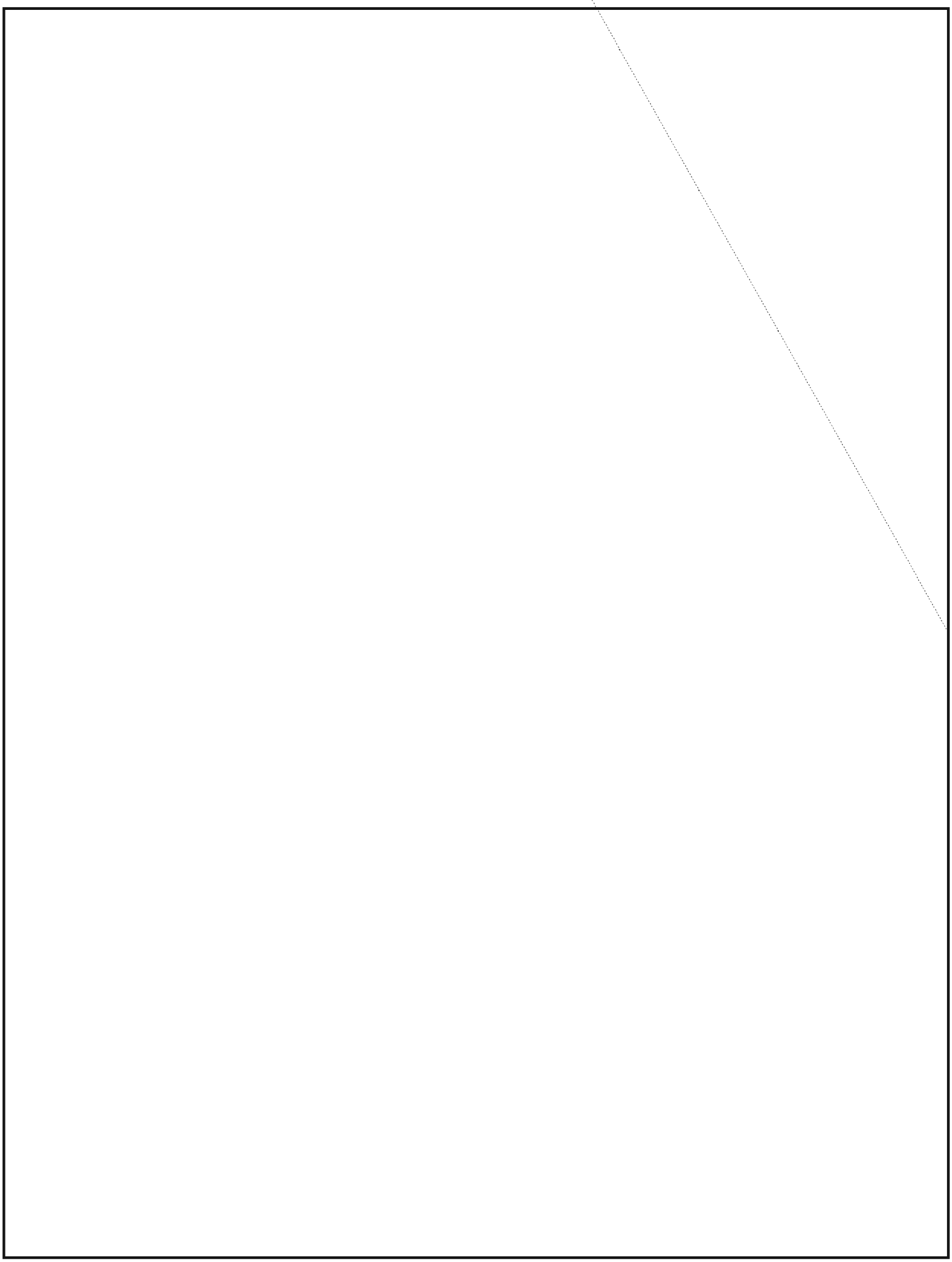
EO 1.4.(c)
P.L. 86-36



DOCID: 4036133

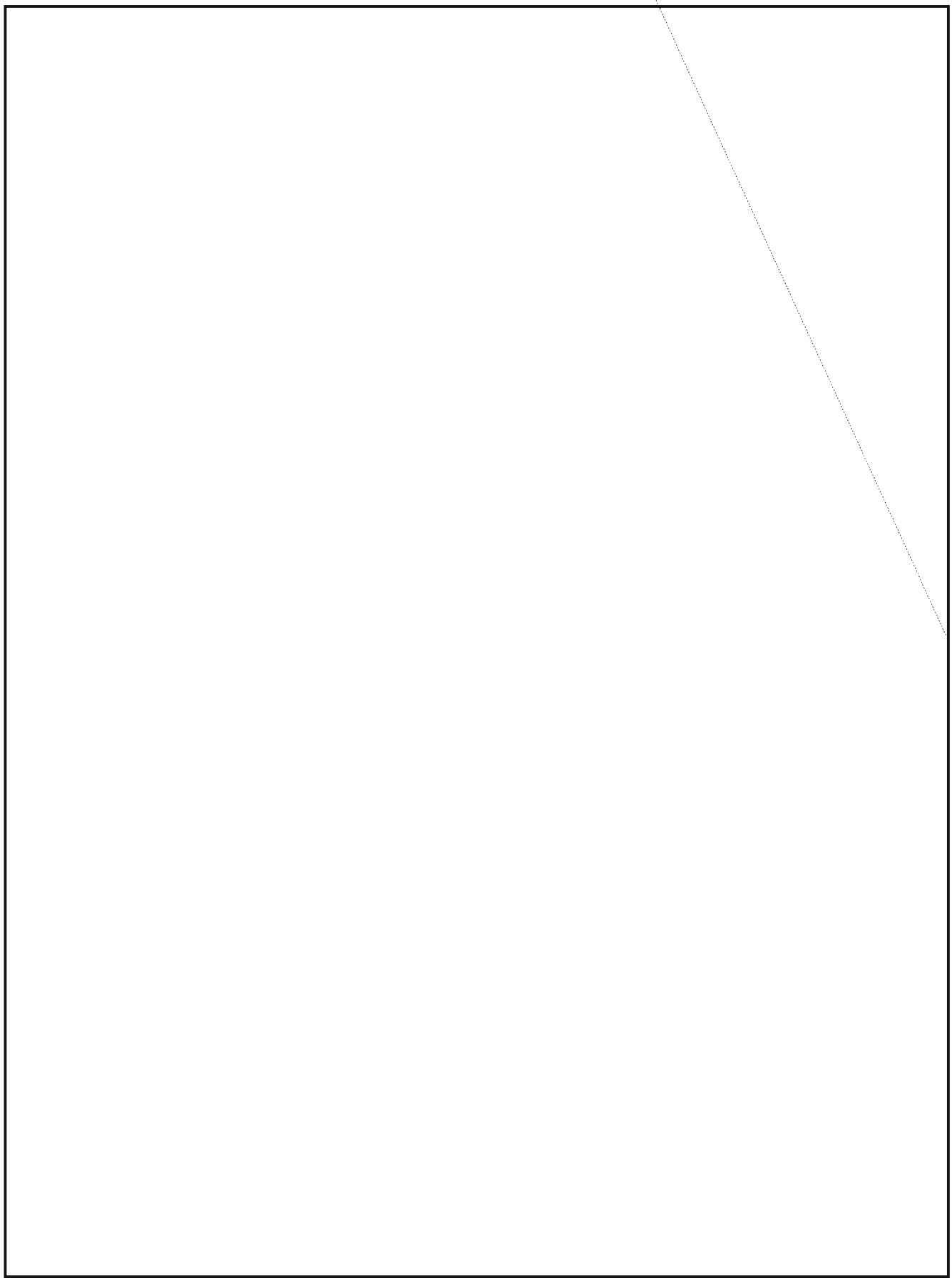
EO 1.4.(c)
P.L. 86-36





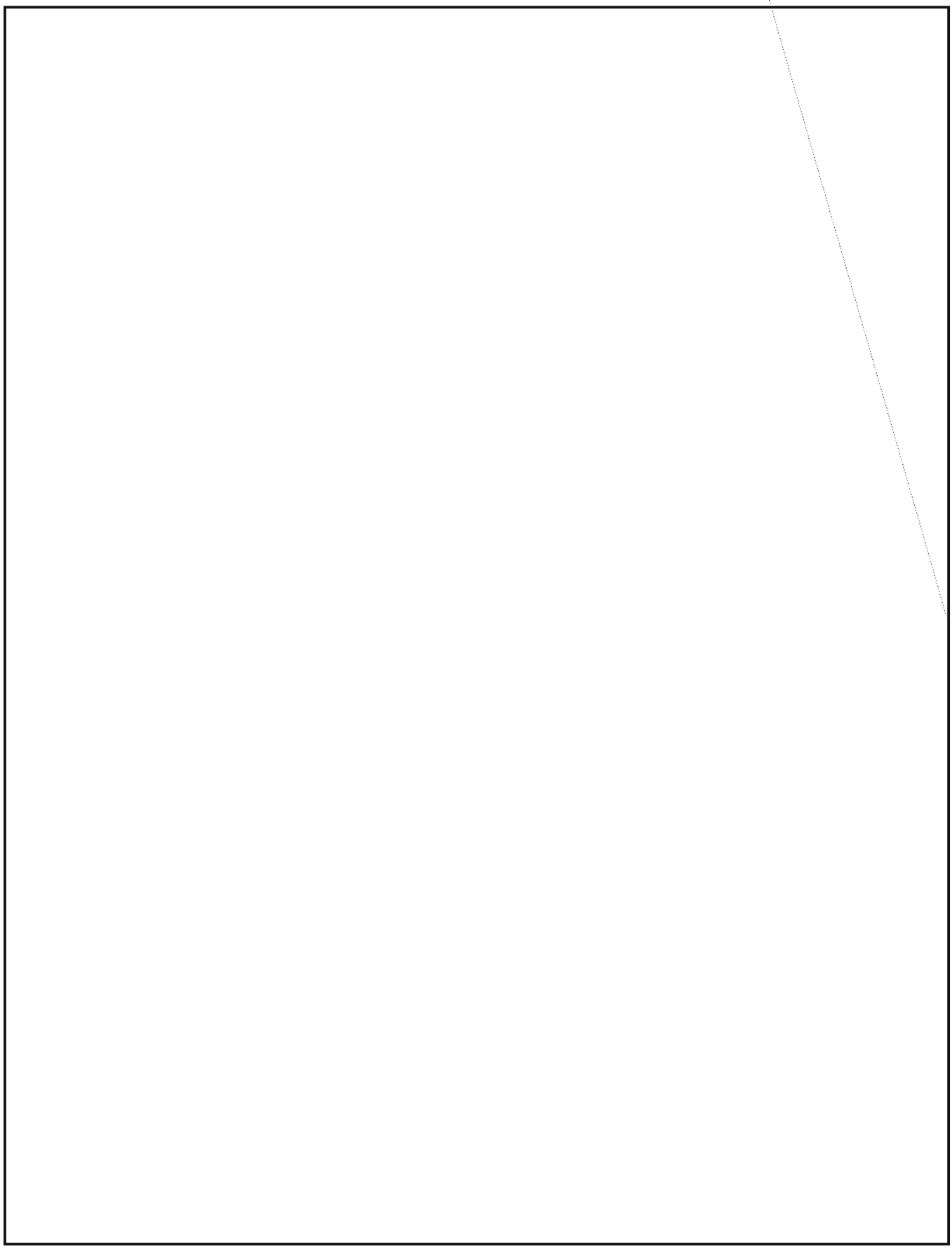
DOCID: 4036133
CRYPTOLOG
Summer 1997

EO 1.4.(c)
P.L. 86-36

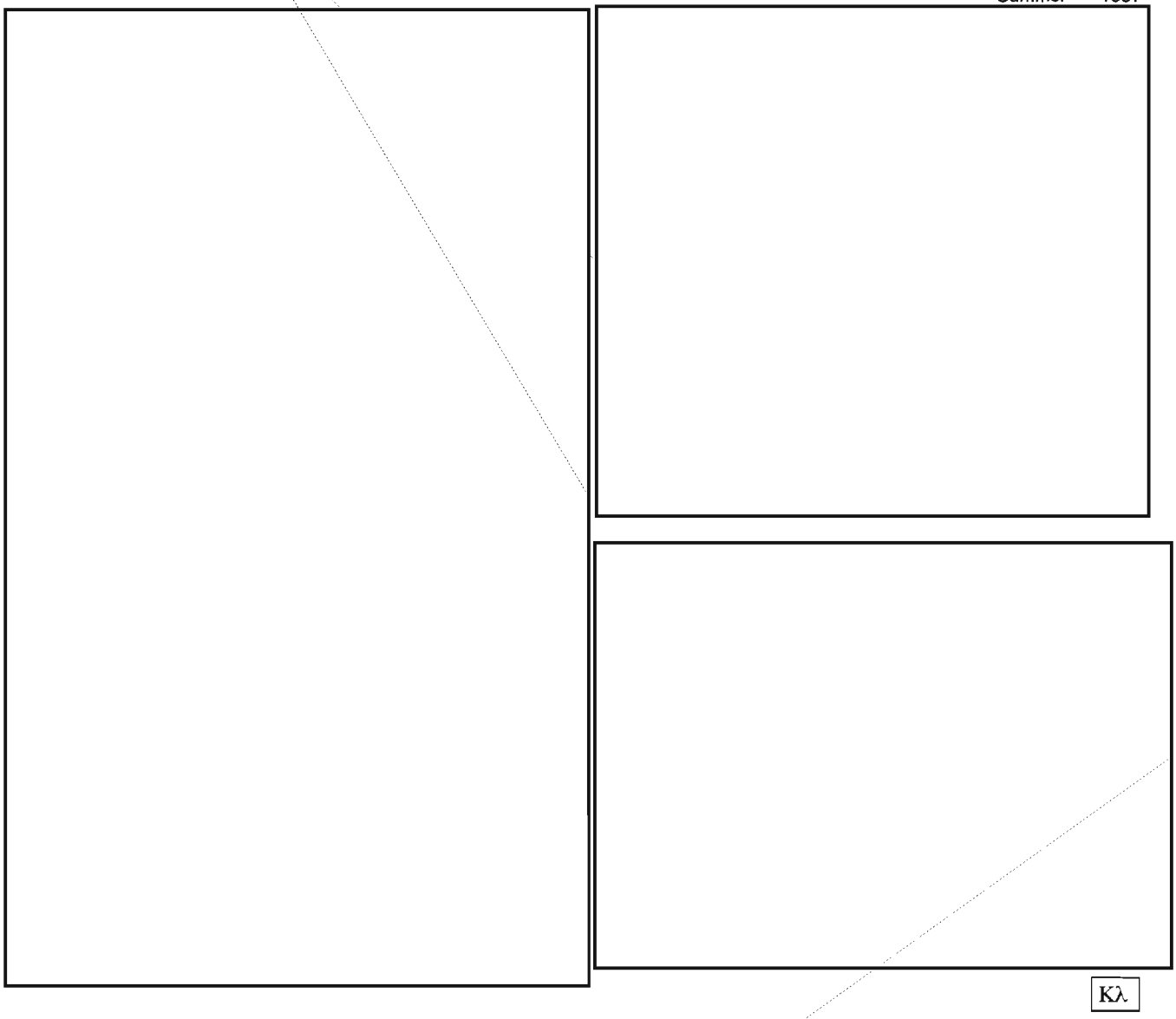


DOCID: 4036133

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

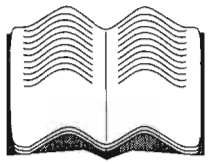


Kλ

P.L. 86-36
EO 1.4.(c)

DOCID: 4036133

Book Review (U)



Steve McConnell. Rapid Development
Redmond: Microsoft Press, 1996. 647 pp.

Reviewed by [redacted] P.L. 86-36

(U) Steve McConnell is chief software engineer at Construx Software Builders, Inc., a Seattle-based software development corporation. He is the author of *Code Complete*, as well as the editor of IEEE Software's "Best Practices" column.

(U) *Rapid Development* is a very well-organized, easy-to-follow book. Icons, specifying such things as best practices, hard data, classic mistakes, further reading and cross-references are placed in the margins. The bibliography is impressive: over 200 references to classic software articles and books, such as Yourdon's *Modern Structured Analysis*, Booch's *Object-Oriented Analysis and Design: With Applications*, even Tom Peters' *Thriving on Chaos: Handbook for a Management Revolution*. Each chapter concludes with a further reading section, which reflects the resources McConnell used for that particular chapter. He uses case studies involving a mythical software development organization, Giga-Safe, which builds business-oriented tools. These case studies show the right and wrong way to manage a program, using very close-to-life examples. As with Scott Adams of *Dilbert* fame, you get a feeling that Mr. McConnell has worked as a software developer for the National Security Agency.

(U) Do you as a software developer want to try to avoid such things as "feature creep" (a.k.a. "requirements creep)", code-like-hell programming, insufficient or inadequate planning, omission of tasks, or unrealistic expectations? Then this is the book you should take time out from your hectic schedule to read.

(U) The subtitle of *Rapid Development* is *Taming Wild Software Schedules*. In Part I of this three-part book, "Efficient Development," Mr. McConnell does a tremendous job of laying out the pitfalls of what he terms the "slow-development" problem and from there shows the path to Rapid Development. He states very succinctly that the slow-development problem pervades the software industry and describes it in a Summary of 36 Classic Software Mistakes, under four sub-headings: People-Related, Process-Related, Product-Related, and Technology-Related Mistakes. In other words, the classic problems that affect your wild software schedule. Additionally, the first part covers the following topics, with a chapter devoted to each: Rapid-Development Strategy; Classic Mistakes; Software Development Fundamentals; and Risk Management.

(U) Part II, "Rapid Development," covers what should be done by Program Managers and Team Leaders to migrate from slow to rapid development by showing the reader how to plan a project from start to finish, how to avoid the classic mistakes, how to build a team, choosing a life-cycle (Spiral, Evolutionary, Staged Delivery, etc.), and how to mitigate risk. He uses pictures, graphs, cartoons, diagrams, statistics, flow charts, and even a dinner menu to illustrate his points. This section covers Core Issues in Rapid Development; Lifecycle Planning; Estimation; Scheduling; Customer-Oriented Development; Motivation; Teamwork; Team Structure; Feature Set Control; Productivity Tools; and Project Recovery. The two chapters devoted to teamwork and team structure are especially informative.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4036133

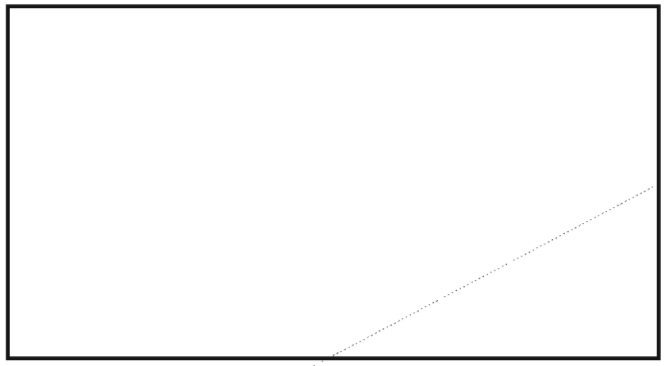
(U) Part III, "Best Practices," finishes the book with a summation of 27 simple yet effective tools to build a quality software product. These practices include: Change Board; Daily Build and Smoke Test; Designing for Change; Evolutionary Delivery; Evolutionary Prototyping; Goal Setting; Inspections; Joint Application Development (JAD); Lifecycle Model Selection; Measurement; Miniature Milestones; Outsourcing; Principled Negotiation; Productivity Environments; Rapid-Development Languages; Requirements Scrubbing; Reuse; Signing Up; Spiral Lifecycle Model; Staged Delivery; Theory-W Management; Throwaway Prototyping; Timebox Development; Tools Group; and Top-10 Risks list.

(U) It's been said that the beginning of a solution is realizing just what the problem is. *Rapid Development* shows how to solve problems incrementally. It is a step-by-step reference on how to go from slow development to rapid development; this will show the path to better software engineering and how to deliver a quality product on time and within budget to a satisfied customer.

(U) You would think that a book about software development strategy would be rather dry reading, but Mr. McConnell adds a bit of humor to the text by comparing things like Classic Software Mistakes to watching reruns of *Gilligan's Island*.

(U) The main target audience for this book is the Technical Leaders of software development efforts, however, the book should also be used by supervisors and managers of Technical organizations to understand what their Team Leaders are talking about. The goal of the work is well-stated in the Preface: "[to] lay out in pragmatic terms why many of our most common views about rapid development are fundamentally broken...and to advocate its own small revolution in software-development practices." And that goal has not only been met, but met very well.

(U) I highly recommend this book as the next much-highlighted, marked-in-the-margins, dog-eared, no-you-cannot-borrow-it-get-one-of-your-own books for every software developer, team leader and technical manager.



Kλ

P.L. 86-36

DOCID: 4036133

Editorial Policy:

(U) Technical articles are preferred over those relating to management, shorter over longer (under 3,500 words). Emphasis should be on improving NSA's technical performance; articles should be aimed at explaining developments in one's career field to those outside it. Readers are invited to contribute conference reports and reviews of books, articles, software, and hardware that relate to our missions or to any of our disciplines. Editorials are also welcome, as is humor. Submissions may be published anonymously, but the identity of the author must be known to the editor.

Submitting Articles:

(N.B. If the following instructions are a mystery to you and your local ADP support is no help, please feel free to contact the CRYPTOLOG editor on 963-5283s or cryplog@p.nsa.)

~~(FOUO)~~ Send a soft copy via e-mail to **cryplog@nsa**, or send a hard copy accompanied by a labelled diskette to the editor at P02 in 2C099, Ops. 1.

Guidance:

For maximum efficiency (as far as possible within the limits of your word processor):

- Classify all paragraphs.
- Do not type your article in capital letters.
- Label all diskettes, identifying hardware (operating system: DOS, UNIX), density and type of word processor used, filenames, your name, organization, building, and phone number.
- FrameMaker format is preferred; ASCII text is also fine. *(FrameMaker users: while we welcome graphics, please include them in the file as separate objects rather than in Anchored Frames as these frames are nearly impossible to reformat to our standard.)* The editor will be happy to e-mail a CRYPTOLOG template on request. Another option is to use J33's document conversion service (CLEANEX); instructions for e-mailing files for coversion can be found at **http://www.j33.j.nsa/q6/q623/cleanex/clean.html**.

DOCID: 4033695

SUPPORT

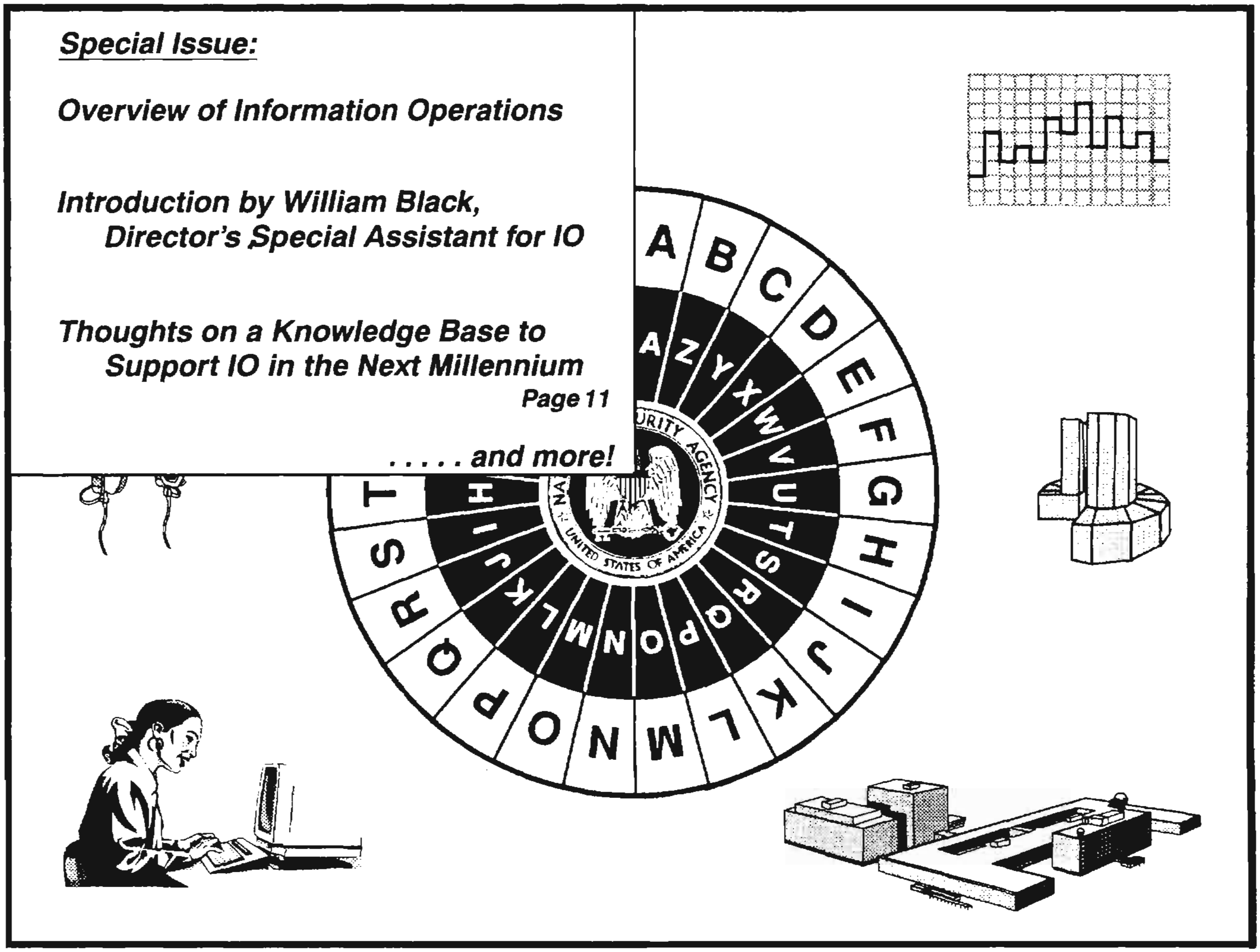
~~TOP SECRET UMBRA~~

NATIONAL SECURITY AGENCY

CRYPTOLOG

The Journal of Technical Health

Vol. XXIII, No. 1 SPRING 1997



Special Issue:

Overview of Information Operations

Introduction by William Black, Director's Special Assistant for IO

Thoughts on a Knowledge Base to Support IO in the Next Millennium

Page 11

..... and more!

~~Derived From: NSA/CSSM 123-2~~
~~Dated 3 September 1991~~
~~Declassify On: Source Marked "OADR"~~
~~Date of source: 3 Sep 91~~

~~REL AUS CAN NZ UK~~

~~TOP SECRET UMBRA~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, NSA Case # 54778

DOCID: 4033695

CRYPTOLOG

Spring 1997
Vol. XXIII, No. 1

Published by P02, Operations Directorate Intelligence Staff

Publisher ..... William Nolte (963-5283)

Guest Editor ..... William Black
Editor..... [redacted] (963-5283)

P.L. 86-36

Board of Advisors

Chairman..... [redacted] (963-7712)
Computer Systems ..... [redacted] (961-1051)
Cryptanalysis..... [redacted] (963-7243)
Intelligence Analysis..... [redacted] (968-8211)
Language..... [redacted] (963-7667)
Mathematics..... [redacted] (963-1363)
Signals Collection ..... [redacted] (963-5717)
Telecommunications ..... [redacted] (996-7847)
Member at Large..... [redacted] (968-4010)
Member at Large..... [redacted] (968-4010)
Member at Large..... [redacted] (961-8214)

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

To submit articles and letters, please see last page.

DOCID: 4033695

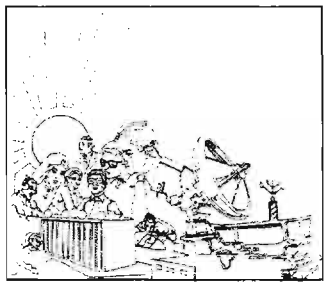


Table of Contents

Thinking Out Loud About Cyberspace (U), by Bill Black 1

IO, IO, It's Off To Work We Go... (U), by [redacted] 5

The Infowar Revolution(s) (U), by [redacted] 10

The Role of Information Warfare in Strategic Warfare (U), by [redacted] 20

Thoughts on a Knowledge Base To Support Information Operations In the Next Millennium (U), by [redacted] 28

Information Operations Training (U) by [redacted] 38

P.L. 86-36

THINKING OUT LOUD ABOUT CYBERSPACE (U)

by William B. Black, Jr.
Director's Special Assistant
for Information Warfare

INTRODUCTION (U)

~~(S REL AUS CAN NZ UK)~~ On 3 March 1997, the Secretary of Defense officially delegated to the National Security Agency the authority to develop Computer Network Attack[1] (CNA) techniques. This delegation of authority has added a new, third dimension to NSA's "one mission" future. That is, in the networked world of Cyberspace, CNA technology is the natural companion of NSA's exploit and protect functions. This delegation of authority is sure to be a catalyst for major change in NSA's basic processes and its workforce. The end result, however, should remain information technology-derived products, services, and experts.

(U) The articles following this introduction were written by the staff of the Director's Special Assistant for Information Warfare. Because confusion still surrounds the emergence and history of Information Warfare (IW), these articles are intended to contribute to the common understanding of why Information Operations and its concepts are important to the future of NSA.

1. DoDD 3600.1, Information Operations, dated 09 December 1996, defines CNA as "operations to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves."

A HISTORICAL PERSPECTIVE (U)

(U) After World War II, an understanding of the core competency underlying the making and breaking of codes — cryptology — resulted in a national decision to consolidate both activities in one organization: NSA. Both activities benefited from this consolidation, and became stronger.

~~(S REL AUS CAN NZ UK)~~ Since the end of the Cold War, in an emerging networked world, an understanding of the emergence of a new core competency — "cyberology" — with its close technological relationship to cryptology has again resulted in a national decision to consolidate. Cyberology's central activities, i.e., "exploitation," "protection," and "attack," will be worked together, thus benefiting all of them.

SETTING THE STAGE (U)

(U) There are certain assumptions that underpin the thought processes related to preparing for our Agency's future in cyberspace. These are premises that are basic to the understanding, the preparations, and the acceptance of major changes. The following presents the main assumptions.

We're On the Edge of a New Age (U)

(U) First is an acceptance that we are on the edge of a new age, called the "Information Age." Also, that this new age is engulfing almost every aspect of society, including the very nature of our business. The basic premise is that the information technology advancements of the last 30 years far exceed any evolution of technology in the Industrial Age. These advances are so traumatic and far-reaching that they clearly represent something truly "new." It is important to note that, historically, technological advancements were called "revolutions" when they make progress of a single order of magnitude (e.g., the automobile "revolutionized" transportation because it was ten times faster than the horse). In the case of information technology, the contention is that the last thirty years have seen an advancement of not one but six orders of magnitude — 1,000,000 times! — in information technology. The end result has been a great deal of confusion and turmoil as human nature attempts to force the "new" of the Information Age into the "known" of the Industrial Age. This "new," however, does not fit; we have to change the thought process.

The Public Sees Government as the Bad Guy (U)

(U) Second, the public reaction to this new age has a direct relationship to the National Security Agency and the way we do business. At the beginning of the Industrial Age, the public centered in on industrialists and/or capitalists as being "the problem." Labor unions were created and child labor laws were enacted to curb their power. In today's Age, the public has centered in on government as "the problem." Specifically, the focus is on the potential abuse of the Government's applications of this new information technology that will result in an invasion of personal privacy. For us, this is difficult to understand. We *are* "the government," and we have no interest in invading the personal privacy of U.S. citizens. Regardless, the public's concerns are real and have an impact upon us. The Computer Security Act of 1987 is one example of this impact, for it clearly represents a first step in limiting any potential NSA involvement in the public sector.

This Age Brought Its Space With It (U)

(U) Third, a major aspect of the Information Age is that it is ushering in a totally new sphere of operations, a new environment called "cyberspace." For many, cyberspace is an ill-defined, comic-book concept — perhaps something created by a science-fiction writer or a Hollywood producer. But for NSA, in the Information Age, cyberspace is both real and virtual: while the real portion consists of physical assets (computers, network terminals, satellites, fiber optic cables, etc.) located on earth and in space, it is the virtual aspect — all interconnected, all networked, all compatible and interoperable — that is the most important. Almost every type of interaction that occurs in the physical world will have a corollary in cyberspace.

(U) In cyberspace, complex networks on networks emerge as an organizing concept upon which our future operations must focus. All networks are interconnected, and routing across the various elements of the network is automatic and not pre-determinable. Descriptors such as Defense Information Infrastructure (DII) or National Information Infrastructure (NII) refer to portions of users of the Global Information Infrastructure (GII) or better yet, the users of cyberspace's transportation system. The future global use and dependency on cyberspace should evolve much the way the use of the Internet has evolved today, i.e., because it should be extremely cost effective. The more important aspect of this inter-connectivity is the fact that, as we move into this complex networked future, computers are in charge, and physical geography becomes less and less important. While computers initially automated routine and mundane tasks, today inter-networking has turned computers and systems to networks, affording opportunities to work with greater and greater amounts of information at any distance. In the future, advances in artificial intelligence, and increases in understanding of cognitive processes, in general, will move us rapidly into a situation where computers and networks work in conjunction with each other, under broad guidance from humans, to actually make decisions and act on our behalf. This is cyberspace's future.

The Future of Warfare is Warfare in Cyberspace — a.k.a. Information Warfare (U)

(U) When we look to the future of warfare in the Information Age, we ask ourselves the question "How do you conduct warfare in cyberspace?" The answer is Information Warfare or, in accordance with DoD's new Directive 3600.1, Information Operations. Information warfare has been the subject of many speeches, scholarly papers, and popular journals. Information warfare has even made its debut in Hollywood in the film *Independence Day.* These many, differing views of IW confuse "information in war," "information technology enhancements of existing combat capabilities or weapon systems," and "warfare in cyberspace." In our view, "information in war" has been with us throughout history, i.e., intelligence on opposing forces was as valuable to Napoleon as it was to MacArthur. "Information technology enhancements" emerged during the Industrial Age with the natural evolution of weapons technology. IW for us, however, is "warfare in cyberspace" and is an exclusive feature of the Information Age. We believe that its biggest impact is yet to come.

(U) Another aspect of warfare that came with the Information Age is that actual, physical combat can be viewed in living rooms of America via television. The horrors of war cannot be hidden. As a result, in the simplest of terms, "body bags" are no longer acceptable. There is considerable societal pressure to find non-lethal means of accomplishing tasks that once called for conventional military action.

(U) For the military, the Information Age presents yet another problem. With the kind of computers, communications, and networking available in the commercial world, how can the military justify separate systems? Commercial communications networks are too inexpensive and too pervasive to ignore. The

good news for the military is that — probably for the first time — they will have interoperable communications in joint service activities and even in multinational operations. The bad news, however, is that they will also be interoperable with their adversaries!

~~(S REL AUS CAN NZ UK)~~ In Information Age terms, IW provides a "digital coercion" option. The primary target of this option is the information infrastructure of an adversary. Such information infrastructures are expected to be primarily computer controlled, operated by the commercial-civilian sector (unprotected), and the primary infrastructure upon which military forces almost totally depend. For IW purposes, access to these computer-controlled infrastructures can permit the degradation, disruption, or destruction of the network and/or the functions they serve. As a result, the "computers" become the intelligence "targets" of highest priority.

~~(S REL AUS CAN NZ UK)~~ There are specific types of weapons associated with Information Warfare. These include viruses, worms, logic bombs, trojan horses, spoofing, masquerading, and "back" or "trap" doors. They are referred to as "tools" or "techniques" even though they may be pieces of software. They are publicly available, very powerful, and, if effectively executed, extremely destructive to any society's information infrastructure.

(U) As a last thought in setting the stage, we expect the Information Warrior of the future to be very different in their thought processes. They will understand the non-physical nature of the future capabilities, will be comfortable with working across the spectrum, and have extensive knowledge of non-military targets. Probably most importantly, they will be comfortable with the concept of networks. They will understand that "information operations" are more than "operations" supported by intelligence and communications; rather, they will understand that all three function together synergistically. Finally, Information Warriors will understand that in the "tooth-to-tail" accounting of personnel, military personnel will be the "tooth" and civilians will be the "tail." Tail equates to the emerging information infrastructure, a primary strategic target of IW.

THE BEGINNING (U)

~~(S REL AUS CAN NZ UK)~~ The following articles will look in depth at various aspects of Information Operations or Information Warfare as they relate to NSA. "Cyberology" and our new CNA mission should provoke much thought and discussion. It is hoped that these articles will serve as a catalyst and basis for these activities.

~~(FOUO)~~ *Mr. Black retired from NSA in 1997 after a long career. He was the first Director's Special Assistant for Information Warfare, and oversaw the establishment of the Information Operations Technology Center.*

Kλ

DOCID: 4033695

P.L. 86-36

IO, IO, It's Off to Work We Go... (U)

(U) The implications of the Information Age are profound. The fundamental underpinnings upon which societies around the globe have existed for the past few hundred years are shifting rapidly and without regard for our personal or organizational interests and equities. T. Michael Elliott, Executive Director of the IEEE Computer Society, sums it up rather eloquently:

> ***"...As we enter the next century, the most critical forces shaping the intersection of computing and culture will be social, not technical, as we come to recognize that "Cyberspace" is not just a pop name for a metanetwork, but a new dimension for human discourse that is effectively as real as physical space. The rules that have governed the relationships among peoples and governments in physical space cannot effectively cope with the interactions made possible by technology. New rules are necessary.***
>
> ***Historically, technological advancement has provided solutions to many social problems. However, the new problems created by our technology will require social, legal, and moral solutions, not technical ones. Current concerns about commerce, taxation, privacy, pornography, personal freedom, human rights, and national security — all approached from the multiple perspectives of different countries — can be expected to multiply.***
>
> ***Despite the differences in culture, traditions, and values, the integrating nature of cyberspace will force common solutions. Governments will never again be able to fully isolate their people from the ideas of the world or keep their guilty secrets from world scrutiny. Ultimately countries will be forced to cope with the reality that traditional national boundaries are meaningless in cyberspace. Or will they?"***[1]

(U) Information Warfare (IW) or Information Operations (IO), as it has now been recast to recognize the concept's applicability across the entire spectrum of "conflict" from competition through crisis and to war, has been recently defined in a much-debated Department of Defense directive as:

> ***Information Operations (IO) : Actions taken to affect adversary information and information systems while defending one's own information and information systems.***[2]

(U) Despite the existence of this directive, opinions on the concept differ as the various public- and private-sector elements struggle to understand the implications of the information age. In military circles, Information Operations is being discussed primarily within a traditional battlefield context and with a predominantly industrial-age mind-set.

(U) To understand the contrast between industrial- and information-age thinking, take an example from the business sector. Today, fundamental thinking regarding economic matters is rooted in industrial-age concepts. Financial analysts, familiar with industrial-age valuation, based on hard-and-fast physical plant, equipment, and inventories, find it very difficult to create an accurate balance sheet for many of the new high-tech start-ups, whose primary assets exist between their employees' ears and in digital form in the companies' computers — information-age intellectual capital.

(U) As societies transition from their indus-

1. T. Elliott, *IEEE COMPUTER*, January 1997, "The Next 50 Years of Computing", p16.
2. Department of Defense Directive S-3600.1, SUBJECT: Information Operations (IO) (U), dated December 9, 1996. Enclosure 1 page 1-1.

~~FOR OFFICIAL USE ONLY~~

trial-age roots to the information age, economic thinking will be transformed[3] as will our concepts of "warfare."[4] The discussions surrounding Information Operations and Information Warfare are crucial to our future — especially in light of increasing global economic competition founded upon information-based societies and enhanced by ever-increasing global connectivity, where information is THE capital commodity.

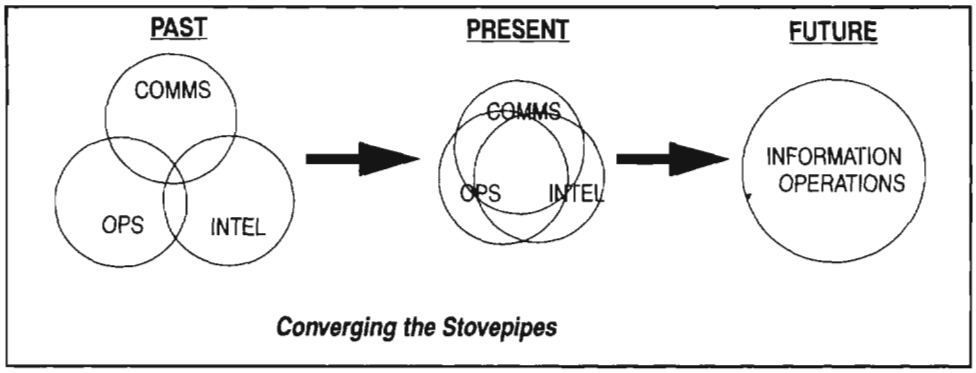
PERSPECTIVES (U)

(U) While there are many reasons for the confusion surrounding this topic, three stand out: the magnitude of the information age's impact, the convergence of organizational roles and missions surrounding the shift from industrial to information age constructs, and the fact that we tend to talk past each other, using different basic concepts of information warfare.

(U) First, the explosion of information technology, and the resultant enhancements in global connectivity, are much more than a revolution in technology — it is, to use the Toefflers' terminology, "a wave change." To understand the impact of a wave change, it's best to take a historical perspective. In the fifteenth century, agriculture was the predominant occupation and the possession of land to produce agricultural commodities the main avenue to wealth. As we moved into the nineteenth century, mechanization appeared. The mass production of simple sewing needles — of all things! — marked the beginning of an industrial revolution, fundamentally changing societies and shifting the basis of wealth and power from ownership of land to possession of industrial capacity. That shift from an agrarian to an industrial society, fraught with apprehension and difficulty for some and excitement and opportunity for others, involved issues of enormous consequence and brought with it broad and profound change. Individuals' lives were altered. Government's role was dramatically transformed. New institutions were formed.

(U) We are now at the leading edge of the information age. Just as in the last shift, we will be forced to tackle issues of like magnitude. Information technology and its age will alter our lives permanently, force the re-orientation of governments, break down old institutions, organizations, and rules, and create whole new ones.

(U) The second major cause of confusion is convergence. At a fundamental level, we see the information age blending our personal and professional lives, blurring the distinction between private and public, and collapsing functional areas of responsibility that, in the industrial age, were separate and distinct. This convergence manifests itself in government bureaucracies as "rice bowl" fights. It is not that we're trying to steal each other's missions and functions — it is that those missions and functions are beginning to overlap.



Converging the Stovepipes

(U) To use an example from the military, the J3s, or the operators of the military world, are beginning to understand that information, traditionally the J2's job, and information technology or communications support, the J6's job, are so integral to their operations that they can no longer do without them. In the information age, it will no

3. For some interesting perspectives on information-age economic thinking, see the article by Kevin Kelly in WIRED, 4.06, June 1996, entitled "The Economics of Ideas" based on concepts of noted economist Paul Romer of the University of California at Berkeley.
4. I refer the reader to the "classic" IW reference *War and Anti-War* by Alvin & Heidi Toeffler for some interesting thinking along these lines.

DOCID: 4033695

longer be adequate for the J2 and J6 functions to be performed in a supporting role. Lt. Gen. Guenther, the head communicator for the U.S. Army, summed it up by saying "we've got to get rid of the stovepipes."

(U) Here at NSA, this convergence is the premise behind our "One Team with One Mission" battle cry. In essence, where in the past we were perfectly capable of performing our protect and exploit mission as practically separate and distinct functions, in the information age, where our customers and targets are all on the same network and using the same equipment with the same vulnerabilities, we have got to converge on a single unified objective.

(U) Finally, our third reason for confusion lies in the vocabulary. In the Information Operations/ Information Warfare business, we tend to talk past each other, largely because we're using the same words but have different notions of what they mean. It's the whole "we've got different Mental Models" problem described in Peter Senge's book *The Fifth Discipline: The Art & Practice of Learning Organizations.*[5]

5. Senge, Peter M., *The Fifth Discipline — The Art & Practice of Learning Organizations*, Doubelday, 1990.

A Taxonomy for Information Warfare: Three Waves, Three Schools of Thought

WAVE	FIRST (AGRARIAN)	SECOND (INDUSTRIAL)	THIRD (INFORMATION)
PHYSICAL SECURITY PROVIDED BY	A Warrior Class, Mercenaries, Militia	Professional Citizens	Information Knowledgeable Leaders
DOMINANT SOCIAL, POLITICAL, ECONOMIC FORCE	Tribe, City, State	Nation-State	Global Conglomerates
ECONOMY DOMINATED BY	Trade	Money	Symbols
WAR CHARACTERIZED BY	Representational Conflict	Mass Armies	Information Attacks
ULTIMATE DESTRUCTIVE CAPABILITY	Gunpowder	Weapons of Mass Destruction	Critical Information Deletion
INFORMATION IN WARFARE	YES	YES	YES
INFORMATION TECHNOLOGY IN WARFARE	NO	YES	YES
INFORMATION WARFARE	NO	NO	YES

~~FOR OFFICIAL USE ONLY~~

(U) As depicted in the chart on the preceding page, there are three fundamental concepts of Information Warfare.[5] Each has its own set of definitions, or interpretations of definitions, and its own distinct set of priority issues and concerns.

(U) First, we have the "information *in* warfare" crowd. These folks originate predominantly from the intelligence community and the ranks of military historians. They view IW as nothing new, pointing out that information has always been important in warfare. Today, there is a lot more information and we've gotten better at moving it around. This group spends its time arguing whether systems should be "push" versus "pull," and how to get the right information to the right person at the right time in the right place. These, of course, are important discussions and valid issues.

"information technology in warfare" gurus . . . view IW as a force multiplier to enhance existing combat capabilities — as another annex to an Operations Plan

(U) Secondly, we have the "information *technology in* warfare" gurus. This group, which is composed of much of the military establishment around the world, takes its lessons from the Gulf War. They perceive that the future of warfare lies in long-range, high-precision munitions. Information warfare is viewed as a force multiplier to enhance existing combat capabilities, i.e. as another annex to an Operations Plan. Along the lines of Michael Hammer's popular book *Re-Engineering the Corporation*,[6] they view information technology as an enabler that will allow them to re-engineer their current "business" and increase efficiencies. They continually look for innovative ways to integrate information and information technology into their industrial-based warfighting machine, seek out information-based targets which will expedite the fight, and push the intelligence establishment to provide greater and greater levels of detail in a more timely manner. This group, however, is still very much rooted in traditional force application.

(U) Finally, we have the "information warfare" group. Proponents who understand the information age and know the fundamental nature of warfare will be dramatically different in the digital realm. This group recognizes that Information Operations will lose its battlefield context in the next millennium. They believe that, increasingly, a society's leadership will desire to limit crisis and conflict and that those leaders will look to resolve conflict before it begins, via "digital" coercion if necessary. This group, to some extent, perceives a diminution of powers vested in nation-states and sees the emergence of trans-national "special interest" groups who will desire to further their objectives with inexpensive, efficient, surgical "bit-based" capabilities. They see the spread of global conglomerates, competing on a global economic battlefield, and point to today's increase in economic espionage as an early indicator of things to come.[7] This group views a future where Cyberspace dependency and information-based societies are the norm, where opportunities and vulnerabilities abound. This group describes "Information Warfare" as warfare in Cyberspace.

MAKING THE LEAP (U)

(U) It is important to understand that Information Operations and the associated cyber-based capabilities are very information intensive propositions. Shaping Cyberspace is a long-term activity which will require a serious continuity of effort. Maintaining an ability to operate in this ever-changing realm will demand a continuous and aggressive pursuit of information and options.

5. This chart originated on a white board at the National Defense University in one of their early Intermediate Information-Based Warfare Courses. Dr. John Alger used Toeffler's waves to describe differing perspectives of Information Warfare.

6. Hammer, M & Champy J., *Re-Engineering the Corporation —A Manifesto for Business Revolution*, HarperBusiness, 1993.

7. By the way, the increase in economic espionage, and computer-based crime in general, has already drawn a response from the Department of Justice, vis-a-vis last year's Economic Espionage Act of 1996, which redefined terminology regarding computer and information misuse and strengthened penalties.

DOCID: 4033695

(U) Secondly, a number of communities of interest, with varying objectives, will need to perform Information Operations at various levels of secrecy. The methods used in the intelligence world — working sustainable clandestine and covert operations, across the entire spectrum, of economic, political, and military targets to exploit systems and produce intelligence in support of a variety of customers — match, very well, the needs of tomorrow's Information Operations community. Our future demands that we devise mechanisms to coordinate among the various communities of interest to maximize our opportunities and minimize the impact of vulnerabilities — in essence, balancing the offense and defense based on a set of common objectives.

(U) Third, while enormous opportunities exist in Cyberspace, there is a down side. The characteristics that make cyber-based operations so appealing to us from an offensive perspective (i.e., low cost of entry, few tangible observables, a diverse and expanding target set, increasing amounts of "freely available" information to support target development, and a flexible base of deployment where being "in range" with large fixed field sites isn't important) present a particularly difficult problem for the defense. Detecting and/or assessing adversary Information Operations will continue to be an incredibly difficult task requiring the ability to track the evolution of an adversary's intellectual capital, and to gather and correlate, in real time, massive amounts of data from a number of non-traditional sources like law enforcement and the computer emergency response community.[9] So, just keep things in perspective; before you get too excited about this "target-rich environment," remember, General Custer was in a target-rich environment too!

CONCLUSIONS (U)

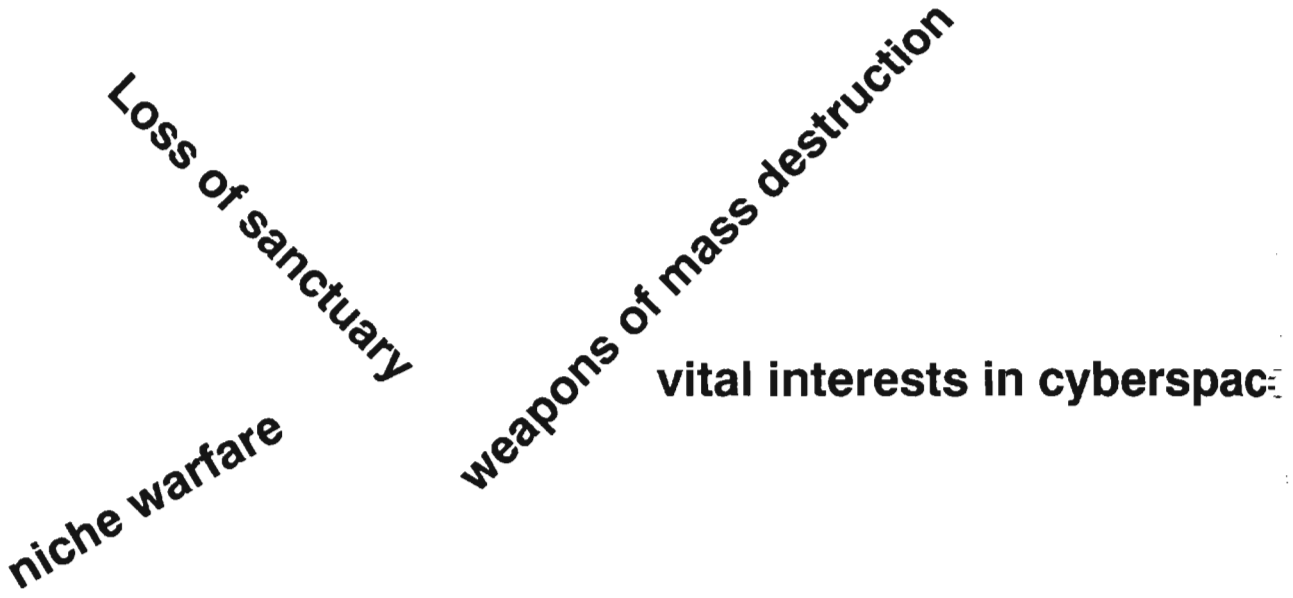
(U) We hope you now have a sense of what Information Warfare/Information Operations is all about and, more important, that you have a feeling for the importance of this debate and are beginning to recognize amazing similarities between the expertise, capabilities, and knowledge required to perform "information operations" and those of the National Security Agency.

(U) Obviously, we have a stake in all three of the IW camps discussed earlier. And as "information providers" and "information protectors," rightfully so. We have to recognize, however, that the future is coming faster than we may care to realize. We must begin today to focus on developing the knowledge, expertise, and partnerships required to perform and/or support Information Operations in the next millennium.

Kλ

9. I direct the reader to DIA's interim report on Information Warfare Indications & Warning. It's an excellent paper that encapsulates the enormity of this task and discusses the current state of warning against this emerging threat.

DOCID: 4033695



The Revolution in Military Affairs

DECISIVE FORCE

Whither conventional warfare?

Compellence
Asymmetry
Anonymity
Time & Space

Connect At Your Own Risk!

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

P.L. 86-36

The Infowar Revolution(s) (U)

by [redacted]

(U) Advances in Information Technology are having profound effects on any number of aspects of societal relations — political, economic, cultural, and military. In some cases, the changes have been sufficiently dramatic to justify calling them revolutionary. In others, the changes in Information Technology allow for significant improvement in the performance of existing systems and structures, but don't fundamentally alter them. Both types of change are important, and it is important to be able to distinguish between the two types in order to better understand and cope with the rapid pace of change. Improvements to performance might generally be accommodated within existing structures and processes; revolutionary change typically requires new ones.

(U) This article describes a view of the Information Technology-related changes going on today and postulates revolutionary change on at least three levels nearly simultaneously. This construct helps to illustrate why the U.S. Government is having such difficulty reaching closure on how to organize for Information Warfare, progress on which has been slowed by the complexity of interrelated changes and the sheer breadth of activities and interests that are affected and therefore must be taken into account. For the most part, however, this is an argument for rapid and large-scale change in NSA, DoD, and the Intelligence Community to respond to the enormous and rapid changes taking place in the world around us.

The Three Revolutions (U)

The Revolution in Political Affairs (U)

(U) Information Technology (IT), by which I mean both the technology per se and its functional application, is fundamentally changing the ways in which the world works. The gradual changes in international commerce (and international crime) that have been brought about over the last few decades by improvements in transportation systems will be dwarfed by the scale and pace of change that IT will make possible. The steady erosion of the sovereignty of nation-states by the border-spanning activities of multinational corporations will be vastly accelerated by the transformation of information into a form of wealth whose movement is unconstrained by geographic borders and largely uncontrolled by governments. Traditional taxation structures and customs controls, upon which governments depend for revenues and the advancement or protection of domestic industries, will not work in the Global Network.

(U) One of the key effects of these changes will be the blurring of the already fuzzy line between international criminal activity and national security concerns. Efforts to deal with the international dimensions of the illegal drug problem have already pointed up the difficult domestic choices — whether and how to use military forces to supplement law enforcement efforts to interdict the flow of illegal drugs — as well as the impact of domestic law enforcement efforts on the conduct of foreign relations. This is hard enough when what we're dealing with is physical commodities (drugs, cash) and international travel arrangements, but just exactly who is going to protect our computers and networks from electronic intrusions that origi-

nate outside the U.S. — local law enforcement? federal law enforcement? the military? our Internet Service Providers? It could be that we're on our own: Connect At Your Own Risk! It might be an electronic parallel to life on the frontier in the middle of the 19th Century — government hasn't yet caught up to you, the Army can't protect you, and nobody (or everybody) claims legal jurisdiction over you.

(U) At the same time, enormous changes are taking place at the level of the individual. For U.S. citizens, there was a considerable sense of security for an individual in the very obscurity of living in a vast country with hundreds of millions of people. But privacy rapidly evaporates as digitized information is created, stored, accessed, and manipulated. For the U.S., in particular, there's a significant loss of anonymity that's implicit in this state of affairs. The other side of the coin, is the increase in power that accrues to the individual by virtue of the access to information, political and societal forums, and the tools and mechanisms of political and economic power. If knowledge is power, then an information-based society is home to an extremely large number of powerful people.

(U) The combination of these macro- and micro-level changes can be expected to produce truly revolutionary change in the political affairs of the nation and the world. This top-level revolution is already beginning and moving very quickly as existing technologies and infrastructures are integrated with new ones in ways so complex and unexpected as to defy any attempt to forecast its course. It's in this context that the other "revolutions" occur.

The Revolution in National Security Affairs (U)

(U) The well-being of societies and their economies is increasingly tied to information systems that provide or control basic services. As a result, a new category of "vital interests" has been created; these interests need to be protected as a function of national security. Such systems can't be defended by means of conventional military force, because there is no means of interposing military forces between the adversary and one's own systems in a networked world. As a fallback, one might attempt to deter cyber attack by threatening to retaliate with military forces. But deterrence relies on being able to identify and punish the attacker, and the anonymity conferred by cyberspace makes detection and identification difficult. In a situation where they can't defend and they can't deter, the usefulness of conventional military forces — one of the strengths of the U.S. — is seriously undermined.

Deterrence relies on being able to identify and punish the attacker, but cyberspace's anonymity makes detection and identification difficult

(U) One of the effects is what has been referred to as "loss of sanctuary": the inability to prevent attacks on the homeland. The combination of geography, conventional military force, and nuclear deterrence that served the U.S. for so many years is largely irrelevant for warding off cyber attacks on our information infrastructure, so we must devise some other means of protecting and defending this vital interest. The first problem is always to determine whose job it is to provide these defenses and who will pay for them — a political as well as a logical decision. Some form of defense will have to be created to restore at least some semblance of "sanctuary." Failure to do so threatens to severely reduce U.S. freedom of action internationally as our ability and willingness to bring military power to bear around the world is called into question. From the standpoint of an adversary, it may not be necessary to devise ways of countering U.S. conventional forces if the U.S. can be dissuaded from employing them in the first place. This is the essence of the "revolution": the concepts and realities of military power that have formed the basis for guaranteeing national security for centuries are giving way to other, non-military means of compelling desired behavior, and we have to adjust our approach to national security accordingly.

(U) Even after the "revolution" actually occurs, some of the more traditional forms of enhancing national security will continue to be in favor. First and foremost, the above-described situation unfortunately increases the incentives for numbers of countries to acquire (and maybe use) weapons of mass destruction as a "cheap fix" for otherwise insoluble security problems. It is virtually unthinkable for most countries to attempt to match the U.S. in conventional military capabilities; their economies could not support the expenditures necessary to deploy and sustain sizable forces with cutting-edge technology. But a truly modest WMD capability could be used most effectively to persuade an enemy not to launch conventional military operations. The other, related area of proliferating military technology is cruise and ballistic missiles. When combined with the coming availability of high-quality and relatively timely imagery from space, missile technology offers practically assured destruction of key strategic targets — regardless of whether the payload is WMD or improved conventional munitions. Such capabilities provide enormous disincentives to enemies to launch military operations against otherwise inferior opponents who can retaliate this way.

The Revolution in Military Affairs

(U) Over the last few years, a lot has been written on the subject of the anticipated Revolution in Military Affairs — the RMA. The problem with all this work is that the "revolution" has already happened. The Gulf War in 1991 confirmed what a few prescient souls had begun to suspect — that the nature of conventional military operations had changed dramatically.

(U) It's somewhat ironic, but not surprising, that the Russians understood some 10 years ago where U.S. progress with integrating weapons and information technologies was going. It's ironic, because for the most part the U.S. was oblivious to the implications of the various thrusts; it's not surprising, because the Russians' dedication and commitment to military science and doctrinal development has always dwarfed our own, particularly at levels above the tactical. (Weapons of Mass Destruction, Operational Art, and Revolution in Military Affairs are all terms and concepts that we "lifted" from Russian military science writings.)

(U) What the Russians perceived happening in the mid-1980's was the creation by the U.S. of a class of "systems of weapons" that integrated near-real-time targeting and fire-control information with very accurate and highly lethal ordnance. The Russians referred to these weapons generically as "reconnaissance-strike complexes" and were gravely concerned that such capabilities would cancel out any advantages they possessed in the realm of conventional (non-nuclear) combat. Their concern was based on an appreciation for the changes that the range and speed (mobility and reaction time) of these systems would have on the spatial character of the battlefield. Since their doctrine called for deeply echeloned forces to concentrate mass at critical places over the course of time, this entire construct was going to be obviated by U.S. abilities to locate, and to deliver devastating fires against, those massed forces before they could be employed — even deep in the theater on Day 1.

(U) The lethality, range, and tempo of this kind of combat was also seen by the Russians as dictating a come-as-you-are kind of war. The high levels of destruction that could be inflicted immediately at the outset of hostilities meant that one couldn't match attrition with production and there would never be more capabilities available than were in existence on Day 1. But this was part and parcel of their basic insight into the nature of the "revolution." The key elements in transforming warfare were:

- *the numbers of new weapons systems available. The technology alone is not sufficient; it must be present in large enough numbers to make a difference in the way the war is fought; and,*

- *the development and institutionalization of a doctrine that would govern the effective use of such capabilities. (In this regard, they may have read more into Air-Land Battle and Follow-on Forces Attack than we ever intended.)*

DOCID: 4033695

DECISIVE FORCE (U)

(U) The U.S. doctrine that emerged from the Gulf War (also influenced by the actions in Panama and Grenada) was one of applying Decisive Force to win quickly and minimize our casualties — attributes that were useful politically as well as militarily. The doctrine seems ideally suited to our posture as an engaged, but not aggressive, lone superpower.

(U) This doctrine will only work, however, if we maintain the numbers of forces, weapons, and capabilities necessary for its execution. That we will do so is not a foregone conclusion. Some contend that we fought DESERT STORM on the residuals from our Cold War investments and seriously question whether we will tolerate the expense of procuring and maintaining such high levels of forces and weapons into the future. High-tech or not, if we can't muster Decisive Force, then we can't apply it and the doctrine is hollow.

~~(S)~~ Decisive Force is an offensive doctrine, but it fails if we can't protect our forces from missile/air attack and WMD. Potential adversaries understand that high casualties might be sufficient to cause the U.S. to disengage from (or refuse to engage in) military actions that were not widely perceived as directly threatening our vital interests. It's precisely this consideration that militates in favor of such measures as:

- *Anti-Tactical Ballistic Missile (ATBM) defenses; cruise missile defenses; and Cover, Concealment, & Deception (CC&D); and,*
- *innovative approaches to neutralizing adversary WMD and missile weapons.*

~~(S)~~ The speed and spatial scope of the operations envisioned in employing Decisive Force put a premium on Command and Control:

- *the U.S. relative advantage in C^2 allows us to fully capitalize on our relative advantage in firepower and mobility;*
- *attacks on C^2 are therefore highly relevant to the probabilities of operational success — i.e., it is likely to be cost-effective for most adversaries to attack the U.S.'s C^2 systems rather than to build a comparable force/weapons infrastructure;*
- *exploiting (vice attacking) an adversary C^2 system is a highly effective and efficient way of gaining advantage, and the rest of the world is becoming more accomplished in the discipline of SIGINT exploitation for military support.*

IN THE FUTURE (U)

(U) Moving to the new plateau in conventional operations — long-range, high-lethality weapons guided by precise, real-time intelligence — is the revolution in military affairs, but there will be follow-on actions that consolidate the new way of fighting:

- *structure changes that improve on "jointness" to achieve better R&D, planning, and execution integration (we won't be able to afford the luxury of four air forces and the Decisive Force doctrine);*
- *better integration of Operations and Intelligence, with Ops becoming more "target-smart" and Intel becoming more responsive;*
- *people will get smarter about this new way of fighting and better able to make use of the information available to them.*

(U) Note that these major changes haven't yet occurred. The present structure's organizational inflexibility becomes a serious source of friction, reducing the potential for realizing the benefits of the weapons and information system capabilities; it

will have to be eliminated by major re-structuring. Ops and Intel will have to be integrated; under the present system they don't work the same problems except when a shooting war forces them to.

(U) The results of the initial application of the doctrine in the Gulf War were so dramatic that one is forced to conclude that it is extremely unlikely that the U.S. will ever again be challenged in a DESERT STORM-type confrontation. Cold analysis and calculation says there isn't a military on the globe that could hope to prevail; and the level of destruction of military equipment and personnel would be so great that few could even expect to survive as functioning entities. Of course, not all such decisions are made on the basis of pure logic, but such a monumental miscalculation has to be considered a remote possibility for the near future.

(U) Unfortunately, the fact that no opponent is likely to engage us in our preferred form of combat doesn't translate into a presumption of no challenges. In fact, potential opponents will expend considerable time, energy, and resources:

- *devising alternative modes of competition,*
- *estimating our threshold for engaging military force and carefully managing their activities to stay under it, or*
- *developing capabilities to attack critical dependencies in our basic doctrine of applying Decisive Force to achieve rapid victory with minimal casualties (for our side).*

~~(S)~~ The last of these options is what has come to be known as "niche warfare." Among the most likely and threatening of these challenges are the following:

- *threats to U.S. forces deploying to or in theater — with the most likely being WMD and ballistic or cruise missile delivery systems;*
- *actions to reduce the U.S. information advantage, probably by means of counter-C2 activities supplemented by the development and use of imagery and signals intelligence capabilities to increase their own force effectiveness.*

(U) The problem for the future, then, is twofold:

- *how do we deter these kinds of challenges?*
- *if deterrence fails, how do we fight in this environment?*

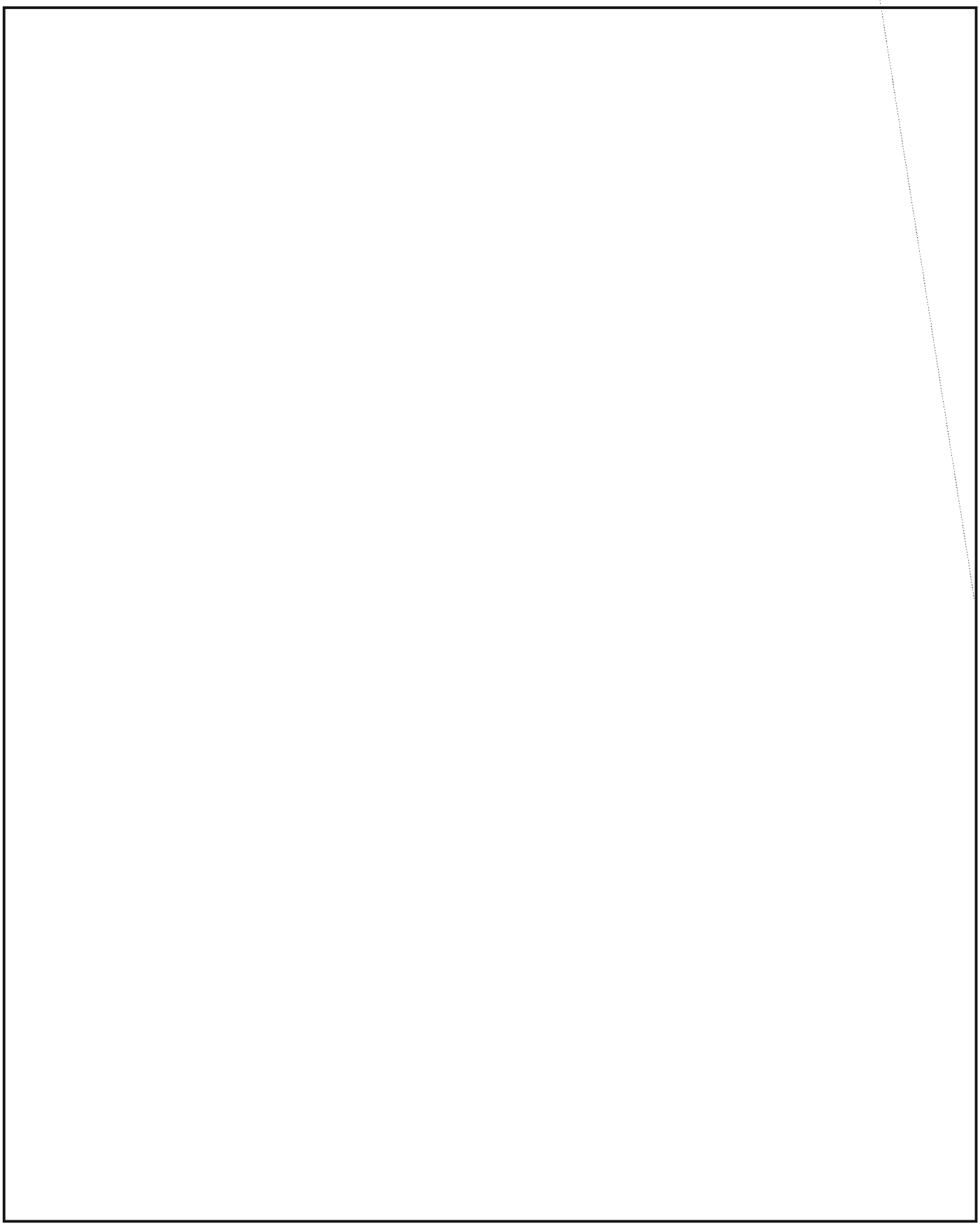
IW Today: The State Of Play (U)

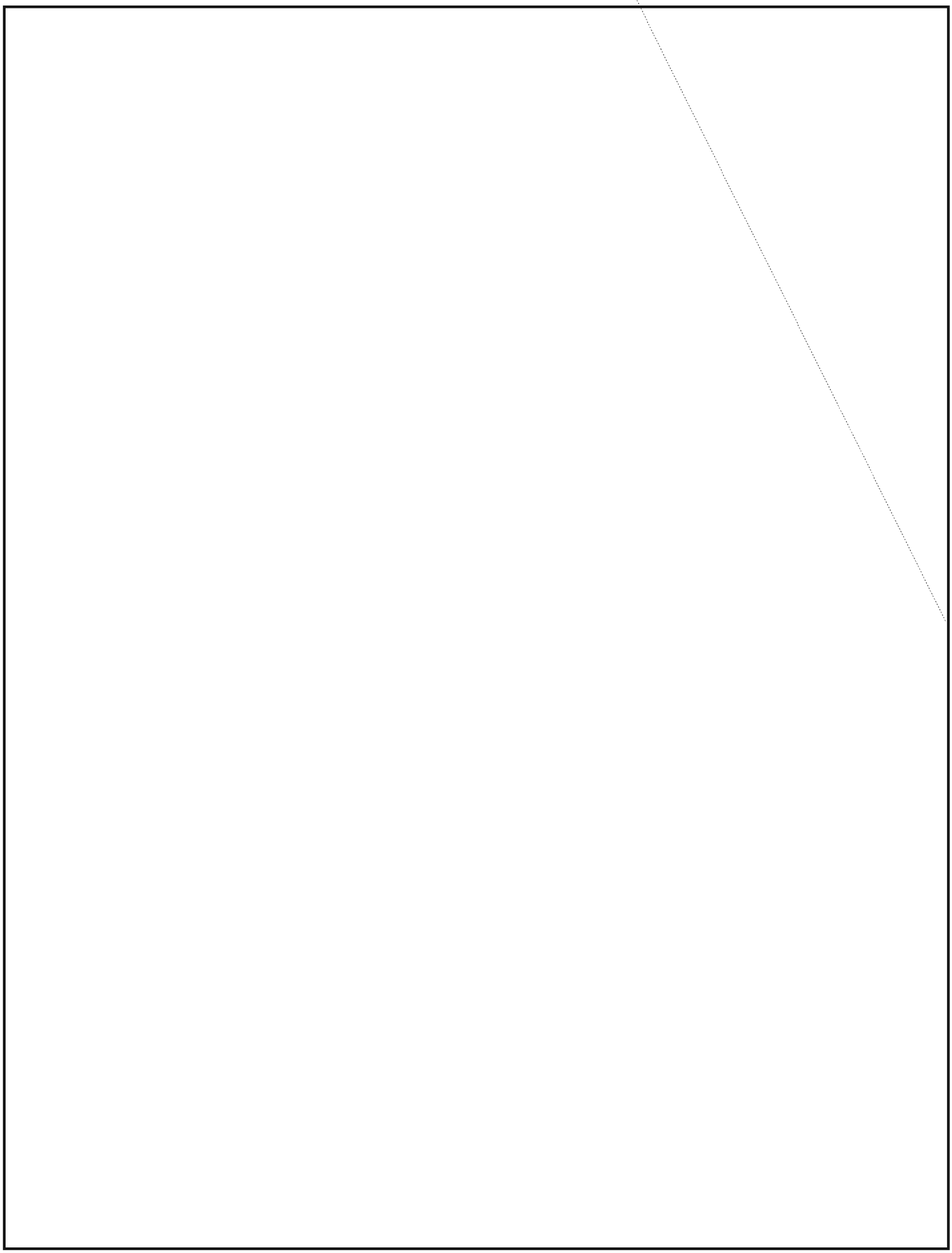
~~(S)~~ IW today is a totally unfocused concept. The description of IW has been continuously expanded since its inception, gluttonously swallowing up whole disciplines and pre-existing categories of activity in what has appeared to be a competition among departments, agencies, and consultants to devise the most all-inclusive — the grandest — definition of the term, thus demonstrating their superior view of "The Big Picture" and validating their claim to the ownership of the concept. Thus the "terminology war" has brought us from Information Warfare to Information Operations, which also includes Information Assurance as well as Information Warfare and Command and Control Warfare, which subsumes . . . Well, you get the idea. The end result of all the hyperbole is that, if IW is everything, then it is in fact nothing.

~~(S)~~ The inability to identify IW as something unique has led to a failure to refine the offensive and defensive aspects into discrete actions to be accomplished. This lack of specificity is compounded by the failure to place responsibility and the consequent absence of guidance. The key to making progress is to fix responsibility and allocate resources accordingly; the centralization of decision-making and resources under bureaucratic actors that can be held accountable is essential.

DOCID: 4033695

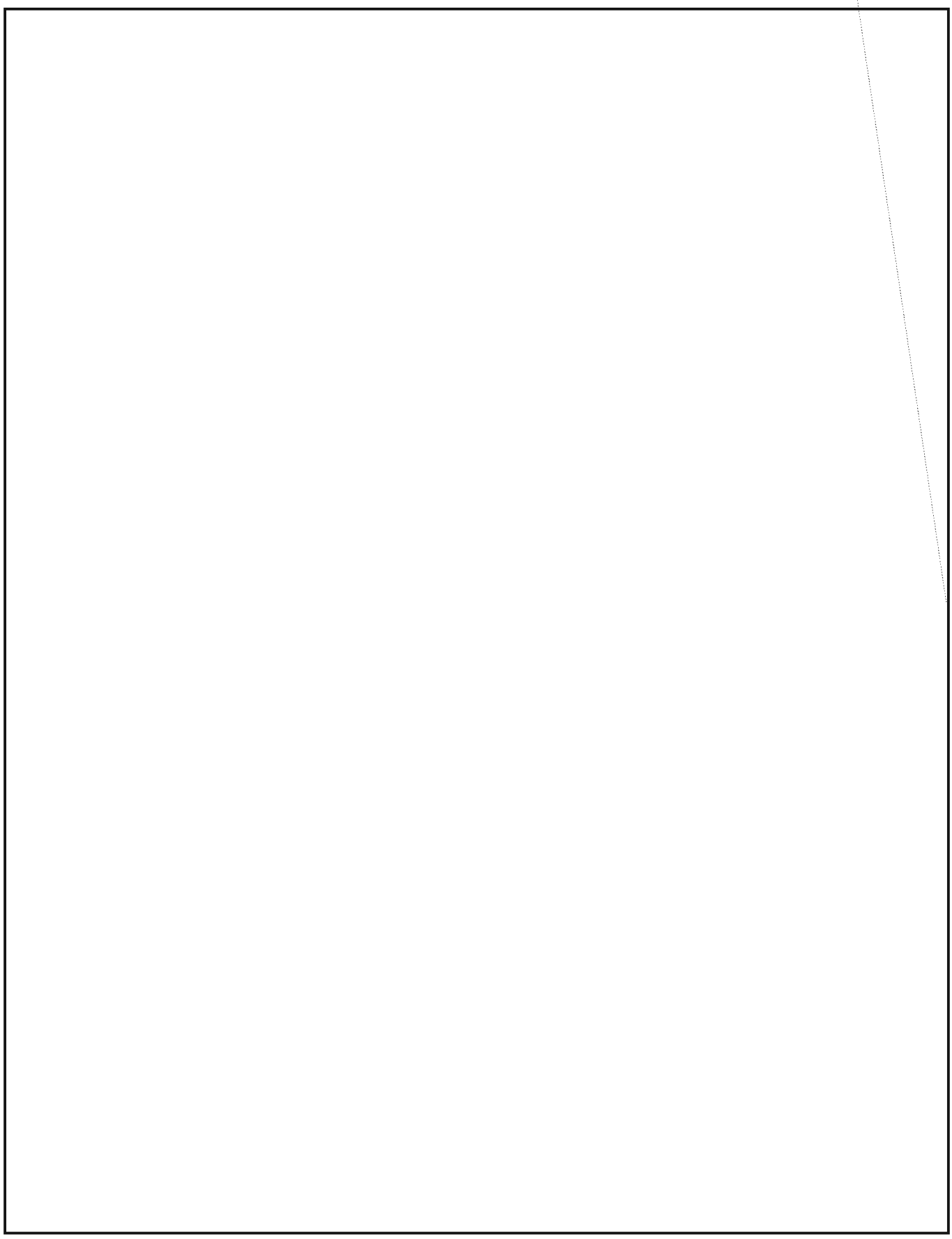
EO 1.4.(c)
P.L. 86-36

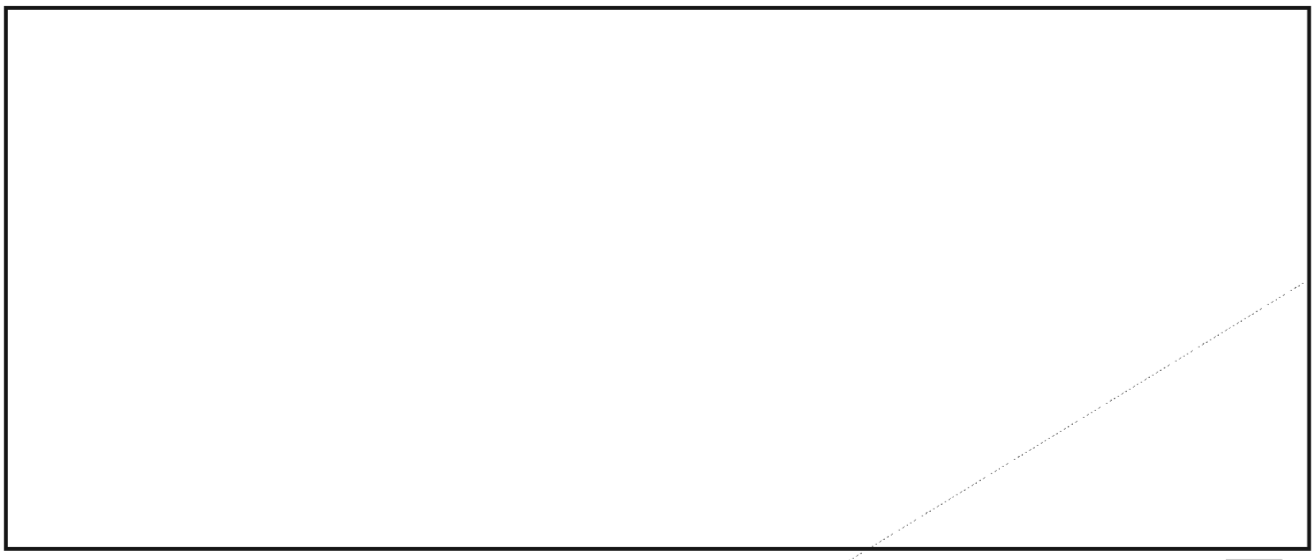




~~SECRET~~

EO 1.4.(c)
P.L. 86-36





Kλ

EO 1.4.(c)
P.L. 86-36

The Role of Information Warfare in Strategic War (U)

by [redacted]
P.L. 86-36

~~(S)~~ If the greatest contribution that an advanced Information Warfare (IW) capability can make to the security of a state is the *prevention* of conflict, then surely the second greatest contribution must be to ensure that the state *prevails* in unavoidable conflicts. Possession of an IW capability confers real advantages in war, including strategic war. It is the contention of this article that consideration of these advantages will yield the following conclusions:

• Information Warfare is neither a pipe dream nor an academic fad. Although it is only in its infancy with respect to technical development, it is apparent that it can make a significant contribution in strategic warfare, as measured by the traditional indices of success, and it needs to be integrated into nuclear war planning.

• IW is not just a "Smash & Jam" capability. It is qualitatively different from those measures executed in previous conflicts under the rubric of "Electronic Warfare" or "Command and Control Warfare." Information Warfare provides capabilities that are a quantum leap more advanced than either.

• The significance of the IW contribution will continue to grow as the U.S. strategic force structure draws down, particularly in a post-START III-world, with an evolving foreign strategic threat picture.

• To the degree that it contributes to maintaining confidence in the robustness and effectiveness of U.S. strategic forces, IW enhances deterrence and strategic stability.

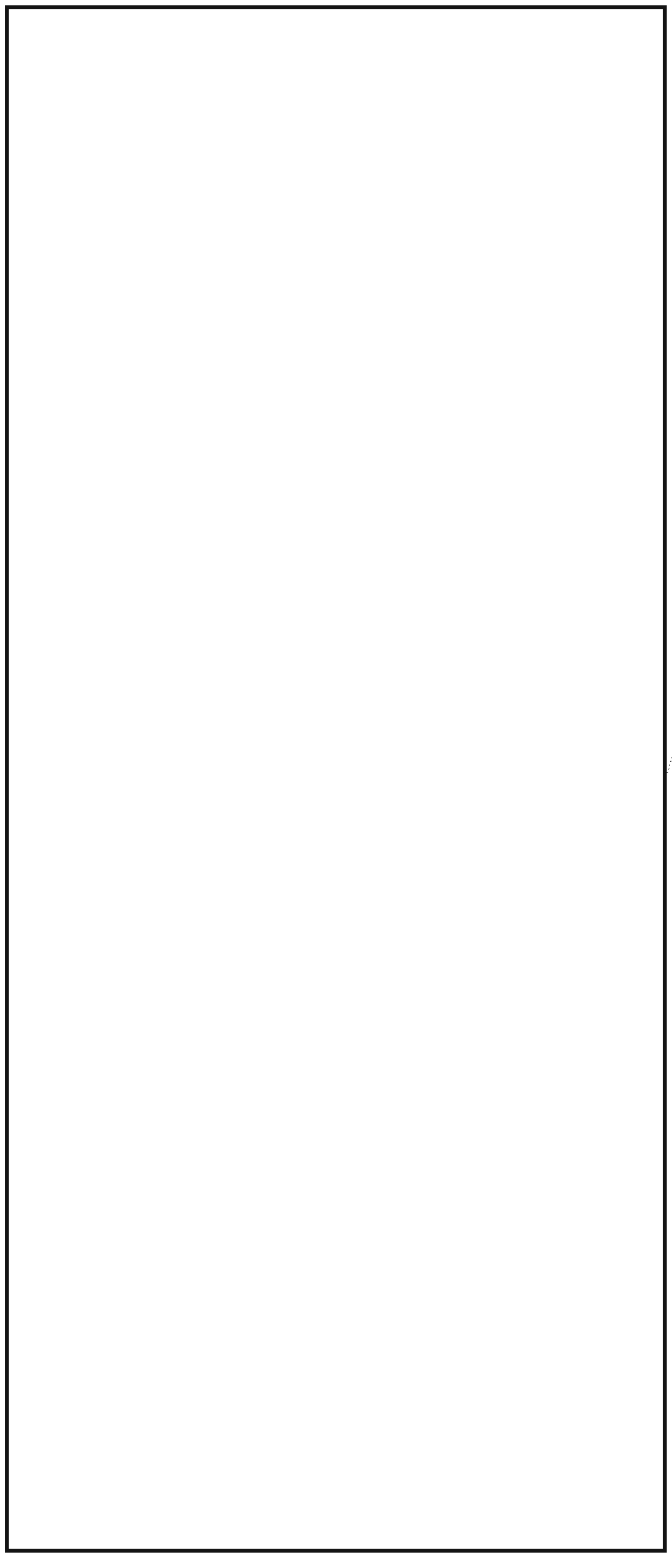
• Real IW will not be cheap. It will require substantial investments to ensure properly specific intelligence support and continuing access.

STRATEGIC WAR IN THE POST-COLD WAR ERA? (U)

~~(S)~~ Everyone recognizes the radical transformation in national security affairs that has taken place since the waning days of the Cold War. To what extent is a concern over the prospect of a strategic war — and the role of information warfare in it — a realistic one? There are several reasons to believe that such concern is not just an exercise in macabre nostalgia. They include: (1) the evolving political context; (2) the changing threat environment; and (3) possible drawdowns in U.S. and allied force structures. Taken together, these developments warrant continued intellectual engagement with strategic issues, and the involvement of IW in particular.

[redacted]

EO 1.4.(c)
P.L. 86-36



~~(S)~~ Similarly, questions need to be asked about future Chinese security policies. As the Communist Party sorts out who will rule China in the post-Deng era, can anyone seriously exclude the possibility of an increasingly assertive Chinese policy, often in conflict with U.S. or allied interests? As the PRC continues to develop economically, it can hardly escape notice that China has continuously upgraded the quality and quantity of its strategic forces, both through indigenous efforts and by upgrades through foreign purchases and by foreign expertise. By 2010, China could pose a serious security challenge to the U.S.

~~(S)~~ Nor should one discount the danger of the "Nth-country" threat. While the capabilities and threats posed by Russia and China are relatively easy to see, they should not cause us to overlook the emerging strategic threats in such countries as North Korea, Iran, Iraq, Libya, or an unknown state. The evidence of ballistic missile and Weapons of Mass Destruction (WMD) programs is quite clear, and these countries also learned the folly of confronting the U.S. with a conventional-only threat. It is not unreasonable to conclude that one or more of these states could pose a strategic threat to the U.S. or (more likely) its allies over the next several decades.

~~(S)~~ One last factor to consider when evaluating the chances of strategic warfare in the Post-Cold War Era is the strategic force posture of the U. S., and, to some degree, its allies. The Strategic Arms Reduction Treaty (START I) reduced the numbers of strategic warheads in the U.S. inventory significantly, but with over 8,000 warheads on ballistic missiles remaining, we were hardly unarmed. The follow-on START II Treaty imposed a ceiling of 4,250 weapons, to be reduced to 3,000 to 3,500 by January 2003. Preparations for a possible START III Agreement appear to center on reducing strategic weapons further to 2,000 to 2,500. Even this reduced figure represents an awesome capability. It is the levels of *post*-START III inventories that take on strategic significance for the period out to the first quarter of the 21st Century, under the scenarios we have been examining. If a post-START III agreement managed to limit U.S. strategic warheads to somewhere in the range of 300 to 1,000, the conjunction of rekindled Russian hostility, enhanced Chinese capabilities, or emerging N-th country threat with reduced U.S. strategic deterrent capabilities could make war "thinkable" in some quarters, undermining strategic stability.

The Role of IW in Strategic Warfare (U)

EO 1.4.(c)
P.L. 86-36

(S) At this point, it would be useful to clarify what we mean by "Information Warfare" and how we see it being employed in strategic warfare. The term "Information Warfare" has been used to describe a variety of activities over the past several years. Within the U.S. Department of Defense, IW has come to mean the application of Information Operations in wartime, and is said to comprise the so-called "six pillars" of Psychological Operations, Operational Security, Deception, Electronic Warfare, Physical Destruction, and Computer Intrusion.

[redacted]

[redacted]

[redacted]

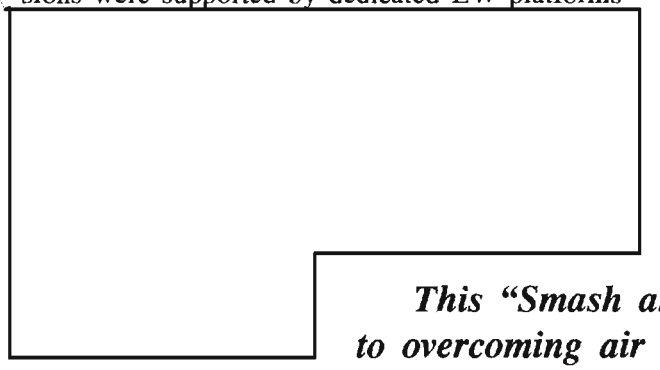
(U) The question occasionally arises whether there is anything fundamentally new about IW. After all, it is argued, the application of Electronic Warfare dates back to 1942 and even C2W dates to early 1991 in DESERT STORM. To respond to this question, I'd like to pose two general strategic problems and compare the solutions from previous conflicts with that available from IW. The two general strategic problems involve (1) overcoming enemy air defenses, and (2) neutralizing an economic-industrial target, in this case a power station.

Case I: Overcoming Enemy Air Defenses (U)

(U) Since World War II, strategic warfare has entailed delivering ordnance on important enemy targets in the rear, usually in the enemy homeland. This has meant facing concentrated, advanced air defenses during the ingress leg, during the drop, and during the egress portion of the mission. These defenses generally comprise some combination of early warning radars, reporting centers, tracking and guidance radars, ground-based fire such as AAA and later, Surface-to-Air Missiles (SAMs), air defense aviation, and the command and control necessary to lash it all together. The heavy losses suffered by the U.S. Eighth Air Force in the early years of World War II led to the incorporation of EW into mission planning. Beginning as early as 1942, USAAF operations featured the use of chaff and jamming in the counter-air defense

mission, along with providing fighter escort and targeting enemy air defense facilities for physical destruction with bombs. ***This combination of EW and physical destruction set the pattern for defeating enemy air defenses for the next fifty years.***

EO 1.4.(c)
P.L. 86-36 ~~(S)~~ During the Cold War, Strategic Air Command planners built an EW plan right into the SIOP execution. Penetrating bombers were provided with increasingly sophisticated EW suites, with both active and passive capabilities, and missions were supported by dedicated EW platforms

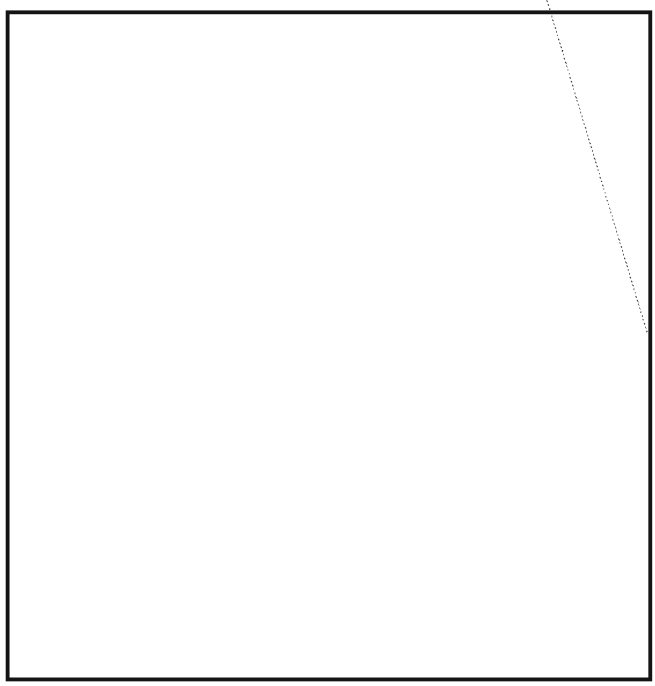


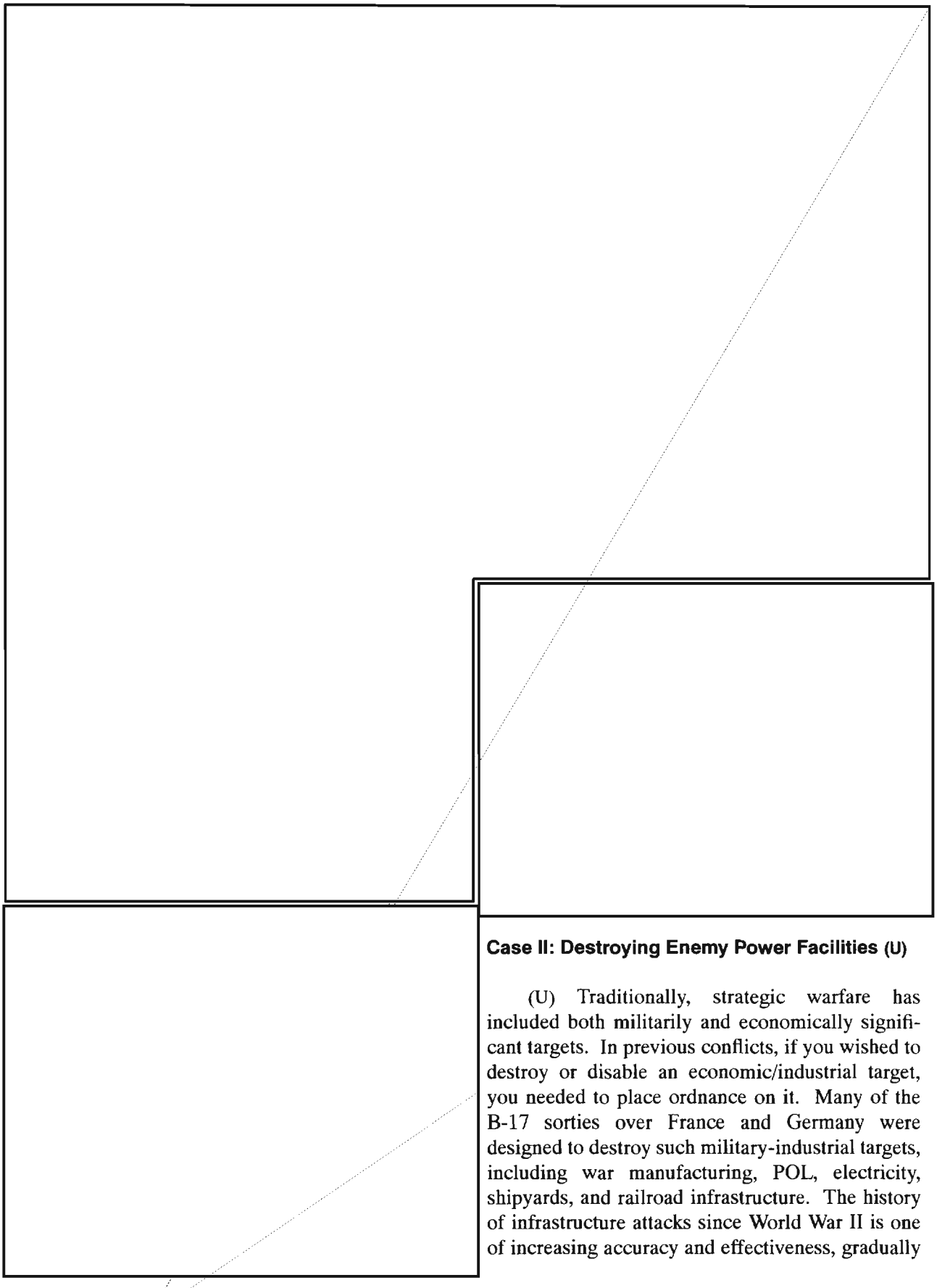
This "Smash and Jam" approach to overcoming air defenses continues to the present day.

(U) Perhaps the closest approximation to overcoming the Soviet air defenses (albeit with conventional weapons) took place in December 1972 during the JCS Operation LINEBACKER II. This round-the-clock bombing operation, involving the then top-of-the-line B-52 and F-111, targeted facilities in North Vietnam in some of the most heavily defended areas of the world. The strike operation was supported by a massive array of support operations involving tactical aviation establishing chaff corridors, performing standoff jamming, as well as active counter-SAM missions by F-4C Wild Weasels and F-105G Iron Hand missions, equipped with anti-radiation missiles (ARM). The combination of soft (ECM) and hard (ARM, iron-bombs) kills was very effective. During the 11 days of the operation, the North Vietnamese launched over 1,000 SA-2 missiles. Out of 724 B-52 sorties, a total of 15 aircraft were lost, for a loss rate of 2.1 percent. Fourteen tactical aircraft were lost in the same period. Another way of looking at these results is that in 11 days of operations, North Vietnam, a well-armed but distinctly Third-World country, had downed 7.4 percent of the participating B-52s, the U.S.'s most capable strategic bombers, putting the lives of 92 SAC crew members at risk.

(U) This combination of hard and soft kill was taken to a new level in DESERT STORM. Air defenses were the first targets engaged when Special Operations Forces and Stealth neutralized early warning and reporting positions on 17 January 1991, followed quickly by telecommunications, leadership, and command and control targets. Ultimately, some 630 sorties were flown against the French-built KARI system — the "nervous system" of the air defense forces to destroy the sector and interceptor operations centers as well as the reporting and listening posts. The EW dimension was stepped up as well: coordinated, preemptive jamming was performed in conjunction with air-launched decoys and ARM-equipped Wild Weasel F-4Gs and F/A-18s. As a consequence of the destruction of the air defense network (as well as the rest of the Iraqi command and control system), the Coalition lost a total of only 38 aircraft and 48 damaged over the period 17 January through 28 February, against an average of 2,140 daily sorties. (Seventy-one percent of those losses were attributable to AAA and IR SAMs.)

EO 1.4.(c)
P.L. 86-36





Case II: Destroying Enemy Power Facilities (U)

(U) Traditionally, strategic warfare has included both militarily and economically significant targets. In previous conflicts, if you wished to destroy or disable an economic/industrial target, you needed to place ordnance on it. Many of the B-17 sorties over France and Germany were designed to destroy such military-industrial targets, including war manufacturing, POL, electricity, shipyards, and railroad infrastructure. The history of infrastructure attacks since World War II is one of increasing accuracy and effectiveness, gradually

reducing the number of sorties required to achieve required levels of damage. IW extends this logic by making possible infinitely scalable, infinitely accurate strikes on infrastructure targets by means of cyber-attacks on the information infrastructure needed to operate it (hence the term Information Infrastructure Warfare, I^2W).

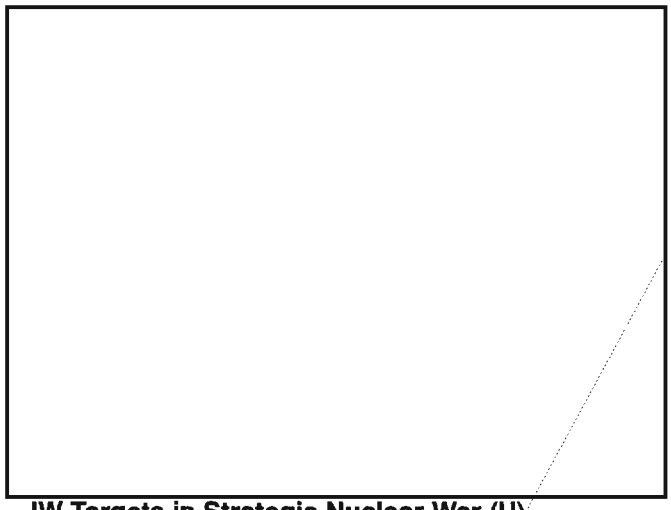
(U) Recalling the strategic bombing campaign against North Vietnam in December 1972, Operation LINEBACKER II, three separate electrical power sites were listed among the strategic targets. The Thermal Power facility at Thai Nguyen was the target of 42 B-52 sorties with a total of 2,185 bombs. The Haiphong Transformer Station was the target of 14 B-52 sorties involving 840 bombs. In addition, 6 F-111 sorties with 72 bombs were ordered on the Hanoi Transformer Station, along with 28 F-4 sorties (245 bombs) and 32 A-7 sorties (348 bombs). Thus, to cripple the North Vietnamese power grids, 122 sorties were conducted dropping some 3,690 bombs on three sites.

IW attacks on a target nation's power facilities are made possible by the growing reliance of the power industry on digital communications and data transmission.

(U) DESERT STORM strike planners mounted an energetic and sophisticated campaign against the Iraqi power system. The grid comprised some 25 major power generating stations and 140 uncollocated transformer stations. While planners had intended to minimize long-term damage to the economic infrastructure (to reduce post-war recuperation time), the majority of the 25 major power stations were struck. Three hundred forty-five strikes were delivered on power grid targets, including 60 TLAM attacks, and including carbon-filament dispensing attacks which were used to ground out power transmission lines. Ultimately, just under 88 percent of Iraq's generating capacity was sufficiently damaged or destroyed, or separated from the national grid making it unavailable.

(U) The IW approach to attacking a target nation's power generating and transmission facilities is made possible by the growing reliance of the power industry on electronic communications methods and digital data transmission for remote operation, monitoring, and supervision.

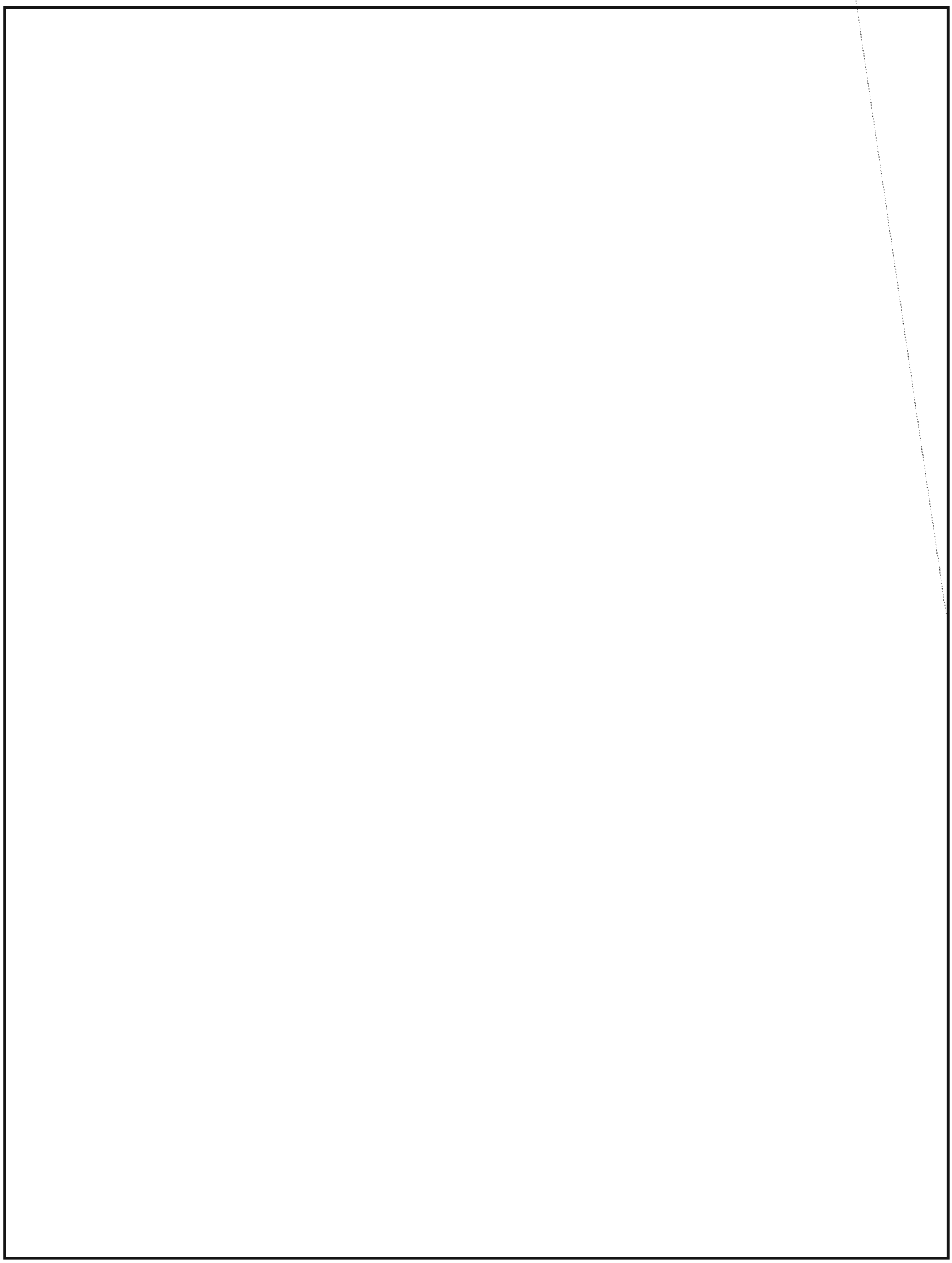
(U) Almost all modern supervisory control systems are computer-based, and consist of a master unit and remote terminal units (RTUs). The master unit is a computer with input and output equipment necessary for transmitting control messages to the RTUs and receiving information from them. The remote units are located at selected stations and are themselves increasingly capable mini- or microcomputers, programmed to perform essential functions. The RTUs are equipped with modems so that they can accept messages from the master and signal that the message has been received and the function carried out. Such functions include opening or closing selected control circuits, monitoring load limits and other system parameters, and alarming when an emergency state is detected. In addition to performing the necessary control functions, the SCADA can provide complete logs of the operation of the portion of the system under its surveillance.



IW Targets in Strategic Nuclear War (U)

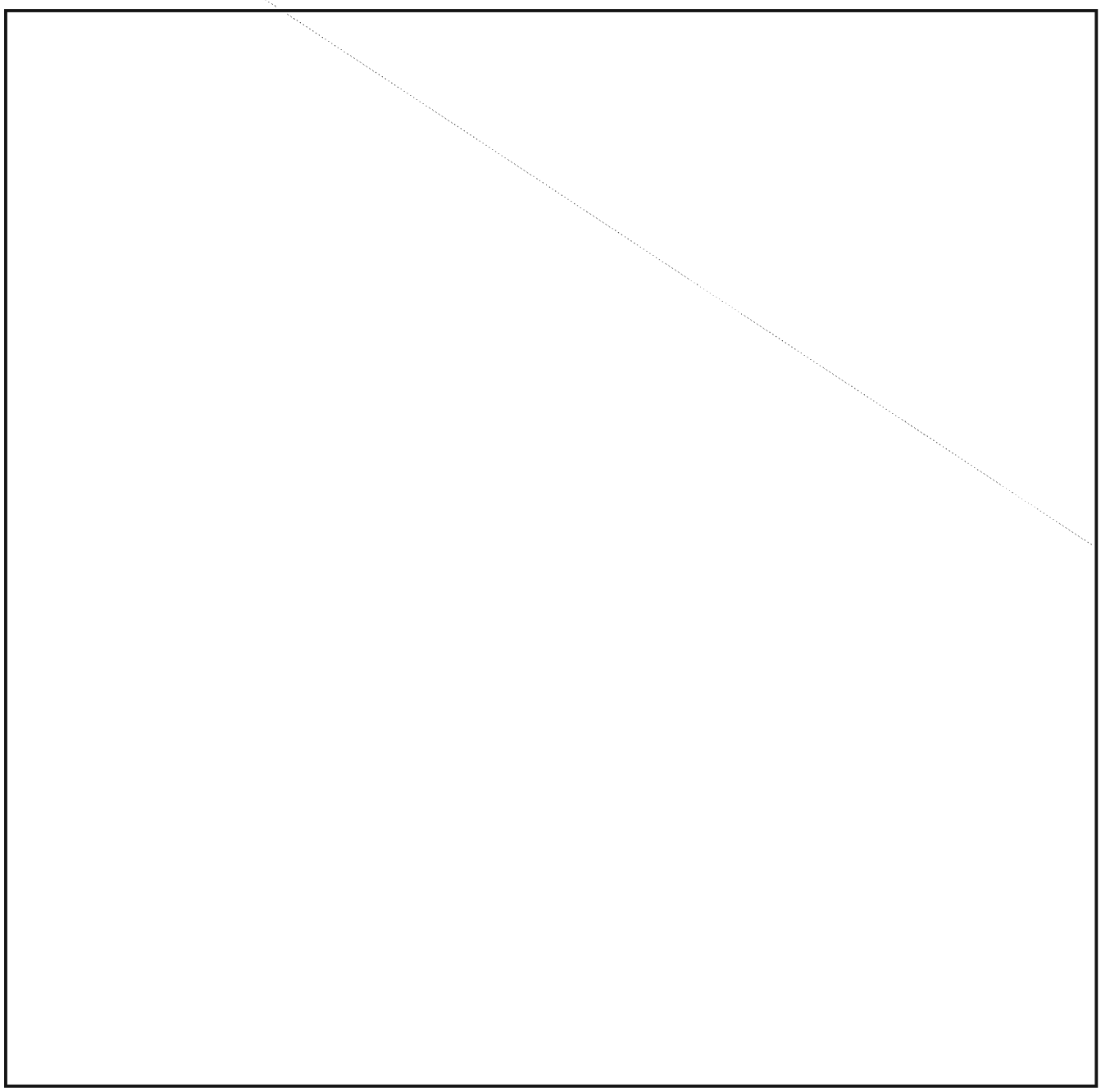
EO 1.4.(c)

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

WHY IW? (U)



NOTE ON SOURCES

(U) In addition to serialized SIGINT reporting, the following sources were consulted during the drafting of this piece: details on LINEBACKER II were provided in Karl J. Eschman, Linebacker: The Untold Story of the Air Raids Over North Vietnam. New York: Ivy Books, 1989. Material on the air campaign in DESERT STORM was derived from Thomas A. Keany and Eliot A. Cohen, Revolution in Warfare? Air Power in the Persian Gulf. Annapolis, Md.: Naval Institute Press, 1995., as well as from Alan D. Campen, ed., The First Information War. Fairfax, Va.: AFCEA International Press, 1992. Information about DELIBERATE FORCE came from Lessons and Implications from the U.S. Air Operations in the Former Yugoslavia 1992-1995 3 Vols. (SECRET) Institute for Defense Analyses Report Number R-397. Alexandria, Va.: IDA, 1996.

Kλ

DOCID: 4033695

CRYPTOLOG
Spring 1997

Thoughts on a Knowledge Base to Support Information Operations in the Next Millennium (U)

by [redacted]
P.L. 86-36

(U) Tackling the information age challenges, focusing the Agency's combined efforts and coordinating a variety of activities, is no small chore. Key to keeping everything straight and aligning our resources is a central repository with which to collaboratively manage the combined intellectual capital that will fuel our nation's Information Operations in the next millennium.

A Notional IO Knowledge Base (U)

Does this mean we need yet another database? Not quite.

(U) Intellectual capital? Central repository? Does this mean we need yet another database? Not quite. Rather, we need a mechanism to collectively view relevant information and knowledge which is currently dispersed, fragmented, overlapped, and incomplete. It's best to think of this knowledge base as more of a management construct — a way to view our collective state of knowledge, understand key relationships, glean insights from linkages, and visualize gaps — dynamically, as a process that continually evolves. We can then use these insights to drive a number of communities, organizations, and even individuals to fill those gaps with information, intelligence, analysis, tools, and techniques.

(U) The Information Operations knowledge base is best described as a series of "templates." A template is simply a layer of information — information that, when combined with other layers, allows you to enhance your understanding of a situation, answer tough questions, and make trade-off decisions. At this point, we envision about nine distinct templates that, when combined together, form a very powerful and essential tool for the effective prosecution of any information operation.

(U) Let's take a look at each of these layers. A graphic representation (see figure 1) will aid in the understanding as we go along.[1] As we discuss each template, keep in mind that the contents of this knowledge base can be utilized for both the planning of offensive operations (i.e., exploit and/or attack) as well as to assess an adversary to support defensive or counter-information operations activities. Therefore, the contents in each template represent, in many cases, both "ours" and "theirs." Different portions of the knowledge base would be used at any given time, depending on whether we are supporting the development of our own operational capacity or developing an understanding of our adversary's.

1. You may notice an older version of this graphic in the Joint Staff's First Draft of Joint Pub 3-13, Joint Doctrine for Information Operations (IO) on page V-6. The original concept was developed based on work NSA performed in support of a customer IW exercise and was basically the culmination of lessons learned while categorizing the threat and vulnerabilities. The templating approach immediately highlighted the offense/defensive synergy and was further adapted to assist the customer in understanding the level of knowledge required to support their evolving IO planning process.

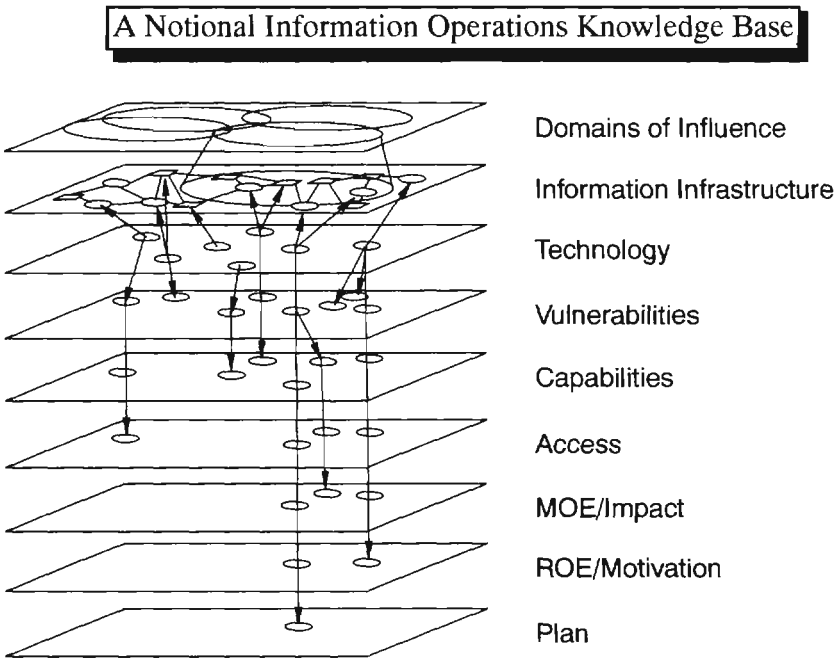


Figure 1 - Templating IO Planning & Assessments

DOMAINS OF INFLUENCE (U)

(U) At the top most level, we are trying to understand how the U.S., its allies and its adversaries, to include non-nation elements, operate. Societies and groups logically disaggregate into economic, political, social, military, and infrastructure segments or sub-systems. Without a fundamental understanding of how various segments function, we have little hope of efficiently exploiting or influencing adversaries through manipulation of their underlying information infrastructures. Likewise, if we don't fully understand our own operations, we'll never be able to assess operational impact and therefore be incapable of making informed risk management decisions. This is by far the most difficult layer of the model to conceptualize. Because of its scope, capturing the subtleties of how the various systems and sub-systems of a society operate and interrelate is enormously complex.

(U) This scope can be limited, however. From an offensive perspective, the current craze in "information warfare" wargaming is crucial. It is through these sessions, realistic operational scenarios will emerge to feed the development of operational requirements which will limit the scope of analytic efforts. On the defensive side, the President's Commission on Critical Infrastructures[2] is likewise essential. Their study will define a reasonable, critical subset of the National Information Infrastructure, which can be used to identify and

2. Executive Order 13010 established the Presidential Commission on Critical Infrastructure Protection on 16 July, 1996. In that document the President observed "Certain national infrastructure are so vital that their incapacity or destruction would have debilitating impact on the defense or economic security of the United States." He noted that the battlespace will be global, threats are of both of a physical and cyber nature, the homeland's sanctuary cannot be assumed and the distinction between military and economic targets may disappear.

develop necessary public/private sector relationships, and effectively limit data gathering and analytic efforts.

(U) The population of this template requires we use various subject matter experts and those familiar with local culture, customs, and perspectives. We should take a page from the concept of operations at the Joint Warfare Analysis Center (JWAC), in Dahlgren, VA, who have evolved a very effective approach — hiring subject matter experts from key industries (power, gas, petroleum/oil/lubricants, telecommunications) and utilizing country teams — to perform focused weapon/target trade-off studies. We need to scale this approach up a notch above the industrial age's physical infrastructures and threats to view and document entire segments of societies (i.e., economic, political, military, and social). HUMINT plays the main role here as well as insights from Department of State, academia, and more and more as companies go global, industry.

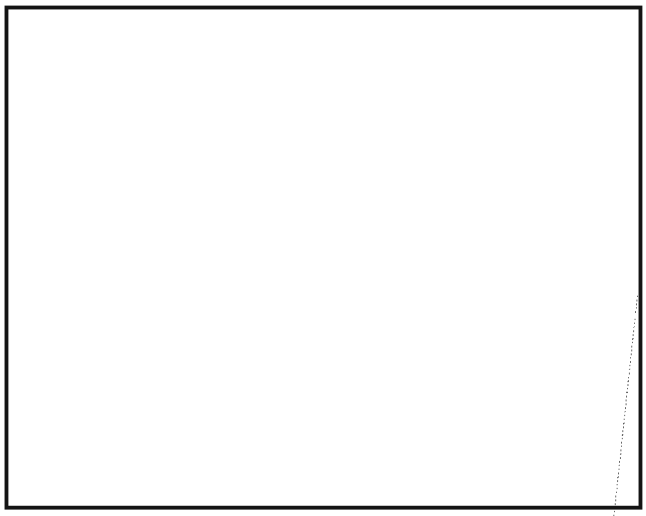
With technology life spans of a mere six to eighteen months, the global information environment moves too quickly for us to keep up our traditional target-chasing mode

(U) After the scope is defined, the most difficult obstacle will be developing a mechanism to capture the intellectual capital of these subject matter experts. This will allow rapid revision and verification, subsequent interrogation, and the establishment of linkages to the lower levels in the model — specifically to the information infrastructure template and the measures of effectiveness/impact template.

INFORMATION INFRASTRUCTURES (U)

(U) Once we understand key "customer" or "target" operations, we need to understand how those functions are supported by information, information systems, and information based processes. In other words, what hardware, firmware, protocols, operating systems, and software are being used where, to perform what functions, and for whom? This template will accumulate as much information, from as many sources as possible, to depict those portions of the global information environment that are relevant to domains of influence where we have an offensive or defensive interest.

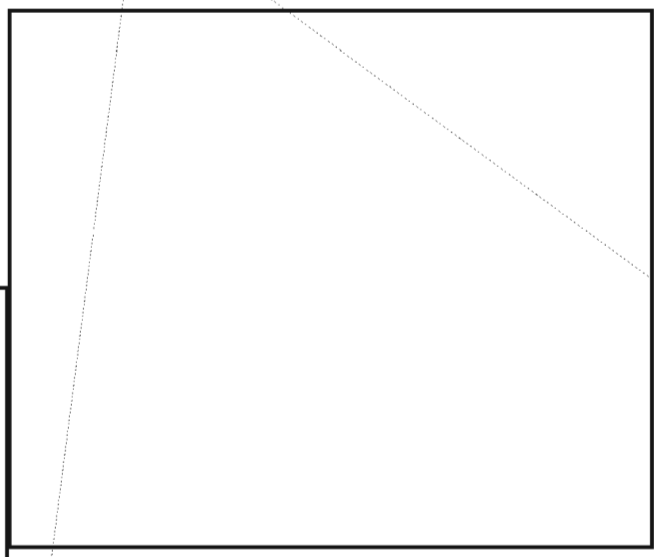
(U) The information infrastructure template is then used to track fielded information technologies, not to drive the development of capabilities, but to look for opportunities to make use of offensive and defensive capabilities that we should already have developed.

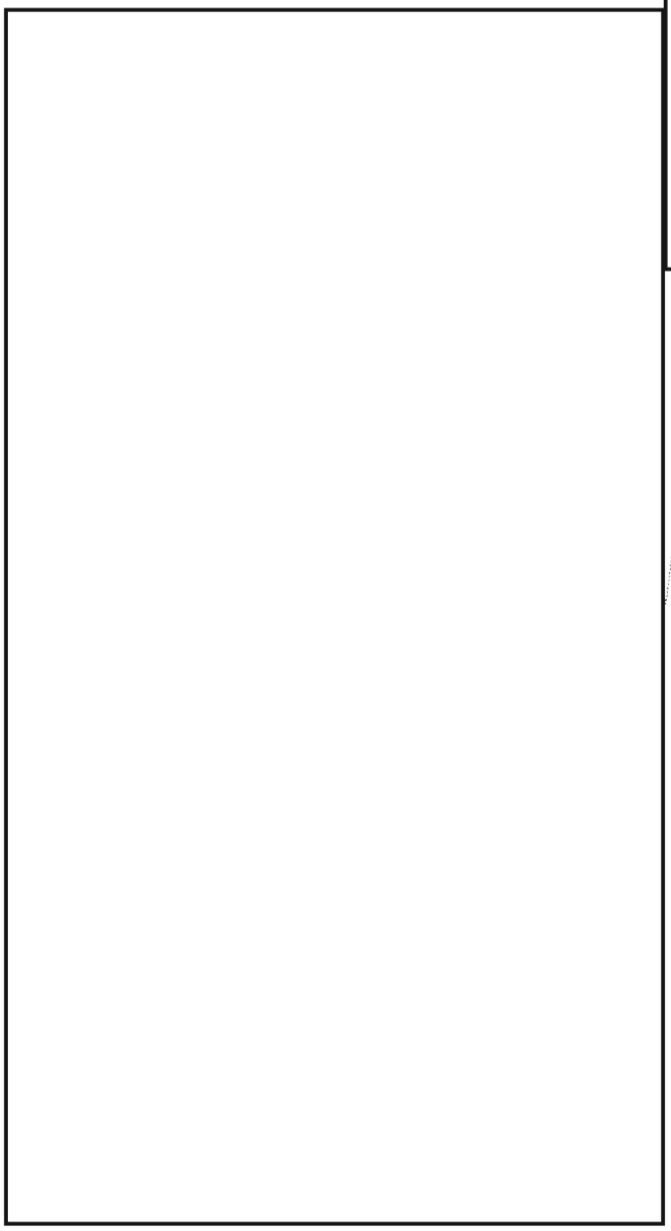


(U) Unfortunately, today, with technology life spans of a mere six to eighteen months, the global information environment moves too quickly for us to keep up with our traditional target chasing mode. The INFOSEC community recognized this a few years ago noting that chasing customer systems, or targets, to add security on after the fact was a losing proposition. Customer dependence on commercial technologies increased the rate at which fielded technologies became obsolete.

EO 1.4.(c)
P.L. 86-36

Increased security requirements demanded an understanding of underlying customer operations. The INFOSEC community responded with an Information Systems Security Engineering (ISSE) approach and various process assurance initiatives to "build security in up front" and get ahead of their "target."





(U) In addition to intelligence activities, engineering analysis plays an important role in the population of this section of the knowledge base. Clearly some of the best talent with which to perform the requisite engineering analysis lie in our support organizations — where experts gain operational insights through the hands-on design, installation, operation, and maintenance of our own systems. These experts must become full partners in the maintenance of this knowledge base, not only to document our own infrastructure but to assist in the analysis of our adversaries in order to fill critical gaps which cannot be obtained by other means. To accommodate this "non-traditional" source and adequately support decision making processes, the template must document what is known and what is postulated.

~~(S)~~ Finally, we must seek out HUMINT sources who have intimate design or working knowledge of key systems and networks. System users and operators are a potentially rich source of insight into the detailed information infrastructure data we require — if we can train the system to recognize their potential, ask the right questions, and then capture and catalog those contributions.

TECHNOLOGY (U)

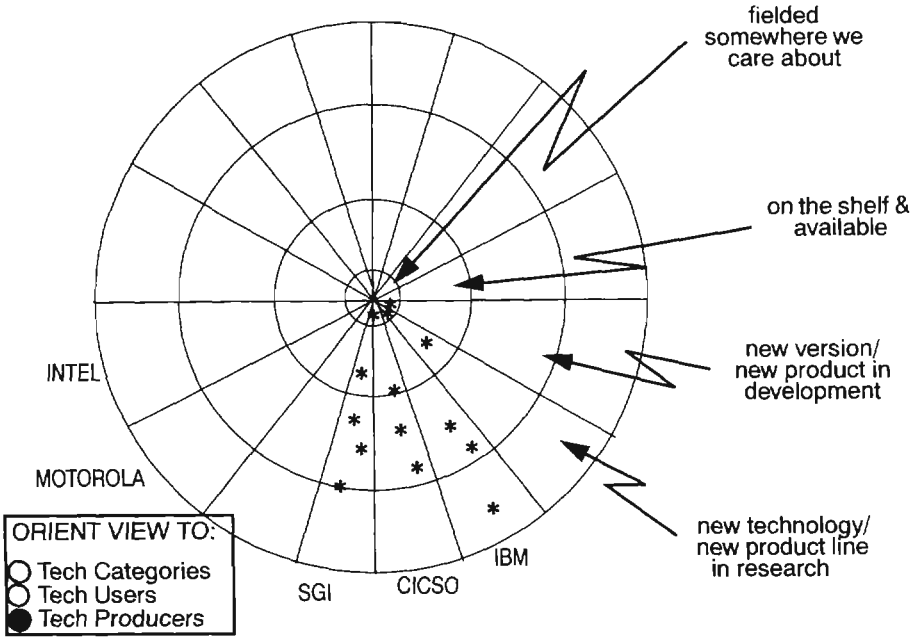


Figure 2. The Technology Radar

(U) In this section, we'll review the technology template. This template must catalog existing and emerging information technologies showing what's on the shelf, what's soon to be on the shelf, and what's a twinkle in some engineer's eye. In order to stay ahead of our targets, we must continuously monitor the information technology market from both a broad and deep perspective and establish a "technology radar" (see Figure 2) that will provide insights into new releases, new products, and new technologies before they hit the commercial shelf and more importantly before they are deployed into the target environment. Note the inner ring of the radar would actually be the information infrastructure template we discussed in the previous section.

(U) The various "range rings" on the radar require very different skill sets to perform the necessary assessments. As we discussed in the previous section, the inner ring requires the combined skills of intelligence analysts and technicians to map the target. The second ring, documenting available technology and assessing high payoff items, will require the skills of a market researcher or consumer trends analyst. The third ring, to project upcoming product releases and new product lines, will require the collaboration of production and applied research engineers, familiar with industrial capabilities, methods, and motives. Finally, the very outer ring, to identify research, determine its relevance, and understand its implications, will require the analytic perspective of core scientists and advanced researchers.

(U) Basically, the goal is to, as accurately as possible, place the "blips" on the radar and determine which are vectoring towards the center at what speeds. If we can track the information technology market in this manner, we will have the knowledge we require to begin to "chase the technologies" instead of "chasing the targets." We will be in a position to make a decision, based on understanding of market trends and customer and adversary acquisition habits, whether we need to send out an "interceptor" to work that technology target or whether we can watch it and hope the blip goes dim before it reaches the center of the screen.

DOCID: 4038695 (c)
P.L. 86-36

~~(S)~~ Currently, we have a number of efforts across the Agency, and others, to identify and document technology trends and produce technology forecasts. These efforts do not draw a distinction between the outer two rings. They are often spot solutions, focusing on specific technologies, and specific points in time. The output is usually a briefing or hardcopy report. Our technology assessment efforts need to move towards a continual process, distributed across the workforce, with the objective of continually evolving a workable taxonomy with which to map technology evolution relevant to our targets of interest.

VULNERABILITIES (U)

(U) Some say vulnerability analysis is an art, other say it's a science. Regardless, we can agree that it does require a unique skill set — a skill set that is the core competency of the information operations community. Individuals across the community with these unique skills are very limited. By tracking the technology in a technology template and the global information environment in the information infrastructure template, we are in a position to make informed decisions to efficiently allocate scarce skilled vulnerability analysts. The results of their efforts, as well as the compilation of vulnerability information for others, will constitute the vulnerability template.

One unofficial survey within NSA listed some eighteen separate organizations who were collecting vulnerability information in one form or another!

(U) Increasingly, organizations are interested in accumulating vulnerability data to support their objectives. There are a number of computer response activities, industry collaboration groups, and elements of the intelligence community and military services working both offensive and defensive angles. Without exception, all recognize the need to track vulnerabilities in some central place and are striving to exchange data. However, there are practical problems.

~~(S)~~ Very few centers exist for the actual derivation of vulnerabilities. Most are identified, involuntarily, by end users, and gathered by computer emergency response activities who serve as conduits between their constituencies and the information technology providers. In order to maintain the support of the technology providers, vulnerabilities are treated by the company as proprietary information, with limited distribution, until they are resolved. Some are identified by industry experts themselves and shared, under strict rules of disclosure in forums like the National Security Information Exchange (NSIE).

(U) As you can see, the practical problem is classification. Companies wish to maintain consumer confidence and their competitive advantage. Computer response activities want to continue dialogs with industry in order to help their constituencies. Professional assessors want to maintain client confidentiality to bolster references. Intelligence operatives wish to protect sources and methods.

(U) To date, the answer to this problem has been to create a number of "central places" for vulnerability data. Just as an example, one unofficial survey within NSA listed some eighteen separate organizations who were collecting vulnerability information in one form or another! Without a macro view of the situation, it is difficult to formulate a workable solution. No one really knows how much unique knowledge exists in each sector.

(U) A large-scale national Information Operations capability obviously requires a macro view of the vulnerability situation. The only hope is that classification issues can be overcome by separating the technology from the operations and working vulnerabilities with a technology focus at some rather high system level. Only with this macro view could the community focus its limited resources, adequately assess threat and operational risk, and balance the offensive and defensive issues in an equitable fashion.

EO 1.4.(c)
P.L. 86-36

CAPABILITIES (U)

(U) Capabilities will leverage vulnerabilities singularly or, more likely, in combinations to exploit, deny, or manipulate target information systems. This template will catalog the various "tools" available to perform cyber operations. Two major issues impede our efforts in this area. First, from an offensive perspective, a single community wide "toolbox" will carry with it a significant compartmentation issue. Secondly, from a defensive perspective, the identification of adversary capabilities is very difficult.

~~(S)~~ Today, the tools are developed by a number of different organizations for a variety of purposes. The majority of these efforts are very

(U) Tackling the defensive issue is a bit more difficult. Today, our approach to assessing adversary capability is rooted in an industrial age mindset. We attempt to identify adversary "IW" capabilities in the same manner in which we have tracked the proliferation of traditional industrial age weapons of mass destruction (i.e., Nuclear, Biological, Chemical weapons). The problem is that the development of an information age weapon of mass corruption has very few observables, especially in the buildup phase.

ACCESS (U)

(U) Simply possessing a capability to exploit a particular computer system does not necessarily mean that the capacity can be used in any productive manner. Access, proximal or remote, is required to "deploy" a capability to its desired target. The logical analogy from the past would be possessing nuclear warheads but no missile or bomber to deliver the warhead to a target.

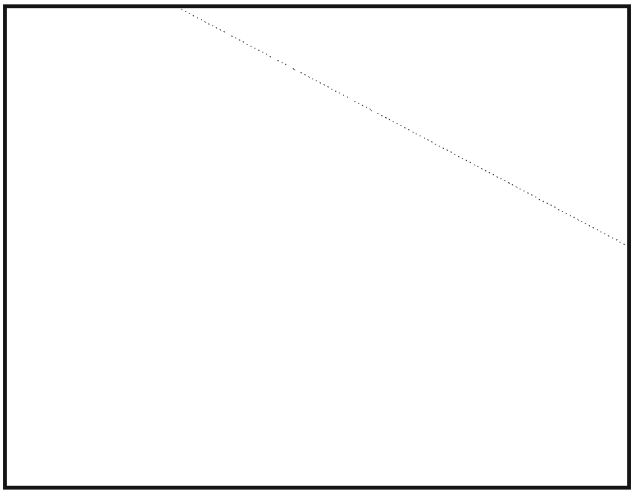
~~(S)~~ Some might see access as simply another dimension of the capability. It was purposely separated into its own template in order to draw attention to its importance. From an offensive perspective, access is the most difficult ingredient in the recipe for cyber operations. Many of the postulated capabilities used in today's exercises and wargames simply assume access will be available, usually provided by the Intelligence Community. That perception must be countered. As we work to devise realistic scenarios with which to drive operational requirements, we must force the operational community to think about the need for both capability and access. Likewise, our technologist's efforts must be constrained by the need for access as well. Much of what we do in this arena today is characterized as "technology push" — we develop a capability because we can. Requiring attention to the access dimension will keep us from expending energy developing weapons for the cyber ops arsenal which could never be deployed.

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

DOCID: 4033695

E.O. 1.4.(c)
P.L. 86-36

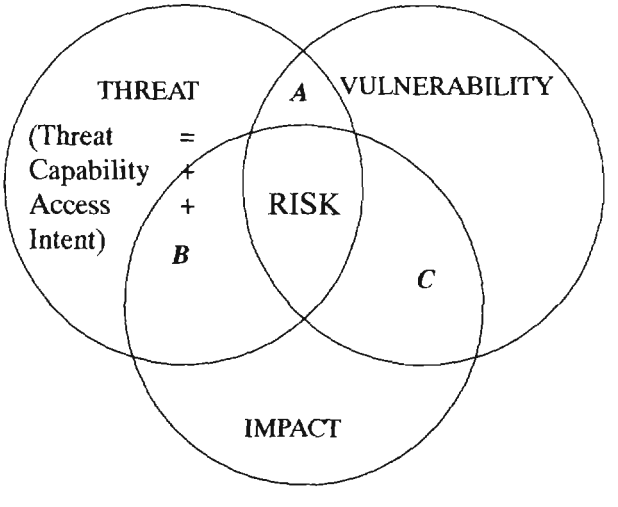


the offensive community to perform some quantitative analysis or assessment of the effects of deploying a specific capability. The defensive world has called this "impact assessment." Clearly, these assessments have to be based on a detailed technical understanding of the interrelationships in the information infrastructure. However, they must be expressed in terms of the net effect to the domain which the operation intended to influence. This is a job requiring significant modeling and simulation capabilities. In fact, this template is envisioned to contain the models and simulators required to perform these offensive and defensive assessment. The actual information to feed these tools would come from the layers above.

IMPACT/MEASURES OF EFFECTIVENESS (MOE) (U)

(U) Okay, we now have an understanding of the circumstances when certain capabilities would likely be used to take advantage of vulnerabilities in the base technologies deployed in the target environment. We still do not have the answer to the "so what?" question. In essence, the term "measures of effectiveness" has been devised by

(U) On the defensive side, risk is traditionally depicted as the intersection of vulnerability, threat, and impact (see Figure #3). Many use the words vulnerability, threat, and risk interchangeably and tend to overlook or inadequately estimate impact. With limited resources in terms of both manpower and dollar to attack residual risk, an ability to estimate or model optional impact will greatly enhance our ability to focus our countermeasure efforts on those areas where they are most needed.



A: vulnerabilities threat can exploit but have no operational impact

B: if vulnerability exists, threat could have impact

C: vulnerabilities with impact that threat cannot exploit

Figure 3. Risk

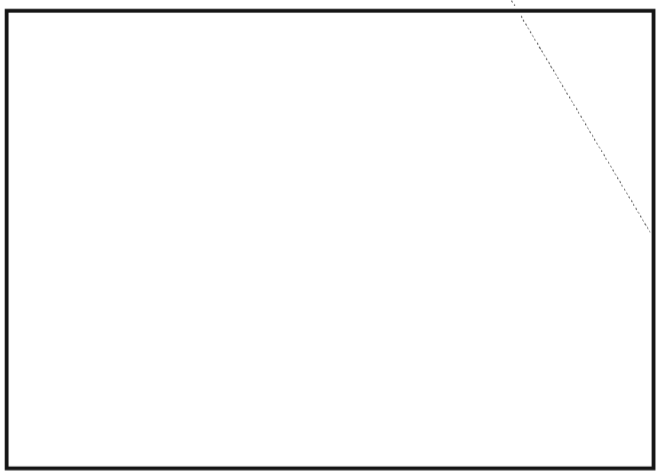
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

(U) As we attempt to look at entire infrastructures and large systems of systems which support entire domains of influence, the level of sophistication in our models rapidly exceeds anything we've attempted before. Cascading effects in both the information infrastructures and the domains of influence will be the norm as interdependencies continue to increase. In addition, the amount of detailed information and computational power required to support simulations of those models is immense.

RULES OF ENGAGEMENT/ MOTIVATION & INTENT (U)

EO 1.4.(c)
P.L. 86-36



(U) On our side, once moral and ethical issues are resolved, rules of engagement for cyber operations become a policy and coordination challenge more than anything else. The major challenge, from a coordination perspective, lies in the convergence of the strategic, operational, and tactical levels these type operations necessitate. In information-age, cyber-operation scenarios envisioned for the next millennium, it is very difficult to discern the strategic from the operational from the tactical in either a targeting, tactics, or decision making sense. The concepts for utilization of the "Bit Bomb," the "weapon of mass corruption" for the information age, might best be considered as similar to those devised for the Atomic Bomb, the weapon of mass destruction from the industrial age. Very stringent policies, highly coordinated practices, and central-release authority may be required. In fact, experiences from today's information warfare games and exercises seem to indicate that information warfare might best be played solely at the strategic level, separately and distinctly from traditional military operations.

(U) Regardless, we need to ensure that we capture the insights we glean from intelligence regarding adversary intent, as well as our own evolving "rules of engagement" to ensure we can adequately model and simulate information operations and support our operational planning and risk management processes.

(U) The representation of this information takes on an almost Artificial Intelligence-like, rules-based, expert-system form in order to represent complicated, compound, conditional assertions, like:

> ***"If leader X perceives an information-based attack on its financial infrastructure, and the state of relations between country X and the U.S. is best characterized as highly competitive but moving rapidly towards crisis, and depending upon the outcome of diplomatic negotiations over issue I, then leader X will most probably retaliate with the deployment of capability C, via access mechanism A, against U.S. infrastructure target T with the expected outcome of O."***

(U) As you can see, the articulation of intent is very difficult — conditional on a number of facts, hypothesis, and dependencies. To date, the best method for developing these assessments has been via prose documentation of probable scenarios based on a limited understanding of adversary capability and intent. On our side of the game, the Rules of Engagement are even more difficult to articulate! The state of the art must be improved in order respond to requests for information and assessments and to maintain the incredibly high operations tempo envisioned as we move towards an active defense.

OPERATIONS (U)

(U) We finally come to the bottom line. If we've done our homework against a specific adversary, we should come up with a list of those capabilities that we can deploy that will take advantage of vulnerabilities that exist in the adversary's information infrastructure to accomplish some level of influence over the target domain — in other words, a viable plan.

(U) Likewise, if I look at the opposite sides of the templates I should see a picture of the most probable scenarios that an adversary would run against a given segment of our society — in other words, a reasonable approximation of their plan.

CONCLUSION (U)

(U) Clearly, the National Security Agency houses a major portion of the intellectual capital discussed in the previous sections. However, the NSA cannot be the sole contributor to this knowledge base. As a community, we must develop the knowledge and expertise required to populate and maintain this knowledge base with which to manage and support a sustainable and superior national information operations capability. It is only through the collective management of our combined intellectual capital that we can maintain our nation's security in the cyberspace environment.

Kλ

~~SECRET~~

Information Operations Training (U)

by [redacted] P.L. 86-36

~~(C)~~ The end of the Cold War has brought many new focuses and challenges to the Intelligence Community. The worldwide proliferation of sophisticated computer technology, the modernization of communications in traditionally less-developed nations, and the resultant increased global connectivity combine to present a whole new intelligence concern: the capability of nearly any foreign entity to exploit or attack the information systems of the United States or its allies.

~~(S)~~ Executive Order 13010, which established the Presidential Commission for the Protection of Critical Infrastructure, coupled with Presidential Decision Directive 35 revisions, which elevated Information Warfare to a Tier 1 issue for many countries, exemplify the growing senior-level concern of the foreign Information Warfare threat to the United States.

~~(S)~~ In response, the SIGINT Requirements, Validation, and Evaluation Subcommittee (SIRVES) validated six new National SIGINT Requirements (NSRs) to support the growing needs of the customers for data to support Information Operations. These NSRs put demands on analysts to produce unique intelligence reports in a new area. To meet these demands, analysts must first understand just what Information Operations is and how intelligence can support it.

~~(C)~~ In response to DDO tasking, the Information Warfare Support Center led the effort to develop National Cryptologic School (NCS) courses IS-231 and IS-232. With support from the DO, DS, and DI organizations, the courses, while designed with SIGINT intelligence analysts and reporters in mind, have a broad enough perspective to be useful to those in other disciplines and organizations. In fact, IS-232 has been in high demand both inside and outside the SIGINT community.

~~(S)~~ IS-232 Information Operations Awareness is a three-hour seminar intended to provide a basic understanding of Information Operations and how intelligence can support it. The course covers the following:

- Defining IO
- IO Conceptual Framework
- Potential Indicators of IO activity
- IO Enabling Technologies
- IO Techniques
- Foreign Information Warfare
- IO Reporting

~~(FOUO)~~ So, in a nutshell: What is it? How to identify it? and What to do with once it has been identified?

P.L. 86-36

~~(FOUO)~~ To date, IS-232 has been presented to [redacted] throughout the Agency and the services. It is currently being offered on an as needed basis to groups of 15 or more. Additionally, the modular design of IS-232 allows portions of it to be included in other curricula and in conferences, briefings, and working groups.

~~(S)~~ IS-231, Information Operations Reporting, a four-day class, was piloted in February 1997 with ten students from analytic, computer science and collection backgrounds. This course expands on the concepts presented in IS-232 and includes a number of practical exercises. After some revisions, the NCS plans to offer IS-231 on a quarterly basis.

[redacted]

Kλ

P.L. 86-36

~~SECRET~~

DOCID: 4011893

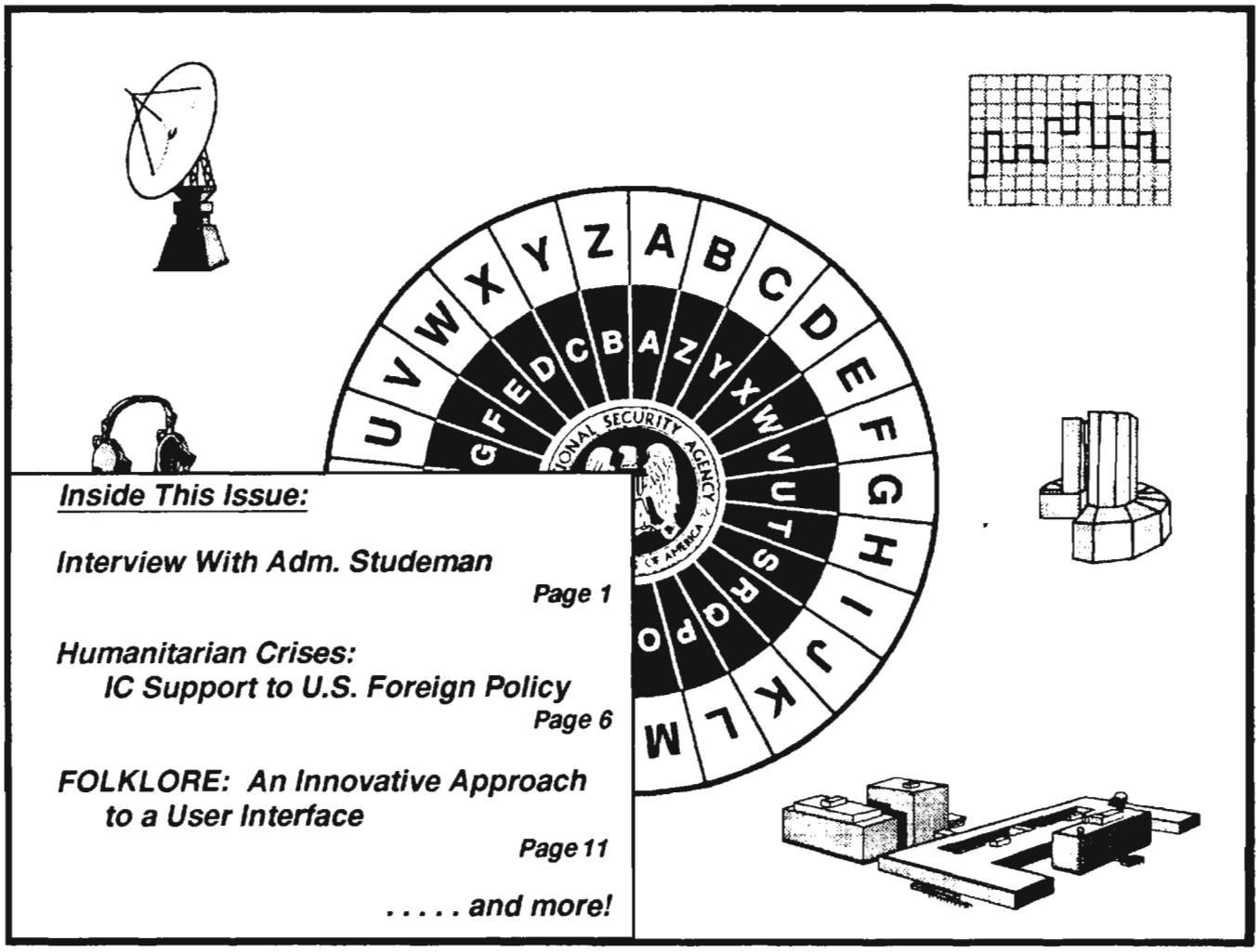
~~TOP SECRET UMBRA~~

NATIONAL SECURITY AGENCY

CRYPTOLOG

The Journal of Technical Health

Vol. XXII, No. 4 WINTER 1996



Inside This Issue:

Interview With Adm. Studeman *Page 1*

Humanitarian Crises: IC Support to U.S. Foreign Policy *Page 6*

FOLKLORE: An Innovative Approach to a User Interface *Page 11*

. . . . . and more!

~~Derived From: NSA/CSSM 123-2~~
~~Dated 3 September 1991~~
~~Declassify On: Source Marked "OADR"~~
~~Date of source: 3 Sep 91~~

Declassified and Approved for Release by NSA and CIA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

~~TOP SECRET UMBRA~~

DOCID: 4011893

CRYPTOLOG

Winter 1996
Vol. XXII, No. 4

Published by P02, Operations Directorate Intelligence Staff

Publisher ..... William Nolte (963-5283)

Editor ..... [redacted] (963-5283)
Graphics ..... [redacted] (963-3123)

Board of Advisors

P.L. 86-36

Chairman ..... [redacted] (963-7712)
Computer Systems ..... [redacted] (961-1051)
Cryptanalysis ..... [redacted] (963-7243)
Intelligence Analysis ..... [redacted] (968-8211)
Language ..... [redacted] (963-7667)
Mathematics ..... [redacted] (963-1363)
Signals Collection ..... [redacted] (963-5717)
Telecommunications ..... [redacted] (996-7847)
Member at Large ..... [redacted] (968-4010)
Member at Large ..... [redacted] (968-4010)
Member at Large ..... [redacted] (961-8214)
Classification Officer ..... [redacted] (963-5463)

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

To submit articles and letters, please see last page.

DOCID: 4011893

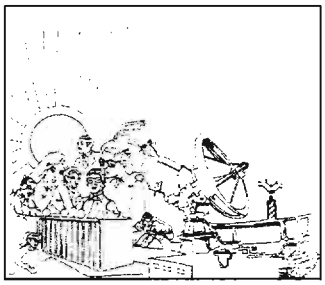


Table of Contents

A Wealth of Experience:
An Interview With Former DIRNSA Adm. Studeman (U), by Bill Nolte 1

Humanitarian Crises:
IC Support to U.S. Foreign Policy (U), by Toby Gati.....7

FOLKLORE: An Innovative Approach to
A User Interface (U), by [redacted] 11

Church-State Relations in the [redacted]
Image vs. Reality (U), by [redacted] 17

Book Reviews: (U)
The Legacy of Tiananmen: China in Disarray (U) 21
Intelligence Analysis: Estimation and Prediction (U) 24

P.L. 86-36

P.L. 86-36
EO 1.4.(c)

A Note From The Publisher:

(U) *Who's on first?* If you have noticed that the Winter 1996 issue (Vol. XXII No. 4) followed the Summer issue (Vol. XXII No. 2), be assured that you have not missed the Fall issue (Vol. XXII No. 3). The demands of producing a separate, unclassified version of the Spring issue (Vol. XXII No.1) dedicated to the memory of Dr. Tordella) in time for the opening of NSA's new supercomputer facility made it necessary to declare the unclassified version the fall issue. 1997 should see us back on schedule.

(U) *What's on second?* The Summer 1996 issue of *CRYPTOLOG* was inadvertently sent to an incorrect distribution. Please contact the editor at **cryplog@p.nsa** or on 963-3123s if you did not receive yours; extra copies are still available.

DOCID: 4011893

Perspective:

EO 1.4.(c)
P.L. 86-36

A Wealth of Experience (U)

An Interview with Admiral William O. Studeman, USN, ret. (U)

former DDCI and former DIRNSA (U)

by Bill Nolte

(U) Let's begin with some background. Did you intend to have a career in intelligence when you joined the Navy?

(U) No, not really. I was commissioned through Officers Candidate School, which is principally a pipeline for surface officers. At OCS, I wanted to go into aviation. My family has had a long history in aviation, my father being an aviation pioneer. So, I went through pre-flight and flight school at Pensacola. I wore glasses at the time, but the Navy had a program both for pilots and naval flight officers. I was in training for the latter, when Washington sent down a directive saying that the people who finished first through fifth in my class and the class behind me would have to go into intelligence because there was a shortage of intelligence officers in the Navy.

(U) This upset the aviators, but nevertheless, I was committed to the intelligence pipeline. So I began my career in 1963 as all young naval intelligence officers start off, as a specialist in intelligence. Of course, the Navy has two officer career fields built around intelligence, one in intelligence and one in cryptology.

(U) Did most of your subsequent assignments remain in the intelligence track, versus cryptology?

~~(S)~~ Right. In Navy terms, I'm an intelligence officer, a "straight stick" intelligence guy. All of my tours were Washington-based or fleet-based operational intelligence tours, including command of the Suitland Naval Operational Intelligence center, the predecessor to the Maritime Intelligence Center. I was also Director of Long Range Planning,

[redacted]

(U) And from there to Director of Naval Intelligence, followed by Director of NSA. NSA must have been your first full-time "technical intelligence" assignment.

(U) Well, naval intelligence is highly technical. The naval intelligence generalist in the Navy is brought up with the idea that most of the intelligence we deal with is technical. It's acoustic, it's SIGINT. Naval intelligence doesn't have much HUMINT, and much of what we have is overt. The HUMINT activities we do have in the Navy have always had to struggle to compete with technical intelligence. The cultural ethos of naval intelligence has always been technical, but within that technical framework, multidisciplinary, with emphasis on putting things together and building processes for moving that intelligence to the user. You need to have constant interactions with the user, and proximity to the customer is one of the most important dynamics of the system.

(U) So, I dealt extensively with SIGINT, and SIGINT issues, and SIGINT liaison throughout my career. So, there really wasn't a surprise to me when I came to NSA. What was different was getting to know the culture and the bureaucracy as a Defense agency, as a combat support agency, and as part of the Intelligence Community.

Another version of this interview was published at a lower classification level in *Studies in Intelligence*.

EO 1.4.(c)
P.L. 86-36

DOCID: 4011893

CRYPTOLOG
Winter 1996

(U) Did the Navy's emphasis on proximity to the user influence your actions as Director of NSA and later as DDCI?

(U) There is the sense that the SIGINT system is isolated, that it exists somewhere at Fort Meade. And to a degree, CIA has the same potential problem or at least the perception. One of the things the agencies have had to deal with is the need to be better connected with their customers on the one hand and their counterparts in the Community on the other hand. What you always worry about is the danger that an NSA, for example, becomes a closed culture. And you have to "manage around" that perception when you come into a leadership position in an organization like NSA or CIA as an outsider.

(U) How much of a struggle was that in your NSA and DDCI positions?

(U) It's not really that much of a struggle. I find if you appeal to people to reach out and consider those wider issues, they'll do it. Sometimes they need to be nagged, but throughout this period the idea of Community or corporateness has been so important that it couldn't be ignored or denied. Sometime you have to attach a "no kidding" message to this effort, but we really are required to build within the Intelligence Community an analog to the jointness efforts that exist in the military. This Community should operate as a Community; if it does, the whole will be greater than the sum of the parts. We are also clearly under the obligation to reduce duplication. Clearly, there was a lot of duplication in the system. So, I was fortunate in being able to work in one culture at NSA and then to come over here to CIA and the Community environment to work on projects that furthered the concept of community.

EO 1.4.(c)
OGA

(U) The analogy between the Defense community as its attempted to work out the problems of jointness and the Intelligence Community is an interesting one. Where is the Intelligence Community in that process, compared to a community that has been at the process for a longer period?

~~(C)~~ I think the Intelligence Community has made significant progress. The orientation of the leadership has shifted substantially.

[redacted]

[redacted]

(U) Certainly it would have been more common before 1991 or 1992 for an NSA officer to spend part of his or her career in the UK at Government Communications Headquarters [redacted] Is all this driving around the Beltway worth it?

~~(C)~~ That's an interesting question from several dimensions. [redacted]

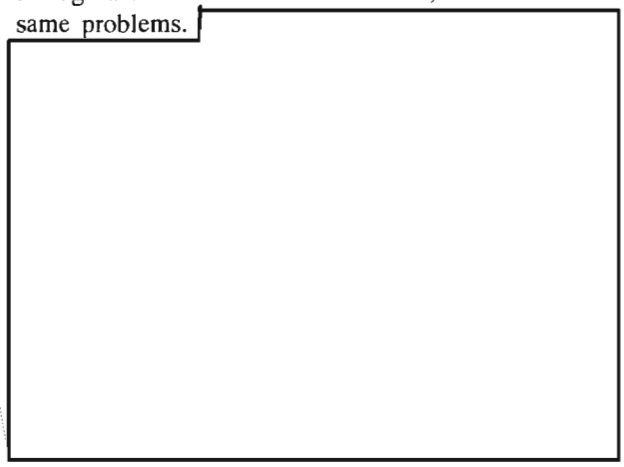
Point number two is that we are burdened by the fact that the Community is spread out from Fort Meade to the new NRO facility past Dulles Airport. This physical separation is a problem, because it keeps the culture apart. As much as we thought things like secure videoconferencing would solve the problem, that really hasn't been case. The truly frustrating point about the problem of physical separation is that it has the effect of keeping organizations and cultures that are actually very similar in character apart. [redacted]

(U) That's a sentiment I've never heard expressed.

~~(C)~~ It's true. I came to CIA after having been

DOCID: 4011893
E.O. 13526
P.L. 86-36

through a whole set of issues at NSA, and I found the same problems.



(U) The issues associated with the implementation of quality management, the requirement to get people out of their fortresses, and the degree to which the culture here, the needs of technologies, the family orientation of the personnel. You can go on and on. These are at least sibling organizations, from the point of view of management challenges.

(U) **Would you want to see the recognition of these similarities and the move toward jointness extend to the creation of a Foreign Intelligence Service, analogous to the Foreign Service, where people get hired into the service and then assigned to one agency or another?**

(U) No. I think an efficiency expert who doesn't know anything about the business areas of the agencies might suggest that. But I wouldn't. These are distinct business areas, each of which requires core competencies which are difficult to sustain even given the scale of the existing supporting cultures. The SIGINT and INFOSEC businesses, for example, are very complex. If you're going to discharge the responsibilities associated with those business, or any of the other business lines, in the Community, effectively, you have to establish a center of gravity. That means you have to establish accountability and coherence. Otherwise, you would find the business areas watered down by considerations that would make it difficult to keep focus on the various primary missions we're set up to deal with. It's just like corporate life: consolidation is important, but one must recognize points of diminishing returns. These are large structures, tens of thousands of people even with downsizing, so the idea that you could package all of this effort in a single structure is an idea whose time has not arrived, if it ever will.

(U) **You mentioned downsizing, and that is the environment you encountered both at NSA and as DDCI and Acting DCI. How serious a problem has that been for the leadership?**

(U) Let me elevate the question up a level: The fundamental problem of recent years has been moving the Intelligence Community from the Cold War to a different world, one that is not yet clearly defined. With that challenge up front, a whole host of issues present themselves, not least of which is "What is the world of tomorrow going to look like?" Ultimately, instruments like PDD 35 will define the grounds on which intelligence has to operate. During this time, we had to deal with downsizing and reengineering issues. And we had a number of problems, especially for CIA, and even more particularly for the clandestine service—with Ames, the French spying issue, Guatemala, class action suits or individual suits by women in the agency; and these greatly complicated the work of the leadership in making the transition the community.

(U) But that transition remained the most important objective. And I think the leadership of the intelligence agencies understood that. I certainly would like to think they understood that. We put heavy emphasis on studies and task forces to look at various aspects of the issue. By the time Jim Woolsey left, we're probably looking at upwards of 125 studies on various aspects for the transition problem, everything from politicization, to covert action. And that's the essence of the legacy of this transition period.

(U) I believe this effort has put us in front of the rest of the federal government in the reinvention effort. We started downsizing before anyone else did, and so on. Only history is going to tell us whether these actions were the correct ones, but I don't think we had any alternative but to make these transitions. We've gotten out ahead on issues affecting incentives in downsizing, with ideas on civil service reform, which I think Director Deutch is going to be talking about in the near future.

(U) We had a major task in shutting down much of the Cold War architecture and determining what our future architecture was going to be. There's been an incredible richness in the issues confronting us during this period, and they all come together to define the future of intelligence. None of the rest of the federal government is close to doing the sort of work we've done on our future.

(U) The problems we've encountered and the transition we've been dealing with has left a morale effect, and that's been part of the downside. But in the long

run, I think it's been fortuitous for CIA, and with it the intelligence community, to go through this process. At times it has seemed like we've been hit between the running lights with a two-by-four, but maybe that's been a wake-up call. The benefit may be that we will be reformed before anybody else. We have an opportunity to use our internal work, along with the work of the Aspin-Brown Commission, IC 21, and all the other external studies, to process this work, go forward with legislation where required, and gain a renewed endorsement for American intelligence.

(U) **Let's return to the endorsement issue in a bit, but it's very clear that you see all the effort and turmoil of recent years as ultimately necessary and even therapeutic.**

[redacted]

(U) **One part of your reputation that preceded you hear was your interest in management techniques, and your belief that we had not incorporated management practices, especially quality management in what we do. It won't surprise you to hear that some people do not share your enthusiasm.**

[redacted]

[redacted]

(U) **Let's go back to the endorsement. Beyond issues of internal management, there is always going to be some skepticism—in the Congress, among the public—that what we do is inherently suspect. Tolerable during wartime perhaps, but less so in peacetime.**

(U) I think you're getting at the openness and demystification issue, and there's no doubt we could have done a better job articulating to the American people and others who count, including the Congress, why we need a capable, robust intelligence system. What I worry about is that you can't assume we're going to make as a nation the commitment to intelligence we've made from the 1930s on. This was a heyday, in which intelligence made extraordinary contributions. Unfortunately, we've been so closed that I don't think this contribution is appreciated, either by decision makers, nor by historians, as well as by the country at large. We have an obligation to be more open—and we now operate under a directive to be more open. Openness is a difficult issue to manage, and you're always going to be struggling over where to draw the line.

(U) One of the things you don't want to do is be naive about how much people really know out there. The recent series of Baltimore Sun articles on NSA prove that if some serious investigative reporter wants to network around and do a serious look at an agency, the reporter can ferret out more information than the system is going to be comfortable with. That said, the example points to the dilemma of having to be more open, and if this is not a contradiction, in a controlled way. Jim Woolsey always cautioned about the use of the term "openness," because we didn't want to imply that we were fundamentally open to having people come in and just forage around. I don't think that's what we've meant by openness, but it's a difficult process to define what it means to be selectively open. It's a tricky issue. And a lot of it needs to be focused on the historians as we declassify.

(U) **One aspect of the endorsement issue is**

endorsement by oversight bodies, giving them a picture we cannot give the public at large and in effect having them vouch for us. How would you describe your experience with the oversight committees?

(U) We all have tactical frustrations, but I'm a big fan of oversight, whether its from the Congress, or from the President's Foreign Intelligence Advisory Board, or from within. The way I look at it is this: Intelligence, in order to do its job, has to be out there at the leading edge of propriety and legality all the time. Our obligation is to penetrate targets that represent threats to the United States. In order to penetrate those targets, you have to be very aggressive in your technology and in your operational concepts. You really want an oversight process to protect you from yourself, and in regard to resources, you might be able to determine that the interaction between the Congress and the Executive Branch has expended some taxpayer money, the product of that interaction has been more positive than negative. In fact, dramatically positive. So I have a very upbeat view of oversight.

(U) I do hope that the Brown Commission will come out with some recommendations to "thin down" our resource burden. The number of committees to which we are accountable for various functions creates a lot of drag for the Community, using resources that could better be expended on targets. As a manger, I want to put mission first. I told the Brown Commission that if you told me declassification would cost $200 million per year, and if I had the option to spend that on modernized SIGINT, I'd rather buy the SIGINT.

(U) We're headed toward a real investment crunch, and I would rather buy tooth than tail.

(U) **Where is that going to occur?**

[redacted]

(U) **One of the significant issues of the last decade has been the emergence of open source and its impact on policy makers. Have we managed that effectively?**

~~(C)~~ I don't think we've managed it at all badly.

[redacted]

(U) **If you had the opportunity to take on, at this stage of your career, a study to deal with any single aspect of our business that has nagged at you, what would that be?**

[redacted]

~~(C)~~ **Certainly, clandestine activity is the thing that has the highest risk for embarrassment, as you've experienced.**

EO 1.4.(c)
P.L. 86-36

(U) Sure, but there are structural changes you can make to manage this. Counterintelligence is another area of interest, and it's an area we tend to take for granted. The whole issue of foreign intelligence and its coordination with law enforcement, information warfare, information security (especially as it relates to commerce and banking)—there are any number of areas you could deal with. That's what makes this business so interesting at the moment. It means that DCIs now and future will have to build on the work that's been done by some of the studies we've talked about. No matter where you turn, there are interesting issues out there.

(U) Overall, how do you think we've done convincing Congress and others that this is a principled, competent set of agencies capable of performing its mission?

(U) I'm not trying to be political in making this statement, but I don't think we've been successful with the current administration in even being defined as being a relevant part of the national security team. And I'm sure the DCIs have been frustrated by it. When you have CNN announcing that the President is meeting with his national security team and you know intelligence is not represented, that's a source of concern.

(U) We've talked about a lot of ups and downs affecting intelligence in this transition period. If you were speaking to undergraduates or graduate students considering a career intelligence, would you encourage them?

(U) Nothing is more wonderful. I spoke this morning to the National Youth Leadership Forum, a group of high school students interested in intelligence, diplomacy, and defense. I concluded my remarks by telling them there was never a day—no matter how bad things got—that I didn't get up and look forward to coming to work in the business of intelligence. It's that fascinating. Particularly if you step back and truly understand its importance to the security of the country. And when you think about the nature and character of the people in the Community, nowhere in the federal government have I run across the skills and character, even management ability, that you'll find in the Intelligence Community. It's a unique set of people, and I think even those of us in the business need to reflect more frequently on that.

Kλ

The most recent presentation of IS-355 (Current Issues in SIGINT Policy) was an inter-agency conference on Responses to Humanitarian Crises: the Role of Classified Intelligence, co-sponsored by NSA, CIA, and the State Department. The opening speaker was Ms. Toby Gati, Assistant Secretary for Intelligence and Research in the State Department. CRYPTOLOG thanks Ms. Gati for permission to reprint her remarks.

Humanitarian Crises: IC Support to U.S. Foreign Policy

(U) Thank you, Mr. Taylor, and thank you, Elizabeth McGranahan, for organizing this conference. It is proving very timely given our high-level policy interest in Eastern Zaire's humanitarian crisis.

(U) I am pleased to see that this event is co-sponsored by NSA, CIA, and the Department of State because the foreign policy and intelligence communities are partners in tackling humanitarian crises. We work on different aspects of the problem, but we need each other if we are to respond in a timely, proactive, and cost-effective way. For the rest of the day you'll be listening to intelligence experts, as well as some important NSC and Pentagon customers, talk about the various roles of intelligence in shaping the U.S. government response to humanitarian crises. They'll give you case studies and specific do's and don'ts. My talk this morning will be on the basic issues that we need to understand before we can determine the appropriate role of classified intelligence in responding to humanitarian crises.

*(U) We need intelligence **before** massive refugee flows begin, [and] that's where the IC can help.*

(U) For example, when we look at a "humanitarian crisis," are we sure we all look at it in the same way? When does it begin and end? What is it we are trying to accomplish? Who are the key actors? How are they being served? What kind of information—open source, diplomatic reporting, non-governmental organization (NGO) reports—is most useful? And finally, what kind of intelligence is required?

(U) Case studies and post-mortems of such crises as Somalia, Sudan, Liberia, Bosnia, and Angola point out that humanitarian crises are complicated, messy problems involving a number of actors often working at cross-purposes. They also clearly show that many times at the bottom of the pile of humanitarian mission goals and logistical plans is the failure of the international community to make a serious commitment to tackle root problems.

(U) Rwanda is a case in point. We have been going around for several weeks now within our government and with other governments over a common plan for intervention. Many actors thought the main task was just feeding people—so what's the problem? After all, we did it in Goma in 1994; why can't we do it again in 1996? Well, Goma is not the same place now that it was then and we can't impose the same type of intervention. I remember that we wrote a memo in 1994 saying the repatriation of Rwandan refugees would be the international community's biggest headache if refugees could not be quickly separated from the Interhamwe Hutu militia and from former government soldiers. So the current crisis did not begin in the fall of 1996; it is not a surprise; and the fact that we have little information and were unprepared for it ought not to be a surprise either.

(U) So, while feeding several hundred thousand Rwandans is a key part of the mission, there is a lot more here that we need to grapple with—and that's where the IC can help. We need intelligence *before* massive refugee flows begin. We need good embassy reporting, analysis, FBIS reports, [redacted] defense attache assessments. We also need to take bet-

ter advantage of crisis-focused databases and assessments by *non*-intelligence agencies, particularly relief agencies who have experts on the ground.

(U) INR and the Department of State have supported one such crisis information system, ReliefWeb, which is an Internet-based, interagency network maintained by the UN Department of Humanitarian Affairs (**http://www.reliefweb.int/**). It aims to serve as a one-stop shop on the information highway for crisis-related information, including the latest UN High Commission for Refugees and NGO situation reports from Rwanda. The IC needs to appreciate the value of these kinds of databases for U.S. interests, and where appropriate help fund them.

(U) Military intelligence from DIA is also critical. For example, can we really think about sending the military in without knowledge of the military factions that are manipulating the refugee flows? Can we ignore the fact that among the refugees are several thousand who are guilty of horrendous murders? Some of these problems are being decided for us, putting policy-makers in the reactive rather than the proactive mode. For example, while we were arguing about how NOT to disarm the Hutu militia chiefs who were holding a half million hostages, the Zairian rebels went in and pushed 600,000 refugees back to their home villages in Rwanda; in two days they changed the whole context of the crisis—which put us and our allies in the quandary of how to respond to the new reality.

(U) Let's be honest, when the guys with four stars on their lapels get excited about a crisis as opposed to just curious, that's when people, resources, and dollars start to flow.

(U) For sure we will need to stay engaged after the refugees return. Their reintegration will not be easy, nor can we give up prosecuting those who have committed genocide. For the U.S. government, the crisis will not be over until we ensure a degree of stability and security in the region. For the intelligence community, it means we have to do more than count refugees with imagery or intercept military communications—it means putting the pieces of the crisis puzzle together. If the IC cannot provide analysis in a concise and timely way, we cannot help the policy-makers, and the lives of U.S. soldiers and civilians—some of whom are in Rwanda right now trying to figure out how to help—may be threatened.

~~(FOUO)~~ If for us at State this crisis began months ago, I fear that for the IC such crises all too often only begin when the Pentagon starts planning for possible military intervention. Let's be honest, when the guys with four stars on their lapels get *excited* about a crisis as opposed to just *curious*, that's when people, resources, and dollars start to flow. We at State deal with crises every day, especially in Tier 3 and 4 countries. We first of all try to *prevent* a crisis from getting to the point where our troops might need to go in. But diplomacy gets a lot less attention—though dollar for dollar, it is a much better investment for the taxpayer than it is to send in the cavalry and the intelligence support that goes with it. We know that a crisis begins long before the "CNN moment" of seeing starving babies on TV, but diplomatic interventions are tricky, frustrating, and drawn out. They do not provide very dramatic coverage—unlike the storming of a beach or airfield—but it could be preventing, at least for the time being, a civil war, which incidentally is the major cause of humanitarian crises.

~~(S-CCO)~~ If this makes sense to you, then ask yourselves: When the Great Lakes crises began, where were the resources for support to diplomatic operations? What happened to our African coverage in the last three years—to FBIS, [redacted] What were the unintended consequences of [redacted] and the Tier process? And then ask yourself: how have the State Department-related budget cuts—which since 1984 have resulted in a 51% funding decline in real terms—affected our ability to negotiate a way out of situations like Rwanda?

EO 1.4.(c)
OGA

OGA

(U) Our focus on the IC, on State, on Defense also has to be put in context, however. Relief organizations, NGOs and others were in Rwanda, in Zaire, in Burundi *before* the crisis and will be there *after* this crisis. They know a lot about the crisis and expect to be involved. We have to exert leadership—but also to recognize that part of our mission is to play a support role so others can continue to do their work. Their agendas do differ from ours, but we need to work together.

(U) This support function gives us two complementary roles, one overt and one covert. Overtly, we should be providing to our partners on the ground, including UN and non-governmental organizations, as much useful unclassified or declassified information as possible. Why? Well, it is NOT because we want to give away U.S. secrets to irresponsible UN bureaucrats (as some in the press seem to think). Let me emphatically state here that intelligence sharing—whether its purpose is to help tackle a humanitarian crisis or any other multilateral mission—has to be in the national

interest, or we should not do it.

(U) In this case, it is clearly in our interest to provide sanitized intelligence and unclassified products, such as LANDSAT and SPOT imagery, that can be used to help relief workers—who, after all, are working the front lines of a crisis. We should and we do carefully screen such intelligence-derived reports through an interagency process, but we have also provided unclassified data in a timely way. (An example of this has been the use of unclassified, updated maps showing locations of refugees and others in eastern Zaire.) This type of support has helped target the distribution of food, medicine, and water, which can mean fewer dying people, fewer costly logistical problems, and most importantly, a speedier resolving of the crisis, at least this phase of it.

~~(FOUO)~~ While the data itself might be unclassified, it still might require the IC's tremendous surge capabilities to collect it, organize it, and distribute it, in paper or electronic form. If the IC's goal in a humanitarian crisis is to help achieve U.S. foreign policy objectives, we have to think more strategically about what types of information—classified or unclassified—are most useful for what types of crises and how the IC's great information management strengths can be brought to bear on solving crisis-linked problems in Tier 3 and 4 countries where the U.S. government has a minimal presence. FBIS reports are an invaluable source of information on crisis-prone regions. We should be augmenting, not cutting, FBIS.

(U) Now, I'm not advocating *only* "open sources";

[redacted] Humanitarian crises always have a political dimension to them: they are often caused by power-hungry politicians and soldiers; relief efforts are manipulated by militias; and those who create the crisis are armed via transnational black markets. In sum, humanitarian crises are often the creations of not very pleasant and usually desperate individuals, and we have to deal with them in some way if we are to save lives and resolve crises.

ICRC

(U) The role [redacted] should be to help policy-makers work with or around these crisis manipulators—unless of course we want to take them head on, which doesn't seem to be a popular option these days because people get killed doing that. For the IC—and perhaps for this conference—this means that we need to come up with better intelligence on the motives, actions, and intentions of key players as well as a way to provide that timely intelligence back to our policy-makers in D.C. and out in the field who are trying to figure out how to intervene effectively. Just like the "open" information, good SIGINT or HUMINT can save lives by making us smarter than those trying to block our humanitarian efforts. It may be less direct, and I hope it would get much less publicity, but its importance in an overall U.S. humanitarian intervention strategy remains critical. At State, the presence of the Cryptologic Support Group helps us enormously to get SIGINT quickly. Now, NIMA and the NRO are working with us to get imagery to us, too. But until those same maps and satellite photos can get to our ambassadors "on the scene" with the same speed as intelligence gets to a general in the field, we are not doing our job well enough.

UNHCR

~~(FOUO)~~ Just as we need to know the intentions of belligerents, we also need to maintain a knowledge base about the context of the crisis. This would include databases on such variables as population distribution, agricultural production, land tenure, and ethnic composition; these are not necessarily "academic" types of information; we are finding out they are essential for effective crisis management and that they cannot be developed within a few days or weeks. In addition, we need to think about investing in shared sources of reliable, region-specific information (perhaps available through Intelink), and creating a roster of crisis experts ranging from in-house intelligence experts and linguists, to scholars and NGO relief professionals. But we can't rely on these people to fill in the gaps if *we* haven't done our homework first. "Surging" is not a substitute for knowing.

(U) Let me end by emphasizing again that today's humanitarian crises do not leave us with easily defined missions, clear roles for participants, and firm ground rules. They require determination, flexibility, and a serious commitment of resources. But they also require us to be smart about how we go in to help the victims of war so that we are not manipulated or ineffective.

(U) The job of the intelligence community is to help make policy-makers understand complicated and fast-moving events and to deal with the competing inter-

ests that make up a crisis. If you here at this conference contribute to that learning curve, you will have served our national interests well.

(U) Ms. Gati is responsible for analytic studies and intelligence assessments essential to foreign policy determination for the Secretary of State. She is also responsible for coordinating departmental programs of intelligence, analysis, and research with other Federal agencies. She has previously served as Special Assistant to the President and Senior Director for Russia, Ukraine, and Eurasian States at the National Security Council. She has been Senior Vice President for Policy Studies at the UN Association of the U.S. and is a published author whose works have appeared in various periodicals and books, including Orbis and The Washington Quarterly.

Look for ReliefWeb at http://www.reliefweb.int/

Unclassified

Emergencies
Bulletin
Resources

Map Center
Financial Tracking

Search
Submit
Forum
Comments

Help
About

Home Page
DHA-Online

Français

Last Updated
2 Jan 1997 1500 GMT

Welcome to ReliefWeb

Serving the information needs of the Humanitarian Relief Community.

ReliefWeb is a project of the United Nations Department of Humanitarian Affairs (DHA). The purpose of this effort is to strengthen the response capacity of the humanitarian relief community through the timely dissemination of reliable information on **prevention**, **preparedness** and disaster **response**.

- **Emergencies:** currently **18** events are being monitored.
- **Great Lakes Crisis:** The Latest - updated twice daily.
- **The Bulletin:** now available **via Email**.
- **Map Center:** contains over 150 maps.
- **Search:** full text search capability.
- **Financial Tracking Database:** updated Dec 1.
- **Document Submission System:** for posting documents to ReliefWeb.

We strive to update at 1200 GMT and 1800 GMT.
[Project Description] [Mandate] [Press Release]

Unclassified

Kλ

DOCID: 4011893

~~(FOUO)~~ *As the following article explains, FOLKLORE had its origins in IDASYS, developed back in the 1960's. A small team of operating systems specialists from NSA took IDASYS and molded it into an "industrial-strength" system on NSA's supercomputers of the time, mainly in support of the cryptanalytic community of users. A richly interactive and highly responsive system, it was a standout during an era of batch-oriented systems. It served a specialized set of NSA users for 25 years before the last FOLKLORE system was recently retired. It provided capabilities and features that some believe are still unmatched today, although it finally had to give way to the fast pace of technological change and the considerable resources that industry eventually applied to the supercomputing arena. There are still some old-timers around who can tell war stories from the FOLKLORE era and the successes that it enabled. FOLKLORE is a significant and rich part of NSA's heritage.*

[redacted] *DO Chief Information Officer and chief of E Group (DO Information Technology Applications Development and Support), participated in the development of NSA's supercomputer development; he was the first chief of the division that took over support for and maintained FOLKLORE.*

P.L. 86-36

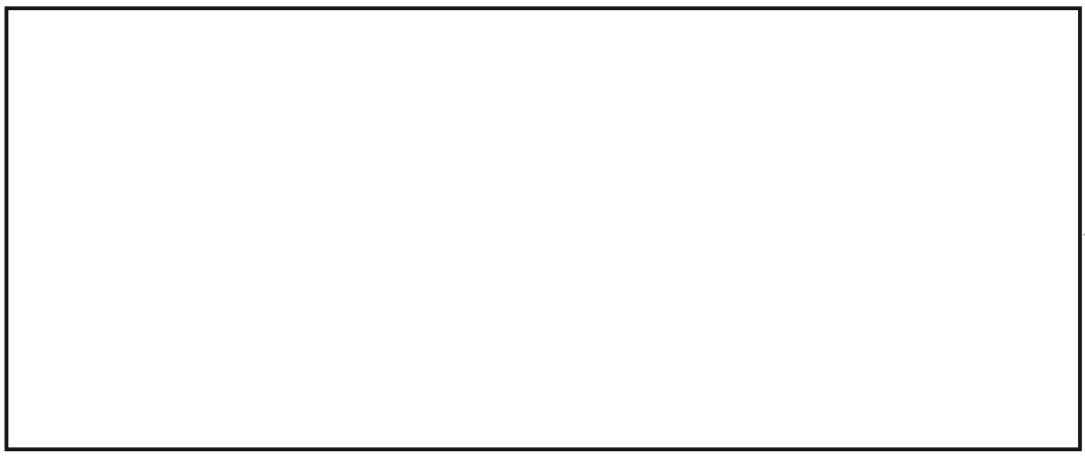
FOLKLORE:
An Innovative Approach To A User Interface (U)

by [redacted]

(U) The purpose of this article is to provide a historical perspective on the user interface characteristics of a 1970's operating system which was very responsive to its customer needs, extremely user-friendly, and anticipated many of the features that are common place today. Most computer operating systems developed prior to 1980 (before windowing systems) presented the user with a command prompt. Editors had to be explicitly executed. In contrast, the FOLKLORE operating system took a different approach. The edit and command modes were one and the same! All interaction was full-screen, not one line at a time!

(U) The IDASYS operating system (as FOLKLORE was known in the beginning) was developed in the late 1960s at the Communications Research Division of the Institute for Defense Analyses (CRD/IDA), Princeton, NJ. It was a highly interactive, multi-user system for the supercomputer of the time (CDC 6600). IDASYS was designed as a supercomputer operating system to provide full supercomputer responsiveness to the user. The target user population was the IDA and NSA cryptanalytic community. IDASYS was renamed FOLKLORE in the late 1970's when NSA took over full support and maintenance of the operating system. FOLKLORE was easy to learn to use for both end-users and software developers. It allowed a lot of flexibility and creativity to be put to productive use rapidly. FOLKLORE survived over twenty-five years. On January 31, 1996, still popular with its users and running on multi-CPU vector processor systems (Cray X-MP), the last FOLKLORE system was powered down.

(U) The user interacted with FOLKLORE through a terminal (CRT and keyboard) using a full screen display for both editing files and executing commands. In the early days this terminal was a directly connected CDC 210 terminal. Soon a Raytheon Programmable Terminal System (PTS) replaced the 210. The PTS terminal concentrators were eventually networked to allow access to multiple systems from one terminal. Finally, in the late 1980s, networked IBM ATs and SUN systems were used with a PTS terminal-emulation window. This last development enabled FOLKLORE for the first time to display high-resolution graphics on the user's terminal.



P.L. 86-36

(U) Since the PTS handled the character display and cursor movement, the supercomputer was free to handle only function key actions. This greatly reduced the number of interrupts that the FOLKLORE operating system had to handle. A FOLKLORE design goal was to deliver the full power (99%) of the system to the users and respond as if it were a single-user system. The PTS contributed a great deal toward meeting this goal.

(U) The window size was a maximum of 22 lines long and 80 characters wide. The lower two lines generally contained information such as file/program name, keyword and line number. This made the effective browsing window 20 lines. The FOLKLORE system input/output (I/O) functions for terminals were designed to make displaying 20 lines of data and/or two lines of information easy. Because the system I/O functions were readily available to FOLKLORE software developers, they could write interactive programs easily at a time when most users were interacting through decks of cards. Terminal I/O was a matter of filling a buffer with the data (which would appear on the screen) and issuing the function call. Other systems which had terminal access were generally graphics- or line-oriented and did not have many interactive programs except a few text editors and applications written by expert programmers.

(U) The FOLKLORE operating system handled all function key stokes simply by storing the value of the function key and some cursor-related information in a table. Programs then checked that table or asked to be interrupted when the relevant table entry was filled. The STOP key generated a program interrupt which could be handled via an error/interrupt handler or, as the default, the system would terminate the program and return the user to the editing state viewing a diagnostic page in a system file. FOLKLORE had a diagnostic file which contained an appropriate message, picture, or instructions with one page for every system error number. The FOLKLORE editor response to the STOP key was to display the beginning of a user-defined default file. Program error handlers often set the user environment to display an error message and allow quick access to the program output file.

(U) FOLKLORE function keys had names, not F1, F2,..., but STOP, GO, +PAGE, -LINE,... This encouraged software developers to use the same key for similar functions. The labels helped the user to remember which key did what. FOLKLORE software developers also made use of simple features which allowed them quick access to source code for almost every program, especially system-provided programs. Also, most programs could easily be called as subroutines. When a function similar to another was needed, it was simple to discover the underlying source, check related documentation for possible parameters, and copy as much or as little as desired. Much FOLKLORE code was reused because it was easy to do so.

(U) Upon successful login to a FOLKLORE terminal, the user generally saw the system news file. New information was placed at the beginning of this file so that the user would see it as soon as the logon process was completed. At this point the user could browse this file, type a file name to browse/edit another file, type a command to execute a program, or use one of the function keys as a shortcut to executing a command or editing a file. Whether a user could actually modify the file that is being viewed depends on whether the user has write-access to the file. FOLKLORE file access control has been covered in a separate paper, *FOLKLORE: One Approach to Security.*[1]

(U) The FOLKLORE editor, program loader and batch command processor were tightly integrated to

1. *Cryptologic Quarterly* Fall 1994, Vol. 13, No. 3.

DOCID: 4011893

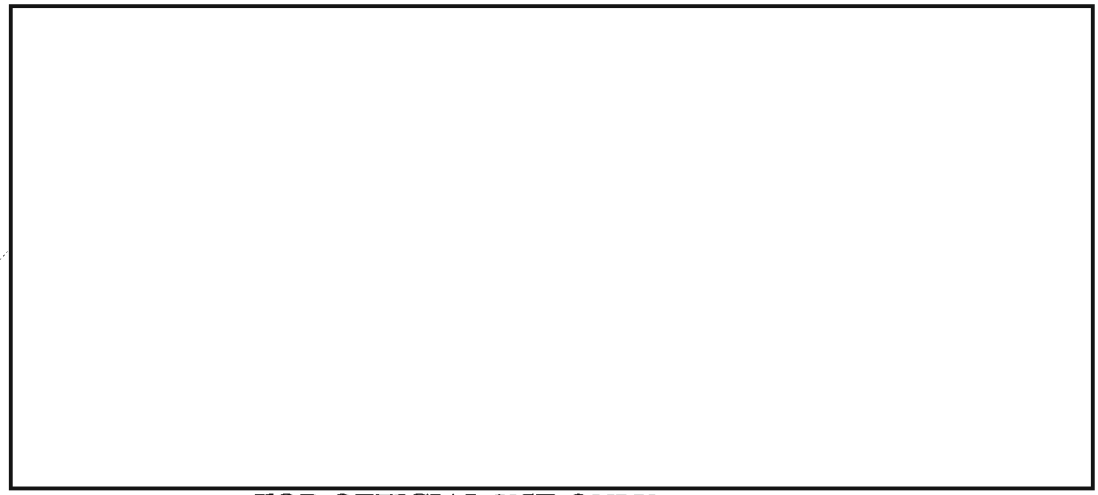
create a unified user interface. Although there were multiple editing processes, they all performed similarly. The actual process in use was determined by the function requested by the user, not by a specific command. Most of the editing services were provided through a single system daemon which handled every terminal (except the system console). For the purposes of this paper, all of the editing processes will be referred to as the FOLKLORE editor. This was the FOLKLORE interface. Every user interacted with it.

(U) The program loader was invisible to the FOLKLORE user. Commands were entered, the GO function key pressed, and the user was back (immediately in most cases) interacting with the editor usually viewing the program output. It did not matter whether the file associated with the command was a fully linked executable, a relocatable version of a main program, or a relocatable subroutine/utility. The program loader "automagically" figured out what to do and it happened quickly.

(U) Initially the FOLKLORE batch command handled only a serial sequence of commands, but it evolved to provide several types of error handling, nested sequences, and the usual logic constructs of today's command script languages such as the UNIX shells. The batch process basically passed each command line to the program loader just as the editor did and the editor returned control to the batch processor when the command completed. The user could tell what was currently being executed because the program loader displayed the program name in the information lines at the bottom of the display window.

(U) FOLKLORE did allow users to customize a few things. The user specified a file to be displayed when the STOP function key was pressed, a default file to be displayed via the ALT function key, a command to execute via the PROG key (to save typing a highly used program name), strides for the -PAGE, -LINE, +LINE, and +PAGE function keys, TAB stop settings, and a file to contain setup information. This setup file contained such information as a list of files to checksum, print header and classification definitions, and lists of files used to build and include program libraries. This customization information could be specified for multiple alteregos, so that the user could change his environment by changing the alterego that he or she was running under. (Alteregos are explained in the previously referenced article, *FOLKLORE: One Approach to Security.*)

(U) A design decision for FOLKLORE allowed unique features to be provided by the editor at very low cost. That is, FOLKLORE text files are contiguous files with an end-of-text string. There were no carriage return or tab characters embedded in the file. These keyboard keys were simply cursor movement keys. The carriage return moved to the beginning of the next line and the tab key moved to the next TAB stop. At the bottom of the display, all cursor movement keys wrapped to the top of the screen. In fact, all FOLKLORE files are contiguous files with no structure except that supplied by the application that produced it. The FOLKLORE editor can be used on any file. Of course, editing an executable file was something best done carefully, but browsing one could be quite useful. Since the FOLKLORE editor does not use carriage returns, but rather blank fills each line to the specified file width (usually 80 characters) some space may be considered wasted. This space was a small price to pay for the cryptanalytic tools that the editor could provide. The block text manipulation feature (BLK) was one very powerful tool. This was implemented in the mid-1980s through a function key and allowed manipulation of text in a rectangle of any dimensions. Common BLK functions were to move, copy, or delete columns of text.



~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

(U) One FOLKLORE function allowed the user to browse a document's index and move directly to a section of the document, in a fashion similar to using today's hyper-linked documents.

Another tool that depended on the fixed width lines was a KEY function which allowed searching quickly down a column. This function was used heavily for searching for left-justified keywords such as message starts. Another use was in browsing the index of a document, moving directly to a section of the document simply by putting the cursor on the line containing the title of interest and pressing the KEY function key. This is similar to using a mouse today with hyper-linked documents, but the cryptanalytic community could do this in 1970!

(U) Programs were executed via the GO function key while viewing a file through the editor. The program name and its parameters were parsed from the line containing the cursor up to the first blank character or the end of the screen. Changes to the display were not inserted into the file being displayed until the INSERT key was pressed. This allowed a user to do full screen command line editing. The user could maintain sample command lines in a file, display the file, edit the appropriate command line, execute it, and retain the original version of the command line. Of course the edited command line could be retained by pressing INSERT before GO if desired. The executing program automatically received some information related to the file currently displayed; the file name, the position of the window on that file, and the cursor position within the window. The program controlled the whole window while it executed. When a function key was pushed during execution, the program could find out the function key number, the cursor position within the window, and the four characters immediately preceding the cursor. FOLKLORE did not buffer function keys. Only the information from the last function key pushed was preserved until cleared or read by a program.

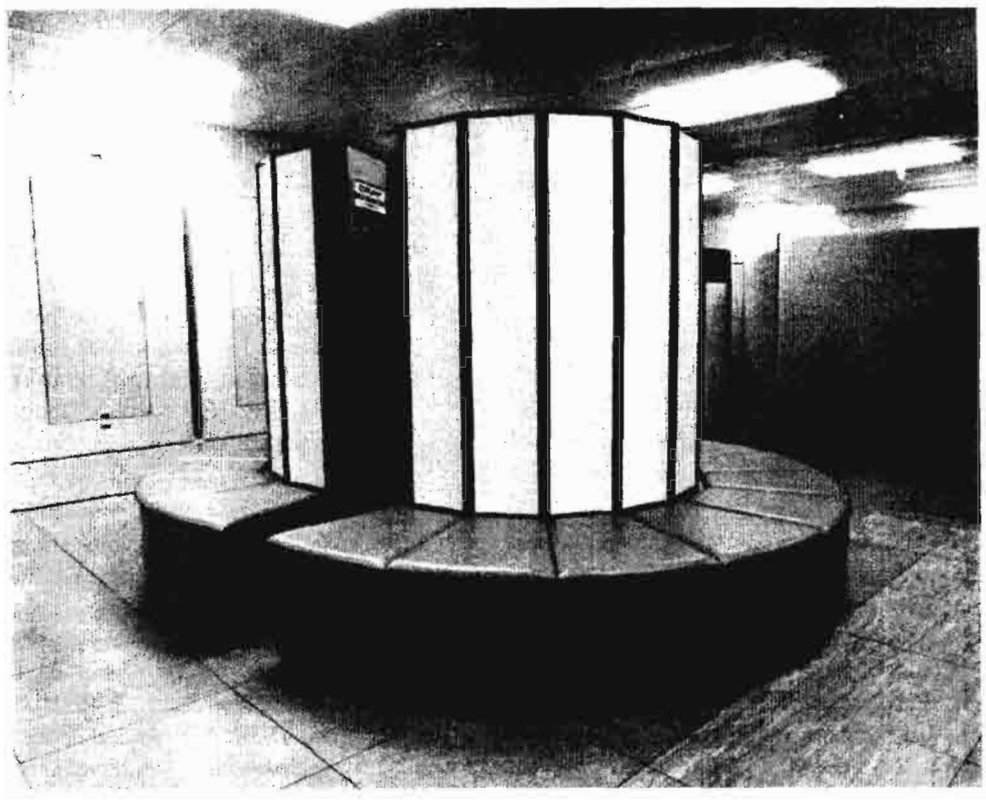
(U) FOLKLORE program source files were generally large files containing the source for many programs. The programs could even be written in different languages within the same source file. The only common thing was that each piece of source began and ended with a left-justified '%' character. Special functions took advantage of this. The SEND function key would quickly position the editor at the beginning of a particular piece of source code. Since this function searched for '%'s, it even allowed quick location of data sections which were delimited by '%'s.' Cryptanalytic applications often used this mechanism to maintain many parameter sets within a single flat file. Another feature that this scheme allowed was great for program development. That is the COMP function which could be used from anywhere within the piece of source code. FOLKLORE would automatically find the beginning of the code (previous '%'), determine the appropriate compiler from the keyword following the '%', and compile the program. In fact, if the GO function was used from anywhere within a piece of source code, all of the compile functions were performed, all the necessary relocatable files were located and linked, and then the program was automatically executed. All of this happened within seconds, so the user did not lose track of the real job that needed to be done. It was amazing how little delay the users were willing to tolerate after having developed experience with FOLKLORE for a short while. In fact, just five seconds was considered unacceptable most of the time. Another common practice, especially useful during debugging, was to keep a sample of the command line within comments at the beginning of the program source code. The user placed the cursor somewhere within the source code, pressed COMP to compile, then ALT to return to the top of the source code, moved the cursor down a few lines to the command line and pressed GO to execute it.

(U) Another commonly used FOLKLORE feature made possible by the responsiveness of the FOLKLORE editor was the use of the ALT function to compare files. The ALT function switched between the current file and the alternate file. The current file became the alternate file and the alternate file became the current file. By using the ALT button quickly, a user could easily spot any differences between the two files a whole page at a time. The screen would appear to stay constant if there were no changes and would flicker in the spots where there were differences. It was quite common to align

(U) Another very useful (and very much missed) feature was the command spelling corrector. If a command was executed that was not found, the system loader or editor would suggest a similar command or file name and gave the user several options for continuing.

DOCID: 4011893

~~FOUO~~



~~FOUO~~

~~(FOUO)~~ On 31 January 1996, still popular with its users and running on a Cray X-MP [redacted] the last FOLKLORE system was powered down. P.L. 86-36

two files, press ALT several times a second, watch to see if the screen flickered, move to the next page of each file, and repeat the ALT sequence. This process would be useless if the switch between files was not "instantaneous"! In contrast, using a file comparison tool could be a tedious series of executions with a varying offset parameter or it could be even worthless without an offset parameter or ability to work on binary data. Suppose a program was changed to insert a certain string of bits periodically in an output data file. These changes between the old and new output files could be easily spotted and verified using the FOLKLORE ALT method. Even if there would be no change in offset required, the FOLKLORE ALT method would sometimes be faster than typing a command. If there were differences, the user had a full screen of context to interpret the reason for the change. This method worked fine even for binary data. FOLKLORE had a different character displayed for every eight-bit sequence. Therefore, a change in one bit would cause a difference in the character displayed. This change would be seen using the ALT file comparison method. Bit-stream cryptanalysts were familiar enough with the character representation to understand what the difference was and why it was there.

(U) The move to the SUN workstations allowed high resolution graphics for the first time, but some FOLKLORE users edited speech waveforms graphically using the PTS terminals in the early 1980s. The responsiveness of the terminals even allowed some creative analysts to produce animated graphics!

(U) There were at least two important observations made in some research reported from IBM in 1982. First, as system response time decreases, the quickness of human interaction responses increases more than linearly. Second, all skill levels benefit from this effect. Also, as the skill level of the user increases, the benefit also increases. The cryptanalytic community was not surprised! They had been reaping these benefits for more than a decade by then. In fact they complained about losing their train of thought when anything slowed down by even half a second.

(U) What was the power of the combination of the edit and command mode? Commonly used commands could be stored in a file. The user's default/STOP file was often a list of these command lines. The user then simply used STOP to view the file and then selected the appropriate line with the cursor and pressed GO to execute it. Often applications would embed command lines or file names in the output to facilitate running follow-on programs or viewing multiple output files. This feature was very useful to reduce wasted time caused by mistyping or omitting parameters. BATCH sequences, a series of command lines beginning with "BATCH,**" and possibly including some simple control structures, were also stored in source code

P.L. 86-36

sections and executed via the GO key. This also greatly simplified the automation of modified source code installation. BATCH sequences were also developed and maintained in separate files particularly for use in production runs. These were initiated using "BATCH,filename" as the command line. When a BATCH sequence was initiated from within a file, the parameter was '**' and when it was initiated from somewhere outside the file, the parameter was the name of the file containing the command sequence to execute. (Actually there were more parameters, but they are not relevant here). The FOLKLORE convention used '**' to mean to input data from the current file beginning at the current location. A single '*' meant to input data from the current file beginning at the start of the file.

(U) Although having command lines stored in a file reduced a lot of mistyping and wrong parameters, another very useful (and very much missed) feature was the command spelling corrector. If a command was executed that was not found, the system loader or editor would suggest a similar command or file name and gave the user several options for continuing. Much of the time, the suggested command was the correct one, so only one key press was needed to correct the problem.

(U) Having a single edit/command mode simplified the life of the user. Only one set of behaviors had to be assimilated and repetitive actions could be stored for reuse. Efficient use of time for both the user and the computer was the result. The *de facto* standards for software development set by the operating system software and its user environment reduced the amount of deviation that develops between multiple software developers. Although FOLKLORE did not have some of the luxuries provided by today's custom environments and the use of COTS products, a lot less time was needed to set up a new user and to learn to use FOLKLORE effectively and creatively. This coupled with the effects of the extremely rapid response time, gave the cryptanalytic community a very productive quarter of a century.

~~(FOUO)~~ I would like to thank [redacted] for their review and very helpful comments.

[redacted]

[redacted]

P.L. 86-36
EO 1.4.(c)

Kλ

DOCID: 4011893

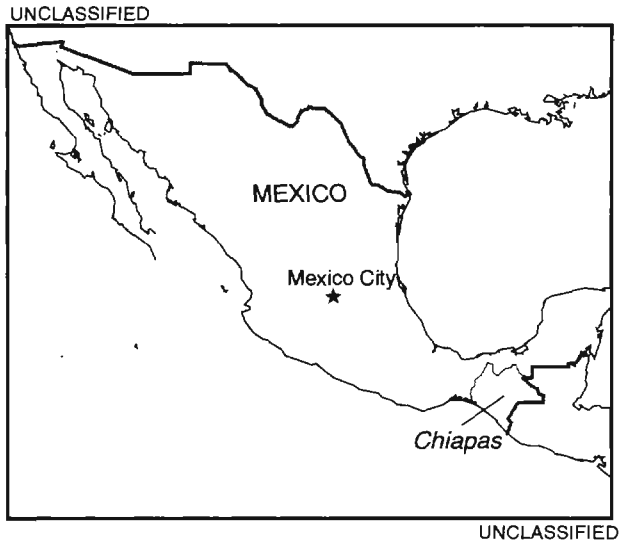
Church-State Relations in the Mexican State of Chiapas: Image v. Reality (U)

P.L. 86-36

by [redacted]

Introduction (U)

(U) The XIX International Congress of the Latin American Studies Association (LASA), which was held in Washington, DC, from 28 through 30 September 1995, provided a platform for renowned Latin American leaders, prominent Latin American literary and artistic figures, career diplomats and politicians, representatives of nongovernmental organizations, and academics to present their views on a broad range of hemispheric issues and topics of interest to students of Latin American culture. Four analysts from B3 were privileged to attend the LASA-95 Congress under the auspices of the DO Technical Health Advisory Board. As one of the four, the author had the opportunity to attend informative and thought-provoking presentations on topics including the transition to democracy in postwar El Salvador, the future of Nicaragua, Cuba-U.S. relations, post-NAFTA Mexico-U.S. relations (with emphasis on the border tension sparked by immigration policy), the future role of the Inter-American Development Bank and the Organization of American States (each presented by the organization's respective Secretary General), and the session that prompted this article: a personal view of the situation in Chiapas, the strife-torn state in the southeast of Mexico, as presented by a U.S.-born priest who was expelled from Mexico in June 1995 for allegedly inciting anti-government activities.



Background (U)

(U) In September 1992, when Mexico restored diplomatic relations with the Vatican, Mexican Government spokesmen attributed the step to Mexico's desire to promote friendly relations with members of the international community who shared its goal of world harmony and peace. The restoration of relations, which had been broken off for 128 years, was the culmination of a process that began in February 1990 with the appointment of personal representatives by then-President Carlos Salinas and Pope John Paul II to facilitate communication on issues of mutual interest and continued with the constitutional reform of 1991 that gave churches legal status.

(U) Then Secretary of Government Patrocinio Gonzalez Garrido, a former governor of the southeast Mexico state of Chiapas, declared in July 1993 that wisdom and tolerance should be the basis of government interaction with the Church, adding that the Mexican government's relationship with the Church was one of openness, harmony, dialogue, and respect.

(U) Such government pronouncements notwithstanding, the archbishop of San Cristobal de las Casas, Chiapas, Samuel Ruiz Garcia, saw little change in church-state relations in Mexico or Chiapas. Responding to a reporter's questions on 10 January 1994, Ruiz conceded that some progress had been made as a result of the constitutional reform, for example, in the acknowledgment of the Church's right to operate schools. Nevertheless, the archbishop maintained that the government's fundamental attitude toward the Church had been altered very little. In fact, Ruiz characterized Mexico's recognition of the Church as a cosmetic step taken only to make Mexico fit the image of a modern country worthy of membership in NAFTA.

DOCID: 4011893 EO 1.4.(c) P.L. 86-36

LASA-95 Roundtable (U)

~~(S-CCO)~~ Whatever one's opinion of the Church's role in what [redacted] the opportunity that LASA-95 provided on the morning of 29 September to attend a breakfast roundtable discussion with the controversial Archbishop Ruiz himself was one that would have been difficult to pass up. Several of us arrived early so as to get a seat at what was expected to be a very well-attended session. Anticipation grew as two members of the clergy entered the room, but neither was Ruiz. Soon it was announced that the archbishop's duties had prevented him from attending, and that Fr. Loren Riebe, a U.S.-born priest with over 20 years' service in Chiapas, was to speak in his place. Riebe was among a group of three non-Mexican Catholic priests working in Chiapas who were summarily expelled from Mexico in June 1995 for allegedly fostering anti-government activity.

EO 1.4.(c)

Unclassified

Unclassified

(U) **The EZLN's military campaign coincided with the implementation of NAFTA**

A Priest's Personal Perspective on Chiapas (U)

(U) Seemingly an unlikely advocate for the underprivileged of Chiapas, California-born Fr. Riebe, in contrast to the diminutive 71-year-old Archbishop Ruiz, is rather portly and appears to be in his mid-40's. He spent 4 years as a priest in Santa Monica before going to Mexico. After 2 years in Tenejapa, he became the priest for some 22,000 parishioners in Yajalon, where he served for 19 years before being deported.

(U) Life in Yajalon for the indigenous peoples, as described by Fr. Riebe, is one of toiling for the equivalent of $1.50 per day on coffee plantations and cattle ranches owned by a few wealthy land barons; being victimized by a corrupt health system and an ineffective education system; and seeking escape in alcohol. In a society where the oligarchs not only control all the good land but also run the judicial and police systems and fill the mayoral and gubernatorial positions, Riebe's parishioners were ripe for political mobilization, but since the indigenous peoples never come to a decision without due consideration and prayer followed by still more thought, it took a few years for them to mobilize. They flocked to the Socialist Workers' Party when it organized in Chiapas, but when a 10,000-man march for peace in 1992 failed to get any media coverage it became clear that the only way to focus attention on their grievances was to resort to more violent action, such as roadblocks and demonstrations. Still, Riebe noted, confrontations in 1993 were not publicized because of the negative impact such developments would have had on the NAFTA negotiations.

(U) When the Zapatistas finally decided on military action, they chose 1 January 1994 to launch their campaign, not only because Army troops could be taken by surprise after the revelry of New Year's Eve but also because it marked the implementation of NAFTA, which the peasants expected to exacerbate their poverty. Fr. Riebe believes that when the Mexican government was subsequently unable to attribute the armed insurgency to external influences such as Communist Cuba or Guatemalan guerrillas, it began a witch hunt among the clergy.

[redacted]

Fr. Riebe's Account of his Arrest (U)

(U) On 22 June 1995, the day of their arrest, Rodolfo Itzal, a Spanish priest with a church in Sabanilla, had been at Fr. Riebe's home and had left with some children from the parish in a Ford pickup truck belonging to the church. Soon after, Mexican police overtook the truck and pulled Itzal from it, apparently on trumped-up charges concerning ownership of the vehicle. Fr. Riebe was contacted and asked to go to the scene with the documentation on the truck. When he arrived, around 3 o'clock in the afternoon, he was detained by plainclothes police. State judicial police (PJE), whom Riebe characterized as "thugs," subsequently arrived with machine guns. Refusing to explain the charges against the priests, the PJE placed Riebe blindfolded, on his knees in the back of a flatbed truck and put Itzal in the cab and drove them to the state capital, Tuxtla Gutierrez, from where they were flown to Mexico City and then deported to Miami. This treatment stands in stark contrast to the former Chiapas governor's description of the government-church relationship as one of openness, harmony, dialogue, and respect. Although the priests were not beaten, Riebe confessed that he was very tense and fearful throughout the ordeal. In retrospect, he noted with a laugh, the only thought that had gone through his mind was, "Why Miami?"

Riebe's Forecast for Chiapas (U)

(U) Discounting allegations that outside influence, whether from Central American revolutionaries, drug traffickers, or the Church, is responsible for the Zapatista movement, Fr. Riebe expresses the belief that the Indian population of Chiapas has accepted responsibility for its own future, has become very good at organizing politically, and is quite capable of carrying on its own rebellion. The time to act has come, he says; the indigenous peoples are challenging the old way of doing business and there is hope that their situation will improve.

Epilogue (U)

~~(C)~~ Although Fr. Riebe was not told prior to his expulsion from Mexico the nature of the charges against him, nor did he in his comments during LASA-95 allude to any illegal activities, the Mexican Secretary of the Interior told the U.S. ambassador to Mexico on 27 September (just 2 days prior to Riebe's appearance at the LASA conference) that the Mexican Government has specific complaints against Riebe of incitement to seize land and threats to parishioners who refused to support such seizures. Meanwhile, Paul Nadolny, another American priest, was refused re-entry to Mexico in September after a month's absence from Chiapas. The Mexican Government, which claims to have incontrovertible evidence of illegal activity by Nadolny, opted not to execute an arrest warrant against him but instead to refuse to allow him back once he had left.

Conclusion (U)

~~(S-CCO)~~ The future of the Chiapas peace process is uncertain; progress to date shows that the pace will be slow and painstaking. Moreover, whether or not Fr. Riebe and his colleagues exceeded the bounds of their pastoral duties, or how the Church's activism in Chiapas will affect church-state relations is difficult to determine. What is clear is that opportunities like LASA-95

[redacted]

[redacted]

Kλ

P.L. 86-36
EO 1.4.(c)

Book Reviews (U)

James Miles. The Legacy of Tiananmen; China in Disarray.
Ann Arbor: The University of Michigan Press, 1996. 379 pp.

reviewed by [redacted] P.L. 86-36

(U) The legacy of Tiananmen continues to provoke debates and prompt further analysis about China's current status and its future development. *The Legacy of Tiananmen; China in Disarray* by James Miles is an excellent addition to these debates and adds to our understanding of contemporary China. In this book, James Miles looks at factors contributing to instability in China, while keeping the lessons of Tiananmen in mind. The Oxford University-trained China-watcher believes that the events in 1989 offered the world a unique opportunity to look at some crucial aspects of China that had long been only dimly perceived. The event briefly illuminated the mood of the public, the workings of one of the most secretive political parties in the world, and the personalities of Chinese leaders before the veil once again came down. Taking the revelations from the Tiananmen incident as a point of departure, Miles examines the different aspects of China and its society. He identifies and describes the political and social tensions underlying and engendered by China's economic boom and contends that what happened so unexpectedly in 1989 should alert us to the fact that an economic boom does not necessarily bring stability in its wake. Although he concentrates largely on domestic issues, Miles also discusses Beijing's efforts to resolve these problems that will have a crucial bearing on China's future and its relations with the outside world.

UNCLASSIFIED

UNCLASSIFIED

(U) Miles calls China today as volatile as it was during the June 1989 turmoil

(U) Miles' analysis has led him to believe that China is now facing the most uncertain period of its political life since the Communists came to power. He joins others before him in stating that the death of Deng Xiaoping will mark the end of a leadership system dominated by veteran revolutionaries whose authority rests on careers dating from well before the Communist takeover in 1949. Those fighting for power after Deng's death are, on the whole, younger men who played little, if any, role in the civil war that brought the Communists to power. Deng's strength, like Mao Zedong's, has depended to a considerable extent on his credibility within the military, built up during his years as a commander and commissar. Deng's designated civilian successors, however, do not have any combat experience and will not enjoy similar support.

(U) Drawing on insights from historical analysis, Miles regards the 1989 incident as one of the periodic upheavals in which China struggled to find a modern identity and come to grips with the outside world. As a result of his own examination, Miles believes that the

~~SECRET~~
EO 1.4.(c)
P.L. 86-36

UNCLASSIFIED

UNCLASSIFIED

anti-government protests in 1989 arose out of a conflict between the fast-growing aspiration of the urban population and the conservatism of an aging and inward-looking leadership, which in many aspects still operates like the old imperial court. The demonstrators in Tiananmen Square wanted an end to corruption, a press that was free to report on real problems, and a government that listened and responded to concerns about everything from inflation to political representation. Miles concludes that Deng's economic boom has done little to address these concerns, thus leaving unresolved the tensions and problems that likely will trigger chaos.

(U) Furthermore, Miles contends that cracks have begun to appear in China's political structure which will open the Pandora's box of rivalry, hatred, vengefulness, and a myriad other destructive emotions just as in some of the former Communist countries of Eastern Europe and parts of the former Soviet Union. He believes that factional rivalries, ideological rifts, personal enmities, and other related problems are already apparent in the Chinese Communist Party (CCP). Public contempt for the party and cynicism about its policies are pervasive; corruption is rampant and uncontrolled and uncontrollable economic explosions are already occurring. Miles further believes that these problems will multiply and intensify, and that China will not have such leaders as Mao Zedong or Deng Xiaoping who can lead it out of chaos.

(U) Miles concludes that China today remains at least as unpredictable and volatile as it was at the outset of the Tiananmen Square protests. Deng's economic reform and development policies have aggravated social tensions and weakened the party's grip; the gap between rich and poor and between rural and urban is widening; and the people, including public officials, have lost faith in the party's future, especially in its ability to meet their basic needs. Miles believes that China in the late 1990s is a country deeply unsure of where it is going, because Chinese politicians and the public are already asking themselves whether China is emerging as a new economic superpower with global influence, or if it is heading toward the chaos they so much fear. Miles argues that chaos is more than likely, given the existence of factors contributing to instability, and as many such chaotic situations have occurred in China's history. He, in short, judges that if chaos ever results in the collapse of the Chinese authority as it did briefly in 1989, the poor and the discontented would be among the first to take to the streets.

(U) It is not surprising that Miles arrives at a pessimistic conclusion about China and its future development, given the fact that he focuses his attention only on what he considers as factors contributing to instability and chaos in China. He basically got what he looked for and did an outstanding job putting together a fairly well-documented, theoretically plausible, and thought-provoking book about contemporary China. No one can ignore or dispute the destabilizing factors resulted by Deng Xiaoping's economic policy. He, however, purposely ignored the positive aspects and consequences of Deng's policy, and failed to understand the dynamics of Chinese politics and China's overall socioeconomic developments. China today is nowhere close to where China was at the onset of the 1989 Tiananmen protests; nor will it in the near future likely resemble the situation that culminated the tragedy. On the whole, China today is more democratic than at any time in its history; and economic inequity and regional disparity aside, the Chinese people are economically far better off today than they were before. The current leadership also possesses an effective mechanism of control backed by the military and the public security forces. An equally strong and credible case can be made in favor of China's ability to manage these factors and avoid chaos while continuing its current economic transformation. While positive changes in China are at a slow and evolutionary pace, they are increasingly evident and likely will appear more frequently, especially at the local levels, if stability continues in China.

UNCLASSIFIED

UNCLASSIFIED

P.L. 86-36

(U) Deng Xiaoping's policies have weakened party's grip.

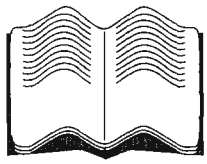
(U) Miles acquired his information for this interesting book from both Chinese and English books and newspapers published in China, Hong Kong and the West. Other sources include his interviews with Chinese officials and ordinary citizens, as well as his observations made during his eight years in China while working as a journalist, mostly with the BBC. However, it is impossible to verify the credibility of some the people interviewed by Miles, since their true identities are not revealed; nor is it possible to establish with confidence the reliability of the information divulged by his oral sources. Nonetheless, this book is well-written, highly readable, and thought-provoking. It is, in short, a valuable contribution to current China research and to the understanding of contemporary China, and I recommend that the NSA library acquire it.

(U) James Miles wrote this book after living and working in Beijing as a journalist, mainly with the BBC, for eight years. He completed his work while on a fellowship at the University of Michigan. He is currently the BBC's Hong Kong correspondent. He began his journalistic career in China shortly after he received his education in Chinese studies from Oxford University in England.

~~(S-CCO)~~ [redacted] *is a participant in the Senior Technical Development Program (STDP), currently undergoing intensive training in the language and reporting fields. He was the* [redacted] *prior to his selection into the STDP Program. Other Agency experiences include language processing and reporting. He is a Master in Intelligence Analysis and a Master in Language in the DO Technical Track Program. His formal education includes a B.A. in history from Vanderbilt University, and a Ph.D. in political science and Asian studies from the University of Notre Dame.*

Kλ

DOCID: 4011893



Robert M. Clark. Intelligence Analysis: Estimation and Prediction
Baltimore: American Literary Press, 1996. 340pp.

Reviewed by Bill Nolte

(U) What do you get when you cross an engineer with a lawyer? Well, you may get one heck of an information gatherer, but you might want to be forewarned about the delivery technique.

(U) We have become accustomed to intelligence history becoming a matter of public record; we should not be surprised to see more and more about technique and process. Nor should we be either surprised or concerned to see our techniques and processes demystified. If what we are about is the collection of information on demand, the processing of that information in some way, and its delivery to the customer making the demand, then we operate in a process very much like those used by stockbrokers, detectives, and medical diagnosticians, among others.

(U) Robert Clark, a former CIA analyst, has attempted to reduce the analytic elements of the intelligence process into something of a text, with emphasis on the analysis of scientific and technical intelligence. As such, it may represent a useful primer for those who have found themselves thrown into the process in some form or another with little opportunity to step back and look at the process itself.

(U) But this is a textbook, and someone should have told the author that the publishing gods freed textbook authors of the requirement to be pedantic and boring some time ago. Or maybe some authors simply freed themselves, the great Yale historian Donald Kagan, to cite an example.

(U) At its worst, Clark's book reminds the reader of the poetry text skewered by Robin Williams' character in *Dead Poets Society.* Audiences will remember the scene where he had his charges rip from the book its first chapter, the one with the x, y graph to be used for plotting a poem's greatness. *Intelligence Analysis: Estimation and Prediction* could only have improved on that graph by making it three-dimensional, adding a predictive coordinate.

(U) "At its worst," implies the existence of some elements that avoid that fate. The book includes a series of Analysis Principles and Case Studies that give it some measure of life. The Principles include everything from Occam's Razor to Newton's First Law, which the author applies to organizations as well as physical bodies. Some of these are puzzling: if the focus of the book is on analysts doing scientific and technical work, a paragraph or two on "S" curves would seem unnecessary; it is the larger, non-S&T-analytic community that could find it beneficial to have their toes dipped in some methodological rigor.

(U) The Case Studies are intelligently selected, described, and applied, deriving from both the intelligence experience (Pearl Harbor) and external, industrial (the development of DOS) experiences. Purists and specialists will probably go crazy at the shorthand description of some complex events, but such imprecision is almost a relief from the expository portions of the book.

(U) Looking for a primer on the analytic process? This could be your book. Looking for "a good read?" Probably not. Finally, the publishing gods, even the minor deities associated with smaller presses, should be ashamed to permit the publication of a text of this sort without a table of contents.

~~(FOUO)~~ *Mr. Nolte, DDO Senior Intelligence Advi-*

Kλ

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

Editorial Policy:

(U) Technical articles are preferred over those relating to management, shorter over longer (under 3,500 words). Emphasis should be on improving NSA's technical performance; articles should be aimed at explaining developments in one's career field to those outside it. Readers are invited to contribute conference reports and reviews of books, articles, software, and hardware that relate to our missions or to any of our disciplines. Editorials are also welcome, as is humor. Submissions may be published anonymously, but the identity of the author must be known to the editor.

Submitting Articles:

(N.B. If the following instructions are a mystery to you and your local ADP support is no help, please feel free to contact the CRYPTOLOG editor on 963-5283s or cryplog@p.nsa.)

~~(FOUO)~~ Send a soft copy via e-mail to **cryplog@nsa**, or send a hard copy accompanied by a labelled diskette to the editor at P02 in 2C099, Ops. 1.

Guidance:

For maximum efficiency (as far as possible within the limits of your word processor):

- Classify all paragraphs.
- Do not type your article in capital letters.
- Label all diskettes, identifying hardware (operating system: DOS, UNIX), density and type of word processor used, filenames, your name, organization, building, and phone number.
- FrameMaker format is preferred; ASCII text is also fine. *(FrameMaker users: while we welcome graphics, please include them in the file as separate objects rather than in Anchored Frames as these frames are nearly impossible to reformat to our standard.)* The editor will be happy to e-mail a CRYPTOLOG template on request. Another option is to use J33's document conversion service (CLEANEX); instructions for e-mailing files for coversion can be found at **http://www.j33.j.nsa/q6/q623/cleanex/clean.html**.

DOCID: 4033694

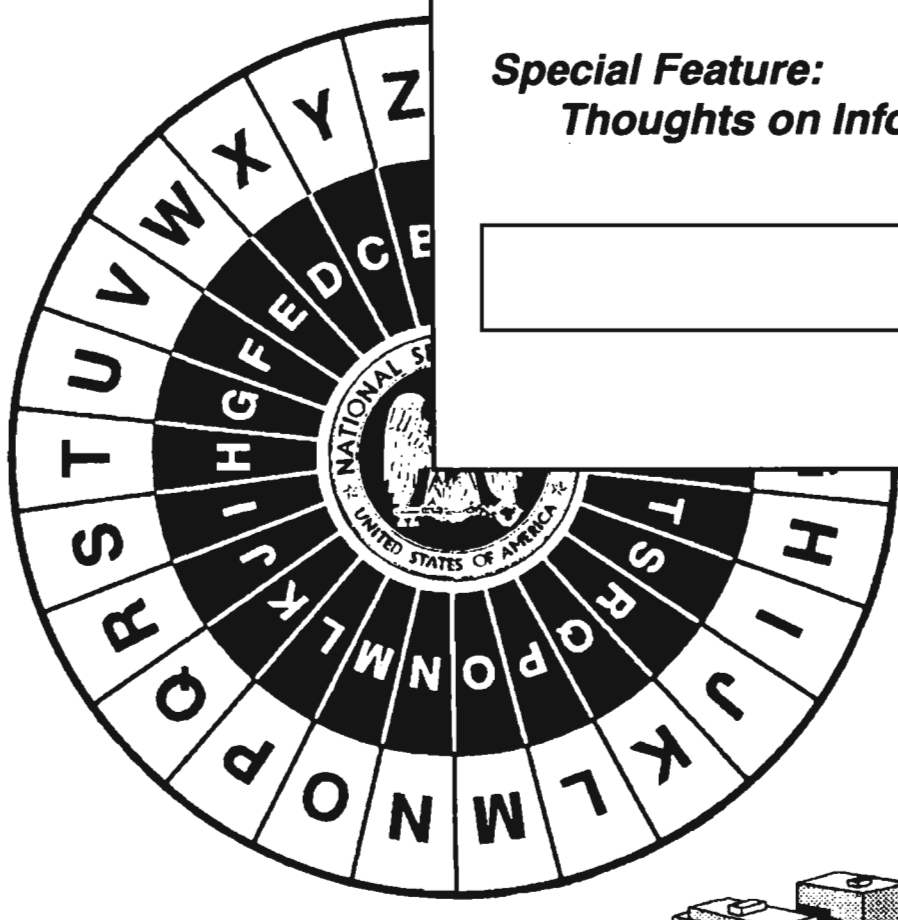
~~TOP SECRET SPOKE~~

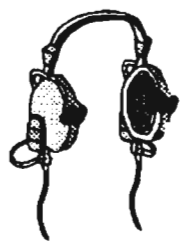
NATIONAL SECURITY AGENCY

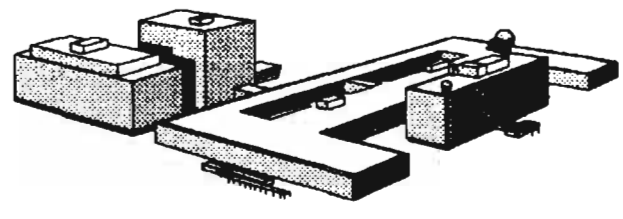
CRYPTOLOG

The Journal of Technical Health

Vol. XXII, No. 2 SUMMER 1996







Inside This Issue:

Interview With the Deputy Director ***Page 1***

Special Feature:
Thoughts on Information Warfare ***Page 6***

Page 27

. . . . . and more!

P.L. 86-

~~Derived From: NSA/CSSM 123-2~~
~~Dated 3 September 1991~~
~~Declassify On: Source Marked "OADR"~~
~~Date of source: 3 Sep 91~~

Declassified and Approved for Release by NSA on 10-10-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4033694

CRYPTOLOG

Summer 1996
Vol. XXII, No. 2

Published by P05, Operations Directorate Intelligence Staff

Publisher ..... William Nolte (963-3123)

Editor ..... [redacted] (963-3123)
Graphics ..... [redacted] (963-1359)

P.L. 86-36

Board of Advisors

Chairman ..... [redacted] (963-7712)
Computer Systems ..... [redacted] (961-1051)
Cryptanalysis ..... [redacted] (963-7243)
Intelligence Analysis ..... [redacted] (968-8211)
Language ..... [redacted] (963-7667)
Mathematics ..... [redacted] (963-1363)
Signals Collection ..... [redacted] (963-5717)
Telecommunications ..... [redacted] (996-7847)
Member at Large ..... [redacted] (968-4010)
Member at Large ..... [redacted] (968-4010)
Member at Large ..... [redacted] (961-8214)
Classification Officer ..... [redacted] (963-5463)

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

To submit articles and letters, please see last page.

DOCID: 4033694

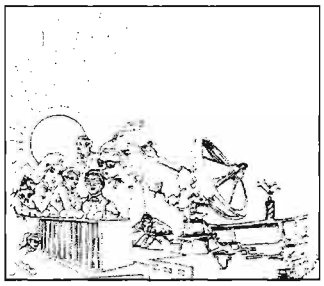


Table of Contents

Confronting the Intelligence Future:
An Interview With NSA's Deputy Director (U), by [redacted] *1*

Special Feature: Information Warfare (U)
NSA Hosts JIWTAWG Conference (U) *6*
IW: The War of the Future (U), by [redacted] *7*
Some Thoughts on IW (U), by William Black *10*

Joint Reporting and Inter-Agency Collaboration:
Moving Out of the Box (U), by [redacted] *12*

An OPENROAD to Research (U), by [redacted] *15*

The Changing Timbre of Conflict and Conflict Resolution
in Sub-Saharan Africa (U), by [redacted] *21*

Calling All Publishers! (U) *26*

[redacted] *27*

An Appeal From the Editor (U) *34*

P.L. 86-36

DOCID: 4033694

Perspective:

Confronting the Intelligence Future (U)

An Interview with William P. Crowell, NSA's Deputy Director (U)

by [redacted]

P.L. 86-36

(U) Let's start with some background: how you got into intelligence and your career at NSA.

(U) I was recruited out of college, which makes me like the majority of the professionals at NSA. It was something of a personal thing. I was so intrigued by the test NSA offered, I said to myself "Any organization that can create a test like that must be an interesting place to work." And so I decided to have the interview. I've never been disappointed, at least not for very long.

(U) And you have worked in private industry?

(U) I left here and went to a high-tech corporation, working in four areas: imagery (that's where I got my chance to learn the imagery field); low observables; mathematics research; and command-and-control systems. I started a business line that broadened their intelligence interests beyond imagery into other areas, including signals intelligence.

(U) But you're not, at least in formal terms, what one would consider a technical person.

(U) No one believes you ever have a life before you come to work at NSA. But I did have a life before I came to work at NSA. I worked for a communications company that had two major lines of work. One was designing and developing commercial communications—radio communications systems, and multi-user systems. And the second thing they did was they built [spy systems].

(U) I think the thing that's missed about my background is that I used my prior technical experience to my advantage while at NSA. In particular, more than anything, I wanted to do computer work, so in almost every assignment I've had here I was the person bringing in information technology or expanding the use of technology. I've been writing software since the early 1970s in a range of fields, including signals analysis and others, and I've never lost that interest. I still spend ten or fifteen hours every week maintaining my programming skills.

(U) Everyone was so quick to predict that the post-1945 period would be the "atomic age," but missed the coming significance of the computer, which, one can argue, has proven a far more influential technology.

(U) I had a conversation recently with the head of one of the largest of the computer corporations, and it was not until the 1950s that we began to develop a viable commercial computer industry. They had grudgingly and reluctantly modified some of their equipment so we could do computing at NSA.

(U) Can you identify two or three areas of greatest concern—make-it-or-break-it issues—as you look to the future of the Community?

(U) Let's center in on information systems and their impact on the two missions of this agency, protecting U.S. information systems and exploiting foreign information systems. One of the biggest challenges we face is balancing the two, particularly since what we do in the Defense Department and in other areas of the US government can influence the commercial market place. The systems or techniques that we develop have the capacity to come back on us in the form of increasingly sophisticated target systems. So that's one challenge I think is more than a little significant. How to draw a policy to balance those two issues is extremely important to our continued success—on both sides.

(U) The second issue is that information systems are becoming increasingly complex. For example, most communications engineers believe that it's a lot easier to ensure an error-free transmission over modern networks if there is an equal number of 0s and 1s in the communication string. And therefore they almost all—after taking lots and lots of channels, and packing them together in time or frequency, and compressing and otherwise

DOCID: 4033694

manipulating everything in ways that are very complex and hard to undo—add randomization in order to get an equal distribution of 0s and 1s. And randomization looks very much like encryption unless you know the way it was randomized. So, it's the complexity of all the different layers of modern information systems—whether it's the information layer, the compression layer, or the signal technology layer, or the randomization layer—that together present a real challenge to the SIGINTer. What you're saying is "undo all of this," and it's exceedingly difficult.

~~(C)~~ Let me add to all of that the third biggest challenge facing us, and that is volume. And I could just end the sentence there and everything is said.

That gives you some idea of the daunting challenge volume presents, forcing us to look for new technologies.

(U) **You don't have to go too far into the public literature to find people saying "volume wins," that the challenge to NSA and its counterparts around the world is going to be overwhelming.**

(C) Volume will never win, the reason being that volume is not the only way the world is constructed.

(U) If you don't believe that, go surfing the Web, with something you absolutely want to find, with no Web Search tools. You'll find out why someone developed Web Search tools.

(U) **One can probably find predictions of the impossibility of codebreaking going back into the 1920s.**

(U) In the 1950s, when microwave and other point-to-point communications systems were being developed, it was absolutely said that NSA would go out of business. But as a result of those communications systems, more modern means of collection were invented. When satellite communications came along in the 1960s, we developed ways of sorting through the enormous volumes of communications: dishes on the ground capable of intercepting those signals, and so on. So, in my view, virtually every communications system that has appeared on the scene, while presenting challenges, at the same time offers extremely exciting possibilities.

(U) **Do these challenges require different relationships within the Intelligence Community?**

~~(C)~~ The new information systems do not allow NSA to conduct its mission from a great distance from the target and in a totally passive manner. Therefore, the partnerships we have, let's say first with the military services, because of the need to mix tactical access with national capabilities, must become closer.

This is absolutely essential, absolutely essential. There's no backing away from that, no matter how the supporting bureaucracies may feel about it.

(U) **Do you occasionally feel resistance?**

EO 1.4.(c)
P.L. 86-36

(U) I've spent the last five years trying to tamp down that resistance, with some limited success. But I'm more persistent than they are.

(U) **But the argument would be, to give it its due, that we have to put extraordinary emphasis on protection of our information, and this of necessity limits how we share and how much we share.**

(U) I think that's an outmoded way of thinking. It's outmoded for several reasons. First, the partnerships I mentioned are essential. You can't succeed without them. And if you can't find a way to share the information essential to the partnership, then you ought to be prepared to sign up to go out of business. Second, the successes you may be trying to protect—the important sources and methods—have always been and will always be short-lived. You may be able to extend their life somewhat by closing the circle to absolute minimums, but you'll also restrict usefulness. And you'll

also restrict the opportunity to be successful the next time, when you're facing one of those inevitable changes.

(U) When you were deputy director for operations, you coined the phrase "SIGINT that counts," touching on what you were just saying. To acquire information, process it, and then hold onto it in such a way that it's not useful is not much of a public service, is it?

(U) I have two great fears for the future of the SIGINT system, and I challenge the system as much as I can to react to and mitigate my fears. The first fear is that we will collect what is easy to collect and pretend it satisfies our customers, instead of going after the hard-to-get (politically or technically) information they really need. The second fear is that we'll get the information and then go back to the old days of "tossing it over the transom," as Admiral Studeman used to say, or sending it to the customer and saying "Well, I finished my job. They got it." We need to realize that we have an obligation to make sure customers get the information, they understand it, and they use it.

(U) Pearl Harbor can be described as a cryptanalytic success but a cryptologic failure, in that the ultimatum message was read in time but the information got to the commanders several hours after the attack. That's a terrible but vivid model.

(U) It's absolutely an important message for us to have learned. The other message, one that comes later, and from other wars as well, is that we don't always know what the person at the other end needs. If we rely exclusively on our picks of what to send them, as opposed to relying on their ability to ask us questions or even go through our data bases to find what's important to them, we'll probably fail.

(U) Are you comfortable with a system in which the customer judges the success or failure of NSA?

(U) I've always been comfortable with that, as long as the customer is judging success within their area of interest. I don't think we should ask the Commerce Department to judge our ability to support military operations, nor do I think we should ask the military to judge our ability to support economic policy. But, yes, even if we didn't realize it, customers have been making those judgments and affecting our budgets all along.

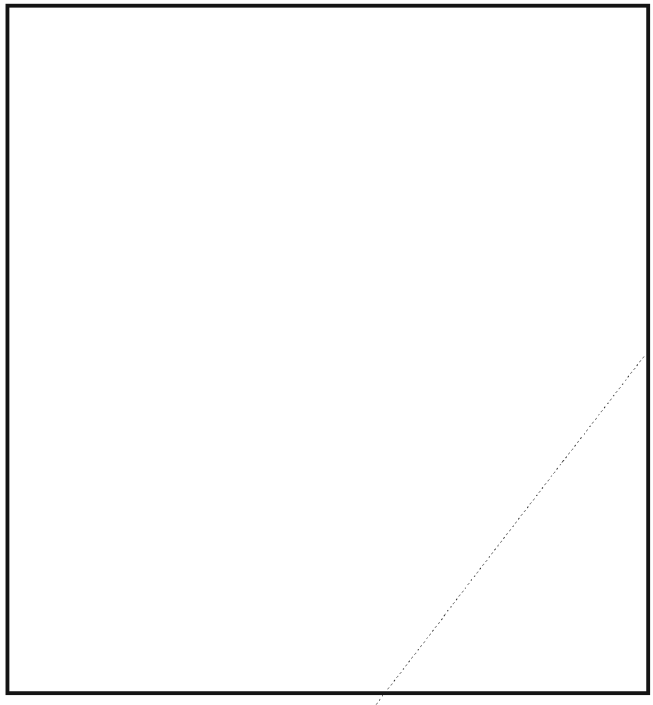
(U) More so now?

(U) But more now, particularly since the demise of the Soviet Union. With that demise came several things, the drawdown of resources, the shift of priorities, and shifts in thinking about essentiality of intelligence.

(U) Aside from the volume issue, one of the things you must hear—from the academic community, and the press, for example—is that we're experiencing a shift in the value of information. That presidents will be reacting to open-source information, on the Internet or on CNN, and that the relative value of covertly acquired information declines.

(U) I'm not particularly interested—if I may call myself a consumer of intelligence, and I think I am—in things that have already happened. I'm interested in two sets of things: those that will affect my future choices. And those aren't all going to come from open source. Second, I'm interested in those things that haven't happened yet because they're in planning. I don't think all the important information about critical, developing events are going to appear in the open.

(U) I also think one of the things we try to do too often is to pit one information source or one intelligence source against another, as if it would be possible for us to "pick a winner," and do away with all the other sources.



(U) Has the Community been successful in making the case, before Congress, among others, that we have provided information of value commensurate

EO 1.4.(c)
P.L. 86-36

with our costs?

(U) I think that at this moment NSA and the community in general have strong stock with Congress. But there are areas of weakness we need to shore up. These range from [redacted] to our ability to cooperate.

P.L. 86-36

(U) DCI Deutch has reaffirmed his support for a policy of openness. How have we been doing with that?

(U) Recently, we've done better. Obviously, the VENONA releases were quite significant moving in the direction of recognizing when a story can be told. And that's essential. We're not going to become irresponsible. But we are going to become more responsible for being positive in our ability to recognize when stories can be released. What is often forgotten when we talk about protecting sources and methods is why we're charged to do that. Having spent the public's money to develop certain capabilities, the public expects us to maintain those capabilities as viable, as long as we possibly can, and to release those capabilities only when they no longer serve an intelligence purpose. That's an economic issue, but we often turn it into a passionate issue of different proportions.

(U) Not only do we have to change that attitude, because of the recent executive order on declassification, but, and this is a very strongly held personal position, we owe it to the American people to contribute to history what the intelligence community has done, once sources and methods are no longer an issue.

(U) VENONA is a classic example of how we can tell the story and convince the public that intelligence, at least historically, had an impact on the direction of the country. The direction of the world, for that matter.

(U) On VENONA, there was a cost to the U.S. of retaining that information, in that many Americans grew up believing there was no Soviet spy effort.

(U) As you know, I was involved with VENONA twenty or twenty-five years ago. It was one story I believed would have to be told one day. It will never end the debate, but now it's in the hands of the historians to make the judgment, not us.

(U) Let's talk about the creation of a national imagery agency. What can NSA provide in the way of lessons learned?

(U) Both Admiral McConnell and I have tried to be extremely helpful and balanced in our presentations, discussing the realities of the SIGINT stovepipe.

~~(S-CCO)~~ The realities are we don't own everything. And of course everyone who wants to reorganize the community into a new stovepipe wants to own everything, because control makes it a lot easier to get on with things. But the real strength of NSA is technical leadership and technical direction over the many people who are engaged in SIGINT, including many whose budgets are determined outside the Consolidated Cryptologic Program. [redacted] I think the imagery problem has to be solved in a similar way. They'll need to decide what the technical issues are and who decides them. What are the resource issues and who will decide those?

EO 1.4.(c)
P.L. 86-36

(U) Is it fair to ask about pitfalls you've warned about?

~~(C)~~ There are some very large pitfalls, with regard to the relationship between a National Imagery Agency and the organic resources within the military services, the picture taking aircraft and so on. How do you balance the need for services dependent on those resources with national needs to ensure that there exists interoperability and compatibility between systems? That will be a very tricky area, as it has been for SIGINT for a very long time. Not yet solved!

(U) The second area we've cautioned them about is when does an image become "intelligence," as opposed to "imagery intelligence?" How do you judge when someone is doing imagery intelligence as opposed to all-source analysis? We know how tricky that one is.

(U) That raises the question of the stovepipes and the bridges across them.

(U) The term "stovepipe" is very unfortunate. What we are talking about is various sets of professional and technical expertise. And we're talking about building a system of systems, one of which is a SIGINT system that has all of the necessary ingredients of training and development and science that has to do with SIGINT. It's obviously best to put all of that into one organization where it can be nurtured. The same is true of imagery, and of HUMINT. You don't want signals intelligence officers out walking the streets collecting human intelligence. They don't have the training or the background.

(U) Where do you build the bridges of cooperation and teamwork? My view is at every level across the stovepipes, instead of trying to build them on top of the organizations. You look for teaming opportunities, whether in the collection arena, in the analysis arena. We need to share technology, we need to share information, and we need to share policies.

(U) **You want to encourage people to develop their strengths in a given field, but not to act in ignorance of other fields, correct?**

(U) Exactly. That's why the bridges have to be built at virtually every level across the stovepipes. You can't just build them on top. You can't have the DDI at CIA and the equivalents at NSA and DIA as the places where the bridges are built, because what you get is three stovepipes with a plank on top.

(U) **When you look to the future and the need for technical leadership, what are your concerns?**

[redacted]

(U) **At what point does this become damaging?**

(U) It's already beginning to have negative effects. Obviously, people coming in from colleges and universities, while not able to tackle our hardest problems, are more up to date on the latest technologies, and are able to bring whole new ways of looking at things to our problems.

(U) Back to the main question, neither NSA nor CIA will ever get people out of colleges and universities—or business, for that matter—that are sufficiently trained or seasoned in this business. We'll always have to invest in specialized training and development. In that regard, I think NSA's strength is our professionalization system, which codifies that training in very identifiable directions.

(U) **As you look at problems you've dealt with over the last four or five years, how pleased are you with the progress made in transition?**

(U) That depends on where you sit. Some people outside the intelligence business may feel we've accomplished a lot, with relatively few tools and relatively little flexibility in making resource decisions. I'm personally disappointed at how long it's taking. Most people within the agency are stunned by how quickly this is occurring and would like to see parts of the process slow down.

~~(C CCO)~~ Why am I disappointed in the pace? We are drawing down, we have ever fewer resources. It is no longer possible to push decisions off into the future without it costing a great deal in the way of a continuing resource burden.

[redacted]

EO 1.4.(c)
P.L. 86-36

(U) **It would not be hard to find critics of those decisions.**

[redacted]

P.L. 86-36

(U) **Any last thoughts?**

(U) One of the things I'll throw in as that I had the opportunity to work at CIA in the Operations Directorate early in my career, and have spent a great deal of my time in the intervening years working closely with the DO and the Science and Technology Directorate. As a result of those experiences and based on my analysis of what we face in the future, I believe the partnership between CIA and NSA can work. It requires commitment at the top of the organizations, and buy-in at the bottom of both organizations. I don't think that's been achieved yet, but it is absolutely essential to both agencies.

Kλ

Special Feature: Information Warfare (U)

P.L. 86-36

NSA Hosts JIWTAWG Conference (U)

by [redacted]

~~(FOUO)~~ The National Security Operations Center (NSOC) and the Information Systems Security Organization (ISSO) hosted the Joint Information Warfare Threat Analysis Working Group (JIWTAWG) conference in September. NSOC and ISSO requested to host this conference to further NSA's understanding of the Information Warfare (IW) threat and the integrated role that NSA can play with the Community on this issue. [redacted] This focus marked a milestone for the working group and will serve to further the exchange of information throughout the IW Community.

~~(C)~~ Lt. Gen. Minihan gave the keynote address titled "Ensuring Information Superiority for the 21st Century." He energized the working group by challenging it to: [redacted]

EO 1.4.(c)
P.L. 86-36

security into one. Following DIRNSA's talk, Deputy Director for Information Systems Security Mr. Thomas McDermott addressed the working group, building upon the ideas presented by the Director and stressing that the ISSO is moving toward those goals.

P.L. 86-36

~~(FOUO)~~ Each of the Services and several civilian agencies discussed their computer incident response team's structure, mission, and specific requirements for intelligence to support their missions. Also several NSA offices discussed the current support they provide and their visions for the future. [redacted]

~~(FOUO)~~ Over 200 visitors and NSA personnel attended the conference, which was the third in a series of working group meetings [redacted]

~~(FOUO)~~ To get further information about this or upcoming conferences contact [redacted] at 963-5243s or [redacted] at 963-5609s.

Kλ

P.L. 86-36

P.L. 86-36

Information Warfare: The War of the Future (U)

by [redacted]

(U) Information Warfare poses the greatest threat to the national security of the United States. Our society today, whether it be in the defense or the public sector, is becoming more technologically dependent. The immediate need for information and information systems to make decisions, to communicate, or to simply survive as a culture has exponentially grown during the last 40 years. Reliance on these expanding information systems has increased our vulnerability as a nation and analysts in the Intelligence Community are ill-prepared to deal with this new "War of Future."

(U) Those who try to fit Information Warfare into existing terminology and concepts do not accept that IW is something new.

(U) Our political and military leaders have always relied on information to plan and fight traditional battles, but the technological-dependency from which our nation suffers has made us more vulnerable to our adversaries. The "Information Age" in which our country finds itself today has led to the belief that all future wars will be information wars, and the winner will be the nation that achieves information superiority over its adversaries. That superiority is reflected in both an offensive (attack and/or exploit) and a defensive (protect) venue. Which leads to the question of how to define Information Warfare (IW)? No one appears to have a concise, clear-cut answer, and if one were to ask 50 different people that question, 50 different definitions would be supplied. The updated draft of Department of Defense Directive 3600.1 (originally drafted in December 1992) defined IW as "actions taken to achieve information superiority by affecting adversary information, information-based processes and information systems while defending our information, information-based processes and information systems." (However, not all members of the Intelligence Community (IC) could agree on the definition, and the phrase "computer networks" is to be added.) Part of the confusion in defining IW is that people try to fit IW into existing terminology and concepts, and do not accept the fact that IW is something new. The commonly held belief that IW and command-and-control warfare (C^2W) are interchangeable is a misconception that, unfortunately, is held by a large portion of IC analysts. The definition of C^2W is divided into the disciplines of attack, exploit and protect. While C^2W is a subset of IW, its disciplines are not encompassing of IW. In order to update the concept of IW, it has been divided into the following: Information Engagement (destroy and disrupt); Information Control (corrupt, deny, and deceive); and Information Assurance (defend and protect). IW includes components such as jamming/interference, physical destruction, disinformation, deception, intelligence operations, computer intrusion, and viruses/malicious codes. What analysts sometimes fail to realize is that all information systems must be considered as targets for IW, although computer systems are the most likely target, especially in the United States, where computers run our nation's infrastructure and economy.

[redacted]

EO 1.4.(c)
P.L. 86-36

P.L. 86-36
EO 1.4.(c)

Unclassified

Unclassified

(U) The most harmful computer virus will not be the one that stops your computer, but the one that randomly changes or corrupts your data over time.

P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)

EO 1.4.(c)
P.L. 86-36

[redacted]

[redacted]

(U) The main point is that an IW attack can come from anywhere in the world, whether it be initiated by groups or individuals, during peace or wartime. The motivation for an attack can be based on the need for recognition, political, economic, or military gain. At this time, the IC is focusing on state-sponsored attacks or plans. However, one can not overlook the individual hacker who has been hired by a foreign government to initiate an IW attack. The Internet has also become a vast resource of knowledge with hacker bulletin boards posting the latest "how to break in" information. Non-state actors, such as terrorist groups, drug-traffickers and political dissident groups, have begun using the Internet as a source to gain worldwide sympathy, supporters and funds, as well as to pass secure communications to their counterparts around the world. Pirated software can also be acquired through connections on the Internet, including several encryption software packages.

[redacted]

[redacted]

Kλ

P.L. 86-36
EO 1.4.(c)

EO 1.4.(c)
P.L. 86-36

DOCID: 4033694

Some Thoughts on Information Warfare:

A critique of *"Some Cautionary Thoughts on Information Warfare,"* an article in the Winter 1995 *Airpower Journal*

by William B. Black
Chief of IW Technology Center

one team, one mission

(U) As revolutions go, so far it has been bloodless. Its battle flag waves from the pages of magazines and newspapers, and its war cry resounds in briefings and speeches. It is a revolution sparked by the digitalization of communications, and fueled by the proliferation of computers and advances in technology. It is the Information Warfare revolution. Kinder, gentler folks call it Information Dominance, Information Assurance, or Information Superiority—regardless, its strategy is the same: seek and maintain the ability to exploit, corrupt, or destroy an adversary's information systems while, at the same time, protecting the integrity of one's own. Like all revolutions, this one has noble purposes: national security and national infrastructure sanctity.

(U) "Revolutions," however, are examples of change. The authors of "Some Cautionary Thoughts On Information Warfare," an article in the Winter 1995 *Airpower Journal*, are apparently uncomfortable with any change, much less a "revolution." Military historians by trade, Messrs. DiNardo and Hughes attempt to point out the problems with the IW "fad." To do this, they examine a selection of open source publications ranging from Tofflers' *War And Anti-War* book and Newt Gingrich's speech at the National Defense University to various magazine articles in *Military Review*, *Army Focus 94*, and *Airpower Journal*. They see IW developing along two lines: a) as developments to "digitize the battlefield," improve "smart" weapons, and provide "deeper-look" intelligence; and b) as an alternative to more traditional forms of war where information can be used as a weapon. It is the latter notion that is of particular concern to the authors. The article then discusses the problems of using information as propaganda (their idea of information as a "weapon"), the difficulty of defining military operations which are non-lethal, and the complications of IW in the civil liberties arena. The authors point out that information has always been valuable to the commander, that "digitalization of the battlefield" brings the danger of data-overload, and that the capability of a high-echelon commander to directly control low-echelon activities fosters micro-management. They disagree with the notion that IW plays a significant part in the Revolution in Military Affairs (RMA) concept that is currently being discussed in the Defense Community. Finally, as an alternative to this IW "fad," the authors stress the importance of commanders having moral courage, of soldiers being well trained and motivated, and of the operation being properly planned and executed.

(U) Unfortunately, their view of IW is shallow. Their mistake is that they never bother to understand what IW is, or how and why it has come about. Explained away by noting that "there is much additional material, including the very definition of information warfare, lurking beneath the shroud of secrecy,"[1] the authors are content to point out the historical mistakes in Tofflers' *War And Anti-War*,[2] to criticize those who find philosophical support in the writing of Sun Tzu, and

1. R.L. DiNardo and Daniel J. Hughes, "Some Cautionary Thoughts on Information Warfare," Airpower Journal 9, No. 4 (Winter 1995), p. 70.
2. Alvin and Heidi Toffler, War and Anti-War, (New York; Warner Books, 1993).

to condemn technological-based options to warfare. Equally important is that they apparently have little or no knowledge of computers, computer networks, modern communications, or information systems. While the authors mention some of the key issues, e.g., the importance of information in warfare, and the use of IW as an alternative to traditional warfare, their comments and criticism of such subjects are based on their understanding of history, specifically the Civil War and World Wars I and II. Lastly, it is hard to argue with the authors' alternative to IW—moral courage, training, motivation, planning—except to say that it ignores the advances in and application of information technology to warfare—advances and applications that will surely continue well into the next decade.

(S) NSA's ultimate success depends largely upon how quickly and completely SIGINT and INFOSEC merge into one in order to handle the information technology explosion of the 21st Century.

~~(S)~~ In the next decade, the requirements of NSA's customers will be largely the same: high-quality, timely intelligence information and high-security cryptographic products and services. The difference, however, will be that the environment which provides the intelligence information and the environment which is protected will be almost identical. NSA's ultimate success at meeting its customers' needs depends largely upon how quickly and completely today's separate missions converge into one in order to handle the information technology explosion of the 21st Century.

Kλ

DOCID: 4033694

CRYPTOLOG
Summer 1996

Joint Reporting and Inter-Agency Collaboration: Moving Out of the Box (U)

P.L. 86-36

by [redacted]

(U) Many forces are propelling us toward new approaches to intelligence production and reporting: oversight committees' criticism, reduced resources, increasing workload and the complexity of intelligence issues. The report of the Aspin-Brown Commission, for instance, criticizes the fact that intelligence agencies tout the virtue of a "Community" approach to intelligence but continue to function as independent systems. Many, both inside and outside the Agency, have been urging that we find new ways of doing business. A9 is preparing for the future by setting the stage for successful collaboration among intelligence producers, both within NSA and across agencies. In addition to explaining the rationale behind joint reporting efforts, this article describes some of the projects under way that are designed to improve the effectiveness of our SIGINT reporting.

Managing the Direction of Change

"A limpet has been a limpet for millions of years. It is a 'success,' but it will never compose a symphony; it is perfectly what it is and it is stuck there."
—Anonymous

(U) The reaction of much of the NSA workforce, both analysts and managers, to collaborative reporting reveals a misapprehension about the need for this effort that leads to the illusion of a dilemma: We can do more collaborative and joint reporting but this will be a drain on the resources needed for day-to-day production. This assertion is false and betrays a lack of understanding about why we need to make this change.

(U) Collaboration isn't something for which resources must be found; it is a production process which will save resources and make the best use of analytic knowledge, whether it is used for long, hard-copy reports or for short intelligence pieces (daily product). It is not going too far out on a limb to say that in the near future there will be fewer analysts and managers but the amount of work will be the same or greater (greater in any case for those remaining). Inevitably the importance and stature of analysts will grow. But more cannot be asked of fewer without serious consequences for our production. Collaborative work is a way out of this discrepancy between need and numbers. The difficulty is that we are not structured for collaboration: our offices and group structures are historical artifacts, not entities created for maximum efficiency; we do not have a working population experienced in collaborative work; and the required information technologies are not in place. Let's examine these issues a little more closely.

(U) The National Research Council studied large-scale collaborations in the scientific community and defined collaboration as a system "linking people, computer-based tools, electronic information, and facilities to support remote, distributed, intellectual teamwork." It is important to note that the NRC definition relies heavily on the presumed existence of a robust system of electronic information exchange between dispersed participants. This is because it is only recently, with the widespread use of Internet and collaborative software, that "distributed, intellectual teamwork" has become practicable. What information technologies can now give us is wide connectivity, multimedia, shared tools and shared access so that the participants can benefit from each others' knowledge, insights, data and information. But while technology can *impel* collaboration it cannot *compel* it. This leads to the second subtext of the NRC definition: that the participants are mutually predisposed to collaborate and freely share information. In other words there must exist "a communal relationship that implies social trust and synergy among participants with mutual benefit as the result." As the Intelligence Community now stands (and this applies to intra-NSA collaborations too) these necessary conditions are not

DOCID: 4033694 EO 1.4.(c) P.L. 86-36

widely found. There is little sense of communal relationship, little social trust (reporting elements often view each other as competitors), and no perception of mutual benefit perhaps because there is no mechanism for rewarding collaborative behavior. A9's collaboration initiatives are designed to address the need for this "enabling culture" as well as the need for implementing technologies.

Evolving the Work Culture

(U) The greatest challenge facing any effort toward collaboration, whether it is between offices in a single agency or among agencies, is that, technology aside, the enabling culture is embryonic at best. Whether this culture can evolve along with the collaborative technologies is moot; those technologies are already far ahead of the current work culture's ability to utilize them fully.

(U) A frequently voiced concern of managers and analysts about joint reporting goes something like, "How will we get credit for a joint report?" Various means of giving credit are already available to us; for instance, multiple by-lines can be added to a report (we have found that customers greatly appreciate this). To allay these and other fears, we can use the successful collaborations in the scientific community as a model. The NRC points out that "from a societal perspective, science advances through extensive, timely sharing of data"—and, we would add, sharing of ***knowledge*** as well—"but to advance as individuals, scientists must use their own data to the fullest extent possible before sharing them with others. Given such constraints, it can be difficult for scientists to openly share data in recognition of communal interest." The same situation exists in our agency among our analysts. To solve these problems, the large-scale scientific collaborations developed a well-defined set of "rules of the road" for their collaborations.

~~(TS-CCO)~~ Drafting guidelines to facilitate consolidated reporting within A9 is one of the goals of the EU Consolidated Reporting Advisory Team (EUCRAT), which is composed of analysts from throughout A9. The EUCRAT members have come to realize that, to be most effective, analysts need better communications, flexibility, and trust. They have only just begun translating these concepts into guidance and tools that line analysts can use. A905 has also experimented with different ways of doing joint reporting, organizing two

(U) The management of this sort of work will be profoundly different from the production process with which managers are familiar. It is essential that managers and analysts be assured that they are not embarking on some management fad, or signing on to a process that lacks leadership and support. We are fortunate in A9 that our management has given sufficient freedom of action to line managers and analysts to pursue novel working relationships and to take risks in the interest of improving the workflow.

Starter Information Technologies

(U) The absence of a completely supportive culture means that the collaborative information technologies cannot be implemented in whole, but must be supplied in functional pieces to assist analysts and managers make the change to a collaborative environment. It is essential that we run pilot studies of collaboration and joint reporting among analysts; this is the only way we will learn how to build the tools analysts need (as opposed to what computer professionals think analysts need) and it is the only way to learn the management of collaborative efforts.

It is essential that managers and analysts be assured that they are *not* embarking upon some new management fad, or signing on to a process that lacks leadership and support.

~~(S-CCO)~~ One of the first information technology tools we would like to implement, and one which will make the management of collaborative production easier, is to develop an interactive bulletin board for analytic production. This idea has been suggested repeatedly by many, including the EUCRAT as well as those who are making it possible for A933 and W9F7 to work together on energy issues. It is based on a simple premise: In order to collaborate, analysts must first know who is doing what and with what information. It has been suggested that analysts maintain a list of current and planned production as part of the NSA intranet. Analysts would consult this tool daily, and add their intentions to it as needed. Greater awareness among analysts of what is being produced by whom can only have a salutary effect on production efficiency. Redundancy in reporting (and in release and dissemination) can be avoided. This bulletin board would have an

effect on the work culture, as it would help analysts to start thinking beyond the immediate scope of their task, and get them used to working in a networked environment.

(U) A second collaborative technology we hope to implement in pilot form is a shared work space that allows co-editing of a report. To have true collaborative production, analysts must have the ability to interact freely in the production process. Some collaborative software tools available now will allow this co-editing.

(U) These attempts to affect minimum work culture and technology needs are a first cut at building intelligence production collaboration. Further steps could follow only after evaluating the results of the pilots and then introducing changes from lessons learned. This iterative process is necessary because so much is unknown. Wholesale application of a given collaborative technology on a workforce and management that is unprepared would be very disruptive. And, like as not, the tool selected would lack crucial features.

(U) It is important to remember that collaboration is not a project; it is a way of life. Individual analysts can and should begin to reach out to colleagues, without waiting for the results of formal collaborative efforts. NSA management has embraced a commitment to reward teamwork and initiative. The NSA of the future will be developed by today's innovators—our analysts and line managers.

P.L. 86-36

~~(S-CCO)~~ [redacted] *is on the Intelligence and Reporting staff of A9, the Office of Europe, Central Asia and Multinational Issues. His long-standing interest in collaboration led him into a series of efforts to promote collaboration within A9, between NSA offices, and between agencies. He has worked as an analyst in the*

[redacted]

EO 1.4.(c)
P.L. 86-36

research. Mike claims to have had nothing to do with the death of any of these targets. He also served as an integrated intelligence officer at the DCI's Nonproliferation Center at CIA, where he was project manager for an inter-agency collaborative reporting effort. Mike is a working microbiologist in charge of the Microbiology Dept. for a clinical laboratory in Pikesville. He spends his free time carving Mt. Rushmore on a grain of rice.

~~(FOUO)~~ [redacted] *received her Ph.D. in Linguistics last May from Georgetown University; her article in CRYPTOLOG Vol. XXI, No. 3 (*Foreign Language Testing at NSA: Time For A Change*) was based on her dissertation. She joined the Agency in 1988 as a French language intern and is certified as a language analyst in French and Spanish. At the end of her NSA fellowship in August 1995, she was assigned to the A9 Intelligence and Reporting Staff. She is currently the Chief of the B Group Language Technology Center (B638).*

P.L. 86-36

An OPENROAD to Research ~~(FOUO)~~

by [redacted] ~~(FOUO)~~

~~(FOUO)~~ OPENROAD is an initiative [redacted] to research and develop methods to simultaneously access multiple heterogeneous databases using a single query. [redacted]

~~(FOUO)~~ [redacted] to research methods and procedures to develop domain data models. We will use these models as the basis for a domain *metacatalog* (a catalog of "terms about terms") from which a user will select terms to build an OPENROAD query. Each term in the metacatalog is referred to as a *metaterm*.

The Metacatalog (U)

~~(FOUO)~~ The metacatalog is the heart of OPENROAD and is the mechanism by which an analyst can perform single-query access to multiple databases and sources. It is the link between the logical data model and the physical collection of databases, tables, fields and files that contains the data of interest. The power of a metacatalog is tthe analyst no longer needs to know the source of the data and mechanics of accessing that data. In addition, the underlying logical-to-physical mapping can change for any metaterm without affecting an analyst's ability to use that term in queries.

~~(FOUO)~~ Of paramount concern to the OPENROAD developers—both software and metacatalog—is to maintain the transparency of the data sources as viewed by the user through the metaterms. The solution we are presenting does not make a distinction between metaterms mapped to structured sources and metaterms mapped to text sources *as presented to the user,* nor does it require two queries to accomplish the same thing, one for structured data access and another for text data access. Instead, an analyst sees a logical model of metaterms from his domain, issues his query, and gets results.

The Analyst's Work Model (U)

(U) Typically, an analyst works with separate tools to gather data from multiple disparate data sources. Each tool has its own user interface and command/query language. An analyst also usually needs to remember a separate log-on and password to access each tool, database, and system. There is often little or no ability to correlate any query results or perform follow-on processing across multiple tools and sources.

~~(FOUO)~~ The focus of the OPENROAD metacatalog development is data-centric vice tool-centric. The modeling effort needed to build a metacatalog is based on the relationships among data items and how data items are used and represented, not on the tools and methods an analyst uses to get the data. The analyst has greater power to do analysis, spending less time doing the manual chores of performing access with multiple tools and interfaces. OPENROAD provides a single interface with a single log-on to all the data sources an analyst currently uses, leaving more time to do analysis.

Domains (U)

[redacted]

(U) Each information domain will have its own metacatalog tailored to its database domain. We expect

EO 1.4.(c)
P.L. 86-36

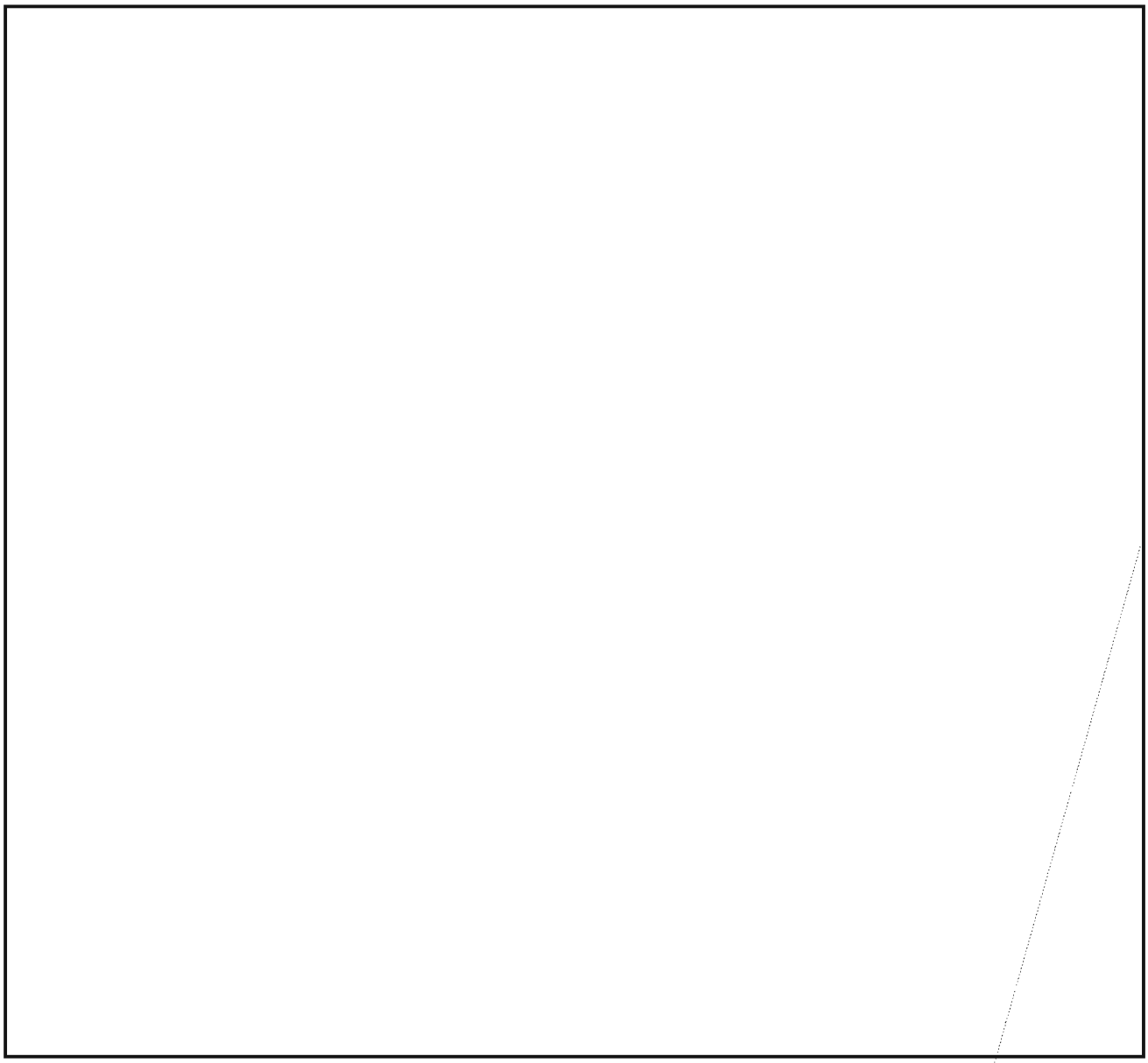
DOCID: 4033694

a significant degree of metacatalog reuse with other information domains that share database domains.

(U) We are currently assisting teams of domain experts (both information and database), analysts and systems support personnel in each of the prototype organizations to develop a metacatalog for that information domain. It is our long-term strategy to have domain experts and systems support personnel maintain and enhance the metacatalog once one is developed for an organization.

Key Abstractions (U)

P.L. 86-36



EO 1.4.(c)
P.L. 86-36

which may or may not be in hard-copy. Clearly, all these abstractions have characteristics that make one "thing" different from another "thing."

(U) Once we have identified key abstractions, we can begin to flesh them out by modeling the attributes, properties, or characteristics of the abstractions. Some attributes may, in turn, be composites of other attributes. In Figure 2, the Position attribute of a Maneuver can be broken down into Latitude and Longitude. We can then reuse Position in any new abstraction that requires geo-positional information.

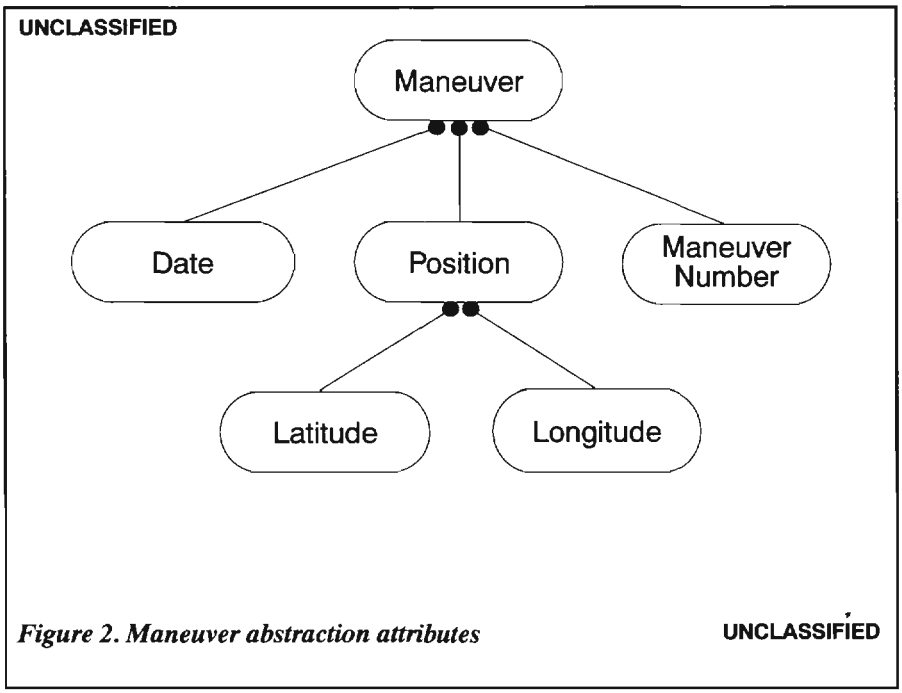


Figure 2. Maneuver abstraction attributes

Metaterms (U)

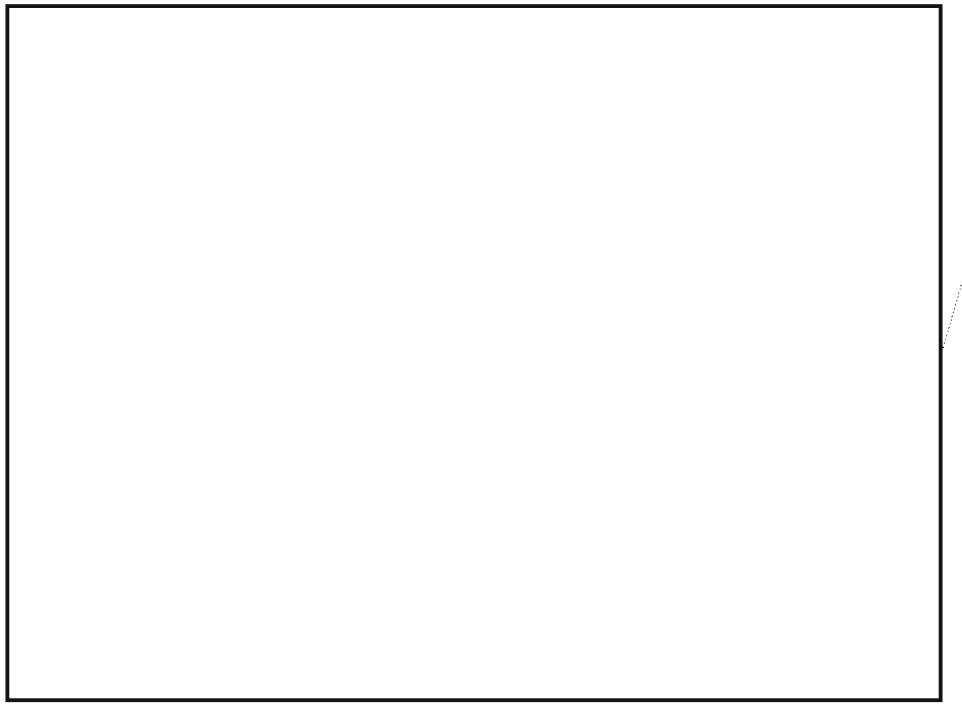
~~(FOUO)~~ When the abstractions have sufficient detail, we can begin to list the candidate metaterms from the model. Metaterms are the basic level of abstraction that an OPENROAD user sees of the information domain contained in the database domain. *Through analysis and modeling, we can create multiple "views" of the information domain.* The usefulness of OPENROAD—and of an analyst's ability to get the necessary data to satisfy requirements—is directly related to the completeness and flexibility of the metacatalog.

P.L. 86-36

P.L. 86-36
EO 1.4.(c)

The Logical-to-Physical Connection (U)

(S) The metacatalog provides the link between the logical domain model and the physical structure of a database. Metaterms can map to one or more fields that are semantically equivalent in one or more data sources, or to an entire data source, such as a user file.

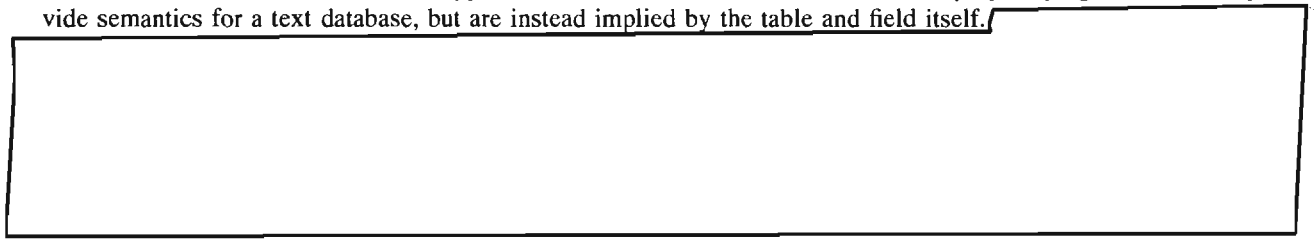


EO 1.4.(c)
P.L. 86-36

(U) One significant benefit of using metaterms is that the logical-to-physical connection can be modified without affecting the metaterm view that the user sees. If a new data source comes on-line, we can transparently (to the user) map its portion of the information domain to existing metaterms (if appropriate), or create additional metaterms.

P.L. 86-36
EO 1.4.(c)

(FOUO) Three types of metaterm mappings are possible. To the user, however, no distinction is made in the OPENROAD user interface. The first type of metaterm is for structured databases only; qualifying values do not provide semantics for a text database, but are instead implied by the table and field itself.



P.L. 86-36
EO 1.4.(c)

(U) The second type of metaterm is for text sources only. Some metaterms, like Name, may not be mapped to a field in a structured database because that source does not contain a field for names. However, this metaterm represents a valid abstraction found in the domain's text sources. A search of a text source using the qualifier "Name = 'Openroad'" would return all documents that contained occurrences of the string "Openroad", if any were found, regardless of the context in which it occurred. This type of term models data that analysts typically find only in text data sources.

(U) The final type of metaterm is for both text and structured data sources. The intent is to search for the qualifying value in both structured databases (based on semantics) and text databases or flat files (in any context).

~~(FOUO)~~ Not included in the metacatalog, but supported by OPENROAD, are free-text terms. This case satisfies a requirement to allow a search for any qualifying value for which there is no corresponding metaterm in any context in a text source or flat file.

Pangaea Virtual DB (U)

~~(FOUO)~~ The OPENROAD development team chose Virtual DB, a member of the Pangaea product line from enterWorks.com, as the tool to create and manage the domain metacatalogs. Each operational prototype will use Virtual DB.

(U) Virtual DB is itself an application, complete with a graphical user interface, for creating metacatalogs and managing access to structured databases. It runs from the GemStone object-oriented database management system from GemStone Systems, Incorporated. enterWorks.com bundles the two applications together and resells GemStone as part of Virtual DB. Since the data models we are creating are based on objects, GemStone provides great flexibility and power in storing and managing the object representations.

(U) enterWorks.com also packages Omni/SQL from Sybase with Virtual DB to provide access to heterogeneous structured databases. Omni/SQL makes the logical connections to the various databases using access modules, one for each major database implementation (e.g., Sybase, Oracle, Ingres). Virtual DB generates the necessary structured query language (SQL) statements and passes them on to Omni/SQL which, in turn, forwards the statements to the appropriate access module for each vendor's database management system. Results are passed back along the same path as the SQL statements, from the database to Omni/SQL, then to Virtual DB. Omni/SQL joins results from multiple tables from different databases and returns the results when all sub-queries are completed.

(U) Virtual DB supports pre- and post-processing data type conversions for differing internal data type representations. For example, a value representing a latitude may be stored as an integer type in one database, while in another it may be stored as a floating point type. Using a Virtual DB type conversion, we can display query results in a common format and perform Boolean operations on the data.

~~(FOUO)~~ Virtual DB can be used as a stand-alone product through its user interface. However, a rich set of application program interface (API) calls allows a custom interface, such as OPENROAD's, to access the full power of the underlying functionality directly. We currently use Virtual DB's graphical interface for development purposes. Though written in the Smalltalk object-oriented language, Virtual DB also supports a C language API. The underlying metacatalog storage mechanism is transparent to the analyst when using OPENROAD.

(U) Though not designed to access text or flat file data sources, Virtual DB does allow external data sources to be mapped to metacatalog terms. This distinction (structured vs. external source, i.e. text) is made as each metaterm is defined in the metacatalog. Each metaterm is processed according to its type.

~~(FOUO)~~ The OPENROAD team is not aware of a commercially available text gateway similar to Virtual DB for general text access. OPENROAD developers have written a custom text gateway for text source queries, using text access modules analogous to Virtual DB's structured access modules. Each text access module generates native query language for each text database (e.g. BRS or Topic); WAIS and flat-file sources are handled similarly.

~~(FOUO)~~ Virtual DB provides term-level security so each term can have its own set of classifications. Each user can see and select only those metaterms for which he is cleared. It can also enforce row-level security for mixed query results if the security labels are built into the tables of the database. Virtual DB does not, however, support security based on algorithms external to the database. Our proposed solution in such cases is to run OPENROAD at system high.

DOCID: 4033694

Future Initiatives (U)

~~(FOUO)~~ The DMATC will continue to evaluate other commercial-off-the-shelf products to support the OPENROAD metacatalog and to develop expertise in domain-oriented data modeling. More broadly, we will continue to research and apply methods for database access and data modeling. We intend to provide access to multi-media data sources, and allow application interoperability using the Common Object Request Broker Architecture.

(U) Our research into the process of developing domain metacatalogs is partly funded by an IDEA program grant. We anticipate additional funds to continue this research to refine and reuse the knowledge we have gained so far. We expect there to be significant levels of model reuse for many widely-used data sources.

(U) In addition, development is underway to integrate secondary queries (follow-on queries based on earlier results), text document grouping based on semantics, and filtering.

[redacted]

Kλ

P.L. 86-36

CRYPTOLOG Bloopers:

[redacted]

(U) *CRYPTOLOG* regrets the error.

P.L. 86-36

DOCID: 4033694

The Changing Timbre of Conflict and Conflict Resolution in Sub-Saharan Africa (U)

by [redacted] P.L. 86-36

(U) Africa has long been misunderstood. Referred to as the "Dark Continent," the "Mysterious Continent," and other inappropriate nomenclature, explorers, poets and politicians have tried for centuries to plumb the depths of this sometimes benevolent, sometimes hostile, always enigmatic behemoth. And just when it seemed like Africa's "truth" was filtering down to an audience ready to grasp its complexity, this truth began to shift once again, undermining the fledgling knowledge we all had so recently committed to memory.

(U) This shift in the foundation we had built is due to a number of factors and not merely to events inside Africa, of course. The end of the cold war changed the "usefulness" Africa held for many foreign governments—both in the U.S. and elsewhere. Africa was no longer seen as a pawn in the East/West game, its importance to politicians often generated in the past by vested national interests. To many influential decision-makers, Africa has become increasingly irrelevant within a global perspective. To a large extent, after the cold war, the world partially untethered Africa from the various links which had been artificially created and moved its focus elsewhere, leaving the enigmatic and problematic Africa more and more to its own devices.

(U) Since the end of the cold war, the world has largely left problematic Africa more and more to its own devices

(U) While the rest of the world was turning its sights to other shores or, in many instances, inward, Africa was undergoing its own evolution, struggling to find its own voice: a post-colonialism, post-cold war voice. And anyone who reads the newspaper knows about the challenges this population continues to face on a daily basis: disease, civil war, nation-building, refugees, democratization, insurgencies, outside interference in countries' internal affairs . . . the list goes on and on. In short, however, conflict in Africa has now become more regional and less global than in the days of the superpower tug-of-war.

(U) For the purposes of this article, I will concentrate primarily on Sub-Saharan Africa, leaving the study of North Africa for another time, since the circumstances of its evolution are quite a bit different for the most part. The 52 countries that make up Africa are far too diverse, their differences more glaring than their similarities, to lump together.

(U) Perhaps the most salient internal shift in Sub-Saharan Africa in the last decade has been the 1994 demise of apartheid in South Africa. Prior to 1994, South Africa was the hub of the African wheel and countries within its grasp either acquiesced to its will or fought—often unsuccessfully—to elude this grasp. Events in that part of the world seemed always to be in reaction: TO South Africa's position on a particular issue. When this relationship of inequality came to an end, at least in theory, another ripple appeared on the horizon, in the untethering most African countries were already facing. This occurred as countries in the area—particularly those contiguous to South Africa—were left to their own resources in deciding their own fate. This worked both *for* them, in some cases, and *against* them in others. It also served as an impetus for South Africa to look inward and not be as intrusive in the affairs of its neighbors. And coupled with that shift to a more defensive stance has been the burgeoning movement in both Zimbabwe and Botswana to assume greater positions of authority in the region.

(U) This new world order that was created with the demise of South Africa's apartheid and the end of the cold war has translated into new rules for co-existence among the African states and into an increasing role for the United Nations, which was paralyzed into inaction by superpower rivalries for more than 40 years. Freed from this paralysis, the UN is now being called on increasingly to help solve conflicts in Africa, to fulfill its commitment of peace-making, peace-keeping and peace enforcement there. At the same time, there has been a commitment by many of the African states to adhere to rules of non-interference in their neighbors' affairs, to maintain territorial integrity, to find African solutions to

African problems and the sovereign right to be able to ask for outside help for problems when the need arises. These rules represent significant shifts in the way that African nations do business because, until fairly recently, the sovereignty of a country could be questioned. In essence, every African was his brother's keeper and could act with impunity: South Africa was accused of interfering in the affairs of Angola, Mozambique, Swaziland, Lesotho, Namibia and other Frontline States. Zambia harbored South African freedom fighters and Liberians viewed "meddling" Nigerians as still another faction entering into the fray of their country's civil war.

(U) What African nations have discovered in many instances is that they are frequently better able to keep the peace themselves than when they ask for outside help. There are several reasons for this: one is that there is greater political acceptance of having their "own" forces present where there is conflict. A corollary to this is the expected inherent knowledge of that country's people, terrain and customs by these internal forces, the financial benefits of using "in-house" solutions for in-house problems and the superior sense of commitment that these regional forces bring to their mission.

(U) A number of events in Africa have added to the sense of confidence that many countries exhibit in handling their own issues: elections in Namibia in the late 1980's, which set up a paradigm for the entire region; peace—albeit tenuous—in Angola; the release from prison of the now President of South Africa Nelson Mandela; the end of the war in Mozambique; elections in Zambia and Malawi, and the 1994 elections in South Africa. These events and others have spurred countries on to follow suit in creating their own destinies and also in more readily cooperating with other states in the region to mitigate conflict.

(U) In a situation in which outside nations intervene in the affairs of a country, the jury is still out as to whether or not this is an effective measure. According to one camp, it is dangerous to assume that peace-keeping forces that do not respect the laws in their *own* country will be effective in ensuring that they are obeyed in *another* country. A further allegation is that these external peace-keeping forces are sometimes motivated more by financial gain than by ideological or humanitarian reasons. Forces called in to help tamp down a crisis are generally rewarded by the donor countries for their efforts with high per diems which are normally very generous, relatively speaking, with material hardware and with communications equipment. Among the more unscrupulous outside forces—these same critics maintain—the visiting forces sometimes skim off the top of the per diem to fill their own coffers.

(U) Detractors also point to the need for outside forces to lessen the appearance of partiality, to become more culturally aware of the country in which they are working, and to nurture better relations with the local population, winning their hearts and minds instead of using force. In this way, hopefully they would be better equipped to gradually earn a sense of legitimacy and a credible capacity to influence rather than to coerce. Finally, these same detractors note that there is currently no joint UN publication which outlines peace-keeping procedures and guidelines, no system of checks and balances to standardize operations. It is left up to the various coalition armies to determine on their own, with their divergent backgrounds, agendas and motivations—not exactly a recipe for success by most standards. And with the UN expected to increasingly play a major role in peace-keeping in Africa, it is incumbent upon that organization—with its 50 years of experience—to help standardize and thus legitimize its missions there.

(U) One problem with UN missions that is particular to Africa is the declining level of awareness of people *outside* Africa. An illustration of this deterioration of external knowledge is the widely-held theory that Africa is composed of hegemonic tribes and subordinate tribes with conflicting philosophies. Under the terms of this theory, every conflict in Africa can be reduced to ethnic terms, regardless of the context. One size fits all in this simplistic paradigm which, unfortunately, is gaining prominence in some quarters, irrespective of the multitude of economic, political, geographical and historical factors which have all contributed enormously to conflict in Africa. For example, four civil conflicts have been cited to corroborate this monochromatic theory: the Congo/Zaire upheaval of the 1960's, Somalia, Rwanda and Liberia. Instead of examining these four situations through the lens of an impartial, astute observer—taking into account the less-than-ideal role played by the UN in all cases—they have been reduced by some to wars between barbaric tribes of Africa, tribes with little else to do than wage war.

(U) There are those who would argue, however, that in the case of the previously mentioned conflicts and in others, a finger should be pointed at the UN, which has traditionally played a more *re*active than *pro*-active role in Africa. In addition, as previously indicated, often there is a lack of a clear framework for UN operations abroad and what starts out as a particular type of mission can sometimes change in midstream,

DOCID: 4033694

without any apparent rationale.

(U) Still another criticism of UN peace-keeping operations is that they are, in fact, peace-*keeping* and not peace-*making* operations, that the emphasis is on the wrong aspect of operations. Allegations have been leveled against UN officials for purportedly bailing out when the "going gets tough." When the conflict escalates—these same allegations continue—the UN threatens to pull out, leaving the country in question in the lurch. Still others accuse the UN of not providing sufficient funds to its peace-keeping operations and of channeling too many funds into bureaucratic areas. Two examples cited as the worst of the UN missions to Africa are Somalia and Rwanda. Finally, the critics charge that the UN needs to address underdevelopment in these African countries or people will continue to be galvanized into fighting against a common enemy: poverty.

(U) Africa's own foreign policy reflects the changing perspective on conflict and conflict resolution. Before the end of apartheid, the Frontline States wielded considerable influence in the region, concentrating their collective efforts on dealing with a common adversary: South Africa. There had also been another common enemy to provide these African countries with a united front: colonial/European rule. With the shift in perspective that resulted in the end of apartheid and the end of colonial-ruled Africa, foreign policy there fractured into multiple, often contradictory and competing philosophies as these once-united African states scattered for divergent political shores and, in doing so, lost much of the power base they had enjoyed when they were part of a more unified whole. Without their former collective power, their leverage in a global sphere has been reduced considerably.

(U) Coupled with this fragmented foreign policy is the lack of an economic power base to recreate some sort of linkage between these countries. African states were so preoccupied in their respective post-colonial periods with nation-building that economic considerations often fell by the wayside.

(U) In order to remedy this situation, some advocates of South Africa's historic hegemony in the region advocate a controversial return to this type of arrangement, but with a benevolent (versus exploitative) model. Under this type of relationship, the constellation of African states would again revolve around South Africa, but a benevolent South Africa which would now act in a manner beneficial not just to its own interests but to those of its neighbors. The previous asymmetry which

Unclassified

Unclassified

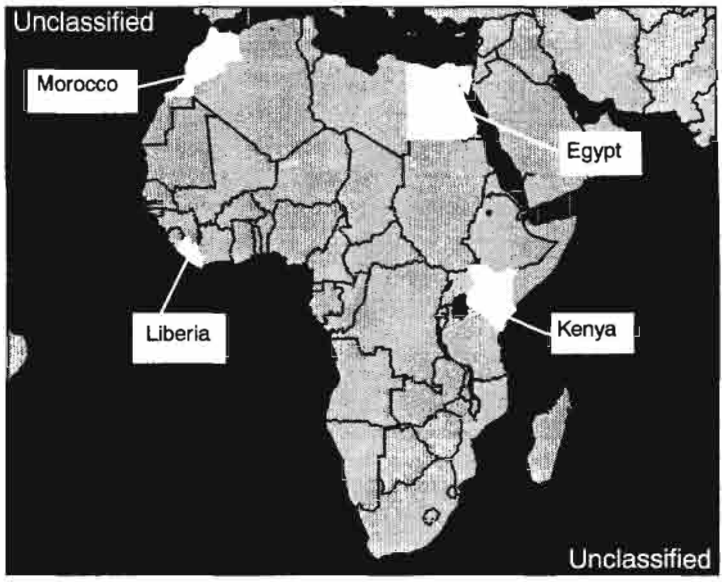
(U) Government forces face increasing challenges from insurgents and/or gangs

reigned in an apartheid South Africa would still exist but under this theory South Africa would temper this hegemony by remaining ever-cognizant of the interests of its wards. The relationship would also be more multilateral in nature, with the economic and institutional needs of each country of prime importance. Naturally, in order to be successful, it would require the willingness of all parties to cooperate.

(U) The antithesis of this benevolent model is an exploitative system, one which was the norm in South Africa for many years. This model harks back to the not-so-distant past when national interests were of paramount importance and countries related to each other on a bilateral basis for the most part, leading to regional imbalances and frequent conflict.

(U) Time will tell if the so-called benevolent model takes root in Southern Africa. In order to meet with success, South Africa's neighbors will have to want growth and stability more than they want to usurp South Africa's hegemony. And South Africa will have to prove to these same neighbors that its goals extend beyond its own boundaries to the common good of the region, and then not exclusively to its European and American counterparts.

(U) Adding to the complexity of the discussion of conflict and conflict resolution in Sub-Saharan Africa is the issue of arms transfers since the end of the cold war. The exodus of the superpowers from Africa has meant that governments there no longer enjoy the luxury of financial assistance in boosting the equipment of their security forces. Conventional military equipment is no longer so easy to come by now. Conversely, in many of these countries, automatic rifles are often cheaper than a



(U) Basing agreements in Liberia, Morocco, Egypt, and Kenya will remain key issues for the U.S., but primarily for purposes of power projection outside Africa.

loaf of bread and often as accessible because of the enormous amount of weaponry brought into Africa during the cold war and then left behind. This means that government forces are now increasingly vulnerable to challenges from insurgents and/or gangs. Furthermore, these same governments are less and less successful in engaging Western governments to assist them in their fight against these hostile forces. It is important to keep in mind, too, that African governments frequently find it difficult to ensure that material resources are distributed to the masses, therefore, the military is becoming a determining factor in ensuring their delivery. If it is under attack or vulnerable to disruptive influences, it affects the entire population of a country. When national armies are outmanned and outarmed by insurgents, political dissidents have no reason to eschew violence.

(U) With this shift in the nature of arms acquisition, conflicts in African states are now being prolonged, and are more intense and frequently more difficult to resolve. And with the decline of legitimate economic activity, force has become the lingua franca in obtaining resources and has meant that conflict often spills into other areas. Examples of this spillover include Liberia (Sierra Leone and Cote d'Ivoire), Rwanda/Burundi (Zaire and Tanzania), and Angola and Mozambique (South Africa).

(U) A corollary of this new paradigm of conflict is that there are very few outright victories in Africa and this is due, for the most part, not to the strength of the insurgents but to the relative weakness of the government in defeating these insurgents. Most African armies are not properly organized, equipped or trained and, therefore, ill-equipped to combat the well-armed insurgencies.

(U) A further impediment to conflict resolution is the fact that negotiated settlements are very difficult to achieve in Africa, for the following reasons:

- the insurgents often have no clear-cut ideology; ideologies are often personality-driven, or new players come into the picture, preventing consensus. This results in an ever-changing and therefore confusing insurgency ideology;

- factions proliferate as the conflict is prolonged. This factionalization inhibits the government's desire to settle the conflict since there is no clear-cut *single* adversary (e.g., Somalia, Angola and Liberia). As a consequence, the government often fails to recognize factions as *legitimate* factions representing the whole. This factionalism also works against achieving consensus among the many disparate parties;

- there is a lack of education in the negotiating process itself (e.g., Mozambique, Ethiopia and Rwanda);

- during the negotiation phase—if reached—few countries have the money to finance the logistical aspect of peace talks;

- there is rarely international support to sustain peace, which may delay the process (Mozambique) or lead to a breakdown of negotiations (Liberia);

- there is a shifting idea of what victory/compromise/defeat mean to the parties involved; and

- the country or countries involved have been virtually devastated.

(U) As the face of Africa changes, a sense of pessimism can be detected in some quarters. As conflicts there increase, there is a marked loss of hope, the long-standing hope that the lot of a post-colonial Africa would be better—both economically and politically.

DOCID: 4033694

After almost three decades the opposite is true more often than not, and the term Third World still applies to most of the continent, with the exception of a portion of South Africa's population and small pockets in other countries.

(U) The United States will always have a strategic interest in Africa and its welfare but this interest will shift as the situation both in Africa and the U.S. changes. Basing agreements in Kenya, Morocco, Liberia, and Egypt will remain key issues for the U.S. but primarily for purposes of power projection *outside* Africa, not inside Africa. In addition, oil, strategic minerals, humanitarian and relief operations and an interest in keeping sea lanes of communication open at both the Horn and the Cape of Good Hope form the basis of continued U.S. interest in Africa. Nevertheless, in an era of decreasing budgets and increasing domestic focus, it will fall more and more to Africans themselves to sort out their conflicts, to find African solutions to African problems without relying on outside help or by relying on the assistance of the United Nations.

[redacted]

P.L. 86-36

Kλ

~~(FOUO)~~

Inter-Agency Conference

"Responses to Humanitarian Crises: the Role of Classified Intelligence" co-sponsored by NSA and CIA.

The purpose of the Conference is two-fold:

1) to identify the types of classified intelligence customers need and do not need in the time leading up to, during, and in the aftermath of humanitarian crises; and

2) to identify intelligence gaps and other issues that affect intelligence producers' ability to meet customer requirements.

Date: 3 December 1996
Hours: 0815-1600 (Registration begins at 0800)
Location: 9A135, Headquarters

Credit for NCS course IS-355 (Current Issues in Intelligence Analysis) will be given for attending this conference; interested students should preregister by contacting Conference Co-Chair [redacted] on 963-6011s.

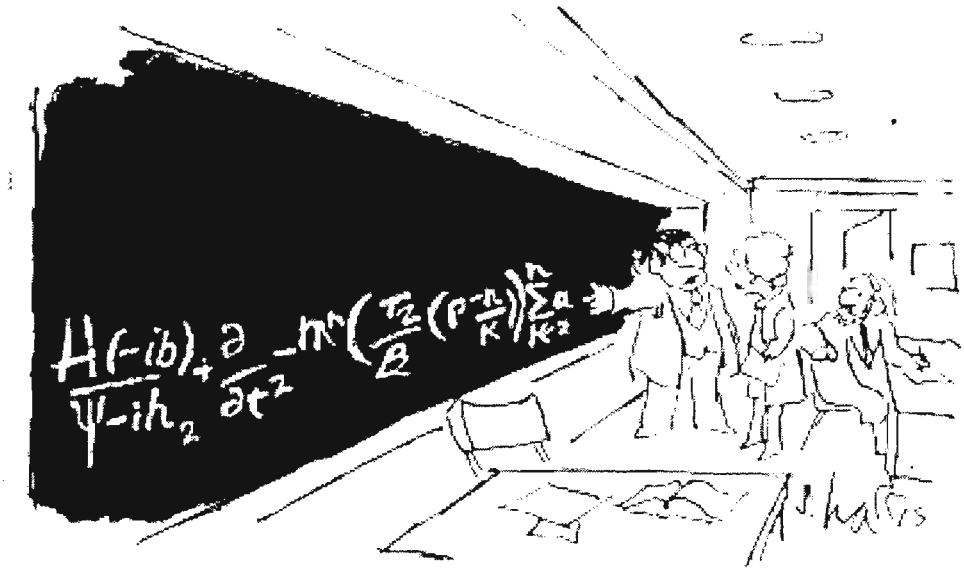
P.L. 86-36

Calling all publishers! (U)

P.L. 86-36

~~(FOUO)~~ We are looking to update an article that appeared in *CRYPTOLOG* Vol. XX, No. 2: [redacted] *Publishing as a Member of the Technical Track*. This article listed a number of Agency publications that provide the opportunity for disseminating information "as a vehicle for both technology transfer and career growth": for instance, *The DD Eye*, *Cryptologic Quarterly*, and the *Infosec Technical Exchange*. Since *CRYPTOLOG*'s focus is on explaining developments in one's field to those outside it, we would like to spread the word that since [redacted] article appeared, a number of new periodicals have appeared, and we have learned of others that existed at the time. *CRYPTOLOG* would like to add to this list of vehicles for contributing to one's skill field. To quote from the article, "Are there any journals which regularly come across your desk or to your computer screen? How about newsletters and other local publications that you've seen? Most Agency technical societies solicit papers on an annual basis for essay contests; look for the announcements or contact one of the society's officers. How about an organizational technical report that carries a wide distribution? Career Panels and Technical Directors can also help point you in the right direction." If you know of such an opportunity, please provide the *CRYPTOLOG* editor with the name of the publication, its editor, a description of its mission, and instructions for submitting articles.

Unclassified



"But this *is* the simplified version for the general public."

Unclassified

~~FOR OFFICIAL USE ONLY~~

DOCID: 4033694

by [redacted] P.L. 86-36

The Need for Multilevel Secure Databases (U)

(U) An information downpour is flooding the Agency. NSANET and client/server architectures have created an environment in which users can transparently access data that resides on remote systems. This situation affords many advantages, including the quick and paperless dissemination of information, but it has also become easier for information to get into the wrong hands. When computers with varying security levels reside on interconnected networks, unauthorized users may read information at a classification level higher than their own. The consequences of unrestricted data access range from the accidental retrieval of classified information by those without adequate permissions to the intentional transfer of classified data to those whose goals lie in the areas of profit and espionage. This clearly is a situation we cannot allow to exist. We must take precautions to ensure that data can be accessed only by users with adequate authorizations.

A Possible Solution: Trusted SOLARIS (U)

(U) The easiest way to protect classified data is to locate it on stand-alone machines or networks that carry data of a single security level. These machines or networks would be accessible only to authorized users. This may seem like an antiquated proposal, but this was the norm until recently. With security mechanisms such as cipher locks on doors, automatic screen lockouts, and restricted local area networks, the necessary controls were provided. Data at a single classification was placed on a machine, and only authorized users could access the machine. Users in today's environment have requirements that make this method inconvenient and overly restrictive. They need to be able to access data remotely across multiple networks and at multiple security levels. They also want to integrate information residing on different machines or networks, or transfer information to their local workstations.

~~(FOUO)~~ Many organizations investigated secure operating systems as a better means of providing data security. These operating systems are known as Compartmented Mode Workstations (CMW) and must fulfill requirements specified by the Defense Intelligence Agency. The K223 BOXOAK project decided to base its architecture upon Sun's version of CMW, the Trusted SOLARIS operating system. This product is designed to allow users at different clearances to handle information at different levels of security while protecting the security of that information and keeping it properly labeled. It accomplishes this through the use of privileges, separation of administrative roles (there is no "root" user), and labeling of users, programs, and information. Trusted SOLARIS is the backbone of the BOXOAK Phase 1 operational system used by K53, and ensures the separation of compartmented information.

~~(FOUO)~~ BOXOAK's plan was to continue using Trusted SOLARIS during later phases, with the addition of a secure relational database management system (RDBMS). SYBASE, INGRES, and ORACLE, the three major databases at the Agency, all have secure versions of their product lines that run on CMWs. A secure RDBMS would make it possible to develop software without the need for any special algorithms to guarantee data security filtering. For instance, if a user was operating at a CONFIDENTIAL clearance level and requested information from a source that included classification levels ranging from UNCLASSIFIED to TOP SECRET, the user would only be provided information at the CONFIDENTIAL level or lower. Furthermore, the fact that information existed at higher levels would not be apparent to the user.

(U) Initially, the INGRES/Enhanced Security product was used, and it performed as desired. Due to the widespread Agency use of SYBASE, the decision was eventually made to switch to the SYBASE database product line; again, data security was provided exactly as described. Although these secure RDBMSs worked well, their dependence on many features pro-

vided by the operating system was a major drawback because concerns about Trusted SOLARIS were surfacing and could not be ignored.

~~(FOUO)~~ BOXOAK had remained in regular communication with Y4, who was performing an operational test of Trusted SOLARIS for use in the DDI Virtual Campus architecture. Y4 found many flaws with the product and eventually decided not to use Trusted SOLARIS. At the same time, BOXOAK was experiencing many of the same problems Y4 was documenting. These problems were all of a fairly serious nature and had to be considered.

- (U) CMWs are not widely used, and it was impossible to find expert guidance and assistance in other organizations.

- ~~(FOUO)~~ SUN was providing only minimal support for Trusted SOLARIS. BOXOAK was dealing with one point of contact who moved to another product line. Support was virtually nonexistent after that.

- (U) Further development of Trusted SOLARIS was negligible at best. It was supposed to keep pace with the non-secure product releases, but this did not happen. As a result, many new tools could not be installed and used. This was a major problem when the Graphical User Interface (GUI) development tool that had been purchased could not be used since it required a newer release of Trusted SOLARIS than was available.

- (U)) There were reports of vulnerabilities with the very security which Trusted SOLARIS was designed to provide. CMWs are built to protect a multi-level, compartmented environment but have been found to be exploitable.

(U) These issues alone would have necessitated a hard look at the wisdom of using Trusted SOLARIS. When coupled with the fact that the secure RDBMSs were 50% more costly and much more difficult to maintain and administer than their non-secure counterparts, it was decided that other alternatives to providing the necessary security had to be found.

Alternative Solutions (U)

~~(FOUO)~~ During conversations with SYBASE, the company had alluded to a new Secure SYBASE product that would not require a underlying secure operating system. This would have met many of BOXOAK's security needs. Unfortunately, this product never became available, and still does not appear to be on the horizon. BOXOAK had to keep its investigation active.

~~(FOUO)~~ An in-house product known as SENTINEL came to the attention of the BOXOAK team. This A74 product provides SYBASE security filtering without the need for an underlying secure operating system. SENTINEL was designed initially to support other A74 applications with security filtering needs much more complex than BOXOAK's. Implementing these requirements incurs some cost in terms of maintenance and performance. SENTINEL also required the purchase of additional SYBASE software which otherwise was not needed. When it was finally determined that BOXOAK did not require as elaborate an architecture as the A74 projects, the costs seemed to far outweigh the benefits.

~~(FOUO)~~ Since there were no other security products to be found, there was only one course of action left. BOXOAK would design and develop its own simple and easily maintained data security mechanism.

The BOXOAK Solution ~~(FOUO)~~

~~(FOUO)~~ The requirements for the BOXOAK implementation were driven by the needs of the customer, the K5 High Altitude Programs, which include many Configuration Control Boards (CCBs). These CCBs operate at varying security levels and will be accessing the same BOXOAK system to manage their programs. It was required that users would only be able to access and be aware of information to which they had an equal or greater security level. Furthermore, the networks over which this data would be transferred would need the same protections.

~~(FOUO)~~ The BOXOAK solution was multi-faceted and was based upon the strategy employed by the SENTINEL product. This strategy was fundamentally sound and its use would facilitate future interfaces between the products. The implementation includes the database design, modified database queries, and a few translation algorithms; it will be used by all BOXOAK systems.

DOCID: 4033694

Database Design (U)

~~(FOUO)~~ Some essential terminology must first be explained. Normally a user has a clearance and data has a classification. BOXOAK, like SENTINEL, deviates from this convention. Both users and data have a **classification** which includes the national clearance (e.g., UNCLASSIFIED, SECRET), handling codes (e.g., US, UK), and compartments (e.g., TK, B). SENTINEL uses the terms **privacy** to refer to handling codes, and **special access** for compartments. For consistency's sake, BOXOAK also used the terms privacy and special access to refer to these codes.

(U) Three database tables containing all possible values for clearances, privacy codes, and compartment codes are the core of the security strategy. The table structures, including some sample data, appear after their descriptions.

(U) The clearance table contains all possible values for clearances. Since only one clearance can be assigned to an item at a time, a single integer is used to designate each clearance. This integer is the value actually associated with an item when it is stored in the database. Also stored in this table are the full and abbreviated labels for the clearance, used for displaying text on the screen or on hardcopy. A color (bgcolor) is stored and is used as the background for the classification stripe on any screen displays. A second color (fgcolor) indicates the color of the text on the classification stripe and is limited to the values of black (B) and white (W). As an example, an UNCLASSIFIED clearance would be displayed on a stripe with black text on a green background.

Clearance Table ~~(FOUO)~~

value	clearance	full clearance	bgcolor	fgcolor
0	U	UNCLASSIFIED	green	B
1	FOUO	FOR OFFICIAL USE ONLY	limegreen	B

~~(FOUO)~~ A data item could have both multiple privacy and special access codes. For instance, a TOP SECRET item could have privacy codes of UK CA and special accesses of TK VRK. As a result, these codes had to be handled differently to facilitate assigning multiple values to a data item. In both the privacy and special access tables, there is a label field which contains the actual code. There is also a position field (stored as an integer) which represents the code's position in a bitmap associated with a data item. When a data item contains a 1 in its bitmap in the designated position, it indicates that the code applies to that data item. For example, if a data item is marked with a 3 in its privacy field, the corresponding bitmap (binary equivalent) is 011. The codes that correspond to the zero and first position (starting at the right) would apply to this item. A lookup of the privacy table shows that a 1 in the rightmost or zero position indicates the US code, and a 1 in the first position indicates a UK code. The same design is utilized in the special access table, which also contains a full label field containing the full text of the code (i.e., Talent Keyhole for TK). This full label was deemed unnecessary for privacy codes.

Privacy Table ~~(FOUO)~~

label	position
US	0
UK	1
CA	2

Special Access Table (C)

label	position	full label
SI	0	COMINT
TK	1	TALENT KEYHOLE
B	2	BYEMAN

(U) Tables with secure data contain these three integer fields corresponding to the three classification tables. Other tables that interact with this data, including users and devices (hosts, networks, printers) also contain these fields. Thus, an entry in the User table contains user information (i.e., name, SID, organization) as well as the clearance, privacy, and special access fields. The values in these three fields can then be compared to the values in the fields associated with a specified data item. Access is allowed only when the values in the data item are dominated (equal to or are exceeded) by the user's values. The mechanism for restricting this access is implemented by the retrieval criteria in database queries, which is described in the next section.

(FOUO) A single integer field can hold up to 32 privacy or special access codes, which is more than sufficient for BOXOAK. This design can be extended to multiple integer fields if an application requires a greater number of codes. Any number of clearances can be accommodated, but since these are controlled at the national level, there is little chance they will be modified.

(U) A Colors table also exists. This table lists all possible combinations of values in the special access table and associates a color with each. If one or more special access codes exist for an item, the color from the Colors table is used in the classification stripe on screen displays and supersedes the color associated with the clearance value.

Colors Table (FOUO)

value	label	bgcolor	fgcolor
1	SI	DarkOrange	B
2	TK	yellow	B
3	SI TK	Tomato	B

Database Queries (U)

(FOUO) Once the data is labelled with the appropriate classification, database queries must be carefully constructed to ensure that security filtering takes place. In the case of the clearance field, the requirement is met by checking that the user has a clearance level that dominates the requested data. Only data that meets this criteria is retrieved. For the privacy and special access fields, security filtering does not equate to domination. The user must possess all codes assigned to the data item before it will be retrieved. If a data item has a privacy code that maps to US, UK and CA, then the user must have at a minimum all three of these privacy codes. Logical bitwise manipulations are used to provide this assurance. The data value is logically ANDed with that of the user and, once again, only the correct data will be retrieved. An example of a query with the correct criteria follows:

DOCID: 4033694


```
select B.board_name

from Boards B, Users U

where  U.username = 'jones' and

B.clearance <= U.clearance and

(B.privacy & U.privacy) = B.privacy and

(B.special_access & U.special_access) = B.special_access
```

~~(FOUO)~~ The results of this query are based on the data in the following tables (bitmaps and sample compartments appearing in parentheses for illustrative purposes only). User "jones" lacks the SI special access code and will not even know that a NW CCB exists. The user's clearance dominates the BOX CCB's clearance, and all of the BOX CCB privacy codes are contained within the user's privacy codes. The BOX CCB will be retrieved.

Boards Table ~~(FOUO)~~

board_name	clearance	privacy	special_access
BOX CCB	3	5 (101)(US CA)	4 (100)(B)
NW CCB	4	2 (010)(UK)	3 (011)(SI TK)

Users Table ~~(FOUO)~~

username	clearance	privacy	special_access
jones	4	7 (111)(US UK CA)	6 (110)(B TK)

DOCID: 4033694

Translation Algorithms (U)

~~(FOUO)~~ Classifications are always displayed to BOXOAK users as text since they have no knowledge of their underlying integer representations. There was an obvious need for a suite of algorithms that would provide the translation from text to integer and from integer to text. Four functions were developed to satisfy this requirement. Two functions support the translation of the clearance, and the other two translate both the privacy and special-access codes. These functions were written in embedded C/SQL so that they could be easily ported to other RDBMSs should there ever be a need. A final function was written to assign colors for classification text. These colors were used to determine the background color for the classification stripe on windows as well as the color of the classification text itself.

Network Considerations (U)

~~(FOUO)~~ BOXOAK systems will communicate with one another across Agency networks. Each system will have both a high and low classification associated with it, defining the full range of information residing there. The network across which these systems will communicate will also have a maximum classification associated with it. These levels will be available to the software to ensure that data cannot be transmitted to a system with an insufficient security level. Encryption is also available to provide security for data transmitted over networks and is employed by BOXOAK. Even when network levels allow the flow of classified information, the classifications of the receiving system and user ultimately decide whether the data transfer will take place.

~~(FOUO)~~ Another threat must be considered. While BOXOAK ensures that data is available only to authorized users, the SYBASE RDBMS can be directly accessed outside the application through the Interactive SQL (ISQL) command. Most BOXOAK users will not be granted the UNIX shell from which this ISQL command is executed; some administrative users will have shell access. The use of the SYBASE OpenClient software also makes it possible for a determined user to access these databases remotely. The ISQL access problem can be handled in a few ways. For instance, a wrapper performing access control can be written around the command to prevent its direct execution. Permissions on this command can be set to include a very limited group, excluding the general user community and eliminating the possibility of back-end access.

Advantages (U)

(U) It is usually preferable to use commercial products to provide system functionality whenever possible. The reasons stated earlier pleaded the case for development of a home-grown tool that meets the fundamental requirements of separation of multi-level information and prevention of unauthorized access. Other significant advantages were found as a bonus. These include:

- **Low Cost.** This strategy is significantly cheaper than the alternative of buying both a secure operating system and RDBMS. Developing the algorithms involves some resources, but these are reusable.

- **Simplicity.** The mechanisms for providing security are easily described and documented. They consist of a few additional classification tables and fields, modifications to queries, and a handful of translation algorithms.

- **Ease of Administration.** A standard operating system and RDBMS are both simpler to administer and maintain than their secure counterparts.

- **Flexibility**. It is easy to modify this design to accommodate other needed features. The original classification tables contained no data pertaining to color. When colors needed to be associated with classifications, the tables were quickly modified to provide this information.

- **Portability.** This strategy can be easily ported to other RDBMS such as INGRES and ORACLE. Creating the tables and modifying the queries is accomplished with the same code for all of these RDBMSs. The translation algorithms are written in Embedded C/SQL, which also can be used in all major commercial databases.

- **Vendor Independence**. Unlike other commercial products, secure operating systems are not well supported and maintained by the vendors. The decision to build a simple solution provides a means of avoiding this reliance on unsupportive vendors.

DOCID: 4033694

Conclusion (U)

~~(FOUO)~~ Security is the Agency's middle name and must always be applied to its resources. As the workforce gains computer awareness, one of our greatest resources, the vast pool of information residing on Agency computers, is increasingly vulnerable. Many measures can be taken to protect this information; the BOXOAK solution described is one approach that makes sense for its requirements. Every system must make a thorough assessment of its security needs and find the appropriate tools to safeguard its data. Publicizing and sharing our solutions lets us maximize reuse and accomplish security with a minimum of effort.

~~(FOUO)~~ *Ms.* [redacted] *started her Agency career twelve years ago as acomputer systems intern. Since then, she has worked in a varietyof areas, including finance, configuration management support, and collection, usually in database-intensive development efforts. Ms.* [redacted] *currently works in K254 as the software development manager for CADENCE, a new dictionary tasking system for DO analysts and dictionary managers. She also enjoys contributing to the Agency's technical health by teaching at the NCS, mentoring interns, participating in software process improvement activities, and writing this paper.*

P.L. 86-36

Kλ

An Appeal From the Editor:

REORG HAPPENS!

~~(FOUO)~~. . . and once again CRYPTOLOG finds itself with an outdated distribution list.

~~(FOUO)~~ We are frantically trying to update the list from the various announcements that circulate, but since organizations often combine as well as appear and disappear, this is not really a solution. Once CRYPTOLOG's home page is updated to reflect the recent P Staff reorganization, the distribution list will be available for viewing so that organizations can notify the editor of changes in the number of copies needed. Until then, we ask for your patience and cooperation if the wrong number of copies arrives in your organization. Please inform the editor of any necessary changes. Individual subscribers, as always, should inform the editor when their organizational designator changes. (For those who are puzzled by this distinction, the print plant no longer sends out copies to individuals or to organizations below the branch level; this is done by the CRYPTOLOG office.)

DOCID: 4033694

Editorial Policy:

(U) Technical articles are preferred over those relating to management, shorter over longer (under 3,500 words). Emphasis should be on improving NSA's technical performance; articles should be aimed at explaining developments in one's career field to thosE outside it. Readers are invited to contribute conference reports and reviews of books, articles, software, and hardware that relate to our missions or to any of our disciplines. Editorials are also welcome, as is humor. Submissions may be published anonymously, but the identity of the author must be known to the editor.

Submitting Articles:

(N.B. If the following instructions are a mystery to you and your local ADP support is no help, please feel free to contact the CRYPTOLOG editor on 963-5283s or cryplog@p.nsa.)

~~(FOUO)~~ Send a soft copy via e-mail to **cryplog@nsa**, or send a hard copy accompanied by a labelled diskette to the editor at P02 in 2C099, Ops. 1.

Guidance:

For maximum efficiency (as far as possible within the limits of your word processor):

- Do not type your article in capital letters.
- Classify all paragraphs.
- Label all diskettes, identifying hardware (operating system: DOS, UNIX), density and type of word processor used, your name, organization, building, and phone number.
- FrameMaker format is preferred; ASCII text is also fine. *(FrameMaker users: please do not put graphics in Anchored Frames as these are nearly impossible to reformat to our standard.)* J334 has a conversion service that converts Interleaf, WordPerfect, OfficeWriter, and MS Word into FrameMaker. Just attach the document to an E-Mail Compose Window addressed to **convert@nsa**.

DOCID: 4036134

NATIONAL SECURITY AGENCY

CRYPTOLOG

The Journal of Technical Health

Vol. XXII, No. 1

SPRING 1996

Declassified and Approved for Release by NSA on 10-10-2012 pursuant to E.O. 13526, MDR Case # 54778

Dedication of the Tordella Building, NSA's Supercomputer Complex October 29, 1996

DOCID: 4036134

CRYPTOLOG

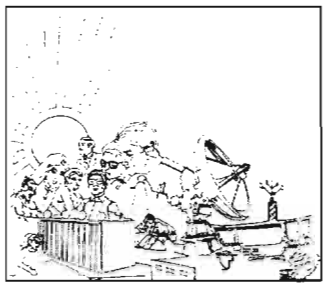
Spring 1996
Vol. XXII, No. 1

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

DOCID: 4036134

Table of Contents



Publisher's Note, by William Nolte iii

Eulogy for Louis W. Tordella, by Walter Pforzheimer 1

Biography of Dr. Tordella, by Thomas R. Johnson 2

KBE Presentation Ceremony 5

"Louis Tordella Led By Example", by [redacted] 7

Louis Tordella: As Colleagues Remember Him 10

Dr. T: The Man, by [redacted] 21

"If Lou Tordella Says It's OK, That's Good Enough For Me", by Gene Becker 25

P.L. 86-36

DOCID: 4036134

Publisher's Note:

Louis W. Tordella and the Making of NSA

by William Nolte

One of the dangers of retrospection, of history itself, is the tendency to see that which has happened as having inevitably happened. Every teacher of history can point to the folly leading to the American Civil War or the First World War simply because we know the events occurred. From the perspective of 1996 (or 1941), Lord Keynes's prediction that the Treaty of Versailles would be but an armistice of twenty years looks incredibly prescient. From the perspective of 1920, it may have appeared merely cranky.

So it is with institutions. First-time visitors to the National Security Agency must be struck above all by the sheer mass of the place. Even the eclectic (to put it gently) architectural style speaks to an institution of some permanence, permanent enough at least to have passed through several generations of general service esthetic fashion.

But it might not have been. The success of NSA, in operational and bureaucratic dimensions, obscures two important realities. The first is the relative novelty of a permanent, peacetime American cryptologic establishment of any real size. Only the Second World War and the subsequent determination on the part of presidents, the Congress, and the American people to remain on a virtual war footing to engage the Soviet Union led to a break in the tradition of nearly two centuries in which mobilization—of intelligence and military capacity—was followed at the coming of peace by an even more rapid demobilization.

In fact, of course, the United States did not break with that tradition in 1945. It did so in 1947 and beyond, when President Truman reversed his and the country's course back to "economy and efficiency." NSA, like the Central Intelligence Agency, is a product of that remobilization.

Which brings us to the second reality: nowhere was it predetermined that a national, as opposed to departmental, cryptologic establishment would be part of the architecture of post-World War II American intelligence. In fact, the first steps in the creation of a national structure were less than fully successful. The British historian Christopher Andrew has observed that the United States suffered strategic surprise in 1941 with two cryptologic agencies; in 1950 (with the invasion of Korea) it took four agencies (Army, Navy, Air Force, and the Armed Forces Security Agency) to achieve the same effect.

Seen from the vantage point of retrospective inevitability, the creation of NSA in 1952 appears to be the tidy completion of the process of nationalization. The Truman administration got it wrong with AFSA, got it right with NSA, and the rest is history.

In that context, Louis Tordella is noteworthy merely because of the length of his tenure as NSA's Deputy Director. His service could be reduced to something of a trivia question for new employees, akin to the bits of arcane service lore committed to memory by Annapo-

lis plebes and their counterparts at the other academies.

But that retrospective inevitably is illusory. NSA might easily have suffered the fate of AFSA. It might have been replaced by yet another attempt at cryptologic consolidations, or it might have performed its missions ineffectively over the next decades. If we believe what we claim about the importance of our missions, the cost of such failure would have been measured in lost American interest, lost American treasure, and lost American lives.

The argument here is that the success of NSA was not foreordained. It was the result of that combination of leadership, resources, and good fortune that underlies so much of human achievement. Success was also the product of skill, a shorthand term for the aggregation of intelligence, imagination, integrity, and patriotism of the generation of American cryptologists of which Dr. Tordella was the acknowledged leader. In no sense, was this his success alone. He was the witting inheritor of the policies and visions of predecessors, including NSA's first director, LTG Ralph Canine. To a great degree, Tordella's success brought to fruition the work of RADM Joseph Wenger, one of the truly great (and greatly ignored) figures in the history of American cryptology.

n retrospect, the Wenger-Tordella vision seems to have rested on principles so evident as to have seemed inevitable in their adoption. There is that word again. This vision centered on three fundamentals, the first of which was the need for national effort, while balancing the interests of the various services and departments of the government. The second principle was that of consolidation within the national effort. From the perspective of several decades, it may seem ridiculous to think that a cryptologic effort would require the placement of stations representing each of the uniformed services to intercept the communications of the counterpart target services. And even that did not address the needs of civilian agencies and departments. So you think, dear reader, that sounds faintly ridiculous? Yet the reality is that it happened, and the transition to a consolidated structure and consolidated operations took years of often intense struggle.

Finally, Dr. Tordella understood that the modern cryptologic establishment was not simply a larger version of the black chambers of earlier times. Code making and code breaking remained; they were not, however, the total reality of modern cryptology. Understanding the signals that carried cryptograms and the electronic computing technology that generated, stored, or routed them were parts of the process.

As was the true miracle of Twentieth Century cryptology, traffic analysis. The very idea that cryptologists, even when unable to produce plain text (the Holy Grail of the black chambers) could provide valuable, even lifesaving information to consumers, revolutionized the field. As an esoteric skill, and in limited applications, cryptology can exist apart from the environment of electronic communications and information management. Secret ink, anyone? But secret ink would not support the construction of the mass on the Baltimore-Washington Parkway. Modern cryptology is a multiphase, multidisciplined process, with the final victory achieved not at plain text, but at the delivery of information needed by a consumer in a format the customer can handle, in time for the customer to act. The central fact of American cryptology in the twentieth century remains that Pearl Harbor was a cryptanalytic success (the Japanese ultimatum being decrypted before the attack) and a cryptologic failure (in that the warning was not forwarded at appropriate speed).

DOCID: 4036134

It has been noted that Dr. Tordella, in addition to being the heir to so much of the achievement of Canine and Wenger, was also the leader of an extraordinary generation of American cryptologists. The preparation of this special issue of *CRYPTOLOG*, like so many of the other tributes to Dr. Tordella, attests to that. His colleagues have supported this effort with the same loyalty, affection, and respect that filled the chapel at Fort Myer for his funeral Mass.

Like Louis Tordella, his colleagues came to the cryptologic service from other fields, expecting, one suspects, to return to those pursuits after the war. Many of the cryptologic personnel of the Second World War did precisely that, rising in many cases to positions of eminence in business, in academic life, or even on the Supreme Court.

A few, including Tordella, stayed on, or resumed service after a short break outside government. Why did they stay? Certainly not because of the promise of fame or fortune. Certainly not because they foresaw an opportunity to get in at the ground floor of a large public enterprise.

Some say, even now, that "the business gets in your blood." All right, up to a point. Who doesn't like puzzles and mysteries? And which of us would not admit, if pressed, to some satisfaction at participating in an adult version of the child's "I know something you don't know."

We ritualistically dismiss the public perception of intelligence associated with the glamor described by Ian Fleming or even the analyst/case officer/covert action officer/policy maker of Tom Clancy (does Jack Ryan also run the motor pool?). But there is a mystique to it all, even amid the day-to-day bureaucracy.

"It gets in your blood" may be a partial answer. But it doesn't tell the whole story. A historian once noted that the Roman Church turned to deal with the wounds of the Reformation and the internal ills that produced it through the handful of adherents to the new Society of Jesus, "for their learning, loyalty, discretion, resourcefulness, and eloquence." Dr. Tordella was a product of the Jesuit tradition and embodied its virtues, chief of which was the determination to confront evil through the development of the intellect.

Over and over, Dr. Tordella's colleagues describe him through characterizations remarkably similar to that description of the early Jesuits: a commitment to education, his own and others; moral authority; integrity; loyalty.

And patriotism. This issue is a tribute to Dr. Tordella. But it cannot fail to be as well a tribute to the generation he led. Cryptology as an intellectual diversion may indeed get in the blood, but one suspects the other motive for remaining in the service for all of these men and women was something even closer to the heart. We, their professional descendents and fellow citizens, owe them every thanks.

DOCID: 4036134

DOCID: 4036134

Eulogy for Dr. Louis W. Tordella

by Walter Pforzheimer

As I look upon this gathering representing the family, friends and colleagues of Louis Tordella—among them great scholars and workers in the field of cryptology to which he devoted so much of his life—I know that the brief remarks I am privileged to make here should not encompass the technical fields to which Lou devoted a life of service to his country, and which so many of you know so much better than I.

But how to remember Lou Tordella in his professional career? A few days ago, I talked with my good British friend, Professor R.V. Jones, sometimes called the "father of scientific intelligence" for his work in World War II, and he recalled Lou's "sense of fair play" and again "his fairness and the balance of his comments." This was why, in part, the British awarded Lou's work and cooperation with the rare (for an American) title of Honorary Knight Commander of the Most Excellent Order of the British Empire. One might also remember that, in 1974, Louis was the seventeenth awardee of the President's National Security Medal—the fourth cryptologist to be so honored. How interesting to reflect that this very day, today, marks the fiftieth anniversary of the appointment of the first Director of Central Intelligence, a concept to which Louis gave so much of his professional NSA cooperation to make our Intelligence Community into a workable, national concept.

But remember that Louis was not all work and no relaxation. Remember his love of family, with the wondrous Barbara and his children at his side. Remember his great love of music—opera in particular. He would sit by the hour listening to opera broadcasts, or attending nearby performances of both opera and symphony. Remember one of his proudest boasts (and he was not a boastful man), as he told of how, when he was a student, he managed to work himself into a walk-on part as a spear carrier in an opera—I think it was "Aida."

Let me now say what is known to all of us—Louis' tremendous capacity for quiet friendship. His arms reached out to embrace so many of us. So did his thoughts. As Alexander Pope wrote in the eighteenth century, "Thou wert my guide, philosopher and friend." So it was with Louis. For me, it has been more than a quarter of a century; for some of you, even longer. It was a warmth of friendship which will be with us always.

Finally, let me say, in what little Latin I can muster: Ave atque vale: Hail and farewell, dear friend.

Walter Pforzheimer's involvement with the OSS in World War II has been described in Robin W. Winks' book "Cloak and Gown." This eulogy was delivered at the memorial service for Dr. Tordella on 23 January 1996.

DOCID: 4036134

Dr. Louis W. Tordella, 1911-1996

by Thomas R. Johnson

Dr. Louis W. Tordella, a former top official of the National Security Agency, died of cancer on 10 January 1996 at the age of 84. Dr. Tordella was a pioneer in the science of cryptology and rose to the position of deputy director of NSA, a position he held for sixteen years, longer than any other official at NSA.

Dr. Tordella was born in Garrett, Indiana, in 1911 and grew up in the Chicago environs. He displayed an early affinity for mathematics and obtained B.S., A.M., and Ph.D. degrees in the 1930s. The outbreak of World War II found him teaching mathematics at Chicago's Loyola University.

He volunteered for the Army, but the recruiter told him that the Army would draft whomever they needed. So Tordella made contacts in the Navy, and he was brought aboard as lieutenant junior grade in 1942. He went directly into cryptologic work for the Navy's codebreaking organization, OP-20-G, where he worked on the German Enigma cipher machine. He was one of a team of brilliant mathematicians who designed the "bombe," a wartime machine used to decipher the keys on the Enigma. He finished the war at OP-20-G collection stations on the West Coast, at Bainbridge Island, Washington, and Skaggs Island, California.

After the war, Tordella stayed on with the Navy, and in 1949 he joined the newly created Armed Forces Security Agency (AFSA), an early attempt to achieve service unity in the business of cryptology. He was a key figure in devising policy for the new agency and for its successor, the National Security Agency which emerged in 1952 to replace AFSA. Although a Navy man, Tordella readily grasped the advantages of unification, and he pushed the concept forcefully in the early years.

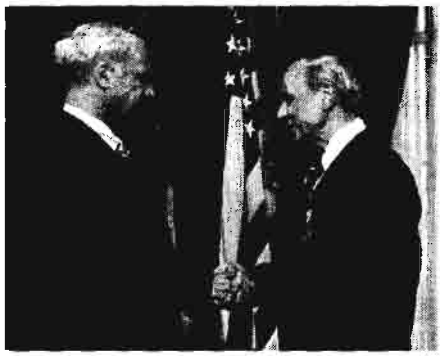
Tordella's career at NSA brought him to the very front rank of cryptologists. On the technical side, he was an early advocate of the use of computers for cryptologic work, and he helped to cement a close working relationship with a new computer firm, Electronic Research Associates, which eventually became CDC. His grasp of computer technology and the associated engineering concepts, coupled with his understanding of cryptanalysis, was invaluable in keeping the United States ahead of the field in this critical skill. Tordella was also a leader in securing American communications, pushing a series of leading-edge new encoding devices to secure U.S. government communications.

During the Eisenhower administration, when the central concern of the government was the growing Soviet nuclear capability, Tordella led the NSA response. He was the driving force behind NSA's response to the threat, and he directed the technical activities of the Agency at a time when President Eisenhower had little else to rely on except signals intelligence. In 1958 Tordella persuaded Eisenhower to fund a new communications initiative, called CRITICOMM, which offered a means to get critical intelligence information to the White House within ten minutes. The new system revolutionized concepts in Ameri-

DOCID: 4036134

can intelligence, bringing with it methodology that is still in use everywhere within the defense and intelligence communities.

As a senior official at NSA, Dr. Tordella played a central role in NSA's outside relationships. Close collaborators in Great Britain and the British Commonwealth built up such a trust with Tordella that many foreign intelligence officials regarded him at the linchpin of their relationship with NSA. He traveled throughout the world building up that trust, and it paid great dividends over many years. He also served as the principal contact between NSA and its American collaborators: CIA, DIA, and the Office of the Secretary of Defense.



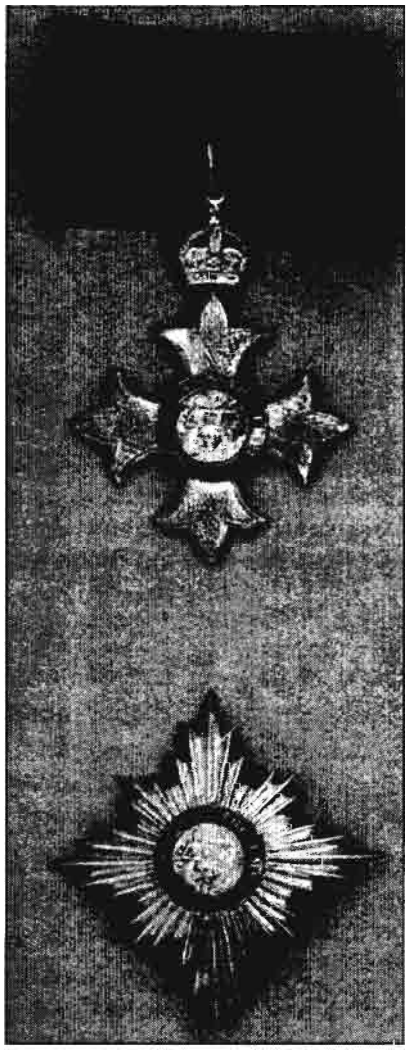
Secretary Schlesinger presents Dr. Tordella with the Baker Medal

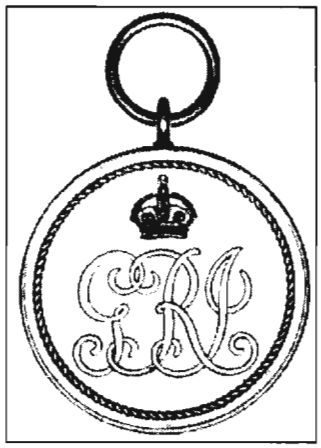
In July of 1958, while he was serving in a liaison post to the secretary of defense, Tordella was asked by then-Director Lt. Gen. John A. Samford to become his deputy. Tordella took office on 1 August 1958, and he continued as the deputy to six successive directors until his retirement on 21 April 1974. He thus became the longest-serving high intelligence official since World War II. Within NSA, he became an institution, and to many he ***was*** NSA. There was no precedent for his tenure, nor has it since been equaled.

Dr. Tordella received unprecedented honors over the years. On his retirement in 1974, the secretary of defense, James R. Schlesinger, presented him the National Security Medal. That same month he received the National Intelligence Distinguished Service Medal from the Director of Central Intelligence, William Colby. His relationship with the British was officially recognized in 1976 when he become an Honorary Knight Commander of the Most Excellent Order of the British Empire. After his retirement, he remained active in the intelligence community, serving on a number of boards and committees and as a consultant to various corporations that held national defense contracts. In 1992 the Security Affairs Support Association, composed mainly of retired intelligence officials, gave him the William O. Baker Medal for distinguished service to American intelligence.

CRYPTOLOG thanks Mr. Johnson and the Center for Cryptologic History for permission to use the official NSA biography, which is engraved on a bronze plaque in the National Cryptologic Museum, and for the many photos of Dr. Tordella that appear in this issue.

AND THE EMPIRE





DOCID: 4036134

Dr. Louis W. Tordella, Honorary Knight Commander of the Most Excellent Order of the British Empire

Presented by Sir Peter Ramsbotham, Her Majesty's Ambassador to the U.S. Washington, DC, February 1976

Ladies and Gentlemen,

It is a very great pleasure to welcome Dr. and Mrs. Tordella and their family, and all our friends and guests, to this ceremony this afternoon.

We have all grown so accustomed to the closeness of the relationship between our two countries, that those of use who live and work in the United States have come to take it for granted. One reason why I welcome the tumultuous and expansive way in which you in America have begun to celebrate the 200th anniversary of your birth as a nation is that, for all the enthusiasm with which we are sharing in your festivities, it does remind us British that circumstances are capable of provoking some very nasty misunderstandings. It is somewhat paradoxical for an ambassador, in speaking to audiences around the country to which he is accredited, to remind them of the differences which drove their ancestors to war. But I do it, because it brings home to us now that the excellent relations we enjoy today are not the result of some divine ordinance.

They have come about more than anything else through the close ties that exist between so many of the separate departments of our countries' activities, both official and unofficial. There is, in peacetime, no natural identity in our national interests, even though there may be compatibility. But there is a continuing opportunity to contribute to each other's enterprises which makes our joint activities more than doubly rewarding and exciting.

It is particularly in this period since World War II that our co-operation has been profitable, the period spanned by the career of the man whom we are assembled to honour today. For his services, Dr. Louis Tordella has already been awarded several of his country's highest distinctions. But his devotion to his own country has been matched by an outstanding contribution to our common cause. The distinction which Her Majesty The Queen has now been pleased to confer upon him is only rarely awarded to a United States citizen. It is, indeed, one of the most senior ranks of the Most Excellent Order of the British Empire and is, in a sense, Her Majesty's gift. Dr. Tordella will be joining the honoured company of those whom the British Sovereign has rewarded over the centuries for services which go far beyond the call of normal duty. The distinction is richly deserved by one whose collaboration with the United Kingdom in the field of national security is a most significant example of the partnership which we value so highly. I am sure that for you all, as well as for my wife and myself and members of my staff, this is an occasion that we will long remember.

DOCID: 4036134

And so it is with the greatest pleasure that I shall now read the formal authorisation for me to make this award on behalf of Her Majesty The Queen:

"By command of Her Majesty Queen Elizabeth II, by virtue of the authority vested in me as Her Britannic Majesty's Ambassador and Plenipotentiary at Washington in the United States of America, it is my honour and privilege to present to Louis William Tordella the insignia which Her Majesty The Queen has been graciously pleased to bestow—that of membership of the Most Excellent Order of the British Empire in the rank of Honorary Knight Commander, in recognition of outstanding services."

Louis William Tordella, I request that you now come forward to accept the insignia of the Order.

February 19, 1976

CRYPTOLOG thanks [redacted] *and the UK Liaison Office for providing the text of the ambassador's remarks and photograph of the medal.*

EO 1.4.(d)
P.L. 86-36

DOCID: 4036134

"Louis Tordella Led by Example"

by [redacted]

P.L. 86-36

On January 23, 1996, I stood in the chill winds among patches of snow in Arlington National Cemetery. I heard the words of the funeral service, saw the American flag folded and presented to Barbara and family. Then came the rifle salute and the lump-in-the-throat sound of "Taps." My closest longtime friend, travel companion, and co-worker had come to his final mortal resting place. Walking to our car, my wife Jeanne and I talked about the great good fortune which brought the Tordella and [redacted] families together. For my part, I again realized how proud and pleased I am to have spent most of my active career life working with "Dr. T" and the rest of the World War II cryptologic crew.

That crew participated in the unification of Army and Navy organizations under the Armed Forces Security Agency (AFSA). Later we all gave fervent thanks when AFSA was replaced by the National Security Agency—a national-level agency.

Louis and I became close friends when we participated in the first London Conference in 1948. Rules and agreements were established for cooperation similar to the wartime UK-USA arrangements which had produced amazing successes on difficult challenges. After our return, we began our career-long cooperation (some called it collusion) by jointly scraping together a total of slightly over $400,000 —from diverse Navy and Army kittys! Then we organized and used the money for a "do-it-yourself" NSG-ASA fabrication project to build radio teletype intercept equipment to cover foreign non-morse communications. The production line was in the basement of the cafeteria at Arlington Hall Station. The equipment worked, and we stayed under budget.

With the unification of the ASA-NSG organizations, the military and civilian components all entered the "Agency Invention" period of AFSA, then NSA. This was a time of travelling, planning and much bureaucratic shadow-boxing (to establish NSA missions and assist Service Cryptologic Agency budgeting, personnel, and operational mission requirements definition and justification).

From 1952 until 1968, I travelled to much of the world with "Dr. T," visiting and evaluating facilities, identifying problems (often with NSA) and participating in base-rights and cooperative international arrangements. With the Director, we also made numerous command appearances before DoD and congressional review and approval authorities to sell (or save) program and budget proposals.

In later years (in fact, in October 1995, while Jeanne and I were staying with the Tordellas for the October Cryptologic Symposium), Louis and I talked about our choice of a career in NSA. We concluded this October that our career decisions were based on (1) the interest, satisfaction and lack of sameness of

[redacted] *is a former NSA senior official.*

P.L. 86-36

cryptology and, (2) personal convictions that the miracles of wartime contributions to Allied success should be maintained as an asset to our nation. The motivation for selecting NSG or ASA was certainly not to join an established operation with existing and clear missions and objectives and a positive career outlook for the future. On the contrary, the stringent security of ULTRA had limited its distribution to a few selected need-to-know military and civilian users. This preserved the anonymity (but also limited the appreciation) of the source. Post-war demobilization further shrank the ranks of knowledgeable, experienced users to a mere handful.

With the defeat of Axis military forces, the highly competent cadre of wartime cryptologists faced a unique dilemma. They felt committed to preserving what they knew to be an essential national security function, however, they were faced with:

- drastic reductions in military expenditures
- no major or high national priority targets
- limited U.S. government customers
- questionable requirements for whatever they might be able to produce.

The stringent security of ULTRA had limited its distribution to a few selected need-to-know military and civilian users. This preserved the anonymity (but also limited the appreciation) of the source.

Yet this problematic venture attracted Louis Tordella, who could have opted for university-level teaching or other stable occupations.

His choice of career is an indication of his dedication. It is difficult today to comprehend the hand-to-mouth existence of the early years of AFSA/NSA. Fortunately, the endeavor had gained a number of sponsors in high government offices through VENONA successes. Later successes justified funding of expanding NSA and also solidified specific missions and functions for the Agency.

One of the greatest problems of the first decade of agency operations was bringing together individualized capabilities and divergent outlooks of very independent, and highly skilled technocrats. Leadership for harnessing and concentrating the exceptional capabilities of these rugged individualists was provided by Dr. Louis W. Tordella. He was accepted and therefore followed because of his brilliant crypto-scholarship, his practical knowledge, and his fair professional judgment. NSA workers and members of the associated Intelligence Community became aware of and admired his combination of technical talent and high moral and ethical standards. It is truthfully said that Dr. T never compromised his beliefs or objectives, and never claimed or derogated success achieved by others.

He led by example and by offering inspiring rationale for focusing limited assets and mindpower on urgent requirements. His leadership was key to NSA responsiveness and contributions when urgently needed by our nation's planners and leaders.

With the passing of years and time to think about past and current events, I have come to realize that the greatest accomplishment of Louis Tordella and his compatriots (and successor cryptologists) may not be easy to define—but is in fact the impact the NSA creation has made in our world and in particular in our nation. Contributions to successes in

DOCID: 4036134

the Intelligence Community, assistance to national leaders, and support for military and diplomatic initiatives have all caused varying degrees of change for U.S. citizens, most of whom probably are not even aware of the National Security Agency. Working in defense industries, I see many programs implementing cryptologic functions which continue to drive home the fact we are all part of history and all of us share in results of past events.

It is truly said that Dr. T never compromised his beliefs or objectives, and never claimed or derogated success achieved by others.

If the real value of a life and its ultimate worth is in part the difference it makes in our world, then Louis Tordella certainly made important differences. All of us who worked with him share a feeling of pride and wonder at having been part of an historic national cryptologic program.

(U) This is my appreciation of an exemplary life and my salute to a true friend: Dr. Louis W. Tordella.

CRYPTOLOG's Former Board Chairman Remembers His First Meeting With Dr. Tordella:

I was truly saddened when I learned of Dr. Tordella's passing, recalling the first time we met. I had entered on duty full-time in June 1966 and automatically entered a six-week orientation program at the old hospital site. The weather was hot and sticky, compounded by the fact that the only air conditioning was a big fan trying quite unsuccessfully to ease the internal smog. Despite the prospects of a long, hot afternoon, an announcement came by phone that the deputy director was coming by to visit with us.

Having spent two prior summers as a summer hire, I was familiar with who the deputy director was: one of the founding fathers, ranking with Friedman and several others who had broken the German and Japanese codes leading to victory in WWII. You cannot imagine my excitement and yet at the same time disbelief that such an important personage would visit our lowly EOD class. Especially that he would do so in such oppressive heat and humidity and then to stay even longer to have lunch with us.

I don't remember what he said, only that he did come by to visit and that he spent a few minutes during lunch talking to each one of us. What I remember most of all is the thought I had then and have never forgotten: saying to myself, so this is what being a great leader is all about.

[redacted] *retired after spent many years with NSA, most recently as the DO Senior Training Authority and Chairman of the Technical Health Advisory Board; he also chaired CRYPTOLOG's editorial board.*

P.L. 86-36

DOCID: 4036134

Louis Tordella: As Colleagues Remember Him

In March 1996, several of Louis Tordella's colleagues assembled in the NSA Broadcast Center for a retrospective on his career. The participants for this session were: Ann Z. Caracristi, former Deputy Director of NSA, Maj Gen John Morrison, USAF (ret.), Mr. Arthur Levenson, [redacted] and CAPT James Pendergrass, USN (ret). An edited transcript of their conversation follows.

P.L. 86-36

(L-R) **CAPT Pendergrass, Maj Gen Morrison, Dr. Nolte, Ms. Caracristi, Mr. Levenson, and [redacted] reminisce about working with Louis Tordella**

CRYPTOLOG: *Each of you knew Dr. Tordella for several decades. Captain Pendergrass, you seem to have the honors within this group for the earliest association with Dr. Tordella.*

Pendergrass: After the war, the Naval Security Group was in chaos, as was everything else in the services. I found myself just back from Bletchley and found myself on a newly created staff, one of the other members of which was Dr. Tordella. This was early in 1946, January or February, and from that point I got to know him quite well.

Was he still on active duty?

Pendergrass: No. He had converted by that time.

Morrison: I met Lou in 1947 at Nebraska Avenue [Naval Security Group Headquarters]. I forget what the occasion was, but we were still busy trying to strap ourselves together. Something was in the wind about reconstructing the business we had been in. We knew that something had to be done about the future of the business, and this meeting was one of those occasions. Later, in 1948, I had the opportunity to travel overseas with him, and the relationship continued from there.

[redacted] This period that John's talking about was a very important time in the postwar development of the cryptologic business. The

P.L. 86-36

DOCID: 4036134

Navy and the Army were coming together, and there were many problems associated with integrating their wartime efforts. At times, it seemed like it was not going to get done, but the AFSA came into being. That did not put to rest all the frictions and suspicions that existed, and this is how I came to know Dr. Tordella. He was recognized, even in those early days, as the kind of person who could serve well as a peacemaker. That may not be the right word, but he had the capacity to develop balanced positions that would lead both sides to trust him and talk to him. This is the area in which I've always thought Dr. Tordella made his greatest contribution: keeping us together in the days when we were very weak and very vulnerable, and we could have been attacked from any direction. Tordella had foresight and vision and held us together in that period. I was already developing a great loyalty to him, and it stayed that way throughout my career.

Most of the audience for this discussion will have no first-hand experience with how tenuous arrangements were during this period. Any other thoughts on Dr. Tordella's role in that time? Was there a danger this consolidation would fail?

Caracristi: I think there was. As in any consolidation of two bureaucracies or two companies, everyone gets very defensive about his own role. Will you be able to play as powerful or important a role in the new organization as you did in the old one? So there was a lot of tension in this period, but I think people who came out of the wartime experience still had a tremendous commitment to what we were all about. We were more interested in accomplishing the mission than in fighting bureaucratic battles, though there certainly was some of that going on.

Morrison: To use the current expression, we had "different cultures."

Levenson: At the working levels, it may not have been that bad, but at the higher levels it got worse. In the Army, we had the feeling that the only way we could find out what the Navy was doing was to go through the British.

So the communication path from Arlington Hall to Nebraska Avenue ran through Bletchley Park.

Levenson: It was really ridiculous. So consolidation was always looked upon as a distinctly frail effort.

Morrison: Younger people here who are interested in the pulling and tugging associated with those days ought to take a look at some of the material on that period, just to see what life in that period was like. It was tough going. You were never sure we were going to end up with a coherent assembly of people who would be mission-centered and with the capability to serve the national interest. Service rivalries were tough, and once the Air Force became separate in 1948, you had another player to contend with. I was very active on that side, pulling and tugging in the direction of the Air Force, while the Army and Navy were pulling in their own directions.

Levenson: Another of the tough issues of the period involved our relations with GCHQ. We had the cooperation during the war, the result of a high-level agreement between Roosevelt and Churchill. Historically, even between the friendliest of countries, people never exchanged cryptologic sources and methods and results. The fact of this cooperation, with the assignment of Americans to GCHQ, was a breakthrough. But with the war over, the question was "Where do we go from here? Do we continue with this cooperation or is it too sensitive?" Lou Tordella played a very important role in this area, as one of the people who established the postwar cooperation.

DOCID: 4036134

We're having this conversation within a week of the 50th Anniversary of that agreement. Was there opposition to continuing this extraordinary cooperation?

[redacted] Of course. There was opposition from other intelligence elements who felt that the cooperation in Signals Intelligence was too close, and other people were feeling left out. Some of this may have been that there were no formal guidelines for the cooperation until the BRUSA agreement, which Lou not only played a role in devising but on which he spent the next several years working on implementation.

Morrison: Lou was recognized early on in this relationship as a leader, as a man of substance. Even as early as the BRUSA Conference of 1948, he was recognized as the leader of the American delegation. Louis stood out; he always stood out.

Was that a consensus view?

Levenson: I can remember a briefing he gave early on. It was so remarkable, in its decisiveness and its clarity, I told him afterward he was going to be the first civilian director of NSA. He didn't quite make that, but then no one else has either.

One of the names associated with Dr. Tordella's early career is that of Admiral Joseph Wenger. Would it be fair to describe Dr. Tordella as a Wenger protege?

Pendergrass: To a certain extent. Lou had worked for then-Captain Wenger, who had a real appreciation for what Lou could do.

In late 1952, AFSA was replaced by the National Security Agency. Where was Dr. Tordella in the process?

[redacted] Lou had run what was called the Collection Division in AFSA, running in effect the intercept resources. This was a natural for him, having come in to AFSA from having been a station commander in the Navy. Then, when General Canine came in 1951, Lou moved to what was called AFSA 12, Plans and Policy. That unit had assembled several of the "bright young stars" of the agency, and it's my recollection that Lou went from there to the National War College in 1953-1954. When he left the War College, he spent a year or so at the Pentagon working for General Graves B. Erskine, who was a great friend of General Canine, NSA's Director. He then became head of something called NSA 70; it had been AFSA 70, but we kept the same numbers and just changed the letters.

Caracristi: I've always been grateful to Lou for the chance to be exposed to an entirely different part of the business.

That tells us something about how momentous the switch was from AFSA to NSA. You went out of business on Friday as AFSA and came back to the same organizations on Monday.

Caracristi: At the time, I was in one branch, and Juanita Moody was in charge of another working a different problem. Lou called us in one day and essentially asked us if we would be willing to [ex]change jobs. Lou was not the sort of person you said no to, but at the time it seemed to me like a strange arrangement. In the end, though, it worked out very well, giving each of us a chance to be exposed to an entirely different part of the business.

DOCID: 4036134

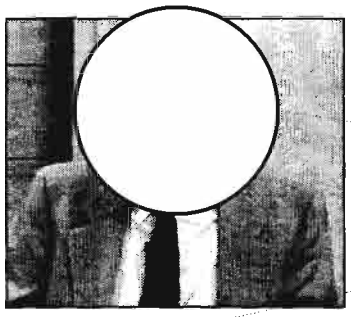
I've always been grateful to him for arranging that.

What was it like working here during that time? It was a technically difficult period. Did that affect morale?

Caracristi: Morale was never hard when the problems were hard. In fact, I recall morale as being very good.

Was there, however, concern being expressed from outside the agency about the future of cryptology?

Caracristi: There were concerns in that regard, and committees were formed to look over our shoulders, an effort in which Arthur was heavily involved.



[redacted] **We were telling companies like Control Data and IBM what we wanted, and Tordella was at the center of that effort.**

[redacted] Of course congressional oversight was a completely different issue. We didn't have any in those days. General Canine's favorite story was that he would go down to Capitol Hill, and some member of the appropriations committee would ask some interesting question to which the general would answer "Congressman, you don't really want to know the answer to that. You wouldn't be able to sleep at night." And the members would look at each other and they were content with that.

Levenson: All the committee chairs were very friendly in those days, and the secrecy impressed them, and they believed that NSA had to operate in a special way to be effective. We got most of what we wanted, and a free hand in how we used it.

In 1958, General Samford invites Dr. Tordella to a meeting in which he asks for Tordella's opinion of what the deputy director should be like. Dr. Tordella tells him the deputy director should be the director's "alter ego," and Gen. Samford says, in effect, you're it. Was that a surprise to anyone?

Levenson: Dr. Tordella had given one of his celebrated briefings to General Samford and a small group at the Pentagon, and they were very impressed. And that may have sold it for Lou.

[redacted] There was another candidate for the job, but I don't think there was any doubt that Dr. Tordella was the natural choice for the job.

P.L. 86-36

That will guarantee us a sotto voce reference or two on the tape to the other candidate. Were there any immediate changes with him in that job?

Levenson: I think the immediate impression was that now we *had* a deputy director, because his predecessors had had little impact. Joe Ream, the first deputy director, may have been a terrific lawyer, but he was out of his element. And Howard Engstrom was a capable man, but he held the job for only a short time before he left too. Once Lou came into the job, you knew there was someone there.

Dr. Tordella told the story of Mr. Ream coming into his office on the day Ream left, handing Tordella all his papers, and saying "Lou, you might as well keep these. You're the only person here who's ever spoken to me."

Morrison: I wasn't stationed here at the time. I was in the field. But the immediate impression was that there was a steady hand on the tiller. These were turbulent times, and peo-

P.L. 86-36

DOCID: 4036134

ple felt safer with Lou up there manning the conn.

Captain Pendergrass, you were not here at the time, but you had remained personal friends with Dr. Tordella.

Pendergrass: Well, when he made deputy director, I was surprised. I was with the Agency, in Melbourne, but even though he was an old friend, I considered it a surprise—a very pleasant surprise. He came out a few months later for a conference. He was still very interested in foreign relations, and he impressed all his colleagues at that conference.

We've entered into the period of his deputy directorship, a time in which, among other things, NSA was doing important work with the emerging technology of computers. [redacted] can you speak to that?

Pendergrass: Lou always knew what he was talking about because he spent time and effort to understand the issues.

Levenson: The computer business was in its infancy. A few years earlier, we'd had the invention of the first stored program devices, like ENIAC, and the British COLOSSUS, which you programmed by setting switches. After the war, several small groups, especially the United States, got into the business. Remington Rand-UNIVAC got started as ERA, Energy Research Associates, and Howard Engstrom was deeply involved in that effort. In those days, AFSA and later NSA operated with something of a "fee hand" in using our money. This amounted at one point to about $20 million dollars [in available funds], which in those days was real money. But we invested that money in several computer projects, including an effort to underwrite research into high-speed computing. We were basically telling companies like Con Data and IBM what we wanted in high-spe high-storage computers. HARVEST was result of that effort. That was all NSA, a Tordella was at the center of that effort. many years, we were IBM's best custom They knew it; we knew it; and we had a cons erable influence on the industry.

In looking at Dr. Tordella's work in this ar one gets the sense of someone very conscious the need to stay in touch with developments places like IBM and other te nical centers.

Levenson: Bell Labs another example. We wor with Bell Labs to develop first instances of shared p gramming, allowing seve users to have access to the s computer. The whole concep virtual storage, in which y keep moving data around so things you're not using imm ately can be shoved out so so thing else can be shoved increasing your storage.

P.L. 86-36

The issue of people skills must have b interesting. You certainly didn't go out and people with computer degrees.

Levenson: Right. We had to develop own skills, but we came up with some crac jack programmers that way. In those days, programming languages were very primiti and very specialized. That was very diffic We eventually decided, however, to go to so thing called "open-shop programming," on theory that it was still easier to teach a cryp lyst to program than to teach cryptanalysis programmer. We had some friction in the e days of cryptanalysts complaining that the grammers didn't know what they wante

DOCID: 4036134

wouldn't deliver what they wanted, so we said, "Here. You do it."

Caracristi: That's an area in which Lou Tordella had to step in and make it open.

Levenson: Oh yes. He had to overcome the resistance of the programmers' "union," that didn't want to open up the field.

Speaking about another "union," what about Tordella's relationship with other parts of the intelligence community?

Caracristi: I think they were excellent. He developed an excellent relationship with Richard Helms, for instance. He was the kind of person who developed respect. Those were times when NSA was recognized, as it continues to be, as the expert in a rather arcane world. Lou was able to bridge the gap between that world and the more general area of intelligence. Most of all, he was able to make understandable what was going on at NSA, using the briefing skills that Arthur has described. His standing in the community was very high, and he was, in effect, our link to the community.

Morrison: Those of us who attended Lou's funeral noted the number of people from other parts of the community. CIA was well represented, as were other agencies. They really turned out.

You get the sense that when Louis Tordella talked, people listened.

Pendergrass: He was a good teacher.

Follow up on that, if you would.

Pendergrass: As a matter of fact, Lou not only taught before he came into this business, he taught at night at George Washington University. He even used that experience to recruit a few people.

Levenson: He was very good at teaching. He would have risen to the top of that field, or any other field he got involved in. On a trip to Alaska one time, we stopped in Chicago to change planes and we were met there by the provost of Loyola University of Chicago, Lou's undergraduate alma mater. At one point, the provost turned to Lou and said, "If you had stayed with us, you would have been the dean."

It sounds like GW's math department needs to erect a plaque of some sort marking the contribution of NSA to its programs. Solomon Kullback and Louis Tordella.

Pendergrass: I think we've missed one point in that Lou always knew what he was talking about because he spent time and effort to understand the issues he was dealing. He wanted to understand all the parts of the business, rather than being a specialist in cryptanalysis or collection or whatever.

P.L. 86-36

[redacted] His student-teacher involvements were a lifelong concern. He taught both before and while he worked here. But even after he retired, he continued to go over to the University of Maryland and take courses in chemistry and physics.

What was it like working here while Dr. Tordella was deputy director?

Caracristi: As Jim said, he worked very hard to keep track of almost everything. One of the things I remember him keeping track of was the VENONA problem, which has recently been declassified. Now everybody knows about it, but for a long time, this was something Lou took a great deal of personal interest in. He kept in touch with the people working it, he looked at the product, he personally arranged to collect material that would enhance our productivity on this problem. It was also an area in which he had great concerns about security and compartmentation.

P.L. 86-36

He kept personal track, as he always did, with the people working problems and issues that interested him. And he knew—personally—vast numbers of the people who worked here, even during periods of rapid growth.

Did he have a role in the continued work on this project so long after collection stopped?

Caracristi: Very much so. There was a great deal of concern that within this material might be revealed who were the missing spies in various cases that had developed. Because he thought this material might reveal some of that information—in effect, traitors in this country or in England—he, together with the British, encouraged the pursuit of this problem.

Were there people in the building who were suggesting that this was not worth continued effort, that it was becoming a historical problem, not a cryptanalytic one.

Caracristi: Yes, there were. I may have even become one of them.

It must have been difficult for a new director to come in here with a deputy who was so firmly entrenched.

[redacted] Some of these directors are still around, so I'd better be careful. But most of these men had very strong personalities of there own, so I don't think they felt challenged by Dr. Tordella. Some, especially those we might describe as more intellectual, actually felt good having him around. General Allen and Dr. Tordella had a great relationship, and General Allen was one of the better-informed directors, technically speaking, we've had. Other directors may have been more political or not as technically skilled, and they may have been intimidated by Dr. Tordella.

Levenson: Let me put in a word for Gordon Blake, who was a very good director and who did not feel threatened by Lou. And they worked well together. Next to Canine, who in my book was in a class by himself, Blake was marvelous.

[redacted] Canine was another one who had a great respect for Tordella. No question about it, Canine helped establish Dr. Tordella's position in this agency. To cite another case, I don't think Gen. Samford was intimidated by Dr. Tordella. I think he regarded him as a friend. I know that Admiral Frost looked to Tordella for help on many things.

Levenson: Admiral Frost looked for help anywhere.

[redacted] Admiral Frost was his own man and made his own decisions. But he was wise enough to understand that Dr. Tordella's understanding of this business was greater than his. He took advantage of that understanding. All the parties associated with this story are deceased, so I think I can tell it without fear of libel suits. But we had a new director, Admiral Frost, and there was a period of several weeks in which he could not take up his position because his predecessor was not eager to give it up. So Dr. Tordella, who had become deputy director at that time, decided Admiral Frost should occupy himself going around visiting places that were going to be important to him in his new job. He wanted him to visit GCHQ, and he asked me to go with him to keep an eye on him, make sure he saw the right people, and so on.

Let's talk about the period just before and after Dr. Tordella's retirement. Was this a surprise?

Caracristi: No. I think it was accepted.

P.L. 86-36

DOCID: 4036134

Morrison: If anything, I think people felt Lou was entitled to retire. He had borne the brunt of an awful lot.

Caracristi: And Buffham was the heir apparent. Buff had worked plans and policy, and had the background to deal with the range of problems associated with the job. So, I think it was a very easy transition.

Levenson: I think it was an advantageous time for him to retire personally, and at some point I think he actually felt he may have stayed a bit too long. It may have been true. He did so many marvelous things, but you can only stay in a job so long. He was ready to go.

What stands out about him personally? What should this generation of cryptologic professionals know about Louis Tordella?

Morrison: He was a dedicated man, a man who just lived this business. The amazing thing is how he found the time to do all the things he did. He ran rings around all of us.

I frequently worked on Saturdays when I was ADP, and Lou would work on Saturdays, and after noon or so, we would go up to the Director's dining room and look in the icebox and get cheese and rolls and "libations," and then we'd really get around to talking about what was on our minds. This was where you saw the real, warm, considerate person he was. I just admired the dickens out of him.

Caracristi: It's important to remember that even though he did work hard, he was able to maintain interests in things other than work. He was very interested in opera, not just the Washington Opera, but the Baltimore Opera. He went to New York to the operas; he was interested in other kinds of music. He was interested in his family. This was a very well-rounded person.

P.L. 86-36

[redacted] There'll never be another Tordella.

Captain Pendergrass, we've done you the disservice of surrounding you with all of these Army people. You get the last word.

Pendergrass: He was a rare combination. He was a very smart man, a hard-working man, a very good leader who was also very loyal. It's not easy to find people who combine all of these. When you think of the funeral and the chapel at Fort Myer absolutely full. I think the staff over there was completely unprepared for standing room only for a Captain, U.S. Naval Reserve. That was a tribute on the part of everyone there.

I know you're all here today to honor Dr. Tordella, but for those of us working here today, it's an honor to have you back. Thanks for coming to spend the time.

DOCID: 4036134

CRYPTOLOG interviews NSA employee Gene Becker:

Mr. Becker, you've witnessed the discussion with Dr. Tordella's colleagues. What's your sense of Dr. Tordella's contribution to NSA?

As has already been pointed out, Dr. Tordella's contribution to this agency was absolutely tremendous. Among the qualities that distinguished him were his integrity, even extending to very minor things. Frank Austin, who was very close to Dr. Tordella, describes how Tordella was in London when Frank was our representative there. Tordella's flight was cancelled and Austin offered to arrange to get him on another flight, first class. Dr. Tordella refused, saying he wouldn't travel first class, because no one else in the agency could. Austin tried to persuade him that it would keep him on schedule, but Tordella wouldn't hear of it. He flew out the next morning, on coach. That was Dr. Tordella.

"When questions came about why did NSA need this or need that, the assurance that 'Dr. Tordella says they need it' went a long way toward gaining approval."

The other characteristic that came out in this conversation was his moral authority. When the Martin and Mitchell case came about, it was one of the worst spy cases in the agency's history to that point. It shook everybody up, the chief of personnel and the chief of security were fired, and the workforce was very restive. Rumors were flying all over. Dr. Tordella convened a meeting in the Friedman Auditorium, and gave assurance to the agency that, no matter how bad the case was, we would go on. People should go back to their jobs and carry on. With his assurance, the shock waves going through the agency were stilled. He had enormous authority in moments of crisis.

But the power of Dr. Tordella's word was enormous within the U.S. government. At the time, for example, he handled the NSA budget practically singlehandedly. He either prepared the director to go downtown or he testified personally. When questions came about why did NSA need this or need that, the assurance that "Dr. Tordella says they need it" went a long way toward gaining approval. That kind of authority is not likely to be equalled.

Someone once said "You manage things; you lead people." And the leadership quality comes across so strong, you could still see it today with our guests. Dr. Tordella was their leader.

And that respect and authority continued throughout his life. There's also that attention to detail. Nothing was too insignificant to escape his attention. When the agency moved to the Friendship complex, the regulations said the government had to pay relocation allowances if the change of station involved a trip of more than 10 miles. The system assured Dr. Tordella that in fact the distance did exceed 10 miles. But that wasn't good enough for Tordella. Joe Burke, who was then a senior executive, used to tell about getting a call from Tordella saying, "Bring your car around in ten minutes." Not knowing what the purpose was, Burke brought his car around to the front of the building, Tordella got in, and directed him to Friendship. And the distance on the odometer was just over 10 miles. But there was that attention to detail. He approved every major project.

He was restless about the development of a more bureaucratic system that seemed to be under-

DOCID: 4036134

mining that personal control that had been possible when the agency was younger and smaller.

Toward the end, the growth of bureaucracy, the increased congressional oversight, and other things must have been significant changes for him

The simple growth of the agency was a factor. We had become a several billion dollar a year corporation, with thousands of people operating a global system. And that may have been part of the feeling, referred to by Arthur Levenson, that Tordella may have felt that he stayed a little too long.

If you go back to that period of consolidation we spoke about earlier, that consolidation was successful. But it's important to note that it could have failed. It was not inevitable.

There was nothing inevitable about it at all. In fact, as someone said earlier, we were on probation in those early years. We were constantly being examined and reexamined. We owed our success in part to Eisenhower, who remembered how important COMINT had been to him during the war, and wasn't going to jeopardize that.

And internally, you look at people like Gen. Canine, Adm. Wenger, and Dr. Tordella as keys to that success, with Dr. Tordella providing much of the continuity.

What Tordella contributed, among other things, was his ability to negotiate between various factions. If he proposed a compromise, people were willing to listen. His personal prestige carried enormous times at a delicate point in our history. The centrifugal forces in the process, a natural restlessness on the part of the services to accept NSA authority, a tendency to wonder whether intelligence they didn't control would be there when they needed it, was an understandable concern. So we always had to prove the case that we would be there. And re-prove it. There's a changing audience out there that constantly has to be reeducated, and Dr. Tordella provided enormous continuity over a long period of time.

You were interviewing him late in his life, when he knew he was very ill. What sort of assessment had he made of his career?

I think he was enormously proud of his role. That came through in the interviews, as did his natural role as a teacher. He left a legacy of technical excellence that he was proud of, and that will endure as long as the agency endures. He was the first NSA employee to attend the National War College, and he pushed programs like that. He pushed people to go into them. It was not Tordella single-handedly promoting this, people like Frank Rowlett and others also contributed, but the emphasis on technical excellence is one of his enduring legacies.

Any last thoughts?

We'll never see another Tordella, for a variety of reasons. We've changed. The world has changed. But the qualities he brought to the agency: integrity, moral authority, and civility, those are always in short supply. And qualities we always need to look for. That too is a part of his legacy.

Not a bad record. Moral authority, integrity, teaching instincts, technical excellence, leadership. All the things we would want to instill into future generations.

Exactly.

DOCID: 4036134

P.L. 86-36

Dr. T. — The Man

By [redacted]

I completed a review of about twenty boxes of former Deputy Directors' correspondence at about the time of Dr. T's death in January 1996. The title "Dr. T" was used almost universally by many mid-level managers. Much of his material will continue to be of high interest to SIGINT and COMSEC (INFOSEC today) historians. Having known him personally, I was always impressed by his technical knowledge, management skills, and writing ability. After reviewing many of his hand-written notes, letters, and memoranda, I am now equally impressed by his humanity. He was extremely logical in his thought processes, a master of the English language, and precise in his instructions, particularly for access to sensitive material. His application of the need-to-know principle was often enforced by obtaining one's agreement not to make copies nor show it to anyone; one's initials usually were mandatory. One could feel the sincerity, and the intensity, as he explained to people in meetings and on the telephone, how things would be. Here are a few of his notes to specific individuals:

- 30 November 1964: "Polly: For your info. Please initial. If you choose to let anyone else see it, please let me know. Please return and we can discuss."

- 8 December 1973: "By Hand. Buff: you should read this. Please return to me by hand."

- 10 July 1973: "This copy retained by me with (the writer's) knowledge."

- December 1973: "**N.B.**: If these papers cannot remain in the D/DIR safe, they should be burned. Under **NO** circumstances should they go to the archives. L. W. Tordella." (Even 22 years later, his wishes were heeded; they did **not** go the archives!)

- 9 July 1974: "Mr. XXXX read in my presence. I stressed no attribution of any ideas set forth herein."

- He once wrote a reply for Lt. Gen. Carter's signature which further typifies his sensitivity to access: "First of all be assured that only Lou and I will know of the contents of your letter until such time as you advise me that the appointment is made public. (Except, of course, the beautiful blonde secretary who typed this and she is the most discreet of the three of us). . . Discreet inquiries lead me to conclude that your choice of a replacement is an excellent one . . . I notice that you have emphasized his tender age—44. It is only pure coincidence, I'm sure, which prompts me also to refer to people in this age bracket as babes in arms and to 54-year-old people as fuzzy-cheeked youths. Us older folk are teen-aged delinquents."

[redacted] retired after 41 years of government service. After a 21-year career with the Naval Security Group, he has worked for five Directors, five Deputy Directors, and ten Chiefs of Staff/Executive Directors.

P.L. 86-36

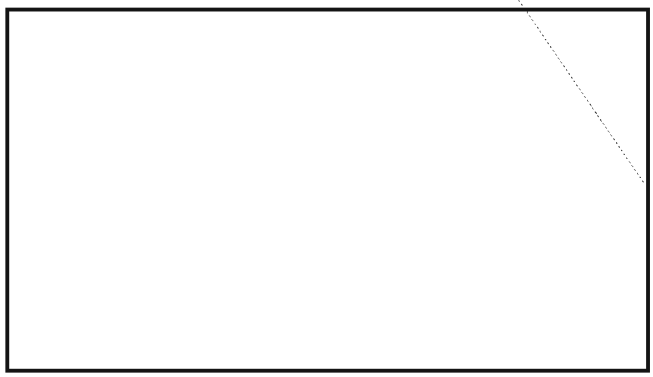
DOCID: 4036134

EO 1.4.(c)
P.L. 86-36

Dr. T. was a champion of the UKUSA agreement and would have surely attended the 50th anniversary of its existence had he lived only a few more months. Also noteworthy was the presence of the current Directors of both GCHQ and CSE at his funeral in Arlington National Cemetery on 23 January 1996.

His letters to the Senior U.S. Liaison Officer, London (SUSLOL) and to GCHQ were extensive; most of them he apparently wrote himself. Among other topics, he, like everyone else, wanted to know how he was perceived by others. In the mid-60's he asked a trusted SUSLOL colleague for an informal assessment which brought a handwritten reply: "Further, in your letter you ask of 'any reflections recently on your performance.' People sometimes tell me you are too busy, i.e. that you do too much yourself. My reply is 'who else?' The only specific thing I have heard from our XXXX friends which is anything but high praise, was their amazement over the XXXX thing. The concern was deep and they had a hard time reconciling the NSA 'position' and their knowledge and opinion of you. They finally attributed it to the fact that you were so busy that you hadn't had time to think it through and XXXX had got you in a weak moment. Otherwise, all and everything I hear from visitors, is fine.

"With respect to how busy you are, Saturdays and all that—you've got to stop it—I don't know how. But you aren't going to be any good to anybody if you get sick. Could you use XXXX more? . . . Have you given any thought to having a couple of junior 'leg men' type assistants? Could XXXX take some of the administrative load off you? Could you maybe keep your door closed more often during the day and not be so available? I really think you must do something." Such cogent advice notwithstanding, no one remembers seeing Dr. T.'s door closed often, nor many horseholders awaiting instructions from the master.



In spite of advice from colleagues to moderate his schedule and rely more on others, no one remembers seeing Dr. T.'s door closed often, nor many horseholders awaiting instructions from the master.

On 27 May 1982, long after he retired, Dr. T. reviewed a 1963 report. He penned a note on the cover which said, "I spent almost 8 days full time on various aspects of this study of NSA and NSA-GCHQ relationships." He no doubt provided his usual sage advice to interested NSA parties.

In a 2 March 1968 letter to SUSLOL: "Another problem which is causing me undue waste of time and energy is the usual agitation and nonsense about reorganization which occurs in every Director's third year of office. Because I don't feel inclined to discuss it in detail without a liberal use of four-letter words, I'll say nothing further about it." And he didn't! But his good sense of humor came through in the final paragraph: ". . . By the time all the miscellaneous nonsense is taken care of, the remaining two to five percent of my time is being devoted to coping with some of the pressing daily problems in the Agency, including, the budget, and one or two other

DOCID: 4036134

minor inconsequential aspects."

Both his ire and humor were evident in a privacy message dealing with an outlandish article in the magazine *Ramparts*. It dealt with US/UK collaboration [redacted]. If you have read the *Ramparts* article, you will note that most of the claims made by [the author] FELLWOCK (and I can hardly resist the temptation to transpose a couple of letters in his name) are fictional . . . The statement that the NSA HQS has no windows is belied by the picture of the HQS building published in *Ramparts* which shows either windows or painted-on black rectangles." For this particular message, he did not even let the communications center keep a copy; the original message form was dutifully returned to him with the date/time group handwritten on it.

His ability to explain NSA's mission and functions was much in demand, both at home and abroad. An August 1973 letter from the President's Foreign Intelligence Advisory Board acknowledged his briefing skills: ". . . you might be interested in learning that there was a uniform sense of admiration for the clarity with which you articulated a series of complex, technical matters, and respect for the ease with which you covered the full spectrum of NSA responsibilities."

EO 1.4.(c)
P.L. 86-36

Dr. T.'s edicts were not encumbered by formal "decision memoranda." He often wandered into your office, exchanged pleasantries, and told you what he wanted done. [redacted] After successful testing, and amid plans for an operational capability, the ever-practical, logical, and sensible Dr. T. feared aircraft collisions [redacted] The coup de grace was delivered personally to the senior manager quietly, efficiently, and irrevocably.

Some may have chafed under the inflexibility of his guidelines, strict accountability, and attention to detail; however, his strong leadership ability was widely respected and obviously served the Agency well in its formative years. There is little doubt that to many, he was, in fact, "Mr. NSA" during his tenure as Deputy Director from 1958 through 1974.

DOCID: 4036134

DOCID: 4036134

"If Lou Tordella Says It's OK, That's Good Enough For Me"

by Gene Becker

The young Navy lieutenant was handed a highly classified message with instructions to decrypt it personally. It was 1943 and the lieutenant was Dr. Louis Tordella, acting OIC of operations at the Bainbridge Island Naval Station, receiving an "eyes only" instruction from Naval Headquarters to set up a compartmented intercept project directed against Soviet naval communications. He quickly assembled a select team of about 15 operators, all of whom had been "on-the-roof-gang"[1] Morse operators and many of whom went on to have highly successful careers in the Navy (six retired as captains, including Chris Currie and Hal Jocelyn). This was the first U.S. Navy collection effort against a Soviet military target, and was Dr. Tordella's first operational cryptologic assignment.

Dr. Tordella's association with the Soviet problem continued after he left Bainbridge Island in 1944. He received orders to go on assignment to China after a stop at headquarters in Washington. On arriving in Washington he learned that his orders had been changed and that he was to report to Bell Laboratories in New York for special training on a new system of equipment that was designed to decipher Japanese voice codes. Before the system could be deployed to the Pacific, however, the military situation there had changed and it was redirected to a newly established U.S. Navy experimental intercept site at Skaggs Island with Lt. Tordella in charge. In addition to personally heading the operation, he designed a crude multiplexer, the first of its kind (then Lt. (j.g.) Art Houseman, who went on to become CEO of Ampex, designed a greatly improved multiplexer); this system, despite being cobbled together, proved to be very successful.

The training assignment at Bell Labs was to have an important influence on Dr. Tordella. It was a valuable lesson in how research and development could quickly provide concrete solutions to operational problems in the field. It was also a lesson in the value of training and hands-on experience in the successful deployment of new and untried systems. Furthermore, it was a practical demonstration of the importance of collaboration and cooperation with the private sector.

The early years of Dr. Tordella's long career in cryptology were one of many subjects that he talked about in a series of interviews conducted as part of the Center for Cryptologic History's Oral History program in the year preceding his death. What follows are some impressions of Dr. Tordella and a few highlights of these interviews (a full account will be published in the future).

In 1960, the defection to the Soviet Union of two junior NSA cryptanalysts named Martin and Mitchell made front-page news across the nation and hit the Agency with devastating impact. Although the Agency had had several spy cases in the past, specifically those of

1. This term was applied to the Navy's Morse intercept operators, who literally were trained in huts on the roof of the Navy Headquarters building.

Mr. Becker is a longtime NSA employee. This article is derived from a series of oral history interviews conducted with Dr. Tordella by the author.

Petersen and Dunlap, none was of the magnitude of the defection to Moscow of Martin and Mitchell. Several investigations were launched into the affair, the most significant of which was that of the House Un-American Activities Committee. There were several immediate consequences of the various investigations: the Chief of NSA security was fired and a number of subordinate officials were transferred; the Chief of Personnel was also fired; and the security clearance procedures were changed to require full background investigations before access to classified material was granted.

The affair continued to reverberate throughout the Agency and rumors of additional firings and adverse actions persisted. Dr. Tordella, by now Deputy Director of the Agency with a well-established reputation for honesty and integrity and with an aura of moral authority, convened an open meeting of employees in the Friedman Auditorium. In a brief address he told a standing-room audience that the Agency had been hurt by the Martin and Mitchell affair, that actions had been taken to improve security and personnel procedures, but that there would be no witch hunt, no draconian measures and that the essential work of the Agency would continue and would prosper. His words of assurance had an immediate calming effect and life at NSA soon resumed its normal pattern.

His words of assurance to the workforce after the defection of Martin and Mitchell had an immediate calming effect.

Dr. Tordella described relations with Congress during most of his career as Deputy Director as being confined to dealing with a few key committee chairmen and senior members in both Houses. He often appeared personally before the committees, either accompanying the various directors he served or by himself. Such was his reputation for probity on the Hill that Senator Saltonstall, the senior senator from Massachusetts and member of the Senate Armed Services Committee, was quoted as saying, "If Lou Tordella says it's OK, that's good enough for me."

Dr. Tordella recalled one occasion when Mendel Rivers, Chairman of the House Armed Services Committee, asked to see him very early one morning to explain why there was need for another Liberty ship for the Navy to use as an intercept platform. Before meeting with the chairman, Dr. Tordella asked about the existing Liberty ship and was told that the Navy had ordered it to take up a position off the coast [redacted] because of a serious internal crisis there. P.L. 86-36 During his meeting, Chairman Rivers asked him where the existing ship was located, and Dr. Tordella responded that it was on location off the coast [redacted] because of the current crisis. "Good," said Rivers. "That's where it ought to be," and approved the request for a second ship.

As Deputy Director, he took a special interest in and played a direct role in the conduct of the Agency's foreign relations. He had been a leading member of the U.S. team that negotiated the original BRUSA Agreement shortly after World War II and later he played a key role in negotiating the follow-on UKUSA Agreement that governed the relationship between NSA and GCHQ. Dr. Tordella's view, which in effect became the Tordella doctrine, was that the Agency had a partnership with GCHQ and that we shared tasking and operations but could function independently of one another. As he said, "We are each mindful

DOCID: 4036134

of our national interests but can still find common ground."

Dr. Tordella was also directly involved in relations with private industry. Here too the high regard and esteem in which he was held served the Agency's interests well. He developed a close and long-standing relationship with Dr. William O. Baker, former director of Bell Labs. Dr. Baker was an influential member of the scientific community, a member of the President's Foreign Intelligence Advisory Board under several presidents and a great champion of cryptology and the Agency. Dr. Tordella had an understanding with Dr. Baker and others in the private sector that if NSA needed help in technical and scientific endeavors they would respond as a matter of the highest priority. NSA was brought in on planning by IBM, Sperry Rand, RCA, and Burroughs, among others, and was able to influence significantly the design of systems and equipment and indeed the pace and direction of research and development, particularly in the fields of telecommunications and computers.

As is evident, Dr. Tordella was involved in every important aspect of the Agency's mission and functions. One aspect that he dealt with that resonates even today was the NSA role in the production of intelligence. The issue began with the establishment of the Agency and the attempt to rein in its cryptologic mission by those opposed to the centralization that NSA represented. The subject was highly contentious and charged with emotion, and issue was joined over NSA's issuing several summary reports during one of several crises in the 1960s when the flow of intelligence had overwhelmed the system.

Dr. Tordella, although forewarned that the summary reports would stir up a controversy in the community, approved their release. Gen. Carroll, then director of DIA, immediately protested this overstepping of bounds by NSA. The issue was taken up at a USIB meeting at which Dr. Tordella represented the Agency. After Gen. Carroll explained his position, the chairman asked him whether he found the reports useful. He replied with a yes. The chairman then asked him whether DIA could have issued the same reports. He replied with a no. The Chairman then asked each member the same questions, received the same replies, turned to Dr. Tordella and said that NSA should continue to publish such reports.

Dr. Tordella was the first Agency civilian to attend the National War College, and thereafter the Agency began to send people to the senior service schools routinely. He was a great believer in the value of training and education, and we mentioned earlier how his own experience at Bell Labs made a lasting impression on him. He also promoted maintaining the highest possible standards of technical and professional excellence and ardently supported the professional career structure that became a hallmark of NSA's career development program.

Dr. Tordella's long and distinguished career chronicles the Agency's passage from its tentative beginning after WWII to its position today as a pillar of national security.

DOCID: 4019611

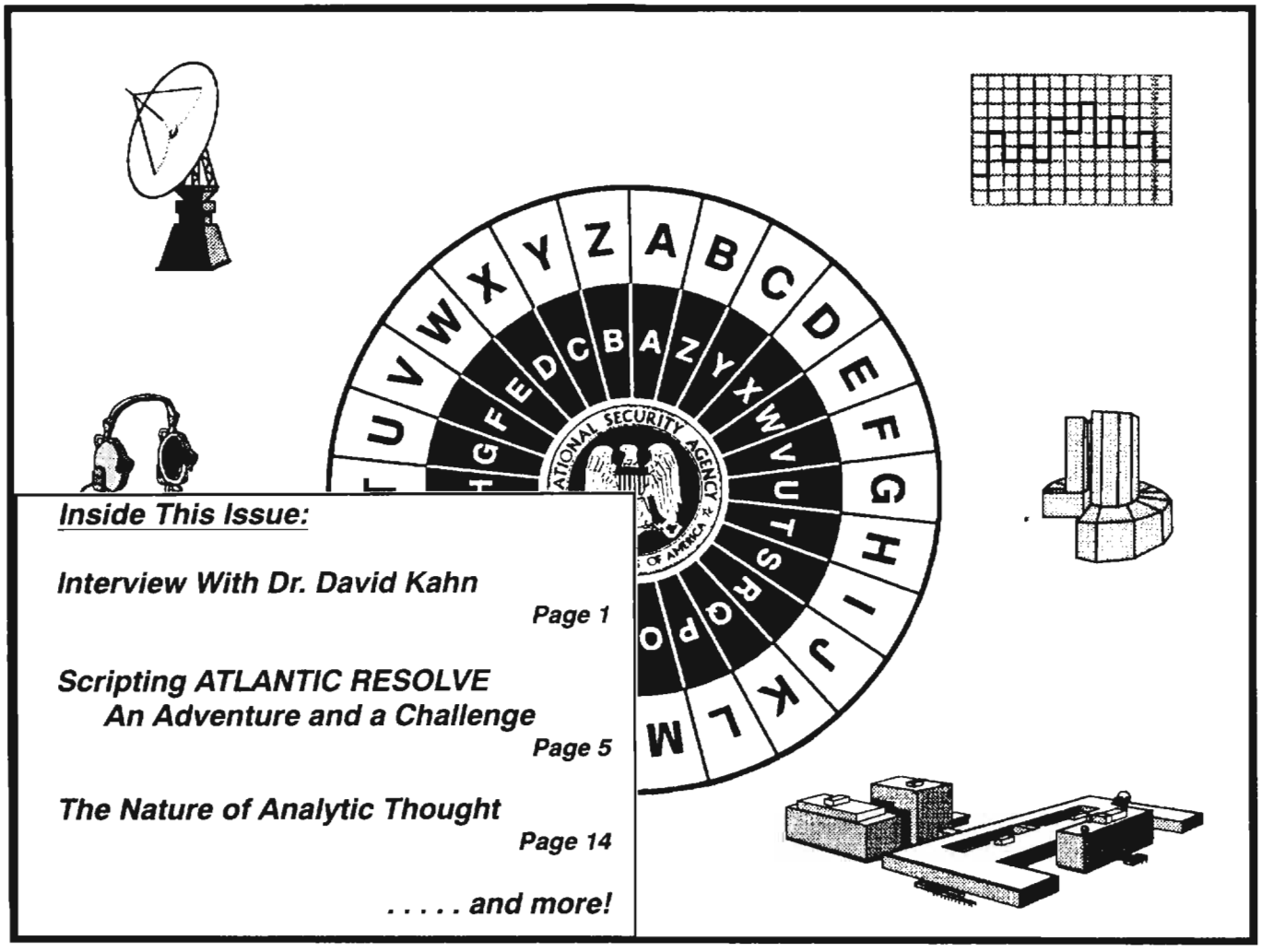
~~TOP SECRET~~

NATIONAL SECURITY AGENCY

CRYPTOLOG

The Journal of Technical Health

Vol. XXI, No. 4 WINTER 1995



~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating~~
~~Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-10-2012 pursuant to E.O. 13526, MDR Case # 54778

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

DOCID: 4019611

CRYPTOLOG

Winter 1995
Vol. XXI, No. 4

Published by P05, Operations Directorate Intelligence Staff

Publisher ..... William Nolte (963-3123)

Editor ..... [redacted] (963-3123)
Graphics ..... [redacted] (963-3123)

Board of Advisors

Chairman ..... [redacted] (963-7712)
Computer Systems ..... [redacted] (961-1051)
Cryptanalysis ..... [redacted] (963-7243)
Intelligence Analysis ..... [redacted] (968-8211)
Language ..... [redacted] (963-7667)
Mathematics ..... [redacted] (963-1363)
Signals Collection ..... [redacted] (963-5717)
Telecommunications ..... [redacted] (996-7847)
Member at Large ..... [redacted] (968-4010)
Member at Large ..... [redacted] (968-4010)
Member at Large ..... [redacted] (961-8214)
Classification Officer ..... [redacted] (963-5463)

P.L. 86-36

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

To submit articles and letters, please see last page

DOCID: 4019611

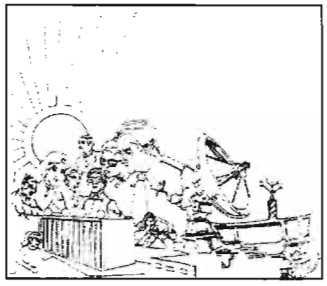


Table of Contents

Interview With Dr. David Kahn (U), by [redacted] *1*

Scripting ATLANTIC RESOLVE ~~(FOUO),~~ by [redacted] *5*

Hitting the [redacted] *~~(FOUO),~~* by [redacted] *11*

The Nature and Process of Analytic Thought (U), by Hugo Keesing *14*

Three V's for SIGINT (U), by [redacted] *17*

American Translators Association Conference (U) *20*

How I Helped Trigger a Greater Involvement in Vietnam (U), by [redacted] *26*

Book Review (U):
High Seas, reprinted from Air War College Newsletter *30*

Letters to the Editor (U) *32*

SIGINT Bloopers (U) *35*

P.L. 86-36

DOCID: 4019611

Dr. Louis W. Tordella
1911-1996
Deputy Director, National Security Agency
1958-1974

As this issue of *CRYPTOLOG* was going to press, we learned of the death of Dr. Louis W. Tordella. In duration alone, his tenure as Deputy Director of the National Security Agency stands as a remarkable event in the history of American cryptology. But even that understates his role in forging this agency and the cryptologic establishment it centers.

Simply stated, Louis Tordella ranks as one of the leading figures in the creation of the post-World War II American intelligence establishment. In its next issue, *CRYPTOLOG* will present a more detailed appreciation of the career of this great and distinguished man.

W.N.

DOCID: 4019611
P.L. 86-36

Perspective:

Interview with Dr. David Kahn,
1995 Resident Scholar at the Center for Cryptologic History (U)

by [redacted]

(U) Dr. David Kahn is a scholar, journalist, and author of a number of important books and articles on cryptology, including *The Codebreakers* and *Seizing the Enigma*.

(U) What led to your interest in cryptology in the first place?

(U) I read a book when I was a kid, and I never grew up. The book was by a civil war naval historian named Fletcher Pratt, a book with a terrific title: *Secret and Urgent*. I saw it in a window of the Great Neck library, and was attracted by the terrific dust-jacket, letters and numbers coming out of the cosmos. I read it, and the whole subject of codes and ciphers just hooked me. Of course I was at that age, 12 or 13, when I think a lot of people get hooked on their hobbies or their interests.

(U) What led to the decision to write *The Codebreakers*?

(U) Codes and ciphers and cryptology had been a hobby of mine for many years. In 1960, in an episode NSA probably doesn't like to remember, two members of the agency, Martin and Mitchell, defected to the Soviet Union. It was a front-page story in the New York Times, and I thought that this might be a good opportunity to write a piece for the Times on the background of that event, telling all about codes and ciphers and the role they'd played in history. I wrote it for the Times magazine, and the next morning I got calls from three publishers asking me to write a book on codes and ciphers with a little introductory historical chapter.

(U) I began researching the history of codes and ciphers, and there was a lot of material in scholarly journals and in other places which I found just by following footnotes through journals that were listed in the standard bibliography. Suddenly I noticed that I was in the year 1600 and on page 250 of this first chapter! Well, something had to change. So I turned it around and made it a chronological piece, and so much hadn't ever been told that the book just kept growing and growing.

(U) What was NSA's reaction to the book?

(U) Oh, NSA hated the book! NSA hated the fact that I had obtained information about NSA, what it had done and what it was doing, some of the effects it had on negotiations and things like that. NSA sent out warnings that the book was to come out, and nobody was to comment on it. That happened in 1967-68, and if you or anybody else at that time had asked me whether I would ever be sitting here and be allowed to enter NSA unescorted (only in certain areas, because I'm uncleared), and be a member of the NSA team, everybody would have laughed at you.

(U) What does one do as a visiting scholar?

(U) I have been dealing with the declassified papers of Herbert Yardley, a very colorful and important American cryptologist of 1917-1929. He was the man who founded the American cryptologic establishment, an organization called MI-8 (Military Intelligence 8), of the General Staff. After the end of World War I it was transformed into a joint Army/State Department agency, technically called the Cipher Bureau, but commonly known as the American Black Chamber, which is the title of the book that Herbert Yardley wrote after Henry L. Stimson, thinking that gentlemen do not read each other's mail, closed it down.

(U) Yardley's documents are mainly technical and administrative, and having been a reporter, I knew I couldn't just write the story from them, I'd have to go beyond them. So lately I've been going into the private papers of people Yardley worked with, expanding the research into other areas. For example, Yardley wrote about a missionary cryptographer who knew Japanese and was brought in when the U.S. was breaking Japanese codes before the Washington Disarmament Conference in 1921-22. This man turned out to be an Episcopalian minister and missionary, so I wrote to the archives of the Episcopal Church in Austin, Texas, and got a couple of articles about this man that I will be able to use when I write the story of the American Black Chamber. So that's the kind of stuff I have been doing.

~~FOR OFFICIAL USE ONLY~~

And writing away at high speed, I might add.

(U) As we complete the 50th anniversary commemorations of the end of the Second World War, do you find that the role of intelligence in conflict is clearly established?

(U) Well, certainly in World War II it was pretty clearly established. It was begun to be established in World War I, when radio first came in. Radio is key to the importance of cryptanalysis because radio turns over a copy of any message to the enemy. There were a number of important cases in World War I. One case of communications intelligence, which was an administrative and not a cryptanalytic failure, was when the Russians failed to distribute cipher systems to their lower echelons very early in the war. As a consequence the Germans were able to win the battle of Tannenberg, the battle that started Russia on its long slide into ruin and revolution. There were many tactical cases of communications intelligence in WWI, and of course the Zimmerman telegram, which brought the United States into WWI and therefore onto the world stage.

(U) Then in WWII, we had all those incredible stories that everybody knows about: the winning of the Battle of the Atlantic through solution of the German Enigma machine; many battles on the Western Front, again, won by the Allies in part because they knew German plans and so forth; and in the Pacific, of course, we were breaking Japanese codes; we won the Battle of Midway, we shot down Adm. Yamamoto; and we sank the Japanese merchant fleet, which virtually strangled Japan. So yes, there's no doubt any more that communications intelligence plays a role. There's a very telling proof of this: the U.S. Army, at least, has now established communications intelligence units within each division, and they're not doing that for fun, they're doing it because the results are there.

(U) You mentioned administrative versus cryptanalytic failures; do you find that one more than another has led to breakthroughs during conflict?

I would say it depends how you define administrative failures. I'm thinking particularly of the Enigma messages. A lot of those messages were solved because we were able to guess the plaintext of stereotyped enemy messages: "Nothing To Report" and stuff like that. Is that an administrative or a cryptographic failure?

(U) We now have VENONA; do you think we're going to see declassified intelligence play a similar role in the history of the Cold War?

(U) That's a terrific question, and my answer is I hope so, and I think so. I don't know how good we were in solving Russian code, and I don't think the Russians, from what I've heard, were very good at solving ours. Nevertheless, you can read third-party codes pretty well, and from this gain information about negotiating positions in SALT and START treaties, earlier economic treaties, and things like this.

(U) We have had, for example, the revelation at the History Symposium, that because we were able to read the messages of our allies, particularly the French, and many Latin American countries, we were able to structure the United Nations pretty much the way we wanted, and I'm sure there are many other cases like that. There was a story in the New York Times just two weeks ago by Tim Weiner on the front page in which he revealed that we were listening in to Japanese telephone conversations and using this information to win economic battles.

(U) As the national security apparatus gets restructured, how much does the public have a right to know about that apparatus?

(U) It has to be done on a case-by-case basis. In some situations it's possible to give a certain amount of information out but in other cases—I knew this intellectually before; now I have more of an emotional grasp of it—that if you start giving too much material away about how codes are solved and so on, you're going to cut yourself off from your sources of information, and this is more harmful to the country than giving the information out is beneficial to it.

(U) Do you think we're where we need to be on openness in intelligence?

(U) Yes, I think things are coming along better because of openness, and I'd love to think that it was because NSA and CIA and DIA and all those other guys suddenly saw the light, but that's not the case. They're becoming more open because of the fight for budget dollars. That's pretty clear.

(U) As the history of intelligence becomes more and more accepted as an academic pursuit, what do you see as the principal lines of inquiry in the future?

(U) I can't say I see any particular individual line, I think it's just a general advance on an overall front. Many sciences or histories go through several periods, one of which is just the gathering of information, and I think we are still in this stage. There haven't been many

DOCID: 4019611

theories of intelligence. I proposed one a while ago, which people seem to think is all right but hasn't gained wide acceptance yet.

(U) It's divided into three areas: past, present and future. The past is that intelligence became important with the rise of what I call verbal intelligence. Animals can see danger and prey, right? What they can't do is what people can do, namely gain information from words. We can overhear a conversation, and we know that someone is planning something good or bad for us. So it's the rise of communications intelligence that has primarily driven the rise of intelligence. If you are just looking at objects on the ground, say tanks, you can guess that an attack is coming at that point, right? But if you are reading a message saying, "We're going to attack," you don't have to think about it or guess at it, you are told. So this gives a much more forward-looking approach than just physical intelligence, looking at objects. This makes NSA look good. That's not why I developed it, but it turns out that way: that communications intelligence is the real driver of modern intelligence.

(U) As for the present, one element is that intelligence is much more important in defense than in offense. When I was writing *Hitler's Spies*, I was looking for little anecdotes, case histories, in which intelligence won a battle or something like that. And I noticed that I was finding a lot more defensive cases than offensive cases. I wondered why this was so, so I looked up the definitions of attack and defense in Clausewitz, and I found a clue there: in defending, he says, "The position or characteristic attitude of defense is to parry a blow." Well, you cannot parry a blow unless you know it's coming, which implies intelligence, right?

(U) So intelligence is essential to the defense, whereas offense, Clausewitz says, is in and of itself. You don't need intelligence in the offense. If you're an attacking army, you just march in, and you don't really need to know where the victims are if you're strong enough. Of course this is a black-and-white explanation that oversimplifies it, but I like to get it down to the basic level to clarify it, and then I can add on qualifications.

(U) Another of the common elements of today is the ultimate purpose of intelligence, which is simply to optimize resources. I'd never really heard it put that way before until one day when I was at St. Anthony's College at Oxford. I walked in and a guy named Patrick O'Brien, an economic historian, was standing there with a glass of white wine in his hand. He asked me how the book was coming, and said, "Listen, isn't all intelligence just optimizing your resources?" It was like he hit me in the face; it was so clear and so down to the basics, that I've adopted it and given him credit.

(U) So what about the future? There are two problems with the future: everybody wants to know everything, and this is the goal we strive for but I don't think we'll ever get to that point. The other problem in the future is (or a perennial problem) that we have to get our bosses, I mean the intelligence consumers, to accept our intelligence.

(U) To accept the need for intelligence, or to accept what we give them?

(U) To accept what intelligence producers say. This will work in some cases. What I think is the situation is this: If someone's beliefs are very strongly held, there's not really anything that's ever going to change those beliefs; no intelligence is going to do that. If, on the other hand, the beliefs are not central to his personality but only deal with the tactics of, say, how we deal with the car situation with Japan or something like that, then you have a chance of persuading him that the intelligence is useful. Take Hitler, for example. There were often occasions where tactics were involved, and he often listened to his intelligence, but if you were going to tell him that the United States wasn't run by Jews, forget it! So how are you going to get around this? Well, I don't see any way to do it right away. You can't put every world leader on the couch, which is what would be required. But it's also possible that as people become more rational—and I think the world IS becoming more rational in its beliefs, for instance, people go to psychotherapists because they realize that things can be done better by reason than by emotion.

(U) Did you follow the Gates hearings, when accusations were made of tailoring intelligence to meet expectations from higher up?

(U) Well, obviously you shouldn't do that. But listen, we know what life is like. You're not likely to say unpleasant things to your boss because he decides whether or not you get promoted. That's why you need strong characters in intelligence, to offer unpalatable truths.

(U) Do you find that with people in your line of work, is there a tendency to start out with a theory or does that depend on whether they're journalists or academics?

(U) I don't know. I can tell you that I started out with a theory when I was writing *Hitler's Spies*, that the Germans had good intelligence. Well, I was totally wrong. And I was very unhappy about that because it meant that instead of maybe getting a best-seller because I was telling the story of a winner in a certain area, I was telling the story of a loser. Who wants to read that? But those were the facts. And by that time I was well into the book. I wasn't going to tailor it. I couldn't do that and call myself a journalist or a historian. I would say that most academics, unless again you're dealing with very deep-seated beliefs, would say they were wrong and revise.

(U) Where do you see your future focus: still more cryptologic history going further back, or new developments in cryptography?

(U) There's an awful lot of new material coming out. For example, 25 or 30 years ago I wrote the *Encyclopedia Americana* article on cryptology. Now I'm revising it. I thought I'd just have to add a few more paragraphs here and there and take a few of the old ones out. Well, the changes in codes and ciphers and cryptology in general, communications security and intelligence, are so far-reaching that I have to rewrite the whole thing. So there's plenty to do there. One of my regrets is that during the time of the data-encryption standard dispute and more recently key escrow and all of those things, that I didn't succeed in selling a story to one of the major magazines, which I would like to have done.

(U) This is probably because in some cases the magazines had their own people working on this, so they didn't want Dave Kahn from the outside to do it. Not that they had experts on codes and ciphers, but they had computer experts and this was kind of a computer story. Another reason is that one of the problems with communications intelligence in general and security, and the reason that NSA doesn't have a much higher profile, is that at the heart of the whole thing, what do you have? A computer chip. What do you see if you see a codebreaker? Someone writing on a piece of paper or sitting at a computer keyboard. What do you see if you see a spy? You see a guy shooting someone, a guy skulking around in the shadows. That's why there are movies like *Die Hard*. You're never going to see a movie called *Think Hard*.

(U) Do you have an Internet account yourself?

(U) No, and I'll tell you why. Because—this is a word Dave Hatch gave me—it's "chronophagous." I was talking to Peter Gross (who wrote a book called *Gentleman Spy*) just the other day; he had called me for some help. I asked whether the Internet used up an awful lot of his time, and he said it did. Maybe that's just temporary and eventually you can go in and get whatever you want, but I don't really care so much about computers. I want to get on with writing Also, people have said to me that if you get on the 'Net, Dave, and they find out that you're there, you'll be inundated with people saying did Enigma win WWII and why didn't we know about Pearl Harbor. I write so that I can deal with a lot of people at once instead of with individuals.

(U) Whit Diffie, one of the researchers whose work was fundamental to the development of the RSA encryption scheme, called your book *The Codebreakers* inspirational. Have you followed much of the public key cryptography debate?

(U) Not closely, but several people have said to me that they have gotten into cryptology because they were hooked by the elegance of the RSA scheme (which relies on research by Diffie and Marty Hellman), which makes sense to me.

(U) Do you think you'll be able to keep up with developments in cryptography?

(U) It's a terrible job. When I was a kid starting out with this stuff, I practically memorized every book on codes and ciphers that came out, and every article. Now it's impossible to keep up with the flood of articles and even books! First of all, the books are tremendously expensive, and they are coming out—well, not as many as the journal articles, of course, but there's a dozen or so a year, maybe more, books on codes. What I do now is try to limit it to good books on the history of intelligence and/or codes, current books on the Ames case, and so on.

~~(FOUO)~~ I've given a lot of talks since I've been here, with Dave Hatch's blessing, representing the Center for Cryptologic History and letting people know about history, in various elements of the agency. I know people have an intellectual awareness that it exists, but once they meet a person and know the face, that helps spread the word about cryptologic history.

KA

DOCID: 4019611
P.L. 86-36

Scripting ATLANTIC RESOLVE: An Adventure and a Challenge (FOUO)

by [redacted]

~~(FOUO)~~ *TDY Chance To Excel!* Now if *that* isn't an eye-catching subject line for an e-mail I don't know what is. I kept on reading and discovered that this particular opportunity included travel, which is one of my all-time favorite things to do. Specifically, a request was being made for my office to provide one body to participate in Exercise ATLANTIC RESOLVE as a SIGINT scripter. What exactly that meant I did not know at the time, but it sounded intriguing. As I am not known to be afraid of trying new things, I put my name forward and hoped to hear good news, although I wasn't sure whether or not my being a civilian would make my chances for selection greater or less.

~~(FOUO)~~ In a matter of days I was told that I'd been selected and would soon head out to Grafenwoehr, Germany, where the exercise was to be conducted, accompanied by two representatives from G563 (NSA's Exercise Shop). While I knew next to nothing about what being involved in such an exercise would entail, I have to say I was excited about the new opportunity and the challenge of it all. As friends and co-workers got wind of my impending departure for "Graf," there was no lack of comments and advice given. "What, are you crazy? Do you know what you're in for? Graf is freezing and covered with snow this time of year. And then when the snow melts, it's one big mudslide." "You'll be sleeping outside in tents for 15 days with no heat and nowhere to shower." "I hope you like MRE's because that's all you'll get to eat." The shorter the time got until my departure, the more freely flowed the comments. I don't know if people were trying to scare me or intimidate me into politely backing out of participating, but to tell the truth, these comments did nothing but make me want to go all the more, if for no other reason than to see what it was *really* like.

(U) Although time was running short, I quickly began to do some homework. What were the objectives of this exercise? Who would be involved? And probably most important to me, what would be my role in all of this? I needed to know.

~~(FOUO)~~ I discovered that this exercise was to be the very first ATLANTIC RESOLVE exercise. It came about as a replacement for the decades-old REFORGER exercises held in Germany annually. USAREUR (U.S. Army Europe, a component of the U.S. European Command (USEUCOM)) was to be the sponsoring Command. The Intelligence Objectives for ATLANTIC RESOLVE 94 were essentially three:

Unclassified

- To exercise and validate the USAREUR intelligence architecture;

- To exercise intelligence collection, analysis, and reporting across the operational spectrum; and

- To exercise Joint/Combined Task Force (JTF/CTF) intelligence operations.[1] Personnel from five nations (U.S., UK, Germany, France, and the Netherlands) and representing all branches of the military

1. (U) "Joint" in this context means more than one military service is involved; "combined" means more than one nation.

would participate. A JTF J2 (Intelligence Directorate) was to be established and supported throughout, and support from a Joint Analysis Center (JAC) in England would be exercised as well.

~~(FOUO)~~ As for my role, I would be part of a three-person team (the other two being the G563 folks) that would work in the Intelligence Control Cell (ICC), the single point of contact for intelligence exercise control. Units manning the ICC were to be primarily exercise facilitators. Through a combination of simulated and scripted intelligence, the ICC would translate the exercise director's guidance into a fully supportive intelligence environment. Along these lines, some ICC personnel would input taskings and directions into one of the many computer systems being used in the exercise—the magical simulators of war. Others (which included our team of three together with a team of four at the JAC in England) would script material to cover the kinds of intelligence-related activity that could not be adequately performed in simulation. (While the team of four in England was co-located with the JAC, they were a separate and distinct entity; the exercise foursome provided a service, while the JAC played the role of customer.) Still other ICC personnel would serve as liaisons to intelligence players in the training audience primarily at the USEUCOM and component level.

(U) With most of my questions answered as fully as they could be in advance, I packed my bags and on 24 October, departed for Grafenwoehr with my two new partners from G563 fresh off the plane from the States. The drive from Stuttgart took several hours but we made it there eventually, despite the normal hindrances to driving in Germany: construction delays and other "staus" (traffic back-ups) that never seem to have any identifiable cause.

(U) Once we reached our destination of Grafenwoehr training grounds, we had several objectives before we could do anything else. First and foremost we needed to try to secure some form of accommodations for ourselves. We'd been assured that there were absolutely, positively NO commercial accommodations available in any of the towns within an hour's drive of the training grounds, as all of those spaces had been booked solid for months. We were aware of the tent option, but we thought that would be less desirable than just about anything else we might be able to come up with. So we set out on what was essentially a scavenger hunt to try to track down a corner of a warm building here or a free slab of cement there.

(U) As it turns out we were fortunate beyond belief. Once we located the building which housed the SCIF which was to be our place of work for the next 2 weeks, we began questioning everyone we could about alternatives to the tents. Unbelievably, one of the women in the SCIF told me that there just so happened to be one spot available in an adjoining room to the work space. Terrific! It was an actual roof-covered, fully enclosed, *heated* room! Of course it did happen to be a tank-repair bay, so it was essential that the occupants be careful not to fall into the open pit that ran the full length of the room down the center of the floor. But that aside, it was more than I could have hoped for, based on what I'd been expecting as a result of all the unsolicited forewarning I'd received.

(U) Sharing the room with eight other women was not a problem either; the tent in which I was expecting to have to live turned out to have 30+ women. Another great aspect (it's all relative) was the fact that I had a cot on which to sleep. The three of us had brought lovely pea-green Army sleeping bags with us, but now I actually had something upon which to place the bag other than the frozen ground.

(U) My two male companions were not as fortunate as I when it came to "housing," although they too were not out in the tents. The best we were able to find for them were some unoccupied coil springs on two bunks in a barracks-type room housing 50 men. And when I say coil springs, that's exactly what they were—no mattress, not even a pad covering the springs. So the next step in our scavenger hunt was to secure some kind of flat protective material to place on top of the coils. As it turns out, the giant silver dumpsters at the end of the street provided the perfect fix: large, empty cardboard boxes which, when flattened and stacked on top of each other, would serve the purpose for 15 days.

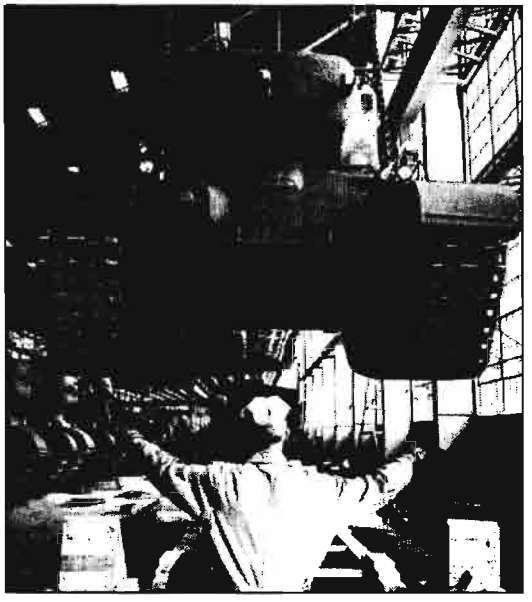
(U) Finally, we began our search for one particular master sergeant who supposedly had been able to secure three hooded, fur-trimmed parkas for us. (*Parkas?* I guess they weren't kidding when they said it would be cold here.) Again through some unbelievably fortunate chain of events, we were eventually directed to the right room in the right building on the right street in the right section of the training grounds to our three parkas. It seemed that, despite our exhaustion and hunger, everything was as it should be.

(U) Our first taste of what this exercise was going to be about began that very same night. We found our way to the building that we were told was the home of

DOCID: 4019611

the ICC—fortunately only a short walk away from the multi-purpose SCIF/women's housing/tank-repair-bay building. We stood there in a kind of zombie-like state as the ICC's day shift personnel gave their pass-down brief to the night shift. As it turns out, personnel had been there a full week prior to the arrival of the three of us. These folks had been setting up from scratch and getting all aspects (computer, security, admin, logistics, you name it) ready for STARTEX, the actual start of the exercise. So in a sense I felt behind the eight ball right from the start, watching and listening to these people talk about all kinds of systems and details of which I knew nothing. It was a language all its own, with new acronyms and names of people and facilities that might have been on another planet.

~~(FOUO)~~ Speaking of another planet, the scenario for the exercise involved just that. Well, actually, it wasn't another planet, but another island, a fictional one called "Atlantis." According to the scenario, the island was divided into the two "nations" of North Titania and South Titania. The North Titanian forces were identified as "red"—the hostile, opposing force (OPFOR). The South Titanians were identified as "blue"—the good guys. According to the exercise concept of operations, the North Titanian forces were designed to portray a threat that required an out-of-area joint and combined deployment to fight a low-to-mid-intensity conflict of short duration. In other words, the bad guys were trying to invade and seize the territory of the innocent good guys and bump off all their forces.



(U) Welcome to the women's dorm

Upon our arrival, it was clear that, despite the fact that the exercise had not yet begun, people were working long hard hours on *something*. As it turned out, what I had thought was going to be one exercise was really composed of three separate exercises:

• the deployment exercise (19-27 October). During this part, all preparations were made and details were finalized regarding how the exercise should flow;

• SHADOW CANYON MINI-EX (28-29 October). This was to involve the same participants in the same roles as in the main exercise; its purpose was to work through as many of the logistical bugs as possible in advance of "the real thing," and

• the warfighting CAX (computer-assisted exercise) (1-8 November). This was ***the*** main exercise and was supposed to run with the fewest glitches of the three.

~~(FOUO)~~ With all this as background, we discovered that the role of the three of us in Graf would be that of information gatherers. We would have to attempt to gain access to as much information as possible with regard to the OPFOR: what they were doing, what they intended to do in the future and when, how they interpreted the actions of the blue forces, etc. Then we would pass the information we had obtained to the exercise team of four at the JAC. This would be done primarily by fax or phone, or so we thought at the beginning. In actuality we ended up securing a computer through which we could e-mail the information to our counterparts, which was infinitely more efficient than the fax or phone could ever have been.

~~(FOUO)~~ As for the foursome in England, their job would begin at this point. First step for them: THINK! They were to try to imagine what type of report the USSS would produce on the activity (serialized product report, klieglight, or TACREP) if this event were really happening. What would that report look like? What information could an analyst at NSA reasonably expect to see? And how would it then be reported? The key to a good end-product was to incorporate all that could realistically be expected to be uncovered by SIGINT in such a war scenario (given collection capabilities, knowledge of a given nation's C^3 network, etc.).

~~(FOUO)~~ The products that the exercise foursome at the JAC produced from the information we had gathered was disseminated to exercise players throughout

the theater, including the JTF HQ, the land component HQ, the air component HQ, and many others (all at Graf), as well as the JAC in England and the UCIRF (USAREUR Combat Information Readiness Facility) in Augsburg, Germany. The people at the JAC would then extract items from the products and incorporate them into their daily summaries, which would go forward to the high-level decision-makers involved in the exercise. With the various types of reports in hand, the exercise players could then formulate strategies to be implemented by their forces.

~~(FOUO)~~ While distribution of a good volume of exercise SIGINT was our goal, at the same time it was critical that *not too much* information be revealed in the reports. It was the responsibility of all seven of us (Graf team and JAC/exercise team) not to blow the exercise by giving away too much or the wrong kind of information. We were considered part of the "white cell"; we were part of neither the red (opposing) forces nor the blue ("good guy") forces, and as such, it was incumbent upon us to maintain neutrality as much as possible. If too much information or the wrong kind of details were published with regard to the red forces' activities or intentions, the blue forces would immediately have the advantage. In the worst case, this could have such an effect on the decisions made by blue-force players that it could cause the exercise to end much sooner than it should have. So the responsibility to "play fair" and remain unbiased lay heavily upon the seven of us.

(U) While we were aware of the potential for bias on our part, the members of the red forces were even more aware of it. This was immediately evident to us as we began during those first few days to meet people, ask questions, and try to put all the pieces together in our minds as to roles and functions of all players. While I can't speak for my two coworkers, I must say that I personally was regarded with the utmost caution by members of the OPFOR. "Now who are you? And what *exactly* is your role in this?" "I don't have to give you that kind of information if I don't want to." "What exactly do you intend to do with the information I provide to you?" Such questions were only fair, I suppose. The OPFOR wanted to be sure they didn't provide any information whatsoever to anyone who could conceivably be a spy for the blue side. We were always 100% truthful with all who asked what we intended to do with the information they provided us. Some reacted positively to us right from the start, while others didn't really cooperate until well into the second phase of the exercise. But as they saw that we were indeed doing what we said we would do with their "secrets," they came to trust us more and more and provided more complete and usable information than they had at the start. By the end of the MINI-EX the exercise's intelligence directors were even calling on us quite regularly to insert scenarios into play when they realized that it was actually the only practical way to accomplish their goals.

(U) Here in what was really the only logical work space for us, we didn't even have a computer to use.

~~(FOUO)~~ And so began our 15-day challenge at ATLANTIC RESOLVE. I say "challenge" because that is exactly what it was. In the course of the 2 weeks we hit one obstacle after another, but we overcame them one by one with perseverance. The attitude of others (particularly OPFOR members) toward us was just one of the challenges we faced but overcame. There were many other factors that tested our patience.

(U) For example, upon our arrival at Grafenwoehr, many of the logistical arrangements for our work spaces and the equipment in them were not as we expected. During the initial planning phase of the exercise it was decided that there would be an SSO SCIF in a building near the ICC building. My team was originally supposed to set up shop in the ICC building, not in the SCIF where we ended up. Upon our arrival we saw that the ICC was already overcrowded and in constant turmoil, so the SCIF seemed like a better alternative.

~~(FOUO)~~ In addition, there was supposed to be a STU-III and fax available for our use in both the SCIF and the ICC. What we found when we got there was that the ICC had only an unclassified fax and no STU-III, which was unacceptable for our purposes. There was one STU-III in the SCIF, but it was already in constant use. The SCIF did have a fax machine, but it was broken. At this point we thought we were totally out of luck and would be unable to communicate with the scripters [redacted] to pass them the information they would need to write reports. But upon claiming some space for ourselves in the SCIF we discovered the presence of two JDISS terminals there. These terminals were cleared for SCI and would have been perfect for

P.L. 86-36

DOCID: 4019611

our use, but they belonged to the EUCOM Collection Management Office (ECMO)'s element and the JAC Liaison Officers' element in the exercise.

(U) Unfortunately, during the exercise's planning stages there was apparently some miscommunication about the possibility of our use of SCI-cleared computers. The information we received indicated that no SCI-cleared computers would be available for our use. That would have been true if there had been any way we could have worked from within the ICC (non-SCIF) building. But that just wasn't feasible, so here in what was really the only logical work space for us, we didn't even have a computer to use.

~~(FOUO)~~ If the truth be told, having our own computer would actually have eliminated the need for the four-person team in England. If the three of us at Graf had had access to our own JDISS terminal from the start, we could have done our own SIGINT scripting, in addition to the information-gathering, and none of the back-and-forth with England would have been necessary. But in the end it actually was to everyone's benefit that we did have the four scripters in England. The separation of duties between the two locations allowed the "Graf three" to concentrate fully on information-gathering, a task which could only be done from Graf. This enabled us to provide the England team with non-stop data, with an end result of significantly more products being produced than would have been if the "Graf three" had had to perform both the collection and production functions.

~~(FOUO)~~ During the first few days, the ECMO element was kind enough to grant us use of their JDISS terminal on a time-available basis. But it was evident quite early on that this would not be a satisfactory way to continue throughout the entire exercise. *We needed our own terminal!* Again by some great stroke of luck, we were able to make contact with an office back at EUCOM HQ in Stuttgart that had plans to come to Graf later that week and agreed to bring a JDISS terminal for us. So despite the frustrations of those first days, before week's end we were properly hooked up. We didn't expect anything but smooth sailing after that.

(U) In addition to the problems we faced with communications, obtaining accurate, timely, and significant scenario data continued to challenge us throughout the exercise, although we did note significant improvement in this area as the exercise progressed and as relations between all other players and our team improved. The more they understood about what it was we were there to do, the more and the better information they were willing to share with us.

~~(FOUO)~~ For future exercises of this type, however, it would be best for the SIGINT team to have one of the "complete truth" terminals. These terminals were few and far between and were always in high demand. Our lack of training on these terminals didn't help any; we always had to seek assistance from someone else who wasn't too busy to help us. If we'd had our own, we could have used it as the primary source to keep us informed on what the base ground truth was at any given time during the exercise; we wouldn't have had to rely on others' whims to find out what we needed to know.

(U) There were insistent demands to run the exercise at the unclassified level. This was simply not possible, as far as we were concerned, and we beat the subject to death.

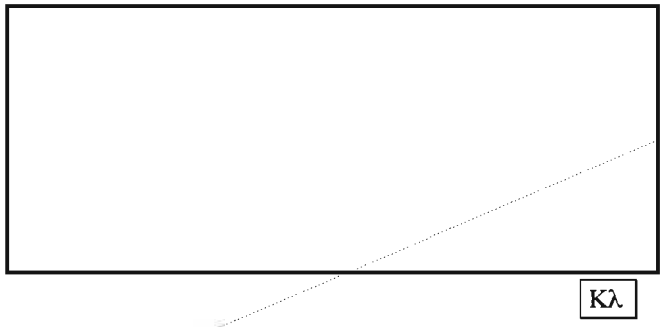
~~(FOUO)~~ Another problem: there continued to be insistent demands to run the exercise at the unclassified level. This was simply not possible, as far as we were concerned, and we beat the subject to death. Admittedly the information we were passing along (which was subsequently being reported) was purely fictitious, but the reporting methods used clearly revealed how the SIGINT reporting business works. That alone was enough to merit some level of classification.

~~(FOUO)~~ With these problems behind us, we spent our time "hunting and gathering." The "hunting" part meant meeting and getting to know the members of the OPFOR, from whom we would obtain most of the data from which exercise SIGINT would be produced. But it also meant visiting many of the various other elements involved in the exercise. One day we visited the SCIF that belonged to the Commander of the Land Component Command. Also on our visitation list that day was the Corps Tactical Operations Center Support Element,

which resided in one of several expandable vans filled with computers. Finally we were able to locate the Joint Forces Aircraft Control Center (JFACC), which served as the Air Component Command. The JFACC itself was housed in a huge beer-fest tent, while their SCIF was located in a van on the back of a truck outside the tent. Both the Ground and the Air Components were located about a half-mile walk from our location in the SSO SCIF/ICC building area.

~~(FOUO)~~ All our long hours (12-14 hours per person every day!) and hard work really paid off in the end. The "Graf three" relayed scenario and control information to the "England four" in close to 100 information reports, feeding them for their product reporting. In other statistics, the two teams together produced 149 TACREPs and 174 product reports covering ground, air, missile, and naval operations. These numbers, while not astronomical, represented reporting on some significant events in the exercise scenario and certainly provided some important training for the players. Even they admitted that this was the case! I was proud of our teams and the work we did; I felt we made a significant contribution that represented the SIGINT system well.

~~(FOUO)~~ And so, after 2 weeks behind concertina wire in a makeshift SCIF, working with military members from all services representing five nations, the first ATLANTIC RESOLVE came to a close. It really was a "TDY chance to excel," as it had been billed in that first e-mail. I learned an immeasurable amount about everything from how various comms systems interact, to the writing of TACREPs, to how a multi-national operation (albeit notional) is run. I even got a little insight into "the enemy mind" and how military tactical and strategic thought evolves. Would I do it again? You bet I would. Would I recommend it for others? No doubt about it. All that is required is a spirit of flexibility, willingness, and adventure. ATLANTIC RESOLVE II, here we come!



P.L. 86-36

DOCID: 4019611

P.L. 86-36

Hitting the [redacted] NSA's Software Reuse Libraries (U)

by [redacted]

(U) With downsizing and budget constraints in our near future, we need to do more and more with less and less. How many times have we heard these words and wondered, "How?" ***Reuse***, although not a new concept, may be the answer. Code reuse has been going on for over 20 years but it has not been formalized as part of corporate system acquistion and development processes.

(U) When applied to software, the word "reuse" means using something again for a purpose other than that for which it was originally intended. Reuse is more than simply reusing code. The basic phases of any life cycle process are requirements/analysis, design, implementation (code), test, delivery, and maintenance. Any or all information in those phases can be reused under the rubric of ***Reuse Engineering***, which comprises software activities that both utilize existing information and produce readily reusable information. With this process, we can reduce development time and cost as well as the cost of maintenance while increasing software quality and productivity. Pockets of reuse activity exist all over the Agency. We need to capitalize on those activities and incorporate reuse into our processes so we can reap its true benefits.

~~(FOUO)~~ [redacted] (NSA's Software Reuse Initiative underway in DT's Applied Technology Center for Software Engineering) is looking at doing precisely that through a phased approach. The first phase entails establishing a corporate-wide reuse repository with easy access and retrieval of software-related assets, which eventually will consolidatee all information generated in the software life cycle. This repository will be the foundation on which we will build our reuse "process". What follows is a brief history of our previous reuse repository, and where we are today (Phase I).

~~(FOUO)~~ It was not too long ago when looking for reusable code was not an easy task. One had to go to anonymous ftp servers [redacted] to look for possible reusable assets. The user had to know which [redacted] to go to, and once there, where to go and what to look for. Then the "Common Collection Console" effort came along in 1989, when Graphical User Interfaces (GUIs) were becoming popular and NSA management recognized the need for a common GUI look and feel. A small team was formed to try to develop GUI applications that could be reused on several projects. The software development community never accepted these GUI applications, but several major efforts succeeded in reusing some foundation libraries; [redacted] A reuse library was establish as more reusable assets were identified, in the first attempt to bring structure to the then ad hoc reuse process.

P.L. 86-36

~~(FOUO)~~ The [redacted] reuse library was a centralized repository that used Web technology. Assets were now centrally located, but the user still did not know much about the assets in the repository. Then [redacted] teamed [redacted] to capitalize and improve on what already had been done, and to establish an NSA-wide reuse repository.

~~(FOUO)~~ [redacted] found MORE, Multimedia Oriented Repository Environment, as a possible solution to the problem. MORE was developed as part of the Repository Based Software Engineering Program (RBSE) funded by NASA. The University of Houston, Clear Lake, directs RBSE through the Research Institute for Computing and Information Systems (RICIS). MountainNet, Inc. of Morgantown, WV operates production prototypes. The MORE product moved from a software warehouse effort on the WWW to exploring, transferring, and utilizing repository technology with a directive to commercialize (MOREplus). Moving to a commercial product would add maintenance and support as well as continued alignment with anticipated WWW improvements.

~~(FOUO)~~ NSA's reuse repository, the Software Reuse Center (SRC), is on line today, with the beta version of MOREplus underlying its capabilities. MOREplus is a distributed library management tool written in GNU C, which interfaces with Web clients and an ORACLE database, and can run on SUNs, HPs, and VAXs. MOREplus is installed on the SRC's server and interfaces with various Web clients and an Oracle database. There is only one hand-coded HTML page for the inter-

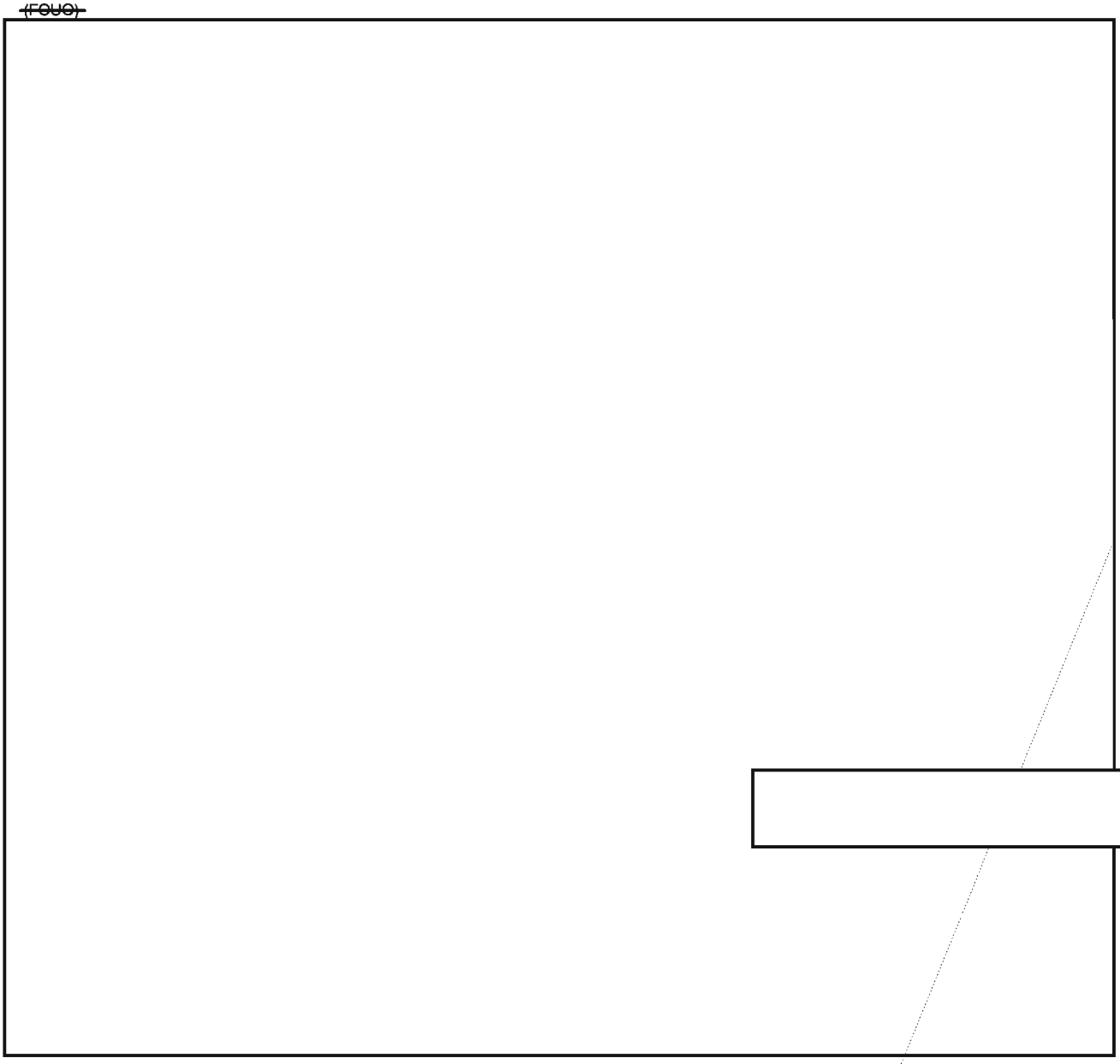
P.L. 86-36

face to the user, all the rest are generated by MOREplus. Metadata (information about the assets) resides on the ORACLE database. Now users can easily look for assets from a centralized location, but those assets can reside any where on the network. The user also can see information about the asset before retrieving it, which saves time when trying to find a candidate for reuse. Another benefit is having the assets distributed, so that the contributing organizations for those assets maintain and control them. These organizations become "remote librarians" with a Master Librarian overseeing the overall repository activities; this alleviates the workload of the Master Librarian and a centralized repository growing out of control.

(U) And now "more" about MOREplus. The classification scheme used is based on hierarchical Collections and Classes, and can be thought of as a library catalog system. Collections are subject- or topic-oriented and classes are type-oriented.

(U) From the user perspective, users can browse or search for assets from the top down through a hierarchy of Collections, or across across Collections through a hierarchy of Classes, more finely pinpointing what they are seeking. MOREplus also provides the user with a natural language- and pattern-match search. The natural-language search explores the entire database of metadata, whereas the pattern-match search looks for patterns in specific fields in the database.

~~(FOUO)~~



P.L. 86-36

P.L. 86-36

DOCID: 4019611
P.L. 86-36

(U) From the librarian perspective, additional capabilities include administrative and operational functions. Administrative functions include such things as add, modify, and delete, to name a few. A librarian simply fills in a form and submits it to the ORACLE database. Operational functions provide reports about the repository that contain useful measurements on assets, users, modifications, usage, acquisition, etc., as well as a catalog report on all assets in the repository. In addition, librarians can set up authorized users to access classified assets by login and password as well as authorized groups to access proprietary classified collections. (Even though the SRC itself is accessible by all, only authorized users will be able to browse or search for classified assets or entire classified collections.)

(U) Other features include a "What's New" function providing information on newly acquired assets; context-sensitive help on every page, with an index of all help pages; help on each field that needs to be filled out by a librarian submitting/changing assets to the repository; and manuals and tutorials.

~~(FOUO)~~ K44, the previous [redacted] team, is the SRC's master librarian and has worked very hard to establish NSA's reuse repository. K44 also contributed a valuable additional capability to the MOREplus product itself: they introduced TCL (Tool Command Language) to MountainNet, Inc. TCL allows the master librarian to easily customize displayed pages and to display a classification label on those pages.

~~(FOUO)~~ Other functionalities provided by the previous [redacted] reuse library includes "User Registration" and "Contribution," to name a few. "User Registration" is currently a voluntary option that allows a user to register with the SRC to be automatically notified of updates to assets of interest. The "Contribution" is a form allowing users who are not remote librarians to contribute valuable assets, these assets reside on the SRC's server, but the contributor can still maintain them.

~~(FOUO)~~ We have only just begun. Our repository will need a well-thought-out management program that includes a process for acquiring assets (COTS, GOTS, public domain), and certification and validation criteria for our assets. The Quality Assurance team under [redacted] is starting to validate existing code assets in the repository, and will assess them for quality and maintainability against industry standards. Soon users will be able to see the quality or risk associated with an asset before retrieving it. We will also need a program to measure reuse activity, beginning with the repository, to determine whether it is successful and to continuously improve our reuse activities. MOREplus provides a starting place for us to measure accesses to each asset and accesses to the repository. What we lack is asset usage, data reflecting the reduction in development time and costs, etc.

(U) In conclusion, the goal of the first phase of our reuse initiative is to familiarize system acquisition and software developers with reuse concepts and its potential. Subsequent phases will, we hope, integrate these opportunities and other reuse methods/techniques into our system acquisition and development processes (also, these processes must be well defined and controlled before reuse engineering can be incorporated into them) so that when we build new systems in the future, we will look for reusable assets from our repository instead of "reinventing the wheel." We will also keep reuse and inclusion in the repository in mind during development. A reuse technique termed Domain Engineering will help us do just that. Domain Engineering encompasses families of systems and captures the true functionality found amongst those families. Productivity will increase as it takes less time and costs less to develop new systems within the same family since common functionality will be reused. This frees up skilled developers to concentrate on the truly critical aspects of the new system, so they need not be concerned with the more mundane routines used over and over again. Software quality and reliability will increase as known and proven assets are reused, leading to a reduction in maintenance costs. We will, in short, be able to do more and more with less and less. We will do it better, faster, and cheaper. Aren t those words everyone would like to hear?

(U) To find software-related assets, go to the SRC at **http://www.src.nsa**.

[redacted]

Kλ

P.L. 86-36

DOCID: 4019611

CRYPTOLOG
Winter 1995

The Nature and Process of Analytic Thought

by Hugo Keesing

Popular culture has been my core preoccupation since stepping off the boat from Holland as a seven-year-old in the early 50s. Popular culture—radio, television, comic books, baseball cards—were the way I learned a new language, made friends and came to understand my environment. I listened, I watched, I read and I collected and traded. There were new things to be absorbed every day: words, facts, relationships. I took them in, but I didn't process. I never asked myself, "So what?"

When I discovered girls a couple of years later, my curiosity increased. My sources and methods, however, were unsuited for the new target. That problem began to resolve itself when I became aware of MUSINT (music intelligence), an important but lightly regarded discipline of SIGINT.

At age 12, an interest in the latest music—because that was of interest to girls—helped me develop skills which are the staple of what communications analysts do today. Let's look at a few.

In 1955, when Washington, D.C., radio stations continued to play Perry Como and Jo Stafford, I became an expert at capturing, identifying, and monitoring "foreign" signals: stations such as WKBW in Buffalo, WCKY in Cincinnati, WLS in Chicago and WOWO in Fort Wayne. I learned about the importance of a good antenna, the impact of atmospheric conditions on signals clarity, about signal-to-noise ratios.

Late at night I learned to recognize the voice patterns and musical tastes of George Lorenz (The Hound), Dick Biondi and numerous other DJs. This enabled me to identify specific frequencies without having to hear the call letters.

I learned the importance of communication attributes such as rhythm and beat. If the song had a good beat and I could dance to it, I wanted to own the record. So began my record collection.

I learned transcription. Sometimes the text was clear voice (Pat Boone); other times it had to be retrieved from garbled transmissions (Little Richard). As I tried to write down the words of songs, it didn't occur to me then to buy sheet music. I sensed intuitively that MUSINT was better than OSINT; that open sources might not carry the real lyrics. (This discrepancy has subsequently been confirmed in at least a few instances.)

I learned cryptology. From decoding lyrical messages to cryptanalyzing enciphered letter groups such as oo ee oo ah ah (ting tang walla walla bing bang).

It was only as I became more familiar with the context for MUSINT that I began to understand the importance of the messages themselves. Song lyrics were more than words; they were the dialogue of 50s/60s courtship. Boys didn't talk to girls; they asked them if they liked certain songs, or what their favorite song of the moment was. From this information intent was deduced (whether you had enough in common to support a friendship).

What's all this *"A wop bop a lu bop, a wop bam boom"* I'm hearing on this thing? Maybe I need to fix my equipment.

I also gained a deep appreciation for traffic analysis: the externals of songs, who sang them, on what label, their peak chart position. Knowing that my "target" liked the Platters and Johnny Mathis was promising information about other, as yet unknown traits. The interest in externals led to collecting information about music; first newspaper clippings and record lists, then magazines and books. I still collect and still make analytic assessments based on musical tastes.

But most important, I was able to satisfy customer requirements with MUSINT. At parties where I supplied the records, or at dances where I DJ'd, I provided an important service. My MUSINT-derived knowledge enabled me to suggest (or select—I have never been averse to making my own policy decisions) the perfect sequence of songs to influence strategic decisions.

So forty years ago I began acquiring and developing skills, knowledge, and analytic abilities which have served me in the past and continue to serve me today. What was most important is that I have never thought that using this skill set was work—only fun. Which brings me to my topic: analytic thought.

Many of you[1] responded to my e-mail query, with answers ranging from a single word to virtual treatises. Despite their differences in length, you and I are in general agreement on the attributes of, and impediments to, analytic excellence.

The vast majority of you identify personal qualities with the former, and environmental or organizational qualities with the latter. Some of the cognitive attributes you (collectively) consider assets include:

Curiosity
An open mind
Creativity
Ability to visualize
Broad subject-matter knowledge
Common sense
Critical thinking skills
Mental flexibility.

This is a good blend of the **raw and the refined** (creativity : critical thinking); the **spontaneous and the structured** (curiosity : ability to visualize); the **native and the taught** (common sense : broad knowledge). In psychological terms, your responses suggest that good analysts are produced by heredity as well as environment. The corollary debate that I've heard here at NSA is whether analysis is an art or a science.

Your experience, which agrees with mine, is that analytic excellence requires both. An undisciplined, creative mind may fall as far short in solving a complex problem as an inflexible, trained mind, yet the shortcomings are not the same. If the raw material is lacking, neither training nor smart tools are going to provide sufficient compensation. On the other hand, training, education, computers and other aids can have a salutary effect on a young (or not so young) mind ready and willing to learn.

There are also enabling personality traits, taken from your experience, that have a bearing on analytic excellence. You have identified persistence, desire, and stubbornness, to which I would add respectful disdain for arbitrary authority and for orthodoxy.

What, then, is the composite of an individual who has all the qualities necessary for analytic excellence? Visualize her and ask yourself how well-suited she is for an organization like NSA, with its highly structured, customer-driven, time-sensitive environment. A setting in which, according to your experience, analytic excellence runs the risk of being subordinated to the requirements of Corporate Cultures, Policy Correctness, For[at] Over Substance, and an assortment of other Management Issues. Can analytic excellence possibly flourish in such surrounding? My answer is, "Yes, if..."

What I would like to do now is to suggest some ways in which NSA can improve on the raw materials and make the work environment more analyst-friendly. While it is up to leadership to address these issues, my suggestions may also identify possible roles for the Communications Analysis Association in ensuring the health of the analytic profession.

Start with the right stuff. Do whatever is possible to recruit into the analyst ranks people who are *curious, creative, and not afraid to be different.* Filling analyst positions primarily through cross-training necessitated by changing missions or down-sizing devalues the Art aspect of analysis, just as inadequate tools and training devalue the Science aspect. I would also add that the legitimate need for security must never become a vehicle for ensuring orthodoxy.

Find out what analysts do for fun. See whether you can help them link their avocation to their vocation. There is a tremendous potential for positive skill transference, whether the hobby is music, surfing the Internet, the stock market, sports, science fiction . . . the list is endless. Once you find out what they do for fun, use it as a springboard to teach analytic techniques in ways that are intrinsically interesting to the learner. Teaching in this way will require creativity, mental flexibility, and broad subject-matter knowledge on the part of the instructor. In short, it will mean *teaching through modeling.*

1. This article is the text of a recent presentation given to the Communications Analysis Association.

Provide frequent, appropriate opportunities for analyst skills to be refined. Formal training and education are two possible ways. Rotational assignments, mentors, and individual, directed research are others. Consider allowing analysts to meet some part of their professionalization requirements through work which has no obvious link to SIGINT (but requires the use of similar analytic tools).

Reinforce behaviors that keep the raw material vital. Encourage analysts to read (on the job!), to browse data bases, to spend time in libraries. To explore new fields, to try and fail. Make sure they don't get stale or complacent. I don't get discouraged easily, but I do when students tell me their work doesn't leave enough time to read. An analyst can't afford not to read! As a supervisor, work from the premise that good analysts are, by and large, self-managing. Give them space and give them support. Getting them to stop work should be harder than getting them to start.

Provide the right level and mix of tools for each analyst. Not everyone needs or wants the latest software upgrade. I have colleagues who became paralyzed after well-intentioned techies "improved" their workstations.

Give frequent feedback and insist on high standards. There should be no tolerance for sloppy thinking. Analysts must not be permitted cognitive biases, untested assumptions, or conclusions not properly linked to evidence. Similarly, they must not be let off the hook with "reporting" vice analysis. In the current language of CIA's Directorate of Intelligence, analysis includes facts (verified information), findings (expert knowledge), and forecasts (judgments based on facts and findings and defended by sound and clear argumentation).

Finally, reinforce good writing. A poorly written analysis that fails to communicate its finding to the customer represents wasted time and effort. What is good writing? Succinct, precise, and incisive are three adjectives that come quickly to mind. My pet peeve as an instructor? Students' use of the passive voice, which hides accountability.

Can NSA afford to do this for its analysts? Jim Devine, Deputy Director for Support, makes it clear that it must. I quote from a 1 November e-mail message:

Stop using that infernal passive voice and tell me who's responsible!

"If we are going to achieve organizational success in a dynamic climate of challenge and change, our people must be more highly trained and educated, more flexible and adaptable to change, and more willing to take risks, to view problems in a creative way, and develop innovative solutions. Organizationally we must provide an environment that fosters risk-taking, innovative thinking, and entrepreneurial activity. We must prepare our people better to deal with change, to take on far more complex technical problems, and to achieve their maximum potential."

Should NSA fail to do so, it may soon be included in Senator Kerrey's recommendation for CIA: "It should survive," Kerrey said recently, "but it will need the organizational equivalent of a sex-change operation." Analysts and their supervisors will have to be in the forefront to keep such surgery unnecessary at NSA.

Dr. Keesing has been assigned to NSA as the Joint Military Intelligence College's Visiting Professor since September 1993. In this capacity he teaches graduate courses on research and on intelligence analysis. He also serves as thesis advisor for some 30 NSA students, some of whom have won prestigious awards for their theses. A psychologist by training, Dr. Keesing taught for four years in the University of Maryland's overseas programs, with assignments in 10 countries on three continents. His elective course in American Studies uses rock music and other forms of popular culture to teach contemporary American history.

Kλ

DOCID: 4019611
P.L. 86-36

Three Vs For SIGINT (U)

by [redacted]

~~(FOUO)~~ ***Vigilance, versatility*** and ***vision*** are three attributes an NSA SIGINT reporter should possess in order to provide valuable intelligence responsive to consumer needs in the post-Cold War era. Reporters should have the vigilance to remain abreast of all developments regarding their target, whether political, economic, social or military in nature, but specifically when those developments affect U.S. interests; the versatility to prioritize and report on the target from varying angles, providing the consumer with key issues up front and in the most concise and understandable format; and the vision to be prepared and anticipate changes in the target as global issues constantly evolve and possibly threaten U.S. or allied interests.

[redacted]

[redacted]

EO 1.4.(c)

EO 1.4.(c)
P.L. 86-36

P.L. 86-36
EO 1.4.(c)

(U) According to an editorial in the Washington Post in November 1994, Russia's nationalist and imperialist tendencies have been viewed by some officials in Washington as sooner or later threatening the fragile states on its periphery and perhaps beyond. There are other officials, however, who feel Russia can be cajoled into joining the ranks of civilized and democratic states, or at least the possibility exists to justify maximum efforts toward that end. In order to formulate a proper U.S. policy toward post-Cold War Russia, policy-makers will continue to need access into Russia's near abroad.

P.L. 86-36
EO 1.4.(c)

(U) A more detailed version of this article was the winning entry in last year's International Affairs Institute essay contest.

P.L. 86-36
EO 1.4.(c)

Kλ

1996 selected calendar of events sponsored by NSA, academia, and professional associations:

Event	Date	Where to call:
• 4th Intl. Workshop on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems; San Jose, CA.	1-3 Feb	Email: zhang@ringer.cs.utsa.edu
• Information and Command and Control Warfare Course; GW University.	26-29 Feb	800-424-9773
• Information Warfare Symposium, AFCEA, Washington, DC.	8 Mar	703-631-6238
• Enemy Eyes: The Role of Visualization and Graphical Technology in INFOWAR; AFCEA, Central Maryland Chapt Technical Seminar; Linthicum, MD.	15 Mar	410-544-8418
• Conference on Computers, Freedom and Privacy '96; Cambridge, MA.	27-30 Mar	Email: cfp96@mit.edu
•7th National OPSEC Conference; Tyson's Corner, VA.	16-19 Apr	301-982-0323
• Tactical Communications Conference; Ft. Wayne, IN	30 Apr - 2 May	215-674-0200
• ICASSP '96 - INtl Conference on Speech Acoustics and Signal Processing; Atlanta, GA	6-9 May	404-894-2948

(UNCLASSIFIED)

DOCID: 4019611

American Translators Association Conference (U)

Contributors to this article include [redacted] *and a tech-track linguist whose job requires anonymity*

P.L. 86-36

(U) The American Translators Association's (ATA) 36th Annual Convention was held in Nashville, Tennessee from 8 to 12 November 1995. The ATA, with its 6,000 members, is the country's premier organization for translation and interpretation professionals. The conference provided an exceptional opportunity to meet with private-sector counterparts and see first-hand the tools and techniques they use; learn different aspects of the craft, such as machine translation and interpreter training; and look for ways to improve our own work. We learned that there are many areas in which the Agency is ahead of the private sector (particularly with training and working aids), and other areas where we need to improve. Those attending from NSA recommend that the DO Technical Health Advisory Board (THAB) continue to send tech track members to future ATA and similar events.

Lessons Learned

(U) The presentations at the conference led us to several conclusions:

(U) The Agency should take a hard look at how it selects linguists.

(U) Almost every ATA member we met got started in the translation field by accident. Most were either born overseas and emigrated to the United States, were raised in a bilingual home, or spent a significant amount of time abroad studying or working. ATA members agree that translation is only half linguistic and the rest cultural; therefore translators are really cultural mediators. Convention workshops consistently stressed that to be good, translators must have four qualities:

- A well-rounded education to understand how the world works.
- At least one year and preferably longer in a foreign language country to understand the societal and cultural biases of that language.
- An outstanding understanding of the language into which they are translating.
- An excellent linguistic knowledge of the foreign language.

(U) This means that a good translator requires as much background, education, and experience as do experts in fields like computer science and engineering.

(U) The Agency is far ahead of the private sector in translator training and support.

(U) The good news is that once we select linguists, they can count on significantly more translation-specific training than their commercial counterparts. Throughout the conference, ATA members lamented the limited number of translator training programs available in the United States. Of the thousands of U.S. colleges and universities, as few as 30 offer full translation programs. As a result, commercial translators move into a field with little or no formal training or experience. ATA is beginning to recognize the need for translator self-training, but materials are only now being developed.

(U) In contrast, junior linguists at NSA regularly receive feedback from more experienced folks on translation skills and hands-on training on translation techniques. Linguists may join the Agency already possessing some degree of the four critical skills mentioned above, but with no translation experience. They may spend their first several months working under the close supervision of several accomplished linguists; the progress of these months would take years had they been forced to learn on their own.

(U) Our linguists also have access to larger amounts of reference materials and working aids than private sector translators. This ranges from using online dictionaries and working aids, to drawing information from computerized databases, to being able to call central reference for help on a particularly difficult question. More important, Agency linguists can turn to colleagues for help with background and terminology questions. Even at the largest commercial translation agencies, linguists often work alone, without access to this most important human resource. In the past, ATA members had to rely on their own personal networks to

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019611

help solve translation problems, but the Internet revolution is providing many ATA members with a means of asking for assistance from other translators. The most popular platform is the Foreign Language Forum (FLEFO) available on CompuServe, but translators may also find the sci.lang.translation newsgroup on the Internet useful. (However, as one translator at the Conference pointed out, not all the advice provided in reply to translators' questions on bulletin boards is accurate—as is so often the case with bulletin boards in general—so one must learn through experience which translators answering queries are authorities in their fields.)

The average U.S. free-lance translator can expect to make about $36,000, slightly less than a GS-11, but cannot count on the health insurance, vacation, retirement, and other benefits Agency employees receive.

(U) Agency linguists are well compensated by industry standards.

(U) Agency linguists earn more than their private sector colleagues. The average free-lance translator in the United States can expect to make about $36,000 in 1995, or slightly less than a GS-11. The free-lancer, however, cannot count on the health insurance, retirement, vacation, and other benefits Agency employees receive. This total compensation, combined with access to working aids, dictionaries, and superior training opportunities, means that our management recognizes the value of language professionals.

(U) In contrast, the private sector generally does not value language services, and the translation field suffers from an image problem in the United States. One reason is that, unlike other professional fields, there is no national standard for translation accreditation. The more significant, however, is that most U.S. businesses do not believe translation is worth the extra cost. They rely on the high-school-level skill of someone at the company or leave translation tasks to their foreign distributor. Other companies simply publish documents and advertising in English only. ATA's position is that U.S. firms are cutting their own throats, and its members are working to educate U.S. companies on the importance of using professional translators to increase sales abroad.

Presentations and Workshops

(U) Public Perception of Translation in the USA

(U) Lee K. Curtis stated that she surveyed several international marketing and sales directors in the United States on the subject of translation. She concluded from the survey that ignorance of good translation is prevalent despite the fact that translation is a vital asset to our economy. In fact, we at NSA are cognizant that our national security often depends on translation when it comes to staving off terrorism.

(U) Ms. Curtis cited the following reactions by businesses in the U.S. to translation:

1. Our distributor takes care of our products.

2. We have people in our company who took foreign language classes in school.

3. We can't afford translation.

4. Why? All we want to do is to substitute the English with the foreign text in our computer. Ms. Curtis gave an example of this. An American company published a commercial in the Middle East that ran like this:

Dirty Clothes - Xabwn Gsil - Clean Clothes
[Xabwn Gsil = detergent]

. . . but the company didn't take into consideration that people in the Middle East read from right to left.

5. We want you to fit the foreign language text into the same amount of space allotted to the English text.

6. We don't do business with anyone who does not speak English.

7. We have a computer software program that takes care of our business.

(U) Ms. Curtis focused on such common misconceptions and shared with the attendants her views regarding "How to educate potential clients by showing them what damage improper translation may do to their business."

(U) Teaching Translation to Undergraduates

(U) Sonia Colina, a translation instructor at the University of Illinois at Urbana-Champaign, focused on "What Do Errors Reveal?" She stated that examining and analyzing students' errors reduces subjective evaluation. She compared two methods of teaching translation. In the traditional teacher-centered classroom, the teacher is the performer and corrects students' errors on the spot. In the modern student-centered classroom, the student is the performer. Students are allowed to monitor and analyze their own errors; this allows the teacher to look into the students' learning process and proceeds to design a more effective curriculum and/or course materials.

(U) A Meaning-Based Approach to Teaching Translation

(U) Two instructors from Georgetown University, Shuckran Kamal and Jacqueline Murgida, ascribed poor translation from Arabic to English to "inadequate command of English writing skills, Arabic reading comprehension, and/or sound translation principles;" plus lack of "awareness of the advantages of membership in the major professional organizations" of translation and interpretation. To remedy this situation, they proposed formal training in translation principles, on-the-job training, and joining organizations like the ATA.

(U) For formal training, the instructors presented a sample lesson of a program of study in Arabic-English translation. They required students to have at least a level-III proficiency in Arabic and to have read Mildred Larson's book "Meaning-Based Translation." Their program offered an assortment of activities. For example, they invited guest speakers to lecture on topics relevant to translation in general as well as to Arabic-English translation in particular. In addition, they selected texts from the Arabic and American media for translation, provided exercises for students to work individually and in teams composed of native English/native Arabic students, and challenged the students to edit and revise professional translations. (One NSA linguist objected that one of the examples, commentaries/editorials by George Will, would frustrate the students more than help them improve their skills because of the complexity of Will's thoughts and writing.)

(U) Medical Terminology Management in a Multilingual Environment

(U) Helen Knight, Brenda Rudder, and Clove Lynch stressed that our technical environment requires that translators be accurate and consistent in their use of specialized terminology. To this end, Family Health International (FHI), a nonprofit organization that conducts medical research, developed a multilingual medical terminology database (TDB). It efficiently stores large quantities of terms and their definitions in different contexts to be retrieved and processed in a variety of ways.

(U) FHI's TDB distinguishes between a term and a word. "A term can be made up of one or more words and has a precise meaning in a specific context." Actually this TDB provides specific relevant and concise contexts to illustrate a term. This kind of programming can certainly improve translation quality by ensuring the accurate and consistent use of specialized terminology.

(U) Machine Translation

(U) Alejandra Koval of AT&T Business Translations' presentation discussed machine translation (MT)—what it is, where it is, and where it's going. Current perception is that MT is stealing work from translators, is hard to read, and can even be dangerous if used for manuals and instructions. But the advantages of high volume, consistency, and customization are too great to ignore. MT will not replace translators; it will redefine their role. Now and in the future, rather than translating a text from scratch, translators will do a pre-translation review, performing text analysis and dictionary building, and will quality control the machine's output in the post-editing and final review stages.[1] Obviously, MT is only as good as the dictionary provided for it. Some things, like polysemous (dual-meaning) words, will always pose problems. The key point is that MT does not replace the translator. It is a tool to be used by a translator. The person using MT will still require all the same translation skills and linguistic knowledge that have always been needed.

1. (FOUO) For information on MT capabilities available at NSA, see "Machine Translation: What Can It Do For Us?" by [redacted] CRYPTOLOG, Vol. XXI, No. 3, Fall 1995.

P.L. 86-36

DOCID: 4019611

About the ATA

(U) The ATA is the only private-sector entity accrediting translators in the United States. As both a professional and a trade organization, its goal is to build recognition and appreciation for the translation field. On the professional side, ATA has an accreditation program whereby translators can be tested or evaluated by their peers. Once accredited, members are listed in the ATA translation services directory. However, less than one-third of the members are accredited, one reason being that the accreditation program is limited to less than a dozen mostly European languages. Accreditation tests for Chinese (due out in spring 1996) and some other languages are in the works. The test-taker is typically required to translate three of five passages on the test. Topics may include a patent and a literary passage, and passages on economics, finance, and technology. Graders try to make the examination general in nature, so that it tests one's command of the language rather than knowledge of subject matter.

(U) ATA stresses the importance of using professional translators to increase sales abroad

(U) Aspirants must take a practice test before taking the accreditation examination because so many people have failed the latter, but no critique is provided for those who fail the practice test. Many of those attending a forum on ATA accreditation expressed dissatisfaction with this policy, considering the separate fees required to take the practice test and the accreditation examination as well as for ATA membership. Furthermore, ATA continues to have no accreditation exam for many languages (there was a session at the conference entitled "How to Get Your Language Accredited"). ATA executives promised to take into account the concerns of accreditation aspirants attending the Forum, but the matter was unresolved by the end of the conference. It was also pointed out that ATA accreditation naturally is less important to translation agencies and customers than quality work completed on time.

(U) As a trade organization, ATA gives professional translators a forum in which to disseminate information, exchange ideas, and work together to educate business on the need for professional quality translations in its literature, documents, and advertising. The nature of translation work discussed or advertised at the conference confirms the notion that technical translation comprises a large portion of private-sector translation (although awards were given at the conference for outstanding translation of foreign literary works). Translation agencies, as one might expect, prefer to employ specialists in technical fields, but are often compelled to use the services of less technically literate individuals who can translate documents in their chosen specialty reasonably well. As one translator with an electrical engineering background who specializes in telecommunications pointed out, "In my field, one must visualize to which pin a given connection leads," adding that well-written translations often mask technical translation errors. He conceded that quite a few translators are able to compensate to a large extent for their lack of formal technical training by extensive reading of technical literature in English on their fields, and advised that a few technical courses at a community college could go a long way toward helping aspiring technical translators with liberal-arts backgrounds.

~~FOR OFFICIAL USE ONLY~~

(U) Interpreter Training

(U) Carol Patrie of Gallaudet University in Washington, D.C. discussed interpreter training. Her school's approach to interpreter training requires students to be at the master's level and to have the language skills, experience, maturity, and discretion necessary to be a good interpreter. The Gallaudet program, intended to train students to perform simultaneous interpreting, emphasizes a step-by-step process, teaching interpreting skills as component parts. The general skills portion begins with language competence exercises to access and develop student's ability. A speaking ability test is administered to see if students can express themselves in the foreign language. Cloze exercises (filling in the blanks) teach students to finish sentences and logically predict the next sentence or idea. Other exercises help students improve how they sound, increase understandability, develop auditory memory, and learn to grasp links between ideas being presented.

(U) Usage Labels

(U) Jean Quirion, a graduate student at the University of Montreal, delivered an excellent paper on usage labels in dictionaries and the impact they have on translation accuracy. He noted that dictionary worship, meaning accepting an entry without question, is common among novice users. This is a problem, since dictionaries often fail. One reason they fail is that general dictionaries are limited to the most common words. But the more common reason for failure, he believes, is that stylistic labels have not kept up with changes in language and society.

(U) Usage labels tell us if a word is obsolete or archaic, slang or colloquial, if it is used only in a specific region, or specific to a field such as sports, religion, or medicine. These labels must also match a given culture. For example, words specific to gender or social class are much more common in European languages (including European versions of English and French) than in North America.

(U) One problem with usage labels is that they still involve a great deal of subjectivity. Another is that lexicographers must leave their field of expertise when assigning usage labels. An experienced translator must use great care when selecting a general dictionary and should also have access to specialized dictionaries. Lexicographers in general should make standardization of labels a valued long-term goal.

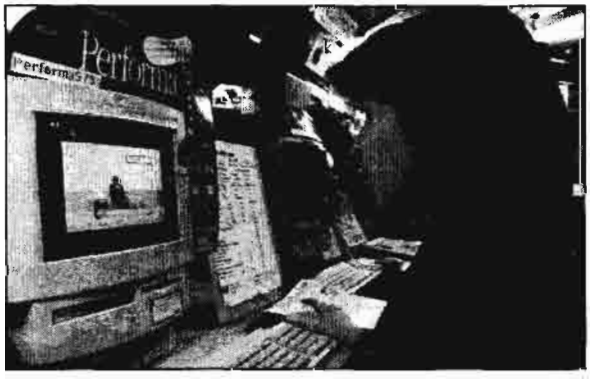
(U) Translation Techniques

(U) Every presentation in whole or in part recommended translation techniques that make for higher quality work. Most of this information is not new for titled technical track professionals. At the same time, hearing it reinforced the techniques taught at the Agency. Here are some examples:

* Cliff Landers, a professor of political science at Jersey City State College, recommended that non-fiction translation be treated like literary translation. His basic premise is that translators need to maintain the information content of the original text, but present the information in a literary style typical of an educated native speaker. His motto: "A good translation sounds as though it were written in English."

* Several presentations stressed how translators and interpreters act as mediators between cultures. For example, in Brazil, salaries are usually expressed by the month, but in the United States we express them by the year. Translations between these two languages/cultures must either be explicit about the time period represented or do the math and express the figure the way the target audience is accustomed to thinking about these matters.

* Another presentation encouraged translators to think in terms of semantic units rather than words to increase translation accuracy. For example, in Hungarian, one word can accurately represent three or four words in German. Conversely, it might take three or four English words to convey the meaning of one word of Finnish.



(U) The Japanese market for software is enormous

DOCID: 4019611

Tips for Free-Lancers

A presentation on how to succeed as a free-lance translator contained a number of valuable tips for increasing one's marketability that could be useful to Agency linguists as well. The growing importance of desktop publishing (DTP) means that a thorough knowledge of DTP programs is an asset. Here again Agency linguists have an advantage over their private-sector counterparts in that DTP training is available through NSA's Learning Center. "Software localization" (for example, translating "shuuryoo" as "the 'done' key," instead of giving it a literal translation of "end" when writing software for Japanese customers) is a hot topic for translators into Japanese and European languages; the Japanese market for software is enormous and the European Union has required all manuals to be translated into Europe's chief languages, thus creating a huge market for translators of European languages.

New translation tools, heretofore only obtainable for European languages, are becoming available for Japanese as well for cross-application purposes, graphics, and text/string-extraction tools. A downturn in the Japanese economy brought the fortunes of Japanese-to-English technical translators to their lowest ebb about 3 years ago. Once the nadir was reached, however, the appreciation of the yen against the dollar ultimately forced Japanese translation agency executives to transfer a considerable portion of their work to the United States and elsewhere where translation costs are lower.

Kλ

Here are other translation events which language technical trackers may want to attend:

The Federation Internationale des Traducteurs World Congress.

Mr. Steve Sachs, a free-lance translator from Annapolis, Maryland, briefed the conference on the Federation Internationale des Traducteurs (FIT) World Congress scheduled in Melbourne, Australia, in February 1996. The FIT is the umbrella organization for over 75 national and regional translation organizations from over 40 countries. Associate members include universities and other organizations. Funding comes from member dues and through UNESCO. Conference activities are much like the ATA convention, only on an international scale. This conference is held only once every 3 years, with the 1999 conference tentatively scheduled for Mons, Belgium.

The Second International Conference on Current Trends in Studies of Translation and Interpreting.

Dr. Kinga Klaudy, President of the Translation Committee of the Hungarian Academy of Science, issued an open invitation to attend the Second International Conference on Current Trends in Studies of Translation and Interpreting. The conference is scheduled for 5 to 7 September 1996 in Budapest and is organized by the Faculty of Humanities at Eotvos Lorand University.

(UNCLASSIFIED)

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019611

CRYPTOLOG
Winter 1995

P.L. 86-36

From the History File: How I Helped Trigger a Greater American Involvement in Vietnam (U)

by [redacted]

(U) In the early 1960's the Military Airlift Command was still using a fleet of lumbering C-121's to ferry servicemen (we rarely saw a servicewoman in those days) to and from overseas duty stations. The C-121 was an ungainly craft that, now that I think of it, looked a lot like a Klingon Bird of Prey. Somewhat slower than the mainstay of the Klingon fleet, the C-121 took about three days to make the trip from Southeast Asia to the West Coast of the United States. [1]

(U) Anyhow, it was October 1962 and an appallingly young and fresh-faced 25-year-old Airman First Class [redacted] was dozing aboard one of these "Connies," as they were sometimes called, while the aircraft labored toward San Francisco from Hawaii. I had boarded at Clark Field in the Philippines, having completed a 21-month tour of duty in Southeast Asia, and was to be discharged from active duty once I arrived back in the States. On the ground stateside, Alvin Dark's Giants were about to lose a heartbreaker to Ralph Houk's Yankees in the seventh game of the World Series, and America was a lot closer to a nuclear exchange with the Soviet Union over the missiles in Cuba than many of us on the other side of the Pacific Ocean had ever realized.

(U) As the engines changed pitch and the plane began to drift down through the clouds toward the Bay area—where within days my military career would be brought to a close—my mind wandered back over the last year and a half and some of the weirdness it had witnessed. I won't dwell on the run-of-the-mill absurdities that routinely befall your average unaccompanied serviceman, but I must tell you that in October 1962 I was still not absolutely certain that I hadn't triggered a heavier American involvement in Vietnam than had existed when I first arrived in the Philippines.

P.L. 86-36

(U) The author in Saigon in the spring of 1962

~~(S-CCO)~~ It happened like this. My primary duty at the 6925th Radio Squadron Mobile at Clark Air Force Base was to analyze and report on the activities of what passed for an air force in North Vietnam—or the Democratic Republic of Vietnam (DRV), as Hanoi liked to be called in those days. And what an air force! Because the 1954 Geneva Accords on Cessation of Hostilities in Indochina specifically ruled out the introduction of combat aircraft into Vietnam, North Vietnam had no tactical aircraft worthy of the name and wouldn't take delivery of their first MiG-17's until August 1964. The largest plane they had at the time was the Ilyushin-14 (Il-14) transport—a twin piston-driven, 25-passenger, light transport which, I am reliably told, cost so much to operate that there was no way it could be made profitable. (The Il-14 was one of the early efforts of Sergei Vladimirovich Ilyushin, who went to his reward in 1977.) The DRV had 14 of these CRATEs, as NATO so aptly named them, gifted to them by the old Soviet

1. (U) Interestingly, Lt. Col. John Paul Vann, whom Neil Sheehan called the closest the United States came in Vietnam to a Lawrence of Arabia, would never have made it to Vietnam in March 1962 if he had boarded the C-121 that was scheduled to transport him and 93 other officers and men to Saigon. Vann had forgotten to have his passport renewed and was pulled from line just moments before he was to step aboard the plane. The C-121 disappeared over the Pacific, all aboard were lost, and Vann took a later flight. Sheehan's *A Bright Shining Lie: John Paul Vann and America in Vietnam* is highly recommended reading.

Union and the East Germans. Four of them were used to fly the two milk-run civil routes south out of Hanoi to Vinh and Dong Hoi and west toward Na San and Dien Bien Phu (farm animals that couldn't be stowed in the overhead compartment or stuffed under the seat in front of you couldn't be carried on). The other ten Il-14's were sent down by the Soviets especially to be used in the airlift into Laos from the DRV in support of the Communist Pathet Lao.

~~(SC)~~ They also had about a dozen An-2's: single-engine biplanes that look a lot like the crop-duster that chased Cary Grant into a cornfield and then crashed into a fuel truck in Alfred Hitchcock's *North by Northwest*. The An-2 in fact began its career as a crop duster in the USSR in the late 40's, and eventually came to be used in such diverse roles as parachute training, rescue and ambulance work, aerial survey, short-haul passenger runs; you get the picture. The DRV used the plane for all these and more, and some weird things happened with their An-2's. Like the time that the Pathet Lao didn't get the word that a couple of An-2's would be coming over and landing at their site in Laos. The first plane encountered a hail of Pathet Lao machine-gun fire; it took a few hits before aborting its approach and heading back to Hanoi. The second An-2, observing all of this, didn't even attempt a landing. We soon noticed the North Vietnamese being a bit more conscientious about disseminating their pre-flight information to the stations who would be directly involved.

~~(C)~~ By far the weirdest event, though, was to occur years after I left the service [redacted] This was the bombing raid carried out by a couple of DRV An-2's against a TACAN transmitter installed by the U.S. Air Force in 1966 in northeastern Laos. The transmitter, located atop a mountain known as Phou Phathi, was used as a navigational aid by U.S. aircraft, and the North Vietnamese were obviously aware of its importance. Sure enough, on 12 January 1967 they sent a couple of their An-2's over to try and destroy the transmitter. It boggles the mind: biplanes strafing, launching rockets against, and dropping bombs on the site. And get this! Their mission failed [redacted] An inspection of the wreckage disclosed that the Vietnamese had installed launching tubes in the floor of the An-2's and were apparently

[redacted]

EO 1.4.(c)

(U) The DRV often used its biplanes in imaginative ways

dropping their "bombs" by hand through these tubes. Some of the blood-spattered navigational material that the Vietnamese pilots were carrying was passed through our office [redacted] and I was able to get a first-hand look before sending it on to Fort Meade.[3]

EO 1.4.(c)

(U) But my own story mainly involves one of the DRV's Li-2's, those scaled-down versions of one of the most reliable planes ever built: the C-47 (or DC-3 as the commercial version is known). The Soviet Union obtained manufacturing rights for the DC-3 during the World War II era and built over 2,000 of them (designating them Li-2's) between 1940 and 1945. The 25 or so Li-2's that the DRV operated during the early 60's had been sent down by the Soviet Union to participate in the Laotian airlift, but, as with the other planes in their inventory, the North Vietnamese used the Li-2's in a variety of roles.

~~(SC)~~ As we know, the Vietnamese were also very big on doing things the simplest way (remember the hand-dropped bombs and the thousands of loaded bicycles that were pushed down the Ho Chi Minh Trail?), and this extended, in the early 60's, to the numbers and

3. (U) An excellent and engrossing account of the fall of Lima Site 85 was prepared by James C. Linder and published in *Studies in Intelligence*, Vol. 38, No. 5, 1995.

DOCID: 4019611

callsigns they assigned to their aircraft. So it was then that two of their Li-2's and two An-2's had huge identifying numbers painted on their fuselages: numbers 01 through 04. (These four planes were used frequently on missions into Laos to provide an air service into the Plaine des Jarres area, and the large numbers were probably meant to keep the nearsighted Pathet Lao from firing on them.) When communicating, these planes identified themselves by the large numbers painted on their sides and used the simple international "Q" signals to communicate the nature of their activities. "Q" signals were used to indicate departures, arrivals, pass-over points, estimated times of arrival, and the like.

~~(SC)~~ Sometime in the first half of 1962 (or it may have been late 1961), Li-2 01 flew from Hanoi down to Phnom Penh, capital of Norodom Sihanouk's Cambodia. We were monitoring the flight service net that handled the flight and knew when the plane departed Hanoi and landed at Phnom Penh. And then things got strange. In the middle of the plane's first night in Phnom Penh (something like 1 a.m.) the Li-2's communicator used his manual Morse key to send the message (using the international "Q" signal) that the plane had taken off from Phnom Penh. (It looked something like this: "QTA 0100") This was strange because the DRV's planes did precious little night flying in those days and stranger still because we didn't intercept any more communications from the plane that night or see any other indications on the net of where it had gone or what it might have been up to. We also didn't see any confirmation of the plane's landing back at Phnom Penh, although we later detected it leaving Phnom Penh and flying back to Hanoi.

~~(SC)~~ I dutifully reported all of the activity by Li-2 01, including the nighttime departure from Phnom Penh for points unknown. [redacted] also charged with reporting on the activities of the North Vietnamese Air Force, independently reached the same conclusion and reported that the Li-2 had left Phnom Penh that night on an undisclosed mission. It's essential to my story that I point out here that the North Vietnamese on occasion had used the "Q" signal "QTA" to mean "The correct time is _____." That precedent, plus what I knew then of other proclivities of the North Vietnamese pilots, left me with a nagging doubt about what had actually taken place that night. Had the plane actually taken off from Phnom Penh or was the radio operator merely checking communications? But why engage in comms checks at 1 a.m., and why had the Li-2 gone to Phnom Penh in the first place? And after all, I wasn't the only one to report that the plane had departed in the middle of the night.

~~(SC)~~ A lot may not have been made of all of this if, on the morning after the mysterious departure message had been intercepted and reported, an aerial observer in South Vietnam hadn't spotted what he took to be parachute panels on the ground between Saigon and the Cambodian border at a point just minutes flying time from Phnom Penh via Li-2. Putting two and two together, U.S. military intelligence analysts in Saigon concluded that the North Vietnamese Li-2 must have flown from Phnom Penh in the middle of the night, crossed the border into South Vietnam, and paradropped something to the Viet Cong before returning to Phnom Penh.

~~(SC)~~ Well, that did it! Now the stuff had hit the fan! Up to this point, North Vietnamese planes had flown no further south in their support of either the Pathet Lao or the Viet Cong than an obscure airfield at Tchepone, located in the northern part of the Laotian panhandle just about due south of the North Vietnamese port city of Dong Hoi. But now, we apparently have that pitiful North Vietnamese Air Force flying its planes almost into Saigon itself in support of the VC.

~~(S-CCO)~~ Not long after this incident, the U.S. Air Force (of which I was a member, remember?) transferred a C-130 into Saigon, from where it began staging in an attempt to intercept North Vietnamese air communications related to Hanoi's nighttime air supply efforts on behalf of the VC. As fate would have it, I was a Vietnamese linguist and, because there was a shortage of such linguists, my tour in Southeast Asia was extended by 90 days and I was sent to Saigon (involuntarily, I must add) to help man the missions. I was a member of the C-130's back-end crew many nights while the plane made endless orbits over the DMZ separating North and South Vietnam. We never intercepted a single word of voice traffic to confirm that the North was flying missions in support of the VC.

~~(SC)~~ So! Did the Li-2 actually fly that nighttime paradrop mission or was he just transmitting the correct time? And were those really parachute panels that the aerial observer spotted the next morning?

~~(S-CCO)~~ We continued to search for North Vietnamese communications in support of air operations in the south but had found none by the time I left Saigon in October 1962, and the American troop presence in South Vietnam had quadrupled by Christmas. Oh yes! Shortly before I caught my flight out of Saigon for the Philippines and then home, I overheard the following conversation in my tent between a couple of G.I.'s, who, as far as I could determine, were not cleared for any

EO 1.4.(c)
P.L. 86-36

level of intelligence (certainly not codeword).

G.I. #1: Hey man, why is it that the United States is sending all these troops over here?

G.I. #2: Hey, don't you know nothin'? It's because of all them Il-yooshins that's been droppin' supplies to them Viet Congs.

True story.

P.L. 86-36

~~(FOUO)~~ [redacted] *who prepared for his Air Force and NSA careers by poaching game in the hills of east Tennessee as a teenager, graduated from the University of Maryland with a degree in international relations and is now* E.O. 1.4.(c) *recovering in P054 from a stint as* [redacted] P.L. 86-36 *under Gen. Odom. He has served the agency in many capacities since entering on duty in 1963 but intends to retire this summer and devote his time and energies to his newly acquired addiction to zydeco and Cajun music.*

KA

(U) We direct our readers' attention to the second paragraph, which gave us quite a sense of déjà vu. We couldn't have said it better ourselves.:

From the History File: Editorial Comment by Dr. Sydney Fairbanks (U)

(U) So many kind inquiries after the Journal's health have been made of late—stimulated apparently by rumors of its early death—that we take the liberty of being rather specific on the subject. The number of articles promised has roughly doubled with each successive issue, and the mortality from all causes (most of them "classification" difficulties) has been less than one in three. Because it is extremely difficult to get the average article written, independently criticized, checked for security, discussed, rewritten, illustrated and typed in final form, all within three months, we are still operating in an economy of scarcity; but the transition to an economy of plenty, when the articles that were not ready in time for the last issue are enough to fill the next one, may arrive quite soon. When it does, the Journal will be on an adequately firm footing, and we find our progress in that direction gratifyingly rapid.

(U) The difficulties attendant on printing the fourth issue have finally been resolved. We apologize for the delay, and wish to thank our readers for their patience.

(U) Please note that this is not, as would be expected, Volume I, Number 4, but Volume II, Number 1. The ordinary periodical in our situation has to weigh the reasonableness of having the first numbers appear in January against the inconvenience of mailing out form letters for the next century explaining the break in sequence, Because of our limited distribution we hope to escape most of this. Nevertheless: Readers please note: There is NO Volume I, Number 4.

(U) It is impractical to list by name all the kind and patient people who have spent hours in advising us informally on specific points, but without them there would have been no Journal, and we hope they will accept a blanket recognition.

Reprinted from the NSA Technical Journal, Vol. II, No. 1, January 1957

DOCID: 4019611

CRYPTOLOG
Winter 1995

Book Review (U)

High Seas: the Naval Passage to an Uncharted World, by Adm. William A. Owens, USN

pub. 1995, Naval Institute Press, Annapolis, Md.

Reviewed by Col. Richard Szafranski, USAF, National Military Strategy Chairman, Air War College

Reprinted with permission from the Air War College Newsletter, Vol. 20, No. 4, Fall 1995.

(U) Perhaps the most visionary and articulate officer serving in uniform today is the Vice Chairman of the Joint Chiefs of Staff, Admiral Bill Owens. Admiral Owens—along with Mr. Andy Marshall, the director of the OSD Office of Net Assessment and superintendent of the Revolution in Military Affairs (RMA), and Dr. Alvin Toffler, world-renowned author and thinker—also addressed the Air War College Class of 1996 at the beginning of the academic year. A big chunk of Admiral Owens' vision is captured in his book, *High Seas*. That a serving flag officer has the time to write a book is itself wonderful, even acknowledging the help of his assistant, Dr. Jim Blaker. That the book is both useful and good is even better. Its 178 pages are a must-read and a quick read.

(U) *High Seas* gives us insight into the present national security environment and the one that Admiral Owens argues is like to emerge over the next several decades. Using a straightforward analysis and "what's going on here" format, he describes the things the United States armed forces need to worry about in the near and farther future. Major superpower fighting having been averted, the primary danger now comes from what Admiral Owens describes as "regional predators." These are land powers threatening the family of nations by threatening the stability of a region. Because they are land powers, we need to focus more closely on our ability to influence or defeat these land predators. All of our armed forces must attend to the job of supporting land operations. Consequently, he eloquently explains the need for real naval presence—as distinguished from the "virtual presence" of air and space forces described in the Air Force's Global Presence—as a requirement for influencing events on land. Our own "virtual presence" was far less well argued and, to some, much less convincing. Admiral Owens asserts that the focus of naval operations for the foreseeable future is not "sea control" (the "why" of a bank-breaking 600-ship Navy), but on helping control the land from the littoral. The Navy's new vision might be described as "from the sea for battlefield support." The potential predators, he tells us, are all reachable from the sea along the littoral. He is supported in this observation by the historian John Keegan in *The History of Warfare*. Keegan notes that of the fifteen decisive sea battles in the history of the planet, all but two appeared on the littoral. In fact, Keegan notes that the terrestrial battlespace historically resides along the littoral between the tenth and fifty-fifth degree of latitude in the Northern Hemisphere and stretches from 90 degrees west of Greenwich to 13 degrees east.

(U) Because land control and helping deter or defeat regional predators is the new focus of the Navy's operations, Admiral Owens argues that the Navy must better understand Air Force and Army operations. Without saying it directly, he suggests that because the Navy has its own army (our United States Marine Corps) and its own air force (in the form of naval aviation and sea-launched cruise missiles), the Navy constitutes a joint and integrated force by definition. Thus, Naval Expeditionary Task Forces (NETFs) may be, or even are, best suited for influencing the land from the littoral. The NETFs can do this, of course, without reliance on overseas bases, the Achilles' heel of short-

legged, land-based air power. His discussion of strategic bombing campaigns on pp. 96-100 is reasonable and he asserts that "no single service can do this alone."

(U) It is about here that Air Force airmen ought to say "Ahoy!" and reconstruct the logic train car by car: regional predators are the threat, these are land powers reachable from the littoral, the Navy's role is to help win on the land, the NETF has joint and unified forces, the NETF is self-contained and not reliant on overseas bases, and even strategic bombing is a joint activity. So what is the niche, the value added, of a separate Air Force, some of our paranoid airmen will wonder? One answer, of course, is "very little," if we follow the logic train to its unspecified destination. This possibility looms more clearly as he describes the Navy's "Force 2001" and "Force 2021" and the need for real naval presence in four regional areas. He suggests that floating mobile bases (artificial islands) are or could be the power projection bases of the future. He concludes that we control our own destiny and asserts, "We should try to do two things. We should design military forces, and use the ones we have, in ways that do not goad others to challenge us militarily, and we should build military forces that are unchallengeable. These are the basic assumptions on which I founded most of the discussions in this book." The armed forces of the future are a "system of systems" in Admiral Owens's view, and naval forces are a, or even the, key component in such a system.

(U) Is there a hidden agenda here? A more appropriate question is, Is a general or flag officer worth his or her salt without a hidden agenda?" Of course not. Sun Tzu admonished the general to remain "inscrutable." Admiral Owens is, pardon the respectful pun, a salt worth his salt. The hidden agenda, my guess is, is to infuse our "blue water" force with post-cold war relevance by using the end of the cold war to reframe its mission as a "brown water" one, but to make this point in such a way that it's as much "between the betweens," as John Boyd would say, as it is between the lines. Littoral operations will remain important, yet the littoral that counts in the future may be the regions of air and space that surround the planet as much as it is the coastlines of the planet. If the force provider of air and space power is reduced to just another air arm, then there is insufficient justification for preserving it. What I think Admiral Owens misses, as Dr. Grant Hammond of the Air War College has pointed out, is the structural fallacy of the notions of jointness built around the "seamless integration" of land, sea, air, and space. The reality, Hammond asserts, is that there really is a seam between the earth and the aerospace and we can neither define it away nor wish it away. Someone, some force element, has to be expert in operating in and controlling the media of air and space. The Air Force has no desire to be the Navy, and others who are not airmen must trust airmen to be expert about air power, just as we must trust sailors to be experts about ships. Jointness doesn't mean that "you collapse into us." It means "we do this together, but if it's an air or space operation we ought to have the lead."

(U) So I recommend that you read this book and read it very carefully. I would not buy it, but only because it's outrageously expensive for its size. If you disagree with this assessment, feel free to contact me on the Air War College's new Internet connection at **rszafranski@MAX1.au.af.mil**.

Kλ

Letters to the Editor (U)

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

Re: The Future of Cryptanalysis (U)

~~(TS-CCO)~~ [redacted] article in the Fall 1995 issue of CRYPTOLOG—at once thoughtful and incisive—led off with an assessment of the state of the art. He called 1994 "the best year for cryptanalysis since the Second World War." Before his readership got all puffed up with self-importance and began high-fiving everyone within reach, however, he set the tone for the rest of the article with a caution.

[redacted]

~~(TS-CCO)~~ We turn the clock back to 1979. NSA Director Lt. Gen. Lew Allen had charged the Scientific Advisory Board with

[redacted]

[redacted]

(U) The cryptanalytic struggle continues as before; only the names change. The components of success remain the same, and the reasons for failure (lack of resources, security leaks) recur decades running.

Tom Johnson, Center for Cryptologic History (968-6156)

Re: Foreign Language Testing (U)

(U) I would like to comment on an article that appeared in the fall 1995 issue of Cryptolog, Foreign Language Testing at NSA: Time for Change. In it, the author makes a number of inspired recommendations for improving the way language testing is conducted at NSA. However, in doing so the author also makes some assumptions about how the work of PQE committees is conducted, and I believe that not all of these assumptions are valid.

(U) I should point out that I am aware that all PQE committees operate differently, and that many take on their own personality based on their leadership and the level of expertise and enthusiasm of their members. I was a member of a highly motivated PQE committee that counted among its members experienced linguists with advanced degrees in that field. In addition, we had 11 very vocal members who loved to argue and convince their fellow committee members of their point of view. Very few decisions were made that were not unanimous.

(U) With regard to suggestion 1 ("Use, in tests, only those texts for which three or more experts independently agree on the level"), I believe that our committee, all 11 of us, agreed on their level. While all of us took LG-020, Language Levels and Their Application, two of our committee members were also full-time language instructors at the NCS. On a daily basis, they selected texts for classroom use based on their language level, and they were quite good at it. Therefore, we were very confident that the texts we selected for use in our tests were the appropriate level—we had too many checks and balances for this not to be the case.

(U) Suggestion 3 ("Require test designers to "socialize" at the start of each testing cycle, discussing several texts that are in the pertinent foreign language and that have previously been determined to be at the various levels") certainly took place in our committee. We had not one, but two or sometimes three meetings to select an appropriate text, discussing a number of samples each time. In addition, we discussed samples that had been put forth in previous rounds, to be sure that we were selecting the best available text. Again, the personality of this committee, and the committee leader's commitment to let every voice be heard may have played a role in the extent of socializing that our committee undertook.

(U) I agree with the author's contention that an analyst's inability to render a text in "idiomatic English" may sometimes be the reason for failing to pass a PQE. However, our committee invited every analyst who took a PQE to meet with a member of the committee for a counseling session. I believe that our committee members were astute enough to determine whether an analyst was having difficulty understanding the foreign language or rendering it in English, and if not, then such a counseling session would have revealed such deficiencies. During the course of the counseling session, the committee member could recommend that the analyst enroll in either another language course or an English writing course, as we often did. Also, when analysts at field locations took PQEs, our committee was required to send them a detailed analysis of their exam, including areas needing improvement. We often recommended in these analyses that analysts seek to improve their English writing skills in addition to their language skills.

~~(S-CCO)~~ I also must comment on the author's assumptions about the scoring of translations. I maintain that syntactical errors are indeed more costly than lexical errors, which is why more points are deducted for this type of error. In the example "the dog / bit / the man" versus "the man / bit / the dog" the nouns are, as the author points out, in the wrong relationship to the verb. However, this error becomes much more egregious when an analyst is drafting a SIGINT report and mistakes "Ecuador / attacks / Peru" for "Peru / attacks / Ecuador." Simply being in the wrong relationship to the verb has rendered these nouns on the complete opposite sides of a war—too costly a mistake to be made by a supposedly "certified" analyst who passed his PQE.

(U) In addition, I disagree that mistakes on repeated instances of the same word should be penalized more than once. One of the advantages of having a long testing period for PQEs is that analysts thus have an opportunity to go back and

reread their translations. A careful analyst will note these translation discrepancies and go back and change previous occurrences of the word. But a misunderstood word that happens to appear more than once in a text should not be repeatedly penalized.

(U) I do appreciate the author's suggestions for improving the PQE system. However, some aspects of the system are not broken. Certainly better training for PQE members would help, but my experience with a PQE committee introduced me to a whole team of energetic, motivated individuals dedicated to improving the quality of certified linguists at NSA.

P.L. 86-36 [redacted] B051

[redacted] A905, responds:

(U) It is heartening to learn that the language PQE committees have so many motivated and capable people who are sincerely trying to follow good test design procedures. I agree with [redacted] that not all aspects of the PQE system are broken. Her comments, however, reflect a misunderstanding of some of the points I covered in my paper, and I welcome this opportunity to clarify these.

(U) The first point she addresses is the selection of texts for use in PQEs. She describes a process in which "vocal members . . . argue and convince their fellow committee members of their point of view" as to text level. This is not independent decision-making; true independence means that everyone comes to the same conclusion on their own, without having to be convinced or cajoled. It is unlikely that all members of a given committee will be equally outspoken or equally adept at getting their way, thus there is a danger (especially on committees smaller than the one she describes) that one or two dominant personalities will sway decisions to their viewpoint, for good or for ill. The "unanimity" thus gained may lead to a false confidence in the final decision. On the other hand, when several people arrive at the same conclusion without debate, they have a more solid basis for confidence in the outcome.

(U) As for diagnosing the causes of poor test performance, I would simply point out that not all aspirants avail themselves of the opportunity to receive counseling. Moreover, it is questionable whether all those who act as counselors (1) are able to make such diagnoses during the counseling session and (2) always attempt to do so. It would be much more desirable to have a testing program in which diagnostic information is obtained through the tests themselves.

(U) Regarding the scoring of translations, [redacted] example of a possible syntactic mistake serves only to demonstrate that this type of error can sometimes be serious. I provided examples in my paper of actual mistakes from my test data, which show that syntactic errors are sometimes NOT so crucial, and that lexical errors sometimes ARE. Lest this deteriorate into a my-anecdote-is-better-than-your-anecdote sort of shouting match, let me reiterate that there is no empirical data to support our current translation scoring system, and I find no sound basis in current linguistic theory for assuming the absolute primacy of the grammar over the lexicon. It is axiomatic to psychometricians that it is irresponsible to base testing decisions on intuition alone; the choice of a scoring system is no exception to this. (These comments also apply to the issue of whether or not to penalize repeated mistakes on the same word.)

(U) I hope that PQE committee members will continue to work to ensure fairness in language tests at NSA. The good in our testing system should not be ignored, but neither should we shrink from questioning our current procedures. This honest questioning should not be seen as disparaging to anyone now involved in language testing, most of whom are, as [redacted] rightly points out, "energetic, motivated individuals dedicated to improving the quality of certified linguists at NSA."

Kλ

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019611

SIGINT Bloopers (U)

(U) Having warned against excessive dependence on spell-checkers, we find ourselves with a new category that appears to be a variation of the Homonym Pitfall, but resulting from *not* using spell-checkers: Writing Wrongs. Such as:

(U) "Negotiations faultered over the issue..."—Wonder whose falt it was?

(U) "Possible Presense of Commandos Noted"—is a "presense" some kind of ESP?

(U) One country has "charged that U.S. hypocracy was increasing." Let's see, would this be government by injection, or by Madison Avenue ad-men?

(U) This column, having condemned the use of "diffuse" for "defuse," should probably accept responsibility for confusing one office into producing a brand-new word, "disfuse," instead: "Officials attempted to disfuse a tension ..."

(U) In the "But I Ran Spell-Check!" category:

(U) A country allegedly began to "access" its chances of joining an international organization. (Wonder where they keep those chances?)

(U) Elsewhere, a government crackdown "served as a lightening rod for international condemnation." Lighten up, guys, or we'll use this rod on you.

(U) Another report warned that the security situation was still "dangerous and very unpredicatable." Ever tried predicating a situation? (Kids: don't try this at home.)

(U) One staff office issued an action memo explaining that "Our tact here is to avoid any potential surprises." Must have been from the Agency's Tact Force.

(U) A field site reported on the deployment of "fixed-wind aircraft," which apparently defy the laws of physics.

~~(C)~~ Perhaps we are too severe in our dislike of neologisms, but we really must protest against the proliferation of the prefix "narco-" in reports and collateral relating to drug activity (strictly speaking, to use "narcotics" for marijuana and especially cocaine is inaccurate, but that's a subject for another column). A few Selections From The Narcodictionary:

~~(TSC)~~ "The jailed narcojournalist, whose role in the narco-cassette case..." (Are narcocassettes those tapes of music that require a Parental Advisory sticker?) This gentleman's documentation of rampant "narco-corruption" led to the embroiling of his nation's president in what has been dubbed the "narcodollar scandal." It must have been widespread, considering the employment of "narcosubmarines" (the mention of these vessels always makes a certain '60s tune run through our heads). On another continent, "narcoviolence" was feared when the well-known "narcotraffickers" metamorphosed into "narcoinsurgents." But our favorite has to be the dubbing of a now-departed Caribbean-nation junta as "narco-putschists."

~~(C)~~ On a tangent, one office issued a summary of "counter narcotics activity" using "counter narcotics" as two words throughout. Perhaps these are those narcotics available without a prescription.

(U) Of course, NSA is not alone: State Department bestowed on Emile Jonassaint, puppet head of the government proclaimed by the Haitian military, the title of "Faux President." (For some reason, though, Aristide was never referred to as Le President Actuel...)

(U) A State Dept. cable rerfers to an act of sabotage being "against Islamic valves." Presumably these valves are not metric.

(U) We all live in a narcosubmarine

As before, thanks to all contributors; examples may be sent to P054 in Rm. 3E027, Ops. 1, or via e-mail to **cryplog@p.nsa**.

ΚΛ

Editorial Policy:

(U) Technical articles are preferred over those relating to management, shorter over longer (under 3,500 words). Emphasis should be on improving NSA's technical performance; articles should be aimed at explaining developments in one's career field to thos outside it. Readers are invited to contribute conference reports and reviews of books, articles, software, and hardware that relate to our missions or to any of our disciplines. Editorials are also welcome, as is humor. Submissions may be published anonymously, but the identitiy of the author must be known to the editor.

Submitting Articles:

(N.B. If the following instructions are a mystery to you and your local ADP support is no help, please feel free to contact the CRYPTOLOG editor on 963-3123s or cryplog@p.nsa.)

~~(FOUO)~~ Send a hard copy accompanied by a labelled diskette to the editor at P054 in 3E027, Ops. 1, or send a soft copy via e-mail to **cryplog@p.nsa**.

Guidance:

For maximum efficiency (as far as possible within the limits of your word processor):

- Do not type your article in capital letters.
- Classify all paragraphs
- Label all diskettes, identifying hardware (operating system: DOS, UNIX), density and type of word processor used, your name, organization, building, and phone number.
- FrameMaker format is preferred; ASCII text is also fine. J334 has a conversion service that converts Interleaf, WordPerfect, OfficeWriter, and MS Word into FrameMaker. Just attach the document to an E-Mail Compose Window addressed to **convert@nsa**.

DOCID: 4010113

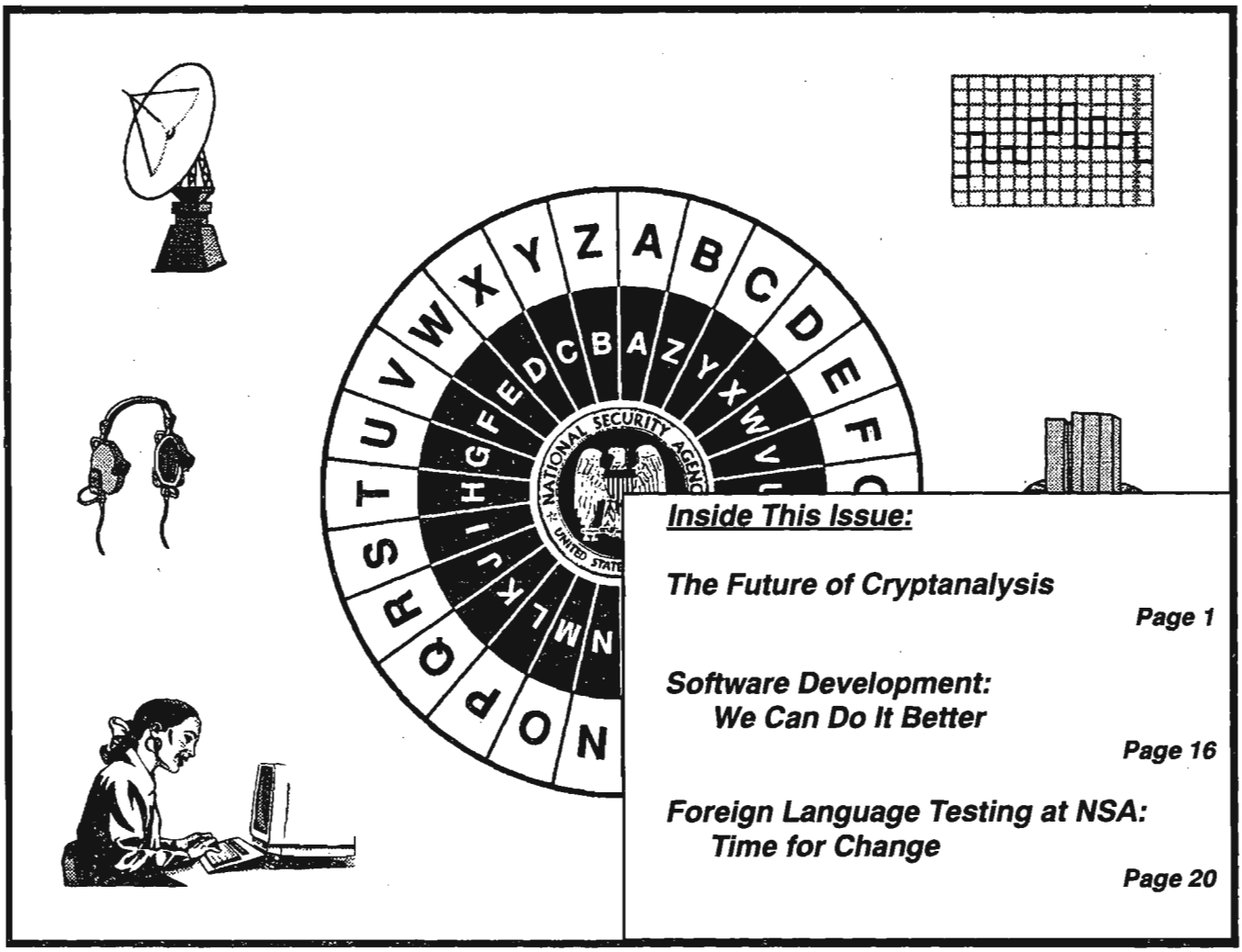
~~TOP SECRET~~

NATIONAL SECURITY AGENCY

CRYPTOLOG

The Journal of Technical Health

Vol. XX, No. 3 FALL 1995



Inside This Issue:

The Future of Cryptanalysis ***Page 1***

Software Development: We Can Do It Better ***Page 16***

Foreign Language Testing at NSA: Time for Change ***Page 20***

~~Derived From: NSA/CSSM 123-2 Dated 3 September 1991~~
~~Declassify On: Source Marked "OADR" Date of source: 3 Sep 91~~

Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~
~~TOP SECRET~~

DOCID: 4010113

P.L. 86-36

CRYPTOLOG

Fall 1995
Vol. XX, No. 3

Published by P05, Operations Directorate Intelligence Staff

Publisher ..... William Nolte (963-3123)

Editor ..... [redacted] (963-3123)

Board of Advisors

Chairman ..... [redacted] (963-7712)
Computer Systems ..... [redacted] (961-1051)
Cryptanalysis ..... [redacted] (963-7243)
Intelligence Analysis ..... [redacted] (968-8211)
Language ..... [redacted] (963-7667)
Mathematics ..... [redacted] (963-1363)
Signals Collection ..... Robert E. Baker, H117 (963-5717)
Telecommunications ..... [redacted] (996-7847)
Member at Large ..... [redacted] (968-4010)
Member at Large ..... [redacted] (968-4010)
Member at Large ..... [redacted] (961-8214)
Classification Officer ..... [redacted] (963-5463)

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

To submit articles and letters, please see last page

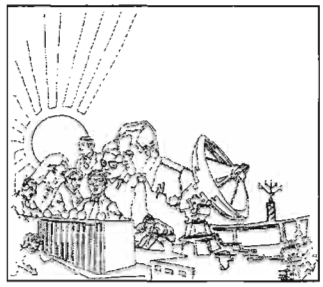


Table of Contents

The Future of Cryptanalysis, by [redacted] *1*

Machine Translation, by [redacted] *5*

Software Development: We Can Do It Better, by [redacted] *16*

Foreign Language Testing at NSA: Time for Change, by [redacted] *21*

SIGINT That Matters: What's the Angle? by [redacted] *30*

SIGINT and the Information Explosion, by [redacted] *34*

Book Reviews:

Recent Publications on Information Warfare, reviewed by [redacted] *37*

China's Air Force Enters the 21st Century, reviewed by [redacted] *39*

Lessons Learned [redacted] *from N25's data base* *41*

SIGINT Bloopers *43*

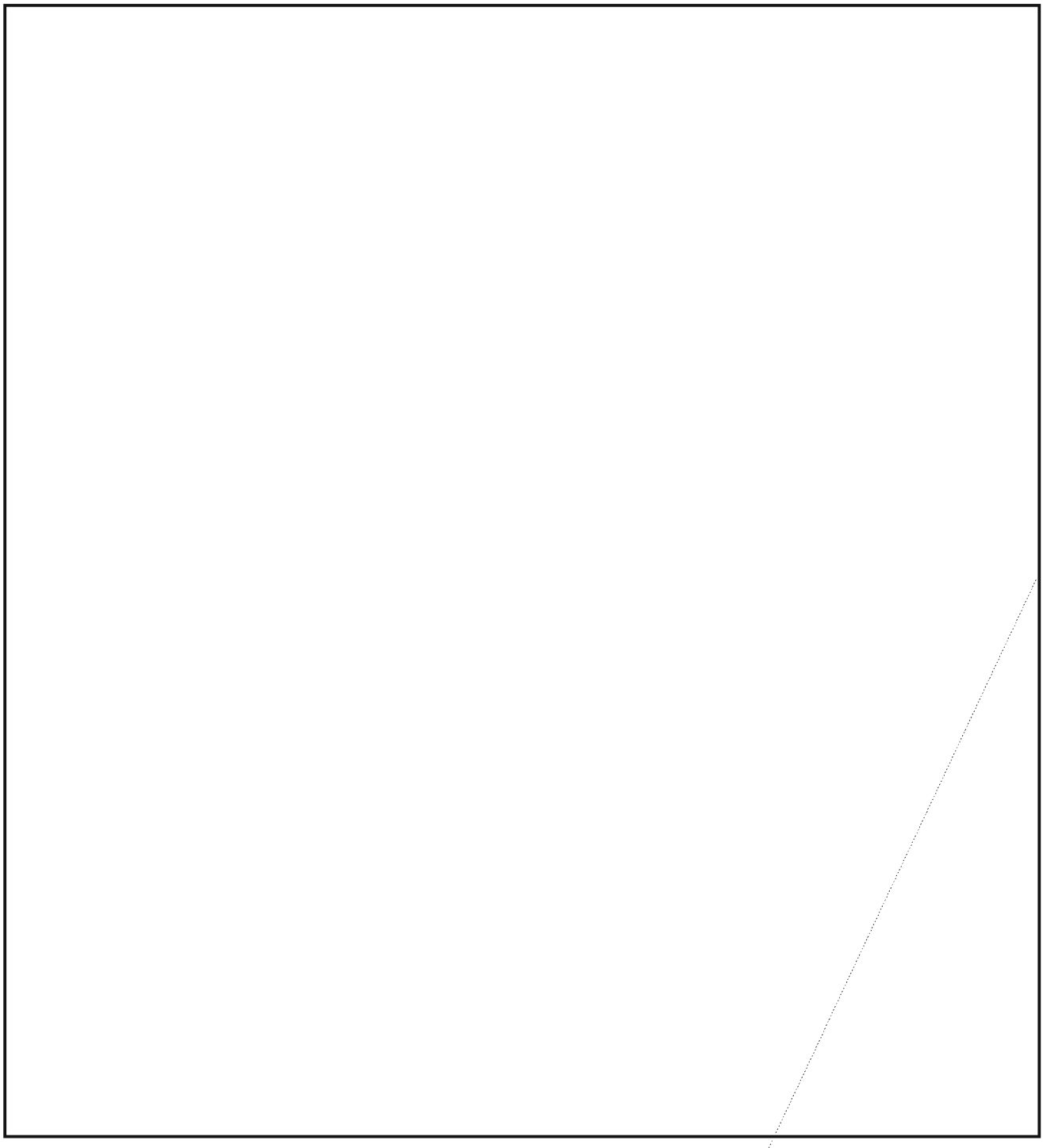
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

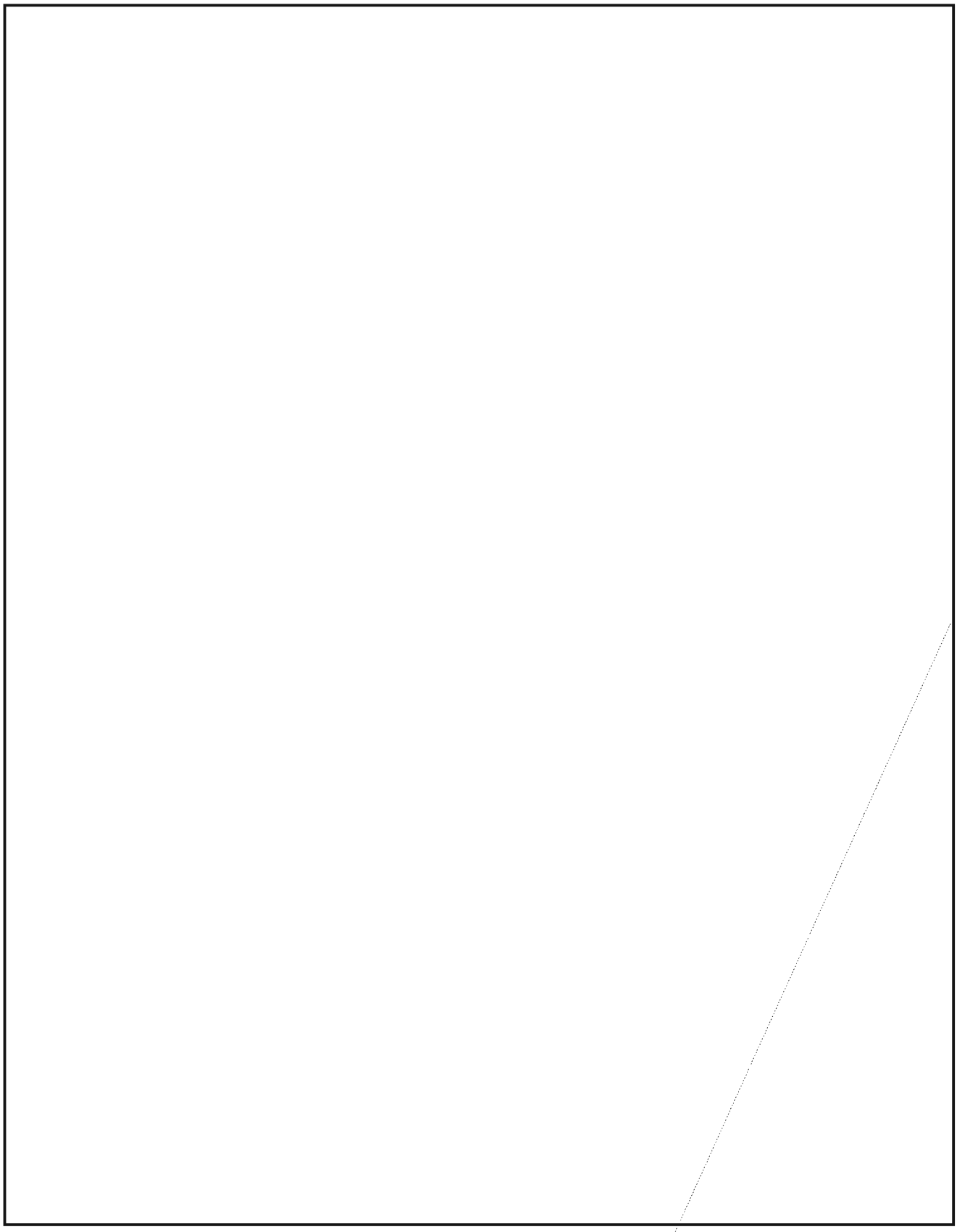
The Future of Cryptanalysis

by [redacted] Chief Z

P.L. 86-36



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

EO 1.4.(c)
DOCID: 4010113 E.O. 13526
P.L. 86-36

Tech Trend Notes publishes a Calendar of Events sponsored by NSA, academia, and professional associations. Here's a sample of what's happening:

Event	Date	Location	Where to call:
Defense Information Warfare Symposium	11-12 Dec	New Orleans, LA	(703) 681-1346
4th Intl. World Wide Web Conference	11-14 Dec		Web site: URL: http://www.crs.lcs.mit.edu/registration-form.html
RSA Data Security Conference	17-19 Jan	San Francisco, CA	(415) 595-8782
DoD Photonics Conference	26-28 Mar	McLean, VA	(703) 631-6128
TechNet Canada '96: "Gov't. and Industry Info Exchange"	17-18 Apr	Ottawa, Canada	(613) 563-0093
Eurocrypt '96	12-16 May	Zaragoza, Spain	email: sec96@aegean.ariadne-t.gr

Reinvention Laboratory for SIGINT Reporting

NO MORE DEFAULTING
TO THE OLD, ENTRENCHED WAYS OF DOING BUSINESS
(" . . . the way we've always done it . . . ")

Officially designated as a reinvention lab (a product of the "reinventing government" initiative), P054 has been given the go-ahead to undertake experiments in reporting. In a continuing search to identify more effective ways of getting SIGINT to customers, P054 will use the ***SIGINT Digest*** and NSA Broadcast Network as test-beds for trying out new reporting styles, content, and dissemination methods, with potential future application by Agency reporting elements.

Your suggestions are welcome.
Please contact [redacted] P.L. 86-36
acting Research Director, at 963-3123s.

MACHINE TRANSLATION:

What can it do for us?

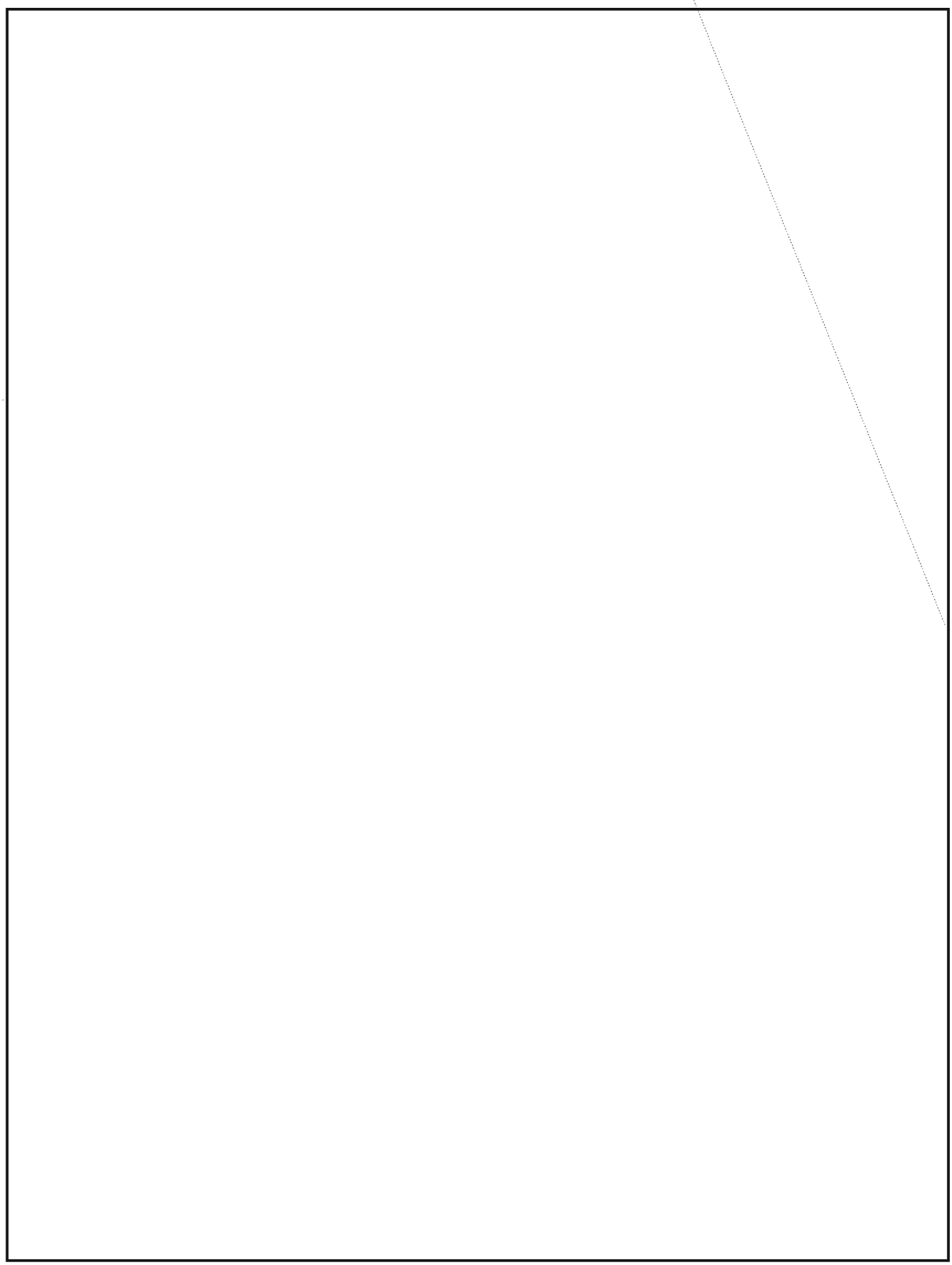
by [redacted] P.L. 86-36

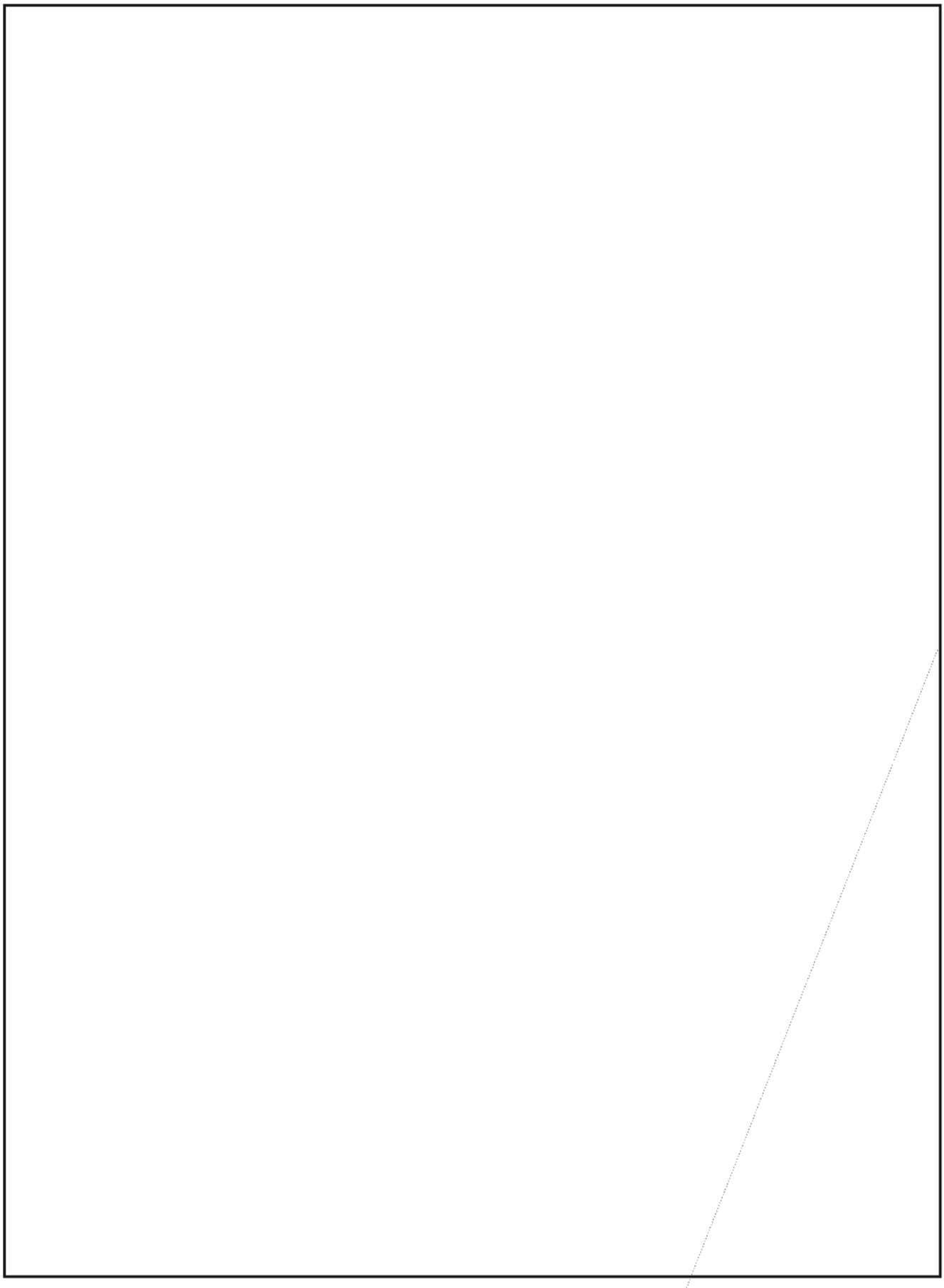
[redacted]

EO 1.4.(c)
P.L. 86-36

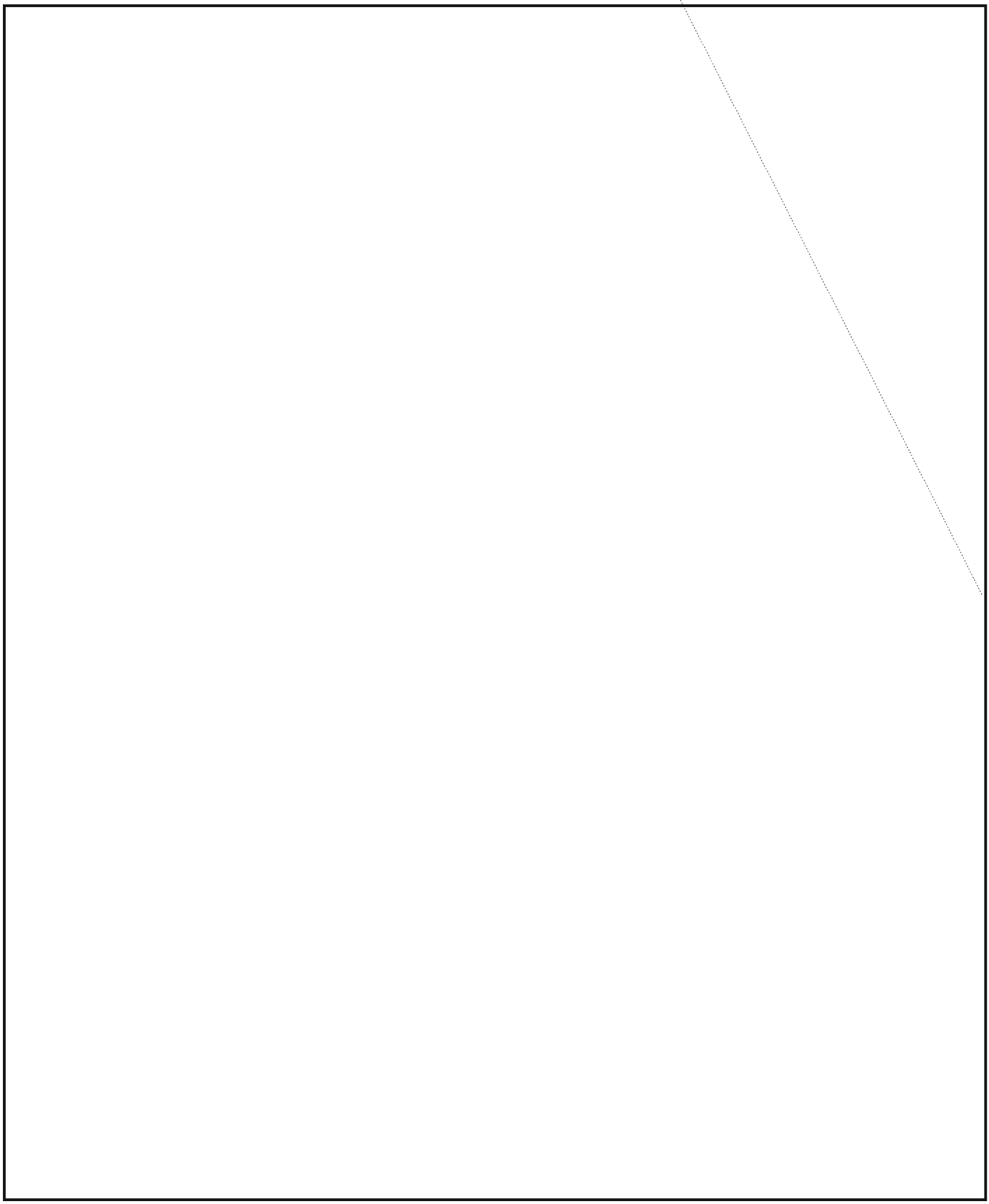
~~TOP SECRET UMBRA~~

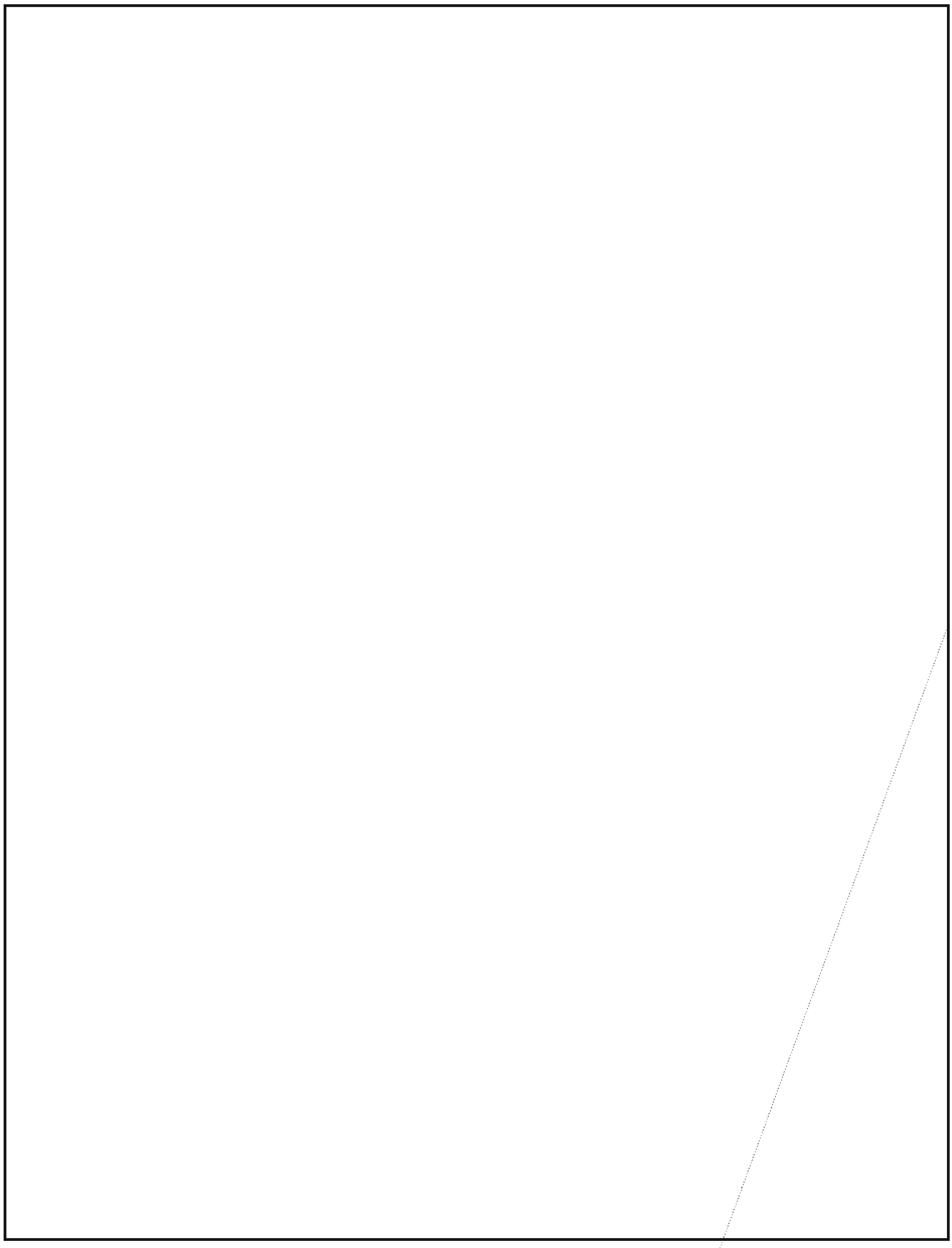
EO 1.4.(c)
P.L. 86-36



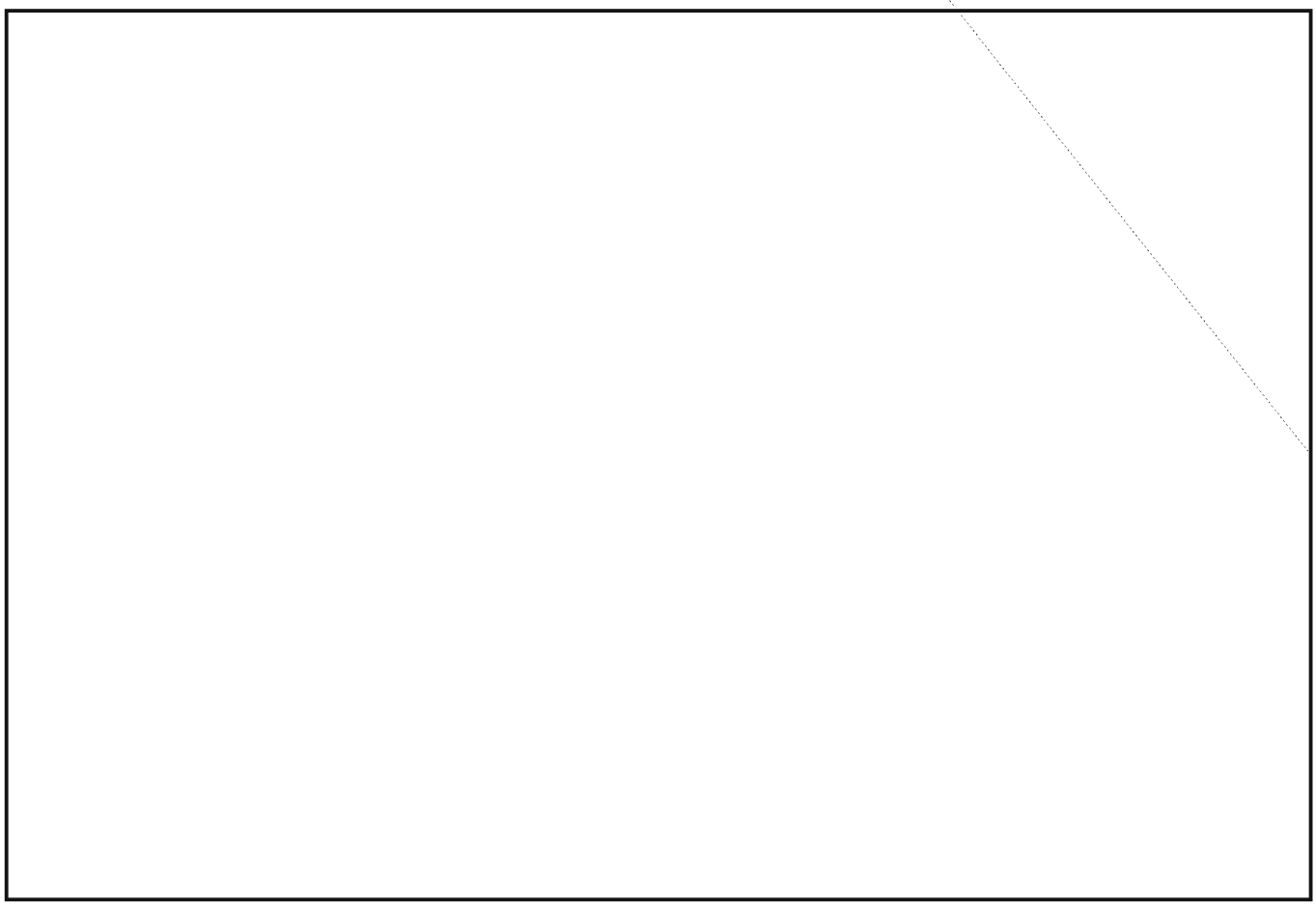


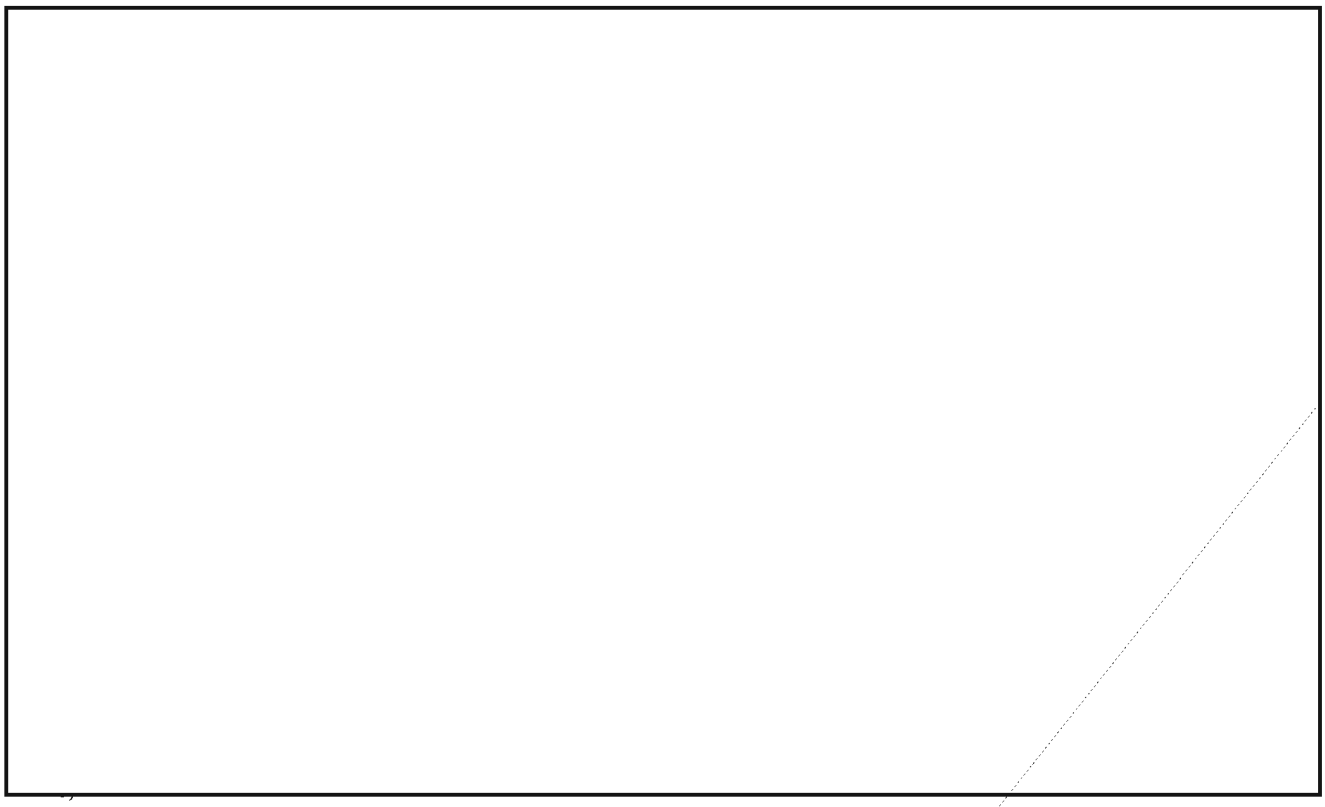
P.L. 86-36
EO 1.4.(c)



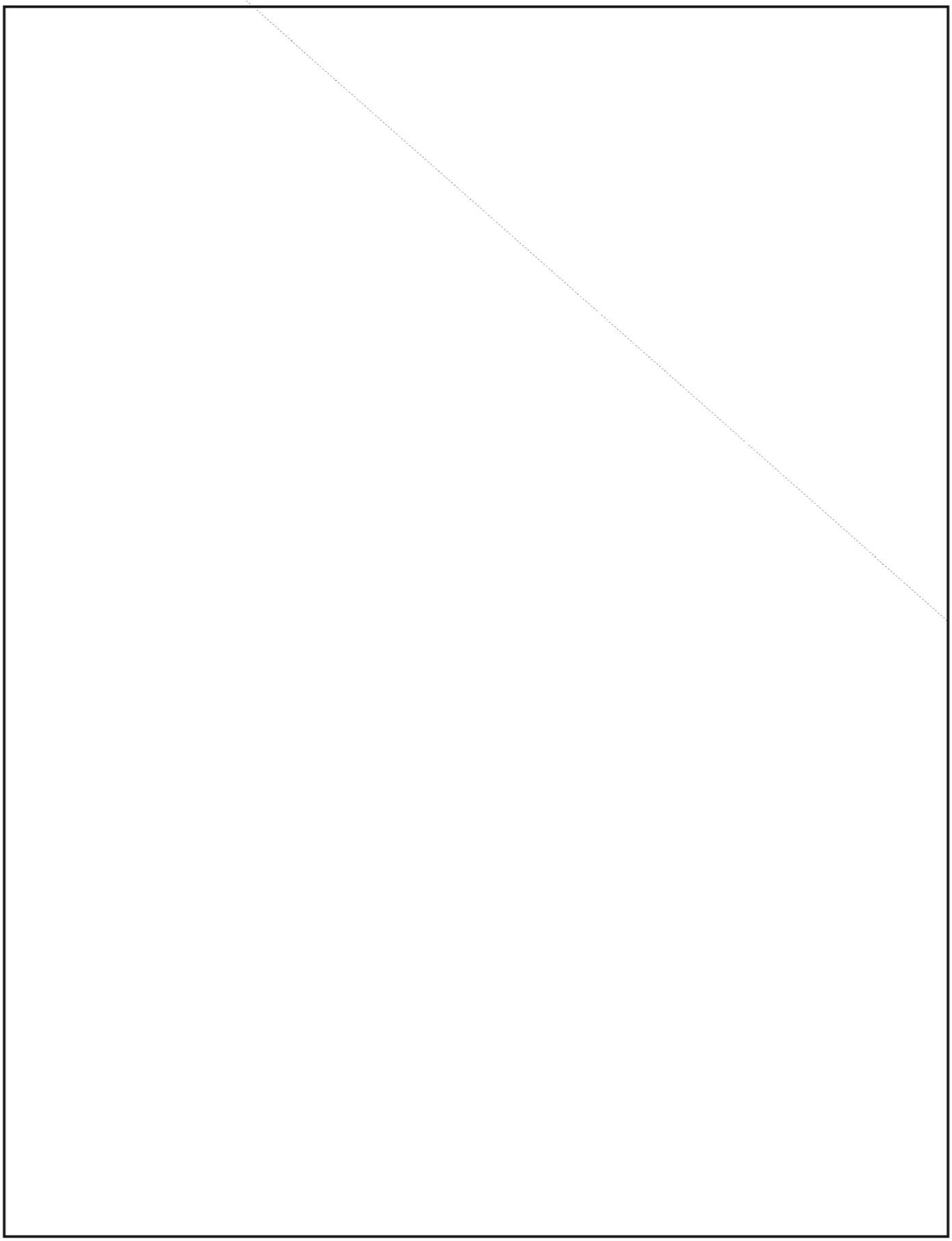


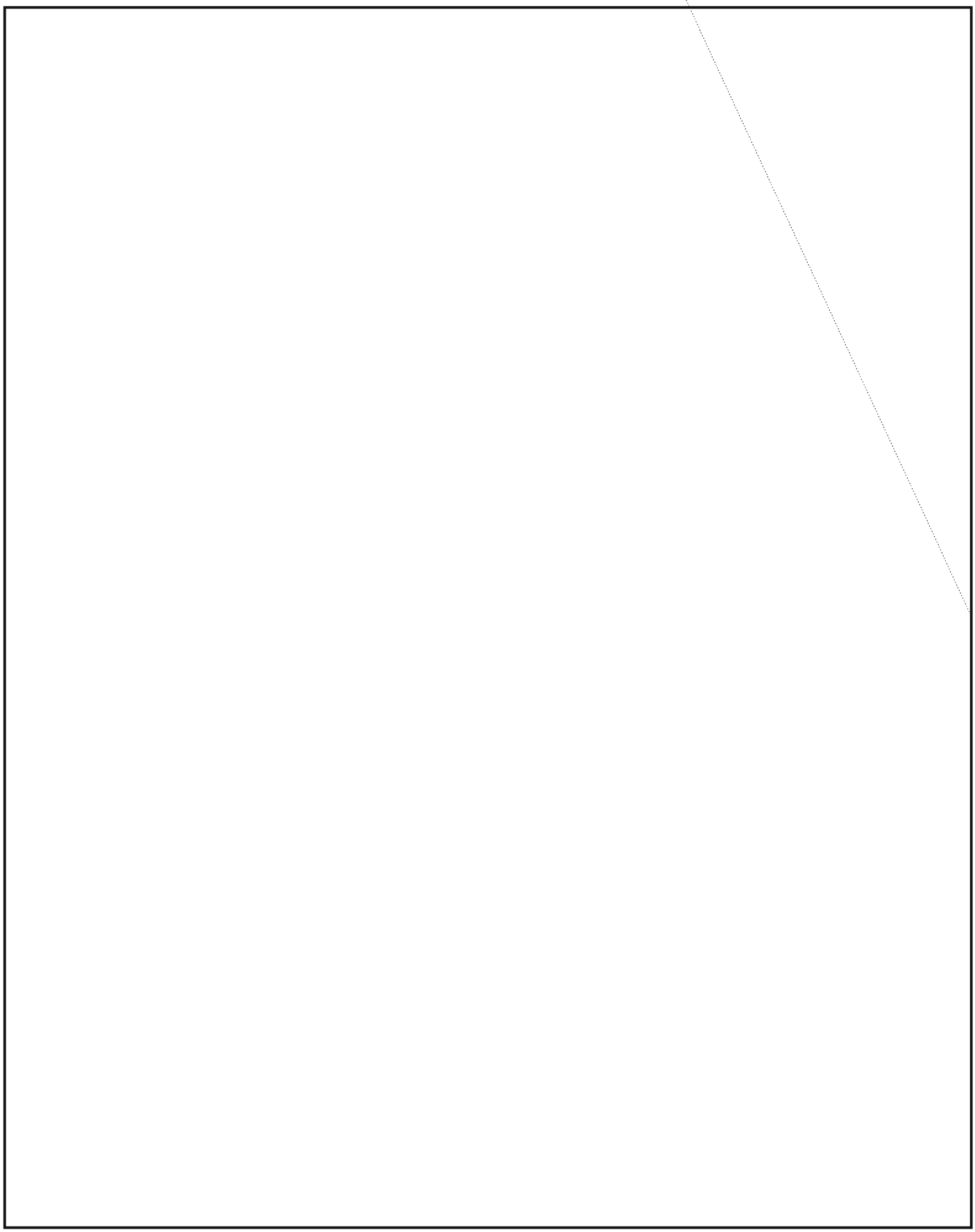
P.L. 86-36
EO 1.4.(c)



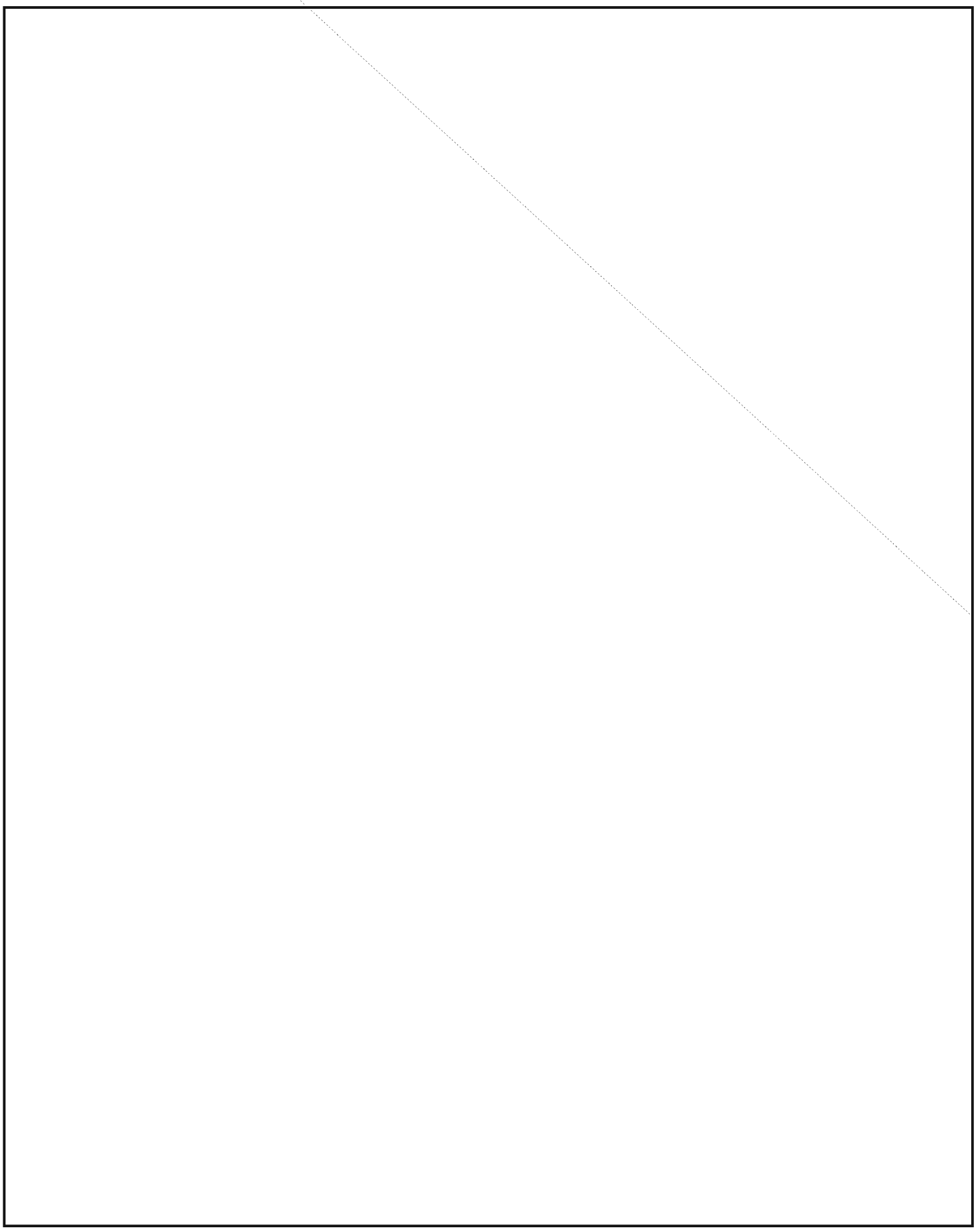


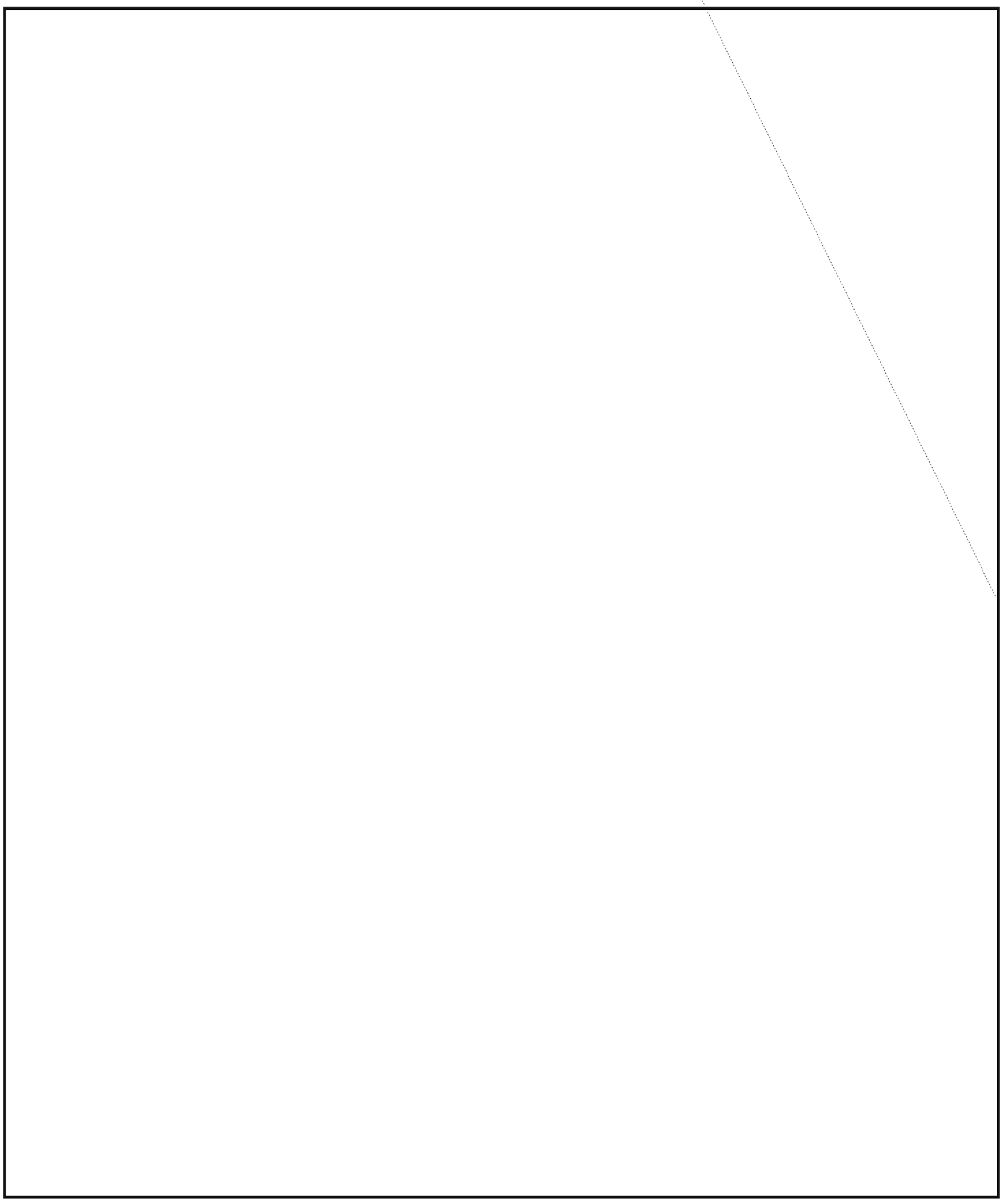
EO 1.4.(c)
P.L. 86-36
DOCID: 4010113

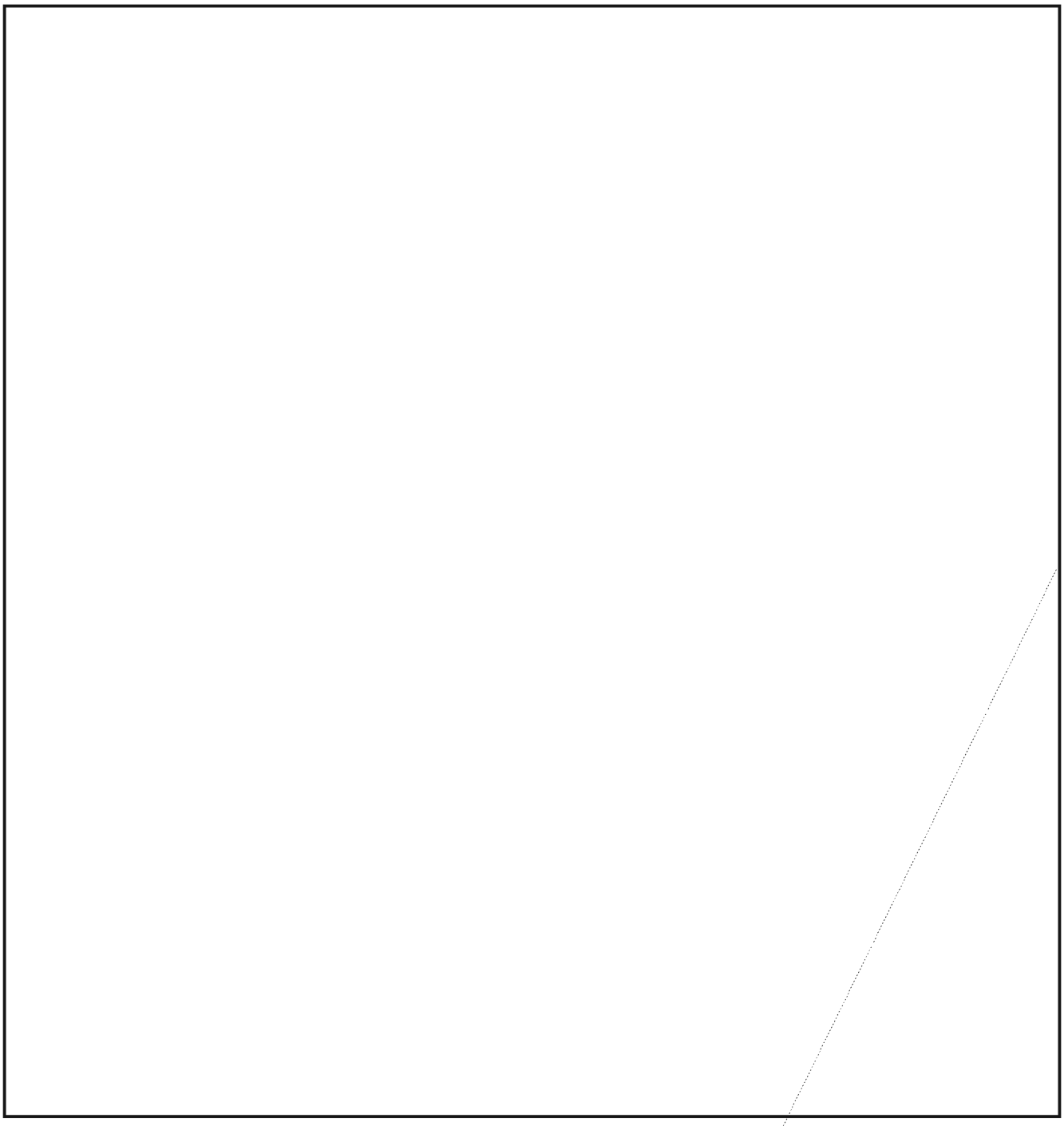




DOCID: 4010113 EO 1.4.(c) P.L. 86-36







P.L. 86-36
EO 1.4.(c)

CRYPTOLOG
Fall 1995

Software Development:

We Can Do It Better—and Faster

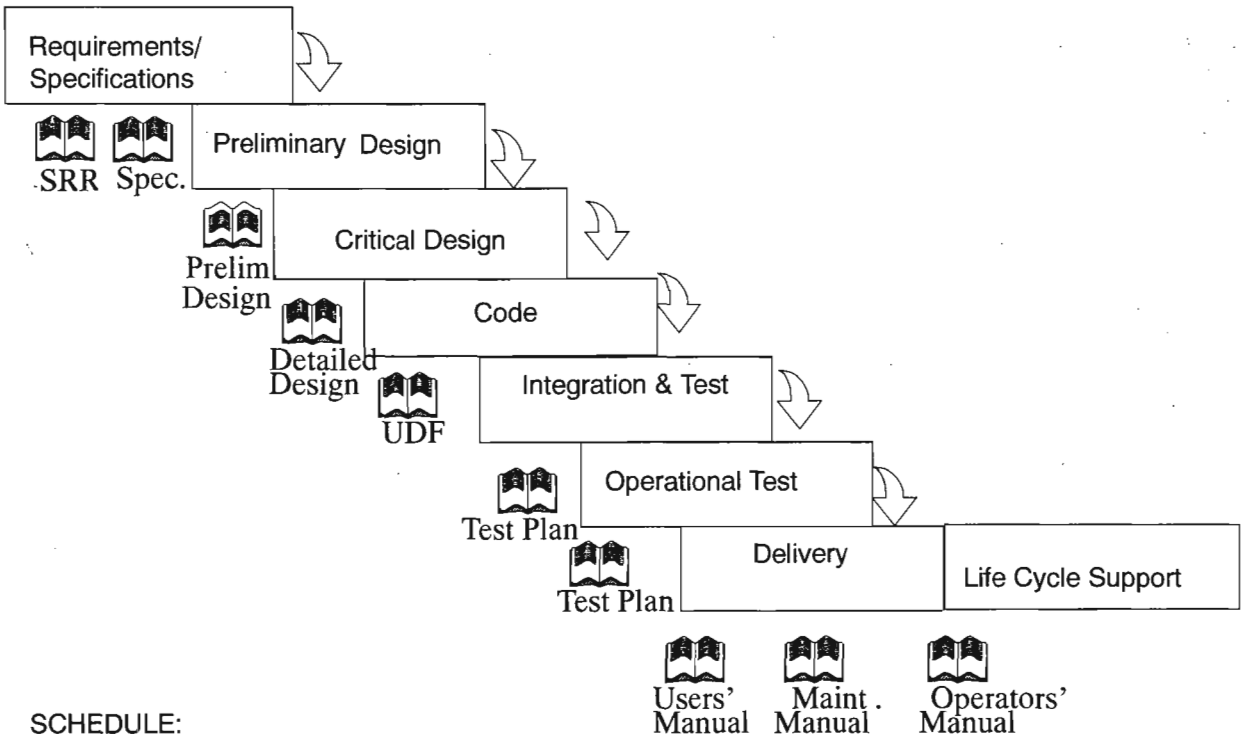
P.L. 86-36

by [redacted]

(U) I believe we can develop better software, deliver it faster and save almost 70% of the cost by changing our acquisition and development methods to what I call "continuous" development. We already do some development this way; we call it maintenance.

(U) In the early days, programming was an art. Programmers were regarded as temperamental artists who produced dense code that was incomprehensible to other programmers, and even themselves after a couple months had elapsed. (As a humorous signature block on the Internet put it, "Real programmers don't document; if it was hard to write, it should be hard to understand.") Development schedules and costs were unpredictable. Code was difficult to maintain. There was no discipline in the process.

(U) Today's software acquisition process, based on a fear of failure, is at the other extreme. Systems analysis and systems engineering principles are applied, and have become disciplines of their own apart from programming. There is great emphasis on reviews and documentation trails to demonstrate that the acquisition manager has done everything that should be done. Each step must be completed, reviewed and approved before proceeding. The goal is to bring order and predictability to the process, to produce code that can be understood and maintained by other programmers, and to produce documentation that will both guide the development and guarantee maintainability over the life of the system. The diagram below shows the essence of this method—often referred to as the Waterfall Method.



(U) A lot of common sense is embedded in these steps. Surely it makes sense to understand and document what you are going to build before you build it. And all the interested parties need to sign up that they agree with the statement of what needs to be built. Likewise, it makes sense to design the system at a top level before proceeding to more detailed levels of design. Like drawing a picture, you can keep the proportions in line if you roughly block out the picture before working on the details of any part of it. If you don't block the design out first, you run the risk of re-creating the old sign we all know and love.

THINK AHEAD

(U) Surely testing is a necessary step. All these steps are necessary. It's plain common sense that disaster would ensue if one of them were omitted. What, then, are the problems?

(U) Let's examine how the process goes astray. The typical acquisition starts out with a year or so of planning activities. Along with starting up the 25-5 paperwork to gain project concurrence and approval, there is a widespread effort to gather all the requirements for the system from the user population. The typical approach to development calls for a set of requirements that are common, consistent, complete and set in concrete. A lot of effort is spent in the process of gathering and coordinating the requirements. Generally, real users do not participate in this process. They are busy doing their jobs, they do not speak "requirement-ese", and they are often cynical about "wasting their time" on a development unlikely to succeed—success being defined as delivering a system the user likes within budget and on schedule. Thus requirements gathering usually is turned over to pseudo-users (user representatives, customers, customer representatives, etc.) who try to specify each capability that will be needed over the life of the system with enough detail that it can be turned into a testable system specification. It can take many months to generate the requirements document. The accepted understanding that a requirement not specified at this time cannot be added later leads to over-specification of the requirements. Requirements that are not fully understood and perhaps not necessary are specified anyway, because of this "now or never" philosophy. When the development runs into trouble, as these developments inevitably do, the requirements process is correctly blamed.

(U) The fix is to realize that the problem was over-specificity, not under-specificity. The development did not fail because some crucial requirement was overlooked. It failed because there were too *many* requirements. There is no good way to sort out the really important requirements from the "nice to haves". In addition, the sheer volume of the number of requirements contributes to the difficulty of understanding them. They are indigestible because of their mass.

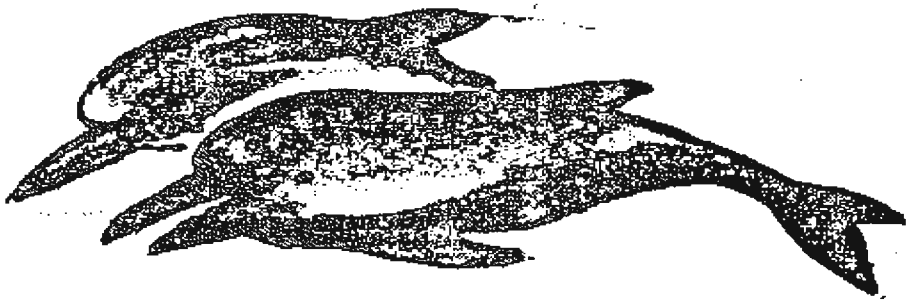
(U) When I was a very junior computer scientist years ago, a co-worker and I were faced with the task of writing the requirements document for a contract. We knew perfectly well what the job was, and could have drawn the top-level design given a moment's notice. Struggle as we might, we could find no way to preserve and communicate our understanding of the problem while using the format required for the Requirements Document. When we finished, the document was incomprehensible even to us, although we had carefully double and triple checked that all the requirements were correct and were included. I think we were both very glad an experienced contractor, who knew how to deal with that mess, was the recipient.

(U) Of course the contractors don't have any magic either, especially when they are unfamiliar with the subject matter of the contract. They have difficulty understanding the big picture of what they need to build and how the system will be used operationally. Imagine trying to assemble a bicycle the night before Christmas without any concept of what a bicycle is—or even the picture of the bicycle on the front of the package. In fact, we religiously keep the picture of the bicycle from the developer because that would imply "a design" and we must give them pure requirements untainted by design assumptions.

(U) Developments usually have a step called System Requirements Review (SRR), which intends to embody the wise practice of "repeat the task back to me so that I can be sure you understood it." Unfortunately, the SRR document that is the medium of communication is as unintelligible as the Requirements document it responds to. Furthermore, the process is hindered by the program review format. Large documents are mailed out to the SRR audience a week or so before the review. Reviewers come to the SRR documents fairly cold and have the monumental, if not impossible, task of comprehending several linear inches of documentation while continuing to perform their other job duties (after all,

they have not just been sitting on their hands doing nothing while the contractor produced this document). The review itself generally consists of several 8-hour days spent presenting viewgraphs of the material in the documents. From the contractor's point of view, the review is a success if no large problems are discovered. Even if they are, there is no time in the schedule for going back to re-do this step, so the plan is to fix the problems later. The result is that after SRR, the developer is free to proceed with the next step of Preliminary Design. And so it goes through the Preliminary Design Review, Detailed Design Review, Test Plan Review. The problem is that the model does not fit how humans think and communicate:

(U) Continuous development consists of breaking the job into small manageable releases. Each release should be a simplified working version of the whole system. We often talk about peeling the onion. Continuous development is like *building* the onion layer by layer. Start with the essential core processes in simplified form and build the framework. Refine and elaborate on that framework in subsequent releases. Each release should accept real data (modify some other data or simulate if you have to) and put out real data in real formats or displays. It should be given to real users to try. If it cannot be used operationally in the early stages, then users should be able to run it for evaluation. My experience is that there are typically four to five releases before the system has all the capabilities originally envisioned. Developer foreknowledge that several more releases are necessary on top of the first one works magic in producing a maintainable design with reduced integration problems. If the design is not maintainable, the developer will learn rapidly on the next release. It is a self-correcting situation. Also, by building the whole system in the first release, they will have had to integrate all the parts. Subsequent deliveries will modify and enhance the already-integrated pieces. You avoid many, many problems by integrating early while the pieces are relatively simple. This is a fundamental strength of continuous development.



"Although humans make sounds with their mouths and occasionally look at each other, there is no solid evidence that they actually communicate among themselves."

(U) The SRR steps *are* necessary, they are just overdone. They are also necessary for the life-cycle-support phase following the development cycle. So, the traditional method actually divides the work into two phases, development and life-cycle support, and maintains the fiction that the life-cycle support phase just fixes minor bugs and keeps up with new releases of the operating system. The constant emotional wrangling at most Configuration Control Boards about whether to call the new work fixes, enhancements, or new requirements should be a clue that reality and the model do not match. There is really one extremely large development cycle followed by numerous smaller development cycles. Why don't we get smart, forget this fiction about "development $\neq$ maintenance", and just develop the whole thing incrementally?

(U) Incremental or continuous development is a model that *does* fit the way humans think and communicate. All of the same steps necessary in the traditional waterfall development are present in continuous development, but in a smaller scale. No one can design without knowing the requirements they are going to address. No one can code without some concept of a design. But the continuous development runs through the waterfall steps for each delivery. There is no separately identifiable maintenance phase, just smaller deliveries as requirements taper off.

(U) The development should try to concentrate on the hard part first. If the hard part is keeping up with a high volume of input data, the developers should concentrate on the parts of the system that deal with the data volume first and go with simplified user graphics until later releases. This is in sharp contrast to most acquisitions, which typically commission studies of the hard parts. For the same amount of time and effort consumed by a paper study or even simulation, you can have real working software that can be run and measured. One can find the bottlenecks and fix them. Even if the software fails (which I have never seen), you learn much more from the software than would have been possible from the study or simulation.

(U) Each release should be built and delivered quickly: in six months or less. This may be the most important rule. It guarantees that the development cannot go too far astray before everyone knows it. No more going directly from "everything is green" to large overruns and delays.

(U) Software is truth; it is not vaporware or shelfware. It either works or it doesn't, and it is there for everyone to see. This is enormously motivating for developers. Anyone can size a six-month effort: a couple of weeks of understanding the requirements and design, maybe four months coding, a month or so of testing and documentation, and a couple of weeks to allow for slips. A pass/fail grade will be delivered before anyone can move on to another job. And people will work incredibly hard and become inspired in their efforts to avoid failure.

(U) *The team must be small, usually four to seven people.* This follows naturally from the small rapid deliveries. You cannot put fifty people on a six-month piece of software. The benefits of the small team are that real communication is possible and each team member has a good understanding of the whole system and how all the pieces fit. This enhances the quality of the design. The system must be designed as a whole and the designers, coders, testers and documenters are the same people. When the increments are small and rapid, one avoids the problems caused by assigning a designer to each function and producing a system that looks like it was designed by a committee.

(U) Another factor is that, given the rapid nature of the development, there is no need to try to communicate through large design reviews and multi-inch documents. Instead of having formal reviews of documents that several layers of management have pre-reviewed, just review the software. Run it. Measure it. Software is truth, while documents can obscure truth. And it saves a lot of useless work and money/manpower for both the customer and developer side. Today it is common to have key developers spend a whole month preparing for a review instead of working on your system!

(U) The final aspect of continuous development is user satisfaction. Real users—the "stuckees"—are involved in the process because you speak to them in their language. You are showing them the real system as it progresses, allowing them the opportunity to influence future releases, and doing it all in a reasonable time frame.

(U) I like to compare building software to building a house. The traditional waterfall method would have us lay out all the requirements needed to make the house a turn-key operation: furniture, lights and rugs in place, towels folded to spec in the linen closet, curtains on all the windows. The house would be divided into subsystems, with lead designers and programming teams for each. Each team of five to ten people would then work on their detailed subsystem design, code, and perform unit test. Most real problems would not be evident until integration is attempted and the linen closet will not fit into the bathroom. The way houses are built in real life, and the way software should be built, is to put down the foundation and some framing first. Framing equates to the first incremental delivery. The user can walk through the house and decide that the traffic pattern through the kitchen is wrong and a door should be moved. Windows, and even staircases, can be relocated. It may take a little extra time and effort to move things at this point, but a better system will result. The alternative is that the user doesn't get to see how the traffic patterns, doors, and windows fit until integration or delivery, and then it is too late to change. They are stuck.

(U) I have discussed this over the years with various skeptics, and a frequent response is that this concept is all right for small analytic systems, but it does not apply to large automated systems. It is true that this type of interactive, iterative development is ideally suited to in-house analytic systems; that *is* how some of our most popular analytic tools (OILSTOCK, TINMAN, SCREENWORK, SUNSHINE, etc.) have been developed, some by small contractor teams and some by small government teams.

(U) However, I have personally used this method of development twice to replace large multi-year, multi-million dollar semi-automated processing systems. The first was the FDPS at Sunnyvale, and the second was

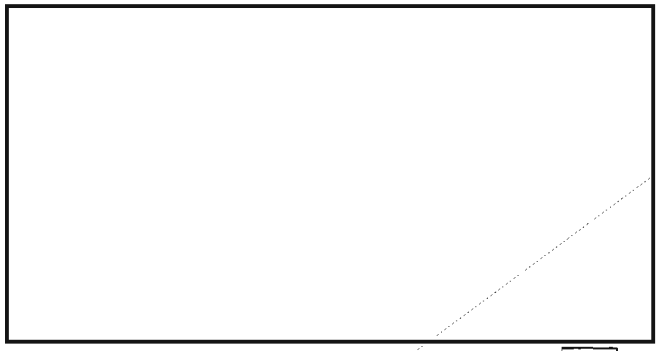
MINSTREL. In both cases, we started an alternative development long after the acquisition was underway because we were convinced that the acquisition system would not operate satisfactorily. In the case of MINSTREL, cost and schedule overruns were also an issue. In both cases, we delivered a much better system earlier, for less than 10% of the cost. I am confident that this method will scale to the largest acquisitions that NSA could conceivably undertake.

(U) Another interesting question I get is, "how do you know when you are done?" Maybe you are never done until it is time to replace the system. As long as there are users, there will be new requirements. Satisfying those new requirements will make the users more productive, and that is why we have ADP support. Since the continuous development team is smaller than many maintenance teams to begin with and since there is a maintenance team for the life of the system even for waterfall acquisitions, I am sure there is not a problem recognizing that continuous development releases and maintenance releases are actually the same thing.

(U) Documentation is another point. Just because you have reduced unneeded documentation doesn't mean there is no documentation at all. The requirements for each release are negotiated between developers and users, and documented to provide guidance and reduce misunderstandings. The code is documented and commented as necessary; since insufficient documentation in one release will cause serious problems in subsequent releases, the developer has more than usual interest in providing adequate design and code documentation. The users' document will improve with each release, especially as user input is incorporated. Finally, documentation for system administrators will also improve as each release is installed.

(U) Continuous development should be adopted as the standard NSA way of doing acquisition. Mil-Std 498, which replaces the NSA 81-3 standard, has the framework for continuous development built in and encourages its adoption.

(U) In summary, continuous development delivers useful results within monthst is much cheaper because fewer people are needed: six or so, versus sixty to one hundred. It eliminates unneeded documentation and the expense of massive program reviews (both man-hours and presentation graphics). The development is a satisfying experience for both the development team and the users. Above all, it works.



Kλ

P.L. 86-36

DOCID: 4010113

Foreign Language Testing at NSA: Time for Change

P.L. 86-36

by [redacted] H431

(U) This article reports the findings of a study carried out in mid-1995 touching on certain aspects of NSA's language testing practices. As an NSA fellowship recipient, I undertook this study in partial fulfillment of requirements for a Ph.D. degree in applied linguistics from Georgetown University, and in the hope of provoking beneficial changes to the current language testing system. It was conducted with the permission of M09 and the Language Career Panel.

(U) I expect that readers of this report will include both experts and nonexperts. For more on the theoretical background, full results, or procedural details, my dissertation (now in progress) will be available. (Many of the comments in this report are intended for NSA only and will not appear in the dissertation.) This article identifies two major threats to the fairness of NSA's language testing which should be addressed immediately; various other potential problems of a less serious nature are also pointed out and recommendations are made as to how they might be corrected. These comments are meant as a starting point for discussion and not as the definitive answer to all of our testing problems.

Objectives

~~(FOUO)~~ I had two main goals in this research, as far as this agency is concerned. First and foremost, I was interested in establishing the validity of the method that NSA and other government agencies use for choosing foreign language test passages. *In a nutshell, I wanted to know whether level 2 texts really are easier to comprehend than level 3 texts, and level 3s easier than 4s, for test takers at all levels of proficiency.* This must be true in order to claim that the levels scheme can appropriately be used as the basis for our testing system.

(U) Furthermore, even if one assumes the validity of the text levels, it is clear that there is a need to increase the reliability, validity, and efficiency of our foreign language tests. Hardly a language analyst has not complained about some aspect of the PQEs; most of them have a feeling that something is wrong, even if they cannot say exactly what. On the basis of my experience in this study, I make several suggestions here for consideration by the appropriate NSA elements.

(U) The study involved testing 56 employees with French language backgrounds for their French reading proficiency. I chose French because, frankly, that is the one foreign language that I know well enough for designing a good-quality test with a high degree of difficulty; and I had to leave aside the area of listening comprehension because of time constraints. Although the results reported here thus can only truly be said to apply to French reading comprehension, it would surely be necessary to show that the testing system works for even one language before we could properly try to extend it to all. Likewise, if the system is not applicable to reading (and by extension, to translation), then applying it to listening comprehension would not likely be fruitful.

(U) Rather than describing the various text levels here, I assume some familiarity with them on the part of readers. I must point out, however, that it is a common mistake to oversimplify what a given text level means, and thus I encourage readers to consult James R. Child's 1987 paper (which is included in the materials for the self-paced course LG-020, "Language Levels and Their Application") for a full description. I am completely ignoring the Interagency Language Roundtable's (ILR) levels 1 and 5, which is where the ILR setup runs into some real theoretical problems; these levels are not of any practical concern to government agencies anyway. In addition, be advised that on theoretical grounds, I do not accept the reading skills hierarchy that the ILR scale incorporates.

Part I: Text levels

Reliability

(U) *The business of determining the level of a text involves judgements by human beings.* Now, we must be fairly certain that, for instance, a level 3 passage really is a 3 and not a 2+ or a 3+, if we are designing a

level 3 test, because we want to ensure a consistent level of test difficulty. In fact, if text levels cannot be reliably determined even by trained experts, there is no sense in going any further in evaluating the validity of the levels theory.

(U) Just as an advertisement that says "nine out of ten dentists recommend Brand X" tends to inspire more confidence in Brand X, we tend to have more confidence in text-level judgements that are backed up by many expert raters. In the ideal situation, if we gave three or more experts the same set of written passages and asked them to determine their levels, the experts would—working completely independently—come up with exactly the same level assignment for each text. In the real world, we have to admit that people are not infallible and that it is perhaps harder to get linguists to agree on text levels than it is to get dentists to agree on chewing gum, but we should still strive to get as close as possible to that ideal target of complete agreement.

~~(FOUO)~~ In developing my experimental materials, I first identified a large number of authentic (naturally occurring, uncontrived) French texts between 250 and 300 words long, at text levels 2 through 4, including some that I thought were 2+ or 3+. I took 30 of these to others for independent decisions about levels; each text was rated by three people (including me). My experts were all current or former PQE committee members who had completed LG-020.

(U) The good news is that almost 97% of the time (29/30 cases), it was possible to get at least a two-way match (at least two experts agreed). Unfortunately, only 23% (7/30) were three-way matches, which is the ideal.

There are two things we can do, given this less-than-perfect situation. One is as follows:

- **Suggestion 1:** Use, in tests, only those texts for which three or more experts independently agree on the level.

(U) In selecting passages to use in this experiment, I gave preference to the three-way matches, using five of them in my test (which contained nine passages in all).The other thing we can do is to try to increase the number of three-way matches by improving the expertise of the raters. One way to accomplish this would be to make it a little more difficult to qualify as an expert rater. This could be done as follows:

- **Suggestion 2:** Double (or even triple) the number of items on the LG-020 exit exam (thereby increasing its reliability), then adopt a higher standard of performance, of 85 or 90 percent.

Another way to promote greater agreement is this:

- **Suggestion 3:** Require test designers (such as PQE committee members) to "socialize" at the start of each testing cycle, discussing several texts that are in the pertinent foreign language and that have previously been determined to be at the various levels.

(U) "Socializing" in this sense is obviously not what happens at cocktail parties, but it means making sure that everyone is interpreting the guidelines in the same way, often by studying examples.

(U) In making the suggestions in this section, I do not wish to imply that we necessarily have a serious problem right now with text level reliability. Reliability is difficult to estimate in this situation, and of course we can always try to improve it. Nonetheless, we may in fact have all the right ingredients for an acceptable level of reliability, *provided that the proper procedures are followed.*

Validity

(U) Now, just because we can determine text levels reliably does not mean that the levels do what we think they do for us. Reliability is a *necessary* condition for validity, but it is not *sufficient*. Let us consider an example of how something can be done reliably but still not be valid. Suppose I decide that all magazine articles are easier to understand than all newspaper articles, and the latter are easier to read than all books. I have no doubt that almost anyone could tell a magazine from a newspaper from a book with a very high degree of reliability, but few people would really be convinced that I have identified a true progression of text difficulty.

(U) It is obvious in this example that something is wrong, but it is not always so easy to determine this. Someone who has read Child's paper might say that the text-level scheme *seems* right for estimating text difficulty. Intuitions are useful for many endeavors, but sometimes they, too, are dead wrong. Science is full of examples of nature contradicting our intuitions (isn't the earth flat?). That is why we often want experimental data to confirm (or refute) what intuition tells us.

(U) It has never been shown experimentally that texts at the different levels really define a hierarchy of

comprehensibility that can be used to separate test takers by level of proficiency. In fact, researchers in academia claim to have found evidence in two widely cited studies that this is not the case. These earlier studies, however, were seriously flawed, suffering from the following problems:

a. The researchers reduced the text-level descriptions to simple genre labels, so that any editorial, for instance, was taken as indicative of level 3 with no further analysis. Level decisions seem to have been based solely on genre, with no concern for the communicative functions that the texts served.

b. Only one or two texts of each type were used, and these texts were not chosen by multiple trained, independent raters. The reliability of level assignments is thus suspect.

c. The range of foreign language proficiency of their subjects did not begin to cover the full ILR range. The higher levels of ability were particularly underrepresented.

~~(FOUO)~~ I set out to conduct a similar experiment that would remedy these problems. I designed a test composed of nine texts of about equal length, including three at each of the levels 2, 3, and 4 (avoiding any "plus level" texts for maximum separation of level effects). The texts were on various topics, including political affairs, social affairs, terrorism, and human rights. Potential test-takers were randomly chosen from among all those who had passed a French test at the Agency within the past 15 years. This included many people who had never used French on the job as well as certified French language analysts, so a wide range of ability was represented.

(U) In the testing sessions, each of the subjects saw multiple-choice questions on six of the reading passages, and did "rough translations" (described in more detail below) on the other three passages. Test versions were rotated so that each text was translated by about one-third of the subjects; the order of presentation of the passages was also varied to control for warm-up and tiring effects.

(U) A 27-item multiple-choice French reading comprehension exam taken from tests designed by the University of Ottawa was also administered to all subjects. This independent measure of proficiency was originally supposed to allow division of the subjects into three groups by ability, but it was not reliable enough for this purpose. Thus a combination of scores on the two multiple-choice sections (Ottawa and experimental) was used to divide test-takers into three groups of higher, average, and lower ability, and my analysis then focused on the translation data only (scoring of the translations will be discussed in Part II below).

(U) As mentioned earlier, for the theory to be valid, the level 2 texts had to be easier for everyone to translate than the level 3 texts, and the 3s easier than the 4s, in a statistically significant way. My analysis of the translation data shows that this is indeed the case *on average*; there were significant differences between the means for levels 2, 3, and 4.

Table 1:

Text set	Level 2	Level 3	Level 4
terrorism/ human rights	87.2	84.7	70.0
social affairs	81.3	83.4	81.5
political affairs	93.3	76.6	68.5
Total	87.3	81.9	73.3

Mean scores on translations (expressed as percentages)

(U) In addition, the most able group of test takers (independently determined by multiple-choice test scores) had to get significantly higher scores than the least able group, particularly on the level 3 and 4 texts. This was also the case, as the following data demonstrate. (The average group was not sufficiently differentiated from the high ability group. This may be due to various factors, including the mediocre reliability of the criterion used to divide subjects by ability, or the different aspects of linguistic competence tapped by multiple choice and translation tests.)

Table 2:

	Level 2	Level 3	Level 4	Total
High	90.5	87.3	80.6	86.1
Middle	88.8	82.5	75.5	82.2
Low	82.9	76.1	63.6	74.2

Test performance by text level and subject ability level

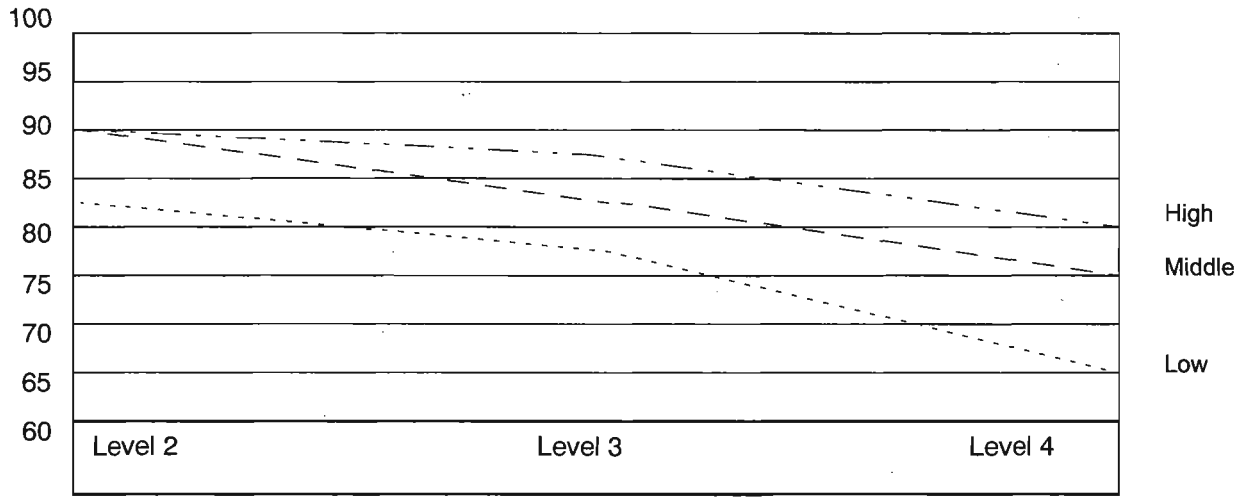


Figure 1. Test performance by text level and subject-ability level.

(U) *One caveat is very important: it is only when a given level of difficulty is represented by* ***at least three texts*** *that the clear pattern emerges.* Group performance on any one text may vary from expectations. As you can see in Table 1, one level 2 passage and one level 4 passage both had about the same mean score, just above 81%—individually they behaved more like the average level 3 text! Each subject in this experiment translated one text at each level; this is supposed to make all test versions equivalent, but in fact, one of the three versions was significantly easier than the others because one or more of the texts in it was easier than predicted.

(U) The need for three texts could be due to some inherent unreliability in the text selection process (see preceding section). It is more likely, however, that the text levels simply cannot be conceived of as distinct entities having relatively well delineated boundaries between them, as in figure 2 on the left. Instead, it may be more appropriate to view the levels as highly overlapping ranges with distinctly different midpoints, as in figure 2 on the right. The levels seem to identify difficulty *tendencies* rather than absolute values.

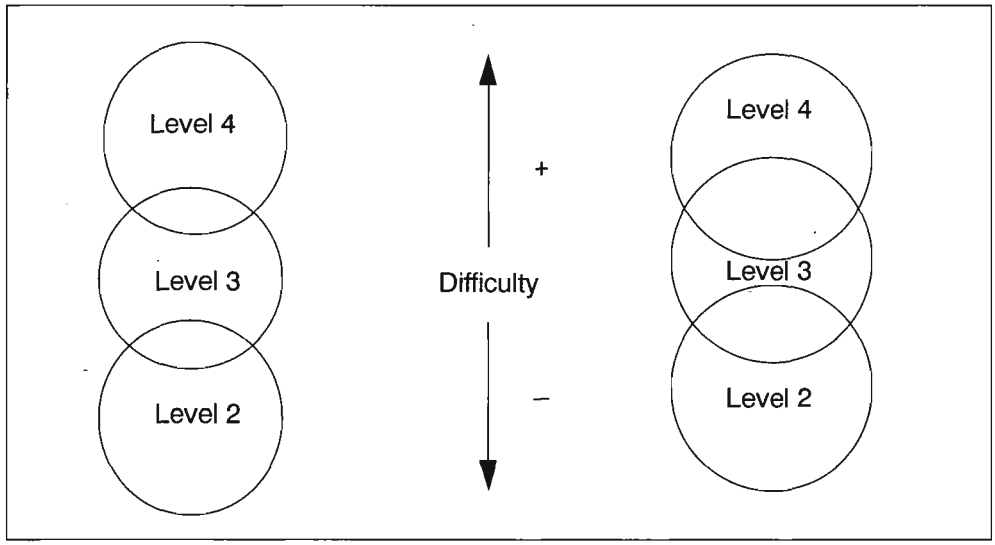


Figure 2. Text levels plotted on a scale of comprehensibility.

~~(FOUO)~~ In practical terms, this means that in order to ensure that test difficulty remains more or less constant from one test to another (as close as possible to the midpoint of the range) without the luxury of pretesting passages to determine their difficulty, we must look at average performance across several texts at the targeted level. This points up the **first major threat** to fairness in our testing: *many PQEs are composed of only one or two passages, so we cannot guarantee that they are all of about equal difficulty.* It is conceivable that we have allowed some people to pass who should not have, and failed some who should have passed. The results of this study indicate that those who are not quite capable of level 3 performance but do not wish to do anything to improve their skills are justified in thinking that one day an easier PQE may come along. Likewise, the capable but not exceptional performer may be unfairly penalized by a PQE that is too hard, being forced to wait until one of more appropriate difficulty is presented.

This naturally leads to the following:

- **Suggestion 4:** All language comprehension tests should employ at least three same-level texts of approximately equal length, from different sources and on different topics.

(U) This recommendation can be implemented immediately without placing an undue burden on test designers. I therefore urge most strongly that it be adopted without delay.

Some have been waiting for an easier PQE.

(U) Equal length is stipulated so that each of the three (or more) texts contributes about equally to the final score. Sources and topics must be varied to ensure that these also are not factors (or at least not important factors) in the outcome. As for the optimal number of texts to use, while clearly more is better in achieving representativeness, there are practical limits to what test takers and scorers can handle, and beyond a certain number, very little would be gained with each additional text. Three is the minimum, but more than five or six would probably be overdoing it.

(U) There is another reason to base tests on multiple passages: by using only one, we cannot be certain that we have obtained a representative sample of each test taker's ability to perform at that level. It is widely accepted in the field of language testing that one should give test-takers as many "fresh starts" as is feasible. Coupled with the findings reported here, this is all the more reason to incorporate Suggestion 4 into NSA testing practice.

(U) A note about "plus levels" (2+, 3+): it is not clear how test takers would perform on "plus level" texts. In terms of text difficulty, does a 2+ behave more like a 2 or more like a 3, or right in between? Most of us probably imagine it as the halfway point between levels, but this is an untested assumption and must be considered suspect. In the absence of any hard data, I would not advocate gearing comprehension tests to "plus levels."

Part II: Other testing considerations

(U) The preceding section may have frightened those who took it to mean that PQEs would now have to be three times as long as before. Rest assured that this is not the case; there are other ways to ensure that language tests are accurate and appropriate!

Test format

~~(FOUO)~~ One might well wonder why I did not use a PQE-style test in my experiment. The choice of testing format, especially for PQEs, has (rightly) been driven by the need to evaluate objectively how well language analysts are equipped to do perform their jobs. Increasingly, however, as the language analysis field changes, analysts can be heard to say that what happens in the PQEs "is not what I do." The traditional translation test is more and more seen as an invalid measure of job competence.

~~(FOUO)~~ *The reality today is that language analysts do a variety of things.* Some must read large volumes of material quickly, making decisions about what they read; some must translate while others simply gist or move straight to an English language report; some

have a great deal of time to complete their tasks, while others work within strict time constraints. Many analysts will find themselves in all of these situations at different times. In designing tests that will indicate competence for this variety of language tasks, we need to ask ourselves what they all have in common. The obvious answer is that a strong ability to comprehend the foreign language is necessary if the language analyst—any language analyst—is to do his/her job efficiently and effectively. That is, language proficiency is the foundation for success in any language-related position in government. Language proficiency, then, ought to be what our language testing is about.

~~(FOUO)~~ The current PQEs place a premium on "idiomatic English" and allow test takers a great deal of time to achieve it. The ability to express oneself well in English is probably much more important a factor in these tests than in most comprehension tests. This is at odds with the way many test users (e.g., supervisors) sometimes see the tests, namely as diagnostic tools for linguistic competence. The hapless analyst who fails her German PQE is thus signed up for yet another course designed to help her understand German, when what she needs may be a course in how to express herself more effectively in English. Unfortunately, the current format has little diagnostic value, as we can never be certain whether poor test performance was due to deficiencies in foreign language comprehension, in English expression, or both.

(U) Now, good English writing ability is no doubt a desired quality in language analysts, and we should probably encourage its development by testing it. Keep in mind that we are not limited to a single testing format. It would be possible, for instance, to proceed as follows:

- **Suggestion 5:** Emphasize speed and comprehension in one part of the PQE, while stressing precision of expression in the other.

~~(FOUO)~~ Since we already have a well-developed translation format in place, I was interested in developing a test oriented more toward measuring reading comprehension. The format I chose for this study, which is described below, is one that allows evaluation of foreign language reading proficiency without unduly relying on English writing skills (as do our current PQEs) or on raw reasoning ability (as do many multiple-choice tests). It is similar to the widely used immediate-recall protocol, but it does not tax the memory and is a more realistic communicative task.

Rough Translation

~~(FOUO)~~ In what I call the "rough translation" format, test-takers are given a limited amount of time to produce a written representation of the meaning of a set of foreign language texts. In this experiment, test-takers had only about 20 minutes to complete a rough translation on each 250-300 word text (or one hour for just over 800 words). This strict time constraint was imposed because researchers have often noted that reading speed is related to reading success. Contrast this with the PQEs, which allow testees several hours to decipher fewer than 600 words, and it is not unreasonable to believe that some nimble dictionary users have been able to pass tests in languages they would not normally be said to "know." (A level 3 reading exam requirement would help to stamp out recreational collection of language certificates.)

(U) Test-takers in this experiment were not allowed to use dictionaries. We may wish to permit dictionary use in actual testing just to reduce test-takers' overall anxiety; however, they should be forewarned that research shows that such use may not help and may even hurt their test scores in a reading test situation.

~~(FOUO)~~ The first step in scoring involves dividing each original text into a countable number of scorable units. This is to provide a meaningful basis for comparison of test takers both within a single test administration as well as across administrations and across languages. This addresses a serious shortcoming of our current scoring system, which is the **second major threat** to the integrity of our translation tests: we have no easy-to-understand, reliable way to determine how many points a text is worth, so we cannot convert scores to a figure (such as a percentage) that can be compared across test administrations. (A method has been recommended based on the count of "propositions" per text, with a maximum score of 8 points per "proposition"; but for some reason—a lack of clarity, a lack of credibility, or a general failure to realize its importance—this method has not been followed consistently.) The result is a points-deducted score that cannot be meaningfully compared to any other scores, except within that particular test. We often say that a test-taker has had *n* points deducted—without saying how many points were *possible*. Choosing an arbitrary maximum number of points for each text—such as 100, as has recently been advocated—does not make the resultant score any more meaningful. A points-deducted method presupposes that all PQEs are exactly equal in difficulty, an assumption that is extremely doubtful (see Part I). One must be able to specify how many points it is possible to obtain

before it will be useful to know how many have been lost.

(U) My model for breaking down the texts into scoring units was the "pausal unit" method, in which several expert readers of the foreign language determine each spot in the original text where it would be possible to pause for emphasis or to take a breath. Everything between possible pauses constitutes a unit. The "pausal unit" approach could easily be implemented by PQE committees with little training. Using my method, most scoring units were between one and four words long. The nine texts used in the study were in this way divided into between 98 and 153 units.

(U) Each scoring unit in which the test-taker had substantially preserved the meaning of the original, without omissions or extraneous material, and which was in the correct relationship to all other units, was worth one point. For ease of scoring, only errors were tallied and then subtracted from the total possible. This raw score was then converted into a "percent correct" score. Conspicuously *not* counted as errors were translated units containing awkward or nonidiomatic English, those infelicities that would have cost test-takers one point each under the current translation scoring system; nor were testees docked points for not following the GPO Style Manual. Remember that the focus here is on meaning rather than on form.

Understandably, some French language testees misunderstood the word "laïque."

(U) The stipulation that units be in the correct relationship to all other units is necessary to catch errors that might otherwise go unpenalized. Because of the redundant nature of linguistic systems, most mistakes due to syntactic misinterpretation will have effects at the lexical level and will thus be reflected in the final score. However, in rare cases it is possible to make an error of interpretation and yet represent faithfully the meaning of the original units, as when "the dog / bit / the man" is rendered as "the man / bit / the dog." In such a case, both noun phrases would be docked one point each for being in the wrong relationship to the verb.

(U) The astute reader will see that in this scoring system, unlike the PQE system, all sorts of errors receive exactly the same penalty of one point. I do not subscribe to the theory that all syntactic errors are worse than all lexical errors, and my data bear this out. For instance, one text in the experimental set had to do with a strike in Corsica which was dubbed "dead island day." Two of the lowest scorers rendered the French word for "day" ("journée") as "journey," and so failed to understand a key phrase; thus a lexical error was an important factor in a major comprehension failure. On the other hand, those who mistranslated "la crise que traverse le pays" in another text on Algeria as "the crisis that is going through the country," instead of "the crisis that the country is going through," made a syntactic error that does not seriously affect understanding.

(U) Also unlike the current scoring system, mistakes on repeated instances of the same word may be penalized more than once. This is because a word may be interpreted differently according to the immediate context in which it is found; a word may be understood in one context, but not another. Thus in one text criticizing religious schools in Paris, some testees were not able to understand the word "laïque" ('lay' or 'secular') in the first instance, when it occurred in contextual isolation, and yet recognized it in the second instance when it occurred in juxtaposition to "religious." Each occurrence of a word must be viewed as a new opportunity for understanding (or misunderstanding).

Test reliability and validity

(U) Since I did all of the scoring of the rough translations myself for practical reasons (not the ideal where judgements about correctness are involved), I should demonstrate that (1) my scoring was consistent and (2) the scores would have come out roughly the same if others had participated in the scoring.

(U) I used two measures to estimate internal consistency, neither of which is the perfect method in this situation (there are no more appropriate methods). Reliability estimates on the nine texts range from .85 to .96, averaging .90. These are quite respectable numbers. (A reliability of at least .85 is *de rigueur* in language testing; it is the minimum acceptable for the Educational Testing Service's raters of written compositions, for

example). Given that certain assumptions of the formulas were violated, reliability is probably even higher than reported.

(U) As for inter-rater reliability, I took a representative sample of eighteen translations (two for each of the nine texts, constituting about ten percent of the total used in the analysis) to independent experts, whom I briefly instructed in my scoring method. The correlation between their scores and mine was .85, once again an honorable figure. I believe it would have been even higher if the raters had had a little more "socialization," or prior discussion and practice, and if they had been allowed to discuss each other's work afterward so that they could catch their own errors and omissions.

(U) I therefore feel quite confident in saying that the test method employed in this experiment enjoys good reliability. Scoring is also fairly efficient: I completed scoring of all 201 translations in one week.

(U) Now that reliability has been demonstrated, we must ask if the test is also valid: does it really measure reading ability? One way to determine this is to see if it lines up test-takers in the same way as another reading test. The rank-order correlation between subjects' average translation scores and their combined multiple choice scores was a fairly strong .83. Thus we can say that the test's concurrent validity is good.

A model testing program

(U) The test method presented here is not the only viable alternative to the current method, but it does seem to be a good way to test reading ability, and it might easily be converted for use as a more traditional translation exam by allowing test-takers more time and being stricter in the definition of an error (this would have to be pilot-tested before implementation). In this section I would like to delineate what our overall testing program might look like, with the inclusion of a test of this type. Please keep in mind that this is only one of many possible scenarios which I hope will receive serious consideration by the pertinent decision-makers.

~~(FOUO)~~ I would like to propose the following plan for NSA's language testing:

- **Suggestion 6:**

At level:	Replace the current:	With:
2	LPT	(nothing)
3	PQE Part I, traditional translation	rough translation
3	PQE Part II, traditional translation	traditional translation (use new scoring method)

~~(FOUO)~~ I am proposing that the PQE Part I be conducted using the method described in this article. Since the PQE Part I would now be a reading test, there would be no need for a separate level 2 test. Both level 2 and level 3 reading ability could be determined simultaneously with the same test, saving a lot of time and personnel resources in test design, administration, and scoring. The people who come to the Agency with a higher foreign language capability would not have to go through three test sessions, while testees who did not achieve a level 3 rating on the first try would have to retake the test at the next offering in order to advance, as in current practice. The cutoff score for a level 3 reading ability would have to be high, at about the 90% level (remember that the mean on the level 3 texts in this study, which included many test-takers who are not language analysts and/or have not used the foreign language in many years, was already 82%). A lower cutoff score of about 75% would determine level 2 ability (this is, of course, average performance across three or more texts on which three or more experts agree about the level, etc.).

~~(FOUO)~~ The Part I test could be administered in just one hour, if texts of the same length as in this study are used. (Following tradition, rather than specifying a length in words, we could say that each passage should result in a translation of *n* words—in this case, 250 to 300.) For the Part II test, we could allow about twice as much time; a new scoring method would have to be found—perhaps an adaptation of the one described in this paper. As for the question of whether to use open or classified sources, if finding appropriate test materials in classified sources is difficult, I can think of no compelling argument for forcing PQE committees to limit themselves to that domain. The interest of ensuring fair tests should outweigh that of sticking to SIGINT.

Conclusion

~~(FOUO)~~ The text-levels theory seems to be a sound basis for our testing program as long as we take multiple samples of reading behavior at a given level, by using a variety of texts. Other aspects of our testing program are in need of some attention, particularly the scoring system used on translations. If further information or clarification is needed, I would be happy to discuss any of the ideas presented in this report. Needless to say, I believe the plans presented here would represent an improvement over the current system. However, I do not believe that we should ever be completely satisfied with what we have decided upon. Language testing is messy enough that there is always room for improvement. It is my hope that others will find the will and the cooperation necessary to carry out other large-scale studies of this sort so that at any moment we can say that NSA has done its best to make its tests as fair as they can be.

Acknowledgements

~~(FOUO)~~ It took the efforts of many, both inside the Agency and elsewhere, to make this study possible. I am especially grateful to the 67 people who suffered through my 3.5-hour testing sessions. I would further like to thank those who provided assistance in the various stages of test design and evaluation, especially

[redacted]

My gratitude also goes to everyone who provided advice and logistical help, particularly [redacted] Last but not least, I would like to acknowledge the assistance of "language levels" author Jim Child as well as my dissertation committee members, [redacted]

[redacted]

Kλ

P.L. 86-36

P.L. 86-36

SIGINT That Matters: What's the Angle?

by [redacted] E4

(U) By now, most intelligence analysts probably have heard the words "journalistic concepts" during discussions about trends in SIGINT reporting. Many of the journalistic techniques being taught in reporting courses and seminars involve changes in writing style, some subtle and some distinct. NSA has incorporated other aspects of journalism into its reporting process, such as using graphics to enhance report presentation and venturing into multi-media techniques such as video reporting, audio reporting and a myriad new dissemination methods. While these efforts have generated very positive responses from our customers, one important aspect of journalistic technique, *finding the best angle for the story*, is only now beginning to get serious attention. The angle will undoubtedly become one of the most important aspects of a SIGINT report, as Congressional budget committees again and again ask for clarification on the unique information NSA offers its customers.

(U) So, what is the angle? It is the art of presenting a topic in such a way that the reader can not only relate to that topic, but can understand the *significance* of that topic. It goes beyond simply stating the SIGINT fact, e.g. "A told B that a meeting had taken place." It helps the reader understand what went on in that meeting that was important, and why he or she should bother to read the report. To put it bluntly, *the angle is what sells the SIGINT.*

(U) Two of our most important jobs as SIGINT reporters are to **recognize** the significance of what we see, and then **explain** this in our product reports. Our customers are being bombarded by what seems to be an infinite supply of information. Unless we show them that what we have to say is important to them, our reports will simply be blown away like so much junk e-mail. We can show them by providing an angle, or focus, in our reports that emphasizes the significance of the information within the report. More than a few reporters already do this for their customers, and they receive very positive feedback. Unfortunately, some of us still believe "it came from SIGINT and nobody else has anything on it" is all the justification we need for publishing.

A Changing World

[redacted]

(U) Furthermore, I knew that since there was no real competition that might scoop me, I could rely on my customers following my every word. I did not worry much about *why* this or that happened or the deeper meaning of what might result *because* it happened. I was happy in my own little world. And I was good at it (at least everybody said so). My customers all agreed that my reports were unique and therefor[redacted] valuable, thus justifying the cost of production. If I thought about putting an "angle" on my reports, I didn't think long; if I had used one, it might well have been "because I know and you don't."

P.L. 86-36
EO 1.4.(c)

[redacted]

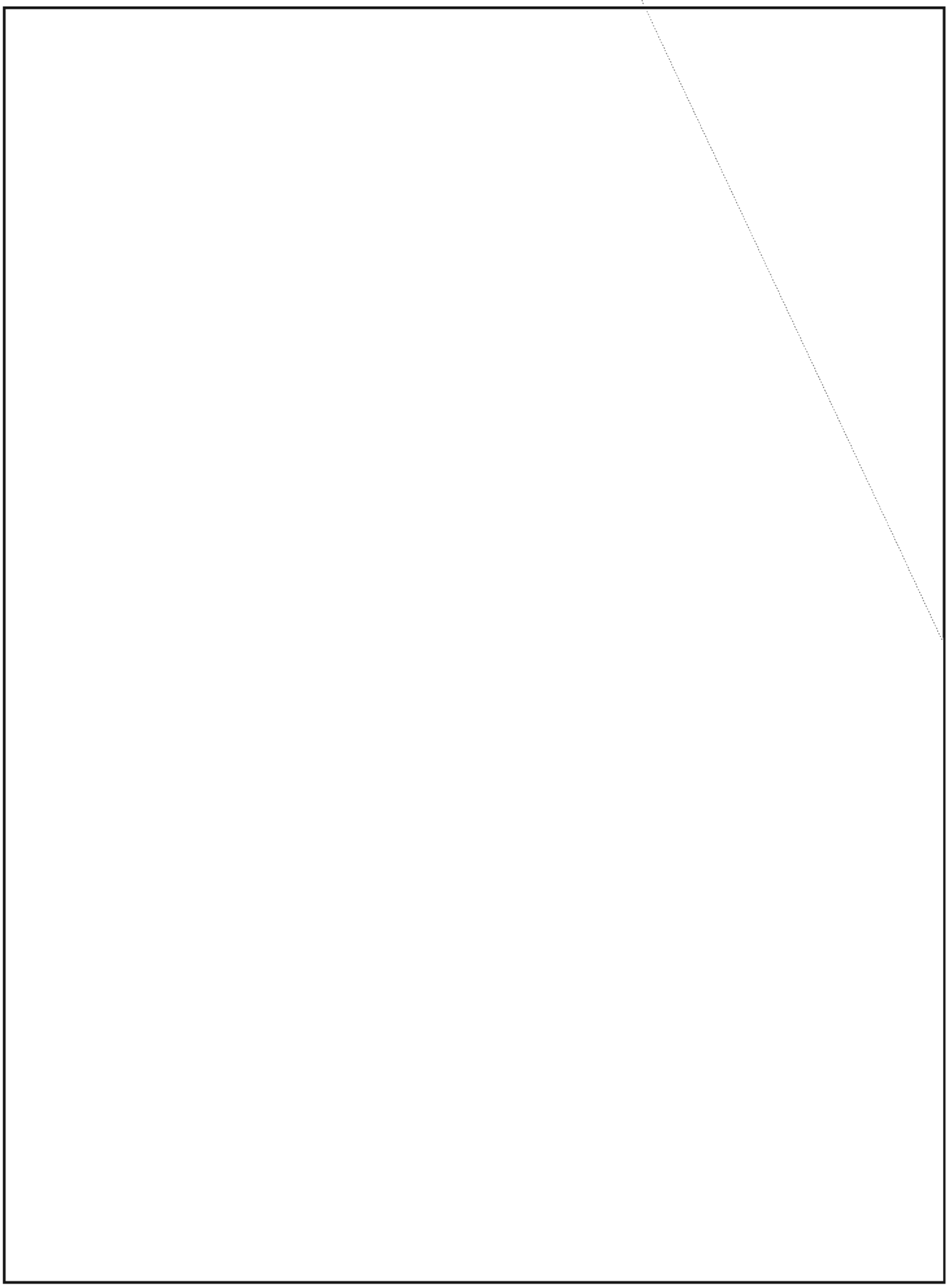
P.L. 86-36
DOCID: 4010113 EO 1.4.(c)

[redacted]

(U) If we start to suffer from blurred vision, we can close the video window and open a CompuServe window to get the latest reports from newspapers like the *Washington Post* or the *New York Times,* or from the AP or UPI wire services. Their reporters often work from an eyewitness angle, seeing things in places where even the intelligence community didn't have access just a few years ago. If we feel the need to enter the Twilight Zone, we can crank up the CD-ROM drive, slip in a disc, and cruise [redacted] to check on some minute details.

[redacted]

[redacted]



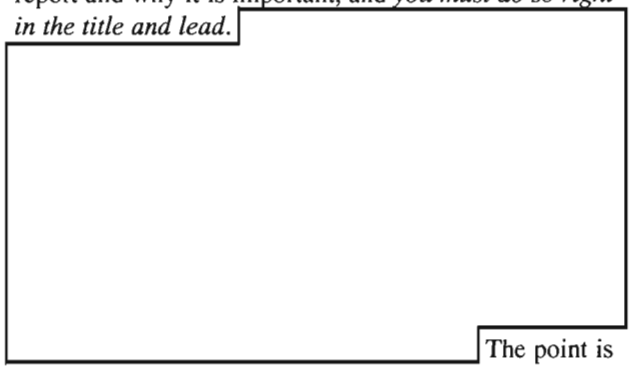
EO 1.4.(c)
DOCID: 4010113 P.L. 86-36

(U) As you keep pace with your target, you should also keep pace with what your customers want to know about your target. With the target, you may have the luxury of getting too much information to process. With customers, you may have the problem of having too little. Furthermore, the pace of change in what customers want may be even more rapid than it is with your target. Several new services can help you. One of the newest available is ESS topic 1442, the DO Customer Statement of Interest. It will tell you what various high-level consumers in the Washington area consider of pressing importance on any given day.

(U) As mentioned before, your customers have at least as much information to sift through as you do. They don't always have time to analyze the significance of some small fact that they may have asked you last week to report, but they will *make* time to read about that small fact if you do at least some of the analysis for them. By keeping track of what your customers might need to know, and by telling your customers what is important about each individual report, you can most effectively use the angle.

Highlighting the Angle

~~(C)~~ The final challenge is to highlight the angle for the reader. You must emphasize what is important in the report and why it is important, and *you must do so right in the title and lead.*

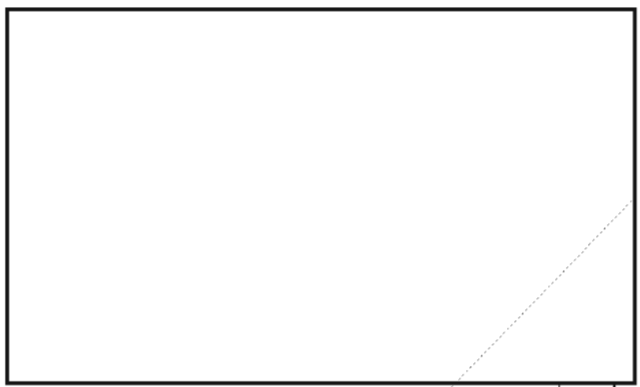


The point is to add to the greater body of knowledge about the target.

(U) *Remember that you are not obliged to make your report follow the same flow as the original traffic.* In other words, just because the Ambassador addressed the weather, the price of eggs, and the exact time that the car bomb would explode, that doesn't mean these topics must appear in the same order within your report, *or indeed that the first two must appear at all.* This is related to one of the most important lessons aspiring news reporters can learn: never leave a press conference/briefing before the question-and-answer session, even if a deadline looms. The best news angles often come from afterthoughts, side stories, or audience reactions. Similarly, the best SIGINT stories often are buried at the bottom of those long diplomatic messages or may come from some associated context. Your job is to identify them and promote them to the top of the page! For assistance in learning how to do this, P054's Reinvention Lab for SIGINT Reporting, is publishing Hints for Better Writing, available via ESS topic 1619 and MOSAIC at **http://gonzo.p.nsa/RLSR/RLSR.html**.

So What?

(U) No, Toto, we're not in Kansas any more. The world has changed. "Because I got it from SIGINT and nobody has anything on it" can no longer be the "so what?" of a product report. We must realize that we cannot report in a vacuum. We must work hard to make sure our SIGINT reports have impact. By keeping up with the target, and keeping up with what our customers want to know about the target, we will know what angle to take in our reports. And, by highlighting that angle up front in the product's title and lead, we will answer the customer's "so what" and meet their intelligence needs right off the bat. It all will add up to SIGINT worth reading.



Kλ

P.L. 86-36
EO 1.4.(c)

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

SIGINT and the Information Explosion

P.L. 86-36

(U) A few years ago I was attending a graduation ceremony. The guest speaker was exhorting the graduates to continue to pursue their education and self-development after graduation. To reinforce this point the speaker cited research on the growth of knowledge during the course of history. According to this individual, human knowledge doubled between the beginning of recorded history and about 1900. Knowledge doubled again between 1900 and the end of World War I. It doubled again between that time and about 1930; then again by 1940, and since then has been doubling every three to five years.

~~(C)~~ Now what, you might say, does this have to do with SIGINT, or, more specifically, with Cryptologic Support Groups (CSGs)? Many things, but as the chief of a CSG myself, I see the greatest challenge in this information explosion is the growth of sources of information beyond our wildest dreams. In the days of the Cold War CSGs had a much simpler job than we do today. We interpreted SIGINT. We had a good time and we made many friends for the Agency. We worked with "all-source" analyst, but I submit to you that all-source analysis in those days was much more straightforward than it is today.

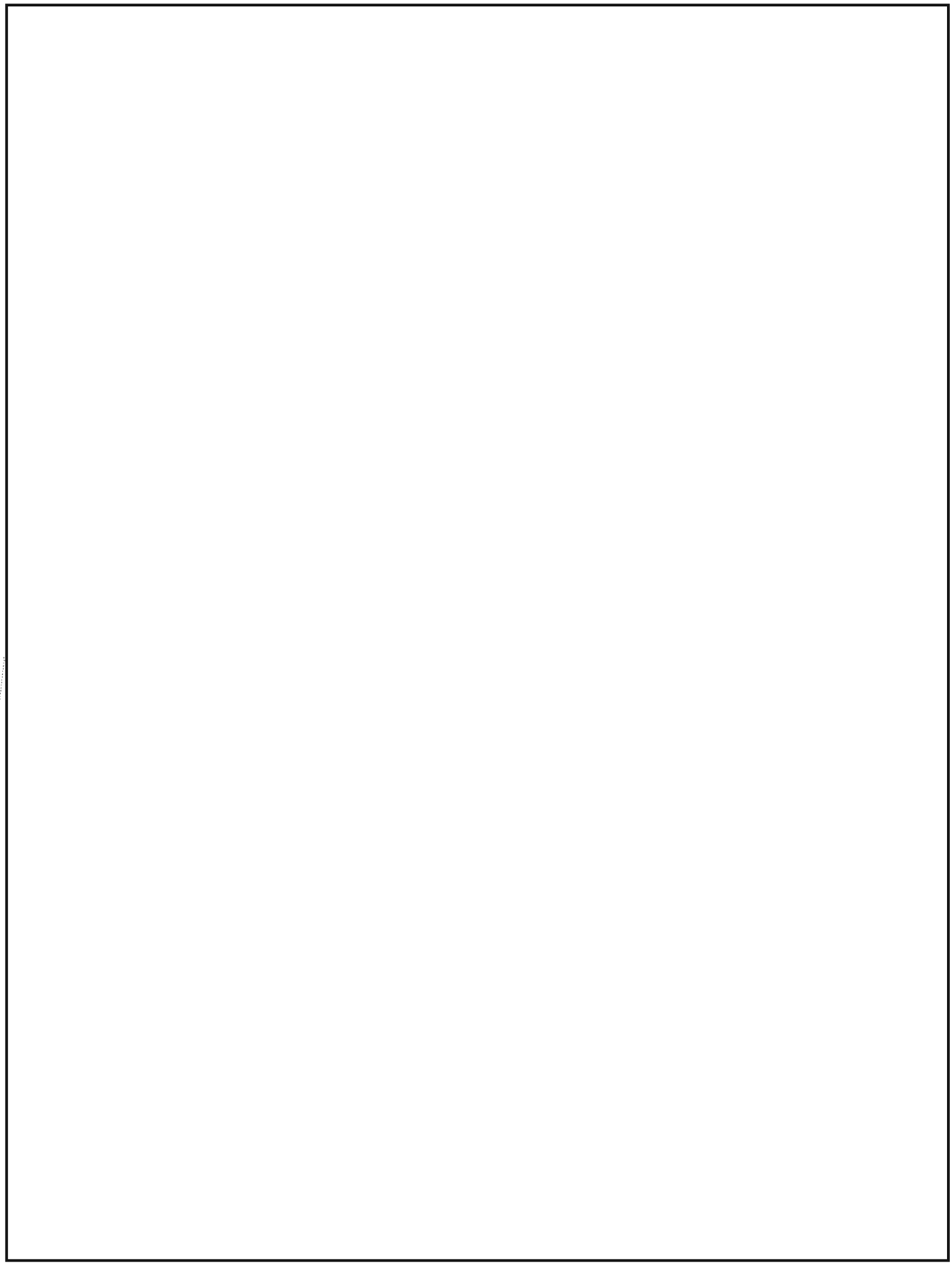
Must call George before we attack. Anybody see a pay phone?

(U) First: the analysis described above is straightforward. Each collection system provides a time, a location and the description of an activity. Analysis mainly consists of looking at the collectors' outputs and verifying that they really do correspond.

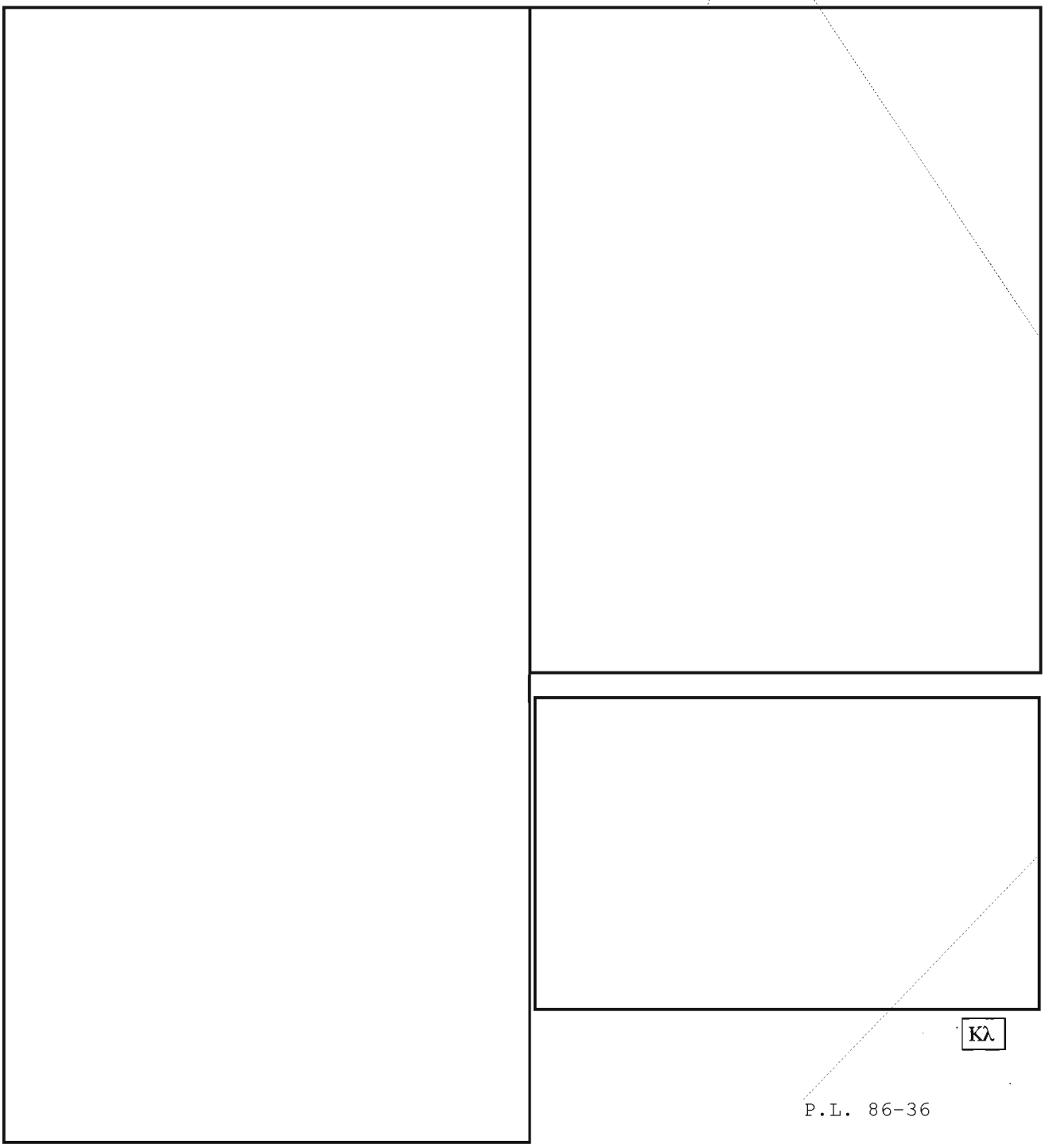
(U) Second: the sources described above are complementary, that is, they fit together neatly to form a coherent piece of "all-source" data.

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



P.L. 86-36
EO 1.4.(c)



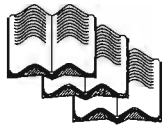
ΚΛ

P.L. 86-36

P.L. 86-36

Recent Publications on Information Warfare

reviewed by [redacted]



(U) Information Warfare or IW is very topical these days. One cannot pick up a newspaper or magazine without seeing an article that at least touches on IW-related issues. Even the Speaker of the House of Representatives regularly holds forth on the subject. It is not surprising that the publishing industry has picked up on the IW trend and printed numerous books on IW, fiction and non-fiction. (Admittedly, it is often hard to tell the difference.)

(U) One of the first problems one encounters in discussing IW is its definition. There is no widely accepted taxonomy of IW. Consequently, it covers a multitude of high-tech material including command-and control-warfare, perception management, computer warfare, gathering intelligence from computers, using computer viruses to destroy data, affecting an adversary's infrastructure through the use of computers, esoteric weapons such as electromagnetic pulse devices and microwave beam guns and so forth. Of course, IW must also address how we protect our information and information systems from the depredations of others.

(U) The basis for much in IW stems from the world's growing interconnectedness. It is this exponentially expanding network of networks that leads many futurists to predict fundamental changes in the way the world works and even in the nature of what constitutes national interests. Heidi and Alvin Toffler have written much on this subject. If they are right and information is the foundation of the next stage of human development, then our understanding of IW-related issues may determine the nature of our future as a world power.

(U) IW is a sprawling field of wide-ranging ideas. It, and its companion concept cyberspace, make up the new Wild West. Fortunes will be made and lost, power centers will pivot and shift, indeed lives will be shaped by how well we adapt to a future based on information. Below are some comments on a few of the recent offerings in IW from the publishing world.

(U) *Information Warfare: Chaos on the Information Superhighway* by Winn Schwartau. Definitely worth reading. Nevertheless, keep in mind that Mr. Schwartau is something of an IW gadfly who does not always have his facts straight. Many NSA readers of this book will spot errors which cannot be discussed in this review. In addition to factual errors, he is inconsistent in his approach to IW. For example, in *Information Warfare* he decries the fact that we as a nation are essentially unprepared for even low-level attacks by hackers and criminals. On the other hand, he recently led an e-mail campaign suggesting people flood the government's e-mail addresses and bring the system to a halt in protest of the very cryptographic policies which might offer a modicum of the protection he says we need. Now, having relieved myself of that editorial comment, let me talk about the book itself.

(U) *Information Warfare* frames many of the IW issues clearly and with imaginative scenarios describing how bad things may become. Mr. Schwartau divides those who would do harm to information systems into several categories or levels. He differentiates between the curious hacker, the criminal hacker for hire, the disgruntled employee, the cyber-terrorist group, and the nation-state. He points out that a well-focused nation-state or terrorist group will be able to do more harm with computer attacks against power grids or the banking system than they would ever achieve with explosives. He also points out the vulnerabilities we all face by having our individual credit histories, medical records and other personal data so easily available in large data bases. The fact that these data bases can be accessed and even altered is no secret. Anyone who has tried to rectify a credit bureau error understands the potential nightmare an attack aimed at one person might produce. Mr. Schwartau is particularly evocative in describing this type of scenario.

(U) While Mr. Schwartau performs a service by pointing to the problem, he fails to offer meaningful recommendations to fix it. He offers some vague advice about government action, but there is nothing concrete. One is left with the impression that he wants a government he doesn't trust to go after "them" and to do so without infringing on anyone's personal privacy in the process. Bottom line: a little shrill but still a good read and a good introduction to some of the fundamental issues.

(U) *War and Anti-War* by Heidi and Alvin Toffler.[1] Don't get me wrong—there are some important ideas here, it's just tough wading through a couple of hundred pages of disjointed prose to dig them out. Instead of reading this book, you may want to read *Creating a New Civilization, Politics of the Third Wave* with the introduction by Newt Gingrich. It is the condensed version not only of *War and Anti-War* but also of *The Third Wave* and other works by the Tofflers. The Tofflers are idea people and they have some good ones, even if they are given to sweeping generalization. They just need a better editor.

(U) If you can tolerate *War and Anti-War*'s "thought-bite" format aimed at those with short attention spans, you will gain some useful insights. For example, the Tofflers believe the way we make war is based on the way we create wealth. In ancient times, wealth was based on agriculture and war was centered on agricultural concerns. In the industrial age it was technology that drove the economic engine and likewise the engines of war. Now as we enter the information age, how well we degrade an adversary's information and information systems while protecting our own will determine our survival.

(U) The Tofflers have derived this concept from some of their earlier thinking about second wave (industrial) and third wave (information) civilizations. One of the problems the Tofflers foresee is that what they perceive as second wave organizations (like the federal government, or NSA, for that matter) are not well suited to deal with third wave (IW and cyberspace) problems. They predict that the first nations to adapt to the information age and the third wave will be the superpowers of the next century. I recently had the opportunity to ask Alvin Toffler what an effective third wave government might look like. He said he had no idea. I guess that's a reasonable answer since one has yet to emerge.

(U) The Tofflers see most modern conflict as arising from the clash between waves. For example, the mess in the Balkans is seen as first wave (country) vs second wave (cities). The American Civil War would also be a first/second wave confrontation. The Tofflers depict many of the current problems in contempory American politics as second/third wave conflicts. They are not sanguine about chances for a peaceful transition to a third-wave world. They point out that such transitions have traditionally been marked by considerable chaos and upheaval. So, if you can get through the chaos and upheaval of the book's poor organization, read it.

1. See "Information Warfare, *War and Anti-War*, and NSA", by Bobby Mitchell, CRYPTOLOG Fall/Winter 1994.

(U) *The Cuckoo's Egg* by Clifford Stoll. Still a classic. This is the story of how the Hannover Hackers were caught and their KGB connections exposed. Reading this book will give you a good understanding of what it takes to detect and then track down a hacker and beat him at his own game. It will also give you an appreciation of the difficulties involved in trying to protect ourselves while staying plugged into the rest of the world. It reads like a detective story and imparts solid knowledge. (Incidentally, neither the computer-security folks at the installations the hackers were invading nor various U.S. government agencies come off too well.)

(U) *Being Digital* by Nicholas Negroponte. An engaging, if shallow, ramble along some of the implications of the brave new world of interconnectedness. If you haven't thought much about the subject, this is a good book. If you have thought about it at all, wait for the library copy and skim it.

(U) *Silicon Snake Oil* by Clifford Stoll. The author of *The Cuckoo's Egg* waxes eloquent about what we seem to be losing in all the hype about cyberspace and being interconnected. He stops short of coming down on the side of the luddites who would have us all unplug and return to the age of Dickens, but he does decry the loss of face-to-face human contact. He makes a reasoned case that much of the cyberspace story has been oversold and that we are in for some disappointments. He says the computer will never provide a real sense of community and in fact works against it. He also reminds us that limiting our connectedness or choosing not to connect at all remain viable alternatives.

(U) *Masters of Deception* by Michelle Slatalla. This is an entertaining and disquieting look into the mind of cyberspace gang members. It centers around the story of a now-famous hacker who is doing time in the "big house" for his exploits. The book is well written and the tale moves along like good fiction. The ethos of the hacker comes through well, as does a solid feel for the hacker culture.

(U) In the fiction category the following IW-related titles have recently been published.

Debt of Honor by Tom Clancy. The Stock Exchange can be used to make a point as well as money.*Black Cipher* by Payne Harrison. An evil cabal in GCHQ tries to hide from a brilliant cryptanalyst (not to mention a

good card player).

Interrupt by Toni Dwiggins. Who says the phone system is always there when you need it?

Heavy Weather by Bruce Sterling. Mad Max meets the cyberpunks in an almost-doomed post-eco-disaster world.

Neuromancer by William Gibson. Still the classic of virtual reality for those who would rather have a cyberlife than no life at all.

[redacted]

P.L. 86-36

P.L. 86-36
EO 1.4.(c)

Book Review

China's Air Force Enters the 21st Century. by Kenneth W. Allen, Glenn Krumel, and Jonathan D. Pollack. Santa Monica, California: RAND, 1995.

P.L. 86-36

Reviewed by [redacted]

~~(C CCO)~~ The principal author of this groundbreaking study of the Chinese Air Force is Kenneth W. Allen (a retired U.S. Air Force major), [redacted] Mary McGarrahan, [redacted]

~~(C)~~ Ken Allen later served with distinction as an intelligence officer with PACAF and at the Defense Intelligence Agency. As a Captain, he was an assistant Air Force attaché at the U.S. Embassy in Beijing at the time of the pro-democracy movement and the demonstrations in Tiananmen Square. This volume is an outgrowth of research begun in Beijing by Mr. Allen in the latter part of the 1980s.

(U) Simply put, ***China's Air Force Enters the 21st Century*** is the single best book on the Chinese Air Force which has yet appeared in the English language. Allen and his co-authors have made unprecedented use of original source material not heretofore available to the general public. They present a cogent and conservative analysis of the Chinese People's Liberation Army Air Force (PLAAF), its history, its organization, and its potential. Unlike a number of commentators, the authors do not treat the Chinese armed forces as if they were marching inexorably toward the domination of East Asia. Messrs. Allen, Krumel, and Pollack quite rightly point to several critical problems facing the PLAAF in the next several years in the areas of leadership, manpower, technology, budget, and competition.

The PLAAF plans to replace obsolete aircraft with models like the upgraded Super-7

(U) Among the specific challenges facing Beijing, the authors cite block obsolescence of aircraft types. In the foreseeable future, the PLAAF will have to replace the F-6/FARMER fighter, a Chinese version of the 1950s era Soviet MiG-19 design. Currently, the F-6 fleet comprises some 65% of the total fighter inventory. The PLAAF is trying to address this need by means of indigenous programs incorporating foreign technology (upgrades to the F-7/FISHBED and the F-8/FINBACK, the Super-7, the FB-7) and through outright purchases of foreign aircraft (notably, the Russian Su-27/FLANKER). Incorporating these new aircraft types into PLAAF tactical operations, however, will require significant changes in procedures and a great deal of training.

(U) Allen and his colleagues make clear that the Chinese Air Force is operating under serious financial constraints. As they put the matter, "It is difficult to understate the scale of resources that would be required for the air force to make an effective transition to a credible, modernized force structure." Simply buying Russian or European or even American systems "off the shelf" may be relatively more cost-effective in the short run than designing and producing these systems indigenously. In the long run such a policy would be extremely damaging to the health of the Chinese aviation and aerospace industries, and would undermine any attempts by the PLAAF to become self-sufficient. A combination of indigenous production and imported technology appears to be the preferred Chinese solution.

(U) If the volume has a measurable flaw, then it is one of omission, not commission. The book cries out for photographs of PLAAF aircraft, senior officers, and the like. Nonetheless, the individual chapters and appendices are chock-full of valuable detail on leadership, force structure, strategy, education and training, budget, the political commissar system, PLAAF ranks, aircraft procurement programs, fighter aircraft, and air defense.

(U) The authors state that the PLAAF does not pose a serious threat to the United States or its interests at present. They point out that this relative situation will not change dramatically over the next ten years or so. In the longer run, however, China may well develop a potent air force—if the PLAAF continues modernizing its aircraft, weapons systems, force structure, aerospace industry, and doctrine. Much will depend on the political will of the leadership in Beijing and their allocation of resources.

~~(S)~~ The so-called "RAND study" apparently has become somewhat of a *cause célèbre* for the senior leadership of the Chinese armed forces. According to the U.S. Defense Attaché Office in Beijing, the Chinese Central Military Commission has begun an investigation into "how such sensitive information on the PLAAF could have gotten into the hands of the RAND people." Allen's book is being translated into Chinese in order to facilitate this investigation. Furthermore, the PLAAF is taking another look at its budgetary requests in light of the critical comments made by Allen and his colleagues.

[redacted]

(U) Mr. Allen and his colleagues could not have asked for a better review of their ground-breaking work on the Chinese Air Force than that. A notable book, indeed.

(N.B. Mr. Allen would be happy to receive questions or comments on his book. Please send your remarks to **cryplog@nsa**. We will pass them on to the author.)

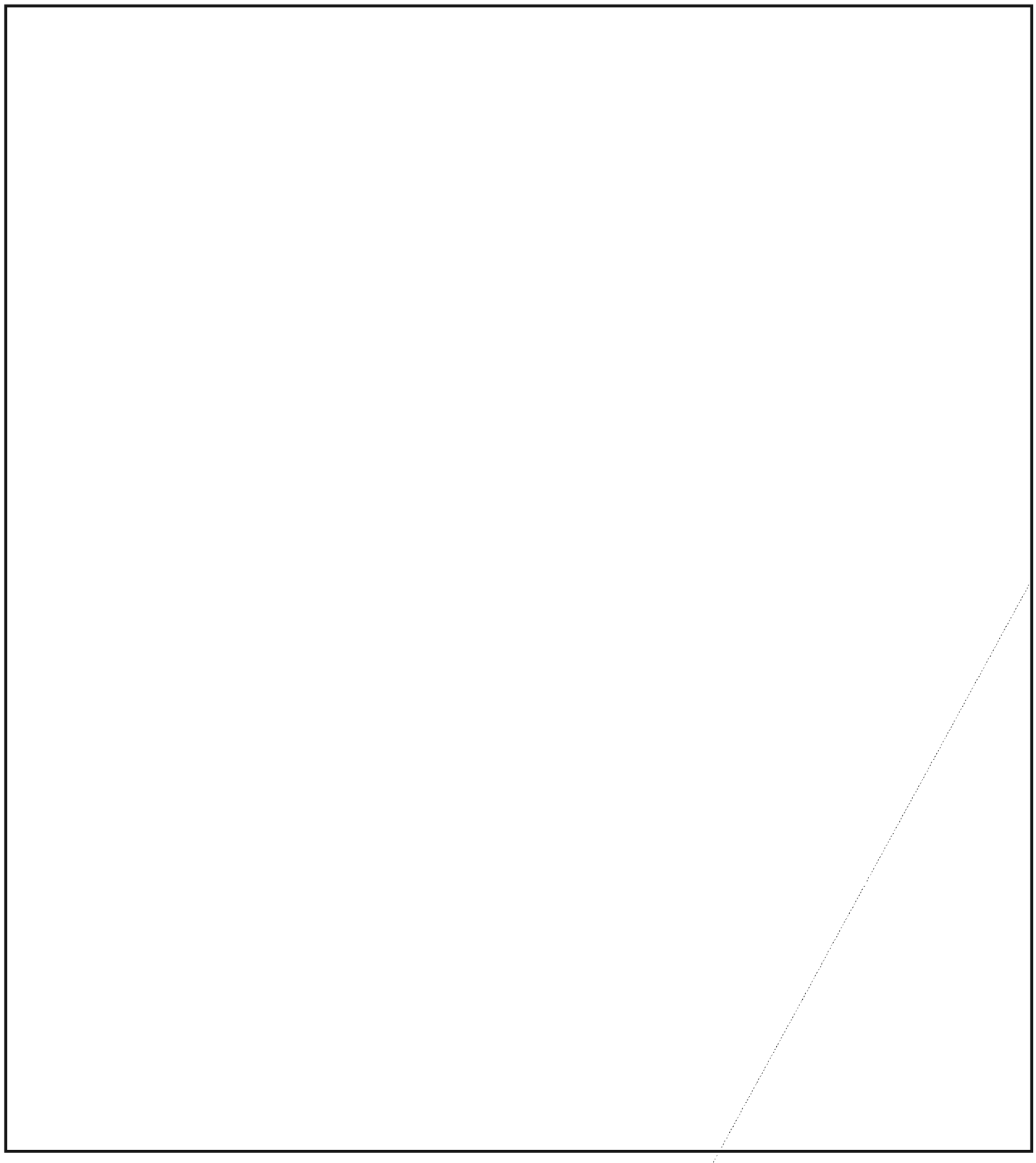
[redacted]

Kλ

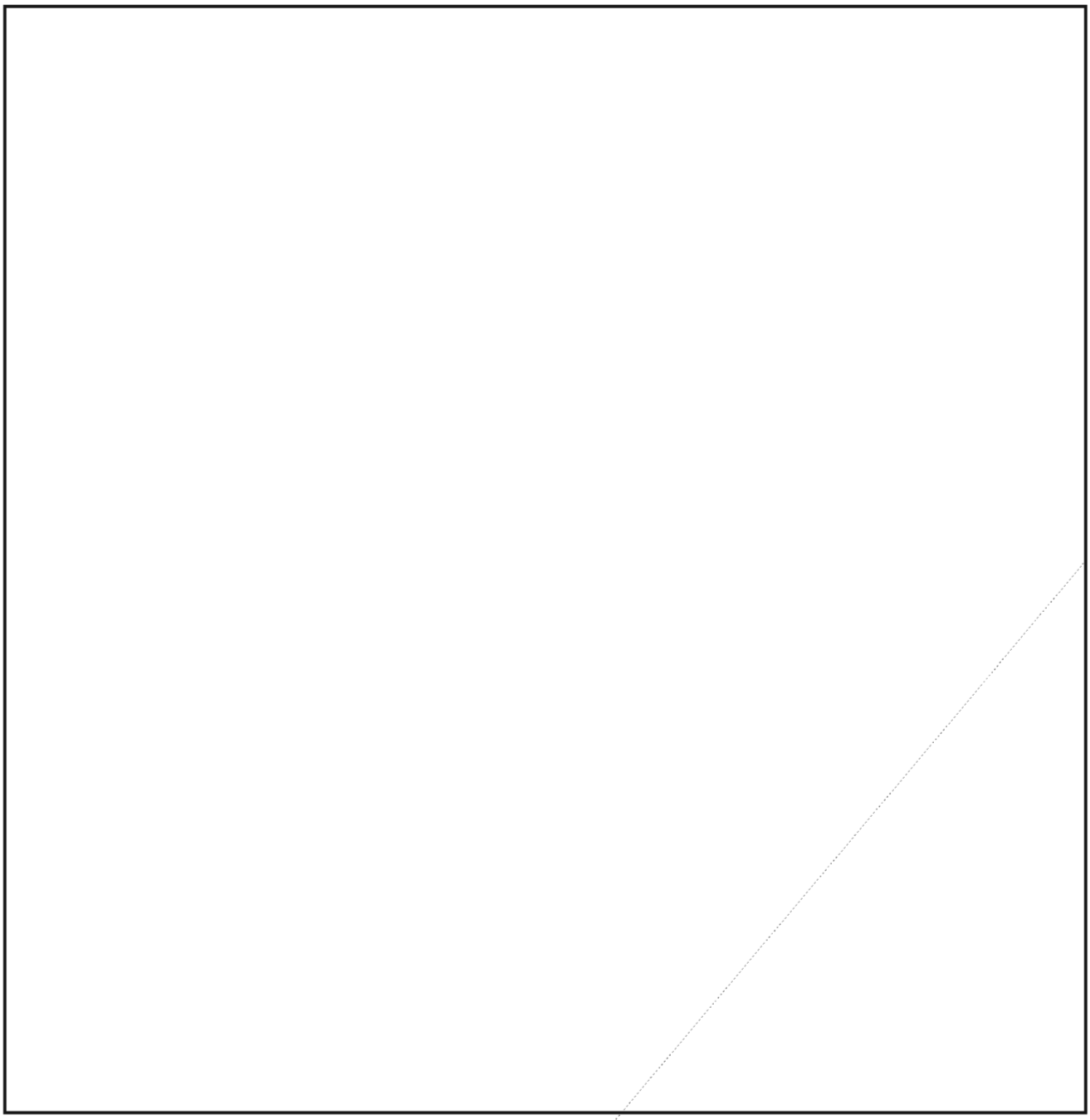
P.L. 86-36
EO 1.4.(c)

Cryptologic Lessons Learned

An Excerpt from N25's Data Base



EO 1.4.(c)
P.L. 86-36



Kλ

EO 1.4.(c)
P.L. 86-36

DOCID: 4010113 UNCLASSIFIED
P.L. 86-36
EO 1.4.(c)

SIGINT Bloopers

We begin, as before, with the Homonym Pitfall:

[redacted] Does the State Department know how frequently the international affairs of that town in Howard County show up in our product? Imagine the USSID 18 restrictions!

Either the reporter or the editing staff must have been hungry when they sent out a product that referred to the capital of India as "New Deli."

"The rebel leader and his principle ally"—nice to know the ethical aspects of rebellion are being handled properly.

Again, it's not just product reports: an official security regulation warns against drawing "undo" attention to one's place of employment, while an office-level action memo asked the organization concerned to "pole" its people.

In the Mark Twain (Almost But Not Quite Right Word) category:

"The UN representative said the political solution was under control but worrisome"—you've got to watch out for those solutions; they can get out of hand.

"Reports on Withdrawal of Heavy Weapons Seem Contrary"—maybe those reports got up on the wrong side of the bed.

One product report referred to "the three phases of the process, vice disarmament, demobilization, and reintegration of the combatants." We racked our brains trying to figure out what those phases could be, if not disarmament, etc.? A phone call to the OPI revealed that the reporter had been thinking of "viz." vice "vice." (On a serious note, this is a prime example of why we publish this column: such errors can result in a report saying the opposite of what was intended, as in this case.)

Other howlers can only be classified as Just Plain Weird Writing. "Bovine medical assistance to Fredonia is imminent"—what Gary Larson-like images this one conjured up! Apparently the reference was to the expected arrival of a team of foreign veterinarians, but references to "udder devastation" and "milking the situation" floated around the office for some time. Our favorite comment on this one was that it gave "Medecins Sans Frontieres" a whole new meaning: Doctors Without Fences...

In another case, the giver and taker of a bribe were described as involved in "bilateral corruption" (as opposed to the ordinary kind).

Anthropomorphism is evident in some OPIs:

"The controlling authority ordered the relay station not to harm the hostages." Who knows what that radio equipment will get up to if you don't keep an eye on it.

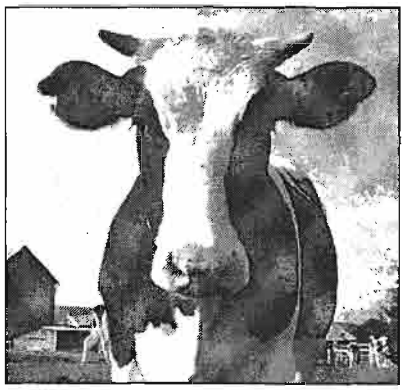
"The nuclear briefcase accompanied the president and was active during the visit."—bet that briefcase was the life of the party.

"The ambassador's Zendian residence learned that he would be leaving." He must have one of those "smart houses" that he can tell when to lower the heat and turn on the voice mail.

From the Department of Redundancy Department:

"Although the situation in Fredonia was untenable due to anarchy on the streets of the capital, Fredonia could remain in untenable straits for quite some time longer." (This was issued by an OPI that thinks "undercurrent" is two words.)

From the same report: "The extent to which the prime minister will act is unknown at this time and no evidence of such is currently available." "He may become a future rival"—well, as long as he stays a future rival, there's no need to worry.



Drink a glass of milk before bed and call me in the morning

As before, thanks to all contributors; examples may be sent to P054 in Rm. 3E027, Ops. 1, or via e-mail to **cryplog@p.nsa**.

Kλ

Editorial Policy:

(U) Technical articles are preferred over those relating to management, shorter over longer (under 3,500 words). Emphasis should be on improving NSA's technical performance; articles should be aimed at explaining developments in one's career field to thos outside it. Readers are invited to contribute conference reports and reviews of books, articles, software, and hardware that relate to our missions or to any of our disciplines. Editorials are also welcome, as is humor. Submissions may be published anonymously, but the identitiy of the author must be known to the editor.

Submitting Articles:

(N.B. If the following instructions are a mystery to you and your local ADP support is no help, please feel free to contact the CRYPTOLOG editor on 963-3123s or cryplog@p.nsa.)

~~(FOUO)~~ Send a hard copy accompanied by a labelled diskette to the editor at P054 in 3E027, Ops. 1, or send a soft copy via e-mail to **cryplog@p.nsa**.

Guidance:

For maximum efficiency (as far as possible within the limits of your word processor):

- Do not type your article in capital letters.
- Classify all paragraphs
- Label all diskettes, identifying hardware (operating system: DOS, UNIX), density and type of word processor used, your name, organization, building, and phone number.
- FrameMaker format is preferred; ASCII text is also fine. J334 has a conversion service that converts Interleaf, WordPerfect, OfficeWriter, and MS Word into FrameMaker. Just attach the document to an E-Mail Compose Window addressed to **convert@nsa**.

DOCID: 4012045

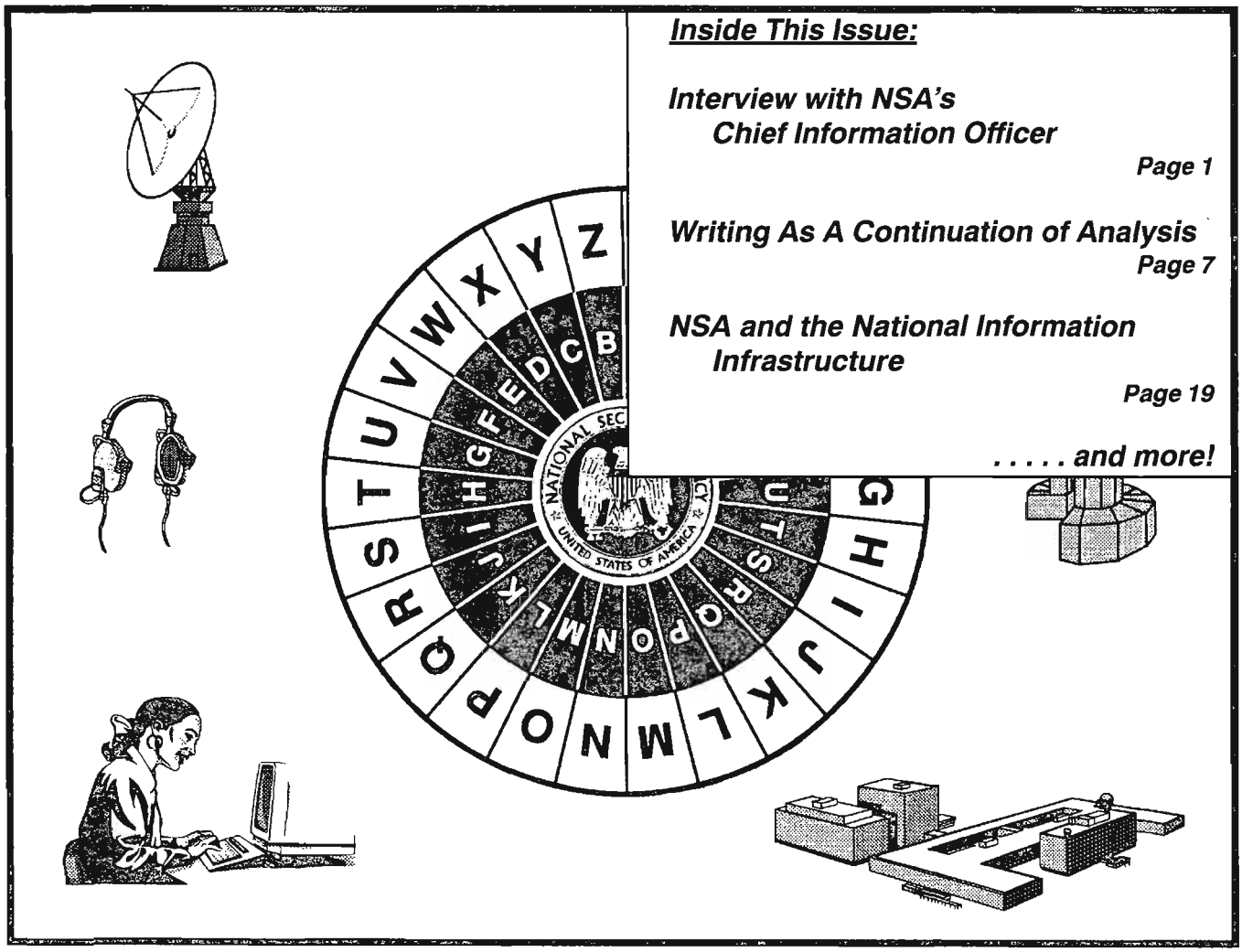
~~TOP SECRET~~

NATIONAL SECURITY AGENCY

CRYPTOLOG

The Journal of Technical Health

Vol. XX, No. 2 SUMMER 1995



Inside This Issue:

Interview with NSA's Chief Information Officer *Page 1*

Writing As A Continuation of Analysis *Page 7*

NSA and the National Information Infrastructure *Page 19*

. . . . . and more!

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~
~~TOP SECRET~~

DOCID: 4012045

P.L. 86-36

CRYPTOLOG

Summer 1995
Vol. XX, No. 2

Published by P05, Operations Directorate Intelligence Staff

Publisher ..... William Nolte (963-3123)

Editor ..... [redacted] (963-3123)

Board of Advisors

Chairman ..... [redacted] (963-7712)
Computer Systems ..... [redacted] (963-6669)
Cryptanalysis ..... [redacted] (963-4382)
Intelligence Analysis ..... [redacted] (963-6283)
Language ..... [redacted] (963-5704)
Mathematics ..... [redacted] (963-1363)
Signals Collection ..... [redacted] (963-5717)
Signals Collection ..... [redacted] (968-7160)
Telecommunications ..... [redacted] (996-7847)
Member at Large ..... [redacted] (968-4010)
Member at Large ..... [redacted] (968-4010)
Member at Large ..... [redacted] (961-8214)
Classification Officer ..... [redacted] (963-5463)

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

To submit articles and letters, please see last page

DOCID: 4012045

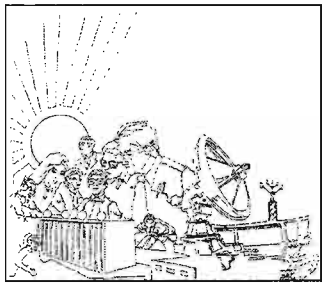


Table of Contents

Interview with NSA's Chief Information Officer, by [redacted] 1

Writing as a Continuation of Analysis, by [redacted] 7

Journalistic style, yes; creeping Clancyism, no! by [redacted] 9

Managing Linguists in Low-Density Languages, by [redacted] 10

The National Information Infrastructure (NII), by [redacted] 19

What's This New Intercept I'm Seeing? by [redacted] 25

The Unfocused Eye: [redacted] by [redacted] 28

Intelligence Analysis Off-site and Open Forum, by [redacted] 32

IA vs. TA/IR: An Editorial by [redacted] 38

The Phoenix HF: An Editorial by N.C. Gerson 40

NSA's "Lessons Learned" Database, by [redacted] 41

The 1995 Joint Mathematics Meetings, ed. by [redacted] 42

SIGINT Bloopers 49

Book Reviews 50

SIGINT Glossary: The Chun Wheel, by [redacted] 55

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

P.L. 86-36

Perspective:

An Interview with Terry Santavicca, NSA's Chief Information Officer

by [redacted] P.L. 86-36

Terry Santavicca, formerly chief of DDT's staff, has become DDO's first Chief Information Officer (CIO). He has served as chief of the DDT staff, Deputy Chief of DDT's Telecommunications Group, and Chief of the Office of ADP Support [redacted]

Why was the CIO position created?

~~(FOUO)~~ It arose from the study commissioned about a year ago by Dr. Mueller (then DDO) to look at the state of information systems and ADP (automated data processing) within DDO. He felt that there were a lot of ADP-related activities going on in DDO that weren't well coordinated and that the culture was "stovepiped." P.L. 86-36

~~(FOUO)~~ So the DDO commissioned what's sometimes called the [redacted] Study: [redacted] chief of J, and [redacted] who was in DDP at the time, spent several months talking to a lot of different people inside and outside DDO. Of the many observations and recommendations of the report they published, the key one was that *DDO needed a CIO who reported directly to the DDO*. Dr. Mueller, who agreed, ran this by his group chiefs, who concurred, and shortly thereafter I was named as the DDO CIO. (Shortly thereafter Dr. Mueller left, but Ms. McNamara, the new DDO, has been every bit as supportive.)

~~(FOUO)~~ I arrived here to take up the CIO job in late February. The idea was that somebody at a senior level in DDO would pull together the disparate activities in the ADP/information systems world and to coordinate and interface with other key components as appropriate to work these issues.

How have the other directorates reacted to the establishment of the CIO?

~~(FOUO)~~ I think very well. In my view, part of the strategy of assigning me as a former (and long-time) T person to DDO was to try to forge better ties between DDO and DDT in particular—those being the two main organizations involved in systems development, ADP and processing, etc. So I consider it part of my mandate to do that, but in order to accomplish that I've tried to expand current or initiate new forums to allow that to happen. For example, the ADPX (ADP Executive Committee), which had existed for some time, did include representation from T. Since I've come on board and now chair the ADPX, I've expanded the ADPX to include representation from all key components. More and more of the ADP issues and architecture and networking and so on really are corporate issues and need to be worked in a corporate way.

~~(FOUO)~~ [redacted] and I have agreed to co-chair a new board called the NSA Information Systems Group (NISG), a high-level IS direction and policy board which will have CIO equivalents from each of the key components who would deal with corporate, cross-organizational ADP-oriented issues, something like the ADPX but at a level higher. The ADPX would work issues, problems, standards, and so on from its level, and then the NISG would determine final policy and implement or promulgate agency-wide.

~~(FOUO)~~ Also, as the CIO, I represent DDO on the Technical Architecture Board (TAB), which is primarily a DT forum that relates to DDO's Requirements Executive Board (REB), which I am also a member. I know, more acronyms, but the point is there are renewed efforts for DO and DT to work more closely in coordinating requirements, architectures, and system developments.

Do you see any potential conflict with DDI?

(U) Well, the kind of issues we're working are not, I think, those that are the mainline business of DDI. It's more architectural strategies, and how they get networked in with the rest of us. When we come up with agency standards, we want to make sure we coordinate with them as well: standard workstation issues, and so on.

Since you mention standard workstations, is NSA going to continue to "recycle" older terminals, or will every analyst eventually have the same functional capability?

(U) Because of the HPW-2 contract, this is a bit of a contentious issue. The HPW-2 has been in effect for some time now but it has not really taken off very well even though the prices on the contract are very, very competitive. But because people have been so locked into Sun, have gotten so familiar with the workstations, and because our system administration is oriented toward Sun, we've had a very hard time taking advantage of the HPW-2 contract.

(U) We're making renewed efforts to better integrate the HPW-2 into our environment but as a longer-term vision, to get back to your original question, I wouldn't like to see an HPW-3 contract bid competitively.

You think that more weight ought to be given to integrating a future HPW with what is here, rather than the basic cost of the next HPWs?

(U) Yes. Well, I think we have to worry about cost, but what we don't want to do is to be locked into any one vendor. And of course the vendor's strategy is to try to lock you in. But if NSA wants to be in a position to take advantage of the very fast-paced technology, the best that's out there, we have to build an environment that will be heterogeneous.

(U) Now I think the right way to do that is to figure out how we can integrate a variety of vendors' products in this environment. And I think the right way to do *that* is to define our environment in terms of standards, the standards that it would take to fit into our environment and operate in a transparent way. Now that's a little bit idealistic but standards *are* moving in that direction. We can't yet define such an environment, but there are standards, for example, a single UNIX standard: the UNIX world *is* converging on a single UNIX and a lot of the vendors are working toward it. SOLARIS, Sun's operating system is on that path as well as IBM's AIX operating system.

~~(FOUO)~~ [redacted] There is certainly a lot more commercial off-the-shelf (COTS) software out there available in the non-UNIX world than in the UNIX world. So in the long term we need to be careful to build an environment and a strategy that will be able to take advantage of all the kinds of things that are out there. That may mean we have to figure out how to integrate Windows NT into our environment—see, I said I'd get controversial. I know this'll make people's hair stand up, but I honestly believe that we cannot close off any of our options. I mean, five years from now UNIX might not be around, it might not be a viable system. When vendors develop a capability they usually develop it first on the systems that have the broadest market, and that typically is not UNIX. So we need to keep our minds open to non-UNIX as well as UNIX.

People like to use what they're comfortable with on the outside.

(U) That's right, and the majority of NSAers probably have personal computers at home, and they're not likely to be UNIX, so we don't really leverage what people learn and use and know how to use from home when they come to work. That's another disadvantage—I mean, UNIX does have a lot of good things going for it. It's always been very good in a networked environment and it's a very rich operating system on a workstation, whereas a lot of these older systems like DOS are very batch-oriented, you couldn't do multiprocessing, but now the rest of the world is catching up and there's not as much of a difference.

(U) I'm not anti-UNIX, by the way; I just want us to keep our options open. UNIX has served us well and will continue to do so. But, the direction nowadays not only at NSA but the entire community is COTS products, and there are a lot of COTS products out there to pick from, and the majority of them are not on the UNIX side.

What skill mix do you see the various computer-oriented specialties at the agency needing? For instance, how enthusiastic are hard-core programmers going to be about—well, the term "peeling shrinkwrap" has been heard.

~~(FOUO)~~ Yes, I can understand why there might be some concern in that area. NSA has a long history of in-house development of major capabilities, major systems. I think the pendulum is swinging away from that. I think there will always be some subset of our capabilities that, because of the uniqueness, will have to have in-house development of at least parts of it. I think we'll have to learn how to do a better job of integrating various software packages together to build a system. The

emphasis is to encourage people to look for software that's already available rather than to think in terms of writing new code: reuse libraries as well as COTS products. I know there are some efforts going on in some of our organizations to do this kind of software re-engineering. We've been holding discussions of perhaps setting up special servers on our networks that have shared libraries on them and encourage people to take advantage of them. Even now, through some systems, you can go in and pull off software.

System administrators will probably have to become more versatile, too, if they're going to be working with a greater variety of products.

(U) Yes. The SA problem is another area that concerns a lot of people, considering the variety of systems that the SAs have to support. Now I want to be careful how I say this, but the quality of our SAs is very uneven. We've sometimes picked people to be SAs from diminishing skill fields and moved them into system administration because they weren't needed elsewhere and some of them haven't had all the training that they probably could use.

(U) We need, through picking the right people, the right kind of training, and the right kind of tools, to make our SAs more effective than they are today. Because the environment is going to get more complex, and the technology is going to get more complex. Although there are some products on the outside and some tools becoming available that should make the SA function easier. Right now, every vendor sort of has his own way of doing system administration and sets of tools that apply only to the systems that they provide. But there are products coming out now that will sit on top of, and work for, a variety of different systems. I know J3 is looking at some things now; whether we can take advantage of some of them remains to be seen.

Do you envision the average analyst having multimedia access at their desk?

~~(FOUO)~~ Well, I don't know about the average analyst, but yes, we do envisage analysts having multimedia capability. In fact, we're in the process of coordinating a multimedia Project Baseline Summary (PBS)

[redacted]

P.L. 86-36

[redacted] Now it's not clear that NSA at the moment is funded at a level that can support that to the degree we think is really necessary. But we've put together a PBS and the new information-exploitation funding category is looking at that very hard and has defined a couple of what we call over-guidance packages to try to get more money to build up the infrastructure support.

~~(FOUO)~~ A little bit of a digression: another one of the recommendations of the [redacted] Study was that once the CIO position was established, one of the things it needed to be given was enough financial control to put some teeth into the CIO functions. In line with that, the categories involved with the ADP areas—the analyst-production, the language-exploitation, and the dissemination categories—have all three been put under the CIO. The analyst-production and the language-exploitation have been combined into a single category called **Information Exploitation**, and it's that one that's sponsoring the multimedia initiative. (The CA community still has their own funding category and they fund their own ADP, so that's not included.)

P.L. 86-36

Doesn't multimedia require tremendous amounts of bandwidth and storage?

[redacted]

Video-teleconferencing is another capability that some see as absolutely essential and others see as merely a frill.

(U) I think teleconferencing can help a lot but it's not the complete solution. I think there are times that sitting together face to face to work out things is the right way to do it. So I wouldn't be one of those that say that the future of communications is that everybody will stay at their desk and just teleconference. And again, teleconferencing requires a lot of bandwidth.

So we're not just talking about saving TDY money.

~~(FOUO)~~ No, in fact, I know Q looked at that, and concluded that the amount of money it would take to set up a reasonable teleconferencing capability would fund a lot of TDYs. So it's not like you can take a couple of TDYs' worth of money and set this up. Even if you could easily switch the money from one pot to the other.

You mentioned information exploitation; what other areas related to that have you gotten involved with?

(U) I'm amazed every day at the things that the CIO gets involved with! I think since the position's been established it's been a target of opportunity.

(U) One of the primary objectives I have is to encourage teaming both within DDO and across organizations, especially DO/DT, but wherever appropriate. With the kinds of things that NSA now gets involved with, everything doesn't always fit nicely in an organizational structure, and we can't afford to reorganize every time something changes, so the current philosophy is to try to form teams to work issues and solve problems and work projects wherever possible and that's something that I'm encouraging people to do. I'm mentoring several different efforts that are using that approach and people have come to me and said, "We are working with some people in this other organization outside ours; here's what we're working on, but we don't know where else to go to, and the CIO seems like an appropriate place to start, so can you help facilitate our project?" So I've taken on a couple of those to help facilitate cross-organizational cooperation.

(U) One of the things that I think in general NSA doesn't do a very good job of, I find after discussions with the A/DDT, is that we don't plan well for success. By success I mean once we come up with a good capability, either developed in-house or perhaps brought it in from the outside, we're not very good at figuring out how to make it available in a broad way in the agency. We'll take it into one organization, put it on some analyst desks and say here, maybe this'll help you out, but what if we were to deploy, say 5,000 of a successful capability? We just don't do that very well. We'll bring things along to a particular point and then not do a good job of making it available in a timely manner and conducting all the associated training.

Do you mean in the sense of acquisition, or in the sense of disseminating the information that a capability is available?

(U) I think all of the above. How many times have you found out about some neat thing from somebody who said, "the guys downstairs brought this up and put it on my desk and boy, is it nice." And you say, well, why doesn't everybody have this capability? We just aren't geared for deploying things in a significant way when they're successful.

This is a cultural problem, too, isn't it? For instance, computer-support people might say we don't know how long it would take us to learn this, so we don't know whether we can sign on to support it.

(U) Yes, that's part of it, too. We don't always fund for it, we don't always consider what's going to have to be in place if a project succeeds, so we don't plan for the training that might be needed for people to take advantage of it. Sometimes we depend on the developers to show their product around.

P.L. 86-36

So we need to do a better job of marketing.

(U) We do. We need to plan *early in the process* for how we deploy if we're successful. I think there have been some very valuable things developed here at NSA that are not as effectively used as they could have been, not as broadly used because we have not done a good job of deploying them.

Are you involved with any of the process re-engineering efforts currently underway?

~~(FOUO)~~ I'm mentoring the [redacted] effort. If you're not familiar with [redacted] let me back up a little and give you some background. DDO some time ago defined its three core processes as ***acquiring data*** (collection), ***adding value to data*** (analysis), and ***reporting*** (dissemination) to the customer. [redacted] was an effort that looked at the reporting side, a core-process review of the systems and processes involved on the reporting side and how to improve, and to consolidate systems. They defined a single reporting vehicle that all reporters would use so that you wouldn't have "pprep" in one organization and something else in another goup. [redacted] is the consolidated reporting vehicle.

~~(FOUO)~~ [redacted] is the core-process review of the analysis function within DDO. While the boundaries are a little bit fuzzier, it incorporates everything from the collected data until you get ready to start the reporting process. The [redacted] team has representation from throughout DDO and DDT. They've

been operating now for several months, and are hoping to finish their process review this fall, but again, they're looking at all the processes involved in the analysis function and the systems involved, looking for opportunities to re-engineer and consolidate, they're looking at and trying to define the **legacy** systems and the **migration** systems for two reasons: one, for internal NSA purposes—that is, which legacy systems do we want to stop putting resources into, and which are the systems we want to migrate to, that is emphasize and build to for the future. This is being done both for NSA purposes and because at the DoD community level Intelligence Systems Board (ISB), there's an effort to do this across the intelligence community agencies. Each agency is being asked to define its legacy and migration systems. These will be looked at across the community and certain agencies will be given the lead to define the "best-of-breed" migration system in a particular area. They will get funding to proceed and provide that capability for the community. The implication of this is that those systems determined to be legacy systems will have money taken away from them and provided to the agencies which have been tasked to lead the charge with their migration systems.

Are you involved with INTELINK?

~~(FOUO)~~ Yes, INTELINK in a sense is the intelligence community's migration system for dissemination, since it's been determined that all agencies will use INTELINK for dissemination.

What is the value of NEWSMAGAZINE? Is this something you think every analyst needs a connection to, or is that the sort of thing that can be limited to staffs? I know some people think of it as "bells and whistles."

(U) I think at the moment it certainly isn't necessary for everybody to have, but I think there's potential there, as we make more and more presentations, briefings, etc. available on NEWSMAGAZINE. Especially when we're split up among buildings, it's very hard to get people to get up from their day-to-day work and go to various presentations. As our infrastructure can support more of this I think we could use it more for desktop training. Even if it's not available on every analyst's desk, if it were at least available in a number of places scattered throughout, people could just go down the hall to a conference room—that would be helpful. There are many occasions when I'll see a briefing or something advertised that I'd be interested in but then I hear it's over in the R&E building, and adding the travel time makes it hard to squeeze into my schedule.

What about things like Internet access? Which you find preferable as far as efficiency or anonymity: bringing Internet newsgroups into the agency or encouraging people to go out on their own?

(U) There are a lot of thorny issues here. Ideally one would like people to be able to go out onto the Internet on their own; there's certainly a wealth of information available—I've attended a couple of briefings where people have talked about very significant things that have come off the Internet—but I think we have to be very careful in how we approach it for security and anonymity reasons. The kind of things that we're capable of doing in networks and so on, you assume other people could do if they really wanted to.

Net exploitation, good old TA term.

~~(FOUO)~~ Right. But I think there are people at the agency right now looking at the whole picture of what our policy should be with the Internet, and I think we will arrive at something that's a compromise between everyone going his or her own way and the opposite extreme, which would be one office, such as E3 (the open-source authority) being the only one permitted access to the Internet and everyone else would have to submit requirements to them. I think the open-source people will have the capability to go out and do research for us, but I think we will also have the ability in a well-defined, structured way, for analysts to go out and find information on the net. There's no replacing the ability for the target analyst who has the ability to follow threads through the net and find out information. But I think we'll have to have some well-defined procedures on how that will happen so that we don't make ourselves vulnerable.

What do you hope to have accomplished by the end of your first year in office? Have you any very definite goals yet?

(U) I guess my goals would be to have made a significant improvement in changing the culture to more of a teaming culture, having organizations think more corporately, rather than an organization coming up with, say, "the Alpha-123 organization's standard or policy on such-and-such," to think in terms of "OK, we think there's a need for such a standard or such a policy, we'll

take the initiative to get it started but let's try to work it as a corporate issue, at least develop it in such a way that it can be built to be a corporate-level vehicle.

Get rid of the culture of "that's not how we do it in Alpha-789."

(U) Yes, and I'd like to do the same thing for when an organization sees the need to develop a capability. They should try to think, "Is this something that has broader applications so that we can develop it not just for our own little component, but where else does such a need exist? Maybe we can form a team with people in other organizations." I think some of the forums that I've tried to put in place for sharing information like the ADPX will help facilitate this.

(U) Another thing I was hoping to accomplish is to make some headway in defining some of the standards which can in turn define our environment. That, as I mentioned earlier, will help us take advantage of technology but it will also make us more efficient; it allows the developers something to use to provide uniformity across the agency. For example, the GUI standard. The graphical user interface (GUI) standard is something that now is being coordinated agency-wide, although we haven't officially promulgated it yet. It's been fully coordinated; the only thing left is to decide whether it should be a standard or a guideline or a manual, i.e. how are we going to promulgate it. But it is now accepted as an NSA standard, and that's something that every project should pick up and use. They should be able to give it out to contractors and tell them to comply with this NSA standard. So it makes us more efficient and it makes the developer's job easier. And it certainly makes the users of the systems more efficient and comfortable when they go from one system to another or one software capability to another; it makes the learning curve a lot easier when, say, the exit button does exactly the same thing on all of them.

Maybe the HPW-3 contract won't be with the company that has five different keyboards.

Yes, the number of keyboards has always been a problem at the agency!

Kλ

And speaking of information...

Tech Trend Notes publishes a Calendar of Events sponsored by NSA, academia, and professional associations. Here's a sample of what's happening this year:

Event	Date	Location	Where to call:
DoD Database Colloquium '95	29-31 Aug	San Diego, CA	(703) 631-6125
Information Superhighway Summit	11-14 Sep	Santa Clara, CA	(800) 225-4698
European Conference and Exhibition on Optical Communications	17-21 Sep	Brussels, Belgium	(44) 132 2660070
Electronic Data Interchange for Government	18-21 Sep	Washington, DC	(301) 445-4400
17th Annual Satellite Communications Users Conference	20-23 Sep	San Jose, CA	(800) 828-0420
C^3I Systems Technology Exhibit	27-28 Sep	Ft. Huachuca, AZ	(520) 452-7493
8th International Symposium on Artificial Intelligence	16-20 Oct	Monterey, Mexico	(52-8) 328-4197
OSS '95 -4th Int'l Symposium on Global Security and Global Competitiveness	7-9 Nov	Washington, DC	(703) 242-1700
ACM Conference on Mobile Computing and Networking	13-16 Nov	Berkeley, CA	(617) 332-1101

P.L. 86-36

Writing As A Continuation of Analysis

by [redacted]

(U) SIGINT people would agree that good analysis is essential to producing a good report. Yet, when presented with a profoundly inadequate report, most are inclined to criticise the reporting, i.e., the writing style, the organization, the lead (if there is one), or the title. Rarely do they merely cite incomplete analysis as the problem. Almost never in such cases does one hear the computer axiom, "Garbage in, garbage out." Maybe this reflects a habit of thinking that report writing is simply documentation of a completed analysis. If so, I suggest that it is a wrongheaded habit, that finishing the report—and that alone—should be viewed as completion of the analysis.

(U) People tend to think of analysis and reporting as a linear operation—first the analysis, then the report. Even experienced analyst/reporters who do not actually do it that way sometimes describe the process in linear terms. At best, those who take the linear pattern too seriously can produce some pretty eye-glazing reports. In the worst case, they put out the thigh-whackers NCS workshops and classes use to show how good reporting is *not* done. These are poorly organized examples without leads, or with buried leads, or with titles that do not reflect the lead.

(U) Such reports did not happen just because the analyst was a poor writer. They got that way because the analyst stopped thinking analytically before beginning to write, which is the worst way to write anything. Having assembled and researched the data, the analyst neglected to apply the most powerful tool in the analytic kit, the self-critical kind of writing that forces reporters to question the evidence, recheck the premises, do more research, and often come to a different conclusion. This is what I call *writing as a continuation of analysis*. It describes a philosophy that I believe ought to become an overriding theme in training intelligence analysts to be reporters.

(U) In the past, we have trained analysts to report, almost as if it were a separate function. If, on the other hand, we defined writing as a continuation of the analytic process, we would not just teach analysts how to write reports. We would teach them that writing the report is part of the analysis—the most important part. This approach cannot be applied to near-real-time, fact reporting, where the only questions are, "Did it happen?" and "Does it meet the criteria?" It is perfectly suited, however, to a situation in which two or more facts are subjected to analysis, research, synthesis, and judgment to report a meaningful event or discovery.

The pen is the tongue of the mind.

— Proverb found on a Thai beer bottle

Inspiration is where you find it

(U) Disciplined writing is analytic by definition. The currently accepted techniques of SIGINT Journalism conform to, and lay out a pattern for, completing an analysis while writing a report. The idea of thinking critically about what you are writing, or have written, is not new. Good writers, including good SIGINT reporters, have always done it. The point is that this is actually an analytic process which can be described, taught, and learned. Using it improves both the analysis and the writing. During the process, the analyst may discover that the data simply does not warrant a report. More often, the process will open a somewhat different perspective than the one with which the analyst began.

(U) Place yourself in the position of an analyst who has been working on a particular problem. You have done some research and pulled out some seemingly related data. Now you want to do something with it. As an analyst, you have to *organize* it, just what the SIGINT journalist has to do. You may have some of your report details, but you will need to analyze them to figure out how many of the critical Ws (Who/What/Where/When/Why/How) you have and what they are.

This will help you select, at least initially, which *organizational format* (Inverted Pyramid, Lead Plus Equal Facts, Chronology, or eclectic) you will use. It should also suggest a working lead/summary.

(U) A lead (we used to call it the SIGINT fact) is the most concise statement possible of what the report is about. Having read it, every reader should be able to make an informed decision to read on or not. Picking out a lead at this point may seem premature, but it will give direction to the analysis. Just remember that you will probably change the lead, maybe several times, before you are done. As a natural outcome of projecting your analysis into the writing phase, you will know more at the end than you did when you started. Now go ahead with a rough draft; you will not know what is missing until you lay out what you have.

They say that William Faulkner once covered the Kentucky Derby for *Sports Illustrated.* It was a beautiful work of descriptive prose that made no mention of the winning horse.

(U) Now you can start working on *thoroughness*; remember, this is analysis. Do the details support the lead? If yes, what questions are left unanswered by the details? If no, what lead do they support? Does the lead reflect what is most important in the details? If not, what is? Bang the lead against the details and the details against the lead; keep doing it with each change or addition. Focus and refocus. Expand your research. Write and rewrite. The goal is to get the lead and the details in perfect balance. That is a quick way of saying that the details should add up to what the lead says, and the lead should be a summation of the details. It is like reconciling your checkbook. If the two are not consonant, you must find out what is wrong and fix it. This may mean looking for new data, reinterpreting the data you have, or eliminating doubtful data and reconsidering your conclusion.

Where there is a surfeit of words,
there is a famine of ideas.

Anonymous, copied from an Air Force TIG Brief @ 1980

(U) Once the report has taken shape, start tightening it up. *Tight writing* is the perfect tool for detecting the less obvious gaps in your report and exposing inconsistencies in your analysis. Fat writing works like static on a radio; it clouds the factual and covers the spurious. Tightening the narrative eliminates the static. It allows you to see what is really there. You can tell what works and what does not. Get rid of the latter, and build on the former. Exclude every word, phrase, or sentence that does not contribute. What works for you, when you are thinking analytically, will work for the reader.

With some customers, the title is your only chance to score

(U) Now review the whole report. Have you answered all the questions you can and balanced the details with the lead? Is it the right lead; does it work? If so, write your title. The lead had to be the most concise summation of the report, but the title should go even more briefly to the core of the lead, invoke the most significant element(s) in the report, and compel the reader to check the lead. With some readers, the title is your only chance to score. Finally, be sure that the title lines up with the lead and the details as inalterably as they align with each other.

(U) There is no need to follow you through the necessary final edit for readability, punctuation, spelling, etc. The report is written; your analysis is done.

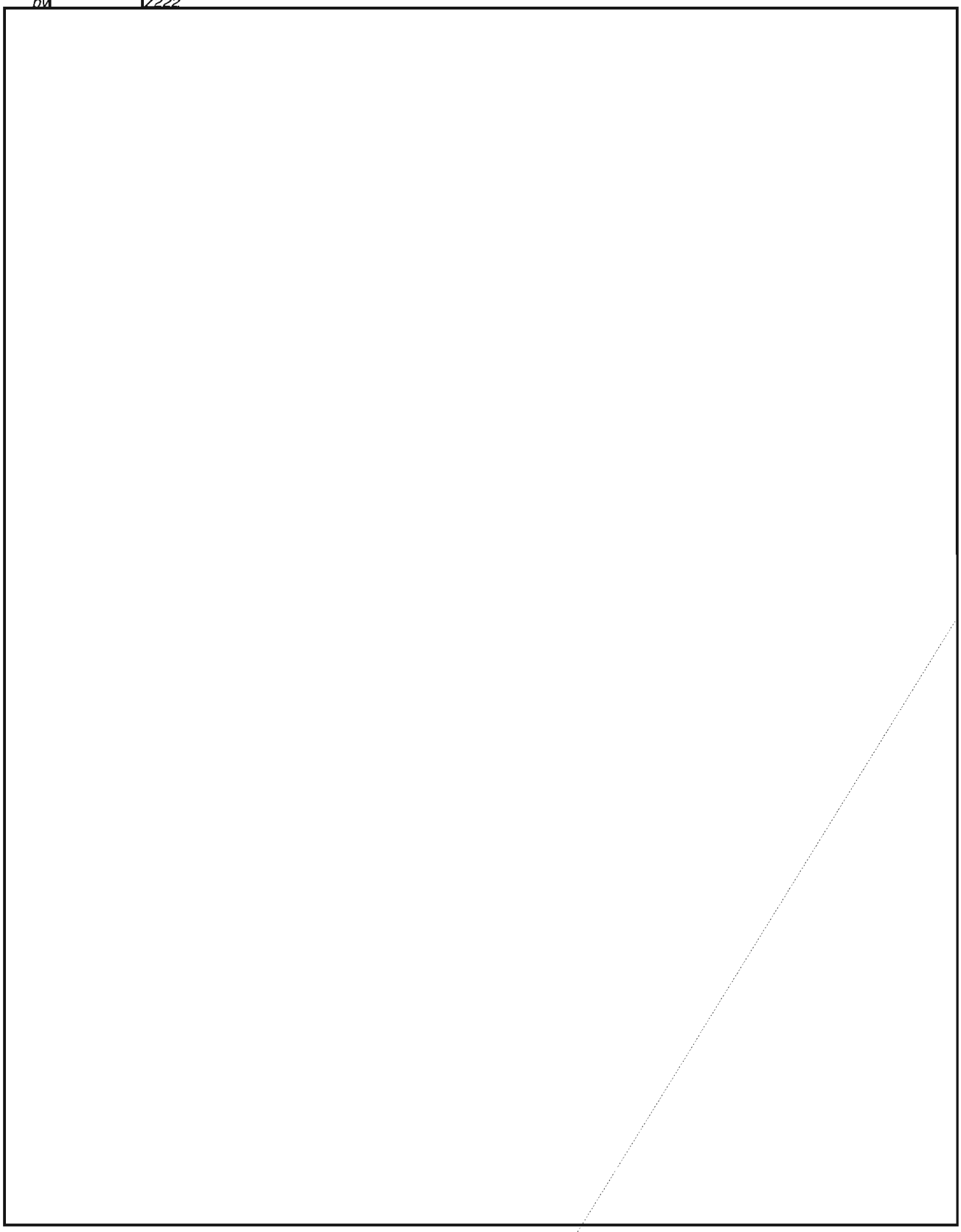
(U) The advantage of *writing as a continuation of analysis* is that it quantifies the analytic process. It provides a template that displays the analytic transformation of intellectual concepts into a measurable, testable thesis. That template is made up of procedures already imbedded in SIGINT Journalism. Thus, it comprises a system that is already taught as the correct way to write reports.

(U) Maybe our philosophy of how to train intelligence analysts to analyze ought to embrace and overlay our method for teaching them to write reports. *Writing as a continuation of analysis* offers that kind of approach. The outcome to be hoped for would be better analytic results more clearly and cogently presented in more widely read and influential reports.

Kλ

Journalistic style, yes; creeping Clancyism, no!

by [redacted] Z222



P.L. 86-36

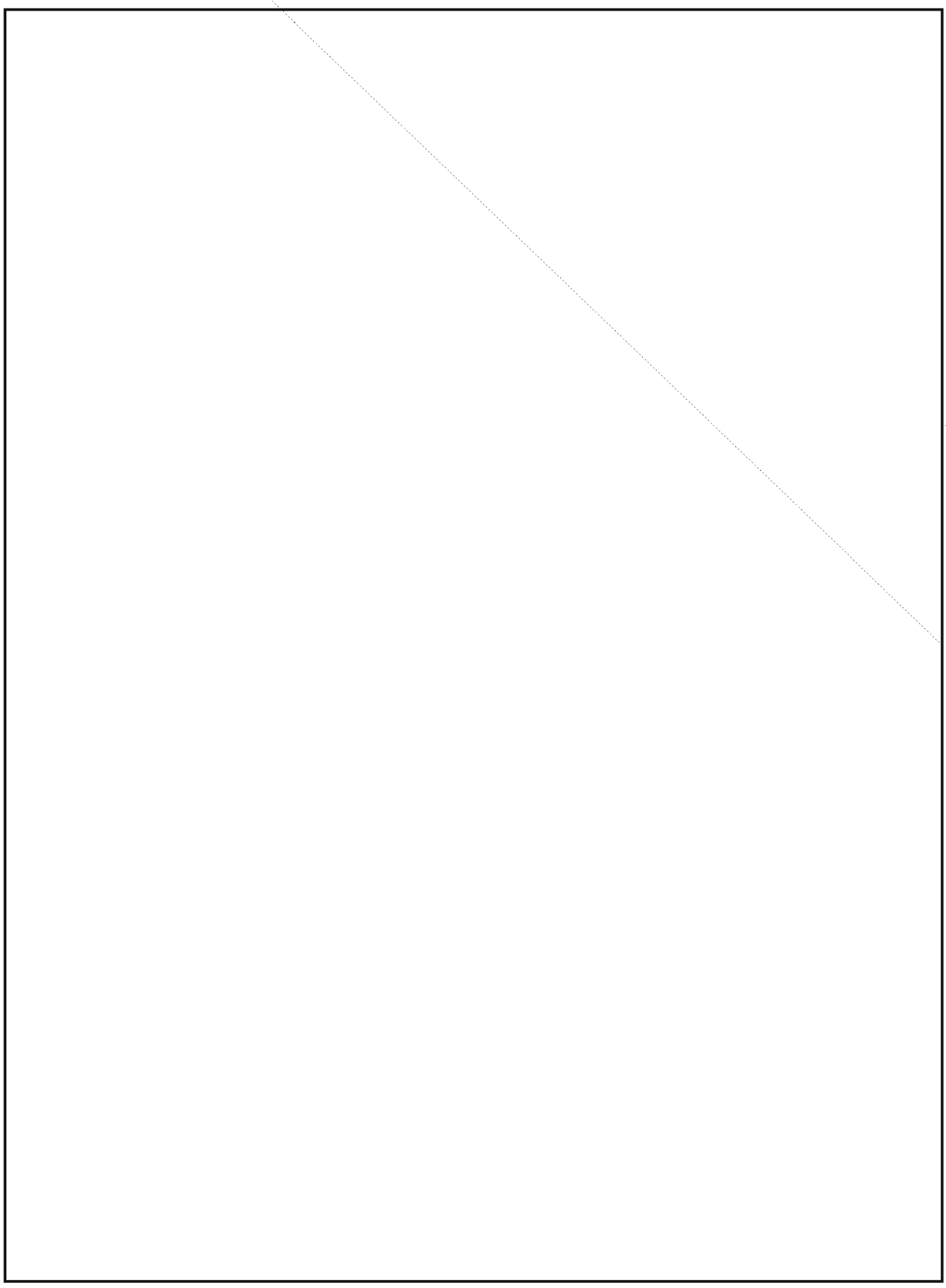
Managing Linguists in Low-Density Languages

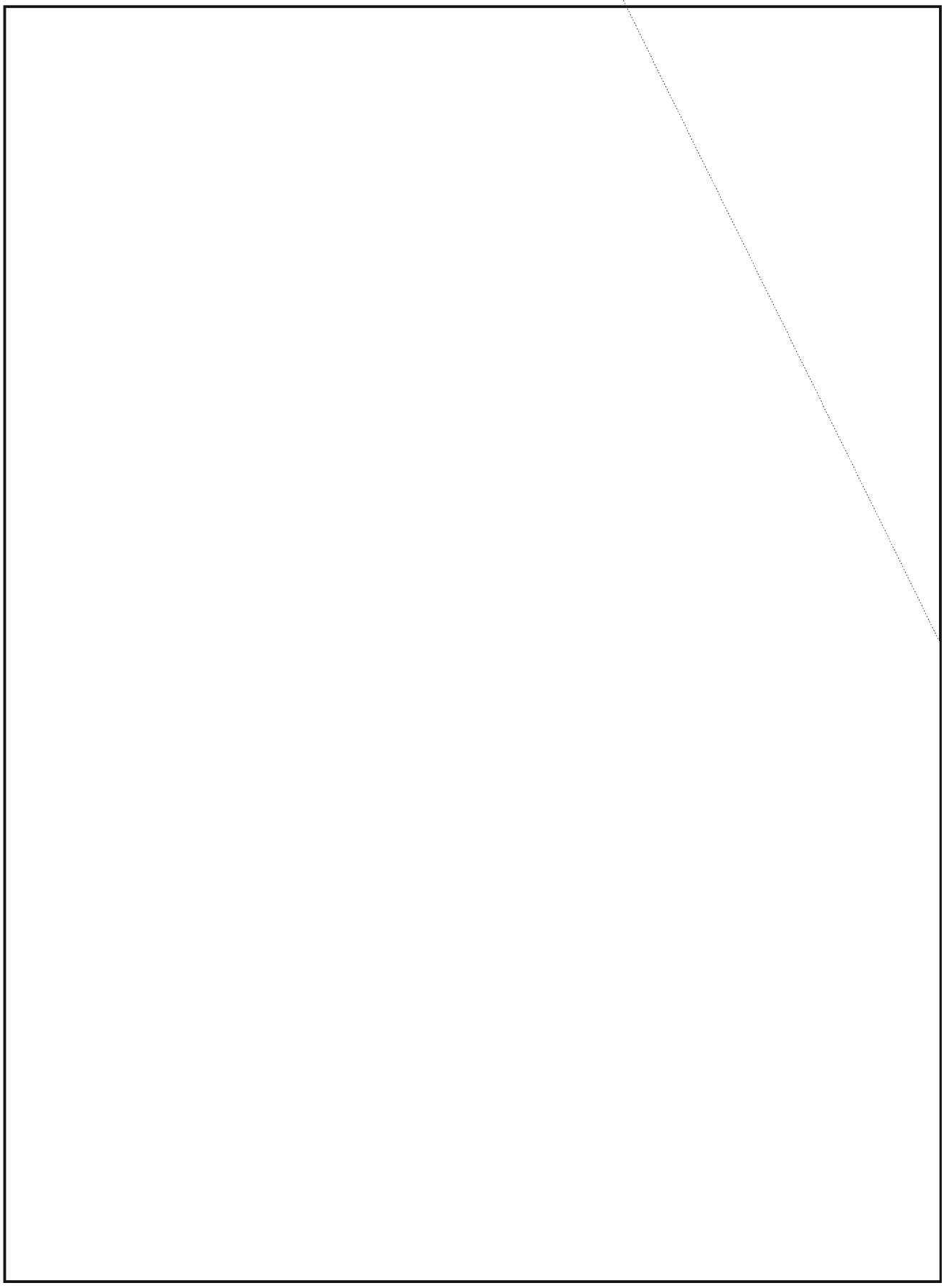
by

P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)

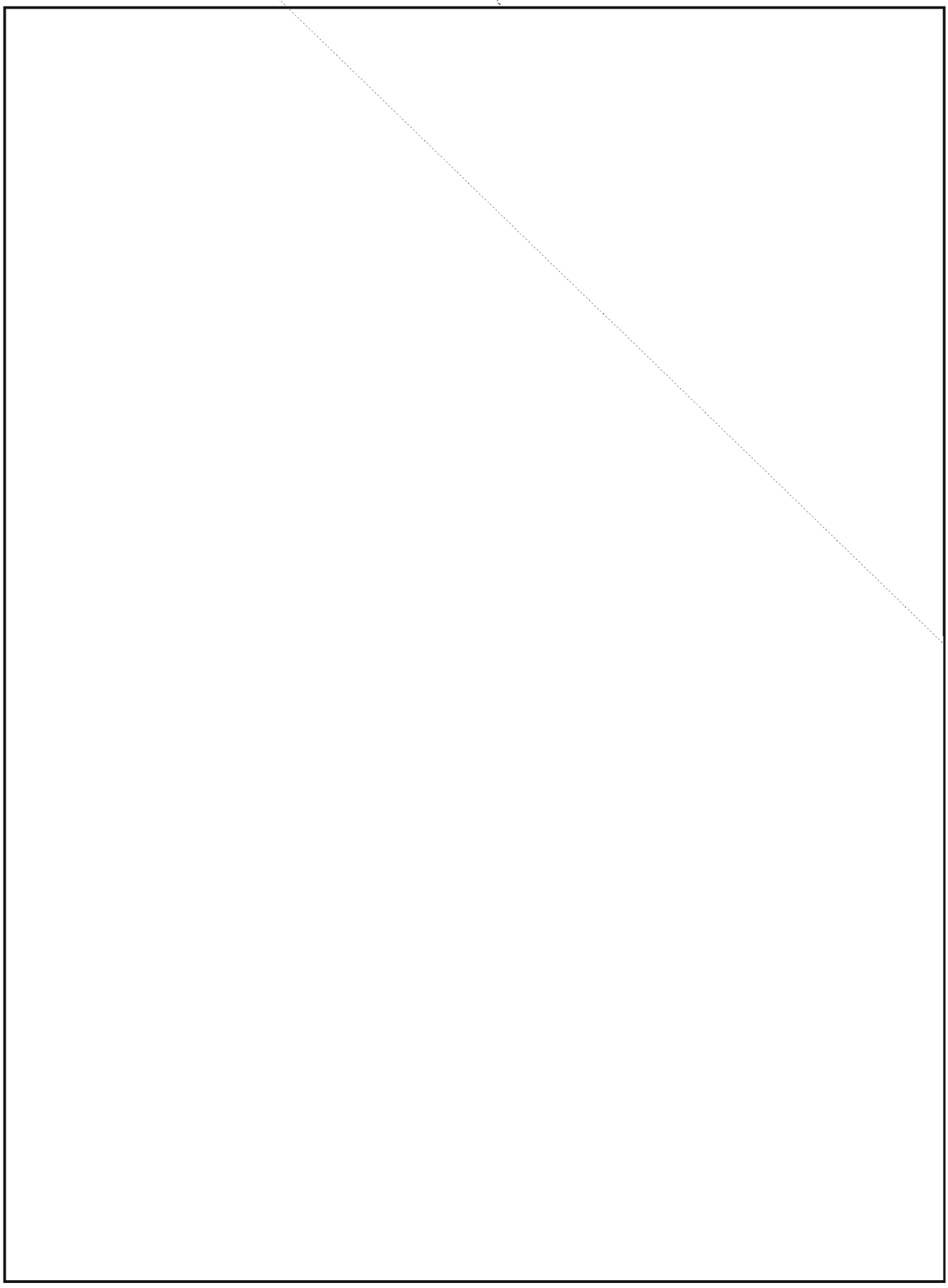
DOCID: 4012045





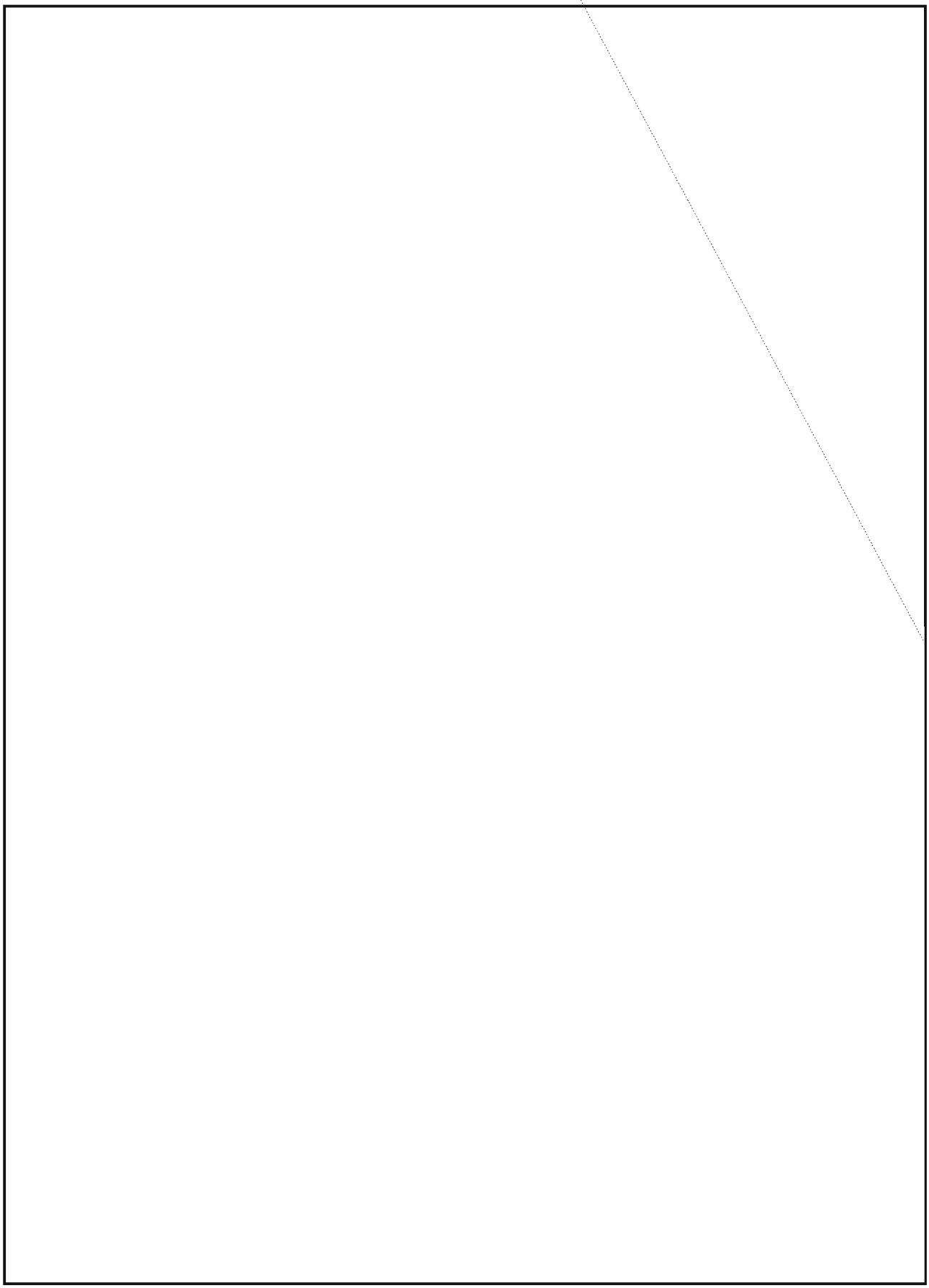
P.L. 86-36
EO 1.4.(c)

DOCID: 4012045



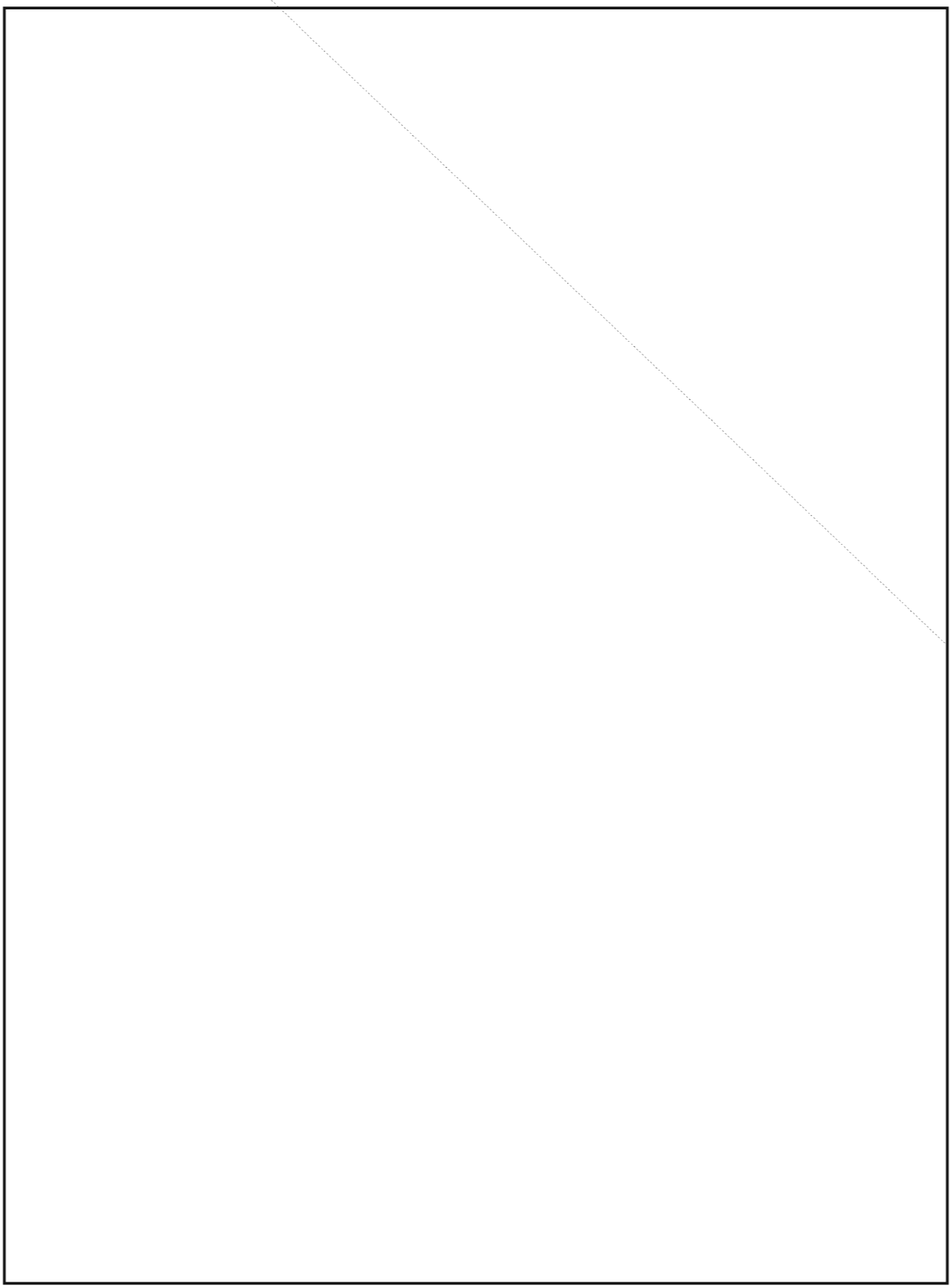
P.L. 86-36
EO 1.4.(c)

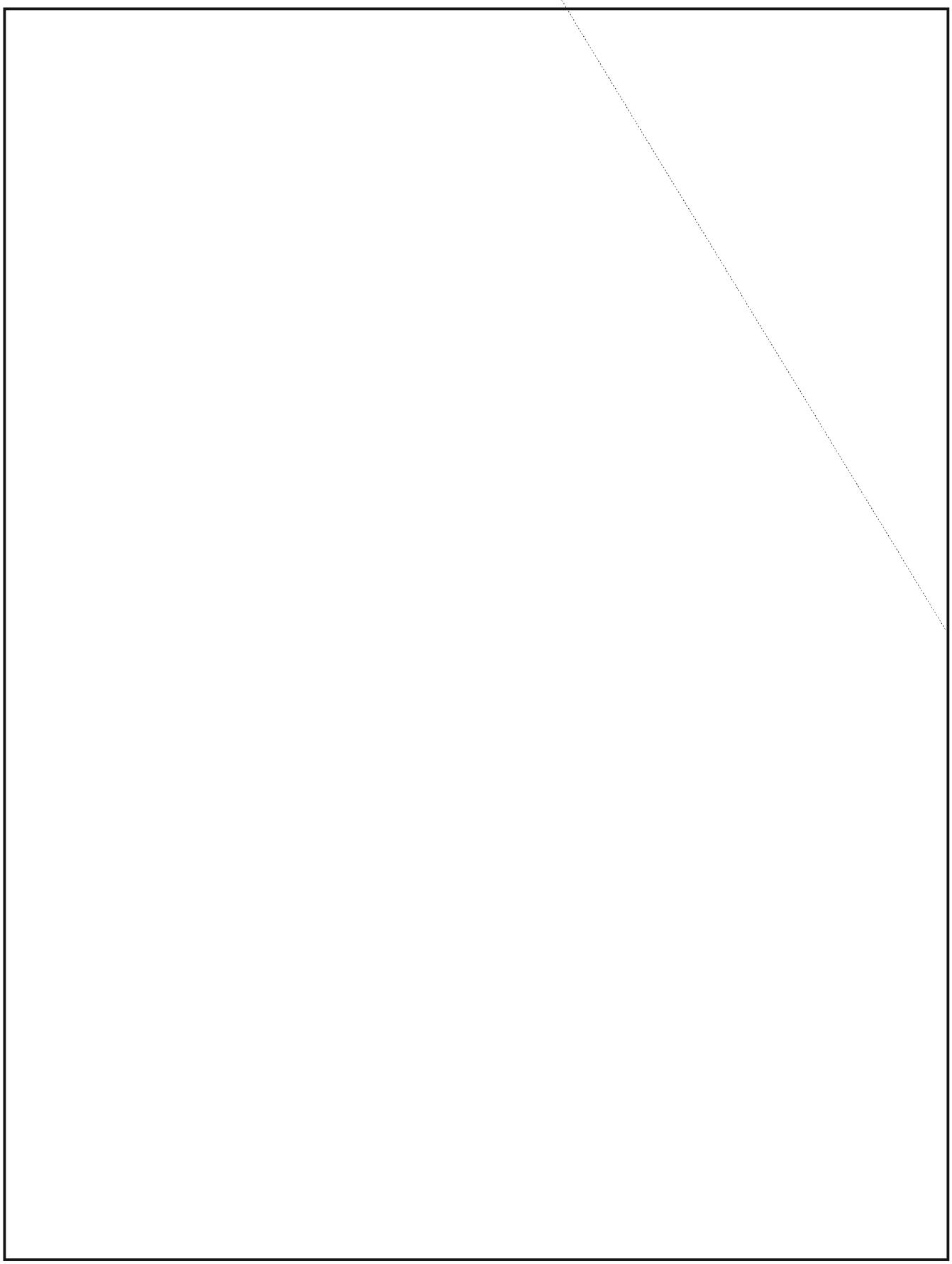
~~SECRET~~



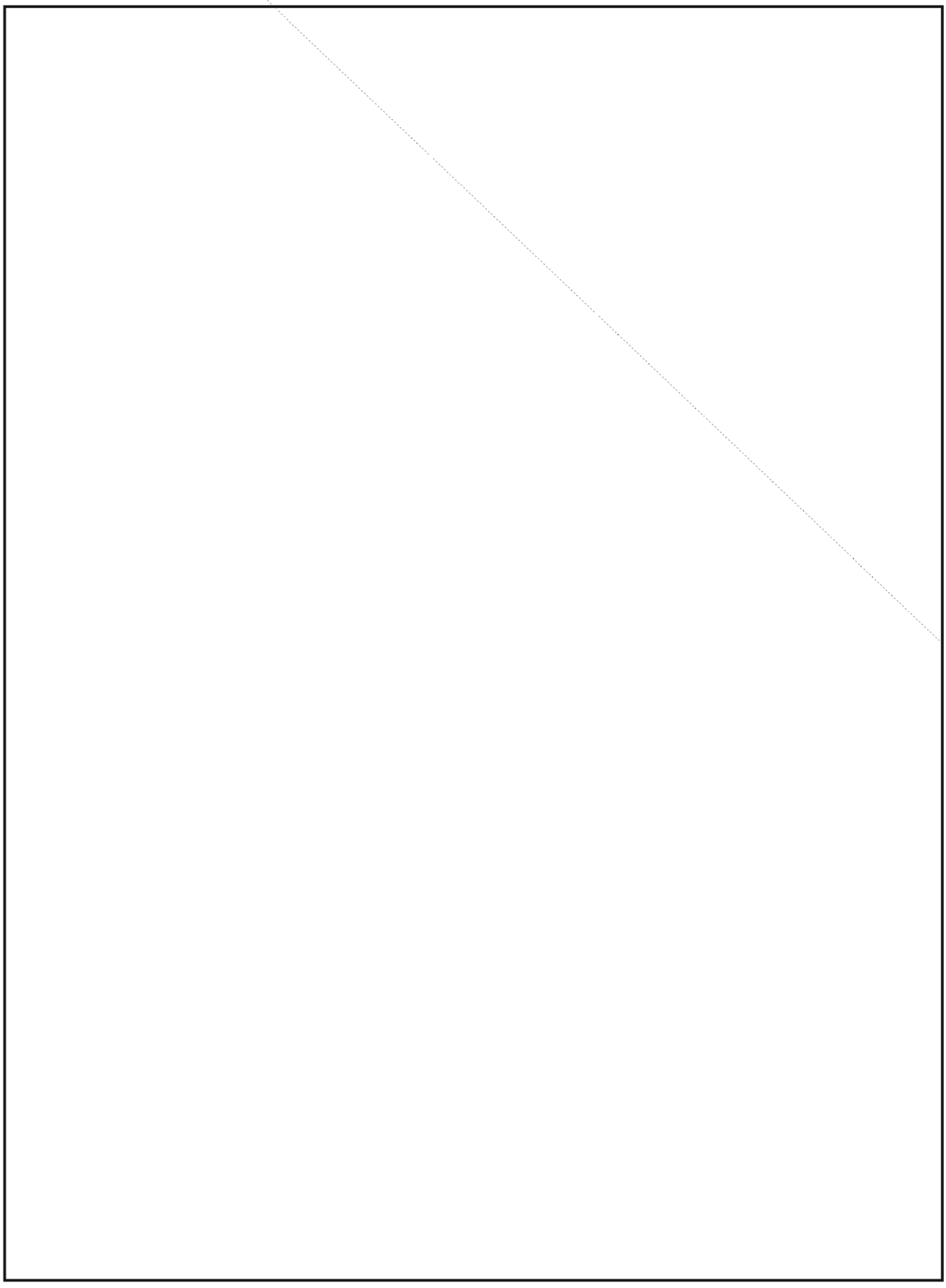
P.L. 86-36
EO 1.4.(c)

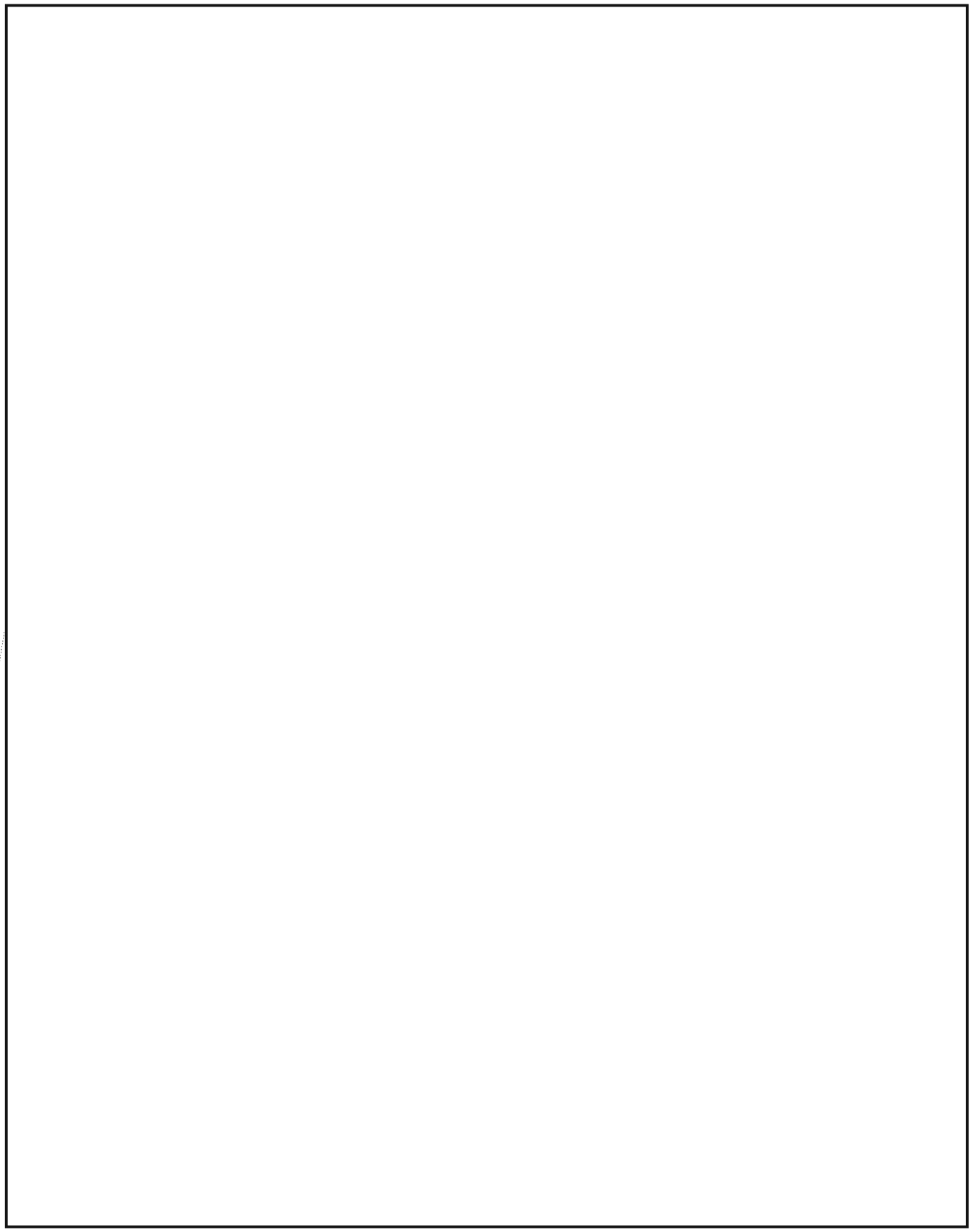
DOCID: 4012045





P.L. 86-36
DOCID: 4012045 E.O. 13526 (c)





P.L. 86-36
EO 1.4.(c)

The National Information Infrastructure (NII)

by [redacted] P.L. 86-36

(U) The NII is a Presidential Initiative whose purpose is to expedite the rapid deployment of advanced computer and communications infrastructure needed for a strong economy in the next century and making our nation more competitive in the international environment. According to the NII vision document, "Agenda for Action", which was published in September 1993, the NII is the seamless integration of communications networks, computers, information, and people, which will provide all Americans with the private and secure information they need, when they need it, where they need it, at an affordable price. This paper describes the background and relationships of the NII with respect to the forming of an Information Infrastructure Task Force (IITF), summarizes NSA's NII participation during the past year, and highlights some of the key NII outstanding issues from a national and NSA perspective.

Background

(U) As the focal point for NII activities, the White House Office of Science and Technology (OSTP) and the National Economic Council (NEC) formed the Information Infrastructure Task Force (IITF) in July 1993 to articulate and implement the Administration's vision for the NII. Commerce Secretary Ron Brown chairs the IITF (see Figure 1) which consists of Government senior-level representatives, three major committees, a security issues forum, and a private sector advisory council:

Telecommunications Policy Committee - formulates a consistent Administration position on key telecommunications issues, such as radio frequency spectrum management, universal access to services, network reliability and vulnerability, international perspectives related to the emerging Global Information Infrastructure (GII), legislative actions, and adequate competition among service providers.

Information Policy Committee - addresses critical information policy issues such as intellectual property rights, protection of individual privacy rights, and the dissemination of government information to the public sector.

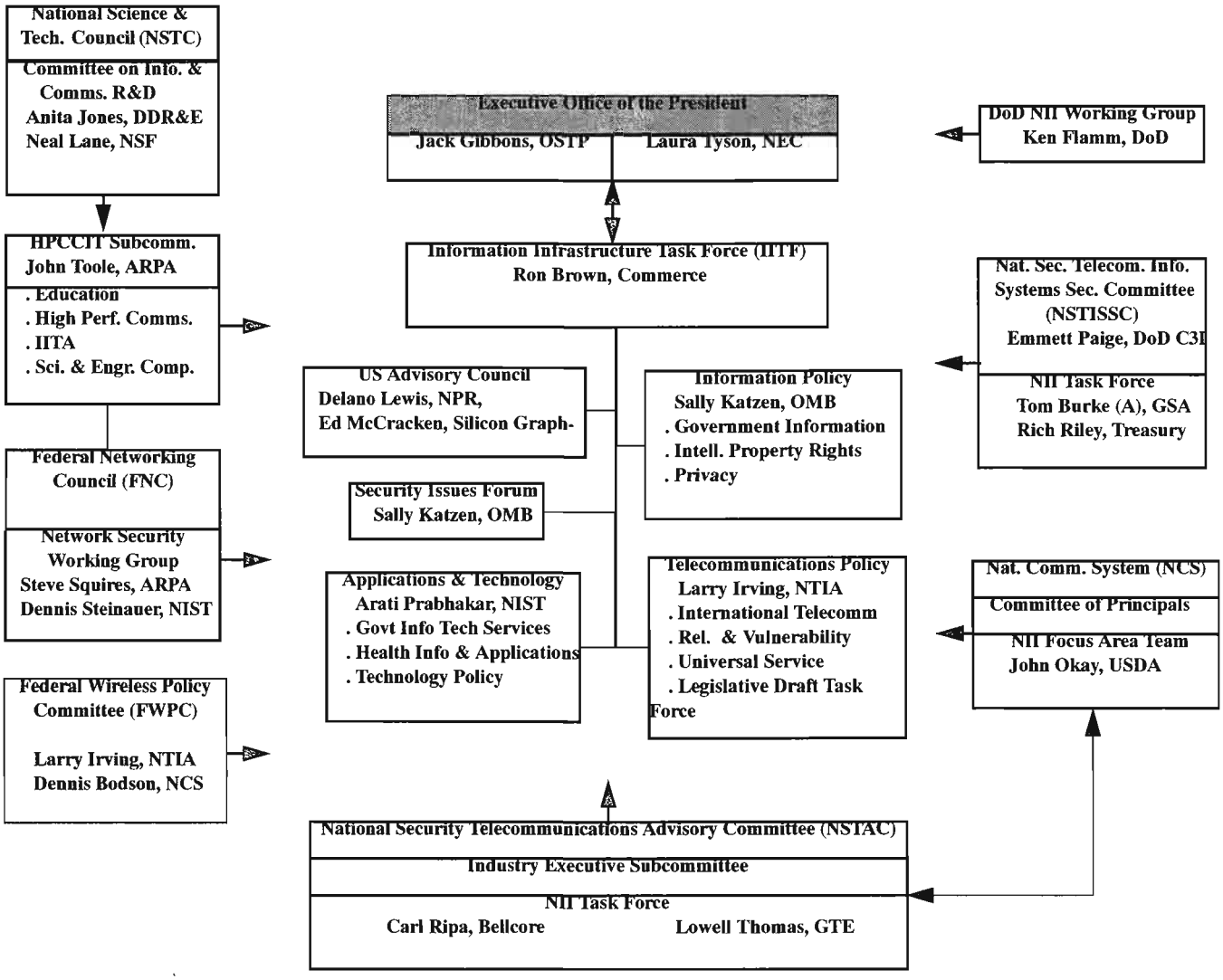
Committee on Applications and Technology - coordinates applications and technology policy efforts to develop and apply state-of-the-art technologies in areas such as health care, government services, education, manufacturing, electronic commerce, and other applications.

NII Security Issues Forum - coordinates security cross-cutting efforts across the Committees and Working Groups of the IITF with respect to confidentiality, integrity, and availability of the information and systems carrying the information.

NII Advisory Council - as established by a Presidential Executive Order, advises the Commerce Secretary on matters related to the development of the NII. There are 37 distinguished members from industry, labor, state and local governments, and public interest groups on the Council. This body is concentrating on three main Mega-Projects: NII visions and goals driven by specific applications; NII access and universal service; and privacy, security and intellectual property rights.

(U) In conjunction with the IITF, there is a host of other Government organizations who have a vested interest in the NII. As illustrated in Figure 1, these include:

National Science & Technology Council (NSTC) - reviews and prioritizes R&D efforts across the Federal Government. The NSTC is a Presidential Council (similar to the National Security Council or National Economic Council), and it consists of nine committees, one of which is the Committee on Information and Communications R&D. The relevance of this committee is that it oversees the High Performance Computing and Communications (HPCC) Presidential Initiative. The HPCC has five R&D component areas, mainly: High



Performance Computing Systems; National Research and Education Network (evolved into the Internet); Advanced Software and Technology; Basic Research and Human Resources; and Information Infrastructure Technology and Applications, which is directly related to the NII.

High Performance Computing and Communications Information Technology Subcommittee (HPCCIT) - plans for and implements the HPCC Initiative under the auspices of the HPCC National Coordination Office. There are ten Agencies on the HPCCIT, and the NSA Chief Scientist, Mr. George Cotter, represents NSA on this panel, as well as the NSTC.

Federal Networking Council (FNC) - administers the Internet in principle and is chaired by the National Science Foundation. The FNC has five working groups, and one of these groups, the Network Security Working Group, is addressing and formulating a security plan for the Internet.

Federal Wireless Policy Committee (FWPC) - addresses Federal Government concerns and issues on wireless communications. There are four subcommittees and a users forum, and NSA participates in all of these arenas. Wireless communications will go hand-in-hand with cable, satellite, terrestrial, and fiber optics media as conduits for NII applications and services.

DoD NII Working Group - serves as a focal point in DoD for NII activities and interests. DISA, ASD(C3I), JCS, DDR&E, NSA, ARPA, and OASD(ES) participate on this group.

National Security Telecommunications and Information Systems Security Committee (NSTISSC) - sets national policy for the security of national security systems with respect to telecommunications and automated information systems. The NSTISSC consists of more than 21 participating Agencies and observers, various working groups, and an NII Task Force.

National Communications Systems (NCS) - oversees and addresses the operations, security, and workings of the U.S. communications systems, such as the public switched network. The NCS has many working groups and an NII Focus Area Team.

National Security Telecommunications Advisory Committee (NSTAC) - advises the President on matters with respect to telecommunications, networks, national security and emergency preparedness, and other areas. Members of the NSTAC are from the private sector, and there are numerous working groups and panels, one of which is the NII Task Force.

P.L. 86-36

NSA NII Participation

~~(FOUO)~~ Realizing the importance of the NII and the potential for NSA contributions, the Director endorsed an initial NSA Plan for NII participation in September 1993. A result of the NSA plan was the formation of an Agency NII Steering Group, which is led by the ADDI, to provide guidance and direction to NSA's NII related activities, as well as serving as a forum to coordinate and resolve NII cross-key component issues of importance to NSA. Similarly, the Director approved the establishment of the NII Process Management Office (NII PMO) to identify, plan for, and provide the required day-to-day focus, support, and coordination of NSA NII activities consistent with Agency mission strategies. The NII PMO originated in V8, evolved into I3, and now resides in V1, Customer Support Services. [redacted] is the chief of the NII PMO, replacing [redacted] who is now Chief, V1. In addition, an NII Working Group of key component members was formed in February 1995 to assist the NII Steering Group and NII PMO address NII issues, develop strategies, and recommend courses of action.

~~(FOUO)~~ NSA is also working with the National Institute of Standards and Technology (NIST) to support the Administration's NII initiatives and to implement the recommendations of the Vice-President's National Performance Review. It is believed that our national information protection strategy must not be limited to only government systems, but must accommodate other important national objectives as well: the availability, reliability, and integrity of systems which support our economic infrastructure, the protection of public safety and the provision for law enforcement, the provision for foreign intelligence, ensuring and enhancing the privacy of all Americans, and facilitating a secure NII.

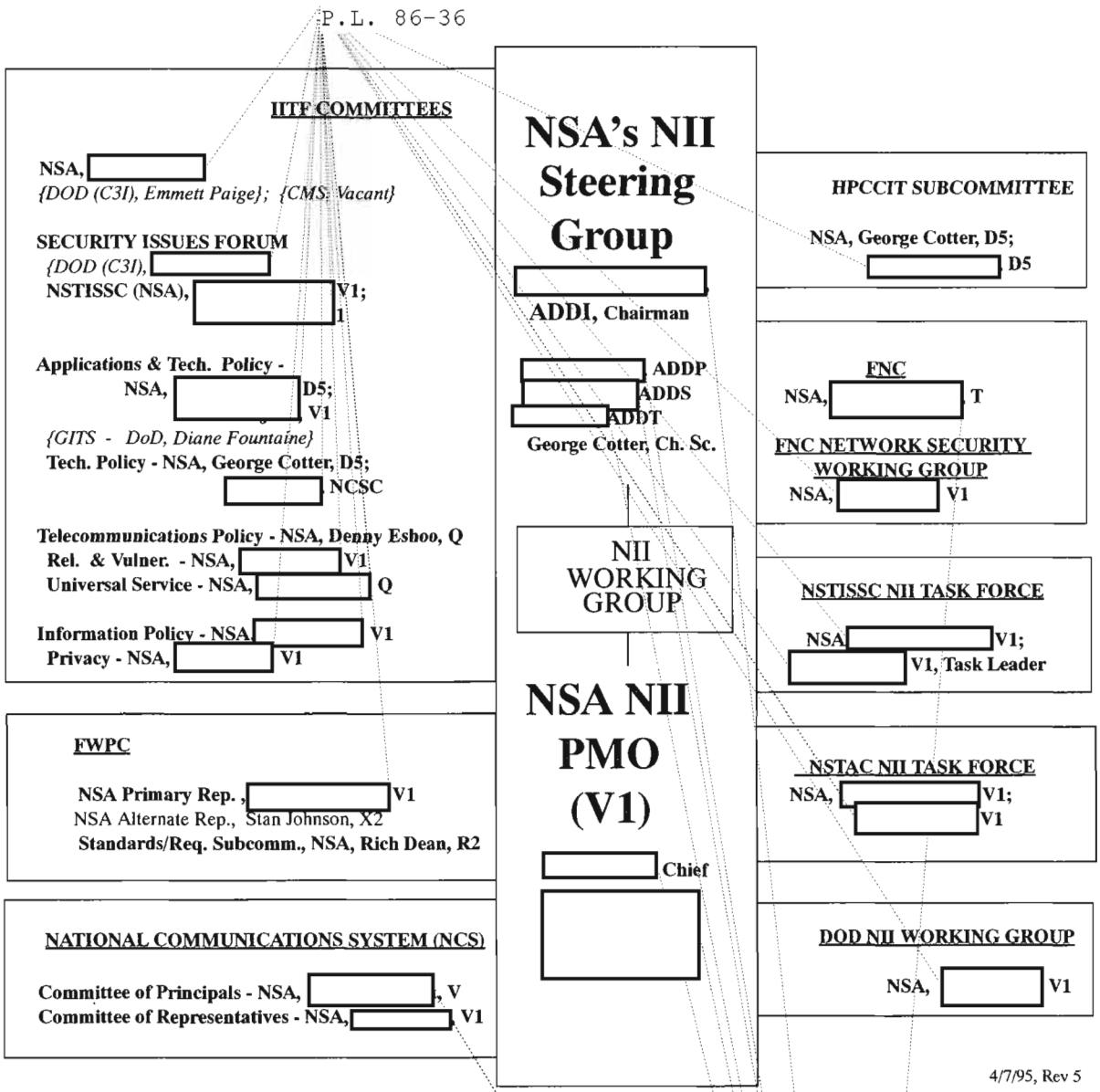
~~(FOUO)~~ During the past year, NSA representatives have contributed to many of the deliberations of the Administration's IITF and various NII working groups (see Figure 2). In particular, the following summary describes some of the more recent contributions to the IITF and miscellaneous NII activities:

a. **Congressional Office of Technology (OTA) Assessment** - Over the past year, the NSA NII PMO and Legislative Affairs Office worked closely with OTA to provide information, participated in various workshops, coordinated participation by other NSAers, and reviewed draft portions of a report on "Information Security and Privacy in Network Environments". A key objective of that dialog was to ensure that the scope of the INFOSEC problem was fully understood by OTA and that the issue of encryption policy, a principal focus of their report, was addressed in a balanced and meaningful way.

b. **Security Issues Forum** - NSA attends meetings as the representative of the National Security Telecommunications and Information Systems Security Committee (NSTISSC). NSA prepared a report on useful security tools and techniques; raised the level of concern and initiated a government-wide effort to increase security training and awareness of computer systems administrators; and provided substantial comments on a draft NII Security Report.

c. **Privacy Working Group** - NSA contributed significantly to working group discussions related to privacy and privacy principles. In addition, NSA provided advice on information security technologies and practices, CLIPPER, and defensive INFOWAR. As a result of our participation and contributions, we have earned the trust of the Government's privacy community and are asked to provide our perspectives on working group and other privacy activities.

d. **Reliability and Vulnerability Working Group (RVWG)** - NSA provided substantial comments on the writing of an RVWG action plan addressing network reliability and vulnerability concerns. In addition, NSA is a partner with NIST in the RVWG's Protection



of the Network sub-working group, and we are helping to identify community-wide network infrastructure protection issues and recommending solutions.

e. **Risk Assessment** - Under the RVWG action plan, NSA was nominated to be the office of primary responsibility for one of the actions on NII risk assessment. In particular, this action calls for the identification of risks to the reliability and availability of NII networks and services, and it is concerned with new uses of existing technologies and uses of emerging technologies.

f. **Committee on Applications and Technology** - NSA reviewed and critiqued all of the committee's applications, services, and technology documents and offered our insights into security needs for these emerging efforts. We also participated in a survey of NSA programs and projects which may enhance the acceleration of the NII and submitted more than 20 candidate efforts. Last of all, we participated with NIST to evaluate and offer input on the Worldwide Web NII home page.

g. **Miscellaneous Activities** -

(1) IITF - At the request of the Administration, the NII PMO recently worked with Commerce personnel to have DDI, Mr. Ed Hart, become a formal member of the panel.

(2) NII Security Infrastructure - NSA assisted NIST and GSA to establish a Government-wide security infrastructure office and integrated NSA personnel into GSA's new Security Infrastructure Program Management Office.

(3) Federal Wireless Policy Committee - NSA chairs the Standards and Requirements Subcommittee and took the lead in writing the Wireless Standards Plan.

(4) Federal Networking Council - NSA is contributing in this community-wide effort to develop an Internet Security Plan.

(5) Information Policy Committee - NSA contributed to the document on intellectual property rights principles.

(6) Telecommunications Policy Committee - NSA was invited to review and offer comments on the vision documents for the NII and Global Information Infrastructure (GII) and provided input for the Committee's FY95 Work Plan.

(7) National Performance Review (NPR) - NSA is supporting OMB and NIST on at least four actions with respect to security information technology and tasked to take the lead on another effort.

(8) Briefings and Workshops - NSA has briefed key NII leaders and officials, e.g., OSTP, NEC, OMB, DoD, Commerce, GSA, OTA, GAO, etc. on protecting unclassified but sensitive information and the vulnerabilities of our national systems. Similarly, we have helped energize NSTAC members to begin to address new security/emergency preparedness issues and arranged for the State Department in providing an NII international organization briefing to the NSA G41 Telecommunications Technology Forum.

National NII Issues

(U) Throughout much of the discussions on the NII, questions arise, such as, what is the NII, who will build it, is it here now, what do I do with all this information, and what should be the role of the Federal Government in the NII?

(U) To answer several of these concerns - the NII is already here in an elementary form. One definition that I like is that the NII is a combination of the phone system, cable systems, private networks, the Internet, video dial tone, wireless, direct broadcast satellites, and the information services and applications that will be carried on these systems. Much of these media will be interconnected in Cyberspace, however, some will not. The private sector will be building and implementing the NII, while Government's role and responsibility will be to provide leadership in certain areas, serve as a facilitator and catalyst in removing legal and regulatory barriers (e.g., the Telecommunications Act of 1934), promote competition, provide better access to Government information, improve Government procurement and distribution of benefits, and promote policies that will support a viable secure information infrastructure for public and private institutions.

(U) Some of the more pressing national NII issues which are on-going and have yet to be resolved include:

a. How much of a leadership role should the Government have in the definition, architecture, development, and implementation of the NII?

b. How should current Federal and State laws, regulations, and policies be changed to be more attuned to the NII (e.g., computer crime, First Amendment Rights, etc.) and the Information Age?

c. How should the "Universal Service" concept be extended to ensure that information resources are available and accessible to all Americans?

d. How will intellectual property rights be protected?

e. How will privacy be ensured and who will provide it?

f. How will information security and network reliability be ensured and who will provide it?

g. Who should develop standards for the NII and will it be interoperable?

h. How will the NII interconnect and work with the GII?

i. Is there a DoD and Intelligence Community role in the NII?

NSA NII Issues

~~(FOUO)~~ NSA interests in the NII appear to be multiple and multi-dimensional and encompass both the SIGINT and INFOSEC missions. Within NSA there is also an on-going debate with respect to the following issues and concerns:

a. How does NSA NII participation fit into the overall Agency mission strategy (e.g., Equities, INFOSEC, INFOWAR, Export, SIGINT, Computer Security Act, etc.)?

b. What are the NSA specific goals or objectives for participating in the NII? Why should NSA concern itself with the NII?

c. Should NSA interests in the NII be from an INFOSEC only perspective or should it be an Agency-wide perspective?

d. Should the NSA Board of Directors be more involved in addressing NII cross-component issues?

e. In many public meetings in which we participate, NSA takes a lot of criticism and "flames" because of who we are and what we do. If we do not have a position on these criticisms or issues, that is a position in itself—failure to make a decision is a decision.

f. Does the Computer Security Act of 1987 limit our participation in the NII? If it does, how should it be changed? What role should NSA have in protecting unclassified but sensitive information in the Government and private sector domains?

g. Should NSA only participate in the DoD Defense Information Infrastructure (DII) portion of the NII? What are the specific NSA objectives for participating in the DII and can these be applied to the NII?

h. Other Government Agencies seem to be getting more involved in INFOSEC research and development efforts. Should NSA be taking more of an INFOSEC leadership role for the Government with respect to unclassified but sensitive information?

i. What impact will the Administration's Security Policy Board/Security Policy Forum have on NSA, as well as our involvement in the NII?

j. The NII is evolving into the GII. What are the NSA interests in the GII?

k. What is the NSA strategy for using the Internet? Do we have any strategic intent into securing our Internet hosts? How do we plan to easily import information from the Internet into our internal systems?

The author would also like to thank [redacted] *who recently left the V1 NII PMO, for his contributions to this paper. (N.B. The views expressed in this paper are those solely of the author and do not necessarily represent any NSA organization or entity.)*

[redacted]

P.L. 86-36

For more information on the NII:

[redacted] contributing reports on various NII-related meetings and decisions, and providing press articles on the NII. He also maintains the NII Calendar of Events, updated monthly:

August - October 1995 (Updated 15 Aug)

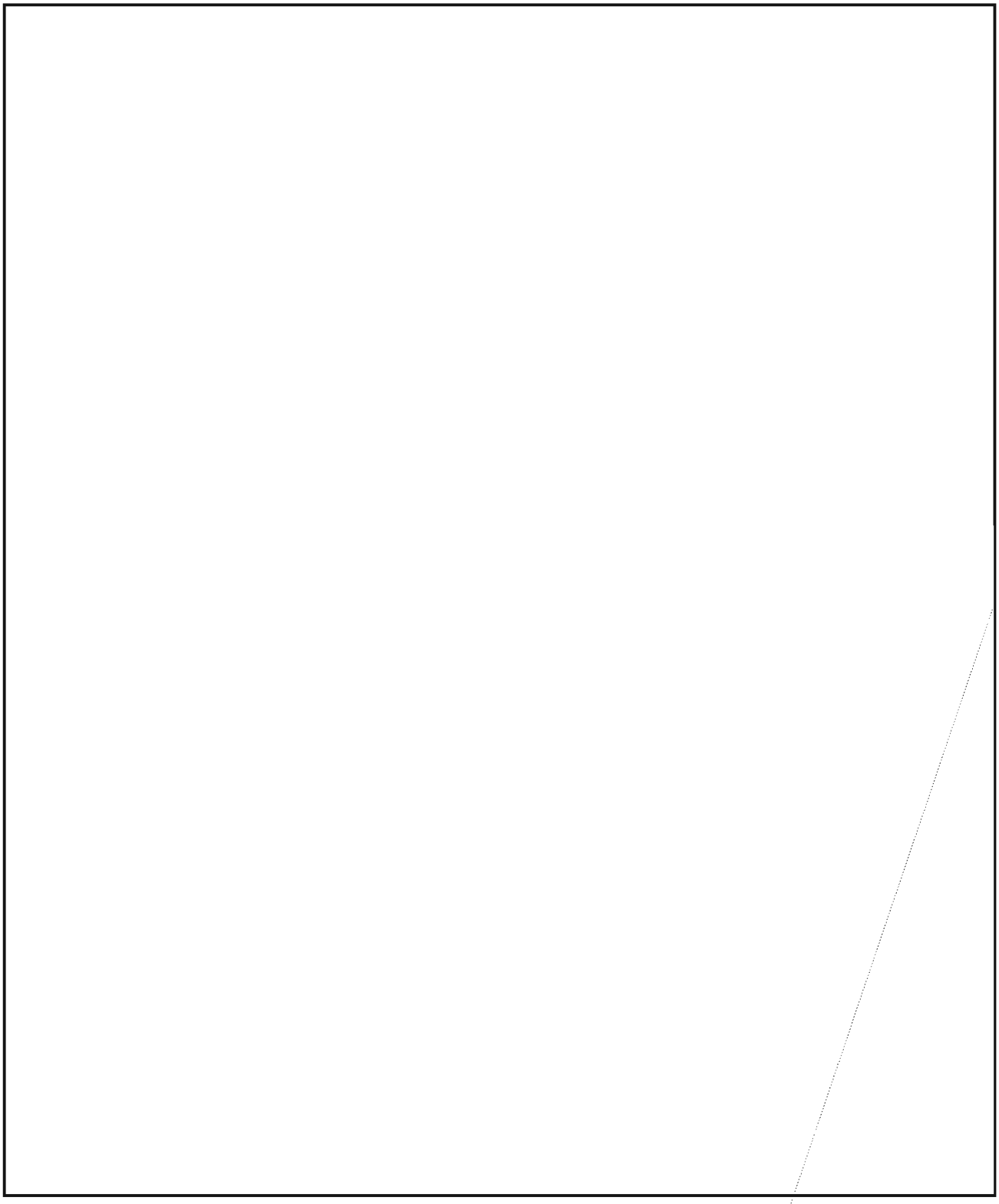
[redacted]

15 August
7 September
20 September
21-22 September
22 September
TBA September
TBD
11 October
TBA October

P.L. 86-36

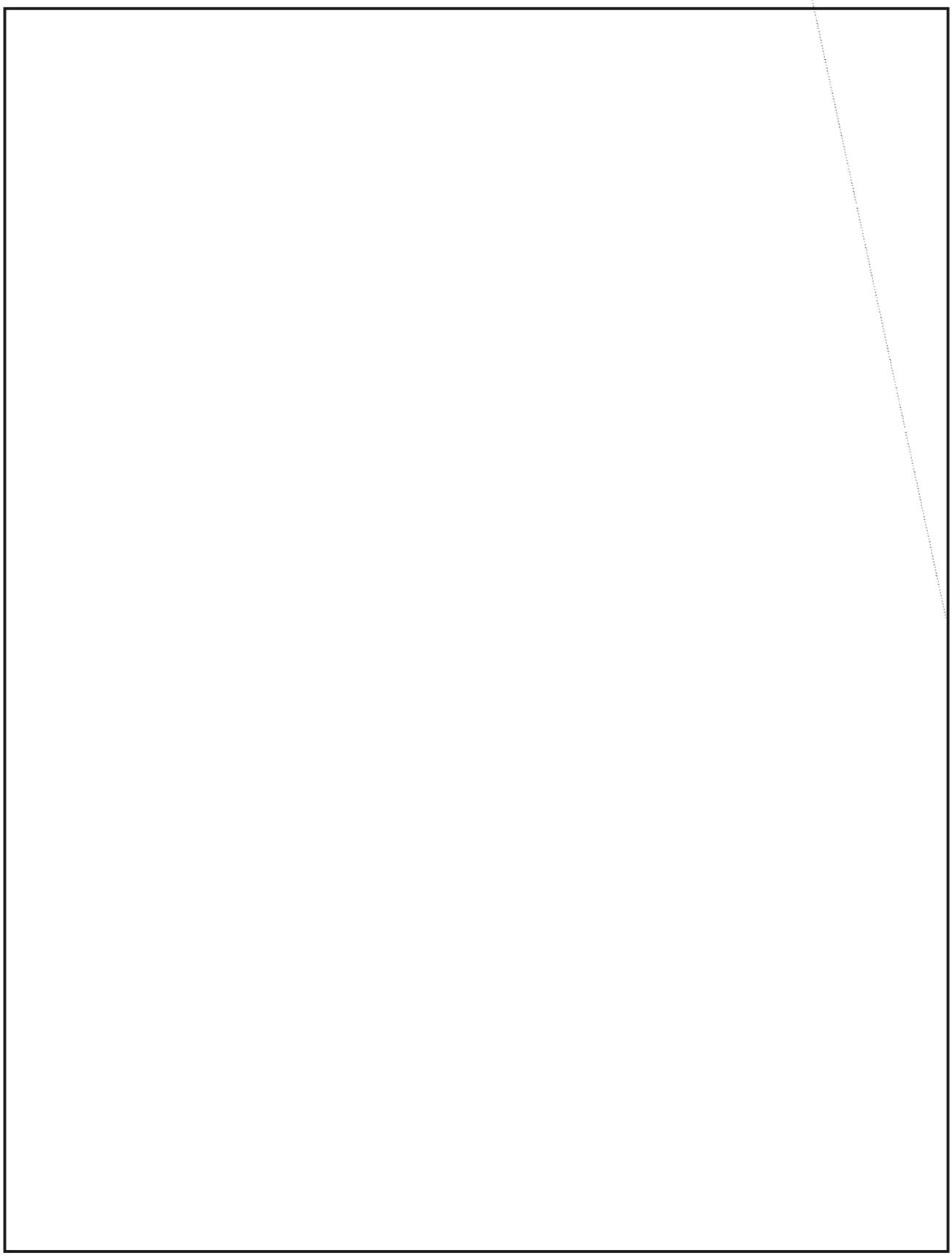
What's This New Intercept I'm Seeing?

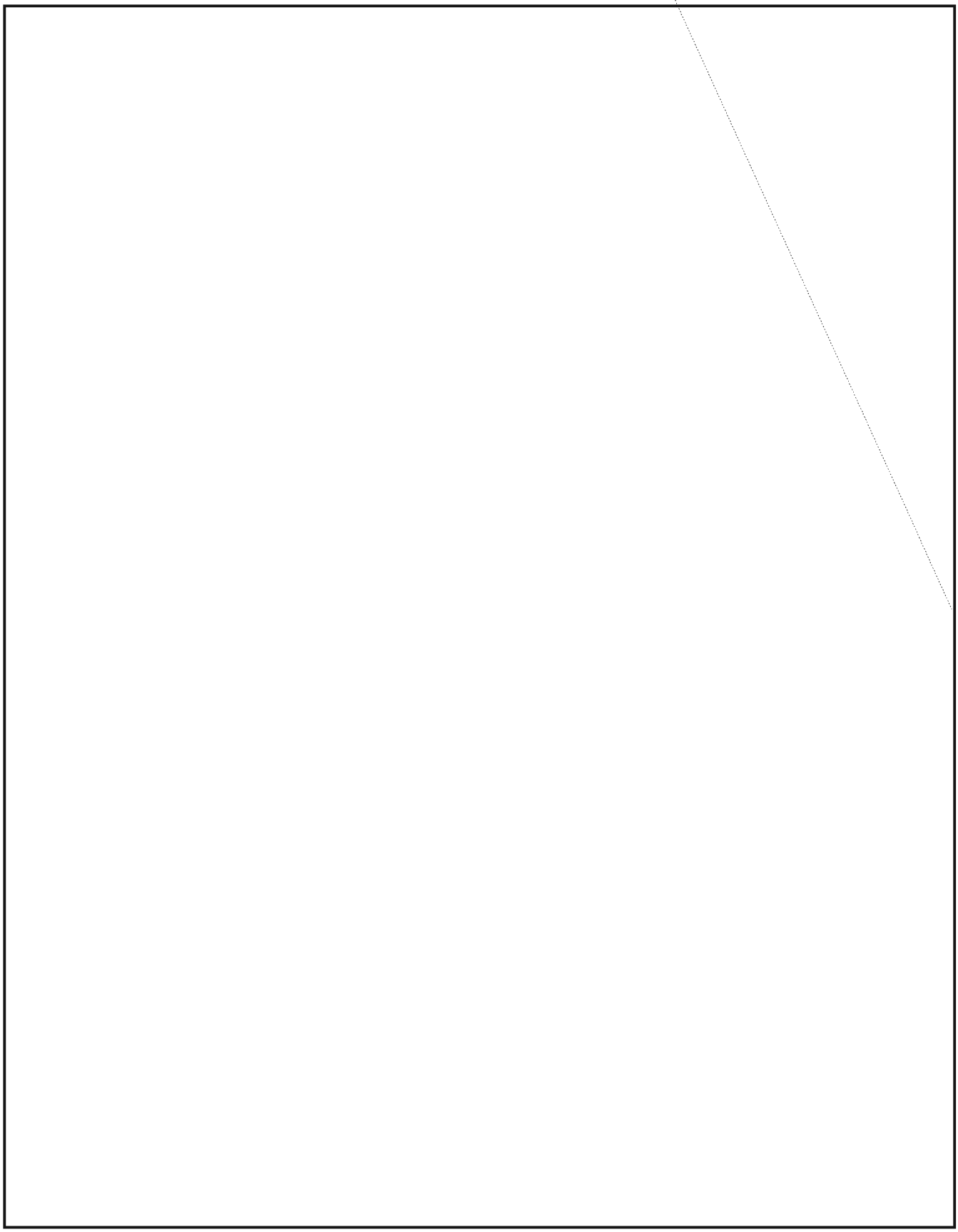
by [redacted] P.L. 86-36



EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36





CRYPTOLOG
Summer 1995

The Unfocused Eye:

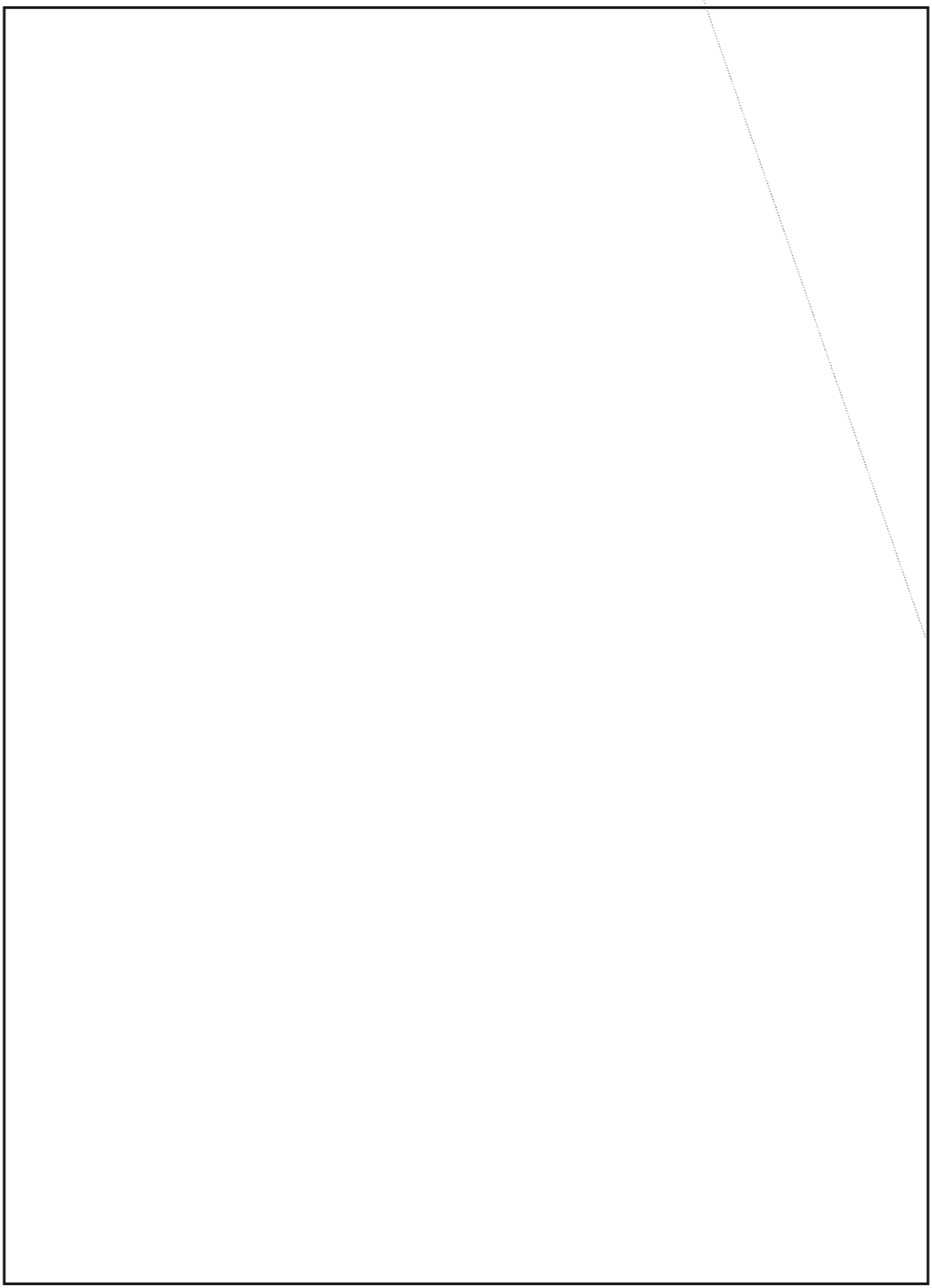
by

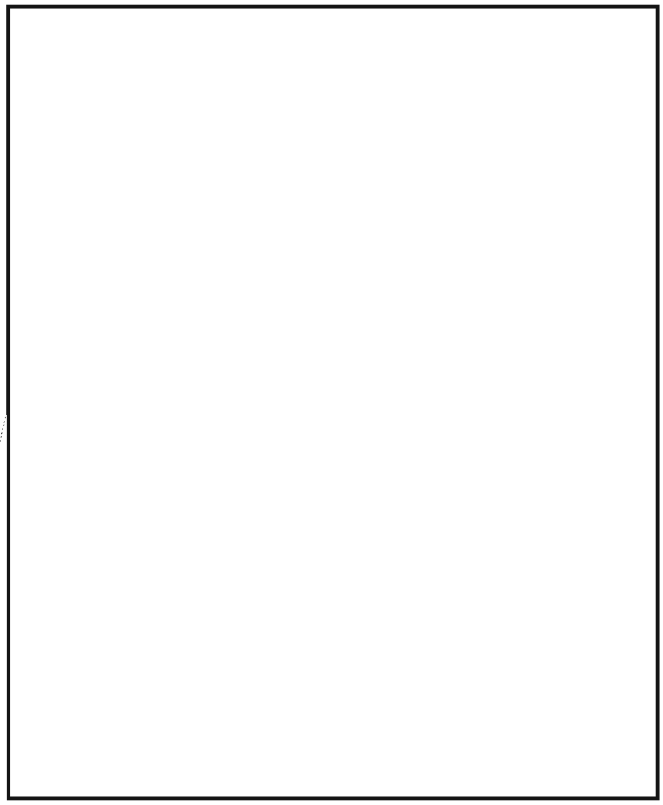
P.L. 86-36

(FOUO) It was the fifth of January 1993 at the Alabino All-Forces Testing Ground west of Moscow. A smiling, overcoated Russian bureaucrat in a black fur hat, harnessed with a backpack radio and surrounded by uniformed figures, was dancing up and down in the snow. That evening a few seconds of his not-ready-for-the-Bolshoj performance were shown on national Russian television news, and next morning several Russian newspapers carried an account of his comments.

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

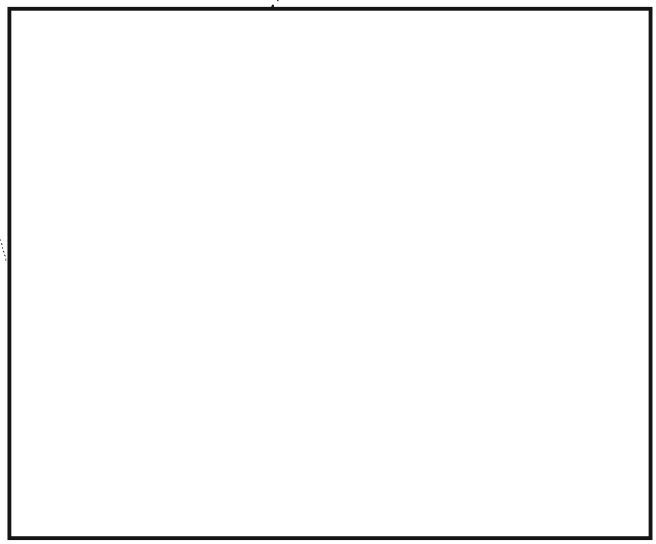


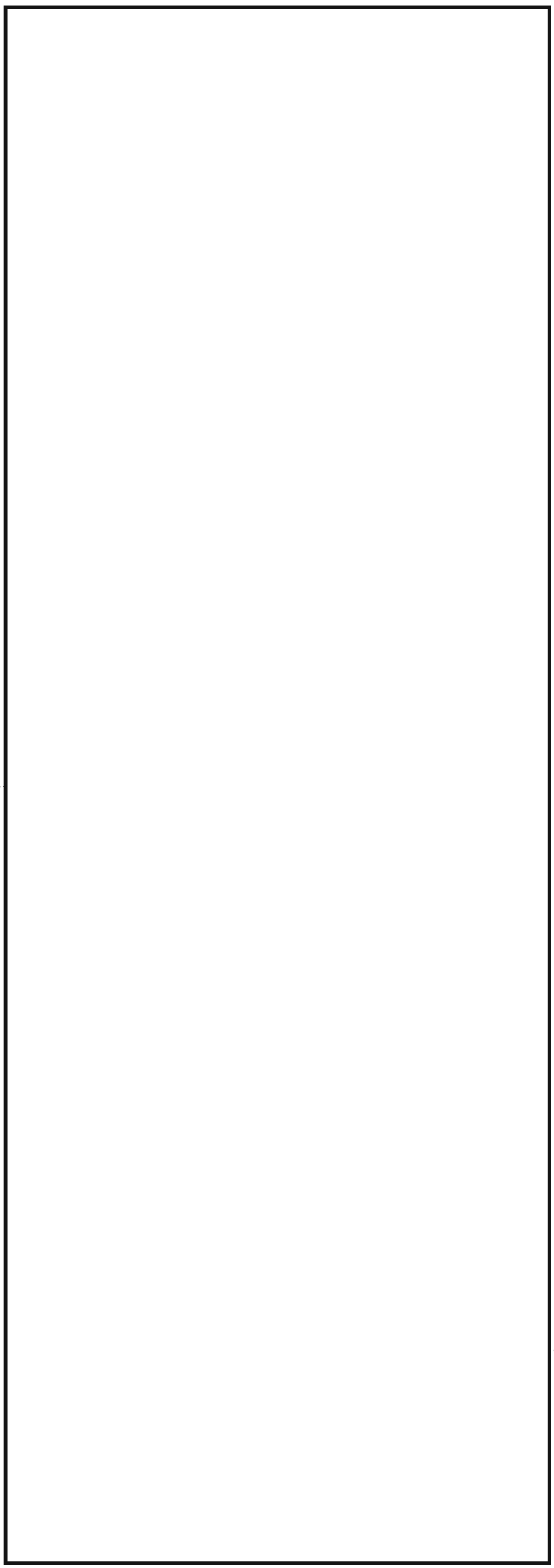


Finding Things in the Dark

(U) As a young recruit in the Navy Reserve, I was taught how to scan a sector of the sea at night. "Do not," I was sternly told, "look directly at a point; let your eyes relax as you scan across the sector, and wait for something to attract your attention." This had something to do, I suppose, with the distribution of rods and cones in the human eye, but also with the fact that the eye can focus on only one thing at a time. Once we focus, everything else becomes peripheral, and other things are not so likely to be noticed until we relax our gaze or refocus it.

P.L. 86-36
EO 1.4.(c)





DOCID: 4012045

P.L. 86-36
EO 1.4.(c)

From the History File:

(U) Dr. Sydney Fairbanks, for 5 years the editor of one of CRYPTOLOG's predecessor publications (the NSA Technical Journal), was, besides a cryptologist, an academician who taught languages and sciences at St. John's and Harvard, a translator, an accomplished musician, and he held a number of jobs in the diplomatic and judicial realms. His editoirials, published in the NSA Technical Journal from 1956 to 1959, are entertaining as well as informative, and surprisingly applicable today. For example, from April 1956:

(U) The history of technical magazines at NSA is not unlike that of the city of Troy, which was, we understand, destroyed by fire and rebuilt on at least five different occasions. This is a matter from which both pessimist and optimist can draw legitimate inferences, but speaking for the latter we say that the idea evidently has extraordinary vitality, and we hope that its latest incarnation will be welcomed.

(U) Part of this vitality may be due to a certain fortunate fuzziness that shelters any ideal until the time comes to embody it. There is always the danger that what the supporter has in mind is a journal full of articles on his own specialty—which, of course, any right-thinking person will understand and enjoy—plus a few outlandish disquisitions on other subjects, which he needn't read. "Even with a Technical Journal devoted to one specialty," we are told, with perfect truth, "no one reads ALL the articles." Unfortunately, any attempt to edit the Journal on this basis, but without bias, would result in perhaps five little quarterlies each containing about one-and-a-half articles, and united by nothing but the cover. It does not seem difficult to prophesy that such a publication would fall apart. Unless at least half our articles are interesting to at least half our readers we shall be hardly more than a rather clumsy unofficial adjunct to the existing system of reports.

(U) To concede or admit this, however, is apt to fill the air with such choice missiles as "popularizers," "intermediate training pamphlets," "writing down," "Do you mean a Technical Journal or a Scientific American?"... all of them carrying a certain barb of truth, but shaped we believe from a misunderstanding. At least two-thirds of the unreadability of the average technical report is due not to unavoidable sophistication but to casualness. An expert writing for other experts in the field can organize his material poorly, express himself badly, avoid deciding what his basic assumptions are, and still be read with interest, because they can almost unconsciously supply what is missing. To reach a wider audience he need not "write down"; he need only write better. If enough of our contributors have the time and the energy to do this—and let no one underestimate the time and the energy that it takes—we believe that we can achieve the necessary level of general interest.

(U) As for the remaining obscurity, due to what we have called unavoidable sophistication, obviously it is no bar to publication. The Journal has been urged to avail itself of the best minds in the Agency as specialists and referees, and readers can be confident that they will not be deprived of any article merely because the Editor is not bright enough to understand it.

ΚΛ

DOCID: 4012045

CRYPTOLOG
Summer 1995

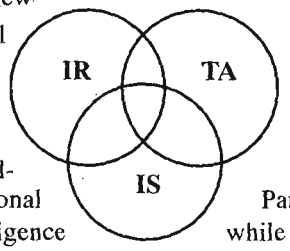
Intelligence Analysis Off-site and Open Forum

by [redacted] P.L. 86-36

~~(FOUO)~~ The Intelligence Analysis Career Panel (IACP) held an off-site on 22 and 23 May 1995. In these open sessions, the IACP asked for input on several issues from the DO Group Chiefs, E1 and E3 Management, Tech Track players, interns, aspirants, and professionalized Intelligence Analysts. The panel reached several decisions about where the IA Career Field needs to be going, the need for corporate participation in and understanding of IA, and the necessity of involving the IA technical population in reaching decisions about the health and future of the career field. The most significant decision of the off-site was to rebuild the Intelligence Analysis Career Field around the "pillars" of Intelligence Research and Reporting (IR), Traffic Analysis (TA), and Information Services (IS). Professionalization criteria will be adjusted to reflect this orientation. After acquiring a strong base in the aspects of the career field that are common to all three pillars, individuals will focus on one of the three areas. With the help of the appropriate senior managers, we will be guiding individuals toward those skill areas which are in particular demand. After the proceedings of the off-site were published [redacted] the panel felt it was necessary to hold an Open Forum to give people the opportunity to listen to the results and recommendations of the off-site and to make any comments or suggestions, voice concerns, or ask questions. The Open Forum was held in the Friedman Auditorium on 11 July; a summary of the question-and-answer session is included here.

I. State of the IA Career Field

(U) In opening remarks, [redacted] reviewed the incentives that prompted the off-site. Over the past 6 months, a major subcommittee of the IACP had been meeting to perform the periodic review of the IA criteria. During the review, several issues repeatedly surfaced that could not be resolved in the regularly held IACP meetings. In addition, the IA Tech Track Review Panels (TTRPs) had been having some difficulties evaluating applications that fell outside the traditional realm of the IA predecessor fields of Intelligence Research (IR) and Traffic Analysis (TA). These problems needed immediate, concentrated attention, hence the decision to hold an open off-site that would bring all the major players together.



(U) For the sake of those that have either forgotten or never knew the reasons for the merger of the IR and TA career fields, here is a review of the start and subsequent progress of the IA Career Field.

~~(FOUO)~~ In the late 1980s, several groups (Project Reload, the Blue Ribbon Panel Studies, the Future SIGINT Capabilities Study, and the M4 Future Skill Mix Study) concluded [redacted] Furthermore, there was a need to develop future analysts/reporters with a broad-based fundamental SIGINT knowledge coupled with a higher level of analytic skills. The major initiative that resulted from these studies was the creation of a new career field for analysis and reporting. This decision was concurred in by the DDO Group Chiefs, the Chairs of the IR and TA panels, as well as DDO, DDT, DDA, and the Director. A Transition Panel was established in February 1988 with members from the IR and TA Panels, representatives from Policy and Career Development organizations in M, and the NCS. This panel worked closely with all parties affected by the change. It purposely moved slowly and deliberately to make sure everything was right! The IA Career Panel was established in February 1990, while the Career Field itself officially came into being in January 1991. The first Intelligence Analysts were certified in the beginning of 1993.

~~(FOUO)~~ By 1993, the IA career field had been around long enough that the IACP was make some judgements about its strengths and weaknesses, or perhaps its advantages and disadvantages. One of the significant conclusions at the criteria review conducted during 1993 was that it was unrealistic to expect aspirants to get through the dozens of NCS courses required for certification. This prompted the IACP to strengthen the core courses with the aim of creating a "journeyman" at professionalization, and of eliminating the requirement that an aspirant specialize in one of the IA skills. The IACP, however, continued to emphasize the need to pursue additional training which would serve to refine or develop one's expertise in one of the core IA disciplines (i.e. specialization) and, accordingly, developed a post-professionalization program—the Agency's first such

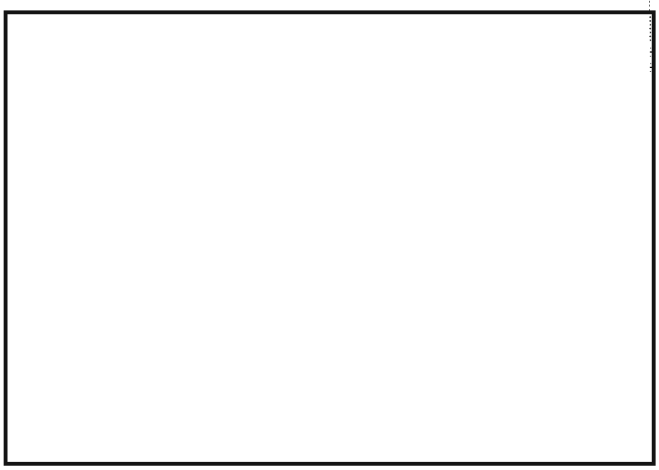
P.L. 86-36

program—which provided a structure whereby analysts and their supervisors would meet with an IACP executive to develop a coherent "continuing education" plan after certification (additional details are available in the Panel office). Also at this time the names and definitions of some of the IA skill areas were clarified

Other new programs that have been developed over the past two years have been the IA portion of the Agency Tech Track Program, the IA and Agency Cross-Training Programs, and the newest one, the Skills Enhancement Program.

II. What is Intelligence Analysis? Is it serving the needs of the Agency? What needs to be done next?

~~(FOUO)~~ During the off-site, the IACP often found itself discussing the question, "What is IA?" The fundamental conclusion was that IA is a diverse, broad field made up of analysts with a variety of skills and assets. *This breadth—although often difficult to describe—is its greatest strength.* A summary of other actions and recommendations follows:



III. Assessment of the IA Tech Track

~~(FOUO)~~ The TTRPs have found several significant challenges as they have conducted the peer reviews of Tech Track aspirants. First, their job is made more difficult by the breadth of the IA career field. They are concerned for those on the periphery of the IA world: the staffers, those working primarily in ADP as it relates to IA, those who might be more connected to the signals aspect of the IA skill area of Signaling Technology, etc. Secondly, each TTRP, as well as the IACP itself, is determined to maintain the integrity of the IA Tech Track program. There was extensive discussion on the need to cultivate a better understanding of the IA Tech Track program with all parties concerned. The discussions led to several actions, many described in the previous section, such as identifying the IA Career Field and its parts, developing a relationship with the TTRPs and the IA Masters, developing a better understanding with senior managers on their technical needs. Other actions:

- Better define the "height" of the step one needs to take to get into Tech Track (action: TTRPs and IA executives, then recommendation to full IACP).

- Help IAs see the benefit of applying to the Tech Track (action: TTRPs and IACP).

- Incorporate more specific examples into the IA Tech Track criteria to give more guidance to the TTRPs (action: IACP).

- Resolve the issue of Technical Leadership at the Member level. This issue has now been resolved. The IACP, with its newest TTRP members present, decided not to make Technical Leadership a mandatory category for the Member level. This will affect approximately 16 individuals who were denied titles in the past based on the perceived lack of technical leadership.

- Initiate ways to encourage and organize mentoring of IAs pursuing membership in the Tech Track by senior members and masters (action: TTRPs, IA Masters, Senior Management, IACP). Until the issues of feedback/mentoring are resolved or changed, the TTRPs still need to provide feedback to the IACP Exec for Tech Track aspirants.

- Discuss the pros and cons of Tech Track positions (action: IACP with input to and from DDO/DDS THAB and Senior Management).

Follow-up: The IA Open Forum

P.L. 86-36

[redacted] opened the forum with a review of the proceedings of the off-site, adding:

"We believe that having flexible training requirements will better meet the needs of all aspirants. This isn't a sudden shift in midstream; it is a move that will enable an aspirant to take courses that are more directly pertinent to one's current job in the IA field. *We're not asking for more or different courses; we're asking you to take a major role in developing your career within the boundaries of IA.* This direction is also more in line with the NCS training philosophy. It will eliminate the problem of taking classes merely to become professionalized, and will allow aspirants to take training that will enhance the skills they need for their current and future IA jobs.

"The idea of an integrated IA Career Field for the cryptologic system of the future is not dead. The IA Career Panel has continued—even renewed—confidence in the interdisciplinary and multidisciplinary vision encompassed by the Agency's decision to create the field several years ago. From time to time, we make additional course corrections, but these should not be seen as the reason for individuals to fear that their careers and programs will be harmed by constant tinkering with the system. We'll do our best to ensure that professionals and aspirants who enter the process under a given set of rules will be allowed to professionalize under those rules.

"Now, one more thing: from some of the e-mail we received, there was some confusion as to where someone might fit in the whole scheme of things. Briefly, there are basic professionalization ***and*** post-professionalization programs.

"Professionalization aims at creating a journeyman in the IA career field. With the breadth of the program, there is a definite advantage to certifying in IA; it gives you a broad base (with some specialization) from which to attack numerous, varied IA challenges. Those who are already professionalized in one of the IA predecessor fields have other choices. An individual may choose to get a second professionalization in IA and further develop the broad understanding of all aspects of the IA career field. On the other hand, he or she may decide to deepen an already acquired skill. One can do that by aiming toward a post-professionalization certificate. This program emphasizes the need to pursue additional, advanced level training after professionalization which will serve to refine or develop one's expertise in one of the IA skill areas. Individuals interested in this path must be certified in IA, in one of its predecessor fields, or in a related field, and must be working in the IA field. Again, we stress the absolute involvement of the individual and his/her supervisor in the development of a training plan that will orient them in a specific direction and cater to his/her personal and professional needs. Our IA Tech Track Program recognizes the post-professionalization program under the category of Advanced Education and Training. By the same token, Tech Track also recognizes all the work that goes into acquiring a second professionalization. You can get additional details on these programs from any of the panel execs.

"With all that said, I would like to introduce [redacted] who, along with the rest of the panel, will be happy to answer any of your questions and address your concerns." P.L. 86-36

Summary of Question-and-Answer Period:

Concerns about availability of NCS classes

What is a reasonable period of time in which one might expect to get the courses required for professionalization? I have been waiting quite some time to get certain courses.

The delays that many people experience in getting courses may be due to a lack of space and/or instructors. The NCS, like the rest of the Agency, is being asked to do more with less. They have to depend on IAs from DDO and DDS to jump in the void and become adjunct faculty members for the IA courses required for professionalization. In fact, the IACP regularly encourages and solicits individuals to become adjunct faculty. We firmly believe that one must "give back" to the career field by mentoring and teaching. It would be wonderful if we could guarantee that you would get a course within months after you've signed up for it. We can't do that right now but we are working very closely with the NCS to work out problems, to develop courses to meet the IA needs, and to prioritize our requirements.

There is a woeful lack of course available at the NCS for those who might be interested in pursuing the Information Services pillar of IA. What is the IACP going to do about that?

We have been looking into outside classes that will provide the training needed by someone working in the IA area of Information Services. We acknowledge that we are obligated to provide the training from other sources if it is not available at the NCS.

How is the IACP going to resolve the tug-of-war between operational necessity and need for training?

This is an age-old conflict. The NCS is looking at new ways of bringing training to the individual when and where they need it so that training will be an more integrated part of one's daily business. The flexible professionalization program we are proposing hopefully will go a long way toward resolving some of these problems.

How do courses dealing with Signals Research fit into the Post-Professionalization program (courses such as those sponsored or offered by the old E5)?

The IACP has always felt that the courses on understanding networks, packet switching, etc. are exactly in keeping with our needs to attack the challenges of the Global Intelligent Network. They have always been accepted in the Post-Professionalization Program and will continue to be accepted.

Tech Track Questions

Why do the standards and procedures for the IA Tech Track program in A and B Groups seem to be so different?

When the IACP first wrote the standards and criteria for the IA Tech Track, we spent a lot of time conferring with the different players to get their opinions. The resulting document purposely gave the TTRPs the latitude to deal with the variety and breadth of the IA Career field. Since the first document, the TTRPs have had the time to work with the document and have found that it needed some adjustments or fine-tuning. That has been done and the TTRPs are definitely working from the same document. However, there are some issues that are larger than the IACP and the TTRPs—issues

such as whether or not to do interviews, the role of managers in tech track, etc. These issues are currently being addressed by the Key Component Tech Health Advisory Boards (THABs).

Does staff work (A05, B05, P05...) apply toward Tech Track? A number of people are under the impression that staff work doesn't count.

The IACP feels strongly that "staff work" definitely is a part of the IA career field. Editing, developing the USSIDs that govern IA work, preparing video reports or the SIGINT Digest, and developing the standards for the career field are all vital aspects of the IA field. These are broadening assignments that enable one to understand all aspects of the IA process. Mr. Goldsmith also noted that individuals probably should not spend their careers in staff positions since one needs to refresh/hone one's skills in a target office and contribute one's expertise at that level on a regular basis.

Why is there such a time lag in evaluating TT applications?

Most tech track applications are evaluated fairly quickly. B Group has had the largest number of applications and has been working diligently to clear up the backlog. The problem is that the TTRP will review two applications and four more will come into the Panel office. The approximate period of time needed to evaluate the applications from members of B Group is 3 months. One of the changes we've recently made was to start including specific feedback with the notification letter. This will at the least decrease the time differential involved in getting feedback to the individual.

What type of incentives is the DDO THAB planning for TT members [in comparison to the DDT initiatives]?

It is worth noting that the DDO THAB authorized expenditures for technical seminars and conferences over the past 18 months that exceeded the DDT's proposal. This was done without the benefit of a specific incentive plan and details have been posted to the Technical Track topic on Enlighten. At the same time, they have been working on a comprehensive incentive plan that would include technical enhancement initiatives such as book purchases, etc. Approval of such a program is complicated by the fact that in order to provide the DDO TT members with a package similar to the DDT package, it would entail an investment of roughly $2.5M contrasted to the DDT $250K. A budget line of this magnitude at a time when we are counting pennies has a difficult path to approval and must be roundly supported and carefully accounted. This is an issue that requires patience and understanding. It is not one that is being or has been ignored. (input fm. Dale Roberts, P04 Tech Track Plan Director)

When will management incorporate technical leaders as a part of a decision-making team?

This is a two-part process. First, managers must recognize the value of using the leadership skills of technical experts on projects; those experts should be tapped on the shoulder and asked to be part of a team. That is happening in some parts of the Agency, but not all. By the same token, the technical expert must step up and volunteer. He/she should volunteer to take on the leadership role in a project and "sell" his/her worth to managers. Eventually technical leaders will become an integral part of management teams.

If I move from DDS to DDO, is the Tech Track title I received in DDS still valid?

Yes, this is an Agency program. The title you receive in one Directorate is absolutely recognized in the others.

Professional Development in IA

What level of competency does the IACP expect at the journeyman level?

As one is professionalized, we expect that you should be able to come right out of the starting gate and tackle a challenging IA problem. You might not be able to succeed at every aspect, but you will know where and to whom to go. The broad range of skills possessed by an IA will enable you to exploit a target without having someone hold your hand.

How does Post-Professionalization fit in with the recommended changes to the criteria?

(How many pillars will there be?) This is still under discussion in the IACP.

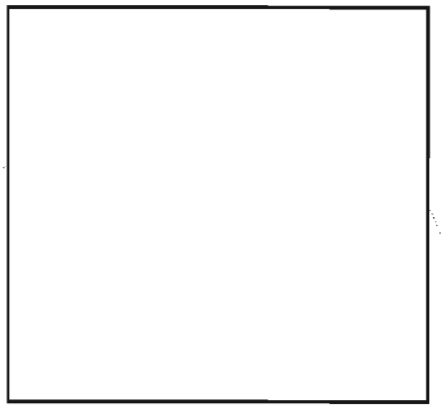
Where does layout and design, video reporting, and SIGINT Digest-type work fit into the IA career field? Is it considered part of IA?

These fields are absolutely an essential part of IA.

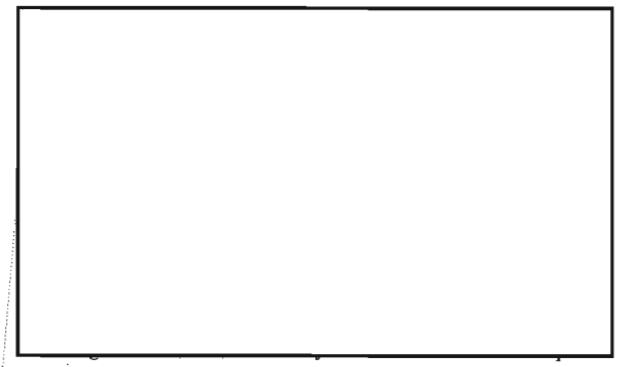
When will the changes be implemented?

We hope to have any changes in place by the fall.

*The IACP hopes to hold an Open Forum at least semiannually as a public vehicle to voice concerns. In the meantime, feel free to contact the IA Panel office (**963-1818s** or **h110@nsa**) or any of the members of the IACP:*



Bill Nolte, P054



*to DDS THAB**

** = has a title in the IA Tech Track*

Kλ

P.L. 86-36

DOCID: 4012045

CRYPTOLOG
Summer 1995

IA vs. TA/IR - An Editorial

by [redacted]

EO 1.4.(c)
P.L. 86-36

The IR-TA debate rages on

~~(C)~~ When I decided to attend Monday and Tuesday's Off-Site of the Intelligence Analysis Career Panel (IACP), I was unprepared for the evident polarization of views with regard to the Intelligence Analysis (IA) Career Field. Since becoming an IA intern in June of '94, I've become convinced that the decision to merge the Traffic Analysis (TA), Intelligence Research (IR), and Information Services (IS) Career Fields was a good one and was a bold and refreshingly innovative step towards equipping analysts with the breadth of skills necessary to meet present and future SIGINT challenges. Not all share this view.

~~(C)~~ On Monday, some vocal members of the IA Technical Track Review Panels (TTRP) voiced concern over the need to place a clear definition of what an IA is. There was also some confusion over what constituted analysis on the job. (Keep in mind that most TTRP members are not IA's. They are professionally certified IR's, TA's or both, and occupy IA COSC's.) The problems arise when these people are required to review the experience and education of a technical track applicant and grant them Member, Senior Member, or Master IA status based on a very general set of guidelines. The guidelines were purposely written that way to allow flexibility in determining what experiences and education applied or developed the skills associated with Intelligence Analysis. Unfortunately, not all agree on what those skills are and several applicants have complained that they did not receive the status they felt they deserved.

Semantics

~~(S-CCO)~~ Take the term "analysis" as an example. Which of the following can be considered "analysis" as performed by an IA?

a. Developing UNIX/PINSETTER shells and computer tools used by IA's to analyze traffic.

[redacted]

e. Working with data-flow personnel to try to determine if a recent drop-off in activity might have to do with the change in field reporting format.

f. Conducting research in the resource center in response to a Request For Information from an Office of Primary Interest (OPI) analyst.

(U) If you're a trained IA, you're likely to say that each of these examples falls within the domain of intelligence analysis. IR's and TA's often don't agree. P.L. 86-36

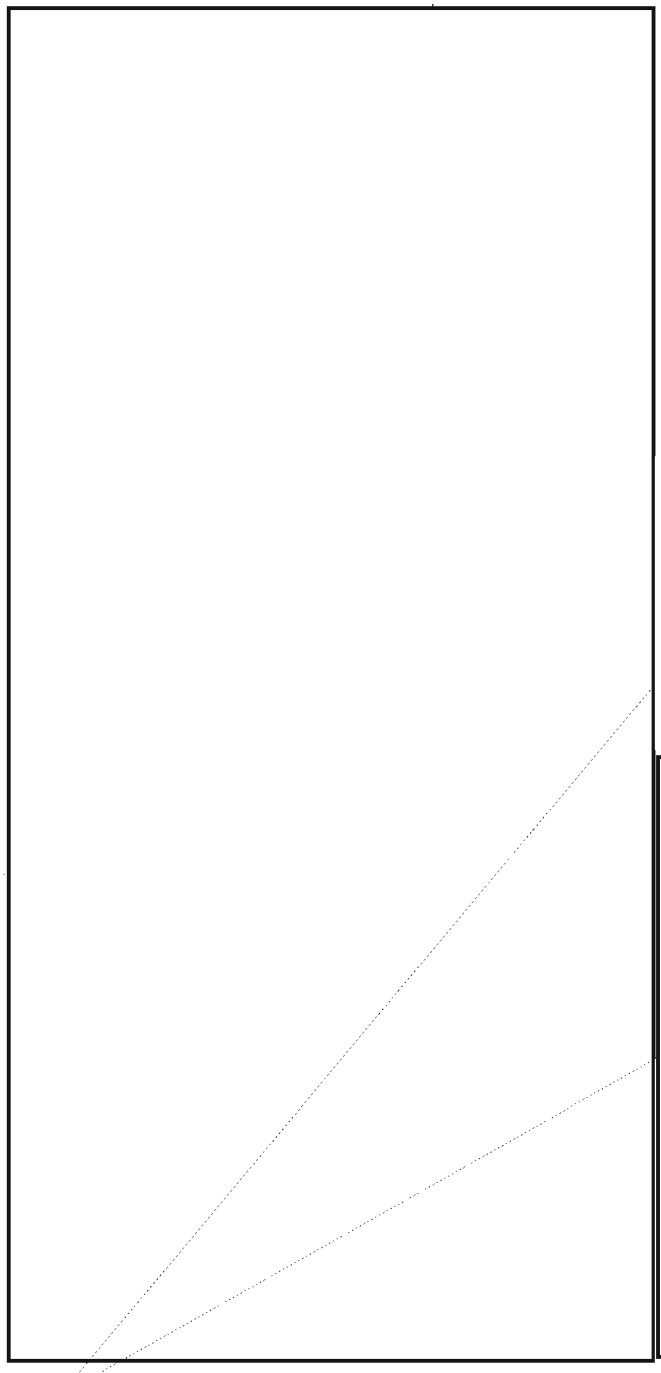
~~(C)~~ [redacted] one of the first graduates from the IA Intern program and previous council chairman defines an Intelligence Analyst as [redacted] I like this definition, and when I compare the above examples, I find that each one applies.

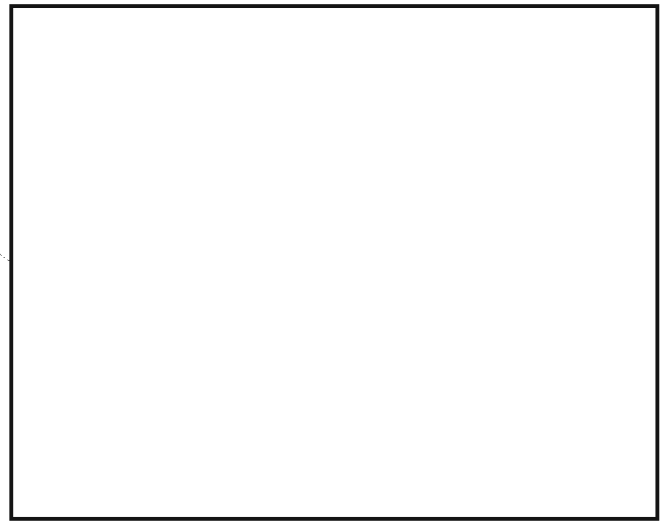
~~(C)~~ The semantics problem is not only one of definition. It is equally one I call *bias of association*. What I mean is that when we hear the terms "Reporting and

P.L. 86-36
EO 1.4.(c)

Traffic Analysis," we tend to envision analysts doing very specific kinds of things. The two jobs don't even appear to be related in any way when we conjure up these traditional images. Some TTRP members seem to believe that the skills associated with each are so different that one cannot successfully do justice to both disciplines. I would agree, if we had unlimited resources and well-defined, static targets, but in our current reality, I disagree.

Generalists Or Specialists?

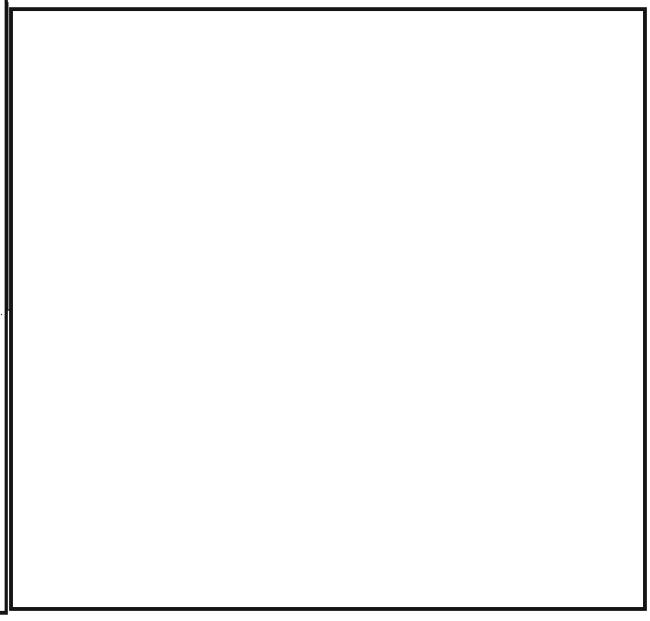




(U) We have to rethink the way we do business (you'll hear this as much as "more with less") and career field architectures of the past (read: IR and TA) are, for good reason, casualties of necessity.

The IA Career Field: Again?

(U) As with any completely new endeavor, the field has endured growing pains. There is resistance from the subsumed career fields, the ambiguity of its definition, and a lack of understanding of its content and objectives on the part of the rest of the Agency. Further complicating matters is that we don't have enough facts (rather than opinions) upon which we can properly judge whether the new career field is meeting the organization's and our national needs.



Whither Now?

~~(C)~~ For at least the third time since its inception in 1990, the criteria of the IA Career Field are under review and will likely undergo change. A decision has already been taken to drop "Technical Leadership" as a requirement for Member-level status in the IA technical track and we are moving forward on defining IA based upon the structure of its "Three Pillars." These Pillars are identified as IR, TA, and IS.

(U) I'm apprehensive about using these terms so aggressively when discussing our architecture for two reasons:

1. The *Bias of Association* which occurs at the mention of IR and TA and...

2. The IA program (required courses and experience) encompasses so much more and is greater than the sum of its parts. What about Signals Research, Target Development, and Collection?

(U) While perhaps having so many general skill categories as we currently do is somewhat cumbersome and confusing, I feel we do more damage than good by using the terms IR and TA to describe the Pillars of our career field...unless we've erred and wish to go back to the past, that is.

(U) Of course this is all my opinion, and as I've attempted to show, everyone has one. I think, however, that there are some valid opinions still left unheard—those of the IA Interns, and especially graduates of the program (and their supervisors!). It is *our responsibility* to make sure that our mentors know whether or not we feel as if we're getting the kinds of experience necessary to carry this Agency through hard times and into the 21st Century. I urge you all to let them know immediately.

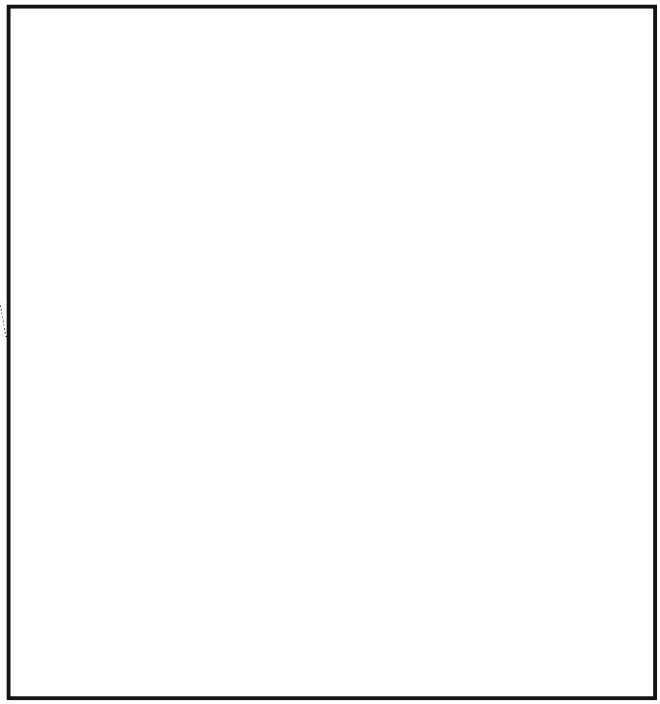
Kλ

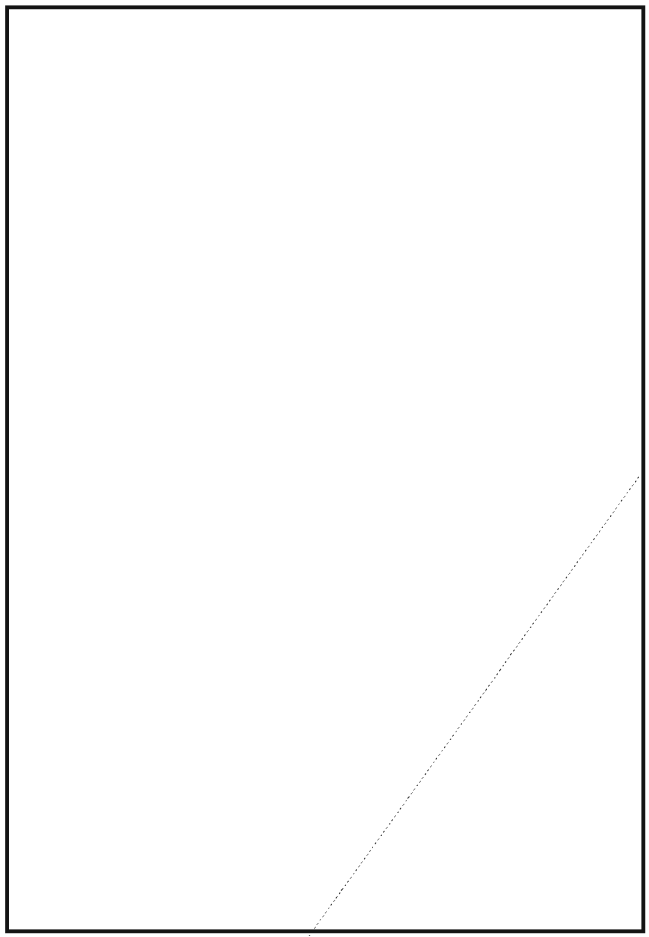
P.L. 86-36
EO 1.4.(c)

The Phoenix HF: An Editorial

by N.C. Gerson, R52

(U) A recent note in NATO's Scientific Technical Planner (STP) acknowledges that HF is not dead but is a reliable contender for long-haul communications. NATO found that on a cost basis (per message or per year) HF is cheaper and about as effective as more costly and sophisticated satellite circuits. In short, NATO discovered what





NSA's "Lessons Learned" Database

P.L. 86-36

by Ben Cwalina, N25

(U) Would you like to know what lessons NSA has learned lately? If you have [redacted] available on your computer then it's easy. Look at the Directorate for Plans, Policy, and Programs (DP) home page and click on the "Cryptologic Lessons Learned" button under DP PRojects and Publications, or, under NSA Projects/Programs, [redacted] After entering the database you will see the menu that provides the categories of lessons learned: Crisis Management, Security, SIGINT, Interoperability, and Communications. A very important part of the database is the "keyword" search. You can place any word in the search area and within seconds, if a lesson was ever written using that word, the lesson number will appear on your screen. [redacted]

Here is a sample:

EO 1.4.(c)
P.L. 86-36

[redacted]

P.L. 86-36

1. (U) TITLE: Near-Real Time Intelligence (NRTI)

2. (U) KEYWORDS: 1537, 1536, 1519, 1539, 1543, 1549, 1559

3. (U) OBSERVATION: On December 19, 1994, the Washington Post reported that the *USS Kitty Hawk*, a U.S. battlegroup carrier, had located and trailed a Chinese nuclear submarine operating in the Yellow Sea from 27 to 29 October, 1994.

[redacted]

[redacted]

5. (U) LESSON LEARNED: New technology displays the value of SIGINT.

[redacted]

Kλ

P.L. 86-36
EO 1.4.(c)

P.L. 86-36

The 1995 Joint Mathematics Meetings

ed. by [redacted]

P.L. 86-36

(U) The Joint Mathematics Meetings of the American Mathematical Society (AMS) and the Mathematical Association of America (MAA) are **the** annual event for mathematicians in the United States. The 1995 meetings took place in San Francisco, California, from January 4 through January 7, and offered a panoply of happenings which cater to the variety of interests of the 4000 registrants and 400 exhibitors. The short courses, invited talks, and contributed-paper sessions allowed us to learn about current areas of research and interest in both academia and industry. But the Joint Meetings proffered much more than these trappings of a traditional technical conference. Many other sessions, organized by individuals as well as professional organizations, delved into related issues. The variety of other issues addressed included teaching and learning (titles include: Calculus from graphical, numerical, and symbolic points of view, Learning styles approach to mathematics instruction, Teaching with original sources), career considerations (Mathematical preparation of the technical work force, Learning about today's job market for mathematics Ph.D.s, How to help your students prepare for and find jobs, Life after retirement), Internet usage (Internet tools: what are they and how do you get them; e-MATH on the World Wide Web), competition and rewards (Mathematical competitions: bringing out the best?, Recognition and rewards in the mathematical sciences), and special issues facing women and minorities (including events sponsored by the Association for Women in Mathematics and the National Association of Mathematicians). An exhibit hall full of prospective employers (including NSA), software firms, publishers, and professional organizations offered additional information to members of the U.S. mathematics community.

(U) The 1995 Joint Mathematics meetings provided an excellent opportunity for Agency mathematicians to develop and maintain contacts with mathematics and mathematicians on the outside. Attendance at this conference allowed NSA mathematicians to keep abreast of the "hard-core" mathematical research being done on the outside. Other sessions, such as those on teaching and mathematical career opportunities, gave Agency attendees a good feeling for the issues of importance to our national mathematics community. Sessions on women and minority issues allowed us to gauge the concerns of these specific populations. Many NSA mathematicians used this as an opportunity to maintain and expand their network of acquaintances in the U.S. mathematics community. Many Agency conference attendees staffed the NSA information booth in the exhibit hall, discussing employment opportunities with prospective applicants and distributing general information to those who were just curious about what we do. Several Agency employees conducted interviews with Agency applicants. The reunion held by the Steering Committee of the NSA Women in Mathematics Symposium (WiMS) (funded by R51) provided an informal opportunity for all interested conference attendees to learn about Agency employment (more on this event follows).

(U) There was an incredibly large number of talks at the conference, with as many as 20 events running simultaneously, ranging from very technical to more general. There were talks oriented toward mathematical research, theories, and history as well as talks discussing the Internet. There was an emphasis on the relationship between academia and industry, with an emphasis on curriculum reform. The Agency representatives attended a variety of talks and activities, including:

(U) **Mathematics and the general public: What do they know? What should they know?** Panel Discussion by the Joint Policy Board for Mathematics (JPBM). The panel included mathematicians and several members of the popular press discussing how math ideas and discoveries are treated in general publications. The panelists stressed the need for mathematicians to tell others (e.g., via newspapers) about our exciting news. Suggestions for getting math articles published included being willing to generalize results (even at the risk of distortion!), focusing more on the human-interest aspect (e.g. how does this math result change people's understanding or life-style?), and learning to state the problem to be solved in language the general reader can comprehend. One panelist thought that the philosophical aspects of math would be of particular interest to the general public. He even won-

dered whether "God was a mathematician" since, as he put it, math is able to describe our world so well.

(U) **Internet tools: What they are and how you get them**, Wendy Bucci (AMS). This presentation introduced people to some of the tools for finding information on the Internet: gopher, veronica, archie, ftp, telnet, WAIS and WWW. Gopher is a menu-driven index of various on-line services (such as card catalogues for some libraries). Veronica (Very Easy Rodent-Oriented Index to Computerized Archives) is an indexed database for gopher sites; it returns a gopher menu. Telnet allows one to connect to a remote system and execute commands as if one were at the remote site. The ftp (file transfer protocol) allows uploading and downloading of files from and to your own local file system. Archie is an indexed database of ftp sites; it returns site and file names. The search is performed only on file names and descriptions; for a search on actual text one must use WAIS (Wide Area Information Service), which returns a ranked list of documents based on the number of occurrences of search strings. WWW (World Wide Web) allows one to search gopher, ftp, telnet, WAIS, and Web sites. Some on-line help is available for commands such as archie and veronica through the e-math telnet site which is operated by the AMS.

(U) **MAA Session on Teaching with Original Sources.** The really interesting thing about this session was the uniform conclusion that there are real benefits to teaching from original sources. Chris Stevens of St. Louis University felt that the use of primary sources in the classroom emphasized to the student how good/bad notation helps/hinders progress on mathematical problems. Professor Stevens tries to emphasize the relationship between mathematics and the culture of a period to show how the knowledge of mathematics distributed in society. She feels that this illustrates what the practical uses of mathematics were (and are) in everyday life, and serves as a good example of how mathematics can be used in the non-academic world. In one particularly interesting assignment, she asked her students to pick a year in the past and find out what the mathematics curriculum consisted of at their college. She reported that students were astounded to find that in the year 1875, students took 2-year-long courses in arithmetic, followed sequentially by year-long courses in algebra, geometry, trigonometry and surveying, and finally calculus! Professor Stevens noted that the math universe seems to be expanding. Today's college mathematics curricula have shifted the focus from the student and instead rush through basic mathematics in order to cover as much advanced material as possible.

(U) **Math in Industry,** Avner Friedman (RPI), Paul Davis (Worcester Polytechnic Institute). This session detailed the results of a recent industry study. To summarize, industry desires the following traits in the mathematicians they hire:

- Broad background with depth in one subject
- The ability to work in teams
- Communication skills (speaking, writing, listening, reading)
- Promise of continued professional growth
- Computer skills

(U) *Bottom line: industry is looking for flexible problem solvers (whatever we call ourselves) who can communicate with non-math consumers.* Industry is not nearly so impressed with our math degrees as our ability to work with others to get answers that are "good enough." The speaker noted that many in industry fear that mathematicians have an interest only in proving theorems, not relevant problems. He added that encounters between academia and industry are limited by geographic proximity to chance meetings. Mathematicians need to be able to understand the practical problem, and communicate their solutions clearly, without generalizing them to the extent that they are incomprehensible to others in industry. He added that mathematics students undergoing a one-year internship in industry, like that program established by Professor Friedman, have found their lives changed. Such an experience provides them with the self-confidence and self-esteem to succeed as mathematicians in industry.

(U) **MAA Minicourse: Teaching Environmental Numeracy To Liberal Arts Students,** Martin E. Walter (University of Colorado, Boulder). Walter is a mathematician and an environmentalist; which passion is stronger would be difficult to tell. His goal is to make mathematics come alive for his students; his agenda is the environment. The enthusiasm with which he embraces these subjects is a pleasure to witness, and the degree to which he combines them quite remarkable, as are his conscious efforts to allay the fear of mathematics that some students have. He uses the environment to teach mathematics and he uses mathematics to teach understanding of the environment and

the need for an "ambient, functioning ecosystem to carry our civilization."

(U) The primary objective for the course is the completion of a project on an environmental topic of the students' choice. By allowing the students to choose the topic, he finds they are much more likely to be motivated to conduct research and learn mathematics. The students make a claim and attempt to prove it. Walter makes extensive use of open-ended environmental problems to stimulate interest in both the environment and the learning of mathematics. For example, a discussion of population growth provides an entree into logarithms. He also challenges students to try to come up with a model to control the population, or at least keep it from exploding. This leads to the need for scaling, or "how to lie with graphs." Other environmental issues that provide content are: deriving energy from junk mail, acid rain, and oil slicks. Health issues such as AIDS and nutrition (e.g. milk and muscle: how high can you climb on a liter of milk?) are also fair game.

Can math explain this?

(U) To allay student fears, the class begins by confronting "mathese." The question is asked, "How would a mathematician say that?" The course is open to students at all levels of mathematical experience. They begin the course by taking a mock exam that Walter uses as a diagnostic tool to assess the students' level of ability. To accommodate the wide range of experience, the level that students attain at the end of the course is not the focal point; rather, the critical factor is that a student makes progress.

(U) Walter uses a variety of exercises to relate to his students; his notes contain descriptions of personal experiences and anecdotes. He also uses examples of poets and architects. His material is current; he even has an exercise that gets students out on "the information highway." Students become mini-experts on their topic of choice. Along the way, they learn to think critically. His goal is to create people who can and will critique, or explain, articles in the New York Times or assertions made by people like Rush Limbaugh.

(U) In reflecting on Walter's style of teaching mathematics, one attendee found a lot that she could take away. Our agenda, of course, is not the environment, but perhaps we could wrap up our teaching of mathematics with our agenda just as effectively and with similar levels of enthusiasm.

(U) **MAA CUPM Subcommittee on Service Courses Special Presentation: Reform in Engineering Curricula.** While coming at the problem from a different perspective, this panel came to many of the same conclusions that the participants of the **AMS Committee on the Profession Presentation** discussion on math in industry. Delores Etter (Electrical Engineering and Computer Science, University of Colorado at Boulder) noted that the CEO of Martin Marietta had come up with the following list of reforms for the engineering curriculum of the 21st century:

1. Emphasize the basics, including applications with hands on experience, and experience in manufacturing and design.

2. Develop team skills.

3. Teach students about the political process and how to present a case.

4. Develop communication skills.

5. Teach system engineering to emphasize the combination of diverse disciplines.

6. Understand international communications since we are moving towards more of a world market.

7. Emphasize greater diversity.

8. Increase commitment to continuing education.

9. Education should be affordable and of quality.

10. Engineering should be a master's degree.

The Director of Engineering at the National Science Foundation came up with the following comparison between today's and tomorrow's engineering approaches:

Today	Tomorrow
vertical thinking	lateral thinking
abstract learning	experiential learning
reductionism	integration
develop order	correlate chaos
understand certainty	handle ambiguity
analysis	synthesis
research	design/process/manufacture
solve problems	formulate problems
develop ideas	formulate ideas
independence	teamwork
technological/scientific base	societal context
engineering science	functional core engineering

(U) **Mathematical preparation of the technical work force**, MAA sponsored panel discussion led by Susan L. Forman of the Mathematical Sciences Education Board. Panelists presented their views and experiences relating to the need that business and manufacturing areas have today for employees with higher levels of mathematical sophistication. Employees are needed who can read charts and graphs, solve problems, estimate, use computers, use and interpret probabilities and statistics, collaborate and communicate mathematically in writing. Discussions focused on the tradition of tracking students into non-theoretical math courses at a relatively early age. This limited their ability to make changes later, to continue to study math at the community college level or beyond, for example. The view of one speaker was that if the curriculum is fundamentally theoretical enough, people will be able to move in and out of the education arena. It was stressed that it is critical to teach the theory through the vehicle of the applications. Another speaker stressed that lifelong learning *is* a reality of the workforce. Examples were also cited where changes such as these have already been made.

(U) One panel member stated that quite often important results are obtained by the sophisticated use of elementary mathematics. (An NSA attendee feels this also is the case at NSA; many times critical problems are solved with rather elementary math, but with the mathematical maturity to know that the answer is right.) One of the reasons that math seems so impractical to the average high school student is that college-prep-type schools emphasize theoretical knowledge rather than the applied skills taught in technical schools.

(U) **The Information Superhighway and You**, panel discussion sponsored by the MAA Committee on Computers in Mathematics Education and Committee on Electronic Services. The first speaker was from Silicon Graphics. His points were:

- Networks were slower in the past but we were only transferring small ASCII files. Systems are faster now but we don't see an increased efficiency because of the huge files (video, etc.) involved.

- The Internet has a lot of good stuff in it but the majority of the information is junk. Like TV, the Internet could be used for tremendous educational advantage but the money is in entertainment, so, as with TV, the Internet is dedicated more to amusement than to education.

- World Wide Web (WWW) services are typically organized very poorly. He also noted that it is easy and fun to set up a home page but very difficult and laborious to properly maintain it.

(U) The second speaker was from Bell Labs. His main points were: The information superhighway is more than just the Internet; it also comprises telephone lines and other communication media (cable, satellite, etc). He mentioned Vice President Gore's ambition for a virtual equivalent of the national highway system his father was instrumental in building, but said that there was no need for the "construction" of such a system since it is already out there and in use. It grows as users increase. In his opinion, the big problem with the Internet is that there is no one in charge; it is running itself. Furthermore, since it is global in scope, there is no governing body capable of enforcing regulations.

(U) The last speaker's points were: There are major potential commercial uses for the Internet if security concerns can be resolved. The ability to post anonymously is one of the problems. In fact, right before the conference someone posted an item that stated that Microsoft had bought out the Catholic Church. While it should have been obvious that this was a spoof, many people on the Internet were fooled by it, or so Microsoft claimed when it issued an official denial. During his

talk, the speaker asked how many people in the audience had never heard of or knew about public-key cryptography. Unbelievably, in an audience of 150+ mathematicians, approximately 30% raised their hands.

(U) **Ingenious Mathematical Amateurs: M. C. Escher (artist) and Marjorie Rice (homemaker)**, Doris Schattschneider (Moravian College). A very interesting presentation on contributions of non-mathematicians. Escher's work is of course well known through his incorporation of various types of symmetry in his art work. Schattschneider presented several samples from his notebooks and discussed a classification system Escher developed. Rice, a housewife from Florida, became interested in tilings after reading an article by Martin Gardner. She developed her own classification system for pentagons which tile the plane and was responsible for discovering several new tiling pentagons which had not been identified previously.

(U) **Synchronous Fireflies**, Steven Strogatz (Cornell University). This talk was part of a contributed paper session on **Chaotic Dynamics and Fractal Geometry**. The speaker described many systems that spontaneously synchronize, and showed how we can model this mathematically. The talk included a fascinating video about South Asian fireflies that flash in synchronicity (North American fireflies don't do this!). This example of a self-organizing system was used to illustrate a discussion on how synchronicity occurs out of apparent chaos.

(U) **AWM Workshop**. The point of the workshop was to give women graduate students and postdoctoral mathematicians an opportunity to present and discuss research with other women mathematicians. Postdoctoral women gave 20-minute talks, and graduate students displayed posters. The lunch buffet was especially nice as it provided time to meet and visit with various mathematicians.

(U) **AWM Panel: AWM (The Association for Women in Mathematics): why do we need it now?** This was a lively meeting attended by approximately 100 people, primarily women (and one baby). The format was a panel discussion followed by a question and answer period. The first speaker, Sylvia Bozeman (Spelman College), commented that there have been a lot of changes since the founding of the AWM in 1971. She noted that, according to a survey taken in 1986, less than 2% of the students in the mathematical sciences are African-American, and added that there is a lot of attrition at each educational level. She pointed out that 1.7% of the mathematics Ph.D.'s go to African-Americans, 15% go to women, and 20% go to women who are U.S. citizens. She believes that there is a serious need for mentors for these women, and that the AWM can provide a forum for discussion of such concerns. Professor Bozeman pointed out the importance of summer math programs like the one held jointly by Spelman and Bryn Mawr. Such programs provide an opportunity for women to enter into mathematics, as well as an excellent networking opportunity. She believes that the AWM provides a badly needed opportunity for minority women to belong to a proactive organization.

(U) Ruth Williams (University of California at San Diego) was the next panel speaker. She discussed a Women in Probability Conference which was held in October 1994 and which she organized [redacted] served as a panel speaker at this conference). She pointed out that a lot of young women, both graduate students and junior faculty, filled out the list of approximately 60 attendees. This provided an excellent opportunity for networking, allowing people to get advice on subjects such as obtaining tenure. Women in general need to be more active at conferences, serving as speakers and organizing special sessions. Professor Williams added that research institutes (e.g. Institute for Advanced Study) are good places to visit early in one's career, but such things as the absence of child care stand in the way of making this a viable alternative for women. P.L. 86-36

(U) During the question-and-answer period several interesting points were made. [redacted] talked briefly about the Women in Mathematics Symposium (WiMS) which was held at NSA in November 1993. She noted that the conference was held for the altruistic reason that the Agency was concerned about how few women are pursuing mathematics as a career, and for the more selfish reason that the Agency is concerned about a future absence of women mathematicians in their applicant pool. She noted that one of the suggestions from the conference, to make the recruiting literature more informative for an audience of women mathemati-

cians, had been implemented in a one-page addendum which was available at NSA's recruiting booth. Dr. [redacted] noted how important it was for the WiMS attendees to keep using the network that this conference created. To that end, she announced a WiMS reunion which would be held Wednesday night and emphasized that all were welcome to attend (immediately following her remarks, another woman got up and insisted that the purpose of the AWM is for women to band together and not work for places like NSA).

(U) Ruth Williams mentioned the NSA Women in Mathematics Symposium which she had attended. She specifically mentioned the *Proceedings* that came out of that conference. She feels that it is very important to document conferences in this fashion to assure the best networking and dissemination of material.

(U) **e-MATH on the World Wide Web** (AMS presentation). Currently, the January 1995 *AMS Notices* are available electronically and soon previous volumes back to 1992 will be on-line. By 1996, it will be possible to have an e-mail subscription of the *Notices* of the AMS and the *Bulletin*. The organization will be the same as for the hardcopy and the cover of the *Notices* will even be scanned in full color (the cover has changed as of January 1995 and is no longer an ugly shade of beige). A preprint service is available via the **AMS home page**, and even if an author has used another ftp service, it is possible to register on the AMS service so that a link will be provided to the other service. The list of availability isn't very large yet, but eventually, abstracts will be available and it will be possible to search for on-line articles by author, subject, issue, etc.

(U) **Teaching Linear Algebra with Technology: Its Impact**, David Hill and David Zitarelli (Temple University). Hill and Zitarelli gave a talk and demonstration of the Linear Algebra course they have been teaching at Temple since the mid-80's. The course consists of 3 hours of classroom instruction plus about 2 hours of lab per week, where they use MATLAB 4.2. The lab experiments are under the control of the student, who supplies the input and the logic, with MATLAB doing the arithmetic and graphing the geometric significance of the results. The student is encouraged to work by hand on the problem at first (for example, doing row operations in the solution of simultaneous linear equations) and then run the program which does the same, and a second program which graphs the past step of the algorithm. The student is also required to explain in writing the scenario for each system of equations (i.e., whether the system is consistent, has a unique solution, infinitely many solutions, etc.). For further understanding, the student can run *rrefmovie*, which runs a "movie" of the changes which take place as the algorithm progresses.

(U) Such technology obviously has the potential to make Linear Algebra more understandable. The speakers emphasized, however, that technology does not make bad teaching good, but that it does make teaching more challenging, because the instructor must adapt to changing technology and also adapt the technology to his own situation.

(U) **NSA WiMS reunion.** The reunion of participants of the November 1993 Women in Mathematics Symposium was well attended with approximately 50 external people. It was an excellent opportunity to mingle with other mathematicians (men and women) in a relaxed, less overwhelming atmosphere. This provided a nice opportunity for us to advertise ourselves. We found that the WiMS Proceedings and the one-page addendum developed by WiMS for our recruiting literature were popular items at this get-together. The success of this function can be largely attributed to the unselfish enthusiasm of many Agency conference attendees. A showing by of a lot of NSA mathematicians, including a lot of young women, went a long way towards showing that NSA is an affirmative action employer with a large community of women mathematicians which it is eager to retain. Leslie Gruis strongly recommends that a similar function be held at the Joint Math Meetings again next year. Such social occasions give a relaxed way for academic women mathematicians to maintain their contacts with the Agency, and serve to maintain the network which was established by WiMS.

(U) **NSA Information Booth and employment registry.** Working the NSA information booth was one of the most interesting activities. We met lots of academic mathematicians, professors and graduate students, who wanted information on job opportunities, and talked to quite a number of women about opportunities at the Agency. It was fairly busy, with most questions pertaining to employment and to summer

programs. One Agency representative felt that there was not adequate information to distribute about the summer programs available here at the Agency—the Director's Summer Program, the Z2 Summer Program, or the Z5 Summer Program. Many instructors came by the booth looking for information on summer employment at the Agency and we had none to give them.

Conclusions

(U) The 1995 Joint Mathematics Meetings provided an excellent opportunity for Agency mathematicians to develop and maintain contacts with mathematics and mathematicians on the outside. These contacts came in a variety of settings: through technical talks, panel discussions, and informal networking events such as the WiMS Reunion. The large number of NSA people sent to the Meetings, and in particular the high proportion of NSA women attending, spoke well for the Agency. It shows that NSA is committed to taking an active role in the mathematics community. It is important to make ourselves seen and to let people know that a wide variety of good mathematics and opportunities exist at the Agency.

(U) Considering the diversity of events at the Joint Meetings, it is hoped that NSA will be able to fund a comparable number of attendees for the 1996 Joint Meetings. So many things went on simultaneously that it was very difficult for the attendees to cover everything. The WiMS Reunion was a good first step towards getting more Agency attendees actively involved in this conference. It is hoped that NSA attendees will be able to maintain a higher profile at this conference next year, perhaps through giving technical talks, organizing special sessions, or serving on panel discussions. Only through active involvement and participation will the U.S. mathematics community come to recognize NSA as a prestigious place with which to be associated.

This article was condensed from a trip report by [redacted]

Joyce Keller, [redacted]

Kλ

P.L. 86-36

SIGINT Bloopers

Despite the best efforts of the IS-180 and IS-290 instructors, some of our product reports contain real howlers. The most common category, of course, is the homonym, or What Spell-checkers Don't Catch:

"The Secretary arrived in a Leer Jet." Who manufactures this aircraft? And does the official in the following example use one?

"Foreign Minister Leary of International Disapproval"—we didn't know there was an Irish Cabinet-level post devoted to international disapproval.

"The ambassador to the Holy Sea"—let's see, would this sea be the Dead Sea, or the Great Salt Lake?

"Zendia waivers on secret ballot"—wavering on whether to waive secrecy, perhaps.

"The journalist, a known confident of the department head"—confidant of his access, no doubt.

And we have lost count of the number of attempts to "diffuse" explosive situations (very effective, spreading those explosive situations around) or to "illicit" a response. Likewise those entities that find themselves in dire straights. (We applaud the field site that actually issued a change correcting a report containing this one.)

It's not just product reports: remember the poster for Law Day proclaiming that a distinguished visitor's talk would "sight" famous court cases? (This one was followed by a memo "siting" examples.) Or the staff memo that referred throughout to the country of "Cypress"? (Was that where the tree-people in "Lord of the Rings" came from?)

Vacancy announcements are not immune: "This opportunity is taylor made for intelligence analysts." Who is this person Taylor, and does she make other opportunities?

Too great dependence on spell-checkers leads to another source of puzzlement: hitting the "correct" key without looking at the suggested correction. We have seen Zagreb described as the "Creatine" capital (creatine, FYI, is a hydrocarbon) and a reference to "the cryptozoite community" (probably a very small community, given the size of your average cryptozoite).

Malapropisms are another category: "This would allow the bank to recuperate its losses."

Then there's the Almost But Not Quite Right Word: "The number of wounded was unaccountable"—we can see those UN observers scratching their heads; there's just no accounting for some things.

"Technicians awarded for good work"—a novel approach; what would you do with a technician you were awarded?

"UN observation post overtaken by rebels"—the post was heading southwest when the rebels caught up with it.

This category reminds us of Mark Twain's dictum that "the difference between the right word and the almost right word is the difference between lightning and lightning bug."

Slipshod cutting and pasting, and other careless editing, results in such gems as "the government, frustrated by a lack of failure to prosecute the case..." or "please cancellation this report." Grammar-checkers are not yet sophisticated enough to catch these.

Nor will they catch such startling titles as "Boutros-Ghali To Be Advised Not To Request Troops To Take Safe Haven From The UN Security Council"—It must have come as a shock to the refugees to realize they were being held prisoner by the UN Security Council.

Thanks to all the eagle-eyed readers who passed on these examples of What To Watch Out For. Contributions to a follow-up column will be gratefully accepted!

Kλ

Patriotic Liz does her part

CRYPTOLOG
Summer 1995

Book Reviews

For the President's Eyes Only

By Christopher Andrew. NY: HarperCollins, 1995.

Reviewed by Bill Nolte, P054

(U) At the risk of stating the obvious, an understanding of American intelligence (or foreign policy) requires an understanding of American ideals and values. While the same could be said of German or Transylvanian intelligence, a particular emphasis in the U.S. on public adherence to high standards of morality (or moralism), openness, and legality provide a context for intelligence operations unlike that faced by any other great power. This carries over even into the scrutiny of intelligence, where the question asked is more likely to be "Was it legal?" than "Did it work?" One consequence of this is that American observers or students of intelligence, academic or journalistic, who accept the necessity of intelligence must often spend a great deal of effort professing that they do so while concurrently believing in democracy, human rights, and other American ideals.

(U) Perhaps because they need not be concerned about running afoul of such ideals, British historians appear to have an advantage in the developing literature of intelligence. An inclination to accept as a necessity of state and an ability to at least understand the context in which intelligence must take place in this country seem to come together in the works of such historians as John Ranelagh and Christopher Andrew. Some years ago, Ranelagh's *The Agency: The Rise and Decline of the CIA* provided a critical but sympathetic look at CIA and American intelligence in general. In concluding that in moments of "achievement as well as condemnation," CIA mirrored the efforts of the "most decent of the great powers . . . the one that even in its darkest passages practiced most consistently the virtue of hope," Ranelagh struck a balance that many American critics would find difficult to achieve.

Bully for intelligence

(U) Christopher Andrew's *For the President's Eyes Only* establishes an equally balanced view. In this account, American intelligence is a mirror both of the fluctuations in America's role in world affairs in the 20th century and in the evolution of American public ideals this century has induced. Even more particularly, and extending back to the beginnings of the Republic, the history of American intelligence, Andrew makes clear, is inextricably linked with the history of its presidency.

(U) For most of this country's history, intelligence enjoyed an even lower rung on the ladder of national interest than did either the military or diplomatic components of what we would in recent times come to describe as the national security establishment. George Washington understood the value of intelligence, but few of his successors did or needed to. The good fortune of this nation was that few of them needed to know much more about military or diplomatic affairs between 1815 and 1914.

(U) By the 20th century, of course, the world had changed, with predictable results across all three components of the national security apparatus. Theodore Roosevelt broke the mold in his interest in intelligence, but that was a typical TR reaction to virtually anything. In intelligence as in much else, Roosevelt was a harbinger of change.

(U) Presidential interest in intelligence from 1917 through 1940 reflects the wide swings in presidential and public attitudes toward international affairs in general. The First World War brought an explosion of intelligence capability (and in cryptology brought to prominence both Yardley and Friedman); the 1920s brought the illusion that "normalcy," as defined by Victorian and Edwardian standards, could be restored. After 1940, of course, U.S. presence as a world power

[redacted] a permanent part of our national life, a development Andrew traces with great skill.

(U) This should not suggest that after 1940, all was linear and progressive, and here perhaps the requirements of the survey form (i.e., so much data, so few pages) lead the author to understate slightly the centrality of the period 1945-1950 as a conscious and difficult redirection of that policy.

(U) Andrew describes President Truman's use of intelligence in fairly positive terms—this, after all, being the President who created the Central Intelligence Agency, the National Security Council, the National Security Agency, and the (more or less) unified Department of Defense, much of the key instrumentation of postwar American intelligence. Andrew might have focused a bit more on the extraordinary transformation of this president, whose early motto of "economy and efficiency" was not far removed from an earlier time's concept of "normalcy."

(U) Though Truman's view of the world had been influenced by the First and Second World Wars, it took a remarkable (and still controversial) series of actions and reactions for this small-town-bred, Midwestern president and his largely Eastern patrician advisors to convince the American people that they had entered into a period of virtual war no less dangerous than the actual war they had just won. In the end, Wilsonian optimism, embodying the view that American involvement in the military and political crises of Europe and Asia could be episodic and conclusive, had failed. The cold, dark reality of the late 1940s was that a permanent struggle was under way, with no assurance it would end in a world in which democracy could survive, let alone be made safe.

(U) The remainder of Andrews' work is a restatement of the drama that followed. What makes this an especially valuable restatement is the author's success in noting the degree to which intelligence reflected the interests and views of the presidents who followed Truman. From the structured mind and extensive experience of Eisenhower, through the romanticism of Kennedy, and the provincial insecurity of Johnson, as through the presidents who followed, the relationship between presidents and the intelligence establishment (especially the CIA) remained remarkably sensitive to personality. It may be an exaggeration, but one suspects that throughout the Cold War era, especially in the pre-Nixon period, intelligence remained remarkably personalized in its support to the president, with a relative lack of institutionalization.

(U) Before the reader scoffs, note the key word "relative." Below the surface seen by the presidents, institutionalization took place, both within those intelligence components subordinated to cabinet departments and within the CIA. And in fact, one of the correctives of the Watergate era and beyond was a continued effort to bring intelligence into greater institutional and regulatory conformity with the rest of American government.

(U) This brings Andrew's study to a close and the rest of us to the present question: as we cope with the still-being-defined post-Cold-War world, what intelligence structure and capabilities does the United States need? In a world in which closed totalitarian societies have (with a few very dangerous exceptions) disappeared and CNN and Internet have provided open sources with access and coverage unimaginable only a few years ago, do we need an apparatus that in its very secrecy moves toward the edge of what the American polity can tolerate?

(U) The good news is that neither the polity nor its values are frozen in time. As we enter a period of transformation, it may be reassuring to keep in mind that three times in this century—in 1917 (with an assist from the German Navy), in 1941 (with an assist from the Japanese Navy), and in 1947-1948 (with an assist from the Red Army)—presidents have asked the American people to take on the responsibilities of a challenging world. And each time an American nation maturing with experience has responded. Whatever the difficulties facing the United States as it moves to the next millennium, the 1970-something comment of a European-born academician that the United States would be "the first country to go from adolescence to middle age without passing adulthood" seems thoroughly wrongheaded.

(U) Taking a leap of extrapolation, Andrew has written a useful text for the era of retooling of the American intelligence apparatus, one that suggests this country will ultimately get the kind of intelligence system it, as expressed through its presidents, wants. With its focus on the relationships between presidents and their intelligence tools, Andrew's study barely touches on the relationship between intelligence and the Congress. This may be the book's greatest flaw, for at some point American intelligence becomes less than fully the prop-

erty of the President and more of a resource shared by and controlled by the legislative and executive branches. And the focus of this study could not encompass this shift. Andrew has examined whether intelligence can function legally and ethically in a constitutional democracy; for the most part, he believes it has done so. How it functions in a democracy where the president's eyes are not the only ones that count is an important issue future historians will need to address.

(U) That said, this is a remarkable and provocative study, one that raises a host of interesting question its author should attempt to answer in subsequent works. Any author who concludes, for example, that "The key to the main U.S. intelligence failures and successes is to be found as frequently in the Oval Office as in the performance of the intelligence agencies" would be well advised to consider that a theme for exploration. *Blurred Visions* would make a wonderful title, with chapters on "For Myopic Eyes Only" (the Bay of Pigs), "In the Eyes of the Beholder" (the Soviet brigade in Cuba), and "Tunnel Vision" (Vietnam, of course, though "End of the Tunnel Vision" would be more precise).

(U) Larger issues aside, the book contains wonderful tidbits. That Yardley found Wilson a cryptologic naif fits into the larger context of this president's career. Andrew's discussion of the Pearl Harbor conspiracy theorists should be yet another decisive step in putting paid to that silly business, though, virtually by definition, conspiracy theories cannot be laid to rest. He treats Roberta Wohlstetter's groundbreaking analytic device of "signals" versus "noise" in evaluating intelligence failure with appropriate deference, while noting that it hardly fits the event she was reviewing (Pearl Harbor), but would do nicely for an explanation of the failure to warn of the Tet offensive.

(U) Revisionist historians of the 1970s and thereafter will find Andrew's dispassionate, reasoned analysis of the "Red Scare" of the 1940s and 1950s disquieting. Yes, Joseph McCarthy and others exploited the issue, and Andrew raises the frightening prospects of the damage McCarthy could have done with all the facts at his disposal. There was, however, an active—aggressively so—Soviet espionage effort in the 1940s, and the familiar cast of characters who themselves or through their defenders have protested their innocence may have to face the reality revealed in the records of Soviet and American archives. In the end, Alger Hiss dressed better and had better teeth (and now has at least one endowed chair named in his honor at an American college), but Whittaker Chambers told the truth.

(U) One discussion that should be read thoroughly by those entrusted with designing the SIGINT system of the future is that of the period between 1945 and the creation of NSA. If two cryptologic agencies were sufficient to muddle the situation in December 1941, we required four to accomplish an equivalent mess in 1950, with the invasion of Korea. Without being didactic about it, Andrew is clear in suggesting that intelligence is not an activity that can, especially in an age of instant communication, tolerate lack of coordination and purpose.

(U) The merits of this study make some of its errors of fact and judgment all the more annoying. By common consent, SIGINT is used in back-formation to cover activities that took place when COMINT is actually the more appropriate term, but to extend the term to Civil War codebreaking is a bit much. It may be understandable that a British subject would think Congressional Country Club is in Virginia, but why should a credible author (British yet!) use Bletchley Park not only as a place of World War II cryptologic operations but as the name of the British cryptologic agency of the time? His stating as a fact that the National Intelligence Council has moved from CIA Headquarters reflects his access to a document that addressed the intent to make that change, but not later documents that would inform him it never happened.

(U) Early in the book, Andrew notes George Washington's injunction that intelligence is necessary and must remain secret. Juxtaposed to that is Andrew's obvious and professional desire to lift the veil of secrecy. "When NSA files for the Cold-War period finally become available some time during the twenty-first century," he concludes, "they are certain to generate thousands of doctoral dissertations and some interesting reassessments of American foreign policy."

(U) Clearly, there are those who will be uncomfortable with what Andrew has revealed in this volume. Some very interesting codewords, along with discussions of sources and successes, fill the book's discussion of SIGINT support to recent American presidents. Is it possible there may be a cost to such disclosures?

(U) Possible. But cost analysis alone proves nothing. The overall impression of SIGINT readers are likely to derive from this book is clear and simple: for

every president since Franklin Roosevelt, SIGINT has been an instrumental source of information. It is a core capability of the intelligence component of the national security apparatus. On a cost/benefit basis, especially at a time of fundamental national review of intelligence and security issues, an intelligent, balanced study by a fair-minded scholar like Professor Andrew emerges as a positive and timely contribution to public discussion of an important issue.

Chinese Intelligence Operations.

by Nicholas Eftimiades. Naval Institute Press, 1994.

Reviewed by [redacted] P.L. 86-36

(U) This book is an unusually valuable contribution to the literature on Chinese politics and Chinese intelligence operations. It stands apart from most of the scarce literature on the same topic. Drawing on his expertise as a counterintelligence analyst and longtime study of Chinese affairs, Eftimiades clearly reveals the structure, objectives, and methodology of Chinese intelligence operations, and how they fit into the conduct of Chinese internal affairs and foreign policy. The goal of this book, as the author states in his introduction, is to identify China's national intelligence structure, objectives, and collection operations, focusing primarily on human-source intelligence (HUMINT) operations. This book also provides some basic information about China's analytic community by identifying the roles and organization of major departments and agencies.

(U) In order to achieve his goal, Eftimiades divides his book into four major parts. It begins with an introduction, focusing on China's use of intelligence, the framework for analysis, and China's information objectives. Part Two basically addresses the structure and domestic and foreign operations of the Ministry of State Security (MSS). Part Three discusses China's intelligence community, mainly providing information about the Military Intelligence Department (MID) of the People's Liberation Army's (PLA) General Staff Department (GSD), and China's secondary intelligence organizations, such as the General Political Department (GPD), and the New China News Agency. Part Four is the conclusion, summing up the author's observation about the current capability and overall efficiency of China's intelligence services, and providing his views on the prospects of its future threat against the West.

(U) In theory and practice all intelligence activities, whether open or clandestine, are directed at either satisfying information requirements or covertly advancing national objectives. In this regard, Eftimiades is correct in believing the information objectives of the Chinese leadership differ significantly from those of global powers because of its unique strategic political and military concerns. In military terms the People's Republic of China (PRC) is strictly a regional power. For military intelligence purposes, the PRC directs its resources toward identifying potential regional threats: the Commonwealth of Independent States, India, Vietnam, Muslim states north of Xinjiang, the United States, Japan, South Korea, and Taiwan. Eftimiades also believes that the PRC has less of an interest in the global political-military environment than nations with worldwide military commitments. Accordingly, the PRC continues to focus its intelligence collection activities on issues that more directly affect its internal stability, regional security, and technological and economic development. However, since the fall of 1989 and as a result of global condemnation of China's Tiananmen massacre, Chinese intelligence apparatus have begun to focus on the specific strengths and weaknesses of the United States, targeting what the Chinese leadership perceive as the United States' "campaign of peaceful evolution." Consequently, the new information objectives target the positions on US-China relations advocated by American institutions such as executive branch agencies and members of Congress. And, overall, Chinese intelligence activities support its policy interests by acquiring dual-use foreign high technology, identifying and influencing foreign policy trends, such as bilateral policy and trade issues, and monitoring dissident

Chinese intelligence activities support its policy interests by acquiring dual-use foreign high technology, identifying and influencing foreign policy trends, such as bilateral policy and trade issues, and monitoring dissident groups, especially those advocating democracy and Taiwan independence

groups, especially those that advocate democracy and Taiwan independence.

(U) It is logical that this book devotes much of its attention on the MSS and the MID, and to a lesser extent on the so-called secondary intelligence organizations, since Eftimiades' study restricts itself only to Chinese HUMINT efforts. The MSS is China's preeminent civilian HUMINT collection agency; and the MID, which is also know as the Second Department of the GSD, is China's second largest organization involved in HUMINT collection. It is in its careful and relatively detailed coverage and discussion of these organizations' structure, foreign and domestic operations in Parts Two and Three that this book makes major contribution to the understanding of China's HUMINT operations. The information on China's agent recruitment methods, training, and deployment is fresh and unique, and should be particularly useful to the counterintelligence specialists and interesting to all intelligence analysts in the China field. Much of this valuable information was derived from well-planned interviews with "Source no. 1" and "Source no. 2," and its worth betrays the significance of interviews, if conducted carefully, as a useful tool for extracting unique and hard-to-get information.

(U) Eftimiades has succeeded in achieving his goal for this book. By putting his information in the context of Chinese history and practice of espionage, and current information requirements in support of state policy, Eftimiades has provided a comprehensive picture of both the constancy and changes in China's intelligence services and operations. His book enhances his professional readers' understanding of the topic and sensitizes their appreciation of the present and future challenge posed by the Chinese intelligence services. Apart from his knowledge gained from many years of careful studying and observing China, Eftimiades' expertise as a counterintelligence analyst has enabled him to gain valuable information from various old and new sources, including interviews with Chinese diplomats, military and civilian intelligence officers, and secret agents. While he faithfully sticks to the framework and the goal he sets for this book, he does not let himself bogged down by excessive and often cut-and dry discussions of the structure of Chinese intelligence organizations. And, throughout his book, Eftimiades is mindful of the fact that the structure, operations, and methodologies of Chinese intelligence services reflect current intelligence requirements levied by the Chinese Communist Party and its leadership, and that they would change in accordance with new requirements.

In spite of their inefficiency, China's intelligence services will become more sophisticated in the future and will be unaffected by Western intelligence and security practices

[redacted]

EO 1.4.(c)
P.L. 86-36

Kλ

DOCID: 4012045

P.L. 86-36

SIGINT Glossary

More Communications Analysis Trivia: The Chun Wheel

P.L. 86-36
EO 1.4.(c)

by

Thanks to the Center for Cryptologic History for permission to reprint this selection from the Cryptologic Almanac

(U) Many analysts at NSA have fond memories of the Chun Wheel (and Chun Board), and the Center for Cryptologic History would like to hear your Chun story. Send your recollections about the Wheel's origins or use to **dahatch@e3.e.nsa.**

Kλ

P.L. 86-36

Editorial Policy:

(U) Technical articles are preferred over non-technical; classified over unclassified, shorter over longer., Emphasis should be on improving NSA's technical performance; articles should be aimed at explaining one's discipline to those outside it. Readers are also invited to contribute conference reports and reviews of books, articles, software, and hardware that pertain to our missions or to any of our disciplines. Humor is welcome, too. Submissions may be published anonymously, but the identity of the author must be known to the editor.

Submitting Items

(N.B. If the following instructions are a mystery to you and your local ADP support is no help, please feel free to call the CRYPTOLOG editor on 963-3123s.)

(FOUO) Send a hard copy accompanied by a labelled diskette to the editor at P054 in 2E062, Ops. 1, or send a soft copy via e-mail to [redacted] or **cryplog@p.nsa** P.L. 86-36

Guidance

For maximum efficiency (as far as possible within the limits of your word processor):

- Do not type your article in capital letters.
- Classify all paragraphs.
- Label all diskettes, identifying hardware (operating system: DOS, UNIX), density and type of word processor used ; also your name, organization, building and phone number.
- FrameMaker format is preferred; ASCII is also fine. J334 has a conversion service that converts Interleaf, Word Perfect, OfficeWriter and MS Word into FrameMaker. Just attach the document to an E-Mail Compose Window addressed to **convert@po**.

DOCID: 4019609

~~TOP SECRET~~

NATIONAL SECURITY AGENCY

CRYPTOLOG

The Journal of Technical Health

1995

VOL. XXI NO. 1

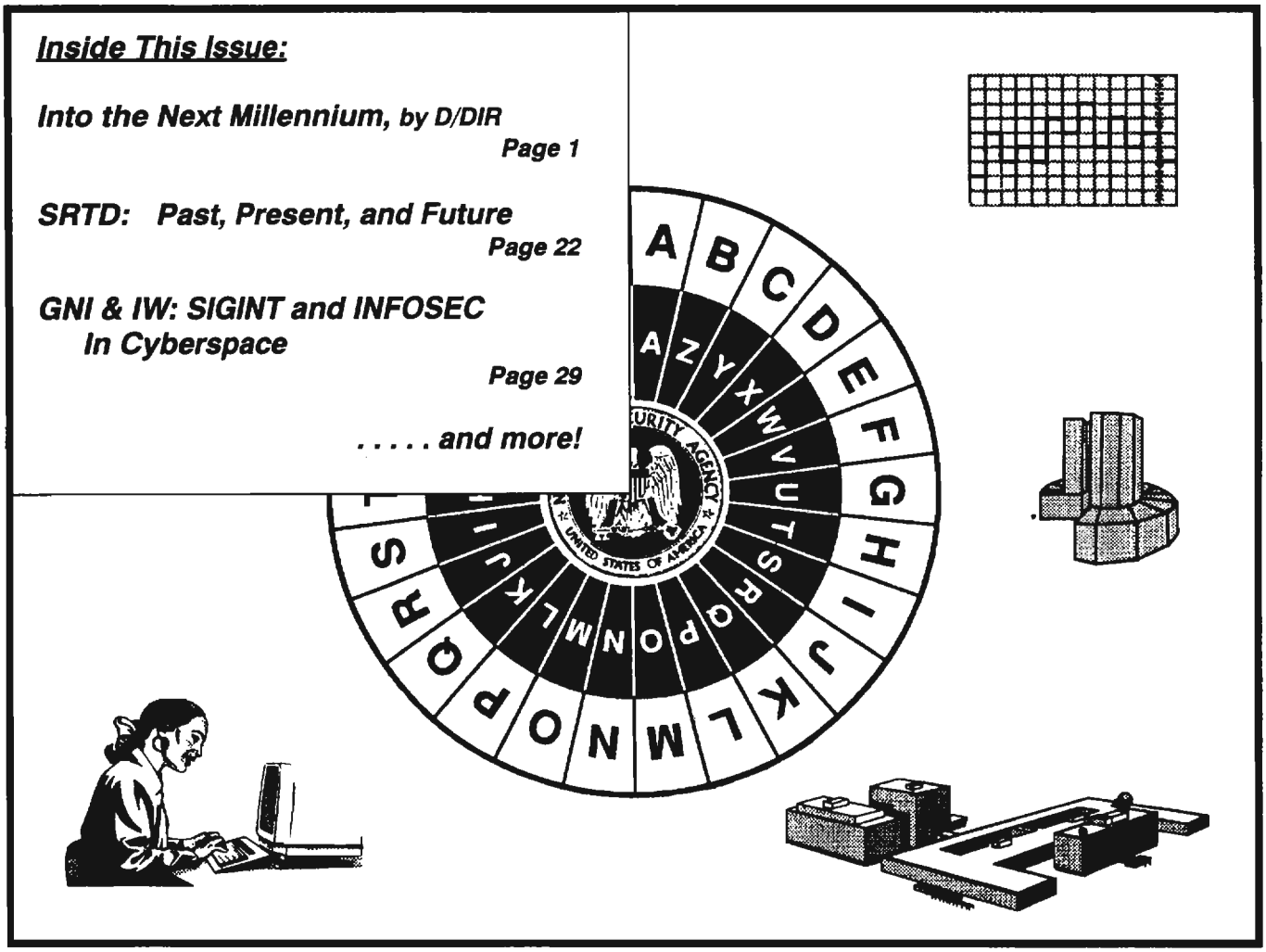
Inside This Issue:

***Into the Next Millennium,* by D/DIR**
Page 1

SRTD: Past, Present, and Future
Page 22

GNI & IW: SIGINT and INFOSEC In Cyberspace
Page 29

. . . . . and more!



~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-10-2012 pursuant to E.O. 13526, MDR Case # 54778

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

CRYPTOLOG

Vol. XXI / No. 1

Published by P05, Operations Directorate Intelligence Staff

Publisher ..... William Nolte (963-3123)

Editor ..... [redacted] (963-3123)

Board of Advisors

Chairman ..... [redacted] (963-7712)
Computer Systems ..... [redacted] (963-6669)
Cryptanalysis ..... [redacted] (963-7243)
Intelligence Analysis ..... [redacted] (963-8211)
Language ..... [redacted] (963-5704)
Mathematics ..... [redacted] (963-1363)
Signals Collection ..... [redacted] (963-5717)
Telecommunications ..... [redacted] (996-7847)
Member at Large ..... [redacted] (968-4010)
Member at Large ..... [redacted] (968-4010)
Member at Large ..... [redacted] (961-8214)
Classification Officer ..... [redacted] (963-5463)

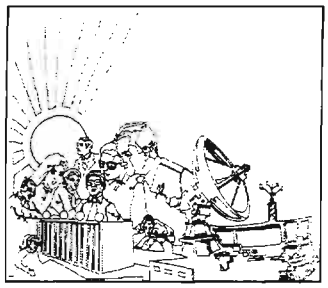
P.L. 86-36

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

To submit articles and letters, please see last page

Table of Contents



Publisher's Welcome ..... *iii*

Information Technology:
Into the Next Millennium, by William P. Crowell, Deputy Director *1*

Signals Collection Career Panel Update:
A Look at Some Goals, by Ken Williams, B46 ..... *4*

Signals Analysis: A Cornerstone for the Future, by [redacted] *E43* *6*

Mathematics: Reaching Out in Space and Time, by [redacted] *Z31* *8*

Cryptanalysis Conference, 1994, by [redacted] *Z211, CACP Chairman* *10*

Linguists and a Changing Future, by [redacted] *LCP* *15*

Intelligence Research + Traffic Analysis =
Intelligence Analysis, by [redacted] *IACP* *17*

Production and Reporting in a Changed Environment, by Bill Nolte, P054 ..... *18*

Signals Research and Target Development:
Past, Present, and Future, by [redacted] *P054, TARS* *22*

The Telecommunications Professional
of The Future, by [redacted] *former Technical Director for Q* *27*

Global Network Intelligence and Information Warfare:
SIGINT and INFOSEC in Cyberspace, by [redacted] *former chief G4* *29*

P.L. 86-36

DOCID: 4019609

Welcome

On behalf of the chairman and members of Board of Advisors, welcome to this very special issue of *Cryptolog*. For over twenty years, long before the phrase "technical health" came into fashion, *Cryptolog* has promoted excellence and dialogue among NSA's professional work force.

Within that tradition, and at a time when the Agency and the Intelligence Community are facing fundamental review and revision, it is appropriate that *Cryptolog* should sponsor a survey of the cryptologic disciplines. We are appreciative of the work of the career panels whose fields are represented here for their assistance in the planning and preparation of this issue. We are especially honored to have the Deputy Director, Mr. William Crowell, as our keynote author.

In presenting itself to the various external groups studying the future of American intelligence, as well as in its own internal studies, NSA has consistently held to a fundamental principle: that cryptology is a process dependent on success across a range of individual skills and capabilities. It is the integration of those skills and our ability to communicate across disciplinary lines that has allowed that process to perform successfully over the last forty years. Our success in the next century will require no less.

Cryptolog has a new look, a new and active advisory board, and a renewed mission. Ultimately, however, its success depends upon the willingness of NSA's talented, multidisciplinary work force to continue and advance the dialogue of techincial health and technical excellence. We invite your participation.

Information Technology: Into the Next Millennium

by William P. Crowell, Deputy Director

(U) Not long ago while driving to work I saw a bumper sticker that really caught my eye. It said: "The Universe is Subject to Change at Any Time. . . And It's Right on Schedule."

~~(FOUO)~~ I think this really describes the universe in which we are living and will experience right into the next millennium. Most of us expect to see continuing rapid changes in technology, but with this rapid technology change come many other social and organizational changes as well. We can expect:

- Increasing pressures for organizations to respond to technology by decreasing cycle times for new products and new services;
- Increasing challenges to the Government's monopoly in areas of specialized information services, e.g. information on economic performance, personal information, and related services . . . AND intelligence . . . AND information-security services.
- Increasing opportunities for us to use technology to allow us to cope with these challenges and pressures, e.g., the use of information technologies and communications connectivity to achieve increased teamwork and knowledge-sharing.

~~(FOUO)~~ The key question for NSA is whether we will take advantage of new technology to help us advance our mission, or will we instead be whipsawed by new technology, be slow to respond, and merely be reactive to new developments that affect our business?

~~(FOUO)~~ In a 1978 CRYPTOLOG article, I argued that we were moving too slowly in responding to the opportunities posed by personal computers that were just then coming into widespread use. In my mind, PCs represented a potential major improvement to the SIGINT analysis process that would allow NSA analysts to move beyond the paper-and-pencil approach we had been using for 30 years. However, our computer acquisition efforts in 1978 focused on buying more of the large-scale computers we had bought in previous years. While these machines were necessary, it seemed to me that we needed to invest as well in small computers that would support analysts more directly and give them personal contact with their data. My observation at the time was: "This is one case where the bureaucratic process has developed a life cycle that far exceeds the cycle of development of new systems and capabilities and costs outside NSA."

~~(FOUO)~~ Where are we now? Well, I think everyone would agree that we have done a lot to improve the technology supporting our analysts. At the same time, technology has continued to advance, our budget has declined, and the world has changed dramatically. The real changes in technology—size, speed, connectivity, together with declining cost—are having a profound effect on NSA's overall mission. In many respects, we find ourselves now, in SIGINT as well as in INFOSEC, in a situation I would describe as hanging on by our fingernails. We're making good progress in many areas, but as the technology explosion continues, we need to move faster to keep pace. In terms of keeping ahead of the technology curve we're not much better off than we were in 1978.

~~(FOUO)~~ A quick review of breakthrough technologies that will affect our targets and our business between now and 2000 provides a sobering view of the challenges ahead. The sheer numbers of people with computers will drive increasingly rapid technology change. Quick and

cheap access to information technology will mean that more of our targets will be converting to computer-to-computer communications. This is in addition to the use of facsimile, e-mail, and voice mail, all of which are already widespread. Multimedia will become a real challenge. The vision of the telecommunications industry—to enable people anywhere, anytime to exchange information simply, reliably, cheaply, and securely over their medium of choice—represents a true challenge to SIGINT in the future.

~~(FOUO)~~ The most startling changes, however, will be in size, speed, connectivity, storage technology, and cost. Size will drive the continuing development of personal computing devices: laptops, personal data assistants, and smart appliances such as digital recorders. Communications and connectivity (networking) improvements will make these devices more acceptable for real work. We will see more telecommuting, greater use of Mosaic-like browser capabilities on the Internet, and a much more complex set of technologies in use by target military forces. Increases in processing speed will allow for continuing performance improvements. Graphics interfaces will be more responsive, and today's relatively poorly-performing algorithms, such as those used for speech recognition, will be greatly improved. Storage technology injects an interesting uncertainty into technology projections for the future. It's very clear that the industry will achieve tens to hundreds of gigabytes at very low cost in the next 5 years. It is not exactly clear how these technologies will fit into the overall architecture of an increasingly networked world. (I can think of several NSA applications, however!) Finally, decreasing costs will fuel the whole cycle of change, promoting ever greater speed of change as the favorable economics of using new technology will push old technology out of the way.

~~(FOUO)~~ I believe the impact of these changes on NSA can be categorized in four interrelated areas:

➢ *Accumulation and availability of information.* This is the problem of data overload. There is much more information available now than ever before. We need to continue to improve our methods of accessing and storing this information in ways that are easily manageable and analyst-friendly. This also means that we may have to discard some of our traditional methods of storing data in the interests of improving efficiency and laying the groundwork for more rapid advances. We may also have to abandon some of our traditional approaches to collecting data, since it does not make sense to continue to collect data we don't or cannot use.

➢ *Organization and structure of work.* New demands for functional and horizontal relationships place strains on NSA's traditional organizational structure. I am not advocating another reorganization. I am saying that we need to build in much more flexibility into the way we approach things. The old boundaries between SIGINT and INFOSEC, between communications as a target and communications as part of our infrastructure, and between cryptologic disciplines, are rapidly disappearing.

➢ *Facilitation of teamwork in developing new skills.* We all know how successful NSA is in responding to crises. Bureaucratic walls collapse, procedural obstacles evaporate, and people pull together to provide unequaled support to policymakers and military commanders. We need to institutionalize this kind of teamwork during non-crisis periods, too. More than that, we need to encourage more cross-training among cryptologic disciplines. We need to provide mathematicians and intelligence analysts training in telecommunications and networking, for example, and we need to develop multi-disciplined signals collection officers who understand modern networks as well as the more traditional forms of communications still employed by some of our targets. We've done some of this already, but we need to do more.

➢ *Developing a focus on results based on value-added information and processes.* The demands of the Information Age mean that NSA must determine how to provide information to our customers that is more valuable than that they can get from CNN. That is, we have to use SIGINT analytic insights and judgments to enhance and explain information that may be widely available through open sources. We must produce core secrets, information not available in open sources, e.g., plans and intentions. We have to be decisive. We have to take risks, stick our necks out, and provide to our customers interpretations that reflect our corporate knowledge and expertise in a way that is meaningful to them and meets their information needs.

~~(FOUO)~~ The articles in this issue of CRYPTOLOG address most of these areas. They also acknowledge a critical fact: that the real impact of technological change is in human terms. That is, how NSA professionals will take advantage of new technology to understand and cope with that

technology as it applies to their SIGINT and INFOSEC missions. The articles contain several important common themes: the need for change; the importance of continual training; and the growing need for cross-organizational teaming.

P.L. 86-36

~~(C CCO)~~ I'm pleased to note the discussion in these articles of many important efforts already underway. The reengineering of the Cryptanalysis Career Field, for example, described by [redacted] and [redacted] is very encouraging. Recognizing the problems caused by the reduction in Agency hiring at [redacted] Its new focus acknowledges the need for multiple skills, provides for multidisciplinary training, and encourages interaction between specialists in subdisciplines like mathematics, engineering, and analysis. New professionalization criteria are being developed as part of this process. Striking a similar note, Bill Nolte compares modern cryptology to the medical profession in which all the participants are critical to a successful outcome.

EO 1.4.(c)
P.L. 86-36

~~(FOUO)~~ The overall impression left after reading these articles is that NSA professionals are working hard to figure out ways to deal with the many technological challenges we're facing. Typical of the optimistic and can-do attitude that has characterized NSA for years, our workforce is taking on these new challenges, too. The challenges are difficult, but people are clearly not discouraged and are developing new and creative approaches to the problems at hand.

~~(FOUO)~~ To me this means three things:

- We need to pursue the improvement of internal NSA core processes. We have begun to address this area in the process-improvement activities now underway. Teams have been established to identify root problems and recommend future courses of action for both SIGINT and INFOSEC. Clearly, we have to focus on the insights these teams develop and respond with improvements that will allow the Agency to be more streamlined and flexible in the future.

- We need to encourage cross-organizational and cross-disciplinary teamwork. We all recognize the benefits of such collaboration and can point to many examples where such teamwork has paid off. We need to examine the reasons why such teaming does not occur routinely, and then make changes as necessary to ensure teaming becomes a routine and accepted business process at NSA.

- We need to reduce bureaucracy so we can more rapidly take advantage of new information technologies to improve our SIGINT and INFOSEC missions. In today's climate of continuing technological advancements, we must find ways to reduce cycle times or risk becoming irrelevant.

~~(FOUO)~~ All these improvements are well within our grasp. We can enhance the organizational and institutional processes for SIGINT and INFOSEC and thus allow our workforce to take advantage of new information technology to do their jobs better. We can overcome traditional resistance to teamwork and optimize the synergistic efforts of the entire workforce. And we can institutionalize technological flexibility to ensure we continue to evolve with new technologies, in both a mission sense and a support sense. We can and we must do these things to keep up with the pace of change. Perhaps our vision ought to be: "The Universe is Subject to Change at Any Time . . . And It's Right on Schedule."

Kλ

Signals Collection Career Panel Update: A Look at Some Goals

EO 1.4.(c)
P.L. 86-36

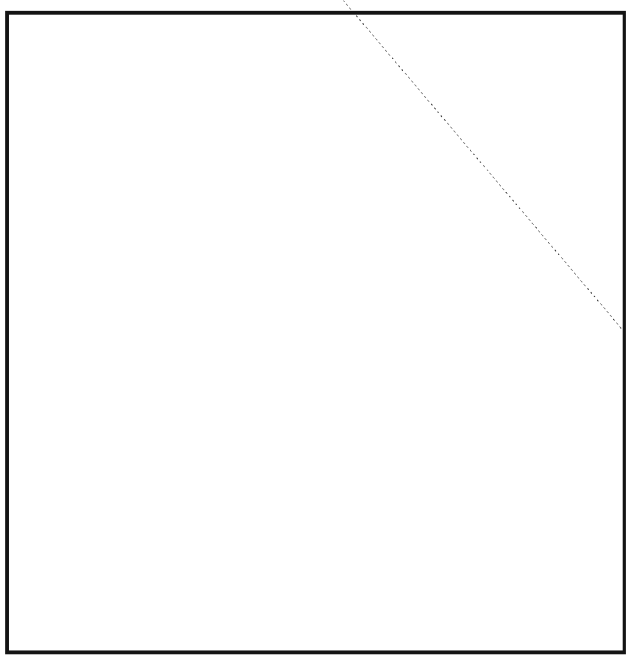
by Ken Williams, B46

~~(C)~~ The Signals Collection Career Panel (SCCP) is taking a hard look at its future and evaluating the viability of the career field as we presently know it.

(C) Although the study is still in progress and the final recommendations are not completed, we do believe that the efforts to affect positive changes over the past decade or two have been more reactionary than planned

DOCID: 4019609
P.L. 86-36
EO 1.4.(c)

and at best have only been cosmetic in attempting to make distinctions between hands-on collection and collection management. Although always a tool of the collector, the realities of personnel draw-downs may force the latter function to be subsumed by the Intelligence Analysis discipline—particularly if the Analyst-Driven System comes to fruition.



~~(C)~~ Whatever is the ultimate solution, greater cooperation and effort must be achieved in joint sponsorship of this program among all concerned parties whether they be a career panel, producers or consumers. The only way to achieve technical excellence—to improve the technical ability and leadership of the individual and to ensure the technical health of the organization—is to form a partnership between management and the technical support infrastructure. The developers must be sensitive to the requirements of the target analysts and management must demonstrate its vested interest in the technical workforce by maintaining positions, providing training, and rewarding achievements.

~~(C)~~ The SCCP has had an extensive partnership with the National Cryptologic School and has supported E4's efforts to develop, upgrade and expand its Signals Collection curriculum. A representative of E4 sits as a full member of the panel and, along with the panel execs, has helped to support a very outstanding advanced technical training program—to include the very latest in computer based training techniques.

~~(C)~~ Among other efforts, the SCCP will be working directly with the DO THAB to expand its Advanced Collection Officer Development Program (ACODP) to satisfy the newly established requirements of the Agency's Technical Development Program (TDP). *Some proposed improvements include the resurrection of the Signals Collection Intern Program, the expansion in advanced collection training, identifying more Titled Tech Track positions, developmental job assignments, cross-discipline team projects, technical conferences, one-on-one mentoring/tutorials with senior technical experts, etc.*

~~(C)~~ As you can see, the SCCP is committed to improving and maximizing the Agency's overall technical health through new and improved approaches and programs. It will also strive to ensure that the technical workforce is properly trained, motivated and challenged and that continued development and performance in the technical track be properly recognized and rewarded—to include incentive pay for those hands-on collectors. We must never lose sight of the fact that without collection, this Agency cannot produce SIGINT. We must nurture this critical skill field and those in it. The SCCP will keep all concerned apprised of our progress.

Kλ

Cryptology will only be effective if it stays close to the evolving new problems and opportunities. Cryptologists are going to have to be actively involved with collection,

we must develop mechanisms for bringing teams together across organizational boundaries and identifying the leaders who will be able to coordinate the talents of a team. We also need to control the parochialism which is rampant at NSA and which often stifles or prevents communication across organizational boundaries. A solution to this problem will require a major change in NSA's managerial mindset.

— Recommendation of the Deputy Director's Cryptology Futures Study

EO 1.4.(c)
P.L. 86-36

DOCID: 4019609

CRYPTOLOG
Issue 1 1995

P.L. 86-36

Signals Analysis: A Cornerstone for the Future

EO 1.4.(c)
P.L. 86-36

by [redacted] *E543*

~~(C)~~ In the past, many Signals Analysts have been technicians, trained to perform a sequence of actions to process taped intercepts. However, Signals Analysis is evolving into a cornerstone profession at NSA. The Signals Analysts of the future will be in a position to make significant contributions to the Agency's mission by focusing collection on critical targets, adjusting to the impact from the modern communications technologies, and taking an active role in managing the large volume of data that could be intercepted in the future.

Focusing Collection

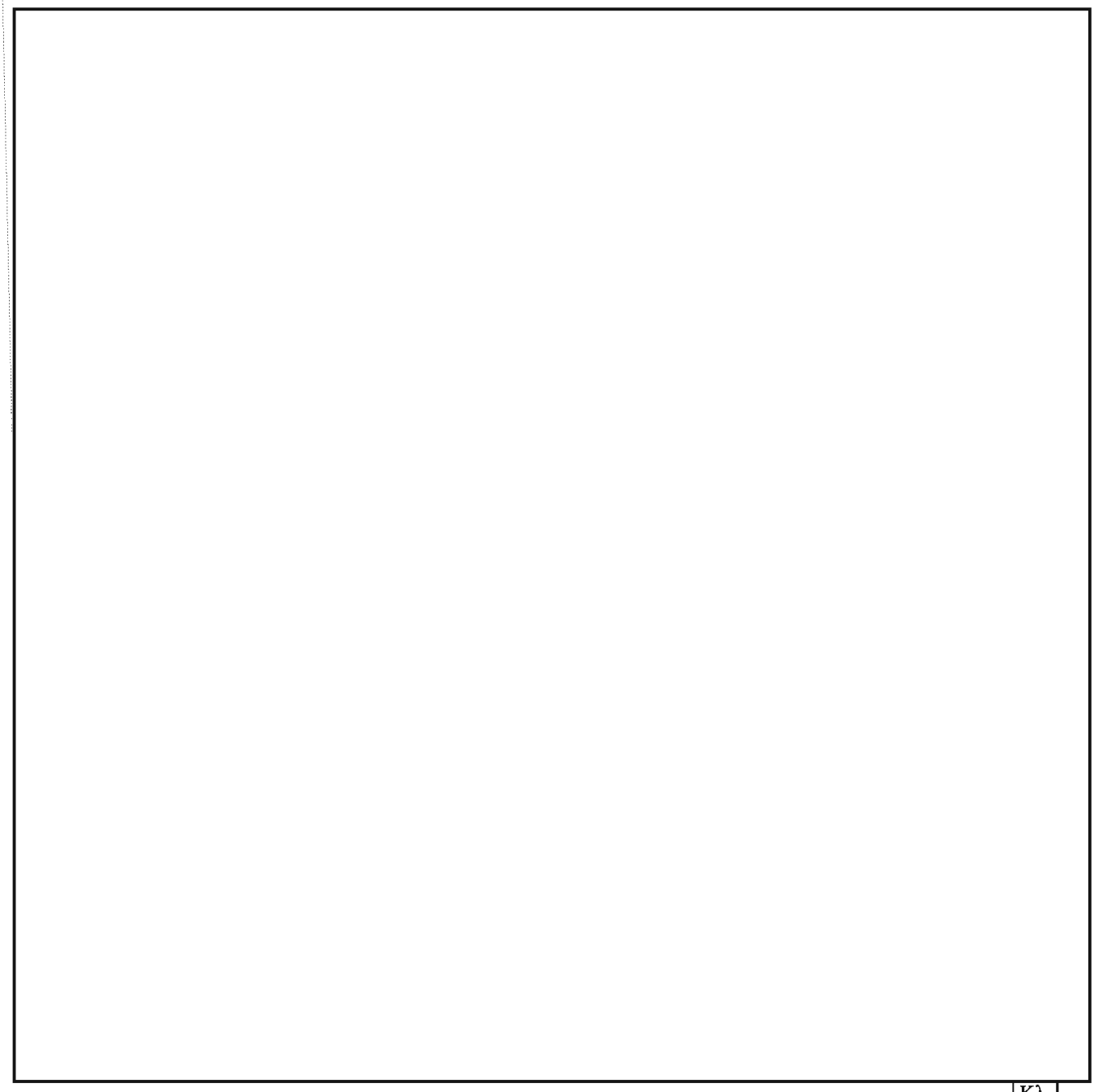
~~(C)~~ ***SIGINT is moving away from a Data-Driven System, and, in the continuing days of doing more with less, Signals Analysts will allocate scarce resources in proportion to the intelligence payoff.*** Future Signals Analysts must take a proactive role to ensure an effective Analyst-Driven System.

[redacted]

[redacted]

[redacted]

DOCID: 4019609
E.O. 1.4.(c)
P.L. 86-36



Kλ

~~TOP SECRET UMBRA~~

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

P.L. 86-36
EO 1.4.(c)

Mathematics: Reaching Out in Space and Time

by [redacted] Z31

~~(C-CCO)~~ Cryptologic mathematics is both a mature discipline, solving incredibly hard Agency problems every day, and simultaneously a youthful, uncertain beginner facing a new world of challenges. The mature capabilities for analysis and design of cryptography, and a host of other mathematical problem-solving functions at NSA, are powerful, success-driven, treasured. Despite the confidence that this success justifies, mathematicians are rapidly learning that they face an unfamiliar, changing world which does not respect many of their assumptions about what mathematicians do, and that they must change with the world—just as every other discipline at NSA is being forced to change.

[redacted]

~~(C-CCO)~~ A second, fundamental aspect of mathematical success is the tool-building that has accompanied classical analysis. The structures involved were modeled and generalized, tools were built which worked on the next problem as well as the last one. An immensely powerful tool-kit has been built up over the years.

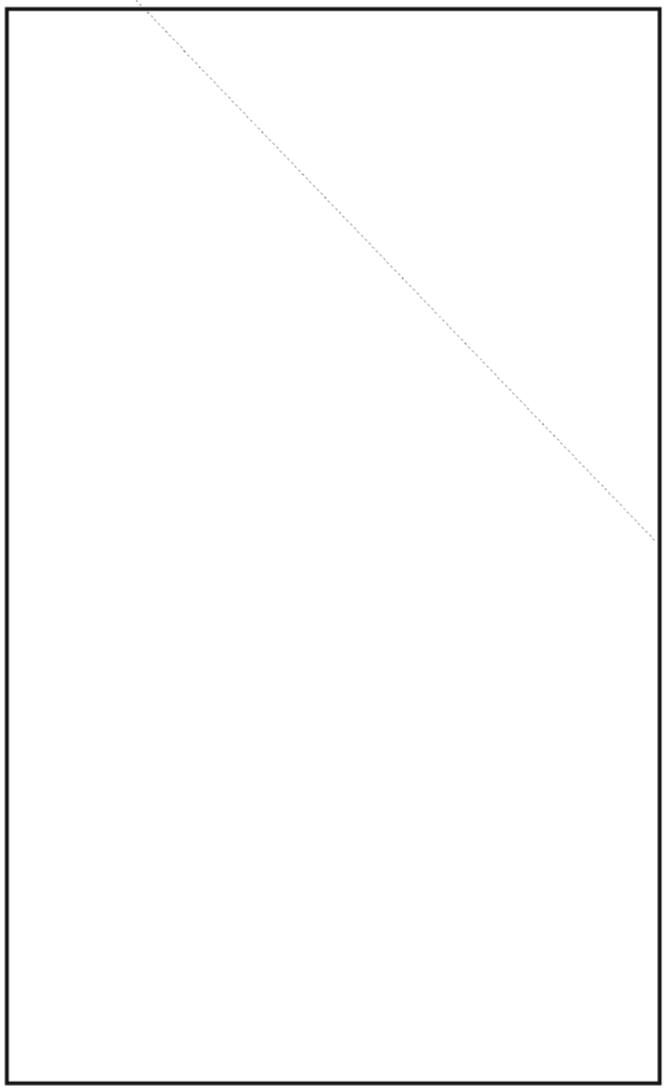
~~(C-CCO)~~ Last, but no less important, success has followed because mathematicians have shared these tools with each other. There has been a very strong sense of community, common training in a relatively stable course of theory and practice, healthy production and wide dissemination of publications, lots of seminars and conferences, reasonable movement among organizations, fresh talent recruited to renew the supply of ideas.

(U) Even so, with all this going for them, mathematicians still find themselves in a world changing too fast for anyone to be complacent.

[redacted]

~~TOP SECRET UMBRA~~

DOCID: 4019609
EO 1.4.(c)
P.L. 86-36



(U) One result of these efforts is an increasing number of mathematicians reaching out to learn from and work with other organizations and disciplines. This trend must not only continue, but expand, to meet the problems we are already seeing. It can only be hoped that management in these related organizations will encourage such contacts, awkward as they may sometimes be under existing boundaries.

~~(S-CCO)~~ Mathematicians are learning where the mathematics is in these new contexts, applying the tools they have, and starting to develop new ones. It is impossible to predict what sorts of advanced mathematical tools will be developed here in the coming years. But the glimpses we have already had of the mathematics needed to address our new challenges clearly indicate that these too will contain and motivate sophisticated, classical mathematical analysis. Depth of research and knowledge in the discipline are proving essential in the new world as well as the old. In fact, the problems and mathematics are just plain getting harder all the time. The combination of this tradition of and need for subject matter depth, with the inspiration of new, hard problems, should generate extremely productive mathematical tool-making.

(U) On the worry side, there is some concern for the health of the mathematical community that has contributed so much to the discipline's success over the years. For one thing, it is not as easy as it once was for a mathematician to move around NSA, spreading and learning new ideas with each new office. Conferences and published papers are not enough: professional development requires extensive work on a variety of problem sets, with a variety of people. For another, diminished hiring diminishes the flow of new ideas and ways of thinking into a field which lives or dies on creativity. Thirdly, it is proving difficult to keep training up to speed with the new material mathematicians are learning or wanting to learn. Mathematicians have generally recognized how much their success depends on the strength of their community. In this stressful time, they must not forget to devote the time and energy needed to keep this community alive and well.

(U) Because of the ferment described above, rather than despite it, mathematics at NSA will prosper in the coming years. It offers powerful tools and well-developed tool-making and tool-wielding experience, no less applicable to tomorrow's problems than today's. But mathematicians also know that they cannot rest on their laurels. And though they have never been off in a corner by themselves, no matter what the stereotype, they realize even more clearly now that they share the same fate as all other disciplines here: work together and succeed, or fall dangerously behind.

(U) *The author wishes to acknowledge a debt to material and themes contained in the 1993 Report of the Deputy Director's Cryptology Futures Study Committee, chaired by* [redacted]

Kλ

P.L. 86-36

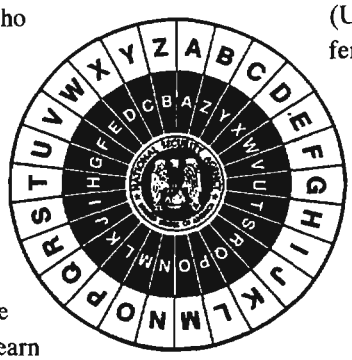
CRYPTANALYSIS CONFERENCE, 1994

by [redacted] *Z211, CACP Chairman*

P.L. 86-36

~~(FOUO)~~ Two critical issues were addressed at the 1994 Cryptanalysis Conference. One was the exciting trend in communications which threatens to reshape our discipline: in what directions are we moving, what problems require our attention, and how have cryptanalysts been successful in analyzing new forms of data? We were fortunate to attract a set of technical speakers who are blazing a trail into this uncharted territory. By sharing with us their experiences, they prepared us for some of the challenges which lie ahead. We also heard overviews from [redacted] who were among the first to envision the revolution which is now upon us.

(U) The other critical issue deals less with the acquisition of individual skills than with the identity of Cryptanalysis as a community. Each of us recognizes that our career field is undergoing rapid transition, and that we must be willing to confront new problems and learn new skills. None of us came to the Agency with academic training in cryptanalysis, so we all have willingly travelled this path before.



~~(FOUO)~~ When we first acquired our cryptanalytic skills, we were regarded as the wizards of the Agency, treated with respect for having accepted a lifework which demands great creativity and offers rewards only seldom. Where do we stand today? Stung by the Agency's unwillingness to hire into our profession, many of us are asking what we should do to revitalize our career field, to restore the place of honor it once deserved.

(U) The Career Panel selected about 70 cryptanalysts to provide advice on these and other issues. We tried to choose many of those whom we expect to be providing our cryptanalytic leadership as we enter the next century. Videotapes of the technical talks are available from the Panel office. The exciting group discussions provided hours of passionate, but always respectful, debate.

(U) The unmistakable conclusions of the conference: cryptanalysts are extremely versatile, willing to adapt themselves to meet any challenge, and they work very well together and with others. Our destinations may be uncertain, and our paths will certainly diverge, but our wills are strong. We will travel many productive miles together.

~~(FOUO)~~ The essay which follows provided only the kickoff for a stimulating two-day conference. Also included here is a report on the popular and pivotal group session organized, and introduced separately, by [redacted] entitled "Reinventing Cryptanalysis." The ideas which arose at that session will form the central theme for this year's Conference, scheduled to be held at SRC, 29-30 March 1995. The functions of cryptanalysis are expanding rapidly, and the Panel is contemplating a very substantial revision of its criteria to encourage the development of the additional skills which will be required to cope with our altered environment.

P.L. 86-36

DOCID: 4019609
P.L. 86-36

Opening Remarks

by [redacted] Z211, CACP Chairman

(U) Good morning, and welcome to the Cryptanalysis Conference, 1994. We are greatly indebted to the Supercomputing Research Center for hosting this conference, as they did last year. Those of us who were here last year are aware of the superb job which the SRC management and staff always do to assure our comfort.

(U) Each of you has been personally selected by the CA Career Panel because we regard you as a key player within our Community. It is a measure of the respect we have for you, individually and collectively, that we have invited you to provide advice, inspiration, and support in our continuing effort to supply the Agency with the best cryptanalysis we can.

(U) These are critical times for Cryptanalysis. Recently organized into a centralized homogeneous Group, we find ourselves enmeshed in the swirling eddies of upheaval, as our sphere of action undergoes unparalleled transition. The cryptanalyst whose methods are limited to colored pencils and "Military Cryptanalytics" is no longer able to contribute effectively to solutions of Agency problems. Each of us needs to be familiar with the capabilities of contemporary computers and must be able to assess both quickly and accurately the speed and the memory requirements of potentially useful cryptographic algorithms.

The single most critical issue which confronts Cryptanalysis today is the lack of hiring.

~~(C)~~ The explosion in computer technology has drawn worldwide attention to the need for security in the transmission of data, with the result that cryptology has outpaced cryptanalysis. The difficulty of our problems has grown much faster than our ability to reduce the resulting cipher to plain text. There was a time, not so long ago, when communications security might well have been sacrificed or compromised in the interest of speed or accuracy, but today our targets can enjoy both security and convenience, with a wide choice of implementations from which to choose.

(U) Cryptanalysts justifiably take great pride in their flexibility. Uniquely among Agency professionals, cryptanalysts have acquired skills which do not come merely from textbooks and are not the subject of university courses. No other professionals could face the impending unrest in their discipline with the confidence we have that we can invent or acquire the new methods necessary to solve important Agency problems.

[redacted]

(U) Each of us has learned a valuable lesson from that experience. Versatility is essential; variety of exposure must be encouraged. Cryptanalysts and mathematicians are uniquely privileged with the opportunity we have for Agency job rotation. We must avoid stagnancy and constantly seek to broaden our spectrum of utility.

~~(FOUO)~~ The single most critical issue which confronts Cryptanalysis today is the lack of hiring. Because it is not a university subject, cryptanalysis is not on the "critical skills" list. We have been unable to achieve recognition from upper management that the stock of cryptanalysts, depleted by retirements, needs replenishing. This is a very favorable time to be hiring—because of the difficult economy, excellent candidates are available—but we have been denied a license to hunt. Perhaps our greatest need is an algorithm, inexpensive to implement, which could be used to identify recent college graduates who have the potential to become productive cryptanalysts. Until hiring is restored, cryptanalysts may explain its absence in any of three ways: (1) maybe cryptanalysis is a dying art form, and we are just slow to leave the sinking ship; (2) perhaps our skill levels are regarded as being so high that we are expected to cover for those departed; or (3) the obvious reasonable explanation is that the very able mathematicians whom we have been hiring will drift into cryptanalysis and will perform well enough to fulfill our obligations. This explanation many will find unsatisfying, maybe even dangerous.

~~(FOUO)~~ Inevitably, our position will be contrasted with that of the mathematical community at the Agency. Mathematicians are multiply blessed. They have benefited from a strong hiring posture, now stronger qualita-

DOCID: 4019609

tively than ever, and their support systems, starting with their immensely successful Cryptologic Mathematician Program, have been the envy of all other career fields. Central to their success has been the magnificent support supplied by the Institute for Defense Analyses.

~~(C)~~ The trend toward the use of mathematical principles in the design of sophisticated cryptologic devices has conferred a substantial advantage upon the mathematically trained cryptanalyst. Those of us who lack such a background have good reason to admire the successes that our mathematically trained colleagues have enjoyed. But admiration can be accompanied by frustration. As our mathematical arm grows strong, must our non-mathematical component wither? This is an issue which deserves an honest assessment.

~~(C)~~ The good news for those of us who lack a strong mathematical capability is that cryptanalysis is expanding in another direction. There are explosive changes in communications which will have aimpact heavily upon both the science and the art of cryptanalysis. Much more of our resources will need to be devoted to preparing new intercept for cryptanalysis. We have far too few people who are facile at this task, and it is one which requires substantial ingenuity. Cryptanalysts should be ideally suited to function successfully in this newly developing area. They know best what form the analyst needs data to take, and they know exactly what information must not be overlooked. I see no mathematical component in this new technology. The keynote talks by [redacted] and [redacted] and today's seven technical talks have been selected to show how classically trained cryptanalysts have solved problems which lie on the border of this new frontier in cryptanalysis. I look forward with great excitement to a glimpse at the future of our discipline. I am convinced that this is not a redeployment of the cryptanalytic workforce, but is a genuine broadening of our field as cryptographic usage changes to include high-speed devices. It is clear that there are big victories to be won, and we must be quick to seize our opportunities.

While hiring may be largely beyond our control, training should not be. If we need exposure to new cryptologic ideas, and we certainly do, we'll need to do it ourselves.

~~(FOUO)~~ Closely allied to the infusion of these new ideas from telecommunications is the need for dissemination of information at all levels. While hiring may be largely beyond our control, training should not be. The cryptanalytic staff at the National Cryptologic School is woefully under strength, and cannot be expected to expand soon. If we need exposure to new cryptologic ideas, and we certainly do, we'll need to do it ourselves. Perhaps in conjunction with Tech Track, a way must be found to make the development and presentation of unfamiliar material an attractive alternative for that huge majority of us who are typically extremely reluctant to leave our current exciting crypt challenge. This inertia, natural as it is for those of us who love our jobs, has become a Community problem. Most cryppies are unwilling to give talks and write papers. We are just not activists. Tomorrow's workshop on "Sending the Public Service Message" will consider how to reverse this trend.

~~(FOUO)~~ I once thought it would be a good idea to institute a Master's program in Cryptanalysis, leading to something like a "Master of Cryptanalytic Arts" offered by the National Cryptologic School. But more sober reflection led to the conclusion that such a degree would likely be won only by perennial classroom students, which includes very few cryppies. Classical education may well be inappropriate for teaching (and learning) cryptanalysis. We hope to learn a great deal from today's timely presentations; waiting until a slick course could be prepared would place too many of us too far behind. We need solutions for our current inability to spread cryptanalytic knowledge, and one of our working groups tomorrow deals with "The Training Challenge." We cryptanalysts are overwhelmingly introverted. Few of us desire to appear before a classroom, even a classroom of our colleagues. Many of us have sufficient initiative to learn for ourselves what we need to know, but something must be done to provide information to our less experienced coworkers who don't realize their deficiencies, and who could become greatly more productive with timely education.

P.L. 86-36

~~(C)~~ Communication poses problems for us in other ways. It was easier for us to show others the fruits of our labors when we were spread across the Operations Directorate. Now we have allowed our sphere of influence to diminish, with the result that our accomplishments are now made known to a much smaller audience. We need to publicize our triumphs to those who could use our expertise. One of tomorrow's sessions, "Marketing Cryptanalysis," will go into this concern in more detail.

~~(FOUO)~~ There is another negative result of our concentration within a single Group. I am not being immodest when I say that cryppies are smarter than many other Agency communities. A comparison of academic records alone is enough to convince anyone of our intellectual capacity, and each of us has gone far beyond our original academic training. But it is unfortunately unrealistic to expect that we will receive promotions at a deservedly increased rate, since bureaucracy decrees that benefits be spread uniformly across organizations.

~~(C)~~ At last year's conference, a number of problems were discussed dealing with issues of morale. Our management should be extremely proud that few of those problems remain. I would like to identify one problem which I think will eventually cause difficulties for us: that is the plight of those among us who have moved away from a purely technical career to deal with the challenges of management. The number of SCES positions is extremely limited and is unlikely to expand. Within Z Group the problem is extremely acute, because our SCES positions are, or soon will be, occupied by very bright and relatively young leaders who seem unlikely (because of the separation of cryptanalysis from the rest of the workforce, and because of the difficulty that cryptanalysts seem to have in entering higher management) to move from their posts in the near future. Also, most of our Office-level managers have been chosen more for their technical excellence than in recognition of their managerial prowess. In short, I would expect any management-oriented cryppie to be very discouraged by the current prospects. Should we do anything to reverse the rising trend of technocracy?

~~(FOUO)~~ This conference presents to your Career Panel a vital opportunity to hear what issues are important to you, our fellow cryptanalysts. The advice and consent which we get from you in the next two days will guide our actions throughout the year. Last year's conference, though times were certainly tough, revealed the cohesion of our Community, the unity and the spirit that helps us move toward our common goals.

(U) So welcome to the 1994 Cryptanalysis Conference. Each of us will find strangers here—but strangers who share our goals and our burdens. I look forward eagerly to meeting those of you whom I do not know. In these two days, we gather to learn from each other, to share with each other, in the hope that each of us will benefit from what we see and hear, and that we will return to spread our new knowledge throughout the Community.

Reinventing CA: A Brave New World for the Career Field

by [redacted]
CACP/Z21
P.L. 86-36

~~(FOUO)~~ Last year's CA conference had as its central theme the role of the cryptanalyst in the modern, post-Cold War, post-reorg world. If you examine the conference speeches, you can pick out some of the issues which led the CACP to call for a hard look at our discipline. New technologies, austere hiring, an apparent contradiction in what outsiders and insiders considered to be cryptanalysis: these realities seemed to be pushing the classical cryppie into the margins of the cryptanalytic establishment, while the latter appeared to be becoming synonymous with the crypto-math community in the eyes of much of the Agency.

Perhaps not surprisingly, the working group stressed the importance of training in related fields.

~~(C)~~ The 1994 conference organizers worked under the assumption that the "ca vs. CA" distinction which I defined in my speech was a valid one, and the conclusions that the "reinventing ca" working group reached seemed to support the perpetuation of that distinction. (For those for whom this is new, I defined "ca" as what someone professionalized in cryptanalysis is trained to do and "CA" as what Z group does.) In its report, the working group defined CA as "the diagnosis and exploitation of data which is, otherwise, not obviously intelligible." Then it went on to carve out a little niche for the "classical" cryptanalyst in diagnosis and exploitation, simultaneously stressing the importance of training in related fields. This is, perhaps, not surprising. We organizers stacked the conference with talks that showed how classically-trained cryptanalysts could be successful in what we termed "modern" cryptanalysis. We believed then that the way forward was to create a distinct identity for ca that would place it on an equal footing with the other disciplines that were involved in doing CA.

~~(FOUO)~~ It took several months for the conference report to come out, and even longer for the Panel finally to put the report on the agenda for discussion. In the meantime [redacted] began his term as Panel chairman. Dan's first initiative was for the Panel to go to the Office Chiefs and Chief, Z and ask their advice on what the CACP could do better to support the activities of their areas. These interviews were extremely enlightening. Another important thing happened during this period; the CA intern program looked like it was on the chopping block. With no hiring and all those empty billets, there was a distinct possibility that we might have to close down. Here [redacted] came to the rescue, suggesting that Z group might benefit by hiring computer scientists and engineers (these are, with mathematics, the relevant critical skills for CA) and training them through the CA intern program. There is still no hiring, but at least there is a plan.

~~(FOUO)~~ By November it was clear that the Panel could no longer operate without a cogent working philosophy of the nature of cryptanalysis. The Panel had promised the community another conference in January, but as we wrestled with the issues confronting us, that conference seemed ill-timed and more and more irrelevant. At long last, in early December, the CACP held an offsite to synthesize the input we had received from the 1994 Conference, Z-group management, and from studies like the "Future of Cryptology." The conclusion of this day of soul-searching was to me as clicking the ruby slippers must have been to Dorothy: *cryptanalysis is Cryptanalysis*. We always had the power, but we had to find out for ourselves.

~~(FOUO)~~ Simple as the concept is, the implications are far-reaching. Z-group cryptanalysis requires the efforts of people in many sub-disciplines. We, therefore, began to try to fashion a career field that would be as relevant to newly-hired mathematicians, computer scientists and engineers as to those in non-technical fields. In the ensuing months we have constructed new criteria for the field which attempt to ensure that every cryptanalyst will have a thorough grounding in the classical subjects: diagnosis, cryptography, related fields, but will also enable him to contribute in the areas for which his academic training has uniquely prepared him. While last year's conference spotlighted how the classical cryptanalyst could move into areas of new technology, this year's gathering will focus on how to embrace diverse technical backgrounds to strengthen cryptanalysis. The new criteria for professionalization in cryptanalysis are a work in progress, and will be a major topic of the conference. Here is what they look like so far.

~~(C)~~ A number of the requirements will seem familiar on the surface. We will still require three years of creditable experience and we will still require a paper and a program. The omission of the PQE from this list is not accidental; an aspirant's grasp of essential knowledge will be assessed in other ways. We will require work experience in three core areas: exploitation, diagnosis and related fields, communications and collection. We will also require two elective tours, to be negotiated with the Panel execs. As an example, a mathematician might elect tours in attack development or algorithm design; an engineer might choose to do hardware reverse engineering or signals analysis; a computer scientist might work on CAPRI or study computer networks; a non-technical aspirant might delve into book-breaking or bit-stream analysis. We're not attempting to pigeon-hole anyone here—the mathematician could do book-breaking and the anthropology major algorithm design—the point is rather in the explicit inclusion of what was previously considered peripheral into our new vision of the career field.

~~(C)~~ Training requirements will be completely revamped, and this will necessitate a great deal of work in course development. Again, we envision a core of required courses and a wide choice of electives. The core will contain some new courses on which we hope to get started at the Conference: a related fields survey course, a "foundations of CA" course which will survey the most significant cryptographies extant, a new diagnosis course which I like to call "patterns of thinking," and a "topics in math, CS and engineering" course that will highlight the ideas in those fields with the most important implications for cryptanalysis. Some of our present required courses will become electives. Does everyone need to know how to solve a grille transposition? Probably not, just as we don't all need to program digital signals processing (DSP) chips—yet.

(U) The Panel is immensely excited about this new direction for the career field, even if that excitement is tempered with apprehension about the hard work necessary to get this new program off the ground. We hope we can count on your help and your counsel as we take cryptanalysis into the next century.

Kλ

DOCID: 4019609

Linguists and a Changing Future

P.L. 86-36

by [redacted] *Language Career Panel*

~~(S-CCO)~~ We linguists are facing a future about which we know little beyond the fact that our environment is changing. We will need to learn new non-language skills, learn new languages and dialects, and sustain language expertise. How do we meet these challenges? The Agency has focused its resources for the past 30 years on developing professional linguists, and it has succeeded. The Agency language population presently consists of approximately 75% certified linguists, a turn-around of significant proportions in demographics over the past 30 years. The future requires that we focus resources on post-professionalization. The Technical Track Program offers us linguists a way to mobilize and maximize resources to cope with the future. It enables the Language Career Panel, Technical Health Advisory Boards, and other Agency organizations and institutions to identify opportunities, establish requirements, and implement courses of action.

~~(C-CCO)~~ The Language Career Panel Staff conducted a study several months ago of the training profiles of over 350 certified linguists who had joined the Technical Track Program at that time. (At the present time, over 450 linguists have joined the program.) The results were alarming. Since 1990, these participants in the program had spent from one to three percent of their annual working hours in any career-skill training or educational endeavors, as registered in Agency records. The percentage was similar for applicants to the Senior Technical Development Program.

~~(C)~~ Is there a lack of post-professional programs for linguists? While the Directorate of Operations' Senior Language Advisor and the National Cryptologic School have created and funded numerous programs over the years to enhance the skills of certified linguists, it is true that many certified linguists have not applied to these programs because the programs did not coincide with their personal and mission needs. It is also true that training funds are limited and are prioritized to go first toward the training of linguists up to the beginning professional level; thus, post-professional opportunities are limited. Other linguists believed that they did not need to develop their skills except through on-the-job experiences. Still others have developed their skills through personal endeavors outside of the Agency; these endeavors have not been registered in Agency records. Regardless of the reasons, certified linguists have not been pursuing registered post-professional training, educational, and development opportunities, which would conceivably have enhanced their language career-field skills.

~~(TS-CCO)~~ If we do not pursue ways to improve our skills and productivity, we shall find ourselves faced with events and circumstances to which we may not be able to respond. Since the Agency will not be hiring linguists in any large numbers, we shall have to rely on our own talents to meet future challenges. In addition to sustaining language expertise and learning new skills, we could accelerate the development of non-certified linguists through intensive mentoring programs, educational and training seminars, and as members of the Adjunct Faculty. The present population of language aspirants is experiencing difficulty in passing the Professional Qualification Examination. We can assist the Service Cryptologic Elements in enhancing the language proficiency of military linguists beyond Level-2 proficiency to cope with the expected future higher-level communications at the Remote SIGINT Operations Centers and elsewhere. There are presently about 900 USSID-4000 military linguists, 13 of whom are certified and approximately 200 are aspirants for professionalization. We need to forge a partnership with the SCEs to address the future of language work and proficiency. Cross-training programs can augment the language work force and shift resources to meet critical-language requirements. To improve the skills of military and civilian linguists, we need to learn and develop interac-

tive computer-aided tools, conduct language seminars, and establish extensive mentoring programs.

(U) Extensive mentoring programs may alter the way in which many of us have previously gone about our business. Master linguists, for example, could provide career and skill-field advice and guidance to Senior Member and Member Linguists, who, in turn, could guide and develop junior linguists toward professionalization. Extensive mentoring programs would require more emphasis on skill development and less emphasis on mission. The goal, of course, would be the linking of skill development and mission needs. Management would need to permit linguists the time to sustain language skills and learn new skills. We linguists would need to focus attention on flexibility in the work place and adapt to sudden changes in circumstances.

~~(FOUO)~~ Because of the nature of our work and security constraints, we must guard against becoming insulated from ideas, concepts, and technology pursued outside of the Agency. We need to join academic and professional societies and assocations and subscribe to related journals and newsletters to keep abreast of national and international innovations and initiatives, and describe or introduce these innovations and initiatives at the Agency whenever it would be feasible. Attendance and participation in conferences and seminars can also expose us to new ideas, concepts, and technology.

~~(FOUO)~~ We shall expect to increase productivity, anticipate and cope with future events and circumstances, and learn new skills. We must, however, also find time to maintain language expertise. As of this writing, several post-professional opportunities and plans, all under the auspices of the Technical Track Program, have been developed. The DO/SLA has developed a mechanism which will identify conferences and seminars, select the appropiate individuals to attend them, and provide the funds for these individuals. The Language Career Panel has developed a draft of a Resource Guide for linguists in the Technical Track Program to use to develop their careers. The Panel recently proposed to the Senior Technical Track Board the establishment of expanded mini-immersion programs tailored to the personal and mission needs of linguists. Many other ideas are in gestation. The THABs, for example, are exploring the idea of creating positions within the Key Components primarily for the career development of selected titled linguists.

~~(C-CCO)~~ Future programs will be derived from ideas recommended by linguists who are participants in the Technical Track Program. Ideas are limited only by our lack of creativity and the shrinking federal budget. The Language Panel has created and implemented an electronic subscription network to keep titled linguists informed of activities, opportunities, ideas, etc. The subscription network has already generated responses and ideas. The Technical Track Program is geared to provide certified linguists with a means to develop their own careers to benefit the Agency as well as the linguists themselves. In the final analysis, each of us must take full responsibility for developing our individual careers in a way that will meet our personal as well as mission needs. The Technical Track Program will evolve as we all cope with a changing future.

Kλ

We must begin now by involving as many from the cryptologic workforce as possible in the process of working horizontal problems across skill field and organizational boundaries. We need a workforce of experts in various fields who are used to working together with others outside their field. We must also identify the technical leaders and give them the opportunity to learn how to provide the unique form of technical management that will be needed to guide these cross-disciplinary and cross-organizational teams.

— Recommendation of the Deputy Director's Cryptology Futures Study

Intelligence Research + Traffic Analysis = Intelligence Analysis

by [redacted] IACP P.L. 86-36

(U) Every cryptologic field at NSA has had to evolve over the years to meet current and future demands. Intelligence Analysis is one career field where transformation has been obvious, as two fields, Intelligence Research and Traffic Analysis, were combined to form a new discipline. Driven by exponential expansion in communications technology and rapid political change, the new field must be greater than the sum of the former fields to enable it to meet the changing needs of the Intelligence Community.

~~(FOUO)~~ Intelligence Analysts will continue to play a key role in the production process, but with the incredible growth of modern communications targets and analytic tools available for use by NSA analysts, we have been challenged to understand not just a single aspect of a target, but much, much more.

[redacted]

P.L. 86-36

(U) NSA is in the *business* of producing intelligence. That intelligence comes in many shapes and sizes and the Intelligence Analyst of the future must be able to tailor the finished SIGINT product to the needs of strategic and tactical commanders, those interested in economic or diplomatic issues, or those involved in making national policy decisions. If it needs to be presented to the customer through video links, we need to do that; if they want it in on-the-spot reports, we have to respond; if they need a 3-month in-depth study, complete with maps and an effective Desk-Top Publishing presentation, that is another step we have to take to fulfill the customer's expectations. Our SIGINT reporting must continue to be useful, valuable, responsive, and top-notch!

(U) How much does this say about the future? Mostly that Intelligence Analysts need to adapt, to know our customers, what they think, what they want, and how they want it. Sound unpredictable? It is. That is why it is essential to be flexible, to be in tune with the unique needs of each of our users, and to stay abreast of new technologies. The benefits of teamwork will become more and more evident in this environment; cooperation between individuals, between teams, between offices and groups, must occur. The field of Intelligence Analysis ensures a breadth of knowledge that will "make" the leaders who understand the macro view. These same leaders will also have the technical competence to know and understand the specific analytic techniques that should be applied to solve our future challenges.

DOCID: 4019609

CRYPTOLOG
Issue 1 1995

Intelligence Analysis:

Production and Reporting in a Changed Environment

by [redacted] P054

P.L. 86-36

~~(C)~~ [redacted] has described one of the several fundamental changes reshaping the Intelligence Analysis career field and its operating environment: the changing shape of the world's communications. Concurrent and equally fundamental changes in the political environment in which SIGINT and its customers must function, and in the relationship between open-source information and "secret intelligence," compound the transformation taking place around us. In rounding out a look at the future of intelligence analysis, we need to examine the impact of those other revolutions.

American Intelligence in Peacetime: A Contradiction in Terms?

(U) For the first time in half a century, the United States is not engaged in real or virtual war. How will the American people respond to that? The evidence of the first five years of the post-Cold War era suggests that traditional American concerns about "foreign entanglements" have not disappeared. The evidence further suggests, however, that the American public that emerged from the struggles of the past five decades recognizes, better than previous generations, that U.S. involvement in world affairs cannot be episodic or intermittent but, for better or worse, is permanent at some (possibly erratic) level of national attention and expenditure. However painful the adjustments of the past few years have been, comparisons with previous "demobilizations" after the First and Second World Wars support the case for maturity.

(U) Within this consensus, it is at least reasonable to suggest that the American people will accept the reality of a permanent, peacetime intelligence establishment. They will not, it is clear, support this establishment at wartime levels, nor will public opinion permit any of the national security components—foreign affairs, the military, or intelligence—the operational latitude that comes with the survival issues attendant to war. In the post-Cold War era, the national security structures will be held to higher standards of stewardship of both the public purse and the public trust. The military and foreign affairs establishments will be required, each in their own way, to confront public controversy about their size and roles; the intelligence community will be asked to deal with the particularly strong American ambivalence concerning secrecy and "espionage" as consistent with our national values.

~~(FOUO)~~ The effects of this change are about us already. For an agency that spent its first four decades heavily tilted toward securing its sources and methods (understandable in an agency where results point to a single set of sources and methods), complying with the reality of "openness" will prove a difficult task. We are sailing a very large ship through a very narrow channel. The hazards of excessive disclosure, with which we have traditionally dealt, continue; the hazards posed by a failure to demonstrate our value are no less real. One thing is clear: we are a long way from "No Such Agency," and there is no turning back.

~~(S-CCO)~~ As the final stage of any given cycle in the cryptologic process, the stage most proximate and intelligible to the consumer, reporting and dissemination (intelligence production in the language of the Intelligence Analysis professionalization criteria), cannot be seen as anything less than a critical, integral stage of that process. In an age when the final assessment of our value will come from the consumers of our products and services, it becomes vital to serve those consumers well. When I suggested some years ago that cryptology had to be defined to encompass this function, one of the published rejoinders concluded that "bulldozer operators may be needed on the periphery of archaeology, but they are not archaeologists." Reporting and disseminating effectively the results of our collective efforts are not peripheral to the success, even the survival, of this enterprise over the next decade. They are central to both.

If Peter Arnett is on the Scene, Can Intelligence Be Far Behind?

~~(FOUO)~~ In serving our consumers, we will not only be required to demonstrate value comparable to that received from the other intelligence "INTs," but with that received from open sources as well. During a

Gulf War briefing by a collection of intelligence analysts to the Senate, one Senator, impatient with the number of times he had heard us say that some information could not be provided in that particular setting, walked out muttering "I can get better information on CNN." A particularly brave member of the briefing team chased the Senator down the corridor to refute that contention.

(U) But the presumption remains among significant portions of the public that we are an expensive duplication of the public print and broadcast media, of universities, and of think tanks. We had better be able to deal with that presumption, not just by sneering at it, and not just by pointing to the limitations of open-source information.

(U) The fact is that the value of open source information available to decision-makers has risen, as new communications technologies have come on line and as open-source access to much of the previously denied parts of the world has improved. In large part, this development caused the near-disappearance of closed, totalitarian regimes, and it has accelerated in the years since.

(U) In a world threatened by totalitarian regimes that made information control a central act of their existence, secret intelligence had advantages of access to information no open source could compete with, at least within reasonable, actionable timeliness standards. A researcher at the Hoover Library, working on bound volumes of *Pravda*, was no competition for the intelligence analyst of the 1950s. Once overhead satellites solved the problem of the Soviet landmass, intelligence had a truly extraordinary edge over other sources. (In fact, one could argue that only once before, in the cryptologic successes of the Second World War, has intelligence provided policy makers and commanders with such an information advantage.)

~~(S)~~ Intelligence retains significant advantages, but not in the way we once did, and not for all the same information. Information technology has altered the rules of information management and fundamentally changed the access picture. Only a few decades ago, Soviet dissidents copied by manual typewriter political tracts or, in a remarkable act of physical endurance and moral courage, Russian novels. Now, regimes and dissidents around the world have access to fax machines, satellite transmitters, laptops, the Internet, and, one sometimes thinks, Ted Koppel's phone number. Even overhead reconnaissance now enjoys only a comparative rather than an absolute advantage over commercially available satellite photography.

(U) How do we compete in this environment? Clearly, not by duplicating open-source information. One of the more difficult but essential analytic tasks of the coming era will be what to concede to open sources. This will be necessary for no other reason than that it will be fatal, in an age of austerity, to be seen as an expensive alternative to the New York *Times*. We must identify and emphasize the information that comes to us (and through us to consumers) uniquely through our sources. Even then, we will be asked to prove, through some calculus, that our information was not only unique but worth the cost of its acquisition. Reporting through intelligence sources information already available in open sources will only demonstrate our ignorance of the open sources. Resource allocators will not tolerate much of that.

CNN: speed, not depth

~~(S)~~ The evidence suggests that we will be able to achieve this objective. While much of the public may equate the Gulf War with the "CNNization of information," a small minority of participants, prominent among them Messrs. Bush, Scowcroft, Cheney, Powell, and Schwarzkopf, must know that intelligence, prominently including SIGINT, supported their efforts in ways no predecessors have ever been served. It wasn't perfect, but in the real world little is. The alternative to paying for intelligence information would have been payment in lives, and that's a cost the American people will be reluctant to bear.

(U) In the short but eventful interval from 1991, open source information has become more pervasive and more compelling, certainly to civilian policy-makers. The researcher at the Hoover Library no longer works from bound issues of *Pravda*; he or she is making frequent visits to Moscow, interviewing key officials,

and staying in touch with a host of correspondents on via facsimile and e-mail.

~~(FOUO)~~ This will force the SIGINT analyst of the future to be more aggressive in knowing and using collateral, both open and classified. It will force the analyst of the future to be more adept at producing "finished SIGINT," defined in this context to mean SIGINT produced by an analyst cognizant of the collateral available on his or her target but identified by that analyst as having value over and above that in the collateral. We should not worry about competing with CNN. Does Cadillac compete with Jeep? Yes and no. Yes, in that there is a finite amount of money in the market to be spent for personal transportation. Yes, in that the technical staffs of each would like to think they are better at their jobs. No, in that the two products attempt to fill different needs in the transportation market and can coexist within their respective niches.

One competitive niche for intelligence must be the ability to alert to an impending event before it happens.

Another will be an ability to give decision makers unique and deeply accessed information to the "why" question, with all it means in judging future intentions.

(U) The same holds true in information. CNN and other open sources will have inherent advantages in reporting the "who, what, when, and where" of events taking place in the open. One competitive niche for intelligence must be the ability to alert to an impending event before it happens. We will not achieve this all the time, [redacted] wonderful "signals" versus "noise" analogy still being true. Another will be an ability to give decision-makers unique and deeply accessed information to the "why" question, with all it means in judging future intentions. In intelligence, as in journalism and history, "why" is still the stumbling block. CNN may get a story first; we must get it right.

~~(FOUO)~~ This does not mean the SIGINT analyst must produce "finished intelligence." In fact, it is hard to imagine, in the environment we are likely to encounter over the next decade, anything less valuable and less defensible than yet another set of finished intelligence producers. But the SIGINT reporting of the next decade must take place in an all-source context. (A small blessing of this difficult transition would be the disappearance of the artificial distinction between "finished" and "unfinished" intelligence. In an age when National Intelligence Estimates routinely include open-source judgments, even judgments that counter those of the Community, it is anachronistic to think the information process is somehow "finished" when an intelligence analyst slaps a classification on a report. The consumer may not consider even a highly compartmented intelligence report "finished" until she has checked for competing views in the press, called a friend at the Kennedy School or Stanford, or scanned CNN.)

~~(FOUO)~~ A final thought on the cryptologic process and the challenge it faces: Any casual reader of the Electronic Subscription Service or other internal bulletin boards will attest to the existence of debates about who's really important in cryptology. Is it the cryptanalysts or the linguists? Tech track or management? And what about critical versus non-critical skills?

(U) All of this is to be expected in an institution experiencing (moderately) hard times. Some of it can even be productive of esprit de corps. Army and Navy, after all, have coexisted in a competitive relationship for two centuries. But within limits; institutions that exceed those limits ("General Short, meet Admiral Kimmel.") are looking for trouble.

~~(FOUO)~~ If we have learned anything in the half century since cryptology emerged from the Black Chamber, it is that this is not a single discipline, but a process. We are more like medicine, an applied process, than a single discipline. In many respects, the break between the Black Chambers and modern cryptology is the invention of traffic analysis, the recognition that cryptologic attack can reveal information of value even when it is successful only in recovering the externals of intercepted communications. At other times, the information of greatest importance to decision-makers has come from unenciphered communications, even though to the purist this must seem cryptanalytically unsporting.

(U) Once we accept the idea of process, however, the goal becomes very simple: to employ the techniques of that process to provide information of value to the consumer. Once we accept the idea of process or system and agree on which components are critical to that process—literally critical, i.e., if any of the critical components fail, the process fails—than the interdependency of the components becomes unarguable. Debating among ourselves whether computer scientists are more important than linguists (one can argue supply and

demand issues, and the compensation decisions that should flow from these, but that is not the same) then becomes a bit like debating the relative value on a surgical team of anesthesiologists versus surgeons. As a patient, my very strong preference would be that both should be competent.

(U) The technical challenges facing the intelligence analysts of the future will be formidable. Anticipating the needs of consumers, converting those needs into requirements for signals intelligence information, informing consumers of what SIGINT can (and cannot) do, integrating those needs into the technical processes of the agency, and employing the full range of dissemination techniques and methodologies in order to get information the consumer on time and in formats that permit the information to be useful rather than academic are among the tasks at hand.

Kλ

The National Performance Review's report on the Intelligence Community made seven major recommendations, each with suggested actions. Since then, significant strides have been made toward accomplishing these recommendations. For example:

Reassess Information Collection to Meet New Analytical Challenges

- The Foreign Broadcast Information Service (FBIS) has completed two exhaustive studies, reviewing its field collection network and examining products and services measured against consumer needs.

- The new INTELINK information system, now in development, promises to facilitate "real-time communication between analysts and collectors."

- CIA and DIA have increased dramatically the number of integrated analytical papers they produce jointly. Joint task forces bring cross-discipline analysts together to work on key issues.

Integrate Intelligence Community Information Management Systems

- A new Intelligence Systems Board (ISB) co-chaired by the Executive Director, IC Affairs and the Deputy Assistant Secretary of Defense for Intelligence and Security was formed late last year to ensure interoperability of intelligence information systems.

- The ISB and the National Intelligence Council have also established an Electronic Publishing and Dissemination Board (EPDB) for developing policy and procedures to allow electronic text exchange throughout the IC. INTELINK, once operational across the Community, will serve as the central focal point for dissemination activities.

Enhance Community Responsiveness to Customers

- Customer advocates or "issue coordinators" were appointed for each of the 16 major issues in the National Intelligence Need Process (approved by the DCI in July 1993), focusing greater attention on individual customer needs. The issue coordinators have recently completed strategic reviews of their assigned areas, involving substantial dialogue with IC customers.

- The IC has made a major effort to bring service closer to customers, including placing additional liaison and briefing officers at customer facilities and greatly expanding electronic connectivity.

Develop Integrated Personnel and Training Systems

- The DCI's Foreign Language Committee has published a "Unified Language Testing Plan" setting Community-wide language proficiency standards. The plan will be implemented this fall with a pilot project in Spanish.

- A vigorous program of inter-agency rotational assignments is now under way.

Improve Support to Ground Troops During Combat Operations

- The IC Battlefield reinvention lab wraps up its final phase this month, with briefings to senior officials. A panel of outside experts has provided support in the activity this year to General Crosbie Saint (USA, Ret.), the lab's coach.

Reprinted with permission from *Quality and Innovation*, the IC Quality Control Newsletter, Vol. 1, No. 8, September 7, 1994

~~SECRET~~

DOCID: 4019609

~~CRYPTOLOG~~
Issue 1 1995

P.L. 86-36

Signals Research and Target Development: Past, Present, and Future

EO 1.4.(c)
P.L. 86-36

by [redacted] P054 TARS

~~(S-CCO)~~ [redacted] Signals Research and Target Development has become the focus of much recent discussion. The number of people involved, however, doesn't fully explain the attention this topic has received over the past few years. SIGINT production is a process. Signals Research and Target Development is our latest refinement of that process. This article discusses what Signals Research and Target Development is, where it came from, and where it's going. Through this discussion, it is hoped that the reader can gain an appreciation of the past, present, and future of Signals Research and Target Development.

~~(S-CCO)~~ SRTD: *WHAT DOES IT MEAN?* Three or four years into its existence, that's still debated in some circles. The views are largely personal—different organizational perspectives result in different definitions. This is natural, coming partially from the fact that different organizations' missions vary, but there is a common element among most definitions:

SRTD is a process

Some practitioners partition it into two distinct, but related, processes. Signals Research (SR) is the process of developing information necessary to exploit a signal. Exactly what that information is can be contentious, but usually includes understanding the operating characteristics of a signal of interest (modulation type, coding scheme, encipherment, etc.), the use and implementation of a telecommunications technology which employs that particular signal (or a set of signals), and exploitation vulnerabilities. The other process is Target Development (TD)—taking knowledge developed through SR and using it to develop sufficient insight to a communications system used by a particular SIGINT target to allow reliable access to information of interest. In either case, SR or TD, the process requires application of multi-disciplinary skills (Intelligence Analysis, Crypt-Analysis, Mathematics, Signals Analysis, Telecommunications, Computer Science, Collection Management, and Language). Sound ambiguous enough? Good!

~~(S-CCO)~~ So, that's the loose definition of SRTD. Who does it? First, it's important to emphasize that SRTD is not a career field. The urge to make it a career field was resisted because of the awareness that the SRTD process required the skills and knowledge of several disciplines. As such, there really isn't any title or COSC for people who do SRTD. In fact, while SRTD elements are primarily staffed by Intelligence Analysts, they also rely heavily on individuals from the Signals Analysis, Collection, Telecommunication, Language, Engineering, and other career fields. For the purpose of this article, SRTD "analyst" will refer to any of the individuals who are involved in the SRTD process.

Past

(U) As recently as a decade ago, the networks that the Agency exploited were very different from those encountered today. Civil networks were very static; military networks were dynamic in terms of Standard Operating Instructions (SOI), but used new technology very gradually. These networks were relatively simple: they employed limited modulation techniques and signal bandwidth was fairly narrow; communications were primarily voice and teleprinter, though use of data and facsimile was growing; and network complexity was only moderate.

~~(FOUO)~~ The state of the Intelligence Community was similarly straightforward. We were in the middle of a long-standing and very dangerous Cold War. The U.S. SIGINT Service was based upon structures put in place during WWII, modified only as necessary for the Cold War. SIGINT priorities were clear. Funding to work against our primary adversaries can now be described as generous—we were able to amass considerable human resources, fund what seemed to be a robust infrastructure, and maintain a healthy investment in systems development.

~~(FOUO)~~ These factors combined to make an exploitation environment that was well developed, with resources sufficient to excel. The Agency met customer demands through focused attacks against networks using passive access techniques. Our understanding of the targets and the technologies they employed for telecommunications was superb. A long history of performance established our technical health in nearly all areas of SIGINT endeavor.

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

~~(C)~~ As a result, monitoring of technology evolution and network modernization was performed iteratively against high-priority targets. Target development was thought of as continuous, performed daily by numerous "U/I" teams (these elements worked against nets operated by users unidentified by the SIGINT system). It was a critical factor in maintaining an understanding of target telecommunications networks and strong technical health among the work force. The primary discipline involved was traffic analysis.

~~(C)~~ The status quo was permanently destroyed by two events: the abrupt overthrow of Soviet leadership, ultimately ending the Cold War and changing world polarization; and the Iraqi invasion of Kuwait and subsequent, massive involvement of global military forces. The first event had drastic and immediate effect on SIGINT requirements and funding. The second highlighted shortfalls in the ability to deal with third-world crises and modern network technologies.

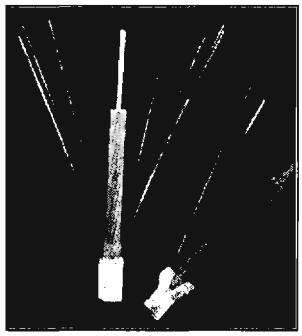
~~(S-CCO)~~ Much of this had been predicted. In the late 1980's, high-level studies (the Perry and Brotzman reports) and several reports written by Agency technical leaders warned of an ongoing technology revolution. They made many recommendations on ways the SIGINT community should evolve. An article in the Fall 1989 *Cryptologic Quarterly* by [redacted] predicted that world developments would force the U.S.S.S. to shift priorities to non-military targets.

~~(S-CCO)~~ With Desert Shield/Desert Storm as a catalyst, these recommendations finally hit home. The Agency underwent major reorganization—so did several career fields. ***During this activity a "new" intelligence process was identified which was referred to loosely as Communications Research and Target Development (later modified to Signals Research and Target Development).*** It was hoped that this process

[redacted]

Present

(U) Today, telecommunications networks are very different from those described above. Network structures are much more complex, being designed in a layered and functional manner. They are more dynamic—both through more rapid introduction of new technologies and through more flexible structures which enable the network to be much more active in reconfiguration. These networks support a wide range of modes and services, from simple voice and teletype, to multi-point video conferencing and broadband data transactions.



Helen Bauer of AT&T's Advanced Intelligent Networking division describes the state of the telecommunication industry as a revolution driven by revenue production. Money is a strong motivator, and the possibility of increased revenues is driving network administrations as never before.

P.L. 86-36

(U) The SIGINT community is undergoing equally radical change. We are wrestling with massive cultural changes—moving from a tiered, closed environment to a matrixed, open structure. We are faced with continually diminishing resources while the requirements on our system are increasing. The result is a very chaotic work environment.

[redacted]

P.L. 86-36
EO 1.4.(c)

Future—Starting Now

(U) The networks of the future will reflect incredible achievements of human endeavor. They will be structured in functional layers, enabling modularity and ease of evolution. The transport of information through the global network will be done transparently, allowing any mode or service to be conveyed in a seamless fashion. Networks are becoming extremely dynamic in configuration with traffic routing becoming very diverse, adapting easily to network outages, temporary massive changes in calling patterns, and time of day, week, or year. It will allow broadband applications and be characterized by user mobility. Software will be the key element in the global network, allowing rapid, iterative service development customized on a personal level. Network administrations, while being extremely competitive, will also be very cooperative, at both the national and international levels. Major international alliances such as those of MCI/BT, AT&T/KDD, or Sprint/FT/DBPT will drive the future of the telecommunications industry and diminish international network boundaries.

~~(FOUO)~~ Who knows what the Intelligence Community will look like? A prolonged military engagement seems unlikely now, but that's the sort of thing that is difficult to predict. The Aspin Commission and two congressional review groups make it impossible to provide any certain assessment of our future. It is possible that the Agency will move out of the realm of the Department of Defense, separating the generation of SIGINT product from the direct influence of the services or other consumers. Another area of uncertainty is the role, use, and implications of Open Sources (OS). ***The OS revolution, spurred by DCI pronouncements to make better use of OS, will have major impact on our future.*** At a time when there are massive budgetary pressures, there are proposals appearing that call for not just supplementary use of OS, but disbanding the Intelligence Community (IC). Some circles believe that the new world order, combined with the research capabilities available via the Internet, make the IC expensive and unnecessary. These seemingly radical views should not be underestimated in times of budgetary crisis.

DOCID: 4019609
P.L. 86-36
EO 1.4.(c)

The SRTD "Analyst"

(U) It has already been said that SRTD is a process, not a career field. What should the SRTD analysts be doing to prepare for the future discussed above?

~~(S-CCO)~~ SRTD analysts necessarily must be multi-disciplined but highly specialized; however, they can't be experts in everything. As mentioned previously, most will come from the IA career field, but many will come from other areas such as telecommunications, Signals Analysis, or Collection Management. The result is that much of the work requires original, innovative thought applied to problems in ways only teams of SIGINT professionals can perform. It requires a great deal of individual initiative, professional independence, and cooperative effort. ***In short, the greatest challenge SRTD "analysts" face is in developing their art and science as a team of experts.*** They are the experts in their field—whether ready for it or not!

~~(S-CCO)~~ [redacted] (SRTD Steering Group representative for A) encourages SRTD people to pursue education in their areas of interest. They know what they need to learn, so they should direct their efforts in the appropriate way.

~~(S-CCO)~~ SRTD, by necessity, is a task requiring several skills employed in very specific ways. Individuals need to develop a diverse set of skills: analytic competence (especially in traffic analysis); understanding the collection process; advanced research techniques; a

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

high level of ADP capability; etc. [redacted]

As [redacted] SRTD Steering Group representative for Z) points out, ***"The SRTD analyst ought to know how to make the system work for them—to get done what they know must be done."*** This requires close interaction with all SIGINT core processes. Ms. [redacted] sums this up by encouraging the SRTD analyst to learn to ask questions. The most important one: **"Where does the information come from?"**

Special thanks to [redacted] *in editing and refinement of the text.*

EO 1.4.(c)
P.L. 86-36

Kλ

Computer Science in the year 2000

Reprinted from Workforce 2000

EO 1.4.(c)
P.L. 86-36

[redacted]

~~(FOUO)~~ System administrators will be needed to support the analysts and the networks to which they are connected. Additional System Administration personnel are required in virtually every area of the Agency, encompassing each directorate, support staff, and field sites. A System Administration Cross Training program is in place within the Computer Science Career Panel to provide a source of qualified administrators through a structured training and performance program.

~~(FOUO)~~ By the year 2000, automation and operations consolidation will result in the need for less computer operators, computer operations specialists and data flow managers. Computer Operations and Dataflow Management will be encouraged to cross-train from these career fields into others. Further, those who work in the computer operations center of the future must be multi-skilled with expertise in computer systems operations, networking, and data flow.

~~(S)~~ Computer skills will continue to be increasingly necessary for most NSA jobs leading to dual professionalizations. Computer Science/Mathematics, Computer Science/Cryptanalysis, and Computer Science/ Intelligence Analysis are some of the combinations that will support our future missions.

The Telecommunications Professional Of The Future

by [redacted] *former Technical Director for Q*

EO 1.4.(c)
P.L. 86-36

(U) When plotted on a cosmic stop watch, virtually all technological advancement has occurred in the last few seconds before the present. The rate of that advancement continues to accelerate unabated. All aspects of human endeavor have been affected by this phenomenon, but none more so than the field of telecommunications.

~~(FOUO)~~ Today, every one of us is inundated with communications. We have instantaneous access to events of interest which may occur in any part of the world. It has been argued that the Western world is in a state of information overload, brought about by the incredible advances in the state of the telecommunications technology art. But what of NSA? What of its mission and the people who work the telecommunications field? A trip to an NSA communications center today would show a mix of technologies, ranging from very old legacy systems to the latest state-of-the-art.

[redacted]

P.L. 86-36

(U) For each generation of technology in our telecommunications network there is also an attendant suite of skills, procedures, and processes. Consequently, our current telecommunications professionals must be adept in making a multi-generation, multi-technology communications system appear as a seamless provider of services. The demands are many. The rewards are few. It is an unfortunate historical phenomenon that the communications network is usually taken for granted by its users—until something goes wrong.

(U) NSA is not alone in having to deal with this problem. To date, industry has found it appropriate to retain much of the familiar process, and the consequent skill mix to implement it. For example, even though there have been significant advancements in the telephony and television industries, telephones and television sets still work very much as they did years ago. There are still people who climb poles, install instruments, or man switches. Advancements in transmission technology (principally fiber) and the trends toward integrating all types of telecommunications services onto the same communications infrastructure are about to change that model. The question is, "Are we ready for it?"

P.L. 86-36

[redacted]

(U) While it is technologically feasible to integrate the disparate types of services into a single network, the requisite tools for operating and managing the resultant network(s) are not yet mature. Capabilities that in the past were either not available or had to be developed by the end user himself, are now being offered as value-added services of the telecommunications system. The users are clamoring for the latest and greatest, the trade magazines try to convince the reader that they simply can't survive without the latest sophistication, and it is left to the cadre of telecommunications professionals to figure out how to make it all work together.

(U) We have made great strides in enhancing the skill mix and developing the procedures necessary to successfully cause a heterogeneous mix of equipment, tools, and technologies to function cohesively, but the task has only begun. The progress made in the telecommunications field in recent years is just the beginning, and we are on the horns of a dilemma. We cannot afford

to ignore the new opportunities, but we also cannot afford to throw away the large investment in legacy systems that were designed and installed without benefit of the newest concepts for instrumentation, operations, and maintenance. Within a very short time we must be able to operate our global integrated services network from a small number of remote operations centers. Equipment must be instrumented so as to report its health, load, and other environmental information across the network to this central authority. Faults or other types of anomalies will be flagged to the attention of the network operator while the system automatically, or with operator assistance, makes the necessary routing adjustments in an attempt to assure that requisite service continues unabated.

(U) What does this mean to the work force? Certainly it will be a different world. Many skills which have served us well for so many years will no longer be necessary. The numbers and types of personnel needed will dramatically change. Our network planners must appreciate that the global network is indeed an integrated system, and plan it accordingly. We will need a cadre of more highly trained individuals to man the nerve centers of our system. A network operator of the future will need to be able to quickly assess the state of the network, diagnose trends which indicate potential failures, understand the implications of failures on the missions being served, and make real-time decisions regarding the steps necessary to assure continued service to the most critical missions. The roles of virtually every telecommunications professional, be they planners, installers, operators, or maintainers, must undergo a metamorphosis.

(U) We must help create a new generation of service providers who can synthesize from the myriad requirements the most appropriate network undercarriage, sense the pulse of the network from a central location, understand the implications of the logical missions which overlay the physical communications undercarriage, and who can engineer in real time the adjustments necessary to continue providing service. Where will we find such people? Will they come from the present cadre? Perhaps. But this new cadre will need to be educated as engineers, computer scientists, or in the fields of network analysis and computer or telecommunications engineering. They will need to be schooled in the latest network management techniques (something not readily available on many campuses). It may even be necessary for them to take the lead in shaping this particular aspect of the field. They will also need to have an appreciation of the nature and importance of the various missions which they will be supporting. Above all, they must be SERVICE-oriented.

Kλ

EO 1.4.(c)
P.L. 86-36

Global Network Intelligence and Information Warfare:

SIGINT and INFOSEC in Cyberspace

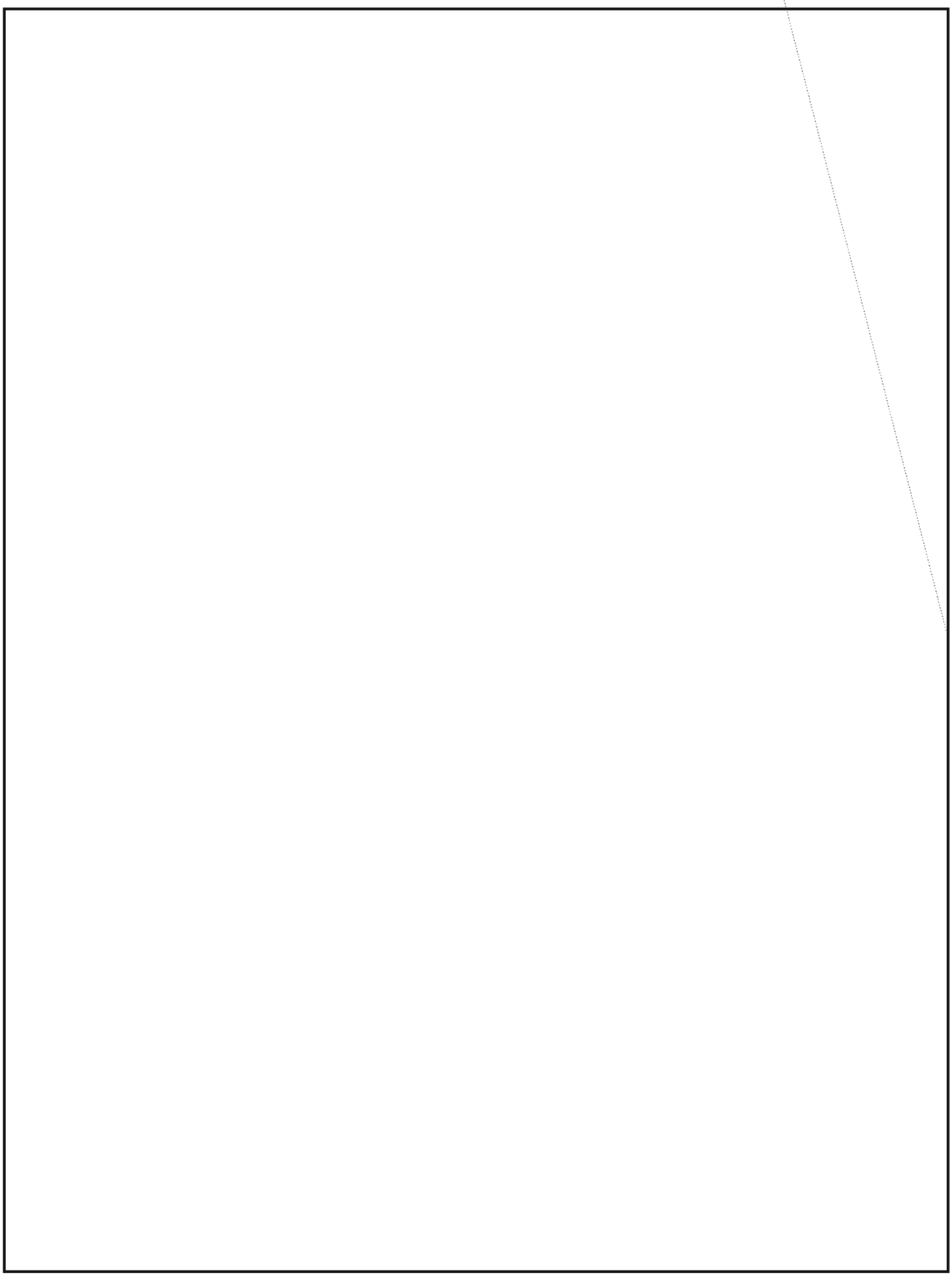
by [redacted] *Former chief, G4*

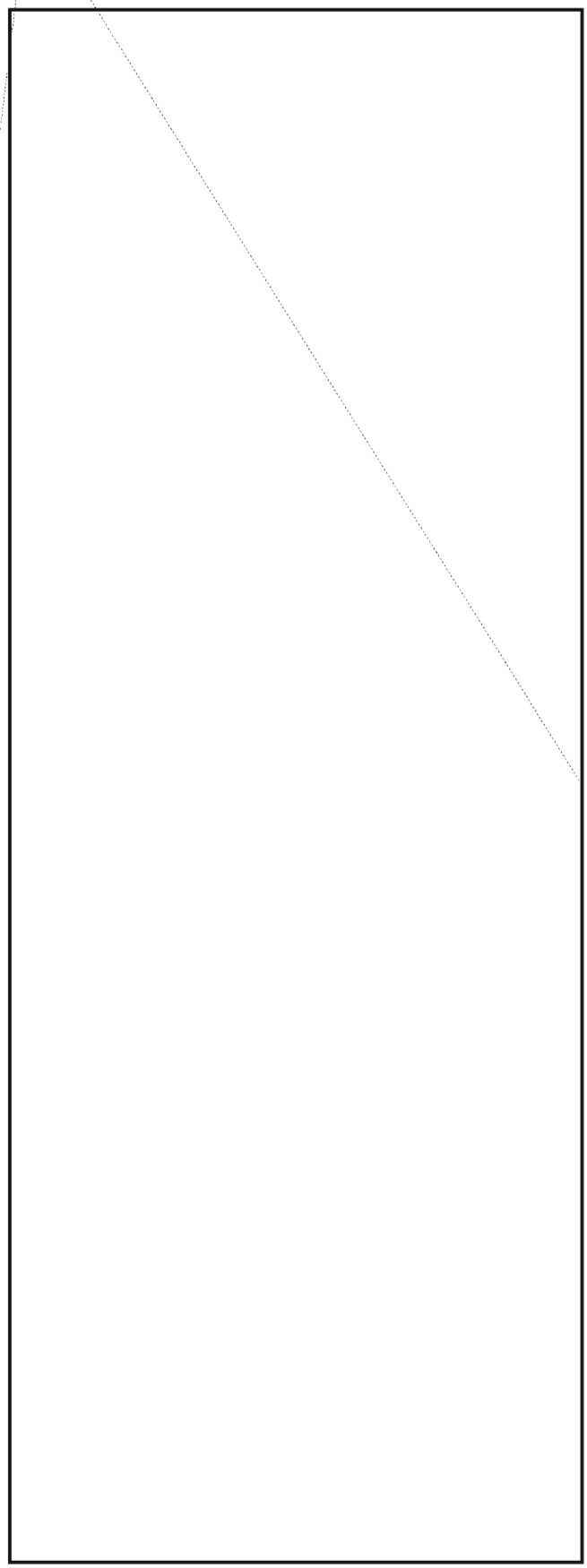
~~(S-CCO)~~ GNI (Global Network Intelligence) and IW (Information Warfare) are two acronyms that have become part of NSA's language over the past couple of years. Both convey new and comprehensive activities that are critical to NSA's future and both dramatically affect the Agency's offensive (SIGINT) and defensive (INFOSEC) missions. The purpose of this article is to provide a general overview of the background and ongoing activities in each area, to explain their interrelationships, and to discuss a few relevant challenges that are of general interest to the NSA workforce.

~~(TS-CCO)~~ GNI and IW are responses to the dramatic changes in global telecommunications that began with the transition from analog to digital communications in the 1980s. The rapid evolution of digital communications and concurrent advances in transmission media—especially fiber optics—and networking technologies have radically altered the complexion of the global telecommunications infrastructure. GNI and IW address these changes, but from different perspectives.

~~TOP SECRET~~

EO 1.4.(c)
P.L. 86-36



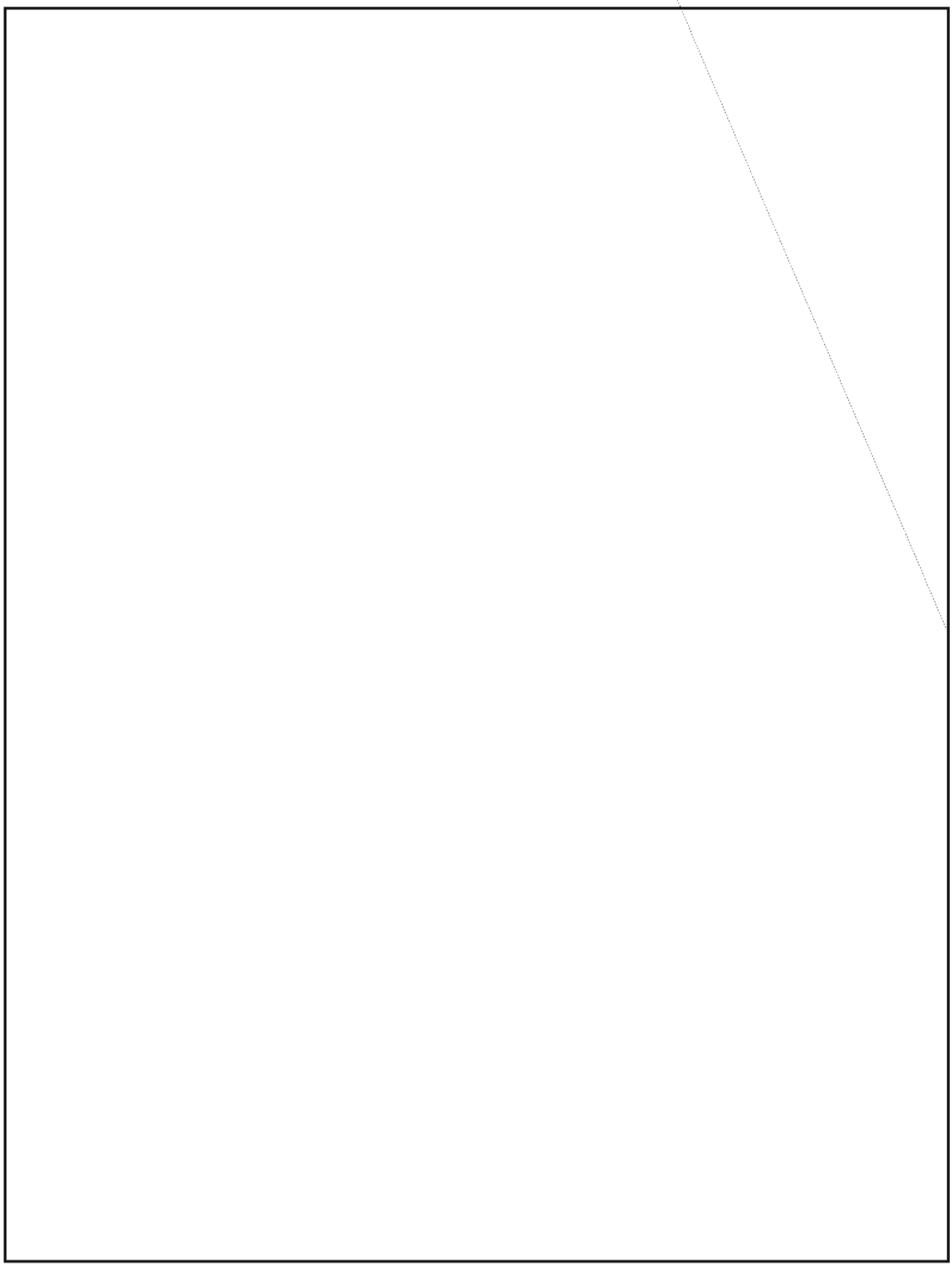


~~(FOUO)~~ Some examples may help to clarify the notion of a "global network" in terms of the telecommunications media involved and functions performed. When Mrs. Jones in Kansas City calls her sister in Tours, France, her telephone call is carried through the local and regional telephone network near her home, over the U.S. domestic fiber-optic network, through the undersea fiber-optic network between North America and Europe, then through the regional fiber-optic network in the U.K. and France, and finally into the local Tours telephone system. In another example, a cellular call from a Japanese businessman from his car in Tokyo to a branch office of his company in Los Angeles will traverse the Tokyo metropolitan cellular, microwave, and fiber-optic system, be routed through either the Pacific fiber-optic network or over a commercial satellite link to the U.S., then pass through the regional, metropolitan, and local fiber-optic network to the Los Angeles office. At the same time, the signalling information for this call—the 1's and 0's that provide key information to route the call and provide billing information for the telephone companies involved—may travel over a completely different path. The global network has the capacity and flexibility to provide many different pathways for connecting one user to another. As the network expands through connections of still more local, regional, and national networks, users will be able to contact other users anywhere on the globe without ever knowing exactly how their calls were completed. The same is true for data communications. This connectivity is already available for personal computer users through the Internet and for an increasing number of telephone and data services users. As technology improves, global connectivity will be faster, more diversified in terms of actual call routing, and encompass a wider variety of advanced services.

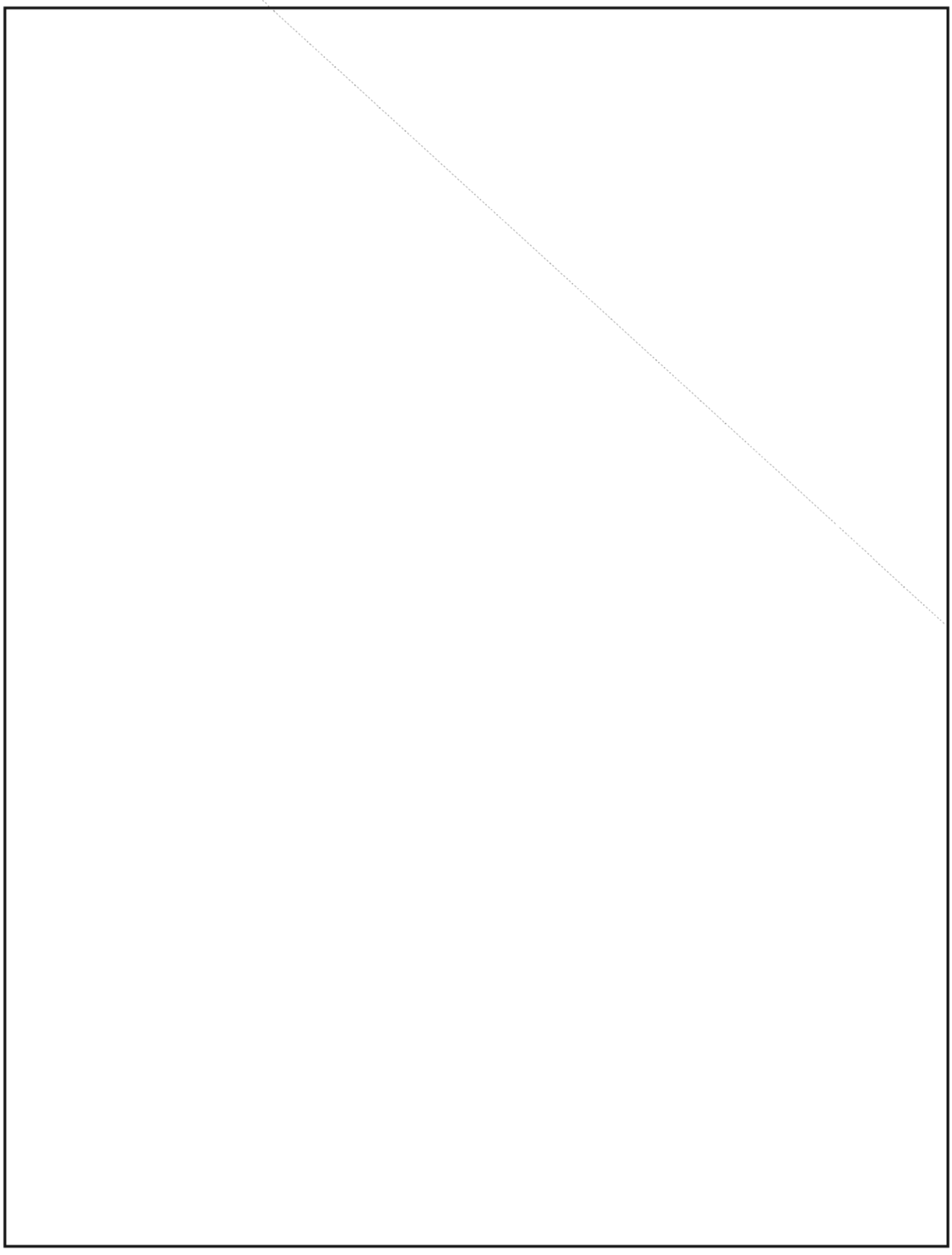
1. INFOSEC information in this and later paragraphs was derived primarily from the NSA/DI booklet, "Security Solutions for Today and Tomorrow," published in February 1994.

~~TOP SECRET~~

P.L. 86-36
EO 1.4.(c)

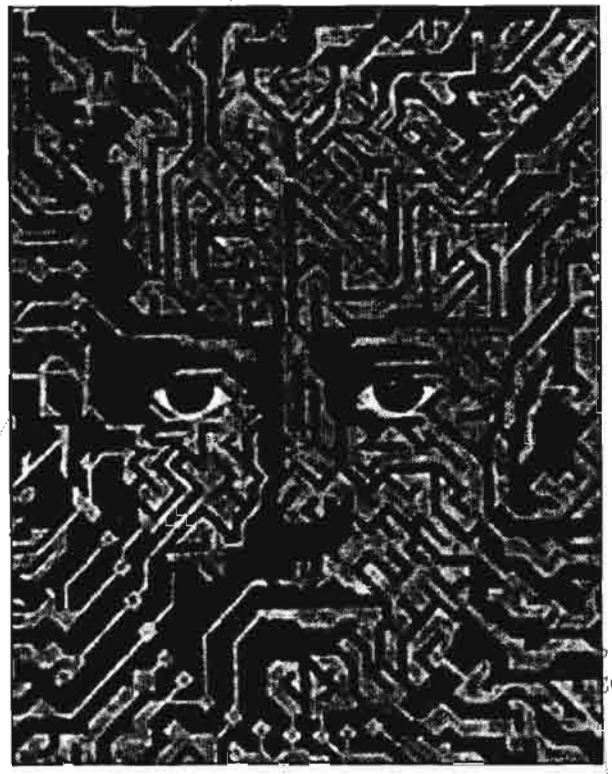


DOCID: 4019609 NSL. 86-36
EO 1.4.(c)



DOCID: 4019609

EO 1.4.(c)
P.L. 86-36



P.L. 86-36
EO 1.4.(c)

Information Warfare

~~(FOUO)~~ Information Warfare addresses the global network from a different perspective than GNI. IW recognizes that the rapid advances in telecommunications will directly affect the U.S. ability to wage war for U.S./Allied forces as well as for potential adversaries. Future wars may well be fought and decided on the "information battlefield" without a shot being fired. The sophisticated telecommunications and data networks now being deployed worldwide make it possible to deny and degrade a potential adversary's command and control communications and sensitive commercial and diplomatic communications from great distances with little or no risk to life and limb. Conversely, the same network technologies make it possible for a potential adversary to damage or cause confusion in communications and information systems supporting U.S. military forces or the U.S. at large.

P.L. 86-36
EO 1.4.(c)

P.L. 86-36

[redacted]

[redacted]

~~(FOUO)~~ Despite the many technical problems, in my judgment the more difficult challenges of the telecommunications revolution are in the organizational/cultural area. NSA has historically risen to technical challenges of SIGINT and INFOSEC by relying on the extraordinary talent and resourcefulness of the NSA workforce. Complex and creative solutions that would be considered science fiction by the general population are routine tools in NSA's approach to signals collection, processing, and forwarding, and information security. One should not take for granted that NSA professionals will be able to meet any and all future technology challenges, but we certainly have a good track record.

~~(FOUO)~~ More worrisome than the technology issues are the challenges posed to NSA as an institution, by which I mean the organizational culture and traditional ways of doing business. The Agency's organizational culture has changed dramatically over the past several years because of continuing budget reductions and the detailed examination of national priorities that has taken place since the demise of the Soviet Union. But as an institution we still tend to function too much as a collection of "stovepipes" in the development of new capabilities. Let me then conclude this essay with a brief description of the organizational/cultural challenges posed by GNI and IW.

~~TOP SECRET~~

EO 1.4.(c)
P.L. 86-36

[redacted]

Cross-organizational Communications

(FOUO) Communications among and between NSA organizations is critical. To really achieve teamwork at NSA, individual developers, analysts, mathematicians, and other specialists have to maintain an awareness of what others are doing, and, conversely, must share knowledge of their work with others. This will allow greater cross-organizational communications about various aspects of a large problem and lead to faster, more complete solutions. We need to do a better job of communicating what is going on across the Agency so that those charged with developing new GNI or IW capabilities can keep abreast of all relevant activities. Communications with external partners is another essential ingredient for future success. Such communications are vastly improved now compared to the past, but GNI and IW impose new and slightly different demands.

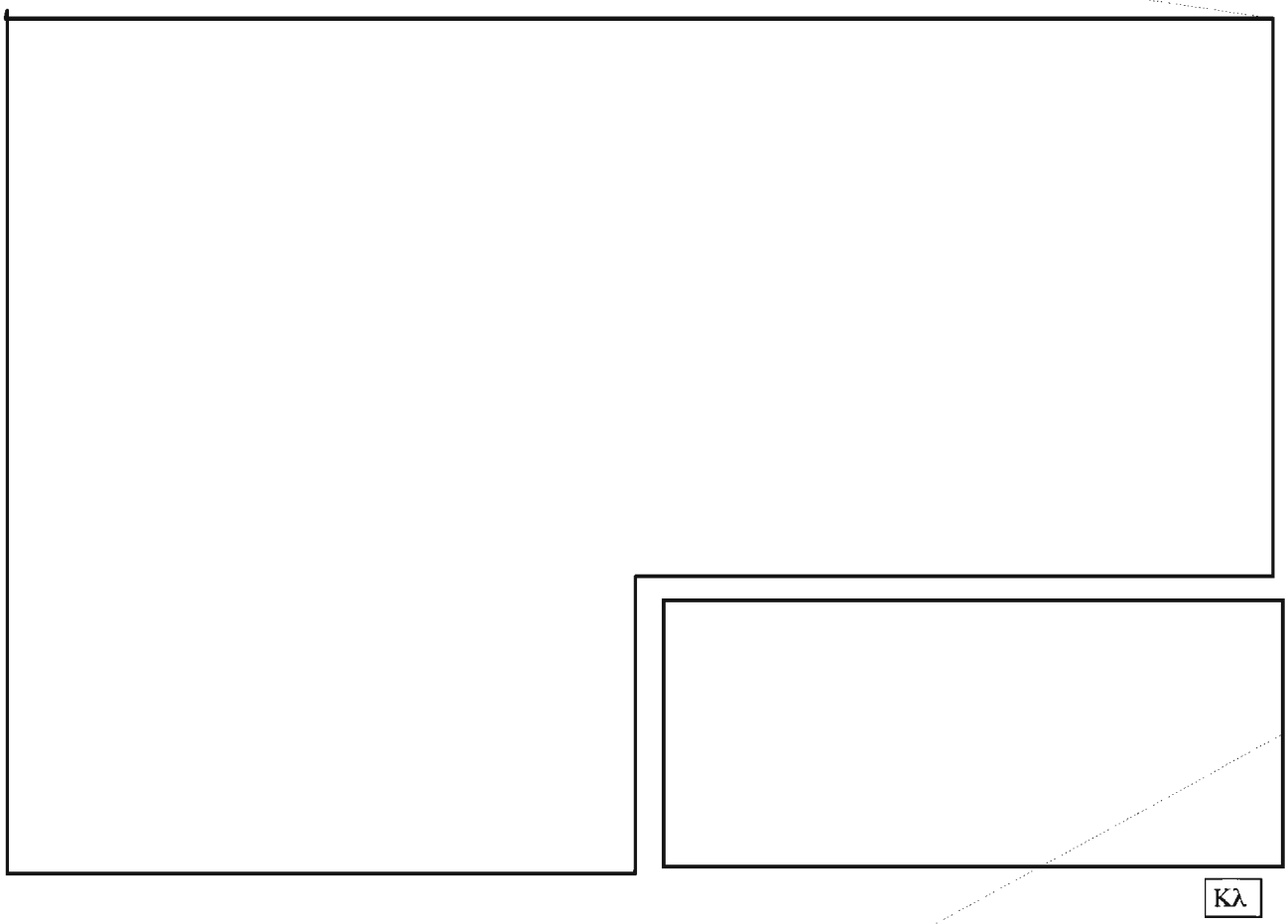
(FOUO) There is an expanded need for cross-organizational communications internal to NSA, too. While there is some overlap between organizations working on GNI with those working on IW, this overlap is not total. There is a continuing need for managers and technical leaders to ensure they maintain awareness of what others are doing and communicate to other organizations the projects and activities underway in their own organization. This way, cross-fertilization of ideas can take place that will help both the GNI and IW efforts.

P.L. 86-36
EO 1.4.(c)

[redacted]

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~



Kλ

P.L. 86-36

DOCID: 4019609

CRYPTOLOG

Editorial Policy:

(U) Technical articles are preferred over non-technical; classified over unclassified, shorter over longer., Emphasis should be on improving NSA's technical performance; articles should be aimed at explaining one's discipline to those outside it. Readers are also invited to contribute conference reports and reviews of books, articles, software, and hardware that pertain to our missions or to any of our disciplines. Humor is welcome, too. Submissions may be published anonymously, but the identity of the author must be known to the editor.

Submitting Items

(N.B. If the following instructions are a mystery to you and your local ADP support is no help, please feel free to call the CRYPTOLOG editor on 963-3123s.)

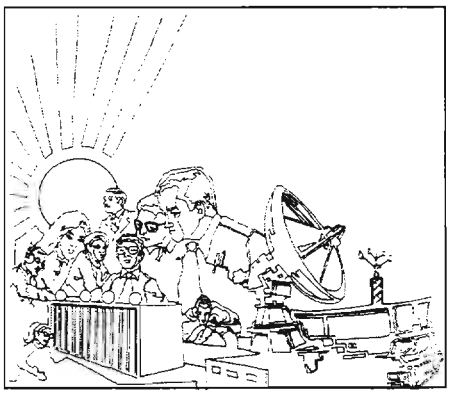
~~(FOUO)~~ Send a hard copy accompanied by a labelled diskette to the editor at P054 in 2E062, Ops. 1, or send a soft copy via e-mail to [redacted] **cryplog@p.nsa** P.L. 86-36

Guidance

For maximum efficiency (as far as possible within the limits of your word processor):

- Do not type your article in capital letters.
- Classify all paragraphs.
- Label all diskettes, identifying hardware (operating system: DOS, UNIX), density and type of word processor used ; also your name, organization, building and phone number.
- FrameMaker format is preferred; ASCII is also fine. J334 has a conversion service that converts Interleaf, Word Perfect, OfficeWriter and MS Word into FrameMaker. Just attach the document to an E-Mail Compose Window addressed to **convert@po**.

~~TOP SECRET~~ 9690



NATIONAL SECURITY AGENCY

CRYPTOLOG

This Issue:

Intelligence and Combat:
Lessons Learned from DESERT STORM
Page 1

A Linguist's Look at the Internet
Page 19

SIGINT Glossary: The GUHOR Stick
Page 36

. . . . AND MORE (Table of Contents, page ii)

Declassified and Approved for Release by NSA on 10-10-2012 pursuant to E.O. 13526, MDR Case # 54778

~~Classified by NSA/CSSM 123-2~~
~~Declassify on: Originating Agency's Determination Required~~

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

CRYPTOLOG

Vol. XX No. 2 ..... 2nd Issue 1994

Published by P05, Operations Directorate Intelligence Staff

Publisher ..... William M. Nolte (963-3123)

Editor ..... [redacted] (963-3123)

Board of Advisors

Chairman ..... [redacted] (963-7712)
Computer Systems ..... [redacted] (963-6669)
Cryptanalysis ..... [redacted] (963-4382) P.L. 86-36
Intelligence Analysis ..... [redacted] (963-6283)
Language ..... [redacted] (963-5704)
Mathematics ..... [redacted] (963-1363)
Signals Collection ..... [redacted] (963-5717)
Signals Collection ..... [redacted] (968-7160)
Telecommunications ..... [redacted] (996-7847)
Member at Large ..... [redacted] (968-4010)
Member at Large ..... [redacted] (968-4010)
Member at Large ..... [redacted] (961-8214)

Classification Officer ..... [redacted] (963-5463)

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

To submit articles and letters, please see last page

Table of Contents

EO 1.4.(c)
P.L. 86-36

A Note From the Chairman iii

Intelligence and Combat:
Lessons Learned from DESERT STORM, by [redacted] 1

Information Warfare: A New Line of Business for NSA, by [redacted] 3

Tour of Duty: [redacted] by [redacted] 5

Target Development in the Field, by [redacted] 7

Spring '94 SRTD Conference Reviewed, by [redacted] 10

Opportunities for Publication, by [redacted] 12

OPSEC in the Post-Cold War World, by [redacted] 16

A Linguist's Look at the Internet, by [redacted] 19

[redacted] by [redacted] 26

[redacted] by [redacted] 30

The NSA Broadcast Center, by [redacted] 33

SIGINT Glossary: The GUHOR Stick, by [redacted] 36

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

A Note from the Chairman:

THE CRYPTOLOG IN A TIME OF CHANGE

The end of the Cold War, the redefinition of vital U.S. interests, increasing fiscal cutbacks, downsizing of the technical workforce, and the proliferation of complex technologies provide the impetus for revitalizing the CRYPTOLOG.

First and foremost the CRYPTOLOG will remain a forum of the informal exchange of information by the analytical-technical workforce and will serve to enhance the knowledge base of technical skills within the SIGINT community.

But in these incredibly rapidly changing times it should also address the purposes Dave Gaddy described in a 1989 CRYPTOLOG article entitled "Where Are Our Textbooks?": "professional literature is...a means through which the profession is defined and...grows and evolves over time. It affords the opportunity to assert and to challenge, to advance ideas and...expose outdated thinking and procedures. It can also supply a more systemized institutional memory, such as that called for by NCS Commandant Whitney Reed in a 1988 memorandum to Agency seniors: 'we are heavily dependent on individual knowledge, recollections of lessons learned (and not learned), and acquired wisdom on the part of our seniors to guide the education of the next generation of Agency leadership.'"

In that spirit, and in an attempt to make the Cryptolog a more relevant and useful publication, I and the new board of advisors invite you to contribute articles, letters and reviews to the Cryptolog which:

- address current and future issues and directions in your field and in the technical aspects of the target and the SIGINT process
- promote understanding and appreciation of the worldwide advances in technology and the changes in the SIGINT process required to respond to them, i.e. technical matrixing.
- describes strengths and, more important, weaknesses in how we have gone or go about our business, e.g., lessons learned, histories etc.
- enlighten the workforce on breakthrough technical advances which could significantly affect all aspects of SIGINT
- disseminate information on professional seminars attended
- encourage discussion and even debate among experts on any controversial subject affecting technical health.

Finally, this journal can serve as a voice of the technical track.

P.L. 86-36

[redacted]
Chairman, CRYPTOLOG Board of Advisors
Ext. 963-7712s

CRYPTOLOG
July 1994

Intelligence & Combat:

P.L. 86-36

Some Lessons From DESERT STORM

by [redacted] P054

~~(FOUO)~~ We in the SIGINT business have long recognized that direct access to the principal player in a given scenario is far more likely to yield accurate and reliable assessments than would be available if we're reduced to listening to what other interested, but perhaps not all that well-informed, sources have to say about that same situation. It was with great anticipation, therefore, that an overflow crowd turned out on 15 April to hear an address in the Friedman Auditorium by United States Air Force Colonel Chris Christon, then the Director of Intelligence, USAF SPACE COMMAND and formerly the Air Intelligence Officer for Lt. Gen. Charles Horner, Commander, Coalition Air Forces, Gulf Theater, during Operation DESERT STORM. Col. Christon—by any definition a principal player during the allied operation to drive the invading Iraqi forces from Kuwait—shared with the assembly his experiences in Saudi Arabia, emphasizing the intelligence successes but, more important, driving home some lessons learned about how to use intelligence to support the kind of warfare that our national security strategy and our force posture will dictate in the future.

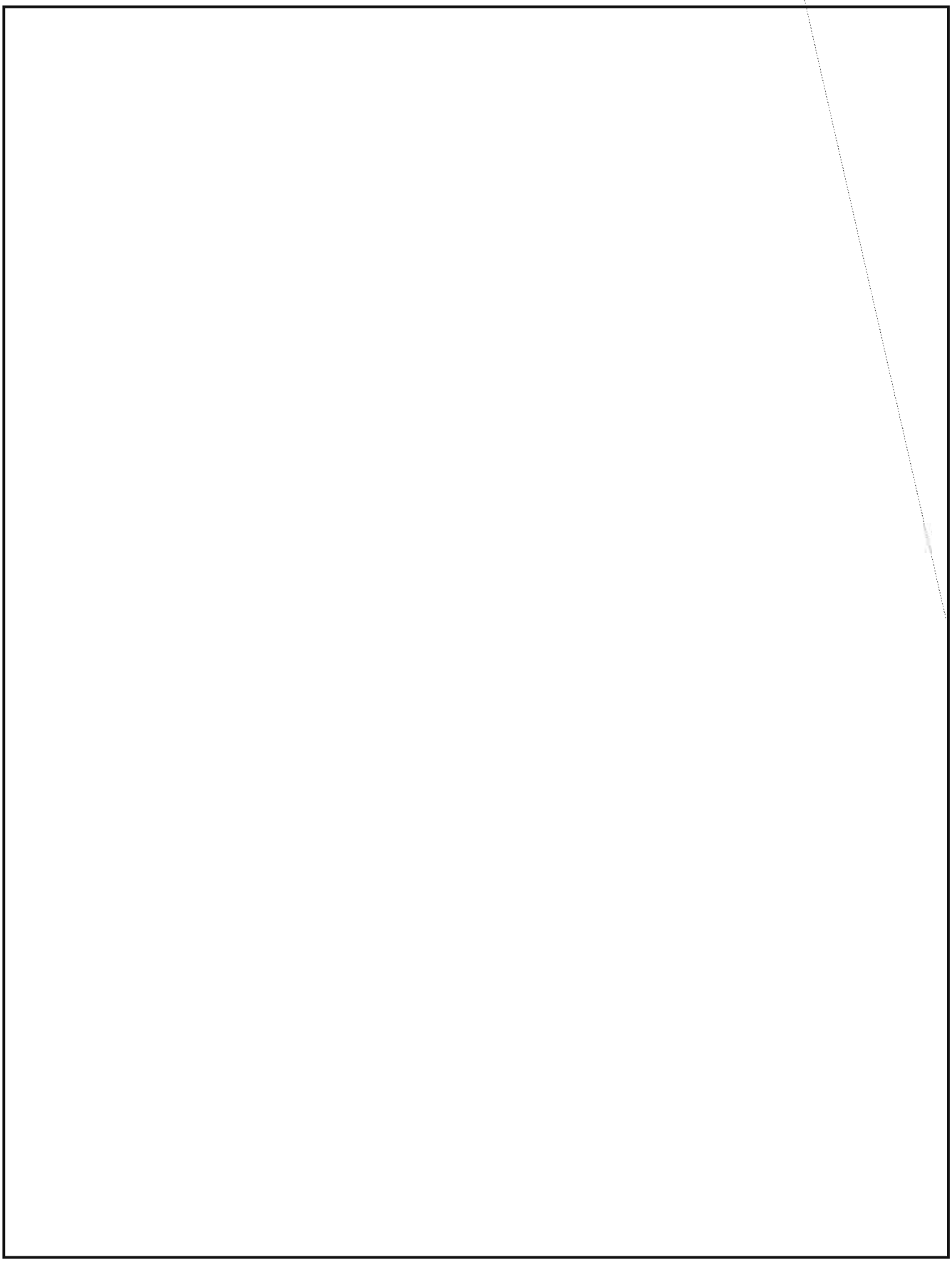
How good was intelligence support to DESERT STORM...

"In combat, everything starts and ends with intelligence." —Lt. Gen. Charles Horner

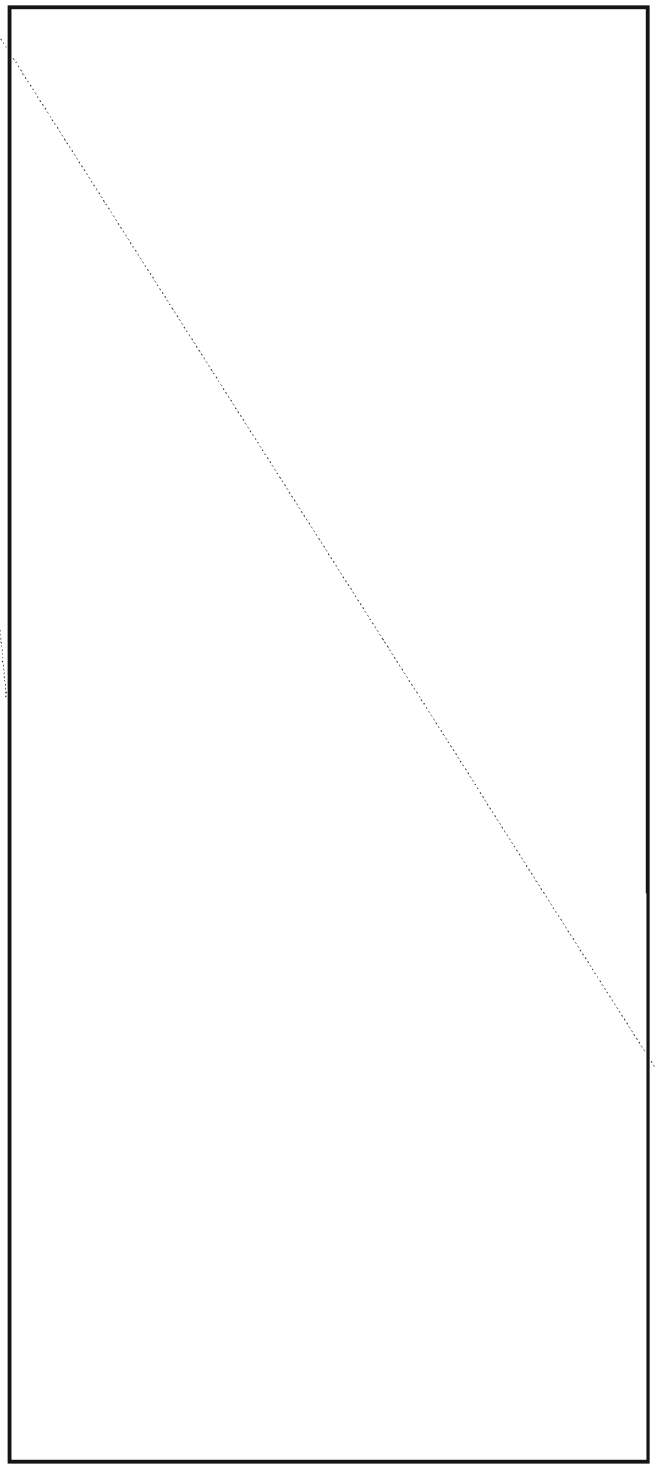
[redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)



EO 1.4.(c)
P.L. 86-36

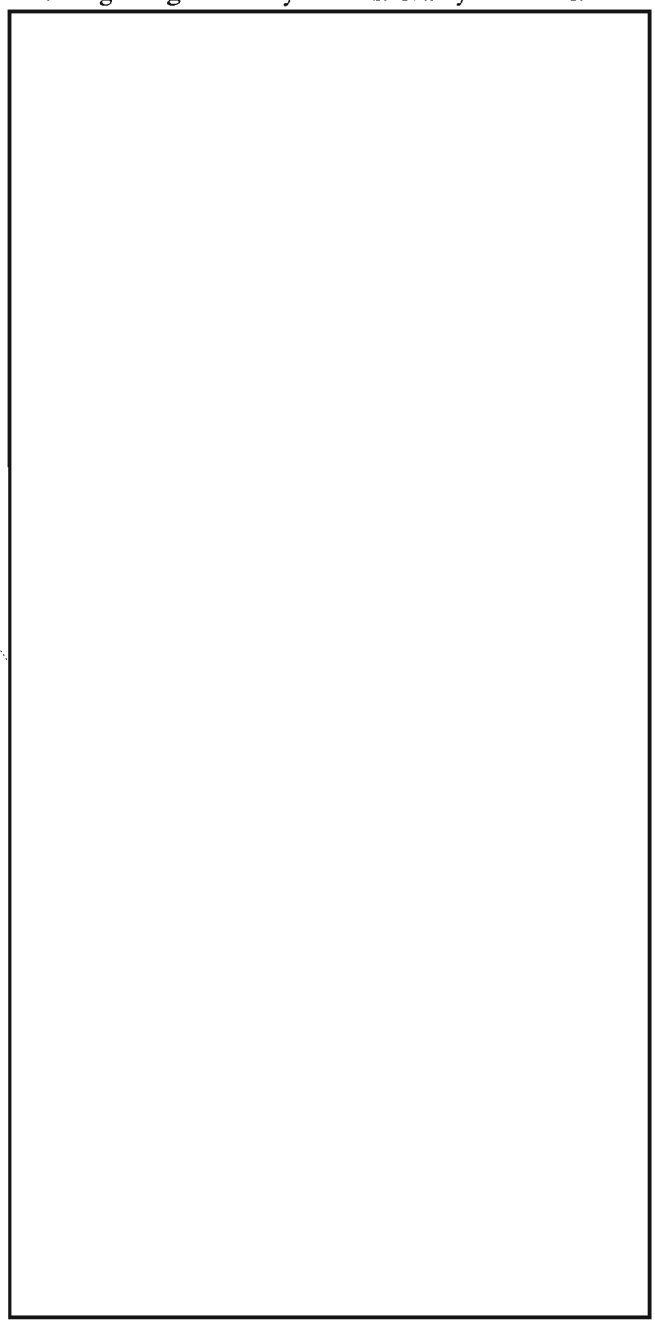


Information Warfare:

A New Business Line for NSA

by [redacted] G42 P.L. 86-36

~~(TS-CCO)~~ One of the new buzzwords in the hallways these days is Information Warfare (IW). IW is defined as the preservation of the integrity of our information systems from exploitation and corruption by potential adversaries while at the same time exploiting and degrading adversary information systems. At the



The author would like to thank [redacted] *of N53 for providing the videotape and slides of Col. Christon's presentation.*

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

(TS-CCO) Information Warfare promises to provide a new way of looking at familiar problems as well as a new set of tools for the war-fighter. NSA will be one of the main players in many future IW developments and our support will be critical to its future.

...and speaking of Information: is anyone going to GIS/LIS '94?

The Geographic Information Systems/Land Information Systems) Annual Conference and Exposition will be held in Phoenix, Arizona from 23-28 October 1994. This will be a multidisciplinary, educational, and scientific meeting designed to foster professional and intellectual interaction among individuals and groups interested in the design and use of GIS, LIS, and related specialties and technologies. The GIS/LIS '94 program will feature the latest ideas, research, and technological advances in GIS, LIS, AM/FM, infrastructure management, surveying, mapping, and related specialties from around the world.

For further information, please contact:

GIS/LIS '94:
5410 Grosvenor Lane, Suite 100
Bethesda, MD 20814-2122

or call: (301) 493-0200
or fax: (301) 493-8245

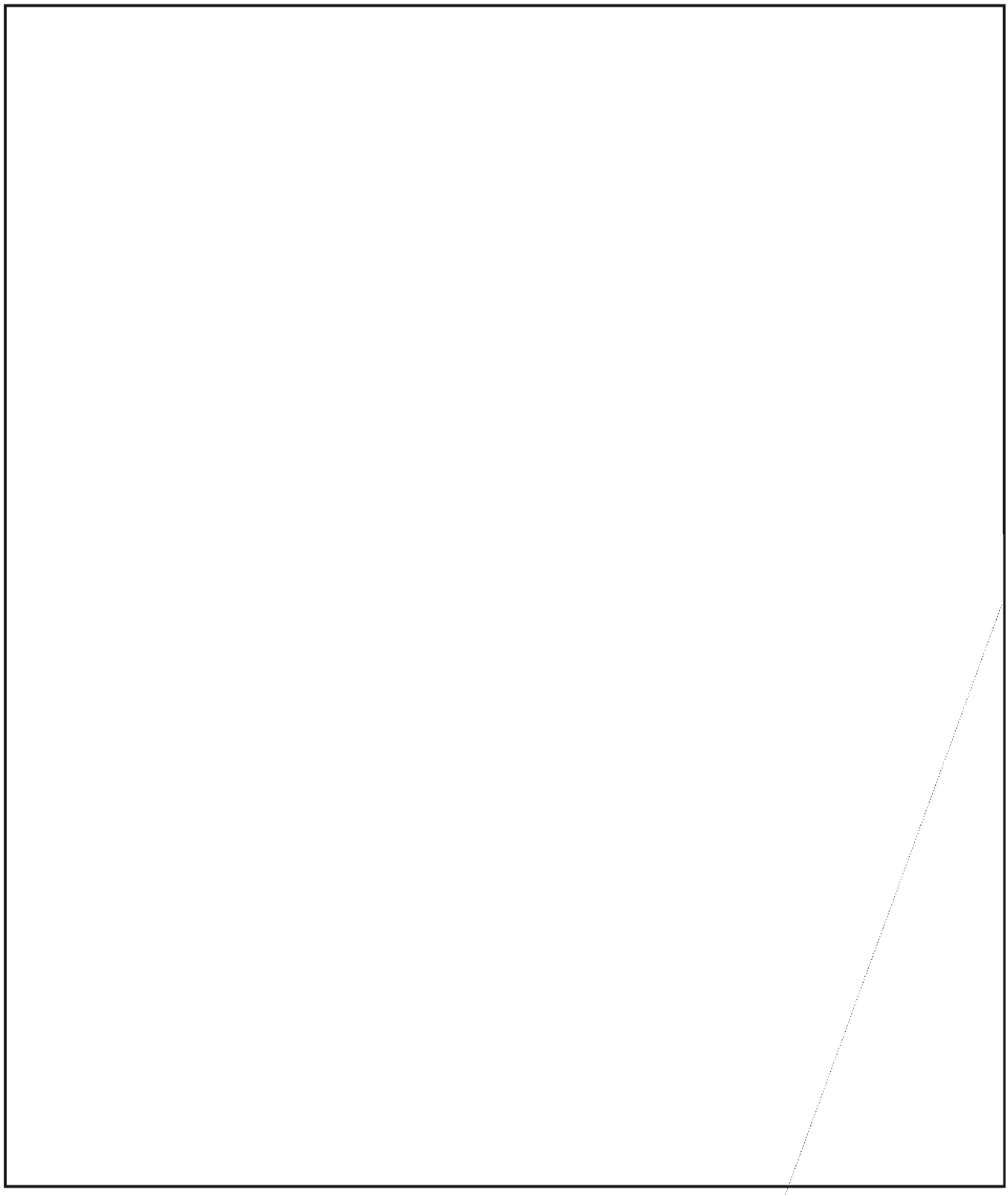
Please consider writing an article for Cryptolog if you attend this event!

EO 1.4.(c)
P.L. 86-36

Tour of Duty:

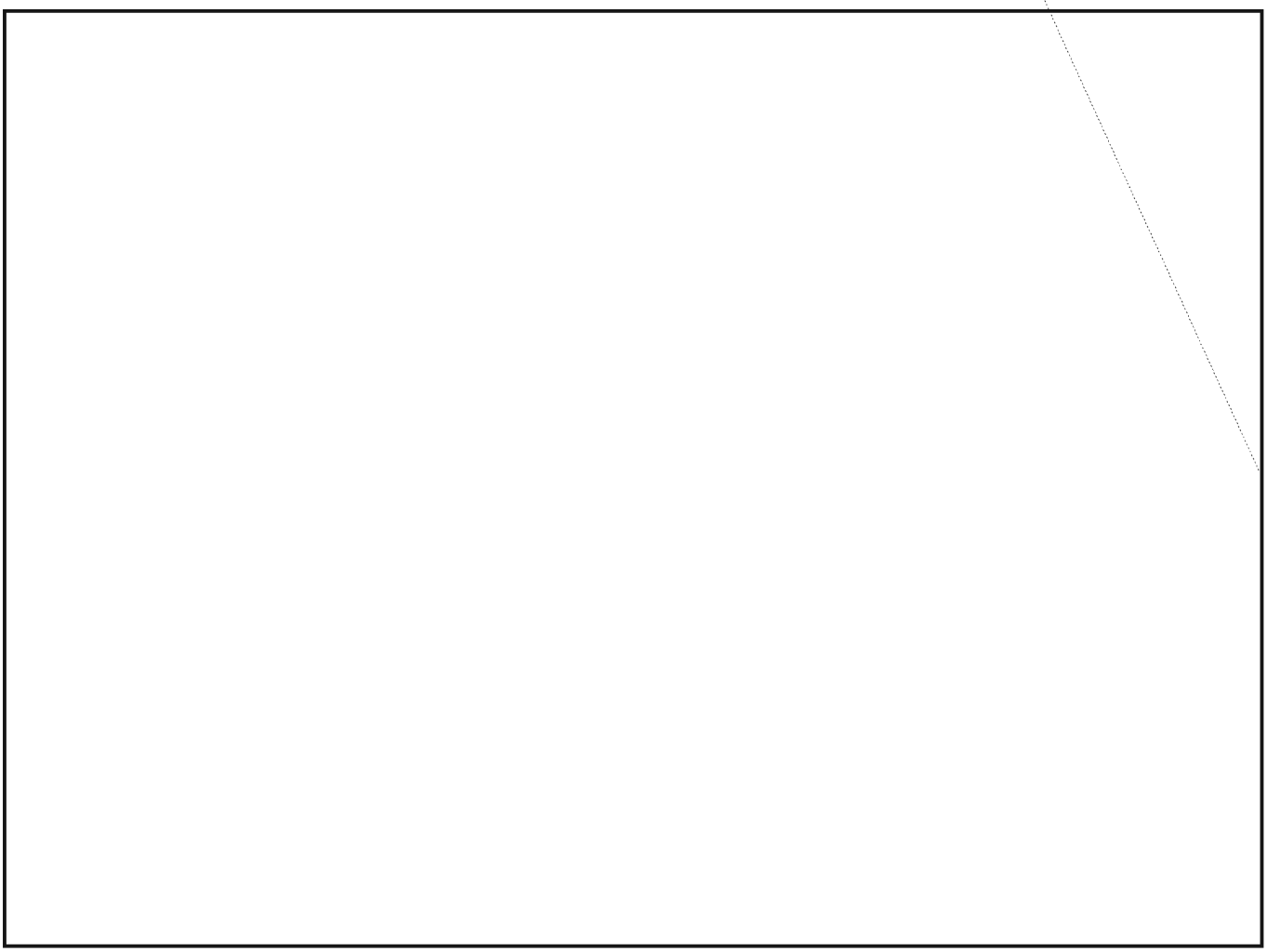
P.L. 86-36

by A05



EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



Target Development in the Field

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

by [redacted]

~~(C-CCO)~~ The purpose of this article is to discuss target development in the field and how it is different from target development as practiced by offices of primary interest (OPIs) at NSA Washington (NSAW). These differences are important for Headquarters analysts to understand, because their ability to work with field target developers will have a direct effect on the product they receive from the field. The ideas in this article are drawn from the author's experience [redacted] to discuss target development issues, and countless telephone and e-mail conversations with target developers around the world. While these thoughts are not universally applicable, they are valid, in varying degrees, for most large field sites.

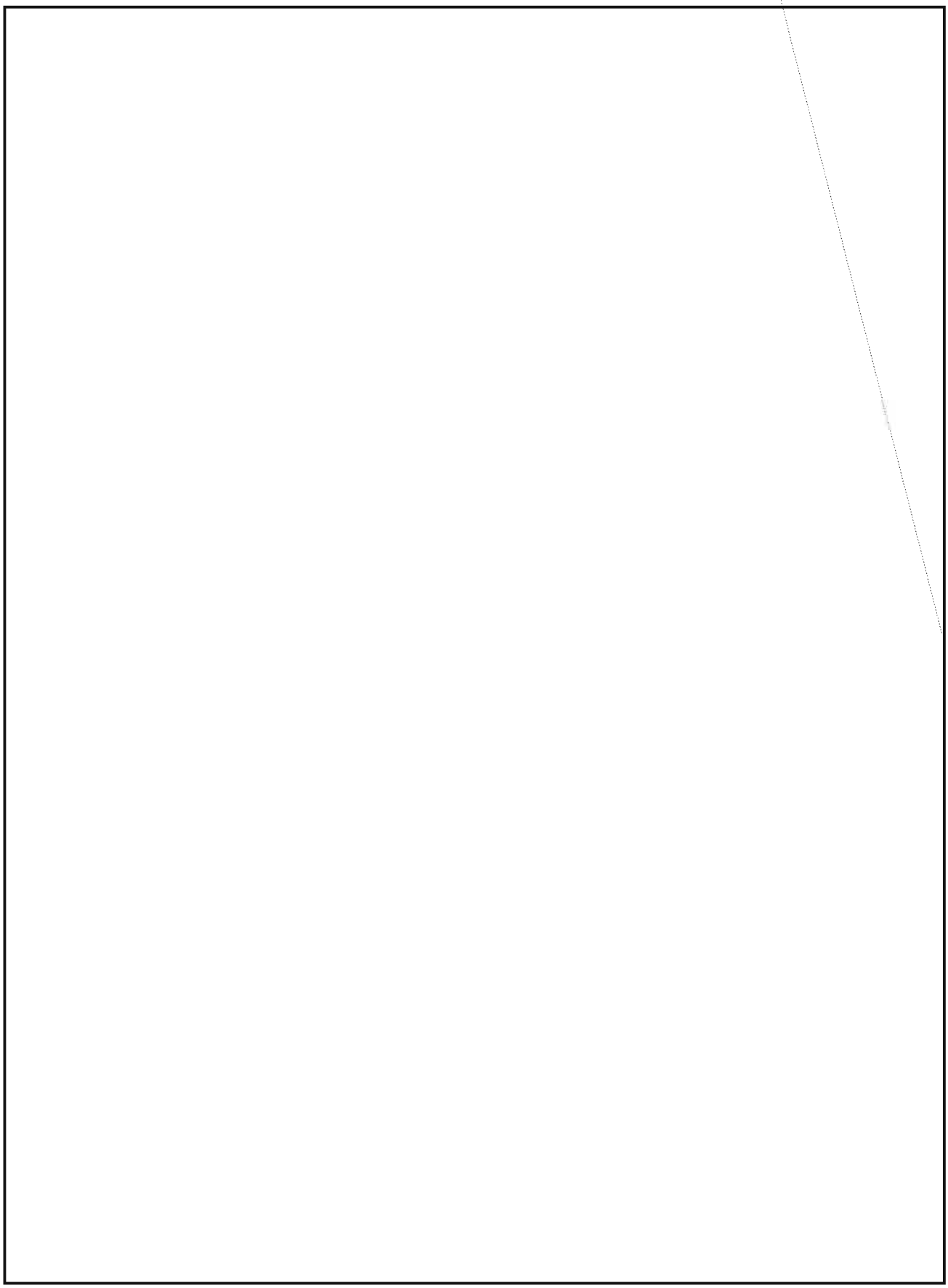
~~(C-CCO)~~ There are probably as many different definitions of target development as there are organizations doing it. One of the problems that arises in discussing the topic is figuring out what is meant by the phrase target development. Since it involves so many different types of activity, there are many different slants on its meaning. [redacted]

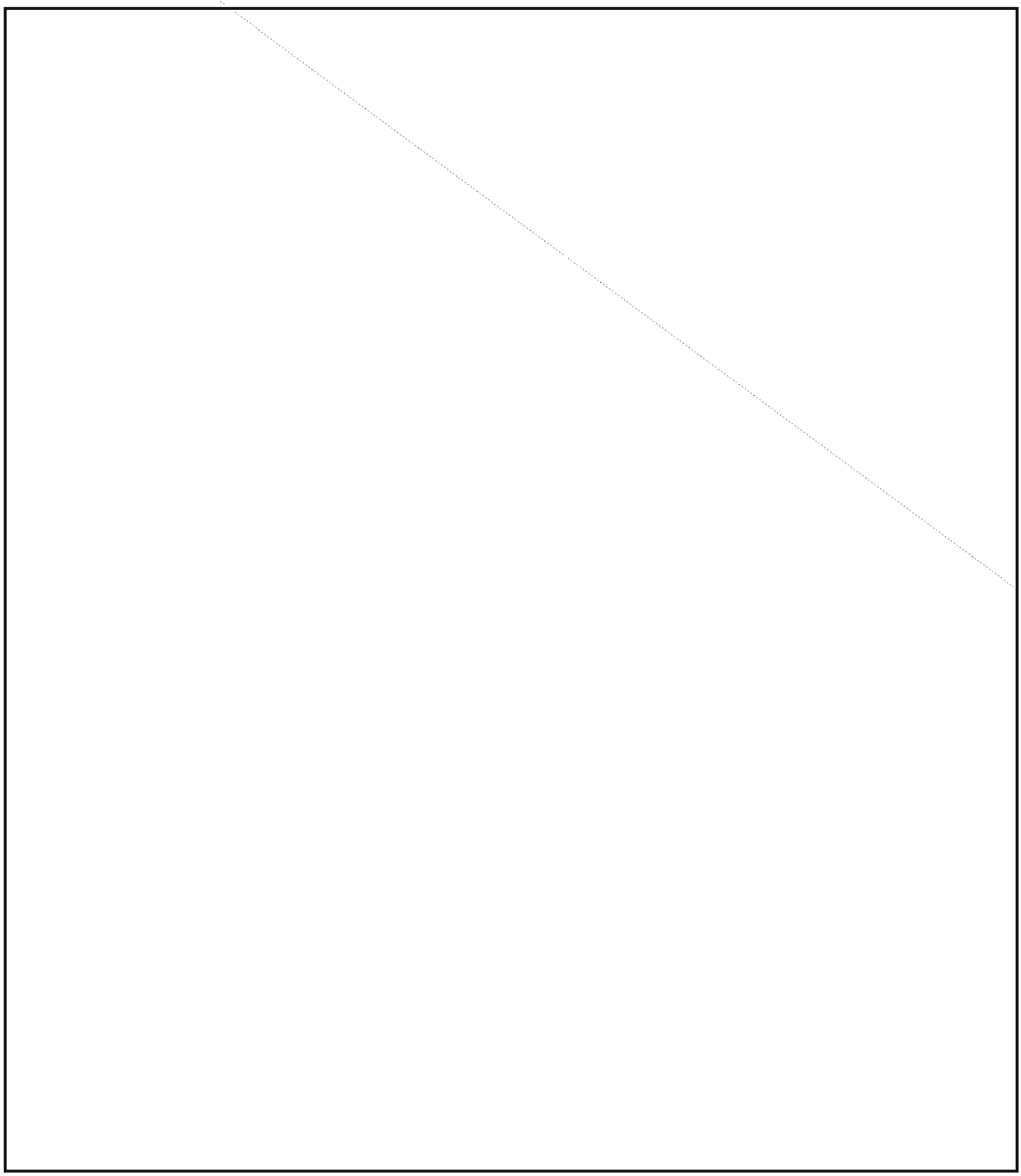
[redacted]

[redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



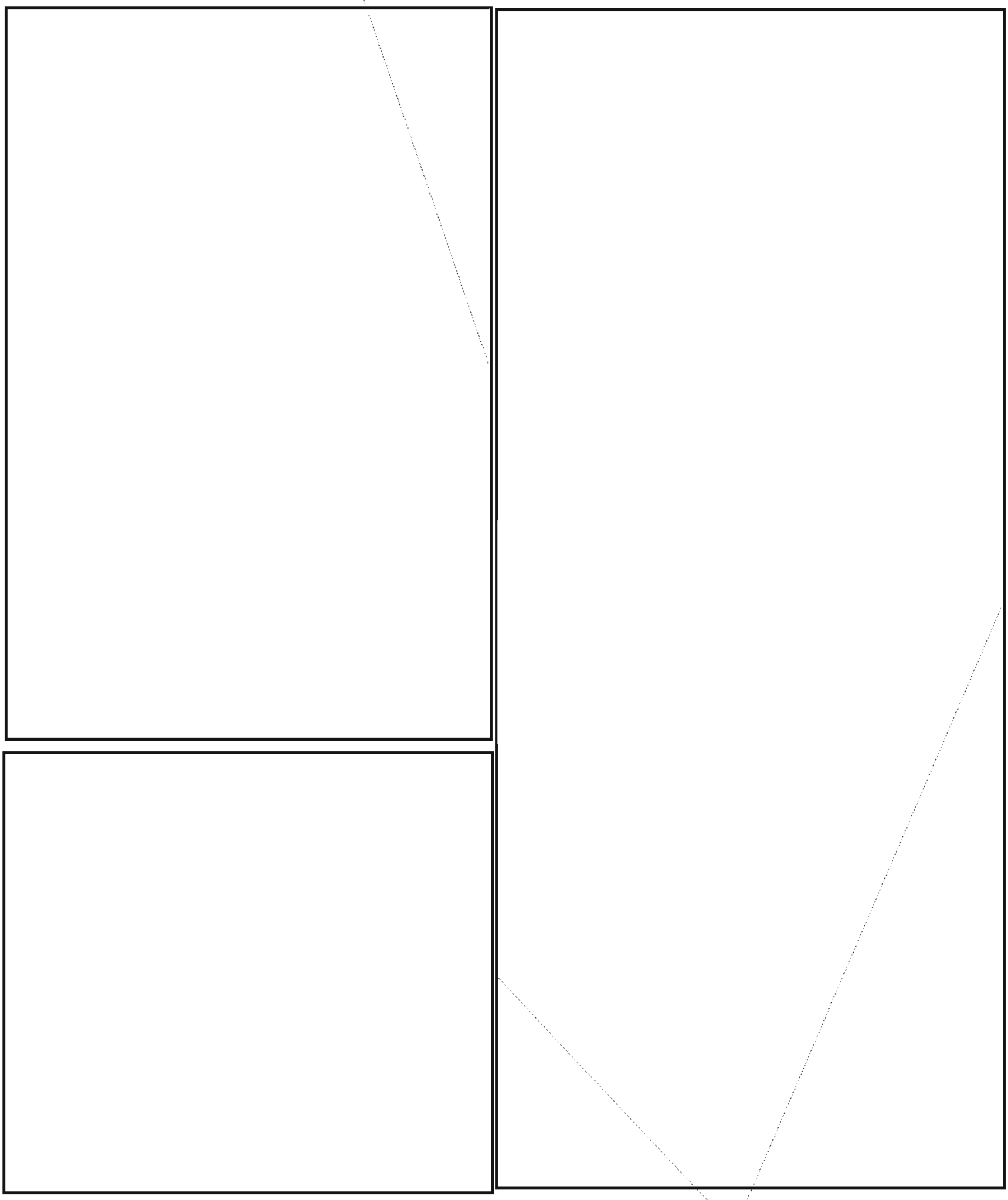


P.L. 86-36

Highlights from the Spring SRTD Conference

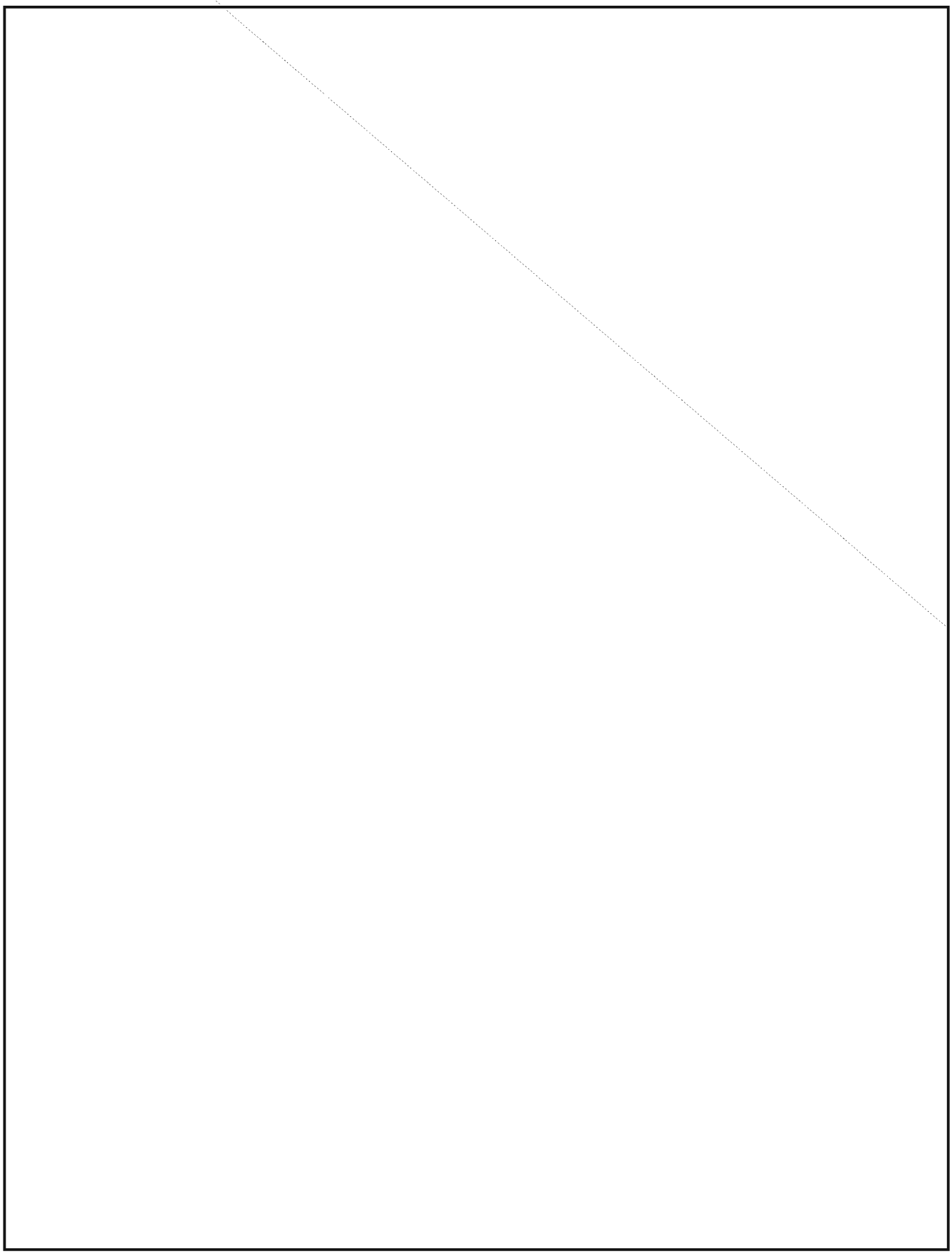
[redacted]

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

DOCID: 4009690
E.O. 13526-36
EO 1.4.(c)
EO 1.4.(d)



CRYPTOLOG
July 1994

P.L. 86-36

Publishing As A Member Of The Technical Track

by [redacted] Technical Director

THE PRIMAL NEED TO PUBLISH

~~(FOUO)~~ The Agency Technical Track Program offers its members an unprecedented opportunity to further their technical skills while growing professionally. Professional growth within the Technical Track is measured by technical accomplishment within three key areas: Performance Factors, Skill Development and Skill Field Contributions. Complete information on these areas can be found in Annex B of NSA/CSS Regulation 32-12, dated 20 August 1993.

~~(FOUO)~~ Within the area of Skill Field Contributions is a section which establishes the need for members of the Technical Track to publish their work as a vehicle for both technology transfer and career growth. It is upon this aspect of the Technical Track Program that this article focuses.

TECHNOLOGY TRANSFER

(U) What is Technology Transfer (T^2)? It has been defined many ways:

> ... the process by which technology, knowledge and information developed in one organization, one area, or for one purpose is applied or used in another organization, in another area or for another purpose ... U.S. Department of Energy (1990)

> ... providing on a timely basis technical information, and assistance in its application, in response to specific, user-identified needs ... J. Wycoff, *Journal of Technology Transfer* (1981)

> ... a purposive continuous effort to move technical devices, materials, methods and/or information from the point of discovery or development to new users ...J. Gilmore, "The Environment and the Action of Technology Transfer: 1970-1980" (1969)

(U) In general, T^2 may be considered as the overall process of moving technology from its point of origin to its point of need.

WHY DO *I* NEED TO PUBLISH SOMETHING?

(U) The simple answer is that it is now your responsibility as a member of, or an aspirant for, the NSA Technical Track Program. Technical Track members have a professional obligation to ensure that the transfer of technology happens. One of the best, and most long-lasting, ways to accomplish this is to simply share knowledge in written form. Having done this, many future opportunities may arise to expand upon that which has been shared. Such opportunities may be delivering papers at conferences and symposia, providing informational briefings based upon the written product, and/or authoring a sequel document to further enhance a good idea. The possibilities are virtually without limit.

BUT I'VE NEVER PUBLISHED ANYTHING BEFORE

(U) Ignorance is no excuse for the law! Sound familiar? Don't worry, the Technical Track police aren't going to "collar" you for simply not being aware of how to go about getting something published. If anything, you'll probably find so much help and assistance that you'll wonder why you ever had any hesitation about becoming an author in the first place. The main point is that you can, and will, find a wealth of resources to aid you in your personal quest to share your unique technical talents. Try asking a member of the Technical Track who has already published something and see how enthusiastic he/she will respond to your request for information. If we all follow the chain-letter principle (everyone tell two people—and they tell two people, etc.), we'll be knee-deep in "best sellers."

(U) Don't be bashful about asking for help. Remember, the Technical Track also means mentoring is alive and well.

OK, SO I WROTE IT - NOW WHAT?

(U) Now we're talking! The hard part is done. At this point, spend a few extra minutes reviewing your manuscript for both its technical content and attention to detail (spelling, grammar, punctuation, style, etc.). Don't forget to use the built-in power of document-processing software to assist you with the attention to detail part.

(U) It's always a good idea to have a few friends provide you with constructive feedback on your creation. Run it up the flagpole (as they say) and see who salutes. Synergy works and is a proven component of success. Don't be afraid to expose yourself to this peer review process; that's what the Technical Track is all about in the first place: people helping people.

WHERE CAN I PUBLISH MY ARTICLE?

(U) The places to publish are everywhere. Are there any journals which regularly come across your desk or to your computer screen? How about Newsletters and other local publications that you've seen? Most Agency technical societies solicit papers on an annual basis for essay contests; look for the announcements or contact one of the society's officers. How about an organizational technical report that carries a wide distribution? Career Panels and Technical Directors can also help point you in the right direction.

(U) Don't forget unclassified commercial publications which may be appropriate for your document. After an Agency publications review, you've got a whole world out there just waiting for your brilliance.

(U) As an aid to aspiring authors, the Appendix of this article lists a few places where you can get started with your publishing career, along with publishing criteria and initial points of contact.

CONCLUSION

(U) Publishing is simply a state of mind. Be positive about your technical contributions and look for opportunities to share them. Too many people have the misimpression that nobody will be interested in what they write about. At this Agency, nothing could be further from the truth. Everyone can make a significant contribution to the overall level of awareness of the Agency's population.

THE BOTTOM LINE

Publishing articles, reports and/or papers has a lot in common with driving a stick-shift vehicle. At first it takes a lot of effort, but over time, it simply becomes hard to imagine doing it any other way.

P.S. It's also a great feeling to see your name in print!

POTENTIAL PUBLICATION SOURCES

The DD Eye

Editors: [redacted] 972-2506
972-2666s
P.L. 86-36

Mission

~~(FOUO)~~ *The DD Eye* Newsletter is published monthly to disseminate information throughout the INFOSEC community. The primary focus of *The DD Eye* is to inform and motivate personnel, increase their knowledge, and improve their performance. *The DD Eye* contains information about Corporate philosophy, organizational missions, career and personnel matters, unique training opportunities and programs, and facilities. The newsletter allows individuals and organizations to share accomplishments with the ISSO work force.

Preferences

(U) Unclassified, short articles that are of interest to the entire work force. Can be technical, but should be written so that non-technical personnel can understand. Will accept classified articles, but they must be classified by the originator. Photos, diagrams, clip art, etc. are encouraged. The author should be identified.

Submitting Items

[redacted]

P.L. 86-36

P.L. 86-36

INFOSEC Technical Exchange

Publisher: [redacted] Y272, 972-2102s
Editor [redacted] Y221, 972-2406s

(U) The following guidelines should be used in writing an article for the *INFOSEC Technical Exchange*. These guidelines are intended to help a prospective author focus his/her efforts toward an article which meets the spirit of the *Exchange*. We invite all members of the INFOSEC Community to submit articles.

Topics

(U) Articles may address any topic which is of interest to a wide range of INFOSEC professionals. All articles should be:

(U) Relevant, topical, and contribute to the advancement of the INFOSEC Community.
(U) Timely, although historical articles may occasionally be used.
(U) May or may not be highly technical; however, if the topic is highly technical, pay particular attention to the CONTENT guidelines below.

Content

(U) All articles should be of a professional nature and serve as a technical resource for the INFOSEC Community.

(U) Articles may disseminate information on:

- R&D efforts,
- findings from general research,
- recent developments in policy which have a broad impact,
- new achievements in ongoing projects

(U) Articles may introduce a new project or program that needs support from or offers support to a wide range of organizations.

(U) Articles should interest a wide range of INFOSEC professionals.

(U) Articles should be written on a level that will allow all readers to understand the main ideas presented. It is expected that there will be some cases in which highly technical details are essential for a complete article. This is acceptable, as long as comprehension does not depend on a clear understanding of the technical details. In general, technical complexity should be considered the exception rather than the rule.

(U) Classification

(U) The *Exchange* will accept and print articles up to the TOP SECRET level. Each paragraph in a classified document should be properly marked with its classification level (U, C, S, TS).

(U) The *Exchange* is distributed to the branch level in the ISSO and is widely available to NSA employees and others with appropriate clearances for U.S. classified information. Protection of caveated or compartmented information cannot be supported.

Length

(U) Articles should be from one to ten pages long, including any relevant graphs, charts, diagrams, or schematics. If an article is longer than ten pages, the author may contact the publisher of the *Technical Exchange*, for a discussion or advice.

Format

~~(FOUO)~~ FrameMaker format is preferred. J334 has a conversion service that converts Interleaf, Word Perfect, Office Writer and MS Word into FrameMaker. Just attach the document to an E-Mail Compose Window addressed to **convert@po**. In the message window, type:

```
Target: FRAME
```

Send it. The document will be converted and returned to you.

(U) Classify all paragraphs.
(U) Do not double-space between lines.
(U) Do not type your article in capital letters.
(U) Include your name, organization, building, and phone number.
(U) Do not type your article in multi-columns.

Submitting Items

(U) All articles must be reviewed and approved by the writer's organization.

(U) All articles must be approved for publication in the *INFOSEC Technical Exchange* by the Publisher and member(s) of the Selection Panel, who reserve the right to edit, abridge, or refuse to publish an article.

[redacted]

P.L. 86-36

NSA Cryptolog

Publisher: William M. Nolte, P054, 963-3123
Editor: [redacted] P054, 963-3123s

Preferences

(U) Classified, technically-oriented articles with emphasis on improving NSA's technical performance; should be aimed at explaining one's discipline to those outside it. Readers are also invited to contribute conference reports and reviews of books, articles, software, and hardware that pertain to our missions or to any of our disciplines. Humor is welcome, too. Submissions may be published anonymously, but the identity of the author must be known to the editor.

Submitting Items

P.L. 86-36

~~(FOUO)~~ Send a hard copy accompanied by a labelled diskette to the editor at P054 in 2E062, Ops. 1, or [redacted]

Guidance

- Do not type your article in capital letters.
- Classify all paragraphs.
- Label all diskettes, identifying hardware (OS: DOS, UNIX), density and type of word processor used.
- Put your name, organization, building and phone number on diskettes.
- FrameMaker format is preferred; ASCII is also fine. J334 has a conversion service that converts Interleaf, Word Perfect, OfficeWriter and MS Word into FrameMaker. Just attach the document to an E-Mail Compose Window addressed to **convert@po**.

Information Categories

Collection
Cryptanalysis
Cryptolinguistics
Information Resources
Information Security
Intelligence Analysis
Intelligence Community
Linguistics
Mathematics
Research & Engineering
Science & Technology
Traffic Analysis

Virtual Campus (VC) Advances

Editor: [redacted] Y471, 972-2355s

P.L. 86-36

Mission

~~(FOUO)~~ *VC Advances* is published bi-monthly to promote and publicize Virtual Campus (VC) throughout the Information Systems Security Organization (ISSO). *VC Advances* contains information about Virtual Campus goals and objectives; helpful hints and tips for new VC users; updates on new products and changes; and technical information for our more technically oriented readers. This newsletter gives the ISSO workforce an opportunity to learn about what is coming, voice their concerns, and contribute their expertise.

Preferences

(U) Unclassified, short articles that are of interest to the entire DDI work force. It is preferred that technical articles be written so that non-technical personnel can understand, but that is negotiable, depending on content. (Articles containing important technical information that could benefit at least a part of the work force have been accepted and well-received.) Photos cannot be accepted, but diagrams, clip art, etc. are welcome. Questions and ideas that could lead to articles are also encouraged. The author should be identified.

Submitting Items

[redacted]

P.L. 86-36

Cryptologic Quarterly

Publisher: Center for Cryptologic History
Executive Editor: Barry Carleen, E324, 968-6558s
Managing Editor: [redacted] E324, 968-6558s

Mission

~~(FOUO)~~ The goal of *Cryptologic Quarterly* is to educate the work force in both narrow technical elements of the cryptologic effort and the broad issues that affect that effort.

Preferences

(U) Articles for *Cryptologic Quarterly* may be written on any theoretical, doctrinal, operational, managerial, or historical aspect of cryptology. The criterion for publication is whether or not the article is of sufficient substance and interest to make a genuine contribution to cryptologic literature. The decision to publish a submitted article rests entirely with the management of *Cryptologic Quarterly.* The author should be identified.

Submitting Items

~~(FOUO)~~ Contributions should be submitted to [redacted] Managing Editor, *Cryptologic Quarterly*, E324, [redacted] 968-6158s.

(U) Manuscripts should be accompanied by an abstract and should be typed double-spaced with generous margins. Two copies are required; a third copy should be retained by the author. Illustrations should be submitted with the manuscript and should be adequately identified. If your manuscript was prepared on a desktop computer/word processor, please submit a disk with the following information: the type of equipment, the operating system, and the word-processing software that you used. All material used in the publication of an article is destroyed when no longer needed unless the author requests that it be returned.

P.L. 86-36

OPSEC In The Post-Cold War Era

P.L. 86-36

by [redacted] 2

(U) As the world settles into the post-Cold War period, the government of the United States finds itself in the awkward position of having no easily identifiable "enemy" at which to point a finger. The threat to our national security, or at least the way we perceive it, has undergone radical changes, yet these changes have only just begun.

(U) To compound the difficult situation faced by our government, we are also in the grip of a budget crisis. Every dollar spent is being carefully scrutinized, with an eye towards "return;" if there is no identifiable benefit from the expenditure of funds on a particular initiative, then the funds will probably be invested elsewhere. Within the Intelligence Community, the "traditional security" measures that have been ritualistically adhered to under the specter of the Soviet Threat have begun to come under question. The question that is being asked, and rightly, is "What is the return on my investment of security dollars?"

(U) In understanding the new concern about the effectiveness of security measures, a word needs to be said about the changing nature of the threat to the Nation's secrets. In the past, there were scores of identifiable cases of espionage. At the height of the Cold War, the Soviet bloc countries had perfected a staggering array of espionage techniques that would enable them to access the guarded secrets of the United States and its western allies. These techniques included sophisticated electronic eavesdropping operations, massive SIGINT and IMINT collection efforts, and the most formidable HUMINT collection network in the world. All of these threats have undergone radical change in the last few years (to say they no longer exist, however, would be a grave error), but the most noticeable change has been in the area of HUMINT operations.

(U) At the height of the Cold War, the Soviets were effectively operating a "closed society," for which we had to develop our own methods of penetration. The United States attempted to make collection of information equally difficult for the Soviets by blanket classification of any and all information dealing with the national security. The Soviets responded with the intelligence collection assets mentioned above, with a particular emphasis on HUMINT. They seemed to like

HUMINT collection, and they were good at it, perfecting a seemingly endless array of techniques for surreptitious entry, penetration of security containers, access to restricted areas, co-opting of trusted employees, illegal agent operations, and other means of "sneaking around." To make matters worse, at least in the mid-1980s, there seemed to be a fairly large number of Americans who were seeking out the Soviets or any other foreign government to which they could voluntarily provide sensitive or classified information. From what we were able to discern at the time, it was apparent that investments in "traditional security," i.e. safes, locks, fences, guards, badges, strict classification policies, TEMPEST countermeasures, etc., were money well spent.

(U) Today, however, we find ourselves dutifully adhering to security policies and procedures that were effective and prudent during the Cold War, but whose effectiveness has been reduced or eliminated. Blind adherence to these policies at times may even impede mission effectiveness, and the justification to continue to spend money on these measures is increasingly difficult to accept. The reason is that many of these security measures are no longer protecting our information. Our adversaries have found that there are more economical

The dawn of the "information Age"....has changed the concept of protection of information...we can no longer "protect it all."

ways of obtaining information that do not involve "sneaking around;" instead, they need only sit down at a computer terminal, visit a library, or submit a request for (unclassified) information to the Federal Government. These methods, unthinkable in the Cold War world of 15 years ago, have been made possible by another phenomenon—the dawn of the so-called "Information Age."

(U) Within the last 10 years, technology advances have changed the way in which we view information. We now literally have the world at our fingertips, with access to worldwide networks and databases that contain virtually every piece of information available. This has also changed the concept of protection of information. What we once protected easily by lock and key is now being transmitted worldwide at the speed of light. This has led us to the realization that we can no longer protect it all. Instead, we need to determine what the truly critical pieces of information are and develop a carefully orchestrated strategy for their protection. The means by which we identify, and subsequently protect, this information forms the discipline of operations security, or OPSEC.

(U) OPSEC is a five-part process (and I say "five-part" rather than the more familiar "five-step" to avoid the suggestion that the five parts occur in a particular sequence). These five parts are:

- **identification** of critical information
- assessment of **vulnerabilities** associated with that information
- assessment of **threats** to that information
- assessment of the risk that the information will be **compromised**
- implementation of **countermeasures** to prevent compromise of the critical information

(U) OPSEC is an analysis of the flow of information, from an adversarial perspective, and the informed application of countermeasures based on that analysis.

(U) In today's world of budget constraints, the risk analysis phase takes on particular significance. Risk analysis means assessing the probability that a particular source of information will be successfully exploited by an adversary. For example, if a determination is made that a vulnerability exists for a particular item of information, but there is no demonstrated threat to exploit that vulnerability, then the overall risk is low. A similarly low risk factor would be assigned to information to which a known threat was posed, but with which no vulnerability was associated. In other words, the expenditure of significant funds to protect that information would not be justified. Also critical to the risk analysis phase is the concept of "value of information." The cost of protecting the information in question should not exceed the intelligence value of that information. It is in this way that OPSEC can be seen as an effective cost-saving tool; it identifies the areas in which limited security resources can be put to their best use. OPSEC can identify areas in which existing, and sometimes costly, security measures are not effectively protecting the information they were intended to protect, and can free up those resources to be applied in another area where they will have a greater effect.

(U) This is not to say, however, that the risk analysis phase is the only one of importance. When seeking to protect information, the critical step that is often overlooked is the identification of exactly what needs protection. Adherence to the OPSEC framework forces an

identification of that critical information. In today's environment of information exchange, it is simply not possible to protect all information that is associated with a particular program or initiative. Instead, that information which is absolutely critical to the success of a program (the "golden nuggets") must be identified and protected. Along with the identification of exactly what information is critical, a realistic assessment should be made of what, if any, information has already been compromised, or can reasonably be assumed to be known or available in the public domain. *We are currently spending enormous sums of money "protecting" information that has been publicly known for many years.*

(U) In identifying the threat to a particular piece of information, we should be careful not to rely on Cold War threat assessments of what an adversary "could" or "might" ascertain, or what his "probable" or "possible" capabilities are. In today's tight financial times, funds will be increasingly allocated toward defending against demonstrated, rather than postulated, threats. If there is a reasonably good indication that there is a threat to critical information, then countermeasures should be applied to that threat. We can no longer afford, however, to defend against threats that have never been demonstrated. We also need to assess the likelihood of a particular threat. Would an adversary mount a sophisticated, expensive, high-risk SIGINT operation against a particular target if he could get the same information from Nexis-Lexis or a similar database? In most instances, the answer would be no.

(U) The assessment of vulnerabilities that could reveal critical information is an equally important part of the OPSEC process. It may be that existing security measures are adequately protecting critical information, but it is this phase of the OPSEC process that will result in that determination. By reconstructing the flow of information into, through, and out of an organization or project, the OPSEC analyst can identify the vulnerabilities of the critical information independently of security measures that are already in place. It will immediately become apparent whether or not the existing security measures are, in fact, protecting the information in question.

(U) The culmination of the OPSEC process is the identification and application of countermeasures. It is in this area that OPSEC often stands alone as the economical alternative to more traditional (and often costly) security measures, because OPSEC countermeasures are frequently simple administrative changes. These changes can range in scope from the development of a deception plan, to the omission of a few items of information from a shipping label, to the decision not to release a particular item to a local newspaper. OPSEC involves an assessment of existing resources, followed by a subsequent plan of re-aligning these resources to provide the maximum protection for the identified critical information. Occasionally, OPSEC countermeasures will include additional changes that do have a cost associated with them, such as the provision of secure communications equipment, but this is not usually the case.

(U) Viewed in this way, it becomes apparent that **OPSEC can be a valuable tool for cutting costs without sacrificing protection**. By identifying the information that really needs to be protected, OPSEC ensures that this information is safeguarded by relevant countermeasures while eliminating unnecessary and often costly security measures that are oriented toward an undocumented or unlikely threat. Furthermore, if OPSEC is employed throughout the entire life-cycle of a program or system, as it should always be, it can provide further savings in the form of dollars that will not need to be spent re-developing or replacing a system or program that has been compromised even before it is fielded. The intention is not to imply that, in embracing OPSEC, we should throw existing security measures out the window. However, in practicing OPSEC consistently, we can determine which security measures are effective and which ones are not, and in the long run ensure that the dollars we spend on security are doing the most toward protecting our truly critical information.

A Linguist's Look at the Internet

P.L. 86-36

by [redacted]

~~(S)~~ Open-source information (OSI) has grown to enormous proportions in recent years. Communicating electronically has become simple and cheap and, as a result, global information access has virtually exploded. We may be reaching the point where it's impossible to track systems, let alone users of systems. Where in the past OSI was given little attention or even disregarded, today its intelligence potential has grown dramatically. It is being turned to more and more to fill gaps in analysis, to validate intelligence assessments, even to interpret SIGINT and to direct SIGINT tasking. The shift in priority from military to civil targets in particular has placed much reliance on OSI to increase understanding of political, economic, and scientific targets and to keep up with events in those areas. The Intelligence Community has recognized the importance of OSI and the need for a broad-based OS program. As a result, NSA may soon be playing a significant role in the acquisition and exploitation of OSI.

P.L. 86-36

(U) Probably the single largest window into the world of Open Source is the *Internet*. For the past six months, my colleague [redacted] and I have been accessing the Internet in search of information, tools, and applications primarily in support of A Group linguists. This article is meant to familiarize linguists with the Internet as a source of unique and timely collateral information. It also describes Internet resources of particular interest to linguists but is not intended as a general guide to the Internet. For some points of orientation I have borrowed from existing literature. For a more complete orientation to using the Internet and for more detailed descriptions of Internet resources, a list of references follows this article.

(U) The A Group Language Technology Center's (ALTC) use of the Internet has been in three general areas:

[redacted]

This paper will describe what we've found in each of these areas which we consider of interest to language analysts. Included are sample snippets from messages and documents which we've encountered as well as listings we've compiled of useful resources. We must emphasize that we've only scratched the surface of what the Internet has to offer. The information presented here reflects only six months of "navigating the Net" and is only meant to give a glimpse of the potential of the Internet as a rich source of useful OS information.

I. The Networks

What is an "internet"?

(U) An "internet" is a computer network which allows computers with differing software and hardware to communicate by translating messages to a common *communications protocol.* The first real internet, the ARPANET, was a wide-area experimental network in the mid-1980's which arose from research supported by the Advanced Research Projects Agency (ARPA), now DARPA, Defense Advanced Research Projects Agency. The ARPANET connected terminal hosts and servers together and, as local-area networks grew, many hosts became gateways to other local networks. A network layer to allow interoperation of these networks was developed and called IP (Internet Protocol). Over time, other groups (NASA, NSF, states, etc.) created long-haul IP-based networks. The collection of all these interoperating networks, a world-wide network or networks, is what has come to be called "The Internet."

(U) Allowing simple PCs and sophisticated mainframes to interconnect, the Internet can be used for an extraordinary range of purposes: long-distance collaborations, transfer of programs and documents between remote computers, accessing library catalogs, logging into supercomputers...the list gets longer every day.

(U) The Internet has become so immense and complex that there probably isn't a single person who understands everything about it. It now comprises thousands of networks and hundreds of thousands of connected computers, serving millions of users. More users and services are added every day, making mailing lists, resource guides, etc., out of date almost as soon as they are generated. Despite its enormity and complexity, however, the Internet global village operates under certain common conventions and standards[1], even a certain global "netiquette." Once one has mastered a few basic skills, using the Internet is actually very easy.

1. RFCs (Requests for Comment) are documents which form the system of standards adhered to on the Internet.

P.L. 86-36

(U) Before we go any further, we need to define the following essential terms.

Internet:	Simply put, the Internet is a large "network of networks." There is no one network known as the Internet; rather, regional networks are connected into one great living thing, communicating at tremendous speeds with the TCP/IP protocol. All activity takes place in real time.
UUCP:	the UUCP network is a loose association of systems all communicating with the UUCP (Unix-to-Unix Copy Program) protocol. It's based on two systems connecting to each other at specified intervals (a process called polling), and executing any work scheduled for either of them.
BITNET:	The "Because It's Time Network" consists of systems connected by point-to-point links, all running the NJE protocol. Mail gateways are in place to reach users on other networks.

(U) These networks are linked in a variety of ways:

1) dedicated telephone lines with 56Kbps connections,
2) special phone lines with 1Mbps connections,
3) special backbone links which can carry a massive 45Mbps load of traffic.

These links are paid for by each participating institution to a local carrier (e.g., Bell Atlantic owns PrepNet, the main provider in Pennsylvania). Also available are special connections which carry Internet traffic (packets) over high-speed modems.

(U) UUCP links (whose connections are of the store-and-forward variety described above) are made mostly via modem. Also in use are Internet-based UUCP links. Using TCP/IP connections, these links provide some blindingly fast "hops," allowing one to communicate cross-country or around the world for the price of a local phone call.

II. Electronic mail:

(U) Electronic mail (e-mail) is the most common form of communication in computer networking. It allows people to write back and forth without having to worry about how messages actually get delivered. Most Agency users are familiar with e-mail addressing and mail-system protocols, so we won't go into detail here.[1] The same **user@somewhere.domain** convention is used on the Internet; every machine connected has a unique IP address or *dotted quad* (e.g. **147.31.254.103**). The trailing domain is often one of the following:

com	**company or commercial institution**
edu	**educational institution**
gov	**government organization**
mil	**military organization**
net	**administrative host for a network**
org	**private organization**

Each country, in addition, has its own top-level domain (**.au**= Australia, **.ca** = Canada, etc.)

(U) Mail messages also have a specific structure that's common across every type of computer system:

```
From:  clinton@hq.mil Sat Feb 27 17:06:01 1993
Received: from hq.mil by house.gov with SMTP
   AA21901 (4.1/SMI for al@house.gov); Sat,
   Feb 27 93 17:05:56 -0400
Date:  Sat, 27 Feb 93 17:05:56 -0400
From:  The President <clinton@hq.mil>
Message-Id:  <9105252105066318hq.mil>
To:  al@senate.gov
Subject:  Meeting

<Text>
```

Note that the first **From:** and **Received:** lines give the "real" address that the mail is coming from (as opposed to the address to which you should reply, which may look very different) and what places the mail went through to get to you. If a message is sent using UUCP there will be a **Received:** line for each system that the mail passed through (unless the mail program filters them out). The second **From:** contains the address to which you would reply as opposed to the address from which the mail was sent..

1. The basic format of an electronic mail message on the Internet is defined in RFC0822. For more information on e-mail, see *!%@:: A Directory of Electronic Mail Addressing and Networks*, Donnalyn Frey and Rick Adams, pub. O'Reilly & Associates, Newton, MA, 1989.

(U) The e-mail one encounters on the Internet is either that routed via a discussion list or a newsgroup (explained later). The header of a typical e-mail message passed over the Russian Electronic Communications network (RELCOM, sort of the Russian equivalent of our PRODIGY service) would look like the following (after converting the Cyrillic for proper display):

```
From newcom.kiae.su!L-relcom@newcom.kiae.su Sun
        Feb 28 08:50:28 1993
Return-path:  <newcom.kiae.su!L-
        relcom@newcom.kiae.su>
Received:  from techno.fuug.fi by
        afterlife.nscs.mil (4.1/SMI-4.1)
        id AA19408; Sun eb 28 08:50:22 EST
Received: from newcom.kiae.su by techno.fuug.fi
        with UUCP id AA10887
        (5.65c/IDA-1.4.4); Sun 28 Feb 1993
        15:27:56 +0200
Received: by newcom.kiae.su; Sun 28 Feb 93
        15:32:12 +0300
To:  subscribers@techno.fuug.fi
Newsgroups:  relcom.bbs
From:  Alex Popov <alex@mechta.mak.su>
Subject:  [News] BBS na Iskre II
Date:  Fri, 26 Feb 93 20:55:28 +0300
Organization:  A&B Net (A&B_Net_gate)
X-Gate:  UU2 1.13b
Sender:  L-relcom@newcom.kiae.su
X-Class:  Big/nPrecedence:junk
Status:  RO
```

This is a message uploaded to a newsgroup (**relcom.bbs**) announcing a new **A&B Net** BBS being set up at **Iskra II** (International). **Newcom** is the news server for the RELCOM network based at **kiae** (Kurchatov Institute of Atomic Energy). Note that this message has been relayed through a European Internet node in Finland (**.fi**). Note also the exclamation point in the address (**newcom.kiae.su!...**). E-mail addresses usually appear in one of two formats: an "at" sign (**@**) for the Internet format or a "bang" (**!**) for the UUCP format. In addition, a percent sign (**%**) often acts as an extra routing method indicating a specific gateway to another network:

user%site.bitnet@bitnet-gateway

For example:

ukraine%indycms.bitnet@pucc.princeton.edu

is the Internet address for recipients of the BITNET discussion UKRAINE. This list is moderated from a host at Princeton University (**pucc**) via the BITNET node **indycms**.

UUCP Maps

(U) The UUCP Mapping Project at Rutgers University is an attempt to manage the growing number of UUCP hosts. UUCP "maps" allow mail routers within UUCP to work properly. The map for a domain is processed by a program called **pathalias** which generates UUCP routes from the data. The map data is in the following format:

```
#N          UUCP name of site
#S          manufacturer machine model; OS &
             version
#O          organization name
#C          contact person's name
#E          contact person's electronic mail
             address
#T          contact person's telephone number
#P          organization's address
#L          latitude/longitude
#R          remarks
#U          netnews neighbors
#W          who last edited the entry; date
             edited
sitename    .domain
sitename    remote1 (freq), remote2 (freq),
             remote3 (freq)
```

The UUCP map for Russia (domain name **.su**), thus essentially contains a database of information about Russian e-mail subscribers to the Internet. For example:

```
#N          ihep.su
#S          VAX-11; ULTRIX
#O          Institute for High Energy Physics
#C          Leonid Yegoshin
#E          egoshin@ihep.su
#T          +7 (Serpukhov) 42952
#P          IHEP, Serpukhov SU-142284 Moscow
             District, Russia
#L          37 10 E / 54 55
#R          The main relay server of local nets
             on the territory of IHEP
#W          egoshin@serp.ihep.su 910215,
             any@hq.demos.su 910708
```

The **ihep.su** server connects other users listed in the map, such as **serp.ihep.su**, which happens to be an IBM PC/AT running XENIX. It's easy to see how useful these maps can be in tracking systems, users of systems, and organizations. UUCP maps are available by *anonymous ftp* (explained below) from **ftp.uu.net** in subdirectory **uumap**. The map for Russia (actually ex-USSR) is in files **u.sun.0,1,2,3,4,100**. A separate map for the Ukraine is in file **u.ukr.1**. These maps were last updated in December 1991.

Mailing and Discussion Lists

(U) People that share interests are inclined to discuss hobbies or interests at every available opportunity. One modern way to aid this exchange of information is by using a *mailing list*, usually an e-mail address that redistributes all mail sent to it to a list of addresses.

(U) There are two general types of mailing lists: 1) those moderated by individuals to whom you should direct inquiries about joining the list, and 2) those open to public access.

(U) An automated mail-list system called *listserv* allows all the functions of adding and removing users to and from a list to be performed under program control. Recent versions of listserv also provide file-server functions which allow moderators to make data files available to subscribers.

(U) Each discussion list run from a listserver has two e-mail addresses. You send commands to the listserv address and messages to the group address. For example, RUSTEX-L is a discussion list maintained at the University of Buffalo concerning the Russian version of TeX, other Russian text-processing systems, thesauri, spell-checkers, keyboards, etc. If you can send and receive Internet mail, you can subscribe to RUSTEX-L by sending the following message to **listserv@ubvm.cc.buffalo.edu**:

sub rustex-l your_full_name

where **your_full_name** is your REAL name and NOT your network user ID. Once your subscription is acknowledged, you can use other commands to learn more about the list:

index rustex-l	sends a list of available archive files
info genintro	retrieves General Information Guide
review rustex-l	returns the network address and names of all subscribers

You can then send mail to the list by using **rustex-l@ubvm.cc.buffalo.edu** as the group address and everyone on the list will get your message.

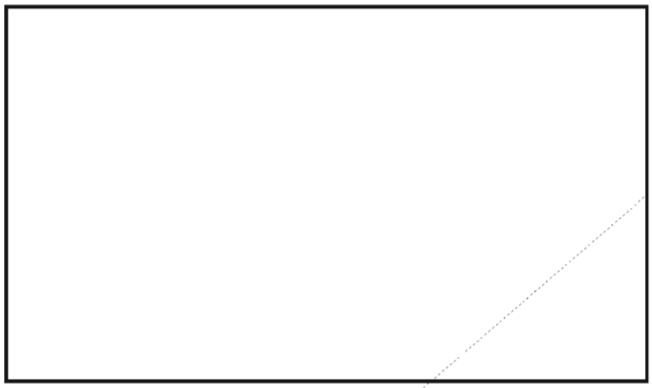
(U) For some lists, administrative tasks are handled with the suffix **-request**. NL-KR-L, for example, is a discussion list on natural language processing and knowledge representation maintained at the Rensselaer Polytechnic Institute. To join the list, one would send the "subscribe" command to the following address:

nl-kr-l-request@cs.rpi.edu

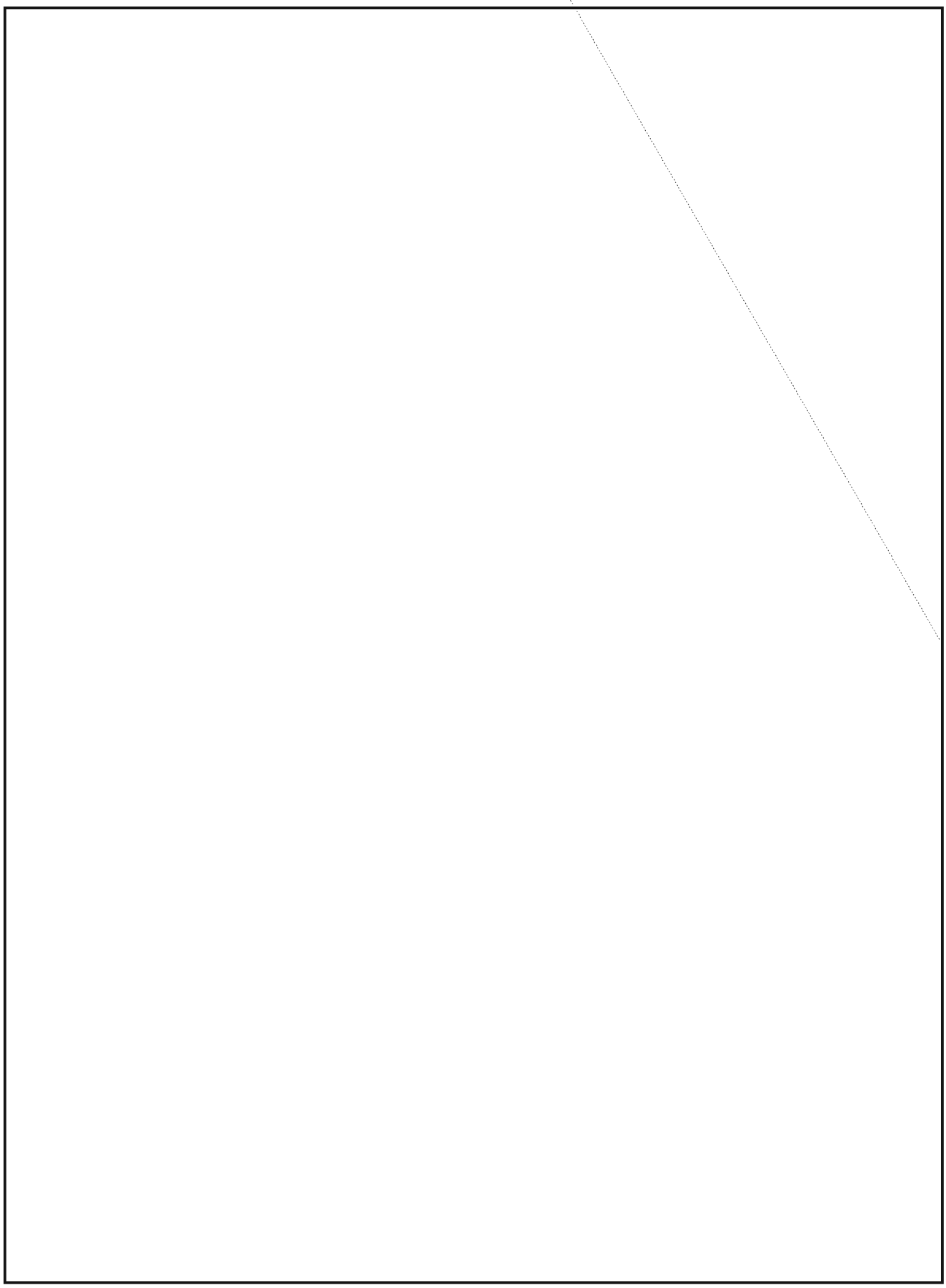
A number of mailing lists are set up not as discussion lists, but as a means of distributing newsletters, digests, reports, bulletins, etc. SUEARN-L, for example, carries a monthly digest on ex-USSR connectivity with the Internet. Many sites channel such digests into newsgroups or similar systems which let many users read a single copy of the digest. If such access is available, reading such a "public" copy is preferable to having your personal copy e-mailed to you (saving some network bandwidth!).

(U) Needless to say, listservs have become extremely popular. The latest issue of "The Eastern European list of Electronic (Computer-Accessible) Resources," for example, contains 124 discussion lists just relating to East European issues. There is even a list (**mailing-lists@ijs.si**) whose sole function is to publish a monthly directory of South Slavic mailing lists.

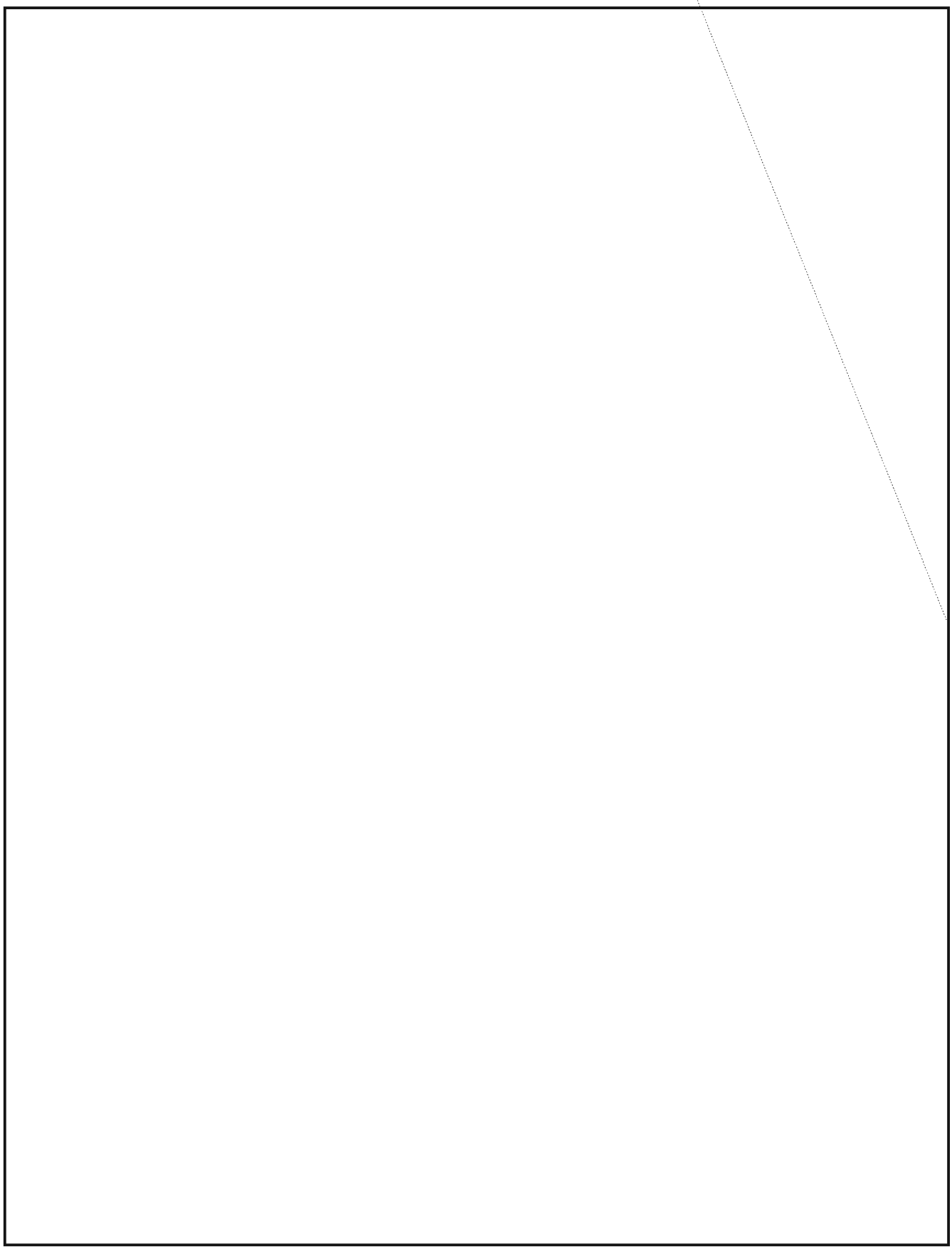
~~(C)~~ The ALTC has been sampling a significant number of discussion lists to gauge the nature of their content and usefulness (see following listings). So far we have remained passive observers, refraining from any active participation in discussions. We can see the benefit, however, of two-way contact now and then with other language professionals on certain topics. This is permitted as long as users are careful not to reveal Agency need, interests, or capabilities.



P.L. 86-36
EO 1.4.(c)



P.L. 86-36
EO 1.4.(c)



General Guides to Using the Internet

(U) The following are useful as introductory and general guides to using the Internet. A more comprehensive list of recent Internet books can be found in RFC #1432 by J. Quarterman, Mar. 93, available on-line by anonymous ftp from **nic.ddn.mil** in subdirectory **/rfc** as file **rfc1432.txt**.

- *Zen and the Art of the Internet: A Beginner's Guide to the Internet, 2nd ed.*

Brendan P. Kehoe, Prentice-Hall, 112 pp., $22.00. Probably the shortest of the introductory books. The on-line first edition, dated Jan 92, 96 pp., is available by anonymous ftp from **ftp.cs.widener.edu** in the **pub/zen** subdirectory as file **zen-1.0.ps**.

- *The Whole Internet User's Guide and Catalog*

Ed Krol, O'Reilly & Associates, Inc., Sebastopol, CA, 376 pp., 13 Sep 92, $24.95. Aimed more at graduate students who want to use the Internet for research. Ed's 1989 paper *The Hitchhiker's Guide to the Internet*, 22 pp., is available on-line by anonymous ftp from **uxc.cso.uiuc.edu** and other sources.

- *The Internet Companion: A Beginner's Guide to Global Networking*

Tracey LaQuey, Addison-Wesley, 196 pp., $10.95. Aimed at the general public. Being made available on line, two chapters per month, for anonymous ftp from **world.std.com**.

- *Internet: Getting Started*

April Marine, SRI International, 333 Ravenswood Ave., Menlo Park, CA; 380 pp., Sep 92, $39.00. How to join the Internet, and some context so you will know why. Neither a guide nor a catalog, but contains numerous contact listings.

- *The Internet Passport: NorthWest/Net's Guide to our World OnLine, 4th ed.*

Jonathan Kochmer and NorthWestNet, Bellevue, WA, 450 pp., 1993. On-line version, *Internet Resource Guide*, 3rd ed., Oct 92, 300 pp., is available by anonymous ftp from **ftphost.nwnet.net** in **nec/nwnet/user-guide** subdirectory, file **nusirg.whole-guide.ps.Z.**

- *The New User's Guide to the Internet*

Daniel P. Dern, McGraw-HIll, New York, 1993.

- *An Internet Primer for Information Professionals: A Basic Guide to Networking Technology*

Elizabeth S. Lane and Craig A. Summerhill, Meckler Corp., Westport, CT, 200 pp. 1992, $37.50.

- *Crossing the Internet Threshold: An Instructional Handbook*

Roy Tennant, John Ober, Anne G. Lipow, foreword by Clifford Lynch; 142 pp., 1993, $45.00. A short textbook on using the Internet, by two librarians at the University of California at Berkeley.

- *CICNet Resource Guide*

Available by anonymous ftp from **nic.cic.net** in subdirectory **pub**, file **resourceguide**.

EO 1.4.(c)
P.L. 86-36

[redacted]

by [redacted] P.L. 86-36

(U) The first coordinated public cellular mobile communication networks came into service in 1981. Since that time, cellular mobile use has grown to the point that there are now over 20 million subscribers to these networks throughout the world. Until recently, all of these networks used analog transmission technology to transmit users' communications. In the late 1992-early 1993 time frame, however a second generation of public cellular mobile networks emerged using digital technology and employing advanced multiplexing methods and modulations. These second-generation digital networks support a variety of new user services and provide for a number of improvements over existing analog cellular mobile networks.

(U) Two digital cellular mobile standards are presently being employed: the IS-54 digital AMPS (DAMPS) in the United States and the pan-European Global System for Mobile Communications (GSM) in Europe. Other standards are also being developed and may emerge in the not-too-distant future.

[redacted]

What is the Global System for Mobile Communications (GSM)?

(U) An oversimplified definition is that GSM is a **public telecommunications system**. The original expansion and eventual system name was derived from the initials of a Conference of European Posts and Telecommunications Administration (CEPT) working group Groupe Speciale Mobile (GSM). CEPT established the public cellular mobile radio "standard" aimed at beginning public service in the early 1990's. Following the 1982 inception, two significant events occurred. First, in 1987 the original GSM system's specifications were modified to reflect a change in technology from analog to digital, due mainly to operational simulations and trials conducted in Paris under the supervision of the GSM working group. Then in 1989, the GSM program was transferred from the purview of the CEPT to the European Telecommunications Standards Institute (ETSI). Since that time GSM's official expansion has become "Global System for Mobile Communications," and ETSI continues to oversee the development of GSM.

(U) GSM is a public digital cellular mobile radio system intended to become the standard for the whole of Europe and differing greatly from the many cellular mobile systems currently in existence throughout Europe and the rest of the world today. It will offer connectivity to all public telecommunications systems, both national and international, and offer all the same services and compatibility of a fixed telephone, including Integrated Service Digital Networks (ISDN), without the restriction of wires.

P.L. 86-36
EO 1.4.(c)

Who developed GSM?

(U) Non-cellular mobile radio communications systems have been in use since the 1920's; however, public cellular mobile networks did not come into service until 1981. Papers describing the concept had been written decades before, but it was not until the 1970's, after the emergence of reliable microelectronic circuits, that practical cellular communications systems could be developed. By the late 1970's, the telecommunications administrations of the Nordic countries (Sweden, Denmark, Finland, and Norway) had developed the Nordic Mobile Telephone-450 Standard. In 1981, while the rest of Europe, the United States, and Japan continued their cellular research, the Nordic countries began public service with the NMT-450, a coordinated mobile cellular communications system that uses analog technology and operates in the 450MHz frequency range.

(U) By 1982, European telecommunication administrations interest in cellular communications was growing and the market was expanding rapidly. CEPT,

realizing the growth potential of public cellular communications and a need for standardization among these systems, established the GSM Working Group. Specifically, it was tasked to provide an outline definition by December 1986 and a specification for a Pan-European public land mobile network by December 1988. Early in 1983, the working group had identified all competing systems and proposals, none of which were acceptable as candidates for the Pan-European system. To avoid standardization obstacles and any interference with the development of a new, clearly defined Pan-European system, the working group declared that all existing systems and system proposals would be considered "interim" systems.

(U) In 1987 the Ministerial Council of the European Community (EC) urged all member countries to introduce the GSM system. According to this recommendation, the start date for the Pan-European digital cellular mobile radio system should be no later than 1991, the most important city areas should be covered no later than 1993, and the main connections between covered areas should be no later than 1995. This recommendation was adopted in 1987 through a memorandum of understanding (MoU) between operators and telecommunications administrators of 16 European nations. Since then, others have signed the MoU, bringing the total number of signatories to 23 operators in 16 European countries, as well as another 20 countries throughout the rest of the world. Most of these countries have agreed to abide by the terms of the EC recommendation including the stipulation to license at least two operators, one private and one public, thereby creating a competitive consumer market.

(U) As the GSM working group's activities progressed, it became quite apparent that the analog systems currently deployed in Europe were overburdened and would be unable to meet future demand for public mobile cellular communications. Therefore, in 1987, it modified the GSM system specifications, citing a change from analog to digital technology. Since 1989, when the program was transferred from CEPT to ETSI, work on the GSM standard has continued as planned, and CEPT continues to provide an open meeting place for European telecommunication standardization activities. It should also be noted that, although CEPT and ETSI have been the overseers of the GSM program, various ad-hoc subgroups and joint groups have been formed periodically to assist in the development of the GSM standards. At one time there were as many as 28 groups involved in the writing of the standard, as well as the theoretical, practical, and simulation studies associated with the program.

Why was GSM developed?

(U) Development of GSM is particularly important at this time, due to the political and economic changes sweeping the world today. Many of the Third World countries (including those in East Europe), are attempting to develop market economies patterned after those of the West, to which efficient communications are essential; therefore, many of these countries are planning massive upgrades of their telecommunications infrastructures and are intent on deploying state-of-the-art equipment in order to compete.

(U) Funding for such upgrades, if not nationally available, is in most instances readily available through various lending institutions like the International Monetary Fund and the European Bank for Reconstruction and Development, or through joint ventures with many western companies designing and building GSM-compatible equipments.

(U) Various factors have driven the development of the GSM system, but probably the most important of these was the need to develop a standard to be adhered to by all digital mobile communications equipment manufacturers and suppliers. This standard will insure compatibility between equipment and provide a capability for the user to roam freely throughout Europe while maintaining communications with another party, be it through speech or data.

(U) Another major factor was the phenomenal growth in the use and deployment of public analog cellular mobile networks. Several European countries, as early as 1983, had deployed mostly non-compatible systems operating in the 450MHz band. This rapid growth, especially in the Nordic countries, resulted in pressure to allow these systems to migrate operationally into the 900MHz band—a logical migration, since the International Telecommunication Union (ITU) had already obtained approval from the World Administrative Radio Conference (WARC) to have this band designated for public mobile communications use in Europe.

(U) The United Kingdom was the first to allocate a portion of the 900MHz band for the operation of their first-generation analog system, known as the Total Access Communications Systems (TACS). Since that time, other countries have followed suit, and the U.K. has gone one better by allocating more of the 900MHz band, just below the original GSM spectrum allocation, for the operation of its Extended Total Access Communications System (ETACS).

(U) The ETACS expansion illustrates just one of the perceived benefits of the GSM system, High Spectral Efficiency. As GSM is introduced, it will be facing fierce competition from numerous analog systems already operating in the majority of the 900MHz band. Therefore, it must use its limited spectrum allocation (905-915MHZ and 950-960MHz) more efficiently than current analog networks. This reportedly will be accomplished through the use of a more complex control system. It is envisioned that the GSM system will eventually migrate to occupy the whole 50MHz, of the 900MHz band designated for public cellular mobile communications throughout Europe (890-915MHz and 935-960MHz). Until this occurs, however, the digital GSM system must perform far better than any analog system within its limited spectrum allocation to be an attractive marketable alternative.

(U) Cost-efficiency is also another benefit of GSM deployment. Initially, equipment costs may be higher than that of present analog equipment for the subscriber as well as the network operator. However, as additional features are introduced by the network operator the GSM equipment actually becomes more cost-efficient for both the subscriber and network operator.

(U) To date, all operational GSM systems are in their infancy and provide no more than national telephony service. Additional services and capabilities such as international roaming and ISDN will be phased in as software is developed and tariff and billing arrangements are established among national operators.

(U) The network operators benefit because there is no additional equipment to purchase when introducing the new features, since they will have the digital equipment in place and the additional features will be incorporated through the introduction of software at a minimal cost. Subscribers will be provided with these additional services as the operator introduces them, probably at a minimum additional charge, and in the end enjoy all the benefits that an analog system cannot provide. Other advertised benefits are smaller, smarter, lower-cost terminals; digital speech quality; improved mobile data and facsimile transmissions; built-in encryption; integral short message capabilities; and the added dimension of national and international roaming.

(U) Overall, the digital GSM cellular system will provide the user with smaller equipment, better quality communications, and all the services normally available on a fixed public telephone network.

Future Use

(U) Estimates vary, depending on the source, but it has been projected that there may be as many as 20 million European subscribers to the Pan-European service by the turn of the century. Future deployments are projected for all western European countries and the central European countries of Cyprus, Hungary, Poland, Turkey, the Czech Republic, Slovakia, and Greece. A number of other countries are considering GSM technology as a basis for their future digital mobile communications network deployments. These include, in the Far East, China, Australia, South Korea, New Zealand, Thailand, China, and Singapore, and, in the Mideast, Bahrain, Kuwait, Oman, Qatar and the United Arab Emirates, just to name a few.

(U) Based on the above projections and the apparent head start the Europeans have on their competitors (the United States and Japan) one could easily see GSM becoming more than a European standard as the world's telecommunications systems migrate from analog to digital technology. It is highly unlikely, however, that the GSM standard will be universally accepted; more likely it will be considered the first step toward the development of a global digital cellular mobile standard.

(U) Many factors will influence the deployment decisions. In the EC, the desire or need of the government to participate in the European "one market" philosophy will be an important factor. Other countries must consider their economic situation, the availability of the required frequency spectrum, and any restrictions which might be imposed by a successor organization to the Coordinating Committee for Multilateral Export Controls (COCOM). Additional considerations include the current state of a country's telecommunications infrastructure, for example the existence of any analog cellular systems and their potential for growth as well as the availability of any competing digital standards.

(U) The acquisition of GSM systems will thus vary from country to country. Many will jump on the bandwagon right away; some will initially deploy analog cellular systems, while others may decide to play a waiting game (especially if they have an adequate telecommunication infrastructure), to see which digital cellular technology, if any, will be accepted as the global standard. The likely scenario for the European continent is that all the western European countries and some central European countries will, as stated above, deploy GSM systems as soon as possible, while the remainder will probably deploy analog cellular systems to augment their inferior telecommunication infrastructures. Even-

tually, even those countries who initially chose an analog deployment will probably migrate to the GSM standard.

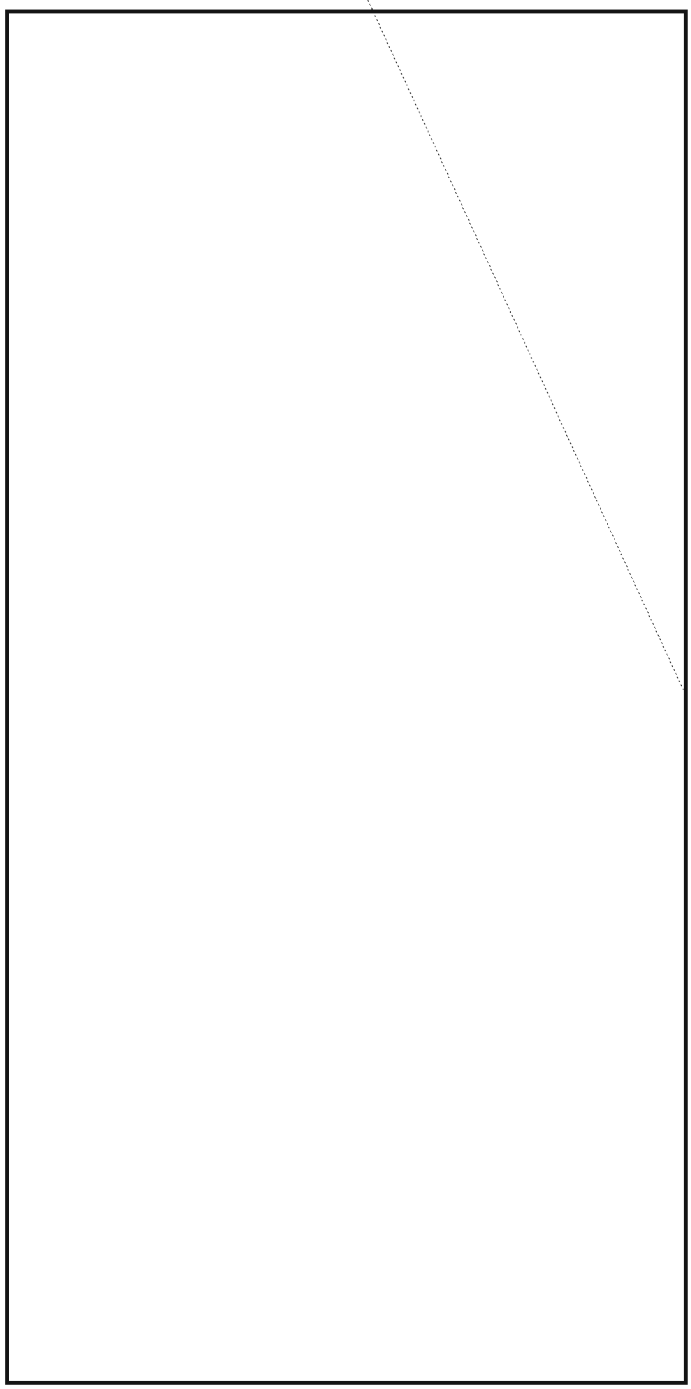
(U) Adoption of the GSM standard by other world nations should also follow the pattern set by those countries throughout Europe. In the lesser-developed and Third World countries some will go the route of the western European countries and immediately deploy GSM systems, providing they can obtain the funds and COCOM-successor restrictions do not apply; others will delay deployment. In developed nations the need to immediately adopt a new cellular mobile standard will be less critical, since most have well-established telecommunication infrastructures to include a number of operational analog systems, or are in the process of developing their own digital cellular mobile standard, as is the case with Japan and the United States.

(U) Therefore, the world's cellular mobile telecommunications picture will most likely, at least in the near term, remain a hodgepodge of analog and GMS digital cellular mobile communications systems, and the number of users/subscribers switching to the new GMS systems will not increase dramatically, due to the initial high costs of equipment and subscribership. In the long term however, as more services become available and costs decline, GSM will undoubtedly become a viable option for the public sector.

Conclusions and Recommendations

(U) **GSM systems provide highly sophisticated communications.** The vast majority of cellular systems currently deployed throughout the world today are incompatible analog systems providing, at best, a national voice telephony capability and other limited services. When these systems are compared with a mature GSM digital system it becomes quite evident that the additional capabilities of GSM—increased data rates, improved signal quality, improved spectrum usage, improved security of communications, and compatibility of systems among countries—provide a cellular mobile communication system far superior and more sophisticated than those in use today.

(U) GSM system deployments and subscribership will increase. There will be a continual migration from analog to digital mobile cellular communications, and the number of system deployments, as well as the number of subscribers, will increase as new phases of the GSM standard are introduced, additional services become available, and the costs of equipment and subscribership to GSM networks diminish. The rate at which this migration and growth of subscribership occurs will differ worldwide, because of variances in governmental telecommunication policies, the current state of an individual country's telecommunications infrastructure, a desire to perpetuate a global market, subscribership growth potential of current analog mobile cellular communications systems, availability of the required frequency spectrum, and the development of other digital cellular standards possibly providing capabilities superior to the GSM standard.



EO 1.4.(c)
P.L. 86-36

[redacted]

by [redacted] P.L. 86-36

(U) In the past several years, there has been a virtual explosion in the use of digital means for transmitting voice telephony and other services. The most prevalent method of converting analog information to digital pulses is pulse code modulation (PCM). Many countries have already made, or are in the process of making, substantial investments in the installation of PCM systems. Third World countries in particular have been rapidly expanding into the digital arena while Western countries are doing so at a slower rate, chiefly because the lack of existing communications infrastructures in the Third World makes a direct move into digital systems economical.

~~(C)~~ Western countries, on the other hand, have invested significant resources in their analog systems, and therefore tend to replace existing systems at a slower pace. The growth rate in digital transmissions in the West over the next several years is anticipated to be about one to two percent per year. This pace is significant enough that it cannot be overlooked by the Intelligence Community.

(U) Economic considerations, enhanced signal quality, and the inherent flexibility of the digital transmission network are important factors in the shift from analog to digital transmission. In addition, many vendors are no longer producing analog FDM systems, thus forcing users to replace them with digital systems. Fiber-optic cable is the preferred mode; however, terrestrial microwave is expected to remain prevalent for short-haul transmissions and as a back-up to fiber.

(U) The concepts underlying PCM have been understood since the mid-1930s. France filed a patent in 1938; British and American patents were filed in 1939 and 1942 respectively. By 1948, studies in Bell Telephone Laboratories had proved that PCM was well understood. Because frequency-division multiplexing (FDM) was easier to implement and further developed than time-division multiplexing (TDM, the basis for PCM), however, FDM was virtually the only transmission mode then in use. The advent of the transistor in the late 1950s helped solve the problems surrounding the implementation of PCM, and American Telephone and Telegraph introduced PCM in the early 1960s.

(U) There are two primary PCM hierarchies in use throughout the world: the CEPT (Conference of European Postal and Telecommunications) or European standard and the North American/Bell standard. The Japanese have developed their own standard, based on the Bell system; to date it has been seen in use only in Japan. Each standard operates on a building-block principle. Voice-grade channels are multiplexed in the basic level to form channel bank units (CBUs), also referred to as the Level 1 multiplexer. Level 1s are combined to form successive signal levels and increasingly higher-capacity systems.

CEPT Standard

~~(C)~~ CEPT, the European standard, has been accepted by the International Telegraph and Telephone Consultative Committee (CCITT) as a standard in the international PCM arena. In this system, each frame is made up of a set of 32 channel time slots numbered from 0 to 31. Voice channels are allocated to 30 channel time slots. Time slot 0 is reserved for frame alignment and alarm indication facilities and 16 is used exclusively for signalling; voice-grade-channel signalling is carried on this one channel rather than within individual channels as is the case with CCITT #5. This type of signalling is referred to as common-channel signalling (CCITT #6). Each channel time slot is composed of 8-digit time slots and sampled at a rate of 8000 samples per second; the complete frame repeats every 125 microseconds. The CEPT format produces a 256-bit frame (32 channels X 8 bits per channel) and an operating bit rate of 2.048 Mbps (8000 samples per second X 256 bits) employing A-Law companding. Level 1 (L1) signals are composed of 30 channels; Level 2, four L1s (120 channels); Level 3, four L2s (480 channels), Level 4 of four L3s (1920 channels), and so on.

P.L. 86-36
EO 1.4.(c)

[redacted]

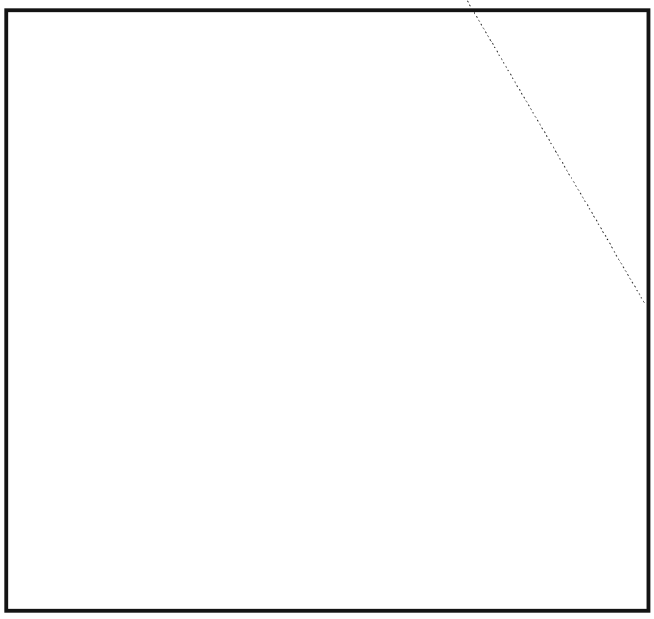
[redacted]

EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)

Bell/North American Standard

(U) The Bell/North American standard has also been approved by the CCITT as a PCM standard. The T1 carrier, also referred to as a Bell Level 1, was introduced by Bell in 1962 and allowed for the multiplexing of 24 voice channels over one transmission medium. Each voice channel is composed of eight bits, giving a frame length of 192 bits (24 X 8). A 193rd bit is used for framing and signalling control. The T1 operates at a bit rate of 1.544 Mbps (8000 samples per second X 193 bits). The T2, or second-level Bell system, was introduced in 1972 and carries 96 voice channels on a single transmission medium. The T2 is composed of four T1s, the T3 of seven T2s for a total of 672 channels and the T4 of six T3s for a total of 4032 channels.



Advantages and Disadvantages of PCM

(U) PCM has several advantages over FDM analog systems. One of the primary advantages is its low cost. Unlike FDM systems which require many precise and elaborate band-pass filters throughout the system, PCM systems require only simple channel low-pass filters. Because of the decreasing costs of large-scale integration (LSI) technology, which is employed in the design and fabrication of PCM system electronic components, and the elimination of expensive filtering, the per-channel costs of PCM are much lower than those of FDM.

(U) A second advantage of PCM is its excellent speech quality and its improved signal-to-noise ratio (SNR) as compared with FDM transmissions. In analog transmission, disturbances caused by noise, cross-talk, intermodulation, and other factors cannot be eliminated once introduced into the signal. Each time the signal is amplified, any associated noise is amplified as well. This is one of the most serious limitations of analog transmission systems. The PCM signal, on the other hand, exists in only two states: 1 and 0 (pulse or no pulse); as long as the presence or absence of a state can be detected, no matter how distorted the signal, the PCM system can handle it. The degradation of the received signal does not alter the information content until it becomes so severe that the receiving equipment cannot distinguish between the presence or absence of a pulse. In contrast with FDM, which is amplified at each repeater, PCM signals are regenerated at each repeater and are therefore not limited by accumulated degradation. Regeneration completely eliminates the perturbations of the preceding transmission, which means there is no limit to the transmission distance. This is one of the unique advantages of digital over analog transmission systems.

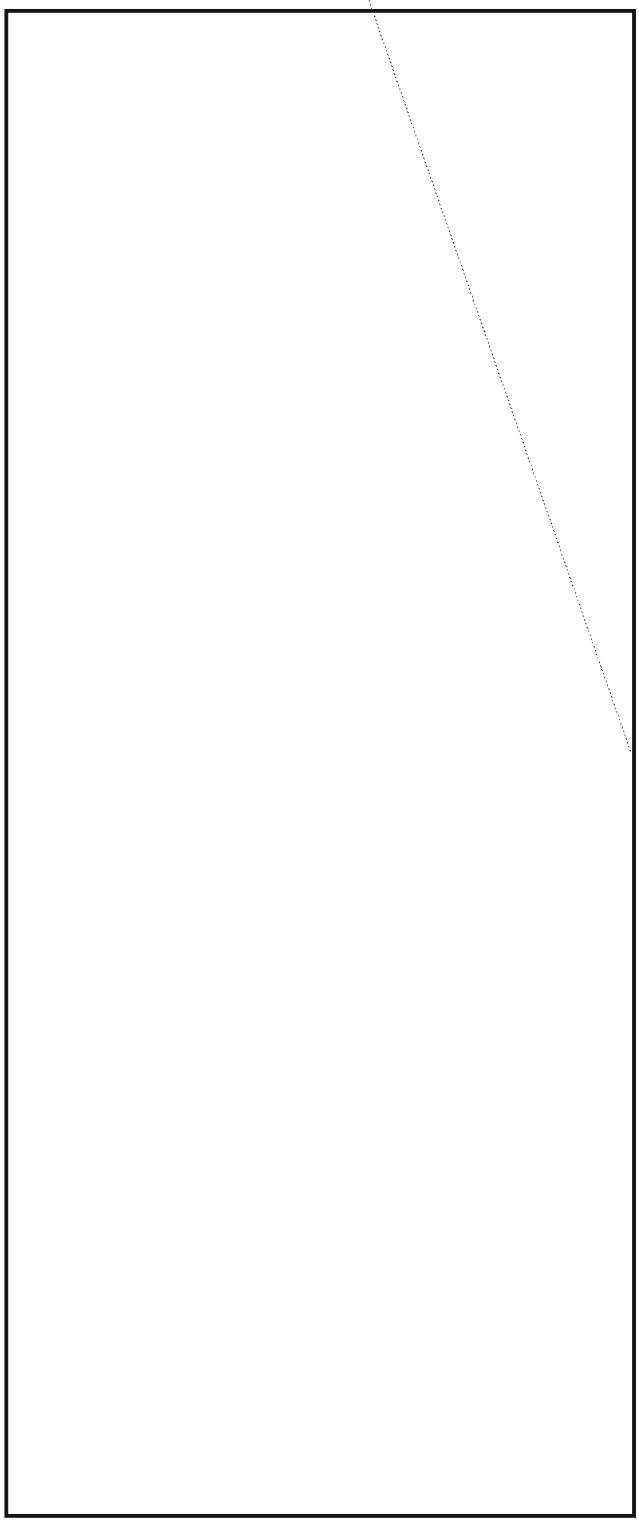
(U) PCM is very flexible, lending itself to all types of modulation schemes. Systems of different rates and carrying different types of service—telephony, data and other digital services—can be easily interconnected. Because it offers direct digital interface, there is no need for modems to convert digital signals to analog prior to transmission over a voice-grade channel. A channel capacity of 64 kilobits per second (Kbps) can be achieved with PCM as compared to a maximum of 2.4 Kbps on unconditioned FDM channels.

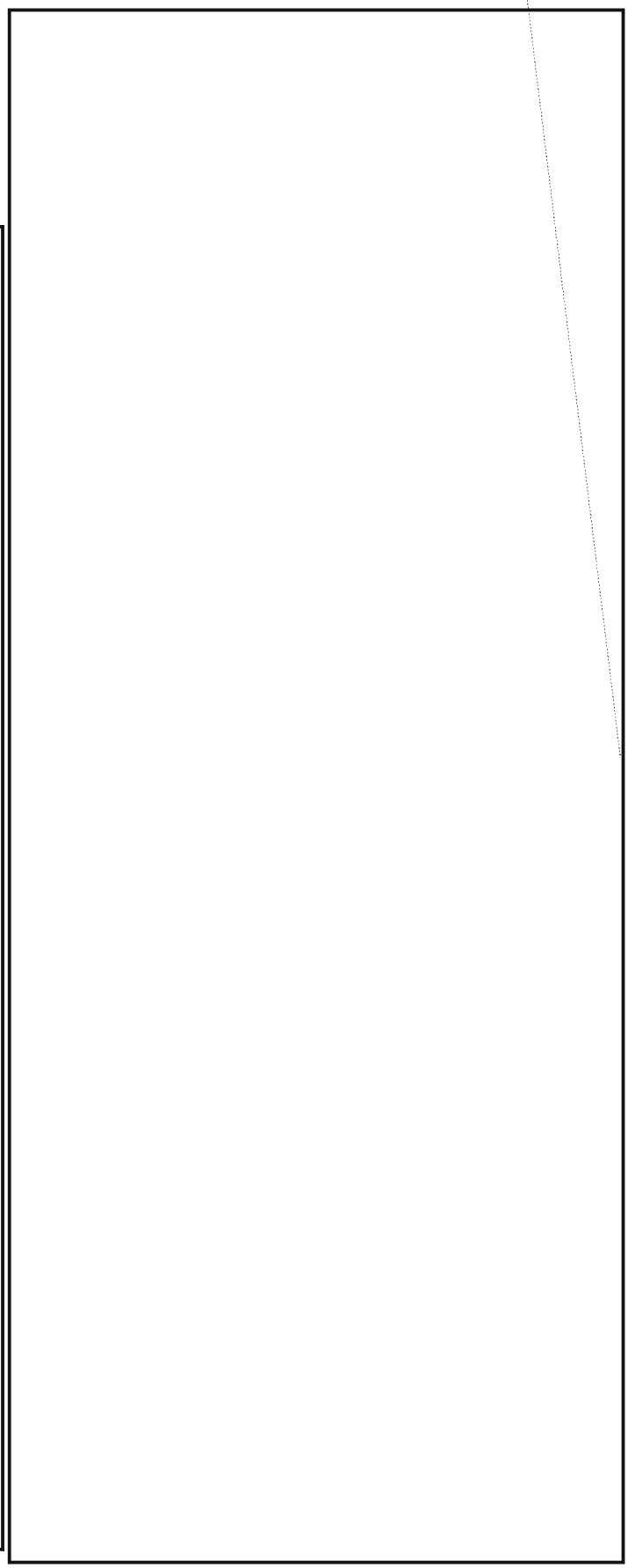
(U) PCM also has disadvantages. First, it requires approximately 16 times more bandwidth than FDM. In addition, in order to maintain transmission integrity, the signal must be regenerated frequently, approximately every 6000 feet on cable and at each repeater on microwave. Lastly, complex demodulation and demultiplexing equipment is needed for voice-grade-channel analog-to-digital conversion at the transmitter and digital-to-analog conversion at the receiver.

Conclusions and Recommendations

~~(S-CCO)~~ It is clear that the worldwide communications environment is undergoing a transition from analog to digital. Cable appears to be the transmission means of choice; however, microwave will continue to be used for short-haul transmissions, in urban environments and as a back-up to fiber, thus making terrestrial microwave collection a viable mission. We can also expect to see increasingly higher data rates in use. Data rates of 140 Mbps are no longer unusual and it is anticipated that data rates up to 300 Mbps will become increasingly common over the next several years. In

addition, new formats, such as forward error correction (FEC), trellis coded modulation, synchronous optical network (SONET), and synchronous digital hierarchy (SDH) will become more prevalent. Higher modulation levels such as 256 QAM can also be expected, as can increased military use of digital transmissions.





Video SIGINT Dissemination:

The NSA Broadcast Network

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

by [redacted] P0542

~~(C-CCO)~~ SIGINT reactions to [redacted]

These are the kinds of things you may see on television in the workplace, as the NSA Broadcast Center pursues its goal of bringing you the latest intelligence news from around the world, 24 hours a day.

~~(C)~~ The NSA Broadcast Center has been broadcasting SIGINT for more than two years via the NSA Broadcast Network and the Defense Intelligence Agency's Defense Intelligence Network (DIN). Through the DIN, video SIGINT reports reach DIA, the Pentagon, numerous military commands worldwide, and certain Washington, D.C. users. Within NSA, classified broadcasts produced by the Broadcast Center appear daily on NEWSMAGAZINE Channel 21. Video SIGINT is a fast-growing medium, providing the busy executive, field commander, and target analyst with instant access to the world's daily headlines and breaking stories, in a readily absorbed form.

~~(C)~~ Since July 1993, the Broadcast Center has been producing live programming that integrates live SIGINT updates, live and taped interviews, interviews remoted from organizations such as DEFSMAC, and taped special programs. All SIGINT Headlines programs are broadcast live to ensure they contain the most up-to-date information. In addition, the Broadcast Center's partnership with NSOC ensures that CRITICs of national level importance can be broadcast as soon as the information has been verified—meaning viewers will be able to learn of them faster than ever before.

How The Broadcast Network Works

~~(FOUO)~~ Time-sensitive video SIGINT is a unique medium, yet it resembles commercial television news in many ways. Video SIGINT reporters aim for timeliness, while striving to meet the standards of commercial news presentations. Video SIGINT reporters—most with SIGINT reporting experience, a few from other SIGINT disciplines—work rotating shifts to cover the SIGINT news around the clock. All underwent a selection process involving a screen test and writing sample.

~~(C-CCO)~~ A video reporter's day is probably at least as busy as that of a CNN correspondent. Arriving in the newsroom, he or she "hits the ground running," poring over the most recent SIGINT product (everything that enters [redacted] is distributed electronically to the Broadcast Center), selecting items based on their newsworthiness. First priority goes to items related to the hottest news stories of the day. In addition, reporters focus on product related to regions of current policymaker interest as listed by the White House Situation Room, or product deemed by the executive producer to be of intelligence interest. Using the selected product, reporters write video scripts, design graphics, and select appropriate video footage. Meanwhile, skilled computer graphics artists convert the reporters' rough sketches into professional on-screen graphics that can incorporate maps, photographs and footage stills.

P.L. 86-36

(U) After the scripts have been edited and approved by the executive producer, the reporter becomes an on-camera anchor, seated under bright lights in the Broadcast Network's studio, reading scripts as they scroll by on a teleprompter. Next, words meet pictures in the Broadcast Network's control room, where video editors, many with commercial television experience, combine the live or taped narration with graphics and footage. In spare time, the newsroom crew carry out innumerable logging and housekeeping duties. In even sparer time, they put together long-term video background reports. In addition, both reporters and executive producers conduct on-camera interviews.

~~(FOUO)~~ Executive producers, the shift team chiefs, perform all the functions of a reporter. In addition, they are responsible for content and quality control of all programs written and produced on their shift. After normal duty hours, the executive producer has Senior Reporting Officer-equivalent authority as the last

person to see NSA visual product before it is released to the DIN and its audience. On days, the producers also do program planning, work on developmental program projects, coordinate the Broadcast Network's activities with Intelligence Community customers, and brief visitors on the Broadcast Network's operations.

NSA Video Compared With Commercial Television

~~(C)~~ Just as commercial television news is faster than print media, video broadcasts have the potential to get the SIGINT fact to the customer faster than standard database pulls, whether on a computer screen or in a stack of paper. At the same time, video aids the viewer through use of graphics such as maps, bulletin boards, photographs, and footage clips. Interviews, a staple of commercial television news, are also proving highly effective in providing SIGINT target expert knowledge and background that are not generally included in SIGINT product.

~~(C-CCO)~~ Video SIGINT differs from commercial television, however, because SIGINT stories respond to National SIGINT Requirements and thus lack the sizeable entertainment component (such as stories broadcast strictly for their humorous, bizarre, or human interest content) of commercial news. Another factor that makes video SIGINT "look" different is USSID 18, which by forbidding the intercept of U.S. communications, results in a distinct lack of local news!

Video Complements Written SIGINT

~~(C)~~ While television news serves a different purpose than print-media news, it definitely has not replaced it, and so it will be with video SIGINT. In the commercial world, print news media have largely ceded the breaking-news aspect of journalism to electronic broadcast media. In somewhat the same way, televised SIGINT will ultimately serve the person who wants the latest news now, at the push of a button, without having to touch a piece of paper or even read a screen. SIGINT on television will also serve the busy executive or policy-maker with little time or inclination to read, as well as the busy analyst with a yen to know what's happening in SIGINT around the world. When large numbers of customers gain access to video terminals, time-sensitive video is potentially the most efficient way to get the basic facts to the most people.

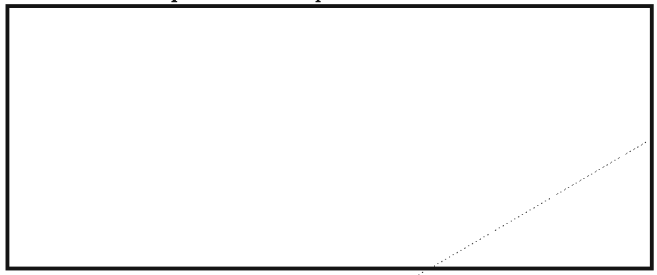
~~(C)~~ Video SIGINT's role is to parallel, complement, and enhance SIGINT in written form. Time-sensitive written-media SIGINT product will, of course, continue to convey vital intelligence to users. For many purposes, including decision-making, people require written reports they can mull over, carry to the next office and discuss, and have sent to them via electronic mail.

~~(FOUO)~~ Television won't replace longer-term SIGINT product, or SIGINT summaries, either. Consider that commercial television has been available for nearly 40 years. While there are far fewer newspapers now than there were 40 years ago, most people still peruse at least one daily paper for in-depth background and analysis of the day's events. As electronic journalism has taken over delivering breaking news, print media have expanded their capacity to give "the full story," to provide perspective, and to serve as the media of record. It is unlikely that a well-informed person, such as an NSA employee, would consider television news sufficient to keep him or her up to date. To an even greater degree, the same considerations apply to SIGINT and other intelligence delivered by video or in written form.

~~(C)~~ However, video SIGINT possesses a unique extra dimension not possible in written form: television interviews. While all SIGINT reporting answers the question, "What did NSA intercept?" interviews can answer, much faster than the written word, the important question, "What does NSA think?" Policy-makers and other customers want and need the benefits of NSA's immense reserves of analytic expertise. To stay informed and make decisions, they require access to the intuition and experience of SIGINT analysts, who in many cases have studied their targets for decades. In a five-minute television interview, an expert analyst can give large numbers of viewers a great deal of valuable knowledge about the "hot" topic of the hour. To this end, NSA's SIGINT Intelligence Officers (SINIOs) are interviewed regularly on the Broadcast Network.

Other Applications For Video SIGINT

~~(S-CCO)~~ Television, in addition to its unique time-sensitive uses, has many applications for long-term SIGINT analysis and background. A short video feature can untangle complex facts about a SIGINT target. Broadcast Center reporters have produced video term studies



DOCID: 4009690
EO 1.4.(c)
P.L. 86-36

~~(C)~~ The possibilities for fusing SIGINT with other intelligence sources, such as human intelligence, imagery, and open source news, are unlimited. During a crisis, video features, combined with expert analyst interviews, would give policy-makers a snap course in events leading to, say, a coup in a foreign government. Customers would learn factors affecting economic relations between the U.S. and another country, or discover key people who may affect the outcome of elections in a fragile new democracy.

~~(C)~~ Besides disseminating SIGINT, video term reports can benefit a diverse audience by addressing collection, management, and personnel issues. Such reports would benefit the viewer by rounding out the picture of what NSA does, NSA's role in the Intelligence Community, and how the individual fits into the intelligence picture.

Audio SIGINT News Service

~~(FOUO)~~ No NEWSMAGAZINE terminal yet, and no word on when your office will get one? You can still hear the latest SIGINT news through the Broadcast Center's Audio News Service by dialing 963-NEWS. It is updated, 24 hours a day, with each edition of the SIGINT Headlines and Highlights; plans are to include other SIGINT news programs as well. During weather emergencies, when the DIN closes and the Broadcast Center does not retain enough personnel to do video programming, the Headlines will continue to be updated daily.

Much Work Yet To Be Done

~~(FOUO)~~ Although video broadcasting at NSA is constantly expanding, there is a long way to go before video is delivering all the "SIGINT on the spot" to every customer who needs it, at NSA, in the Intelligence Community, and within military commands. Some issues that must first be addressed include:

- Increasing the number of NEWSMAGAZINE terminals (presently there are about 400) throughout NSA. Access currently is limited by the number of terminals, as well as by security and distribution considerations. Our broadcasts may not use compartmented product, and certain ORCON Intelligence Source Indicators are off limits as well.

- Expanding the NSA Broadcast Network to include National Cryptologic Representatives, Cryptologic Support Groups, Special U.S. Liaison Officers, and ultimately, field sites and Regional SIGINT Operation Centers.

- Establishing remote video links for two-way broadcasts.

- Expanding our partnership with NSOC.

- Increasing the Broadcast Center's manning, resources, and space, and going on line 24 hours a day, 7 days a week.

- Tailoring our programing to a variety of customers downtown and around the world as the DIN expands its customer base.

Thanks to the Tech Trend Notes, which publishes a Calendar of Events sponsored by NSA, academia, and professional associations, there is now a greater than ever opportunity to disseminate information on technical breakthroughs to the workforce. Here's a sample of what's happening this year:

Event	Date	Location	Where to call:
DoD Database Colloquium '94	29-31 Aug.	San Diego, CA	(703) 631-9125
Satellite Communication Users Conference	19-21 Sep.	Oak Brook, IL	(312) 938-3500
INFOTECH '94 Conference & Exhibition	11-13 Oct.	Dayton, OH	(703) 631-6200
Global Telecommunications Conference	27 Nov.-1 Dec.	San Francisco, CA	(415) 375-4338

SIGINT Glossary

Communications Analysis Trivia:

The GUHOR Stick

P.L. 86-36

by [redacted] P0542

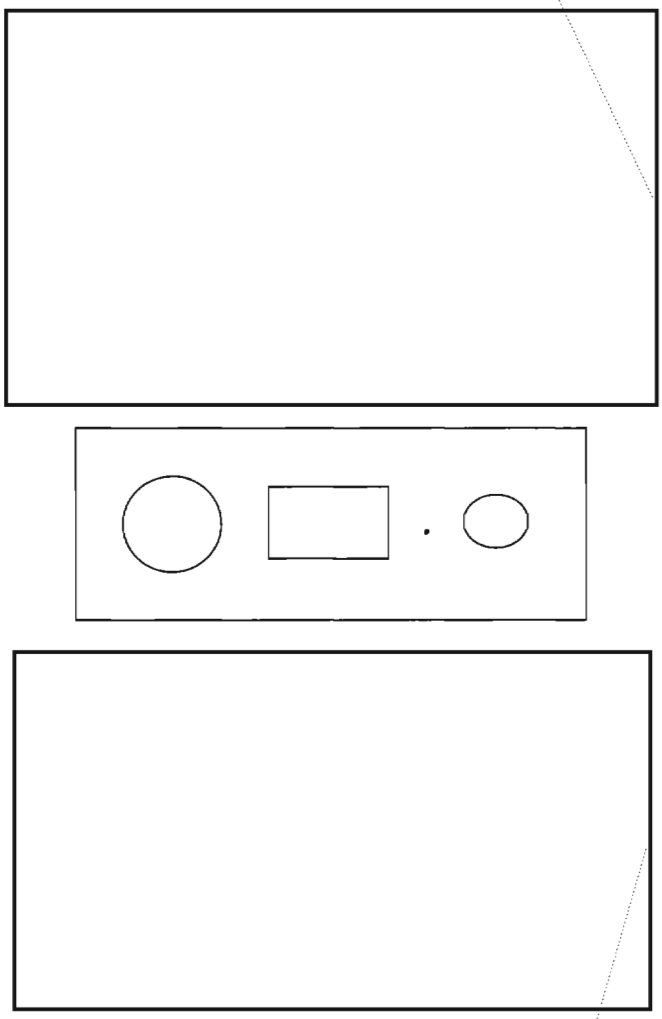
EO 1.4.(c)
P.L. 86-36

This is the first of what we hope will become a regular feature. Contributions from the Agency's corporate memory are welcomed.

(U) The what? No, it's not a Russian popsicle or the latest dance craze in Bosnia. It's only the most important tool ever invented for the traffic analyst of yore. Solutions to the most intricate communications networks often began with this simple device. No self-respecting TA was ever without one close at hand. Like the six-shooter of the old West, the analyst kept it at his side, always ready to draw—circles, boxes, and lines, that is.

(U) The GUHOR Stick, in its most recent and best-known iteration, is merely a 6" by 1.5" clear plastic template. Its prime purpose is to facilitate the drawing of communications diagrams, although its secondary uses are endless. It comes equipped with a large circle at one end to draw control terminals, a smaller circle at the other end for outstations, and a small rectangle in the center for communications relays and CQ calls. The straight edges are used to connect these stations and show communications paths. With this tool, a #2 pencil (with extra erasers), some graph paper, and several pencils of various colored leads, the analyst of old was fully prepared to face any communications adversary.

(U) But whence came this strange name? A GUHOR Stick? Putting my analytical skills to work, I set out to research the issue. To my surprise, there was a higher than expected number of individuals who had heard the name. Most were seasoned veterans from a mixture of professions, including linguists, reporters, managers, executives, and, naturally, traffic analysts. But there was more than a little discussion about what this device was and where its name originated.



(U) The early returns were mixed, however. I was still searching for the definitive word. It was at this point when I began to get responses via e-mail from

EO 1.4.(c)
P.L. 86-36

1. Those on field duty in the Pacific used a similar device which they called a "pooka-maker." Pooka is a Hawaiian word for "hole."

EO 1.4.(c)
P.L. 86-36

members of a Communications Analysis Association (CAA) interest group. A number of seasoned veterans recounted their GUHOR experiences and, in a number of colorful responses, gave me what I believe to be the true scoop.

(U) GUHOR Sticks as traffic analysis tools have been around for decades. Some CAA respondents remembered seeing or using them in one form or another from at least the early 1960s. Even so, a couple of questions remain unanswered. Who invented it? Why was it given this curious name? Someone out there knows. If you can solve the mystery, we're ready to hear a good story.

(U) All this discussion about GUHOR Sticks may be moot. These devices are few and far between these days. The GUHOR Stick does not have a federal stock number. They were made in batches at NSA by special order; however, they are fast becoming collector items. With the advent of the desktop computer, many analysts are using computer graphics to diagram their targets. The traditional circles and lines on paper are becoming passe. Most GUHOR Sticks that are found are being employed for many a sundry task—not for crafting the intricate networks of old, but for drawing nondescript lines and symbols unrelated to the trade of traffic analysis.

(U) Now, is there a similar wealth of knowledge out there about the Chun Wheel?

The author would like to thank the many CAA members whose phone calls and e-mail postings contributed to this article.

CRYPTOLOG

Editorial Policy:

(U) Technical articles are preferred over non-technical; classified over unclassified, shorter over longer., Emphasis should be on improving NSA's technical performance; articlesshould be aimed at explaining one's discipline to those outside it. Readers are also invited to contribute conference reports and reviews of books, articles, software, and hardware that pertain to our missions or to any of our disciplines. Humor is welcome, too. Submissions may be published anonymously, but the identity of the author must be known to the editor.

Submitting Items

N.B. If the following instructions are a mystery to you and your local ADP support is no help, please feel free to call the CRYPTOLOG editor on 963-3123s.

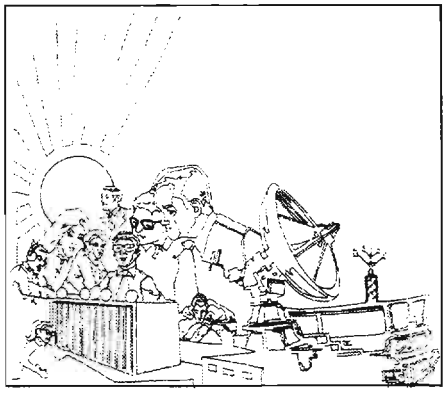
~~(FOUO)~~ Send a hard copy accompanied by a labelled diskette to the editor at P054 in 2E062, Ops. 1, or [redacted]
For maximum efficiency (as far as possible within the limits of your word processor):

P.L. 86-36

- Do not type your article in capital letters.
- Classify all paragraphs.
- Label all diskettes, identifying hardware (OS: DOS, UNIX), density and type of word processor used.
- Put your name, organization, building and phone number on diskettes.
- FrameMaker format is preferred; ASCII is also fine. J334 has a conversion service that converts Interleaf, Word Perfect, OfficeWriter and MS Word into FrameMaker. Just attach the document to an E-Mail Compose Window addressed to **convert@po**.

DOCID: 3689

18 APR 1964



NATIONAL SECURITY AGENCY

CRYPTOLOG

This Issue:

The Director's Summer Program ***Page 2***

The Closing of NSGA Philippines ***Page 9***

An Agnostic Look at TQM ***Page 20***

. . . . AND MORE (Table of Contents, page i)

Declassified and Approved for Release by NSA on 10-10-2012 pursuant to E.O. 13526, MDR Case # 54778

~~Classified by NSA/CSSM 123-2~~
~~Declassify on: Originating Agency's Determination Required~~

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

DOCID: 4009689

CRYPTOLOG

Vol. XX No. 1 ..... 1st Issue 1994

Published by P05, Operations Directorate Intelligence Staff

Publisher .....

P.L. 86-36

Editor ..... (963-7595)

Collection..... Marian Brown (963-1197)
Cryptanalysis ..... (963-1461)
Cryptolinguistics..... (963-4382)
Information Resources..... (963-3258)
Information Science..... (963-3456)
Information Security..... (968-8013)
Intelligence Community ..... (963-5800)
Language..... (963-3057)
Linguistics ..... (963-4814)
Mathematics..... (963-3709)
Puzzles ..... (963-1461)
Research and Engineering ..... (961-8362)
Science and Technology ..... (963-3544)
Special Research..... Vera R. Filby (968-6558)
Traffic Analysis..... (963-3369)

Classification Officer ..... (963-5463)
Unix Support..... (963-3369)
Macintosh Support..... (961-8362)
..... (963-4382)

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

To submit articles and letters, please see last page

DOCID: 4009689

Table of Contents

The Director's Summer Program 1

Open Systems: What Does It Mean? 4

The CIM TRM and the NSA Profile 6

The Closing of NSGA Philippines 9

Eurocrypt '92 Reviewed 12

An Agnostic Look at TQM 20

Technical Literature Report 23

Principles for Successful Guidance 24

Lexicography at Second Hand:
Producing an "Exotic Language" Glossary 25

Book Review: English-Arabic Scientific & Technical Dictionary 26

Letters to the Editor 27

DOCID: 4009689

CRYPTOLOG
March 1994

The Director's Summary Program

P.L. 86-36

R51
R51

~~(C)~~ Mathematics is the fundamental science that supports the twin disciplines of cryptology: the design of encipherment systems, and cryptanalysis, the "breaking" of codes intended to be unbreakable. The ever-increasing mathematical sophistication of cryptographers and cryptanalysts outside NSA, the increasing number of important cryptologic problems, and the increasing complexities posed by modern modems and communications systems requires us, more than ever, to bring the newest and most powerful ideas in mathematics to bear on our problems.

(U) For the past four summers, the R51-sponsored Director's Summer Program (DSP) has invited exceptionally talented young mathematicians from across the nation to NSA for up to 12 weeks and exposed them to the excitement of cryptologic mathematics by giving them hands-on experience working on some of our most difficult and important cryptologic problems under the direction of top Agency mathematicians. The program has been enormously successful in its first four years (1990-1993), obtaining surprisingly effective operational solutions to very hard problems, encouraging participants to continue their study of mathematics, and helping NSA to become better known in the active network of outstanding young mathematicians.

(U) Entry into this program ideally will take place between the junior and senior undergraduate years, but exceptional older or younger undergraduates and high school students may be considered.

DSP's Beginning: 1990

(U) Even before the evidence of decline in mathematics research and education was so prominent on the front pages, NSA mathematicians were aware of it and were trying to do something about it through a number of grass-roots efforts. With the austerity we face, we are not going to be able to survive beyond the nineties with business as usual. We are going to have to scour the nation for the best mathematicians we can find. In October 1989 the Agency began an energetic program to seek out top young undergraduates who showed great promise and interest in mathematics and expose them to our exciting problems. Many thought we were doing this as a long-term recruiting program. Indeed, we were recruiting, but for mathematics, not for NSA. Our interest and intent was to use a summer experience with us, to generate evidence that mathematics provides both subject matter and training for challenging careers. We had hoped for a few more students, but we were pleased that eight were able to stick it out through the processing and come, because they were eight very special young people.

(U) We were hoping that we could put these eight young people in a room by themselves, working on our best problems, so that the experience would be strongly peer-interactive. But such an aggressively structured experience could be pulled off only if our top mathematicians took on responsibility for technical direction. The first two mathematicians that we asked to lead the 12-week 1990 DSP not only said yes, but they worked hard during the spring to prepare for the students, identifying and developing the best problems to present to them.

(U) The first two weeks of the 1990 DSP were extremely difficult, for both the technical directors and the students. The students had to learn decades of classified cryptologic mathematics in two weeks, as well as a myriad of details about the four problems presented to them. During these two weeks, some learned to program for the first time. All were proficient programmers by the end of the summer.

(U) By the third week, the students knew everything there was to know about the problems, had developed into overlapping groups, and knew NSA slang and jargon so well they sounded as if they had worked for us for 10 years. We had five Sun terminals connected to the Cray in the room for the eight students and two technical directors, but we had to add three more terminals. The students made substantial contributions to all the problems they worked on and even came up with innovative ways of looking at our problems.

(U) On the fifth and tenth weeks, the DSP students obtained very important results by substantially solving two of the problems, convincing the last of the skeptics that this program was very worthwhile. The real payoff was not the contribution to our product, impressive as those contributions were; the real payoff was the pipeline. Incredibly, before they met us, two of our DSP students, juniors, had not been planning to go on to graduate school following their senior year. These two were performing exceptionally well in their current, demanding academic programs and, ironically, made the most direct contributions to the most significant results of the workshop. One went home from the DSP with a surge of confidence, applied to all the top graduate schools and is now in a Ph.D. program on a fellowship. The other wished to become an NSA employee, but we talked her out of joining us right away. She took all pure mathematics courses her senior year and is now in graduate school in a Ph.D. program on a fellowship.

EO 1.4.(c)
P.L. 86-36

DSP 1991

~~(C)~~ The 1991 DSP was also very successful. With the 1990 success, it was easy to recruit three top technical directors. They led a larger group of participants, including some 1990 returnees, to complete solutions of three problems and significant results on four others. We had 20 Sun terminals for both the technical directors and for this group of 13 bright young mathematics students, which included two graduate students, four beginning graduate students, three seniors, two juniors, and two sophomores. Eight problems were chosen, from Z, C6, R2 and W and presented to the students. By and large, the problems were quite difficult. Nevertheless, significant progress was made on several of them.

[redacted]

~~(TSC)~~ Success was also achieved on the COMSEC problem [redacted] In addition, important progress was made on the W problem. All but one of the submitted problems were addressed and two or three additional short problems were introduced.

~~(C)~~ Three technical directors and three problem supporters were on hand for the 1991 session. The participation of these agency mathematicians was crucial to the program's success. An overview of 30 years of cryptologic mathematics was distilled into the first two and one-half weeks. Concurrent with these introductory talks on the problems and certain topics in cryptanalysis, the students selected a problem or problems (most settled on one or two) and worked individually, or together, or with one of the NSA mathematicians towards a solution.

(U) A series of Wednesday "progress reports" was held in which students would present work in progress, partial solutions, difficulties encountered, etc. These talks were attended by interested personnel from around the Agency. It was found that these progress reports were valuable to the technical directors, technical support personnel, outside listeners, and students alike.

[redacted]

(U) At the end of the 1991 DSP session, some of the students gave talks on their work to audiences in Z, C6, and R51. Three of the students wrote R51 mathematics papers on their work. In October 1991, [redacted] Chief R51, briefed the final report on the DSP for 1990 and 1991 to the Director NSA.

(U) We can say without reservation that every one of the thirteen students of the 1991 DSP left NSA a better mathematician than when he or she arrived. Each developed a perspective of how mathematics can be used to create and destroy, to win and lose, and to succeed and fail. They saw how their country needs their skills and they came to appreciate how these same skills can be used as a potent weapon against their country.

DSP 1992

(U) The 1992 DSP session clearly eclipsed the success of the previous two summers in terms of attracting its most talented group of young mathematicians and solving cryptologic mathematics problems. We had an exciting set of top-notch applicants for the 1992 DSP. This can be attributed to the NSA recruiting process which has helped to generate a very impressive group of more high-caliber students than in previous years. Thus, this third annual DSP brought together 16 matchless mathematics students for the 12-week session which commenced on 3 June 1992. Three technical directors provided full-time mathematical support, and 21 Sun terminals were used in this year. Of the 16 DSP participants, 13 were first-timers and 3 were returnees.

~~(S-CCO)~~ As before, the first one and one-half weeks consisted of cryptanalytic orientation and workshops, comprehensive programming in C, and lectures on classified mathematical techniques. The week of 15 June focused on problem presentations. Eight difficult problems were chosen from Z, W, C61, R21 and R51.

[redacted]

(U) For the latter, the team working on Golomb's Conjecture successfully programmed a sophisticated algorithm for generating all sequences with the desired properties and tested the conjecture on the output. Their results will appear in an outside technical journal.

EO 1.4.(c)
P.L. 86-36

DSP 1993

~~(C)~~ The group of 17 new students gathered for the 1993 DSP set a new standard which will be difficult to exceed. Nine problems were presented to the group and all but one received attention. The group met in a new room in the R&E building which was especially designed for the DSP. Each student and each of the four technical directors had a SUN work station tied in to a CRAY computer. The room is large with ample blackboard space for lectures and discussions.

EO 1.4.(c)
P.L. 86-36

~~(TSC)~~ The summer started with the usual course on cryptologic mathematics and the presentation of the problems. Once the students settled down to work there was no stopping them. The first solution came in the

[redacted]

DSP's Future

~~(C)~~ We hope austerity will not diminish our ability to continue this program and attract outstanding summer employees. The need for brilliant young mathematicians will only increase as cryptology and cryptanalysis become more and more mathematical. We need to cultivate deep roots within the academic mathematics community and establish a network of academic consultants who understand our mission.

(U) All this makes the Director's Summer Program even more important and timely.

DOCID: 4009689

CRYPTOLOG
March 1994

OPEN SYSTEMS: What Does it Really Mean?

[redacted]
A7 Architecture and Planning Branch

P.L. 86-36

Ask any dozen people what the term "Open Systems" means and you're likely to get a dozen different answers. Some interpret "open" very literally and presume that they can build an open system by throwing together any mix of commercial products and *voila*! they have one. At the other end of the scale, some equate open systems with particular products and brand names. "Open" is confusing at best because open systems really aren't open at all. A far more accurate expression is "Standards-Based Systems" since open systems are based on open standards, and standards imply restrictions.

For instance, the specification for an electric outlet is an open standard. The availability of such a specification allows any entrepreneur to produce electric outlets for public consumption at a reasonable cost, and allows others to produce components which work in concert with them; most notably electric plugs attached to electric appliances.

The same general definition of open standards applies to the computing world. The most visible example of an open computing standard is the IBM PC hardware specification. When IBM released the PC in the early 1980s, they did something unprecedented (for them at least). They released the hardware specification to the public in order to encourage entrepreneurs to develop products for their microcomputers. The result was a revolution that spawned an entire industry and made desktop computers as familiar to the average American as a television set.

Another prominent example of an open computing standard is the X/Windows specification. Developed and refined almost completely in an academic environment, it has had a profound influence on our current view of corporate computing. The X/Windows specification is available from the Massachusetts Institute of Technology (MIT) for the cost of the medium on which it's delivered, or alternately the cost of the phone call required to download it from the Internet.

Open standards, by definition, are supposed to be non-proprietary. This means that no individual or organization holds exclusive rights to specifications adopted as open standards. But the fact that the standards are publicly available doesn't necessarily mean that they are in the public domain. Formal specifications are often protected by copyright, and the product characteristics they define may be protected by patent. Therefore, the existence of an open standard doesn't always imply that you can get it and use it for nothing. Access to the specification and its subsequent use may be contingent on payment of a license fee or royalty of some sort. Note there is nothing in the DoD or NSA open systems standards documentation that states that all open standards specifications are to be available at no cost.

To recap: first of all, when we use the term "Open Systems" we're really referring to standards-based systems. Those systems are based on "open standards" which are available to the general public, but their use may have some strings attached such as royalties or license fees. With that understood, we can move on to the real issue, which is:

What "Open Systems" means to the typical NSA employee

- To computer users, it means more robust software with a consistent "look and feel," more effective ADP support, and more rapid delivery of essential capabilities and services at lower overall cost.

- To acquisition planners and managers, it means that at long last there are consistent metrics by which proposed hardware and software acquisitions can be evaluated for "goodness of fit" in the NSA computing environment

- To computer system developers, it means that there will be a stable, predictable, and consistent hardware, software and communications baseline available to them because everyone is playing by the same rules. The most obvious benefits to be realized by developers in such an environment are: vastly improved opportunities for software component re-use, significantly reduced development time, and dramatically reduced support costs. It also opens the door to effective sharing of resources across organizational boundaries.

Our computer users are the big winners because, by conforming to a globally accepted set of specifications for hardware, software, and communications (i.e., open systems standards), it's far more likely that any given application will have to be written only once with full confidence that it can be easily moved to any other platform which provides the same specified services and interfaces. Not only that, but also many of the formerly "error-prone" parts of software development, like programming for communications and graphics, can be minimized through re-use of highly reliable "canned" components. Since such functions are fundamentally the same on every computer because of inherent portability, users will be able to move from one conforming system to another (even on a different vendor's hardware) and perform the same without culture shock or retraining.

Obviously, it's important during the process of selecting components for new systems to be able to stick exclusively with products which conform to the standards. However, it's more important to understand not only the basic character, but the limitations of the standards as well, because there are very few standards-based products on the market which reflect a one-for-one mapping of standards specifications to features. Vendors make their standards-based products desirable by adding attractive bells and whistles which make their products easier to use or more powerful than their competitors'. It's these value-added features which sometimes tend to lock us into specific vendors and eventually make interoperability and portability of applications difficult. Knowledge of the standards allows computer system developers to avoid product features which jeopardize portability and interoperability, or allows them to at least associate some degree of risk with those features should a decision be made to take advantage of them in an operational application. Caveat emptor!

In summary, "Open Systems" is simply another way of referring to standards-based systems. ***It is essential to remember that standards are specifications and not products.*** It is equally important to remember that standards do not carry the force of law. Rather, they are guidelines to be followed. If the standards inhibit getting the mission accomplished or blow the budget, the non-standard specifications are the correct choice.

The rewards for following Open Systems Standards will be a significant improvement in the way we design, develop, and support systems, more productive users, and reduced cost at every step of the acquisition and support cycle. The NSA standards baseline is the NSA Open Systems Standards Profile, which is an adaptation of DoD's standards—the Center for Information Management's Technical Reference Model (CIM TRM).

The success of the whole open-systems venture depends on the willingness of vendors and developers to build products which conform as closely to the standards as possible. It also depends on the willingness of acquisition officials, from division level on up to the key components, to support the purchase of those products which conform to standards, with full awareness that doing so may sometimes mean sacrificing power and convenience in favor of portability and interoperability.

That, in a nutshell, is a view of Open Systems. Anyone interested in getting a copy of the NSA Open Systems Standards Profile, in learning more about Open Systems at NSA, or becoming actively involved in the Open Systems implementation process should contact [redacted] the chairman of the NSA Open Systems Working Group. Ken can provide information on DoD and industry standards efforts and can point you toward sources of information and working groups already involved in formalizing an NSA Open Systems implementation process. He may be reached via NSA e-mail by sending a message [redacted]

P.L. 86-36

The CIM TRM and the NSA Profile

[redacted]
A7 Architecture and Planning Branch

P.L. 86-36

What's in it for NSA? Why are we cooperating with the DoD Corporate Information Management (CIM) Office?

(U) The CIM TRM (Technical Reference Model) is the statement of its open-systems standards available. It describes the entire open computing environment (i.e. hardware, operating systems, communications, etc.) in terms of standards. The intent is to create a set of standards that DoD can use to increase its buying power, decrease the cost of what it buys, and give DoD more of a voice in the development of future computer products. NSA is working on adapting the CIM TRM to meet NSA's needs, not because of a DoD requirement, but based on our self-interested desire for a framework of specific standards which will let us buy hardware, software, and integrated systems that will work together with a minimum of tinkering and that will continue to work together without constant pampering. The NSA adaptation of the TRM is known as the NSA Open Systems Standards Profile, or "the Profile" for short.

Why Does NSA Want the Profile?

~~(C)~~ Over 75 percent of the total cost of any computer system made today is for maintenance. The lion's share of that cost is for support personnel. At NSA today, there is about one identified computer support person for every 8-10 computers. However, that ratio is understated. There are a lot of computer gurus working under non-computer COSCs who spend most of their time doing computer support tasks. With NSA being told every year to justify its budget using ever more restrictive criteria, this has to change. What is needed is a strategy which reduces the support tail. Adoption of a standards-based architecture can provide the foundation for such a strategy.

(U) The purpose of the NSA Standards Profile is to provide the guidelines for that standards-based architecture. Rather than a list of "must do" actions and "must use" products, it talks about what the standards are, which ones are currently fully enough developed to be widely and most easily used and which ones we are looking at for the future. The Profile also talks about our legacy systems. While those systems have served well, they do not and often can not support our need to move toward an open systems environment.

(U) An open standard is based on widely recognized and used specifications which are in the process of being made into formal standards, or which have already been formally adopted as standards by groups like the American National Standards Institute (ANSI) or the International Standards Organization (ISO) and catalogued by the National Institute for Standards and Technologies (NIST).

(U) Through judicious application of appropriate standards, the Agency hopes to improve:

- ***user productivity*** with a consistent user interface, intelligent integration of applications, corporate data sharing, and consistent security control;
- ***developer efficiency*** with more common development efforts for problems, providing a standards-based information-processing environment The best way to improve developers' efficiency is with the use of Commercial Off-the-Shelf (COTS) and Government Off-the-Shelf (GOTS) software, setting up mechanisms for component reuse and resource sharing;
- ***application portability*** from one type of computer to another and scalability (from one size task to another) through attention to standards and a deliberate effort to address the largest number of computers possible;
- ***opportunities for interoperability*** of systems and applications through a common, standards-based communications and computing infrastructure and common services; and
- ***manageability of systems and resources*** by simplifying development and acquisition processes.

(U) At the same time NSA wants to reduce:

- ***dependence on vendors*** by acquiring or developing interchangeable, non-proprietary software;
- ***life-cycle support costs*** by eliminating duplicate development efforts, improving maintainability, and improving training.

What Needs to be Done?

(U) Agency seniors personally supported and directed the Profile's development by creating an all-seniors NSA Open Systems Steering Group (NOSSG). In turn, the NOSSG selected mission-critical ADP personnel to chair and staff the NSA Open Systems Working Group (NOSWG). Subgroups consisting of experts from all relevant key components were then formed:

Programming Services classified existing and proposed programming languages according to their conformance to ANSI, ISO, and POSIX standards.

User Interface Services standards describe how a user will interact with a computer's programs, especially the graphical display of information. NSA will use the X Window standard and the DoD Human-Computer Interface Style Guide.

Data Management Services: standards, for database designers mostly, describe how data will be stored, accessed, modified and loaded.

Data Interchange Services: another set of standards mainly for database designers, dealing with data exchange formats, from software package to software package.

Multimedia Standards: deal with how multiple types of information (text, audio, pictorial, tactical, etc.) will be presented, edited, or integrated.

Network Services: how computer hardware and related communications nets will work together to deliver information and operate.

Operating System: the basic package of instructions that turns a delicately carved piece of sand into a device that can process information. NSA has selected POSIX as its future standard operating system.

Security Services: interacts with all the other standards to insure that data will be accessible only to authorized individuals, and that data will not be maliciously or accidentally destroyed or corrupted.

Management Services: for software tools used to keep software, hardware and network communications systems working and productive.

Real-Time Services: for systems that need to collect, process, or evaluate information as it is occurring;

(U) Next, an implementation mechanism was built for the Profile. The NSA Open Systems Standards Profile will be implemented by a transition plan prepared as an accompaniment to the profile. It provides a road map for getting from where we are today in terms of our computer capabilities to where we expect we will need to be in the future. This means the plan will provide for compatibility testing and information dissemination; create a mechanism for projecting future requirements; and for investigating new standards and products to satisfy future needs.

(U) Creating a way of discussing and classifying existing standards took a lot of time. But this classification system will allow developers and managers to understand how much risk they are taking when selecting standards for a project and the various products that use that standard. The Profile does this by breaking standards into six levels:

1. Now: a product conforming to this standard can be freely used. The investment risk of using a product meeting this standard is minimal.

2. Now: a product conforming to this standard can be used with prior approval. The investment and risk of using a product meeting this standard must be considered. Also, the standard may not be in line with established guidance.

3. Future: a product conforming with a proposed standard can be used with prior approval. The standard is still moving toward approval, can still change unpredictably, and so long term investment risk exists.

4. Gap: no recognized standards exist for this capability or product availability is limited. The risk of using such a product is moderate to high and requires prior approval.

5. Void: while NSA hopes standards will emerge in the future, none have yet. The risk of using such a product is extremely high. Since products in this area have no standard, their use is discouraged.

6. TBD: a standard has been proposed, but either has not begun evaluation or is in the early stages of being evaluated. Since very substantial changes can occur, the risk level is high and prior approval is recommended.

P.L. 86-36

P.L. 86-36

How Will the Profile Affect You?

~~(FOUO)~~ Some groups will benefit immediately, while other groups will see no changes or benefits. However, over time (at a guess, five to ten years) everyone stands to benefit. Examples are: the Agency needs to constantly update the computers we use and the [redacted] communications system.

[redacted]

~~(C)~~ [redacted] The solution to these concerns that the Profile encourages is to decrease the cost of our equipment purchases by adhering to DoD and government-wide standards while using our software-development resources for problems that need to be solved on a custom or time-critical basis. This benefits analysts by freeing up more programmers to perform software work for them. Computer professionals will benefit by having more time for developing software for analysts and needing to spend less time maintaining existing systems.

~~(C)~~ [redacted] initially benefited no one. It tied almost no one to almost nothing. But it has since become invaluable. It delivers information electronically, ending the drudgery of sorting out the mail twice a day. Also, you can now send e-mail to a person instead of spending days playing "telephone tag."

P.L. 86-36

(U) The NSA Open Systems Standards Profile is designed to be a living document providing advice—not guidance—about open standards rather than products. It is intended to be periodically updated as the technology changes. It is NSA's response to the challenge not just of the DoD's CIM—but more important, to the changes that are accelerating as the Information Age finally moves beyond its barest beginnings. ***Within fifteen years NSA must either adapt to that age's requirements or die.*** The adaptation process will require a wholesale reinvention of NSA; the Profile will be one of the guideposts of that process.

(U) Information on the Agency's open systems efforts is available in NetNews under the heading of org.noswg. This contains the minutes of NOSWG meetings, and NOSWG subgroup meeting notes and working drafts.

EO 1.4.(c)
P.L. 86-36

DOCID: 4009689

CRYPTOLOG
March 1994

The Closing of NSGA Philippines

P.L. 86-36

[redacted] USN

This article is dedicated to all those persons who perished as a result of the eruption of Mount Pinatubo Volcano.

It began in February 1991. A volcano which had remained dormant for over 600 years was now showing signs of coming back to life again. Although no one could have foreseen the extent to which Mother Nature's fury would be cast upon the Republic of the Philippines in the months to follow, it began with a series of what seemed to be innocuous ventings of steam from the depths below. By early March 1991, enough venting had occurred to warrant some professional investigation and analysis. Several volcanologists and seismologists arrived on island to determine the extent of the activity. There, scientific readings and measurements told them that the mountain was capable of erupting within twelve months.

With this information, Clark AB, located approximately 9 miles from the volcano, soon began publishing information in order to prepare the base for a possible evacuation. A plan was quickly put together by on 6 June 1991, when the eruption of Mount Pinatubo was almost a reality.

While each tenant command aboard Clark AB passed on the seismological information to its people, NSGA Philippines had been working more diligently on a different approach. Specifically, a plan to close down the command, which had been drafted some twelve months earlier in the event the base negotiations with the Philippine government were unsuccessful, had been dusted off and examined. The plan essentially listed all those actions necessary to close and disestablish a command. Its 180-day timeline was merely modified into separate 3-day, 7-day and 30-day action processes, depending entirely upon Mother Nature's cooperation, of course.

As I recall, on 9 June 1991 word had quickly spread that the mountain could blow within a matter of days. It was venting more, and the color of the steam had changed from a pure white to grey within the past few days. Venting could now be seen from different sections of the mountain as well.

At 1700 hours on 9 June 1991, an emergency recall of NSGA Philippines was ordered. All leave was cancelled. The skipper briefed us on the latest scientific findings, which concluded that there was a good chance the volcano would erupt within 48 hours, and that a decision to evacuate Clark AB could come as early as 0500 the next morning. The theme was "don't panic but be prepared to go." Earlier that week a list of items that should be readied in case of an evacuation was provided to each person and family as well as being posted throughout the command. Also during the previous week, information concerning lodging, transportation, food, and a host of other items was similarly disseminated.

With 100 percent of the command recalled, a Phase I (precautionary emergency destruction) was ordered by the Commanding Officer and passed on to the CDO to carry out. For several hours and until almost midnight on 9 June, we destroyed as much classified information as we could. What had been an otherwise quiet weekend within the operational spaces of NSGA had turned into a command-wide emergency destruction operation within a matter of hours. What we could not destroy under Phase I, and all Phase II and III material, was boxed up, double-wrapped, and would eventually be couriered to Subic Bay Naval Station, which was designated as the evacuation safe-haven site; we intended to return to Clark after the eruption.

At 0500 on 10 June, the order to evacuate Clark AB came. All personnel, less a five-man closure team, mustered on the flight line as previously instructed. Within a few hours, a convoy of some 25,000 military, civilian and dependent personnel were on their way to Subic Bay, some 35-40 miles away. The trip lasted approximately five hours, and everyone arrived safely. The five-man closure team from NSGA Philippines remained behind to continue the destruction of classified material and the powering down of electronic equipment.

Without lights and with flashlights in hand we continued to check each safe, desk, and cabinet for classified material. What little we did find, we destroyed. However, owing to the sheer volume of paper products in the building, it was clear that a 100-percent sanitization certification could not be given unless all paper products were destroyed.

The First Eruption

On 12 June 1991 at 0700 the five of us who constituted the closure team once again departed the barracks for the Operations Building to continue our search for classified material. Armed with our flashlights and radios, we continued the search. At 0848, however, a call from Alpha Alpha (the CO) was received. *"This is Alpha Alpha, major eruption, get out of the building."* Instinctively, I began to stuff the burn-bags back into the safe and had planned on securing the safe. This took approximately 45 seconds. My second thought was to call Subic Bay and advise them the eruption had occurred and that we were evacuating. By this time a second call from the radio was heard: *"Major eruption, get out of the building NOW!!"* Not knowing the extent of the "eruption" and whether or not the pyroclastic flow would reach the base (which reportedly travelled at a rate of 125 miles per hour), nor what I would find once I got outside of the building, I was determined to notify NSGD Subic before I exited the building.

After I secured the material, I ran, flashlight in hand to one of only two phones working in the Operations Building. The building was completely dark and smelled of must. By this time, approximately one to one and a half minutes elapsed since the first radio call from Alpha Alpha. Just as I began to dial Subic's telephone number, I received (in a much more direct tone) another call from Alpha Alpha, which meant that if I knew what was good for me, I would get out of the building now. I did just that.

Upon running out of the Operations Building, I looked to my starboard side. I was in awe! What had for months been a steam venting "hill" had transformed itself into a monstrous grey plume rising 88,000 feet. It looked exactly like a nuclear detonation. The surprising thing was that it made no noise at all.

I reached the vehicle parked outside the gate where the skipper and the other three were waiting, motioning me to hurry. We departed for the barracks approximately 1/4 mile away to pick up our bags. With sirens blaring we retrieved our "go bags" and headed to the flight line (the primary evacuation point). Upon arriving at the flight line about 10 minutes later, we saw the plume, which at one point appeared to be overtaking the base, now seemed to be retreating in the opposite direction, owing to a shift in the wind. In any case, an order to proceed to the secondary evacuation point was given and we drove through town approximately 10 miles to Mount Arayat. There we waited approximately five hours before receiving the all-clear sign where we returned to Clark AB. As I found out later, we evacuated to Mount Arayat because of the uncertainty of the pyroclastic flow.

The skipper didn't go to Mount Arayat; he and Lt. Col. Hurst, Commander of the USAF ESS element at Clark AB, remained on the base. We eventually met up with him when he decided to leave Clark and proceed to Subic. It was just too dangerous to stay. So at 1800 hours on 12 June 1991, the five of us departed Clark AB for what we thought to be the last time.

We arrived in Subic Bay at 2145 that evening, met by the OIC, XO (Lt. Cdr. Keith Ludwig) and the CDO. Berthing arrangements were made in advance and we called it quits for the evening.

The next two days were spent trying to keep a 137-man organization and its detachment of approximately 50 sailors together, fed, and informed. Additionally, destruction of the classified material transported from Clark to Subic continued. This time, however, the Commanding Officer ordered a full emergency destruction of all Phase I, II, and III material. His rationale, I believe, was that after having personally seen the eruption just a few days ago, it was important to destroy as much as we could while we still had the chance. After all, it would be easier to ask for another copy of this or that, than to justify what we lost, why we lost it and the extent of compromise. His decision was certainly the correct one under the circumstances.

The emergency destruction of Phase II and III material took about 18 hours. Dumpsters were made into infernos, shredders were used around the clock. Axes and sledgehammers were used for the disk-packs and equipment. Of course, accounting for the items destroyed was important. During the entire period, a strict accounting of all of the items destroyed was maintained. The resultant 92-page destruction report containing 5500 line items was an achievement in itself, considering the circumstances under which the destruction and reporting took place. There was no power (we had portable generators hooked up outside of the building, one or two of which belonged to personnel from the detachment); we had been eating MREs for the past three days; there was little or no potable water (we flushed the commodes with sea water); and we were in the midst of a non-combatant evacuation (NEO) of all civilian and dependent personnel to the island of Cebu for transportation to the United States. Needless to say, there was a lot going on at one time.

The Major Eruption

We continued the destruction of classified material and tried to organize the two commands (NSGA/NSGD) into one cohesive unit as best we could. But on 15 June, all that changed. At approximately 1000 Mount Pinatubo erupted again. This time the plume reportedly reached 120,000 feet or so. But this time we were all located at Subic Bay, well out of danger zone, or so we had been told.

The very instant the mountain erupted that second time, Typhoon Yuna (or Yuma, I can't recall) happened to blow our way. As a result of that eruption, a plume of 120,000 feet of ash blown by the winds of the typhoon not only blanketed Clark AB, but wiped out Subic Bay Naval Station, covering it with 10-12 inches of ash fallout. The sheer weight of ash mixed with water toppled buildings left and right. Approximately 30-40% of Subic Bay's building structures had collapsed. Moreover, the magnitude of the eruption was so great that it put much of the Philippines in total darkness for over 28 hours. It reminded me of a New England blizzard, except for its color (destructive grey) and the surrounding temperature (90 degrees).

"Gainfully employing" members of both NSGA and NSGD had new meaning now. Shoveling crews were assembled and dispatched to various locations and buildings to remove the fallen ash to prevent further damage and collapse. Roads were plowed, sidewalks cleared and power lines hosed off. Within approximately 10 days, Subic Bay was operationally restored.

For the next few weeks, plans were made to close down NSGA Philippines and transfer its people to other bases. Upon receipt of the go-ahead, PCS orders began arriving via fax and within three weeks, the admin crew had completed all transfer evaluations, fitness reports, medical screenings and all of the other associated paperwork which normally accompanies a PCS transfer. By the end of July approximately 85% of the command had transferred. It was a remarkable achievement administratively, and a testament to the professionalism displayed by the admin crew.

The remaining weeks were largely spent deinstalling, inventorying and shipping over $15 million worth of sensitive electronic equipment from the Operations Building at Clark AB to Subic Bay for transfer to the U.S. Additionally, the closure team, assisted by members of the detachment, ensured that all NSGA members' personal property (each household and barracks room) and POVs were packed and shipped.

On 1 September 1991 at Cubi Point, a brief change of command ceremony was held between CDR Bernas and LT Wickham. Lt. Wickham, now officially the Commanding Officer, had bidden farewell to the remaining few as we boarded Hawaiian Air for home.

To say the least, it was an eventful eight-month tour. I did however enjoy those months and have learned many things as a result of them. I will especially miss the people of the Philippines and the food. And I will always remember the team work which was displayed by the sailors of NSGA Clark and NSGD Subic. It was teamwork which kept us going and brought us through 90 days of frustration, danger, and uncertainty.

To all of you, Godspeed.

ACKNOWLEDGMENTS

Special thanks are due to:

CDR Barry L. Bernas, USN, Commanding Officer, U.S. Naval Security Group Activity, Clark AB, Republic of the Philippines;

LT Kenneth Wickham, USN, Officer-in-Charge, U.S. Naval Security Group Detachment, Subic Bay, whose staunch leadership and concern for the safety of the crew prior to and after the emergency were truly inspirational.

DOCID: 4009689

CRYPTOLOG
March 1994

P.L. 86-36

EUROCRYPT '92

(U) Eurocrypt '92 continued the string of successful congresses sponsored by the IACR (International Association for Cryptologic Research). For the first time, the meeting was hosted by an Eastern (Central?) European country: the venue was Balatonfüred, Hungary; the dates, 24-28 May 1993.

(U) Attendance was announced as 253, but a preliminary registration list which was circulated contained only 240 names. From that preliminary list, we have the following accounting, by home address, of the registrants:

Germany	42
U.S.A.	30
France	27
Hungary	15
Great Britain	14
Sweden	14
Italy	12
Austria	10
Switzerland	10
Netherlands	8
Denmark	7
Japan	7
South Africa	5
Spain	4
Belgium	4
Norway	4
South Korea	4
Canada	3
Romania	3
P.R. China	3
Israel	2
Australia	2
Yugoslavia	2
Czechoslovakia	2
Singapore	2
Saudi Arabia	1
Egypt	1
Finland	1
Ireland	1

(U) There were some prominent "cryptologists" who did not attend: Adi Shamir of Israel (we've heard that he may by preparing a book, probably containing his work on "differential cryptanalysis"); Ron Rivest and Silvio Micali of MIT; Canada's Claude Crépeau and Gilles Brassard; Gus Simmons of Sandia; Agnes Chan of Northeastern; David Chaum of CWI, Amsterdam; Louis Guillou of France, and Ivan Dåmgard of Denmark. All of these have been more or less regular attnedants at previous IACR meetings. Three world-class mathematicians attended: Arjen Lenstra of Bellcore, Harald Niederreiter of Austria, and Andrew Odlyzko of Bell Labs.

(U) The General Chairman was Tibor Nemetz of the Mathematics Institute, Hungarian Academy of Sciences. I understand that some people experienced difficulties with bus connections, but I personally had no problems. As usual, I did not participate in any of the scheduled social activities, even eschewing the communal lunches and dinners. This policy is probably an error, and in the future I may try a more friendly posture.

(U) Rainer Rueppel, the excellent Swiss (formerly with Crypto AG) who is operating a free-lance consulting business, chaired the Program Committee, which included some of the best researchers in the community: Kevin McCurley (Sandia), Yvo Desmedt (University of Wisconsin, Milwaukee), Joan Feigenbaum (Bell Labs), Jovan Golic (University of Belgrade), Tor Helleseth (University of Bergen) Peter Landrock (University of Århus), Tatsuaki Okamoto (NTT Labs), Jennifer Seberry (University of New South Wales, Australia), Othmar Staffelbach (Gretag), Jacques Stern (ENS-DMI), and István Vajda (University of Budapest.)

(U) Of the 88 papers submitted, 54 were evaluated favorably, but only 35 could be accepted. The leading countries, with their acceptances/submissions, were:

USA	8/14
Germany	7/13
Japan	4/12
France	3/7

One was submitted from Russia, two from China. The Program Committee also served as chairmen for the sessions.

P.L. 86-36
EO 1.4.(d)

(U) The program was (for me) awkwardly scheduled (maybe it was convenient for some Europeans who could drive from home in a morning). In the past there had been a lively informal rump session on Tuesday night, as there was again this year, but in compensation Tuesday afternoon had always been left free. This year the free time was Monday morning (!), and Tuesday afternoon from 4:00 till 6:00 was devoted to a potentially controversial panel discussion on "trapdoor primes and moduli," so there was little respite from the concentrated dosage of research reports. Altogether 34 papers were presented (one cancelled), each allotted 15 to 30 minutes, and the schedule was adhered to fairly strictly (good!). The order of the program, which will be followed in this report, was as follows:

Monday afternoon: secret sharing, hash functions.

Tuesday morning: block ciphers, stream ciphers.

Tuesday afternoon: public key I, factoring, panel discussion.

Wednesday morning: public key II, pseudorandom permutation generators.

Wednesday afternoon: complexity theory and cryptography I, zero-knowledge.

Thursday morning: digital signatures and electronic cash, complexity theory and cryptography II.

(U) Three of the last four sessions were of no value whatever, and indeed there was almost nothing at Eurocrypt to interest us (this is good news!). The scholarship was actually extremely good; it's just that the directions which external cryptologic researchers have taken are remarkably far from our own lines of interest.

(U) There were no proposals of cryptosystems, no novel cryptanalysis of old designs, even very little on hardware design. I really don't see how things could have been any better for our purposes. We can hope that the absentee cryptologists stayed away because they had no new ideas, or even that they've taken an interest in other areas of research.

(U) I had thought of offering a representative "theorem" from each of the papers, so you could judge for yourself that the paper was without interest (that is, except to the small number of researchers whose livelihood depends upon being able to publish in that field), but most of them require elaborate definitions of terms or symbols, and that extensive a review is merited in only a few cases.

(U) Also, it should be noted that in some cases authors had, in the time between submitting the preliminary abstract and delivering the talk, significantly improved (or corrected) the presentation. In such cases, the change was usually great enough, and my understanding so poor, that instead of trusting my memory for what was said I shall usually rely on the printed abstract.

(U) The first six papers were on secret sharing (2) and hash functions (4). Alfredo DeSantis (University of Palermo) spoke on "Graph decompositions and secret-sharing schemes," a silly topic which brings joy to combinatorists and yawns to everyone else. Gus Simmons, Doug Stinson, and Marijke de Soete are the big names here, and Stinson is a coauthor of the current work, along with the Italians C. Blundo and U. Vaccaro.

(U) Yvo Desmedt, the "mad Belgian," seems to have caught on at the University of Wisconsin, Milwaukee. He's also been getting respect from the IACR, being on the Program Committee and also on the Board of Directors. As befits a person of honor, he no longer rattles the rafters with his staccato delivery, but his interest to us has not changed. His offering this year was "Classifications of ideal homomorphic threshold schemes over finite Abelian groups." His student Yair Frankel is listed as coauthor.

(U) The session on hash functions was as interesting as any. Marc Girault (SEPT, Caen, France) led off. His coauthors were Henri Gilbert, who has done some good work in the past on FEAL, and Thierry Baritaud, both of CNET, Paris, with "FFT-hashing is not collision-free," a criticism of Claus Schnorr's hash function scheme which had been presented at the rump session of Crypto '91. Unfortunately their work was, as Girault admitted, "essentially the same" as the attack by Daemen, Bosselaers, Govaerts, and Vandewalle given at the rump session of Asiacrypt '91.

(U) But have no sympathy for the much-maligned Professor Schnorr (University of Frankfurt)! In an oft-replayed scenario, he was the next speaker, and presented ("FFT-Hash II: efficient cryptographic hashing") a small revision of his sullied scheme. Perhaps it is beneficial to be attacked, for you can easily augment your publication list by offering a modification.

(U) Jim Massey is a prominent American scholar and educator (he's been at the Swiss Federal Institute of Technology, ETH, for many years, and has produced several of the best young cryptologic researchers) whose most recent doctoral student—he's just completed his degree, but I don't know where he'll go next—Xuejia Lai, presented their joint effort, "Hash functions based on block ciphers." A hash function is a special type of function which collapses long messages

into a compressed representation; one thinks of their application as being in signature or authentication *schemes rather than encryption*: Lai and Massey presented some sound theoretical analysis in the case that the function is constructed by iterating an easily computable function. As usual, all the functions considered are very general; no specific proposal is considered. They conclude that it is not easy to produce hash functions which satisfy the usual security concerns.

(C) One specific hash function which has been proposed is Ron Rivest's MD5 algorithm, which produces a 128-bit output for an input message of arbitrary length. Tom Berson, in a very interesting paper, "Differential cryptanalysis mod-2^{32} with applications to MD5," showed that the popular "differential cryptanalysis" technique, introduced outside by Adi Shamir [redacted] can be applied effectively in this situation. Shamir's method has so far been used only in attacking systems which use addition modulo 2, but Berson showed that it can be adapted to fit the mod-2^{32} addition of MD5. This would not have been a particularly attractive piece of work, but Berson carried out quite a bit of tricky analysis, showing commendable analytic power. Berson is the retiring President of the IACR, but I had no previous knowledge of his technical prowess. His work applies only to a single round of the MD5 process and will probably not cause a revision of the algorithm, as there is no reason to think that consecutive rounds can be attacked simultaneously. In particular, Berson's attack poses no threat to the NIST "secure hash standard," which is based on MD4.

(U) The busy Tuesday began with three talks on block ciphers. The first represented a Mitsubishi attack on the NTT FEAL algorithm. It has become popular to pick on FEAL, and several other attacks have been presented at IACR conferences. This one is again based upon possession of matched plain and cipher, and seems to require quite a bit less than its predecessors. They (Mitsuru Matsui and Atsuhiro Yamagichi, "A new method for a known-plaintext attack on FEAL cipher") claim to be able to solve FEAL-4 with 5 plain texts (and 350 seconds of processing), FEAL-6 with 100 plain texts (and 40 minutes of processing), and FEAL-8 with 2^{15} plain texts (but their computer is not large enough to see this through).

(U) Kaisa Nyberg, of the Finnish Defense Forces, now gives a Bonn address (maybe she's at some joint European command). She has been doing good work for several years, and her talk "On the construction of highly nonlinear permutations" was not disappointing. Her interest lies in Fourier spectra of Boolean functions and she is particularly enamored of bent functions. She defined the nonlinearity $N(f)$ of a function $f : F^n \rightarrow F^m$ to be the minimum (Hamming) distance from f to the set of affine functions—that is, f and any affine function on F^n differ by at least $N(f)$ (and in at least one case differ by exactly $N(f)$) values in their truth-table representation. She was able to compute $N(f)$ for quadratic forms, and she asked if the maximal nonlinearity attained by quadratic functions was indeed maximal for all functions (of course, only the case of odd n is in question). Again, this is not new and exciting work, but she showed considerable technique in her investigations.

(U) An East German, Ralph Wernsdorf (SIT Gesellschaft fur System der Informationstechnik mbH, Grünheide; Mark King said that he had been told by his German friends that this company was composed of ex-Stasi people), presented the talk "The one-round functions of the DES generate the alternating group." This result has no cryptanalytic application, but it serves to answer a question which someone with nothing else to think about might have asked. I think all of us would have been surprised if the result had been otherwise, and indeed all earlier research on this problem had pointed to this answer. Everyone feels that in fact the same result holds true for 16-round DES functions (and this is the question that really merits research), and someone will in the near future prove this, though it may be considerably more daunting technically.

(U) The three-paper session on stream ciphers was shortened when Luke O'Connor (Waterloo) failed to appear to present "Suffix trees and sequence complexity," but from the abstract we can see what he had in mind. He has seen Rainer Rueppel's beautiful work on the linear complexity of a sequence (the length of the shortest linear shift register which will generate the sequence), he is interested in using Kolmogorov complexity to generalized the finite case to a "semi-infinite" analogue, and he attempts to deal with the "complexity" (that is, using *any* function, not necessarily linear). Now the methods one should use in this case are quite different, and he seems to be incorrect on one matter (he "proves" a theorem which says that the expected degree of a random function of n variables is near n/2—I'm no statistician, and I know statisticians can prove wonderful things). He produced a really quite remarkable computer study (I don't see how it could possibly be true, but computer scientists have marvelous powers too) of the spans of functions which generate 100,000 32-bit sequences.

(U) Even if his results are correct (and I have on many occasions been shown how simple these things are to understand), the work is, as viewed by cryptanalytic eyes, typical of much of the best work presented at this conference: it may be good statistics (or mathematics, or computer science, or philosophy) but it is not good cryptanalysis. The methods employed would no doubt make a researcher in the appropriate science quite comfortable, but I tend to find them mystifying.

(U) The O'Connor talk was replaced by a talk which had, strangely, been scheduled to be presented at the rump session! Rafi Heiman (Bellcore), probably an Israeli, talked about "Secure audio teleconferencing: a practical solution." His concern is in permitting conference calls through a central "bridge" without the bridge being able to monitor the conversation. There are clearly a great many problems to be solved, and he was able to give us an actual audio demonstration of how the enciphered speech would sound. I was certainly not impressed, but then I've never tried to do it. Certainly security has not played an important role in his concerns.

(U) The other two talks were authored by Jovan Golic, of the Institute of Applied Mathematics and Electronics, School of Electrical Engineering, University of Belgrade. Golic has been active at other IACR meetings (both at recent Eurocrypts and at Auscrypt) but his work has never inspired me. His presentation was very good, but the collection of abstracts did not include his paper "Correlation via linear sequential circuit approximation of combiners;" instead, there were two copies of "Convergence of a Bayesian iterative error-correction procedure on a noisy shift-register sequence," presented by his much less effective coauthor Miodrag J. Mihajlevic, which provided us with yet a third copy. The first Golic talk concerned combiners with memory, and considered their linear approximations.

(U) Tuesday afternoon began with three talks on public-key systems. The first was given by Birgit Pfitzmann (University of Hildesheim), whose coauthor was Michael Waidner (University of Karlsruhe), "Attacks on protocols for server-aided RSA computation." They are attacking a protocol presented at Crypto '88 by Matsumoto, Kato, and Imai on speeding up secret computations with insecure auxiliary devices. Essentially they envision a smart card which interacts with a much more powerful "server," which is regarded as untrustworthy. The Japanese researchers had concocted an RSA-based scheme, but the Germans have found an attack which puts its security under a shade. We were certainly not interested in the original scheme, but the attack shows a certain amount of analytic ability, and the paper is worth at least casual study.

(U) Another German effort, "Resource requirements for the application of addition chains in modular exponentiation" by Jörg Sauerbrey and Andreas Dietel (Technical University of Munich), really had no cryptologic component, being concerned only with the speed of carrying out modular exponentiation.

(U) The allegation (almost certainly correct) that certain public-key systems might be implemented more securely by using elliptic curves has produced the predictable spate of papers on elliptic curves. We were fortunate to have only two such talks on the current agenda. One ("Public-key cryptosystems with very small key lengths") was by Scott Vanstone (Waterloo), working with his students Greg Harper and Alfred Menezes (the latter spoke very well at last year's Crypto). Though the emphasis was undeniably mathematics rather than cryptology, I thought the material was well presented, and that Vanstone never lost sight of the connection.

(U) The same could not be said of Brandon Dixon's talk "Massively parallel elliptic curve factoring." Dixon (Princeton; his coauthor is Bellcore's Arjen Lenstra) is obviously a very smart guy and a clever computer scientist, but his talk was devoted wholly to describing the implementation of the elliptic curve factorization method on a SIMD (single instruction, multiple data) massively parallel computer. The talk was very stimulating, well organized, and provided a useful update on progress in this area of research, but it contained no cryptology.

(U) I think I have hammered home my point often enough that I shall regard it as proved (by emphatic enunciation): the tendency at IACR meetings is for academic scientists (mathematicians, computer scientists, engineers, and philosophers masquerading as theoretical computer scientists) to present commendable research papers (in their own areas) which might affect cryptology at some future time or (more likely) in some other world. Naturally this is not anathema to us.

(U) The most interesting part of the 1992 Eurocrypt was the panel discussion on "trapdoor primes and moduli." Let us set the stage for the uninformed. One of the most critical issues facing the international cryptologic community (and also NSA) is the establishment of universal standards for various cryptologic needs. International trade and banking people, especially, are clamoring for a security system which they may use as though it were secure (they care very little about secu-

DOCID: 4009689

rity, of course, but very much about adverse lawsuits). The American NIST, which sets our policy on these matters, needs to consider a great number of issues in setting standards (it seems that everyone else expects American recommendation to become the international standard). NIST has recently announced its endorsement of (a variant of) El Gamal's public-key system for the "digital signature standard."

(C) This decision has been vigorously criticized by the RSA company, which had hoped to realize an enormous profit from the (American) patent it holds on the popular "RSA" algorithm. Of course, while throughout we refer to the extremely popular algorithm as "RSA," it was in fact first conceived by GCHQ's Cliff Cocks, following the introduction of "nonsecret encryption" ideas (Note: now known as "public-key cryptosystems") by James Ellis, also of GCHQ. This poorly kept secret has never been acknowledged publicly, and is still CONFIDENTIAL.

(U) NIST came under fire immediately, and its position became even less comfortable when the eminent number theorist Arjen Lenstra (Bellcore) demonstrated that some the choices of parameters for the proposed system would be unexpectedly weak. Lenstra apparently submitted a paper to Eurocrypt, but the Program Committee decided that the issue deserved more careful attention, so they convened a panel discussion, which proved to be an exceptionally wise decision. It was also thought that Eurocrypt was an appropriate venue for discussion, as the debate in America has acquired a certain amount of rancor.

(U) The panelists were a varied lot. Arjen Lenstra and Andrew Odlyzko are mathematicians of the highest order. Rainer Rueppel and Kevin McCurley are excellent cryptomathematicians. Miles Smid, a former NSA employee (many years ago) now with NIST, lacks the technical ability of the others but is, of course, the most familiar with the issues and their relative importance. Peter Landrock is a capable mathematician, the new president of the IACR, and Yvo Desmedt has published a number of papers. Lenstra is Dutch, Desmedt Belgian, Rueppel Swiss, Landrock Danish, Odlyzko Polish-American, and McCurley and Smid are Americans.

(U) The panel concluded that the RSA's ardent objections were based almost exclusively on financial grounds, and were therefore without merit. They discussed the two systems and found little to choose between them. Everyone knew that the patent difficulty (which applies only in the United States) had influenced NIST's decision, but no panelist quarrelled with the choice. They all agreed that the difficulty which Lenstra had found was extremely subtle (so is unlikely to have been intentionally designed) and would be most unlikely to occur by chance.

(U) Rueppel, playing the "neutral Swiss" role, sketched the many interest groups which needed to be considered, and described the algorithm which had been selected. Lenstra detailed the threats to security, and emphasized the ease with which a clever programmer could, with little danger of detection, sabotage an otherwise secure system. He described the state of the art of solving the "discrete logarithm" problem, and counselled the acceptance of a 1024-bit variable (agreed to by Smid), saying that a 512-bit variable provided only marginal security.

(U) Smid was the central speaker, and clearly felt himself to be under attack. He especially resented the implied slur on his character that the trapdoor insinuation represented, and allowed his sensitivity to prevent a balanced presentation.

(U) McCurley, sometimes a little too clever in making allusions to events or people who would be unfamiliar to much of the audience, made the valid point that DES and DSS have been the most challenged cryptosystems essentially because they were designed by the (untrustworthy!) U.S. government. He mentioned the "Biden Bill" (Senate bill 266) which, he said, authorized trapdoors in an effort to entrap drug dealers. He castigated a *Wall Street Journal* article which had described the Lenstra attack as "potentially devastating," and Lenstra agreed that he had not used such language. McCurley displayed a 2-page cartoon (which he said had appeared in April, 1992 *Discover Magazine*) which badly distorted the facts of the case. I inferred from his words that he felt the cartoon had been inspired by RSA or by one their cronies.

(U) Desmedt referred to a letter written by Marty Hellman criticizing NIST. I had all but forgotten about Hellman; he has not been active on cryptologic scene in many years, and I've always had doubts about his moral principles (by contrast, I regard Rivest as being above all this dirt). Desmedt (and several other speakers) mentioned that trapdoors are a more severe problem for RSA than for the chosen DSS.

(U) Odlyzko, always a stimulating speaker and deep thinker, described trapdoors as a "minor distraction" and the risk due to trapdoors as "insignificant" relative to the importance of an extended key length. He regards 512 bits as "do-able in a couple of years," 768 bits as "do-

DOCID: 4009689
EO 1.4.(c)
P.L. 86-36

able in maybe 10 years" and 1024 bits as "maybe not out of reach." He gave an assessment of the importance of enhanced computational power (increased by about 10^3 to 10^4 over the past 15 years: we could factor 38- to 45-digit numbers in 1977, 115- to 129-digit numbers now) relative to algorithmic improvements, and described that proportion as "typical."

(U) Landrock seems to have missed the importance of the moment. He insisted on talking of some of his own research and overstated its importance to factoring and to trapdoors.

~~(C)~~ Jim Bidzos, the aggressive RSA representative, was unable to attend, but curmudgeon Whit Diffie presented a frail RSA position (Bidzos would have much more implacable) and was essentially ignored by the panel. Jim Massey pressed Smid gently on why RSA, described (by RSA, but also by others as well, and not without good reason) as a *de facto* standard, had not been selected. I think everyone understood that financial motives weighed heavily in the decision and in the subsequent quarrels. Apparently the patent issue even now has not been resolved. One wonders about the motives (and probability of success) of the appellants. Stuart Haber of Bellcore asked how NIST would skirt the exportability difficulty. The response was that any algorithm designed principally for encryption will probably run afoul of the State Department's restriction, while an algorithm deemed to apply to authentication need meet only Commerce's more lenient standards.

(U) A few other question were asked by the audience, but they were either innocuous or too technical to be included this informal trip report.

(U) Tuesday's night's rump session, as always, was a mixed bag. The chairman was Laszlo Csirmaz of Budapest, who is unknown to me. In fact, none of the Hungarians present made any impact on the technical side, nor do I remember them for their past contribution (except Nemetz, who is not yet a cryptologist). I attended only the first 10 (of 12) talks, wandering off to bed at 10:30.

(U) Kenji Koyama of NTT presented "Secure conference-key distribution schemes for conspiracy attacks." Koyama's proposal surfaced first at Eurocrypt '88. At Asiacrypt '91 a "conspiratorial attack" (by Shimbo and Kawamura), in which two or more users conspire to overcome security efforts, sent Koyama back to the drawing board. He has now announced a modest modification.

(U) Rafi Heiman returned with "A note on discrete logarithms with special structure." He has an interesting goal: suppose that we know that the elements whose logarithms we need to able to find satisfy some special condition (such as a small Hamming weight). Can an algorithm be found which has time on the order of the square root? Heiman has been unsuccessful, and ultimately this problem is unlikely to contribute much, but it would be a significant achievement if it could be resolved in the affirmative (or in the negative!)

(U) Ueli Maurer, who at a very tender age has established himself as a major contributor (he's one of Massey's students, and is still at ETH Zurich), spoke on noninteractive key-distribution systems. I couldn't see that he had must to say, but he said it very well. Nine minutes is not much time to present a talk, but his sentences contain much more than most.

(U) Another talk with an excellent speaker was "Implementation of an elliptic curve cryptosystem," presented by Canadian Gordon Agnew, representing joint work with Ron Mullin and Scott Vanstone, all of Waterloo. He described their implementation of discrete exponentiation in GF (2^{593}). Their most recent effort involved an optimal normal basis structure in GF (2^{155}). I don't have enough computer science knowledge to assess their progress, but I report to you that they utilized a limited instruction set and fewer than 11,000 gates. They attain a 40MHz clock speed and, using a Motorola 68030, they claim a throughput of 60 Kbps implemented on less than 1 square mil (less than 4% of the area of a smart card).

(U) Ivan Damgård and Li-dong Chen (she is a student of Landrock at Århus, where Damgård also works) presented "Security bounds for parallel versions of ID protocols." Fortunato Pesarin (of the statistics department at Palermo) laid the biggest egg with "On randomized cipher systems," but countryman Andrea Sgarro (an information theorist at Trieste) did better with "Information-theoretic bounds for authentication codes."

(U) Peter Mathys (he's either Swiss or Austrian, but he's been at Colorado for quite a while) presented "A fast serial encryption algorithm based on random transpositions," and Belgrade's Golic gave another reasonable performance with "A generalized correlation attack with a probabilistic constrained edit distance" (an improvement, he says, on the constrained Levenstein distance, if you know what that is).

DOCID: 4009689

(U) There was another talk, by Keiichi Iwamura, but it seemed to be a subset of the talk he was to give the following day, so we now turn to that program, devoted to public-key cryptosystems. Iwamura is at the Canon Research Center and is working with the very productive duo of Tsutomo Matusmoto and Hideki Imai of Yokohama University. He is interested in a speedy implementation of the RSA scheme, and has seized upon systolic arrays to implement modular multiplication. He says that for a 512-bit exponent e and a 512-bit modulus N they can achieve 50Kbps with about 25K gates.

(U) The other two talks in this session also dealt with efficiency. Yacov Yacobi of Bellcore (his coauthor is colleague Michael Beller) is interested in batch processing, and found that Batch-RSA cannot be employed effectively. He was happier with his efforts to apply batch processing in a Diffie-Hellman scenario, and the result was "Batch Diffie-Hellman key agreement systems and their application to portable communications," which uses composite moduli. Unfortunately one of the audience pointed out a flaw in one of his proofs; he made a hand-waving recovery, but the blunder had been clearly established.

(U) Kevin McCurley and his Sandia colleagues Ernie Brickell, Dan Gordon (now at the University of Georgia), and David Wilson (now at MIT) have been optimizing the exponentiation operation, both in conventional groups and in elliptic curve groups ("Fast exponentiation with precomputation"). Again, this subject is of undoubted importance (though it is perhaps not worth squeezing out the last epsilon, except to him who does it) and this is a powerful team which can be trusted to do the job well. I guess we as cryptologists should be happy to have such tasks carried out for us, freeing us to think of our own problems.

(U) The next four sessions were given over to philosophical matters. Complexity theorists are quite happy to define concepts and then to discuss them even though they have no examples of them. Jacques Patarin (Bull, France) wrestled with several of these at once in "How to construct pseudorandom and super-pseudorandom permutations from one single pseudorandom function," and, for those who needed another dose, one could listen to Babek Sadeghiyan (a student of Josef Pieprzyk at the University of New South Wales, Australia) discuss "Construction for super-pseudorandom permutations from a single pseudorandom function," but the next time I have the option, I will find something else to do.

(U) Ueli Maurer (ETH, Zurich), in "A simplified generalized treatment of Luby-Rackoff pseudorandom permutation generators," tried to persuade the philosophers that information theory may have something to say about their concerns. Maurer is remarkably versatile, and seems to be able to contribute substantially in several areas.

(U) Don Beaver (Penn State), in another era, would have been a spellbinding charismatic preacher; young, dashing (he still wears a pony-tail), self-confident and glib, he has captured from Silvio Micali the leadership of the philosophic wing of the U.S. East Coast cryptanalytic community. The subtitle tells it all in "how to break a 'secure' oblivious transfer protocol (or, good definitions mean everything)," in which he patched a tiny hole in a protocol of Bert den Boer which appeared at last year's Eurocrypt.

(U) Beaver collaborated with Stuart Haber (Bellcore) to produce "Cryptographic protocols probably secure against dynamic adversaries." Haber gave this talk, but it was not his finest hour. In past talks, he has injected some welcome humor, but this year he just preached the gospel, even though he conceded that what they were doing had also been done a few years ago by an MIT graduate student named Feldman, but that they "didn't like Feldman's definitions."

(U) The other talk in the first complexity-theory session was "Uniform results in polynomial-time security" given by the very young Paul Barbaroux (University of Paris). He found time to present only about one-third of his talk, which was probably just as well.

(U) Those of you who know my prejudice against the "zero-knowledge" wing of the philosophical camp will be surprised to hear that I enjoyed the three talks of the session better than any of that ilk that I had previously endured. The reason is simple: I took along some interesting reading material and ignored the speakers. That technique served to advantage again for three more snoozers, Thursday's "digital signature and electronic cash" session, but the final session, also on complexity theory, provided some sensible listening.

(U) The first talk, "Local randomness in candidate one-way functions," was by the amazing Austrian Harald Niederreiter (Austrian Academy of Science), representing work done jointly with Claus Schnorr (University of Frankfurt). Niederreiter writes beautifully and lectures beautifully too. I quote from their paper "A major open problem in cryptography is to establish one-way functions. While we cannot prove

one-wayness" [neither can anyone else—rek] "it makes sense to analyze candidate one-way functions and to prove properties of these functions that are useful in cryptographic applications." You might think this statement would be obvious to all, but in most cases, complexity theorists have never concerned themselves with actually finding a one-way function! Niederreiter also distanced himself from contemporary complexity theory by announcing that his results would depend on no unproved hypotheses.

(U) Now I cannot tell you that the veil has been lifted, and that one-way functions are finally fully (or even partially) understood. But it is refreshing to find a complexity theory talk which actually addresses an important problem! For this special occasion, I would really like to tell you what I think he said, but unfortunately it would require a string of definitions just to get to the statement of the two main results. Over Z_N he takes m linearly independent (modulo the linear polynomials) polynomials $f_1, f_2, \ldots, f_m$ and maps the integer x in Z_N to the m-tuple formed from the least significant bit from each of the functions. He proposes such a function as a candidate one-way function. And of course there is the prospect of taking more than one least significant bit from each of the functions. How easy are these functions to invert?

(U) The other two talks again avoided anything of substance. Tatsuaki Okamoto of NTT (joint authors, Koichi Sakurai of Mutsubishi and Hiroki Shizuya of Tohomu University), in "How intractable is the discrete logarithm for a general finite group?" thought it worthwhile, in dealing the general discrete logarithm problem, to prove that the problem is contained in the complexity classes NP and co-AM, but is unlikely to be in co-NP.

(U) And Ueli Maurer, again dazzling us with his brilliance, felt compelled, in "Factoring with an Oracle" to arm himself with an Oracle (essentially an Omniscient Being that complexity theorists like to turn to when they can't solve a problem) while factoring. He's calculating the time it would take him (and his Friend) to factor, and would like also to demonstrate his independence by consulting his Partner as seldom as possible. The next time you find yourself similarly equipped, you will perhaps want to refer to his paper.

(U) The conference again offered an interesting view into the thought processes of the world's leading "cryptologists." It is indeed remarkable how far the Agency has strayed from the True Path.

(U) Hungary is a beautiful country that has freed itself from an oppressive occupation which lasted almost 45 years. From a tourist brochure: "Hungarians are now diligently learning English and German and are even more diligently forgetting Russian." The people sport American T-shirts but speak little English; they expect tourists to converse in German. Balatonfured is in a resort area around the region's largest lake (Lake Balaton). Accommodations are generally better, and prices higher, than elsewhere in the country. My Hungarian-American wife Donna and I spent three weeks in the country and experienced really wonderful weather: sunshine every day, cool nights (no need for air conditioning!). Twenty per cent of the 10 million people live in Budapest, but the next largest city is only one-tenth as large. The economy is basically agrarian; we observed extensive cultivation in virtually all of the countryside outside of the capital.

An Agnostic Look at TQM

William M. Nolte, P054

Management techniques are like a tool box. The box does not contain a single magic tool for every job, but an assortment of tools that need to be selected according to the job at hand.

Total Quality Management can be an effective set of tools, offering impressive strengths: focus on the customer, empowerment of employees, action based on information, and continued improvement of processes. These strengths have led many organizations to adopt TQM techniques; some have gone even further and embraced the cult or religion of TQM. Despite my respect for the potential value of TQM—truth be told—I am a nonbeliever, a management school agnostic. NSA as an institution, however, has become a TQM believer, born again in the gospel of Deming. Actually, given the Agency's past enthusiasm for other management philosophies over the years, NSA can perhaps best be described as born again—and again—and again.

Is TQM a useful tool? Absolutely, but only if we recognize its weaknesses—even the risks—its incorporation entails for NSA. If we fail to do so, TQM not only will fail to improve the agency's operational performance, it will hamper a critical agency's ability to adapt to a difficult set of changed operating circumstances and encourage a the cynicism that will erode the morale of the agency's workforce.

The Private Sector-Public Sector Gap

First of all, we must recognize that TQM, like most management schemes, derives from a private-sector experience. Such schemes inevitably translate only roughly into the public sector. For example, TQM's focus on the customer is essential for an organization that sometimes judges its success by internal measurement: that is, we think we do a good job, so we must be doing a good job. But what is the external measure for a public-sector organization? Private-sector organizations ultimately cannot judge their own success or failure. The market performs this function, except of course where a business is a monopoly or near monopoly. Utilities and regulated industries can evade the market, but look out if they lose their monopolistic or regulated niche. We will suffer, as public-sector organizations always do, from the absence of analogous measures for judging success or failure.

Even in the private sector, market circumstances can cloud or at least delay a true measure of success or failure. The American automobile industry represented, before the Japanese onslaught, something of a collective monopoly, with a virtually closed market and start-up costs too enormous to invite new players into the game. GM, Ford, and Chrysler (all their advertising notwith-

standing) barely competed with each other, as historically stable market shares would demonstrate. In this environment, a true measure of performance (and quality) was difficult to maintain. With the introduction of enormous numbers of Japanese cars, cheap, reliable, and efficient, the true measure of Detroit's inefficiency was apparent. Chrysler almost died, while GM and Ford recorded truly impressive losses.

P.L. 86-36

As a virtual monopoly, NSA has been largely spared the cost of inadequate support to its customers or lapses in quality of service rendered. We have been permitted to measure success in internal terms:

Most perversely, NSA, like other public sector organizations, has measured its success not in profit or productivity but in expenditure. The bigger the budget, the more successful the agency.

The Factory

The second risk associated with TQM is that it adopts an industrial metaphor. This is especially unfortunate for NSA which has traditionally been burdened with such a metaphor. After all, we produce "product"—not information, not a service, but product. Or at least that's what we've always said.

Wrong. We're in the service business, the information service business, to be exact, and one of the first things we need to do to remind ourselves of this is to drop all references to "product."

What's wrong with the product metaphor? Mostly that it confuses the measure of success. For years, we have graded our performance, at least in part, on the basis of how much product we have produced. If the number of product sections rose, we must be doing well.

Now, production statistics are useful in the private sector because they have a strong, though not unerring, correlation with efficiency and market savvy. If you're producing more product, customers must be demanding and buying more product. But the connection between demand and production is hazy at best in the public sector. (And even in the socialized private sector. Admiral Arleigh Burke used to tell of visiting a UK subsidiary of an American auto firm. Outside each plant, Burke was horrified to see acres and acres of cars. "How are you going to sell those cars?" Burke would ask, only to be told that selling them was less important than making them. The government, anxious to maintain employment levels, would reimburse the company for unsellable cars. This attitude has been satirized in the British comedy "Yes, Minister;" a bureaucrat rebukes his minister for demanding results: "We do not measure success by *results*, but by *activity*.")

We need to concern ourselves with satisfying our customers' needs for information. In some cases, those needs may require more reports. In others, the volume of reports may overwhelm the customer; then, the proper service might entail fewer reports. The point is we need to disconnect quality of service from number of (ugh!) products. They are only roughly related, if at all.

While we're on the subject of jargon, we need to take a look at the tendency to speak of customers' "requirements" rather than "needs." We give the customer the product they (say they) require. We must work on developing mechanisms to give them with the information they need, even if that means anticipating the customer's sense of those needs.

"Getting it Right the First Time"

Another unfortunate industrial memory from TQM is this business about "getting it right the first time." True and appropriate for GM—once they've entered production. But what a lousy idea this is for an organization that needs to tailor its service to an amazing range of customers whose needs will change dramatically and unpredictably as the world changes.

TQM seems to be best employed as an explicit strategy by companies operating in a relatively static environment and confronting significant repetitive precision, i.e., industrial quality, problems. It seems less attractive to firms that have to adjust to developing realities or, even more, operating in environments so fluid it makes no sense to even think about getting it right the first time. They may not even know what "it" is. When was the last time you saw Bill Gates of Microsoft emoting about how he has caught the TQM spirit? More likely, one is likely to watch Robert Stempel, former head of GM, talking about his commitment to the concept. Bill Gates has made billions for himself, created thousands of jobs, and enriched his stockholders. Stempel made millions for himself while disemploying thousands of workers and costing his stockholders billions. Now there's quality!

An emphasis on getting it right the first time also appears to contradict the TQM premises of continuing process improvement and eliminating fear from the

DOCID: 4009689

workplace. In the first instance, the very idea of process seems to contradict the stasis implicit in getting it right every time. Secondly, getting it right every time seems to assume that one is dealing with variables that will react with uniform predictability to the imposition of a given procedure. Shaping body panels probably reduces itself to this; dealing with people does not.

At the Master's Feet

(or Other Obsequious Positions)

Much of the TQM mythology leans heavily on a gross misreading of the career of the late W. Edwards Deming. Deming: the man who rebuilt Japan while his own country shamefully ignored him!

First of all, Deming did not rebuild Japan, the Japanese did—aided by the generosity of the United States. In the intricate matrix of ethic, skill, and capital that together encourage industrialism, the easiest component to replace is capital. It is also the one that requires the most frequent replacement. A skilled people, a work ethic intensified by the hardship of war, defeat, and occupation, and a rebuilt physical plant after about 1960 virtually guaranteed Japan some measure of success. Did Deming play a role? Yes, but he largely reinforced existing ethical and cultural tendencies. He did not supply them, a fact made clear by comparing Japan's post-1945 economic success with that of West Germany.

West Germany confronted the same basic situation facing Japan, a skilled people with a strong achievement ethic, confronted by lack of capital and the destruction of much of the country's physical plant. Like Japan, and in very similar time, Germany overcame its difficulties to become a great economic power—despite, miracle of miracles, the absence of Edwards Deming. Without question, Deming was useful to the Japanese and his role cannot be ignored. But Japan's economic emergence (really a continuation of a process that had begun in the 19th Century, only to be interrupted by the blunders of Japan's military leadership in the 1930s and 1940s) would have taken place without him.

Most importantly, the great danger of the myth of Deming is that it contributes to the overselling of TQM, especially through the evangelical quality of the sales pitch sometimes employed. One of the films being shown to agency TQM classes is a classic of the genre. A breathless "journalist," so thrilled to merely be in the presence of Dr. Deming she can barely speak, recounts that thousands of executives "have taken Deming to heart," caught his spirit, or otherwise experienced some sort of conversion. Companies of course must be "totally committed" to TQM for it to work, explaining why, despite Mr. Stempel's best efforts, GM did not turn around faster: Mr. Goodwrench didn't feel the spirit.

Deming was a fascinating man, especially for his often subtle, often overt fascination with the spiritual aspects of work. He believed, for example, that the job of a manager is to see that employees take joy in their work. A challenging concept? Yes. An admirable one? Probably. But the concept of joy is so subjective and the sources of joy so diverse and ultimately individual, that one could argue that it is something management cannot ultimately provide. Maybe all a job can do is offer the rewards—psychic and material—that permit individuals to pursue joy in the rest of their lives.

The Fallacy of Total Commitment

One of the problems with TQM as faith is embodied in the repetition of the mantra "total commitment." Faith indeed demands a total commitment. One can't believe in just nine commandments; faith in two parts of the trinity won't cut it; and the idea that there is probably only one God and Mohammed is one of several, equally valid messengers is not going to light the fires. Faith is an all-or-nothing proposition. You believe or you don't believe. Or you remain agnostic.

If this is the case, what are the Deming disciples to make of his contention that good ideas virtually never come from within an organization? If it's part of the dogma, we are at great pains to accept it. But for an agency like NSA, rightly if sometimes obsessively closed to the outside, this particular doctrine means we are in big trouble. We get only one truly significant outsider into the place every three years or so, with a relatively small, vitally important, but still insufficient infusion of outsiders from the military services. Do we believe Deming? Or do we conclude, on this and other issue, that Deming is valuable but not infallible?

If we accept the latter, we need move away from preaching TQM to teaching TQM, and that means teaching it warts and all. Management is not a faith process. It is not ideology. It is a technique: eclectic, applied, and particular. It is eclectic in that many tools exist for many different tasks. It is applied in much the way the late Ronald Lewin said wartime intelligence needed to be judged by its application: "The battle is the payoff." In management, performance is the payoff and the choice of tools is often secondary and sometimes academic.

Management is particular in that management experiences transfer only imperfectly from one organization to another. What works for Marriott may fail miserably for General Dynamics.

By all means, let us use TQM. Let us put the customers first, where they should have been all along. Let us empower our employees. Let us develop (and use) measures for judging programs and supporting decisions. And finally, let us make continuous improvement of our processes an agency-wide commitment. ***But let's stop worshipping a screwdriver.*** That's not even good religion; it's idolatry. Rather than demanding total commitment, effective management requires a constant skepticism. Is the tool working? Is it the right tool?

Ultimately, managers must be prepared to admit they have been using the wrong tool and employ another—without fearing that they will be accused of heresy or infidelity. Here we cross from management to leadership, recalling what the late Grace Hopper said: "You don't manage people. You manage things. You lead people." And NSA, like other organizations is, in the words of another famous management authority, simply a collection of people—period!

Quality management is an effective interim goal for NSA; but our real objective must be **quality leadership**, consistent with our claim to be the world's leader in cryptology. TQM, of its own, will not produce this objective.

P.L. 86-36

Technical Literature Report

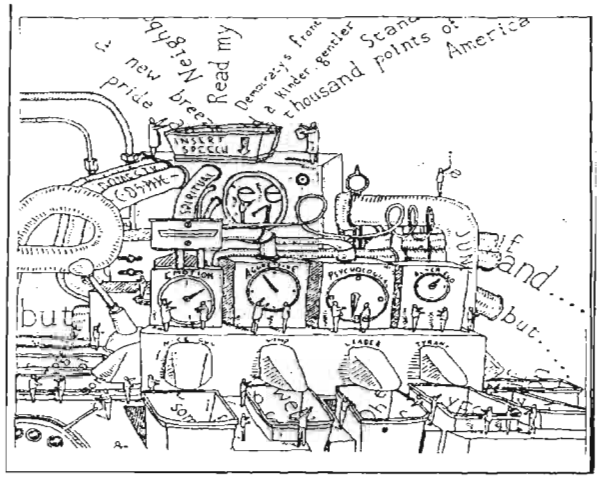
By [redacted] Z03

If you're looking for good articles on leadership, you can find one in (of all places!) the August 1992 issue of *Computer Language* magazine. The author, Larry Constantine, describes an interesting British study with some provocative results.

It seems that a British staff college was conducting a study of leadership in high achievers, so it assembled a large group of candidates and tested them for individual achievement. The candidates were sorted by achievement level, then regrouped. The new groups were tested again and regrouped a second time. The final groups ranged from "the best of the best" to "the worst of the worst." The groups were then assigned a collective task, with each one to be graded on its achievement as a group.

The results were not what the researchers expected. The group achievements bore little relationship to the individual achievements of the groups members. In fact, the "best of the best" group did much worse than "the worst of the worst." The immediate question was "What could possibly have happened?"

On reflection, the answer was simple. The initial tests had selected the "best" from the "worst" based on individual achievement; the "high achiever" selectees had focus, energy, drive, and the ability to get things done by themselves. But the final test was based on group achievement, and the groups of "high" achievers didn't show as much creativity, flexibility, and co-operation—as groups—as the groups of "low" achievers.



In fact, in one critical respect, the "lower" groups had a mix of leadership. Some of the members were *drivers* (although weaker ones than were found in the higher groups), but others were *innovators* (leaders in thinking of new ideas), *facilitators* (leaders in resolving conflicts between other members), and *implementers* (leaders in doing the dirty work), among others. While none of these "other leaders" was as effective—as individuals—as the members of the "higher" groups, the "lower" groups had people with leadership strengths in each of the specific problem areas they faced, so their group performance was better overall.

The lesson is clear. To build a high-achieving group, we need to look for—and appreciate—people who are different from ourselves. They may well not be classic individual "high achievers"—in fact, picking all uniformly "high achievers" may be the quickest way to disaster. Instead, we need to pick a mix of people, each of whom bring different strengths to complement each other's weaknesses and can work together to build the strongest team overall.

DOCID: 4009689

In commemoration of World War II, 1941-1945

Principles for Successful Guidance

The Congressional Joint Committee on the Investigation of the Pearl Harbor Attack, after its thorough investigation of the attack, reached the conclusion that certain supervisory, administrative, and organizational deficiencies existed in the armed forces of the United States and recommended that serious consideration be given by the Army and Navy to twenty-five principles which it enunciated in the hope that something constructive might be accomplished that would aid our national defense and preclude a repetition of the failure of 7 December 1941. The twenty-five principles presented by the congressional committee are set forth below.

I. Operational and intelligence work requires centralization of authority and clear-cut allocation of responsibility.

II. Supervisory official cannot safely take anything for granted in the alerting of subordinates.

III. Any doubt as to whether outposts should be given information should always be resoived in favor of supplying the information.

IV. The delegation of authority or issuance or orders entails the duty of inspection to determine that the official mandate is properly exercised.

V. The implementation of official orders must be followed with closest supervision.

VI. The maintenance of alertness to responsibility must be insured through repetition.

VII. Complacency and procrastination are out of place where sudden and decisive action is of the essence.

VIII. The coordination and proper evaluation of intelligence in time of stress must be insured by continuity of service and centralization of responsibility in competent officials.

IX. The unapproachable and superior attitude of officials is fatal: There should never be any hesitancy in asking for clarification of instructions or in seeking advice on matters that are in doubt.

X. There is no substitute for imagination and resourcefulness on the part of supervisory and intelligence officials.

XI. Communications must be characterized by clarity, forthrightness, and appropriateness.

XII. There is great danger in careless paraphrase of information received and every effort should be made to insure that the paraphrased material reflects the true meaning and significance of the original.

XIII. Procedures must be sufficiently flexible to meet the exigencies of unusual situations.

XIV. Restriction of highly confidential information to a minimum number of officials, while often necessary, should not be carried to the point of prejudicing the work of the organization.

XV. There is great danger of being blinded by the self-evident.

XVI. Officials should at all times give subordinates the benefit of significant information.

XVII. An official who neglects to familiarize himself in detail with his organization should forfeit his responsibility.

XVIII. Failure can be avoided in the long run only by preparation for any eventuality.

XVIX. Officials, on a personal basis, should never countermand an official instruction. Personal and official jealousy will wreck any organization.

XXI. Personal friendship, without more, should never be accepted in lieu of liaison or confused therewith where the latter is necessary to the proper functioning of two or more agencies.

XXII. No consideration should be permitted as excuse for failure to perform a fundamental task.

XXIII. Superiors must at all times keep their subordinates adequately informed, and conversely, subordinates should keep their superiors informed.

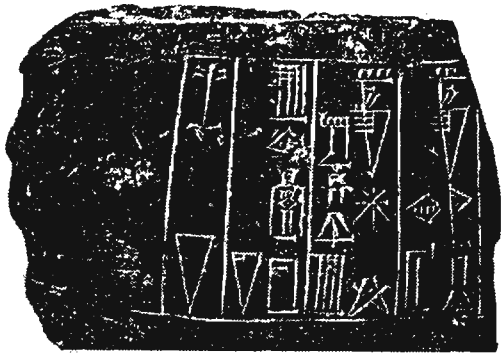
XXIV. The administrative organization of any establishment must be designed to locate failures and to assess responsibility.

XXV. In a well-balanced organization there is close correlation of responsibility and authority.

Lexicography at Second Hand:

Thoughts on Producing an "Exotic Language" Glossary

A631



~~(S-CCO) The~~ former Division of Languages and Linguistics (P16) was sometimes charged with creating an "exotic language"-English glossary, by translating the common side of an "exotic language"-common language glossary. An example is translating the Chinese side (the common side) of a Wa-Chinese glossary to produce a Wa-English glossary. Wa is of interest because it is spoken by a small group of people active in the drug trade who live in Southeast China and the adjacent area of Burma.

(U) This method of producing a glossary requires much less time and fewer resources than does the production of such a glossary from scratch—but it does have some pitfalls. In this case, for instance, the Chinese team that gathered the Wa vocabulary and wrote the glosses and explanations was based in Yunnan province. The local Yunnanese names for many of the common plants and wild animals do not exist in any published Standard Chinese dictionary. Sometimes, the Standard Chinese and Yunnanese gloss for the same character had different meanings—leaving me, the translator of the Chinese, groping for a proper gloss. The Chinese editor must have been a little near-sighted also, as some of the characters had elements that didn't fit the context, which gave me fits, unfamiliar as I was with the new orthography anyway.

(U) To make up for the difficulties encountered, I amused myself by reflecting on the life-style observed in explanations of some entries, and on things learned through them. In the Wa language, I ran across ideas that were expressed in unusual ways, that is, concepts that are foreign to someone whose first language is American English. For instance, the phrase accompanying the gloss for "hiccup" was, "Don't hiccup while eating; it will upset people." How does one hiccup? Thinking about the possibility of upsetting others by hiccuping while eating just might make one hiccup. And the phrase illustrating "going to bed" contains the passage, "lie nice and straight, don't curl up." What would prompt a parent to admonish a child with such a phrase? Is space so restricted in a Wa bed that curling up is a no-no?

(U) Going further afield one comes across the Wa words meaning "false leopard" which require the explanation that "false leopard" is a structure of bamboo over which the skin of the slain leopard is placed and used by the Wa to represent a leopard in a dance with religious significance performed after the hunt. A "blood mark" is made by a Wa hunter on the stock of his crossbow in the blood of the beast recently slain, to boast of the hunter's prowess with that weapon. An *ndo* is a "head pole"—a pole on which the severed head of an enemy is placed, while *nbing gaing* is the spot in a field where the pole is placed. (The Wa are said to have believed that placing a Han Chinese head at each of the four corners of a field would guarantee a good harvest.)

(U) At another level, the abundance of words relating to one area of life contrasted to the paucity of those relating to others can give an insight into the culture of a people. The Wa have common names for many things that they consider edible that the Western does not—many plants whose tender young leaves are edible—plants which we think of as only ornamental or regard as weeds. The glossary even lists an edible toad, unless the Chinese have mistakenly used the toad character to mean frog, which is highly unlikely. And what do we call the lump of flesh on the tail of a chicken? The Wa call it *beed*; it seems to be a logical thing to have named, since every chicken has one.

(U) The many grasses that are described as thatching material, and the descriptions of thatching methods and patterns, give an insight into what the typical Wa house might look like. One interesting pattern is said to look like sawteeth when seen from the inside of the structure.

(U) The consequences of careless behavior around a lac tree (a tree related to poison ivy on which the lac scale is parasitic) are brought out in the explanation that a child's hands are red and swollen because he was climbing and playing in a lac tree. The Wa word for "to carry in the mouth" is illustrated by the phrase, "the panther is carrying a piglet in its mouth." That, along with several other references to large carnivores, gives a little of the flavor of the Wa environment.

(U) Taken all together, I believe that the gains from a glance into another world more than make up for the difficulties met along the way.

DOCID: 4009689

CRYPTOLOG
March 1994

Book Review

New Dictionary of English/Arabic Scientific and Technical Terms
by Ahmad Sh. Al-Khatib, 6th ed. 1991

Reviewed by [redacted] P.L. 86-36

(U) The New Dictionary Of Scientific and Technical Terms by Ahmad Sh. Al-Khatib is, in my opinion, one of the best technical reference aids that no Arabic linguist who must function in the scientific and technical Arabic language arena should be without. It is unmatched in breadth of technical terms as well as depth of any given term. The composition of the dictionary as well as the definitions and illustrations are based on western science and engineering concepts, which should prove the most beneficial to the educated Western reader/researcher. By and large, this dictionary provides definitions, but not encyclopedic descriptions of many of its terms. In some cases, the reader may have to use a more complete general Arabic/English Dictionary, such as the Hans Wehr, 4th ed., or the Al-Mawrid, to get the best meaning of a researched word.

(U) I've found that the definitions are mostly given in adherence to the true Arabic root, versus an English-sounding cognate, and the author as been as faithful as possible, when possible, to link newer concepts of science and engineering to traditional Arabic roots.

(U) The English used in this dictionary is more British English than American, but again, where possible, the author has taken care to give both the American and British term for the same Arabic word. For example, the Arabic word "miftah" can be found as the British term "spanner" and the American term "wrench"—under "S" and "W" respectively. Both of these definitions come with illustrations so the reader isn't necessarily thrown off by unfamiliar terms.

(U) In fact, there are illustrations (photos and drawings in both black-and-white and color) on almost every page. Some aren't as detailed when compared to the "Al-Mughni Al-Kabir" English/Arabic dictionary, but the collection in the "Sci/Tech Terms" is broader and quite satisfactory. Within the diagrammed illustration of an automobile, for instance, the reader will not see a steering wheel highlighted with both the English and Arabic word for it side by side, but will see the illustration with a brief description of what's being pictured on the margin in both English and Arabic.

(U) There are comprehensive tables in the back of the book which cover such items as the Geological Time Scale, equivalent Centigrade and Fahrenheit temperatures, the elements and their physical properties, and 4-place common logarithms, to name a few.

(U) There is one rather irritating problem that I discovered while searching for nuclear-related terms: pages 401-416 are missing. Page 400 ends with "Nitrogen Fixation" and page 417 begins with a chart on "Optics." I hope the problem is just with my copy and not with the entire pressing.

~~(FOUO)~~ In closing, let me say again that this dictionary, because of its depth and breadth of scientific and technical terminology and its adherence to traditional Arabic roots where possible, is a valuable linguistic asset to either the educated non-native English speaker, or the educated non-native Arabic speaker. We would do well to buy it.

To the Editor:

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

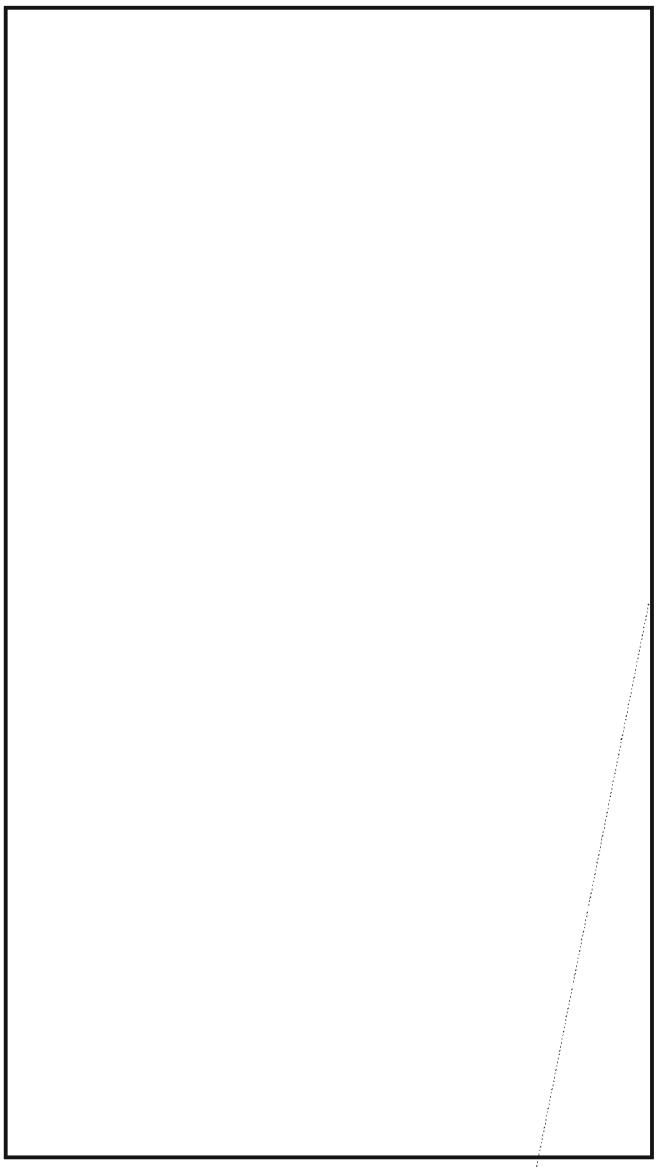
~~(C)~~ There was an interesting juxtaposition of articles in CRYPTOLOG's second issue of 1992, specifically [redacted] "Who Am I and What Am I Doing Here?" and [redacted] "On the Taxonomy of the Oyster." [redacted] discussed the definitions of bookbreaking and cryptolinguistics and the question of how to ensure fair recognition of those who are firmly planted in a hybrid of two demanding disciplines, while [redacted] differentiated between conventional substitution cryptosystems and codes.

~~(C)~~ In drawing the distinction between substitution and code systems, [redacted] touched upon a significant aspect of [redacted] question. Codes have traditionally been lumped among substitution systems by process of elimination, since they clearly do not fall into the transposition family. The shortcoming in this, however, is that it ignores a fundamental difference in the purposes of codes and substitution schemes. A code is used to alter the appearance of a language, while the more conventional substitution systems are used to alter the appearance of words. While this may seem subtle, to a bookbreaker it is crucial.

[redacted]

[redacted]

~~SECRET SPOKE~~



~~(C)~~ There are thorny questions aplenty to address, among them being: What is to be the official definition of a cryptolinguist? What are the essential skills? How do we develop those skills? How do we measure them? How do we determining what constitutes "professional" competence? How do we encourage diversity? For that matter, do we encourage diversity? How can we identify tours that will enhance a cryptolinguist's career? How do we identify and recruit potential cryptolinguists? How do we keep them?

~~(C)~~ We need to recognize bookbreaking/cryptolinguistics as a discipline in its own right. Ms. Goodlin touched on an obstacle to this recognition when she referred to her linguist friends and colleagues considering her to be a cryppie while her cryptanalyst friends and colleagues considered her to be a linguist. This attitude is harmless enough in your immediate peers. I think it important, though, that we be aware of and respect the unique talents required, and appreciate that neither a strictly language board not a strictly cryptanalytic board is the appropriate vehicle to adequately address the development of this particular set of cross-disciplinarians.

[redacted] Z422 P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~

Government Communications Headquarters
Room No E.0603
Priors Road Cheltenham GL52 5AJ
Telephone Cheltenham (0242) 221491 ext 2512
GTN Number 1366 ext 2512

P.L. 86-36

[redacted]
Editrix
CRYPTOLOG
c/o PO541,
NSA
[redacted]

Your reference
[redacted]
Date
2 July 1993

EO 1.4.(d)
P.L. 86-36

Dear Virginia,

CRYPTOLOG 3RD ISSUE 1992

May I please make two points about the article by Lambros Callimahos "A History of cryptology"; as it happens both refer to page 28.

First, he states that "In 1525, The British lion begins four centuries of successful cryptanalysis". This gives the impression that the British effort may have stopped around 1925. Nothing could be further form the truth! As just about anyone in Z Group will surely testify, the fifth century of British cryptanalysis is in full swing and continues to be as effective as ever...

Second, nobody seems to know when or where this lecture was delivered: but Lambros says that Brigadier Tiltman was then in the middle of his fifth decade as a cryptanalyst. I can confirm that the Brig joined GC&CS (the precursor of GCHQ) on 1 August 1920, so this would date the lecture as mid-1960s.

I was privileged to hear Lambros lecture when I was an integree in A5 in the late 1960s, and on another day he gave a flute recital in the Friedman Auditorium. A remarkable man, indeed.

Sincerely,

[redacted]

EO 1.4.(d)
P.L. 86-36

CRYPTOLOG

Editorial Policy:

CRYPTOLOG is a forum for the informal exchange of information by the analytic workforce. Criteria for publication are: that in the opinion of the reviewers, readers will find the article useful or interesting; that it is accurate; that the terminology is correct and appropriate to the discipline. Articles may be classified up to and including TSC.

Technical articles are preferred over non-technical; classified over unclassified; shorter articles over longer. Comments and letters are solicited. We invite readers to contribute conference reports and reviews of books, articles, software, and hardware that pertain to our mission or to any of our disciplines. Humor is welcome, too.

Please note that while submissions may be published anonymously, the identity of the author must be made known to the Editor. Unsigned letters and articles are discarded.

How to submit an article:

N.B. If the following instructions are a mystery to you and your local ADP support is no help, please feel free to call the CRYPTOLOG editor on 963-3123s.

Send a hard copy accompanied by a diskette (either 3.5" or 5.25") to the editor at P0541 in 2E062, Ops. 1, or send via e-mail to mebutle@p.nsa. For maximum efficiency (as far as possible within the limits of your word processor):

- do not type your article in capital letters
- do not double-space between lines
- but do double-space between paragraphs
- do not indent for a new paragraph
- classify all paragraphs
- do not format an HD diskette as DD or vice-versa
- label your diskette: identify hardware (operating system: DOS or UNIX), density of medium, and word processor
- put your name, organization, building and phone number on the diskette

CRYPTOLOG is published in FrameMaker on a Sun HPW. If you do not have access to FrameMaker, ASCII format is preferred.

DOCID: 4036135

I9, [redacted] (82)

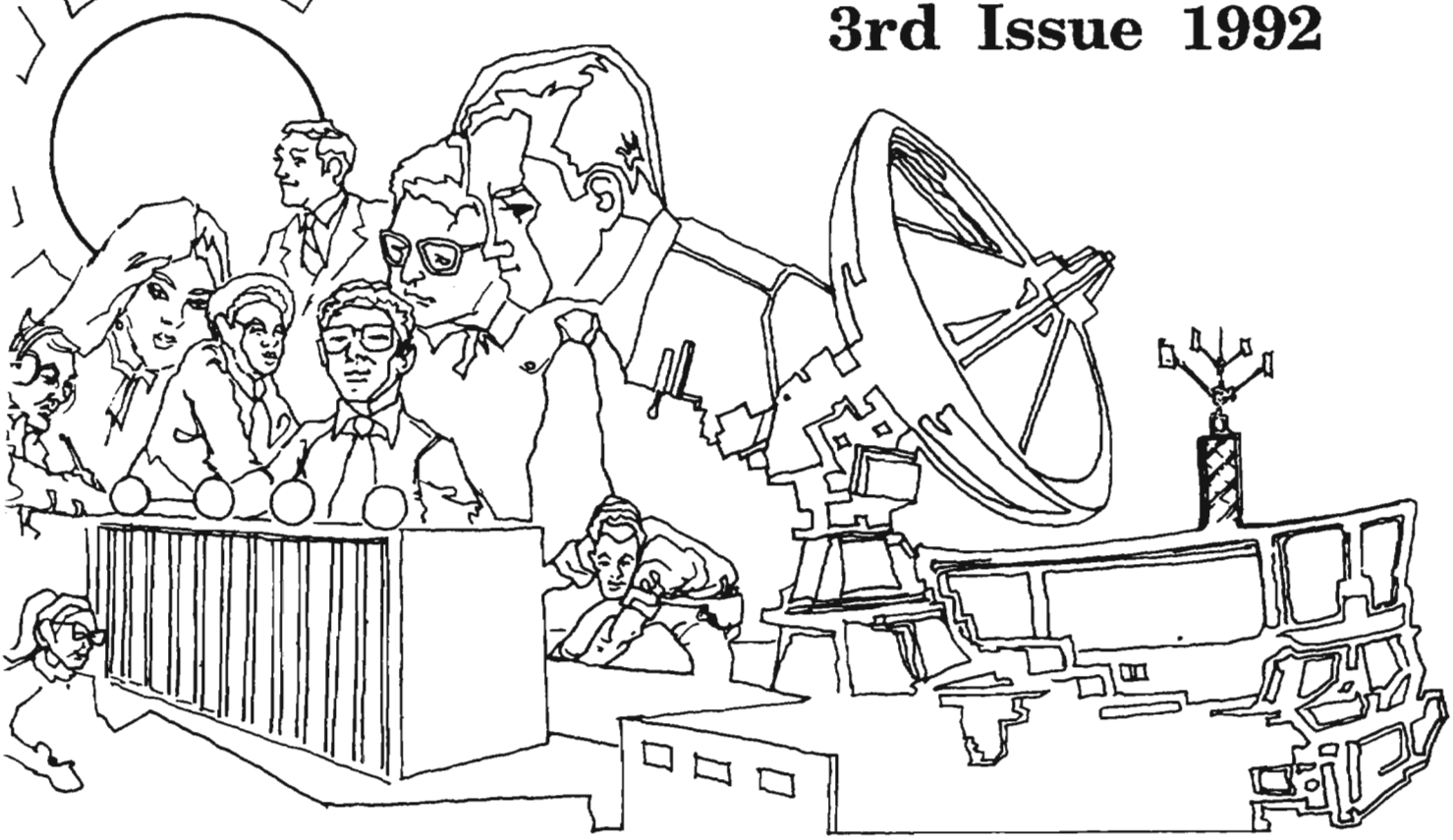
~~TOP SECRET~~

P.L. 86-36

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

3rd Issue 1992



THE THIRD OPSEC CONFERENCE	George Jelen	1
A QUANTITATIVE APPROACH FOR EVALUATING . . . .A FACILITY'S TECHNICAL SECURITY.	[redacted]	3
GOLDEN OLDIE.		9
[redacted]	[redacted]	10
WRITING IN A JOURNALISTIC STYLE	[redacted]	16
MINIMIZING THE BURDEN OF MAINTAINING SOFTWARE	Christine McCormick.	17
CETA	[redacted]	21
A HISTORY OF CRYPTOLOGY	L. D. Callimahos	23
HARDWARE-SOFTWARE REVIEW: MAT	[redacted]	36
NSA AND COMPUTER VIRUSES.	Richard Sylvester.	44
FROM THE PAST		45
LETTER.		46
BULLETIN BOARD.		47
EDITORIAL		48
TO CONTRIBUTE.		49

P.L. 86-36

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

P.L. 86-36

Declassified and Approved for Release by NSA on 10-10-2012 pursuant to E.O. 13526, MDR Case # 54778

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

DOCID: 4036135

CRYPTOLOG

Published by P05, Operations Directorate Intelligence Staff

VOL. XIX, No. 3 . . . . . 3rd Issue 1992

PUBLISHER. . . . . [redacted]

BOARD OF EDITORS

EDITOR . . . . . [redacted] (963-7595)

Collection . . . . . Marian Brown (963-1197)
Computer Systems . . . . . [redacted] (963-5877)
Cryptanalysis. . . . . [redacted] (963-1461)
Cryptolinguistics. . . . . [redacted] (963-4382)
Information Resources. . . . . [redacted] (963-3258)
Information Science. . . . . [redacted] (963-3456)
Information Security . . . . . [redacted] (968-8013)
Intelligence Community . . . . . [redacted] (963-5800)
Language. . . . . [redacted] (963-3057)
Linguistics . . . . . [redacted] (963-4814)
Mathematics. . . . . [redacted] (963-3709)
Puzzles . . . . . [redacted] (963-1461)
Research and Engineering. . . . . [redacted] (961-8362)
Science and Technology. . . . . [redacted] (963-3544)
Special Research. . . . . Vera R. Filby (968-6558)
Traffic Analysis. . . . . [redacted] (963-3369)

Classification Officer. . . . . [redacted] (963-5463)
Unix Support. . . . . [redacted] (963-3369)
Macintosh Support. . . . . [redacted] (961-8362)
Xerox Support . . . . . [redacted] (963-6867)
Illustrators. . . . . [redacted] (963-3360)
. . . . . [redacted] (963-4382)

P.L. 86-36

To submit articles and letters, please see last page

For New Subscription or Change of Address or Name

MAIL name and old and new organizations and building to:

Distribution, CRYPTOLOG, P0541, OPS-1

[redacted]

P.L. 86-36

Please DO NOT PHONE about your subscription or matters pertaining to distribution

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

DOCID: 4036135

The Third OPSEC Conference

George Jelen, D2

Good morning. It is my pleasure to welcome all of you to the third annual NSA/CSS OPSEC day.

We have all heard of the "Age of Enlightenment" and many of us have lived through the "Age of Aquarius." Well, I'm here to proclaim this as the "Age of Operations Security." After being around since the days of the Vietnam War, Operations Security, or OPSEC, has finally come of age. I attribute this to two causes: first, partly as a result of the 1988 presidential directive, more and more people have become exposed to OPSEC and have learned of its potential. This has led to the application of OPSEC to many different kinds of operations and activities. And second, people are beginning to discover that as they are forced to shrink their budgets for security, OPSEC and its methodology can be very useful in choosing where to focus their security protection and in applying that protection uniformly and consistently.

There are many indications that the interest in operations security is picking up. OPSEC tracks are now being offered as part of several major security conferences, including the International Security Systems Symposium and the conference of the American Society for Industrial Security. The National OPSEC Conference itself has been growing in attendance, and the membership in the OPSEC Professionals Society is continuing to expand steadily. The last couple of years have also seen a developing body of OPSEC literature. Here at NSA, a COSC has been established for the OPSEC field; and NSA/CSS OPSEC Association has been instituted and is aggressively planning activities; and there is a panel actively working to create criteria for professionalization.

Initially applied to military operations during the Vietnam War, OPSEC is now seeing application in a rapidly widening set of circumstances and activities. The Secret Service is applying it to personnel protection, the FBI to law enforcement, the defense community to weapon system acquisition, the Coast Guard and the Customs Service to drug interdiction, and the Intelligence Community to clandestine and covert operations. At a national level, we are now examining how we might employ OPSEC to help protect critical economic information as well. This latter application is clearly the growth area of the future.

OPSEC has also found varied application here at NSA. We have applied it to site closure plans, to SIGINT support to military operations, to sensitive acquisitions and procurements, to personnel movements, to financial transactions, to logistics shipments, and to counternarcotics support. The purpose, in every case has been to improve the effectiveness of our operations. We have come to understand that whenever there is some advantage in concealing our intentions, OPSEC proves quite useful.

There is a second reason why operations security has been receiving more attention of late, and why this is likely to continue. With the collapse of the former Soviet Union, the U.S. has entered a period during which our expenditures for security are being challenged. The changed world situation, and the altered security threat that it has brought with it, have caused many to question the continued need for security protection. The question I hear all the time is, "Where's the threat?" It's a

~~FOR OFFICIAL USE ONLY~~

reasonable question. Most would answer that there is still a threat, but that it is reduced and it is directed differently — focused more on economic and technology secrets than on military secrets. Motivated by a need to reduce our expenditures and encouraged by this generally-accepted reduction in threat, resources for security are being cut. As this happens, OPSEC and its methodology become ever more useful.

As resources applied to protection are reduced, if we are not to sacrifice too mush security in the process, this reduction needs to be done sensibly. Two basic premises of the OPSEC discipline are that not all information justifies protection and that not all vulnerabilities are worth correcting. We need to have some way to distinguish between what really needs protecting and what does not. Presently, we are spending far too much money trying to protect information that is either not worth protecting, is already known, or is fundamentally unprotectable. This makes no sense and we can not afford to continue to do it. This is where operations security can help. The more important it is to be selective in the application of our security resources, the more relevant the OPSEC methodology becomes. As resources for security grow more scarce, it becomes that much more important to apply them where they are most needed and where they can do the most good. The proper application of the operations security discipline and its methodology can be extremely useful in sorting out what most needs protection and in making sensible decisions about where and where not we can best afford to cut resources.

Our decision process needs to weigh the importance of the information, the motivation and the capability of our adversary, the ease with which that adversary could obtain that information, and the risk of leaving the secret unprotected versus the cost of protecting it. All of this is precisely what the familiar five-step OPSEC process does, and all OPSEC professionals know how to do it.

The OPSEC process imposes a rigor that can be profitably employed in many security resource decisions, sometimes with dramatic results. For example, when the U.S. was preparing for the arrival of Soviet inspectors as a result of the Strategic Arms Treaty, teams went around to a number of contractor facilities and Air Force bases looking at what special security arrangements would be required. Applying the OPSEC methodology, the teams were able to reduce the projected expenditures for security by more than seventy million dollars.

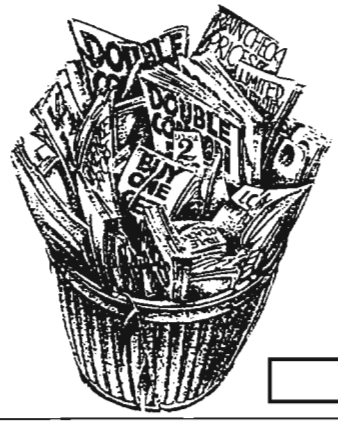
Once we have identified the information that is in most need of protection, it is equally important that we apply security resources consistently and completely — that we do not spend money on a robust lock for the front door and leave the back door unbolted. Here again, OPSEC can be helpful.

The various traditional security disciplines do a pretty good job of protecting against direct disclosure. But our secrets can be revealed indirectly as well as directly, and OPSEC complements these other disciplines by seeking also to protect those same secrets against indirect disclosure as well. Failure to consider ways in which an adversary might piece together the same secret from bits and pieces of information could mean that we spend a considerable amount of money in security protection and give away the secret anyway. Without operations security, the envelope of protection is incomplete.

We in D2 understand that our organization can not perform OPSEC for NSA or the CSS. OPSEC, by its nature, cannot be centralized. To implement OPSEC effectively, it has to become part of the normal way everyone of us conducts our daily business. In other words, the NSA and the CSS will only have effective operations security when every single person understands it and practices it within his or her organization. Everyone has to know what it is, how it works, what are its goals, methods and mechanisms. That is what this day is all about. It is aimed at deepening your understanding of OPSEC so that you might be more able to apply it to your own activities. Or employing the words of this year's theme, the day is intended to help you keep your mission on target through the sound application of OPSEC principles.

I am pleased to see you all here and I hope that many of you can remain for the rest of the day.

A QUANTITATIVE APPROACH FOR EVALUATING A FACILITY'S TECHNICAL SECURITY



R551

This Article is classified ~~SECRET~~ in its entirety. P.L. 86-36

Center for Security Evaluation (CSE) has been working on various initiatives to support the decision process in evaluating technical security at facilities. One recent effort, referred to as the Aggregate Countermeasure Effectiveness (ACE) model, helps to provide a quantitative measurement that integrates the multitude of factors that impact technical security. The model takes into account the value of the targets in the facility, the capability of the threat, and the overall effectiveness of the associated countermeasures. A prototype of the model has been developed and is currently being evaluated by CSE, with promising preliminary results.

HISTORY

In early 1991, the Standard Division of CSE decided that a new method was needed for evaluating the technical threat to a facility. At that time, a means was needed to help decide on the best combination of Technical Surveillance Countermeasures (TSCM) for the conditions particular to each facility. To this end, CSE set the wheels in motion to develop an analytical methodology that could be used to help make more informed decisions in two specific areas, namely:

- in establishing TSCM standards and policies, and
- in evaluating overall TSCM investment strategies.

THE INTENT OF THE EFFORT

Simply stated, the goal was to create a mathematical model that would tie together all of the factors that impact technical security at a facility. Results from the model would provide a quantitative "barometer" that could be used to compare the degree of technical threat at one facility with that of another. The model had to be understandable, represent the overall state of technical security,

EO 1.4.(c)
P.L. 86-36

The intent was to support decisions in three general areas. First, to help evaluate alternative sets of TSCM, either by looking at strategies specific to one facility or policies applicable to U.S. facilities in general.

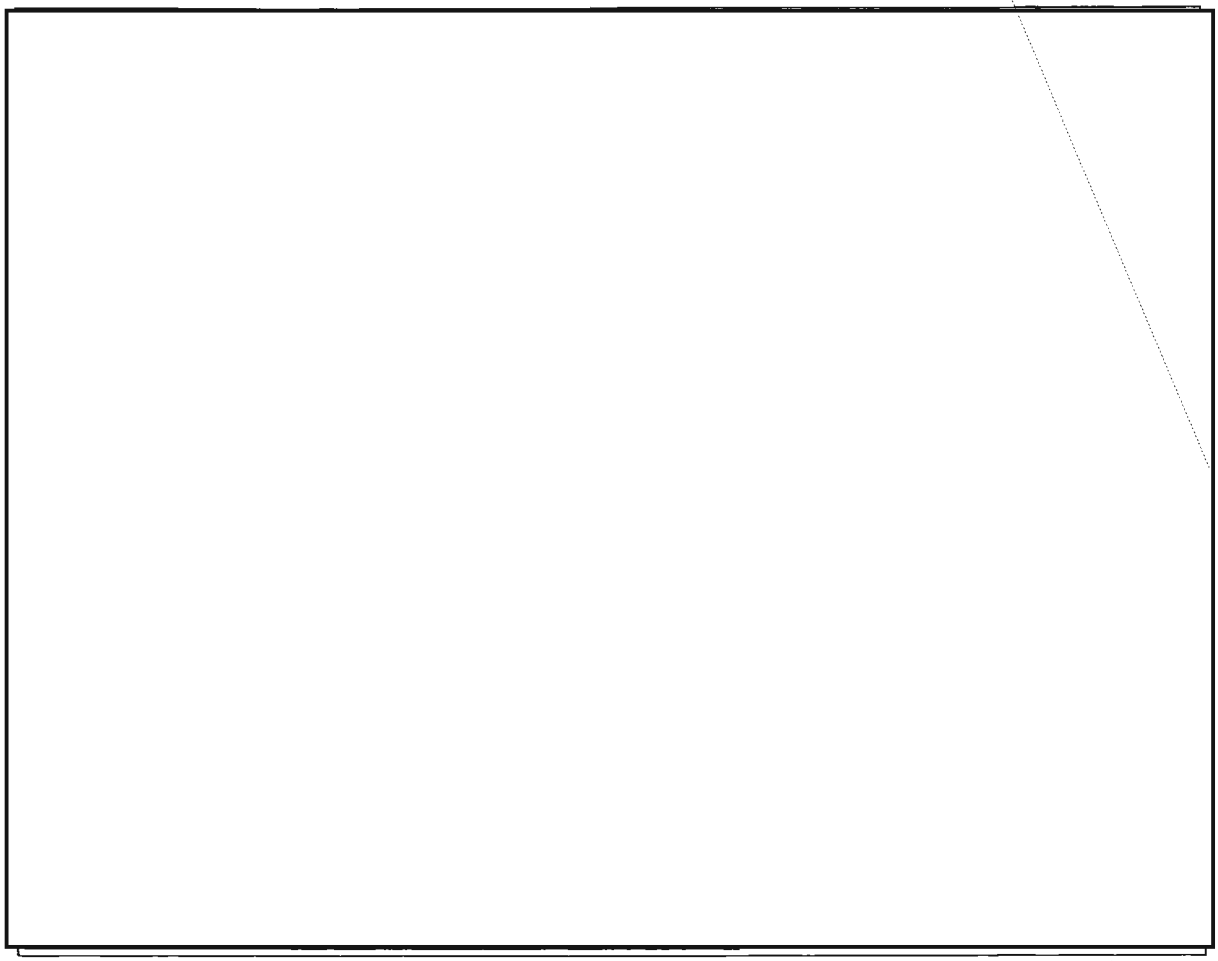
EO 1.4.(c)
P.L. 86-36

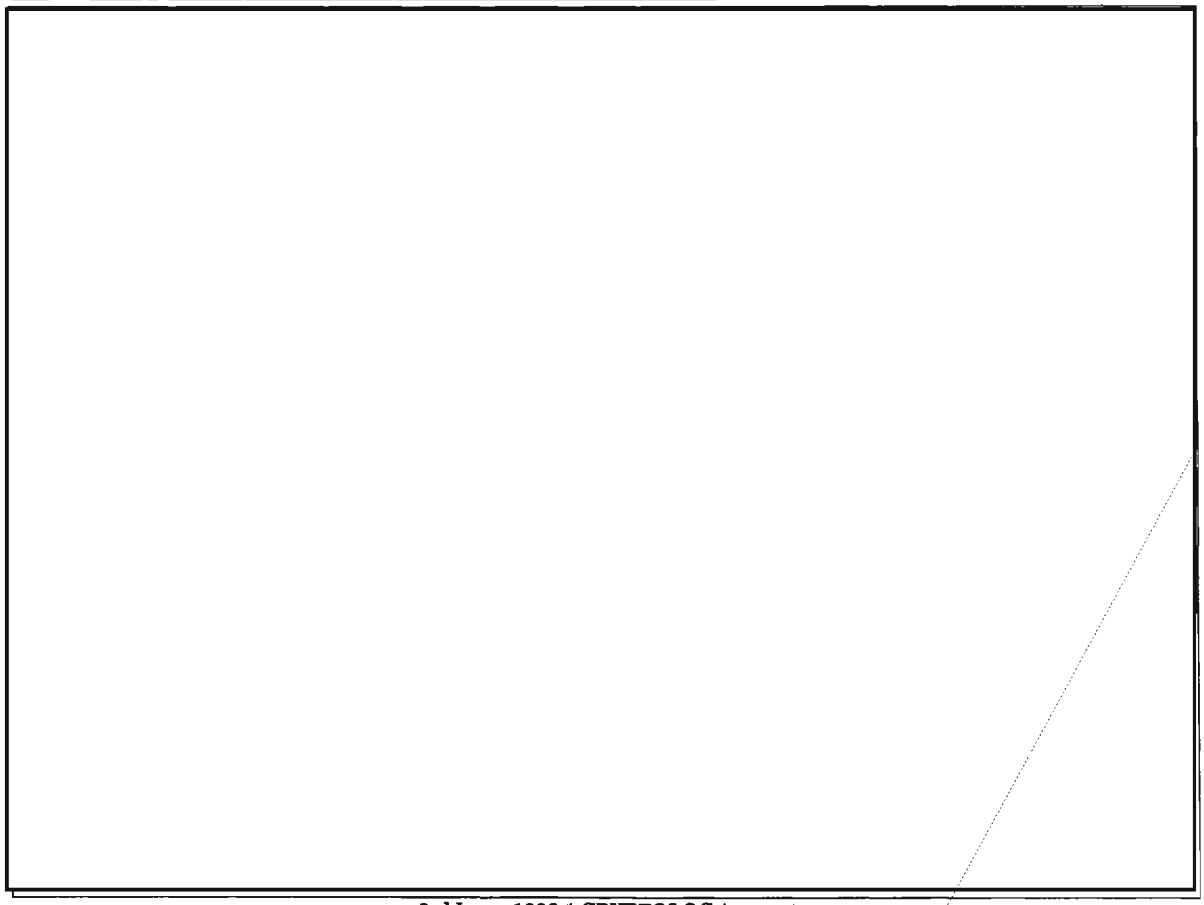
Finally, the model would be used to examine proposed resourcing concepts either at a particular facility or across a selected set of factilities. The model was to address such

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

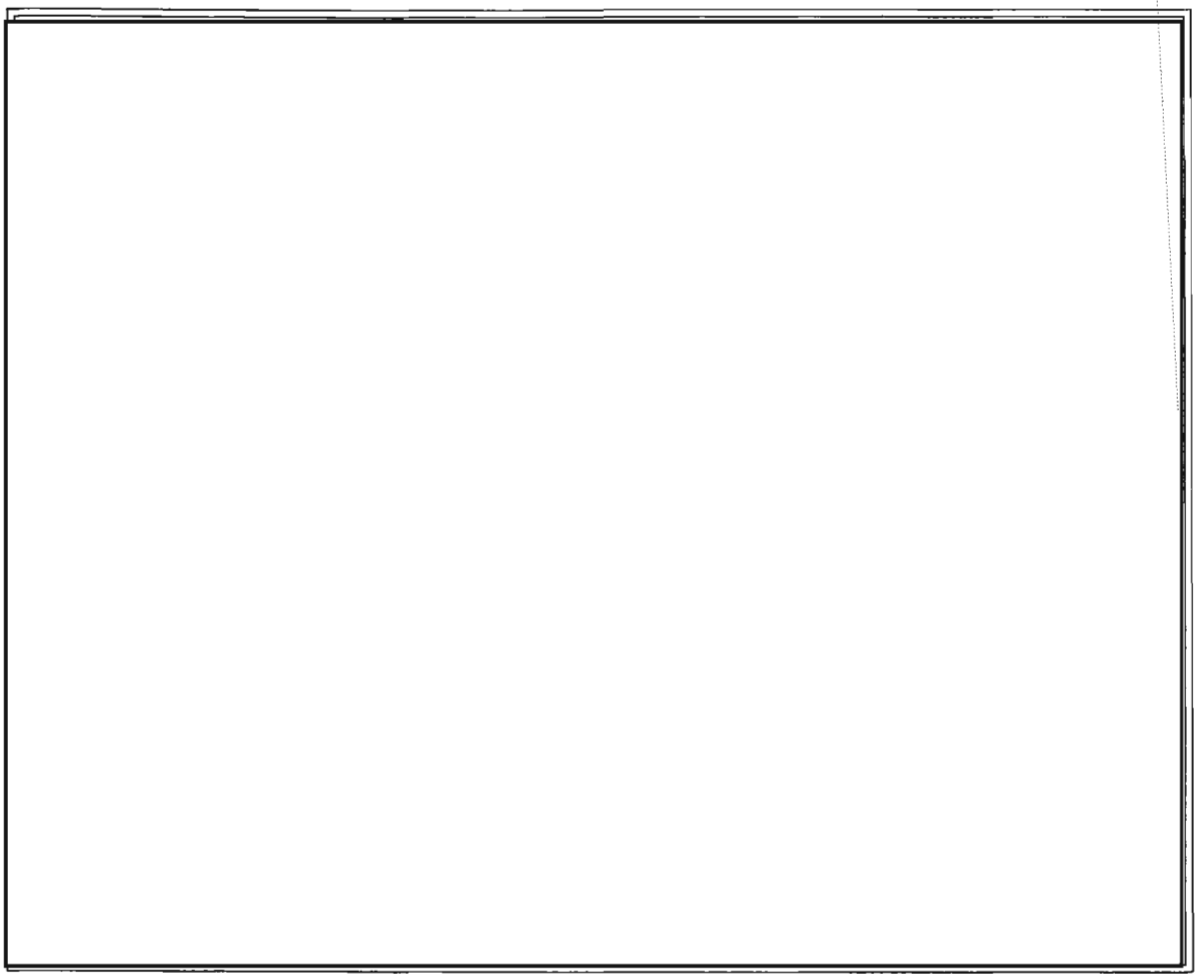




~~SECRET~~

EO 1.4.(c)

EO 1.4.(c)
P.L. 86-36



using basic engineering principles.

THE SOLUTION: WHAT THE MODEL DOES

It was decided that this new methodology (referred to as the Aggregate Countermeasure Effectiveness model, or just ACE), would be created in two stages to expedite the development process, and to provide a quick turnaround product that could be readily evaluated for its usefulness. In the first stage, a prototype microcomputer-based software package would be built for a reduced portion of the problem. If the prototype is determined to be of value, then a production version (with full capability and user-friendly features) would be created.

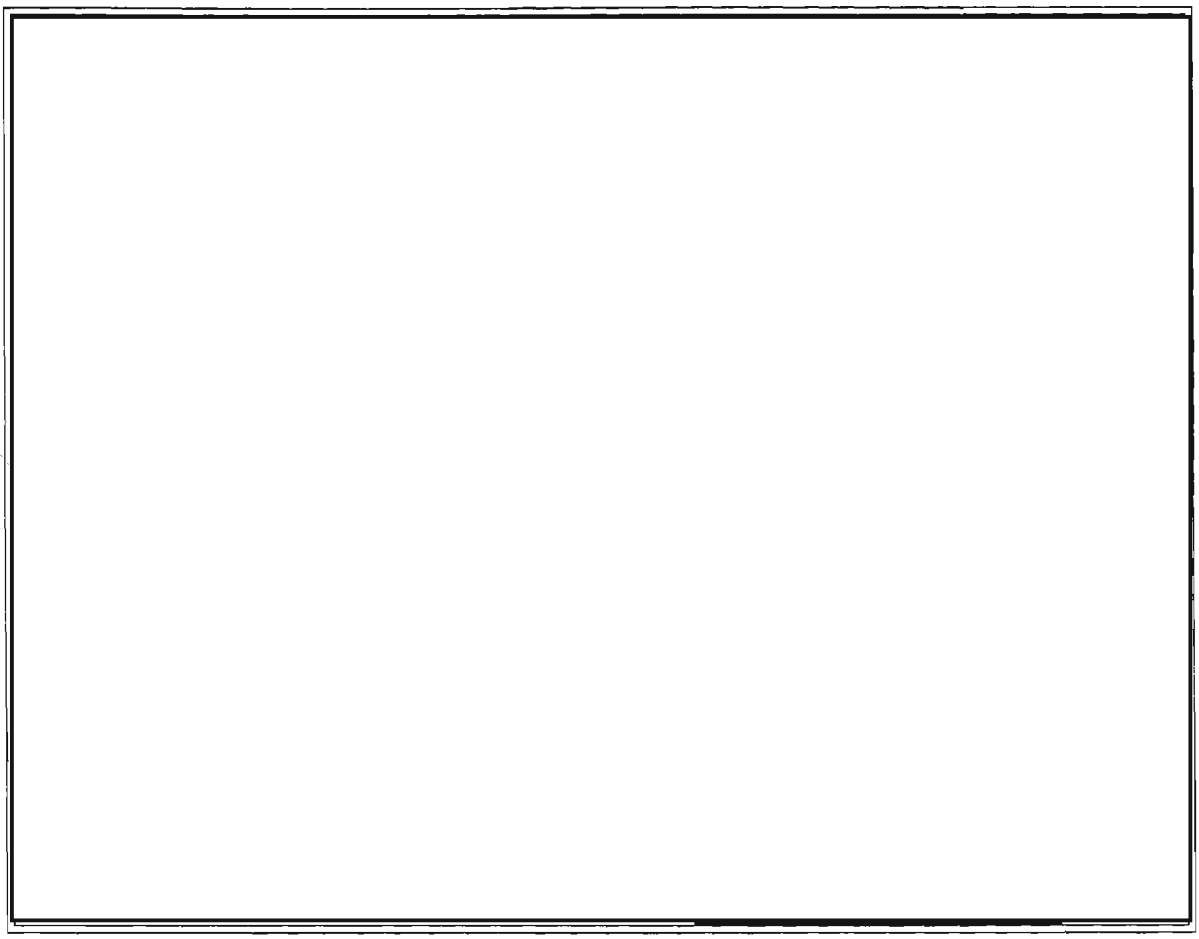
To develop the model, technical security at a facility was analyzed as a general flow problem

DESCRIBING THE PHYSICAL PROBLEM

For this "flow model" concept to work, a series of mathematical expressions were developed that

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



represented the relationships between the amount of sensitive material potentially compromised at a facility and the multitude of factors that determine its state of technical security (the expression at the bottom of exhibit 1 illustrates a few of the factors). The first step in translating the real world problem (exhibit 2) to a "mathematically oriented model" was to define the physical relationship between the targets at the facility (conversations between people, workstations, copiers, computers, etc.), the TSCM intended to protect the sensitive material processed by these targets

, and the various techniques used by the threat

HOW ACE WORKS

There are three basic parts to ACE (exhibit 4). First, the value of the sensitive material processed at the facility is estimated for each target based on the volume of activity and the worth of the material. Second, the effectiveness of the TSCM is computed for each path by summing the attenua-

EO 1.4.(c)
P.L. 86-36

DOCID: 4036135

EO 1.4.(c)
P.L. 86-36

tion provided by each individual countermeasure. This, in turn, is degraded by the state of operational security at the facility, both in terms of the adequacy of the preventive maintenance program and the level of P^3 (personnel, procedural, and physical) security. The natural attenuation provided by the controlled access distance is then added, resulting in an estimate of the combined effectiveness of the TSCM for each path. Finally, the capability and intent of the threat is brought into play.

[redacted]

HOW THE RESULTS ARE USED

[redacted]

[redacted]

WHERE ARE WE NOW

EO 1.4.(c)
P.L. 86-36

In October 1991, the prototype version of ACE was completed. The microcomputer-based software package is being evaluated by CSE and run through a variety of scenarios. The purpose is to perform a preliminary "sanity check" (does ACE provide reasonable results? Can we explain and understand what is happening?).

To help evaluate the model, sample cases have been run using "rough estimate" data readily available on three facilities. The preliminary findings are very encouraging. The sample runs have provided realistic results and have highlighted interesting observations.

EO 1.4.(c)
P.L. 86-36

At present, ACE is going through an extensive shakedown to validate its consistency and to examine its sensitivity to the precision of the input data (number of targets, attenuation of the TSCM, risk of threat discovery, etc.). Although a

[redacted]

CSE is now using the prototype version to evaluate technical surveillance countermeasures. Actual data from an OCONUS site was input into ACE prototype. The results were verified by CSE and the R55 team. A brief of the results will be presented [redacted] P.L. 86-36 in September. Actual data from OCONUS sites will continue to be collected and input into ACE.

EO 1.4.(c)
P.L. 86-36

DOCID: 4036135

Golden Oldie

The Dying Programmer's Lament

The programmers spoke in a fading voice,
"That diamond shows it's a multi-choice
And a loop is seen where the line returns
And a block is cleared, but my fever burns:

"O, pin me not to a completion date
When the machine is down and the assembly late,
O, think of the errors I might have made
And the debug sessions so long delayed.

"The symbolic deck with the cards transposed,
Subroutines opened, that were not closed,
The card Operations dropped on the floor,
The Sponsor's shadow beyond the door.

Yet I fought the fight. It will surely run
At the next debug, or the next but one."

So we buried him on his completion date
When the machine was down and the assembly late.
And we sighed for the errors he might have made
And the debug sessions so long delayed.

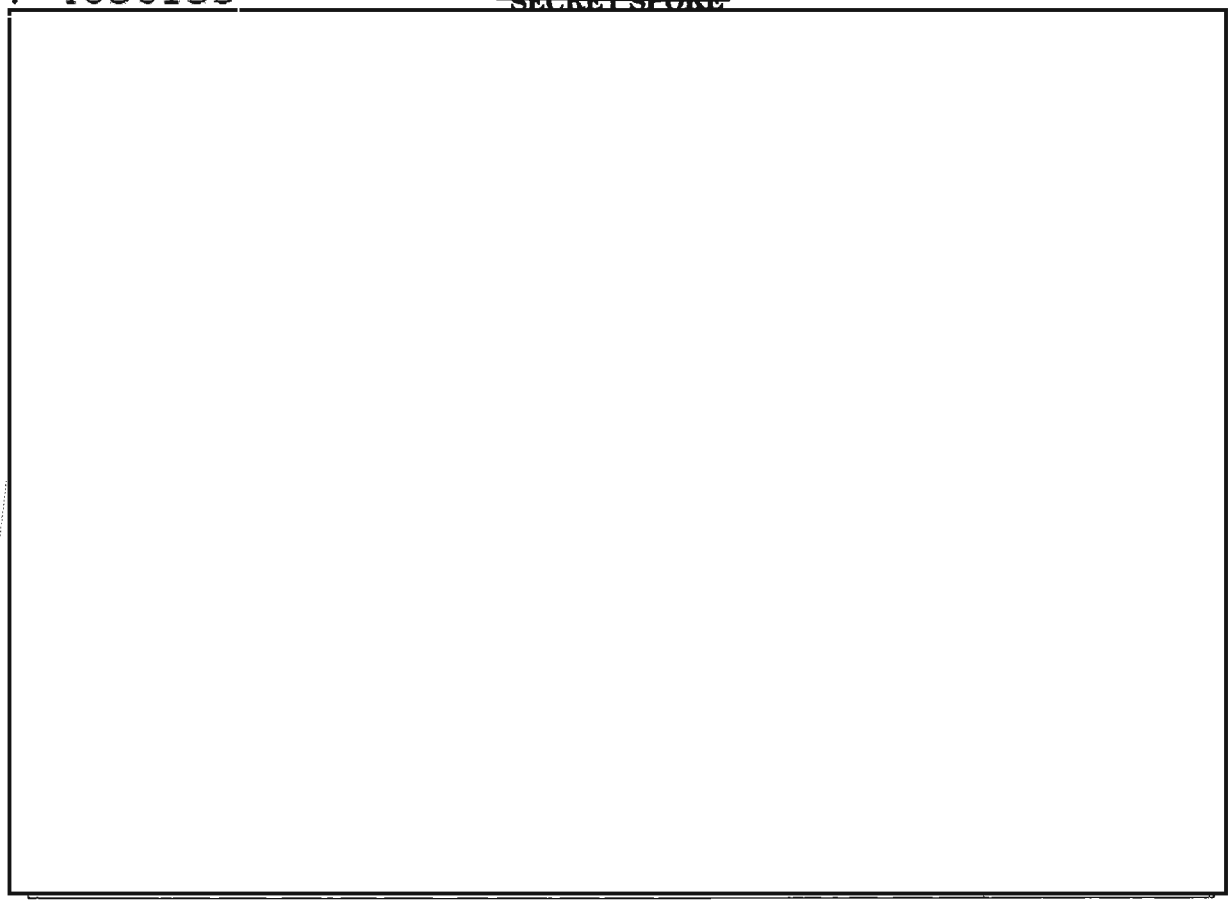
[redacted] P.L. 86-36

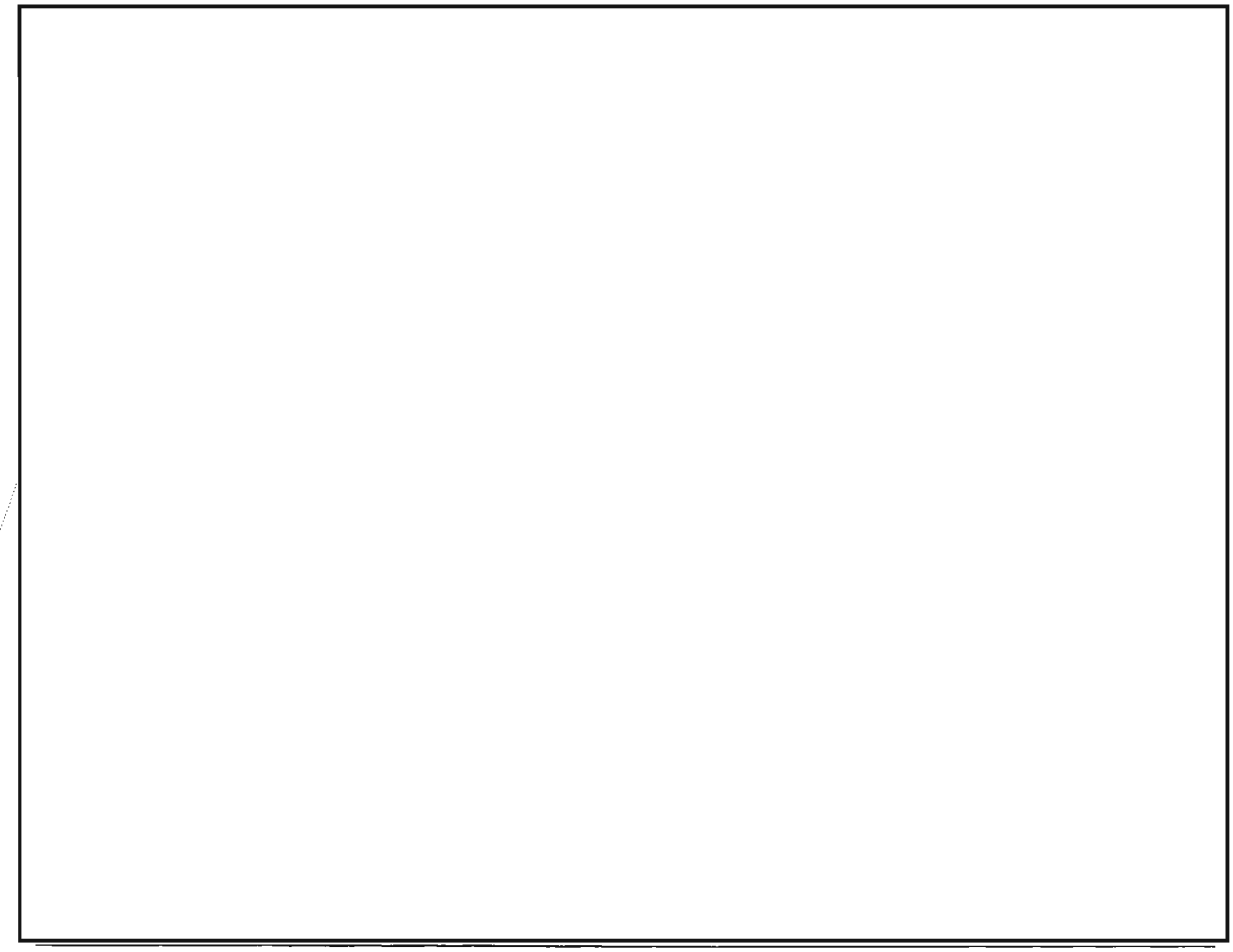
reprinted from bits & bytes

C4 MACHINE INFORMATION PROCESSING BULLETIN,

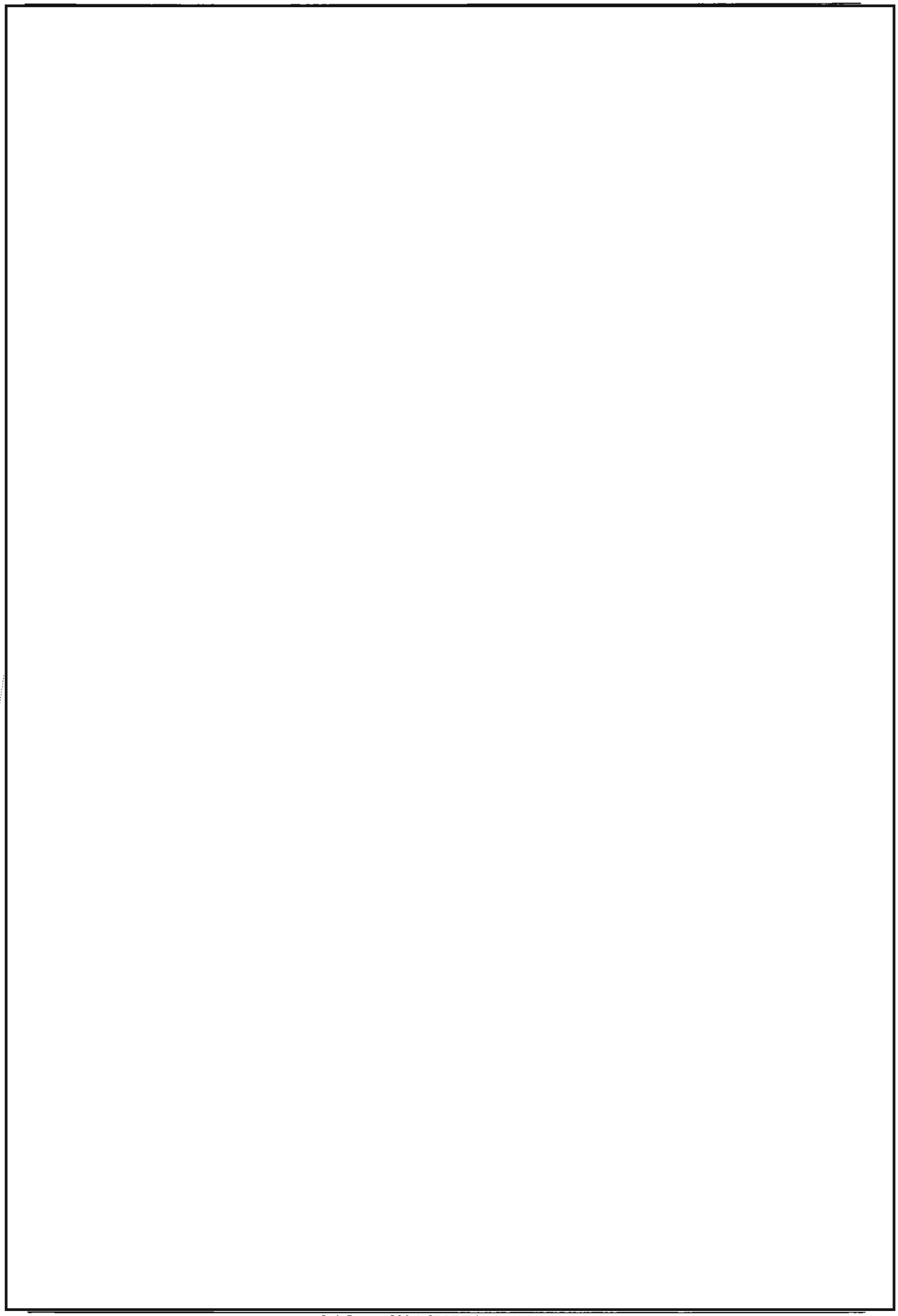
Vol I, No.2
June 1965

~~FOR OFFICIAL USE ONLY~~





EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

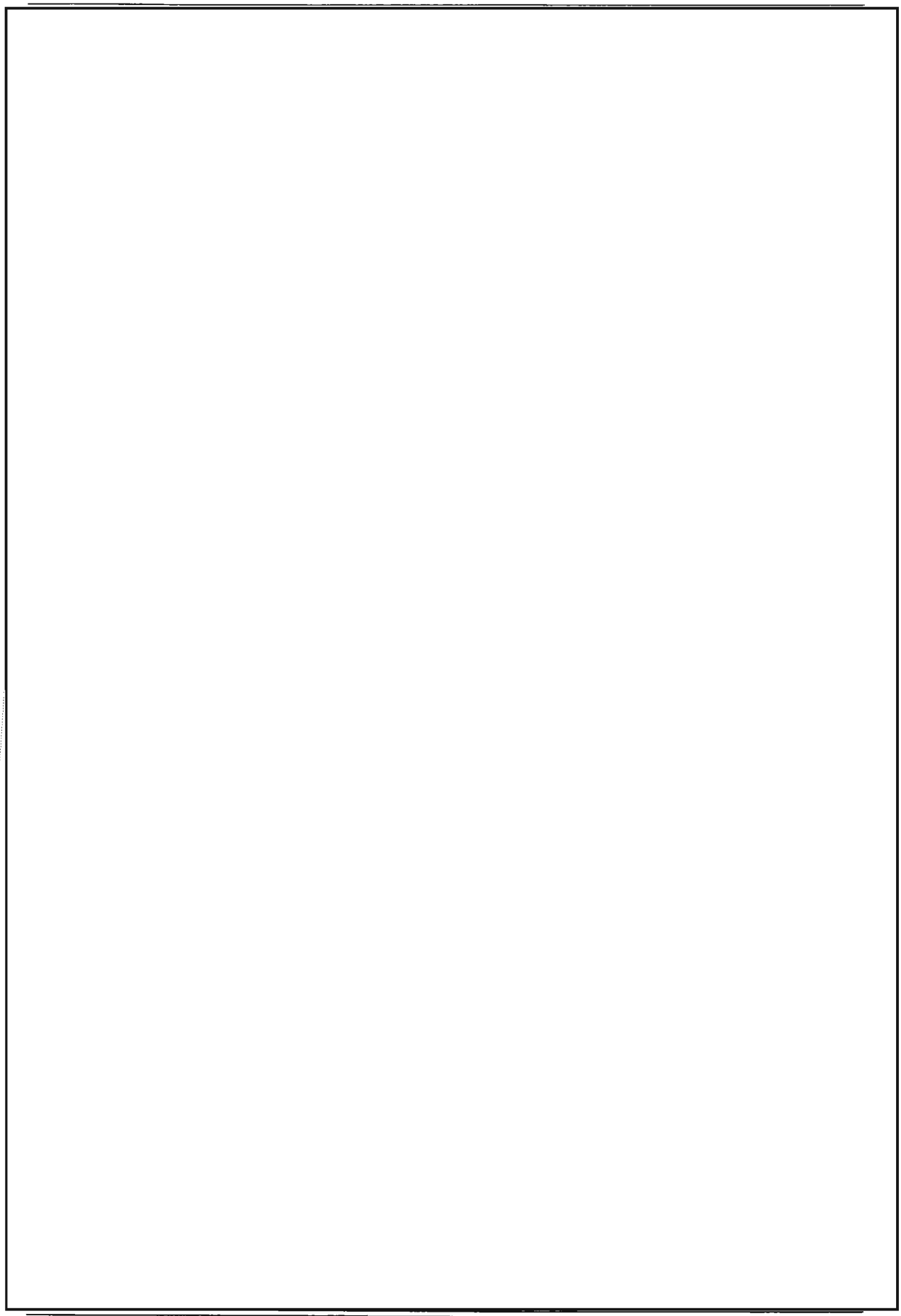


EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

DOCID: 4036135

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

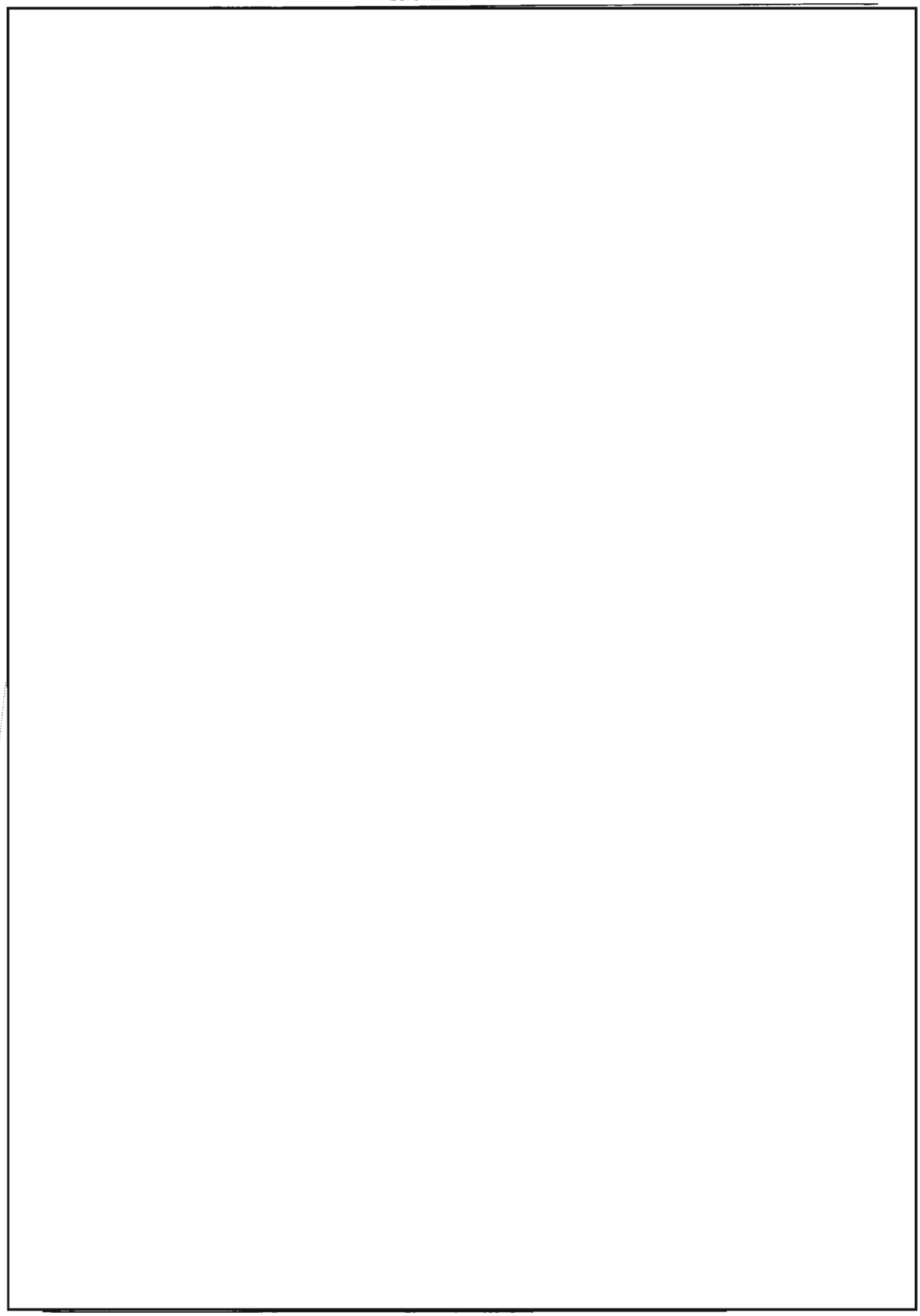
DOCID: 4036135



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

DOCID: 4036135



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

DOCID: 4036135

Writing in a journalistic style

Somali bitterness toward the United Nations runs deep, derived from what is perceived as its neglect of this country following the fall of the Siad Barre regime in January 1991. When the United Nations sent an envoy here, Algerian diplomat Mohammed Sahnoun, he publicly criticized the world body's performance.

Boutros-Ghali reprimanded and later replaced Sahnoun, who, in his six months in the post, had become widely appreciated here. His replacement, Iraqi diplomat Ismat Kittani, has run into trouble in his first weeks. His meeting with Aideed has been called a "disaster" by some of Aideed's advisers, who say Kittani spent the first few minutes criticizing Aideed for ignoring proper protocol in arranging the venue.

Boutros-Ghali is a former minister of state for foreign affairs in the Egyptian government, and Egypt is held in disdain here for having supported Siad Barre's dictatorship until Mohamed, as Somalia's interim president. Thus, Egypt—and by extension, Boutros-Ghali—is seen by many of Aideed's supporters as being biased and incapable of playing a mediating role.

Shortly after Bush made his surprise offer to send U.S. combat troops to this war- and famine-wracked nation, Boutros-Ghali was quoted as telling an interviewer that a U.N. trusteeship might have to be established here. Aideed's people describe that as a recolonization.

Aideed's ready acceptance of the American troop offer, after he had previously balked at allowing more U.N. peace keepers into the country, was seen as the warlord's way of trying to undercut the United Nations and bring America in as a political mediator.

Within days of the first U.S. Marines' arrival in Mogadishu on Dec. 9, Aideed and Ali Mahdi made their first public peace after 18 months of

P.L. 86-36 [redacted] P054

(U) During the past year, we have witnessed a myriad of local, national, and international events. "The Birds Move Into Camden Yards," "Hurricane Andrew Sweeps Devastation Across Southern Florida," and "American Troops Victorious in Persian Gulf" were but a few of the headlines that captured the attention of diverse audiences. What do each of these stories have in common? Well, no matter where you read, heard, or saw these stories, the information presented to you was planned, published, and distributed to you in a journalistic style and format.

(U) The journalistic approach to reporting tells a story. It seeks to provide the reader or viewer with a direct presentation of the facts, with minimum interpretation. You remember, the kind of reporting delivered by Walter Cronkite when he signed off at the end of each Evening News show with, "And that's the way it is . . ."

(U) The headline gives the reader or viewer a quick synopsis of the main element in a story. It attracts the reader or viewer and serves as kind of a marketing hook to get people to buy newspapers, watch television, or read NSA SIGINT reports. Never thought we were in the marketing business with our SIGINT products, did you? But indeed we are!

~~(FOUO)~~ The headline also allows each reader or viewer to pass over a story and move onto another of greater interest. Each reader and viewer has individual preferences. So in essence, every SIGINT customer constantly "tunes in and tunes out" topics of the day. Additionally, each customer also has individual preferences for receiving information. Some prefer to read, while others prefer to hear or see information presented to them. That's why newspapers, magazines, radio, and television have all flourished.

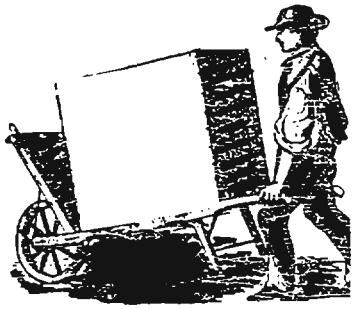
~~(FOUO)~~ Who determines story topics, what will be published for print and produced for television, and what priority each story will take? Well, in the media, a team led by a managing editor or executive producer works together to answer these tough questions. The team oversees day-to-day production while at the same time planning for the next issue or program. Quite often media senior managers get involved in these collaborative editorial group discussions to provide additional input into pre-publication planning, special event coverage, and post-publication reviews. The objective is to serve the customer's thirst for information in an accurate, timely, and highly competitive fashion. The journalistic process of identifying stories, prioritizing topics, and overseeing production never ends.

~~(FOUO)~~ The journalistic topic experts are the analysts, reporters, correspondents, writers, and producers who have intimate first hand knowledge of developing and breaking stories. The journalistic process of reporting empowers these individuals to produce and meet deadlines. The journalistic process also supports follow-up reporting and timely correction updates.

(U) The journalistic process of reporting is much like a total quality management (TQM) process. Journalism products are geared toward satisfying diverse customer demands for information, the editorial boards are collaborative process action teams, and the staffs and support mechanisms of the journalistic process are empowered to put out the best quality products possible while striving for the competitive edge. The journalistic process of reporting and TQM go hand in hand in satisfying both the customers' demand for excellence and the desire of journalists to contribute and be an integral and essential part of the process.

DOCID: 4036135

Reducing the Burden of Maintaining Software



P.L. 86-36

P043

Seven suggestions will be proposed to help minimize the burden of software maintenance. If these methods are implemented, the resulting system will be less of a burden on the data processing department that supports it. One method used to improve the maintainability of software is for the project manager to set explicit maintenance objectives and priorities. Another is to use quality-enhancing techniques and tools that will improve maintainability and will improve the system's documentation. Establishing activities that assure quality, choosing a maintainable programming language, and establishing file systems that are independent from the programs are three design concepts that will greatly improve maintainability. Finally, I will give suggestions on how to contract for a maintainable system when that system is supplied by a vendor.

SETTING MAINTENANCE OBJECTIVES

The best way to build anything into a system is to ask for it; therefore, setting explicit maintenance objectives and priorities will improve the maintainability of a software system. By setting maintenance objectives and priorities, we make it possible to influence quality, and therefore maintenance. According to the Weinberg studies each project team will achieve the highest goal set for it; whatever system qualities are stressed, those are the qualities that will be delivered. The manager of the project team must tell the maintenance programmers what quality factors their system is expected to contain. A maintainable program will possess most of the seven quality factors (i.e., reliability, understandability, testability, modifiability, usability, efficiency, and portability) but it is seldom possible to cost-justify all seven for any one program. Another block to all factors receiving equal importance is the fact that some of these factors are in conflict; one must be sacrificed to improve another. A common example is the efficiency/understandability conflict. Again, the project manager must rank the seven quality factors, and emphasize to the programmer which factors are to be delivered for the specific system in question.

QUALITY-ENHANCING TOOLS

The use of quality-enhancing techniques and tools will improve the maintainability of a system. The quality-enhancing techniques and tools that will be discussed here are: structured techniques, restructuring, reformatting, and prototyping.

Structured techniques

Structured techniques should be utilized in all phases of a system; structured techniques improve understandability (i.e., quality) and therefore, reduce the overall software costs. Structured techniques standardize the style of the software system this standardization helps programmers become familiar with the system more quickly; their understanding of the system is more complete; the quality of the system is upheld. Structured code is the introduction of standardization into the program's form. Modularization is the traditional approach for enhancing quality; the theory here is that independent pieces will simplify the program's understandability, and the maintenance task. When modularization is taken another step further, structured programming results. Structured programming is a modularized system that represents a logical and hierarchical relationship. Coupling is low; the execution flow among modules is simple and easy to understand.

Restructuring

The objective of restructuring is to improve the understandability of the existing software system and, therefore, improve its useful life. Complex, error-prone, and frequently changed modules are

~~FOR OFFICIAL USE ONLY~~

prime candidates for restructuring. A caution: we must be careful not to take poor, unstructured code, and develop poor, structured code. The goal of any structured technique is to improve the quality, understandability, and maintainability of the system.

Reformatting

If a manager considers restructuring too risky, there is still a technique that can be utilized without the introduction of restructuring. Reformatting, the introduction of indented code, standard label conventions, one instruction per line, and standardization of keywords, are much less risky than restructuring, and have also been shown to improve understandibility.

Prototyping

Prototyping is a quality-enhancing tool that can be just as useful in maintenance as it is in the development cycle. It provides usability since it allows the maintainer to understand the needs and requirements of the end user. Prototyping is most useful during life cycle support, since it minimizes possible user misinterpretations. It is a valuable, though underutilized quality-enhancing tool.

IMPROVING DOCUMENTATION

Documentation, along with quality, is one of the factors that contribute to the difficulty of maintenance. If a system's documentation is improved, so will its maintainability. Documentation can be classified into four types: user, operations, program, and data documentation. Since each performs a specific function, maintainability is improved if all forms are present. This is primarily because the maintenance programming team will be able to find exactly the information it needs, without extensive searching.

User documentation provides instruction on the use of the system's programs. Instructions are provided for the entering of data, interpreting of output information, and reacting to error messages. Usually, this consists of a user manual, but a more usable approach is an online documentation system. This online transaction would be available on the end users CRT. High quality user documentation promotes system usability. When user documentation is poor, misinformed people report errors. These hypothetical errors are really differences in the interpretation of the system's functions. Most managers agree that proper documentation is a good idea, but they seldom require it.

Program documentation is used to help the maintenance programmer understand the internal structure of the program. It is also used to demonstrate the software's coupling (how the modules interact within the system), the systems interactions with the operating system, and within other software systems. Program documentation includes external program specifications, program flowcharts, source code commentary, and system flowcharts. The most useful documentation is high-level. This documentation explains the overall purpose of the program and describes the relationships among the various program components. External (separate from the source code) documentation is necessary. HIPO diagrams and Warnier diagrams are two examples of external documentation. Low-level documentation (line-by-line descriptions) is not necessary. The best way to provide low-level documentation is through the use of self-documenting programming languages. Program documentation is produced in the design phase; problems occur since it is rarely updated to reflect maintenance changes.

Data documentation is needed in addition to program documentation. There are two ways to document data: data modeling and a data dictionary.

- The data modeling provides a graphic model identifying the structure of the data and its functional dependence .

- A data dictionary lists all the forms of data used, their definition, how they are used, where used, and who is reponsible for them.

Data documentation needs to be included, but often is not.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4036135

QUALITY ASSURANCE

Another method for improving the maintainability of software is the establishing of explicit quality assurance activities. Commonly called quality assurance audits, these activities are important in maintenance, as well as in development phases of a system.

Briefly, there are four types of quality assurance audits:

- ***Checkpoint reviews*** are used in the development of new software. They are used between the phases of development, to check the development work as it progresses; again, the sooner the error is found, the less expensive it will be to correct.

- ***An acceptance review*** is a special checkpoint review that occurs between the development and production stages. An acceptance review, sometimes called project turnover, is the last chance to ensure maintainability before the software becomes operational and becomes the responsibility of the maintenance staff.

- ***Periodic maintenance audits*** are used on operational software to recognize changes in quality. Since software systems are not static, periodic audits are necessary, and any changes in quality should be investigated. Because of the importance of overall system understanding in the maintenance function, it is helpful to have the maintainers involved in the development of the system. Ideally, they should be involved not only in the maintenance acceptance reviews, but also at other checkpoint reviews.

- ***The benchmark audit*** is used on packaged software, and it will be discussed in the section on improving maintainability in packaged software.

Audits are the most powerful techniques for introducing and preserving software quality. Managers often feel that quality assurance activities are not necessary, especially in a maintenance activity. They usually state that audits cannot be cost-justified, and quality cannot be measured. Although audits seem like a tiring, time consuming activity, they actually reduce the time allocated to maintenance; the earlier an error is discovered, the more easily recoverable it is, and the less costly the error is to correct. We have already discussed seven factors that contribute to quality (i.e., reliability, understandability, testability, modifiability, usability, efficiency, and portability) and by measuring these, we can measure the cumulative quality of the system. This should convince managers that they should practice quality audits.

CHOOSING A LANGUAGE

Choosing the proper language can affect the program's maintainability. Low-level languages are difficult to learn and understand, as are programs coded in a low-level language. 'C' language is easier to understand than Assembler, because Assembler is not structured well and does not support meaningful variable names. Recognizing this, the project manager should choose the highest-level language possible. Fourth generation languages should be utilized when possible.

Fourth generation languages are easy to use, understand, and modify. Therefore, development and maintenance in a fourth generation environment is faster. Since most fourth generation languages are non-procedural (defining what is to be accomplished, not how) these systems can be modified by the end users and may not require the help of an analyst. Even if analysts are required, they can obtain the results faster by the use of a fourth generation language than if they were to write out program specifications.

It is generally thought that the use of fourth generation languages will help the maintainability of a system. The quality of the system is improved by the use of fourth generation languages. Understandability is better, since the language is simplier and less complex. The code must be structured; since unstructured code is not obtainable with the use of a fourth generation language. These languages often are equipped with self-documentation capabilities, thus reducing the maintenance difficulty.

FILE STRUCTURE INDEPENDENCE

I think we all can agree that a file cabinet is a flexible way to store data; data can be added,

~~FOR OFFICIAL USE ONLY~~

removed, or rearranged without major difficulty. This is not always true of a computer file system; computer data files often have flexibility problems. They often have high levels of redundancy and inconsistency can occur when data are in different stages of update. Since computer files are inflexible requests for a new data arrangement can take weeks or months.

Seemingly trivial changes to a file system can set off a chain reaction (or two). The goal is to avoid changing programs when a file's physical structure changes. The data base environment was introduced to solve this problem. The intent of the data base environment is to isolate the program from changes in the structure of the data files. This environment allows the program's perspective to be different than the physical record. The programmer perceives a "make-believe" record and therefore does not worry about changes to the data's physical structure; the programmer can represent all data structures, and dynamically create new access paths. One of the factors (discussed earlier) that contributes to the difficulty of maintenance is the dependence of the programs on the file structure; the data base environment provides program and file structure independence.

PACKAGED SOFTWARE

Package software applications should be purchased with maintenance in mind. Again, the principle applies: you get nothing unless you ask for it. We should plan for the future maintenance when a software application package is purchased. Each vendor's reputation should be examined; will the vendor provide adequate service? The customer is dependent on the vendor to perform maintenance on the software; the software must be kept in good working order. This is especially true when the customer does not have access to source code and/or is not allowed to modify the software.

Current users of the packages under consideration should be sought, and potential users should discuss the package's performance. It is best to conduct a benchmark audit to ensure the quality of the protential software package. A benchmark audit is a program test conducted by the proposed users to ensure that the software package performs according to their expectations. If the vendor refuses to allow a benchmark audit as part of the selection process, another vendor should be considered. The conduct of these benchmark audits are an important part of the acquisition of an application package.

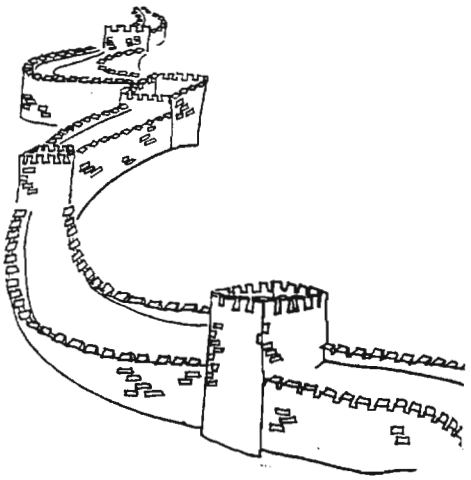
Once a package has been selected, an appropriate contract must be written. The user must have a good contract to ensure that the vendor will keep the software package in good working order. A contract contains some important specifics. A reliability clause is needed to guarantee adequate maintenance support; it should specify how quickly the vendor can be expected to respond to a request for service, how quickly the software error will be repaired after it is reported, the methods for correcting software errors, and the penalties incurred by the vendor if the reliability guarantee is not met. The software lease agreement should assure the customer knowledge of, and access to, new releases of the software package. The vendor should provide a renewal option in the contract. This clause allows the purchaser continuing maintenance even though the supplier has a short contract term. The final clause is the termination clause. This provides the purchaser with the source code in the event of vendor bankruptcy.

CONCLUSION

"Nice suggestions," you may be saying, "but I have heard all of them before. It just is not that easy to change." Although these statements are true, I feel that, with a little effort, the time and money that is put into maintenance each year will be reduced. Although all seven of these methods will help reduce the burden of maintaining software, the system should be considered when determining the appropriate method. Generally the first three methods will make the biggest impact on maintenance. Setting explicit maintenance objectives and priorities, using quality-enhancing techniques and tools, and improving program documentation will improve the quality and understandability of the computer system. Using these suggestions alone can reduce the burden of maintenance significantly. Sometimes, understanding the problem is half the solution. ⊡

~~FOR OFFICIAL USE ONLY~~

CETA



P.L. 86-36

A631

~~(S-CCO)~~ Sometime this year a data tape will be delivered to B6 containing a data set of some 250,000 Chinese-English dictionary entries. Development of a local software package will make those entries retrievable by English term, or by Chinese term in characters —both long and short forms—or by Standard Telegraphic Code from networked workstations in B Group. The delivery of that tape will mark the high point in the Agency's long, and at times difficult, participation in an organization called CETA. For a period of six years I was the Agency (acting for DoD) representative to the CETA group. Following is a brief history of its 20-year existence.

COMPOSITION

(U) The Chinese-English Translation Assistance (CETA) Group is an organization of persons from the U.S. Government and the private sector who share a common interest in the development of Chinese-English translation aids. Its purpose is to promote cooperative efforts among linguists, lexicographers, computer specialists, and others in compiling and updating computer-stored, machine-readable, Chinese-English dictionaries and glossaries; and to make available the products of those efforts to its members, and insofar as feasible, to other users of Chinese-English translation aids.

(U) Membership of the CETA group consists of agencies and individuals interested in Chinese-English translation. There are no formal requirements for membership in the CETA groups, aside from an interest in the furtherance of its objectives.

HISTORY

(U) In mid-1964, the U.S. Government sent academia a list of government needs of gaps in China research. The government, in this case, was the China Committee of the interagency Foreign Area Research Coordination Group (FAR). The contact point in the academic word was the Joint Committee on Contemporary China (JCCC), established in 1959 under the auspices of the Social Science Research Council and the American Council of Learned Societies, and funded by the Ford Foundation. The late John Lindbeck of Harvard, then chairman of the JCCC, in his reply to the government initiative, made it very plain that the scholars he represented (covering most of the private China studies programs in the United States at that time) had sufficient vague indications of general interest in government-private cooperation to support such a project. He rejected most of the topics on the list, however, such as "Minority Groups in China" and "The Relationship between China's Foreign and Domestic Policies" as non-starters in developing truly meaningful government-private cooperation.

(U) Lindbeck focused instead on a lowly project near the end of the list: "Development of a Comprehensive Dictionary of Modern Chinese Terms." Here, he said, was an area where government and academia simply had to work closely together, if the need were to be met, and time was running out.

(U) Beginning in 1964, the former Foreign Documents Division (FDD), now under the Foreign Broadcast Information Service (FBIS), assembled materials for use in compiling a general-purpose listing of contemporary Chinese terms with English translations. One of the source materials was a Chinese-Japanese dictionary containing many Communist Chinese terms; others came from China, or from U.S. Government institutions including the Joint Publications Research Service and the Foreign Service Institute. The original FDD plan was to merge six dictionaries and glossaries with computer assistance, and to have the resultant compendium published ultimately in a thoroughly-researched, commercial dictionary form.

(U) A CETA Workshop in March 1972 was designed for just that purpose. It produced the guidance and momentum that led to joint funding of CETA by 9 of its 12 member agencies, beginning with FY 1973. In two days of panel and open discussion in the informal workshop atmosphere, the mixed group of 290 government representatives and 24 academic participants (from 20 private institutions) worked smoothly together.

(U) After a well-pitched keynote address by E. Raymond Platig, Director of the State Department's Office of External Research which had funded the workshop (including travel from all over the United States and from three foreign countries), the CETA dictionary effort was explained along with the varied projects of 16 other institutions that bore on the Chinese materials processing problem under discussion. At the end of the discussions, which many described with some emotion as the most fruitful they had ever known in a conference situation, four main conclusions were reached:

- Steady increase in the flow of materials from China on research on China was likely;

- Efficient processing of those materials in Chinese and English for both government and private use in research was a definable problem of considerable importance;

- The CETA man-machine system should be encouraged to attack not only definition of that problem but also its solution;

- Further development of CETA's "living" dictionary with appropriate purpose and quantity should retain first priority among the Group's efforts.

(U) The first run of the CETA dictionary was published and distributed in September 1971, but an oversight occurred that caused long and recurring argument within the group over the dictionary. The first run was quite crude and was intended primarily for contributors to look at and evaluate, with a view toward acquiring considerable guidance and input from them. But a caveat to that effect was omitted, and as a consequence, many people looked upon it as merely a crude compilation of reversed English-Chinese dictionaries of no great value; they overlooked the fact it was a printout from an online database that could be easily corrected, supplemented, and edited, as opposed to a typeset book with its attendant difficulties.

~~(S-CCO)~~ Agency representatives, however, were most interested in this database, especially in anticipation of the SEMESTER system. Eventually, after editing, a large subset of the database was loaded into the SEMESTER system and became the central core of computerized lookup capability for B Group Chinese transcribers. By 1986, many analysts were demanding more readily accessible and manipulable computer-resident dictionary database, so greater effort was expended to refine the CETA database and to make more readily and conveniently available to Agency analysts.

~~(S-CCO)~~ Now with the acquisition of the Chinese character set on the SUN system, and the opportunity to buy large, relatively inexpensive storage capability, all of the elements finally merged to bring the best of CETA onto the desks of Agency analysts.

DOCID: 4036135

A History of Cryptology

Lambros D. Callimahos

The wartime contingent of linguists, codebreakers and cryptanalysts was an exotic mélange of multi-talented people, many of whom had already made their mark in the world. Some were foreign-born, some had already had prestigious careers in academia. There were missionaries and biblical scholars, mathematicians, classicists and linguists; there was a Russian Polish noblewoman who had been rescued by an American gunboat, a Hungarian prima ballerina who had been awarded a medal by the Pope, a professor of philosophy who was also a navy officer, cryptanalyst, and Chinese linguist, and there were others who later were to achieve fame: Eugene McCarthy, McGeorge Bundy, William Bundy, Edwin M. Reischauer; also columnists Joseph Kraft and Charles Barnett, journalist Al Friendly, and the elder statesman of bridge, Oswald Jacoby.

Among them were musicians, counted by the dozen. Scratch a cryppie, find a musician, or so it seemed. Peter Nickels, a conservatory-trained concert violinist doubled as the conductor of a dance band in the late 30's [redacted] *conducted concert versions of Gilbert and Sullivan at Arlington Hall—with a cast of equally gifted musicians;* [redacted] [redacted] *who in 1962 received the 10th Annual International Jazz Critics' Poll's "Best Unknown Trumpet Player in Jazz";* [redacted] *a jazz piano player-cum editor, and so very many others.*

And then there was Bandmaster L. B. "Red" Luchenbach, USN Band #16, assigned to the CALIFORNIA. On December 7 his ship was hit and sunk. Meanwhile his bandsmen vanished. The fleet personnel officer refused to tell him where they were, but Red persisted, and eventually joined them at Combat Intelligence. Though it was to be a temporary assignment, the musicians proved too valuable to be replaced, and so they served as machine processing specialists and cryptanalysts. By the end of the war Red had a commission. Later, in civilian life, he represented IBM at the Navy Security Station.

The star was the late Lambros D. Callimahos, dubbed "the Paganini of the flute" by music critics, a flute virtuoso on the international scene in the 30's. At the prestigious Mozarteum in Salzburg, Austria, he was the youngest professor ever.

Also in the early 30's he developed an abiding interest in the history of cryptology. LDC was a collaborator with William Friedman on MILCRYPT I and II, wrote MILCRYPT III and IV and other papers and monographs. He developed and taught the seminal course in cryptanalysis, CA-400, that Gradus ad Parnassum *encompassing the cryptography of the then known cipher systems.*

This lecture was delivered at an unknown time and place and to an unknown audience.

This lecture was entitled on your programs, "The History of Cryptology." It's had several other titles, one of which was "26! or Bust." 26 x 25 x 24 . . . x 1. To those of you who use the slide rule, to 1 digit of accuracy, it is four times 10 to the 26th.

Cryptology is an ancient profession; in fact, the second oldest profession, one that abounds in drama and fascination, and one that has had a

P.L. 86-36

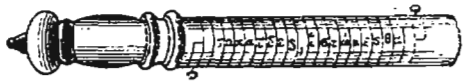
~~FOR OFFICIAL USE ONLY~~

profound impact on the turn of events in history.

We start off with communication. The Greeks did have messengers. In sending communications from one commander to another, they had the usual runners, but sometimes they wanted to be on the safe side and conceal the messages. For one idea, the Greeks would shave the head of the slave, and inscribe the message on the bare skin of the head. And then, you wait awhile—deferred message—and the slave was dispatched, not executed, but dispatched to the distant commander who would shave the head of the slave and read the message. If the message were particularly sensitive, it would be a one-time slave. These slaves are also, as you well know, normally distributed. The Greeks also used secret inks, the juices of various berries, milk, etc., brought out by heating. They used sputum and other effluvia.

On concealment, Hieronymous mentions that messages would be concealed in the belly of a hare, or inscribed on a wooden tablet and then covered with wax, or even inscribed on the leaves covering the putrid ulcers of disguised beggars. Also, on concealment, Sir Francis Bacon in 1623 wrote his renowned work, *The Advancement of Learning*, wherein he showed how he could disguise some of his innermost thoughts, thoughts which might be considered heretic in those days, by means of concealment within a covering text. It is the same system used today in our modern teleprinters. On the subject of concealment, there is also Boccacio, those of you who may have read the magnificent work in the original Italian, you know that Boccacio gave methods of information retrieval, that is, by means of the positioning of curtains or shades, but that's neither here nor there.

Cryptography was practiced, among other things, by the ancient Egyptians, only God knows why, because their hieroglyphic writing was enough of a disguise as it was, except for the learned class, the priests. And on the subject of priests, let us not forget that it is the ruffians and priests and scoundrels who have made great advances in cryptography and cryptanalysis throughout the ages. (I, myself am the son of a priest. Greek priests: a married man may become a priest, but priests cannot marry.)



ΣΚΥΤΑΛΗ

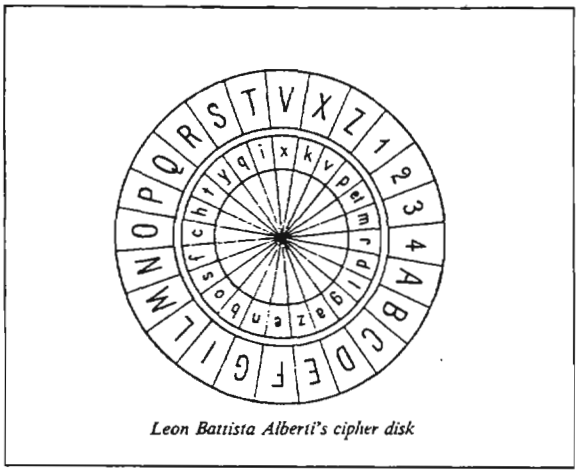
400 B.C. Lysander used a device known as the scytale; in the dictionary it is pronounced "sitale" s-c-y-t-a-l-e, but I don't like "sitale", it is a ΣΚΥΤΑΛΗ. The scytale consisted of a baton that the marshall carried, about yea long, tapered with a notch at one end, and the marshall would take off his belt, and wind the belt around the scytale and then write the message (in Greek, of course) across the bars; then he would take off the belt and dispatch that to the distant commander, who having a scytale of the same size, would affix the one end of the belt on the notch, wrap it around, and lo and behold, the Greek plain text came out. So that was our first transposition system. Also in 400 B.C., we have Aeneas the Tactician, who wrote a voluminous tome on the defense of fortifications, one chapter of which was devoted to the subject of cryptography. This was the first treatise on cryptography.

100 B.C. Julius Caesar, in corresponding with Cornelius, Baudus, Opius—whoever the devil they were, and others—used a simple scheme of replacing each letter in the Latin alphabet by one three removed from it, in other words, A plain would become D cipher, B plain would be E cipher, etc. But this was too much for Augustus' brain; he preferred a simpler scheme, where A plain was replaced by B, B by C, etc.

Now we jump to 1200 A.D. and the Papal States. By this time there were active cryptographic bureaus in the clergy, and the Papal States were the first ones to engage in systematic crypto correspondence. They often substituted vowel marks for the vowels, leaving the consonants unchanged. In other words, Mississippi would be spelt M.SS.SS.PP., where one dot might be an I, two dots an E, etc. In

DOCID: 4036135

1378, Gabriel de Lavinde of Parma, who worked for Clement VII—and if there are any historians here, they know Clement the seventh did not flourish at that time, it was the anti-pope Clement the Seventh. Lavinde wrote an SOI, a signal operating instruction, which is on deposit in the Vatican right now, and he gave many alphabets for which he had multiple equivalents for the single Latin letters.



Leon Battista Alberti's cipher disk

In 1470, Leon Battista Alberti wrote his *Trattati In Cifra*. He was an architect, painter, musician, writer on art, and the most universal genius of the First Renaissance. He invented, among other things, the cipher disc. In 1404, on Monday, July 4th—imagine what prescience the man had—Cicco Simonetta, an Italian, but nevertheless born on the 4th of July, wrote a little tract on cryptanalysis, the oldest tract extant, and he observed what you can do with Latin secret writing, by capitalizing on frequencies, on patterns of words, and on vowel identification. His methods were so good that they hold even today. He didn't get very far; in 1480, he lost his head. That was Monday July the 4th, 1404.

In 1531 David Trithemius, the German Abbot, wrote volumes I and II of a projected 4-volume work. He never finished the work but it was the first extensive treatise on cryptology. He was also a magician—after all, in my business, every little bit helps—and he was accused of being in league with the devil, and his books were burnt, but fortunately he wasn't.

Now the meaning of 26! There are 26! ways of scrambling the letters in the sequence ABCDEFGHIJKLMNOPQRSTUVWXYZ. You all know the number. If you set up here a set of letters for the plain component for the cipher, under **A** plain you may put anything you want—suppose you put an **X**. You had 26 choices here. Having an **X** here, there are only 25 choices here—make that an **O**. To gain some idea of the great size of this number, if you had 1,000 machines capable of testing 1,000,000 different alphabets per second, it would still take you over one billion years to go through the gamut of all alphabets. However, since you have a .5 probability of hitting before you reach half-way through, you can say roughly, you have the expectation after 500 million years.

One of Giovanni Battista Porta's cipher disks

You don't, though, in solving a simple substitution cipher, have to make all these trials. We do work on frequencies, the fact that the letters composing language are not equiprobable. We do work on repetitions, not only of letters, but also of digraphs, trigraphs, et cetera, and of long sequences that you hope are complete words. And we do work on patterns, like the word CEMETERY has an A B A pattern

~~FOR OFFICIAL USE ONLY~~

DOCID: 4036135

Three Victorian amateur cryptologists: Sir Charles Wheatstone, inventor of two important cipher systems; Lyon Playfair, First Baron Playfair, who gave his name to one of Wheatstone's ciphers; and Charles Babbage, who solved many difficult ciphers.

for the 'e m e'. The word BATTALION has a A B B A pattern for the repeated letters 'a t t a', et cetera. So, quite early in the game, when people realized the weakness of simple substitution, they thought they'd get around it by having variants. So, where E is 13 per cent in English, instead of having one cipher symbol that would stand out 13 per cent, you'd now have 5 symbols that stand out about 2 or 3 per cent each.

All these remarkable ideas in cryptography were offset by even more ingenious ideas in cryptanalysis. We'll come back to codes in a minute. The departure was in the latter part of the nineteenth century—I'll skip over that for a minute, and go on to what happened.

In 1914, a First Lieutenant Mauborgne published a paper put out by the Army Service School's Press, Ft. Leavenworth, Kansas, and the title, "An Advanced Problem in Cryptography and Solution," had to do with the Playfair cipher. (It was invented by Sir Charles Wheatstone, who did invent the Playfair cipher, but it was Lord Lyon Playfair who sponsored it in the Foreign Office, and gave it its name. But that's all right, because Wheatstone didn't invent the Wheatstone bridge. Wheatstone applied Cristi's dimension to the measurement of the bridges, so you see, it balances out in the end. On top of that, for those of you who might be interested, Wheatstone also invented the concertina.)

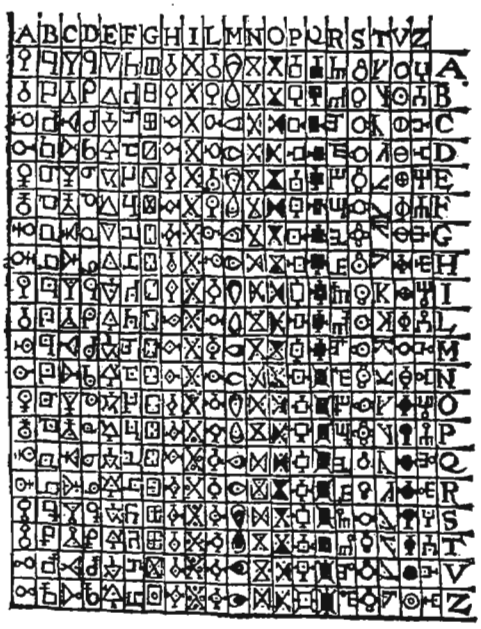
Instead of encrypting one letter at a time, in the Wheatstone Playfair, you encrypt two letters at a time. So EN is CP; this diagonal of the imaginary rectangle is enciphered by the other diagonal of the imaginary rectangle; and PC is NE.

This was a brilliant idea, because it suppressed the frequencies of single letters. However, Mauborgne did show them one method of solution. And he made good anyway, because he rose to be Chief Signal Officer.

Leon Battista Alberti (1404-72) considered the father of western cryptology. Alberti was also a talented musician, writer, artist, and athlete—a universal man.

In 1902, a chap by the name of F. de la Stelle—F I suppose was François, but it could be Felix, nobody knows—wrote in 1902 a book called *Traité de Cryptographie*. He mentioned in this book a system by which some letters might be enciphered by single digits and other letters by pairs of digits. This was an academic curiosity until the '30's, when this system took on major proportions, not as is, but with certain kinds of disguise. I mentioned briefly some ideas of simple substitution, and also the idea of transposition as exemplified by the scytale.

~~FOR OFFICIAL USE ONLY~~



The earliest known digraphic system: Giovanni Battista de la Porta replaced each pair of letters with the sign at the intersection of their row and columns.

In the 16th and 17th centuries, transpositions came to the fore. In a transposition system, you retain the same language elements of the original message, except that you permute them about. Their identities remain the same, but their positions have been changed. The substitution systems, of course, the positions remain the same, but the identities change.

The first idea of polyalphabetic substitution was given really in 1470 by our friend Alberti in his cipher disc. In 1563, we have Giovanni Batista de la Porta. He was a physicist, inventor of the camera obscura, which was a predecessor of the Kodak, and he was a healer of the sick, just as we are healers of sick messages. He is known as the father of modern cryptography because it was he who pushed the idea of polyalphabeticity. In 1586, a French gentleman by the name of Blaise de Vigenère was travelling, and one of the things he picked up while in Italy was the idea of a square table to which he gave the name 'the Vigenère tableau'. He didn't invent it, moreover, he never said he did, but he gave his name to this idea with which you could perform true polyalphabetic substitution with no limitations.

That was in 1586.

In 1765, there flourished in the true sense of the word a truly great man, Giovanni Jacopo de Seingalt, otherwise known as Casanova; he was a remarkable scholar, a savant, a person who, well I can't say we should all emulate, but at least study because I'm sure we could all learn from him. One of his remarkable exploits was the fact that—thank you, somebody who was asleep is now awake—was his solution of a polyalphabetic cipher 100 years before the method of attack was announced to the world by the German Major Kasiski. Of course, Casanova was a privileged person; he managed to get cribs in the most remarkable places. But, the way this came about, I'll give you very briefly the background of all this—oh my gosh—the background will have to rest—if any of you wish to see me privately I'll give you the full story about what happened to the Marquis when he solved her cryptogram.

1863 was the date of Kasiski.

Now we come to codes. The ancients went from simple substitution to variant systems, to dissimilar writing wherein certain groups of characters, or for that matter, certain plaintext words, took on a new meaning, like 'ALMONDS' means 'I won't be home until Friday.'

So codes came out quite early in the game, but it wasn't until 1640, the great French cryptanalyst Orsignon that the two-part code came into being. In a one-part code, the code groups are arranged alphabetically and the vocabulary elements are in alphabetic order also. In a two-part code, one section, the encoding section, has the vocabulary elements in alphabetic order with a scramble of the code elements, and then another part with the code elements in alphabetic order for ease in decoding. The idea of an enciphered code soon followed, because of certain weaknesses of unenciphered code systems.

We might go back for a moment —to the earliest cryptanalysis. 550 B.C.—Please note the date—Daniel read a cryptogram for Bathsheba. It was a good stunt: there were symbols on the wall. He not only pronounced the symbols, but also gave the meaning. And since there was nobody

~~FOR OFFICIAL USE ONLY~~

there to contradict him, why, he made hay while the sun shined.

In 1510, Yulan deSoto of Venice solved many ciphers, including those of Charles the Fifth, which had been intercepted by the Papal Court and not solved by it. So he was an outsider, like an NSA consultant.

In 1525, the British lion begins four centuries of successful cryptanalysis.

In 1556, Alberti solved a message for the Portuguese ambassador who had lost his own code. This wouldn't happen today. I mean, if a diplomat loses his own code, he doesn't come to NSA asking for help.

1567. A prior in St. Peters, according to Vigenère, deciphered in less than six hours, a large page of cipher in the Turkish language, of which he did not even know four words. Having travelled, I can imagine what the four words were.

1589. François Viete, also know by his Latin name of Vieta, who as Privy Counsellor in

John Wallis, clergyman and mathematician, England's first great cryptanalyst

France, solved a 500-group code of Spain's Philip the Second. Philip bitched to the Pope that France was using sorcery, so there was a miniature Pearl Harbor investigation on Viete, who to avoid conviction of sorcery, a capital offense, told all.

Antoine Rossignol, the father of French cryptology

That's 1589.

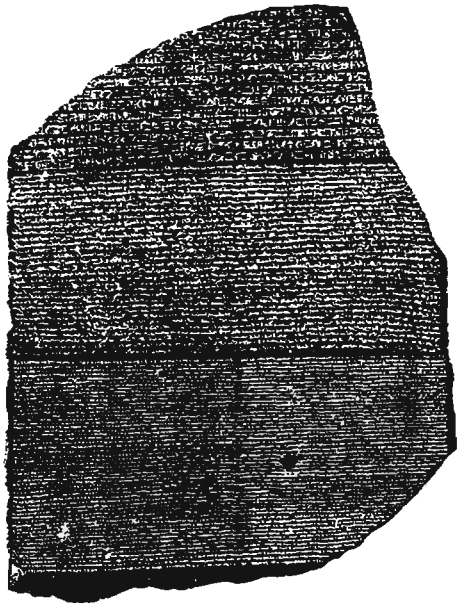
1595, in June, Viete, by this time was a good blabbermouth, in conversation with the Vatican ambassador to France, revealed that his ciphers were being read. That's the worst of all the sins that one could commit.

1626, Rossignol, who was remarkable for keeping his trap shut, began a cryptanalytic career with Louis the Fifteenth. When Louis was dying, he told the queen that Rossignol was one of the men most essential to the State. He was fifty-six years a civil servant. Brigadier Tiltman is second only to Rossignol. Wallis in 1645, the great English mathematician, began a career of five decades as an active cryptanalyst. (The Brigadier is in the middle of his fifth decade.) He was under Cromwell, and he solved the secret cipher of Charles the First. In 1689, still going strong, he solved the cipher of Louis the fourteenth, a 600-group two- and three-digit code.

In 1821, Jean François Champollion, a miserable little fellow, with a pale complexion, yellow

~~FOR OFFICIAL USE ONLY~~

skin, slaty eyes, was very gifted as a child. He told his brother, who later became his keeper—not in that sense, I mean his brother sacrificed his life for the more adept junior— little Champollion became imbued with the idea of reading the Egyptian hieroglyphs. He fell to work reading everything he could get his hands on, Modern Egyptian, et cetera—he was a gifted linguist—and in 1821, Champollion succeeded in breaking the secret of the hieroglyphs.



The Rosetta Stone

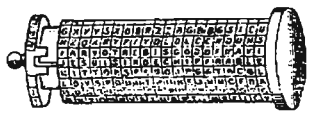
The hieroglyphs were broken by means of the Rosetta Stone, a piece of black basalt, three feet high two feet across, with three inscriptions, evidently parallel inscriptions, in Greek, Egyptian demotic, and hieroglyphs. He had what we call isologs, and he was very, very fortunate, because to recover an unknown language takes some cryptanalytic 'in', some cribs, and this was the height, where he had parallel texts in three versions.

We come now to cipher devices, again to our friend Alberti in 1470, the first one to dream up a cipher disk. Then by 1500, the idea of a cipher disk occurred to many many people, a disk, let's say of 26 letters revolving inside a frame of another circle of 26 letters. The idea was invented dozens of times.

In 1867, Sir Charles Wheatstone, inventor of the Playfair, thought up an ingenious little mechanical contrivance, to which he modestly gave the name, 'The Wheatstone Cryptograph.' It, for its day, was the most sophisticated idea in cryptography, but it lay buried in the archives.

Incidentally, although Sir Charles' idea was in 1867, in 1807, an American got there first, Decius Wadsworth, who was later chief of Ordnance, U.S. Army. He invented the same principal as the Wheatstone cipher device and executed it even better, mechanically. This device rested in limbo and the British knew about it, and in World War I, the British wanted to use the idea. Now the solution was known, the solution where the plain component was the normal sequence and the cipher component an unknown mixed sequence. But there was no known solution to the Wheatstone Cryptograph with two unknown sequences. But we'll come back to that story after a few minutes Let me do some more on cipher devices.

In 1891 a French major on the General Staff, a reservist, by the name of Etienne Bazeries, published in 1901 an essay showing the idea of a spindle with 20 disks permutable on the spindle, each of the disks had an alphabet a mixed sequence inscribed on the periphery, you arrange the disks on the spindle according to the key, set up the disks along a guide bar for your first twenty letters of plain text, and send the cipher text, every other row. At the other end, the deciphering clerk would have the same disks arranged in the proper order, he would set up the cipher text on the disks and look around. One and only one row



Bazeries Spindle

~~FOR OFFICIAL USE ONLY~~

DOCID: 4036135

would have plain text all the way across. He had a picture of this device in his book and across the guide bar was the sentence "Je suis indechifférable," "I am indecipherable."

Let's see, the book was published in 1901, it was 1891 when Bazeries thought of it, but it was in 1893 when a buddy of his, the Marquis d'Viares, another one who didn't have to work at cryptology, who was very skilled—I consider this piece of cryptanalysis the greatest piece of cryptanalysis, considering the age in which it was done. D'Viares showed Bazeries how he could arrive at a general solution of the device having only possession of the disks. This you would assume in time of war that the device would be captured.

It was Bazeries who published it first, then in 1915 an American army captain by the name of Parker Hitt invented the device again, He was the third inventor, because I didn't mention that the first inventor was Thomas Jefferson, but his papers weren't discovered until 1926, and he showed in his papers the idea of 36 disks on such a spindle, and that was a most remarkable cryptographic idea of its day.

Now we come to World War I. Radio.

To coin a phrase, radio is a two-edged sword, and you can go on from there. Every lecture you hear at NSA has that phrase in it, so it's wise to remember it. On the 26th of August, as you all remember, in 1914, the battle of Tonnebre, lasted three days; 100,000 men were killed or wounded, and missing in action. Two Russian commanders—Samsonov commanded the Second Army, Rennenkampf commanded the first Army. They didn't like each other, they had no contact with each other, not even on the staff level.

Samsonov went out in the field with the old code, but in the meantime Rennenkampf received the new code from Moscow, so he promptly destroyed his old code. He sent a message to Samsonov, who couldn't read it. He asked for a relay in the old code. He couldn't get it because Rennenkampf had destroyed his old code. So then Rennenkampf proceeded to send his messages in plain language. The Germans couldn't believe their ears. They read the messages where the Russians were supposed to be, they sent out reconnaissance patrols, found out that the Russians were there, then every day—it wasn't every day for long, just a few days, they waited for the day's take before they made up their battle plans, and in three days everything was lost. So that is a fine example of how things can go wrong.

The next item I wish to cite in World War I, was 16 January 1917. The Zimmerman telegram. Perhaps the most famous cryptogram in history. Zimmerman, the Foreign Minister, sent a message to Bergstoff here in this country for transmittal to Eckhardt in Mexico. This telegram offered Mexico parts of Texas, Arizona and New Mexico if Mexico would enter the war on the side of Germany. Of course this is a dreadful abuse of the hospitality of a neutral country. The British solved the message, and conveyed it to us with some misgiving, because they didn't want to reveal what they had been doing. At the beginning, the anti-British faction here thought that it was another trick to get us into the war, but Zimmerman was queried in Berlin, and he admitted to having sent the telegram. Six days later we were in the war.

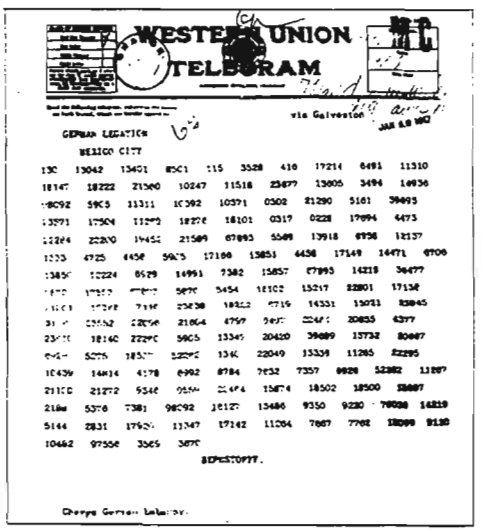
The U.S. Army went to war with three dreadful systems. One was the War Department Telegraph Code, which was safe because it was large enough so you couldn't hide it under your tunic, you'd have a bulge, and it had to have a certain amount of security to go with it because of the size, and the U.S. Army Cipher Disk, with reversed standard alphabets, the solution of which you'd do in the first lesson of Military Cryptanalytics Part II, and you could solve a single message, you could solve a portion of a single message.

In any case, that's what we had as the mainline system, and for emergency, we had the Playfair, but on every SOI every two or three days when they changed the key word, there was a warning: please don't use it because it's weak, insecure.

~~FOR OFFICIAL USE ONLY~~

So that was on the U.S. Army side.

The Germans were more fortunate, they had double transposition, they had complex polyalphabetic substitution systems, and very ingenious combined substitution transposition systems known as the ADFGVX cipher. It was so remarkable that if I sent you a message, and then I had a power failure—not me, the station—when I sent only half the message, you still could reconstruct the entire message from the half that had been sent. You can't do that today.



Zimmerman Telegram

The Germans were methodical so-and-so's, and instead of having check procedures to make sure that the system was working right, what they did was they sent aphorisms or parables early in the morning first day of change and they had various axioms, one of the most frequent parables was "Morgen Stunde hat Golden Munde," "the early bird catches the worm." So whenever there was a key change or a system change, the Allies would search through early in the morning for a short message, find it, put against it one of these parables, and in an hour or two they'd have that system.

Now we'll come back to the Wheatstone Cryptograph episode. The British wanted to introduce the Wheatstone Cryptograph into World War I, but were reluctant to because if the Germans captured it they too would have the indecipherable cipher—remember, there was no known solution if you had two mixed components. So it was judged unsolvable by the British, the French, and the Americans, both in the AF and in Washington, until someone remembered the group of people out in Geneva Illinois, industrial laboratories called Riverbank Laboratories, headed by a megalomaniac named George Fabyan. A private concern.

At this joint there was a young geneticist named William F. Friedman. What happened was that this chap Fabyan had a hobby of Baconism. He wanted to proved that Bacon wrote Shakespeare or vice versa, and he got a young lady in his employ by the name of Miss Elizebeth Smith, to read what there was in English (there wasn't much, God knows) to help him with his hobby. So then she had small classes in cryptology, and one of the gents was this William Friedman, who did very well, and so he later took over the section.

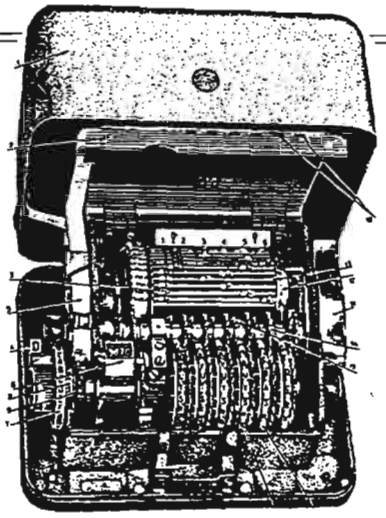
Anyway, Somebody remembered Friedman and the people at Riverbank so they decided to send six short messages out to Riverbank Laboratories, to see what could be done with them. Now they were only about twenty or thirty letters each, and that's really not a very good test, but Friedman by 'horsing around'—those were the words he used—managed to

The Wheatstone Cryptograph
Plain is outside, cipher is inside

~~FOR OFFICIAL USE ONLY~~

scrounge out a cipher component. But he didn't know what to do with it, because it wasn't until 1923 that he discovered a very strong principle, the reduction to monoalphabetic terms.

So not knowing what to do, he called in Miss Smith, told her to sit down, make herself at ease, put on lipstick—I suppose she had some on before, but—anyway, and "I'm going to give you a word, you tell me the first word that comes to your mind." So he said 'machine', she said 'cipher'. I forgot to mention that the cipher component was based on 'machine' —a transposition mixed-alphabet based on 'machine'. So he didn't know what to do, but he asked Miss Smith, and she gave it to him. The plain component was based on 'cipher'. To keep it in the family, he married Miss Smith. The solution that went back to the British was quite embarrassing, because the method he described for getting the cipher component was so strange that even today you can't fathom it. It was part astrology, part cryptanalysis, that's hard



The Hagelin machine

enough to understand, but then about the plain component: I asked Miss Smith, and she gave it to me. So that's the story about the Wheatstone Cryptograph in World War I.

Then in the early twenties, a number of cipher devices came forth, the early Damm device, not damn, D A M M, Aubry Damm, operating with chains and gears and what not. This Damm firm was predecessor to the Achting-Bolotek Cryptographe, which is the firm headed by the Swede Boris Caesar Wilhelm Hagelin. More of that later. It was Damm who really invented the first rotor. In 1924, a German by the name of Alexander von Kryha invented a gadget which had an astounding number of possibilities, like the number I wrote on the board before, the Kryha machine, and he got a buddy mathematician to explain in precise mathematical language, but even if you went through all the alphabets in time, blah blah blah, you could never go through them. However, the device is solvable and even on a single message.

This broke the man's pocketbook and also his heart; in fact, he committed suicide a few years back, perhaps because he couldn't push his device. This mathematician buddy of Kryha's came up with the statement that the number of possibilities with this machine was 1.4 times 10 to the 64th. And since the number of atoms in the universe, according to Sir Arthur Eddington is only 3 times 10 to the 74th, you can see it's a very favorable comparison indeed. Factorial 26 is only in the order of magnitude of 10 to the 26th, and here we're talking about 10 to the 64th.

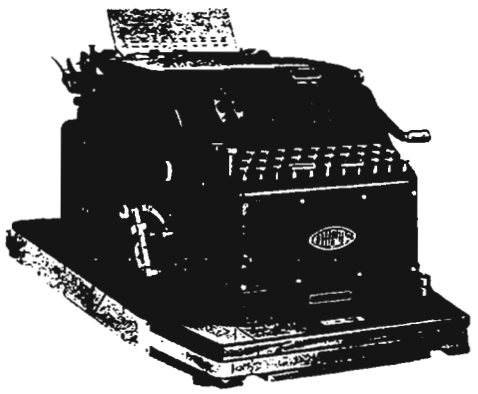
B. C. W. Hagelin—a brilliant engineer, who came forth in the early 1920's with a whole series of devices. The first one was an ingenious contraption—fractionating principle. What it amounts to is this: you press a key on the typewriter keyboard, it sets into action two rods, mechanical rods, which are the left-hand the row components and column of a fractionating square; in other words, A is 1 6, then K is 2 0, for instance, this 1 6 would be enciphered separately, by separate schemes, recombined through this square, to get a single letter output. In other words, one letter input is fractionated into two halves, they go their separate ways, in a complex fashion, and join together in holy matrimony at the other end.

This was a wonderful idea, except when examined by William Friedman and his people in the early S.I.S days (Signal Intelligence Service of the U.S. Army), when this was found wanting. It's like a young girl who has had many offers of

~~FOR OFFICIAL USE ONLY~~

marriage, and never the knight on a white charger, or whatever it is.

They broke up every cryptographic idea that had been proposed to them, or that they heard



The Enigma

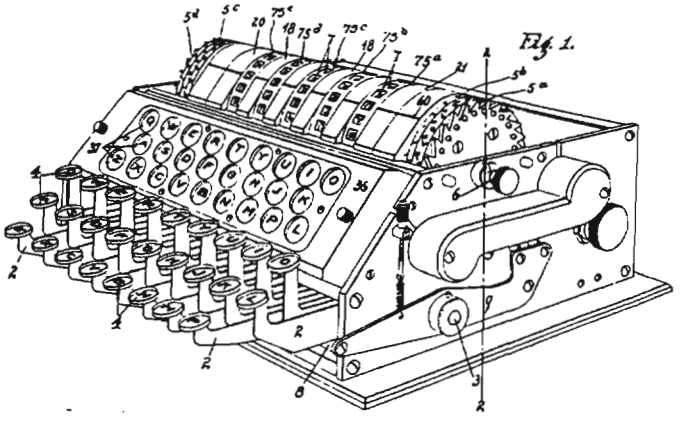
of—they demolished, but they didn't come up with any good ideas themselves. They realized the enormity of their crime. They know no matter how complex something looked, the solutions may not have the same order of complexity. That's why in 1923 we adopted for the lower level cipher device, a tactical cipher device, the M-94, which is this disk device that harkens back to Jefferson days. This was in use until 1942. The solution is a childishly simple matter, especially since it was published in 1893.

Significantly, we're the only nation that adopted it; the French refused to have anything to do with it. We had nothing better until one of Hagelin's devices came along, accompanied by Hagelin, and this ingenious device about seven pounds, this big, gave rise to a very long key, the alphabets were known components, reversed standard alphabets, but the key was 26 x 25 x 23 x 21 x 19 x 17. So that's a very long cycle. It didn't mean that for a solution you had to wait for a message that long, but it did have certain fundamental weakness that nevertheless, in spite of the advice of Friedman and the Army, we did lease the North American rights and thousands of the devices were made by the L.C. Smith-Corona Company during the war.

The Hagelin machine was a very fine advance over the M-94, but still no good compared to what we should have as a major power. The better idea, now this was a tactical machine, something you could carry about with you, they even had the paratroopers landing with the 131 pins, their own two pins and the 131 pins of the M-209, and all 54 lugs zeroized on the assumption that after the poor devil hit the ground, if he was still capable of so doing, he'd get his key list out and do this while the tracer bullets were going over his head.

I'm sure there must have been more than one violation of security, where a man dropped with his machine already set up.

The first patent for a wired wheel machine was in 1918 in Germany. In 1923 the Enigma was patented. These machines involved discs, known as wired wheels there's switching combinators. With every encryption or decryption, one of these discs changes its position to give rise to a new alphabet. So if you had five of these cipher



Hebern Electric Super Code

~~FOR OFFICIAL USE ONLY~~

wheels, you have a potential of 11,880,000. The inventors of the first German rotor machines, we're not sure whether it was Scherbers or Korn.

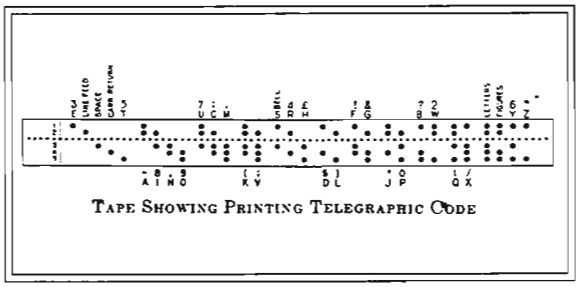
In 1923, an American by the name of Edward Hebern, out in California, also invented a rotor machine, to which he gave the name "the Hebern Electric Super Code." He interested the Navy in this device, it was a three-rotor machine, but he was asked to build a five-rotor machine. At that time the Army and the Navy were not talking to one another, and Friedman, who was on the Army side of the business, found out that the Navy was interested in buying some of the these. The Navy wouldn't let them have one of the machines, so the Army bought two. Then Friedman said the machine was weak. Actually he said so out of his hat, because he had no idea how to tackle it. It had a potential 90 billion cipher alphabets. Any self-respecting cryptanalyst should have thrown up his hands in horror.

Anyway, he found out that the machine the Navy had was not the same as the one that he had, because he asked for some letters to be encrypted with a certain setting across the wheels. So, to make a long story short, the Navy sent ten messages encrypted on this device, and Friedman, who was terribly unmathematical—in fact, he was just very, very lucky. He blundered his way into solution time and again.

In 1917 an American engineer by the name of Gilbert S. Vernam thought of a way for encrypting teleprinter signals. As you know, the teleprinter code is a binary code—I used to say two things taken five at a time, but mathematicians objected—it's five things each of which can take one of two states, on or off, whatever you want to call it. So the symbol for an **E** let's say, on a teletype tape is a hole and in the next four hole positions, there's no hole. That's an **E**. This is a **T**, et cetera. So Vernam thought up an idea of having a key tape prepunched random tape used to key a plaintext message tape. Then he thought he could do one better (this key tape, of course should be one-time, because then the security is infinite if the key tape was produced at random). But of course, it's clumsy, and then there's the difficulty of distributing the tapes, et cetera. So then he thought why not have two key loops, let's say of a thousand characters and 999 characters, so, since they're relatively prime, it takes 990,000 encryptions before you get back to the same arrangement of the two tapes. He even had an idea for less security—he proposed the idea of a single key loop. In MC II I wrote that the security of this scheme, however, is either negligible or only two or three times that amount. To us it makes sense.

It's interesting that Friedman, in 1919, meantime had been a good boy and gone overseas; he was a captain with the AEF in the code compilation section. After the war he went back to the Riverbank Laboratories, and there examined some traffic sent for test purposes by the State Department.

So the State Department was about to use this



TAPE SHOWING PRINTING TELEGRAPHIC CODE

two-tape idea. To be on the safe side, they sent a series of messages to Riverbank. Friedman and his staff worked two or three weeks on this traffic and got no place. They were sore in mind and body. This was the first time they worked for such a long period without solution. Everything they had come across they solved, and they couldn't understand what was wrong with them; there must be something wrong with them; they were all losing their buttons, and they wanted to leave him. It was a total of five weeks that they worked. One by one they wanted to leave and Friedman said "Give me a last chance. Let's go over our steps, we'll work one more week, if we get no place, we'll give it up." So they went over their steps (by the way, they had no tape printers for getting hard copy;

~~FOR OFFICIAL USE ONLY~~

DOCID: 4036135

they had the teletype tapes sent to them, and they had to transcribe the holes, et cetera, with the Baudot code in front of them on sheets of paper.) And in the transcription, one chap left off a character that happened to be at the crucial spot. By the end of the week, they solved the system.

WORLD WAR II

We can go in the last five minutes, to World War II to give you some idea of the COMINT successes we've had. By the way, these items came out in a very dry article in *Time* magazine shortly after the war, when they had the Pearl Harbor investigation, when everything was revealed, to our detriment. That particular *Time* issue said that through MAGIC, which was the then cover name for our COMINT product, it enabled a relatively small U.S. force to intercept a Japanese invasion fleet and win a decisive victory in the battle of the Coral Sea, thus saving Australia and New Zealand. It gave the U.S. full information on the size of the Japanese forces advancing on Midway, enabling our Navy to concentrate ships which otherwise might have been three thousand miles away, and thus set up an ambush which proved to be the turning point of the Pacific War, directed U.S. submarines to sea lanes where Japanese convoys would be passing; and made possible the reading of messages from the Japanese Ambassador Oshima in Berlin, often reporting interviews with Hitler, giving our forces invaluable information on German war plans.

When the lid was blown, which was a dirty shame, because the world at large knew the cryptanalytic potential of the United States. In the report of the Joint Committee on the Pearl Harbor attack, there are two other quotes I would like to read you:

> With the exercise of the greatest ingenuity and all obvious resourcefulness regarded by the committee as meriting the highest commendation the War and Navy Departments collaborated in breaking Japanese diplomatic codes. Through the exploitation of intercepted and decoded messages between Japan and her diplomatic establishments, the so-called Magic, a wealth of intelligence concerning the purpose of the Japanese was available in Washington.

Another quote:

> Important diplomatic messages were intecepted, transmitted to Washington, decoded and translated, and disseminated with utmost speed. Not infrequently , they were in the hands of the authorized recipients of Magic in our government as soon as they were in the hands of the Japanese overseas. Many of the civilian and military personnel engaged in the handling of the Magic worked long hours, far in excess of those prescribed, without additional compensation or special recognition. Now this is in italics: T*he success achieved in reading the Japanese diplomatic codes merits the hightest commendation, and all the witnesses familiar with Magic material throughout the war, have testified that it contributed enormously to the defeat of the eneey, greatly shortened the war, and saved many thousands of lives.*

In fact, one estimate—they went through three or four sheets of foolscap to show this —and it was General Chamberlain, who was then G2 out in the Pacific—that one dollar spent on COMINT during World War II was the same as a thousand dollars spent elsewhere.

Editor's Note:

It seems evident that LDC in many ways inherited the many talents of his father, who was a renown theologian, a gifted linguist, and an authority on Byzantine music. Coincidentally, his father was my mother's professor of music and theology in Athens.

So it seems only right that I, in turn, became LDC's student —not in theology or music, but in that landmark course in cryptanalysis, CA-400.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4036135

MT Report:

Fujitsu's "Atlas G-160" Machine Translation System: A Preliminary Evaluation

[redacted] P.L. 86-36

EO 1.4.(c)
P.L. 86-36

In 1986, [redacted] began evaluating commercially available Japanese-to-English machine translation (MT) systems developed and manufactured in Japan. After a three-year evaluation period, which focused on appraising the quality of raw translations produced by nearly every system on the market, [redacted] decided in July 1989 to purchase Fujitsu's Atlas G-160 system, a personal computer (PC)-based system just placed on the market that April. [redacted] initiated purchasing arrangements in July 1989, and took delivery of the system in late December 1989. [redacted] has been evaluating all aspects of the Atlas's role in producing translations from a range of original Japanese text. This report is a product of that evaluation.

In order to present a meaningful evaluation of the Atlas G-160 system, it is first necessary to briefly introduce the system's components and each component's role in the document processing-translating sequence. This information is presented in Sections I and II. Just as crucial to the output quality as the machine itself is the type and quality of documents inputted for processing.

Section III of this report outlines the kinds of documents [redacted] is translating or hopes to translate using the system. The actual evaluation of the system as a whole begins in Section IV. Based on the background offered in Section I through II, the system's strong points and weak points with regard to specific [redacted] applications are discussed and the overall system evaluated. Recommendations for use of the Atlas system at [redacted] as well as some general conclusions about current machine translation technology in general, follow in Section IV.

P.L. 86-36

While it specifically addresses the Atlas system and its use within the [redacted] environment, this report is being presented in the hope that it will help readers gain some insight into the machine translation process, enable them to measure current system capabilities against their own particular translation requirements, and ultimately place them in a better position to judge whether a machine translation system could be "right" for them.

I. The Role of Each Component in the Document Processing-Translation Sequence

The document processing-translation sequence using the Atlas system involves five basic steps:

- Japanese-Language inputting and creation of a corresponding Japanese-language file on the system (inputting can be done in any one of three ways-via keyboard, floppy disk, or OCR);
- pre-editing of the Japanese-language document in the newly-created file (optional);
- translating the file using one of two programs: "batch" or "interactive" translation;
- post-editing of the translated file (optional);
- outputting of the translated document as a printout in one of several formats: original Japanese text with side-by-side English translation, English translation only, etc.

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4036135

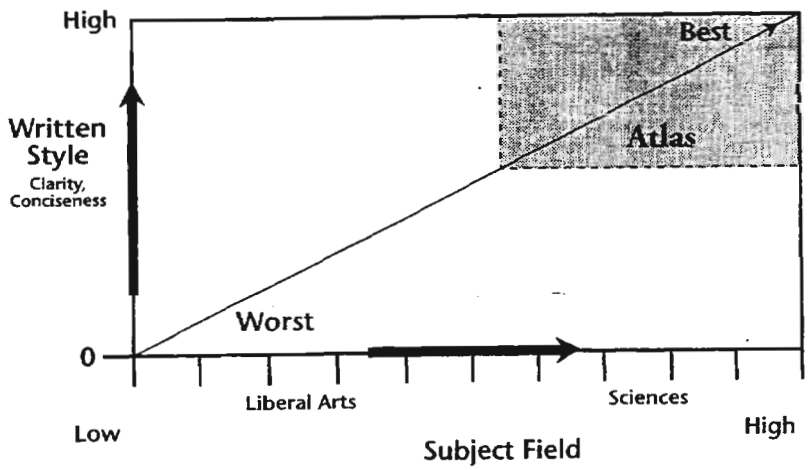


Figure 1. Document Types Atlas Most Effectively Translates

Document Inputting and Creation of Japanese-Language File

This step involves taking a Japanese language source document—either in printed form or on a floppy disk-and creating a new electronic version of that document in a Fujitsu "EPOWORD-G" file which subsequently can be processed by the Atlas program. This process can be done manually via the keyboard (basically, re-typing the original document into the computer), by transferring from floppy disk, or by use of the OCR.

• ***Manual Input:*** The Atlas incorporates a JIS key-board for the manual inputting (typing) of documents into the system. Conventional Japanese text consisting of kana (syllabary) and kanji (Chinese characters) is input as either Roman letters or kana. Additionally, keystrokes convert the letters or kana to the required kanji. The keyboard enables the input of 10,000 kanji (including the most common Chinese simplified kani), the English, Greek, Russian, French, Italian, Spanish, Portuguese, Danish, Scandinavian, and Norwegian alphabets, and hundreds of symbols used in mathematics, science and technology, and graphics compilation.

• ***Floppy Disk Input*** : The system incorporates an MS-DOS conversion function that enables input via floppy disk.

• ***OCR Input*** : This device, consisting of a scanning unit (which looks much like a desktop copier), a connection unit and related software, "reads in" hardcopy documents placed on the scanner, brings up a "bit image" of the document on-screen for the operator to selectively edit, and then produces a standard "EPOWORD-G" file containing the newly-created electronic document. The OCR can process typeset or word-processed Japanese text in a variety of fonts, pitch, and type sizes, although it cannot process text whose foreground or background contains color. It has a character recognition speed of about 20 characters a second and can process a page containing about 1,400 characters in roughly three minutes.

The OCR was designed to process Japanese text only, although Fujitsu is currently developing an English-text OCR. The device is simple to operate: the operator sets various processing parameters (vertical or horizontal text format, pitch, document name, etc.), pushes the START button, and feeds the document through the device. Each page's bit image is displayed on the monitor, allowing the operator to electronically adjust skew, erase spurious images, and select exactly how much of a page is to be processed. Each page is then processed by the OCR and compiled as a Japanese-language document. The operator then merges the pages to form a single document, and begins proof-reading prior to translation.

Pre-editing

Pre-editing, along with post-editing, is what separates a "raw" translation from a "polished"

~~FOR OFFICIAL USE ONLY~~

translation. It basically involves clarifying and simplifying complex grammatic structures into text more amenable to successful machine translation. Since the Atlas system provides "better" (i.e., more accurate and more understandable) translations from text characterized by relatively short, clear and concise sentences, pre-editing, even of the most basic kind, result in significantly improved end translations. On the Atlas system, the process includes, for example, artificially pluralizing nouns and pronouns, enclosing words and phrases in brackets to clarify governance and string boundaries, and replacing complex syntactic structures with simpler ones. Pre-editing can be carried out in two ways on the Atlas, manually or through a software program called "suiko" ("brush-up").

• ***Manual Pre-Editing***: This method, carried out either before or during the course of "interactive" translation (see "Translation Methods"), involves the operator simply going through the document manually and changing words and/or grammatical constructions which the translator perceives, based largely on previous experience, will represent a stumbling block for the Atlas translation program. Generally, the operator is concerned with only the most egregious errors, since minor changes can be made during post-editing.

• ***"Suiko" Pre-Editing***: This method employs a distinct program selected from the Atlas menu which is run against a document file; the program "flags" on-screen such items as incorrect kanji (not quite the same as a "spell check" function), the incorrect use of parentheses, overly long sentences, missing subjects, inappropriate kanji, and superfluous or ambiguous expressions. The operator then has the option of correcting the items "flagged" or ignoring them. Although extensive, the process is extremely time-consuming, especially if a multi-page text is being processed. In fact, [redacted]pperators do all pre-editing manually during "interactive" translation.

Translation Methods

The Atlas system carries out translation in two user selected modes: "batch" and "interactive."

• ***Batch Mode***: In this mode, the system attempts to translate an entire document file in a single operation. No operator intervention is involved. The only information displayed on the monitor screen during batch translation is the total number of sentences in the original text and the number of the particular sentence being translated.

• ***Interactive Mode***:: The interactive mode involves extensive operator involvement; the operator selects exactly which sentences in a text are to be translated, pre-edits, re-translates, adds or changes words in the Atlas dictionary system, or post-edits as necessary.

Atlas Dictionary System

The Atlas system incorporates an 80,000-word standard dictionary and a user's dictionary as standard onboard programs. In addition, specialized dictionaries in over a dozen scientific fields, such as physics and information processing (see Section 2.B above, representing the full set of specialized dictionaries offered by Fuijitsu as of late 1989) also are available options. The dictionary system allows the operator to adjust English-Japanese word equivalents in order to improve translation accuracy-changing words, adding new words, deleting words, or adjusting word priorities.

In the user's dictionary, there are two ways to register word priorities. The first method is the so-called "kan'i" ("simplified") method used for registering nouns only. When a Japanese noun encountered in a text has not been registered (correctly) in any of the three dictionaries (standard, user's, specialized), the operator extracts the noun, inputs it onto the "kanji" dictionary screen, types in the appropriate English translation, selects the appropriate noun class (object, personal noun phenomenon, organization, etc.), and selects the appropriate English plural form. The operator then goes back to the text and re-translates the sentence(s) containing the newly-registered noun. Registration of other parts of speech is a far more complex process, involving, for example, careful classification of a verb's semantic and syntactic functions in both English and Japanese.

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

Post-Editing Methods

The Atlas system allows for post-editing of the translated English language text either as an integral part of the interactive translation process (see above) or as a separate step once the English translation has been isolated in a separate English language text file. The software features a number of word-processing functions common to U.S. word processors, such as "move" and "copy" commands, but is still somewhat awkward to use.

Output Methods

The Atlas system can output translations in two forms—printout and floppy disk.

• ***Printouts***: Through the use of Atlas's "media conversion" program, processed documents can be printed out as original Japanese text only, original/pre-edited Japanese text only, original/pre-edited Japanese text with English translation (with or without Japanese-English vocabulary for those sentences the system cannot translate), or English translation only. This flexibility allows the operator to maintain a hardcopy of each stage of document processing/translating if desired.

• ***Floppy Disks***: Atlas output, i.e. English translations, can be output onto a floppy disk, but when transferred to English-language word processors, will contain only the English translation, and no part of the original Japanese source document.

II. Document Types For Translation On The Atlas

Documents processed thus far on [redacted] Atlas system are of two broadly-defined types: draft Japanese-language information reports produced by Japanese nationals [redacted] and, other Japanese-language documents ranging broadly from technical reports and newspaper articles to contracts and specification tables and charts. The differences in the two types of documents are important to consider, as they have a major impact on how the documents are processed on the Atlas system and what results are achieved (see SYSTEM EVALUATION).

[redacted] **Draft Information Reports**: These Japanese-language documents, produced in-house by [redacted] analysts, contain largely science and technology-related information extracted from original sources. After translation into English, these draft reports are edited and eventually published as final-form information reports. Most of these draft reports contain English-language glosses for the more complex specialized terms, and all reports submitted for machine translation are in the form of work-processor printouts. Because the reports are written by the [redacted] own analysts, the style in which the reports are written can be controlled to a certain extent. The draft reports are generally no longer than four or five pages.

Other Japanese-Language Documents: These documents, while in Japanese, come from various sources and generally do not contain English-language glosses for specialized vocabulary. Moreover, [redacted] has no control over the style in which these documents deal with communications and electronics and are at least ten pages long. All are submitted for translation in the form of xerographic copies or hardbound books.

P.L. 86-36

III. Sysytem Evaluations Capabilities vis-a-vis ASD Applications

Having briefly described the components of the Atlas system, the role each component plays in the MT process, and the types of documents meant to be processed on the system, a more meaningful evaluation of the Atlas's capabilities in processing [redacted] documents can not be offered. The central question for [redacted] of course, is this: Can the Atlas provide acceptable translations of the two broadly-defined types of [redacted] documents?

P.L. 86-36

The answer to this question is, essentially, this: since its operational introduction in February 1990, the Atlas system has shown itself to be generally NOT suited for producing POLISHED translations of [redacted] documents, particularly given the wide variety of topics and writing styles these documents encompass; rather, the Atlas is most efficient and effective in producing RAW

~~FOR OFFICIAL USE ONLY~~

DOCID: 4036135

1. ROSTERS OF PROPER NAMES (personal names, place names, company names, etc.)
   POOR without devoting a lot of time to dictionary registration; OUTSTANDING after completing dictionary registration
2. NEWSPAPER ARTICLES
   FAIRLY GOOD for articles on new products or technologies; TERRIBLE for articles on politics, economics (Atlas cannot handle journalistic Japanese w/out extensive pre-editing)
3. ABSTRACTS OF TECHNICAL PAPERS
   EXCELLENT; concise style, well defined terminology
4. TITLES OF S&T-RELATED BOOKS AND PAPERS
   OUTSTANDING; concise style, technical vocabulary probably already in technical dictionaries
5. CONTRACTS
   WORTHLESS; too many problems with long-winded "legalese" styles
6. USER'S MANUALS FOR EQUIPMENT
   EXCELLENT, unless the translation must contain both Japanese and English text (e.g. translation of Atlas User's manuals)
7. TABLES, CHARTS, MAPS
   GREAT translations, but cannot reformat back into original graphics the latest Atlas Ver.13 DOES have this capability, however)
8. "SHUKAN" MAGAZINE ARTICLES
   VERY POOR, generally; very colloquial style requires extensive pre-editing
9. UDC DRAFT INFORMATION REPORTS
   POOR TO VERY GOOD, depending upon style and subject of original document (see fig. 1)
10. NUMERICAL DATA (price lists, etc.)
    OUTSTANDING

Figure 2. Results of Testing Atlas' Ability to Raw Translate Various Types of Documents

P.L. 86-36

translations from documents written in a very concise style and dealing with as narrow a technical field as possible (see fig. 1). In other words, the Atlas system cannot provide acceptable translations of ALL types of [redacted] documents; instead, its strength lies in its ability to provide in a minimum amount of time a high volume of raw translations of certain kinds of documents (see fig. 2).

Underpinning this evaluation are the strengths and weaknesses of the Atlas system itself. There are many positive features to the system which streamline and simplify the processing-translation sequence. However, it is unfortunately the system's inherent technical weakness which place restraints on the Atlas's overall translation capabilities.

Atlas Strengths and Weaknesses: Their Impact on the NT Process

Among the system's strong points is its ability to input via both floppy disk and OCR (in addition to manual keyboard input). Also, its interactive translation mode and extensive dictionary systems add an important measure of flexibility and expendability to the MT work process. Overall, the Atlas menu system and operating environment are well-designed and user friendly, and the fact that the system is PC-based makes the system a very attractive alternative to larger, more expensive mainframe-based MT systems.

Its weak points, on the other hand, include technical limitations of the OCR in processing certain character styles and document types, the need to manually check all OCR output, the extreme difficulty of the pre-editing process, the fact that the translation program provides no translation whatsoever in cases where it finds the text too difficult, and the relative awkwardness of the system's English work-processing capabilities in the post-editing process.

Evaluating the system's strengths and weaknesses in the various steps of the MT process reveals the following specifics:

Input Process: More than 99 percent of the documents processed to date on the Atlas have been input via the OCR. The device has proven indispensable to the Atlas translation process, as it allows hardcopy documents to be "read into" the computer without having to type them in manually word-by-word. This, of course, saves time on the part of the operator and represents a major system strength. However, in many cases much of that time can again be lost when the operator goes to proof-read and correct the OCR inputted file. Depending upon document characteristics, the OCR device can reproduce text with an accuracy rate as high as about 95 percent (for original hardcopy that has good contrast and contains only Japanese text) and as low as 40

~~FOR OFFICIAL USE ONLY~~

percent (for third or fourth-generation xerographic copy with spurious or colored images, poor skew, English-language text, or mathematical formulas, etc.). Any inaccuracies must be corrected through manual proof-reading (Japanese work-processing systems do not have highly-developed spell-check capabilities), which in the case of many OCR mistakes - can be extremely time-consuming and tedious.

Specifically, the OCR has difficulty with text containing any of the following:

- non-Japanese script (including English)
- handwritten text
- text with color foreground/background
- poor xerographic copies
- complicated mathematical formulas (Greek symbols, etc.)
- underlined characters
- free-form "designer" characters
- characters smaller than 7-point in size
- "Layered" characters not clearly separated (see fig. 3)
- unusual characters outside the finite set included in the OCR software

Although this seems long, most normal word-processed or typed-set Japanese-language text conforms to standards within the range of the OCR's capabilities. One solution to the OCR "dilemma" (i.e., quick read-in time but possibly time-consuming proof-reading and correction process) is input via floppy disk. If the source document can be initially created (such as a [redacted] draft information report) or downloaded (such as an on-line data base file, etc.) as an electronic document, then it could be input into the Atlas system directly via floppy disk, bypassing the OCR and accompanying proof-reading entirely. Having both the OCR and floppy disk as input options provides much flexibility and is a definite strong point of the Atlas system.

P.L. 86-36

Pre-Editing Process: If the Atlas system has an "Achilles heel", then this step is it. The reason being that it is the difficulty of this particular step which makes completing a truly polished translation such a painful task. This process is the most complex of all system procedures. It requires near-native Japanese-language proficiency to be done properly, and requires a considerable amount of time to pre-edit any but the simplest of writing styles. Moreover, the "suiko" or "brush-up" program that comes with the Atlas and which is intended to help facilitate the difficult pre-editing task actually does little to reduce the amount of time required. For these reasons, [redacted] operators have found that attempting polished translations-and doing a complete job of pre-editing-is generally impractical, opting instead for a raw translation. A quite satisfactory raw translation can very often be produced relatively quickly for S&T-type documents, so long as the source text is clearly and concisely written and characterized by a clearly defined set of vocabulary, which is often the case with such documents. If subjected to some simple post-translation English-language "post-editing", moreover, such raw translations can sometimes approach the quality of fully pre-edited polished translations.

P.L. 86-36

Translation Process and Dictionary Systems: The "batch" translation mode, because it does not allow for human interaction for editing purposes and cannot be viewed by the operator, has been found by [redacted] operators to be almost useless. The interactive translation mode, on the other hand, has proven to be the better method by far and certainly represents one of the Atlas's strong points. This mode offers the operator tremendous flexibility. It gives him/her the freedom to decide how much or how little to pre-edit, the ability to make dictionary changes in the midst of the translation process, and the option of re-translating any particular sentence as many times as desired. An operator, for example, would generally have the system translate the first few sentences of an input text. Based on how well these sentences were translated, the operator would then register any new words in the user's dictionary, pre-edit as necessary, and re-translate the entire text interactively, repeating this procedure. This procedure generally leads to a translation that, while not a truly polished one, is substantially better than a raw one.

Post-Editing: The Atlas system, while it does possess some rudimentary English-language word-processing functions, generally lacks the

DOCID: 4036135

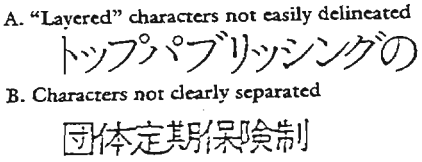


Figure 3. Example of Character Types Frequently Misread by the Atlas OCR

U.S. English-language word-processing programs. It has thus been found that using a Wang or IBM System for post-editing is far more efficient than using the Atlas.

Output Methods : The ability to furnish to post-editors and consumers hardcopy printouts containing the pre-edited Japanese text, the English translation, and English translations of individual words in sentences the Atlas was unable to fully translate represents a strength of the Atlas System. However, since files for transfer to English-language word-processing systems via floppy disk can contain only the English translation, the use of floppy disk output for anything but polished translations is prohibited.

IV. Conclusions and Recommendations

The Atlas G-160 system represents state-of-the-art machine translation technology, yet at the same time displays some of the fundamental technical limitations seemingly generic to all such systems today.

Simply stated, while the machine has been well engineered and slickly packaged, it is not able—nor does it claim to be able—to produce consistently coherent and accurate translations across broad or varied subject fields. Current algorithms and associated natural language processing techniques simply are not that far advanced. And while the use of extensive, time-consuming pre- and post-editing procedures can somewhat remedy this basic shortcoming, such procedures are almost always extremely inefficient. For these reasons, the Atlas MT system does not represent the "ultimate" answer to all [redacted] translation needs. Rather, it is a tool which—with the proper investment to time and effort—can yield definite benefits in improved productivity in specific documents fields.

For example, a 20-page typewritten document dealing with telecommunications and written by specialists in a very "plain" style can be input via the OCR, proofread, translated in raw form, and output as an Atlas printout in anywhere between 4 hours (very few OCR mistakes) and 10 hours (many OCR errors). This raw translation can be given directly to a consumer for determining whether further translation is necessary. If no further action is required by a translator, hundreds of dollars have been saved by not having to work for two to three weeks to produce a polished translation that is not needed by the consumer. If a polished translation IS required, substantial amounts of time and money are still saved. [redacted] operators have found that on average, and Atlas raw translation of the same type of document followed by off-system post-editing by a translator results in producing 10 pages in the time it takes to translate seven pages by conventional methods only.

On the other hand, [redacted] operators have found that a polished translation of even five or six pages of a handwritten document not related to an S&T field and written in a too-elevated, too colloquial, or too illogical style invariably takes anywhere between four and five times longer on the Atlas system than by conventional translation methods. Use of the Atlas for translating this type of document is simply not worth the trouble.

The important thing, therefore, is to use the MT system where it is most effective, where it can assist by speeding up the translation process instead of slowing down that process. For [redacted] that means using the Atlas for documents which are concise and well written from the standpoint of style and vocabulary, which is most often the

~~FOR OFFICIAL USE ONLY~~ P.L. 86-36

DOCID: 4036135

case for documents in S&T-related fields. Moreover, it means concentrating—for the most part—on producing a high volume of raw translations for subsequent screening by consumers. Encouraging the use of input via floppy disk—[redacted] draft information reports, for example—would also contribute to increased productivity by eliminating the need to manually check for OCR errors. In sum, if used in a way so as to exploit its strengths instead of its weaknesses, the Atlas MT system can be a valuable tool in increasing translation productivity; yet, it is no "dream machine" and should never be purchased or used as an excuse for not hiring, training, and retaining the very best translator work force possible.

P.L. 86-36

V. System Components

Hardware

Fujitsu G160 oc with a single 5.25" floppy disk drive
Expansion memory to 8 megabytes
135-megabyte hard disk drive
JIS keyboard
Color display
Mouse
Kanji printer
Optical character reader
OCR connection unit

Software

Atlas-G set
30-dot character group
MS-DOS data connector
Image processing option
OCR control option
Dictionary (biology & medicine)
Dictionary (industrial chemistry)
Dictionary (meteorology, seismology, astronomy)
Dictionary (mechanical engineering)
Dictionary (civil engineering & construction)
Dictionary (physics & atomic energy)
Dictionary (transportation)
Dictionary (electricity & electronics)
Dictionary (mathematics & information)
Dictionary (plants & factories)
Dictionary (automobiles)
Dictionary (biochemistry)
Dictionary (information processing)

Cost

Cost of Hardware:	¥5,974,700
Cost of Software:	¥3,614,950
Total Cost:	¥9,589,650

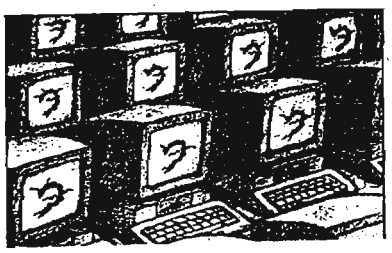
We welcome reviews and reports of hardware, software, training materials, books, technical literature, and conferences.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4036135

NSA and Computer Viruses

Richard Sylvester, B Group



(U) There has been considerable discussion in the Agency about computer viruses and the possibility that NSA's computers and computer networks have been invaded. In discussing the viruses, writers must be aware of the classifications that apply to the discussions.

(U) As most of us know, a computer virus is a software program designed specifically to reproduce itself and to modify or destroy computer software, damage or destroy equipment, or compromise sensitive data. Some of us, however, are unaware that **any** personal computer network or office automation system is susceptible to invasions by a virus, infecting any host in which the program is used. Owing to the insidious nature of a virus, any unwitting user can become an unwitting propagator.

(U) We have established classification guidelines to discuss viruses that may be summarized as follows:

- (U) the fact that NSA is aware of computer viruses and that we take steps to minimize the risk of introducing viruses into our automated information systems (AIS) or networks is UNCLASSIFIED.

- (U) the fact that we employ commercially produced software to scan for virus infections also is UNCLASSIFIED.

- ~~(FOUO)~~ an admission of vulnerability, i.e., the acknowledgment that NSA has experienced the intrusion of a computer virus in any of its systems is classified, at a minimum, CONFIDENTIAL.

- ~~(FOUO)~~ The disclosure of the extent of infection or the name of the specific virus that may have been discovered in an NSA AIS or network is classified, at a minimum, SECRET.

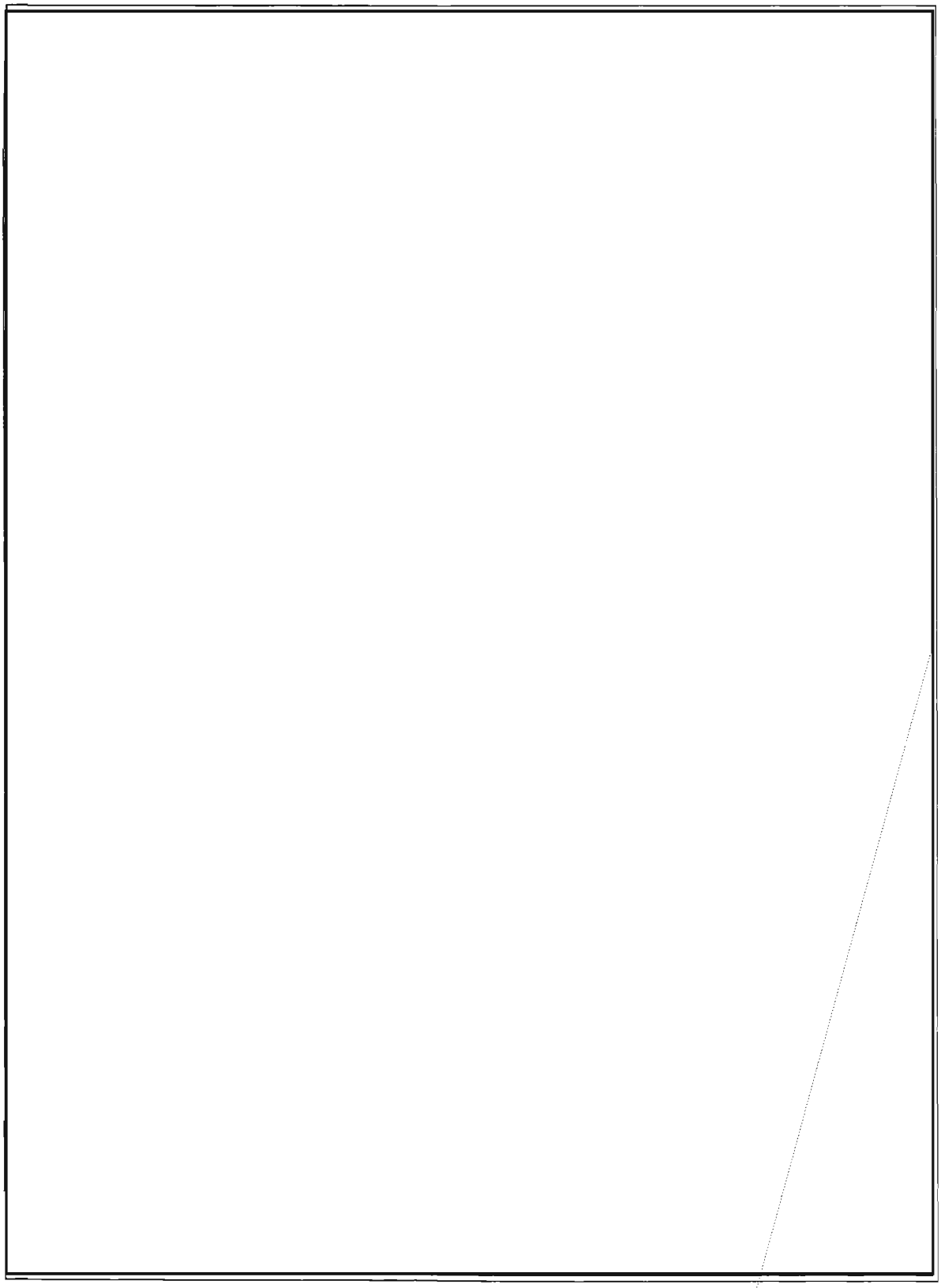
- ~~(FOUO)~~ Specifics concerning an infection, such as the severity of the infection, the extent of damage done, the complexity and expense of eradicating the disease, or the impact of the virus on operations is classified TOP SECRET; in some instances, if certain details concerning the AIS, the network, or the database in which the virus was discovered are revealed, any of the above revelations may require handling in COMINT channels (HVCCO) or even in codeword channels.

~~(FOUO)~~ In summary, be careful what you say and to whom you say about NSA and computer viruses. For further information concerning the classification matters pertaining to computer viruses, contact your classification advisory officer (CAO), your local Computer Security Officer or Computer Security Manager, or J06, the TCOM office of Operational Computer Security.

~~FOR OFFICIAL USE ONLY~~

From the Past

The Department of Defense is commemorating the 50th Anniversary of World War II in 1991-1995. Unlike the immediate post-WW I period when cryptology went underground, the organizations involved during World War II remained on the post-war scene. Even in the darkest hours of the war it had become evident that one of our one-time allies was already an adversary. To a great extent this cryptologic agency owes its continuance to the Cold War that had its origins in the bitter war years.



EO 1.4.(c)
P.L. 86-36

DOCID: 4036135

Letter

To the Editor:

When General Matthew Ridgeway retired as Army Chief of Staff—this was the man who had entered Nazi Germany as commander of the First Airborne Division, who relieved General Douglas MacArthur as Supreme Allied Commander in Korea, who stopped the Chinese advance while in command of the Eighth Army—he was asked what he considered to be most important accomplishment of his career. His response was simple: "I protected the mavericks." General Ridgeway's answer may seem surprising, but it reflects a profound understanding of both the realities of organizations and the requirements for their success.

In theory, "protecting the mavericks" is easy: "mavericks" are the people whose new ideas and approaches make their organizations uncomfortable today but that will be invaluable in solving the problems of tomorrow. We all know the TQM "school solution"—new ideas are "good" and people who have them must be encouraged, rewarded and protected. What could be plainer, and why was General Ridgeway proud of such a simple thing?

Of course, the real problem is much harder. Good ideas are like gold: they are rarely unalloyed, they are often found in unattractive surroundings, and they sometimes require lots of work to refine and forge a final product. Mavericks are the prospectors who find them.

But sometimes it's easier for a leader to decide that the sparkle of a new discovery is iron pyrite—"fool's gold"—and tell the prospector to leave it in the ground. Unfortunately, when that happens too often, the loss can extend far beyond one idea. Like prospectors whose claims never pan out, some mavericks just give up and stop having new ideas. Still others keep having them, but for new employers after they resign or are penalized for sins like "unpredictable creativity"—against which at least one military officer has been strongly counseled.

The truth is that mavericks make us feel uncomfortable; they "question authority," they "rock the boat," and they "don't understand how we do business."

But these three phrases are often the best descriptions of really new ideas. For example, Kodak applied them in 1948 when they turned down an inventor named Charles F. Carlson when he proposed a new copying process. Carlson's idea was to use high-voltage electrostatic charge to attach fine black powder to plain paper, then to heat the paper and melt the powder into its fibers. Kodak turned Carlson down flat; the process was too complex, the machines were too expensive, and, anyway, the whole thing was unnecessary—everyone at Kodak knew that if you want a picture on paper, the best way was to start with a picture on Kodak film.

Kodak was wrong. Carlson took the ideas that Kodak turned down and sold them to an unknown company named Haloid Corporation. Today Haloid's name is Xerox.

There are two important lessons here, but they're not simple ones, like "don't turn down another Xerox" or "don't make `bad' decisions." There won't be another Xerox—the next revolution will start with another idea—and at the time the decision to turn it down wasn't a "bad" decision, it was a "good" decision made in the wrong context.

Carlson's process *was* expensive, it *was* complex (the "copier repairman" is still a standard figure in

~~FOR OFFICIAL USE ONLY~~

business cartoons), and it *would* have been in direct competition to Kodak's traditional business—and there was a good chance it wouldn't work outside the lab. In the everyday context of a Kodak operating manager, *investing*—not declining—would have been the "bad" decision. After all, the project involved high-cost, substantial risk, and the best foreseeable outcome would be launched another competitor for Kodak's existing positions in the markets for film and photographic supplies. The "real" measure of the right decision—Xerox's subsequent commercial success—wasn't available until years later.

So what are the two lessons? I think they are these:

1. Always look for the *largest reasonable context* in which to evaluate a decision, and,
2. Have the courage to *risk* some "bad" decisions.

In the Kodak-Xerox case, making the decision in the largest context would have begun with recognizing that Kodak's real business was "putting pictures on paper," not "selling film and photographic supplies." Seen this way, Carlson's invention of plain-paper copier that could be used by people with no special training right in their offices fits right in as a logical extension of (and not a competitor to) Kodak's existing business.

Of course, neither of these lessons is as easy to apply without the benefit of hindsight; as the saying goes, "When you're up to your ass in alligators, it's difficult to see that your objective was to drain the swamp." It's even more difficult to see something like "economic enhancement through the provision of retail jobs in a suburban shopping facility in a soon-to-be-drained swamp" as the "largest reasonable context." With alligators alongside, it may seem like the *only* "reasonable" context for any decision is "keeping all my body parts" or just "not becoming someone's lunch." At times like these, we need reminders, like the slaves who accompanied victorious Roman generals in their triumphal parades, reminding them of their mortality. But our reminders should be to "consider the largest context" and "have the courage to take risks."

And that's exactly why we need mavericks. They are the people who ask questions in the "largest context" and suggest the new solutions for difficult problems—questions like "Why *are* we draining the swamp?" and solutions like "First thing, let's tame all the alligators." Their ideas may be annoying, frustrating, embarrassing, and even threatening (perhaps we picked the swamp ourselves!), but they may also lead us out of the muck and up to drier ground. Perhaps Robert Kennedy thought of himself as a maverick when he wrote:

> Some people look at things as they are and ask "Why?"
> I think of things as they could be and ask "Why not?"

Don't think of your mavericks as "trouble-makers" or "boat-rockers," think of them as "principal staff for thinking of things 'as they ought to be' "—and, if they do tame the alligators, how easy it will be to drain the swamp.

Anonymous

Bulletin Board

~~(FOUO)~~ L143 has a degausser for large objects like disk drives. It can handle objects 8" x 18" x 22". The degausser is located in SAB-3. It has been approved by T03, now J06.

~~(FOUO)~~ In the past we discarded defective disk drives. This will allow us recoup our investment. For example, SUN disk drives cost about $16,000 each.

~~(FOUO)~~ To degauss your drive, write a memo to J06, with specifics about the drive.

DOCID: 4036135

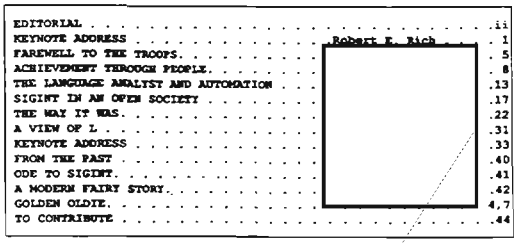
Editorial

ABOUT THE DISTRIBUTION OF CRYPTOLOG

We regret to inform subscribers that we lost our ability to distribute individual copies beginning with 3rd Issue 1991. We're looking for an alternative. For the time being we ask you to be patient. And as there are many ongoing changes in organizational designators and people are moving about, it will take quite a while until everything is on even keel again. So please be patient. Meanwhile, if you have missed copies, you can ask for them, using the form shown below, or write a note to CRYPTOLOG Distribution, P0541, Ops-1. **As there are over 3,000 subscribers, it stands to reason that you should not call about your subscription or distribution.**

For your convenience, the contents of the issues published beginning with 3rd Issue 1991 are shown below. **NO TELEPHONE REQUESTS FOR BACK COPIES WILL BE HONORED.**

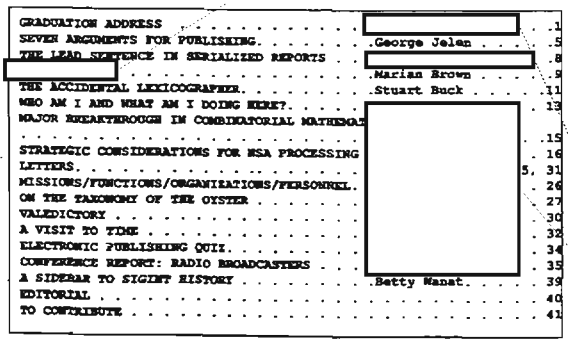
3rd Issue 1991



EDITORIAL ii
KEYNOTE ADDRESS . . . . . Robert E. Rich . . . 1
FAREWELL TO THE TROOPS 5
ACHIEVEMENT THROUGH PEOPLE 8
THE LANGUAGE ANALYST AND AUTOMATION 13
SIGINT IN AN OPEN SOCIETY 17
THE WAY IT WAS 22
A VIEW OF L 31
KEYNOTE ADDRESS 33
FROM THE PAST 40
ODE TO SIGINT 41
A MODERN FAIRY STORY 42
GOLDEN OLDIE 4,7
TO CONTRIBUTE 44

2nd Issue 1992

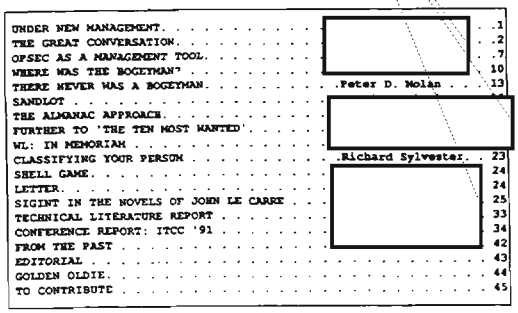
EO 1.4.(c)
P.L. 86-36



GRADUATION ADDRESS 1
SEVEN ARGUMENTS FOR PUBLISHING . . . . . George Jelen 5
THE LEAD SENTENCE IN SERIALIZED REPORTS 8
. . . . . Marian Brown 9
THE ACCIDENTAL LEXICOGRAPHER . . . . . Stuart Buck 11
WHO AM I AND WHAT AM I DOING HERE? 13
MAJOR BREAKTHROUGH IN COMBINATORIAL MATHEMAT 15
STRATEGIC CONSIDERATIONS FOR NSA PROCESSING 16
LETTERS 5, 31
MISSIONS/FUNCTIONS/ORGANIZATIONS/PERSONNEL 26
ON THE TAXONOMY OF THE OYSTER 27
VALEDICTORY 30
A VISIT TO TIME 32
ELECTRONIC PUBLISHING QUIZ 34
CONFERENCE REPORT: RADIO BROADCASTERS 35
A SIDEBAR TO *SIGINT HISTORY* . . . . . Betty Wanat 39
EDITORIAL 40
TO CONTRIBUTE 41

P.L. 86-36

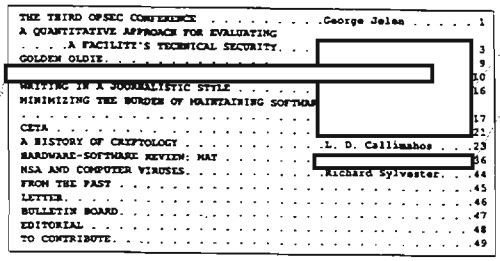
1st Issue 1992



UNDER NEW MANAGEMENT 1
THE GREAT CONVERSATION 2
OPSEC AS A MANAGEMENT TOOL 7
WHERE WAS THE BOGEYMAN? 10
THERE NEVER WAS A BOGEYMAN . . . . . Peter D. Nolan . . . 13
SANDLOT 16
THE ALMANAC APPROACH 17
FURTHER TO 'THE TEN MOST WANTED' 20
WL: IN MEMORIAM 21
CLASSIFYING YOUR PERSON . . . . . Richard Sylvester. . 23
SHELL GAME 24
LETTER 24
SIGINT IN THE NOVELS OF JOHN LE CARRE 25
TECHNICAL LITERATURE REPORT 33
CONFERENCE REPORT: ITCC '91 34
FROM THE PAST 42
EDITORIAL 43
GOLDEN OLDIE 44
TO CONTRIBUTE 45

3rd Issue 1992

P.L. 86-36



THE THIRD OPSEC CONFERENCE . . . . . George Jelen 1
A QUANTITATIVE APPROACH FOR EVALUATING 3
. . . . A FACILITY'S TECHNICAL SECURITY 9
GOLDEN OLDIE 10
WRITING IN A JOURNALISTIC STYLE 16
MINIMIZING THE BURDEN OF MAINTAINING SOFTWA 17
CETA 21
A HISTORY OF CRYPTOLOGY . . . . . L. D. Callimahos . . . 23
HARDWARE-SOFTWARE REVIEW: NAV 36
NSA AND COMPUTER VIRUSES . . . . . Richard Sylvester. . . 44
FROM THE PAST 45
LETTER 46
BULLETIN BOARD 47
EDITORIAL 48
TO CONTRIBUTE 49

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

PLEASE SEND ME THE ISSUES MARKED BELOW

3RD 1991———

1ST 1992———

2ND 1992———

3RD1992———

NAME———————————

ORG———————————

BLDG———————————

MAIL TO: CRYPTOLOG DISTRIBUTION, PO541, Ops-1

~~FOR OFFICIAL USE ONLY~~

DOCID: 4036135

Editorial Policy

CRYPTOLOG is a forum for the informal exchange of information by the analytic workforce. Criteria for publication are: that in the opinion of the reviewers, readers will find the article useful or interesting; that the facts are accurate; that the terminology is correct and appropriate to the discipline. Articles may be classified up to and including TSC.

Technical articles are preferred over non-technical; classified over unclassified; shorter articles over longer. Comments and letters are solicited. We invite readers to contribute conference reports and reviews of books, articles, software and hardware that pertain to our mission or to any of our disciplines. Humor is welcome, too.

Please note that while submissions may be published anonymously, the identity of the author must be made known to the Editor. Unsigned letters and articles are discarded.

N.B. We regret that we must now do cost accounting. For every original submission—not written for another purpose— please indicate how much time you spent writing your article or letter, and what your hourly rate is.

If you are a new author, please request "Guidelines for CRYPTOLOG Authors."

How to Submit your Article

Back in the days when CRYPTOLOG was prepared on the then state-of-the-art, a Selectric typewriter, an article might be dashed off on the back of a used lunch bag. But now we're into automation. We appreciate it when authors are, too.

N.B. If the following instructions are a mystery to you, please call upon your local ADP support for enlightenment. As each organization has its own policies and as there's a myriad of terminals out there, CRYPTOLOG regrets that it cannot advise you.

Send two legible hard copies accompanied by a floppy, disk, or cartridge as described below, or use electronic mail. In your electronic medium (floppy, disk, cartridge, or electronic mail) please heed these strictures to avoid extra data prep that will delay publication:

- do not type your article in capital letters
- do not right-justify
- do not double space between lines
- but **do** double space between paragraphs
- do not indent for a new paragraph
- but **do** paragraph classify
- do not format an HD floppy as DD or vice-versa–our equipment can't cope
- label your floppy or cartridge: identify hardware, density of medium, software;
- put your name, organization, building and phone number on the floppy or cartridge

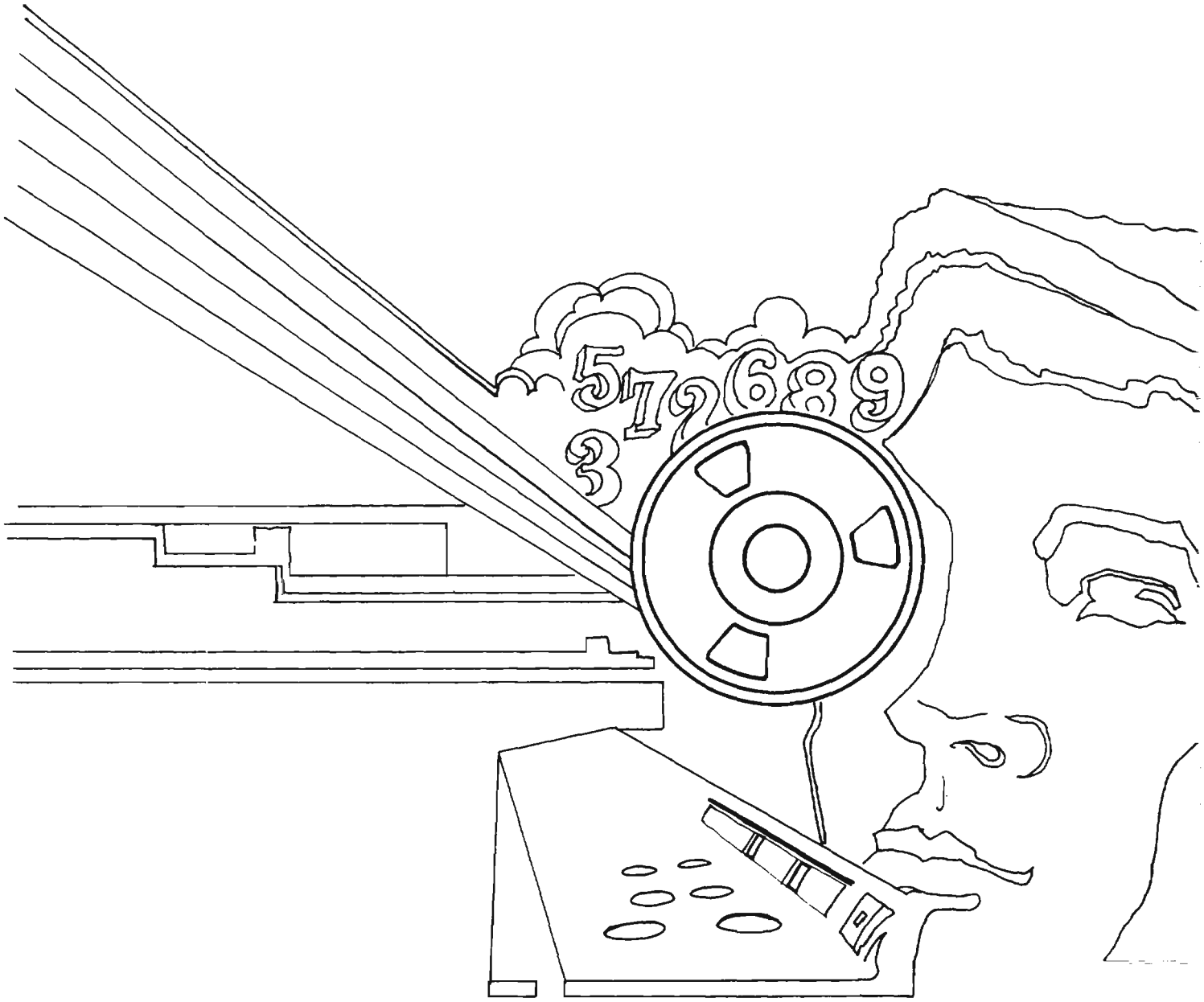
The electronic mail address is [redacted] (pass to CRYPTOLOG)
or [redacted] (pass to CRYPTOLOG)

P.L. 86-36

CRYPTOLOG publishes using Macintosh and Xerox Star. It can read output from the equipment shown below. If you have something else, check with the Editor, as new conversions are being added.

SUN	60 or 150 MB cartridge	ascii only
XEROX VP 2.0, 2.1	5 1/4" floppy only	
WANG		Stand-alone or Alliance
Macintosh	3 1/2" DD disk only	Please furnish a copy in TEXT as well as in your software, as we may not have all the software upgrades
IBM & Compatibles	3 1/2" DD or HD 5 1/2" DD or HD	Please furnish a copy in ascii as well as in your software, as we may not have all the software upgrades

~~FOR OFFICIAL USE ONLY~~


5 7 2 6 8 9
3

DOCID: 4011853

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

2nd Issue 1992

GRADUATION ADDRESS . . . . . [redacted] . . . 1
SEVEN ARGUMENTS FOR PUBLISHING. . . . . George Jelen . . . 5
THE LEAD SENTENCE IN SERIALIZED REPORTS . . [redacted] . . . 8
[redacted] . . . . . Marian Brown . . . 9
THE ACCIDENTAL LEXICOGRAPHER. . . . . Stuart Buck . . . 11
WHO AM I AND WHAT AM I DOING HERE?. . . . [redacted] . . . 13
MAJOR BREAKTHROUGH IN COMBINATORIAL MATHEMATICS
. . . . . [redacted] . . . 15
STRATEGIC CONSIDERATIONS FOR NSA PROCESSING [redacted] . . . 16
LETTERS. 25, 31
MISSIONS/FUNCTIONS/ORGANIZATIONS/PERSONNEL. [redacted] . . . 26
ON THE TAXONOMY OF THE OYSTER . . . . . [redacted] . . . 27
VALEDICTORY . . . . . [redacted] . . . 30
A VISIT TO TIME . . . . . [redacted] . . . 32
ELECTRONIC PUBLISHING QUIZ. 34
CONFERENCE REPORT: RADIO BROADCASTERS . . . [redacted] . . . 35
A SIDEBAR TO SIGINT HISTORY . . . . . Betty Wanat. 39
EDITORIAL 40
TO CONTRIBUTE 41

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~CLASSIFIED BY NSA/CSSM 123-2~~

Declassified and Approved for Release by NSA on 10-10-2012 pursuant to E.O. 13526, MDR Case # 54778

~~NOT RELEASABLE TO CONTRACTORS~~

DOCID: 4011853

CRYPTOLOG

Published by P05, Operations Directorate Intelligence Staff

VOL. XIX, No. 2 . . . . . 2nd Issue 1992

PUBLISHER . . . . . [redacted]

BOARD OF EDITORS

EDITOR . . . . . [redacted] (963-7595)

Collection . . . . . Marian Brown (963-1197)
Computer Systems . . . . . [redacted] (963-5877)
Cryptanalysis . . . . . [redacted] (963-1461)
Cryptolinguistics . . . . . [redacted] (963-4382)
Information Resources . . . . . [redacted] (963-3258)
Information Science . . . . . [redacted] (963-3456)
Information Security . . . . . [redacted] (968-8013)
Intelligence Community . . . . . [redacted] (963-5800)
Intelligence Reporting . . . . . [redacted] (963-5068)
Language . . . . . [redacted] (963-3057)
Linguistics . . . . . [redacted] (963-4814)
Mathematics . . . . . [redacted] (963-3709)
Puzzles . . . . . [redacted] (963-1461)
Research and Engineering . . . . . [redacted] (961-8362)
Science and Technology . . . . . [redacted] (963-4958)
Special Research . . . . . Vera R. Filby (968-6558)
Traffic Analysis . . . . . [redacted] (963-3369)

Classification Officer . . . . . [redacted] (963-5463)
Bardolph Support . . . . . [redacted] (963-3369)
Clover Support . . . . . [redacted] (963-7060)
Macintosh Support . . . . . [redacted] (961-8362)
Xerox Support . . . . . [redacted] (963-6867)
Illustrators . . . . . [redacted] (963-3360)
. . . . . [redacted] (963-4382)

P.L. 86-36

To submit articles and letters, please see last page

For New Subscription or Change of Address or Name

MAIL name and old and new organizations and building to:

Distribution, CRYPTOLOG, P0541, OPS-1
or
via PLATFORM: cryptlg @ curator *inoperative at*
via CLOVER: cryptlg @ bloomfield *present*

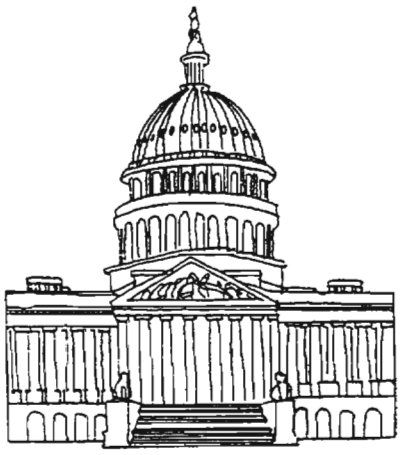
Please DO NOT PHONE about your subscription or matters pertaining to distribution

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011853



Address to the graduating class of CY-500, 21 May 1992 by the Honorable Helen Delich Bentley (R), Representative, Second District, Maryland

Good morning ladies and gentlemen and distinguished guests.

It is a pleasure to be asked to address you at a time like this in your lives, a time of satisfaction, a time of looking forward: graduation means not only an ending, but a beginning.

I do enjoy such an occasion, because in my own life, in my own experience, there have been so many endings to quite a few careers: reporter, editor, columnist, television producer and journalist, Agency chief, international trade consultant—all of the leave takings leading, eventually, to Congress.

It has been a demanding path, but rewarding and exciting.

And in Congress, at this particular time, I have to focus on the rewards of serving one's country in difficult times. The Congress, as a body, is struggling against a public perception of privilege and corruption and ineptitude.

To one identified with the Hill, it makes no difference that I bounced no checks (I didn't even have an account at the House bank), that I won a primary in March handily—with a fairly heavy turnout—that most of my mail is favorable, etc., does not affect the overall atmosphere. It is a very sad time for the establishment, and a very bad time for the country.

There is never a good time for both the Executive Branch and the Congress to be under siege from the press and the public, but in the political dynamic where timing is critical, conditions of the world demanding strong responses, strong support from the "leader of the free world", make a weakened Congress and a beleaguered President and the nation particularly vulnerable.

We face a $4 trillion debt ceiling this year, interest costs in excess of $1 billion per day, 12 to 14 million unemployed or underemployed, and a debilitated infrastructure: bridges, sewers, roads.

And a Europe in flux from the Volga through the Balkan Peninsula into the European Community: turning on itself, breaking off on all manner of trade agreements, threatening GATT, announcing the end of NATO with the establishment of a Franco-German corps.

The dissolution of the balance of power—some would call it a balance of terror—between the two super powers was anticipated, was discussed and written about, but there is no evidence from the behavior of this government ***that we were any more prepared to deal with it than were the Russians themselves***.

No aid package was in place that addressed the particular and peculiar needs of a fragmented USSR. The answer to the food shortages of the winter were massive shipment of grain, tried and

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011853

true business for the last twenty years for our commodities dealers—***when there was a stable government infrastructure in place to handle the movement and disbursement of commodities*** .

I led a drive in the Congress, with 119 congressional supporters, to have at least a part of the shipments be shelf-ready canned goods.

We, also, should have been ready to barter aid for influence in the decisions made on the sale of nuclear weapons. I should have considered: food or money in exchange for keeping weapons out of the hands of extremist groups.

Hard ball? You bet! Business as usual will not work when there is not one strong government to deal with, but a group of floundering governments driven by the need to survive.

This is true, also, on the Balkan Peninsula. It is not a situation that responds to the old diplomacy. The EC and the United Nations should be considering plebiscites called by constituencies ***which occupied territories in place prior to 1941***. Every effort must be made to reconstitute the nation of Yugoslavia prior to Tito's terrible policy of redistribution of minorities across ethnic territories.

Without proper planning, a reactive response frequently makes us a victim—as much as any of the participants—because without preparation, our responses are either inflammatory or inept. But once the house is really on fire—guess who is supposed to field a half million men and weaponry to put it out?

Iraq-Kuwait is a wonderful example of what we can do when the situation gets of of hand—however, along with such success goes a huge bill. But I hear little discussion about the U.S. policy prior to that time vis-a-vis Iraq and Kuwait. Had we been wiser, had we handled Iraq better, would we have had to be there in the first place?

Certainly the Panamanian action revisited tends to convince one that we were not well briefed on the local political scene, or if we were, we did not have a plan in place to respond to a popular uprising. Had we supported the domestic insurgency in the fall of the year, we would not have had to land our troops there in December.

Appropriate intelligence is of no value if it is not properly used. The horror of a modern war, comparable to the scale of WW II, is beyond the ability of the average American to imagine, and the costs beyond the ability of any nation to pay. We must short-circuit any of these threats by using intelligence—our brains—to counter modern force.

If it is true, as some believe, that the cost of ever-escalating weapons developments forced Russia into glasnost, it pushed us into bankruptcy.

Dr. Martin Van Crevald's book, *Transformation of War*, presents a strong case for the disappearance of "great wars" and the emergence of a series of low-intensity conflicts. Call them insurgencies or counter-insurgencies, label them riots in Los Angeles or revolts in Bangkok, civil wars in Yugoslavia—locale specific or country-contained, driven by local issue, no monolithic ideologies fueling the madness, the United States is placed in a leadership role, which demands policies based on regional histories, anthropology and sociology, and an acceptance of standards for the countries involved that are sometimes alien to the West.

It is long past the time that we can go into the world as soldier-preachers and receive any kind of welcome. If we would spread our values, it will be by example ***only.***

In order to do this well, timely information—all kinds of intelligence—about these countries will be of the greatest value. If Dr. Crevald's premise about the changing nature of warfare comes close to what is actually occurring, then the nature and focus of the intelligence community will have to change also.

The question becomes, then, who will initiate the changes? The National Security Act of 1992 (HR 4165) seemingly has received little support, inside or outside of the government. In a series of hearings held over this winter, the majority of the testimony from experts—former Agency officials and academia—seems to suggest that the legisla-

tion goes too far and may be seen as Congress trying to micro manage too much.

CIA chief Robert Gates testified, in answer to the proposed bill, on changes already under way in the structure of the Agency and in the efforts—across all intelligence-gathering departments of all agencies—to better integrate information and to share analytical findings.

It should be of special interest to you in NSA that when Director Gates was explaining some of the proposed changes in the area of strengthening the management direction and coordination of intelligence collection, he stated, "in making the structural changes that I am about to describe, I have used as a model some aspects of the National Security Agency, where one individual not only is able to task all of the signals intelligence collectors available to the DoD and the Intelligence Community, but also has the responsibility for establishing standards, ensuring interoperability and budgeting and strategic planning in this area."

He qualifies that position slightly by pointing out that "the collection disciplines are sufficiently different in that they all cannot, and perhaps should not, exactly be modeled on NSA. Indeed, none can." He continues by commending the basic idea of having one individual ultimately responsible for each discipline, with a specific responsibility for the coordination and management of requirements for that discipline, including oversight responsibility for standards and strategic planning.

Now, my mother always told me that imitation is the sincerest form of flattery. More than that, it tells me that the "NSA model" has proved itself over time, and that is worth much more than flattery.

Mr Gates' testimony on April 1st reported changes in focus in intelligence as early as 1980 when only 58% of the Community's resources were dedicated against the Soviet Union. By 1990 the figure had dropped to 50%. I am sure you are aware of this, but most of the Congress and certainly, most of the American people are not.

But of greater importance, to me and to the business community in this country, is the report from testimony by Mr. Gates on April 29th before the Judiciary Committee outlining some new thrusts for the remaining 50% of resources: tasking against foreign economic espionage.

Remember, the ultimate purpose of warfare is to seize the wealth of another country, to be able to use its resources, both human and material, for the enhancement of the aggressors' own nation. A successful leader achieves this at the least possible cost to his own people with the least damage to the territory taken.

Modern warfare cannot satisfy these demands any more. It is too destructive. It is too costly. Outside of the internecine wars, the popular uprisings, major nations in the 21st century will wage war with dollars instead of missiles.

I am heartened that Director Gates addressed the economic threat at such length. However, I am gravely concerned that neither the Congress nor the Administration has addressed changes in the legislation which recognizes this threat.

One particular area of concern to me: dual-use technology. There is a pattern, over my time in the Congress, of technology being bartered offshore: for foreign policy concerns, by the State Department; for economic concerns, the sale of T Bills and foreign investment, by the Treasury Department; for the profits of U. S. businesses, by the Commerce Department.

The only Agency with any concern for the long-term strategic position of the United States—DoD—frequently is outvoted by the big three. The actions of CIFIUS, a major case in point ***where not one sale of companies owning valuable state-of-the-art technology has been stopped*** by the Committee ***even when semi-conductor technology was involved.***

We are in a global economy, one into which it seems we slipped and slid, tumbled and fell ***without any preparation to protect the wealth of this great nation represented not only by its dollars and raw resources, but by its markets and its intellectual properties.***

Small U. S. companies are encouraged to go joint-venturing with foreign corporate giants, never understanding until much too late that a contract drafted under U. S. law is binding only so long as the small company has resources to stay in court for months, sometimes years enforcing the terms.

The IRS is running into the same court confrontations with these corporations that our small companies have faced. And, if you think that Uncle Sam has the deepest pockets and will win, consider this: currently there are 45,000 cases under dispute. Even the government doesn't have pockets that deep, and even though estimated underpayments run as high as $100 billion.

If I am frustrated that the great informational resources of this country are not being used to plan and prepare our policy makers well, how much more frustrated analysts must be. We work with statistics in our office, as broken out and basic as we can get.

Ladies and gentlemen, they are dreadful on the economy of the U. S.

They are frightening on the health of our people, both physical and mental. Recall when the intelligence community, using Russian data—I think it was in the '70's—came up with mass alcoholism as a major problem in Russia? The Russians promptly stopped printing the information.

Overlay those models on the U.S. Someone has been waging a very successful war against this country—devil, man, or nation, or a concordance of the three. We are in trouble, and as the President has said, you are the first line of defense.

Get the best information possible. Disseminate it throughout the government. Treat it honorably. We cannot heal ourselves if we do not know what is wrong—not only in the world, but inside our own system. Be courageous of the truth—there is no other way to secure freedom!

As Americans, we are the descendants of the toughest survivors of every nation on the face of the earth. We will endure.

I wish you well. God bless.

SUBSCRIPTION TO CRYPTOLOG

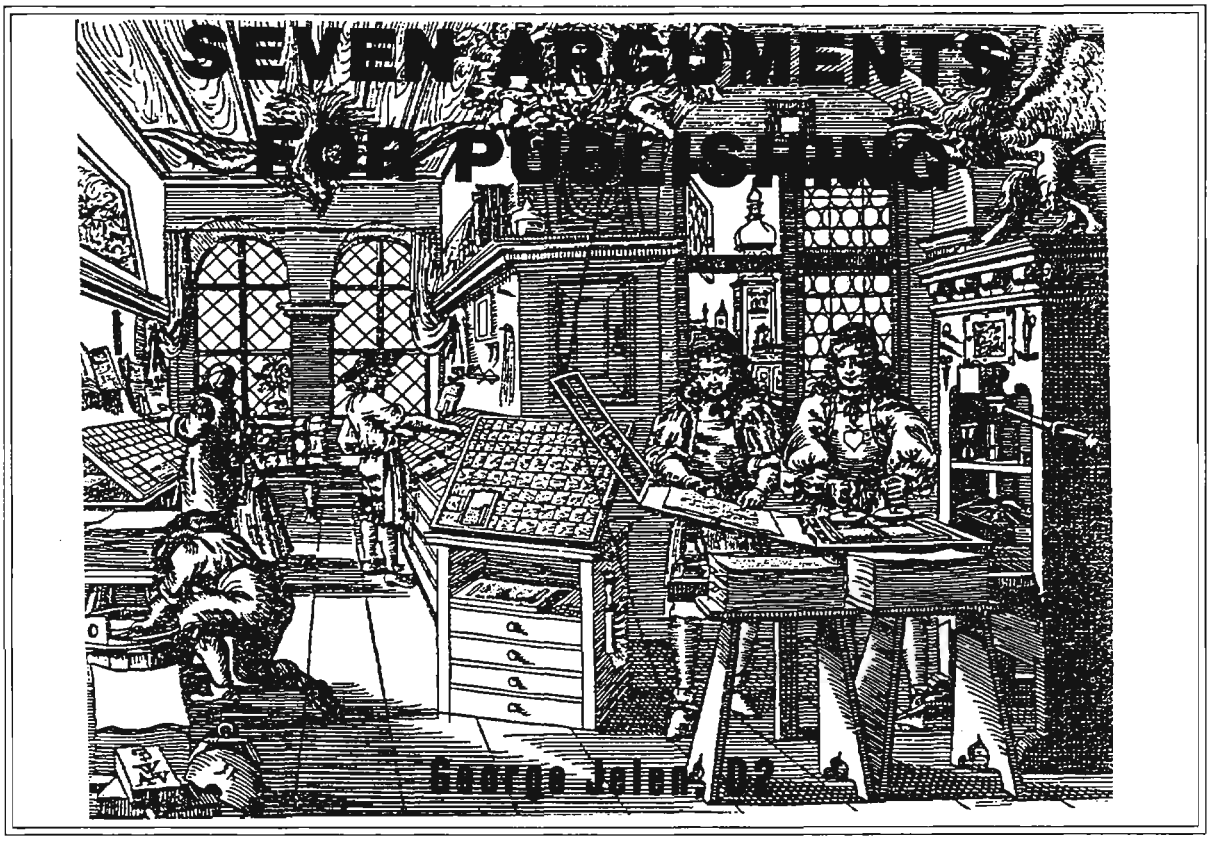
- ❒ Please enroll me as a new subscriber
- ❒ Please check my current mailing address
- ❒ Please change my mailing address
- ❒ Please change my name
- ❒ Please remove my name from the mailing list because I am
  - ❒ retiring or resigning
  - ❒ going to a field site
  - ❒ taking long-term training
  - ❒ too busy to read CRYPTOLOG (though I know I'm missing a lot)

OLD NAME AND ADDRESS		CURRENT OR NEW NAME OR ADDRESS	
----------		----------	
Name (Last, first, mi)		*Name (Last, first, mi)*	
---------	-----	---------	-----
Org	*Bldg*	*Org*	*Bldg*

Mail to: Distribution, CRYPTOLOG
P0541 Ops-1

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011853



Over the years, I have often found myself extolling the value of publishing, pointing out to younger members of the workforce the value to the organization and to the individual of writing for publication. I do it for several reasons. First, I believe it contributes positively to the professional culture and climate of the organization; second, there seems to exist within NSA an unhealthy disinclination to publish, possibly due to a misreading or misunderstanding of our security rules and focus; and third and most important, because no one ever did it for me. I had to learn the secret for myself, and it took me the better part of my career, more than twenty years, to do so. Invariably, when I finish my little exposition, the employee tells me that no one in his or her entire career had ever pointed this out before and thanks me for doing so. It is as if I have let the person in on a secret of success that had hitherto been concealed.

Since at the rate I am going I will never reach more than several dozen of the agency's employees and since I now believe that there are literally thousands of others who might profit from my message, I decided to turn my little speech into an article so that more might be exposed to it.

It is hard to explain why publishing is not more aggressively pursued. I find it difficult to believe that the value in doing so has escaped everyone's notice. Security and the attendant shyness we have regarding undue public notice explains some of it, although there are numerous outlets for classified articles including our own *Cryptologic Quarterly* and CRYPTOLOG, there are many valuable lessons and insights from our work that can easily and adequately be dealt with in an entirely unclassified manner; and portions of the agency's work are unclassified anyway. Another reason, based upon the testimony of many employees, is that supervisors are not encouraging it — nor are they providing an example by publishing themselves. The sad result of this is a lost opportunity for the organization, the individual, and the profession. I would hope that some supervisors can be persuaded by this article. And finally, there is the matter of simple inertia. Publishing does require effort. But there is a payoff.

Having given the subject a fair amount of thought, I have come up with seven reasons why someone among the NSA workforce might wish to consider writing for publication.

~~FOR OFFICIAL USE ONLY~~

Reason 1: It forces one to think more deeply about the subject.

We often think we understand a subject until we try to explain it to someone else or write about it. It is only then that we realize that we do not understand it nearly as well as we had thought. And so often, when we read something we have just finished writing, we are often embarrassed to discover that what we just produced simply does not hold together. This forces us to step back from the subject, think about it more deeply and work our way through the subject again. Oftentimes this even leads us to challenge some of our original assumptions and beliefs. The end result is that our understanding deepens. This is an extremely valuable process, the benefit of which accrues even if we never actually publish the article.

Reason 2: It can be an excellent source of psychic income.

No one should be embarrassed to admit enjoying being the beneficiary of a little psychic income now and then. Seeing in print something you have written is one of its best sources. Justifiable pride derives from the realization that someone else thought enough of what you had to say to publish it so that others could read it too. Actually, the psychic income can occur in two increments. The first increment occurs when you first see your piece in print. The second increment occurs when you discover that the published article has been cited by someone else. To have an article cited by another author has to be one of the highest forms of praise. I remember vividly the first time this happened to me. I was in a bookstore browsing when I noticed a book on a subject about which I had once written. I picked it up and was thumbing through it when I happened upon a footnote reference that began with my name. I promptly bought the book.

Reason 3: One can make money from it.

Under present law, even if you wrote an article entirely on your own time, you could not accept money for it. But you can enter it in some contest or other, and there are such contests all the time. Many of NSA's professional societies sponsor annual essay or writing contests with cash prizes. NSA's largest reward for writing, the Cryptologic Literature Award, carries a first prize of $2500, not an insignificant amount. One of CIA's publications, *Studies in Intelligence,* automatically enters any accepted article into an annual contest for the best article. The odds are quite good. There are four issues a year and approximately nine articles per issue. Last year, the publication awarded nine cash prizes. Thus, the odds of receiving a prize, once the article is accepted, is about one in four. And the prizes range from $200 to $2000.

Reason 4: A published work is an entry in a Personnel Summary or Resumé.

Resumés offer a chance to list your publications; NSA's own Personnel Summary has set aside a specific space for such a listing. It may be useful to know that there are some of us who always look specifically at the Publications entry to see what if anything is included. I realize there are not many people who do this, and therefore most would not notice if there were nothing listed. However, most of these same people would notice if something *were* listed. And certainly, any entry is better than a blank.

Reason 5: Publishing is a professional obligation.

Most people consider themselves professionals, though they may have done little to contribute to the advancement of their profession. It seems to me that if you wish to call yourself a professional, you should pay some dues to your profession. What you do on the job constitutes the dues you pay to that job; professional activities such as publishing constitute the dues you pay to your profession. Although there are many ways in which you can contribute to your profession, contributing to the literature of the profession is one of the best. Writing and publishing a professional paper confers upon the author considerable stature in the profession. Also, publishing is a professional activity with enormous leverage. Many people belonging to the profession can be stimulated by the article. What you write can inspire new thinking on the part of someone else. The reader then expands on your idea in another article. In this way, the profession advances.

~~FOR OFFICIAL USE ONLY~~

Failure to publish is to miss this significant professional opportunity and, in my view, to ignore an important professional obligation.

Reason 6: A published work constitutes a part of your legacy

At some point in life, you realize that you are running out of time and you begin to think about what you will (or will not) leave behind. You begin to consider your contribution to the world, your legacy. Your legacy is what you pass on to future generations. It could take the form of material possessions, creative products, enterprises, or simply influence on others. Legacies are important. Ultimately, our legacy constitutes whatever claim we have on immortality.

Legacies are not generally a concern of the young. People tend not to think in these terms until they reach mid-life. I have noticed, for example, that people become more concerned with their legacies as the date of their retirement nears. This has certainly been true in my own case. In fact, it was probably an influencing factor in my decision to write this article.

I am sure that you have had the experience in which a valued, long-time employee finally hangs it up and retires. In the thirty-some years that one employee had worked, she had amassed a considerable amount of knowledge and experience. But because she had not written much of it down, when she retired, that knowledge and experience went with her. Now, several months later, the organization she left behind faces a thorny problem, its members note that if Thelma were still around she would know what to do. But of course, Thelma is not around, and neither is any reflection of her considerable experience. It is a sad situation: sad for the organization and even sadder for Thelma. Sad for her because there is a natural generative imperative in all of us to want to leave something behind. The Talmud contains the observation that there are three things one should do in the course of one's life: have a child, plant a tree, and write a book. All three are generative activities; all three involve leaving something behind that is likely to survive us; all three constitute part of our legacy. Publishing an article may be the first step to *your* book.

Reason 7: It makes it easier for your boss to get you promoted.

For those of you who have not been moved or influenced by any of the first six reasons, this seventh and last one may have some persuasive appeal.

I like to think of our promotion system as consisting of two gates. The first gate is a binary gate; it determines *whether* a person will or will not be promoted. This first gate is controlled by one's immediate supervisor and perhaps by the next person up. The second gate is an analog gate. It determines *when* the promotion will occur; and many, many people control this second gate, particularly for promotion to the higher grades.

A key group of people who exert influence on the second gate are promotion boards. Among other evidence, promotion boards receive written and oral testimony. Because they read and hear so much testimony, most of it glowing, they become anesthetized to adjectives. It would take a very creative testifier to come up with an adjective that a promotion board had not heard. Every person that the board is considering is hard working, highly motivated, tenacious, highly effective, etc. If it were were not so, that person would not have been recommended for promotion in the first place. Nevertheless, the testifier has to offer up a suitable serving of adjectives just to keep that candidate even with the others.

The testifier is then likely to relate some recent contribution that the candidate made that is considered particularly significant. The problem is that there is a strong likelihood that most of the board members will not understand nor appreciate the significance, because the contribution is in a field or discipline foreign to theirs. Nevertheless, the contribution is presented. To the typical member of the promotion board, the contribution certainly sounds positive. Clearly having made the contribution is better than not having made it. But how does it compare with the specific contribution of another candidate in an entirely different field, both of which are foreign to the direct experience of the board member? How is the board member supposed to compare the contri-

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011853

bution of a mathematician with that of a lawyer, or a linguist, or a logistician? Yet that is exactly what members of promotion boards are required to do. Again, the testifier has to present such a contribution, but because of the difficulty in comparing them, the net effect may be no more than to keep her candidate even with the competition.

If, however, the testifier is then able to produce some published work of the candidate, that candidate is likely to slip ahead of the others. Why? Well, first of all because most of the competition will not have anything published. Second, and perhaps more important, all members of the promotion board can identify with a published work. They may not understand what was written (they won't take the time to read it anyway) but they know what it means to publish. They all know what it means to write and they all know what it means to have one's work deemed worthy by some outside arbiter and actually published. Having done a bit of testifying before promotion boards myself, I can attest to the utility of this strategy. I have used it successfully on several occasions.

So there you have it: seven good reasons to write for publication. I hope I have stimulated you to consider doing so. I look forward to seeing some of your names as authors of future articles.

The Lead Sentence in a Serialized Report

SIREN
SIGINT REPORTERS NOTES

P.L. 86-36

[redacted] P05211

The lead or topic sentence of a well-written SIGINT report should concisely convey the essential facts of the report to provide the reader, especially the time-pressed executive reader, with a well focused précis of the contents of the report. This lead sentence should always answer, when possible, the "Five W" questions —who, what, where, when, and why. It should expand upon the title, focus on the main theme of the report, and highlight the most significant foreign intelligence and any conclusions drawn from the SIGINT facts. Reporting the "who" is vital to the SIGINT user for assessing the importance of the information.

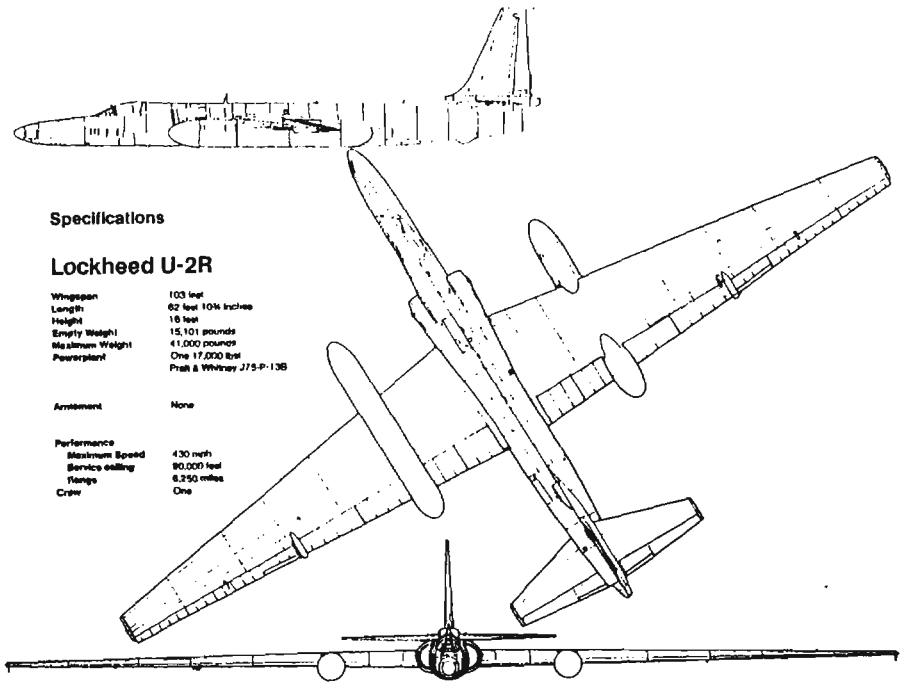
While the lead sentence should expand upon the report title, it should not be cluttered with clarifying data such as unit subordinations, coordinates, abbreviations; such information should follow later in the report. In a short report, this information would be in the second sentence or paragraph, and in a long report, in the section labeled "DETAILS." Note that short reports do not require sections headings, but long reports require at least the sections heading labeled "SUMMARY" and "DETAILS."

Elaborations of this guidance are contained in USSID 300, Sections 4.3 and 6.2.

~~FOR OFFICIAL USE ONLY~~

[redacted]

P.L. 86-36



UNCLASSIFIED

Figure 2. Lockheed U-2R

P.L. 86-36
EO 1.4.(c)

~~(C)~~ Remote airborne operations have long been a major part of this country's overall SIGINT effort. Over the years, we have employed several types of airborne platforms and have enjoyed excellent success in accomplishing our mission. However, these conventional platforms have limitations that somewhat restrict our collection potential. This article will show the support to military operations provided by the [redacted] through its involvement with the highly capable U-2R aircraft.

HISTORY

(U) The history of the U-2 is unique. Developed in the early 1950s by Lockheed, the prototype resembled a jet-powered sailplane with a slender fuselage. It was 49 feet 8 inches long with a wingspan of 80 feet 2 inches. To balance the wings, a set of dropable stanchions with small dolly wheels (called pogos) were attached at mid-span on each wing. These fell away when the aircraft took off and were retrieved by ground crews to be reused when the aircraft landed.

~~(C-CCO)~~ By the late 1960s the aircraft had undergone dramatic changes. The new U-2R's (R for revised) overall length was increased to 62.7 feet, with a wingspan of 103 feet and a range of 6200 miles. However, the true utility of the U-2R was seen in its ability to operate at altitudes in excess of 60,000 feet. This capability benefited SIGINT operations by making platform detection and interception more difficult and by allowing a deeper look into the target area than afforded by conventional airborne efforts.

[redacted]

~~CONFIDENTIAL~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

REFERENCES

(U) Larry Davis, *U-2 Spyplane in Action*, Texas, Squadron/Signal Publications, Inc, 1988

P.L. 86-36
EO 1.4.(c)

Stuart Buck, ret.

The Accidental Lexicographer

(U) Fifty years ago we were in the darkest days of World War II. Experienced linguists were urgently needed for translating and for code and cipher work. Stu Buck was among the seasoned scholars of language called to the colors.

~~(S-CCO)~~ Operationally he worked on Japanese, Chinese, Romanian, French, Mongolian, Tibetan and Dzongkha as a bookbreaker and cryptolinguist, as well as a lexicographer.

(U) This article is based on a talk to the Crypto-Linguistic Association at an unknown time.

~~(FOUO)~~ Sometimes I think that I have been involved in lexicography, to a greater or lesser degree, throughout my entire career at NSA. The projects have ranged from small informal card files stashed away in my desk to a regular, full-fledged dictionary. For our discussion today, I shall confine my remarks to three dictionary projects, each of which had certain distinctive features.

The Japanese Technical Dictionary

~~(S-CCO)~~ At the end of World War II, I was asked to assist in compiling a Japanese technical dictionary. Certain aspects of this particular project were unique in my experience. First of all, the task itself was taken seriously. No one viewed it as busy work. Linguists were carefully selected for their special skills—and tested in order to determine that these skills were not illusory. Once the group was set up, it stayed together until the project was completed. Guidelines were made crystal clear to all involved—and were enforced. It was all very simple: we were told to extract from various dictionaries any technical terms not included in *Kenkyusha*, the standard dictionary.

~~(S-CCO)~~ I was assigned to work on a French-Japanese dictionary, so my basic task was to translate the French expression and to determine, as best I could, if the Japanese equivalent was acceptable. All my cards were checked by another French linguist; then we turned them over to [redacted] the editor-in-chief—and a superlative Japanese linguist. P.L. 86-36

~~(S-CCO)~~ We saw the trees, he viewed the forest, and took personal responsibility for the overall product. I recall that there were about a dozen linguists in our group, working from lists of Japanese words defined in some other language—or, in a few instances, from Japanese sources. Streams of cards flowed to [redacted] who accepted or rejected items in terms of his basic objectives. The high value of the dictionary that was finally published is suggested by the fact that the publishers of *Kenkyusha* appear to have incorporated it intact into their latest edition. P.L. 86-36

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~
EO 1.4.(c)
P.L. 86-36

(U) I soon found myself writing essays on all the key words encountered, including as many example of usage as I could find. I had little choice but to use the eclectic method, so I examined, for every word under study, everything said in every available dictionary, compared the results, added what I had gained from my own experience, and made out a card for my files.

P.L. 86-36

(U) The whole thing was totally foolhardy. In a sense was trying to do all alone what had been accomplished by [redacted] highly trained team.

EO 1.4.(c)
P.L. 86-36

~~(C-CCO)~~ Give me credit, however. I realized that it was madness, but I never took my eye off that [redacted] Thus, I tended to go easy on the flora and fauna, and to bear down heavily on common vocabulary, particles, function words, idioms, likely loan words, personal names, titles, place names, organizational terms, hierarchies of all types, etc. Until the very end, I viewed the dictionary as a technical aid required to solve a specific [redacted] problem. Perhaps I went overboard, but it seemed to me that the problem demanded quite a lot. Even so, I was surprised to discover that the dictionary, when completed, contained some 833 pages.

[redacted]

EO 1.4.(c)
P.L. 86-36

[redacted]

(U) Included in the listings were a gazeteer and a list of personal names. There were three sorts:

- transliterated Dzongkha, in true dictionary order;
- a phonetic transcription, according to a system devised by Indian scholars; and
- English meanings.

EO 1.4.(c)
P.L. 86-36

(U) I like the system of deriving vocabulary from current texts and the ability to correct, update and edit periodically, but I miss the essays or articles that were characteristic of key words in my Tibetan dictionary.

Problems in Lexicography

(U) Certain problems were common to all three dictionary projects described above. Most important of these was the answer to the question, "what shall I include, and what shall I leave out?" Exactly what am I trying to do: tend a dustbin or forge a precision tool?

(U) Also, who will answer for the final product, a lot of anonymous contributors or a single individual? What shall I do about things I do not understand—ignore them and hope they will go away? Suppose I understand some tricky expression or usage that is devilishly hard to explain to someone else? Can I assume that everyone else understands it just as well, and save myself the trouble of clarifying it?

(U) Is it enough to provide one-for-one equivalents (if there is such a thing), or am I, as lexicographer, obliged to get into language structure?

□

EO 1.4.(c)
P.L. 86-36

~~(C-CCO)~~ Once upon a time there were graphic linguists and voice linguists, and then there were cryppies. At that time and place I was called a "cryppie." Not a cryptanalyst, mind you, but a language person

EO 1.4.(c)
P.L. 86-36

~~(C-CCO)~~ A good command of the language was and is absolutely essential for this work.

~~(C-CCO)~~ Well, since I did no reporting, and translated only an occasional cryptanalysis-related message, I didn't feel like a graphic linguist, and so I started thinking of myself as a cryptolinguist. (Perhaps this was in self-defense, as linguists would always see me as a "cryppie," while cryptanalytst would refer to me as a "linggie.")

~~(C-CCO)~~ But once in Z, I discovered that there was a whole other world out there. While in some languages cryptolinguists need a great degree of depth—years of experience, target knowledge, and excellent language skills—other Z people worked on targets which required somewhat less depth but more breadth—introductory course in language, possibly in a number of languages, but requiring far more knowledge of cryptanalytic techniques.

~~(S-CCO)~~ So what is the correct definition of the term "cryptolinguist?" The Glossary of Cryptanalytic Terminology (30 Sept 91) defines cryptolinguistics as "the branch of study embracing the characteristics of language which have some particular application in cryptology

EO 1.4.(c)
P.L. 86-36

[redacted]

(C-CCO) The question remains, "What is a cryptolinguist?" And, "Am I one?"

(C-CCO) Over the years, many people have met for countless hours to try to put together a COSC for cryptolinguists. Yet the toughest part of that is defining what a cryptolinguist is. Is this a broad field encompassing both those "majoring" in CA but using language daily, as well as those who "major" in language [redacted] How do you set up criteria for a COSC that covers both? Must a cryptolingist be professionalized in both fields?

(C-CCO) Or are these really two totally separate fields? It has been suggested that the cryptanalyst using language is a cryptanalyst, and should be considered as such by tech track boards, etc. But what of the language-cryptolinguists?" Are they cryptanalytic enough to be considered (fairly) by CA boards, or must they earn their accolades elsewhere—through A and B Group language boards?

(C-CCO) If we define a cryptolinguist as someone who is somewhere on a continuum that stretches between two poles, language and cryptanalysis, but who needs to use both, we could embrace both the language-cryptolinguist (needing depth) and the cryptanalyst who uses language (needing breadth). A COSC could be set up with two tracks, the primarily CA track, and the primarily language track, working with both the CA and Language career panels.

EO 1.4.(c)
P.L. 86-36

(S-CCO) [redacted]

How will they be treated by language boards? Is as much value given to cryptolinguists as it is to voice linguists? (For a clue, look at FLIP allocations.) If we had not been split up, would there be enough of us to consider as a separate group?

(C-CCO) What do you think, linguists, cryptolinguists, and cryptanalysts out there? Is there any chance that we can finally come to a consensus on what a cryptolinguist is? Can we come up with a COSC which encompasses both those strong in language and those strong in cryptanalysis? Or should these two groups of people be treated separately?

(FOUO) I would like to hear your views. You may call me on 963-5071. On e-mail I can be reached [redacted] or hard copy can be mailed to me at Z443, Ops-1. Your responses would be most welcome.

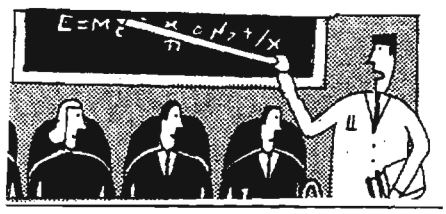
P.L. 86-36

Answers to Electronic Publishing Quiz, page 36

1. Advanced Function Printing
2. All-Points Addressable
3. Computer-aided Acquisition and Logistics Support
4. Cathode Ray Tube
5. Dynamic Job Descriptor Entry
6. Dots per inch
7. Disk Operating System
8. Forms Description Language
9. Generalized Markup Language
10. Job Control Language
11. Job Entry Subsystem
12. Magnetic Ink Character Recognition
13. Optical Character Recognition
14. Overlay Generation Language
15. Print Description Language
16. Print Service Facility
17. Revisable Format Text
18. Standard Generalized Markup Language
19. What You See Is What You Get
20. Xerox Escape Sequences

Major Breakthrough in Combinatorial Mathematics

[redacted] R51



A major breakthrough in combinatorial mathematics has been achieved in R51, where researchers constructed a ***Hadamard difference set in a group of order 100***—a feat thought to be impossible by most experts in design theory, a highly developed science in which conventional wisdom held that the order of such a group could not have a prime factor greater than 3.

The new difference sets provide a means of constructing highly structured block designs and related Hadamard matrices which are square arrays with entries +1 and -1 and whose rows are pairwise orthogonal. Such arrays have a myriad of applications in areas as diverse as statistical design and coding theory which exploit their pseudorandom correlation properties. These properties are similar to those of M-sequences, bent functions and perfect binary arrays which correspond to difference sets in more familiar *abelian* groups.

Until this recent discovery, the only known Hadamard groups had order of the form $4N^2$, where $N=2^a3^b$. Since the family of Hadamard groups is closed under products, the new result may be combined with the old to produce Hadamard groups of orders of the form $4N^2$, where $N=2^s5^{s+1}$ or $N=2^a3^b10^c$. There is hope that these constructions may be generalized to produce Hadamard groups of any order $4N^2$, $N=2^a3^b5^c$, and perhaps others as well.

The new result also provides a counterexample to a long-standing conjecture of Thomas Storer of the University of Michigan that a nontrivial difference set could exist in a nonabelian group only if there exists a difference set of the same size in an abelian group of the same order. It is ironic that the nonexistence of *abelian* Hadamard groups of order 100 was proven recently by University of Minnesota-Duluth researcher R. L. McFarland who was the one who promoted the subject of difference sets in the Agency when he was stationed here as a young Air Force lieutenant twenty-five years ago.

The break-through work was performed as part of a project to determine which (if any) of the sixteen groups of order 100 could contain a difference set. The four abelian groups were ruled out by McFarland, and, of the twelve nonabelian groups, six had been ruled out by the combined efforts of R. [redacted] R. L. McFarland, [redacted] Work was then focused on the six remaining undecided groups, and in particular, on the so-called G_9. P.L. 86-36

Ken Smith of Central Michigan University, here on sabbatical last year, outlined an approach to this problem and did a preliminary computer search which reduced the size of the final search (the sought-after difference set is a 45-element subset of the group of 100 elements, but trying all such subsets is out of the question). [redacted] did a more careful costing of algorithms to effect the final search and did more computing to build a database which would constitute the search space for a branching algorithm. In early January the approach looked feasible but had not been programmed. [redacted] presented a status report on the project at the Baltimore meeting, expressing optimism at the prospects of G_9. Other duties then intervened.

In anticipation of the AMS meeting at Lehigh 11-14 April [redacted] resurrected his work and enlisted [redacted] to write the final program. Ted quickly wrote a very clever C-program which effectively found all difference sets in G_9, and thus, immortality. ▫

Strategic Considerations for NSA Processing

[redacted]

~~(C)~~ The purpose of this article is to evaluate the likely effect upon NSA processing of technological and non-technological factors over the next decade and to propose strategic considerations for evaluation in determining how best to deal with these changes. In particular, this document seeks to update the prior Future SIGINT Capabilities (FSCS) documents with respect to NSA processing.

~~(C)~~ The User Interface System(UIS) is a multi-level ADP architecture that is intended to satisfy current and projected analytic support requirements, while providing an individual user with access to data and services regardless of physical location. It represents a long-term continuing effort, already well underway, to specify and provide an architecture that adapts to changing and evolving processing and support requirements. As such, it becomes the starting point for the strategic considerations developed in this document. The basic UIS (3-Tier) architecture is illustrated in Figure 1.

THE DISTRIBUTION OF PROCESSING

3-Tier UIS Architecture

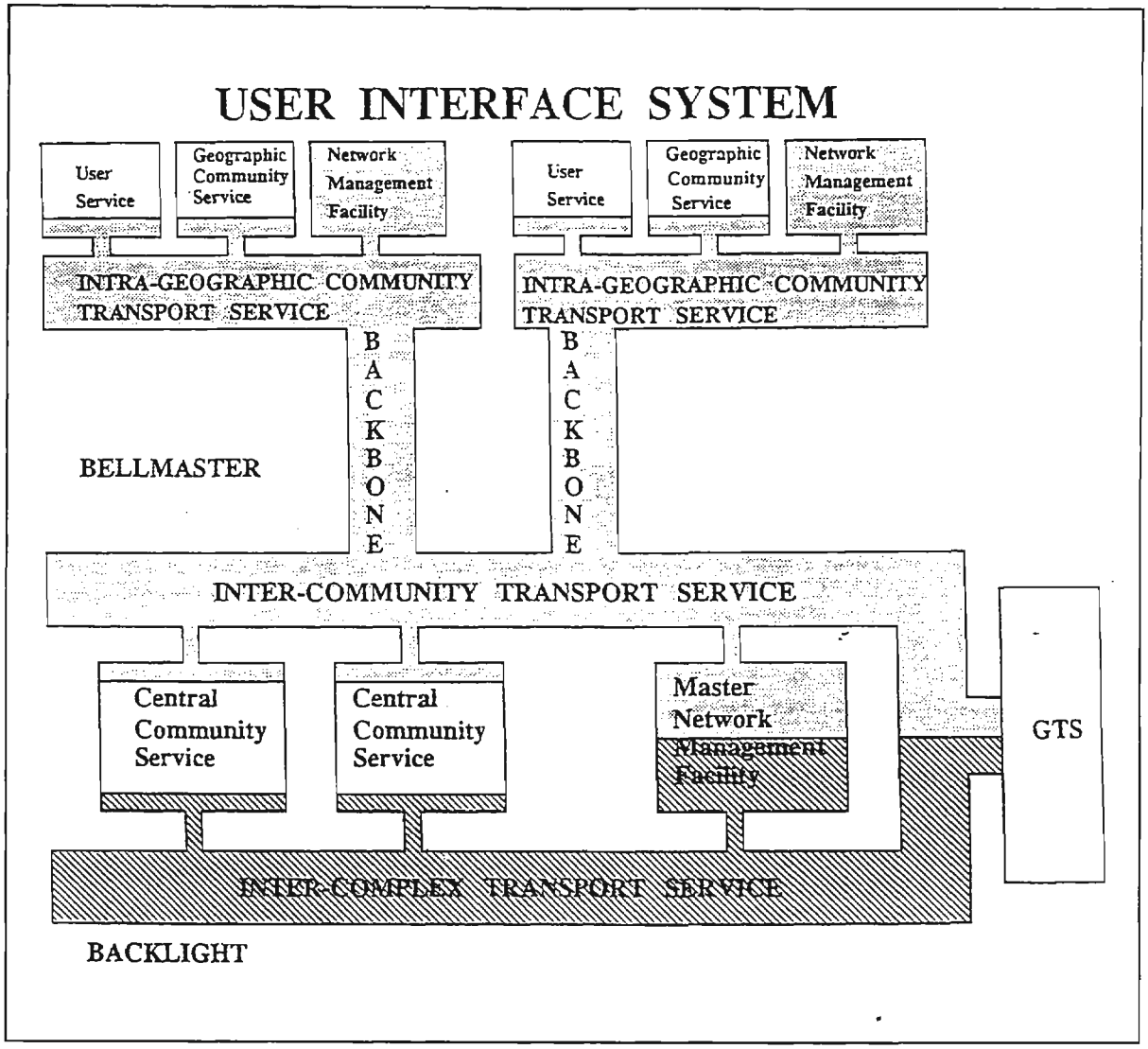
(U) The high-level UIS architecture (Figure 1) developed in the early 1980's was predicated upon processing trends at that time, and mirrored industry expectations and architectural trends of that period: widespread processing distribution with decrease of large mainframe processors. Users were expected to interact, through either "smart" or "dumb" terminals (Tier 1), principally with intermediate (often referred to as "departmental") capability computers (Tier 2), where the bulk of the processing needs for that community of users was expected to be accomplished. These Tier 2 processors (typically thought of in terms of the mini-computers of the day) would, where necessary, communicate with a relatively small number of increasingly powerful mainframe computers or computer complexes (Tier 3) for compute-intensive ("number-crunching") processes; for access to (and often down-loading of) portions of very large data bases; and for eventual storing of processed data which might be needed by users outside the immediate community. Users were expected to have little concern with the mainframes which might be accessed, since the primary processing would be accomplished by the ever-more-numerous Tier 2 computers.

(U) The 3-Tier architecture is currently the accepted standard for a large installation—and is pertinent to smaller installations as well, principally by eliminating the need for one or more tiers—and is expected to be relevant well into the next century. The basis for the Tier definitions has already changed, however, and will change further as technology evolves.

Processing Distribution Trends Among Tiers

(U) Already the "personal computer revolution" has exerted great influence. There are very few "dumb" terminals still in use, and even "smart" terminals have been largely supplanted by powerful personal workstations. As the power of these workstations increases—already the high-end Tier

~~SECRET~~



1 processors are approaching the power of the early supercomputers—more and more processing will be, and is, accomplished in user areas. This capacity and the increased sophistication of end-users are certain to support the momentum toward dispersing processing functions to Tier 1. It is likely that in a few years, most tasks previously carried out in Tier 2, and many in Tier 3, will be accomplished routinely in Tier 1.

~~(C)~~ That leaves a less predictable future for Tiers 2 and 3. Some need for Tier 3 processing appears to be certain for the foreseeable future, at least for certain highly computation-intensive processes such as cryptanalysis, and for storage and retrieval of very large databases, only a small subset of which might be relevant to any particular set of users. It is possible, however, that the majority of the functions now carried out by mainframe complexes might migrate to the next (substantially more powerful) generation of Tier 2 (departmental) computers, serving to replace those current Tier 2 processes which will migrate to Tier 1.

(U) Another possible scenario, which appears to be somewhat more likely, is that most of today's Tier 3 processing will remain in Tier 3, whose computers will also become ever-increasingly more powerful. If this happens, it is likely that much of the Tier 2 processing that is not suitable for Tier 1 may be redistributed to Tier 3, leaving the very real possibility that Tier 2 will largely disappear. There is much in favor of such a coalescence, including architectural simplification, reduction of support costs, reduction of operator costs, and simplified network management. Opposing this are the cost of mainframe processors, vendor flexibility, power and air conditioning needs, and,

~~SECRET~~

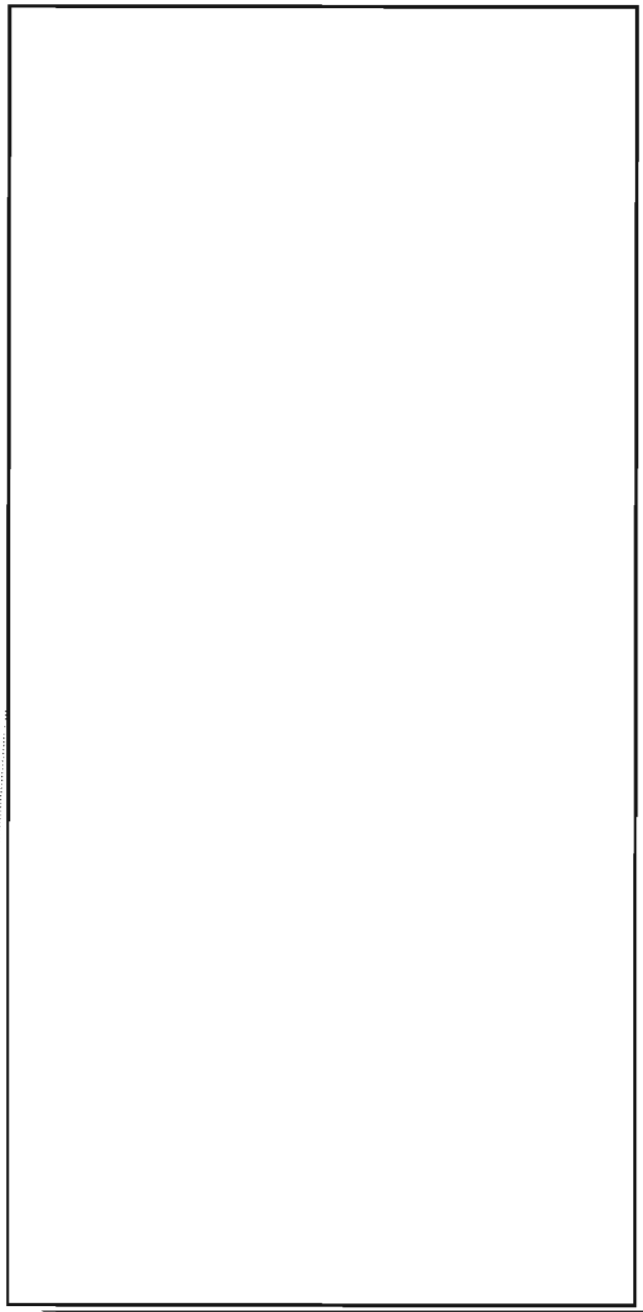
~~HANDLE VIA COMINT CHANNELS ONLY~~

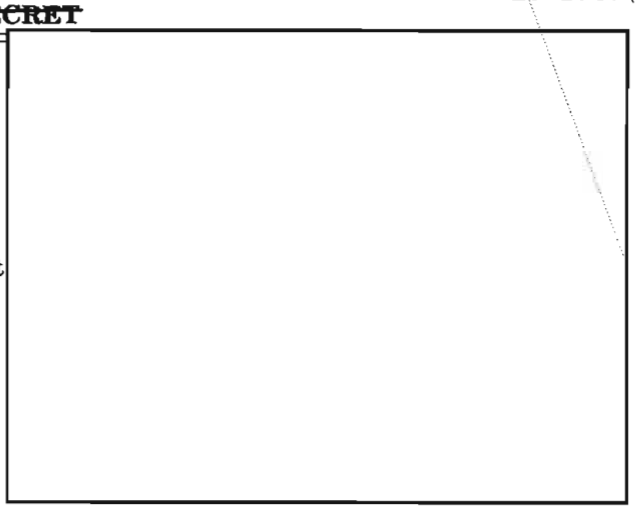
P.L. 86-36
EO 1.4.(c)

possibly, elimination of whatever security benefits may be inherent in the use of departmental machines. Both industry direction and cost-benefit analysis will influence the choice.

(U) It is safe to say, however, that Tier 2 will remain relevant at least into the late 1990's, albeit with a reduced and less important role, such as support for Tier 1, rather than processing functions per se. Likely functions include those of file servers, traffic distribution, database repositories, and input/output support processors for Tier 3 processors.

The Distribution of Processing





MAN-MACHINE INTERFACE

Standard User Interface

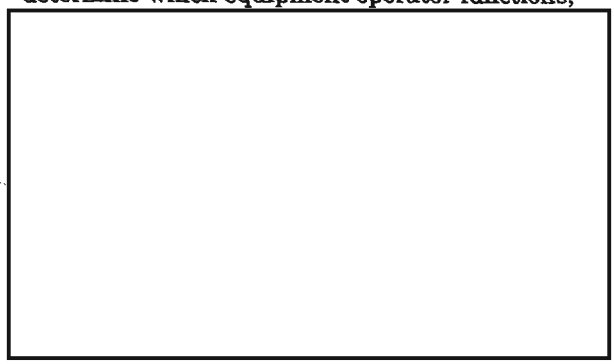
(U) There has been much discussion, both at NSA and elsewhere, about the desirability of having a single, user-friendly mechanism to permit any class of operator to interface with the equipment. An early goal was to define and implement a standard interface for all programmers, operators, and analysts who deal with computers. At first it appeared possible to come close to this goal in terms of a single workstation (ASTW) with a single keyboard configuration, connected to a single intermediate computer (ASH), using a single operating system (UNIX), and a single programming language (C). Now we know that none of these assumptions has, or will come to pass. We realize it to be a nice theory with more apparent than real benefits and at a staggering cost, if in fact it proved to be technically feasible. It did not address the problems of freezing on outdated technology in a rapidly changing field.

Realizable Man-Machine Improvements

~~(C)~~ The planned use of windowing software packages for high performance workstations permits access to many systems through a single keyboard and workstation. This in itself is a major improvement in man-machine interface, simply by requiring an analyst or programmer to learn only one machine, keyboard, and set of procedures for any given job. Now that the basic technology is here, there is a need to acquire modern workstations with state-of-the-art user interface devices and capabilities, and to train our workforce to make use of them. Further analysis is required also to

P.L. 86-36
EO 1.4.(c)

determine which equipment operator functions,



P.L. 86-36

STANDARDS AND PROTOCOLS

(U) The use of standards, particularly standard protocol suites, is required by the UIS architecture and is essential for achieving interoperability and commonality among differing functions and systems. Even though the Agency is in the process of adopting a much more flexible hardware standards program, its principal standards efforts are moving away from the low-level standardization on hardware and toward the higher-level standards available for both software and protocols.

Problems

(U) Since the mid-1970's, there have been increasing Agency efforts to provide a degree of standardization on computer hardware in an attempt to curtail the enormous support burden inherent in a multi-vendor, multi-component environment, and also to try to achieve the obvious benefits of system compatibility by use of identical hardware. As the computer marketplace has evolved toward the widespread use of standardized packages of both hardware and software, the Agency has attempted to do the same. It has become obvious, however, that a single choice for any given purpose cannot handle the multiplicity of uses which Agency elements require. As a result, standardization efforts are moving increasingly into the realm of software and, especially, protocol standardization.

(U) The focus of NSA's software acquisitions has clearly swung toward UNIX-based systems. This trend can be expected to continue and it is expected to enhance software portability and to make commonality among different NSA systems easier to achieve. Nonetheless, it is not a panacea. In particular, there is as yet no "standard UNIX" nor is there likely to be one in the near term. Moreover, as hardware becomes relatively cheaper with respect to total system cost, system vendors increasingly differentiate their products with "value added" software functionality. As a result, the software features available from vendors are not common across the industry and will not be so in the future. If one NSA element makes heavy use of proprietary "value added" features of one vendor or consortium of vendors, portability to a different element or application may be lost.

(U) Although software or hardware standardization may alleviate some difficulties that hinder interoperability, it is difficult to achieve commonality, let alone standardization, for many reasons. While commonality is a rational goal (to promote software cost sharing, for example), the real key to SIGINT production in a joint environment is system interoperability. System interoperability can come about most easily when the parties involved are following the same architecture, which is heavily dependent upon common usage of a set of standard protocols at all logical levels. Unfortunately, although NSA and other organizations are moving in this direction, there is not yet widespread availability of stable commercial packages that implement the protocols necessary at all levels. It is reasonable, however, to expect this problem to be resolved over the next few years.

Movement Toward Standards

(U) It has been the case, and will continue to be, that there exists a multiplicity of available standards in any given arena. In most cases a choice from among a (hopefully) small set of "acceptable standards" will be available to implementers. Even in cases in which we attempt to use a single standard, the magnitude of the installed base together with the rapidity of technological (and standards) change make it unlikely that we will ever deal exclusively with a single standard throughout the processing system. There must, however, be an increasingly strong movement away from vendor-proprietary technology and toward the use of open standards and components which can be acquired from multiple vendors.

Even here it is unlikely that large segments of the installed base will actually be converted, largely because of the immense investment in software. Rather, we must attempt to encapsulate proprietary communities, minimize the proliferation of proprietary technology to new systems, and provide "standard" gateways and bridges to interconnect the proprietary complexes to the external, open UIS world.

Categories of Standard

(U) Regardless of the type of standard, experience has shown that a single, usable-in-all-situations standard is probably neither achievable nor desirable. Rather, small families of "acceptable" standards should be defined in most instances, to balance the conflicting needs of interoperability and lowered support costs with flexibility of choice and optimization for a given environment. This leads to a grouping of standards in three basic categories:

(U) ***Mandatory Standards*** These are, and must remain, few and far between. Currently there is a single mandatory standard for the USSS, that of the network address protocol standard, currently the DoD Internet Protocol "IP." This is necessary in order that all systems throughout the SIGINT system can address one another and mutually interact, but even this requirement is less than absolute. IP must be made available for exchanges between communities, but it is not mandated for use within a local community of users. Moreover, some complexes, historically dependent upon a given vendor and that vendor's proprietary protocols, are unlikely to provide even IP as a canonical in the foreseeable future, relying instead upon their own internal protocols and on gateways to make the necessary translations to the standard world outside.

(U) ***Recommended Standards***. In addition to "required" standards, there will be an increasing number of "standards of choice," recommended for use unless there is strong rationale for using a competing standard. Reasons for such recommendations may include both technical and resource-oriented rationale, to include economies of scale, bulk-buy discounts, user familiarity, and ease of portability.

(U) Thus the UNIX operating system is highly recommended for most applications (and will be even more so as the various versions of UNIX coalesce toward a single universally recognized standard). There may always be some applications for which UNIX is inappropriate and some (especially large mainframe-oriented) complexes for which its introduction within a reasonable period does not appear to be feasible (technically or economically). Still other areas may have an installed software base, dependent upon a competing operating system, which may preclude any movement toward UNIX.

(U) Similarly, a relational DBMS is recommended for most applications, with the highly available and economically competitive INGRES recommended as the DBMS of choice. However, it is recognized that there are some applications for which this choice would be inappropriate, and for which a different relational DBMS or a traditional hierarchical inverted file DBMS would be more sensible. Such choices should not be dictated, and system designers should be free to choose an alternative for cause. In the same vein, certain DoD standard protocols (e.g. TCP, the transport layer networking protocol) may be recommended as the protocol of choice for most applications. It is recognized, however, that the associated capabilities (and, often, overhead) may not be justifiable for some applications, and also that emerging competing (e.g. Open Systems Interconnect) protocols may be an appropriate alternative even in advance of acceptance of the full OSI protocol suite.

(U) ***Selectable Standards.*** There will continue to be many instances in which selection from a small set of approved standards will be acceptable, permitting system designers the flexibility necessary to make an informed choice for a particular application, while still adhering to the requirements for meshing with a controllable, supportable architecture. For example, one can select freely from among the various higher-level standard DoD protocols, and this freedom of choice will undoubtedly continue after OSI is embraced.

(U) With respect to languages, we will attempt to reduce the number which are used (and thus must

be supported), but will not try to impose a single language for all purposes. It is likely that use of "C" will continue to increase within the class of applications for which it is appropriate; FORTRAN use, though likely to fall off, will not disappear in the near future; and use of Ada will increase, especially for new applications, eventually supplanting many of the older languages such as PL/I. For networking, IEEE 802.3 (Ethernet) technology is expected to predominate in the near future, yet IEEE 802.5 (Token Ring) will likely increase within its own realm of applicability. By the mid-1990's, FDDI (Fiber Distributed Data Interface) is expected to be the dominant technology.

(U) Regardless, existing proprietary technologies will continue for the foreseeable future within existing local complexes, due to their widespread use in many of our current applications. They will, however, become increasingly encapsulated within the complexes where they predominate, and standard, commercially available interfaces will be used to connect them with other elements of the processing system. Their use will gradually wither and die out, as they are replaced by new or updated systems in which standard, open protocols are built in.

Summary

(U) The use of standards, of all varieties, is key to our architectural planning and is essential to meet our requirements within acceptable cost. However, standards should never be viewed as absolutes, and must be used in a sensible rather than dictatorial manner. In particular, practicalities indicate that the most promising road to compatibility and easy accommodation of technological change is by emphasizing well-defined protocol and interface standards which are widely supported and available. Secondary benefits will result from use of common software to the extent possible. Standardization of hardware, while very beneficial in areas where it can be accomplished, is very difficult in a broad sense. It is incumbent upon system designers to be aware of the various standards available, to consider carefully the benefits which they offer, then to make a reasoned decision, accepting in advance the problems which will arise if they select a different choice for cause.

CONNECTIVITY

UIS Connectivity Goals

(U) The requirement to provide connectivity among the various systems and personnel within the USSS is the most basic goal of the User Interface System architecture. The strategy for achieving this is, once again, to follow the lead of industry wherever possible and to concentrate on use of commercially available components and standard protocols. Our connectivity requirements are very similar in concept to those faced by a broad array of industrial and governmental organizations, although the number of connections, anticipated data volumes, and geographic dispersity of our environment present particular problems faced by only a few. Three UIS connectivity precepts affect all network planning:

All-to-All But Not Any-to-Any

(U) To meet the basic UIS goal of providing any user, at any location, with whatever processing and data resources are necessary to accomplish its job, it is necessary to provide the technical capability for any person or system to interconnect with any other person or system. At the same time, it is necessary to provide the capability to restrict such paths to those that are permitted and necessary for operational and security reasons.

Networks Must Accommodate Devices

The USSS processing system does, and will, encompass a vast array of systems and devices, from many vendors, representing a variety of technologies and technical generations. It would be unreasonable and unrealizable to require each potential vendor to make special modifications to its standard product line to interface to our networking structure. As a consequence, our networks must be designed to accept, unmodified, connection of this array of devices. This requires, once again, use of standard network technologies, standard protocols, and standard interfaces, all compatible with the technologies and protocols supplied as a matter of course by the majority of systems being produced by the various vendors

Management and Security

(U) Although network management and security are problems faced by all large organizations, our needs are, and will remain, more severe and more stringent due to the size and diversity of our system and, especially, to the unique security requirements which we must meet. It is in this area, probably more than any other, in which we will have to push industry to meet our needs, fund special developments, and utilize much in-house expertise to satisfy our requirements

Network Segments and Technologies

(U) Global networking in the 1990's and beyond can be thought of as consisting of five categories of networking segments (four UIS, one GTS), each with different requirements and each, at least potentially, using a different type of technology. These segments are the following:

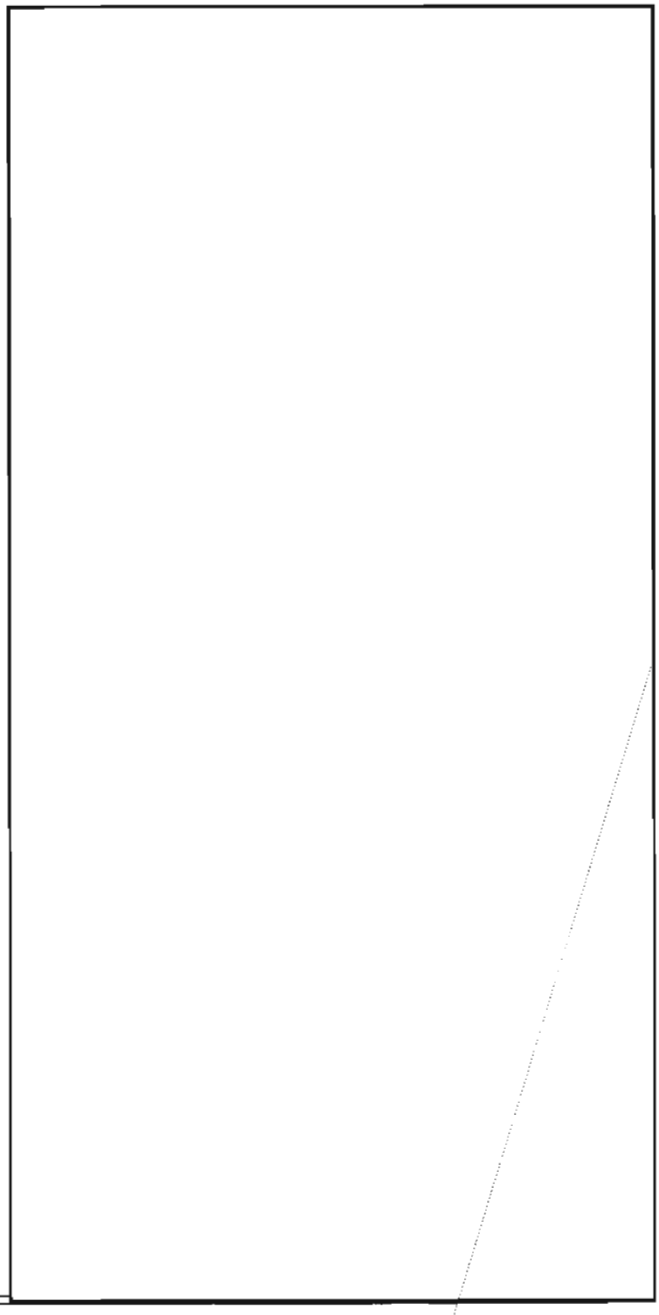
User Area Local Area Networks

(U) These LANs will interconnect user workstations and small departmental computers or servers within a local area, often defined in terms of a community of interest. Typically these are 10 Mbps ETHERNET (IEEE 802.3) LANs today, and this technology is expected to dominate in the near-to-medium term. By the mid-1990's we will likely still have ETHERNETs in place, but 100 Mbps FDDI fiber optic LANs will become dominant, as fiber is extended into user areas throughout the system. This technology should remain adequate for such use well into the following decade, and cost considerations indicate its early replacement to be unlikely.

Interactive Backbone Segments.

(U) These high-speed LANs are used to interconnect user area LANs with one another, with intermediate (i.e. Tier two) processors, and with central processing complexes. BELLMASTER 1.5 (80 Mbps) backbones are being installed to satisfy this requirement today (under Project CLOVER), and BELLMASTER is expected to become the ubiquitous controllable, supportable architecture. For example, one can select freely from among the various higher level standard DoD protocols, and this freedom of choice will undoubtedly continue after OSI is within NSAW in the very near future, and ultimately throughout the system. This technology will be upgraded to FDDI as soon as it is available, and might well be upgraded again to enhanced FDDI (probably 200 Mbps) during the course of this decade, assuming that this technology is defined and becomes available. Even the basic FDDI version should remain adequate into the next century, however, and a replacement of markedly different technology is unlikely, principally for cost reasons. This technology can be expected to be standard, consistent, and long-lived throughout the system.

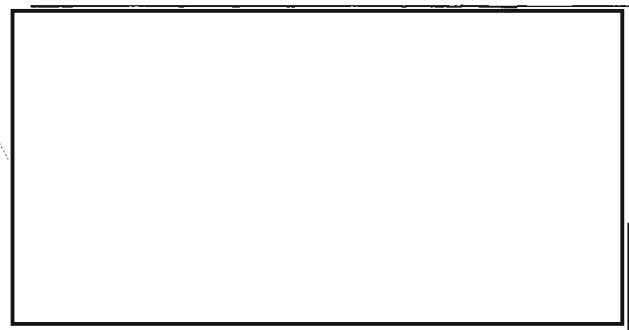
Inter-Complex Segments



P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)
DOCID: 4011853

EO 1.4.(c)
P.L. 86-36



Wide Area Network (WAN) Segments

~~(C)~~ The final category of segment is the WAN, which will be defined under auspices of the Global Telecommunication System (GTS). These segments will be used to interconnect instances of UIS (i.e. campus processing complexes) at each facility throughout the world. Represented by a variety of communication links today (packet-switched, dedicated circuits, T1 and T3 carriers, fiber, satellite, etc.), these segments can be expected to embrace a variety of rapidly changing technologies at any given time. Once again, standard protocols and interfaces, including use of carefully selected gateways, will permit GTS to pass processing data from one UIS network to another, in as transparent a fashion as possible, thereby effecting truly global processing connectivity. The WAN segments must be capable of interfacing to both the interactive backbone LANs and the inter-complex backbone LANs, as well as embracing new communications technologies.

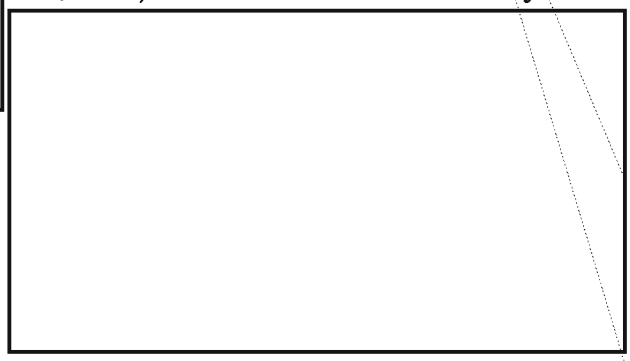
PLANNING AND BUDGETING CONSIDERATIONS

Cost Considerations

(U) Cost ramifications, both dollars and personnel, are necessarily an inherent part of the planning process, regardless of the issue being examined. Consequently, cost considerations will not be separated in this plan from other planning considerations. It must remain obvious, however, that affordability is the sine qua non for any aspect of planning, and that all cost factors must be considered in the planning process, including those (e.g. facilities) which are affected in the aggregate, but which are difficult to quantify as a function of a specific decision

Systemic Balance

~~(C CCO)~~ The historic and on-going question of proper balance between collection and processing, both with respect to capability and resource commitments, is certain to continue indefinitely.



~~(C CCO)~~

Equally important are considerations of having sufficient (i.e. neither too few nor too many) personnel with the proper skills and training in the proper locations to fully utilize the technical collection and processing assets available. Moreover, we must have sufficient and robust communications to ensure that whatever amount of data are collected can be moved in timely fashion to the point of processing. These considerations must be balanced also against such aspects as provision of the proper levels of support for equipment and personnel, regardless of location; proper facilities (to include power and cooling needs); and, more difficult to assess, the cost-effectiveness of modernization and asset optimization against the constrained investment resources which we must face.

Cost Drivers of Modernization

~~(S CCO)~~ We must continue to move the SIGINT system forward to meet the ever-increasing challenges which it faces, but any form of progress has cost ramifications. Some of these cost-drivers represent simply the cost necessary to achieve a new, necessary capability. Others may represent the initial investment cost necessary to achieve improvements which have the potential of reduc-

ing costs, for a given level of capability, in future years. Still others represent potential cost savings, short-term, at the expense of some operational capability. All of these must be examined on a cost-benefit basis, based upon relative potential to fulfill our mission; timing of costs incurred (and the time-value of money); degree to which various resource expenditures equate to relative fulfillment of requirements; and to the timing of when given capabilities must be available. Typical cost-drivers to be so considered include the following:

- survivability (in all its aspects);
- computer security (to include networks and systems);
- need for pushing industry (via funded efforts) to advance technology in given areas to achieve the benefits of that technology earlier, instead of waiting for the technology to develop on the basis of market forces;
- benefits and drawbacks of attempts to achieve commonality (e.g. use of a single programming language such as Ada), and the extent to which such commonality should be mandated;
- effect upon facilities of new processing hardware which often takes up far less room, but requires far more power and generates far more heat;
- benefits (and cost savings) of preserving existing software (and the costs and problems of doing so) compared with the presumed later benefits of new, more standardized, more easily maintained rewritten software;
- loss of capability inherent in disestablishing existing, outdated systems compared with the benefits to be achieved in supportability, space, and compatibility with newer systems;
- benefits, drawbacks, and reasonable extent of use of standards, to include use of a common undercarriage for diverse systems;
- proper investment balance between general processing systems and infrastructure which support all organizations, and the need for improvements in particular operational areas;
- benefits versus cost and complexity of multimission processing systems, cross-correlation across collection types, and flexibility for use in varied scenarios (peace, crisis, and war); and
- cost-benefit analysis of various productivity enhancement programs, including personnel training and use of such technical developments as artificial intelligence and expert systems.

Organizational Considerations

(U) It can be argued easily that the current organizational structure of the Agency, not changed significantly in the last decade and predicated upon 1970's concepts of missions and roles, is already highly inefficient in dealing with our current problems. If unaltered, it is certain to become even more obsolete and ineffective in the years to come. Recent trends in technology and processing have had a particularly pronounced blurring effect upon the relevant roles of technical personnel in the Operations, R&E, and Telecommunications Organizations. There is already a great deal of duplication of activities across these key components, often at cross purposes and with little coordination or mutual visibility, and widespread misunderstanding of (or refusal to recongize) defined organizational roles. If left unchecked in the coming years of still more rapid technological change, we will be faced with a highly inefficient, immensely costly, technological anarchy.

(C) Careful analysis must be made of the proper roles of each organization with respect to current and impending processing technology; a partial reorganization may be desirable; and the defined roles must be understood and accepted by all. We will not be able to afford the levels of organizational autonomy which we have today, yet we must be very careful not to go overboard in defining roles to the extent that we are left with a stifling inflexibility of options. Of particular impact in these decisions are the ramifications of the current trends away from centralization and toward enhanced processing power at each analyst's desk. Although there is a potential for enormous gains in productivity and SIGINT output, there are also potentially many problems, most of which have been ignored heretofore. It must be realized that analysts are not trained programmers; that the efficiency of use of their workstations, as processing tools, will be substandard; that there will be widespread duplication, with little reusability, of software pro-

duced; and that little regard will be given toward maintainability, adherence to standards, and other precepts of good programming practice. The extent to which these aspects should affect rules, roles, and organizational structure cannot be foretold without detailed study. Nonetheless, it is essential that such areas be addressed, rather than the current practice of simply ignoring the problem and letting changes evolve without a concerted plan.

Summary

~~(C)~~ We must recognize that there has been an irreversible change in the way in which processing is accomplished; that continued change is certain; and that responsiveness in a purely technological sense is insufficient. A flexible plan, regularly revisited, is needed to ensure that our organizational, procedural, regulatory, and personnel practices are responsive to the changes.

Author's Note:
This paper was written three years ago; prior to the breakup of the Soviet Union; prior to the recent DDO restructuring; prior to the current emphasis on downsizing; prior to Paul Strassmann's CIM initiative; and without knowledge of the past three years of technological innovation. Nonetheless, its basic precepts appear to be nearly as relevant today, and the crystal ball of 1989 appears not to have been very murky.

Letter

To the Editor:

Another reply to the article, "Where was the Bogeyman?":

Hysteria over "the Islamic threat" is grounded in ignorance of the Arab peoples, their religion, and their culture. A close examination of all three would reveal a society whose basic beliefs and values are not dissimilar to our own. It would also highlight the individuality of the Islamic sects in the Middle East and their desire to establish national identities—factors that make a jihad unlikely.

It may be that the word "Islam" and "terrorism" are so linked in the minds of Westerners that we are unable to distinguish between the two. There is no doubt that terrorists have used and continue to use Islam as a pretext for their actions. The terrorists do not, however, speak for the majority of Muslims. We need to listen to the voices of the majority—not the over-publicized shouts of the extremists.

In any debate on Islam there are legitimate issues to address. We need to understand the reasons for the spread of Islam and the appeal that extremist groups hold for some Muslims. It would be a mistake to allow fear or hatred to distort our understanding, or to let the actions of a few blind us to the legitimate concerns and problems of the many. Only by objective analysis, and by laying aside our Western biases, can we hope to achieve progress in East-West relations.

[redacted] *B732*

~~FOUO~~

P.L. 86-36

P.L. 86-36

[redacted] *P05/SAO*

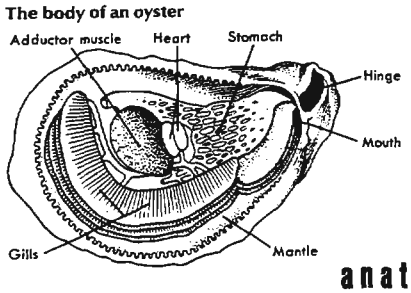
Missions/ Functions/ Organizations/ Personnel

~~(C-CCO)~~ Questions often arise concerning the classification of NSA's missions, functions, organizations, and personnel. The following is a list of items and the classification, if any, of each.

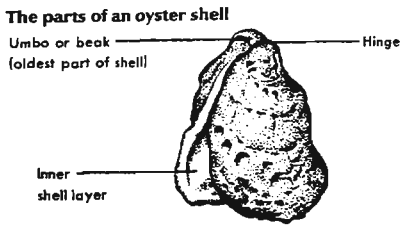
FACT OF	CLASSIFICATION
• NSA's missions of SIGINT, INFOSEC, or OPSEC training	UNCLASSIFIED
• Information revealing the general missions and functions of COMINT activities without revealing specific COMINT techniques, procedures or targets	UNCLASSIFIED
• NSA's organizational designators below key component level	FOUO
• NSA's use of supercomputers as part of its mission	UNCLASSIFIED
• NSA's total budget or individual line items	CONFIDENTIAL
• Total manpower strength of cryptologic community, NSA or SCEs	CONFIDENTIAL
• Individual job title and description that does not contain classified information requiring classification (NSA Reg. 10-11 provides unclassified job titles and descriptions)	UNCLASSIFIED
• The statement "cleared for TOP SECRET, Special Intelligence (or cleared TS/SI)	UNCLASSIFIED
• The statement "cleared for TOP SECRET, indocrinated for CAT III COMINT"	~~C-CCO~~

DOCID: 4011853

ON THE TAXONOMY OF THE OYSTER



anatomy of the oyster



P0541

P.L. 86-36

(U) Turn the clock back to 1,000,000 B.C., plus or minus three sigmas. Our ancestors had just accumulated enough little gray cells to work with.

(U) They looked around and marveled at nature. They made note of the cycle of the seasons. They made note of the progression of the heavens. They made note of the tides.

(U) And they noticed that some matter replicated itself and some did not. That was a step in taxonomy: animate and inanimate, though they might not have used those terms.

(U) Then they also noticed that some of the replicable matter moved under its own volition, and some did not.

(U) People move at will on land, birds in the air, and fish in the sea. So, therefore, they must fall in the same class—animate matter that moves at will. Then there is also replicable matter that does not move under its own volition. For example, trees and oysters. Our ancestors noticed that trees are rooted in the earth. They noticed that oysters are rooted on rocks under water. Therefore, trees and oysters must fall in the same class—animate matter that cannot move under its own volition.

(U) Just as trees and oysters are related, so are substitution systems and codes. Superficially, they appear to behave in the same way.

(U) But it wasn't until 980,000 years later that our ancestors learned about complexities in the oyster that distinguish it mightly from a tree. It did take a while for them to realize that it was a difference in kind, not in degree.

(U) It's not surprising, therefore, that it has taken us until now to recognize that substitution systems and codes differ in kind, not degree. Actually, it was known years ago, but as that knowledge was based on instinct it was set aside as unscientific.

BASIC CRYPTOGRAPHY

(U) Let us review cryptographic principles. In cryptographic systems, there are only two possible operations:

- substitution: replacing one character by one or more characters.
- transposition: rearranging the characters.

It's possible to apply both to a single message.

~~(C CCO)~~ So we see that, on the surface, it seems reasonable to assign codes and ciphers to the same

EO 1.4.(c)
P.L. 86-36

family. After all, the ***enciphering*** process is the same—replacement. In a substitution system, one plaintext character is replaced by one (or more) cipher characters. The process is similar in a code system. The plain text (called "the meaning" in codes) is replaced by cipher called a code group. Therefore, the two enciphering processes are similar.

(U) Now let us turn to the ***deciphering*** process, as cryptanalysis was called in the early days.

~~(C-CCO)~~ The critical factor that distinguishes code from substitution cipher is the matter of the plaintext component. And this difference is a difference in kind, as you shall see.

~~(C-CCO)~~ In a substitution cipher, the possible plaintext equivalents for each cipher component are finite: the cipher letter can become one of only so many possible plaintext letters. It does not matter whether the plaintext component is only letters, or only digits, or a mix of letters and digits, or a mix of letters and digits and punctuation. It's a closed system.

~~(C-CCO)~~ This is true whether the substitution system is monoalphabetic, or polyalphabetic; whether it is based on a hand system or a machine system; or, even, whether there are variants to suppress the plaintext frequencies The possibilities for plaintext values are finite and known. If the enciphering process is complex—using shift registers or true one-time pad, for example—recovering the plain text correctly may be exceedingly difficult or even impossible; nevertheless, the cryptanalyst is confronting a system with a finite plain text population. The plain text must be "one of the above."

~~(C-CCO)~~ By contrast, in a code system, the possible number of plaintext equivalents (known as "the meaning") is very very large, for the plain text element may consist of a letter, digit, word, phrase, or sentence, or even, a complete message. Therefore, the possible plaintext values are, for practical purposes, infinite, and unpredictable as well. The nature of code is its high compressibility. For example, the plaintext component (the meaning) represented by a single ciphertext element (the code group) may be:

- a word: "treaty"
- a complete sentence: "This morning I had a long private conversation with the Prime Minister."
- a phrase: "under no circumstance"
- time: "1800 hours"
- a spell: "-Y-"
- a family of verb, abstract noun, agent noun, adjective, adverb, gerund
- a selector: "take fourth meaning of previous group"
- an oblique form of noun or verb: "would have signed"
- a place name: "Paris"
- a title "HR the Crown Prince of Ruritania"
- a ship: "the gunboat MAGNOLIA"
- an organization: "24th Battalion"
- deciphering instructions: "beginning with the next group use the PERSIMMON table."
- a complete message: "Attack at Dawn."

(U) So as you can see, unlike a substitution system that consists of a finite plaintext population, in a code system the plaintext possibilities are virtually infinite. For that reason the meanings cannot be recovered by purely statistical means, though statistics plays a part in the recovery of the meanings.

DOCID: 4011853

• study past traffic and combine frequent clichés such as "Reference your message Number 364" as one group. (Except you have unexpected subjects like Boris and Gorby, and narcotics interdiction, and Bosnia and Hercegovina, and GATT . . .)

(U) And then there is the famous case of a French World War I compiler who organized the codebook meanings by whether or not the nouns were derived from verbs—and this for a trench code!

THE FREE-WHEELING CODE CLERK

(U) To compound the difficulty of recovering the meanings of code groups, any rule the compiler sets for encoding plain text the code clerk may undo. Take, for example, a codebook that is in caption order—when the meaning is filed under the most important word in a phrase. If the caption is

1234 TREATY

thereafter you may see phrases incorporating TREATY:

1245 treaty of peace
1267 commercial treaty
1278 to sign a treaty
1289 the Queen signed the treaty

(U) The code clerk who is not familiar with the codebook very likely will encode the equivalent of 1289 as three groups, or even four:

Queen
Sign
(past tense)
Treaty

(U) And if the code clerk is looking for the number 1800, to measure distance (1800 kilometers) and runs into the military time 1800 hours first, that's what will be used. The decoding clerk at the other end knows to decode it as "1800 kilometers."

THE SYLLABARY

(U) Then we have the case of the syllabary, a gray area: these, like codes, should be catalogued separately as "syllabaries," not as substitution systems, for syllabary systems are open-ended and as unpredictable as codes.

WHY IT MATTERS

~~(C-CCO)~~ In the past we used to peruse hard copies of the system descriptions to learn about the past cryptographic habits of our targets. But now we're into information retrieval. If we're looking for a specific type of system, we must type in the appropriate term to access the database. And if we're looking for code, we will not find it, for codes are tagged as "substitution" systems. It's a loss of information that once was known.

(U) How did this state of affairs come to pass? I believe it was an excess of zeal in taxonomy, and misguided at that, with a large dollop of pedantry laced in.

(U) And this ties is in with recent practice.

~~(C-CCO)~~ Consider the term pentagraphic, used of a code (or cipher) group consisting of five characters. In parallel construction, one of twelve characters would be called dodecagraphic! We have puzzles enough set by our targets without concocting our own and confusing cryptanalysts who have not had the benefit of a classical education.

(U) It's time we dropped that clunky usage and reverted to that of an earlier, more elegant time, when a dodecagraphic group would be written as 12-character (or -digit-, or -letter, as the case may be). The important word in the compound—the length—is instantly recognized. And that's as it should be. Let our documentation be self-evident. Eschew polysyllabics.

(U) And on that note, let me invite everyone to drop forthwith the indiscriminant use of "superenciphered." Super means on top of. A code is "enciphered" using an additive, let's say. Period. Only if there is still another encipherment over the first should the term be "superenciphered":
• A 4-letter code enciphered with polyalphabetic substitution.
• A 4-letter code enciphered with polyalphabetic substitution, and superenciphered (ore "re-enciphered") by transposition.

(U) Isn't that neater?

(U) Let's get rid of the overburden of polysyllables.

(U) Keep it lean, mean, and clean.

~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4011853

P.L. 86-36

Valedictory

[redacted] *Z5,*
Formerly Chief, P1
CRYPTOLOG *Publisher Emeritus*

Address at a luncheon on 31 January 1992 to commemorate P1's 30 years of service.

(U) We were all saddened by the recent death of Bill Lutwiniak, but we know he would have wanted us to commemorate the occasion for which we are gathered. So today we dedicate this proceeding to his memory, and I ask that you join me in a moment of silence.

~~(FOUO)~~ P1 came into being, as nearly as I can ascertain, on Flag Day in 1961 as part of an NSA reorganization. John Kennedy had been in office only a few months and there was a mood of excitement in the country, tempered by an apprehension caused by the cold war and the potential Soviet menace. After all, part of the reason we reorganized was because of Martin and Mitchell. No more would we be ADVA, ALLO, GENS, or MPRO, but we would be A Group, or B Group, or G Group. How mundane!

~~(FOUO)~~ I was a young analyst in GENS which became A4 and very little changed for me. I had never even heard of P1. [redacted] who is here with us today, was appointed the first chief. He was chief for about a year. I got to know Dale later when he was chief of C, I believe, and when he helped G4 get a computer. He was succeeded by Frank Raven. Once of the things that happened while Frank was chief of P1 was the start of the cryptomath program in 1963 just as I was signing up for a new job in P1. I tried to get into the CMP, but Frank said I had been at the Agency too long, and he assigned me to work with Glenn Stahly in G4. By then, Lyndon Johnson was president and the world situation continued to be bleak.

~~(FOUO)~~ After about a year in G4, Mr. Raven told me I had a choice: stay in P1 and move to A5, or, if I wanted to stay in G4 I would have to transfer there. Since I was in the middle of a major project I opted to stay in G4, and my association with P1 became a lot less for the next 20 years.

~~(FOUO)~~ For a while, Ted Leahy helped me on my projects. Then he stopped coming by, and one day, seeing him in the hall, I asked him where he had been. He said he was helping people who needed the help more, that I didn't need him anymore. This was not exactly true, but it does reflect the P1 spirit and what it represented.

~~(FOUO)~~ In the meantime, George Vergine and Art Levenson—neither of whom, unfortunately could be here with us today—were the 3rd and 4th chiefs of P1 for about 7 years between 1966 and 1973. Nixon was President and Watergate consumed the nation.

~~(FOUO)~~ I had gone to GCHQ in 1971 on a G4 billet which was created because P1 would not let me be on their billet, which at the time was reserved for CMP graduates. I returned to the states in the summer of '74, and my family and I watched the hearings on Nixon from our motel room on Route 3 in Bowie, and later, listened on the radio to Nixon resigning while we were sitting in our empty house awaiting our furniture.

~~(FOUO)~~ At that time Bill Lutwiniak was in the second of his eight years as Chief of P1. This was the longest time for any of the chiefs of P1. I hope some of the speakers will talk about those years because I really had no direct dealings with P1 during all the years between 1965 and 1985 except through the CMP.

P.L. 86-36

~~(FOUO)~~ When Bill retired, he was succeeded by [redacted] as the sixth Chief of P1. Ford, Carter, and now Reagan occupied the White House and the country's cold war continued without much change.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011853

~~(FOUO)~~ During the 80's there was tremendous growth in the Agency, both in dollar and manpower allocations. I was still in G4 and experienced this enormous influx of new people into our already cramped quarters. It was, nevertheless, an exciting time, and we were accomplishing a lot of miracles, as [redacted] liked to say. So it was with some reluctance and misgivings that I accepted the job as the 7th Chief of P1 in 1987. Soon after, George Bush became the 7th president in the same 30-year period. I am not trying to draw a parallel between any one chief of P1 or any president; just that there were the same number.

P.L. 86-36

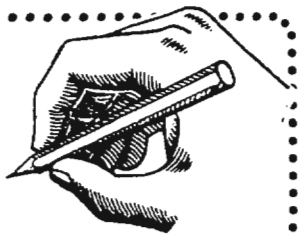
~~(FOUO)~~ Now the world scene was radically changing, and austere times were in store for almost everyone. The demands for restructuring were everywhere, and with the recent collapse of the Soviet Union, the reorganization, which had been planned for two years, raced towards completion. As the restructuring took shape, it became clear that a P1-like organization was not appropriate in a functionally aligned DDO.

~~(FOUO)~~ Now we enter a new era, and from my perspective, it will be exciting. About half of the old P1 will be going to the new Z Group, with some of the functions and individuals dispersed. The CMP will remain intact and unchanged in Z5 which I am heading. Other parts of P1 will survive in various other groups and the new operations staff.

~~(FOUO)~~ It is wonderful to see so many people, both present employees and retired P1'ers who have come out today to pay tribute to this wonderful organization. It is now time to hear from some of the other people who made P1 what it was in the past.

~~(FOUO)~~ In closing, while we salute the old, I leave you with the thought that it is people who make institutions great. We have not lost that magic ingredient with the demise of P1, so let's go forward and remember:

(U) "These are the good old days!"



To the Editor:

The Government Code and Cypher School was formed under the control of Cdr. A. G. Denniston. In 1938 Denniston was preparing for war, and encouraged the Foreign Office to buy the property at Blechtley Park. It had several advantages: 45 miles from London and 50 miles from Oxford and Cambridge, where Denniston hoped to recruit most of the mathematical and linguistic specialists. When war broke out, everything was in order, and scholars from the universities were rapidly recruited. For a short while the staff could be accomodated in the large country house, but soon it became necessary to build huts where various sections were housed—Hut 5 for the Italian Army cyphers, and others for weather and similar subjects. Many of the sections and huts have long been identified, but there were a few where top secret work was done, so secret that it was not until 1973 that Group Captain Wintherbotham made it known that teams at Bletchley had broken the German High Command cyphers—the Enigma.

The chief hut for this work was Hut 6, and to this day, it still stands. But Bletchley Park is slated for development, and the remaining huts will be bulldozed.

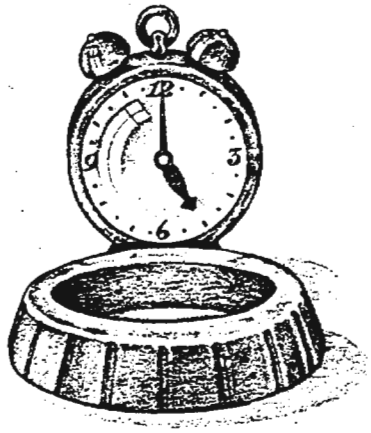
As many of those who worked in Hut 6 and elsewhere in Bletchley have objected to the disappearance of Hut 6, the Bletchley Park Trust has been formed. Already much has been done. It is likely that the Government will halt the demolition.

The Trust would like to hear from those who have an interest. The Trust may be reached at Suite 8, Denbigh House, Denbigh Road, Bletchley, Milton Keynes, Bucks, MKI 1YF. The chief executive is Ted Enever.

William Filby, former member, GC & CS.

DOCID: 4011853

A Visit to TIME



P.L. 86-36

Reported by: [redacted] *P05,* et al.

For some time agency reporting specialists have suggested adapting the organizational structure and publication techniques used by print journalism. In an effort to see which of these techniques can be used in agency reporting, a group of senior reporters visited TIME magazine on 17 and 18 June 1992.

P.L. 86-36

Persons Visiting: [redacted]

We were very openly and hospitably received by senior officials of TIME, Inc: the TIME Magazine Managing Editor, the Deputy Managing Editor, the Editorial Operations Director; two Senior Editors; the Picture Editor, and others.

From the very first, TIME insisted that we spend two days with them. They wanted us to see the progression of articles through the editorial process from one day to another. On both days we were privileged to sit in on the 1000 a.m. editorial session that the Managing Editor held with his key staff members to discuss ideas for the weekly issue of TIME Magazine, the status of articles already underway, etc. At these one-hour meetings the senior leaders of TIME, in concert with key staff members, decide what story lines will be pursued by the magazine. This is an intentionally free give-and-take regarding both domestic and international topics.

The morning session is followed by a series of additional section-level editorial meetings. It is at these meetings that TIME managers direct the reporting effort, channeling and focusing the various story lines. Once the actual article is written, there are quality checks throughout the production process by researchers, fact checkers, and copy editors.

In separate sessions, the Managing Editor and his deputy told us that what we witnessed in these editorial sessions was not always the procedure for TIME. Not too many years ago, it was a top-down structure, with the top telling the bottom what articles should be written, and even at times, the ideological thrust of those articles. This was particularly true when Henry Luce owned the magazine.

Now, stress is put on bottom-up collegial communications. This has not been an easy process for TIME, and both the Managing Editor and the deputy emphasized that one has to have patience in implementing such a process. They told us that some managers and employees feel more comfortable with a top-down structure. There is still some hesitancy among the staff to be openly contributory. But they say that the bottom-up approach is definitely the right one, because for the magazine to compete successfully these days, it has to have the fresh ideas and the proprietary involvement of its employees. We were struck by the similarity of the problems facing TIME and our own evolution toward a lower-echelon decision-making and employee-involved Operations

~~FOR OFFICIAL USE ONLY~~

Directorate and Agency.

TIME has about 400 persons to carry out its weekly publication; this does not include another about 200 who are involved in the business end—subscription handling, etc. Junior reporters start at about $35,000. There aree 28 bureaus, with about 55 correspondents outside New York. Henry Cabot Lodge was their first correspondent.

TIME does not have a formal training program for their reporters. They expect individuals whom they hire to already be trained journalists with experience gained elsewhere. Their staff is composed of experienced individuals trained in the journalistic style of reporting. They are required to follow the "TIME style" of writing. The deputy editor kindly gave us a few copies of "Writing for TIME", which is their internal style manual.

There is a Wednesday afternoon critique session, but there are many quality checks all along the line throughout the production process.

Researchers are used to assure that the facts are right in an article. TIME does not have a formal training program, except for training some persons on new equipment received. They do not train their reporters and writers. The deputy manager told us that it is still a "buyer's market" with TIME having their pick of young people anxious to come to work for TIME. He said this stems from the interest in journalism generated by the Watergate case.

Their final product is disseminated to numerous CONUS (e.g., Philadelphia, Atlanta, Wisconsin, Illinois, Dallas, Los Angeles, San Francisco) and four overseas locations for printing. The international edition is different from their domestic edition, and ads are matched to the various regions of the world.

We were told that within the U.S., even individual subscribers receive different ads in their issue of TIME. Depending upon facts related to a specific subscriber, a computer determines what ads to include in a particular issue: things like age, sex, ZIP code, salaries, etc., are used as the basis for determining the make-up of the individual copy. This amazed all of us, and we were wondering if there were some application of this software that we could apply here. TIME offered to discuss it further with us, if we desired.

Most of their non-management employees belong to a union, the Newspaper Guild, so like those of us in the federal service, TIME is not as free to hire and fire as one might think, we were told.

A large number of their employees work three days a week, twelve hours a day, and like it. This has to do with the natural production pressure that builds on Thursday and does not end until about 0300 Sunday morning when everything has to be electronically sent to the printing and distribution points. About 80-90% of the work is done on Thursday and Friday, with the crescendo coming between 3 pm Saturday and 3 am Sunday. The goal is to have the magazine on the street early Monday morning. When asked why Monday, they told us that this is just the way it has evolved over the years. Long, pressure-filled hours are normal during this time.

About 80% of the foreign bureau personnel are U.S. nationals, with foreigners hired to handle the clerical and administrative matters.

As for technology, the Managing Editor told us that the TIME goal is to have Macintosh terminals for everyone, with the ability to do article preparation on the terminal, and transmit to a large number of other terminals. At present they use a variety of computer terminals. Eventually, all the Macintoshes will be part of a single network so that article preparation and transfer of material can easily be accomplished from reporter to editor to photo desk, and so on. They plan to abandon their present ATEX system (a company name, we were told, which does not expand). We were told that a company named Stratus was great for preventing any down time in their vital operations.

As in nearly all news magazines, photo and graphic design play a large role in each issue. Once a story line is decided upon, photo taking and selection is usually done before an article is completed. TIME has independent photo journalists under contract as well as access to an electronically delivered photo service, similar to the

AP or Reuters wire. TIME is implementing a new high-resolution National Digital system which will enable them to quickly receive and incorporate photos into their magazine.

The art director decides the layout. Three or four of the picture editors are also photographers. Magazine covers are planned as long as eight weeks in advance, unless some special event, like the Los Angeles riots, occurs.

We met the individual who is responsible for TIME covers. Just 12 years ago, he said, TIME was a black-and-white publication. In 1981, they went to six pages of color, and finally in 1984, went to all color.

Actual readership is a lot higher than the sales number, because they know from surveys that copies are read by approximately four persons beyond the person to whom the magazine is addressed. They estimate a 30-million readership weekly.

Every article in TIME is carefully read by company lawyers to see if the magazine could be liable for something written. The managing editor estimated that the magazine has about one serious suit per year.

We will be reviewing our trip to TIME and to other publishers to determine what we might use to improve our reporting at NSA. We are particularly interested in generating greater interest in the editorial-board approach to production.

Electronic Publishing Quiz

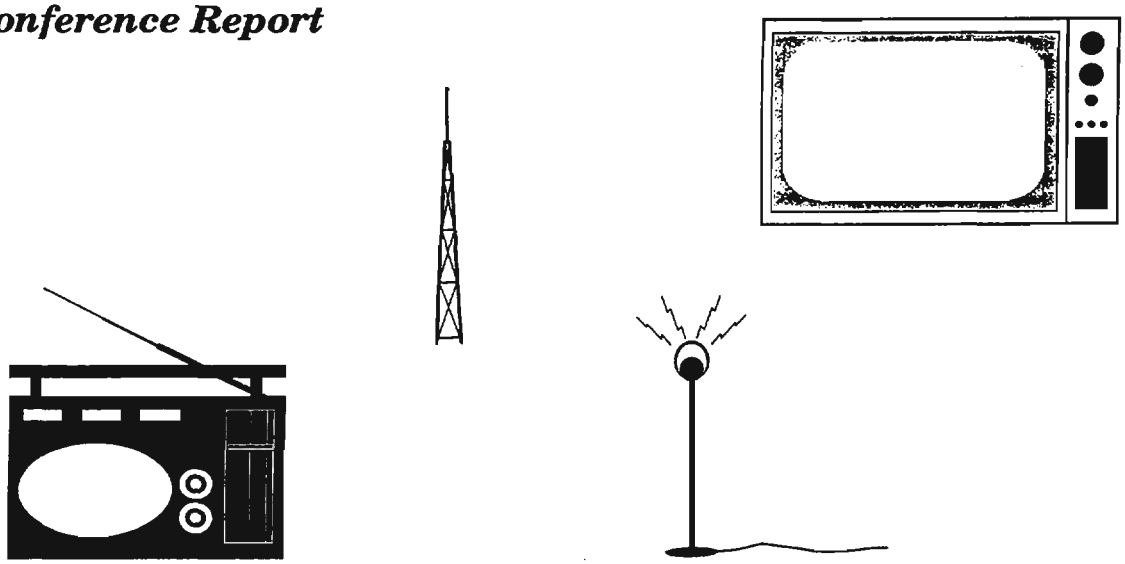
Expand the Acronym

1. AFP _____
2. APA _____
3. CALS _____
4. CRT _____
5. DJDE _____
6. DOS _____
7. DPI _____
8. FDL _____
9. GML _____
10. JCL _____
11. JES _____
12. MICR _____
13. OCR _____
14. OGL _____
15. PDL _____
16. PSF _____
17. RFT _____
18. SGML _____
19. WYSIWYG _____
20. XES _____

Answers on page 14

~~FOR OFFICIAL USE ONLY~~

Conference Report



(U) 1992 National Association of Broadcasters Convention and Exhibition; The Annual Broadcast Engineering Conference; and HDTV World '92 Conference and Exhibition; held concurrently in Las Vegas, Nevada, 12-16 April 1992.

P.L. 86-36

Reported by: [redacted] *P054 S/A*

~~(C)~~ The primary purpose of this trip was to provide me with the opportunity to assess current and emerging broadcast, video, teleconferencing, and multimedia technologies associated with the Operations Directorate dissemination initiatives [redacted] and other associated publication projects.

(U) Second, the trip provided the opportunity to assess new broadcast related digital, encryption, and laser technologies and continued escalating foreign interests in visual information production, hardware, and distribution technologies.

P.L. 86-36

~~(C-CCO)~~ Third, the knowledge gained from this trip will further assist the Operations organizations and Agency support organizations in developing new intelligence dissemination opportunities in video and multimedia technologies, and aid in the assessments of front-end SIGINT collection opportunities.

~~(FOUO)~~ Fourth, the NAB provides a unique assessment opportunity for those Agency employees involved in implementing the NSA/CSS Visual Information Services Working Group Report of November 1991. Information gleaned from NAB seminars and exhibitions will assist me in developing and maintaining a "state-of-the-art" understanding of facility planning and design, facility management, reporting production techniques, storing and retrieval techniques, archiving techniques, and technical equipment integration.

CONFERENCE OVERVIEW

(U) This annual convention and exhibition continues to be the largest of its kind in the world, and continues to grow with a record number of over 52,700 registered attendees and exhibitors, and a record international attendance of more than 8,651. International attendance reflected an increase of over 20% from NAB '91. New technologies, software developments, recording formats, and multimedia applications continue to be exhibited.

CONFERENCE SEMINARS

(U) NAB seminars were divided into Engineering, Radio, Television, and HDTV categories. In an effort to get a flavor of diversified areas of interest, I attended the following seminars:

Engineering Sessions

- Interactive Video , The Birth of an Industry, TV Answer, Reston VA
- The In-Touch TV System, A Technology Description Interactive Systems, Beaverton, OR

- Production Processes for Interactive Television Interactive Network, Inc. Mountain View, CA

- Pay Per View-Video on Demand, Jerrold Communications, Hatboro, PA

- Update on New Interactive Television, Applications of T-Net Radio Telecom and Technology, Inc. Perris, CA

Video Production & Post Production

- Driving Towards PC-Based Post Production, Autodesk, Inc. Sausalito, CA

- Bridging Computer Graphics and High Quality Video Tektronix, Video Products Operation Wilsonville, OR

Television Sessions

- Controlling Our Future, Broadcasters, Cable, Telco

- All-Industry Luncheon with addresses by Eddie Fritts, NAB President/CEO; Topic: Strategic Planning and Innovation (The Armed Forces Radio Television Service was honored), and by Former President Ronald Reagan, Distinguished Service Award Recipient (Ironically, I witnessed a second attack on this President at a Hilton Hotel, this time as he delivered his NAB keynote address.)

- Law and Regulation Conference Luncheon, Alfred C. Sikes, Chairman of the FCC. Topic: The Future of Broadcasting, Merging of Technologies, Need for Adaptability

PERSONS VISITED

(U) David Lyon, Chairman, CEO Basys Group

(U) Comments: Basys Automation currently has a system installed in the T5 Media Center area. Basys CEO provided insights for future business areas and technologies that the company is actively pursuing in information management systems and services related to video production, databases, library and archive, and multimedia technologies.

(U) Jean Gard, Entertainment Industry Segment Manager for Digital Equipment Corporation (DEC)

(U) Comments: Ms. Gard shared insights for future business areas and related technologies that DEC is actively pursuing related to multimedia technologies and services.

(U) Geoffrey S. Roman, Vice President, Technology and New Business Development for Jerrold Communications, a division of General Instrument Corporation

~~(C-CCO)~~ Comments: Mr. Roman is a former MITRE principal. In his public NAB engineering presentation, Roman mentioned that TCI and US West are using cable distribution technologies. Roman predicted major domestic US telecommunications implications in six to nine months. Although Roman did not go into detail with this statement, I believe Roman alluded to a potential new business enterprise for US Cable Companies in the telephone and data business in direct competition with the Baby Bell companies. After his formal talk he gave an interactive video engineering presentation

~~(FOUO)~~ Representatives from the National Cryptologic School's Visual Information Services Facility, E23, Research and Engineering, R8, and the DIA J2 Defense Intelligence Network (DIN) executive production staff.

~~(FOUO)~~ Comments: This provided an excellent opportunity for informal management and technology networking between NSA/CSS elements as well as interagency liaisons.

CONFERENCE ASSESSMENTS

Telecommunications Policy and New Technologies

(U) The FCC, through the dynamic leadership of its Chairman and proactive Commissioners, is continuing to drive the US into world leadership in digital communications. Featured at this year's NAB was the first over-the-air broadcast of digital HDTV on experimental TV Channel 15 as authorized by the FCC. (For those of you who have not seen demonstrations of HDTV, the image quality

will knock your socks off. It will revolutionize the broadcast and entertainment industries, not to mention what it will do to the telecommunications industry because of digital technology, video compression techniques, and non-video digital services.) The FCC anticipates announcement of a US digital TV broadcast standard in 1993. Shortly thereafter, US broadcasters are positioning to rapidly enter this new market opportunity. Digital AM and FM radio has already been developed. Digital data services are positioning for the radio market and new receivers will soon be installed in US-sold autos to provide alphanumeric information.

~~(FOUO)~~ Many international NAB attendees continue to assess and procure US developed video production and distribution technologies for a variety of entertainment, business, government, and military applications. The NAB has reached such an international scope, that the US Department of Commerce and Foreign Money Exchanges maintain sizable on-site convention presence.

Hardware

Video Production

(U) Off-the-shelf hardware technologies continue to develop for both linear and non-linear video production. Linear technology allows only ordered video production, i.e. item #1, then #2, then #3 and so on. Non-linear technology allows immediate random access broadcast quality video production, much like a word processor. Analog motion video, analog still images, and analog voice narrations are first digitized in non-linear editing and then randomly manipulated to produce a final video product. You can cut, paste, and transition combinations of both audio and video using computer technology, control software, an icon control screen, and a special-purpose mouse developed to expedite video productions.

(U) Television cameras and video recorder devices are both moving to digital technologies with approximately 1000 lines of resolution. As these digital devices develop, they will expedite the non-linear video production process because raw materials for video and multimedia productions will already be in a digitized format. I certainly believe non-linear video production is the way to go in the future. However, because this developing technology is expensive, I recommend using linear video production technology until the market settles a bit and there is a wider selection of vendors and established vendor standards and interfaces.

Video Recording

(U) New tapeless video production formats include rewriteable optical disc and rewriteable magneto-optical disc. Manufacturers exhibiting this equipment at the NAB included Panasonic, Pioneer, and others. These video recording formats support both linear and non-linear video production, storage and retrieval, and archiving requirements. These optical technologies are currently limited to approximately 55 minutes to 2 hours of record/playback time, depending on the manufacturer as well as analog, digital, and compression formats. The optical recording media is quite expensive when compared to videotape. Example: a one-hour Beta-CAM SP broadcast quality videotape costs about $25 versus a one to two hour magneto-optical disc which costs about $1200.

Duplication

(U) A high speed VHS duplication system was exhibited for the first time by The Sony Corporation. Other manufacturers including Sony, Panasonic, and others exhibited a number of real-time duplication systems, some with auto cassette feeds.

Teleconferencing

(U) Fully assembled teleconferencing units and integrated teleconferencing technologies were not featured at this convention. However, a number of manufacturers and system integrators exhibiting at the NAB offered such systems.

Software

~~(FOUO)~~ Software development is not currently a strong point for video hardware producers. Although a diversity of off-the-shelf hardware solutions exist for video SIGINT production, storage and retrieval of motion video and still images,

and long term archiving, at this point, I anticipate some limited software machine control development with a hardware vendor or related broadcast software developer to maximize automation capabilities of existing commercially available off-the-shelf hardware systems.

~~(FOUO)~~ There is currently no software standard for desktop video production. As in word processing, a number of software suppliers provide unique applications programs. Important to note is the fact that mouse hardware technology is being reworked for video production. Video editors using computer mouse technology for video production are not happy with current mouse designs for speed, hand-eye coordination, and physical durability.

~~(FOUO)~~ Several vendors are working toward software that will combine scripting, database searches, production, and machine automation control. This software development will greatly increase the flexibility of video production facilities.

Encryption

~~(C)~~ A number of companies are currently manufacturing and selling commercially available off-the-shelf analog and digital video encryption devices. These companies include: Leitch, Macrovision, Scientific Atlanta, and Sony. Sony, among others, now offers an international teleconferencing network.

Transmission

(U) Canon Broadcast Equipment Division introduced a new Optical Beam Communications System called the Canobeam. The NAB Broadcasters Daily News reports that this laser devise, using a high-speed modulated optical beam, can transmit up to eight video signals and 18 audio signal channels in both directions. Canobeam transmits wide-band signals up to 500 MHz. Data can be sent at speeds up to 156 Mbps. Transmission distance can range up to 2 km, and digital data transmission distance can be increased without signal degradation by using the Canon 3R function relay. (Can you imagine this type of technology in the next war?)

CONCLUSIONS AND RECOMMENDATIONS

[redacted] EO 1.4.(c) P.L. 86-36

[redacted] (The NAB and the US Department of Commerce maintain records of overt convention participation by name and country.) P.L. 86-36 EO 1.4.(c) Commercially available off-the-shelf technologies supporting visual information (VI) production, teleconferencing, and encryption continue to be exported to foreign countries for diversified multimedia information flow capabilities.

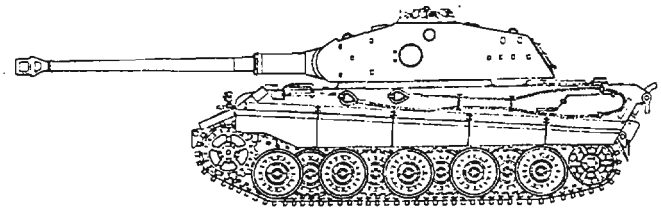
~~(C)~~ The Operations Directorate should continue representation at conferences, conventions, and expositions, such as the NAB, which will enhance the knowledge base required for the management, production, engineering, exploitation, teleconferencing, and multimedia development of cryptologic visual information (VI) activities.

(U) In order to adequately cover the growing magnitude of the NAB Convention, Exhibition, and Engineering Conference, I recommend expanded Operations Directorate representation, and I encourage representation of other Key Components at future conferences in support of expanding requirements for Agency Visual Services.

(U) New for 1993, the NAB announced a premiere conference and exhibition called "Multimedia World: Merging Video, Audio, and Computers." Beginning next year, this new annual event will be held concurrently with the NAB Convention and will provide a new forum for post-production video, business video, computer professionals, and broadcasters.

DOCID: 4011853

A Sidebar to SIGINT History



Betty Wanat, Rct.

~~This article is classified **TOP SECRET UMBRA** in its entirety~~

In early November 1977, the political situation between Ethiopia and Somalia had reached a crisis. At the same time the American Embassy reported that Ethiopia was considering breaking relations with the United States, though Ethiopia needed the food and equipment that the US had been providing.

P.L. 86-36
EO 1.4.(c)

EO 1.4.(c)
P.L. 86-36

DOCID: 4011853

Towards a Viable Tech Track

To whom it may concern:

Towards a viable tech track I hereby offer some suggestions.

• Establish a program of post-professionalization rotational tours.

• Sharply increase the proportion of promotions awarded to tech trackers. It is the traditional way: the more opportunities for advancement, the more enticing the prospect for remaining a tech tracker.

• Add to all promotion boards a voting tech tracker who will look out for other such.

• Convert some of the SCE slots to SLEs. We will be needing even more technical experts in the future.

• Be generous about sending tech trackers to professional conferences. The insights that can be gained are invaluable. In our closed society a breath of outside air is absolutely necessary. What's more, the attendees can share the wealth by writing up a conference report for CRYPTOLOG!

• Allow tech trackers time to document their projects at their conclusion. Documentation should be an integral part of any professional's duties.

• Give due credit to people who pass on the torch. These are the people who document their knowledge and techniques for coming generations, who act as technical mentors to interns and to seasoned analysts as well, who develop courses, who teach and lecture, who develop the professional examinations and grade them, who write philosophical papers on futuristics in their discipline, who compile lexicons and working aids of all kinds. They provide the hard core of technical and historical continuity.

• Honor the technical types who manage peopleless projects rather than people. Let's take a look at our own resources in these tight budget times. We are wont to make heavy weather about managing a long-term, big-bucks project. But we already know from the write-ups of the productivity awards that we have gifted people who can knock a complex project off in no time flat, and on a shoestring at that. Reward them suitably.

• Do not overlook the technical staffers. These are the people who fight the dragons that besiege our gates for secrets. We depend upon them to devise an unimpeachable defense for retaining classification.

• Be very very careful about overriding an evaluation of a tech tracker that is done by a technical board. If you think it necessary to do so, explain your reasons to the technical advisors.

• Last, but not least, about TQM: cumulatively, our professional cadres have a lot of smarts, imagination and ingenuity. Sound them out. Use them to solve problems.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011853

Editorial Policy

CRYPTOLOG is a forum for the informal exchange of information by the analytic workforce. Criteria for publication are: that in the opinion of the reviewers, readers will find the article useful or interesting; that the facts are accurate; that the terminology is correct and appropriate to the discipline. Articles may be classified up to and including TSC.

Technical articles are preferred over non-technical; classified over unclassified; shorter articles over longer.

Comments and letters are solicited. We invite readers to contribute conference reports and reviews of books, articles, software and hardware that pertain to our mission or to any of our disciplines. Humor is welcome, too.

Please note that while submissions may be published anonymously, the identity of the author must be made known to the Editor. Unsigned letters and articles are discarded.

If you are a new author, please request "Guidelines for CRYPTOLOG Authors."

How to Submit your Article

Back in the days when CRYPTOLOG was prepared on the then state-of-the-art, a Selectric typewriter, an article might be dashed off on the back of a used lunch bag. But now we're into automation. We appreciate it when authors are, too.

> *N.B.* If the following instructions are a mystery to you, please call upon your local ADP support for enlightenment. As each organization has its own policies and as there's a myriad of terminals out there, CRYPTOLOG regrets that it cannot advise you.

Send two legible hard copies accompanied by a floppy, disk, or cartridge as described below, or use electronic mail. In your electronic medium (floppy, disk, cartridge, or electronic mail) please heed these strictures to avoid extra data prep that will delay publication:

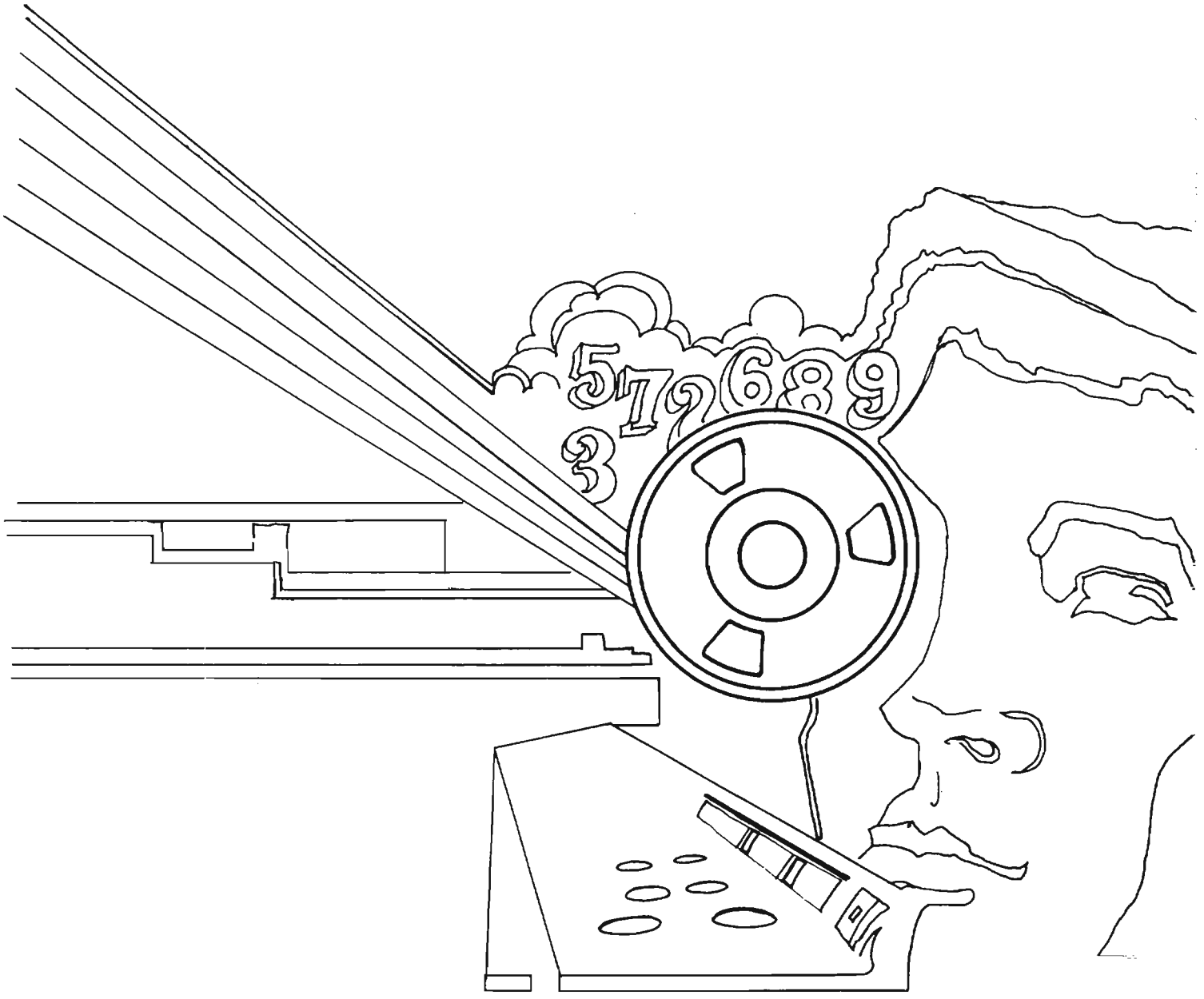
- do not type your article in capital letters
- do not right-justify
- do not double space between lines
- but **do** double space between paragraphs
- do not indent for a new paragraph
- but **do** paragraph classify
- do not format an HD floppy as DD or vice-versa–our equipment can't cope
- label your floppy or cartridge: identify hardware, density of medium, software;
- put your name, organization, building and phone number on the floppy or cartridge

The electronic mail address is *via* PLATFORM: cryptlg @ curator
or *via* CLOVER: cryptlg @ bloomfield

CRYPTOLOG publishes using Macintosh and Xerox Star. It can read output from the equipment shown below. If you have something else, check with the Editor, as new conversions are being added.

SUN	60 or 150 MB cartridge	ascii only
XEROX VP 2.0, 2.1	5 1/4" floppy only	
WANG		Stand-alone or Alliance
Macintosh	3 1/2" DD disk only	Please furnish a copy in TEXT as well as in your software, as we may not have all the software upgrades
IBM & Compatibles	3 1/2" DD or HD 5 1/2" DD or HD	Please furnish a copy in ascii as well as in your software, as we may not have all the software upgrades

~~FOR OFFICIAL USE ONLY~~



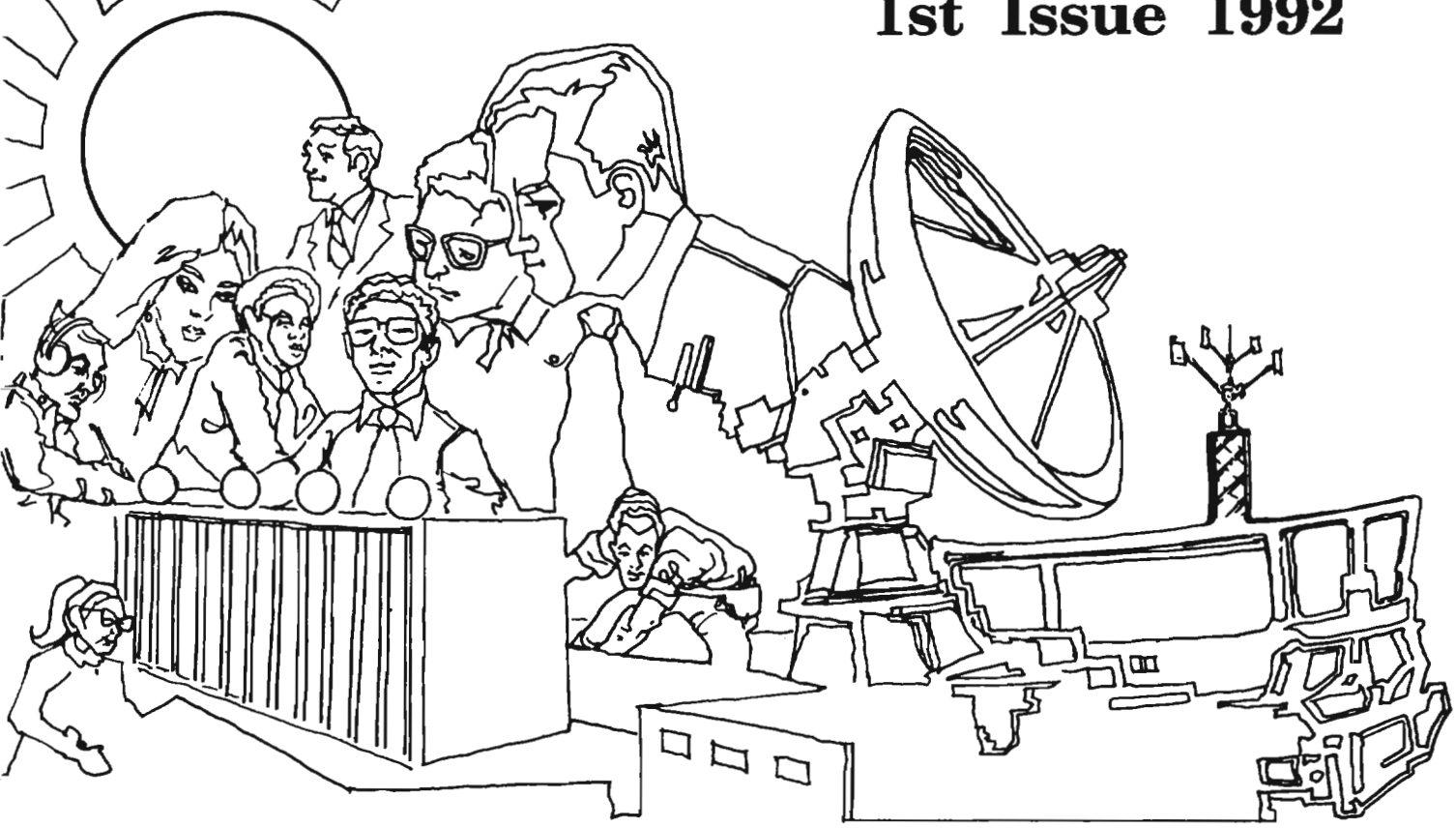
DOCID: 4011851

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

1st Issue 1992



UNDER NEW MANAGEMENT	[redacted]	1
THE GREAT CONVERSATION	[redacted]	2
OPSEC AS A MANAGEMENT TOOL	[redacted]	7
WHERE WAS THE BOGEYMAN?	[redacted]	10
THERE NEVER WAS A BOGEYMAN	Peter D. Molan	13
SANDLOT	[redacted]	15
THE ALMANAC APPROACH	[redacted]	17
FURTHER TO 'THE TEN MOST WANTED'	[redacted]	22
NL: IN MEMORIAM	Doris Miller	22
CLASSIFYING YOUR PERSUM	Richard Sylvester	23
SHELL GAME	[redacted]	24
LETTER		24
SIGINT IN THE NOVELS OF JOHN LE CARRE	[redacted]	25
TECHNICAL LITERATURE REPORT	[redacted]	33
CONFERENCE REPORT: ITCC '91	[redacted] et al.	34
FROM THE PAST		42
EDITORIAL		43
GOLDEN OLDIE		44
TO CONTRIBUTE		45

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~ ~~CLASSIFIED BY NSA/CSSM 123-2~~

Declassified and Approved for Release by NSA and DIA on 10-10-2012 pursuant to E.O. 13526, MDR Case # 54778

~~NOT RELEASABLE TO CONTRACTORS~~

DOCID: 4011851

CRYPTOLOG

Published by P05, Operations Directorate Intelligence Staff

VOL. XIX, No. 1 . . . . . 1st Issue 1992

PUBLISHER . . . . . [redacted]

BOARD OF EDITORS

EDITOR . . . . . [redacted] (963-1103)

Computer Systems . . . . . [redacted] (963-1103)
Cryptanalysis . . . . . [redacted] (963-5311)
Cryptolinguistics . . . . . [redacted] (963-4382)
Information Resources . . . . . [redacted] (963-3258)
Information Science . . . . . [redacted] (963-3456)
Information Security . . . . . [redacted] (968-8013)
Intelligence Community . . . . . [redacted] (933-1139)
Intelligence Reporting . . . . . [redacted] (963-5068)
Language . . . . . [redacted] (963-3057)
Linguistics . . . . . [redacted] (963-4814)
Mathematics . . . . . [redacted] (963-5566)
Puzzles . . . . . [redacted] (963-1601)
Research and Engineering . . . . . [redacted] (961-8362)
Science and Technology . . . . . [redacted] (963-4958)
Special Research . . . . . Vera R. Filby (968-6558)
Traffic Analysis . . . . . [redacted] (963-3369)

Classification Officer . . . . . [redacted] (963-5463)
Bardolph Support . . . . . [redacted] (963-3369)
Clover Support . . . . . [redacted] (963-1103)
Macintosh Support . . . . . [redacted] (961-8362)
Xerox Support . . . . . [redacted] (963-1103)
Illustrators . . . . . [redacted] (963-3360)
. . . . . [redacted] (963-4382)

P.L. 86-36

To submit articles and letters, please see last page

For New Subscription or Change of Address or Name

MAIL name and old and new organizations and building to:

Distribution, CRYPTOLOG, P0541, OPS-1
or
via PLATFORM: cryptlg @ curator
via CLOVER: cryptlg @ bloomfield

Please DO NOT PHONE about your subscription or matters pertaining to distribution

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011851

UNDER NEW MANAGEMENT

[redacted] *P05, Prop.*

(Successor to [redacted] *Publisher Emeritus, Z5, late of P1)*

P.L. 86-36

The recent restructuring of the Directorate of Operations has landed many people in new places. I'm delighted to report that one such change is that [redacted] the editor of CRYPTOLOG, was reassigned to P05. That, in turn, puts me in the position of publisher of CRYPTOLOG.

It's a pleasure to be associated with this friendly journal. With its mix of technical, expository, philosophical, futuristic, argumentative and historical articles—with a light touch here and there—there's always an article or two to engage the reader. While CRYPTOLOG was originally intended to provide a forum for the informal exchange of information by the DDO technical cadres, it has gone well beyond that. Vigorous exchanges have taken place in its pages that have shed as much light as heat, evidence of commitment and concern.

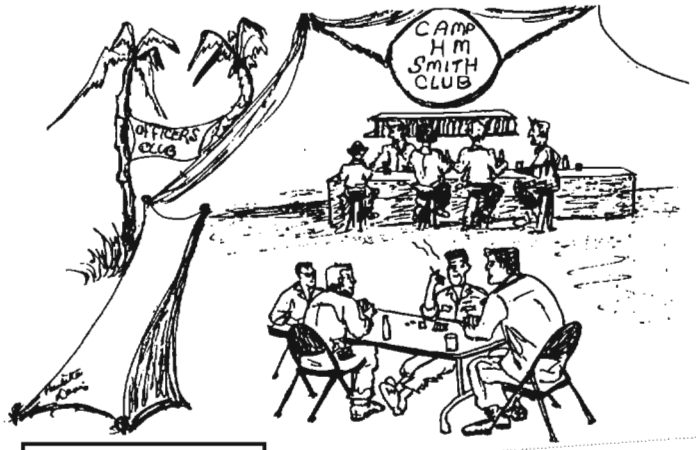
Along with Virginia, I look forward to a still brighter future: publishing more issues, covering more topics, enticing new authors to write. We intend to continue CRYPTOLOG's tradition of challenge and openness. But there's a catch: you are not only the readers, but also the writers. The future of CRYPTOLOG truly depends on you, the readers, to provide the copy, to write the letters, to add that one more piece of information.

I exhort you to lay fingers on keyboards, and put in writing the concerns you talk about around the coffee pot. Don't just talk about them, write them up! You need not limit the scope of your technical exchange to your immediate coworkers. Put your ideas and experiences in CRYPTOLOG and share them with fellow professionals, some of whom you may never have met—some older, some younger. This is ultimately the value of CRYPTOLOG. You can enhance its value by writing for it.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011851

THE GREAT CONVERSATION



P.L. 86-36

Interagency OPSEC Support Staff

This is an extract of a talk delivered at the first National OPSEC Conference, the Maritime Institute, Baltimore, Maryland, April 1990. A complete trascript was published in the Operations Security Monograph Series, under the title, The Great Conversation, *April, 1991.*

The concept that we call "operations security," or OPSEC, reflects ideas and motivations that are as old as the history of human conflict, but as an organized program based on a more or less defined methodology it is a little over two decades old. Its history has not yet been written, and it is still more of an oral tradition than anything else. I've had the opportunity to observe and take part in some of the events that transpired in the two decades that brought the idea from the battlefields of Southeast Asia to the Oval Office. In my short address I'll briefly describe how this concept emerged, how the idea was disseminated beyond Southeast Asia, and how it ultimately was transformed into a national program. While it may not be a children's bedtime story, it's a pretty good yarn.

Three Sundays in the 20th Century

Let me set the stage by telling you what happened on three Sundays in the twentieth century. There is a common thread that ties together the events that occurred on these Sundays, and our being here today is particularly tied to the most recent of these Sundays. The dates of the three Sundays are June 28, 1914; December 7, 1941; and February 6, 1965. Sunday, December 7, 1941, "a day that will live in infamy," was, of course, the date of the Japanese attack on Pearl Harbor and the first day of America's combat involvement in the Second World War. What happened then in 1941 echoed what happened in 1914. No, it wasn't the date when the guns started firing on the Western Front but, in retrospect, they were the first shots of the carnage called World War I. On that Sunday in 1914 in Sarajevo a young Serbian nationalist, Gavrilo Princip, fired two shots and killed the heir to the Austro-Hungarian throne, Archduke Franz Ferdinand, and his wife Sophie. The response of the Austro-Hungarian Government to the assassination led to a train of events that soon engulfed all of Europe. It was the opening bell for round one of a three-round conflict that has consumed most of the twentieth century: World War I, World War II, and the Cold War.

Sunday, the 6th of February 1965 is an outgrowth of the Cold War. And while it is not imbedded in our nation's memory like December 7, 1941, it is no less significant because it was on that date that the longest war in America's history can be said to have begun. In the early morning hours at a town called Pleiku, some two hundred miles north of Saigon, a platoon of Viet Cong troops made a surprise attack on American military personnel at the airfield there. Eight Americans were

~~FOR OFFICIAL USE ONLY~~

killed and 119 wounded. This was a direct assault on Americans whose role in Vietnam up to that time had been purely advisory. This was not the first attack upon American personnel and equipment in the south, but it was the first attack that resulted in a continuing American military response. (I use the word "continuing" to distinguish our response at this time from the "quid pro quo" response to the Gulf of Tonkin incident six months earlier.) With President Johnson's approval, a campaign of fighter-bomber strikes against military targets in the North Vietnam was begun. Known as "Rolling Thunder," these air operations played a unique role in the emergence of OPSEC as a concept and as a program.

The first Rolling Thunder mission was flown on February 11, 1965 four days after the attack at Pleiku and one day after another bloody attack on American personnel at Qui Nhon. Our war had begun, and I do wonder whether we would all be here today if Gavrilo Princip had missed on that Sunday in 1914. We can only speculate idly about this.

As the Rolling Thunder missions continued to be flown in the weeks and months that followed that Sunday in early 1965, they were accompanied by normal military concern over retaining the element of surprise. This concern gave rise to a Joint Chiefs of Staff-initiated undertaking to identify any actual or possible sources that the enemy might exploit to derive forewarning or foreknowledge of our intentions. Such identification could provide a rational basis for the development of countermeasures. This undertaking, of course, was the genesis of OPSEC and began a train of events which has finally brought all of us here today.

Origins of the Term "Operations Security"

Now let me jump ahead in time some two years to the spring of 1967 and shift the scene to the bar in the Officers' Club at Camp H.M. Smith, Hawaii, the site of the Headquarters of Admiral U.S. Grant Sharp, Commander-in-Chief, Pacific (CINCPAC). Four of my associates were exercising the dice cup and discussing subjects that seize men's minds at such times. They also addressed the question, "What are we going to call ourselves?" They were, in fact, continuing an extended discussion about naming a new branch to which they would be assigned that was going to be established within the Operations Directorate of the CINCPAC staff. "Purple Dragon," the name that had thus far been applied to their activities, was considered inappropriate for a staff element. Respectable functional titles were the rule of the day. "Purple Dragon," in fact, was a rather exotic, unclassified nickname from a Joint Chiefs of Staff repertoire that was applied to the one-time "survey" that they and a number of other persons had just completed. The Purple Dragon survey addressed retaining the element of surprise vis-a-vis the Rolling Thunder missions (which provides our linkage to the events on that Sunday in 1965 of which I've already spoken), and two other air operations that were subsequently begun in southeast Asia, the B-52 "Arc Light" operations, and unmanned drone operations.

What do you call a new organization whose mission would be to continue to perform Purple Dragon-type surveys, i.e. an activity to identify actual or probable sources of enemy advance knowledge of our intentions? There was no problem in agreeing on the inclusion of the term "operations," since military operations was what it was all about. But then what would follow? The most appropriate candidates were "Operations Analysis," "Operations Assessment," and "Operations Effectiveness." Each had its merits. The Purple Dragon methodology was analytic; and yes, it did involve an assessment to determine the extent to which we were denying critical information to the enemy; and, ultimately, it was concerned with improving our operational effectiveness.

But neither "Operations Analysis" nor "Operations Assessment" sounded unique among the welter of titles within the Department of Defense, and "Operations Effectiveness" (which, to a man, we considered the most accurate term) just didn't seem to grab one's imagination. But worse than that, the language of the Department of Defense is not English. It is a strange mixture

of familiar sounds interspersed with other sounds that are called acronyms. And was the Department of Defense ready for acronyms that would be derived from Operations Assessment or Operations Analysis? Thus these terms were rejected. What about "Operations Security?" It makes a nifty acronym that can be stated clearly by even the most fuzzy-tongued speaker. But where did "security" come from? Was this choice due to a profound and searching intellectual discourse on the part of the conversants at the bar in the Camp H.M. Smith Officers' Club? Hardly. Between rolls of the dice for the next round of drinks, the sole civilian in the crew thought it would be a neat idea if the name of his employer was included in the title of this new branch on the CINCPAC Staff. His employer was the National Security Agency, and the middle name of his employer followed nicely after "operations." Indeed, it did make a rather good acronym, but [redacted] was motivated less by the appropriateness of the title than by the fact that inclusion of "security" would increase the chance that he, a communications security specialist, would be assigned to it. At some time in the foggy discourse, the prospective chief of the new branch, Air Force Colonel Jim Chance, grunted approvingly.

P.L. 86-36

And thus it came to pass that "Operations Security" was born at the bar in a saloon in Hawaii. As for [redacted] he was right. Characterizing this branch as a "security" organization clinched his assignment to it.

For myself, [redacted] and the rest of the men who were assigned to this new branch and who applied the OPSEC survey concept to combat operations in Southeast Asia, the term "security" was a bit wide of the mark. Our thought processes were geared to terms such as "effectiveness," "surprise," "indicators," "foreknowledge," and "forewarning," and most of the time we used "Purple Dragon" in lieu of "Operations Security." The cover for the regular OPSEC reports that we produced, for example, was emblazoned with a rather striking illustration of a dragon and the words "Purple Dragon." But in retrospect, opting for "Operations Security" was a good decision for reasons that were not foreseen by the stalwart few.

In my opinion, OPSEC by any other name would not have lasted beyond the Vietnam War. We live in a world of symbols, "sound bites," and executive summaries, and the implications of a title can have as great an impact as lengthy, conceptual discourses. The term itself, "Operations Security," has probably had as much, if not more, of an impact than any number of written and verbal explanations of the concept it entitles. It has both a built-in righteousness (who in their right mind could be against such a thing?), that it is something different from plain old "security," and an intriguing absence of complete clarity (I think I know what you mean, but you'd better explain). I doubt whether "Operations Assessment," for example, would have seized the imagination of civilian executive-level decision makers during the years in which OPSEC was transformed into a national program.

And so in the course of a rambling discussion in April 1967, under the most casual of circumstances, a proper noun was agreed upon. It is at best a minor footnote to an episode of the Vietnam War, let alone the cataclysmic events of this century. But it has had an effect upon all of us who are here today. Ironically, a few steps from the bar in the Camp H.M. Smith Officers' Club is the veranda from which you can gaze upon Pearl Harbor in the distance, and if you listen closely, you can almost hear the echoes of the infamous Sunday in 1941.

Disseminating the Idea: the Vietnam Years

The formal establishment of the CINCPAC OPSEC branch occurred in June 1967. For the next five years this small organization conducted some sixty or so OPSEC surveys. Most of these were of combat operations in Southeast Asia, but a number of them addressed operations elsewhere that continue to this day. During the years 1967 through 1972, OPSEC was a concept that was primarily applied by the 17 members of the CINCPAC OPSEC branch (who, not surprisingly, spent most of their time in Southeast Asia), a few officers assigned to the

DOCID: 4011851

Military Assistance Command in Vietnam, and a sprinkling of persons assigned to some other major commands. The major focus was, of course, on combat operations.

Throughout the war years, the CINCPAC OPSEC branch distributed a series of "Purple Dragon" reports which described the surveys, their findings, and recommendations. To the credit of the CINCPAC himself, these reports were not subject to the normal staffing process. They were essentially distributed as we wrote them. Although classified, they contributed to the dissemination of the OPSEC concept. In addition, representatives of the branch regularly briefed the Joint Chiefs and other high-ranking military and civilian commanders and managers in the Washington area. We did this two to four times per year. In my own opinion, the regular briefings and across-the-table conversations we had with the Joint Chiefs themselves sustained that vital ingredient of program success: command emphasis. I had a feeling that they looked upon us as a source of information that was unfiltered, unfettered, and unaltered by the normal staffing process.

The first formal effort to disseminate the OPSEC concept beyond Southeast Asia and the Pacific command occurred in 1968. Colonel Jim Chance, the first Chief of the CINPAC OPSEC branch, was subsequently assigned to a newly created OPSEC billet within the Operations Directorate of the Joint Chiefs of Staff. Through his efforts and and the efforts of others, the first Worldwide OPSEC Conference was held at Arlington Hall in the Washington DC area in April 1968, less than a year after the establishment of the CINCPAC OPSEC branch. Attended by military and civilian representatives from throughout the Department of Defense and one or two other agencies, the OPSEC concept was introduced to a broad spectrum of representatives.

At this conference one of my fellow Navy officers, Lt. Commander Bob Johnson, delivered a briefing on OPSEC methodology. In a few words he expressed what I believe is a fundamental precept of OPSEC: "We put ourselves in the position of the adversary and study our operations step by step, from conception through execution to completion and beyond." To this I would add, that whenever possible we correlated this chronological, step-by-step information about our operations with whatever we knew or could reasonably postulate about what the enemy was concurrently doing that could reduce the effectiveness of our operations. Such correlation provided unique insights and a means to isolate what we referred to as "indicators."

Post-Vietnam Loss of Focus

After the U.S. combat role in Vietnam ended in the spring of 1973, the CINCPAC OPSEC branch dwindled in size, eventually being reduced to a single officer and an NSA representative. OPSEC had entered the doldrums. Without a war, OPSEC had lost its focus. But the OPSEC process that had been devised was actually applicable to any competitive or adversarial situation, whether in peace or war, or in the civil or commercial environment. Now it had to be applied, interpreted, and explained in ways that would make this evident. It had to be divorced from the notion that OPSEC was an exclusively Vietnam War activity. What was originally conceived as a pragmatic response to relatively short-term combat operations in which the measures of effectiveness were generally apparent, e.g., loss rates, bomb damage assessments, now had to be adapted to longer term, non-combat operations in which the measures of effectiveness were not readily apparent. At the same time, the omnipresent problem arising from its name, that OPSEC was nothing more than a conglomeration of security programs, had to be overcome. Not without difficulty this is what was accomplished in the post-Vietnam years of the 1970s. The main vehicles of this accomplishment, I believe were:

- Joint Chiefs of Staff support and establishment of programs in the military services;
- adoption of the OPSEC process to peacetime, non-military activities by NSA;
- the "Great Conversation."

Role of the Joint Chiefs of Staff

After the first JCS-sponsored OPSEC Conference in 1968, some six years passed before another

~~FOR OFFICIAL USE ONLY~~

such conference. But beginning in 1974 the JCS presented a series of annual two- and three-day "Worldwide OPSEC Conferences." With the exception of two years, a conference was held each year through 1988.

The JCS conferences, attended by up to one hundred representatives from throughout the government, were valuable forums in which ideas were exchanged and the challenge of adapting a combat-oriented concept to the circumstances of a peacetime environment addressed. At the same time in the latter 1970s OPSEC programs, at least in name, were being established within the military service and the Unified and Specified Commands, accompanied by implementing directives and regulations. Although there was no unanimity of agreement as to what OPSEC was or ought to be, and even though the resources dedicated to OPSEC were usually meager, the important thing was that OPSEC was afforded enough emphasis to keep the idea alive. By the end of the decade the military services and the Unified and Specified Commands were conducting their own OPSEC surveys.

Role of NSA: The Great Conversation

In addition to the JCS Conferences and military programs, the corporate knowledge from the OPSEC experience in Vietnam was being assembled at the National Security Agency, more by accident than design. A few persons who had applied and developed the concept in Southeast Asia were already working for or were hired by the Agency in the early 1970s. Further, NSA continued to fill, without a break, its single billet in the CINCPAC OPSEC branch and became its corporate memory. Through these individuals NSA became the purveyor of the original concept and vital element in adapting it to peacetime military and non-military operations and activities. In due course this was conveyed to other departments and agencies. But this was not without difficulty, since there was the perennial problem arising from the name "operations security." Some chose to emphasize "operations," while others chose to emphasize "security." A lot depended on the interpreter's background and area of interest. However, the NSA experience, in turn, was informally conveyed to others in the Washington community and contributed to a phenomenon through which ideas rise and fall. I allude to the phenomenon which is often blithely termed the "cocktail circuit," but which I would rather, and believe more appropriately, refer to as a "great conversation."

CONCLUSION

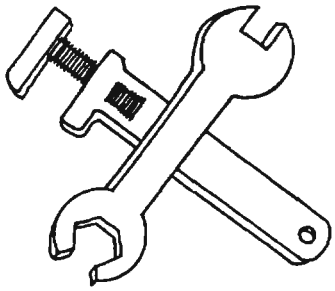
We're here today as a result of an initiative by the Interagency OPSEC Support Staff. This staff, in turn, was established as a result of national policy set forth in January 1988. But the policy directive was the result of events and circumstances which transpired since the advent of "Purple Dragon" almost a quarter of a century ago and the emergence of what I have characterized as a "great conversation" about OPSEC. All of us are participants in this conversation during and after this conference. What I've briefly covered here can hopefully add an element of historical perspective to this conversation.

In conclusion I would add that the story of OPSEC is a story about the durability of a good idea that was, at one time, nothing more than a pragmatic response to circumstances relating to combat operations. But in retrospect, the concept that we call "operations security" did not survive and become a national program because it has a catchy acronym, or because it was skillfully proselytized, or because of the challenges that face us in the Information Age, or for any number of other reasons; rather, I would submit, OPSEC lasted beyond the Vietnam War and became a national program because of two primary reasons: one, very simply, it's a good idea. But that's not enough in a world of competing ideas and interests. And this leads to the second reason. I've alluded to it throughout my talk without actually spelling it out. OPSEC endured and became a national program because it has had top-down support. In whatever agency or department of the government, it has become a viable program only when it has had top management backing, and when this is lacking it has not succeeded. If there are any lessons that are to be learned from the history of OPSEC, this is certainly one of them.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011851

OPSEC as a Management Tool



P.L. 86-36

[redacted] A04

(U) Operations Security (OPSEC) is not a security program intended to protect **only** classified information. It really is a business management tool for **controlling** systems and information, classified or not, that expose vital Agency operations to unauthorized persons.

~~(FOUO)~~ Nothing about OPSEC procedures themselves is unique to SIGINT, intelligence in general, or even Government operations. Of course, the secrets NSA protects, and some of the means used to protect them, are specifically SIGINT-oriented, but that's because SIGINT is the business NSA is managing. The same principles apply whether the secrets being protected are:

- (U) Plans for a surprise birthday party;
- (U) Christmas presents for a child;
- (U) An impending acquisition, new product line, or bankruptcy by a company;
- (U) A country's plans to go to war, and fighting the war;
- ~~(FOUO)~~ Intelligence sources, methods, and results.

~~(FOUO)~~ There are many ways to use OPSEC, and there are many ways to penetrate it. Spouses infer plans for surprise parties from demands to be home by a certain time. Children learn where to look for hidden presents. Civic associations use various means to ferret out and contest the plans of developers. Drug runners monitor law enforcement operations to evade the law. All of these are OPSEC penetrations, just as careless management of SIGINT can make possible the penetration of NSA secrets.

(U) The essence of OPSEC is expressed in the Native American prayer, "Oh Great Spirit, before I criticize my neighbor, let me walk a mile in his moccasins." OPSEC is about managers placing themselves in the moccasins of others. It's about using the perspective of the person one wants to keep uninformed to identify ways that that person can use to help gain information the manager wishes to keep secret. And it's about taking cost-effective countermeasures to defeat such efforts.

~~(FOUO)~~ This challenge goes beyond the traditional security procedures so respected at NSA. In our business, we're used to protecting "classified" information. But people desiring that information don't care whether we consider information "classified"; they consider only whether it might be useful to them. Even the new Government category "unclassified but sensitive" doesn't completely encompass what these people might find useful for their purposes.

~~(FOUO)~~ For OPSEC purposes, managers ought to consider the terms "no need to know" and "unauthorized person" interchangeable. Sometimes people think of only "hostile intelligence services" or terrorists as adversaries to whom we must deny our secrets. NSA managers also should think of the following to be denied access, in approximately descending order of benignity and increasing order of access to sensitive data and methods:

- ~~(FOUO)~~ People who for some reason want to prevent the Government from doing intelligence work;
- (U) News media and authors seeking an exclusive story;

• ~~(C-CCO)~~ Intelligence users (who often insist upon information about sources and methods which they don't need);

• ~~(FOUO)~~ Foreign collaborating services (especially Third Parties) who aren't participating in the specific project; or even

• ~~(FOUO)~~ NSA Green Badgers without a need to know (for example, with compartmented projects);

~~(FOUO)~~ The OPSEC process works best as a project-specific, cost-risk analysis integral to management thinking. It needs to be project-specific, because each project has its own operational and security characteristics. It begins with defining as specifically as possible:

• ~~(FOUO)~~ What "core secrets" must be protected if a project is to meet its mission;

• ~~(FOUO)~~ Who the "adversaries" are for that project (that is, who outside the project might be trying to learn its secrets);

• ~~(FOUO)~~ What capabilities these adversaries have to gain access to and use the information or equipment to be protected;

• ~~(FOUO)~~ What there is about the management of the project that makes it vulnerable to those capabilities; and

• ~~(FOUO)~~ What, if anything, can be done to reduce those vulnerabilities.

(U) Managers use information like this to decide how to deal with risks. Sometimes, they decide that eliminating a specific vulnerability is impossible without cancelling the project entirely. Sometimes they decide that certain vulnerabilities are too low a risk to justify the cost and effort to eliminate them. Sometimes they decide that steps to remove a risk would have the opposite effect of calling attention to it, and the best thing to do is nothing. And sometimes they make changes that remove the vulnerability, or at least reduce it to acceptable levels of risk.

~~(FOUO)~~ Project managers sometimes want to consult outside advisors to help them identify system vulnerabilities and threats. NSA has in place a network of OPSEC coordinators to provide help of this kind. This is when an OPSEC Survey is a useful tool. A team is formed of people knowledgeable in the technology or kind of operation to be studied, but not involved in managing that project. The team applies its experience to study the project the way the adversary would study it, and report to the project's managers the weaknesses they find, as well as logical ways these weaknesses can be removed. (They become, in effect, a "Red Team," to compare their findings with those of the "Blue Team" comprising the project management.) The survey team is duty-bound to treat the study results as the property of the regular management team, just as a contractor would do if hired commercially to do the survey.

(U) Like all management processes, OPSEC requires follow-through. An ongoing program has a continual stream of management decisions. Some degree of cost-risk consideration should be a factor in each of these decisions. OPSEC is at its functional best when this happens.

DIRECTIVES

(U) In January, 1988, President Reagan signed National Security Decision Directive (NSDD) 298, which designated NSA as the executive agency for providing Government-wide training in OPSEC. In response, NSA formed a Directorate of OPSEC (D2) and also the Interagency OPSEC Support Staff (IOSS), which has offices in Greenbelt, MD. The IOSS has staff officers from several government agencies. It provides a range of OPSEC awareness and assistance programs, including publication of a series of monographs and publications. Those who want to know more about including OPSEC in their management thinking are urged to get copies of these monographs from their OPSEC coordinators, the OPSEC Directorate, or the IOSS.

~~(FOUO)~~ An NSACSS Directive (No. 120-01) provides OPSEC procedures and instructions. NSACSS Circular 25-5 requires that Systems Coordination Papers (SCPs) and Program Baseline Summaries (PBSs) include discussion of OPSEC planning for new NSA programs.

TRAINING

~~(FOUO)~~ The National Cryptologic School's Management Faculty (E9) offers a one-day orientation class (OP-200) in OPSEC. There also are OPSEC modules in some other Cryptology courses. The faculty there welcomes critiques of these courses and suggestions for others.

SOME EXAMPLES OF OPSEC VULNERABILITIES

(U) *The launch profile of spacecraft.* Media reporters often deduce from these profiles when intelligence satellites are launched. This is an OPSEC vulnerability that cannot be removed and at the same time, ensure that the the satellite is put into the right orbit.

(U) *The azimuth and elevation of a satellite antenna.* An alert person armed with a Boy Scout compass can measure these and learn toward what geo-stationary satellite the antenna is pointed.

P.L. 86-36

(U) *Parking lot analysis.* What cars are parked in the reserved spaces of senior executives can reveal which executives are away from the office. (Some executives blur this by letting their secretaries use their spaces when the executive will be absent.)

[redacted]

EO 1.4.(c)

[redacted]

[redacted]

[redacted]

(U) It should be clear that good OPSEC is not some elaborate or revolutionary new management concept. It is merely an orderly and common-sense way to keep one step ahead of opponents in managing the business of SIGINT.

BOOKBREAKERS FORUM

on

MACHINE AIDS

If you are working on codes, programming for codes, or managing a code problem, join the Forum and exchange methods and techniques with others doing the same type of work.

Write your Name, Organization, and Building on a piece of paper and send it to the Chairman:

[redacted]

2509
North.

P.L. 86-36

Please re-register even if you are an old hand, for the reorganization has played havoc with the mailing list.

~~FOUO~~

DOCID: 4011851

P.L. 86-36

[redacted] E34

WHERE WAS THE BOGEYMAN?

An Analysis of the Response of Islamic Fundamentalist Groups to the Persian Gulf Crisis

(U) Who could forget those chilling scenes in late 1979 when Iranian "students" took over the U.S. Embassy in Tehran? Hordes of Muslims marched in the streets chanting "Death to the Great Satan", burned effigies of President Carter and Uncle Sam and exhorted fellow Muslims to rise up against the West. These pictures, repeated over and over throughout the entire Iranian hostage crisis, were burned into the minds of Americans and other Westerners. For years after the hostage crisis, the foreign policy of the United States and other Western countries on the Middle East seemed to be based upon the premise that some new situation or crisis could again ignite the fundamentalists' fervor and unleash a "bogeyman"--mobs of sword-wielding Muslims sweeping down on the non-believers as punishment for their transgressions against Islam.

~~(TSC)~~ Just prior to the invasion of Kuwait in mid-July 1990, [redacted] in Iraq Saddam Husayn called for Kuwait and other Gulf oil-producing countries to relent on their over-production of oil quotas or face Iraqi retribution. That speech set in motion events that tested the resolve of not only the Secretariat but of all Islamic Fundamentalists throughout the Middle East.

(U) Saddam Husayn's occupation of Kuwait in the summer of 1990 precipitated what many thought would be the event that would unleash the fury of Islamic fundamentalism. Shortly after the occupation, he issued a call to all Muslims for Jihad (Holy War) against the United States and other Western countries who had come to the aid of Saudi Arabia. But according to Islamic law, Husayn had no legal basis for his call for Jihad. His use of the term Jihad was probably intended to bolster the morale of the Iraqi people in general and the Iraqi military in particular. The fact that he could not legally call for Jihad suggests that Husayn's strategy may have been to play on the fears of the U.S. and other Western countries.

(U) Islamic law (Shari'a) sets out the conditions under which Jihad can be invoked. As law, the Shari'a is subject to interpretation and the various sects of Islam have each chosen to define Jihad in their own way. The largest sect of Islam, the Sunni, has adopted the most conservative interpretation, in which Jihad includes both temporal and spiritual efforts to defend Islam. In fact, the Sunnis have identified four types of Jihad: of the heart, the tongue, the pen and the sword. The first three of these address challenges to Islamic values, including a personal moral struggle of the soul. The fourth refers to a challenge from a non-Muslim source, such as that posed by Operation Desert Storm. The Shi'ia sect of Islam, the most radical, tends to have a more militant interpretation of Jihad. Their concept of Jihad

EO 1.4.(c)

DOCID: 4011851

embraces the idea of martyrdom. The Shi'ias have even extended their definition of Jihad to include the Sunnis, whom they regard as heretics who must be brought back to Islam.

(U) Technically in today's Islamic world, no single Muslim leader can declare Jihad. The schism created by the secession struggles after Mohammad's death has, over the many centuries of Islamic history, eroded the legal and religious authority to declare Jihad for all sects of Islam. Islamic jurists agree, however, that Jihad against an enemy threatening the very existence of Islam itself remains a collective obligation of the entire Muslim community.

(U) Saddam hoped, in addition to bolstering the morale at home and among his troops, that his call for Jihad would have an emotional impact among all Arabs and galvanize support among Islamic fundamentalist groups for his struggle against the coalition forces. Indeed, during the early period following the Iraqi occupation of Kuwait, some groups heeded the call, but not in the way that Saddam Husayn had hoped.

~~(TSC)~~ The evidence suggested that these groups were intent on defending the honor of Islam vocally or intellectually rather than taking up a military or terrorist option. Indeed, as the occupation wore on, it was clear that the majority of fundamentalist groups did not really care about Husayn's religious beliefs, but were intent upon their own nationalist goals and attempted to use the Persian Gulf crisis as a front. In general, the Persian Gulf crisis appeared to provide various fundamentalist groups with a perceived legitimate reason to stir up dissent in their own backyards. Diplomatic observers in many countries in the region saw the popular dissent surrounding the crisis as resulting from pressure from local fundamentalist groups upon their governments.

~~(TSC)~~ Arab countries supporting the coalition, especially Egypt and Saudi Arabia, expected fervent reactions from indigenous fundamentalist groups. As it turned out, there were demonstrations and protests, but nowhere close to the number expected or predicted. The Muslim Brotherhood in Egypt staged protests in mid-September and early October 1990, but even these revealed inconsistencies in the fundamentalists' objectives. Several of the demonstrations decried Husayn's annexation of Kuwait as the 19th province of Iraq, but at the same time protested the U.S. and Egyptian involvement in the crisis. It soon became apparent that various Egyptian social and political issues were behind many of these protests, once again indicating that the crisis was being used as a springboard for local fundamentalist objectives. Saudi Arabian fundamentalists, on the other hand, declared their willingness to actively oppose Saddam Husayn and volunteered to defend Saudi Arabia's holy cities of Mecca and Medina against aggression. Morocco, another Arab country that was part of the coalition, was also the scene of some fundamentalist protests; these the local diplomatic observers dismissed as minor, unplanned incidents.

~~(TSC)~~ Elsewhere in North Africa, both Algeria and Tunisia were more overt in their support of Husayn's actions. But even there, the response to the crisis by local fundamentalist groups was not overwhelming. The growing fundamentalist movement in Algeria, the Islamic Salvation Front (FIS), swayed the government to announce its support for Husayn's invasion of Kuwait. But the Algerian government stopped short of supporting Iraq's annexation of Kuwait. This indication of the government's ambivalence in the crisis was attributed to the fact that various political and social groups in the country, including the fundamentalists, were all seen as using the crisis to gain power for themselves. Diplomatic observers even hinted that the FIS, the strongest of the Algerian fundamentalist groups, was using the crisis to cover up its poor performance at home. In

DOCID: 4011851

Tunisia, however, the struggle was along more classic lines. The rift within fundamentalist groups appeared to be between the leaders, who leaned toward supporting Kuwait and Saudi Arabia, and the younger members of the groups, who supported Iraq.

~~(TSC)~~ As the birthplace of modern Islamic fundamentalism, Iran might reasonably have been expected to play a leading role throughout the Islamic world with respect to the responses of fundamentalists against Operation Desert Storm. To be sure, Iran played a role, but it could not be characterized as a leading one; it adopted a wait-and-see attitude. This was consistent with Iran's overall policy during the war, which was one of relative neutrality towards both sides in the conflict. Several smaller fundamentalist groups, notably in North Africa and the Sudan, took pains to seek Iranian guidance and advice before publicly responding to the crisis. This was probably an effort by these relatively minor groups to acknowledge Iran's leading position in the fundamentalist world and achieve some measure of credibility in their own countries by being perceived as having Iranian support for their actions. The Maghreb Islamic Movement in North Africa even sought Iran's view on the legality, under Shari'a, of sending volunteers to fight alongside Iraqi forces.

~~(TSC)~~ A more universal fundamentalist response to the situation in the Gulf was noted in Jordan, which might have been expected in view of King Hussein's overt support for Saddam Husayn. Early in the crisis, the Jordanian Muslim Brotherhood attempted, unsuccessfully, to mobilize the support of fundamentalist groups in Egypt, Syria, Iraq, and several other Islamic countries. Muslim Brotherhood members of the Jordanian Parliament were outspoken and vocal in their support for Husayn, taking the view that the larger issue was one of a battle between Islam and the "infidels".

~~(TSC)~~ The regional experts who foresaw that some situation or event would unleash the full fury of Islamic fundamentalism upon the offending foreign power(s) did not find it in Desert Storm, which pitted not only Muslim against "infidel", but also Muslim against Muslim. The predicted fury of the Islamic uprising turned out to be just a handful of localized events that fizzled out with no serious impact, not the all-encompassing force some had predicted.

(U) Does the "bogeyman" exist at all? It's not clear, as there were ambiguous circumstances in Desert Storm that cloud the issue. It was not clearly an infidel versus Muslim affair, and many Muslims recognized the invalidity of Husayn's actions. Were there to be another situation in which the US or other Western power attempted to unilaterally insert itself into the internal affairs of an Arab nation without UN sanction, it could be a different story. Under *shari'a*, this could be interpreted as threatening the very existence of Islam and make it easier for Muslims to act together, and a call for jihad might then be effective.

~~(TSC)~~ The Gulf crisis did not produce a region-wide, cohesive Islamic fundamentalist response. Consistent with the history of politics in the region, fundamentalists and their organizations used the crisis as a springboard for their own particular political or nationalistic agendas. Even Saddam Husayn's call for Jihad failed to coalesce the various personalities or groups.

END NOTE

~~(C)~~ [redacted] provided an excellent treatment of the subject of Jihad in relation to Operation Desert Storm in DIA Defense Intelligence Memorandum DIM 32-91, January 1991.

OGA

DOCID: 4011851

There Never Was a Bogeyman

a Reply

Peter D. Molan, P04/SLA

P.L. 86-36

When [redacted] gave me a pre-publication copy of his article, I read it with the sense of satisfaction that one feels when one sees that the views of a respected colleague are in accord with one' own--until I reached the conclusions. Then I was disturbed.

It was clear to me that the whole thrust of Ron's article had been to debunk the threat of a wide-spread rally to Saddam Husayn's call for a *jihâd,* a "Holy War," against America in the run-up to Desert Storm. And yet, Ron's conclusion--despite all the evidence which he himself had mustered to show that the fear had been overblown--was that we must be on the alert to that very danger in the future. I believe that Ron's conclusion plays into the hands of a troubling tendency which is more and more apparent in American thinking.

As *Washington Post* commentator Jim Hoagland noted on 6 February '92, we seem to have "an urge to identify Islam as an inherently anti-democratic force that is America's new global enemy now that the Cold War is over." The manifestations of that urge are rife. The most egregious example I know of appears in an article by *Newsweek's* chief diplomatic correspondent, John Walcott. It dates back to 15 July 1985, but is a common enough, if particularly virulent, statement of the urge:

"Fighting terrorism is not unlike fighting *malaria.* It is not enough to swat the mosquitoes; it is necessary to drain the *swamps* where they breed ... (but) ill-considered or poorly executed attacks on suspected terrorists (in Beirut) may only succeed in replacing today's Republic of Nihilism with something even more dangerous: the Islamic Republic of Lebanon... Preventing such a vulture from hatching should be the goal of the United States..." (my italics).

More recently, Rowland Evans and Robert Novak in a *Post* column of 2 March '92, expressed their fear of a "dangerous fundamentalist *tide*" arising from Iran and sweeping over Central Asia (my italics).

Where does the disgust and loathing of Islam which are manifest in such statements come from? Are they really rooted in, and justified by, the harsh punishments specified by Islamic law for theft, fornication, and apostacy as occasionally applied in three or four countries? I doubt it. Such loathing is generally rooted in fear.

That fear seems to be linked to the dreaded word, jihâd--"Holy War"--itself. The word conjures up images, precisely, of Evans and Novak's "tide"--of religious fanaticism--arising out of Walcott's "swamp"--of some uncontrollable primitivism--to overwhelm all that is progressive and good--us--and then pick over our bones like some "vulture"

But, that fear tells us more about our own subliminal terrors than it does about any real "Islamic threat." That fear reflects the primal, childish dread of the bogeyman and not a rational assessment of risk.

Ron has already pointed out the major arguments as to why a wide-spread coalition of Muslims aligned against Western interests is

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011851

unlikely to occur. Let me only add an historical observation: ***there never has been a jihâd!***

Muslim leaders always "call for" "Holy War" against the "infidels" when they are in trouble, of course. Every one who has done so, however, has gotten the same reaction that Saddam Husayn did--a brief flurry of attention in certain Muslim circles and then nothing.

The two most famous calls for jihâd came from Saladin, during his struggle against the Crusaders, and from 'Abdul-Hamid II, during World War I. During the Crusades, the Caliph in Baghdad barely deigned to respond to Saladin's appeals for help. Other Muslim Amirs continued lucrative trading arrangements with the Venetian and Genoese merchants who were supplying the Crusaders, and Sultans concluded treaties with Christian Princes against Saladin whenever it suited their purposes. Saladin did succeed in checking the Crusading enterprise, of course, but that success had nothing to do with "jihâd."

When 'Abdul-Hamid called for a Holy War, the Muslim soldiery of the British colonial armies ignored him. The Arabs of North Africa and the Najd remained quiet, and the Arabs of the Hijâz revolted against him. That Saddam would fare no better than his predecessors was entirely predictable.

Posing the question of how serious Saddam's call for a jihâd might be was not inappropriate at the time, of course, but differences of language, sect, nationality, and local history militate against a generalized Islamic threat to the "West" so strongly as to make any great concern about a jihâd silly. There *is* another, *real* danger, of course.

Hoagland describes that danger in these words: "... America now has the burden, and opportunity, of making complex foreign policy choices instead of replacing one set of blinders with another..." To make those choices, American policy makers will have to receive accurate information, from their analysts, on the realities of a world in which more and more people, Christians, Jews, and Hindus, as well as Muslims--be it noted--seem to be turning to religion as a solution to their problems.

As Hoagland points out, "Replacing blind anti-communism abroad with an equally crude anti-Islamic doctrine would be self-defeating." Blind anti-Islamism will prove to be "self-defeating" for two reasons. As an analyst, I believe that the more important of those two reasons is that such blind fears can only distort our abilities to render accurate analysis.

The second reason is that mindless hostility can only provoke a hostile response from those against whom it is directed. Such hostility will scarcely produce a jihâd, but it will complicate relations. When the American Muslim Louis Farakhan described Judaism as "a gutter religion" and White people as "devils" he was loudly, and properly, condemned for anti-Semitism and racism. How do we expect Muslims to respond to those who characterize their religion as a "dangerous tide" or a "malarial swamp" or a "vulture"? How do we expect them to respond to those who do not condemn such rhetoric and the primitive terrors in which it is rooted?

This is not to say that there can be no criticism of Muslim thought. One may, on the grounds of Islamic history as much as our knowledge of human psychology, condemn as absurd the assertion by 'Abdul-Halim Mahmud, the former Shaykh al-Azhar, that "Application of the *hudûd* punishments is the only cure for the spread of the crime which we see today. Stealing will be ended once and for all if we cut off the hand of one thief." But, both our analysis and our criticism must not, for our own sakes as well as for the sake of our relations with our Muslim neighbors, descend to the realm of the irrational fear and distorted thinking manifest in a grossly exaggerated concern over "jihâd."

Note: **NEW** mailing address for

CRYPTOLOG
P0541
OPS-1

NEW e-mail:
cryptlg @ curator

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

~~SECRET~~

SANDLOT

[redacted]

Networks

P.L. 86-36
EO 1.4.(c)

P.L. 86-36

[redacted] T336

~~(C)~~ The SANDLOT program was originally envisioned as a more-or-less turnkey analytic support system. [redacted]

Today SANDLOT is not a turnkey system; rather, it is a flexible, modifiable, tailorable system, one that allows users to dynamically select software alternatives according to individual preferences. [redacted]

P.L. 86-36

A Word on Terminology

~~(C)~~ SANDTERM is software that runs in a user's workstation and facilitates connectivity and communication. [redacted]

DOS Compatibility

(U) Although SANDLOT itself is firmly wedded to the Unix operating system, workstation technology and commercial software have evolved to a state where most workstations permit users to freely traverse between the entirely commercial DOS software applications world and the Unix connectivity-oriented environment.

Editors

(U) SANDLOT supports the in-house developed [redacted] which is used in [redacted]

P.L. 86-36

DOCID: 4011851
P.L. 86-36

because of its superior performance, the choice is up to the individual analyst.

Database Systems

(U) SANDLOT permits the user to select from among a variety of commercial Unix Database Management Systems such as INGRESS, Sybase, and BRS Search; and also supports the in-house

Electronic Mail

(U) User-friendly electronic mail has transformed the way business is conducted at the Agency.

Desktop Publishing

(U) SANDLOT supports both the INTERLEAF and FRAMEMAKER commercial desktop publishing systems.

Applications

(U) By observing a few simple rules and using shared code libraries, applications developers all over DDO have been able to produce software

There are two substantial benefits to this approach:

- the applications programmer delivers software to the user with the same user interface — the same look and feel — as all his other software;
- he has removed substantial risk as to the portability of his code when new hardware is purchased.

Sharing Resources

(U) With the deployment of large numbers of Local Area Networks (LANs) under the SANDLOT program it has been possible to widely share costly resources such as letter-quality printers and color plotters amongst large user populations.

Software Standards

(U) By adopting the toolkit approach to SANDLOT, significant time and money was saved in the acquisition process. Additionally, customer satisfaction is higher because permitting substantial choice in tool selection and development enhances the customer's feeling of "ownership" of the system. Certain software standards have been most important in achieving this goal:

- Unix, primarily AT&T System V Unix, but with some difficulty SunOS as well;
- X11 — an industry standard, adherence to which provides complete software portability for keyboards and display devices;
- TCP/IP communications protocol, enabling networks to be reliably and quickly developed.

(U) We are enthusiastic about further standards development which might continue to make our job of delivering analytic support easier in the future.

Conclusion

~~(C)~~ Industry-wide software standards, coupled with more and better commercial software are making possible the more rapid development and deployment of significant end-user capability. The SANDLOT program has been able to integrate more commercial software than ever before, while preserving necessary NSA-unique software. This approach has yielded dividends to SANDLOT end users who have the benefits of access to NSA-specific data, yet the manipulation tools of the commercial world.

Note NEW mailing address:

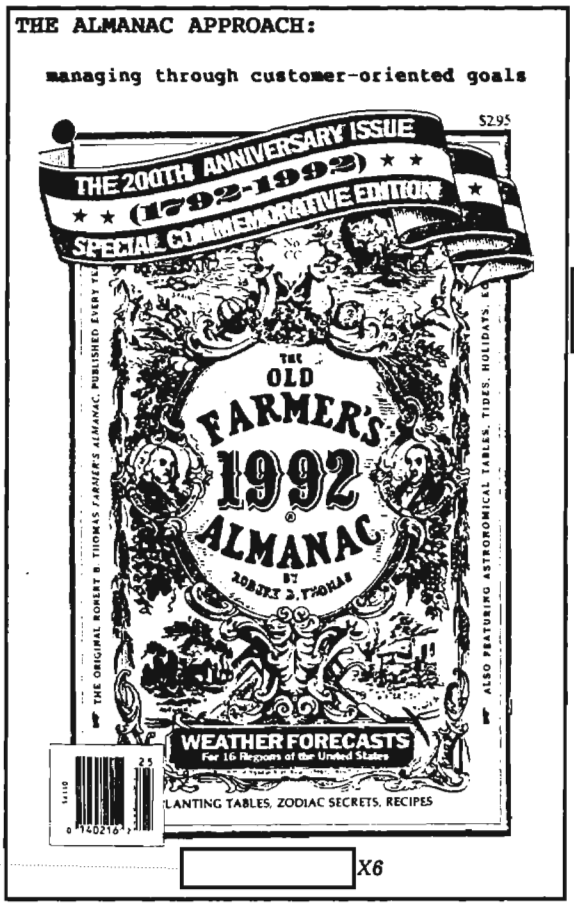
CRYPTOLOG
P0541
Ops-1

and new e-mail address

cryptlg @ curator

P.L. 86-36

DOCID: 4011851



P.L. 86-36

Have you ever noticed how traditional resource management tools really don't help you manage your resources? Have you ever noticed how seldom your Mission and Function statement, Resource Allocation Document or Table of Distribution has the information you need?

In Y Group we decided that we needed a management planning approach that is more "manager friendly." The result of our efforts is what we call the **Y Almanac**. We believe it may apply to other organizations as well.

The Almanac enables us to identify where we want the organization to go and helps to ensure that we are putting our resources on our stated priorities. It is a customer-conscious, goal-oriented planning system that recognizes the need for obtainable short-term goals, for job ownership, and for quality performance. The following describes the Almanac Approach and why we develop it.

BACKGROUND

Y Group consists of 3 traditionally structured but unrelated office-level organizations. It is the largest Group within the Information Systems Security Organization, both in the numbers of people assigned and in the diversity of skills needed to meet mission requirements.

P.L. 86-36

Our challenge was to find techniques that allow us to "get (and keep) our arms around" such an organization in terms of its tasks and its effectiveness. While traditional mission and function statements define the individual parts, in our opinion they leave something lacking in regard to the organization as a whole. We needed another approach.

Our efforts led us to develop the Almanac, which is a series of six parts providing the in-depth insights we sought. The Almanac is a "living" approach, in that the documents are regularly reviewed and updated. The six parts are:

Goals, Objectives and Tasks;
Task Matrices;
Manpower Utilization Report;
Financial Plan Matrix; .
Accomplishments Report; and
Demographics Report.

THE GOALS, OBJECTIVES, AND TASKS

The use of goals and objectives seems to come and go in management literature--and it seems to be out of fashion at the moment. Nevertheless, we believe some form of a goal-oriented approach is necessary to ensure that everyone in the organization knows where the organization is heading.

The Goals, Objectives and Tasks concept recognizes that lofty, long term goals seldom are motivating forces. People need to be able to work towards something that is obtainable within a reasonable period of time to feel pride in accomplishment, rather than frustration in never getting to the end of a very long journey. At the same time, the organization needs to

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011851

reach for things just beyond the immediate or it will become very short-sighted and focus only on the near term.

Our solution is to layer our goals into three levels. The **Goals** are the long term items for which we expect to strive for the foreseeable future. Supporting each Goal are one or more **Objectives**, which are more readily achievable in a reasonable period, though relatively long-term and general in nature. The Goals and Objectives provide a clear picture of the direction in which the organization is moving.

The merger of the organization's long term goals and mid-term objectives with short-term achievable ones is in the **Tasks**. As each Goal has supporting Objectives, each Objective has subordinate supporting Tasks. Each Task is a short term, achievable job, somewhat broadly stated but specific enough that managers and those involved in the Task can clearly understand the boundaries.

The principle of job ownership is task management. Each Task is assigned a Task Manager who is responsible for seeing that the Task is accomplished. We decided that as a general rule, Task Managers should be no higher than division level, and preferably, we push the responsibility down into the organization as far as practical.

In our case, we identified 14 Goals which cover the day-to-day requirements with room for the "stretchy, reach for the stars" items as well. These 14 Goals have over 35 supporting Objectives, which in turn envelope over 170 Tasks. No one is expected to know all of the Goals, Objectives and Tasks. Senior managers know the 14 Goals, and know well those against which they have resources. Every employee should know the Task or Tasks on which he or she is working, and the Objective(s) and Goal those Tasks(s) support. The entire set of Goals, Objectives and Tasks is available to every employee who wishes to know the direction in which the organization is heading.

We looked to the big picture when we considered how to organize the Goals, Objectives, and Tasks for publication. In any organization the work can be categorized into three basic **Activities:** Customer Support; Internal Operations; and Investment in the Future.

- **Customer Support:** All organizations make products for or provide services to customers, some external to the overall organization (**Support to External Customers**), some within the organization (**Support to the ISSO**).

- **Internal Operations:** Work done for the organization itself. This included senior management,clerical support and administrative staffs. We also placed our engineering support here--the work that keeps the production lines going.

- **Investments in the Future:** Successful organizations have to spend some effort to develop new processes, new equipments, or new services in order to remain competitive and successful.

We examined our Goals, Objectives and Tasks and matched them against the activities without regard to the organizational unit in which the work was to be done. This is the point at which we clearly leave the traditional mission and function approach to organization work, for we are primarily interested in the total organizational effort. Some work fits into a single organizational sub-unit, other crosses organizational lines. Key generation, for example, is done in one division in one Office. Quality control, on the other hand, uses manpower in several divisions in each Office.

By arranging the Goals, Objectives and Tasks in their appropriate activity category, we have a clear road map of where the organization is going. To keep the Goals, Objectives and Tasks up to date, they are revised semi-annually. The process begins with the subordinate Y organizations, which recommend changes or additions and deletions. These are forwarded up the chain of command, and are consolidated at the Group level. The draft revision is then re-coordinated with the Y Office Chiefs and published after final approval by the Chief, Y.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011851

THE TASK MATRICES

We demonstrate our commitment to the concept of **job ownership** through the appointment of Task Managers. Each Task Manager completes a Task Matrix, an eight-column document that:

- States the what, where, how, why, for whom and by whom of the Task, to include the quality objective;
- Identifies the resources required to do the Task, and
- Identifies the standards by which success in achieving the Task, to include the quality objective, is measured.
- Notes expected changes in the Task;
- Identifies the resouces required to meet the expected change;
- Defines the delta between what is required today and the expected future change;
- Identifies any issues involved in the new requirements; and
- Identifies the standards by which success in achieving the delta will be measured.

Task Managers brief senior management periodically on their Tasks. We select about 10 Tasks each month to be discussed informally. The Task Matrices achieve multiple management objectives:

- They force local management to think about and commit to writing what they are doing and how they measure success. (Our emphasis on measurement happily coincides with that given under the Total Quality Management philosophy to which the DoD is committed.) For most tasks local managers must formally look at least two years ahead and address the issues. We have found that this aspect has been very beneficial to the Task Manager--some have admitted that in preparing the matrices they looked down the road for the first time.
- They provide an avenue for persons involved in the detail work of the Group for discussions with senior management.

CUSTOMER SUPPORT	ISSO SUPPORT
Goal 1 Goal 2 Goal 3 Goal 4 Goal 5	Goal 6 Goal 7 Goal 8 Goal 9 Goal 10 Goal 11
INVESTMENT IN FUTURE	**INTERNAL OPS**
Goal 12	Goal 13 Goal 14

- During the briefings they offer opportunities for senior managers to observe more directly the capabilities of employees at every level.

THE MANPOWER UTILIZATION REPORT

We also needed a means to provide a good visual presentation of how we employ manpower on the Goals, Objectives, and Tasks. The semi-annual Manpower Utilization Report tells us where our manpower resources are.

It uses a standardized format. For each Goal, the information on the first page:

- identifies the Activity supported at the top of the page;
- provides a Goal overview, stating how many man-years of effort are required;
- lists Objectives in keyword, bullet format;
- identifies pertinent facts the reader should know;
- and states some additional resources comments such as use of overtime or shift work.

When appropriate, the overview page also contains a line graph or bar chart depicting the anticipated future requirements.

We chose to identify separately the management and support overhead involved with these major functions. The Management and Clerical lines are listed under Internal Operations.

Objectives with large numbers--usually 15 or more--of man-years are split out in "break out"

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011851

KEY MATERIAL PRODUCTION (Goal)

Objective	Man-Years
Production Requirements	xx
Key Generation	xx
Paper Key Production	xx
Special Key Production	xx
Electronic Key Production	xx
	--
Clerical	x
Management	x

Selected Tasks	Production Facts
* aaaaaaaaa	* zzzzzzzzzzzzz
* bbbbbbbbb	* yyyyyyyyyyyy
* ccccc	* xxxxxxxx

Resources Comments	Forecast
* xxx hour overtime * 2 shift operation	

pages placed immediately behind the overview page. The Activity support is identified in the upper left corner, and the Goal and Objective involved are shown in the upper right corner. For the remainder, the same basic format of the overview page is followed, with the focus on the man-years required for the component parts displayed in a pie chart. For example, a break-out page on the Paper Key production Objective contains a pie chart reflecting the man years if effort involved in Design, Production Control, Typesetting, Photo Lithography, and Press/Bindery operations. The Tasks, Production Facts, and Resources Comments boxes contain specific information about paper key production.

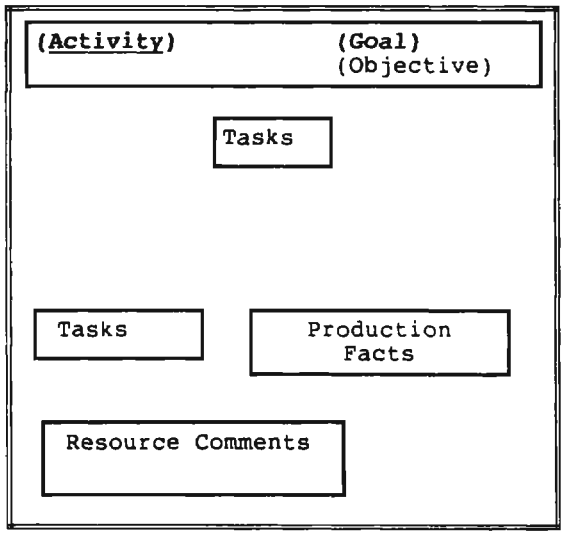
The advantage of this concept is that it tells senior managers exactly what the manpower costs of a function actually are. We found that the traditional TD and RAD approach just doesn't give the whole picture.

THE FINANCIAL PLAN MATRIX

In this part of our Almanac, we look at dollar resources applied to the Goals, Objectives and Tasks. Each line item is matched against the Task which it supports. Thus, we can identify how many dollars we are allocating to each Task, each Objective and each Goal. By combining this Report with the Manpower Utilization Report, we have a complete picture of where we are putting all of our resources.

As stated earlier, our Almanac is a living approach, one that changes and grows as required. An example of one element of the Almanac that has changed considerably is the Financial Plan Matrix. The Matrix, maintained on a PC using LOTUS 1-2-3 software, reflected only the information indicated above. After the first Matrix was published, we added a few columns and some calculations, and now use it as a summary sheet for the entire concept. The Matrix is shown on the top of the next page.

The dollars programmed for each line item are identified by Budget Code and totaled under the Task Column. The man-years of effort for each Task is also shown. In the Objective column, the sum of the dollars programmed for the various Tasks under the Objective are totaled, and the percentage that figure represents for the total dollars programmed for the Objective is shown (% 0). Also, the total man years of effort is shown, both for "line" (n(1)) and for management, clerical and staff (n(a).) The Goal column similarly reflects the total dollars programmed for the Goal, the percentage of the total FINPLAN those dollars represent (% FP),



~~FOR OFFICIAL USE ONLY~~

DOCID: 4011851

Goal	Objective	Task	Budget Code	Dollars	Man Years	Task Manager
Aaaaa	Wwwwwww	Ccc	Gxxx	$$	nn	Name
$$$$	$$$	$$				
% FP	% 0					
		Ddd	Nxxx	$$	n	Name
n(1)	N(1)	$$	Lxxx	$$		

and the man-years of effort for the Goal. The Task Manager column is self-explanatory.

THE ACCOMPLISHMENTS REPORT

The Y Accomplishments Report is our annual publication that highlights examples of important things that we have done during the previous Fiscal Year. It follows the format of our Goals, Objectives and Tasks concept, with each accomplishment identified as to the Task, Objective and Goal which it supports. Each page, in key word or bullet format, identifies the Activity, Goal and Objective(s) under which the reported Tasks fall. A sample of a page is shown below.

THE DEMOGRAPHICS REPORT

The Demographics Report, published annually, provides a typical "people facts" summary--facts about grades, educational levels, promotions and awards data, etc.

SUMMARY

The Goals, Objectives and Tasks is the keystone of the Almanac concept. It tells us where we intend to go and how we intend to get there. The complimentary Task Matrices, FINPLAN matrices and Manpower Utilization Report provide senior management the long sought ability to get our arms around the entire organization and plan with more confidence than ever before. Our Almanac approach has proven itself to be a valuable planning management tool over the past two years. It is flexible, and can incorporate new ideas without having to rebuild the concept.

It works.

CUSTOMER SUPPORT **KEY MATERIAL PRODUCTION**

Generate & produce keying material

Selected Tasks	Selected Accomplishments
Paper key & publications	Saved over $xxx,xxx over the base year through the paper waste reduction program.
Sealed systems, tapes, and cards	Produced over xxx,xxx sealed systems, which included almost xx,xxx PAL/CS related products.
	Established yet another production record of x.xx million key tapes, up xx.x% over the FY-88 previous record.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011851

~~SECRET~~

Further to THE TEN MOST WANTED

[redacted] *P04*

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

~~(FOUO)~~ I read the article on The Ten Most Wanted in 2nd Issue 1991 with a great deal of pride, I admit, for I, too, am a former manager of the program. But one thing the article did not mention was how the program got started.

~~(S)~~ The program was prompted by the Future SIGINT Capability Study that challenged NSA, and specifically the Office of Search (W3), to ensure the SIGINT system's survival through the year 2000 in the face of exploding technology. One of W3's reponses was to establish at the DO level the DO Ten Most Wanted Systems Program. [redacted] then DDO, approved the idea, and on 5 April 1986 announcements went out everywhere: fieldgrams, booklets, and posters. In addition, W3 sent message to [redacted]

The first manager was [redacted]

~~(C)~~ One point I did want to emphasize is that it is the ***Operations*** Ten Most Wanted Signals Program. W3 is the simply the manager of the program.

(U) Incidentally, you might be interested to know that the illustration shown above was used as a logo for the program.

~~SECRET~~

WL: in memoriam

We regret to report the death of William Lutwiniak, Founding Publisher of CRYPTOLOG. Following is an appreciation by Doris Miller (ret.), Founding Editor of CRYPTOLOG.

William Lutwiniak was always Mr. Lutwiniak to me: a benign but rather distant front-office figure to whom I submitted the typed pages of CRYPTOLOG each month and from I got them back, almost invariably, with a sweeping "O.K."

A severe budget cut had suspended publication of the so-call "underground press" of DDO—four small struggling periodicals, or aperiodicals, as they often turned out to be. Readers grumbled to me as the editor of one of those publications. So I proposed combining them into a single publication to be produced in P16. It is a tribute to Mr. Lutwiniak's persuasive powers that he succeeded in his advocacy.

The *NSA Technical Journal*, of course, had existed forever, and it was a great coup to have had something published in that professionally printed periodical, and distributed not only within NSA but also in collaborating agencies. But the *NSA Technical Journal* was not for all, being heavily biased towards mathematics in its more abstruse forms. (A typical title, which lives in my memory, is "A Random Walk along a One-dimensional Lattice.")

The mass of practitioners in our various fields needed a less imposing and more responsive forum, in which they could share their knowledge and plead their causes, and this forum CRYPTOLOG provided. It also allowed for some family-style discussions on agency policies, and an occasional bit of humor, all with Mr. Lutwiniak's cheerful support.

I have long since been banned from reading CRYPTOLOG, but I'm glad to learn from collateral sources that it still flourishes, bigger and better than ever, a lively part of William Lutwiniak's legacy. ~~FOUO~~

DOCID: 4011851

CLASSIFYING YOUR PERSUM

Richard D. Sylvester, B Group CAO

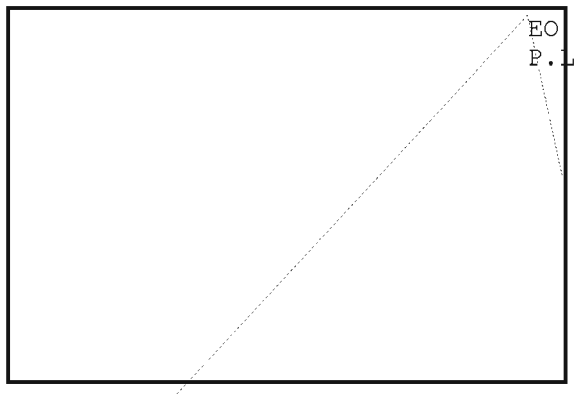
(U) Civilian Personnel Summaries (Form P3267) are strictly formatted, and for this reason it is often cumbersome to employ portion marking procedures for all the information contained therein. Nevertheless, if standard portion marking cannot be applied throughout, you should devise a method to clearly indicate the classification level of all information inscribed. Normally, the information entered in blocks 8 (Summary of Current Assignment) and 9 (Summary of all Previous Civilian and Military Service of a Cryptologic Nature) is in narrative form and it is a simple matter to apply portion markings to these narrative presentations.

(U) But there may be instances wherein certain information entered in other sections of the PERSUM also is classified. They, too, should be afforded portion marking protection. For example, you may list classified publications you have authored in block 12. If the titles of the publications are classified, you should, in parentheses, cite the classifications following the titles. In the case of certain field assignments in block 10 that require classified handling (discussed below), this information also should be marked in the most coherent and discernible manner possible.

~~(TS-CCO)~~ For example, in the first column of block 10, you might list the organization to which you were assigned

~~(TS-CCO)~~ There are certain other factors to be considered when composing your PERSUM: You may include information classified up to and including Category III COMINT (TOP SECRET UMBRA). But PERSUMS should not contain information that requires compartmented handling such as TK, BYEMAN, GAMMA, LOMA, etc. The reason for this restriction is obvious: the individuals who may be required to review your PERSUM may not be cleared for these special accesses.

~~(TS-CCO)~~ Certain field sites to which NSA personnel are assigned may also classified. If you specify in block 10 of your PERSUM that you, as an NSA employee, have been assigned to one of the following field sites, you must assure that your PERSUM is classified, at a minimum, in accordance with the classification specified.
To cite just a few examples:

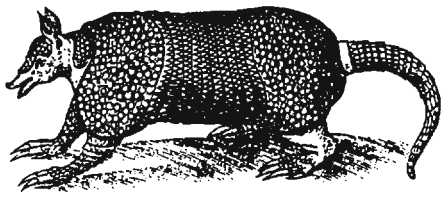


(U) Finally, you must affix an overall classification at the top and bottom of each page of your PERSUM, on the lines indicated for classification, commensurate with the highest classification of information contained within the PERSUM.

(U) Be sure your PERSUM is appropriately classified!

(U) In addition to neatness, brevity and accuracy, certain reviewing officials may judge you on the proper classification you have assigned to the information set forth in your Personnel Summary. Consult your element Classification Advisory Officer for assistance in classifying this most important document.

Shell Game



P.L. 86-36 [redacted] *P0433*

I hope to make this column a regular feature of CRYPTOLOG once again. It has been absent since the retirement of the original author.

It started as a tipsheet on using UNIX shells in the early days of PINSETTER development. At that time UNIX was relatively new to the Agency, so any tips were well received. Now we've advanced well beyond that stage, so I would like to use the column as an information exchange.

For those who may not know, PINSETTER is a P14 project to develop software tools for traffic analysts. It has come to be closely associated with the UNIX environment simply because that is the development platform we eventually settled upon. We use the UNIX shell extensively to package the tools into processing cycles. As most of the tools are simply data handlers and manipulators, they are often useful to disciplines other than traffic analysis. So we are using the pages of CRYPTOLOG as a way to reach the entire analytic community .

[redacted]

We've recently implemented a software distribution scheme for PINSETTER that takes advantage of [redacted] capabilities. Call [redacted] on 963-3369s for instructions. Network

[redacted]

A revised basic PINSETTER manual pages will be available shortly. At present several PINSETTER and UNIX-related tutorials are available. Among the titles: *How to Use SED* (October 1988), *How to Sort* (April 1991), *How to Search* (August 1991), and *How to Rearrange* (November 1991). Contact P0433 on 963-3369s for copies.

Letter

To the Editor:

I have just read *Improving NSA's Processes: Looking at the Problems*, published in January 1992. This document conveys a great deal of interesting information about the Agency. So does the photograph of senior Agency personnel on the cover: nineteen men and one woman. Moreover, that lone woman is doing double duty as a female and as a minority.

The picture is even worse when you look at the composition of the task force for the various subjects: planning, financial, and so on. Even the task force for the SIGINT production process has only one woman among the seven members.

Vera Filby, D9

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

DOCID: 4011851

SIGINT in the Novels of John le Carré

[redacted] *G41* P.L. 86-36

(U) The nine espionage novels John le Carré has written since 1964 have been widely read and analyzed on many levels—authenticity, political slant, and even literary symbolism. This article will look at the ways in which SIGINT has been portrayed in those novels—how often, how accurately, and to what effect. It will also demonstrate that while le Carré has often found it handy to use SIGINT as a plot device, he does not hold SIGINT or the other technical intelligence disciplines in particularly high regard. Rather, he is a fervent partisan of HUMINT and a persistent critic of the technical disciplines and the people who practice them. A warning: the article will summarize some of the plots of these superb stories, so stop here if you intend to read them in the near future. (One ending is revealed here only because of the role played by SIGINT in the novel's outcome.)

(U) There are no SIGINT references at all in le Carré's breakthrough 1964 novel *The Spy Who Came in From the Cold* nor in his third novel, *A Small Town in Germany* (1968). But SIGINT does play a key role in his second novel, *The Looking Glass War* (1965), which was much less successful both commercially and critically. In this book a decrepit intelligence department of the British Ministry of Defence undertakes to train an agent and infiltrate him into East Germany to check out tenuous reports of Soviet missile deployments there. The department hasn't run agents since WW II, but hopes that a success will put them back in business and increase their budget and influence. Out of touch with contemporary tradecraft and operating on a shoestring, they engage a WW II agent who became a garage owner after the war. One of the planners asks George Smiley if MI6 will loan them modern short duration signal agent comms gear for a "training exercise." When Smiley says that he cannot risk compromising new equipment and techniques, the MOD man says they'll have to use a WW II-era agent radio and asks Smiley how often a transmitting agent must change frequencies in order to foil direction-finding. Smiley says "every two or three minutes," but warns that there are several other factors—"luck, reception, amount of signal traffic, and density of population."

(U) After refresher courses in marksmanship, unarmed combat, German, missile technology, ciphers, and communications, the agent "Mayfly" crosses the border carrying an ancient and heavy HF radio in his suitcase. His first transmission is so slow and clumsy that the listening Vopos initially believe it's a child rather than an illegal agent. A U.S. SIGINT site in West Germany also intercepts Mayfly's report, and the Americans ask MI6 if it's one of their agents. The head of MI6 sends Smiley to the safehouse on the German border; Mayfly has killed a sentry, which has given the MOD cold feet, and, now, caught in an unauthorized operation, they agree to close it down. When Mayfly makes his next transmission, only the East Germans and the Soviets are listening. He's easily located by D/F and captured (or killed). The British govern-

ment disowns him and issues a plausible denial. In the final cynical twist, Smiley learns that MI6 knew all along that the MOD was running a real operation and allowed it to continue in the hope that it would fail and keep the Ministry out of the HUMINT business forever. Le Carré has since said that this book was heavily influenced by the Bay of Pigs disaster.

(U) In 1974 le Carré published *Tinker, Tailor, Soldier, Spy*, the first of a trilogy in which Smiley pursues the Soviet mastermind Karla, head of the KGB's Thirteenth Directorate. This is also the book which showcases le Carré's many colorful eumphemisms for intelligence functions and personnel, some of which have been widely adopted by the American and British media to describe the intelligence business. In *Tinker, Tailor* he also locates British SIGINT organizationally for the first time and names its practitioners—"wranglers." It is apparently a division within MI6, comparable to the dirty-tricks people ("scalphunters"), the bug detectors ("ferrets"), the forgers ("shoemakers"), and the operations support people ("lamplighters").

(U) *Tinker, Tailor* is concerned primarily with Smiley's search for a high-level mole in MI6, recruited by the Soviet superspy Karla and run under his direction. A key element in the search is analysis of a failed operation in Czechoslovakia in which a British agent was shot and captured. When Smiley interviews the man who was duty officer during the operation, the man recalls having been informed by one of the wranglers that "all hell had broken loose on the Czech air: half of it was coded, but the other half was *en clair*. He kept getting garbled accounts of a shooting near Brno." Later Smiley reminisces about meeting Karla in 1955 in New Delhi. Karla had gone to California to activate a dormant agent network and to establish its radio communications with Moscow Centre. A coding mistake on the Moscow end allowed the British cryptanalysts to break the system. When Karla traveled to New Delhi to assess a potential Chinese agent, the Americans allowed him to leave, rolled up his agents, and had the Indians arrest him. Smiley visited him in his cell and suggested that he come to England and tell all; Moscow would blame him for the fiasco in the U.S. and he faced a bleak future at home. But Karla spurned the British offer. The Indians then deported him to Moscow, where he outmaneuvered the boss who wanted his head, had him shot, and replaced him. After that, Smiley notes, Karla never again used clandestine radio communications, and never allowed his field agents to use them either.

(U) An interesting aspect of this story is the way the mole manipulates compartmentation procedures. In 1971 the Soviets begin giving the mole relatively high-grade intelligence, and he tells three other top MI6 executives (whose assistance he'll need) that it comes from a source—"Merlin"—who will deal only with him. This accomplishes two things. First, Merlin's success puts one of the three executives, an unsuspecting and pliable man, on the fast track to head MI6. It also gives the mole a reason to meet regularly with the KGB officer who is actually running him. Smiley realizes that Merlin is the key and that the mole must be one of the four top executives privy to the compartment. The rest of the novel follows Smiley as he tries to determine which of the four is the mole. In this sense this is a cautionary tale about excessive compartmentation.

(U) The next novel, *The Honourable Schoolboy* (1977), finds Smiley, after exposing the mole and uncovering the dry rot within the service, running MI6—"appointed the captain of a wrecked ship." Some believed that they had heard "the last beat of the secret English heart." One London rumor had it that it was the Dutch SIGINT service which was really responsible for identifying the British mole, by breaking a Moscow Centre code. Believing that every activity of the service was compromised, Smiley "scraps the lot," including the SIGINT service. He describes it as having been "working practically full time for Karla for the last five years." We also learn that SIGINT operations were run from a headquarters in Bath and paid for by Foreign Office funds.

(U) Smiley's task at the beginning of 1974 is to rebuild the service and to produce intelligence that will induce the now very leery CIA "cousins" to return the Anglo-American intelligence relationship to its former status. He is also obsessed

DOCID: 4011851

with putting Karla out of business. He and his team—former colleagues sacked or descredited by the mole—begin by looking at an aborted investigation of a Moscow Centre money-laundering operation for paying agents, run out of Vientiane. The operation is now in Hong Kong, and an agent—the "Honourable Schoolboy" of the title—is sent there to run it down. Against the backdrop of the fall of South Vietnam, the Schoolboy goes all over Southeast Asia gathering information. Leaving Udorn, Thailand, after using the comms facility at the CIA station there, he passes the U.S. SIGINT facility and remembers having heard that 1,200 linguists work there.

(U) *Smiley's People* (1979) was the last of the Karla trilogy. It seems that Karla had a daughter, by a mistress he eventually sent to the Gulag when she became politically unreliable. The daughter is schizophrenic and confined to an asylum in Switzerland; Karla has been illegally using operational funds funnelled through his man in Paris for a ghost agent to pay the considerable expense involved. The man in Paris is told to use couriers whenever possible, since Karla "is against excessive use of radio." Smiley notes that Karla's earlier vow not to use clandestine radio was apparently "subject to review." An Estonian emigre living in London, a former agent of Smiley's, learns all this through a complicated chain of events, but is killed on Karla's orders before he can tell Smiley; Smiley is again brought out of retirement to investigate the murder.

A DEPARTURE TO THE MIDDLE EAST

(U) *The Little Drummer Girl* (1983) was a departure from the earlier books in terms of both location and characters. Le Carré told an interviewer in 1983 that his original concept was for a novel about the Middle East set in London and Washington, but he couldn't find a credible way to involve MI6 and Smiley and ended up making the Israelis the central characters and setting it in part in the Middle East. This novel deals with the efforts of a team of Israelis to capture or kill a Palestinian terrorist ("Khalil") whose speciality is bomb attacks against Israelis in Europe. They grab and eventually kill Khalil's younger brother Michel and recruit a British actress named Charlie to pose as a sympathizer and Michel's lover. While SIGINT plays no role in this novel, the Israeli communications gear is described in some detail. Most of the operation is supported by a mobile comms van equipped with both secure voice and enciphered printer. When forced to use clear voice, they use the callsigns and jargon of taxi companies and other legitimate users of mobile comms.

SIGINT TRAPS A "PERFECT SPY"

(U) SIGINT does play a significant role in *A Perfect Spy* (1986), which le Carré has described as his first work not submitted to Her Majesty's Government for prepublication review. It is the story of one Magnus Pym, MI6 station chief in Vienna in 1983. As the novel begins, Pym, haunted by the death of his con-man father, has disappeared. His wife and colleagues are baffled and fear that he's defected. He has in fact gone to ground in a rooming house in a coastal town in the UK, where he is writing the story of his life for his teenage son. The novel's chapters alternate between the story of Pym's life up to his disappearance and MI6's efforts to discover where he's gone and why, and to keep the CIA from learning that there may have been another major British security disaster.

(U) Pym was induced into the intelligence business after WW II by the MI6 Station Chief in Bern; Pym was studying at a university there and met the man, Jack Brotherhood, at the local Anglican church. Brotherhood uses Pym for various low-level tasks, such as collecting the names of leftists at the university and translating stolen documents. Pym tells Brotherhood about Axel, an illegal German refugee whom he has befriended at his rooming house, and Brotherhood informs the Swiss counterintelligence service in order to accumulate "barter material." They arrest Axel and deport him.

(U) After graduating from Oxford in modern languages and taking a commission in Army intelligence, Pym encounters Axel again in Austria. Axel is described to Pym as a Czech Army officer who wishes to defect, but it's a ruse. Axel proposes that he become Pym's agent and gives

him a great deal of classified information to establish his bona fides. Soon Axel tells Pym that their relationship has become known and that Axel can protect himself only by making it look as if Pym is Axel's agent. To pull this off he will need legitimate classified information from Pym. Pym never seriously considers not doing it; he has vowed not to betray Axel a second time, and there is also the problem that his own reputation rests on what Axel is feeding him. (We learn later that the material Axel is providing looks good but is of little actual value.)

(U) Upon demobilization in 1953 Pym enters MI6 and is sent abroad again—to Czechoslovakia, of course. He is soon caught and pitched by Axel again. This time, Axel says, they'll make each other into intelligence superstars, by "making straight for the biggest diamonds, the biggest banks." But what Pym will get from Axel over the years will be largely disinformation, supplied by nets of agents fully controlled (knowingly or otherwise) by the Czechs and other Eastern European counterintelligence services. Piling success upon success, Pym goes to Stockholm, back to London, to Berlin, and then to Washington as Deputy Chief of Station, followed everywhere by Axel. But the Americans begin to become suspicious; the Eastern European networks produce good material only when Pym (and Axel) are actually there. Pym is summoned to London for an investigation, but MI6 does only a cursory check and sends him back to Washington with a clean bill of health.

(U) The CIA keeps pushing, however, and sends a team to London to present new evidence of Pym's treason. This is after Pym has disappeared, but the British have concealed his absence from their American colleagues. Artelli, the SIGINT analyst in the American team, is described as "a distraught mathematician" from "Signals Intelligence." The new evidence is traffic analysis of clandestine communications from the Czech Embassy in Washington and from other Czech facilities in the U.S., particularly the consulate in San Francisco in 1981 and 1982. The significant point is that the transmissions stopped every time Pym left Washington, and the assumption is that they're meant for Pym and aren't broadcast when he's away. Artelli adds that the communications techniques are old-fashioned and give off a "sense of long habituation, one human being to another." Although the communications are unreadable, the cryptanalysts know that the keys are derived from some kind of text. Artelli also reveals that there are strange things going on with Czech clandestine radio in the last few days—the equivalent of blind calls to someone.

(U) The Czechs, like the British, are trying to find Pym, although the CIA doesn't make the connection because they don't know that Pym is missing. Then another team member brings up more new evidence—the travels of a Czech intelligence officer named Hans Albrecht Petz, AKA Alexander Hampel, AKA Jerzy Zaworski. Petz is Axel, of course, and his travels in Europe and the U.S. coincide perfectly with Pym's. The British still refuse to believe it, arguing that the Czechs have mounted an elaborate deception to discredit someone who's been particularly effective against them. Their ambiguity about where Pym is and what he's doing convinces the Americans that he's flown the coop. Brotherhood, still in MI6, finally comes to believe Pym's treachery, and learns from Pym's wife that Pym takes a battered copy of a 17th-century German book entitled Simplicissimus everywhere he goes. The book (actually Der Abenteuerliche Simplicissimus Teutschroughly, (*The Adventures of a Simple German*) was given to Pym by Axel when they first met in Bern, and it's a somewhat heavy symbol. The author, Johann Jakob Christoffel Grimmelshausen, fought on both sides during the Thirty Years War, and used many pseudonyms which were anagrams of his name. Brotherhood tells the British SIGINT service to run the Czech clandestine traffic against the book, and it works.

(U) Now everyone is looking for Pym—his wife, the British, the CIA, and Axel, who fears he is suicidal and wants him to defect to Czechoslovakia. The CIA Station Chief in Vienna, an old friend of Pym's from Washington now obsessed with nailing him, has enlisted his own wife to help watch Pym's wife there, and she sees Axel contacting his wife in a church. She immediately calls her husband at the U.S. Embassy in London on an open phone and tells him with a clumsy prearranged code. The British,

who have tapped the embassy phones, intercept the call. But Pym's wife evades both the Americans and the British, makes it back to England, and tells Brotherhood that Axel has unknowingly let her know where Pym probably is. The book reaches its climax as all the interested parties rush to reach Pym first.

A COMMUNICATIONS DECEPTION

(U) SIGINT plays a small but important role in le Carré's 1989 novel *The Russia House*. It is his Glasnost novel and his most political book to date. The central character is one Bartholomew "Barley" Blair, an alcoholic British publisher and saxophone player. A dissident Soviet scientist who met Barley briefly at a party tries to have a manuscript delivered to him via a Moscow book fair; it eventually ends up at MI6. According to the manuscript, Soviet military technologies—particularly missiles—simply don't work. The Soviet military research establishment has not only produced weapons that don't work, they've faked the test results to conceal the failures from their own government. The scientist, one Yakov Savelyev, wants the manuscript published in the West, believing it will lead to large-scale disarmament on both sides. The British and the Americans have another idea, of course. Their biographic research reveals that Savelyev—now code-named "Bluebird"—is responsible for, among other things, telemetry encryption. Part of what he has provided is the original telemetry—before it was faked and before it was encrypted. They want to use Barley to determine whether the material is genuine and then have Barley run Bluebird as an agent in place. Against all his instincts, Barley agrees to do so.

(U) After three weeks of training Barley goes back to meet Savelyev in Leningrad, takes more material from him, and promises him he will get the manuscript published. Barley then travels to the U.S. for a combination debriefing and interrogation by the CIA, now the senior partner in the operation. A senior CIA official warns Barley and the British that the American military-industrial complex doesn't welcome the Bluebird manuscript and will work hard to discredit it.

(U) Barley returns to Moscow with a shopping list of questions for Savelyev, and the CIA smuggles in a truck full of "surveillance" gear to monitor developments. The British officer who has been functioning as Barley's case officer (identified only as "Ned") begins to get cold feet, aware that the Anglo-American shopping list tells the Soviets everything we don't know about their strategic weapons programs—and, by inference, everything we do know. The rest of the team ignores his concerns, convinced that everything is on track. But Ned is right—Savelyev has been caught and turned. Meanwhile, the Soviets practice a bit of deception to ensure that they'll get the shopping list. A Soviet military entity in Leningrad sends a message to Moscow authorizing Savelyev to take a recreational weekend there after he delivers a lecture; it is intercepted by a U.S. SIGINT facility "in Finland" and decrypted. The Americans and the British buy it, although Ned suspects it was planted. He points out that it was enciphered by an ancient Soviet machine and that there are no other messages intercepted like it. Barley delivers the shopping list and then disappears, a good juncture at which to end this plot summary.

GEORGE SMILEY'S VALEDICTORY

(U) *The Secret Pilgrim* (1991) features the first appearance of George Smiley since *Smiley's People*. Ned of Russia House was made the scapegoat for the Bluebird fiasco and exiled to run the MI6 agent training school. He invites Smiley, his mentor and father figure, to talk at the graduation dinner of a class of agents, and Smiley agrees to do it. Every anecdote Smiley tells reminds Ned of an operation of his own, and the book is basically a collection of Ned's vignettes from three decades of espionage. There are no references to SIGINT as such, but in the stories both the British and the Soviets continue to rely heavily on clandestine radio through the 1980s.

(U) What can we say about le Carré's apparent knowledge of SIGINT from this review of the novels? To use the Watergate question, what did he know and when did he know it? He seems to have a good grasp of clandestine radio techniques and counter-clandestine SIGINT capabilities. If there is a tradecraft moral, it is that "agents

shouldn't use radio." "Mayfly" in Looking Glass War, Karla, and Pym are tripped up by successful counter-clandestine SIGINT operations. Le Carré does not display much awareness of broader SIGINT applications, such as on political, economic, and military topics. This is consistent with what is known about his intelligence career—he was a case officer in the 1950's and 1960's and would probably not have had regular access to mainstream SIGINT reporting. There is also the matter of censorship by the British government; le Carré claims that he submitted every novel prior to *Perfect Spy* for pre-publication review. It is unlikely that official reviewers would have allowed any accurate information about British or American SIGINT activities to be published. In this regard it is interesting to note that no le Carré novel has ever referred to "NSA" or "GCHQ"; this could not possibly have been because he didn't know about those organizations.

(U) People involved in any of the intelligence disciplines have an ambivalent attitude towards having their craft described in fiction. On the one hand, we sneer at the more lurid and fanciful fictional descriptions of our profession; on the other hand, we are appalled and often want legal action taken against writers who get it right. So in this sense, as SIGINT professionals we should be happy that le Carré's references to our business are few and mostly uninformative.

HUMINT vs TECHNICAL INTELLIGENCE

(U) But le Carré has another agenda which is more interesting. He is not only a strong partisan of HUMINT as an intelligence discipline, but he actively disparages the other more technical means of collection and analysis. He is to intelligence as the 19th Century Luddites were to the industrial revolution—a rabid foe of technology. This is manifested in several ways in the novels which may not be readily apparent from these brief plot summaries. For one thing, he portrays intelligence technologies as peculiarly—and offensively—American. Some of the most despicable characters in his books are British officials who make deals with the CIA to share the fruits of American intelligence money and technology. His heroes are HUMINT practitioners who detest depending on Americans and scorn nearly all uses of technology. Alleline, the mole's pawn in *Tinker, Tailor* adored Americans, while MI6's Director, Smiley's beloved father figure, detested them and all their works. The mastermind in *Little Drummer Girl* was described as out of tune with Mossad's polygraphs "and their ever-growing faith in American-style power plays, applied psychology, and crisis management." The noble Jack Brotherhood in *Perfect Spy* objected to MI6's pandering to American "methods and example." Conversely, the people in his novels who are good at technology are often unpleasant characters. One particularly nasty MI6 officer in Russia House was described in this way: "Clive was a technology man, not at ease with live sources, a suburban espiocrat of the modern school. If he liked anything at all in life apart from his own advancement and his silver Mercedes, then it was hardware and powerful Americans, in that order." For Clive, human nature was "one vast unsavory nightmare." In *Secret Pilgrim* Ned, in praising the successes of an MI6 officer against the Khmer Rouge, notes that espionage technology "can't break the codes of an army without radios." Ned also reflects with nostalgia on a time before MI6's registry was computerized, when it "could still find what it was looking for, or know for sure that it was lost."

(U) Le Carré has developed this theme even more explicitly outside of his fiction. In a 1986 interview he attributed what he called the "flagrant failures" of Western intelligence to an "obsession with high-tech espionage." In a 1989 interview he said that "the shift of professional confidence from human assets to electronic ones is a direct consequence of U.S. domination of Western intelligence." He went on to say that when human agents are well recruited and well targeted, "they are affordable and often far more reliable than the inductive fantasies which result from the reading of signals and codes and photographs."

(U) There are several possible explanations for le Carré's animus against the technical intelligence disciplines and their practicioners. One is that it's a manifestation of an obvious anti-American bias, although he adamantly denies that he's anti-

DOCID: 4011851

American and cites as evidence the number of obnoxious and incompetent Brits who appear in his novels. This means, he says, that he's even-handed. Although the reader will have to make his or her own judgment, it seems to this writer that criticism of American power and policies is a consistent theme in both his fiction and his public statements. It makes for a fairly simple equation—le Carré scorns SIGINT and imagery because they are dominated by the U.S.; they exemplify American technological arrogance.

(U) Another explanation may be that he has never really been exposed to SIGINT and imagery and doesn't understand their value or their complexity. A senior CIA HUMINT officer who came to NSA in another capacity as a retired annuitant told this writer that for his entire CIA career he thought that all NSA employees were like the State Department communicators he encountered in embassies—skilled communications technicians. This person was astounded to learn what we actually do in terms of signals processing, cryptanalysis, language work, and analysis. There are also people who disdain technology because they don't understand it and secretly fear it; it wouldn't be surprising if an early 1950's graduate of Oxford in modern languages harbored such attitudes. The answer may well be a mix of all three.

THE MORAL COST OF HUMINT

(U) What is striking about le Carré's relentless public championing of HUMINT is his refusal to acknowledge its human and moral costs. The relative morality of intelligence activities is a complex question. The current U.S. official position is that some acts are so odious that they cannot be justified even when they would advance the national interest; an example is the apparent prohibition on assassinating foreign officials. (The purist may argue that assassinations, like covert actions, have nothing to do with intelligence, but past involvement in assassination attempts has blurred the distinction.) Acts less grave than assassinations that would otherwise be considered immoral and/or illegal are deemed acceptable if done in the national interest. There are dissenters on both sides of the political spectrum, of course. For some on the left, such acts can never be justified by invoking the national interest. For some on the right, there are no acts which cannot be justified if the threat to the national interest is sufficiently grave. (This is similar to the theological debate about a"just war.") A middle ground might be that there should be some proportionality between the gravity of the activity and the expected benefits—one should probably not blackmail an official of a foreign government to acquire the annual projection for rutabaga production. One way to measure the relative morality of various intelligence activities might be to assess their potential for harming individual human beings. The technical intelligence disciplines have little or no impact on human beings; HUMINT, by definition, involves the exploitation of people and carries a high risk of harming them.

(U) Le Carré's failure to address the human costs of HUMINT is striking precisely because his novels are intensely concerned with questions of personal morality. As William Buckley noted in a 1983 review,"" 'The Little Drummer Girl' is about spies as *Madame Bovary* is about adultery or *Crime and Punishment* is about crime." There is endless agonizing in these novels about the moral dilemma of the case officer, whose task it is to obtain information by corrupting or seducing vulnerable human beings. Smiley speaks in *Honourable Schoolboy* about having to be "inhuman in defence of our humanity, harsh in defence of compassion, single-minded in defence of our disparity." The Schoolboy himself recalls Smiley speaking at the MI6 training school about being grateful that intelligence service provided the opportunity to repay one's country, but the Schoolboy notes that "the paying is actually done by the other poor sods."

(U) There is a strong sense in le Carré's novels of what has come to be called by conservative American commentators the concept of moral equivalence—that if those who act on behalf of the West and the USSR both commit immoral acts, there is no real moral difference between the two. As George Will put it, "In [le Carré's] espionage novels the 'ambiguity' consists primarily of the idea that means as much as ends reveal where, if anywhere, justice lies in political conflict." So a

DOCID: 4011851

case can be made that it's inconsistent and perhaps even hypocritical for a man so concerned with moral questions to uncritically promote the intelligence discipline most likely to harm individual human beings.

WHY THESE NOVELS MATTER

~~(C)~~ Since le Carré's writings and public pronouncements (whether because of ignorance, discretion, or censorship) don't appear to pose any threat to SIGINT sources and methods, does it matter to us what he writes? It matters because it adds to a public mystique about HUMINT that has a real (although intangible) impact on the way the Intelligence Community is perceived both by the public and by the rest of the government. Many former intelligence officials and other commentators have relentlessly pushed the idea that "American intelligence" was crippled when then-DCI Stansfield Turner cut 820 CIA Operations Directorate billets (none overseas) in the 1977 "Halloween Massacre." Although the CIA and the rest of the Community continued to perform well after this event, some have gone so far as to suggest that some major U.S. foreign policy mistakes in the late seventies and early eighties were due to this modest reduction of HUMINT assets. In a more recent example, the Congressional committees responsible for the intelligence budget added money for CIA HUMINT operations for both FY91 and FY92, while reducing the rest of the National Foreign Intelligence Program. In a perfect world decision makers should be so well informed that they couldn't possibly be influenced by an Ian Fleming, a John le Carré, or a Tom Clancy, but in this imperfect world it sometimes happens.

~~(C)~~ It is hard to develop an appropriate awareness in the right places of the actual and potential contributions of the SIGINT system without putting ourselves out of business. It was one of the primary reasons for the establishment of J8, the Office of Corporate Representation, and it would make a good subject for a separate article in this publication. In the final analysis, we're obviously better off that a writer as widely read as le Carré doesn't write accurately about SIGINT. But it is galling to know that his books and public comments make marginally more difficult the task of ensuring that resources are allocated within the Intelligence Community on the basis of real contributions instead of on the basis of myth and mystique. It is also ironic that the CIA would benefit from all this in even a small way, since le Carré has made his distaste for that organization so obvious.

REFERENCES

Monaghan, David. *The Novels of John le Carré.* New York: Basil Blackwell, 1985.

Le Carré, John. *The Looking Glass War.* New York: Coward McCann, 1965, p. 170.

—— *Tinker, Tailor, Solider, Spy.* New York: Alfred A. Knopf, 1974, p. 223.

—— *The Little Drummer Girl.* New York: Alfred A. Knopf, 1983, p. 28.

—— *A Perfect Spy.* New York: Bantam Books, 1987, p. 175.

—— *The Russia House* New York: Alfred A. Knopf, 1989, p. 89.

—— *The Secret Pilgrim.* New York: Alfred A. Knopf, 1991, p. 211; p. 179.

—— *The Honourable Schoolboy.* New York: Bantam Books, 1978, p. 461; p. 489.

Lelyveld, Joseph. "Le Carré's Toughest Case," *New York Times Magazine*, March 16, 1986, p. 90.

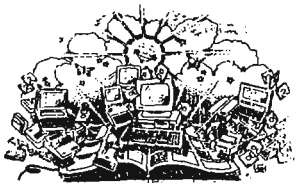
Trueheart, Charles. "John le Carré, the Spy Spinner After the Thaw," The Washington Post, May 25, 1989, p. D1.

Buckley, William F. Jr., "Terror and a Woman," New York Times Book Review, March 13, 1983, p. 23.

Will, George. "Le Carré's Unreal Mideast," The Washington Post, April 28, 1983, p. A13.

DOCID: 4011851

Technical Literature Report



Communications, Computers, and Networks:
The September 1991 Special Issue of
Scientific American

P.L. 86-36

Reported by: [redacted] *W31*

(U) Once a year, Scientific American publishes a single-topic special issue. The 1991 special topic is Communications, Computers, and Networks. It is "required reading" for analysts in a number of fields, not just computer science.

~~(S-CCO)~~ The structure and use of high-capacity computer networks is covered in various articles. This includes network protocols, packet switching, and projections for the future of networks. The consensus is that the use and capacity of networks will grow tremendously in the next decade. Senator Al Gore writes that networks will be as important to the competitiveness of America as the interstate system was during the 1960's and 1970's. (He has gone so far as to introduce the High-Performance Computing Act of 1991, an attempt to create a national high-speed fiber optic network.) [redacted]

EO 1.4.(c)
P.L. 86-36

(U) The discussion of networks is entwined with that of communications. Various types of data communication are currently carried via computer networks—everything from E-Mail to graphics. Several writers see that the distinction between the telephone, television, mail service and other means of messaging is becoming increasingly blurred.

~~(S-CCO)~~ One of the most intriguing possibilities is that of virtual reality (VR). By the use of electro-mechanical feedback, special viewing goggles, computers, and high-speed networks, people can not only watch "the action", but they can become part of it as well. [redacted]

EO 1.4.(c)
P.L. 86-36

~~(S-CCO)~~ Another interesting topic is ubiquitous computing currently in use at the Xerox Palo Alto Research Center (PARC). There, the network pervades the workplace. Via the use of infra-red and radio relay, people can carry small computer "notebooks" which are in constant communications with mainframes, workstations, other notebooks, printers, and even "smart" active badges. The display on the notebook is customized automatically to fit the needs of whoever is currently using it; this is done via the active badge. At NSA, an employee's badge carries a picture and PIN for the wearer. At PARC, the badge carries data files, wearer identification and location, voice communications, and can even forward phone calls to the right room. The use of such a system at NSA could be a mixed blessing. (People would never be out of touch with their office. But then, it would be harder to dodge unwanted phone calls!) [redacted]

EO 1.4.(c)
P.L. 86-36

(U) There are othere topics of interest to us in the special issue, such as data security, cryptography, and the legal ramifications of the use (and abuse) of large scale national and global networks. Reading this issue can help understand some of the possible intelligence challenges of the 21st century.

DOCID: 4011851

International Technical Communications Conference, 13-17 April 1991, New York

P.L. 86-36

Reported by [redacted] *A64, et al.*

Many NSAers spend some time writing and editing documents of one kind or another. While our audiences and topics may vary from office to office, our responsibility does not. The information that we are tasked to communicate is of vital importance. Therefore we have an obligation to produce documents of the highest quality possible—models of accuracy, clarity, succinctness, and elegance, easily grasped and gentle on the eyes. This standard is a difficult and elusive one, achieved only through great effort and no little study.

With this in mind, a contingent of writers and editors from NSA attended the 38th Annual International Technical Communications Conference in New York City, sponsored by the Society for Technical Communication. The conference attracts technical writers, editors, designers, and managers from all over the world. The three days of sessions featured over 185 seminars on various aspects of writing and editing, research and technology, visual communications, and management.

I. BENEFITS OF ATTENDING SUCH A CONFERENCE

It has been said that NSA's SIGINT reporters are at a disadvantage because unlike mathematicians and linguists, there is no outside professional society for them. This is not quite true. Actually, there are several for journalists, though membership in them is inadvisable. But there are two professional societies of writers, editors, and audiovisual presenters that can provide guidance on presenting information: the STC, whose conference is reported here, and the National Association of Government Communicators.

NSA is at a disadvantage in selling our product for two reasons: one, is that CIA has several years' start on professional-looking publications, thanks to the mandate of a senior official who demanded and got professionals experienced in publications to set standards. Since then, the homespun look of our product has tended to diminish its authority, though we may believe that our product has more validity. Another is that the new DCI is emphasizing HUMINT and de-emphasizing technical intelligence, DESERT STORM notwithstanding. So we must take still another hard, critical look at our publications. We must not fall behind in the very competitive intelligence arena. Presentation is all.

A very large conference like this is ideal for getting a quick update on what everyone else is doing. First of all, there is a lot to learn about the new editing, writing and layout techniques that are based on scientific experiments: electrodes are implanted in the brain to track eye movements and test message understanding. From these experiments new rules have evolved.

Then, from discussions at the sessions and from chatting during coffee breaks you may begin to develop an appreciation for the norm: what is usual, what editors and writers are expected to do in other organizations, the degree of freedom in substantive matters, in management, and in personal relationships.

The specific topics of interest to our group were those dealing with the nuts and bolts of document production: the basics of communication, editorial responsibility, managing the editor-author relationship, how to tailor documents to meet the needs of intended users, page layout and design, and document maintenance. In the course of these three very intense days of lectures, workshops, exhibits, and panel discussions, we gathered a great deal of information. Following is a summary of the information presented at the sessions attended.

II. COMMUNICATION AND EDITORIAL RESPONSIBILITY

Effective communication consists of five basic steps:

1. research—ascertaining exactly what the customer needs and wants, and identifying potential users;

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011851

2. planning—how to achieve objectives;

3. collection of pertinent, useful information;

4. composition of concise, consistent, and understandable prose from often diverse sources; and

5. final presentation of accurate material in a user-friendly format.

In the course of this process, a communicator often acts as coordinator, synthesizer of information, editor, designer, and, very often, producer of ideas for new documentation. With its many demands, modern communication is a challenging task with a number of potential pitfalls. For example:

• ***Implementation at the expense of planning.*** The pressure to produce to meet a deadline often precludes this essential preliminary step. Important factors may be minimized or completely overlooked. Effort taken to identify and plan for potential problems early on can save valuable time in the latter stages of production. You must communicate with customers to find out exactly what they want. Avoid ambiguous tasking; make sure that job requirements are explicit. Also, ***get them in writing***.

• ***Depersonalization.*** Ease of collection and manipulation of data can lead to neglect of the needs, values, perspectives, and biases of both the people who supply the information and those who will ultimately use it. Know the people behind the work—in other words, ***be sensitive***.

• ***The Hothouse Effect.*** This results from a lack of feedback or input from people from other organizations, publications, etc. The consequence of this insular approach is complacency and a tendency toward self-service, which ultimately renders your work useless to anyone else. Canvass others for input, opinions, ideas, and feedback. Find out what is important to them. Exchange ideas, concerns, and technologies with people with similar interests and experience. Generally speaking, when you go into any interaction with people, be prepared to learn something from them. Chances are, you won't be disappointed.

• ***Technological guilt.*** This is defined as sacrificing the needs of your users to a self-indulgent fascination with the many "techno-toys" on your desktop publisher. It can lead to an abuse of available capacity, user disservice, and compromised communication. Don't use all the fancy gimmicks available to you just because they are there. Decide what best meets the requirements of the document and its potential users, and design accordingly.

• ***Premature buy-off.*** This is the tendency to underdevelop material for the sake of getting the job done. Don't allow others' expectations or uninformed perceptions of required time and effort force you into an unrealistic production schedule. Objectively assess what it will take to use the material to its best and fullest advantage, then proceed from there. *Also, don't bite off more than you can chew.* If you can't do the job with the time and resources allocated to you, say so!

Remember that the primary goal of communication is to convey information in the clearest, most precise and succinct manner possible.

Take Positive Steps

To further this goal, a communicator should keep in mind these important points:

• ***Make communications as usable as possible.*** Anything that helps users acquire information easily is a worthy tool for the technical writer: extra leading and/or kerning, more graphics, larger type, a bigger trim size, wider margins, spiral binding instead of perfect, etc.

• ***Take an active role.*** Don't let your customers push you around. If you don't think the job can be done, *tell them.*

• ***Talk to people.*** Talk to your sources, users, colleagues in the field. Find out what they know, what they think is important, what they like, what they don't like, etc.

• ***Be curious.*** Try to take an interest in what you're writing about. If you're not interested, your writing will suffer.

• ***Avoid complacency.*** Ask, listen, be informed; be open to new ideas and procedures.

• ***Resist specialization.*** Cultivate a diversity of experience. Produce materials on a variety of subjects, in a variety of styles (within reason, of course). Accept new challenges. Above all, be a team player. Accept success (and failure) as part of a team effort.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011851

• ***Be humble.*** Remember: You can *always* learn—from anyone!

Working with Authors

In addition to their aforementioned responsibilities, communicators are often called upon to act as editors whenever it is necessary to incorporate the work of others into their documents. In this context, a whole new set of skills is required, perhaps the most important of which is the ability to work effectively with authors.

The purpose of the editorial process is to help authors communicate their ideas in the clearest, most concise manner possible, while at all times preserving the character and integrity of their individual styles. Whatever contributes to this process lies within the scope of the editor's task. There are a few points to remember regarding this principle:

• ***Learn to submerge yourself.*** Don't allow personal biases to skew your treatment of others' work. Try to operate consciously at many different levels. For example, try to imagine yourself as the author, expressing ideas that mean a lot to you. Imagine yourself as the reader, trying to make sense of difficult concepts. Develop a sense of perspective, that is, other people's.

• ***Know that editorial skills are tools.*** And, like tools, they are to be used to perform a specific task—in this case, to help authors communicate most effectively. Any other use constitutes abuse. Also remember—

Editing is only a part of the system, comprising all the other elements of document production: proofreading, design, typesetting, art work, printing, binding, etc.

It is easy to make mistakes. That is why the world (whether or not it wants to admit it) needs editors. The point? Be nice, be patient, be sensitive, be diplomatic. Being the "victim" of an edit is often a painful experience. People do not like having their mistakes pointed out to them or their masterpieces carved up. Also, editors, being human themselves, are liable to make mistakes. Try not to err, but, if you do (and you will eventually), learn what you can from the experience, then *forget it.* Learn to forgive yourself, as you forgive others.

Things are not as simple as they appear. Respect what you edit, whatever it is. Carefully examine the job to determine how best to treat it. Let other editors read the original for their assessment before you edit, then give them your edited version for comments and suggestions.

Some Common Editing Styles

• ***Editing by whining.*** This is defined as letting authors get away with murder (in this context, illiteracy) and then complaining that their work is bad. Don't let authors push you around. When they're wrong, tell them!

• ***Editing by fiat.*** A few representative pronouncements associated with this one are, "I'm the editor, and what I say goes!", "Rules are rules. If you don't like 'em, lump 'em!", "What do you know? You're just the author!", etc. Sometimes known as the "brickbat method," this approach, as you might have guessed, is detrimental to the author-editor relationship. Don't do it. Respect your authors; respect their work, opinions, and desires.

• ***Editing by restraint.*** This method, a combination of the above, requires good judgement—a sense of when to say "no" and when to let things go. If something an author wants to put into a document, while perhaps technically incorrect, is sufficiently insignificant to overlook, let it go. It doesn't matter. On the other hand, stick to your guns when you know that an editorial change is an important and necessary one.

• ***Editing by instruction.*** When confronted by situations in which authors wrongly object to editorial changes, attempt to enlighten them, in a tactful, non-patronizing manner, as to why changes were made. If they remain adamant despite your explanation, do it the way they want it. Remember, it's *their* names that will be associated with the work, *not* yours.

III. PRODUCTION AND MAINTENANCE of EFFECTIVE DOCUMENTATION

"Contextual Inquiry" is a field research technique for observing users in their work environment. Before producing documentation on job-specific procedures, the writers must understand the context in which they will be applied. This will assure that documents are tailored for the intended audience. For example:

• ***Work language***—the language they use to describe what they do. Are the words you're using the same as those used by the people for whom the document is intended? If not, change your language or provide a glossary. Also,

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011851

ascertain the level of knowledge of your audience; this should determine the words you use.

• ***Work structure***—the way they do their work. How does your prospective audience work? At home *and* at the office? Just at the office? In the field? Do they work with their hands? Is their job one that can be done 8 hours a day or only for a few hours at a stretch? Do they have the time to read the documentation? The answers to these questions will determine what sort of document you produce. For example, if it's a do-it-yourself manual, you'll need a publications design that is easily accessed by someone whose hands are occupied. A flat-lying, spiral-bound document with large print and plenty of white space and graphics would probably work best.

• ***Work goals and intentions***—their overall work goals and concerns. What are the deadlines and/or constraints under which users must work? What is the ultimate goal of their work? For example, if their job requires a thorough knowledge of a given subject, a textbook-like approach might be more appropriate. Should a basic working knowledge be all that's needed, a quick reference guide with section markers would probably suffice.

• ***Work product***—the product they need to create or the task they need to accomplish. How do existing working aids contribute to the performance of their task? What is it about those working aids they like? dislike? What would they like to see in future documentation?

When you create documentation that matches users' work language, structure, intentions, and product, that documentation is said to be "usable." By using Contextual Inquiry early in the documentation process, you are more likely to produce material that is usable and meets user needs.

Steps for Conducting Contextual Inquiry

1. ***Focus.*** Decide what it is you're trying to find out. Make sure your focus is narrow enough to allow you to zero in on pertinent and useful information in your interviews with prospective users.

2. ***Select participants.*** Find representative interviewees or, if you have time, take a cross-section of the work force.

3. ***Schedule the interview(s).*** Find a time most convenient for interviewees, when they can give you their undivided attention. Schedule the interview for 2 to 3 hours each. (Any longer will tend to fatigue both parties.) Get permission to record. Make sure you can see your interviewees in their work environment.

4. ***Conduct the interview.***

• Begin with a traditional interview.

• Observe the interviewee's work and discuss ideas concerning it:
- Ask open-ended questions.
- Let the interviewee lead the conversation.
- Listen!

• Conclude the interview
- Summarize your analysis.
- Ask "pet" questions, that is, questions you think you know the answers to.

• Thank the interviewee.

5. ***Extract the Data.*** Sift through the interview for usable information, but don't alter the data in any way and don't attempt to interpret. Use the interviewee's words. Extract important points for analysis and record them on Post-Its. Stick them up where you can see them.

6. ***Organize.*** Data are organized by their characteristics and relationships. Take the bits of data (on the Post-Its) and arrange them into groups of items that seem to go together. Allow the various categories to emerge. Come up with representative names for these groups. See if any categories fit under higher-level categories.

This mass of information should allow you to draw some valuable conclusions as to how you might best serve users of your product. By learning their specific needs, concerns, work environment, goals, etc., you will write and design materials tailored-made for them.

IV. DESIGN AND FORMAT

Having developed a thorough knowledge of your audience and collected the information required of your subject, you must create a strategy for presenting the material in the most effective manner possible.

Effective documentation requires the clear and concise translation of technology into accessible communication. Information design, while not

DOCID: 4011851

contributing quantitatively to a reader's knowledge, can facilitate the conveyance of information by presenting it in a "user friendly" fashion.

Information design should combine attractiveness with optimum functionality and effectiveness. The design process is a three-stage one:

1. ***Planning.*** Learn your subject. Find out everything you can about it. Again, *know your audience (potential users)* and find out what *they* need.

2. ***Development.*** Come up with an appropriate design. Write the documentation. Put together a prototype. Test the document on potential users. Collate and evaluate the results, and incorporate them into the final version.

3. ***Implementation.*** Produce and publish the manual. Solicit and monitor user responses. Create a schedule of maintenance for updates and design improvements.

Issues in Developing a Design

- Is the design you're creating appropriate to the subject? What is the purpose of your documents: are they going to be a quick, easy reference guide or a detailed instruction manual?
- Is the design durable? Is it one that will work in any context at any time, or is it perishable?
- Does it have impact? Does it make the user want to read the text it's attached to?
- Is it verifiable? Can it be demonstrated, through user testing, to be most effective?
- Is it cost-effective?
- Is it accessible, that is, easy on the eyes, well-organized, and interesting?
- Does it have lots of white space?
- Is it something you *don't* notice? A good design doesn't distract the user.

Visual communication (design) can have significant impact on how effective your text is in communicating your subject to a reader. "Visual literacy" is defined as the ability to create and use design to convey information.

Some Tools for Effective Information Design

- *Chunking.* This is defined as the breaking up of information into manageable sections. Related topics are placed together in an attractive, usable manner. This can be achieved with section dividers (tabs), separate volumes, headers.
- *Queuing.* This involves creating a logical progression of information so that each chunk of data builds on that which came before it. This should be done visually; possibly the simplest way to achieve this is with different levels of headers.
- *Filtering.* A way of organizing information for quick access, this method requires the arranging of information, whenever possible, into lists.
- *Multiple access.* This is defined as mixing the above elements in a document to accommodate the myriad ways people take in information.

V. DOCUMENT MAINTENANCE

Once you have produced your manual and released it to the field, it becomes necessary to document its reception by the intended audience and to keep abreast of developments in its subject area. This will allow you to perform the next important step in the process of producing documentation—maintenance. Maintenance in this context is defined as the revision of documentation for the purposes of keeping its information current, correcting mistakes, and/or incorporating user feedback to create a better product.

There are five basic steps for revising and rewriting manuals:

1. Preparation

- If need be, acquaint yourself with the subject of the original manual. Do some research.
- Look at the original type specifications and style sheets. See what was done before. If you don't like something, change it.
- Get training and input from subject-matter experts. If you don't feel you know enough about the subject (even after researching it), find people thoroughly versed in that area and pick their brains.
- Look at how the old manual is organized. Discard this organization if you feel it's not working. New information may require a change in the way the document is structured. Also, examine the current manual's table of contents; this, too, is a good indication of how the manual is organized and what it's about. Looking at the table of contents, you can tell

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011851

whether or not the document was chunked properly.

• *Solicit and document user feedback on the old manual.* Make sure you incorporate as much of this as possible into your revision.

2. Reading Phase: Read the original manual, then ask yourself the following questions:

• Does each chapter achieve what it sets out to do?

• Is there any text that just does not seem to belong where it is?

• Are any of the concepts confusing?

• Is any of the information outdated?

• Are the chapters properly laid out?

• Can you identify the target audience?

• Is it indexed? This is *very* important. A manual should have an index; it's not nearly as useful without one.

3. Research and Verification Phase: Get answers to those nagging questions that still remain and verify what information you have already. Refer to your subject-matter experts.

• Prepare your questions for these people in advance.

• Find a quiet place and a good time when they can give you their undivided attention.

• State a time limit in advance and stick to it. If you need more time, ask for it.

4. Organization Phase: Draft a new table of contents reflecting your additions and changes. Have your subject-matter experts check it out. Only they can determine if the organization you've imposed on the work is correct and the most useful.

5. Edit and Reworking Phase:

• Use your table of contents as an outline. Based on what you see there, estimate the time it will take for initial and second-party edits.

• Use a checklist of all the elements in the manual. As you proofread or edit each element, check it off and keep a record of how you treated it in a log book. This will come in handy for future revisions.

The maintenance of manuals (updating, redesigning, reorganizing, etc.) is seldom planned for or even taken into consideration. It should be, of course. If you don't plan for maintenance, chances are you'll put it off until your manual is so outdated, it requires a hurculean effort to bring it up to standard.

The 3-Step Cyclical Maintenance Process

1. Plan for maintenance. If your document is being published for the first time, create a maintenance schedule. Determine how often the document needs to be updated—every month? 6 months? a year? This depends upon the perishability of the information. For example, if the subject about which you are writing is in a contant state of flux, you may have to update the documentation for it fairly frequently.

2. Publish the initial document. If you *plan* for maintenance, you can get the document out where people can use it and, in due course, give you feedback for future revisions. Be sure you *ask* for feedback; set a deadline for it. Keep a log of all the comments you receive, then, when it comes time to perform maintenance on the document, act on what you've been told. Should you receive feedback *after* the deadline, save it for the next maintenance cycle.

3. Create a maintenance guide. This should contain the following:

• a cover page with the title, authors and/or contributors, and any other information that helps to identify your manual;

• a table of contents;

• a brief description of the document—what it's about, what it looks like, etc.;

• maintenance requirements
- maintenance schedule;
- a person responsible for each section (the subject-matter expert, or, if the project has been divided among a number of editors, the editor in charge of each section);
- maintenance process—the detailed plan to bring a particular manual up-to-date;
- location of material—where is it, how to get it, where all the originals (graphics, photos, charts, etc.) are kept, how the material is organized;
- software used to generate the original copy;
- style guidelines (specs, style sheet, a list of your deviations from the original);
- a list of graphics, figures, charts, and tables, and a brief description and the source of each (Note how these elements were incorporated into the document—scanned, drawn, pasted, waxed, or typed in);

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011851

- production information: schedule, cost (if applicable), tabs, loose leaf or perfect bound, trim size, cover design/color, paper stock; two- three- or four-color; where printed, number of copies;

- distribution—who gets it and where are they located. (This is important. You need to know your customers' names and addresses in order to send them updated versions, solicit their feedback, and to keep track of how many manuals you have in circulation.)

VI. SOME POINTERS

• Rag right is the most "user friendly" text format; besides preventing "rivers," it also rescues the reader from the rigidity of "boxed in" justified text.

• Rag left is very unusual and can be a most effective attention-grabber if used sparingly.

• For long blocks of text, serif type is still preferred over sans serif.

• Heads, lists, anything not strictly text, are forms of graphic and should be treated as such.

• You must have *some* white space in every graphic.

• Half of a text page should be white space (includes margins, leading, gutters, etc.).

• For more interesting headers, put rules above them. This will make them stand out more. Also, make sure all heads, lists, etc., are consistent throughout your document.

• If you use bullets for lists, make sure that the bullets are 2 points smaller than the text they precede and are centered.

• A line of text on a single column page should run 1½ to 2½ alphabet lengths (40–60 characters depending on the font).

• Use en-dashes (–) for inclusive numbers and em-dashes (—) instead of standard dashes to separate clauses.

• *Never* underline text unless you are typing. Use italic for anything you're emphasizing.

• You may want to consider vertical rules between two or three columns of rag right text. They help to separate columns visually, and they look nice.

• Borders can either be physical, visual elements (rules, for example) or white space. Make sure all rules are proportional to the text they set off.

• While color can make your document look especially sharp, it is very expensive. A workable alternate is to use screening, a relatively inexpensive and simple procedure, that allows you to take one color, black for example, and turn it into gradations of grey. You can thereby have a number of "colors" for the price of one. Colored paper is another way to sneak in additional color.

• When dealing with printers, get samples of something similar that they have done to see how they handle it.

• Non-standard trim sizes are *very* expensive and can cost more to mail. Unless you have a compelling reason for using a non-standard trim size, don't.

VII. THE EXHIBITS

As is usual in professional conferences, various vendors and contractors were present: printing and publication services, translation tools and services, data conversion, editing and design consultants, commercial trainers, university courses in rhetoric. Not surpringly, the printed word is yielding to electronics; CD roms are replacing multi-volume reference books. The GPO is a leader in CDs with maps, statistical information, and other references, from agriculture to zoo. Some vendors had drawings and contests, with rewards ranging from keychains to computers.

The highlight was the exhibit of prizewinning entries in many categories: technical articles, whole publications, brochures, newsletters of small, large, and medium circulation, books, computer documentation, house organs, organizational materials, and so on. From the top down, the four levels are Distinguished, Excellence, Merit, and Achievement. Those of us working on periodicals paid particular attention to the categories Whole Periodicals and Newsletters. The Distinguished were simple in design and easy to read, while Achievement were more cluttered. We paid particular attention to details that characterized the contrasting top and bottom categories.

A concurrent competition was also held for Technical Art. In addition, there was an

DOCID: 4011851
P.L. 86-36

audiovisual theater in which the prize-winning entries were shown.

It should be noted that under the aegis of [redacted] *the NSA Newsletter* won an Achievement award in the regional competition of 1985. (*N.B.*: it was submitted, with permission, through channels.)

Special mention must be made of the Online Hit Parade. It consisted of well over a dozen computers, with just about every operating system, including multimedia. Users were invited to test the demos and evaluate them. Among the interesting ones was "Civil War and Reconstruction," a hypercard stack to teach high school students about the civil war. This was designed by Miss Shirley Moore's History Class at the Emma Willard School, Troy, NY.

VIII. A NOTE on PROTOCOL and MORE ADVICE

Exchange of cards is a ritual common to professional societies. Some of us had privately printed cards with our home address and telephone numbers, listing ourselves as "Editor-Writer" or some such. It is advisable to have cards made up--at your own expense--otherwise you may be conspicuous. (The CRYPTOLOG editor can help you on this.) Besides, you might win something in a drawing!

The sessions consist of lectures, panels, workshops, "progressions," (in which you rotate after some minutes) and storyboard talks. A lecture is best if the subject is new to you, while workshops usually require command of terminology and some experience. "Progressions" is suitable for people who are very experienced in the subject. Unstructured panel discussions and storyboarding vary greatly in quality.

The proceedings are mailed to you in advance. We recommend taking that hefty tome with you to help select your choices among the concurrent sessions; you might want to change sessions. Also, we recommend loose-leaf format rather than perfect binding. It's easier to reproduce articles.

We wish that we had thought of taking a camera with us for shots of winning entries. Some people bring tape recorders, as well.

XIX PROFESSIONAL SOCIETIES and JOURNALS for WRITERS, EDITORS, and PRESENTERS of INFORMATION

Society for Technical Communication, 901 N. Stuart Street, Suite 304, Arlington, VA 22203. (703) 522-4114. Individual membership, $85 per year. Includes quarterly issues of the journal *Technical Communications* and 10 issues of the newsletter *Intercom*. There are local chapters in Washington and Baltimore.

Annual meetings are held in major cities in the US and Canada. Future meeetings:

1992 May 10-13, Atlanta
1993 June 6-9, Dallas
1994 May 15-18 Minneapolis
1995 May 7-10 Washington DC
1996 May 5-8 Seattle
1997 May 11-14 Toronto

Another society concerned with presenting information is the National Association of Government Communicators, 669 S. Washington St., Alexandria VA 22314. (703) 519-3902. Annual dues are $65. Includes 10 issues of the magazine *GC*. Local chapters have monthly meetings. It, too, sponsors a competition. Its next conference will be held the second week of January 1993, in Old Town Alexandria.

The *Proceedings* of the 1991 conference may be seen at the A64 Publications Office; Ops 2A 0950. Please call [redacted] at 963-5683 for an appointment to view.

P.L. 86-36

The *Proceedings* of 1988-1991 and other publications of the STC may be consulted at the CRYPTOLOG office, Ops-1, 2N018. Please call the Editor, [redacted] on 963-1103 for an appointment to view.

The *Journal of Technical Writing and Communication* is published quarterly by the Baywood Publishing Company, 26 Austin Ave., P.O. Box 337, Amityville, NY 11701. Annual subscription is $36.00, plus $4.50 per volume in the US and Canada. The executive editor is on the faculty of Rensselaer Polytechnic Institute, Troy, NY. CRYPTOLOG has a sample copy.

~~FOR OFFICIAL USE ONLY~~

From the Past

922

DISPOSITION FORM

SECURITY CLASSIFICATION (If any)

~~CONFIDENTIAL~~
Modified Handling Authorized

FILE NO.

SUBJECT Model for Cryptanalytic Technical Reports

TO Distribution FROM AD/PROD DATE 27 February 56 COMMENT NO. 1

1. The preparation of clear and concise technical reports is an important facet of PROD operations. In technical reporting, clarity and detail are paramount, especially when writing reports on the solution of a new type of cryptosystems encountered for the first time. Such reports should embrace a complete resume of the diagnostic techniques employed in the identification of the system, as well as a comprehensive outline of the steps taken to arrive at the first recoveries of plain text. It goes without saying that close attention should be paid to precise cryptologic terminology in all descriptions of methods and techniques, so as to lessen the chance of ambiguity or possible misunderstanding by the reader. A cryptologic glossary should be freely consulted when the writer is not sure of the exact meaning of a term he is about to use.

2. The attached paper, an extract from the NSA text "Military Cryptanalytics, Part I," is published as recommended reading by, and for the guidance of, all PROD personnel engaged in writing cryptanalytic technical reports. It illustrates what may be considered as a model for such reports. There is no fixed, standard format for these reports because the form and content of each individual report depend on circumstances at the time of writing. However, the attached report on the solution of a hypothetical system is intended to illustrate the amount of detail that might be included.

A. Sinkov
A. SINKOV
Assistant Director
Production

Inclosure
a/s

Distribution: Branch level of
NSA-70 and NSA-90

9221 [illegible]
9222 [illegible]
9223 [illegible]
9224 [illegible] file

922 GH
922K [illegible]
~~922 file~~

DD FORM 1 FEB 50 96 REPLACES NME FORM 96, 1 OCT 48, WHICH MAY BE USED.

U. S. GOVERNMENT PRINTING OFFICE

A copy of the document in question may be obtained from CRYPTOLOG. For a copy write your name, organization, and building, and send it to: CRYPTOLOG, P0541, Ops-1.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011851

Editorial

PERSUMs, TECH TRACKERS, FOR THE USE OF

Now is the time to reconsider the PERSUM.

In his article, "Where are our Textbooks?" (1st Issue 1989) Dave Gaddy decries the lack of technical papers, textbooks, and monographs of recent vintage. They are no longer produced as they once were in the past. Why is that, he asks. And then he speculates on the reasons, and offers a few suggestions.

What he has not taken into consideration, however, is the wording of the instructions in the PERSUM on listing publications. Turn to page 3:

12. PUBLICATIONS (List titles; do not confuse this with reports prepared as a regular part of the job)

Now, at last, we know what really happened. You are not to list reports written as a regular part of your job. So there are no brownie points for writing a working aid, a technical how-to, a reference, a wrap-up report, or the documentation of a technique, as writing them is considered "part of your job." For such papers—when written—are published in an organization's own series, and often, for a limited distribution. They are designed for a specific purpose, for a specific application. They do not fall into the category of general information that would or should appear in a publication such as *The Cryptologic Quarterly* or CRYPTOLOG. Nevertheless, these are the very publications whose absence Dave laments.

So, as the effort is not rewarded, such papers are not written.

Rather, the technical person is better off publishing an unclassified piece, however trivial, in an outside journal: there's far more prestige attached.

Is there a solution? Of course there is.

To encourage the publication of our technical papers, to ensure the continuation of our very own heritage, thus assuring the passing on of the torch, what we should do is to revise #12. It should read:

12. PUBLICATIONS

a. Documentation, working aids, technical how-tos, references, wrap-up reports and monographs prepared as a regular part of the job.

b. Articles in NSA journals.

c. Articles in outside journals.

As a columnist recently wrote in the business section of *The Washington Post*, the greatest assets of IBM are its smarts, yet, according to its accountants, its "massive intellectual property holdings are worth less than swamp land in Florida."

This principle applies in NSA as well. We know that our adversaries are moving heaven and earth to get information about our knowledge and techniques. And we know all too well the value, in dollar amounts, they place on specific pieces of information.

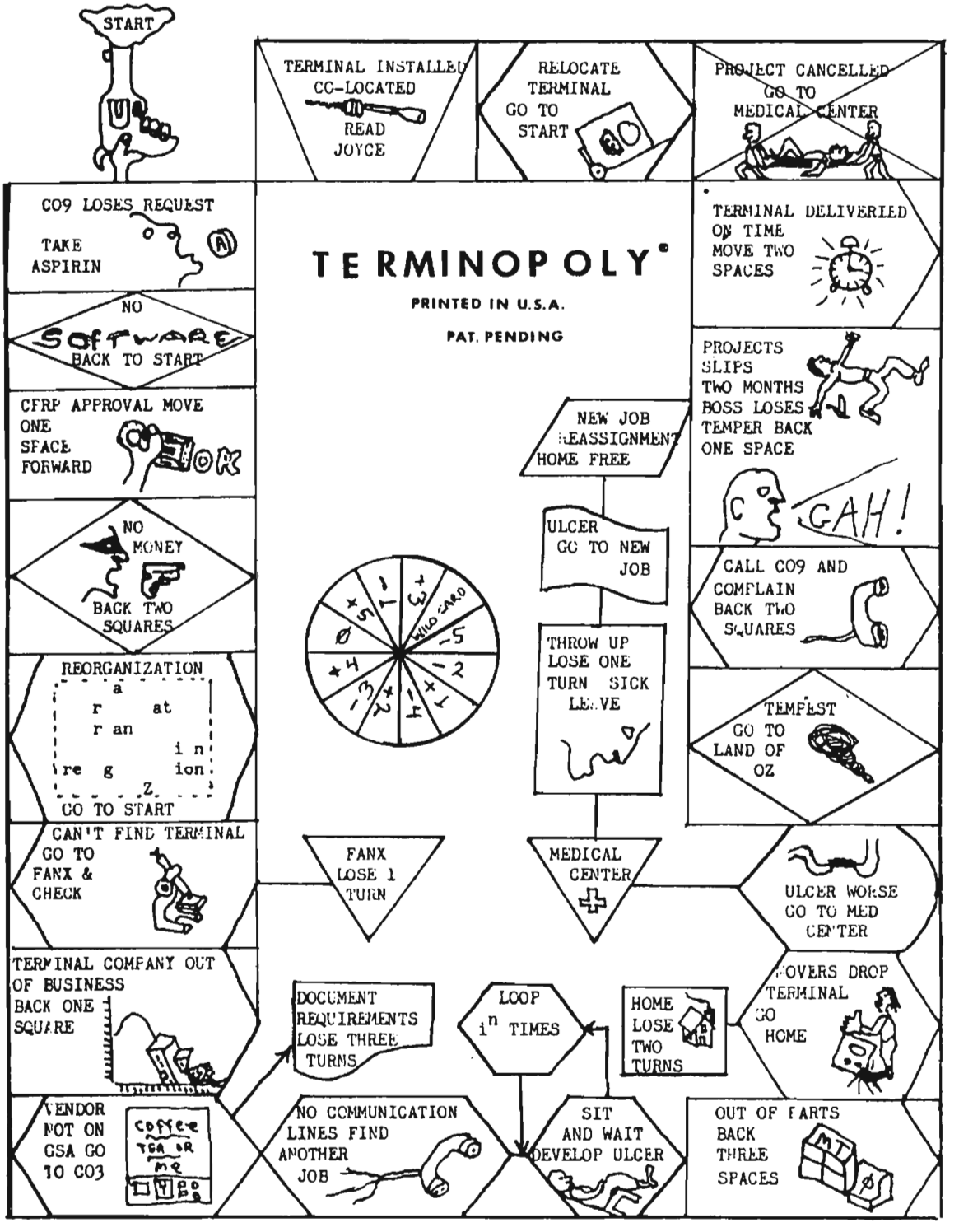
But this intellectual property, this knowledge, these techniques, are not held in high regard at NSA.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011851

Reprinted from C-Liners, *Vol. II, No. 3, Issue 13, November 1973*

Golden Oldie



~~FOR OFFICIAL USE ONLY~~

DOCID: 4011851

Editorial Policy

CRYPTOLOG is a forum for the informal exchange of information by the analytic workforce. Criteria for publication are: that in the opinion of the reviewers, readers will find the article useful or interesting; that the facts are accurate; that the terminology is correct and appropriate to the discipline. Articles may be classified up to and including TSC.

Technical articles are preferred over non-technical; classified over unclassified; shorter articles over longer.

Comments and letters are solicited. We invite readers to contribute conference reports and reviews of books, articles, software and hardware that pertain to our mission or to any of our disciplines. Humor is welcome, too.

Please note that while submissions may be published anonymously, the identity of the author must be made known to the Editor. Unsigned letters and articles are discarded.

If you are a new author, please request "Guidelines for CRYPTOLOG Authors."

How to Submit your Article

Back in the days when CRYPTOLOG was prepared on the then state-of-the-art, a Selectric typewriter, an article might be dashed off on the back of a used lunch bag. But now we're into automation. We appreciate it when authors are, too.

> *N.B.* If the following instructions are a mystery to you, please call upon your local ADP support for enlightenment. As each organization has its own policies and as there's a myriad of terminals out there, CRYPTOLOG regrets that it cannot advise you.

Send two legible hard copies accompanied by a floppy, disk, or cartridge as described below, or use electronic mail. In your electronic medium (floppy, disk, cartridge, or electronic mail) please heed these strictures to avoid extra data prep that will delay publication:

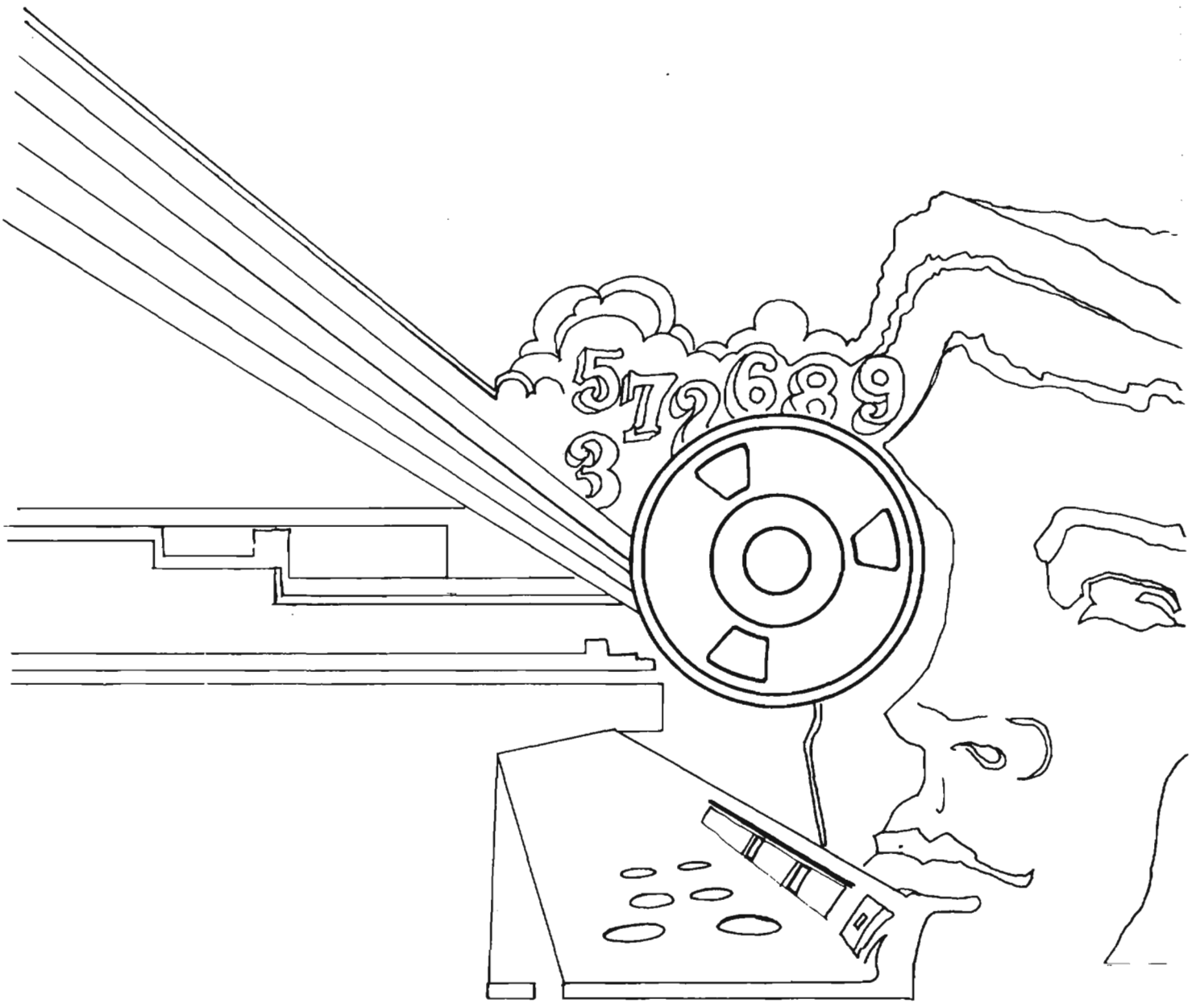
- do not type your article in capital letters
- do not right-justify
- do not double space between lines
- but **do** double space between paragraphs
- do not indent for a new paragraph
- but **do** paragraph classify
- do not format an HD floppy as DD or vice-versa–our equipment can't cope
- label your floppy or cartridge: identify hardware, density of medium, software;
- put your name, organization, building and phone number on the floppy or cartridge

The electronic mail address is *via* PLATFORM: cryptlg @ curator
or *via* CLOVER: cryptlg @ bloomfield

CRYPTOLOG publishes using Macintosh and Xerox Star. It can read output from the equipment shown below. If you have something else, check with the Editor, as new conversions are being added.

SUN	60 or 150 MB cartridge	ascii only
XEROX VP 2.0, 2.1	5 1/4" floppy only	
WANG		Stand-alone or Alliance
Macintosh	3 1/2" DD disk only	Please furnish a copy in TEXT as well as in your software, as we may not have all the software upgrades
IBM & Compatibles	3 1/2" DD or HD 5 1/2" DD or HD	Please furnish a copy in ascii as well as in your software, as we may not have all the software upgrades

~~FOR OFFICIAL USE ONLY~~


5 7 2 6 8 9
3

DOCID: 4019718 Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

3rd Issue 1991

P.L. 86-36

EDITORIAL ii
KEYNOTE ADDRESS . . . . . .Robert E. Rich 1
FAREWELL TO THE TROOPS. . . . . [redacted] 5
ACHIEVEMENT THROUGH PEOPLE. . . . . [redacted] 8
THE LANGUAGE ANALYST AND AUTOMATION . . . [redacted] 13
SIGINT IN AN OPEN SOCIETY . . . . . [redacted] 17
THE WAY IT WAS. . . . . [redacted] 22
A VIEW OF L . . . . . .Dale Seaberg 31
KEYNOTE ADDRESS . . . . . .Gerald R. Young. . . .33
FROM THE PAST 40
ODE TO SIGINT. . . . . .Al Friendly. 41
A MODERN FAIRY STORY. . . . . [redacted] 42
GOLDEN OLDIE. 4,7
TO CONTRIBUTE 44

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

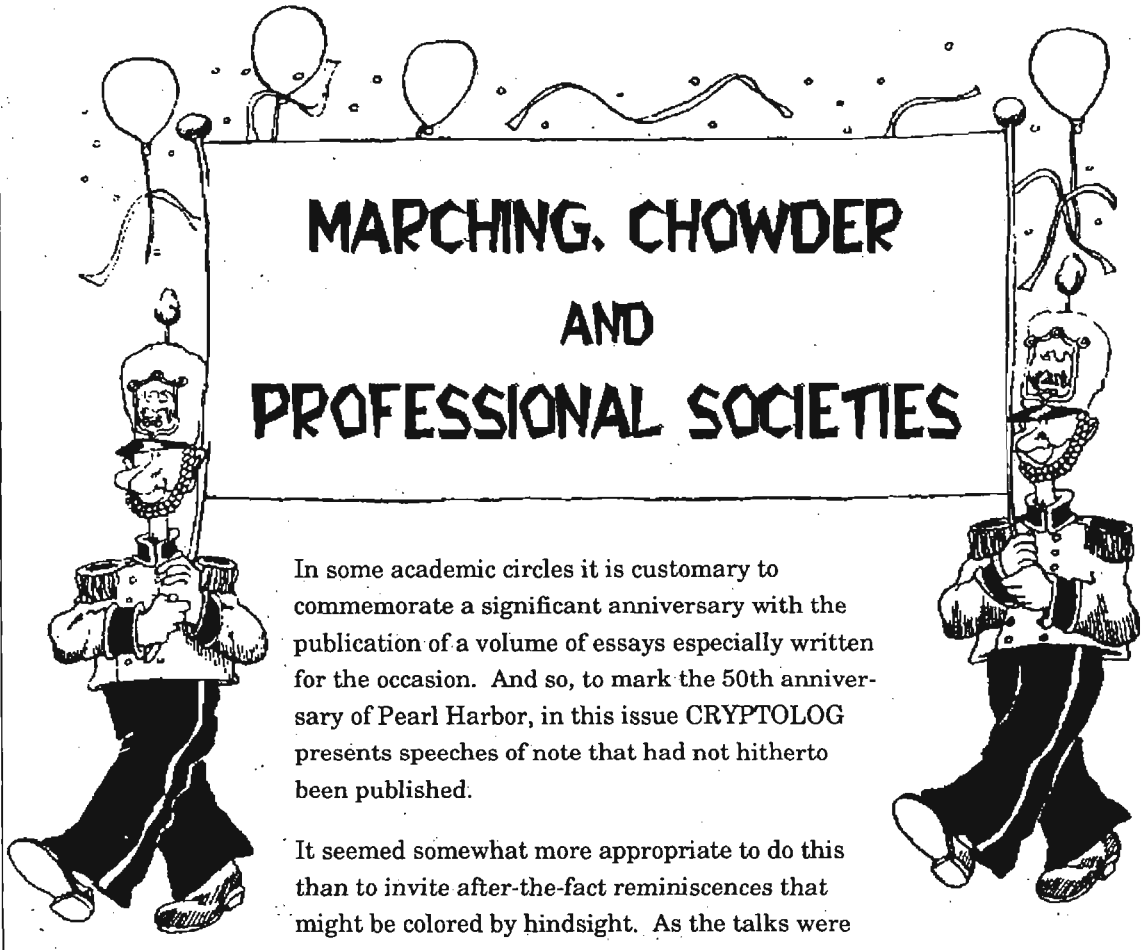
~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

DOCID: 4019718

Three Cheers For NSA's



In some academic circles it is customary to commemorate a significant anniversary with the publication of a volume of essays especially written for the occasion. And so, to mark the 50th anniversary of Pearl Harbor, in this issue CRYPTOLOG presents speeches of note that had not hitherto been published.

It seemed somewhat more appropriate to do this than to invite after-the-fact reminiscences that might be colored by hindsight. As the talks were contemporaneous, they express the actual concerns of the moment. They are snapshots of our past: what we thought was important at the time; what we were worrying about.

It is interesting to compare the salutatory and valedictory articles; each by a deputy director, to the same audience five years apart. But what five years!

Another custom in academic circles is to dedicate the publication to a worthy party.

Though little known outside the confines of our stronghold, NSA's professional societies play a critical role in disseminating information. To a great extent, the talks, symposia, conferences and seminars they sponsor serve to educate the technical cadres in a manner that formal courses of instruction cannot approximate. Classification permitting, any analyst may attend any talk, whatever the discipline. No requirements! No tests! Just information.

And so this issue of CRYPTOLOG is dedicated to NSA's professional societies.

Long may they flourish!

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019718

Keynote Address

Robert Rich, ret.

This article is classified ~~TOP SECRET UMBRA~~ in its entirety

This is an abridged version of the Keynote Address delivered to the 1985 session of CA-305, Contemporary Issues in Cryptanalysis. At the time the author was Deputy Director of NSA.

The business of the Agency is decrypting secret communications, so cryptanalysis is the crucial NSA activity, and the cornerstone of cryptology. I hope it will be of interest to you to start the week with an assessment, from my perspective, of the state of health of our cryptanalytic activity and what the future may bring.

As Deputy Director I am rather removed from matters of substance, but I believe that the present state of health is quite good. In considering the health and the future of cryptanalysis and cryptomathematics, it is meaningful to use a broader definition of the scope of our cryptanalytic activity. [redacted] people that we consider to be included in our cryptanalytic effort at NSA have diverse skills in such fields as language, engineering, signals analysis, collection management, and other fields, as well as cryptanalysis and cryptomathematics. Indeed, it is common for individuals in our analytic population to be highly knowledgeable or expert in several of these areas. In most of my remarks about the health and future of CA I will refer to this broadly defined cryptanalytic arena since I think the topic can be better addressed in this way.

I also think that the health of cryptanalysis has improved markedly, especially in the last three or four years. This assessment is based on the results being achieved, opportunities being presented by our targets, quality of the workforce, the present work environment, available tools, benefits provided by collaboration, and some organizational factors. I will touch on each of these because I think they are important in determining the current state of our cryptanalytic health.

RESULTS

[redacted]

~~TOP SECRET UMBRA~~ EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36
DOCID: 4019718

[redacted]

The other kind of CA results, those produced by our COMSEC cryptanalysts, continue to have profound influence on the design of our own cryptologics.

EO 1.4.(c)
P.L. 86-36

THE WORKFORCE

Looking at the cryptanalytic workforce, we find that it has been growing steadily for the past four years at a rate well above the Agency average, and that attrition, especially that due to resignation is very low—less than half of that for the entire Agency—which, by the way, is also remarkably low, about 2.7% for resignations. The CA intern program and the P1 cryptomath program are operating with [redacted] about 70% increase over the number of three or four years ago.

Considering the work environment and the opportunities it offers, it is fair to say that it is good. I see the creation of the technical track and the increased opportunity for reward through promotions and awards to be very positive for your profession. Furthermore, I think that we are doing a reasonably good job in providing for seminars, conferences, and other means of bringing our analysts together for sharing views and problems. Such gatherings as the annual Cryptomathematics Exchange, the Kryptos meetings, and CA-305 are very well attended, and the reports I hear are good.

The [redacted] program, in my opinion, bodes well both for improving the quality of analysis and for contributing to the continued professional growth of our analysts. It will enhance the variety and richness of work experiences that analysts already enjoy and which think is a major factor in the low attrition rate. I would emphasize here that we intend to operate this program intelligently, giving due consideration to the need for continuity on the various problems. I hope that you have noticed that the [redacted] managers have operational backgrounds.

P.L. 86-36

TOOLS

Turning to the tools and systems available for our cryptanalysts' use, it would be difficult to find a more impressive work environment or one better served by computers and special-purpose electronic equipment. [redacted]

Our relationships with our major cryptanalytic collaborators [redacted] are strong and profitable, and add greatly to the cryptanalytic health. [redacted]

ORGANIZATIONAL FACTORS

Finally, there are organizational factors which relate to cryptanalytic health. As you know, we are organized principally by target because we think this maximizes synergism. When people talk about functional organization, cryptanalysis is one function often singled out as potentially benefitting. We have repeatedly opted not to change our mainly target orientation but instead, to rely on such cohesion-producers as seminars,

EO 1.4.(c)
P.L. 86-36

conferences, Kryptos, CMI, CA-305, the math and intern programs, and the panels to promote within-professional contacts.

In addition, at the recommendation of NSAAB the Director appointed a CA Council three years ago which I chair and which serves the functions of high-level advocacy and oversight. For the past three years, we have made an extensive annual review of our cryptanalytic effort for the Director and top Agency leaders. The purpose is to better inform of the progress and state of Agency cryptanalysis. I think these organizational arrangements are close to the best that we can design at this time.

So as not to portray the view that I think everything is roses, I must tell you that some our cryptanalytic managers believe that our exploitation-research split is out of kilter; that is, we are too exploitation-oriented and are not devoting enough resources to the difficult research problems; much of our success stems from past research successes and our current exploitation may, to an extent, mortgage the future.

I do not totally accept this view, but I do agree that we need to be devoting more effort to difficult unresolved problems and those that we know are coming up in the future. I further think we are making reasonable strides in doing this now. Our research efforts have been strengthened markedly in the past two or three years, particularly in A5, S6, and R5.

LOOKING AHEAD

The rest of this talk concerns the future of our cryptanalytic activity. There is at least one thing we can say with confidence: the long term future ultimately depends on continued success. In my view, the outlook for continued success is good, based on our present posture, knowledge, and momentum. These factors are often forgotten or greatly minimized when prognosticators discuss the future. I want to emphasize them. We have an impressive knowledge base concerning our targets' structures, practices, habits, and systems. It derives from years of study by dedicated analysts and probably one of the most important parts of it is the information our analysts carry around in their heads. In this connection I want to again mention [redacted] We mean to be sure that [redacted] is run in a way so as to enhance the knowledge base.

But our knowledge and momentum, while exceedingly important, will not alone ensure success in the future. I must hasten to add that there are enormous technical challenges to be dealt with. We must devise very clever ways to obtain solutions using all our "black art," as cryptanalysis once was considered. But with appropriate effort we can deal successfully with sufficient numbers of these challenges to keep our production strong and our own systems secure.

THE CHALLENGES

The major technical factors and trends that must be faced by our Operation analysts are well known to most of you. Basically, they include advances in transmission technology, advances in cryptography, and difficulties resulting from a greater world-wide awareness of cryptography and cryptanalysis. [redacted]

Added to that are the important cryptographic advances stemming from the rapid spread of microprocessor technology and greater use of software-based or more easily changed systems. We are seeing many more new commercial machines and a significant growth in the number of indigenous machines being developed and employed by our targets. Solving these problems will require a dramatic speedup of some of our current methods as well as development of totally new and imaginative techniques.

Our COMSEC cryptanalysts have to cope with the growing complexity and rapid development of US civil and military communications systems and the complex crypto requirements related to securing these systems.

Moreover, public awareness of cryptanalytic techniques, the declassification of WW II data and publications about that era, along with the in-

DOCID: 4019718

crease in non-governmental requirements for cryptography and the attendant public research, have stimulated interest in cryptography and cryptanalysis worldwide and will affect future target cryptography. Another factor affecting the future is the recent strong academic interest, resulting in numerous international conferences and publication of papers on the subject. Operationally, we already see more attention to COMSEC by some of our targets which probably can be traced, at least in part, to the new awareness.

Balanced against these kinds of developments that cause problems for cryptanalysts are many opportunities [redacted]

Also, of major importance is the fact that our successes have given rise to a general recognition by SIGINT users and government officials of the value of our product and a demand for SIGINT that is difficult to overestimate. The result is powerful support for obtaining the resources we need to do the job.

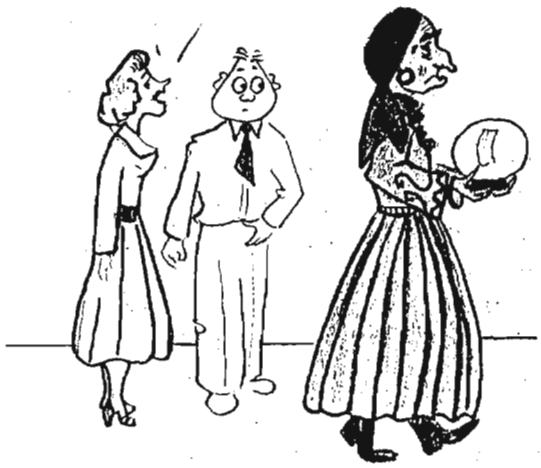
To summarize, I conclude that the health of our cryptanalytic effort is exceedingly good. I am optimistic about the future, but I think we should brace for the challenges to be faced. To help insure future success we intend to continue to pursue objectives that we are already committed to: namely, a broadened research capability; superior development and training opportunities for the workforce; the ability to recruit and hold the best talent available; maintenance of superior tools and processing systems; devotion of sufficient resources and talent to collection, signals processing, and other supporting problem areas; and provision of rewards for technical accomplishment.

P.L. 86-36

Golden Oldie

[redacted] *c 1955*

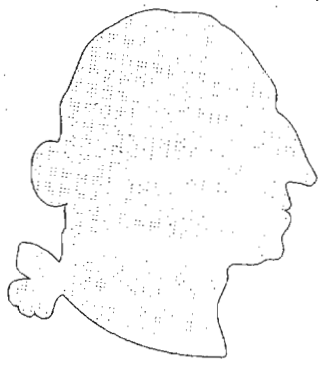
EO 1.4.(c)
P.L. 86-36



She's cracked TWO systems ALREADY!

DOCID: 4019718

Farewell to the Troops



P.L. 86-36

This address was delivered by the author on the occasion of his retirement in May 1979. At the time he was head of audiovisual services at the National Cryptologic School and the Learning Centers.

(U I don't like saying good-byes. They're difficult for me to say. Almost—but not quite as difficult as saying to my various bosses during these past 38 years,"You're sure right, boss. You're absolutely correct." What I have said to them has varied depending on the situation—but it hasn't been **that**!

(U) I must ask your indulgence in my using a script. It is my nature to become emotionally involved with the people and issues of work—and I didn't want that inclination to becloud the message—which concerns the School. Sorry about that, S folks. In any event, think of these next few moments as acupuncture—a friendly needle.

(U) Start with O'Brien's Law; O'Brian is a first cousin of Murphy: "At some point in the life cycle of every organization, its ability to succeed in spite of itself runs out." The NCS may be approaching that point. I think so because of two different problems which have been distantly related but now are converging rapidly:

- the organization and internal processes of the School
- the consolidation of all cryptologic training under NSA, under a single training director.

(U) Let me take them in order. This School teaches a much greater variety of more complex courses to a more and varied and operationally demanding student group than do the Service schools. Despite this obvious fact, two years we reorganized along the Service pattern, who in turn had gotten it from some contractors who had developed it for industry—and profit. But the new structure is only part of the problem. The other, and even more serious part, is the growth of minimum-value work engendered by the theory behind the structure. I refer to requirements analysis and course development by formula.

(U) Requirements analysis done only after someone else has identified a need and describes it in writing is as ritualistic as swearing in a witness and about as useful a tool for getting evidence. This analysis is followed by course development-by-formula which starts with micro-documentation of trivia. These activities occupy the time and energies of many people. I don't object to the fact that the analysis follows when it should precede requirements. Instead of reacting to training needs discovered by people in the operating jobs, we should have qualified school people living full time in the operating elements, people who are given easy access to the DDs and ADs—access as least equal to that of contractors—as well as to the section chiefs. These should be people who become sensitized to the smell of trouble and who can sniff hard enough to figure out the cause and whether training could help.

(U) And I do object to fixed-formula documentation which can easily result in professional people spending almost as much time in planning and

~~FOR OFFICIAL USE ONLY~~

scheduling and reporting and concept writing and getting permission to do what their various certificates and job descriptions say they are capable of and paid to do as they spend in creating the actual lessons and tests.

(U) In my view the result of all of this is that first, inadequate attention is being given to NSA's urgent training needs early in the power curve of their emergence.

(U) Second, wrapping the development action in layers of paper loses more time and insulates the developer from the grime, the essence, the reality of the training need. In fact, the whole analysis-development formula reminds me of previous flashes in the managerial plan. Remember PERT? and MBO? Know any place where they are still being used by the people who are doing the work? These techniques are valid but probably only in the specific conditions which spawned them. Their wholesale adoption by a management for different conditions is where the mistakes have been made.

(U) As I said, the current NCS organization is based on a training development formula developed by other people for other conditions. I've no doubt it's valid for those conditions—but for the NCS they are a mistake, a disaster. Well, you're not obliged to accept this mistake any more than my successor is obliged to perpetuate my mistakes. One of the benefits, as well as a prime reason, for changing managers periodically is to provide a graceful opportunity to abandon the previous manager's mistakes. I urge that this opportunity not be allowed to slip away.

(U) The second of the converging problems is the consolidation of all cryptologic training—which seems to have been launched though it hasn't left the ways. I know that we didn't initiate the current action—remove the blocks, to continue the metaphor—and I know, like a genuine launching, it's impossible to stop once started. But then we didn't protest very hard against it, either. Worse yet, for years we didn't attempt to deal realistically or imaginatively with the problem that got Congress upset in the first place: namely, the rapidly escalating costs of training. We still haven't. Instead, a succession of Commandants have gone in the opposite direction from economical training and have steadily worked at creating a pseudo-college, an institute, complete with deans, curriculum chiefs, learned journals, accreditation, an enormous catalog; in short, all of the trappings and burdens and costs and irrelevance of academia.

(U) Meanwhile, needs here and in the field go unmet or poorly met and contractors grow fat doing system operating and maintenance—even the management—that the Agency is incapable of keeping up with using its own people. For the fact is that building a liberal arts college when we should have been building a trade school—a multilingual trade school, to be sure— has not done much for the real need, namely training in the acquisition, operation, upkeep and management of the galloping technology of SIGINT and COMSEC.

(U) No wonder Congress got frustrated and pressured DoD into consolidation. But that's a mistake too, for the belief in consolidation stems from the myth that one **big** something is more economical and efficient than several **small** somethings. General Motors learned that it isn't necessarily true years ago. Consolidation is a huge red herring, large enough to stock all the delicatessens in the Baltimore-Washington area for a year.

(U) It is a political issue from start to finish. There is no indication that consolidation will materially improve the numbers or quality of cryptologic technical and management people. In fact, the ITRO report did not seriously address quality. And I can accept that, for the ITRO team was, in effect, given a decision to justify. And that's okay too in a political area. The trouble, **the real trouble here**, is that the training arena and the political arena are all under one roof, the NCTS. Thus, it is here that the two problems I identified at the start are in fact converging. And I think that unless that convergence is deflected, O'Brien's law will inexorably take over; our ability to succeed in spite of ourselves will run out.

~~(FOUO)~~ My criticism of the current NCS structure and procedure centers on my belief that the

need is not for formula development of courses or centralized management of training. The urgent need today is to find ways to derive the training directly from, and fit it to, the technology and pressures of the operations. If that is correct, then it follows that training action comes first and political action second. And I say that neither critically or cynically. To the extent that there is a tangible, separate, schoolhouse—to use today's buzz term—is the extent to which we have failed to meet the urgent needs of the cryptologic community. Instead of talking about and planning consolidation of schoolhouses, we should be talking about and planning training outposts, outposts stafffed by a Training Corps whose members go out and live in the native villages [redacted] –not sitting back here endlessly and wistfully planning larger and more elaborate central facilities.

(U) Oh, but you say, be practical, be realistic. Congress has pressured us and the Secretary of Defense has directed us. Okay, I'll be practical and realistic and do so with one recommendation:

(U) Remove the political activity from the schools and do it somewhere else. Cut the TDNS/CNCS double hat in half. Remove, and I mean **physically**, from the NCS and the Service schools, the small group needed to develop and orchestrate the consolidation plans and actions. Take them, all of them, out of the operational and managerial channels of the schools. Take the political activity and all the attention it demands off the backs of the teachers and developers and requirement analyzers. Give the School—each school—a full-time commandant with the authority and the opportunity to get the training done as his or her first priority. And then reorganize the school part in such a way that it molds itself to the operating needs and not vice versa. Start up the Training Corps and post them out there. A separation of training action and political action could result in both being done better. It puts neither politics nor training in second place.

(U) And take it from one who knows full well the price that goes with putting politics in second place.

□

Golden Oldie

[redacted] *1955*

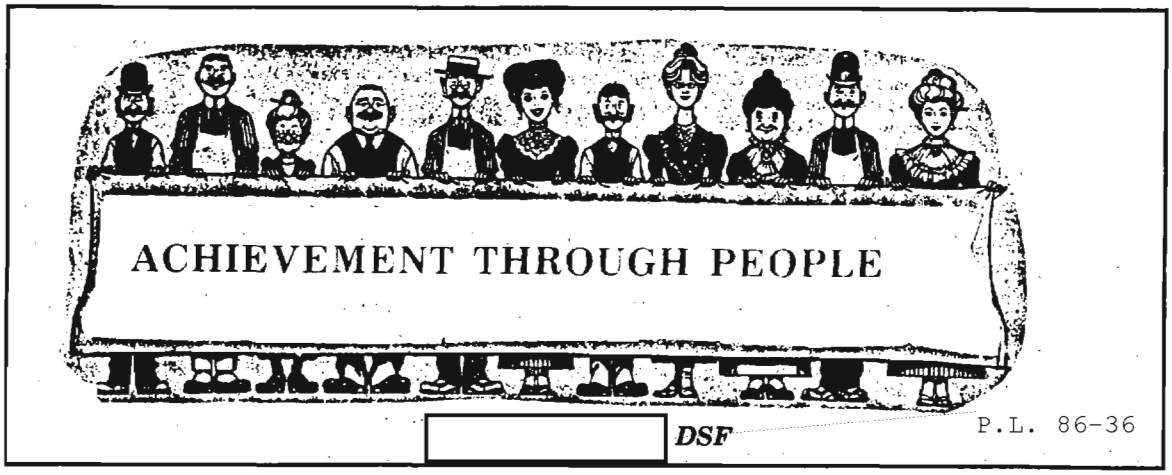
I JUST KNOW I'M GONNA BREAK INTO SOMETHING TODAY!

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

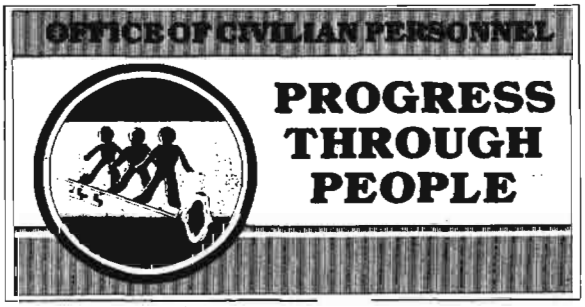
P.L. 86-36

DOCID: 4019718



This article is a condensed version of a talk given to the Human Resources Management Association on 27 February 1986. At the time the author was Director, Civilian Personnel, Chief, M3.

"Achievement Through People" -- this is the goal of every organization and every manager everywhere. No one can achieve an organization's mission without people. People are the most important resource, the key, as our M3 logo shows:



This logo was designed by a person in M3 as part of our 5-Year Plan, which I'll describe later. One of the Task Groups under that plan held a logo design contest and the winning one has become our official M3 logo. We use it everywhere: on posters, awards, all printed publications.

The word "Management" means achievement through people. The task that every manager faces is to find the best way to use this precious resource to accomplish the mission. In this paper I am going to talk a bit about management and what my philosophy is; show specific examples of some creative things we are doing in M3, and conclude by telling you how we are doing--where we've succeeded and where we still have a way to go.

MANAGEMENT PHILOSOPHY

Obviously there are many ways to manage people. One's management style is very individual, a blend of one's personality, energies, interests, enthusiasms and skills. It is also a product of what you yourself have experienced under different managers. In my own case, I have always had a lot of ideas. From the day I came to work here I have always wanted to contribute those ideas to help solve problems and to improve the way we do things. Sometimes I could, but sometimes I couldn't. It depended a lot on the management style of the person I worked for. So my own experience influenced my management style.

The climate, culture and traditions of an organization are also important. What do employees expect on the basis of their experiences? This last item is particularly important and particularly tough. When you want to change an organization, you really want to change its culture and that's difficult to do. Some employees cannot accept change; they are comfortable with the status quo perhaps. And there is risk involved for them and for you; some may not be willing to take those risks. Others may not support your goals; you simply may not win them over no matter how hard you try. You may want to encourage innovation, candor, speaking out, but the existing culture may be one where innovation has not been particularly encouraged, where speaking out was frowned on. Thus, new ideas may not be readily accepted.

So it is important to lay the proper groundwork and then work to effect change through education, persuasion and leadership. You must also demonstrate that you are sincere in wanting candor, ideas and help. You must

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019718

reward, not punish, for these things. You must be willing to tell the bad with the good; you must also be willing to hear the bad along with the good. It is crucial to get people to trust you.

One of my first initiatives as the new Chief of M3 fell flat because I jumped into it too fast: Town Meetings. I believe communicatiing with all employees. So I began to hold quarterly Town Meetings in 3 locations: Headquarters, FANX and Airport Square. But they did not turn out as I'd hoped. Some said I didn't tell them anything they didn't already know. Others didn't believe what I said, especially in the Question and Answer period. I was being honest but some did not think so.

Whatever the reason, my timing was off. I had not laid the proper groundwork. So I stopped having Town Meetings. It is interesting that now, a couple of years later, I am getting requests to do them again. People say they miss them. I see this as evidence that the culture is changing.

This is a problem that all creative managers face: they risk not being understood or appreciated by their peers, their subordinates or their bosses. It takes real courage and some sacrifice to persist.

CREATIVE MANAGEMENT IN M3

My philosophy of management is to try to take advantage of people's skills and abilities by **involving employees** and **having them participate** as much as possible in helping execute our mission. I want to challenge them, to help them be more creative, able to contribute more and be more productive. I believe that **communication** is vital to this process, as is **providing the tools needed to do the job and to grow**, such as training and modern technology. I think it is important to say thank you by giving **awards** for doing a good job. And it's important to remember to stop now and then to have some **fun** together. I'm going to discuss these five topics, leaving the first until last because I have the most to say about it.

The most striking feature of M3 is its geographical dispersion.

Some of us are centralized at Airport Square 1 but the rest are all over the place. This decentralization is intentional. The IPA concept (the decentralized units are called Integrated Personnel Activities) is built on the idea that we need to be close to the people we serve. While it all works very well for that purpose, it does make managing M3 much more difficult. The fact that the IPAs have 2 masters--the Key Component and Group Chiefs they serve and M3--and that we are geographically dispersed sometimes creates a "we" and "they" atmosphere. One final note -- when I joined M3 in January 1982, I was the third Director of Personnel in just four years. This means that the change of direction and leadership happens frequently in M3. And the Director has always been someone from outside the organization.

COMMUNICATION

I place a very high priority on telling people what they need to know to do their jobs. Let me give a few examples.

We have an electronic mail system on our computer called COMET. We use it constantly throughout our geographically scattered organization for all sorts of quick communications. We announce M3 assignments, reassignments, promotions and training opportunities. We advertise internal vacancies and use it to distribute minutes of DDA staff meetings. This, by the way, is one of my innovations that people do like. And distributing staff meeting minutes on COMET insures that everyone gets a chance to see them.

Once a month we hold a **monthly program review**. Anyone in the organization who wants to attend is invited; it is not meant just for certain higher grades or just for the managers. The idea is to give all the people in M3 the chance to broaden their knowledge about things going on throughout the organization and the Agency. We review budget, policy, resources, the status of major programs and reports on our 5-Year Plan.

Our biggest problem is finding a room at FANX large enough to hold our MPR. Recently I started to hold a mini-Town Meeting as the first 15 minutes of the MPR, giving news of interest and then answering questions.

We publish an **annual report** on M3. It is no ordinary report as you can tell from the index: "Welcome Aboard" tells about our hiring program; "On The Front Line" describes activities in our IPA's; "It Pays to Advertise" is about our Competitive Selection Program; and "More Cold Cash" reports on our Awards Program. We all look back with pride on the year's accomplishments. And we circulate the

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019718

report to a wide readership, including the Director and Deputy Director of NSA as well as DDA.

Every so often we have an informal give-and-take around our conference table with DDA and A/DDA. We call it a **rap session** and all my Division and Staff Chiefs as well as a representative from the IPA Chiefs attend. This allows us to talk together about anything that's on our minds. We can discuss hard issues, or things we just need to understand better. The chance for all of us to do this face-to-face and directly with senior management rather than my bringing it back to my managers secondhand has been extremely helpful, especially when discussing policy and philosophy. After we finish the RAP session, we all go out to lunch together.

I believe that **giving the tools needed to do the job and for personal development** go hand in hand. The more people learn, the better they can do their jobs. I have really emphasized this in M3 in all aspects: education and training, professionalization and cross-development.

We encourage people in M3 to become active in developing themselves and have designed an **annual assignment questionnaire** for them to use for this purpose. Anyone who wants to can complete and return it. We use the information to help plan the moves of M3 people for diversity, for professionalization, a move from technical to management or vice versa, and an opportunity for cross development. In the first year, almost all those who returned it got one of their choices for a different assignment.

EDUCATION

My emphasis on **education** has finally paid off: In just 4 years, we have greatly increased the number of people in M3 with higher education. In fact, M3 has now surpassed the NSA average in numbers of people with college degrees. This was not easy to do, and it took a corporate decision and commitment of all my managers to pull it off. We do not get new billets in M3, but we agreed that whenever we did get an empty one we would hire or bring someone into M3 who had training in our preferred fields of interest. We now have a large number of well qualified new people in M3 and the results are what you have seen.

I have high regard for my on-board employees as well; they have also responded magnificently to the challenge to develop themselves. 54 of them are in college now, including many of our clericals. I am especially pleased at that. Those not able to pursue college are using opportunities for training at NCS and OPM. We have also arranged to hold special OPM courses and some college courses here at NSA for our M3 people, so larger numbers of them can attend.

We have set up a special program called a **staffing plan** to train and develop all the new people we have recently brought into M3. It's like an internal intern program. The idea is to make sure people start out right and learn all the things they need to know to serve this Agency's personnel needs into the next century.

PROFESSIONALIZATION

One area that is still somewhat disappointing is **professionalization**.

Our many new hires have not yet been here long enough to become professionalized. But a lot of our middle-grade people (grade 12 especially) have still not gotten professionalized. We have encouraged these people, but the results are disappointing.

The NCS has created several courses especially for M3, including a tailored one-day version of "Time Management" and a brand new course on "Creativity." Again, everyone in M3 had an opportunity to attend these courses; they were not limited to managers, to certain grade levels or COSCs.

I have had some criticism for my emphasis on education, in part, at least, it is because it is different from the past. But I have persisted and my managers have supported me. The results clearly show success. M3 is hiring very high quality people for all the rest of the Agency; we feel that we must do the same for M3. This is yet another example of a change in culture.

AWARDS

One of my most pleasant duties is to be able to say **thank you** for jobs well done--to give our **awards**. I have established two new awards just for M3 so I can express my personal gratitude to the M3 people. One is the Director of Personnel Award. It is a plaque accompanied by a check. I have given out only two of these so far: to [redacted] Chief, M3G, and to [redacted] M33. Just recently we had designed and printed a Director of Personnel

~~FOR OFFICIAL USE ONLY~~
P.L. 86-36

DOCID: 4019718

Certificate which I will be awarding in the future.

Our **monthly award ceremony** is a special event in M3. I always conduct this ceremony myself. I want to give wide visibility to the things M3 people have done and let them have some wel- deserved glory. The photographer says he likes to come to our ceremonies because they are so interesting and so much fun.

FUN

Speaking of **fun**, we feel we just have to stop now and then and enjoy ourselves and each other. Our **Christmas open house** has become a traditional annual event. Everyone pitches in to cook and bake tasty and beautiful foods for our all day buffet. We set up the spread in our conference room and invite everyone, from all the far flung areas of M3, to stop by to visit, talk and have some goodies. I enjoy this once a year chance to see almost everyone in M3 and to chat personally with them.

One of our most successful pleasure activities was a combination of work and play. The Image Task Group under our 5-Year Plan came up with the idea for an **image seminar**. They felt that M3 is a service organization, that we have a public face and can improve it. We invited every single person in M3 to attend: all grades, all skills, military and civilian. I was told: "Virginia, You can't shut down M3 for a day." I said: "Just watch me." It was so important to me that everyone come because everyone is important to the M3 mission and I wanted them to know that. We heard an outside speaker tell us how to deal with the public and each other. She gave the seminar twice that day, once in the morning to half of us and again in the afternoon to the rest. But the highlight was the luncheon--we had everyone together for that. It was the first time eveR that all of M3 had been in the same room together. People met other people who had been only phone voices to them.

We had a lot of fun over Christmas with a new idea--a **pet show**. Actually it was a PET **picture show**. The pictures were judged and prizes were awarded in a ceremony. There were carrots for the rabbits and horses, catnip for the cats and bones for the dogs.

INVOLVING EMPLOYEES

Two of my most important objectives fall into this category. I consider them the bases on which everything else builds and depends.

First, I wanted to **build teams**. I did not want independent fiefdoms of Divisions, Staffs and IPA's. Secondly, I wanted to provide chances for **wide employee participation**. I believe that everyone has good ideas, whatever one's grade level or position in the organization. The problem is--how do you tap all that talent, creativity, ability? Well, here are some of the things we have done in M3.

We use our **M3 staff meetings** primarily to **solve real problems**. We do, of course, exchange information as is traditional in such meetings.

We set out deliberately to build some teams. The first one we established was our **career management board**, informally called our People Meeting. All our Senior managers (Division and Staff Chiefs) sit on that Board and they put on their M3 hats to handle all internal staffing for M3: reassignments, rotations, reassimilation and developmental assignments. They also meet as our M3 promotion board. The results of their deliberations are then made as recommendations to me. It was hard at first to break old patterns; the instinct to look out for number one first is very strong. But I have been very pleased at the ability of the M3 managers to look at the overall good of M3 and the Agency.

We have had a number of formal **team builds** on specific topics. The M3 managers and the IPA Chiefs recently met to discuss the inevitable problems created by being so geographically dispersed. Personal contact is not very frequent and it generates lots of misunderstandings. We felt that the "We" and "They" problem needed to be discussed. After it was over, we agreed that this was one of the best experiences we've ever had--our critique scores were exceptionally high. Note, however, that we had been working together for several years before we did this. We had built the climate and culture for it. It probably would have gone the way of Town Meetings had we tried it earlier.

The Team Build idea has percolated through the whole M3 organization. We have had successful team builds for the M3 Training Coordinators, the M3 Classifiers, the M Secretaries and the Country Desk Officers in Field Support. Every single team build has resulted in lists of solutions to problems and new ideas to try.

Our most successful initiative has been our **M3 5-year plan**. We have done this for three years

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019718

now and always done it wholly in a participative environment with broad representation from throughout M3. HRMA, the newest professional organization (Human Resources Management Association) at NSA, started out as an idea in our 5-Year Plan. I put it up during the brainstorming and the whole group bought the idea. The GOODIE Task Force is starting Quality Circles in M3.

The RAP Task Group started program evaluation for us. We have not had any billets for years for this important function. But the 5-Year Plan colected some volunteers from all over M3 willing to help us get it started. They have now all attended a formal training course, and are busy evaluating the Competitive Selection Program. It's another example of doing more with the same--of increased productivity.

The AUTOMAN Task Force is automating the PMM (Personnel Management Manual) with the goal of making it available through remote access throughout the Agency eventually.

TWOTEN and PROSPECT got a small personnel research effort started. Again, we have had no billets for a long time for this important function. And, again, we have done it anyway using volunteers and by increasing productivity. Their first publication in our new series "Issues of the Eighties" is entitled "Comparable Worth." The SOS Task Force, or Secretaries on the Spot, are studying how we might set up a Kelly Girl type program at NSA. The group is composed mostly of M3 secretaries.

HOW ARE WE DOING?

The last thing I want to discuss is: **"how are we doing?"** I might not have had a very good feel for this if it weren't for still another 5-Year Plan Task Group called ENTERPRISE. This group interviewed and surveyed a sampling of the M3 work force to find out.

How are we doing interview questions

1. What steps could you take to become a more effective employee? How could your co-workers help you to do your job better? What could management do to enable you to be more effective in your job?

2. If I were your supervisor, what suggestions would you have for me that would enable your work group to become innovative?

3. Describe how your immediate supervisor encourages airing of problems, concerns, or differences of opinions.

4. How are suggestions to change plans, procedures, or goals reacted to and handled by your supervisor? Give examples.

5. What suggestions can you make for M3 management that would encourage creativity in the "rank and file?"

6. What suggestions do you have for M3 management that might improve their own effectiveness and creativity?

Other comments.

I can't tell you how wonderful it is to have this kind of information directly from the people. I've learned some really helpful things. I've been pleased to find out that, on the whole, things are going very well indeed. Everyone in M3 seems to know about and to like the 5 Year Plan. And they also know about and like the emphasis on creativity, innovativeness and the chance to participate in the Task Groups and the Quality Circles.

My interest in sharing information may not have penetrated as far down through the organization as I'd like. Also my goals may not always be interpreted and reported as accurately as I'd like. The communications problem again! For example, everyone says we need more resources. I know that, of course, but apparently my people don't know that I know.

I also learned that I must talk directly to my people more often. So I am starting RAP sessions every month with small groups of employees, a different group each month.

So, I find that things are going well. I am blessed with a wonderful Deputy, a super group of senior managers (Division, Staff and IPA chiefs), and a very capable, dedicated and loyal group of employees throughout the organization. I'll end with a few words of encouragement from my people. One said that in all the many years she has been working, mostly outside NSA, she has never before felt such freedom to use her talents and do things to contribute to her organization. They show me that there are many people in the work force who are eager to try something new and different. They like what I am trying to do and are encouraging me to keep at it. And I will.

~~FOR OFFICIAL USE ONLY~~

EO 1.4.(c)
DOCID: 4019718

THE LANGUAGE ANALYST AND AUTOMATION

[redacted] *ret.* P.L. 86-36

This is an abridged version of a talk to the Crypto-Linguistic Association in 1979. At the time the author chaired the Language Automation Committee of the CLA.

~~(FOUO)~~ Before speaking about the Language Analyst and Automation, I'd like to explain what I intend to convey by the term "language analyst" and just who I perceive that person to be. I suppose our last speaker at yesterday's session would consider the phrase a contradiction in terms—I hope [redacted] will not be offended if I proceed to use the expression anyway. Then I plan to give a brief overview of:

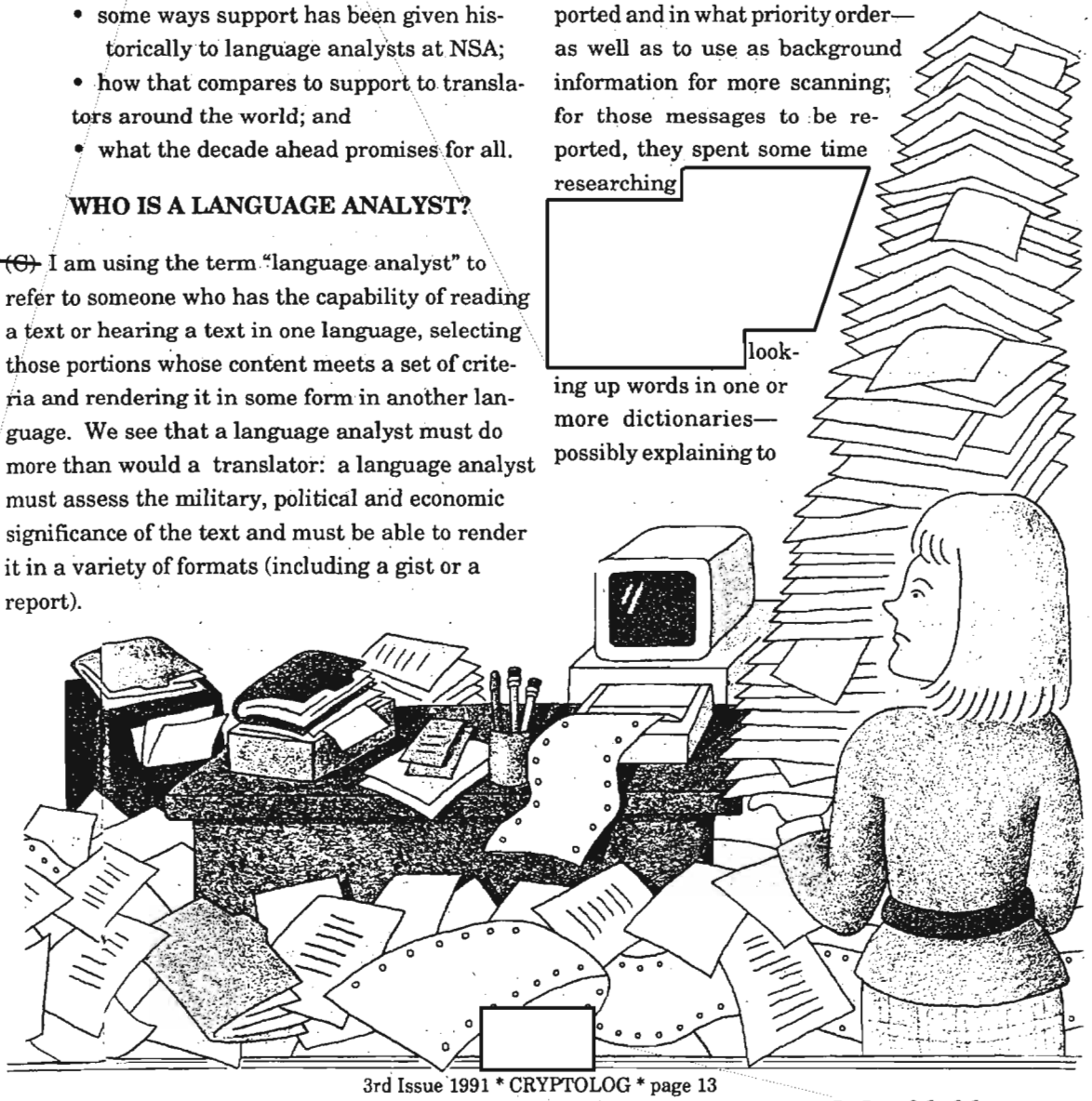
- some ways support has been given historically to language analysts at NSA;
- how that compares to support to translators around the world; and
- what the decade ahead promises for all.

WHO IS A LANGUAGE ANALYST?

~~(C)~~ I am using the term "language analyst" to refer to someone who has the capability of reading a text or hearing a text in one language, selecting those portions whose content meets a set of criteria and rendering it in some form in another language. We see that a language analyst must do more than would a translator: a language analyst must assess the military, political and economic significance of the text and must be able to render it in a variety of formats (including a gist or a report).

~~(C)~~ We all know what language analysts look like: they are recognizable by the tools they use—pencils, papers, and a shelf-full of dictionaries, a grammar or two, some working aids such as word lists, rhyming dictionaries, lists of first or last names, abbreviations, phonetic renderings, biographic data, geographic data, and a style manual. We hand language analysts some pencils and some traffic and come back a little later for the product. How have our language analysts spent the time?

~~(C)~~ In the world of written text, they are likely to have spent some portion of time reading [redacted] possibly reviewing new requirements, scanning a stack of traffic to determine what needs to be reported and in what priority order—as well as to use as background information for more scanning; for those messages to be reported, they spent some time researching [redacted] looking up words in one or more dictionaries—possibly explaining to



P.L. 86-36

DOCID: 4019718

EO 1.4.(c)
P.L. 86-36

a consumer representative that the translation is not yet ready even though they have had the message for ten minutes already-

[redacted] when our language analysts had finished, then another language analyst called a checker reviewed all these jobs, assuring that the product represented a faithful rendering of the original, that all addressees had been included, and that the language analysts who did the product gets adequate feedback.

~~(C-CCO)~~ The voice world differs in a number of ways, but is no less exacting: the language analyst who is a transcriber mounts tapes, listens to them for content, engages in the same kind of research to determine the who, what, when, where, and why of the traffic.

[redacted]

EO 1.4.(c)
P.L. 86-36

COMPUTER SUPPORT

~~(S-CCO)~~ If that is what language analysts do, what support does the computer provide? Here are just a few examples:

- For support to bookbreakers, we have [redacted]

P.L. 86-36

- For message separation and distribution programs there have been [redacted]
- Word lookup was provided to the Chinese language analysts via [redacted]
- In Russian and a number of other languages, reverse dictionaries were created, to help the language analysts struggling with a garble.
- In Vietnamese, dictionaries were sorted on the second and third syllable, for the same purpose.

[redacted]

- Indexes of English-to-Russian dictionaries were created, as a means of getting back to the English from the Russian.

P.L. 86-36
EO 1.4.(c)

- Large "dictionaries" were created, beginning with the Spanish-to-English CAMINO system and expanding to many other languages.

[redacted]

[redacted]

- For Information Retrieval, [redacted] were developed to facilitate searches through raw traffic and end product.

EO 1.4.(c)
P.L. 86-36

- Remember the Farrington Optical Character Reader? The Kurzweil Data Entry

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

DOCID: 4019718
P.L. 86-36
EO 1.4.(c)
EO 1.4.(c)
P.L. 86-36

Machine is the recent version of such a scanner.

P.L. 86-36

- A lot of these programs—or their successors—are still going strong. [redacted] probably merits some kind of longevity award.

[redacted]

- There are now dictionary files in the CAMINO format and other format in several languages.

- High quality printing of the scripts is available through use of the SEACO 1700, which produced a hard copy of the Turcofile. For the English, variable-width characters may be selected, and both right and left margins may be justified.

- The same is true of the Russian-to-English Glossary [redacted]

[redacted]

~~(S-CCO)~~ That's all well and good, you say, but what can a computer do with garbles?

[redacted]

[redacted]

~~(FOUO)~~ Transcribers have not been forgotten in this process: we have a terminal for data entry, complete with some text editing or word processing capabilities. Eventually the transcriber should be able to access a variety of files from this terminal as well. The analog tape will be replaced by a digitization procedure, making it possible to skip most of the silent por tions and have great power in selecting the next cut to process.

EO 1.4.(c)
P.L. 86-36

[redacted]

WHAT'S BEEN HAPPENING IN THE REST OF THE WORLD?

~~(FOUO)~~ If I were to name the single biggest contribution of technology to the NSA language analyst during the 1970's, it would probably be the widespread development of language files on computer tape. Much the same sort of thing was happening in many other parts of the world. Gov-

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

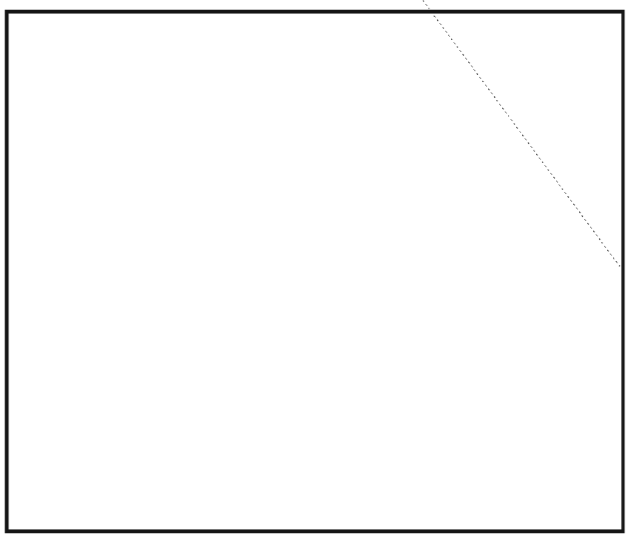
ernments and industrial firms alike became immersed in developing adequate lexical support to translators, in this age of rapidly advancing technology and hence rapidly changing terminology. In Canada, Holland, the Federal Republic of Germany, and the European Economic Community a variety of terminology banks were designed and developed. An organization called INFOTERM assumed the task of coordinating these various term banks.

(U) Another notable occurrence during the 70's was the widespread adoption of dictation equipment to speed the work of the translator. The translator reads the translation into a dictating machine, and the tape is then transcribed by a specially trained clerical person known as a transcriptionist. At the UN and many other places, transcription is the preferred method of rendering a translation.

WHAT'S AHEAD IN THE 1980s?

~~(FOUO)~~ I believe that the big news in the decade ahead for the language analysts at NSA, as well as for the translator at large, will be the widespread use of interactive terminals to provide various kinds of programming support.

~~(FOUO)~~ Some analysts at NSA already use terminals for data entry, for receipt of materials and/or for information retrieval. In the years ahead, terminals will become commonplace. The language files developed during the 60's and 70's will be made available to NSA language analysts via the terminal, as will those information files so prevalent today. But another development will be various kinds of machine-aided translation.



~~(FOUO)~~ Their philosophies may differ slightly, but the message is much the same—the ubiquitous computer terminal has much to offer the translator, the transcriber, the lexicographer, the terminologist, and, yes, NSA's language analyst. Just to prove it, I'll point out that this presentation was prepared with the aid of
prepared with the aid of
prepared with the aid of
a terminal attached to an NSA system called
[redacted] And it came out just fine.

P.L. 86-36

Notice to Contributors

Please note the new mailing address

OPS-1, P054, CRYPTOLOG

Look carefully on the box or disk before you format your disk.

If you are using a 5 1/4 disk, see whether it is HD or DD. If it is HD, do not format it as DD. It will not read. It must be formatted as HD.

If you are using a 3 1/2 Mac disk that is 1.44 mg, it must be formatted as HD.

Remember to label your floppy with the following information:
Your last name, organization, building, secure telephone number

DOCID: 4019718

Secrecy in an Open Society

James Martin

This is a condensed version of a talk given at the Business Luncheon Series on 21 January 1987. At the time the author was a staff member of the Senate Select Committee on Intelligence.

Let me give you a little background on exactly what I do for the Senate Intelligence Committee. I'm the number two budget officer and, as such, unlike some of the other professional members of the staff, I'm not tied to any on particular senator on the committee. We have fifteen senators on the committee and each one has one member of the staff who, in effect, works for that senator. Then there are a few members of the staff which are core professionals who work for the committee as a whole. I'm one of those core professionals.

What that means is that I scrupulously avoid being at all partisan in my work. I serve the Democrats and Republicans equally. That's really not to difficult since our committee is not nearly as partisan as most committees on Capitol Hill. The members of our committee take their oversight responsibilities very seriously and recognize that the sensitive nature of the information we handle makes it imperative that the committee operate in a bipartisan or non-partisan manner. That being said, you have to recognize that the United States Senate is a political organization, and it would be naive of me to try to convince you that politics does not sometimes intrude on the business of the committee. It does and that's just a fact of life.

But, I can assure you that our committee, senators and staff, strives to deal with the issues from the perspective of what is in the best interest of the National Security of the United States. I had breakfast last week at the Pentagon with General Peroots, the head of DIA, and he told me that Senator Byrd, and the new Majority Leader of the Senate, asked him for his advice as to how he should handle the Iran/Contra investigation. General Peroots told him to be a patriot--be an American. I know it sound corny, but that is really how we try to approach our oversight responibilities. We get sidetracked from time to time, but on the whole I think we do a pretty good job of avoiding the political pitfalls.

Specifically, what I do for the committee is to review the budget requests of different elements of the Intelligence Community including, among others, NSA. I plow through the myriad of documents, books, briefings, etc., which in excruciating detail explains what General Odom proposes to do with the budget that the President is requesting for him. That's the easy part. Then I have to boil it all down to a brief,

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019718

coherent and understandable for the senators who, of course, make the final decisions. And remember, senators are extremely busy people and this material is very technical and confusing even for someone who deals with it all the time.

Of course, I don't spend all my time reading budget material and briefing senators. In order to really comprehend how all of the various components of US Intelligence operate, I do get out from time to "kick the tires" so to speak. Since joing the committee staff, I have been fortunate enough to visit Moscow twice, England and Germany twice, Australia, California, Colorado, and several other nice and some not-so-nice locations. And then there are activities which develop on an ad hoc basis which demand my time and attention. The current situation involving the Iran/Contra affair is a prime example of this.

When Minnie Kenny first mentioned the series of lunches and asked me to speak at one, I was both flattered and surprised. I wondered why 150 people would want to pay $8.50 to eat lunch and hear me talk. After I finish you may be wondering the same thing. But, in any event, I thought it would be fun and I said sure, why not?

What should I talk about? I doubted whether I could hold anyone's attention describing such aspects of the congressional budget process as the difference between an authorizing committee and an appropiating committee, or the effect budget authority versus budget outlays have on calculating the amount to be sequestered under the Balanced Budget Act of 1986--otherwise known as Gramm-Rudman-Hollings.

I decided to talk about "secrecy in an open society" for many reasons, not the least of which was that it might stir up some interest and perhaps som skepticism on the part of people who might attend the lunch. My goal is not to lecture--or to titilate for that matter. What I hope to do is to give you some food for thought on the subject--to give you some opinions I have on the issue and, more importantly, to stimulate discussion.

My fifteen months with the committee have been anything but dull. I am reminded on the proverbial Chinese curse: "May you live in interesting times." Well, we in the intelligence business certainly live in interesting times! 1985 will long be remembered as the "Year Of The Spy" with this discovery of the Walker family spy ring; the arrest on espionage charges of a former colleague of yours, Ronald Pelton; the defection/redefection of Vitaly Yurchenko; and the Jonathan Pollard/Israeli Caper.

THE YEAR of the LEAK

1986 may well be known as the "Year of the Leak." We were bombarded with headlines based on leaked information such as: "U.S. discloses secret plan by the Sandinistas"; "CIA Anti-Quadaffi plan backed". And, of course, there was the role of the media itself in reporting leaks and in how it should cover spy trials. I'm sure you remember the controversy involving Bill Casey, General Odom, and *Washington Post* editor Ben bradlee over what information the Post could use in its coverage of the Pelton trial. Whether you agree with Casey/Odom or Bradlee and the Post, I'm sure your opions were strongly held.

And finally, in 1986, in case you have been travelling in a remote and inaccessible part of the world, we have the current situation involving the arms sales to Iran and possible diversion of funds to the contras.

We're going through another round of leaks now which raise several questions. I cringe these days whenever I pick up my *Washington Post*. Just two Sundays ago, for example, you good folks were prominently featured in the headline for the lead story. I know it is troubling for you and I can assure you the committee is frustrated and disturbed by the developments of the past few weeks.

I guess I'm still naive enough to think that secrets given in a closed session in a secure facility would remain secret--at least for a day. So you can imagine how I felt a few weeks ago when, after a long day at the committee during which Robert McFarlane testified before our committee, driving home about 10 p.m. I heard the lead story on WTOP, "former National Security Adviser Robert McFarlane, in secret testimony before the Senate Intelligence Committee today, detailed his role in the etc., etc., etc." I about went off the road. It was just the beginning of a long series of similar occurrences.

That being said, I would like now to throw out a few thoughts on the nature of secrecy in this country and the climate in which we all have to operate. In a recent essay entitled, When Secrecy Meets Democracy, *Time* magazine posed the question, "Can Americans do anything in secret anymore?" The essay points out that one

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019718

consequence of the arms for Iran story would be an unravelling of an endless eries of disclosures--names, dates, places, faces, etc., that will make it very unsafe to be an American agent: remember this was written back in early December. As we now know, that is precisely what has happened.

In the early 80's, Israel had, then lost, contacts in the middle levels of the Iranian military. They died out according to an Israeli official. He told the *New York Times* that the contacts were executed. There was also a recent series of stories in the press about a number of KGB agents who were executed in Iran after their identities were made known to Khomeini. The premise of the *Time* essay is that Americans are passionately democratic, and thus accutely sensitive to the contradiction between democracy--which promises openness--and the secret world of diplomatic and paramilitary intrigue. Americans do not take easily to the notion, for reasons of state, secrecy may sometimes be necessary. We have only to look back to 1929 when Secretary of State Stimpson found out about American code-breaking and interception operations and stopped them with those famous words I'm sure you're all familiar with, "Gentlemen do not read each other's mail."

Since then we have had another warld war, the cold war, and now "low-intensity conflicts." According to *Time*, the first of these spawned to OSS, the second gave us the CIA, and the third produces everything from the Delta Force to Ollie North and the cowboys at the NSC.

So what does all this tell us about the climate in which we find ourselves today? Certainly I'm preaching to the choir, and by the way I consider myself to be an active member of that choir, to say that there is a legitimate need to conduct certain sensitive government operations in secrecy and that some information, because of the harm its disclosure would do to National Security, must be protected as classified information.

PROTECTING THE "REAL" SECRETS

By the way, I strongly believe that one of the things we are going to have to do is to sharply limit the amount of information that we protect as classified. There is an old saying which says, "He who seeks to protect everything, protects nothing." I believe that. Some of the information we try to protect today just does not stand up to the supposition that its disclosure could harm the National Security. We simply do not have the resources to protect everything--nor should we try. Obviously I can't give you any examples in an open session, of classified information which shouldn't continue to be classified--either because it just doesn't meet the standard or because it is already common knowledge. The Stillwell Commission, which was set up after the disclosures of the Walker case, concluded the same thing and has recommended sharply limiting the amount of information the government classifies.

We need to protect the "real secrets." Another point I want to make regarding secrecy is that, while it is potentially a breedimg ground for lawlessness, it is also a breeding ground for genius. Without secrecy, we wouldn't have had Henry Kissinger's secret trips to China or the most recent interception of the hijackers of the *Achille Lauro*--an idea, by the way, that most people attribute to none other Ollie North.

People have to realize that the test of a policy or a program is not whether or not it is conducted in the open, but whether or not that the policy or program makes sense. What I hope is not lost in all the outcry from the public, the press, and yes, amazingly enough, the congress, for no more secret operations like the Iran/Contra program, is that, like it or not, the United States has to face the responsibilities of a superpower. And one of those responsibilities it the occasional necessity for secrecy.

Time Magazine concludes--and I agree--that if we are going to play the great power game, and ask others to risk their lives to help us win it, we had better accept the need for secrecy.

AN OPEN vs A CLOSED SOCIETY

Now, if you accept that premise, how do you square it against that thing called democracy, which, as I've said, tends to frown on anything that is not conducted out in the open? Of course, in an ideal world, I think we would agree, the affairs of state could be open for all to see. But with the likes of Khomeini, Ghadaffi and all those faceless terrorists running around the world, to say nothing of our good old adversaries in the Kremlin, we cannot enjoy the luxury of a completely open society.

Which does not, it seems to me, mean that we have to settle for a closed society, run by the government, where the people have no right to know what their government is up to, and

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019718

where the press is controlled by the government and can only print what the government says it can print. There are many examples of such societies around the globe and I doubt if anyone in this room would opt to live in any of them.

As anyone who has ever been there will attest, the Soviet Union is the classic example of a closed society. The people hear only what the party wants them to hear. In Moscow, if you don't know what you are looking for you won't find it--there are no signs on the buildings nor is there a telephone directory.

You can't criticize the government--there's no C-Span. There's also no fast food chains--the place is really the pits. It is a third-rate economy with a first-rate military.

We had a chance to talk to our ambassador to the Soviet Union, Arthur Hartman, when we were in Moscow, and he told us how difficult it is for our diplomats to operate there. The Soviet diplomats-spies in the US enjoy a tremendous advantage on our folks in Moscow. They have a far greater access to government officials, our scientific and technical organizations--think of the advantage the Soviets enjoy with the information we provide in the open--let alone the material that leaks out.

We are beginning to see signs of Gorbachev's attempts at openness, candor, and publicity--all summed up in the Russian word **glasnost**. Some early signs are promising--the release of Sakharov, more openness in the Soviet press--there was an unprecedented story last week in Pravda about the firing of a senior KGB officer who engineered the illegal arrest of a local investigative reporter. On the cultural front, the new line has created a literary pre renaissance. But it is far too early to determine if these represent real reforms or only empty rhetoric.

THE PRESS

So what do we do? How do we ensure that the government has the wherewithal to conduct certain operations in secret, that congress--or more accurately--that certain representatives in congress--are apprised of these secret operations, and that the public knows whatever it has a right to know about the operations of its government, through whatever mechanism, whether it be a free press, or through its elected officials or whatever?

And by the way, just as an aside with regards to the press, I'm sure a lot of you have the same feelings as I do about some of the press--the Sam Donaldsons and the Jack Andersons of this world. And during the last couple of months, we've had the press all over the place down at the committee and at times it can be quite a nuisance. But I read something the other day and I think it applies to the press, "If you want a watchdog to warn of intruders, you must put up with a certain amount of barking. If you muzzle him and leash him and teach him to be decorous, you will find he doesn't do the job that you got him for in the first place.

Some extraneous barking is the price you must pay for a service as a watchdog." I think that story also should by heeded by people in the evecutive branch when they think about congressional oversight.

And since I am part of that congressional oversight process, I thought I would focus on that as one way of dealing with the question I posed a minute ago, that is, "How do we ensure that the government has the wherewithal to conduct certain operations in secret, etc., etc., etc."

THE ABUSE OF POWER

As many of you remember, the intelligence oversight committees were established in the post-Watergate period as a reaction to Watergate and other excesses which made the public aware that there must be a constitutional guard, if you will, against the abuse of intelligence services by those in power. If the United States is to have an intelligence capability, the public must be assured that it remains an American intelligence capability, bound by the constitution and the law of the land.

Another concern which surfaced as a number of intelligence fiascos have come to light, has been that covert action programs carry with them a significant risk, particularly if there is little consensus on the foreign policy goals such programs are designed to serve. In order to make sure there is adequate accountability by responsible political authorities, formal oversight was seen as necessary. By the way, its sort of axiomatic that you accept that there is such a thing as a "responsible political authority." Without that assumption, we have no common ground for agreement.

Finally, and this is becoming more and more true all the time, the public has come to

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019718

recognize that we as a nation cannot afford to do everything. We have to make trade-offs between guns and butter. It's critical that a dollar's worth of investment produces a dollar's worth intelligence. As the budget officer that's my job.

THE VALUE OF OVERSIGHT

In sum, formal congressional oversight should help to keep our intelligence services healthy. It does this by providing an essential filter between the intelligence community and the public which it serves. One way that this filter operates is that it gives the intelligence community an opportunity to short-circuit actions which, for whatever reasons, may not have been fully thought out. Or they might be just plain stupid.

THE CASE OF NICARAGUA

A prime example of how this aspect of how oversight didn't work is the infamous CIA covert action operation in Nicaragua two or three years ago involving the mining of the harbors. Had the oversight committees had the opportunity to comment on this plan they perhaps could have pointed out how short-sighted and politically explosive the plan was, and thus could have saved CIA a tremendous amount of embarrassment and harm to its overall operation. There are still repercussions of that episode being felt by CIA today in its relationship with the Hill. You spend years building up credibility and you lose it overnight.

The same could be said, possibly, about the current situation involving the US policy towards Iran. Nobody in congress was consulted. And I know what you're thinking: If congress had been told about these programs the plans would have been leaked and the programs would never have gotten off the ground. Maybe, but I would argue that because you don't think the system works is no justification to abandon the system. We have laws and they must be followed. There are just too many success stories--which obviously nobody ever hears about--involving cooperation between the oversight committees and the intelligence service to hold that view, in my opinion.

Besides filtering out bad ideas, oversight can also provide a very useful service to intelligence agencies. There is no greater threat to intelligence than revealing how conclusions are revealed--the sources and methods. That is the *sine qua non* of our business. Now in the last year or so there has been a great deal of consternation within the intelligence community and also, I can tell you, within the intelligence committees, concerning disclosures of certain intelligence information by government officials--including the president--to justify either a response to terrorism or to obtain the conviction of an accused spy. Some would question, and legitimately, I think, whether or not it's worth those results to give away sources and methods.

But there is an alternative that would allow us to it both ways. That is for the American people to be assured that the actions of the executive branch--an attack on Libya or a prosecution of a Pelton--are justified by the evidence--the intelligence--without having to reveal the sources and methods associated with that evidence. And that is for the oversight committees to know enough at the appropriate time to be able to say, in public "Mr. President, we have seen the proof and it justifies your response."

THE MATTER OF TRUST

The key ingredient in that scenario is, of course, trust: Trust in the oversight process and trust in the actions and motives of the executive branch. Because at some point, let's face it, we simply must trust our leaders. But the must earn that trust. And trust and confidence in the oversight process is also critical and must also be earned.

Over the past ten years, this country has taken a major step toward building public trust by substantially strengthening the process of congressional oversight through the intelligence committees of the house and senate. Meeting the challenges of the coming decades will require continued strengthening and support for that process.

I don't pretend that these issues are simple or that there are easy solutions. Remember, we are dealing with a situation which goes to the core of the relationship between the legislative and executive branches of government. By definition, we are talking about bureaucracies and political bodies which make cooperation difficult at best. But our responsibilities to National Security--and to the values of an open and democratic society--demand nothing less.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019718

P.L. 86-36
EO 1.4.(c)

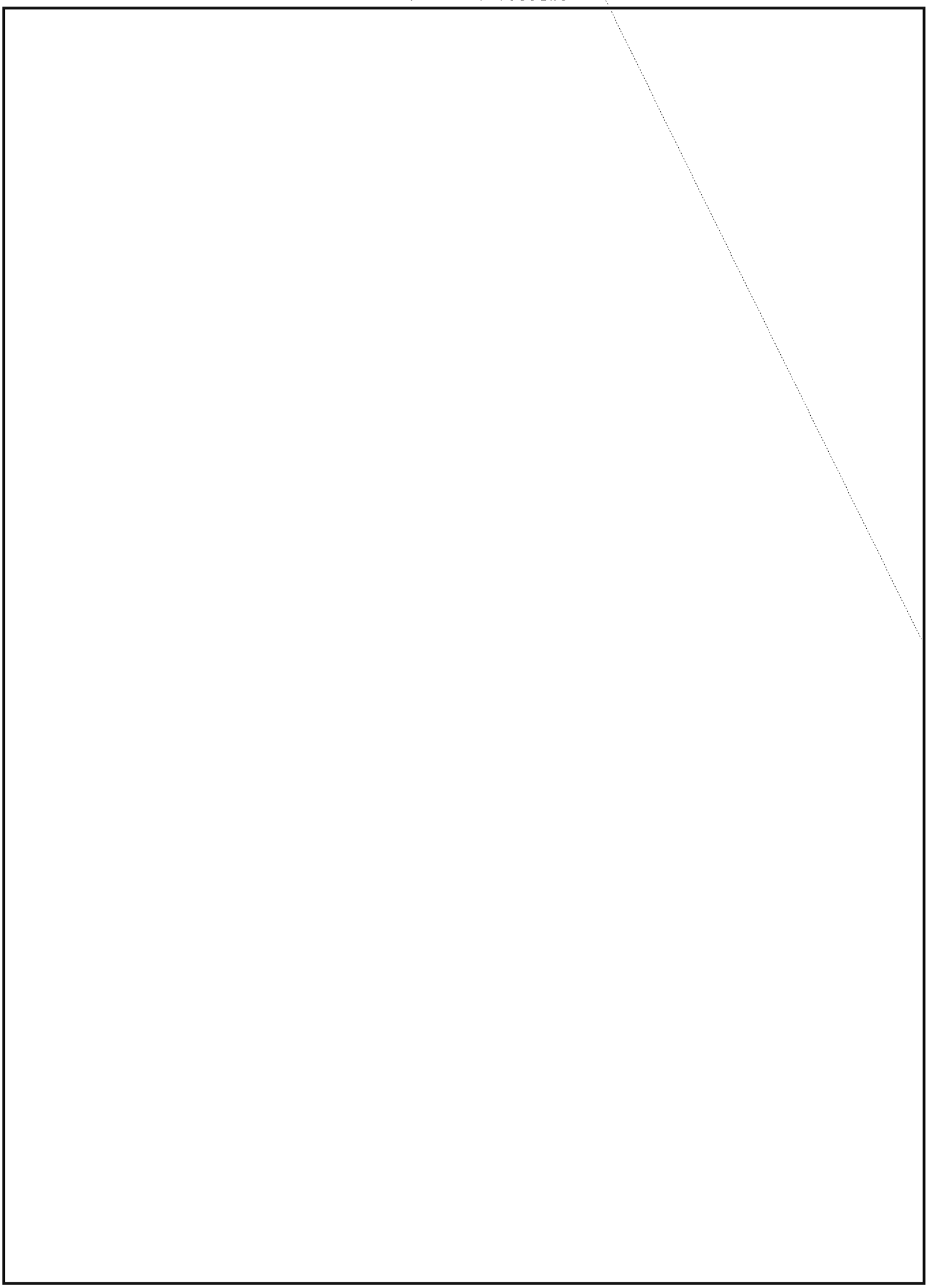
THE WAY WE WERE

~~This article is classified TOP SECRET UMBRA in its entirety~~

EO 1.4.(c)
P.L. 86-36

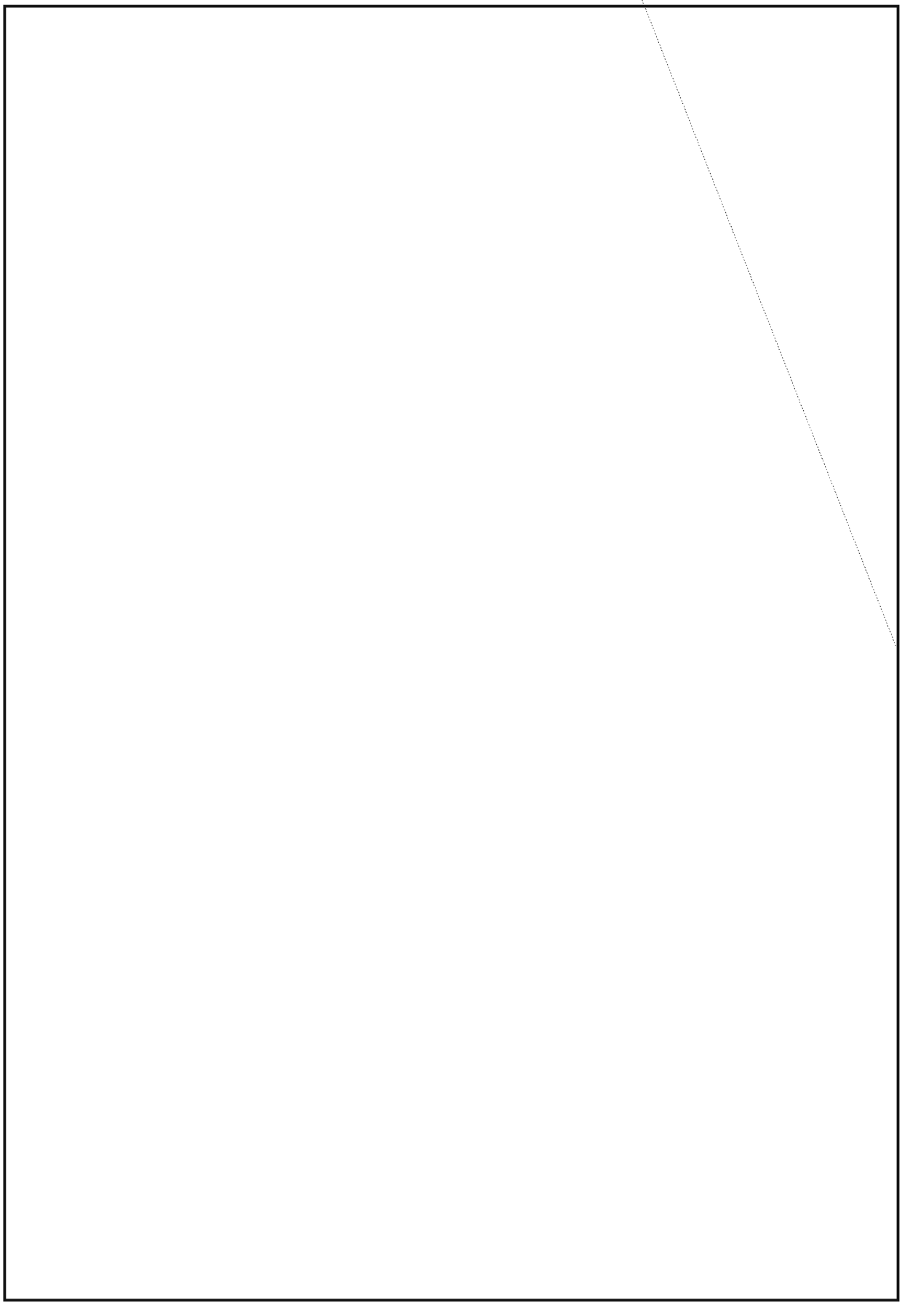
DOCID: 4019718

EO 1.4.(c)
P.L. 86-36



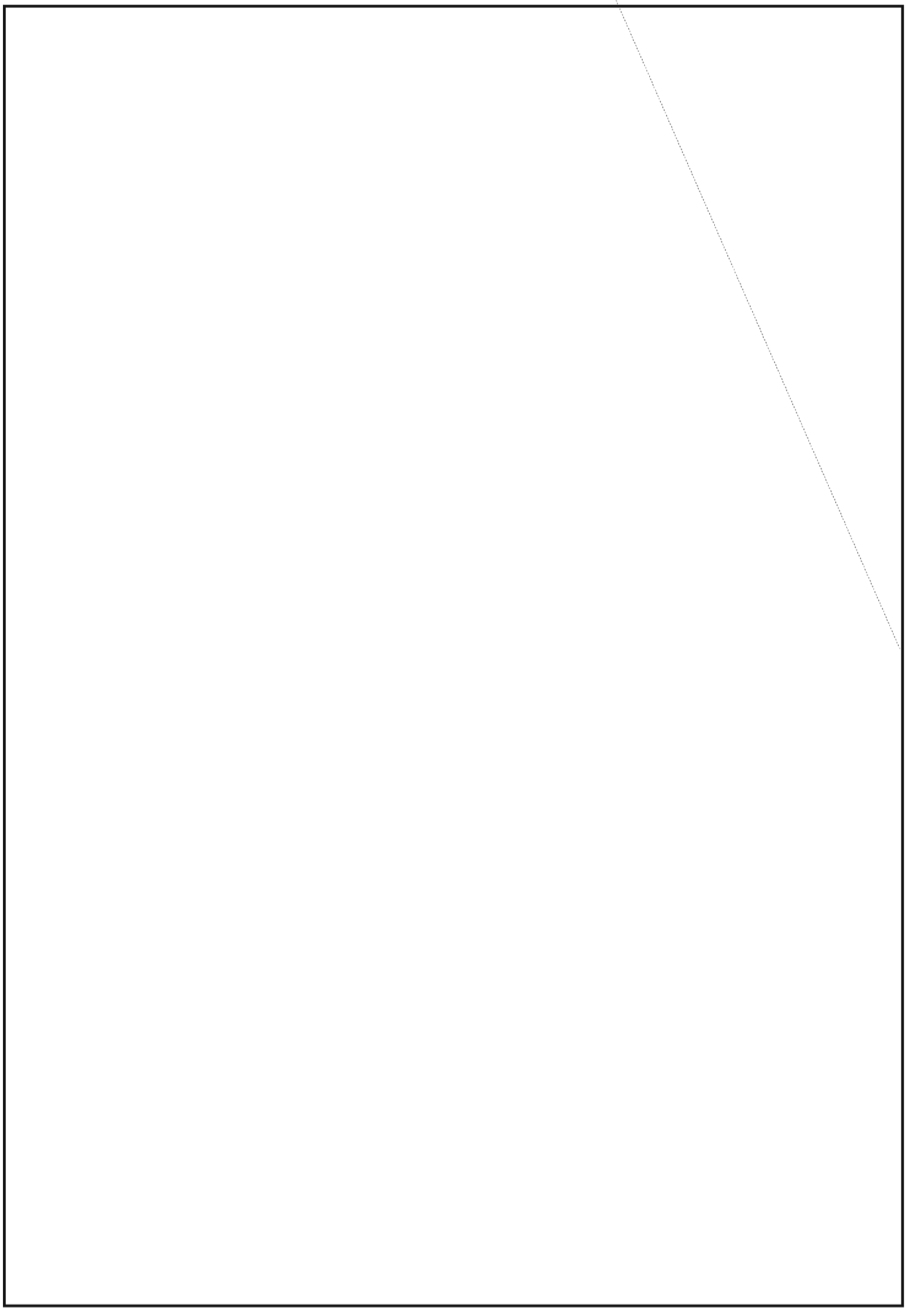
DOCID: 4019718

EO 1.4.(c)
P.L. 86-36



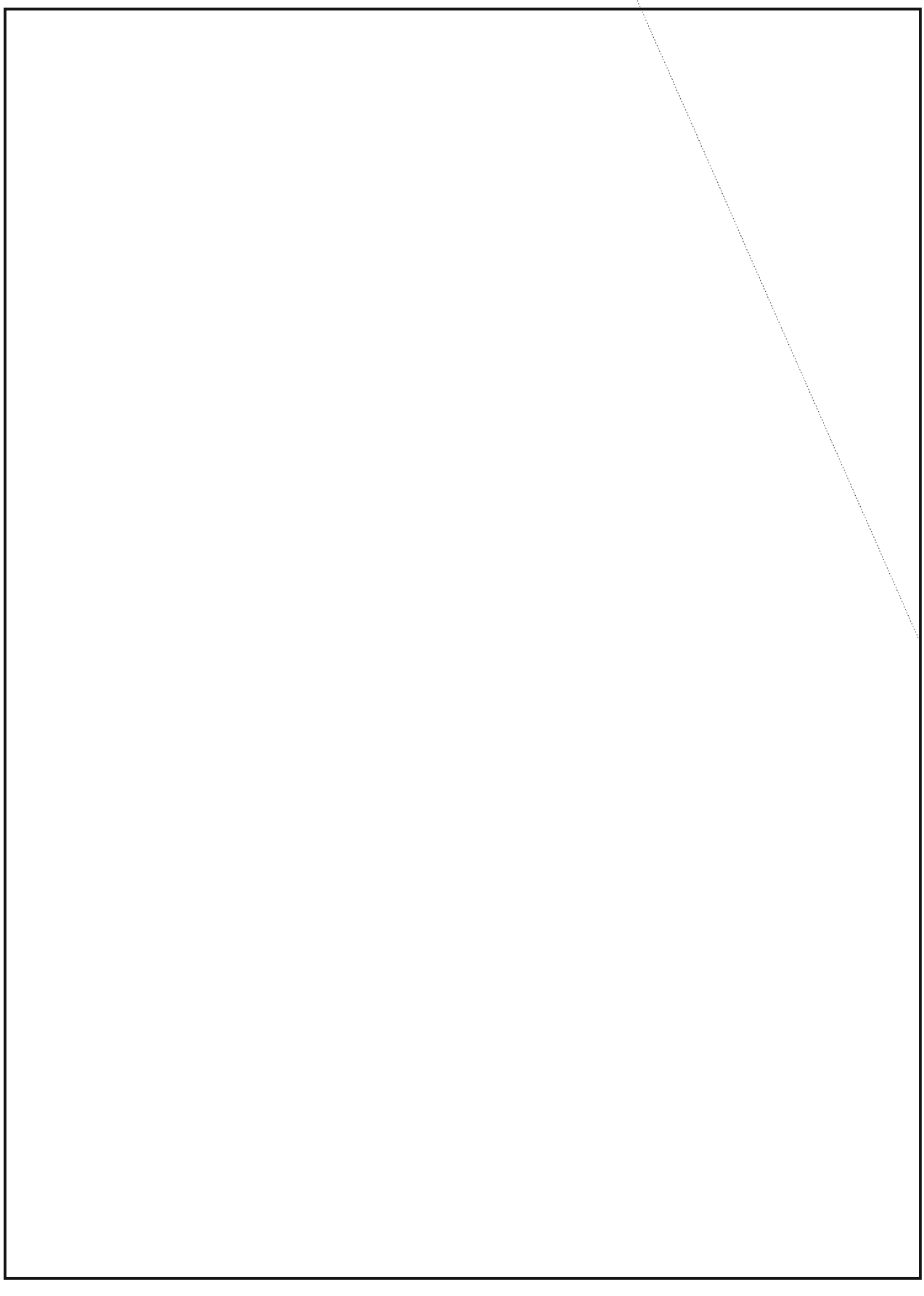
DOCID: 4019718

EO 1.4.(c)
P.L. 86-36



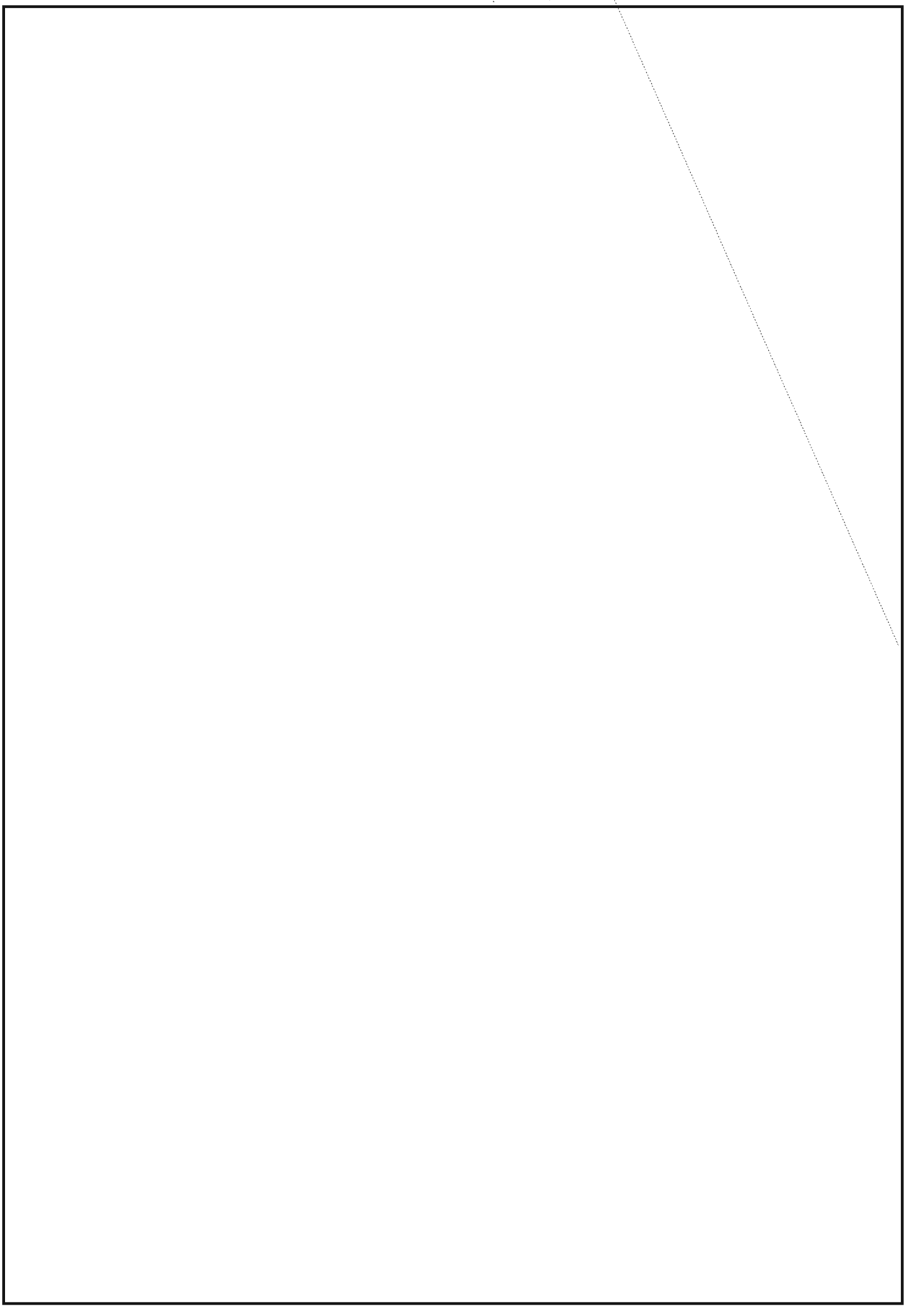
DOCID: 4019718

EO 1.4.(c)
P.L. 86-36



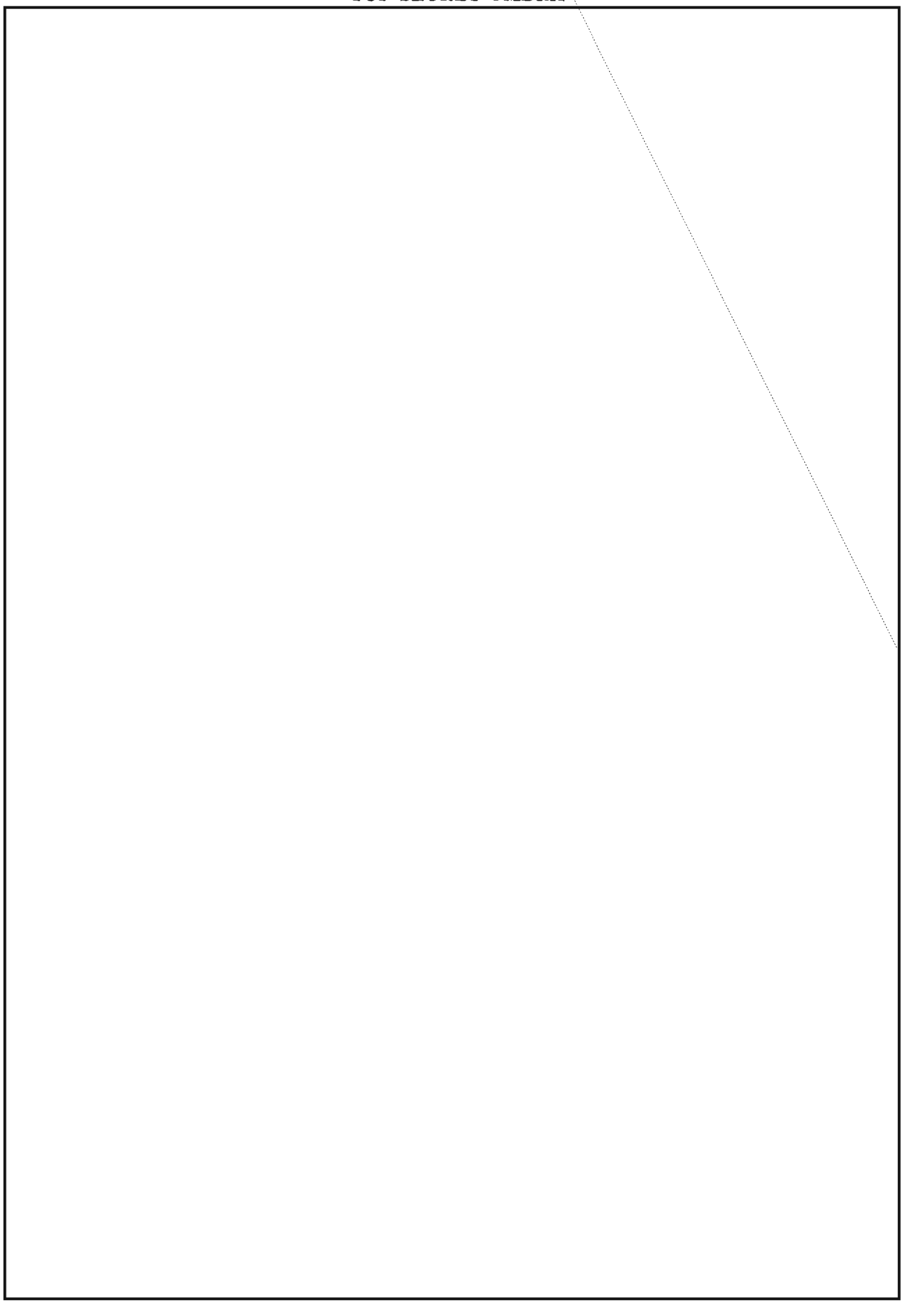
DOCID: 4019718

EO 1.4.(c)
P.L. 86-36



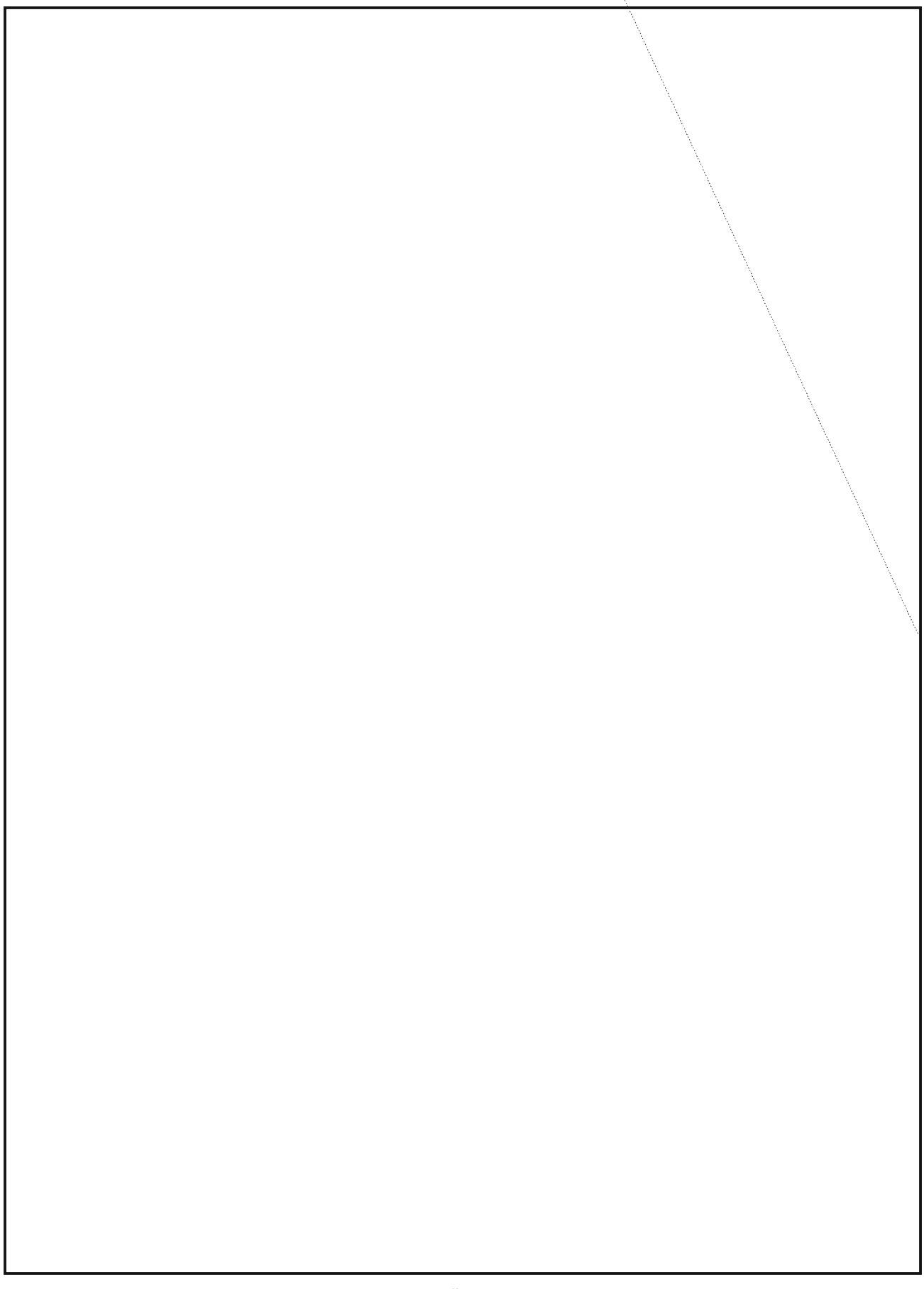
DOCID: 4019718

P.L. 86-36
EO 1.4.(c)



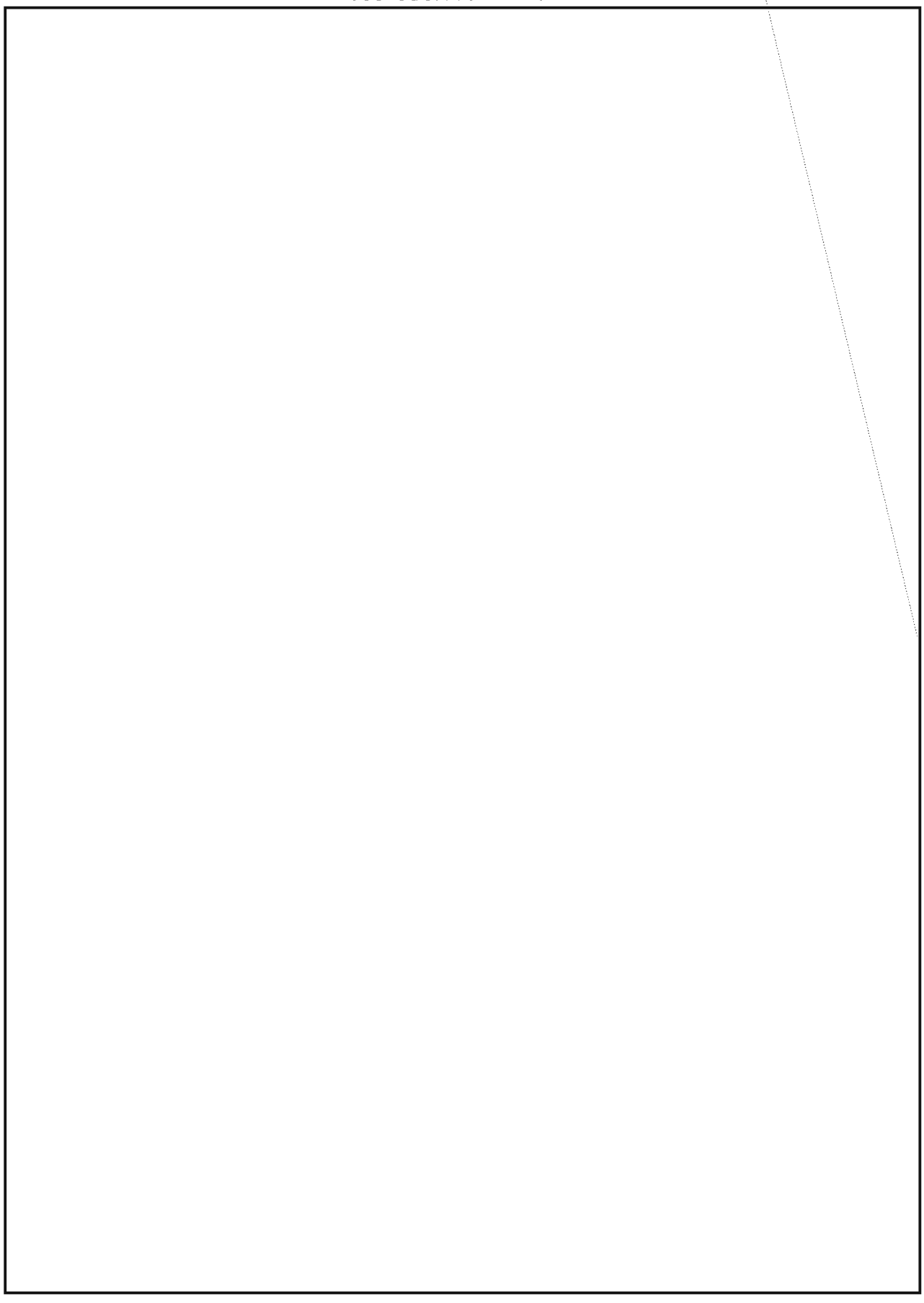
DOCID: 4019718

EO 1.4.(c)
P.L. 86-36



DOCID: 4019718

P.L. 86-36



DOCID: 4019718

A View of L

Dale A Seaberg

The author was ADIL when he gave this talk at the third annual Federal Women's Program on 6 November 1985.

THIS ARTICLE IS CLASSIFIED ~~CONFIDENTIAL~~ IN ITS ENTIRETY

I am a business person and I run L like a business!

The type of business I run demands that I make the maximum use of all the people in the work force--both men and women. In terms of the female population in L, if I didn't make maximum use of their potential, I would be wasting 38% of my work force. In terms of population, L realized only a 2.5% population growth in FY84. The ratio between the overall female-male population has not changed more than 2% during the FY83-85 period.

In FY84 the male population decreased 2% with a corresponding increase to the female population. It's noteworthy to point out that in grades 7-11, which represent the largest segment of the L population (63% for men, 36% for women), the percentages of males and females correspond with the total female/male population (62% for men, 37% for women).

Also, during the FY83-85 period, it is interesting to note that even though the female population in grades 13-15 decreased slightly (1%) from FY84, the female population in grades 7-12 increased by 43%. This high increase in population for women in grades 7-12 is significant because it suggests a tremendous amount of potential for women to attain the higher grades.

Other speakers during the Federal Women's Program have said the Agency must do better in promoting the women in our work force- especially to the more senior grades; and I agree with this. But, before you can promote women to senior grades, you have to make sure there is a sufficient number of women in the middle grades from which to draw. In this regard, L has an outstanding rate of promotion for women. To use a popular phrase, "What's the bottom line?" The bottom line is this: promotions in FY83, [redacted] This represents roughly a 50% ratio. This statistic compares to a 46%-53% male-female ratio in FY84, and evens out slightly in FY85, but with more women than men getting promoted.

EO 1.4.(c)
P.L. 86-36

DOCID: 4019718

Looking at the three years FY83 through FY85, there is one major point that should be made, and I'll ask a question before making it.

What are the percentages of male-female promotions against eligible male-female populations? The answer is:.

PROMOTIONS			
	Men	Women	Delta
FY83	22%	38%	+15% for women
FY84	23%	37%	+14% for women
FY85	30%	50%	+20% for women

Again, this high rate of female promotions strongly suggests that there is a great deal more opportunity for advancement for women working in L. More so, I would guess, than most other Agency organizations. To quote Napolean: "Ability is of little account without opportunity." What I try to do in L is to give all deserving employees an opportunity to advance.

Women supervisory positions are on the increase in L. So much in fact that since the figures for the briefing were put together, the number of female supervisors in L has increased by three. Indications are that with the rate of women promotions in L across the years we've looked at, the number of women supervisors will increase also.

In the area of training and from the standpoint of total female-male population [redacted] a slightly higher percentage of women than men receive training in L. In FY85, 73.7% of the male population received training against 77.5% of the female population.

As a business person, I want the best people to negotiate contracts, build buildings, manage supply systems, and defend logistics resources. It doesn't make any difference to me if the person performing these functions is male or female. I push the women in L hard, maybe harder than the men. I do this because the women are as tough, fast thinking, and dedicated as the men. There is nothing that disappoints me more than a high potential woman who lacks confidence, drive, or commitment. There are not many women at higher grades in L, but looking at the percentage of promotions over the entire population, females have a higher ratio of promotions. This is because many of the types of jobs in L have not been traditionally women's areas in the past. However, we are breaking with tradition in this respect and are capitalizing on talent instead--and we will continue to do so!

The future for women in L is very bright. In recent years, more women in L are filling positions of contracting officers, engineers, illustrators, and programmers, as well as other positions that were male-dominated in the past. This is the result of a vigorous intern program in L, and a growing recognition that if we are going to be successful in the business we are in, we have to make the best use of all the people in the L work force. As far as I'm concerned, the L Organization offers a great deal of opportunity to anyone--female or male--with a commitment to do a good job.

In conclusion, I'll paraphrase the old Chinese proverb, "Behind an able man there are always other able men". I would change that to: "Behind an able person there are always other able people." In the L organization, I am fortunate that there are many able people who carry out our important business.

EO 1.4.(c)
P.L. 86-36

DOCID: 4019718

Keynote Address

Gerald R. Young, SUSLO

~~This article is classified TOP SECRET UMBRA in its entirety~~

This is a condensed version of the Keynote Address to the 1990 session of CA-305, Seminar on Contemporary Issues in Cryptanalysis. At the time the author was Deputy Director, NSA.

I'm very pleased to have this opportunity to speak with you today! I think it's most appropriate that my first address of the new decade is to an audience of cryptomathematicians, cryptanalysts, and computer scientists because your work is at the very core of the work of our Agency.

Your past successes have aided immeasurably to further enhance the security of our nation and are central to the fine reputation our Agency has earned over the years. What's more, our future rests with you and your ability to meet the difficult challenges on the horizon. I challenge you to continue to be creative, bold and aggressive in finding solutions to the ever increasing number of cryptosystems being used in the world today and, in addition, providing the information security capability needed by the nation.

In a sense I believe conferences like this give us an opportunity to check up on ourselves and to see how we are doing and where we are going. Gatherings such as this symposium provide a real opportunity in bringing together the analysts from the SIGINT and INFOSEC communities to update each other on significant successes, trends, and technological advances and, what's more, gatherings like this are essential catalysts to improving productivity and for making significant advances in your craft. I'm certain that each of you will come away from this seminar with some new and innovative approaches to apply to the problems you are working now or will be facing in the future.

As I reviewed the agenda for this seminar on Contemporary Issues in Cryptanalysis, I couldn't help but be impressed with the degree of sophistication in the technical work that is taking place in the Agency today. And it's important that we continue to make leading-edge, high-tech breakthroughs to keep pace with the rapidly changing world around us.

Today I'd like to share with you some of what I believe are the most significant trends and challenges we face, and along the way, I'll weave in some of the critical projects now underway that we must ensure are nurtured through the period of fiscal uncertainty facing us.

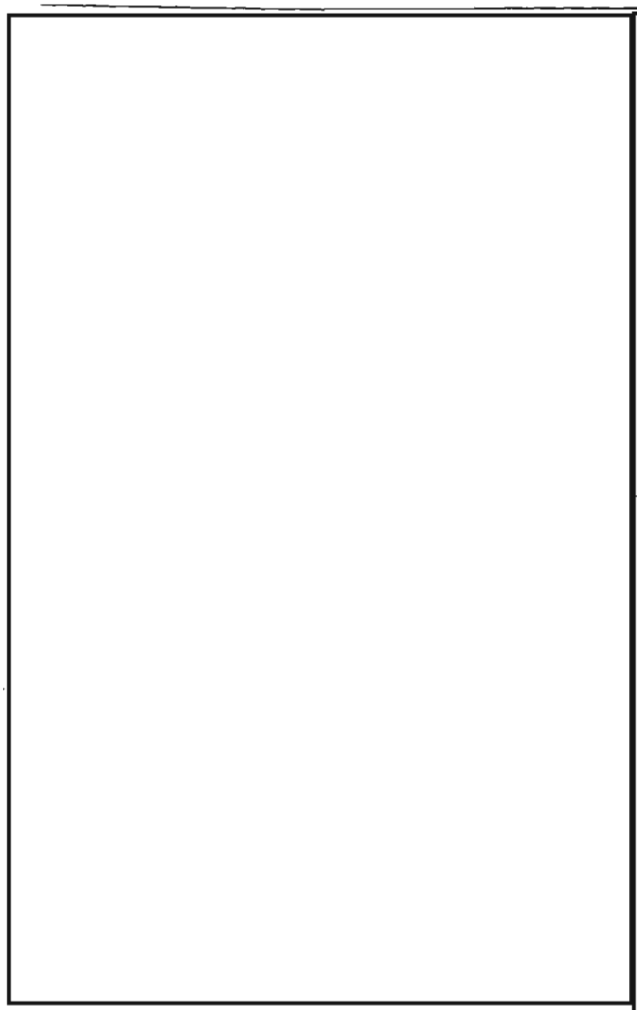
LOOKING AHEAD

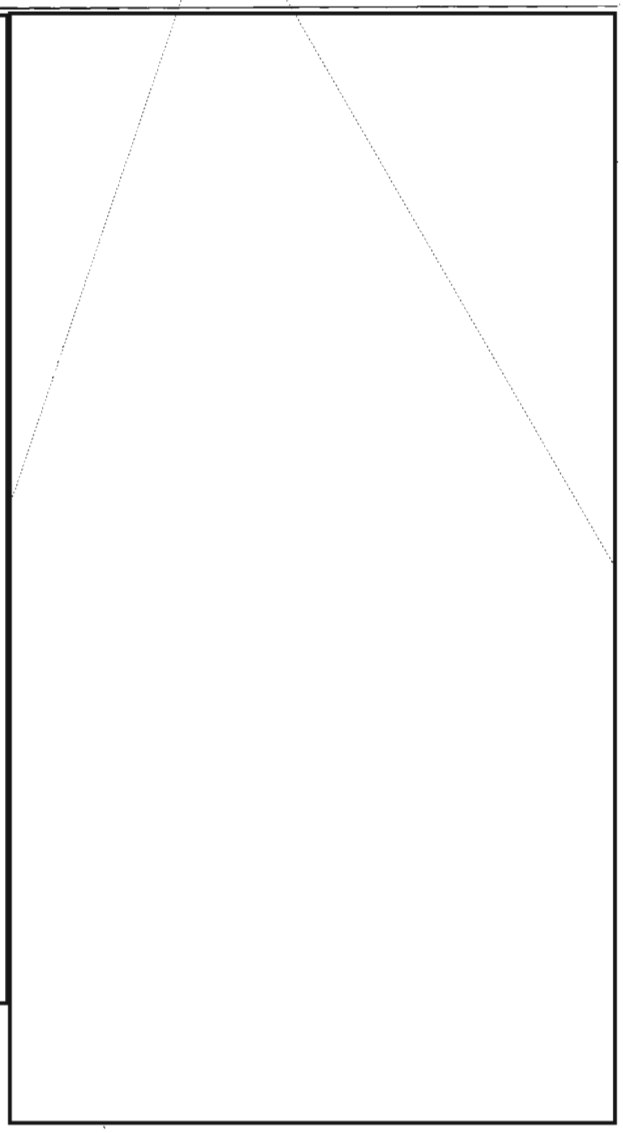
Many so called "futurists" are still scratching their heads over the rapid, unforeseen changes that

EO 1.4.(c)
P.L. 86-36

have taken place in Eastern Europe. The true impact of these changes is still not clearly understood and it is yet uncertain how the dramatic changes in Europe will influence the intelligence requirements levied on us by our customers. With that in mind, let me dust off my own crystal ball. I'm reminded of the person who said the future is a bit like heaven—everyone exalts it, but no one wants to go there just yet! But the '90s are here so let me tell you what I sense are some of the major challenges facing the Agency.

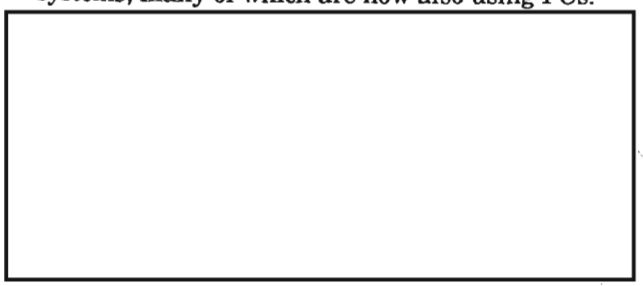
EO 1.4.(c)
P.L. 86-36





Terrorism and Narcotics

Terrorist groups are also increasing the numbers and kinds of systems they are using. At any one point in time, we may work a large number of systems, many of which are now also using PCs.



INFOSEC

Advances in technology also are having a dramatic effect on our own INFOSEC world. During the week you'll be hearing about many of these technological breakthroughs and in addition, you will also hear about vulnerabilities found in some of our operational systems. However, just a word of caution—just as we have seen the proliferation of cryptosystems by our SIGINT targets, to include commercial and private sector targets, the United States is facing increasing demands to quickly design and evaluate increasing numbers of INFOSEC products.

More and more US communications, both government and private sector, require protection by cryptography. As a result, we are faced with many more proposed INFOSEC products each year and we must balance our urge to accredit these systems with the credibility problems we'd face if we act too quickly and problems are later found in our "endorsed" systems. We can't afford to allow that to happen.

RESOURCES FOR THE FUTURE

Having stated some of our challenges, let me now spend the next few minutes addressing the current resources we have to meet these challenges. But before I do, let me relate a story which I believe is appropriate to the environment we are certain to face in the near future. It's a short story of a farmer who hired a hand and set him to chopping wood. In the middle of the morning the farmer went down to see how the hand was coming along. To his astonishment, he found the wood all chopped. The next day the farmer told the man to stack the wood in the shed. This involved a lot of work and the farmer figured the job would keep the man busy all day. But by noon, he had it all done.

On the third day the farmer thought he'd give the fellow a light job for a change and told him to sort out the potatoes in the bin. He told him to put the good ones in one pile, the doubtful in another an to throw out the rotten ones. An hour or so later he went back to see how the job was coming. He found the fellow passed out cold with virtually nothing done. After throwing water on the man's face and bringing him around, the farmer asked what had happened. "Hell, the man said, "The other work was easy. It's making all those decisions that's killing me!"

The prospect of hard choices is certainly facing us today.

People

As we make our choices, we must keep foremost in our minds that we have and will continue to need highly talented people, because it's the people who get the brilliant ideas that drive our efforts. It's folks like you that give our Agency its uniqueness, and although your contributions are well recognized by senior management.

I do not believe that the pool of people we need to get the cryptanalytic job done is going to grow substantially in the near future. We are entering some austere times. Therefore, we must seek imaginative strategies to gain further efficiencies and leverage to achieve our mission. We must place our people where they can make the greatest contributions. The CA Council is studying the manpower situation and has made recommendations to Senior Management which will be given very serious consideration as we formulate our plans and programs to deal with the multitude of challenges facing the Agency in the future.

The Cryptanalysis Intern and Pl Math Programs will bring new hires, but probably not a significant number of additional billets, to be used against the growing number of CA targets. For the near term, we expect the hiring for these programs to continue, with a modest number of new hires authorized for the CA Intern Program in FY 90 and a somewhat larger number for the P1 Math Program. The picture, however, is less clear for the individual cryptanalytic organizations. Most of the hiring in the Agency, at least in the foreseeable future, will be to replace attrition.

Supercomputers

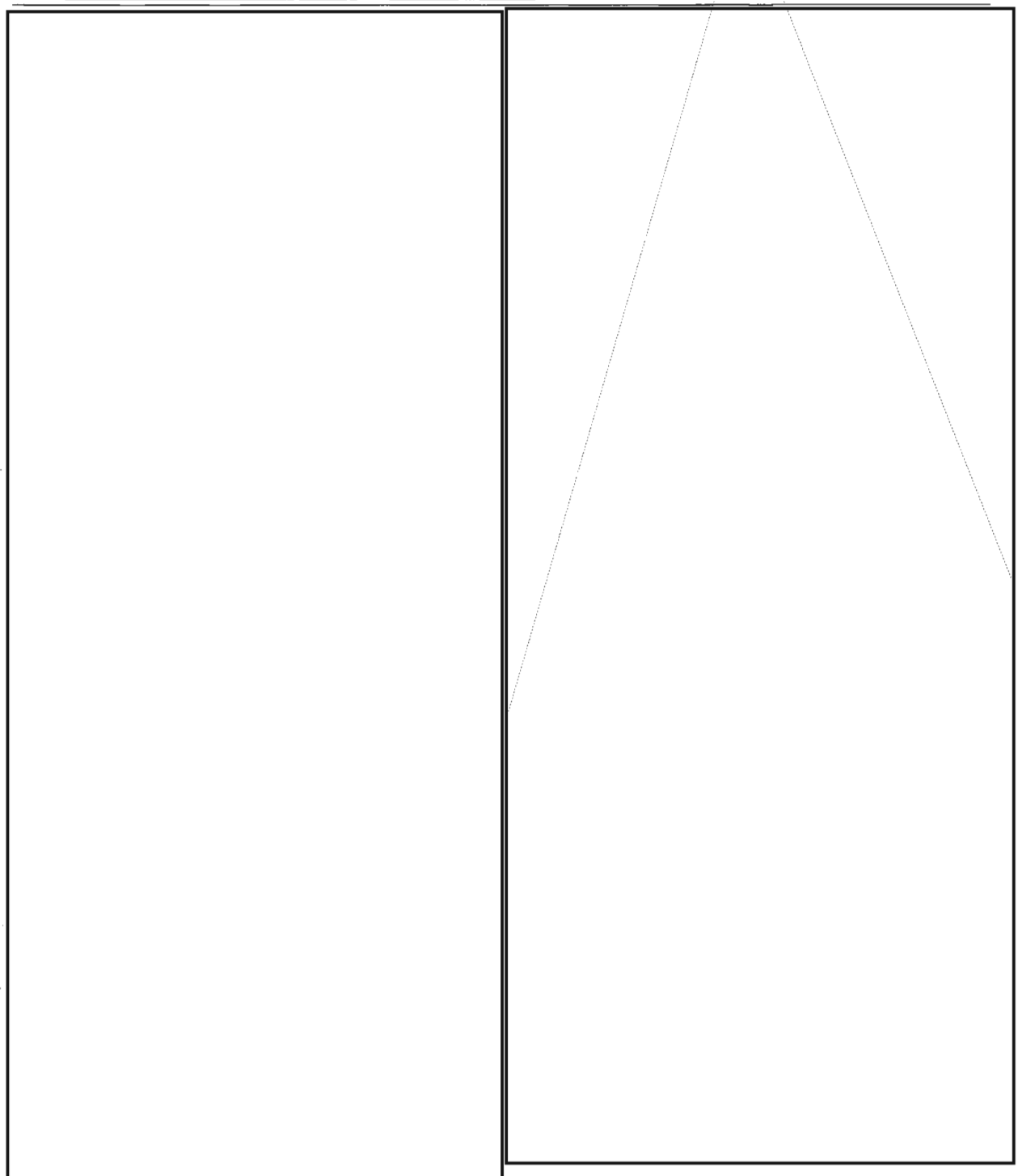
Moving now to our equipment resources: As you know, our main sources of computing

EO 1.4.(c)
DOCID: 4019718

equipment are supercomputers as well as the special-purpose devices we build when we can define a precise problem.

DOCID: 4019718

EO 1.4.(c)
P.L. 86-36



New Cryptanalytic Techniques

Another upward trend is in the development of new cryptanalytic techniques. From my work with the CA Council I believe we may be upon an age of new technique development. In particular, the conditional reestimation technique developed in conjunction with SRC holds great promise as a

EO 1.4.(c)
P.L. 86-36

major new technique; it already has resulted in several successes and appears to have wide spread applications in both the machine and manual areas.

There are a number of other sessions this week on techniques including ones on cluster analysis, branching methods, discriminant analysis, the work on neural networks, the work on garbled linear equations, and others. I find the work on the "SPLASH" boards, where we are achieving Cray 1 and SPD power on the SUNs on some specific applications, especially impressive and the applicability of some of these advanced techniques to manual systems is also encouraging.

[redacted]

Management

I am optimistic that we will continue to have successes against our targets and in our own INFOSEC efforts. The reorganization in 1987/88 of the G Manual effort will continue to pay off with additional intelligence being produced.

[redacted]

[redacted]

In closing, let me say again that we face many formidable challenges, but I am confident that we are up to those challenges. Given your continued dedication to the problems, I'm optimistic that we will continue to achieve significant cryptanalytic successes against our SIGINT targets and in the area of Information Security.

Thank you again for allowing me to speak with you this morning and I wish you a useful, productive week.

EO 1.4.(c)
P.L. 86-36

From the Past

Categories of NSA Specialties

PERS Planning Group S/SST 8 Jan 54
(Mr. Friedman)

1. In reference to your DF, dated 22 December 1953, subject: "Categories of NSA Specialties," it appears that the committee concerned made an effort to establish general categories of specialties along functional lines. This is considered a good initial step.

2. After studying the proposed list, some of the specific observations made include the following:

(a) The functions of P/P, LOG, PERS, and TNG are completely omitted. In order to execute the Agency's War and Disaster Plans, skilled personnel will be needed to fulfill some the functions of each of these.

(b) Under the group title, Cryptographic Equipment and Material, the listed functional specialties of Research, Design, and Production omit the functions of Procurement, Maintenance, Distribution, and Accounting. Further, this group seems to be overlapped, if not duplicated, by a group titled "Crypto-Material."

(c) Under the group title, T/A, are listed several functions. However, the entire incoming sorting and distribution functions are omitted. Further, it would seem reasonable to include Radio Telephone and a specific reference to the [redacted] functions.

(d) The listings under Crypto-Linguists seem to omit the need for linguists who are no necessarily cryptanalysts.

(e) The group title [redacted] is itself a misnomer. In regard to the [redacted] functions listed, it would seem appropriate to include the functions of Procurement, Operation and Maintenance.

E.O 1.4.(c)
P.L. 86-36

(f) Under the group title, Mathematics, it might be desirable to include specific references to those personnel currently familiar with applied key studies, theoretical research, and long-term machine programming.

(g) Under the Weather function, it might be well to include specific references to weather [redacted] etc.

(h) The functions listed under Management are not clear.

(i) The functions listed under Communication omit operations.

3. The following observations are made:

(a) The suggested list of NSA specialties cover some broad functions, and a few specific functions.

(b) Some broad functions necessary to execute the Emergency War and Disaster Plans and to sustain the Agency under emergency conditions are omitted.

4. In the light of the foregoing, it is suggested that:

(a) The next group who meet to discuss this problem include personnel who are familiar with the overall NSA mission and the Agency's War and Disaster Plans.

(b) The suggested list be expanded into a more complete list of critical NSA functions and that it be made more specific so that ultimately the names of personnel can be inserted into the list down to the level required for the successful execution of the Agency's War and Disaster Plans.

WILLIAM F. FRIEDMAN
Special Assistant

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019718

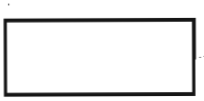
Ode to SIGINT

Come live with me in halls of marble
Where we can loaf and love and [G]
We'll spend our days in hugs and kissing
As for nights, [15 groups missing].

Forsaking spots where black gloom hovered,
Forsaking life that's [U]
Forsaking tumult, noise and rackets
Making love in [[double brackets]].

As when Apollo Thetis marries
They soon produce some ??double queries??
To cares and sadness were driven . . . . .*

**Line breaks off here; text as given.*



c1943

E.L. 86-36
EO 1.4.(c)

~~FOR OFFICIAL USE ONLY~~

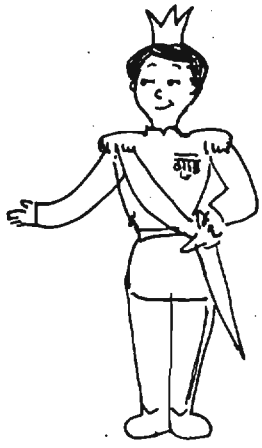
DOCID: 4019718

A Modern Fairy Tale

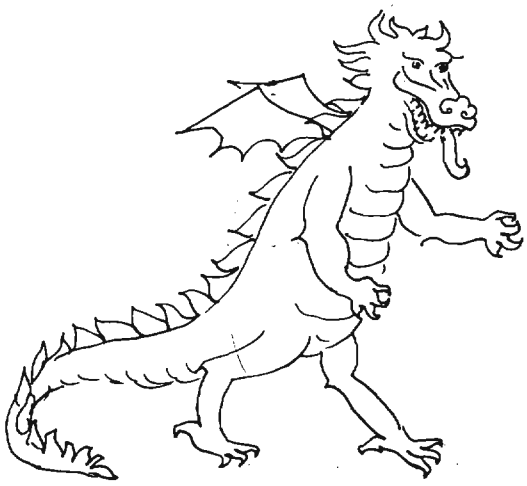
Once upon a time a fair damsel lived in the Kingdom of the Brown Bear.

The King of Centralia offered her a position of power in his kingdom. There she did many wondrous things and became well known in the scattered kingdoms of the Kingdom.

For example, the King of the Kingdom of All Other Kingdoms appreciated her efforts on behalf of his subjects. He was content that she should remain in her position in the Kingdom of Centralia and help all the subjects of the realm.



On the other hand, the King of the Kingdom of the East, also known as the Dragon of the East, or, less affectionately, as the Beast from the East, decided to lure her into his kingdom to do service only unto his subjects.

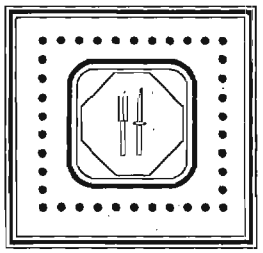


He offered her three inducements to make this change.

The first was a dingy cave for an office in contrast to the palatial quarters at Centralia.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019718



The second was an opportunity to spend two feeding times a week with the King and Queen of the Kingdom of the Brown Bear, the King and Queen of the Kingdom of All Other Kingdoms, the King of the Kingdom of Centralia, and the Wizard of Things Manual. Their mission was to draw up a unifying plan for all the kingdoms, and they became known as cohortus octo, an expression of scorn throughout the realm as 21 months of this brought them no closer to success even to this day.

The third inducement was the most unkindest cut of all. She would rule at the side of the Beast from the East instead of in a position of great power with the kindly King of Centralia.

Who would take such an offer? The King of Centralia consulted with the Wizard of Things Manual and they concluded that the Dragon of the East had cast a spell on the hapless victim!

And now to the sad conclusion of this modern fairy tale: for there was no way to break the spell except to take an early out from the Kingdom.

So Godspeed, Fair Barbara.

This Way Out

An oration on the occasion of the retirement of [ ]
September 1991, composed and delivered by [ ]

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019718

CRYPTOLOG

Editorial Policy

CRYPTOLOG is a forum for the informal exchange of information by the analytic workforce. Criteria for publication are: that in the opinion of the reviewers, readers will find the article useful or interesting; that the facts are accurate; that the terminology is correct and appropriate to the discipline. Articles may be classified up to and including TSC.

Technical articles are preferred over non-technical; classified over unclassified; shorter articles over longer.

Comments and letters are solicited. We invite readers to contribute conference reports and reviews of books, articles, software and hardware that pertain to our mission or to any of our disciplines. Humor is welcome, too.

Please note that while submissions may be published anonymously, the identity of the author must be made known to the Editor. Unsigned letters and articles are discarded.

If you are a new author, please request "Guidelines for CRYPTOLOG Authors."

How to Submit your Article

Back in the days when CRYPTOLOG was prepared on the then state-of-the-art, a Selectric typewriter, an article might be dashed off on the back of a used lunch bag. But now we're into automation. We appreciate it when authors are, too.

> *N.B.* If the following instructions are a mystery to you, please call upon your local ADP support for enlightenment. As each organization has its own policies and as there's a myriad of terminals out there, CRYPTOLOG regrets that it cannot advise you.

Send two legible hard copies accompanied by a floppy, disk, or cartridge as described below, or use electronic mail. In your electronic medium (floppy, disk, cartridge, or electronic mail) please heed these strictures to avoid extra data prep that will delay publication:

- do not type your article in capital letters
- do not right-justify
- do not double space between lines
- but **do** double space between paragraphs
- do not indent for a new paragraph
- but **do** paragraph classify
- do not format an HD floppy as DD or vice-versa--our equipment can't cope
- label your floppy or cartridge: identify hardware, density of medium, software;
- put your name, organization, building and phone number on the floppy or cartridge

The electronic mail address is *via* PLATFORM: cryptlg @ barlc05
or via CLOVER: cryptlg @ bloomfield

CRYPTOLOG publishes using Macintosh and Xerox Star. It can read output from the equipment shown below. If you have something else, check with the Editor, as new conversions are being added.

SUN	60 or 150 MB cartridge	ascii only
XEROX VP 2.0, 2.1	5 1/4" floppy only	
WANG		Stand-alone or Alliance
Macintosh	3 1/2" DD disk only	Please furnish a copy in TEXT as well as in your software, as we may not have all the software upgrades
IBM & Compatibles	3 1/2" DD or HD 5 1/2" DD or HD	Please furnish a copy in ascii as well as in your software, as we may not have all the software upgrades

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019718

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XVIII, No. 3 . . . . . 3rd Issue 1991

PUBLISHER . . . . . [redacted]

BOARD OF EDITORS

EDITOR . . . . . [redacted] (963-1103)

Computer Systems . . . . . [redacted] (963-1103)
Cryptanalysis. . . . . [redacted] (963-5238)
Cryptolinguistics. . . . . [redacted] (963-4382)
Information Resources. . . . . [redacted] (963-3258)
Information Science. . . . . [redacted] (963-3456)
Information Security . . . . . [redacted] (972-2351)
Intelligence Reporting . . . . . [redacted] (963-5068)
Language. . . . . [redacted] (963-3057)
Linguistics . . . . . [redacted] (963-4814)
Mathematics. . . . . [redacted] (963-5566)
Puzzles . . . . . [redacted] (963-1601)
Research and Engineering. . . . . [redacted] (968-7315)
Science and Technology. . . . . [redacted] (963-4958)
Special Research. . . . . Vera R. Filby (968-5043)
Traffic Analysis. . . . . [redacted] (963-3369)

Classification Officer. . . . . [redacted] (963-5463)
Bardolph Support. . . . . [redacted] (963-3369)
Clover Support . . . . . [redacted] (963-1103)
Macintosh Support. . . . . [redacted] (968-7315)
Illustrators. . . . . [redacted] (963-3360)
. . . . . [redacted] (963-4382)

P.L. 86-36

To submit articles and letters, please see previous page

For New Subscription or Change of Address or Name

MAIL name and old and new organizations and building to:

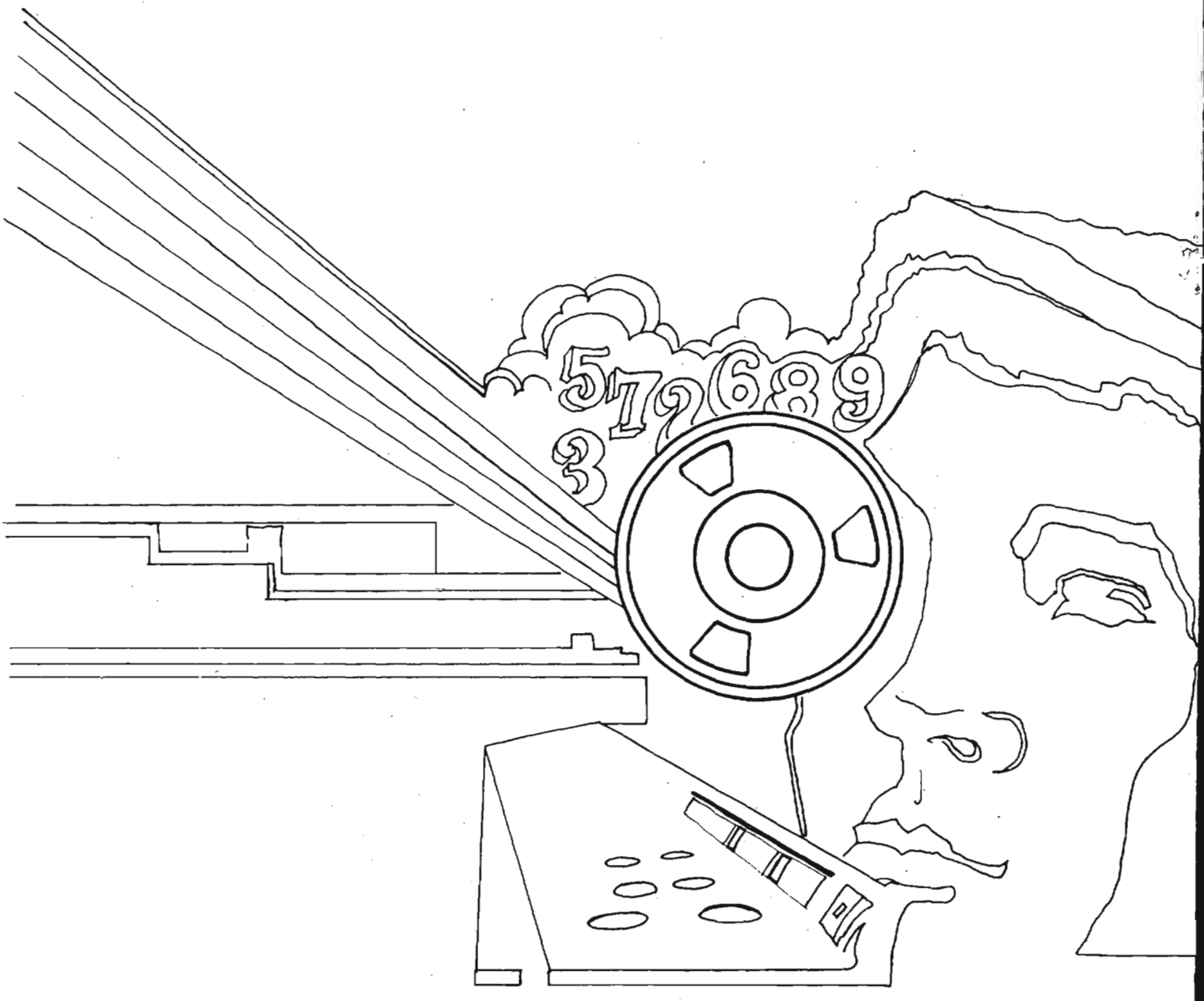
Distribution, CRYPTOLOG, P1, NORTH
or
via PLATFORM: cryptlg @ bar1c05
via CLOVER: cryptlg @ bloomfield

Please DO NOT PHONE about your subscription or matters pertaining to distribution

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

~~FOR OFFICIAL USE ONLY~~


5726893

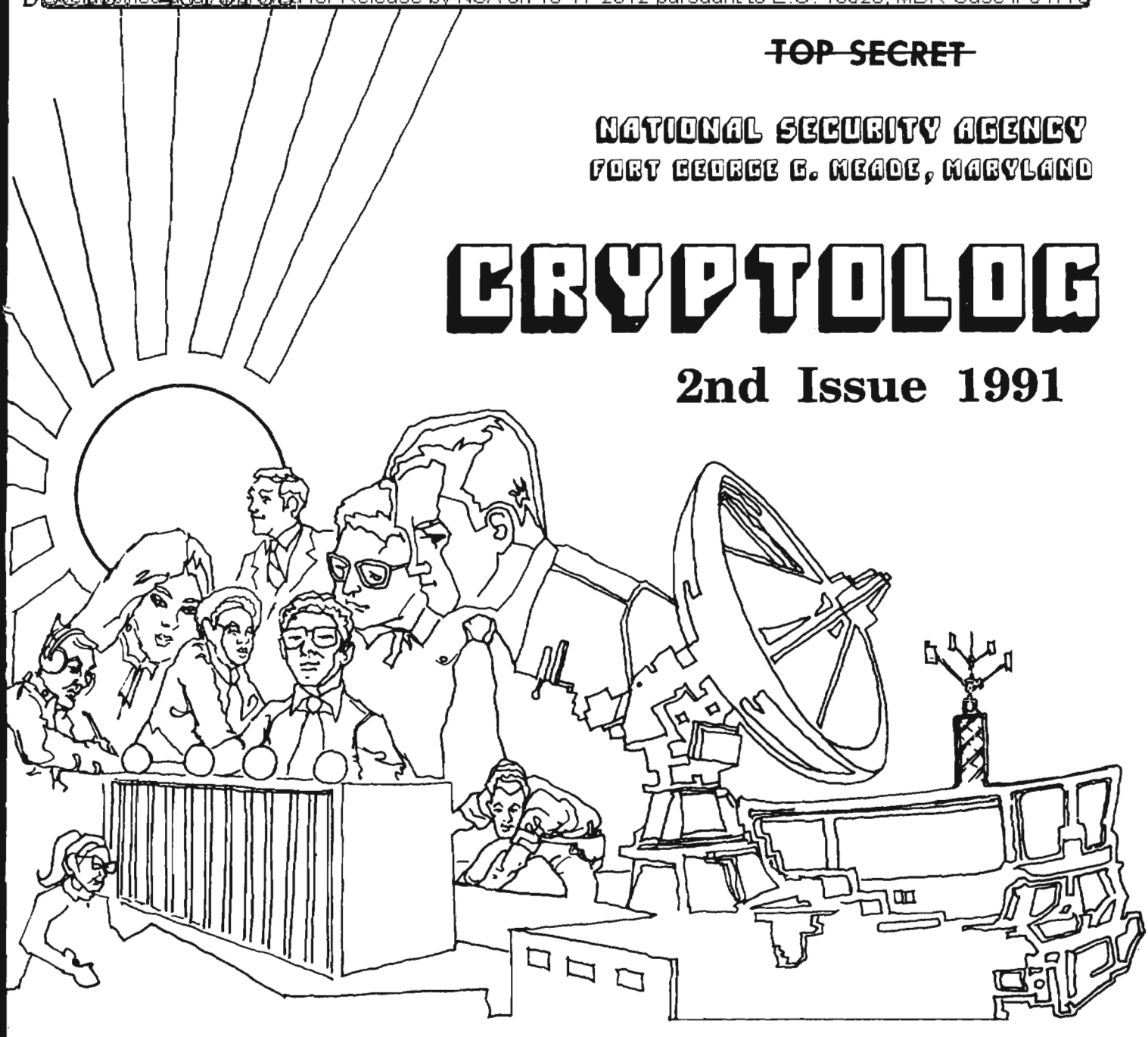
DOCID: 4011018 Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

2nd Issue 1991



SEA HUNT. . . . . [redacted] 1
BOOKBREAKERS' FORUM ON MACHINE AIDS 4
TEXTURE REPORTING . . . . . [redacted] 5
THE TEN MOST WANTED . . . . . [redacted] 7
MILLIMETER WAVE DETECTION SYSTEMS . . . . . [redacted] 9
ON BECOMING A WELL-ROUNDED CHINESE LINGUIST . . . . . [redacted] 17
CRYSCOM REQUIREMENTS FOR UNIX-TO-UNIX
DATA ENCRYPTION-DECRYPTION EXCHANGE. . . [redacted] 20
DATA FUSION 22
ON THE LIGHTER SIDE 22
FINGERTIP INTELLIGENCE. . . . . [redacted] 23
COMMENT ON GISTER . . . . . [redacted] 24
USING C++ FOR COMPUTE-INTENSIVE CODE. . . . [redacted] 25
BOOK REVIEW: SEIZING THE ENIGMA . . . . . Vera Filby 28
BULLETIN BOARD. 30
ON THE ENIGMA . . . . . [redacted] 31
BREAKING INTO OUR PAST: AN ENIGMA OF ANOTHER KIND . . . . . .
. . . . . David Gaddy. 33
EDITORIAL 36
LETTER. 36
TO CONTRIBUTE 37

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

DOCID: 4010108

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XVIII, No. 2 ..... 2nd Issue 1991

PUBLISHER .....

BOARD OF EDITORS

EDITOR ..... (963-1103)

Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Cryptolinguistics ..... (963-4382)
Information Resources ..... (963-3258)
Information Science ..... (963-3456)
Information Security ..... 972-2351)
Intelligence Reporting ..... (963-5068)
Language ..... (963-3057)
Linguistics ..... (963-4814)
Mathematics ..... (963-5566)
Puzzles ..... (963-1601)
Research and Engineering ..... (961-8362)
Science and Technology ..... (963-4958)
Special Research ..... Vera R. Filby (968-5043)

Classification Officer ..... (963-5463)
Bardolph Support ..... (963-3369)
Clover Support ..... (963-1103)
Macintosh Support ..... (961-8362)
Illustrator ..... (963-3360)

P.L. 86-36

To submit articles and letters, please see inside back cover.

For New Subscription or Change of Address or Name

MAIL name and old and new organizations and building to:

Distribution, CRYPTOLOG, P1, NORTH
or
via PLATFORM: cryptlg @ bar1c05
via CLOVER: cryptlg @ bloomfield

Please DO NOT PHONE about your subscription or matters pertaining to distribution

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

~~FOR OFFICIAL USE ONLY~~

EO 1.4.(c)
P.L. 86-36
DOCID: 4010108

SEA HUNT

[redacted]

~~*This article is classified* TOP SECRET UMBRA *in its entirety*~~ P.L. 86-36

[redacted]

[redacted]

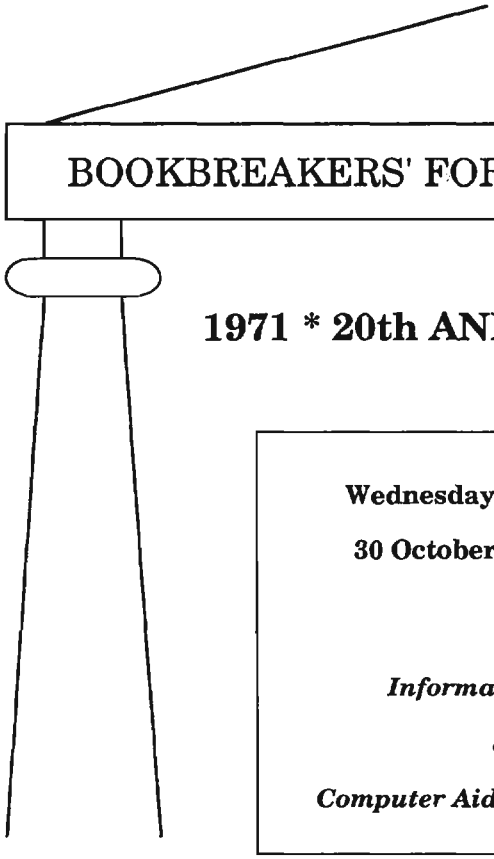
P.L. 86-36
EO 1.4.(c)

DOCID: 4010108

P.L. 86-36
EO 1.4.(c)

DOCID: 4010108

P.L. 86-36
EO 1.4.(c)



BOOKBREAKERS' FORUM ON MACHINE AIDS

1971 * 20th ANNIVERSARY * 1991

Wednesday, Thursday, Friday

30 October—1 November 1991

❖ ❖

Informal Seminars

on

Computer Aids to Bookbreaking

Who should attend? Anyone working on codes or code charts:

Linguists
Cryptanalysts
Bookbreakers
Cryptolinguists
Providers of computer support to code problems
Managers of code problems

For more information and to get on the mailing list, please fill out the coupon below, or write your name, organization, and building on a piece of paper and send it to:

[redacted] Chairman
Bookbreakers' Forum on Machine Aids
P15
Ops-1 NORTH

P.L. 86-36

- -

Name_____

Organization_____ Building_____

- -

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010108

Textur e Reporting

SIGINT with Feeling

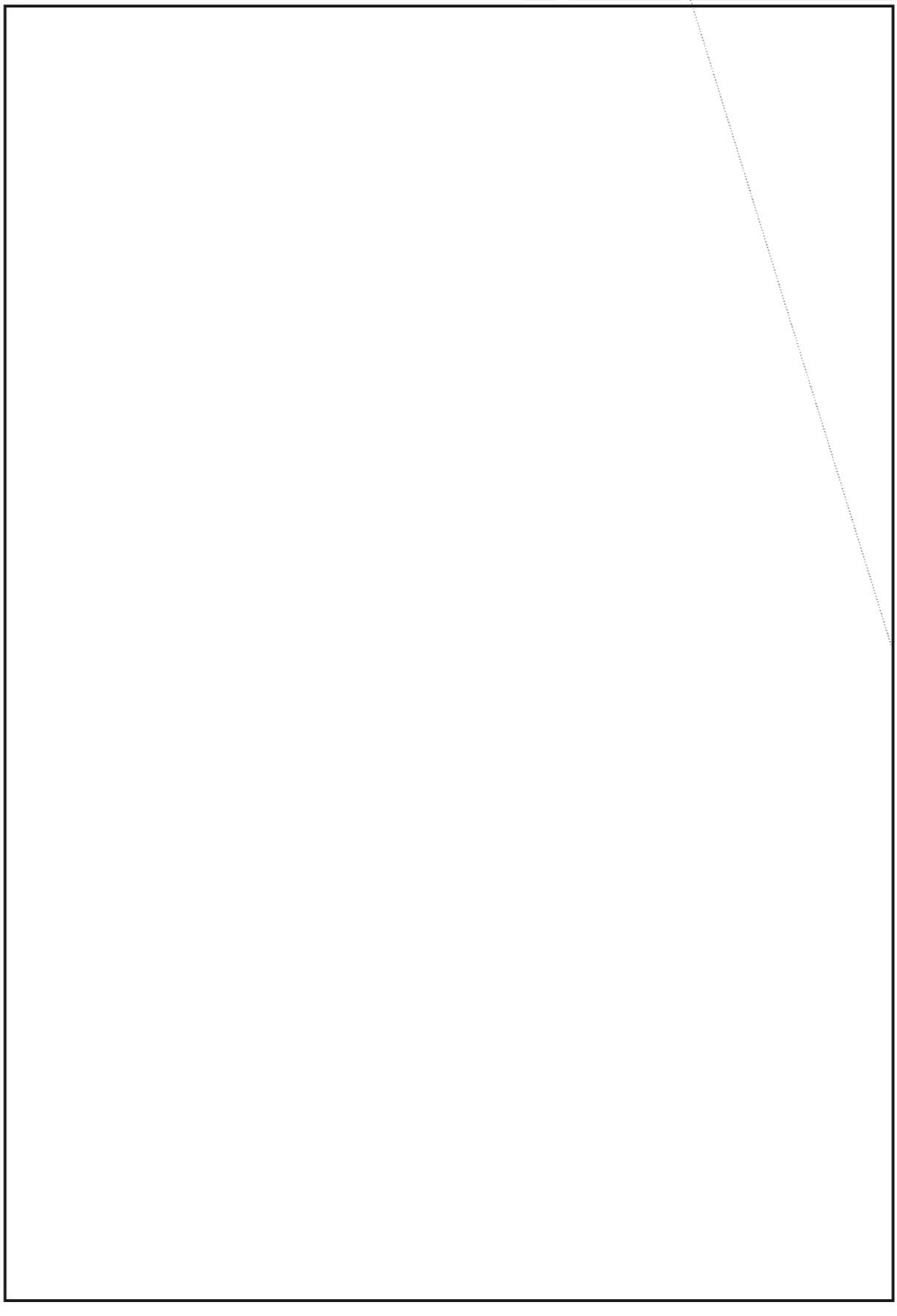
P.L. 86-36

E34

EO 1.4.(c)
P.L. 86-36

DOCID: 4010108

EO 1.4.(c)
P.L. 86-36



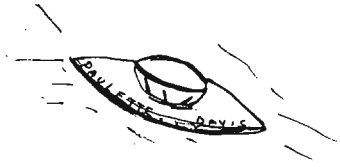
DOCID: 4010108

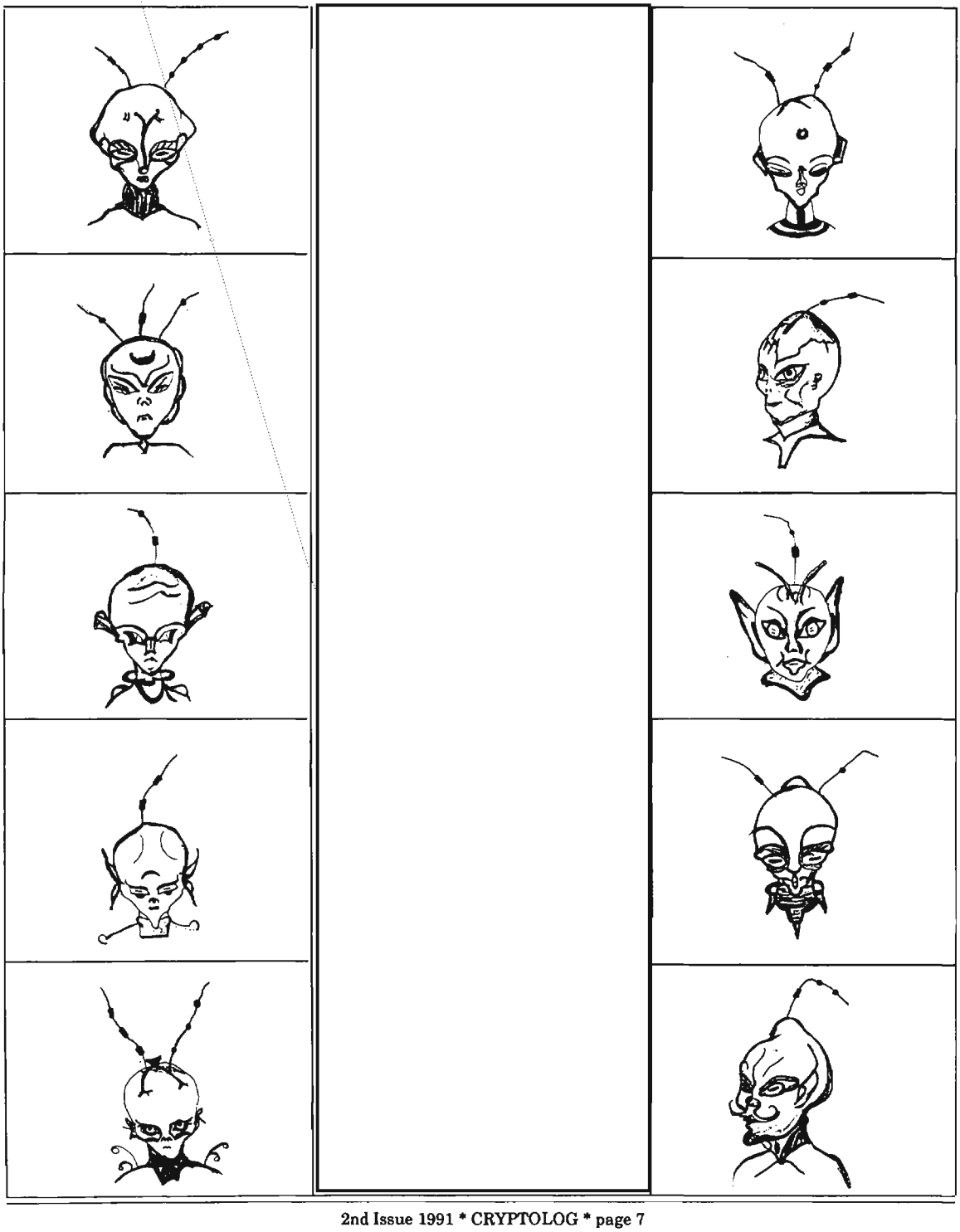
~~SECRET~~

THE TEN MOST WANTED

by [redacted] W332 P.L. 86-36

P.L. 86-36

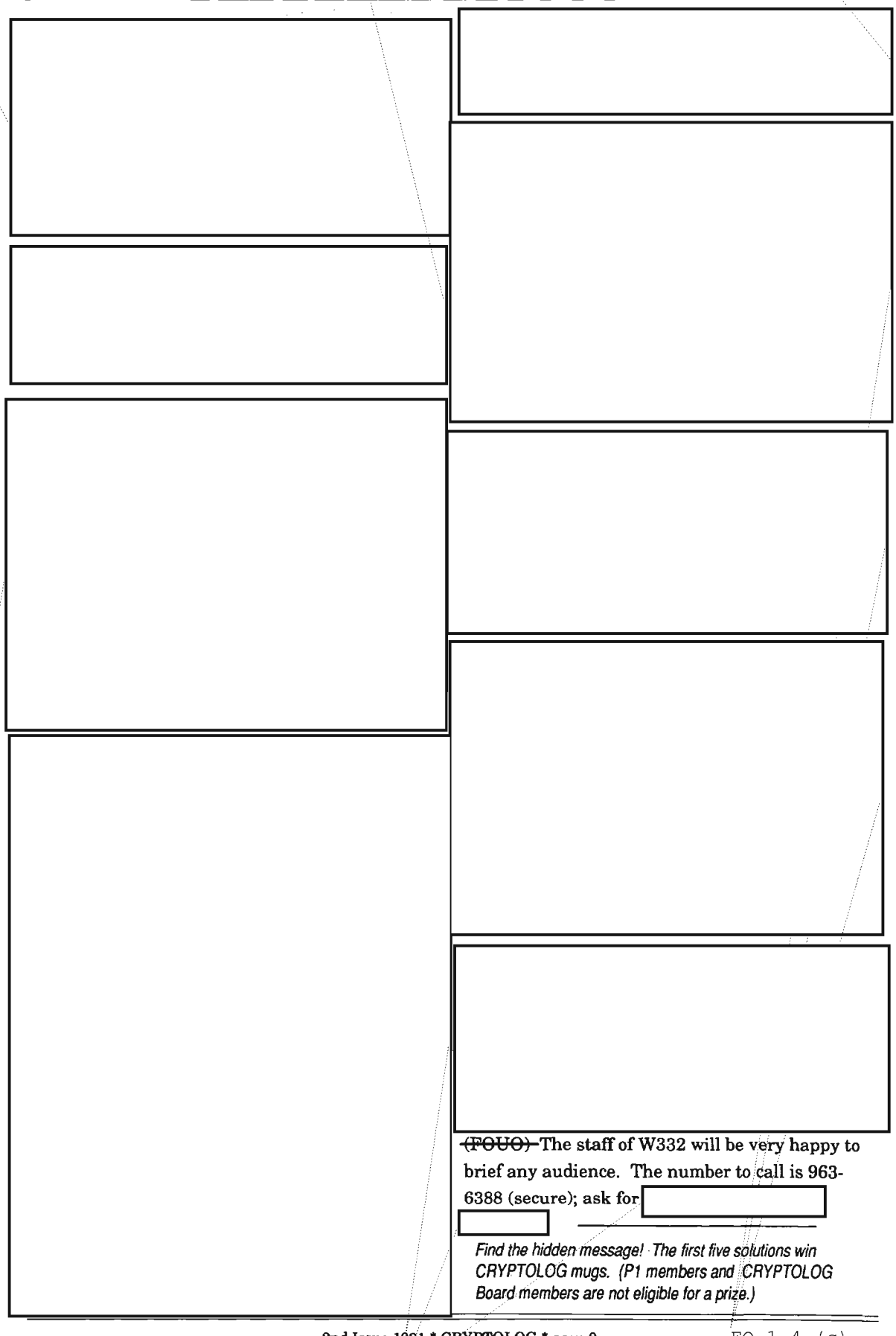




~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36
DOCID: 4010108
P.L. 86-36
P.L. 86-36

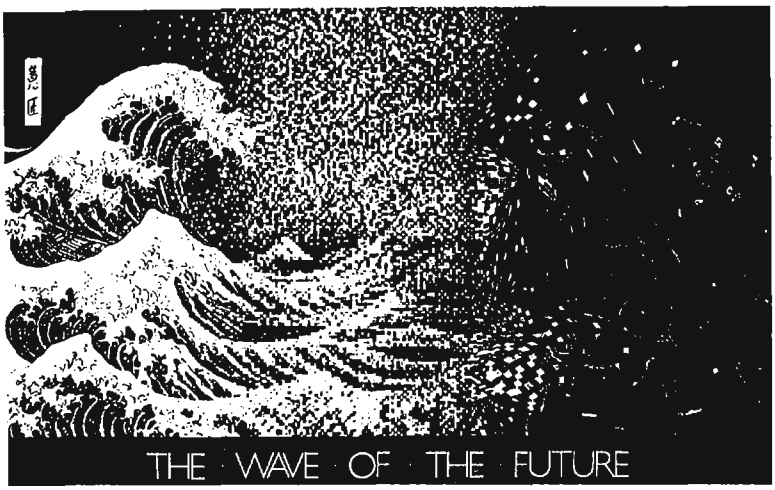


~~(FOUO)~~ The staff of W332 will be very happy to brief any audience. The number to call is 963-6388 (secure); ask for

Find the hidden message! The first five solutions win CRYPTOLOG mugs. (P1 members and CRYPTOLOG Board members are not eligible for a prize.)

EO 1.4.(c)
P.L. 86-36
P.L. 86-36
EO 1.4.(c)
P.L. 86-36

DOCID: 4010108



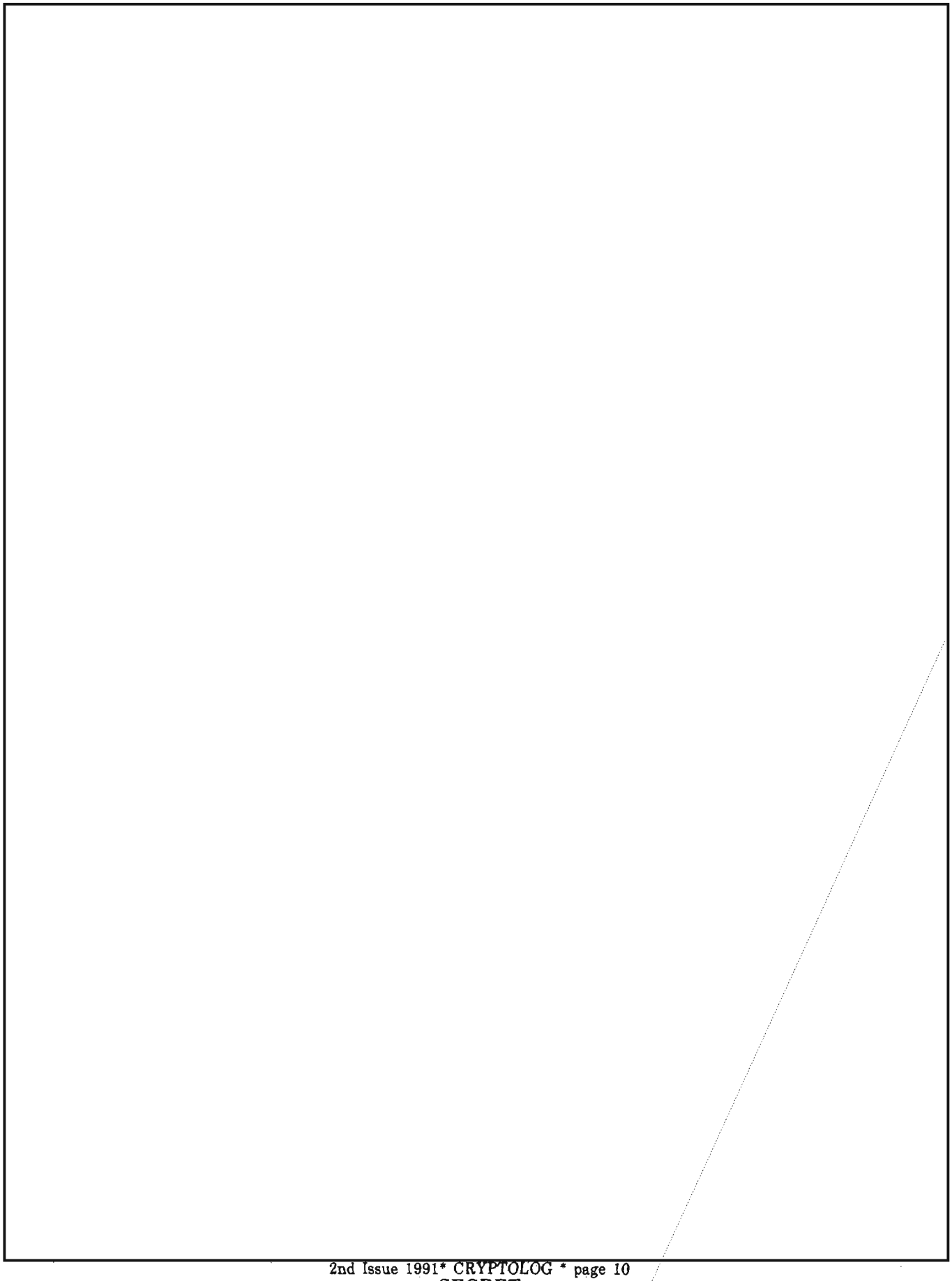
NEW MILLIMETER WAVE DETECTION SYSTEMS

R541

(U) One of the strongest images of the recent war in the Middle East was that of reporters broadcasting seemingly effortlessly from rooftops in Baghdad or the sands of Kuwait. But this kind of mobile reporting is really not so easy because the equipment needed is quite heavy, the antennas are about 7-8 feet in diameter, and several technicians are necessary to operate the equipment. This may change quite rapidly in the future, however, as the push to higher frequencies in the millimeter range, conventionally, 30-300 GHz, will make truly suitcase-size earth terminals possible. With antennas as small as a foot or so in diameter and with enough bandwidth to accommodate all the reporters of a future operation (a truly large number!), such millimeter wave systems will really "wire" the global village. The military is already studying the use of this wavelength region for communication satellites which would use much smaller, much less complex ground sites, yet provide an enormous increase in channel capacity. Can the commercial world be far behind?

(U) Another image left with us from DESERT STORM was of smart bombs that homed in on their targets with surprising accuracy. Although these weapons were hardly news to even the most casual reader of *Aviation Week*, their actual successful use in combat will surely spur further research in this direction. One of the most promising proposals in the continuing search for battlefield superiority is the use of millimeter-wave guided weapons. This wavelength region is very well suited for such a mission. Metal targets stand out well from any natural background, and the target is not obscured by dust, fog, rain, or the smoke of burning oil wells. The small antenna would fit into a modest missile of only 3-6 inches in diameter, yet it would provide both sufficient gain and small enough beam width to readily find tank-size targets. Together with some modest processing capability such as "fire and forget," warheads delivered from long range could provide an enormous advantage on the future battlefield.

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~ EO 1.4.(c)
P.L. 86-36

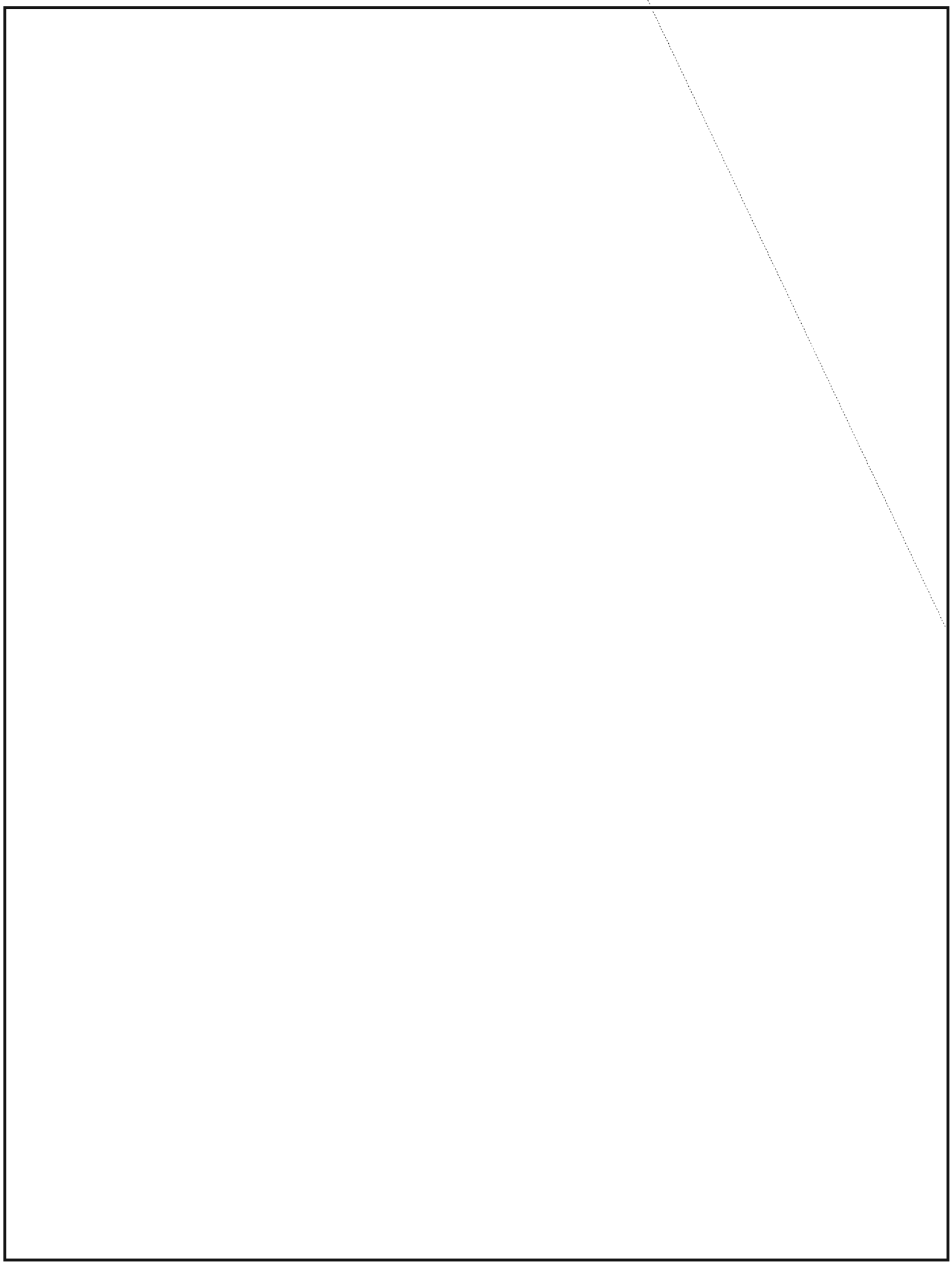


~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36

DOCID: 4010108

EO 1.4.(c)
P.L. 86-36



Quasi-optics

(U) Quasi-optical concepts treat millimeter radiation as one would optical radiation in that lenses and other focusing elements are used to concentrate the energy to be detected. The main advantage over standard parabolic reflectors is that the system can be designed so that an array of detectors can be in focus and at the same time allow a "staring" nonscanning system to cover a whole sector without any need for mechanical movement. To take full advantage of this new capability implies that a detector array is available that has dimensions no larger than the wavelength of the radiation. In the millimeter wave region this means that the detectors must be made by some photolithographical process.

(U) Figure 3 shows a millimeter quasi-optic configuration that will be used in this new design. The detector is of a planar design which also incorporates an antenna placed at the focus of the quasi-optic system. There are several candidates for the detectors; two will be discussed in detail: superconducting tunnel junctions and Si/Ge superlattices.

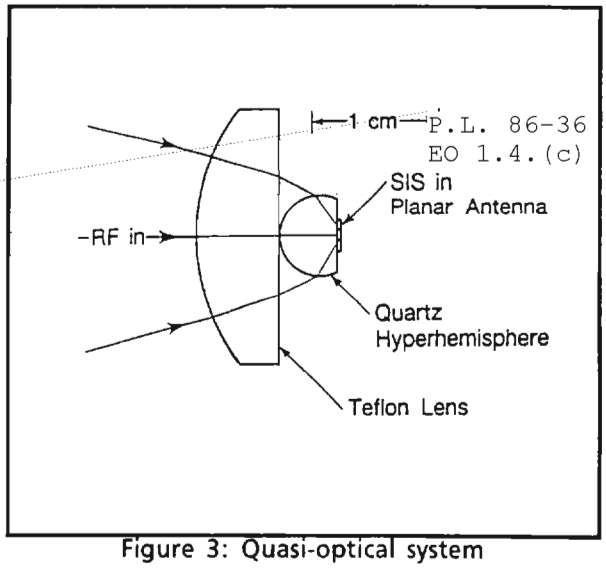


Figure 3: Quasi-optical system

Detectors

(U) The superconducting detector depends on the quantum mechanical tunneling between two superconductors. This effect is best understood from studies of tunnel junctions consisting of two thin superconducting films separated by a several-nanometer-thick tunnel barrier made from the oxide of one of the metals or from some other insulating material.

(U) Superconducting receivers for infrared and millimeter waves depend on the nonlinear response of the tunneling currents when they are driven by constant and RF voltages. In fact, it has been said that this current-voltage nonlinearity is the strongest known in physics.

(U) Figure 4 shows an experimental I-V curve for a tunnel junction. The time-dependent

DOCID: 4010108

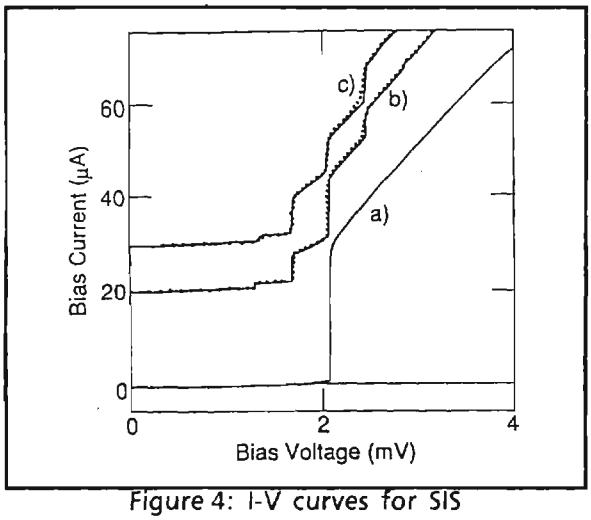


Figure 4: I-V curves for SIS

current I(t) resulting from a voltage V across a tunnel junction can be written :

$$I(t) = I_c \sin\phi + V[G(V) + G'(V)\cos\phi] + C\frac{dV}{dt}$$

The first term on the right is the lossless Josephson-pair tunnel current which depends on the phase difference Φ of the wave function of the two superconductors. The second term VG'(V) is the product of a voltage and a nonlinear coductance called the quasi-particle term. The third term represents an interaction between the first two.

(U) Most infrared and millimeter wave devices can be classified as either Josephson effect or quasi-particle devices depending on which nonlinearity is the important effect. The nonlinearity in quasi-particle conductance G(V) arises from the energy gap of width 2Δ in the density of excited single particle (quasi-particle) states. In an ideal junction at T=0°K, quasi-particle current can only flow when a bias voltage V>2/Δ/e is applied. Because of the singularities in densities of states at the gap edges, the onset of tunneling current at 2Δ/e has infinite slope in superconductivity theory.

(U) Figure 4 shows the discontinuity at 2 mv bias voltage. Though the slope is very steep, there is always some rounding of the corner at 2Δ and some leakage current is apparent at lower voltages. The other curves in Figure 4 involve photon assisted tunneling leading to an enhancement or reduction of quasi-particle current on a voltage-energy scale of the millimeter wave photon.

(U) It is the nonlinear tunnel junction I(V) characteristics that are to be used in this new millimeter wave detector system. These junctions are made by photolithographic techniques together with any tuning structures needed to match impedances. Arrays of junctions can easily be fit into the quasi-optic concept.

Mixers

(U) The junction I(V) due to quasi-particles can be used in several ways to make a broadband receiver system. The nonlinearity can be used to make a quasi-particle heterodyne mixer which converts signals from some high RF down to a lower frequency where amplification and signal detection are more convenient. When strongly pumped by a local oscillator at ω_{LO}, the local oscillator frequency, the mixer produces a linear response at the intermediate frequency ω_{IF} when a small signal is supplied at the signal frequency $\omega_S = \pm m\omega_{LO} + \omega_{IF}$.

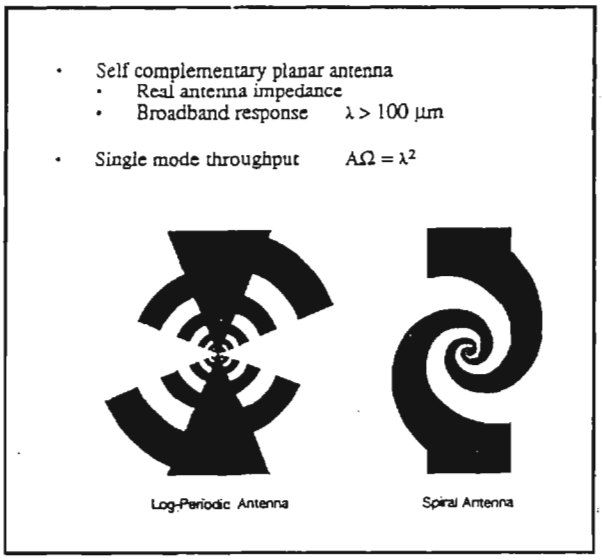
(U) The full quantum theory is required to describe mixing in Superconductor-Insulator-Superconducting (SIS) junctions whose I-V curves are sharp on the voltage scale hω/e. When quantum effects are important, the theory predicts net mixer gain and very low noise and because of arguments related to the Heisenburg uncertainty principle, there is a minimum zero-point noise power for mixers of hωB. SIS mixers have been built at 33 GHz and at 90 GHz which have measured noise temperatures within a factor of two of this quantum limit. It should be pointed out here that the requirement of small current flow at voltages below 2Δ/e sets an upper limit of about $T_c/2$ on the operating temperatures that can be used for SIS mixers, where T_c is the critical temperature

DOCID: 4010108

Operating temperatures that can be used for SIS mixers, where T_c is the critical temperature where superconductivity vanishes. This cryogenic problem has been eased with the recent availability of NbN junctions with $T_c = 15°K$. At present there is no appropriate high T_c SIS junction technology.

(U) Thin film SIS tunnel junctions can be integrated in a planar configuration with log-periodic or log-spiral antennas which have central lobes and are self-complementary, meaning they have a real impedance of 120 Ω. These antennas, shown in Figure 5, fit nicely into the quasi-optical concept of Figure 3.

Figure 5: Wide Band Antennas



Direct Detectors

(U) Another SIS concept for a detector is the direct detector, also called a video, or square law detector. This design uses the nonlinearity of the quasi-particle I-V curve to rectify a coupled RF signal. The current responsivity S_I of such a detector is defined as the induced direct current divided by the available signal power $S_I = \Delta I_{dc}/P_S$. In the quantum theory, the current responsivity is obtained from the small signal limit of the theory of the pumped I-V curve for millimeter wave photons of energy $\hbar\omega$, at the bias point V_0:

$$S_I = \frac{e}{\hbar\omega}\left[\frac{I_{dc}(V_0+\hbar\omega/e)-2I_{dc}(V_0)+I_{dc}(V_0-\hbar\omega/e)}{I_{dc}(V_0+\hbar\omega/e)-I_{dc}(V_0-\hbar\omega/e)}\right]$$

(U) The quantity in square brackets above is the second difference of the unpumped I-V curve for the three points $V = V_0$ and $V = V_0 \pm \hbar\omega/e$, divided by the first difference computed at $V = V_0 \pm \hbar\omega/e$. In the classical limit, where the current changes slowly on a scale of $\hbar\omega/e$, the differential approximation gives the usual result for a diode detector:

$$S_I = \frac{1}{2}\left(\frac{d^2I}{d^2V}\right)\Big/\frac{dI}{dV}$$

If the I-V curve is sharp enough that the current rise at 2Δ occurs within the voltage scale $\hbar\omega/e$, and if the bias voltage V_0 is just below $2\Delta/e$, then $SI = e/\hbar\omega$. This quantum limit to the responsivity corresponds to one extra tunneling electron for each coupled photon.

(U) Since direct detectors do not preserve phase, there is no quantum limit to the detector noise analogous to that of the mixer. The intrinsic noise of the SIS direct detector is simply the shot noise in the dark current $<I>$ at the bias point V_0. For a postdetection bandwidth B, the noise equivalent power (NEP) in units of $W/Hz^{1/2}$ of a RF-matched detector is:

$$NEP = \frac{<I^2>^{1/2}}{S_I B^{1/2}} = \frac{\left[2eI_{dc}(V_0)\right]^{1/2}}{S_I}$$

(U) When the signal power is increased, the responsivity of an SIS detector falls; however, the power required to saturate the device is much greater than that of a single junction mixer.

Experiments with SIS Direct Detectors

(U) The first experimental test of an SIS direct detector in 1980 showed excellent agreement with the quantum theory. The current rwith the quantum theory. The current responsivity

DOCID: 4010108

S_I of 3600 amperes per watt was within a factor of 2 of the quantum limited value e/hω at 36 GHz. These results have been repeated at much higher frequencies recently. The NEP measured at 36 GHz was 2.6 x 10^{-16} W/$Hz^{1/2}$ which is essentially the performance of the best millimeter wave astronomical instruments.

(U) Little progress in the sensitivity of SIS direct detectors has been made since the first experiments. However, the limit set by shot noise in the junction current is not fundamental. The fundamental thermally activated leakage current is of order $I \sim \exp(-\Delta/kT)$, which is many orders of magnitude smaller than the extrinsic leakage current that is observed in all SIS junctions. Progress has been slow because relatively few applications of SIS junctions depend in a critical way on leakage current. This situation is now changing. The promise of X-ray detection concepts based on quasi-particle trapping and subsequent tunneling has greatly increased recent activity. Several well funded groups in the US (and in Europe) have announced their intentions of producing junctions with leakage currents reduced by orders of magnitude.

Integration of Direct Detectors and Antennas

(U) The SIS direct detector is a fast very broadband RF detector and is the most sensitive detector at millimeter wavelengths for temperatures >1°K. As a planar lithographed structure it is compatible with planar lithographed antennas, coupling structures, filters, etc. Such elements can be fabricated into focal plane arrays by conventional optical lithography. This includes the self-complementary structures discussed above such as log-periodic and log-spiral which have no characteristic length dimension, and therefore have real terminal impedances and extremely wide bandwidths. The impedance of the SIS detector junction, however, has both real and imaginary parts so that a matching network is needed for coupling. This is also shown in Figure 6 along with the equivalent circuit.

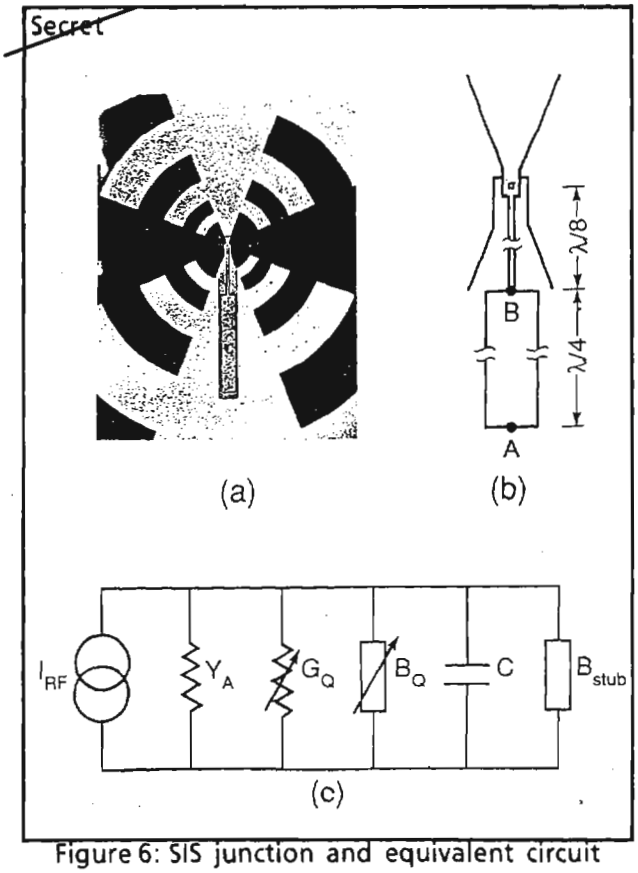


Figure 6: SIS junction and equivalent circuit

(U) The full power of microstrip technology can be applied to the coupling of SIS direct detectors for millimeter wavelengths. The loss in superconducting films is negligible for films at temperatures well below T_c; therefore, lossless broad band couplers, band and low pass filters, and even multiplexors can easily be implemented. The possibility also exists to deposit several direct detectors on a single antenna and to couple them via multiplexors and band pass filters. A frequency multiplexed spatial array of detectors can be produced in a way that can meet all the objectives of a search system.

Novel radiometer for millimeter waves

(U) A novel radiometer configuration, suggested by Prof. Richards, uses one SIS junction pumped with a local oscillator as a heterodyne down

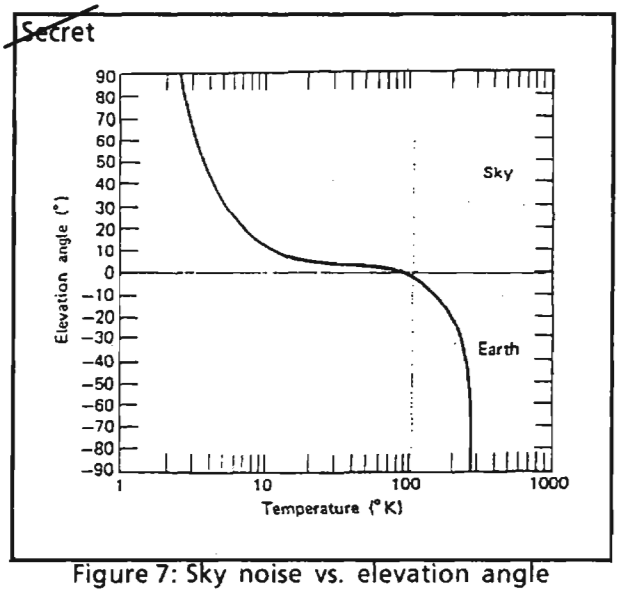


Figure 7: Sky noise vs. elevation angle

converter followed by a second SIS junction, which is used as a millimeter wave photon detector. From one viewpoint, the mixer is a preamplifier for the photon detector. It amplifies the photon arrival rate by the product of its power gain and the frequency down-conversion ratio. The SIS photon detector is used at the relatively low IF frequency where its NEP is better than at the RF frequency. From another viewpoint, this system is a simplified version of a heterodyne radiometer that avoids the need for the IF amplifier because of the conversion gain of the SIS mixer and the excellent performance of the SIS direct detector. This configuration appears to have higher sensitivity than the SIS direct detector while retaining its high speed and operating temperature. It appears to be simple enough that planar integrated arrays or detectors are possible. Prof. Richards may apply for a patent for this novel receiver design that uses the strengths of each part of a tunneling junction operations.

(U) Preliminary steps have been taken to test this receiver concept. The antenna coupled SIS mixer and the SIS direct detector have been fabricated and separately tested. The new element, which has been successfully tested, is an efficient low pass microstrip filter required to connect the mixer to the detector. The overall system is being assembled for a proof of concept.

FIELDABLE SYSTEMS

(U) With the very low noise wideband receivers available from SIS technology ($T_N < 4°K$), there are several options as to how an actual fieldable system architecture would look. For example, at W band (75-110 GHz), one can see from the data in Figure 2 that present mixer noise alone leads to a temperature of 9000°K (15 db = 9000°K). If the system is constrained to look at the earth at $T \approx 300°K$, then the increase in bandwidth for the same sensitivity would be $9000/300 = 30$.

EO 1.4.(c)
P.L. 86-36

DOCID: 4010108

EO 1.4.(c)
P.L. 86-36

~~TOP SECRET~~

On Becoming a Well-Rounded Chinese Linguist

(U) One of my lifetime goals is to feel comfortable with the Chinese language and to understand Chinese culture and society. The trouble is that Chinese is difficult to learn, and nobody knows that better than a student of Chinese, even after 30 years. With that in mind, I'd like to present my views on what becoming a well-rounded Chinese linguist means in the SIGINT environment and to offer some suggestions on how to become one.

(U) In these days of high technology, people in all walks of life necessarily have become increasingly specialized. Doctors specialize in various kinds of ailments; lawyers specialize in various kinds of law; mechanics specialize in different makes of car. At NSA we are no less specialized. We have specialists in computers, traffic analysis, collection, and language analysis, just to name a few fields. Furthermore, our specialization extends beyond these major categories; for the SIGINT linguist, the result can be using language that is very narrowly focused.

(~~C CCO~~) NSAers tend to be so specialized that we are encouraged to diversify in order to broaden our experience. But in the language career field one can specialize in graphic or voice. I did not support the distinction because I believe that a major goal of the language certification process should be to identify "all-round" good linguists, encompassing both graphic and voice, but I will concede that it works well for individual career advancement.

ON THE TESTING PROCESS

~~(C CCO)~~ The PQE testing process has evolved from identifying "all-round" professional linguists to identifying linguists whose "professionalism" is somewhat more focused. If you have been around since the Chinese PQE first began, you will remember that in the early days aspirants were required to demonstrate expertise in graphic AND aural Chinese.

~~(C CCO)~~ To have passed one of the early PQEs was a major accomplishment, and those who did, genuinely could be considered to be good, all-round linguists, not only in a general sense, but also as SIGINT linguists. Furthermore, they reasonably could be expected to be capable of handling any language task with a minimum of training. They certainly met the standard of the day which went something like, "Professional (Chinese) linguists should be able to handle any language task which they might be called upon in the middle of the night to perform without assistance, and produce finished material upon which an end-product report reliably could be based."

P.L. 86-36

~~TOP SECRET~~ EO 1.4.(c)
~~HANDLE VIA COMINT CHANNELS ONLY~~ 86-36

EO 1.4.(c)
P.L. 86-36
DOCID: 4010108

~~(FOUO)~~ The point is that the certification process in my opinion identifies and fosters well-rounded linguists only in the sense that they are well-rounded with regard to related-fields and SIGINT disciplines, not in the sense that their specific language expertise is broadly based.

THE WELL-ROUNDED LINGUIST

(U) Now my idea of an well-rounded linguist doesn't mean that you have to be highly proficient in every aspect of the language, although that's certainly a noble goal to shoot for. I do believe, however, that well-rounded Chinese linguists should have certain basic skills, and those skills are the same for virtually any language, either native or acquired. Namely, they are the abilities to read, write, and speak the language to a sufficient degree that they can function well in-country.

~~(TS-CCO)~~ So how does one go about becoming an well-rounded Chinese linguist? There is no single roadmap on how to do it, but if you haven't already guessed, I have some personal opinions based upon my own experience and those of my colleagues.

(U) First and foremost, of course, is education. That doesn't necessarily mean having a college degree, but it certainly means having a solid background in formal Chinese language training. Many of us acquired this training through intensive instruction at the Yale University Institute of Far Eastern Languages, and later, the former American Embassy School of Chinese Language and Area Studies in Taichung, Taiwan.

(U) Secondly, and perhaps equally important is that one just has to love the language and culture. There has to be a desire to go beyond the minimum necessary to perform the job, and this, I believe, is the key to success in learning beyond the classroom walls. I like to think of linguists who have that desire as "purists" to some extent; we learn because it's there. I don't mean to imply that we consider ourselves scholars, although I'm sure there are some among us who fit into that category.

(U) What I'm really driving at is that learning Chinese has to become an avocation, and wanting to become better at it is just natural. However, as natural as that desire may be, it also takes a fair amount of work.

~~(TS-CCO)~~ Since I'm just a student of Chinese and not a true scholar, I want to share a few of my ideas, which upon reflection helped me, in the hope that others might find them useful.

Written Chinese

(U) Let's start with written Chinese. I can't over-emphasize how important learning Chinese characters and reading are. The more characters you know, the easier it is to learn new characters and new character compounds, thereby, increasing yourreading and oral vocabulary. Remembering a word or phrase is easier if you can visualize the characters for it. So, firstly, you should take as many formal reading courses as you can, but don't stop there. Subscribe to—at least, scrounge—original language magazines and or newspapers, and read, read, read. Take the time now and again to mark characters which you don't know in at least one short article, look them up in a dictionary, make and study flashcards (I'm a staunch advocate of flashcards). Translate a short passage occasionally to keep your skills sharp, especially if you don't get that kind of practice on the job. As your vocabulary grows, the reading gets easier and more enjoyable for you are relying less on the dictionary. Also, frequent reading in Chinese helps keep you abreast of what's happening in Chinese society.

(U) As to learning cursive script, take a basic course, learn to write some of the cursive forms, and whenever you have some time, practice using them until they become second nature (you don't have to become extremely proficient to make it useful). When you doodle, doodle on your note pad in Chinese using what you have learned.

DOCID: 4010108

Think of word compounds and write the characters a few times just to improve your handwriting and for retention. If you can't recall a character, stop and look it up. Read as much handwritten material as you can get your hands on until you feel fairly proficient at it. Once you are proficient, though you'll get rusty if you don't use it often, you will be able to pick it up fairly quickly when the need arises.

~~(C-CCO)~~ Become familiar enough with the STC book so that you can at least turn to or get close to the correct page for a given radical when you want to look up a character. Even if you don't learn the exact STC groups for lots of characters, simply knowing how to find them rapidly may help you either on the PQE, in solving garbles in STC traffic, and other operational situations where STC is required.

Aural Comprehension

(U) For aural comprehension, listen to recorded materials from the radio, or videotape the Chinese language news from Taiwan off the PBS television station in Washington if you can. Take every opportunity to speak Chinese in restaurants, or wherever else you find someone with whom to talk—being ever mindful of security considerations, of course. If you have a good ear, take a tour in transcription to improve your aural comprehension and expand your general knowledge.

MUSINGS

(U) On a more general note, pick up a Chinese-English dictionary from time to time and just browse through it. You'll be surprised sometimes to find the characters for word compounds you know how to say but not necessarily write, not to mention revisiting compounds long since learned and forgotten. Moreover, you can learn some interesting things which you might not otherwise learn from newspapers and other media.

(U) Now, I know that family, friends, outside interests and commitments all compete for the same free time needed for language study such as I have described. Nevertheless, I've found that if you're serious, you can find some time in a busy schedule even if it's not daily. I sometimes think of what my calligraphy teacher in Taiwan once said about practicing writing Chinese characters with a brush pen. When I reached a certain point, he told me that I no longer needed his instruction, and that if I would just take 15 minutes to practice each day, I would do just fine.

(U) Sixteen years later I often wish I had taken his advice. Instead, I let something or other interfere with my practice sessions so my calligraphy never reached the point I had hoped it would. Recently it dawned on me that if in all these years which I have been associated with Chinese language, I had learned just one new character per day, even with interruptions from other activities, I would know all the characters I would ever need to know.

~~(C-CCO)~~ Will the effort to go an extra mile to learn through self-study ever pay off or will it simply be an academic exercise? I believe it does pay off. It goes without saying that you will derive self-satisfaction as your skill with the language expands, but I believe you will find that by increasing your overall language capability your efficiency on the job will improve as well. You'll spend less time consulting dictionaries, increase your ability to scan for significant items, and be able to handle a wider variety of subject matter.

~~(TS-CCO)~~ Moreover, you never know what opportunity may present itself in the future if you have the proper skills. You will look back and thank your lucky stars that you expended extra effort over the years to round out your language and cultural training and experience, and take pride in the accomplishments derived from your efforts to become a well-rounded Chinese linguist.

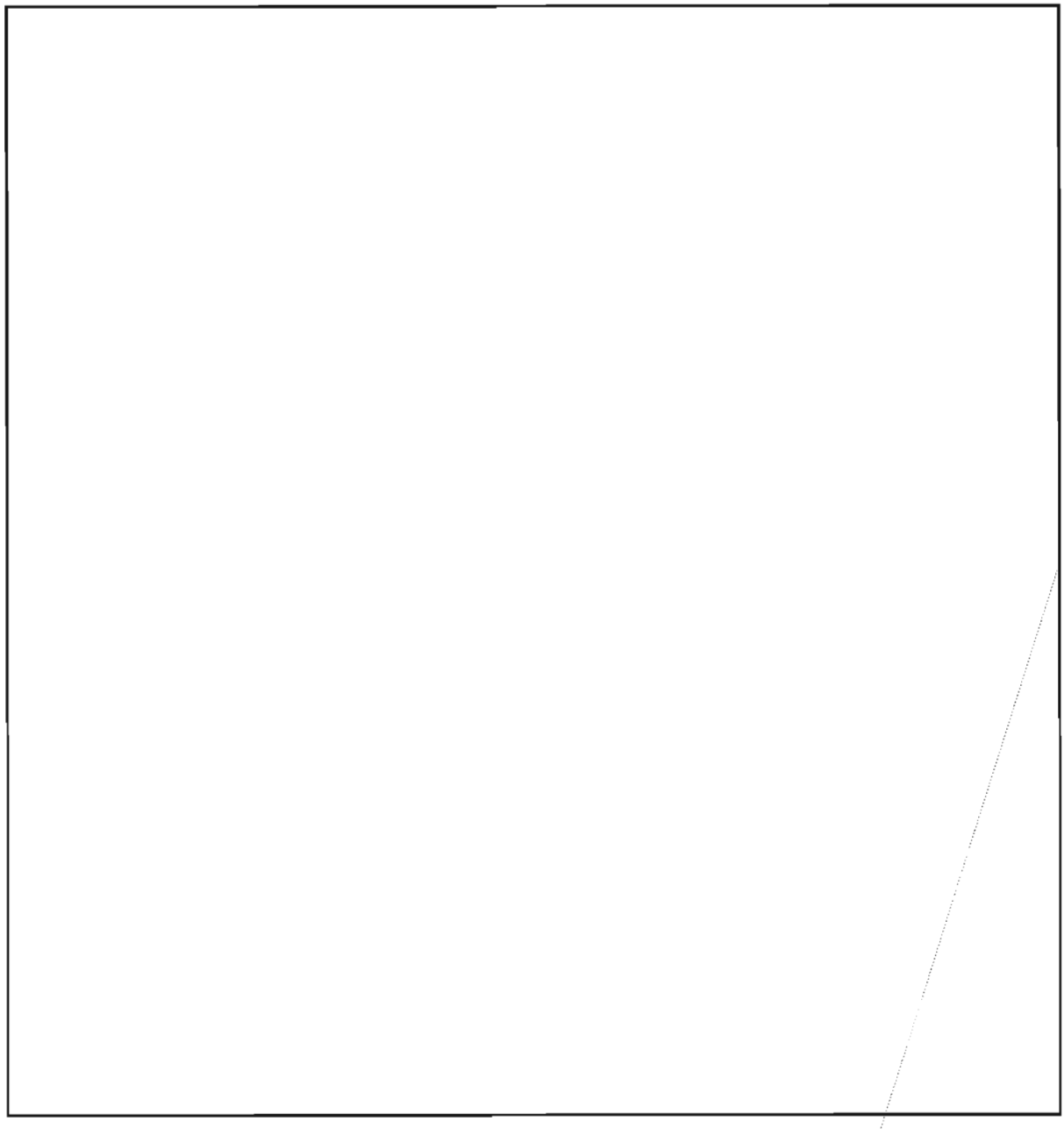
□

EO 1.4.(c)
P.L. 86-36

DOCID: 4010108

CRYSCOM Requirements for Data Encryption-Decryption Exchange

[redacted] P13, CRYSCOM Exec P.L. 86-36

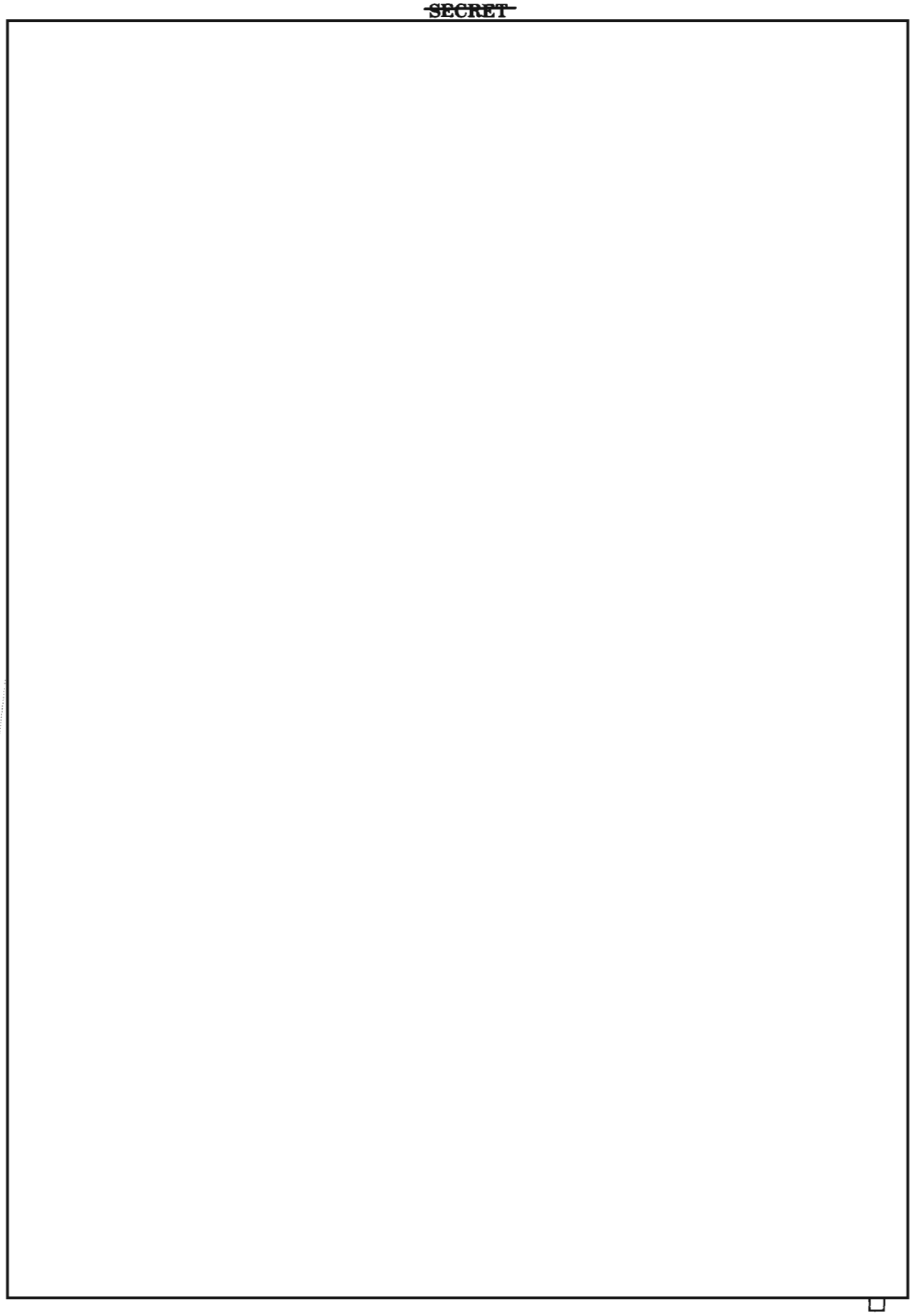


~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

P.L. 86-36
EO 1.4.(c)
P.L. 86-36

DOCID: 4010108



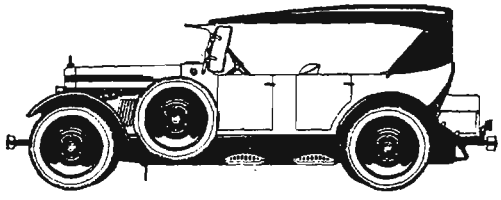
P.L. 86-36
EO 1.4.(c)

DOCID: 4010108

On the Lighter Side

~~SECRET SPOKE~~

RANK HATH ITS PRIVILEGES



EO 1.4.(c)
P.L. 86-36

Contributed by

~~SECRET SPOKE~~

Computer and Information Sciences Institute

Special Interest Group on

If you use data from multiple sources (or support those who do) to track, identify, or evaluate targets, you are doing and may benefit from exchanging ideas and software.

MONTHLY MEETINGS

Wednesday 25 September 1991 0930 9A135 P.L. 86-36

Subject: Geographic Information Systems

Speaker: T51

Thursday 31 October 1991 0930 9A135

Subject: New Multi-media technologies for information dissemination

Speaker: P05

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

(U) In 1987 W2 set out to expand access to information in order to increase productivity and to improve the quality of its products. We were hoping, at the same time, to make the production process more enjoyable for the analysts by giving them graphical user interface (GUI) and personal computer networking technology. Both are now an integral part of our systems and applications.

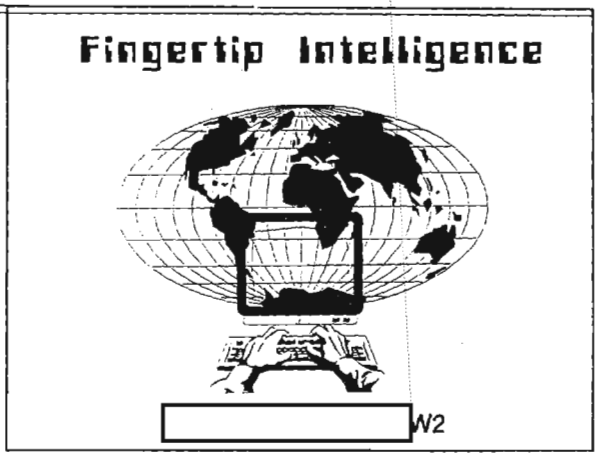
~~(FOUO)~~ We have made progress towards the goal of reaching out with our fingertips for intelligence information via computer keyboards; we call this "fingertip intelligence." This means making computers the indispensable tool that people instinctively reach for when they need information, or want to share it. The process calls for:

- a graphical user interface via windows software that provides a what-you-see-is-what-you-get (known as whiz-e-wig, from the initials) view on the monitor;
- running multiple applications (word processing, spreadsheet, graphic editing, etc.) in multiple windows with some background processing;
- scanning in graphics and images to use in publications or in vuegraphs and slides, or to pass on to others over the network;

[redacted]

- running analytic processes on minis and mainframes remotely;
- using an ever-growing number of applications. The possibilities are astounding!

(U) We are taking advantage of the better and faster hardware and software that the computer industry is developing, and also the more appealing features, so that now, people are using computers not because they have to, but because they want to. For example, we have been successful in retrieving data from the VAX, then running an analytic program and outputting the results using Corel Draw graphics, and then importing it all into PowerPoint presentation software or into an Excel spreadsheet, and inserting the results in a



reported created in the Word for Windows word processor. And we don't have to close anything down to switch applications.

~~(FOUO)~~ That all these applications can talk to one another has proven the value of our set-up. For example, the new data on target performance we have just entered on the spreadsheet is automatically updated in the report sitting in the word processor. Keeping the documentation in sync, that is, not having to enter newer data manually everywhere it appears, save time and assures accuracy. This is what analysts like.

(U) This process is not limited to the confines of W2, but through networking it can reach the other side of the world! We are now working to integrate intelligence information and to automate procedures to manipulate, assemble and distribute it. We are also trying to improve electronic mail.

P.L. 86-36

~~(FOUO)~~ It is new technology that has made this possible—the faster machines with more storage and computational capabilities. Now we are poised to bring all the pieces together on our UNIX-based [redacted] workstations as part of the W2 project [redacted] It will incorporate the features described above, a boon to the analysts. But no one division or office can implement this vision alone; we are working diligently with other people in the Agency and outside, too.

(U) If you'd like to pay us a visit, call [redacted] W24, on 968-8963, or me on 968-4236. We'll schedule a demo for you in our dynamic and ever-changing environment.

□

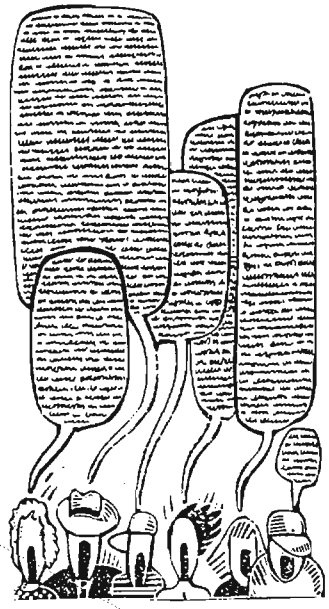
~~FOR OFFICIAL USE ONLY~~

DOCID: 4010108

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

Comment on GISTER



[redacted] W044

~~(FOUO)~~ The article on the GISTER program (CRYPTOLOG, 1st issue 1991 pp 1-7, by [redacted] G52), was intriguing.

[redacted]

(U) The spreadsheets that can perform these tasks are: Lotus 1-2-3 Release 2.2 for IBM machines; Lotus 1-2-3 Release 3.1 for IBM and Unix machines; Wingz and Excel for Macintosh machines. There are ways to enter the GISTER text files from the DOS machines to the Macintosh machines to use these spreadsheets. I would be glad to give a demonstration of the technique to anyone interested.

(U) I am happy that [redacted] a linguist, has written such a useful and impressive program on his own, which could have cost the Agency a tidy sum were it contracted out.

(U) It is also nice to have a publication like CRYPTOLOG handy that allows feedback on the articles written. I would never have known about Jim's work, because I am not involved in language problems, and my technique mentioned above, if useful to anyone, would not have been published.

[redacted]

Update on GISTER

[redacted]

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4010108

Using C++ for Compute-Intensive Code:

Linear Discriminant Analysis

[redacted] 503
P.L. 86-36

C++ offers advantages besides allowing a programmer the use of the magic phase "object oriented". It encourages writing code that is easier to read and easier to maintain. This article describes a short experiment to measure the run-time penalty paid when using C++ specifically to write readable code.

C++ allows the programmer to define data types and operations on those data types. This can be used to allow the programmer's code to more directly represent the algorithm. I have been looking at some linear discriminant analysis software and decided to use it as a test. The first step of this software creates a covariance matrix from known data. The experiment described here compares the run times of this first step using Microsoft C version 5.1 as the standard C. This result was compared to a C++ version compiled using Turbo C++ version 1.0 and Zortech C++ version 2.1.

An early experiment was done using Rogue Wave's matrix classes for C++. This software was discarded because the increase in run time was incredible and also because the package would not allow the operation matrix = vectorT * vector. The Rogue Wave package is written in the same style as the NIH classes. This style has classes inherit properties of more basic classes which inherit properties of still more basic classes... This approach has advantages, but it causes the software to run slower because of a lot of nested subroutine calls. (Turbo C++ and Zortech C++ both refuse to inline code with loops, and most of the matrix code has loops.)

I wrote a simple matrix class which is used in the results below. The test code reads 500 data vectors from a file, each 90 elements long. These vectors are used one at a time to build the covariance matrix. Most of the time in the entire test program is consumed by the operation:

$$\textbf{covariance\_matrix} = \textbf{covariance matrix} + \textbf{data\_vector}^{T} * \textbf{data\_vector}$$

Two C++ versions were created. One uses code that directly follows this expression, the other uses a subroutine. Except for this one line of code, the two C++ version are the same. The straight C version uses a subroutine. The run times were as follows: (times are in minutes:seconds)

Type of code used	Microsoft C	Turbo C++	Zortech C++
code follows expression	N/A	1:22	1:06
code uses subroutine	0:18	0:18	0:18

~~FOR OFFICIAL USE ONLY~~

The times are good only to the nearest second or two. The table shows that to achieve the run time of the straight C version, the time-intensive calculation needs to be in a separate subroutine. The results are the kind that make everybody happy. If you don't want to change to C++, they show that C++ has terrible run times. If you want to use C++, they show that C++ doesn't have to be slower than straight C.

Here is the critical line of code used in each of the three versions:

Straight C: ddiadic(quapar,vector,vector,len,len,len);
C++ (fast): quapar.covar_calc(rowvector);
C++ (slow): quapar += (rowvector.transpose()).product(rowvector);

Unfortunately the easiest to read code is also the slowest.

C++ "attaches" the data to the code that processes it. For example, it is very easy to give each matrix a name so that the code can report not only a error, but the matrices involved. This means that if you tried to add two matrices of different sizes together, the code would not just report "Error: matrices are different sizes", but could also tell you which matrices are involved. This makes for very friendly code. The straight C code used for the test follows the traditional math programming style and doesn't check for any errors.

WHY THE C++ CODE IS SLOWER

I believe that the creation and destruction of scratch variables is the major reason that the C++ code runs slower. Look again at the critical calculation:

covariance_matrix = covariance_matrix + data_vectorT * data_vector

The C++ expression causes the following steps to be done:

1. Create a data vector and put data_vector^T into it.
2. Create a matrix and put data_vector^T * data_vector into it
3. Destroy data vector containing data_vector^T
4. Add matrix from step #3 to covariance_matrix
5. Destroy matrix containing data_vector^T * data_vector

Each time the line is executed, two intermediate values are created, used, and destroyed. By replacing the line with a call to a subroutine, the need for the intermediate values is eliminated. It would be interesting to see how much time could be saved by using some sort of cache for intermediate data elements. That is, instead of destroying a intermediate data element, put it aside in case you will need it the next time through the loop.

CONCLUSION: USE C++

The two major steps of real time programming are; first make the code run right and only then make it run fast. C++ has significant advantages for writing code that runs right and as this experiment shows, C++ can run fast.

DOCID: 4010108

WHY IS ZORTECH C++ FASTER THAN THE TURBO C++?

The test code had a verbose option that would print out each time a data element was created or destroyed. For example, the critical calculation caused the following lines to be printed when the Zortech C++ version was run:

```
column_vector (rowvector transpose )(90,1) created
matrix ((rowvector transpose ) matmul rowvector)(90,90) created
matrix ((rowvector transpose ) matmul rowvector): deleting data, destroyed
column_vector (rowvector transpose ): deleting data, destroyed
```

The format of the line is type of matrix, the matrix's name in parenthesis, the size if created, and a comment saying created or deleted. An intermediate data element takes the name of the original element with the name of the operation added. For example, the line:

```
column_vector (rowvector transpose )(90,1) created
```

says that a column vector with name "rowvector transpose" with size 90,1 was created.

Here is the corresponding output when the Turbo C++ version is run:

```
column_vector (rowvector transpose )(90,1) created
column_vector (Copy of (rowvector transpose ))(90,1) created
column_vector (rowvector transpose ): deleting data, destroyed
matrix ((Copy of (rowvector transpose )) matmul rowvector)(90,90) created
matrix (Copy of ((Copy of (rowvector transpose )) matmul rowvector))(90,90) created
matrix ((Copy of (rowvector transpose )) matmul rowvector): deleting data, destroyed
matrix (Copy of ((Copy of (rowvector transpose )) matmul rowvector)): deleting data,
      destroyed
column_vector (Copy of (rowvector transpose )): deleting data, destroyed
row_vector (Copy of (Row 20 of means)): deleting data, destroyed
```

Notice all the "Copy of . . . " lines generated. Turbo C++ is creating copies of matrices that the Zortech code didn't need. Why are all these extra copies made?

The difference between the two is caused by how the compiler handles return values. For example, look at this subroutine:

```
Matrix dummy(void)
      {
      Matrix X();    // X is an automatic variable
      X = ...        // Put a value in X
      return(X);     // Return X
      }
```

The above subroutine returns a variable ("X") that is automatic and goes out of scope when the subroutine returns. Turbo C++ creates a copy of X and destroys the original when the subroutine returns. Zortech C++ postpones the destruction of X until the subroutine's return value is no longer needed. At least one of the reasons that Turbo C++ runs slower is because of all the extra copies it makes.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010108

Book Review

Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943, David Kahn, Houghton Mifflin Company, Boston, 1991.

Reviewed by: Vera Filby, D9

Many NSA people have read or know of David Kahn's first book, *The Codebreakers*, a massive and erudite world history of cryptology. With this background of knowledge, an Oxford doctorate in history, and the acquaintance of many who remember the events recounted, Dr. Kahn was well equipped to tell the story of the German naval Enigma cipher machine and the struggle to turn it into a weapon against the U-boats.

Readers who have followed the cryptologic history of the Battle of the Atlantic will find much in this book that is familiar, but they will enjoy it all the more for that reason and will appreciate it for its new information, its entertaining style, and its novel approach. The theme is the recovery of Enigma materials from U-boats through circumstance of war and from ships by chance or by planned seizure.

Information encrypted in naval Enigma was desperately needed in Britain's deadly battle against the U-boats, and the struggle to break the system was long and hard. Veterans of that effort were among the more than 70 people interviewed and 20 reached through correspondence - German, Polish, French, British, and American. They included cryptanalysts, U-boat and ship captains and crew members, intelligence officers, radiomen, and others.

Among them were Gustave Bertrand, wartime head of French espionage, Norman Denning, head of German intelligence in the Operations Intelligence Centre, and Harry Hinsley, who as a Cambridge history student joined the G.C.&C.S. (now GCHQ) at Bletchley Park, taught himself traffic analysis and soon demonstrated its operational intelligence value. He became a naval intelligence analyst, and many years later was chief author of the UK Government's official *British Intelligence in the Second World War*. Dr. Kahn is reputed to be a skillful and persistent interviewer, with a knack of asking questions to which he already knows the answer or part of it, perhaps in the hope of confirming it or eliciting more information.

Other sources, besides many of the books and articles published on the subjects covered, included ships' logs, reports, memoranda, and personal papers in German, British, and American libraries and archives.

Dr.Kahn's accounts of the ship captures are full of color, excitement, and suspense. He is a great teller of sea stories. The parallel story of the Enigma machine and its ramifications he treats with thoroughness and clarity, beginning with the day, 15 April 1918, when the inventor, Arthur Scherbius, offered his cipher machine to the Imperial German Navy, up to the end, when the Enigma decrypts were no longer needed. He recounts vividly the Polish, French, British and American experience, with special attention to the Polish story. He describes in detail the construction and workings of the machine, the means and methods of atttack, and associated codes and ciphers, with the focus always on the naval Enigma. Luftwaffe Enigma was first broken on 22 May 1940 and thereafter air traffic was read regularly. But the naval remained resistant. Naval Enigma was more complex and naval communications more disciplined, and only limited and temporary successes were achieved until December 1942.

~~FOR OFFICIAL USE ONLY~~

With the Enigma buttoned up, the analysts at Bletchley worked on and broke lower level systems. One of these was the Dockyard Cipher, which was used for messages to and from shore stations and patrol boats, minesweepers, auxiliaries, and other vessels. In time the analysts discovered that messages sent in Dockyard were sometimes sent also in Enigma to ships equipped with Enigma, thus producing cribs, which they called "kisses."

GIFTS FROM THE SEA

A bit of help for the analysts in Bletchley's Hut 8, the naval cryptanalysis section, came from an unexpected source early in 1940 when the minesweeper *H.M.S. Gleaner* encountered and attacked the German U-boat U-33 at the entrance to the Firth of Clyde 12 February. The skipper of the damaged submarine decided to surface and make a run for it. Enigma parts were distributed among crew members to be dropped into the sea if they had to abandon the submarine. The *Gleaner* spotted the U-33 and continued the attack. In the danger and confusion, one seaman forgot to sink his piece–a wired rotor.

On 26 April a British destroyer returning from Norway stopped and boarded a trawler identified as Dutch and named *Polares*. A crew member threw two canvas bags overboard, but the boarding party was able to capture one of them. When the contents arrived at Bletchley they were found to contain Enigma keys for four days in April.

Nearly a year passed before the struggling cryptanalysts received another gift from the sea in the form of key tables for February. In March 1941 a destroyer accompanying troop ships carrying commandos for a raid on German-occupied Norway encountered an armed whaling trawler, the *Krebs*, in the Lofoten Islands. Documents retrieved from the ship after it was fired on and destroyed included gridded charts, the February Enigma keys, rotor settings, and the plugboard setting. With their help, the Hut 8 analysts decrypted messages which included weather reports and information on the movements of weather ships to and from fixed areas where they were stationed for periods of several months. The analysts were soon getting kisses from weather messages.

WEATHER

Germany could not do without weather information from northern waters. It was essential for current data and forecasts for all purposes but especially to support air operations against England. Only ships at sea could provide a steady flow of observations, so fishing vessels were used to serve as weather stations. Even U-boats were pressed into service. To deny the data to the British, reports had to be encrypted, and the system used to do it was the Enigma.

Weatherbirds will appreciate the significance of this. Not many NSAers know about the Weatherbirds–an informal club of SIGINT weather analysts. Weather is usually a low priority target for SIGINT–until there is a crisis; then everybody wants the weather support. SIGINT weather can provide identifications and locations, contribute to traffic analysis, give tipoffs to related activity, reveal information about the entities it serves, reflect such events as airfield openings and closings, and indicate future events. In *Seizing the Enigma* Weatherbirds will learn how the Enigma encipherment of weather led to its own undoing.

Losses of ships carrying war materiel, food, and other necessities of survival were increasing, and help from Bletchley was urgently needed. Harry Hinsley, studying the weather messages along with his other traffic, had a stunning idea. Why not go after a weather ship? His suggestion went through channels, and the *Muenchen*, which was about to sail to a grid square northeast of Iceland, was selected. A task of force of destroyers located the ship on 7 May and shelled it. Before abandoning ship, the radioman, who had been transmitting a weather report, gathered up the Enigma machine, the current keys, and other materials, put them into a lead-weighted bag, and threw them overboard. But the boarding party did succeed in collecting some documents. Among them Bletchley identified the Short Weather Cipher, Enigma settings, and the June keys. The Short Weather system reduced synoptic weather ele-

~~FOR OFFICIAL USE ONLY~~

ments to single letters which were then enciphered in Enigma and could be transmitted in 15-20 seconds.

Recoveries from the U-110, captured only two days after the seizure of the *Muenchen*, and from the targeted fishing vessel *Lauenburg* on 28 June brought gold to Bletchley–keys, an indicator book and enciphering instructions, the U-Boat Short Signals Book, machine instructions, settings, and the July home waters keys.

In contemplating the damage the encipherment of weather brought on the Germans, one cannot help wondering why they risked their most powerful system for it. Why not some other cipher? The objective was to secure the weather information, but more important was concealing the fact that the information was weather, specifically weather from ships at sea. But why put Enigma in double jeopardy, by using it for that purpose and sending it out on small vessels vulnerable to capture?

There is another mystery. Short-form Enigma weather reports from U-boats were decrypted and sent to the weather central in Germany. Selected reports were reenciphered in a weather system and broadcast to ships at sea and shore stations. How could the COMSEC authorities have allowed this to happen? The only answer is that the Germans had absolute faith in the impenetrability of Enigma. They did conduct investigations when compromises were suspected, but the findings always concluded that the source could not have been Enigma.

THE BATTLE OF THE ATLANTIC

As Dr. Kahn notes, the Battle of the Atlantic was the only battle that lasted from the first day of the war to the last. Thoughout much of that time, the numbers of ships lost to U-boats reflected the status of solution of enciphered commuications on both sides. The picture could be modified by other influences–improved DF techniques, for example–but the effect was always there, sometimes dramatically. Sinkings in the last half of 1941 amounted to 600,000 tons. In the same period of 1942, losses reached 2,600,000. The Germans broke Naval Cypher No. 3 and read much of the naval traffic throughout 1942. Naval Cypher No. 5 replaced Nos. 3 and 4 in June 1943, and from that point on, British naval was denied to them. Meanwhile, the British lost the Enigma when the M4 model was introduced on 1 Februry 1942.

Salvation came from the destruction of the U-559 by the destroyer *Petard* in the eastern Mediterranean in October. Men from the *Petard* boarded the sinking boat, with bodies floating all around them. They succeeded in getting many documents out, but an officer and a seaman went down with the U-boat. The documents they had given their lives for were current editions of the Short Signal Book and the Short Weather Cipher.

The sequence of events that followed their arrival at Bletchley led to a break into the Atlantic U-boat key SHARK in December. By January and February 1943 sinkings were reduced to half of the losses in the previous two months. In June 1944 an American task force captured the U-505 and retrieved from it the grid position Adressbuch. This filled the last gap, and thereafter the Allies read naval Enigma currently.

To complete the picture, Dr. Kahn devotes a chapter to the American role in the naval Enigma. Once coordination was achieved, the naval analysts at Nebraska Avenue worked closely with those in Hut 8, exchanging cribs and recoveries.

In a final summation, Dr. Kahn writes that ULTRA's greatest gift was that "it saved lives. Not only British and American lives, but German lives as well. That is the debt the world owes to Bletchley codebreakers; that is the crowning human value of their triumphs."

BULLETIN BOARD

Will the person who borrowed *Editing Your Newsletter* in looseleaf format kindly return it to the CRYPTOLOG office, Ops-1, 2N018. No questions asked.

~~FOR OFFICIAL USE ONLY~~

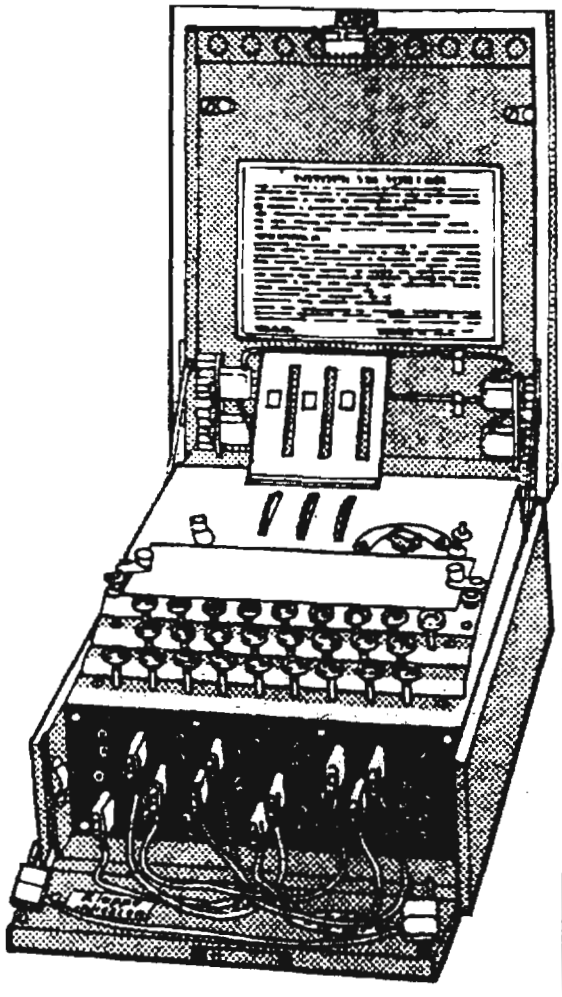
DOCID: 4010108

On the Enigma

P.L. 86-36

ENIGMA, an off-line cipher machine, was the first wired wheel machine to be used to any significant extent. It appeared in Germany about 1925 as a commercial offering, at which time it had three wheels and a reflector (Umkehrwalze). In 1926 the German Army introduced a version which had different wirings, a different reflector, and a new feature, the plug board (Stecker-verbindung, or "stecker" between the wheels and the input-out functions. The Poles attacked the German Army usage and made limited progress by discovering that some from of ENIGMA was being used and that the first six letters of each message were probably indicators. In October 1931, the French intelligence services developed a source within the Cipher Bureau of the German Ministry of Defense who supplied them with copies of code clerks' instructions for ENIGMA and, subsequently at regular intervals, with copies of daily key lists (but no wirings).

The French Cipher Service looked at these and immediately declared the machine impossible to solve. French intelligence then obtained permission to give the information to France's allies and to suggest a common attack on the problem. GC & CS (Government Code and Cypher School, the predecessor of GCHQ) was given first chance, but they "Filed their copies of the documents" and did not respond to the offer of cooperation. (Gordon Welchman, however, believes the British had more effort against ENIGMA before the war than they indicated to the French.) The French then approached the Poles, who accepted with enthusiasm and promised to share results of their work. However, all cryptanalytic efforts failed. At that point, 1 September 1932, those in charge of Polish intelligence brought in three mathematicians, Marian Rejewski, Henryk Zygalski, and Jerzy Rozycki. In the middle of October, 1932, Rejewski was put to work on ENIGMA and, using information in the documents from the French which showed how the Grundstellung indicator system worked, he was able to in about a month to develop a theoretical method for recovering wheel wirings based on the fact that message settings (of the three wheels) were enciphered twice to produce the six-letter indicator sent at the beginning a a message (this was the Grundstellung indicator system).



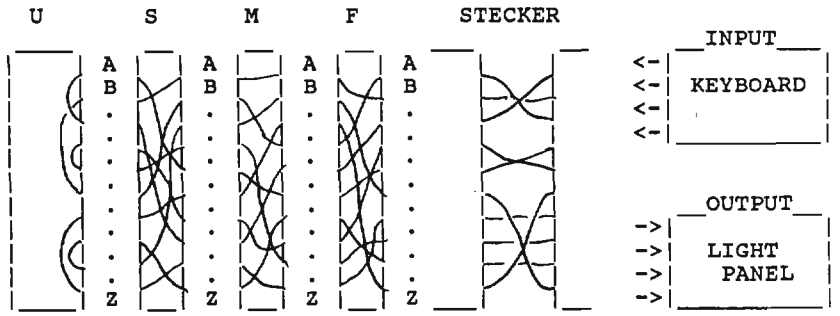
Above: the Enigma machine, a mechanical device for coding invented by the German Arthur Scherbius. Its keyboard is similar to a typewriter, but the letters strike rotary disks that choose substitute letters at random to create encoded messages.

Unfortunately, the amount of work needed to carry out the calculations was prohibitive (and might be prohibitive even with modern computers). Then Rejewski was given two more documents that had been procured by France, these

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010108

The ENIGMA as it was at that time looked like this:



containing two monthly schedules of daily settings (Wheel orders, Grundstellung wheel settings used for enciphering message setting, and plug board connections). At this time, wheel orders were being changed only every three months, but by luck the two months provided by the German source fell in two different quarters. All this information permitted the theory to be simplified sufficiently for Rejewski to recover wirings of the three wheels and reflector by the end of December 1932.

There were three 26-point wired wheels which could be inserted into the machine in any order (but not backwards). There was a reflector (Umkehrwalze) which had input-output contacts on only one side that were connected to each other in pairs. Each wheel had one notch on it which controlled the stepping of the wheels. The fast wheel, F, advanced one position for each encipherment of a letter; the medium wheel M, did not advance for an encipherment unless either F advanced off of its notch or unless M itself was at its own notch, in either of which events M advanced on position. The slow wheel S, did not advance for encipherment unless M advanced off of its notch, in which case S advanced on position. The reflector, U did not step during the encipherment of a message (and in fact was not settable). The stecker between the "maze" and the input-output mechanisms could be changed by the operator but remained constant during the encipherment of a message; it consisted at this time of 14 points connected straight through and 12 points exchanged in pairs.

In addition to all these variable, the alphabet ring on each wheel (by which the wheel could be set in a specified position at the beginning of a message) was rotatable relative to the core of the wheel and could be put at any one of 26 offsets. Thus, setting the wheels so that the same letters appeared at the bench marks would produced different settings of the wirings themselves if the alphabet ring offsets (Ringstellung) were different. Once all these variable elements were appropriately set up, the code clerk typed each plain text letter in turn and, for each one, wrote down as cipher text the letter which lit up. Depressing the key also caused the wheels to advance appropriately.

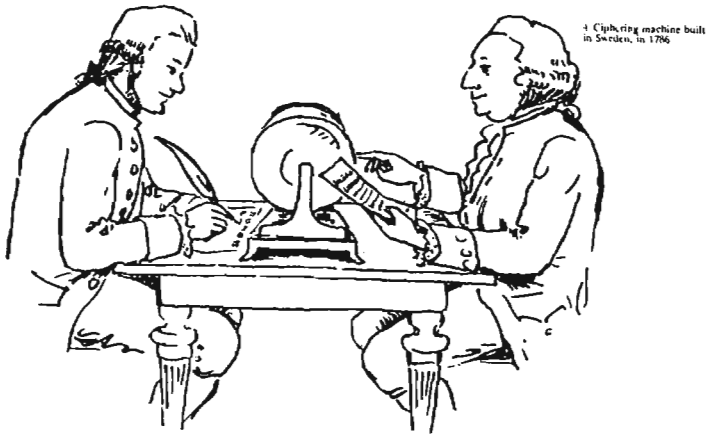
In July 1939, the British and French were informed of the Poles' success on ENIGMA and GC & CS accelerated its own partly successful work against it. ENIGMA was used by the German Army, Air Force, and Navy, among other government elements. Although rather heavy, it was small enough for one person to carry and it operated from batteries, so it was suitable for field use. The Germans continually improved their usage of ENIGMA by changing wheel and reflector wirings a number of times; by increasing the number of available wheels from which daily wheel orders could be selected (they went from three to five to eight in the course of time); bu changing the indicator system several times; by increasing the number of steckered letters from 12 to 20; by devising the number of steckered letters from 12 to 20; and by devising nonreciprocal steckers.

□

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010108

David W. Gaddy, D9



Breaking into Our Past: Enigmas of Another Kind

Cryptology embraces two ancient practices—concealing the meaning of one's communications from unintended eyes, and deducing the hidden meaning of the communications of others. One we term cryptography; the other, cryptanalysis: "code making" and "code breaking." Cryptanalysis, we say, yields communications intelligence, COMINT. But COMINT is both a product and a process.

Historically, cryptanalysis was a matter of circumstance, of the chance capture or interception of a cryptogram. No thought was given to organizing systematic efforts to capture cryptograms—the communication technology would not prompt thought along those lines or support an effort. (How many "daily hours of cover" would one devote to capturing enemy couriers?) But the technology changed in the 1860s in America—not with Morse's telegraph, which required a physical tap—but with a system of visual signals invented by an army surgeon, Albert James Myer. The Myer system (a binary code, by the way) made battlefield telecommunication practical. It also introduced a communication technology susceptible to interception. The rudiments of cryptology are evident in the American Civil War.

A little more than a decade after that war, the telephone came on the scene, and it was enthusiastically adopted by our army signal corps. But, from the standpoint of cryptology, this was little different from Morse's electromagnetic telegraph—interception required physical contact with the wire involved. The invention of wireless communication near the turn of the century changed everything. Technology would now support an organized, systematic COMINT effort, even as it was demanding a new look at security.

Modern cryptology is built on the foundation of the First World War, when military use of wireless first became widespread. The advanced nations maintained some interest in the subject during the 1920s and '30s, albeit in varying degrees. For the United States, this was the era of Herbert Yardley and his *American Black Chamber* and William F. Friedman, who created a scientific basis for cryptology.

But it is to World War II that we look when we think about the origins of modern cryptology, and for good reason: cryptology continued from "hot war" into "cold war" without dropping a beat. In fact, it thrived. Now a half century separates us from the exploitation of the German Enigma and the Japanese Type 97 machine Americans called PURPLE. That generation has largely passed from the scene. Sons and even grandsons (yes,

~~FOR OFFICIAL USE ONLY~~

and daughters and granddaughters) have displaced them.

The passing of the generation that established modern cryptology has removed from our ranks the pioneers in what we now consider our profession. We have lost some of the lore, some of the technical knowledge, and some of the enthusiasm that they possessed, when ciphers were broken by individuals, and when each accomplishment broke new ground. The process has become less individualistic and more mechanical. Mathematicians and scientists have replaced students of the humanities. Sometimes it is difficult for newcomers to understand their role in the greater scheme that engulfs them.

In the fall of 1989, we moved to remedy this by putting greater emphasis on recalling to memory the past accomplishments and the pioneers who laid down the trail we follow. The Center for Cryptologic History is an effort to rejuvenate our history program and to make it relevant to the needs of a new generation of young professionals and modern decision-makers. The scope of our inquiry extends from a better understanding of the sweep of American cryptologic history and its European antecedents, all the way to the lessons of DESERT STORM.

While the recent subject may be of more pressing interest, our present purpose is to share a puzzle from the more distant past. It is somewhat like the "missing link" to anthropologists: in our case, it is an unidentified cipher device that may extend our knowledge of our craft.

The Cylinder-Cipher Enigma

In 1890, a disgruntled French cryptographer revealed a device he had been unsuccessful in persuading his own government to adopt. The Bazeries "cylinder-cipher" comprised 20 disks or wheels—rotors, one might say—arranged in a specified order on a shaft or axle. The letters of the alphabet were placed around the rim of the disks, scrambled. The cryptography was that of polyalphabetic substitution, an improvement on the familiar Vigenere in that the alphabets were mixed. To encipher, one aligned the disks to spell the plain text, then selected and transmitted as his cipher text any other line of mixed letters. On the receiving end, one set up the cipher text, then simply turned the cylinder until plain text was revealed.

This concept, and virtually the identical device, was adopted by the United States Army Signal Corps and introduced in 1922 as its M94. That same year a scholar (and former World War I cryptologist) who was working among the papers of Thomas Jefferson in our Library of Congress discovered in Jefferson's own hand two papers describing the manufacture of just such a cipher device, called a "wheel cipher" by Jefferson. Since that time Jefferson has been considered the inventor of this type of cipher device. He is so identified in the most recent book on the subject, Silvio Bedini's *Thomas Jefferson, Statesman of Science*, published in 1990. Bazeries, it was assumed, independently invented the same device; the Signal Corps copied him, unaware of the achievement of its esteemed countryman. Bedini followed the directions and made a copy. But now the plot thickens, as they say in detective stories.

A few years ago there appeared at a sale in the Washington area a device of this very type. It was suspected of being of American Civil War origin, perhaps Confederate. The price was right; we bought it. Upon examination, it was evident that pieces were missing, including several of the disks. Some disks had been removed and replaced in reverse order. Letters were obscure or even obliterated altogether. But nothing about the device suggested Confederate use. On the contrary, accented letters showed that it was intended for the French language. Superficial appearance suggested that it was older than the war of the 1860s, perhaps early 19th Century or even late 18th.

The former owner was from West Virginia, an area that was part of Jefferson's home state during his lifetime. Could this be the source of Jefferson's knowledge of such a cipher machine? His undated description is not necessarily evidence of original thinking. But how did the device come into American hands, and when? It retains 35 of a possible 40 disks, each bearing 42 mixed

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010108

letters, digits or punctuation. Would this larger, more involved version be earlier or later than the Jefferson-Bazeries-Signal Corps concept? We have no answer as yet. The mystery remains. But the mystery deepens with another bizarre parallel.

Some years back another former cryptologist was working among the historical archives of his own nation. He, too, discovered a description of a cylinder-cipher, similar in principle to the one we are studying. The researcher was Sven Wasstrom of Sweden. The documentation he had found was dated 1786, well before the earliest date postulated for Jefferson's description. It described the invention (dare we say?) of a Baron Fridric Gripenstierna, offered to King Gustav III. Working with Boris Hagelin's famed CRYPTO AG, Wasstrom assisted in making up a copy of the 18th Century device.

And there our story ends for the moment. It is an amusing curiosity, a diversion. Or is it more than that? In 1865 the United States Army came into possession of a type of cylinder-cipher used by the army that most threatened the very existence of the United States, the Confederate States Army. It was simply a mechanical means of using the conventional, straight-sequence, 26x26 Vigenere square or tableau. But suppose each column had been separated by sawing through the cylinder. Suppose the alphabets to have been scrambled, instead of in direct sequence.

Now come forward in time: apply electricity to this manual device. The disks become rotors, the heart of mid-Twentieth Century cipher machines, the embodiment of another Enigma. Whether for the old cryppie or the youngest member of the new generation, discoveries of this nature illumine the still obscure background of our technical history. They hint at continuity "behind the scenes," perhaps even at international cooperation—or espionage. At a minimum they give us a fuller appreciation of our heritage. We believe that such knowledge enriches our profession and justifies the modest attention we devote to the subject.

□

Notice to Subscribers

Distribution for this issue reflects changes received by COB 30 August 1991.

To change your mailing address, please write your name, old organization and building, new organization and building, on a piece of paper, put it in a **shotgun—not one-time**—envelope, and mail it to:

DISTRIBUTION, CRYPTOLOG, P1 NORTH

or send it by electronic mail:

PLATFORM: cryptlg @ 1bar1c05

CLOVER: cryptlg @ bloomfield

Please do not phone about your subscription because:

- After every issue there are over 300 changes to the distribution, about 300 in the first two weeks after CRYPTOLOG hits the streets.

- The distribution list is kept on line on a shared computer in another room.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010108

Editorial

Dump Core! Recycle!

Now is the time to come to the aid of the future.

Just about every analyst has a stash of technical papers, working aids and other materials on favorite projects worked long ago that have been saved "just in case" or that "really should be documented," as people tell their friends, "some day when there's time."

There's no better time than the present, with reorganizations in the air and rumors of an early out.

Getting started is the hard part, for it's a formidable prospect to document a project years later, and it's tempting to put it off to a time when you'll feel up to it.

Maybe you should try for Plan B: instead of trying to document the entire project, organize your materials as a resource for future research. All you have to do is put the papers (or mag tapes, or whatever) together neatly. (Those red accordian envelopes are just the thing.) Write a "Scope and Content" paper—it could be hand-written on one sheet of paper. This means indicating:

what's it all about
why it was important, or proved not to be
what years the materials cover
what your role was
any details you can recall. (It's all right to say you don't know!)
other comments
your name, present organization, date.

There! That's not so hard! Now set it aside and take out your persumm. Using it as an outline, dump core! Tell all you know about those projects—opening and closing field stations, setting up the very first whatever . . . What it was like back in the olden days . . . Add those comments to the surviving papers.

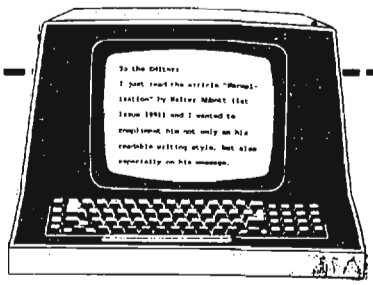
What about those general working aids and monographs that do not belong to any one project: MILCRYPT III, a monograph in the Blue Ribbon Series, a "How to" ITN that's still valid . . . too good to throw away though it's coffee-stained, maybe it should go somewhere . . . but maybe it's filed somewhere? Don't bet on it! Recycle!

Send cryptanalytic materials to:

SAB 2, Door 22, T5411 [redacted] P.L. 86-36

Send all other materials to:

SAB 2, Door 22, T5411, NSA Archives



To the Editor:

I just read the article "Normalization" by [redacted] P.L. 86-36 [1st Issue 1991] and I wanted to compliment him not only on his readable writing style, but also especially on his message.

I have been dealing with several third party organizations for years and have even visited one of them for a short TDY. Most of these relationships have existed since long before I came on board at the Agency, and I've always dealt with them from this side of the ocean, so I guess I have considered them as bureaucratic construction, a "given" that was to be dealt with in the context of today's world. I've never really given a lot of thought to the reasons, beyond the obvious monetary ones, that motivated our third party partners to enter into the relationship in the first place.

In the age of the computerization of everything to the point where all some of us is push buttons all day long, it's refreshing to be reminded that our relationships with our partners is really very personal sometimes.

[redacted] *A3204*

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

CRYPTOLOG

Editorial Policy

CRYPTOLOG is a forum for the informal exchange of information by the analytic workforce. Criteria for publication are: that in the opinion of the reviewers, readers will find the article useful or interesting; that the facts are accurate; that the terminology is correct and appropriate to the discipline. Articles may be classified up to and including TSC.

Technical articles are preferred over non-technical; classified over unclassified; shorter articles over longer.

Comments and letters are solicited. We invite readers to contribute conference reports and reviews of books, articles, software and hardware that pertain to our mission or to any of our disciplines. Humor is welcome, too.

If you are a new author, please request "Guidelines for CRYPTOLOG Authors."

How to Submit your Article

Back in the days when CRYPTOLOG was prepared on the then state-of-the-art, a Selectric typewriter, an article might be dashed off on the back of a used lunch bag. But now we're into automation. We appreciate it when authors are, too.

> *N.B.* If the following instructions are a mystery to you, please call upon your local ADP support for enlightenment. As each organization has its own policies and as there's a myriad of terminals out there, CRYPTOLOG regrets that it cannot advise you.

Send two legible hard copies accompanied by a floppy, disk, or cartridge as described below, or use electronic mail. In your electronic medium (floppy, disk, cartridge, or electronic mail) please heed these strictures to avoid extra data prep that will delay publication:

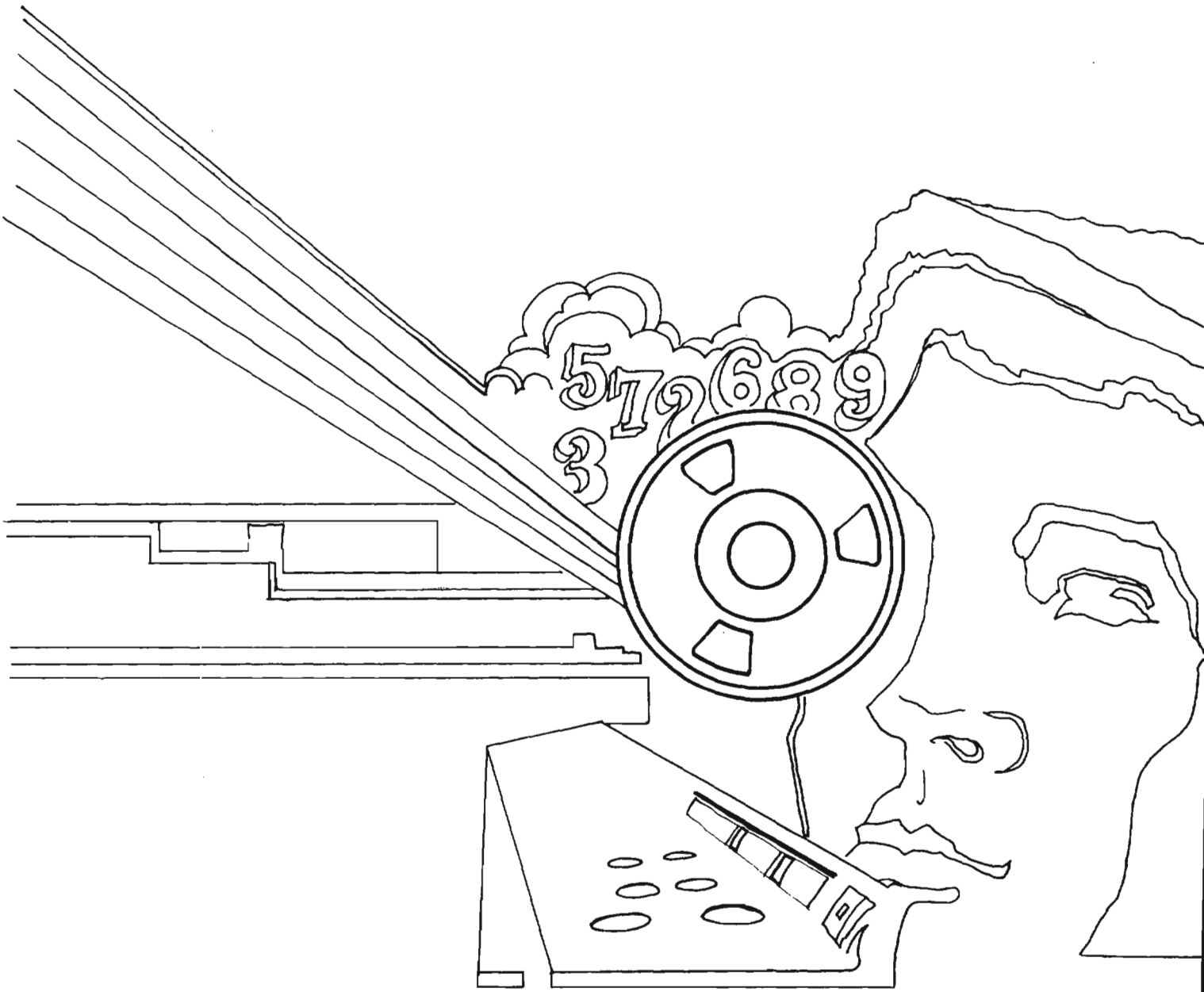
- do not type your article in capital letters
- do not right-justify
- do not double space between lines
- but **do** double space between paragraphs
- do not indent for a new paragraph
- but **do** paragraph classify
- do not format an HD as DD or vice-versa–our equipment can't cope

The electronic mail address is *via* PLATFORM: cryptlg @ barlc05
or *via* CLOVER: cryptlg @ bloomfield

CRYPTOLOG publishes using Macintosh and Xerox Star. It can read output from the equipment shown below. If you have something else, check with the editor, as new conversions are being added. Be sure to label your floppy or cartridge as to the hardware, density, format, and software you used. Don't forget your name, building, organization, and phone!

HARDWARE	MEDIUM	SOFTWARE	FORMAT
SUN	60 or 150 MB cartridge	ascii only	TAR or RAW
XEROX VP 2.0	5 1/4" floppy only	n/a	n/a
MACINTOSH	3 1/2" DD disk only	MS WORD MacWrite TEXT WriteNow	n/a
IBM & Compatibles	3 1/2" 1.2 MB disk 5 1/4" DD or HD floppy	MS WORD WordPerfect WordStar ascii DCA (IBM revisable)	DOS
WANG	n/a	n/a	n/a

~~FOR OFFICIAL USE ONLY~~


5 7 7 6 8 9
3

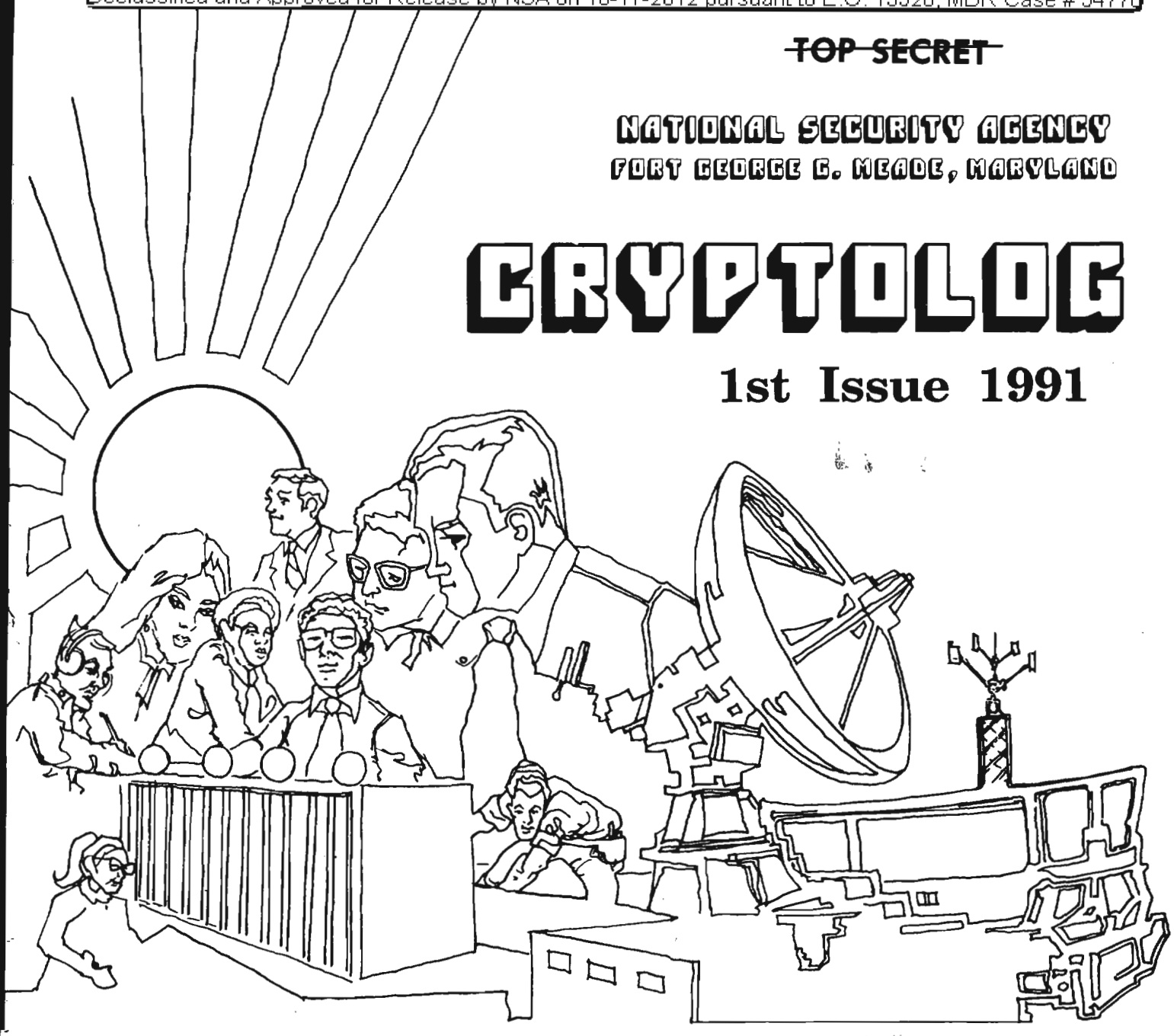
DOCID: 4019720
Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

1st Issue 1991



GISTER 1
50 7
JOINT--THE FUTURE OF INTELLIGENCE? YOU BET! 8
BULLETIN BOARD 12, 32
THE DIGITAL DRAGON 13
ICH SPRECHE DEUTCH 16
A MATTER OF COMPRESSION 17
ALL YOU WANTED TO NOAH ABOUT ARC 21
ERRATA 22
CRYSCO '90 23
LETTERS 24, 29
NORMALIZATION 25
in re PROFORMA 30
CROSSWORD PUZZLE: BUSMAN'S HOLIDAY . . . . . RLW 31
EDITORIAL 32
TO CONTRIBUTE 33

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

DOCID: 4019720

P.L. 86-36

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XVIII, No. 1 . . . . . 1st Issue 1991

PUBLISHER . . . . . [redacted]

BOARD OF EDITORS

EDITOR . . . . . [redacted] (963-1103)

Computer Systems . . . . . [redacted] (963-1103)
Cryptanalysis. . . . . [redacted] (963-5238)
Cryptolinguistics. . . . . [redacted] (963-4382)
Information Resources. . . . . [redacted] (963-3258)
Information Science. . . . . [redacted] (963-3456)
Information Security . . . . . [redacted] (972-2351)
Intelligence Reporting . . . . . [redacted] (963-5068)
Language. . . . . [redacted] (963-3057)
Linguistics . . . . . [redacted] (963-4814)
Mathematics. . . . . [redacted] (963-5566)
Puzzles . . . . . [redacted] (963-1601)
Research and Engineering. . . . . [redacted] (968-7315)
Science and Technology. . . . . [redacted] (963-4958)
Special Research. . . . . Vera R. Filby (968-5043)

Classification Officer. . . . . [redacted] (963-5463)
Bardolph Support. . . . . [redacted] (963-3369)
Clover Support . . . . . [redacted] (963-1103)
Macintosh Support. . . . . [redacted] (968-7315)
Illustrator. . . . . [redacted] (963-3360)

To submit articles and letters, please see inside back cover.

For New Subscription or Change of Address or Name

MAIL name and old and new organizations and building to:

Distribution, CRYPTOLOG, P1, NORTH
or
via PLATFORM: cryptlg @ barlc05
via CLOVER: cryptlg @ bloomfield

Please do not phone about your subscription

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019720

EO 1.4.(c)
P.L. 86-36

GISTER

G52 P.L. 86-36

P.L. 86-36
EO 1.4.(c)

DOCID: 4019720

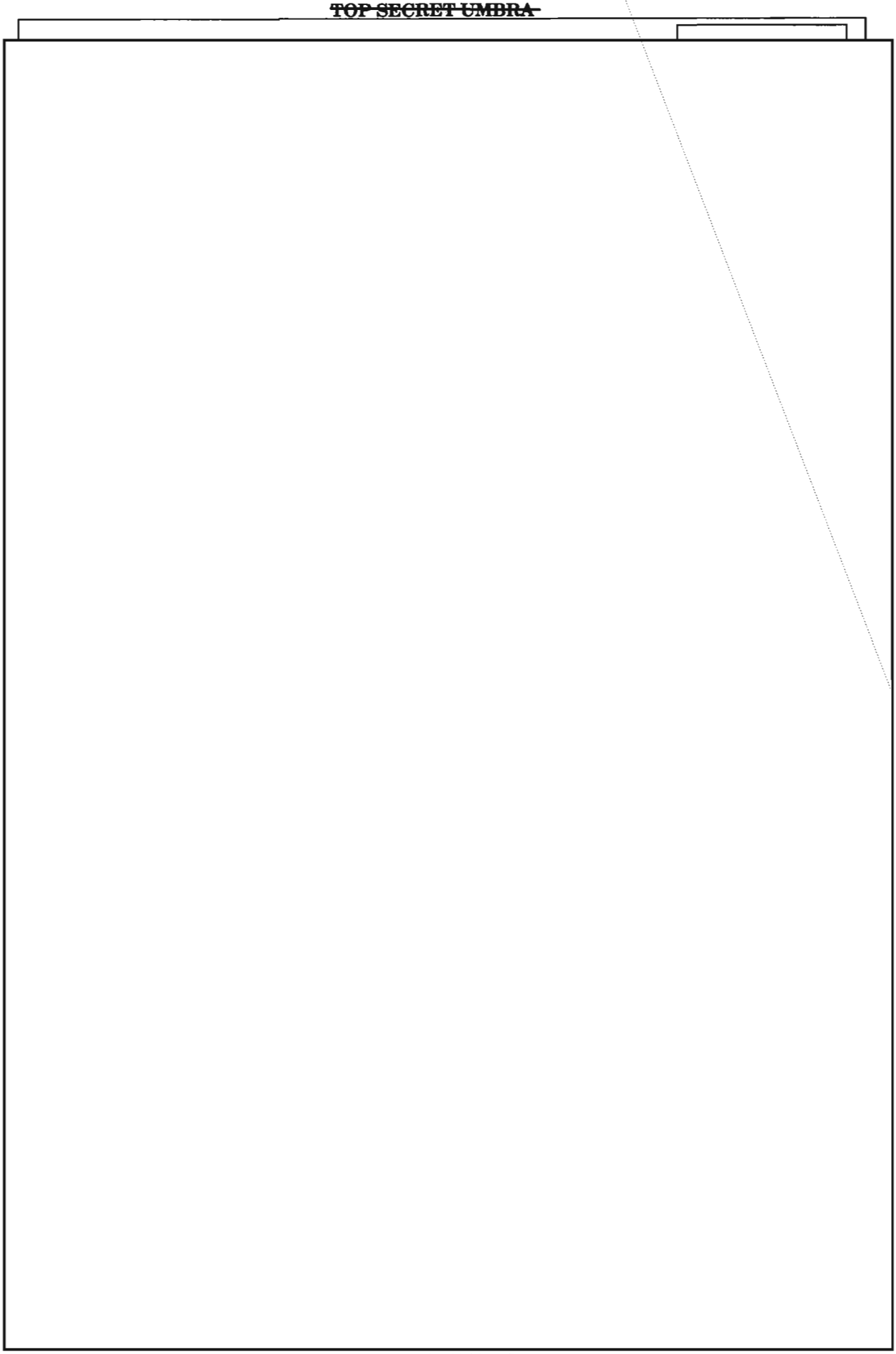
P.L. 86-36
EO 1.4.(c)

DOCID: 4019720

P.L. 86-36
EO 1.4.(c)

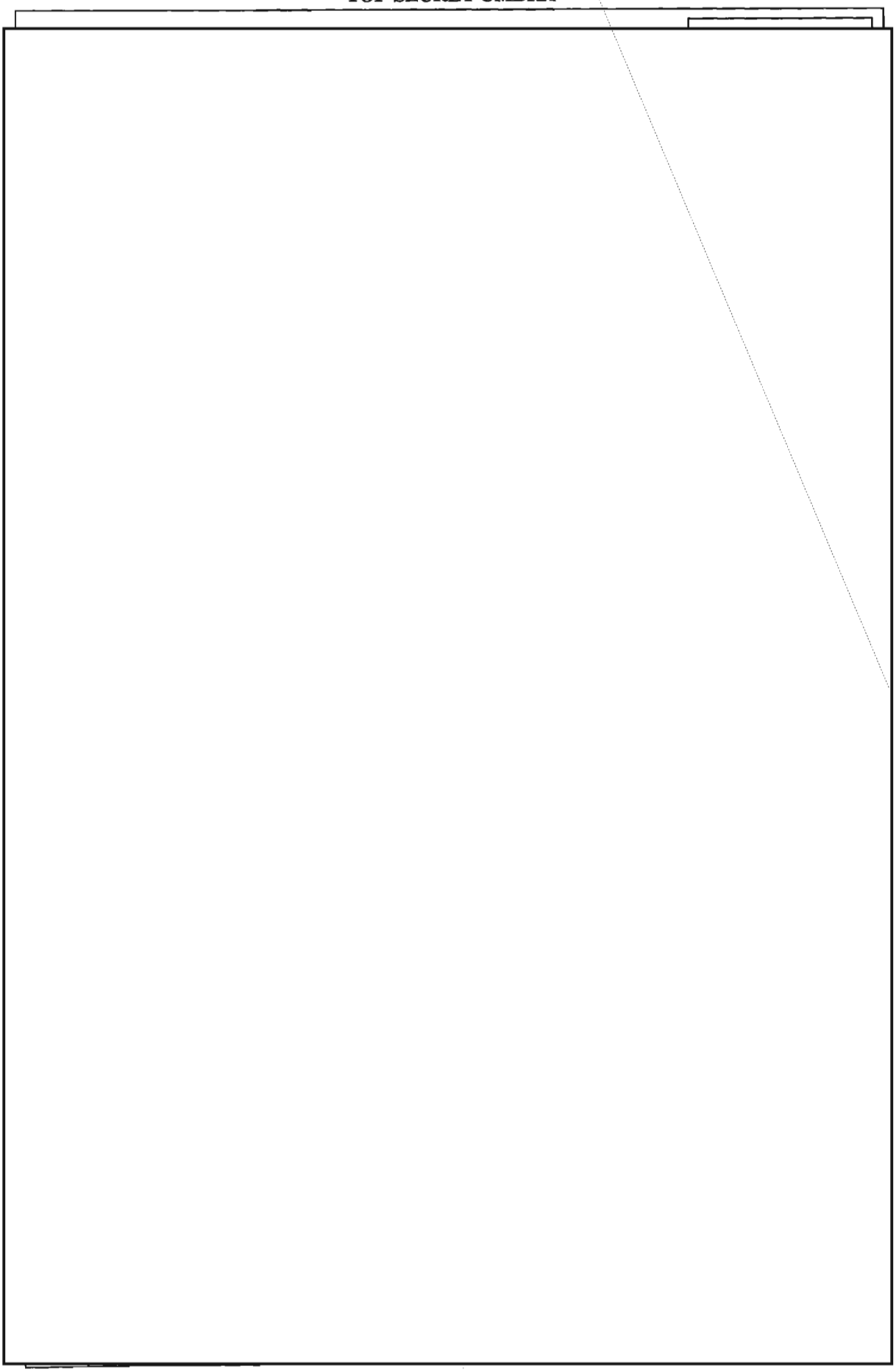
P.L. 86-3(
EO 1.4.(c)

DOCID: 4019720



DOCID: 4019720

P.L. 86-36
EO 1.4.(c)



DOCID: 4019720

P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)

P.L. 86-36

- 50 -

At an informal ceremony held in P1 on 5 February 1991, a small group met to commemorate the passage of 50 years since Bill Lutwiniak started to ply his arcane trade of cryptanalysis in the sanctuary of the organization–now NSA–that was founded on, and is nurtured and sustained by this discipline.

Bill retired in 1981 and has worked as a reemployed annuitant since then. He continues to make significant contributions as a consultant to P1, solving systems himself, and more importantly, assisting our younger generation of cryptanalysts. Bill served for many years as chief of A5, then of P1, and is a distinguished member of both Kryptos and the Crypto-Mathematics Institute.

At the ceremony a crossword puzzle (elsewhere in this issue) was presented to Bill, turning the tables on this well-known cruciverbalist.

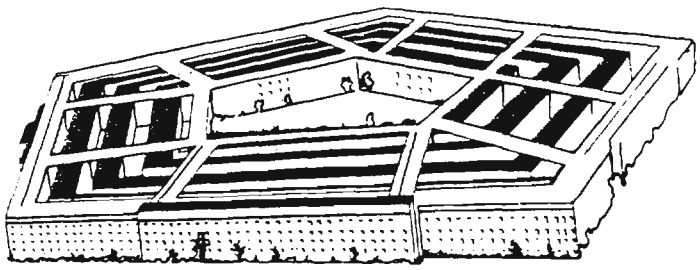
Later this year a series of interviews with Bill, conducted by [redacted] will be released on videotape.

[redacted]

~~FOUO~~

DOCID: 4019720
P.L. 86-36

~~SECRET~~



J O I N T—The Future of Intelligence? Y O U B E T !

(U) Picture this; A room full of analysts representing practically every intelligence element located anywhere in the Washington area and beyond; folks from NSA, DIA, AIA, AFIA, NOIC, NPIC, ITAC, SRD, ESC but none from CIA or KAOS. Uniforms from the Army, Navy, Marines, and Air Force, all side by side with civilians mixed among them. PC word processors on many desks, volumes and volumes of relevent textual materials all brought together by the individual who believed that it was needed "just in case", and more map boards with push pins, acetate overlays, boundary lines, and arrows than anyone could have followed intelligently anyway. Secure phones and STU-III's next to each other. Classified conversations in this hectic environment in the background of calls home. Fax machines that are tempermental, and open phone lines to the various commands in Saudi Arabia. Clocks set for other parts of the world with all their minute hands pointing to different minutes. A few small fans blowing stale air around staler bodies. CNN monitors of various sizes in different parts of the room without logic to their placement. With these 24-hour operations, nothing was turned on and off, except the copier when the new one was worn out and it was replaced with the other new one. Got the picture?

(U) I have just completed my assignment at the Joint Intelligence Center (JIC), Pentagon, in support of the Secretary of Defense and the Chairman, Joint Chiefs of Staff during the DESERT SHIELD and DESERT STORM Operations. I came away from there with a very good understanding of how all the different intelligence agencies contribute to the Joint Operations INTelligence (JOINT) picture. More importantly, I became aware of how this agency is perceived by others and how attitudes affect our validity and how knowledge affects attitude. P.L. 86-36

(U) I was in the first group of people selected for duty at the Joint Intelligence Center in August '90. That first Saturday when we all met was surely a hectic day. And, right from the start, it was evident that NSA had sent its best. By afternoon, the original dozen of us were dubbed Weasels" USN was in charge of the group), an enthusiastic group eager to get to the task.

(U) We all attended many meetings We were even briefed on

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~ 1.4.(c)
P.L. 86-36

the other wars in the area. Thanks to the professional experts at NSA who had prepped us, we arrived at JIC very well informed. Getting the necessary working aids, phone numbers, and office supplies was very reminiscent of a scavenger hunt. A tour of the JIC facilities, still under construction, and the Pentagon badging processes completed our preparations.

(U) The Sunday of Labor Day weekend 1990 was the first day on the job in the JIC. I was first on the ground desk which I thought was appropriate anyway since I was the only Army person on the NSA team. It also allowed me to set many of the desk policies and procedures used throughout the lifespan of the JIC. There were a few growing pains as each member rotated through the desk for the first time. But, being true professionals, we adjusted. The "housekeeping"—arrangement of files, desk areas—was better than I expected, and the equipment held up remarkedly for the abuse we gave it. Transportation to and from the Pentagon was provided for us and was truly a life saver. George and Steve, our drivers on the night shift, were especially friendly, courteous, and safe.

(U) In the first few days of the DESERT SHIELD operations, when the Joint Intelligence Center was a newborn, organized chaos was the best descriptor. People from all these different agencies were just coming together, sizing each other up, establishing boundaries, assuming roles—all the routines that surface when two or more clans come face to face. Shy and quiet would eliminate you from the team discussions. If you wanted to be a part of the team, you had to push into it. Once that was done, however, you were in for life. Duties were created as they were deemed necessary. Division of efforts were naturally established based on the most likely source of the information required. The NSA desk was responsible for all the SIGINT material, the imagery guys for imagery, etc.

[redacted]

[redacted]

Participants in JOINT

AFIA: Air Force Intelligence Agency
AIA: Army Intelligence Agency
DIA: Defense Intelligence Agency
ESC: Electronic Security Command
ITAC: Intelligence and Threat Analysis Center, AIA
NOIC: Naval Operations Intelligence Center
NPIC: National Photo Interpretation Center
NSA: National Security Agency
SRD: Special Research Division, ITAC

(U) Each team in the JIC had its own personality. Of course, I like to think that the team I was on was the best. The only real problems I saw were personnel changes and role definitions. No one on the desk really understood what the NSAer's role was as a part of the team. I envisioned my role as a key player in the

[redacted]

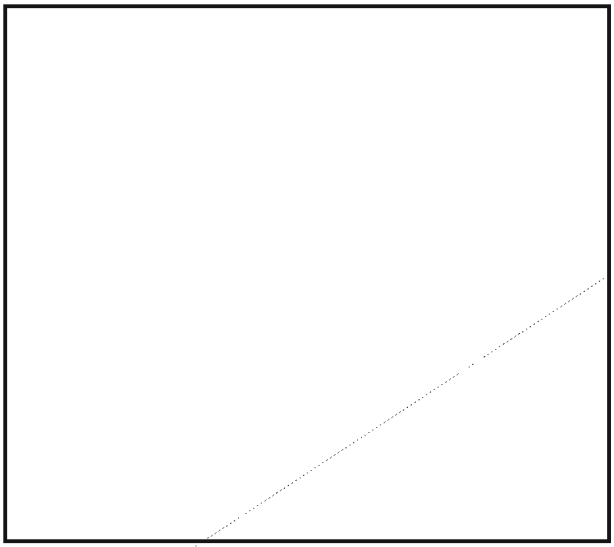
This last duty is what all the other members of the team thought my job was until they were convinced otherwise. [redacted] I had to insert myself into the whole team again. But, after awhile, I was able to steer some discussion and even successfully suggested tasking, based on my SIGINT and JOINT understandings. This tasking provided positive results, too. I never felt at any time that anyone on the team was overly interested in the technical aspects

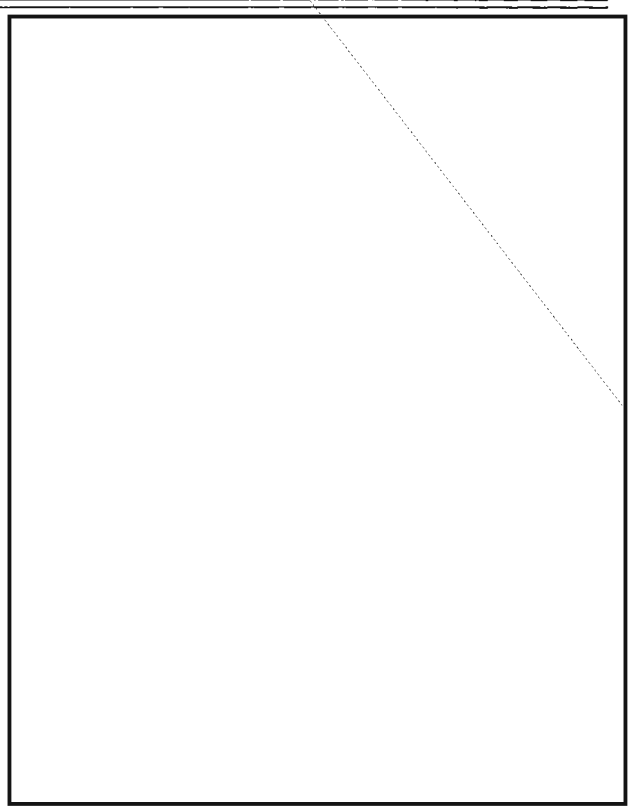
EO 1.4.(c)
P.L. 86-36

the Klieglights coming over the NTSS. But, it was helpful to me to have them. I could speak my native SIGINTese to the NSA ground forces analysis team based on the tech details I had seen in the KLIEGLIGHTS.

~~(C)~~ The mission, as it grew on the Ground Team was to provide all-source intelligence estimates to Rear Admiral McConnell, the intelligence officer answering to GEN Powell and to Secretary Cheney. All source meant all source, too. It also meant that efforts would have to be combined. A joint effort from each of the intelligences was needed. Not only that, based on these efforts, a reasonable assessment of what happened, what is happening, and what will be happening, by whom and when and how and etc, had to be presented each morning to the Admiral. Also we provided support to military operations directly in theater at Riyadh, Saudi Arabia.

(U) Wisely, two only routine reporting vehicles were established, rather than the many one might expect. One was the Military Situation Summary. This was designed to keep the field elements apprised of the current order of battle and the JIC's assessment of events relative to the order of battle. The other regular publication, the Defense Special Assessment, published significant tactical and strategic intelligence. This vehicle had a much more limited audience and was sometimes focused for the Washington area alone.





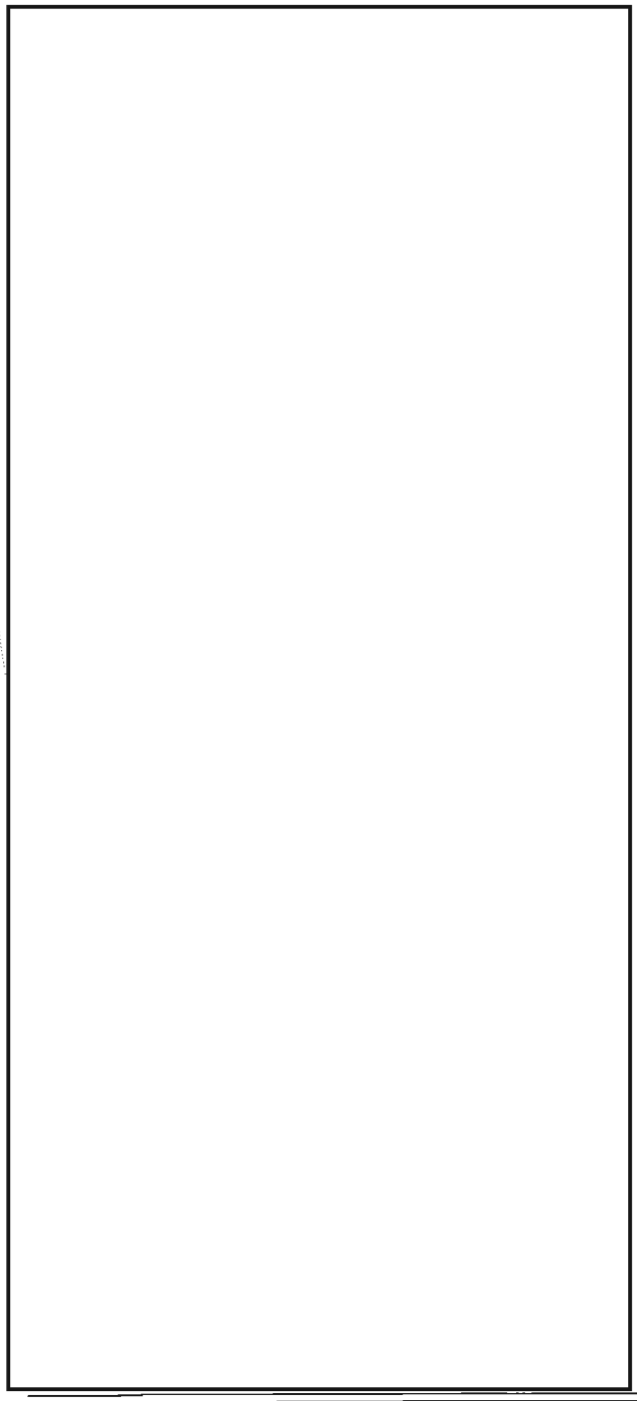
(U) In a matter of minutes, usually, all the national-level intelligence in the community could be brought to bear in a cohesive, complete, and conclusive picture for the warfighters and decision makers "upstairs". There was little interaction with parent agencies. No one at NSA had to say "Wait till the day shop comes in and we'll get you an answer." The same held true for every other agency. The around-the-clock operations and the on-hand expertise from all the different agencies could usually handle the task quickly and efficiently. I really believe that this type of operation was a key element in the successes in joint operations planning and in theater, and because of it, we contributed significantly to the field commander's nearly instant knowledge of the battlefield immediately in front of him.

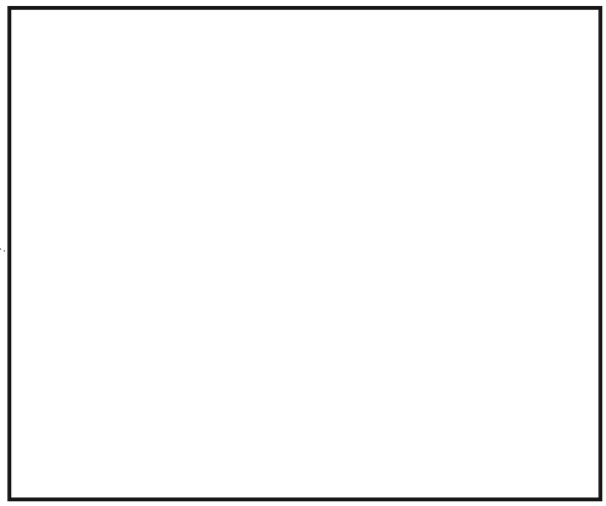
~~(FOUO)~~ From time to time, my connections with "the fort" were tested. At the beginning, I had carte blanche access to the NSA ground desk just as the Director had intended. Then, for some reason, that was nearly choked out and without warning. I discovered later that the choking of access came from a single source, and that soon

EO 1.4.(c)
P.L. 86-36

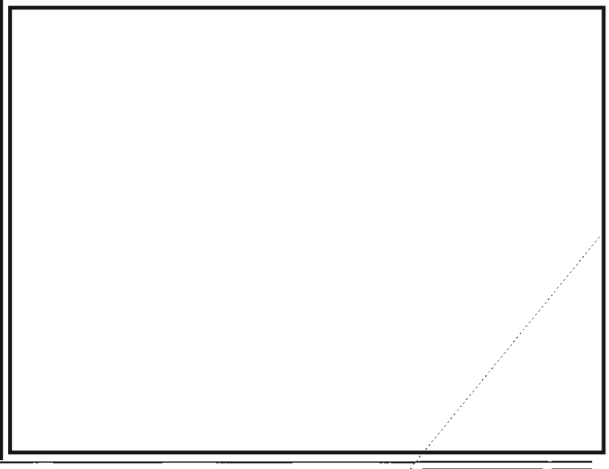
EO 1.4.(c)
P.L. 86-36
DOCID: 4019720

was obviated. At least with most of the military members on the desk, my rank helped to keep lines open. The sergeants did not really want to tell the warrant officer that they were not permitted to talk to him. (Good choice on their part.) Don't take me wrongly, there were many professional analysts who understood the magnitude of the mission and readily assisted in spite of some of the inane management directives.





~~(FOUO)~~ Back to JOINT— **J**oint Operations **INT**elligence. JOINT provides probably the quickest, all-source analysis of events to the national decision-makers. And it does it very well. The down side of what the JIC could do dealt mostly with the classification sensitivities, especially for SIGINT. Reports that were ORCON often contained the most usable intelligence for the field commanders, except that the field commanders couldn't receive the reports. Attempts at stripping out the relevent parts and removing ORCON caveats was almost always a time-consuming, thankless chore. But we did it. We also got angry when the field reported an ORCON TACREP in their summary as SECRET Releasable to Multi-National Forces. Yes, that happened, too. There were moments, in the heat of the battle as they say, when your conscience made the ORCON release decision for you. Then the paperwork followed.



EO 1.4.(c)
P.L. 86-36

DOCID: 4019720
EO 1.4(c)
P.L. 86-36

agency represented and an appreciation for the process of producing finished intelligence at those agencies. What we did was take all the work of many many people and consolidate it, encapsulating for the folks "upstairs" the meat of the matter in a complete picture. What each of us did was provide our own expertise in the intrepretation of products for those who may have incorrectly intrepretated or misread a product. My many explanations of how the SIGINT processes work changed attitudes and that, in turn, changed the validity factor.

(U) In light of the huge successes of Operation Desert Storm, what happened in this first-of-its-kind JIC probably indicates the future of intelligence for the battlefield and definitely for Pentagon and the White House. I think many of us agree that future conflicts will necessarily be joint service, if not combined national, ventures. And the one in charge of these ventures will have to be well versed in the intelligence community and its capabilities. It was smart to put the JIC together and the JIC provided tons of information where and when it was needed. An intel-smart General or Admiral could appreciate the JIC response to his needs and temper it appropriately in his planning. The use of national resources real-time during warfare operations can often provide a broader perspective and analysis of current events than a smaller, less equipped, more narrowly focused, in-theater service asset can provide. And the JIC proved it could be done with very good accuracy and timeliness. I do not believe the JIC portends the demise of our individual organizations, merely it enhances the intelligence they produce and provides a complete nationally derived, usually more sensitive, intelligence information for our leaders to respond to today's fast-paced, short-fused decision requirements.

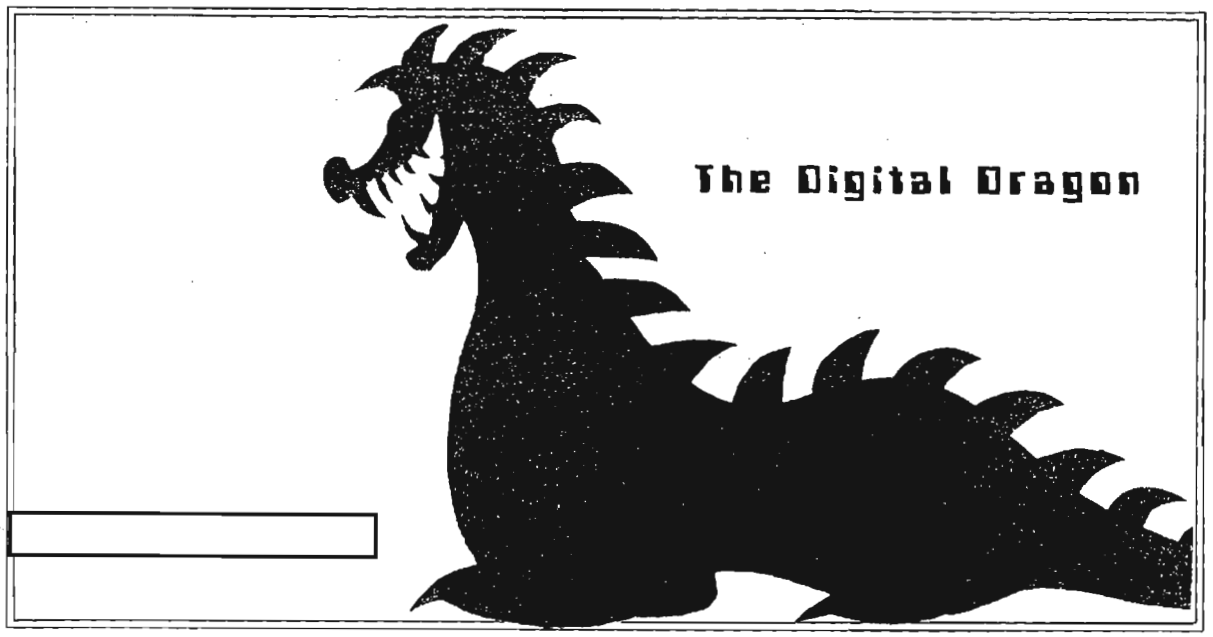
(U) Finally, I very much enjoyed serving in the JIC and feel I did contribute to our victories. It wasn't as sandy as the gulf, but I'd bet it was just as arduous. I have been in the Army for over 20 years. I always felt, especially in the intelligence fields, my mission was not to wage war, but to preserve peace—prevent war. I started my career in the Army in Vietnam. I am ending my military career as this war ends. As I look back, I wonder if I have done my job to keep the peace. The successes of this war and the miniscule number of casualties would suggest that our intelligence was right on—that I did do my job and did it well. However, this euphoria is hazy. What would have happened if the enemy really wanted to fight? I never want my brother and my nephew who served in the Gulf to know. Nor do I want my son to know in the future wars. I want the next JIC to be just as succesful, if not more so, in providing the politicians the ammunition they need so we, as a nation, do not need to provide ammunition to servicemen and women.

BULLETIN BOARD

SOUTHEAST ASIA AND VIET NAM ~~(S-CCO)~~

~~(S-CCO)~~ The Center for Cryptologic History, D9, is attempting to locate surviving materials pertaining to Southeast Asia and Viet Nam, whether official records or private holdings. The massive destruction of records in the mid-1970's has left significant gaps in the record of our efforts, especially VH/VC. If you know of any material about our efforts in this region—records, working aids, etc.—please notify D9, Ops 2B, 963-7292.

DOCID: 4019720



P.L. 86-36

(U) The People's Republic of China (PRC) has undergone a revolution in its telecommunications field within the last five years. This resulted from the decision to become a formidable world economic power early in the 21st century, with help from industry in Europe, Japan, Australia, and the United States. But industry of the developed world found that communication via telephone or telex was hampered by outdated and overused switching and transmission equipment. Nothing could be done until the many services involved in the complex chain of modern industry could "talk" to one other. This meant that an integrated telecommunications system had to be established quickly, including modem-connected computer-to-computer data transfer, telex, and business facsimile traffic, and be interfaced efficiently with the international telecommunications system through gateway facilities via communications satellite services and international undersea cables.

(U) Telecommunication was accorded a very high priority in the Seventh Five Year Plan (1986-1990) and has contined to remain so in the Eighth Five Year Plan (1991-1995). Innovation will be required to modernize to world standards.

(U) The Ministry of Posts and Telecommunications (MPT) is the primary center for telecommunications standards, long haul interprovincial systems, communications research, and equipment production. But each province and each Ministry is responsible for establishing its own standards, equipment purchases, and telecommunications structure. Except for the People's Liberation Army (PLA), all entities are to use European (CEPT) standards. The PLA, which does not need to meet international standards for its telecommunications needs, initially adopted a 512 kb/s mobile troposcatter system (TS193) and subsequently standardized with 460.8 kb/s mobile microwave (204A) and troposcatter (GS207 III) for flexible strategic communications requirements.

(U) The MPT has the telecommunications engineering and production expertise needed to support its function. Through the mid 1980's the Chinese used FM/FDM equipment almost exclusively; however, since 1988 microwave radio relay lines serving Beijing-Tianjin, Beijing-Shijiazhuang, and Beijing-Shanghai (including route cities Jinan, Xuzhou, and Nanjing) are being connected using CEPT Level 4 PCM (140 mb/s) equipment. Current planning provides for major Level 4 microwave lines to connect Beijing with most of the provincial capitals in the populous eastern and the industrial central portions of the

DOCID: 4019720

country by 1995. Most of the provinces have installed and are now operating digital microwave systems interconnecting the key nodes within their borders. East-West cross connection between Chengdu and Shanghai will be accomplished using multimode optical fiber cable, portions of which are currently under construction. In addition, a national digital 300-baud telex system using V.26 standard was initiated in the Spring of 1989. This telex system is replacing the older stacked Voice Frequency Telegraphy telegram systems, long the mainstay of PRC record traffic.

SWITCHING CENTERS

(U) The wealthier coastal provinces, because they are more involved with foreign business, moved rapidly to modernize their telecommunications. Indigenous production of digital telecommunications was limited mainly to smaller size Level 1 and Level 2 equipment or to small PBX switching systems. Some Level 3 microwave equipment was produced but its quality was considered poor in comparison to Japanese, American, and European products. The microwave routes were established, towers constructed, and antennas bought in-country. The digital telecommunications equipment was imported.

~~(S-CCO)~~ A modern telecommunications structure begins with a fast, flexible, digital telephone switching system. The current standard in advanced industrial nations today is the Digital Stored Program Control (DSPC) switch. This form of telephone switch is electronic and controlledby software. The combination provides the necessary flexibility to allow adjustments as conditions change, as well as the electronic speed to handle large volumes of telephone traffic. Cost of the switch is initially expensive, 150-300 USD per line, but over its life it is cheaper to operate than electromechanical equipment such as crossbar switches. An extremely important consideration is that DSPC switching capability is critical for an Integrated Services Digital Network (ISDN), long the hoped-for dream of the telecommunications world. As the technology to produce the large public DSPC switches did not exist in the PRC, both provincial and private networks have to import them. Among the equipments imported are: FETEX-150, Fujitsu, Japan; DMS-10/DMS-100, Northern Telecom (NT), Canada; AXE-10, L. M. Ericsson (LME),Sweden; System 1240, Alcatel, France; (NEC), Nippon Electric Corp.; NEAX-61, Japan; EWSD, Siemens, W. Germany; 5ESS, American Telephone & Telegraph.

(U) In addition to selling full switches to PRC customers, Fujitsu, and Alcatel established Joint Ventures to produce the components of their switching systems in the PRC. Fujitsu based its (FETEX-150) software support Venture in Fujian Province and Alcatel bought out the Shanghai based Bell Venture, Shanghai Bell Telephone Exchange Manufacturing Corporation (SBTEMC) to produce System 12 (System 1240) switches.

(U) Principle consumers for the DSPC switch market in the PRC include provincial and city level PTA/B's, the MPT, the Civil Aviation Administration of China (CAAC), the various electric power regional authorities, the railroad (MOR), and the People's Liberation Army (PLA). The PLA, although not a large scale buyer, is listed because it is a user on any systems established by the other functions.

(U) As of the date of this report, all provincial capital cities and a number of large prefecture capitals have installed one or more DSPC switches into their telephone structure. The initial entry was made by the Japanese companies Fujitsu and NEC. They had a good sales infrastructure within China and provided their products at a lower cost per line than European, American, or Canadian companies. Fujitsu was particularly successful, greatly aided by its Joint Venture in Fujian province. The Japanese, however, had delivery delays caused by stringent export license regulations. As the money for telecommunications dried up, companies who were able to swing the necessary long-term, low interest rate soft loans became more competitive. Even where the soft loans were available

DOCID: 4019720
P.L. 86-36
EO 1.4.(c)
P.L. 86-36
EO 1.4.(c)

in Japan, however, the long delivery time caused many Chinese customers to look elsewhere. Owing to these factors, the Canadian firm, Northern Telecom is in a good position for marketing its DMS-100 line.

[redacted]

Provincial Post and Telecommunications

(U) The manner in which the individual provincial Post and Telecommunications Authorities or Bureaus upgrade their telecommunications is dependent upon the degree of industrialization, the desire to attract foreign investment, the percent of the population in an urban or rural environment, the wealth of the province, and the innovativeness of the leadership. As discussed above, the initial step has been to establish a core system using digital Stored Program Control Switches in the provincial capitol and key large cities.

[redacted]

SUMMARY

(U) The infusion of digital technology into PRC telecommunications over the period 1986-1990 has progressed at a rate probably surpassing any other major country. Progressing from having one Level three (34 MBs) microwave line operational between 1981 and 1985, the PRC now has Level three and Level four microwave lines operating in most provinces and state of the art digital SPC switching systems in place and operational for most major cities. Telegrams are now routinely passed through a nationwide digital 300-baud Telex using V.26 modem. Connectivity has been established with world digital standards in the gateway cities via IntelSat and the way is being rapidly paved towards an ISDN environment within the next five to ten years if desired. In terms of telecommunications, the digital world is happening now in the PRC.

(U) **China is truly becoming a Digital Dragon.**

DOCID: 4019720

Ich spreche Deutsch

or

Wie ist ihr toiletten?

P.L. 86-36

[redacted] M312

Back in the olden days of 1971, I took a Permanent Change of Station (PCS) assignment to Stuttgart, Germany. My sponsor picked me up at the airport. That day she taught me the word „neun". If you know your eins, zwei, drei, you know that „neun" is German for nine. By stepping up to the reception desk at the Vaihingerhof and trying to make my lips form that unfamiliar word, I was able to get the key to Room #9. That room—Zimmer #9—would be my temporary home until I found an apartment.

As you can imagine, knowledge of this one German word did not afford me an easy passage throughout Deutschland. During my tour in Germany, fortunately I increased my vocabulary. I took German I and II offered on post through the overseas division of the University of Maryland. I also took several German conversational courses. With the knowledge gained from these courses, I was able to order meals at restaurants; reserve a room while travelling and determine if the room was with or without Bad (bath), and if it included Fruehstueck (breakfast), etc.

After awhile I was also able to recognize when German was used incorrectly. I went to dinner with a friend one evening. During the course of the evening, my friend asked the waitress, „Wie ist Ihr Toiletten?" The waitress graciously gave him directions to the men's room. On his way back to our table my friend was grinning sheepishly because he realized that he had used the interrogative wie instead of wo. In so doing, instead of asking "where" the lavatory was, he had instead asked the waitress "how" her lavatory was.

Once on a German bus trip to Italy, my fledgling German language ability came in handy. The German bus driver (who spoke no English) and the tour guide (who spoke fluent German and English) got into a spat. For days they would not talk to each other, but instead communicated through me. It was somewhat hairy at times, but nonetheless a challenge.

I am sure that many NSA employees who have been on PCS assignments have similar humorous experiences with the language of the country. Indeed, I was totally unprepared linguistically for my first experience on foreign soil.

Now, many years since my PCS, I am happy to say that the Office of Personnel provides language tapes to PCSing families. Often there just isn't time to attend a language class before you PCS no matter how well-intentioned you may be. As anyone who has been PCS knows, there is a myriad of concerns about your field tour: where will you live; what will the job be like; what about schooling for your kids. All of these changes are traumatic enough without compounding your discomfort by being unable to speak, read or understand the language.

As most of our lives become busier, more complicated and often plagued by traffic, language tapes can fill a void. By popping a cassette into the car tape deck, you have an opportunity to learn a language during your daily work commute. Why not have a "leg up" by at least learning some of the basics of the language, such as, yes, no, please, thank you, etc. Then when you are approached by someone who asks you, „Wo ist der Bahnhof?", you can competently say, „Rechts um die Ecke, dann geradeaus".

So, if you are processing for an overseas assignment, don't forget to ask the personnel in M31, Field Staffing and Personnel Administration, about the language tapes. The following tapes are available from M31:

[redacted]

Auf Wiedersehen, Viel Glueck, and Prosit!

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

EO 1.4.(c)
DOCID: 4019720

A Matter of COMPRESSION

P.L. 86-36

P11

COMPRESSION

(U) The compression algorithm we are discussing is to be embodied in a new type of modem, the V.42. CCIT standards for the V.42 have been approved and a number of companies have committed to building their version of it. The British firm HAYES already has a V.42 modem on the market.

(U) The impetus for the V.42 was the rapidly advancing state of the microelectronics art. Industry realized that small, relatively cheap modems could be built with a capability to perform complex functions requiring a high compute and large storage capacity. The V.42 does its own framing and employs an effective error detection and correction by retransmission procedure.

(U) Because the V.42 can ensure that virtually error-free data is received, a "lossless" compression algorithm was selected to be incorporated in the modem. Unlike "lossy" compression algorithms which are error-tolerant, successful decompression by this "lossless" compression algorithm, known as V.42 bis, requires that the data received be exactly that which was sent. The V.42 bis is adaptable, an advantage over most compression algorithms, which are designed to compress a specific kind of data. In the latter case, if the data differs from the type for which the algorithm was designed, performance of the algorithm suffers greatly.

(U) In the V.42 codebook (more generally referred to as a "dictionary") the entries are made dynamically, representing character strings that occurred earlier in the current transmission, so V.42 bis adjusts automatically to the nature of the data being sent. If the modem is used for an Italian language transmission, for example, the dictionary will fill mainly with entries that represent character strings that occur with a relatively high frequency in Italian. If an

DOCID: 4019720

accounting report is sent, most entries will represent number strings, row or column labels, or other items in the report format. While the compression ratio achieved by V.42 bis is a function of the roughness of the data being transmitted, it is not affected by the type of data. This versatility, together with its relatively low price and small size is likely to make the V.42 attractive for a wide variety of communicators.

(U) The CCIT standards for the V.42 are flexible enough to allow manufacturers to build models of the modem that range from "stripped down" to "full bells and whistles." Maximum dictionary size may extend from 512 entries to an unspecified upper limit. Maximum string size, i.e., the greatest number of characters that may be represented by a codeword, may range from 6 to 250. Modems with differing capabilities will be able to communicate with each other. At the beginning of a transmission, the corresponding modems automatically "negotiate" parameters. Each proposes a maximum dictionary and string size. In each instance, the low bid wins since the modem with the greater capacity can adjust to the lesser parameter proposed by the inferior modem.

(U) At the beginning of a transmission, the dictionary contains 259 entries. Codewords 0 to 2 are reserved for control functions. The remaining 256 codewords represent the characters of the transmission code. Each character is assigned to the codeword that is 3 greater than its transmission code value. (The expected transmission code is ASCII. Since A = 65 in ASCII, Codeword 68 would represent the one character string A.) These initial 259 entries, known as "root nodes," constitute the fixed portion of the dictionary.

(U) The number of bits transmitted to represent a codeword is the least number needed to convey the value of the last entry in the current dictionary. At the beginning of a transmission, the last entry is codeword 258, requiring nine bits to represent as a binary number. As the transmission proceeds, the dynamic portion of the dictionary begins to fill. When an entry is made for codeword 512, the number of bits transmitted per codeword jumps to 10 because at that point, the dictionary contains an entry whose codeword value cannot be represented by 9 bits. Later in the transmission when an entry is made for codeword 1024, the bits sent per codeword increases to 11, etc.

(U) During a transmission, the compression algorithm looks at the consecutive characters to be communicated. Each time it adds a character to the string it is currently processing, it checks the dictionary to see if it contains an entry that represents the current string. If it does, the algorithm adds the next character to the string. If it does not, the algorithm outputs the codeword that represents the current string minus the last character added and creates a new dictionary entry that represents the current string (including the last character). If the dictionary is not yet full, the codeword assigned to this new entry is the next one available. (If the last entry in the current dictionary is 1000, the new entry will be assigned codeword 1001.)

(U) Say, for example, that the first two characters to be communicated are **AR**. The algorithm would first check the dictionary to see if there is an entry that represents the single character **A**. There is. The initial dictionary contains an entry for each of the characters in the transmission code. The algorithm would then add the **R** to its string and checks to see if the dictionary contains an entry that represents **AR**. It does not. The algorithm would then output the codeword that represents the 1-character string "**A**" and create an entry to represent "**AR**". Since the last entry in the initial portion of the codebook is codeword 258, codeword 259 would be assigned to the string "**AR**". Since an output would have been made to represent the "**A**", it would be deleted from the current processing string. The current processing string would then be the single character "**AR**", to which the next character to be transmitted would be added and processing would continue.

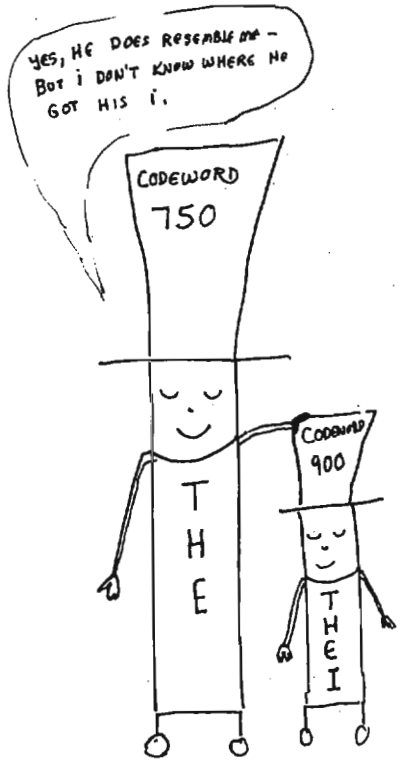
(U) The dictionary grows in the form of a tree structure. It might be thought of as a family tree. Except for the immortal root node primogenitors created by the CCIT Gods, every dictionary entry has a parent. The entry "inherits" its parent's string to which is added one additional terminal character.

(U) Once the dictionary reaches its maximum size, the algorithm cycles around to the beginning

DOCID: 4019720

of the non-fixed portion of the dictionary (which starts at codeword 259), and begins searching for "leaf nodes." A "leaf node" is a codeword that has no children, i.e., there is no dictionary entry that represents its string plus one additional character. When a leaf node is found, its string is released and its codeword number is used for the next dictionary entry to be made. (This is a merciless algorithm that tells its creations, "Be fruitful and multiply. If you are barren when next I pass this way, I will zap you!")

we capture the entries that were made from the point where the cut-in began? We know the process. We know that a dictionary entry was made when codeword 700, the initial codeword of our cut-in, was sent. We know the string to assign to the new entry is the string represented by its parent (700) plus the first character of the string



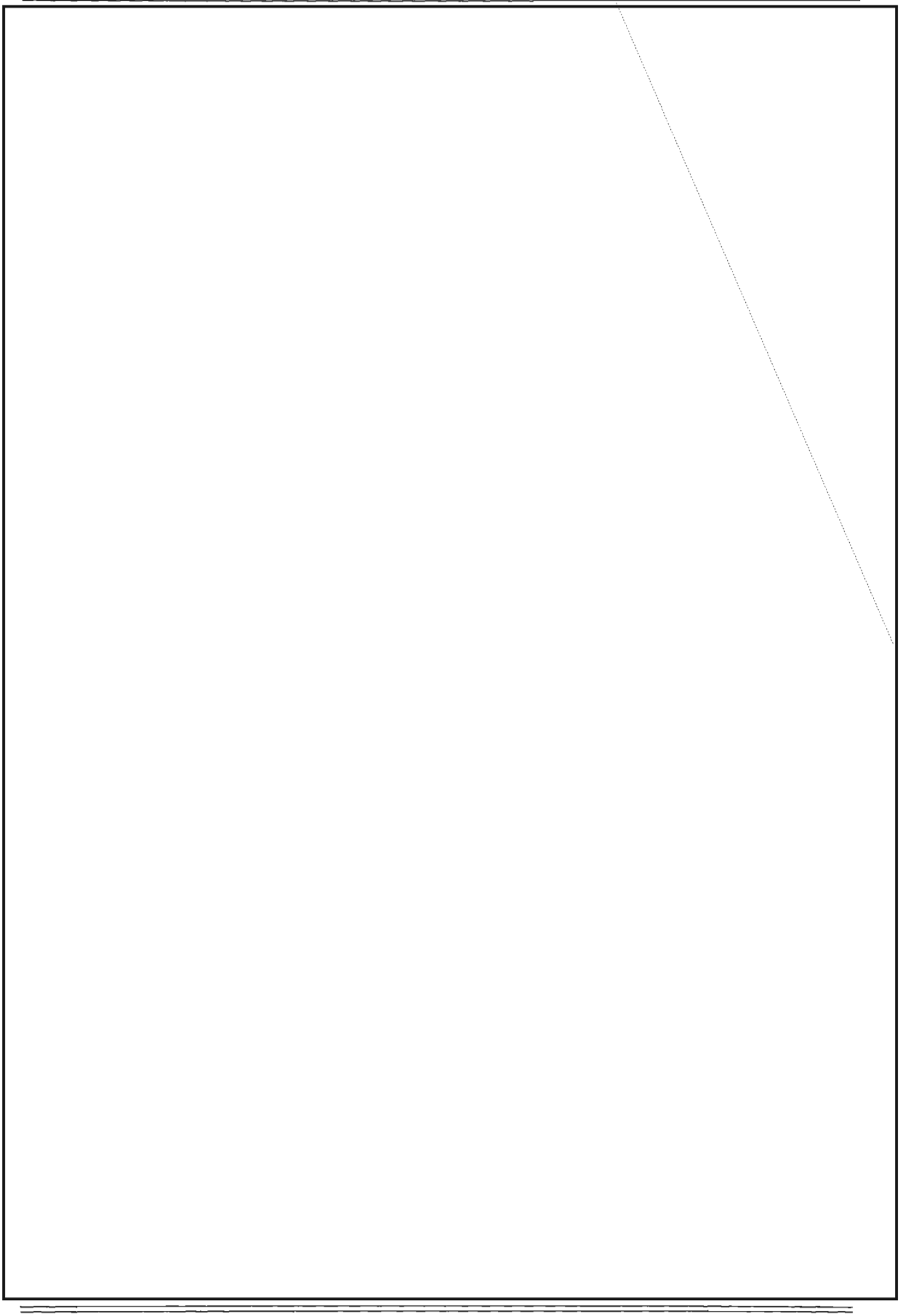
Each non-root node has a "parent." The "child" represents the "parent's" string plus 1 added character.

(C) For some months, Dr. Ralph Jollensten and I have been developing tools to attack this cut-in problem. Designing the tools has been a cooperative venture. I turn them into software routines and then Ralph has the fun of testing them against simulated cut-ins that I create for him.

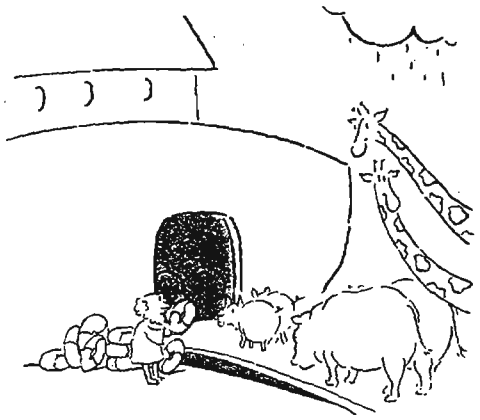
EO 1.4.(c)
P.L. 86-36

DOCID: 4019720

EO 1.4.(c)
P.L. 86-36



DOCID: 4019720

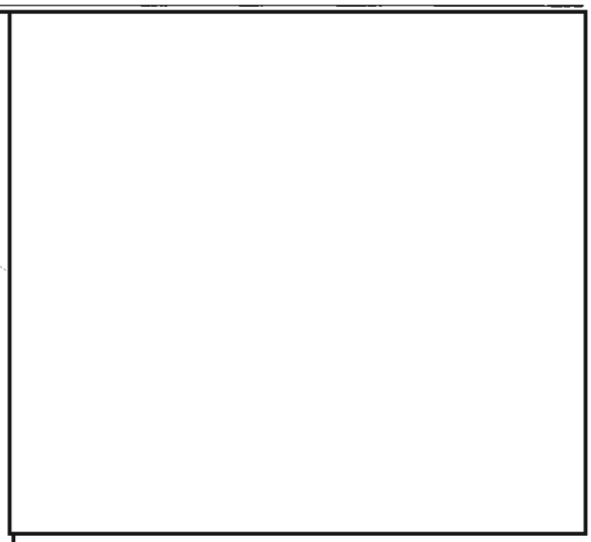


ALL YOU WANTED TO NOAH ABOUT ARC

P.L. 86-36

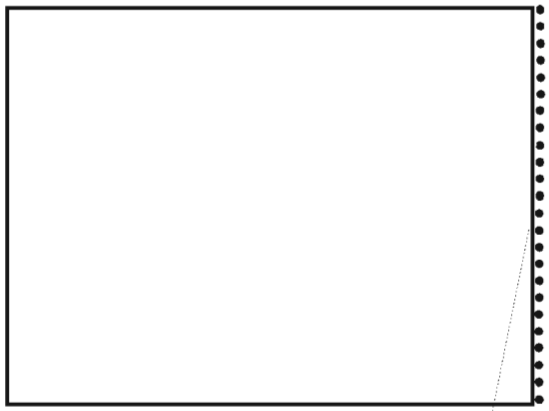
P.L. 86-36
EO 1.4.(c)

DOCID: 4019720
P.L. 86-36
EO 1.4.(c)



ERRATA

In 3rd Issue 1990, several lines were inadvertently omitted between pp. 14 and 15. They should read:



FILTERING AND CHARACTERIZATION

~~(C)~~ Filtering is decision making. Every act within the SIGINT cycle in which items are identified and evaluated for retention or rejection is an act of filtering. The act can be mechanized, or can be performed by humans who make the selection, allocate the sensors for the collection activity, and make other decisions about the SIGINT process.

EO 1.4.(c)
P.L. 86-36

In 3rd Issue 1990, on pp 14-18 and 20, please change the issue to ""3rd Issue 1990"

CRYPTOLOG regrets the errors

~~CONFIDENTIAL~~

DOCID: 4019720

CRYSCO-90

~~This article is classified CONFIDENTIAL-HANDLE VIA COMINT CHANNELS ONLY in its entirety~~

The Cryptanalytic Software Committee (CRYSCOM) was established in May 1984 as a volunteer organization to improve the use of computers throughout the entire cryptanalytic community by providing a forum where representatives of the CA computer complexes could exchange ideas. In 1987 it was officially sanctioned when its charter was signed by the Office Chiefs of the major CA complexes at NSA. CRYSCOM provides a formal mechanism for the collection and dissemination of information on computer support [redacted]

EO 1.4.(c)
P.L. 86-36

The Cryptanalytic Software Conference (CRYSCO) is an annual event where current topics on cryptanalysis and computer science are presented. Following are the recommendations stemming from CRYSCO-90.

1. Software Availability

Develop and promote a softcopy method of listing all available software on all appropriate machines in the CRYSCOM community, to include pending software, also to include software which makes use of special purpose boards or devices.

Status: Notesfiles, software.ad and software.quest, were created. Some user organizations are using them, while other organizations are developing their own library functions.

2. Software Exchange

a. Continue efforts to establish and promote software exchanges. [redacted]

b. Encourage organizations to adhere to agreed upon standards.

c. Promote the goal of a man page for every piece of software.

Status: The number of software exchanges is growing and ground level satisfaction with and success using the procedures has encouraged the organizations to adhere to the agreed upon standards. The goal of a man page for every piece of software exchanged has been attained. Feedback through the Software Points of Contact has been perceived as effective.

3. CRYSCOM Character Message Format:

Resolve outstanding disagreement on header line tags.

Status: Parties involved recognize the header line tag issue as a difference to be aware of as opposed to an outstanding disagreement. The committee agreed to table this recommendation.

4. X-Window Widget Sets :

[redacted]

Status: A working group has been formed and is evaluating toolkits.

P.L. 86-36

DOCID: 4019720

5. Public Domain Software

a. Look for a method of obtaining public domain software.

b. Establish a procedure to propagate error reports for public domain software back to originators, particularly, X-Windows, Gnu products.

c. Establish a procedure to propagate fixes back to the users.

Status: R5 is setting up a mechanism for evaluating public domain software, which will be available for use by community members. After this evaluation process, CRYSCOM intends to submit a list of specific software to T03 with a request for consideration.

6. System Administrators:

Organize a forum for the various system administrators, especially those of the numerous SUN networks, to discuss mutual concerns, such as security issues, response times, network transparency, etc.

Status: Completed.

7. Training

P.L. 86-36

Lack of UNIX training is seen as a big problem in the move [redacted] Promote UNIX training, such as through brown bag seminars.

Status: Brown Bag seminars will be reinstituted to promote UNIX training and expertise.

8. NQS Checkpointing and Restarting:

Promote the resolution of NQS checkpointing and restarting problems.

Status: A list of capabilities wanted in NQS has been supplied to Cray, who will work to incorporate them in a future release.

9. Software Development Tools

Promote development, acquisition and use of appropriate software development tools; especially optimization tools, graphics aids, timing tools.

Status: CRYSCOM is working with W352 to arrange for a brown bag seminar on optimization. This recommendation is one which will be an ongoing concern.

10. CRYSCOM "Official Papers"

Create a directory/catalog of such papers to include: CRYSCO recommendations, position papers, guidelines, standards, etc. In short, any voted on document.

Status: Completed

To the Editor:

Though there's a lot of expressed concern about "The" language problem and keeping linguists happy, management actions belie that concern. Look where they located the Language Career Panel, for one thing. It's at Friendship. Where are the linguists? At Fort Meade.

Linguists have more in front of them than they can possibly do. For a lot of languages there's a severe shortfall. So why are they compelled to travel to Friendship in connection with career development?

Why does management allow this inane situation to continue?

Why don't the linguists rise up and protest?

"Al Enquist"

~~FOUO~~

DOCID: 4019720

Normalization

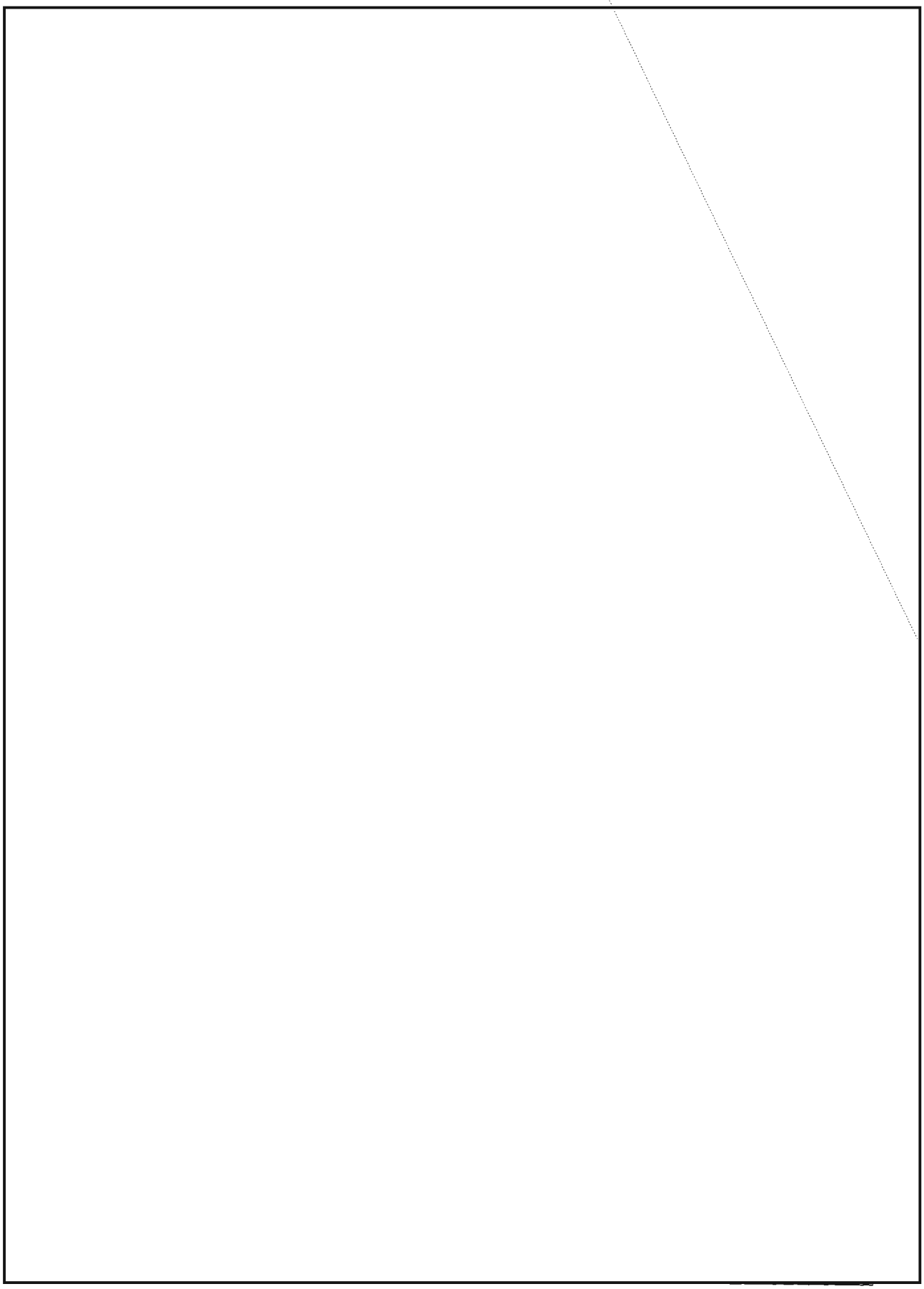
P.L. 86-36

[redacted] *A26*

~~SECRET~~ EO 1.4.(c)
~~HANDLE VIA COMINT CHANNELS ONLY~~ 86-36

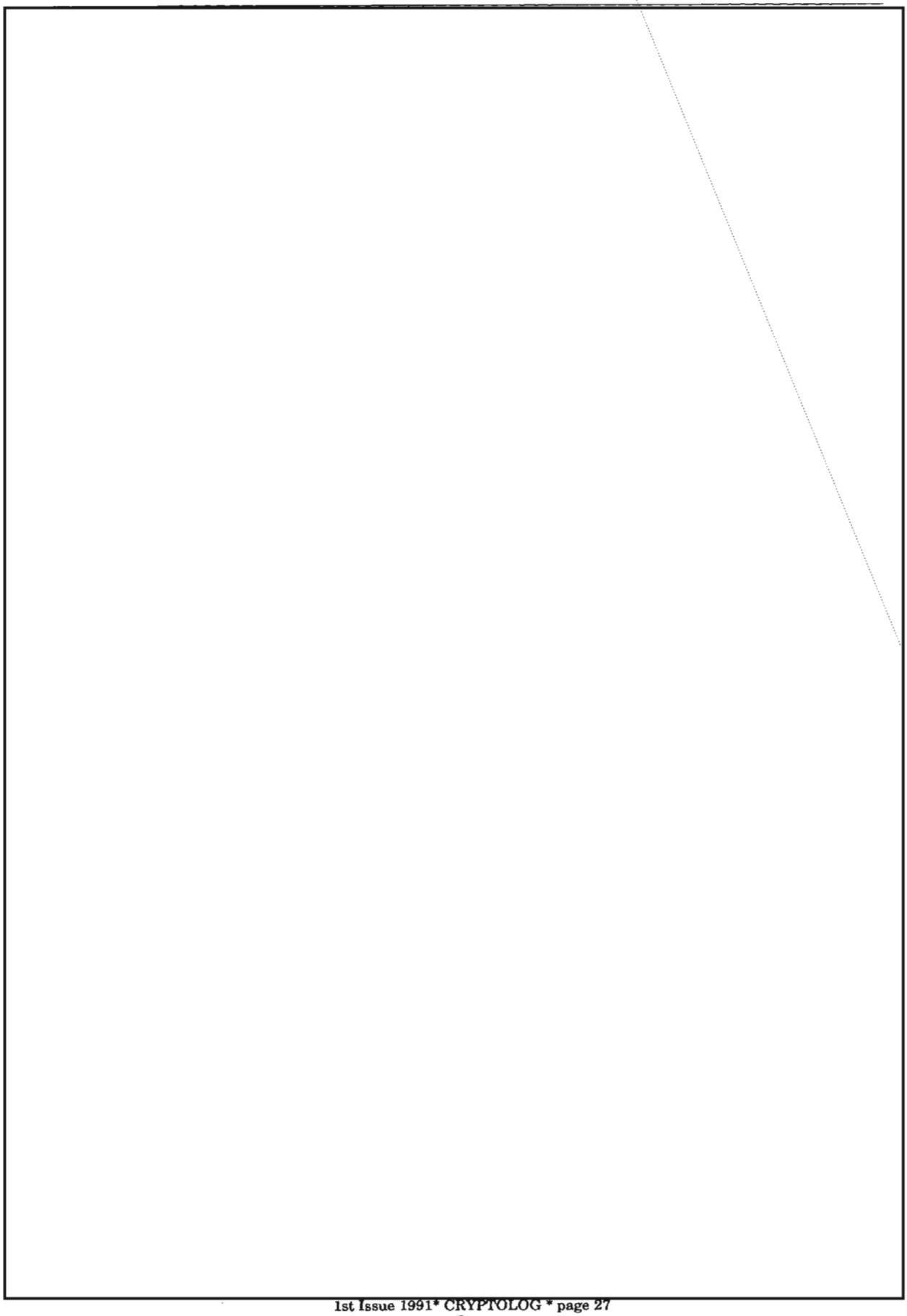
DOCID: 4019720

EO 1.4.(c)
P.L. 86-36



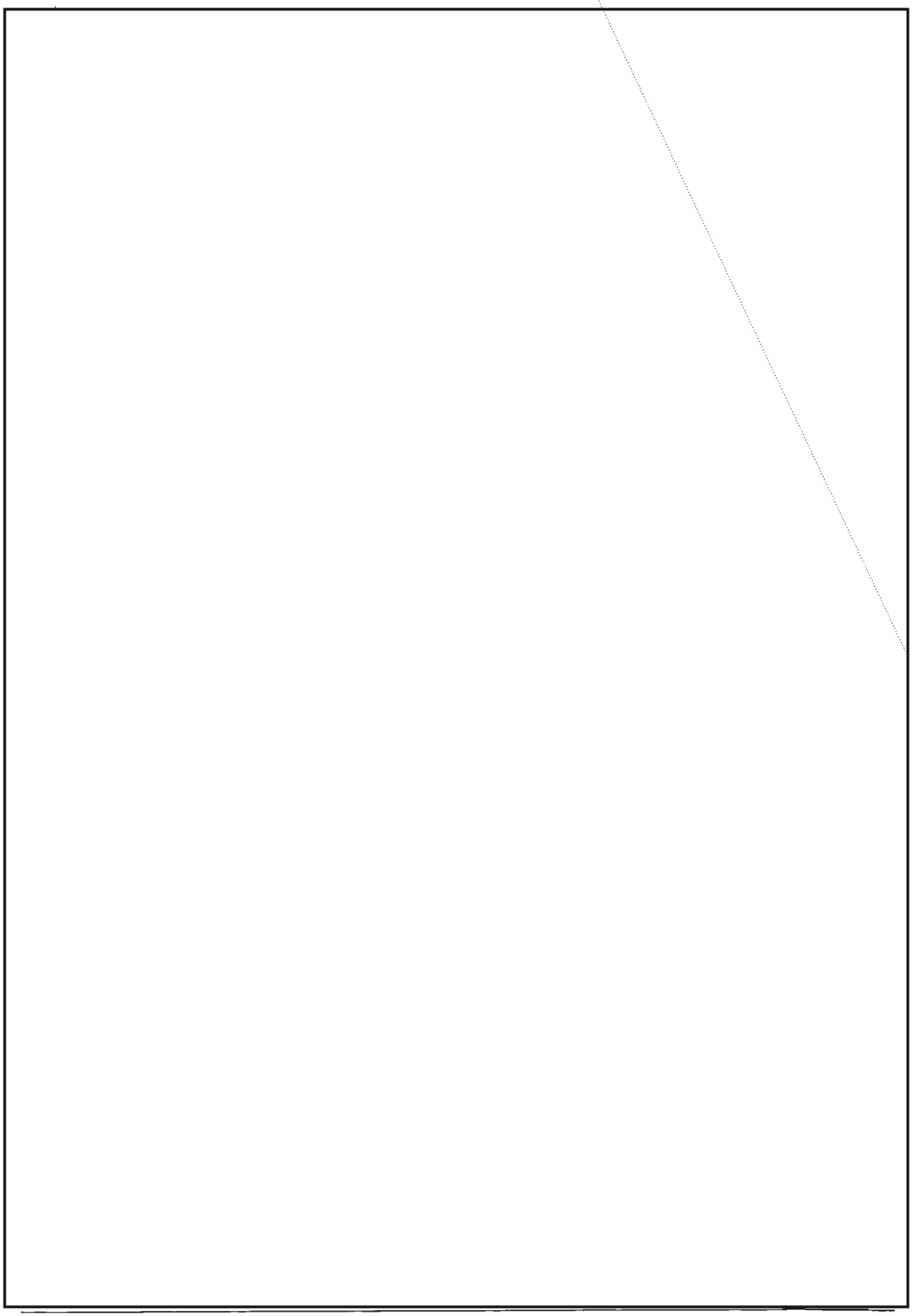
DOCID: 4019720

EO 1.4.(c)
P.L. 86-36



DOCID: 4019720

EO 1.4.(c)
P.L. 86-36



P.L. 86-36
EO 1.4.(c)

~~CONFIDENTIAL~~

To the Editor:

I read with interest the item by Preston Currier on the subject of Cryptographic Habits and Cryptanalytic Diagnosis, an extract from his 1969 papers [CRYPTOLOG, 3rd Issue 1990].

I thought you be be interested in knowing that T54 (Archives and Repository Services) is attempting to record historic cryptographic information, i.e., codebooks and technical papers for the period pre-1975, in a special electronic database referred to as the "Cryptographic Codes and Ciphers Collection." This information is unique and does not duplicate C/A information in other Agency collections, i.e., P1 Collection, etc.

This endeavor by T54 is quite massive and will require considerable time to complete; however, the initial progress that has been made to date has proven extremely worthwhile and has attracted the interest of many cryptanalysts from various OPIs in the Agency.

I am taking the liberty of forwarding you two recent communications by [redacted] G424/H111 after his research into various T54 treasures and the results of his efforts in support of a current high-interest cryptosystem that he was assigned. I believe you will find these of interest.

Should you wish a follow-up to the [redacted] article, these comments by a young cryptomath analyst may alert other analysts in this discipline to the wealth of information developed by our predecessors and now becoming available in T54, Archives and Repository Services, and D9, NSA Center for Cryptologic History.

[redacted] *T541 Archivist for C/A*

~~CONFIDENTIAL CCO~~

P.L. 86-36

~~SECRET~~

P05/SAO

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

in re PROFORMA

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

P.L. 86-36

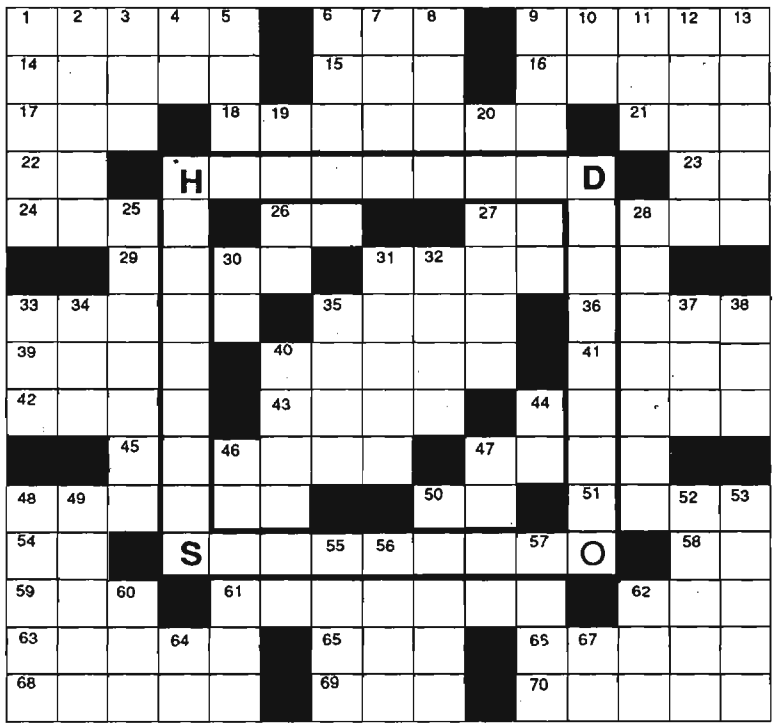
~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36

DOCID: 4019720

Busman's Holiday

This puzzle is dedicated to William Lutwiniak, the founding publisher of CRYPTOLOG, himself a noted puzzle-maker, to mark a half-century's association with cryptology. *See page 7.*



ACROSS

1. '50's chewing gum favorite
6. Word with fly and about
9. *Enterprise*- ing mate
14. Seen less often
15. Basketball great(?) Blab
16. Give a full 10%
17. Wilder pronoun
18. *Odd assortment*
21. Oldie but goodie "___ Then"
22. Correlative alternative to 60-D

*** CLOCKWISE**

23. Generic Mrs./Miss
24. Marx missing from *Monkey Business*
26. "___ you is or ain't you ain't . . ."
27. Syria's second-largest city
29. Now-stout Guinness
31. Entertaining Lola
33. Washington August forecast
35. Guitar-wielding Hendrix
36. *Imperial contents*
39. Man from Medina
40. Donny's little sister
41. "A ___ by any other name . . ."
42. Hero Jones at the 500?
43. The class of Hitchcock's creatures?
44. Thomas or Bob
45. *Detroit's Joe Louis and Baltimore's Baltimore*
47. Pull a long face
48. Place name in the '60's news
50. Cerium's symbol
51. ___ off, angry à la Curtis Strange
54. A's pre-vowel substitute
58. Behold's partner
59. Anais
61. Settle the details
62. Coulomb per sec.
63. Imperturbable one
65. Explosive stuff
66. Plains home
68. Down to ___
69. Opp. of WNW
70. Angel-owning cowboy crooner

DOWN

1. Flashback: your President is not one
2. A Dern-good actress?
3. Hockey great
4. Fine day in 1945
5. Bombeck
6. Drinks in air
7. Far and ___
8. Xiaoping
9. Brando cry in *Desire*
10. ___ are not ^{2}
11. Baseball great
12. Bonzo, for one
13. Horse racing great
19. *The Iliad* or *The Odyssey*
20. Netminder
25. Fast month in 27-A
28. One who has done his time—partially
30. Wilbur Post's pet
31. Bakes pottery
32. Kingsley
33. "Bali ___"
34. Coffee maker
35. Contents of above, in Indonesia?
37. ___ a matter of fact
38. Another Kingsley
40. Crèche component
44. Ti's successor
46. Fortify bread
47. *La carte*
48. Saint-Saens ___ *Macabre*
49. Baker who's "Giving You the Best That I Got"
50. $100
52. Siwwy Wabbit's foe
53. One of Doc's little buddies
55. Participate on the 2nd Tues. in Nov.
56. Holiday and Days
57. ___ boy!
60. See 22-A
62. Likely to be good at?
64. Stephen King's ___
67. Prefix opp. to *dys-*

RLW

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019720

Editorial

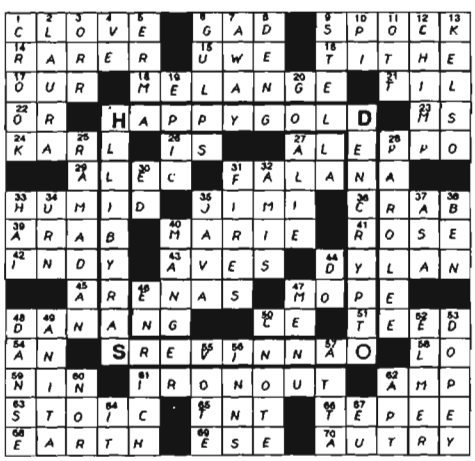
Lessons Learned

With a certain amount of euphoria, some veterans of past crises were commenting on the most recent one in which they were but spectators. They were pleased with the high interest in "lessons learned." It's important to record and act upon these, they believe, and the record should include the minutest detail of things gone wrong. The causes of serious problems can often be traced to the snowballing effect of many minor errors that were disregarded.

From their distant perch, these veterans noticed the beginnings of changes in some of the operational elements that were not directly involved in the crisis but that contributed people and material resources. Somehow those elements found ways to function more efficiently with fewer people. Maybe they, too, should be included in a "lessons learned." In a leaner operation, there was no time to pay tribute to arbitrary prerogatives. Surely the newly streamlined mode deserves close study, and perhaps, emulation elsewhere.

Va

Solution to Puzzle on page 31



BULLETIN BOARD

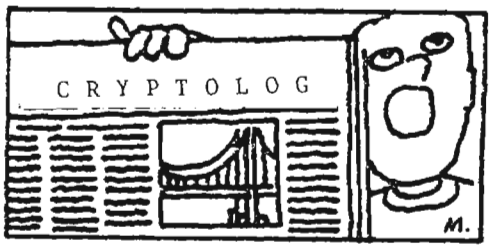
RECOVERING DELETED DATA ON THE SUN

~~(FOUO)~~ R522 found a way to recover deleted data on the SUN. A typing mistake had resulted in the deletion of an entire directory of files dealing with the TANCIL software. The SUN people and other experts estimated that the chances of recovery ranged from poor to none.

~~(FOUO)~~ But R522 experimented with a method that proved to be successful in recovering files, especially source code. All you have to do is lock the file system long enough to make a copy to work with offline. Using this technique, R522 was able to recover most of the TANCIL software. For more information call [redacted] R522, 968-8411.

P.L. 86-36

Notice to Subscribers



Distribution for this issue reflects changes received by COB 13 May 1991.

If you move or are reorganized, please notify CRYPTOLOG DISTRIBUTION, P1, NORTH. Be sure to indicate both your old **and** new organization and building.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019720

CRYPTOLOG

Editorial Policy

CRYPTOLOG is a forum for the informal exchange of information by the analytic workforce. Criteria for publication are: that in the opinion of the reviewers, readers will find the article useful or interesting; that the facts are accurate; that the terminology is correct and appropriate to the discipline. Articles may be classified up to and including TSC.

Technical articles are preferred over non-technical; classified over unclassified; shorter articles over longer.

Comments and letters are solicited. We invite readers to contribute conference reports and reviews of books, articles, software and hardware that pertain to our mission or to any of our disciplines. Humor is welcome, too.

If you are a new author, please request "Guidelines for CRYPTOLOG Authors."

How to Submit your Article

Back in the days when CRYPTOLOG was prepared on the then state-of-the-art, a Selectric typewriter, an article might be dashed off on the back of a used lunch bag. But now we're into automation. We appreciate it when authors are, too.

> *N.B.* If the following instructions are a mystery to you, please call upon your local ADP support for enlightenment. As each organization has its own policies and as there's a myriad of terminals out there, CRYPTOLOG regrets that it cannot advise you.

Send two legible hard copies accompanied by a floppy, disk, or cartridge as described below, or use electronic mail. In your electronic medium (floppy, disk, cartridge, or electronic mail) please heed these strictures to avoid extra data prep that will delay publication:

- do not type your article in capital letters
- do not right-justify
- do not double space between lines
- but **do** double space between paragraphs
- do not indent for a new paragraph
- but **do** paragraph classify
- do not format an HD as DD or vice-versa–our equipment can't cope

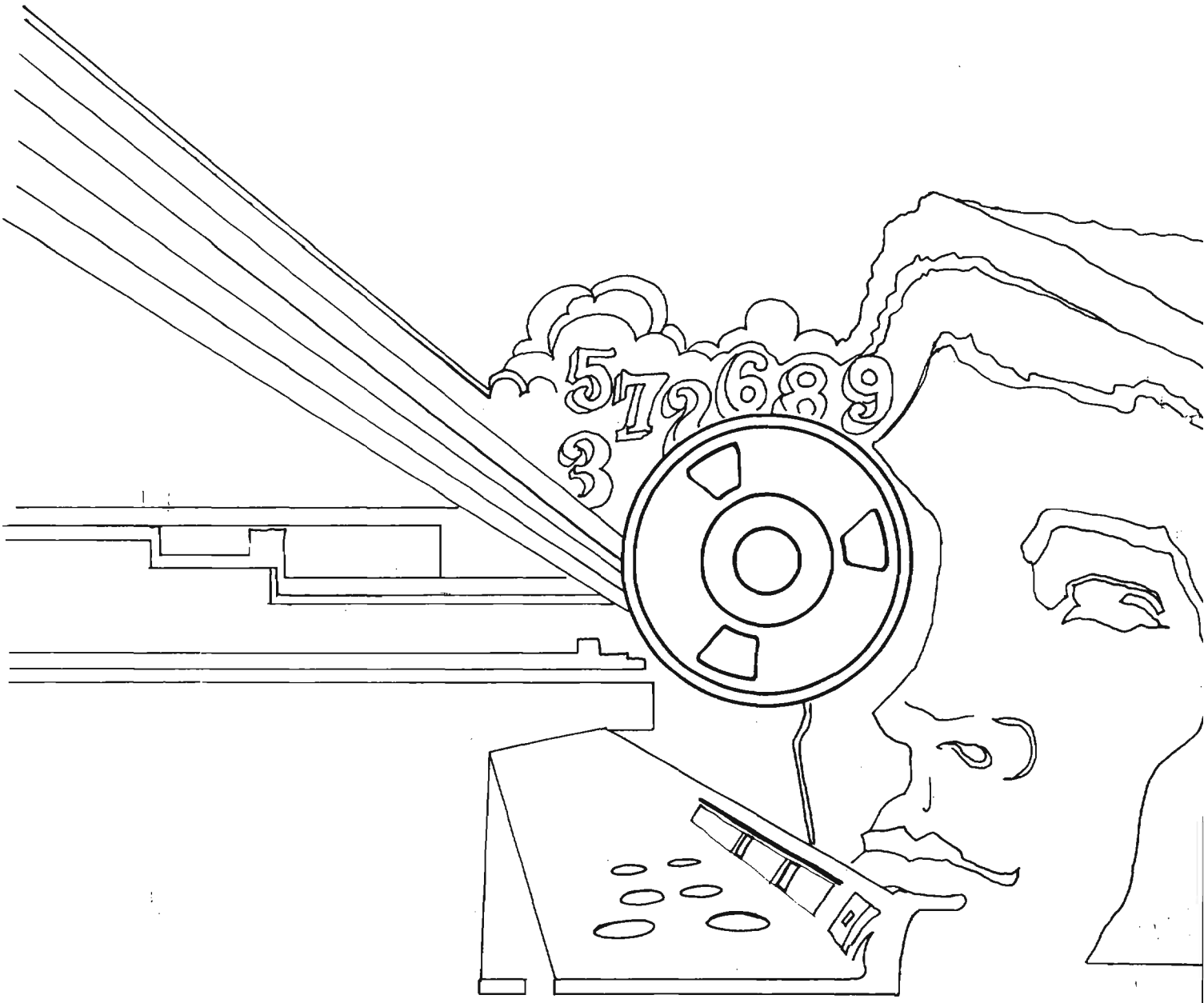
The electronic mail address is *via* PLATFORM: cryptlg @ barlc05
or *via* CLOVER: cryptlg @ bloomfield

CRYPTOLOG publishes using Macintosh and Xerox Star. It can read output from the equipment shown below. If you have something else, check with the editor, as new conversions are being added. Be sure to label your floppy or cartridge as to the hardware, density, format, and software you used. Don't forget your name, building, organization, and phone!

HARDWARE	MEDIUM	SOFTWARE	FORMAT
SUN	60 or 150 MB cartridge	ascii only	TAR or RAW
XEROX VP 2.0	5 1/4" floppy only	n/a	n/a
MACINTOSH	3 1/2" DD disk only	MS WORD MacWrite TEXT WriteNow	n/a
IBM & Compatibles	3 1/2" 1.2 MB disk 5 1/4" DD or HD floppy	MS WORD WordPerfect WordStar ascii DCA (IBM revisable)	DOS
WANG	n/a	n/a	n/a

~~FOR OFFICIAL USE ONLY~~

~~TOP SECRET~~



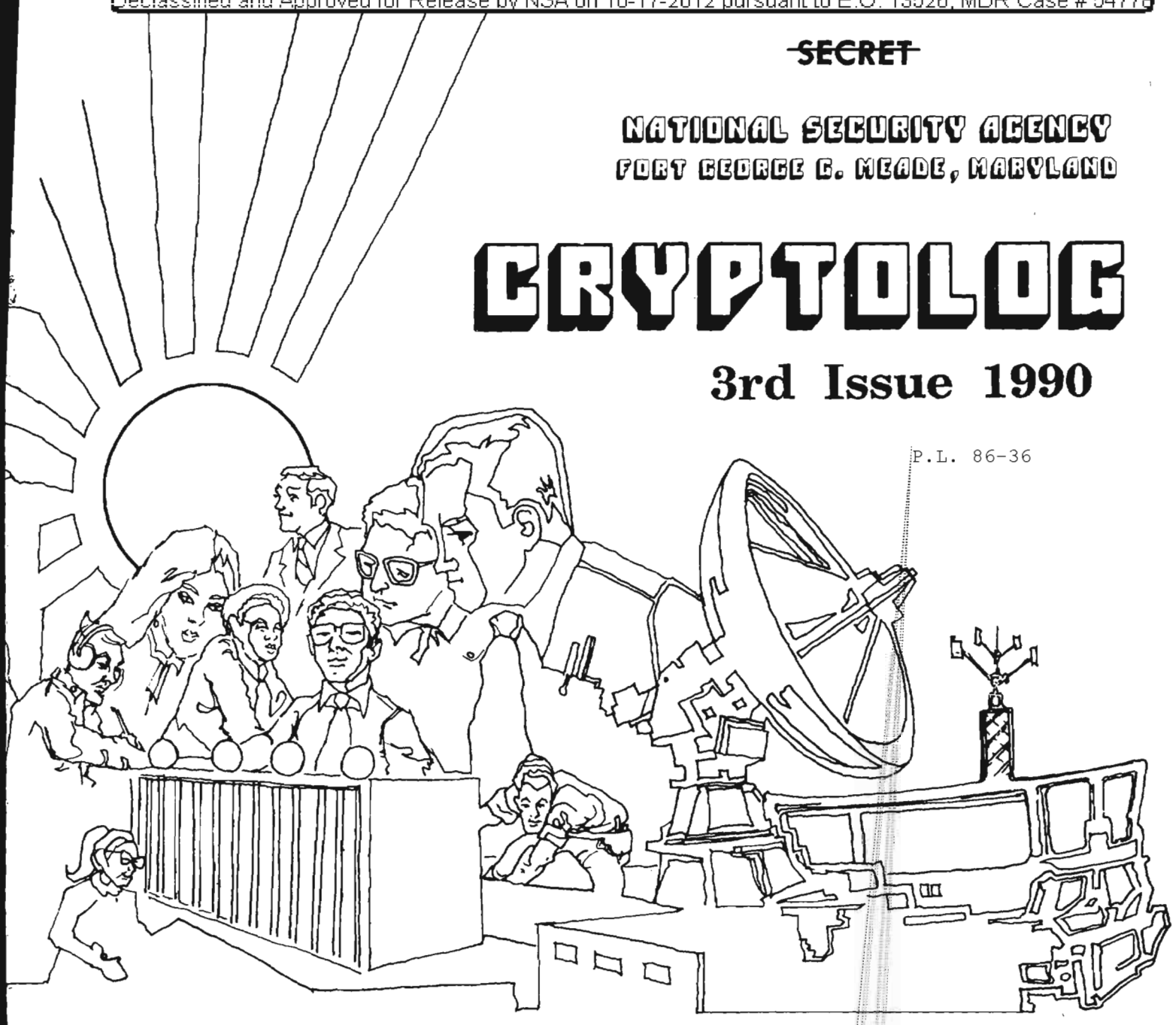
DOCID: 4012034
Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

3rd Issue 1990



P.L. 86-36

HAIRCLOTH . . . . . [redacted] . . . 1
UNCLASSIFIED FACTS. . . . . [redacted] . . . 7
QUOTE WITHOUT COMMENT . . . . . [redacted] . . . 8
AURAL LANGUAGE IDENTIFICATION . . . . . [redacted] . . . 9
SIFTING WHEAT FROM CHAFF. . . . . [redacted] . . .14
LETTERS 18, 33
THE MAYAGUEZ INCIDENT . . . . . [redacted] . . .19
THE THREE FACES OF COLLECTION . . . . . [redacted] . . .21
HOW IT STARTED. . . . . .David Gaddy. 22
HOW THE FRIEDMAN AUDITORIUM DID NOT GET ITS NAME! . . . . . [redacted] . . .23
TECHNICAL LITERATURE REPORT . . . . . .David Harris 25
EDITORIAL 30
BOOK REPORTS: DOUBLESPEAK . . . . . [redacted] . . .31
. . .HOW TO EDIT A SCIENTIFIC JOURNAL . . . [redacted] . . .32
GOLDEN OLDIE. 36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

DOCID: 4012034

P.L. 86-36

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XVII, No. 3 . . . . . .3rd Issue 1990

PUBLISHER. . . . . [redacted]

BOARD OF EDITORS

EDITOR . . . . . [redacted] (963-1103)

Computer Systems . . . . . [redacted] (963-1103)
Cryptanalysis. . . . . [redacted] (963-5238)
Cryptolinguistics. . . . . [redacted] (963-4382)
Information Resources. . . . . [redacted] (963-3258)
Information Science. . . . . [redacted] (963-3456)
Information Security . . . . . [redacted] (972-2491)
Intelligence Reporting . . . . . [redacted] (963-5068)
Language . . . . . [redacted] (963-3057)
Linguistics . . . . . [redacted] (963-4814)
Mathematics. . . . . [redacted] (963-5566)
Puzzles. . . . . [redacted] (963-6430)
Science and Technology . . . . . [redacted] (963-4958)
Special Research . . . . . .Vera R. Filby (968-5043)

Classification Officer . . . . . [redacted] (963-5463)
Bardolph Support . . . . . [redacted] (963-3369)
Macintosh Support. . . . . [redacted] (968-7315)
Illustrator. . . . . [redacted] (963-3360)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, NORTH

If you used a word processor, please include the floppy or cartridge with your hard copy, with a notation as to what computer, operating system, and software you used.

via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five: note: no 'o')

via ALLIANCE, send to:
PLBROWN [note: all caps]
attn: CRYPTOLOG

Always include your full name, secure phone, organization, and building.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, NORTH
Please do not phone.

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012034

HAIRCLOTH

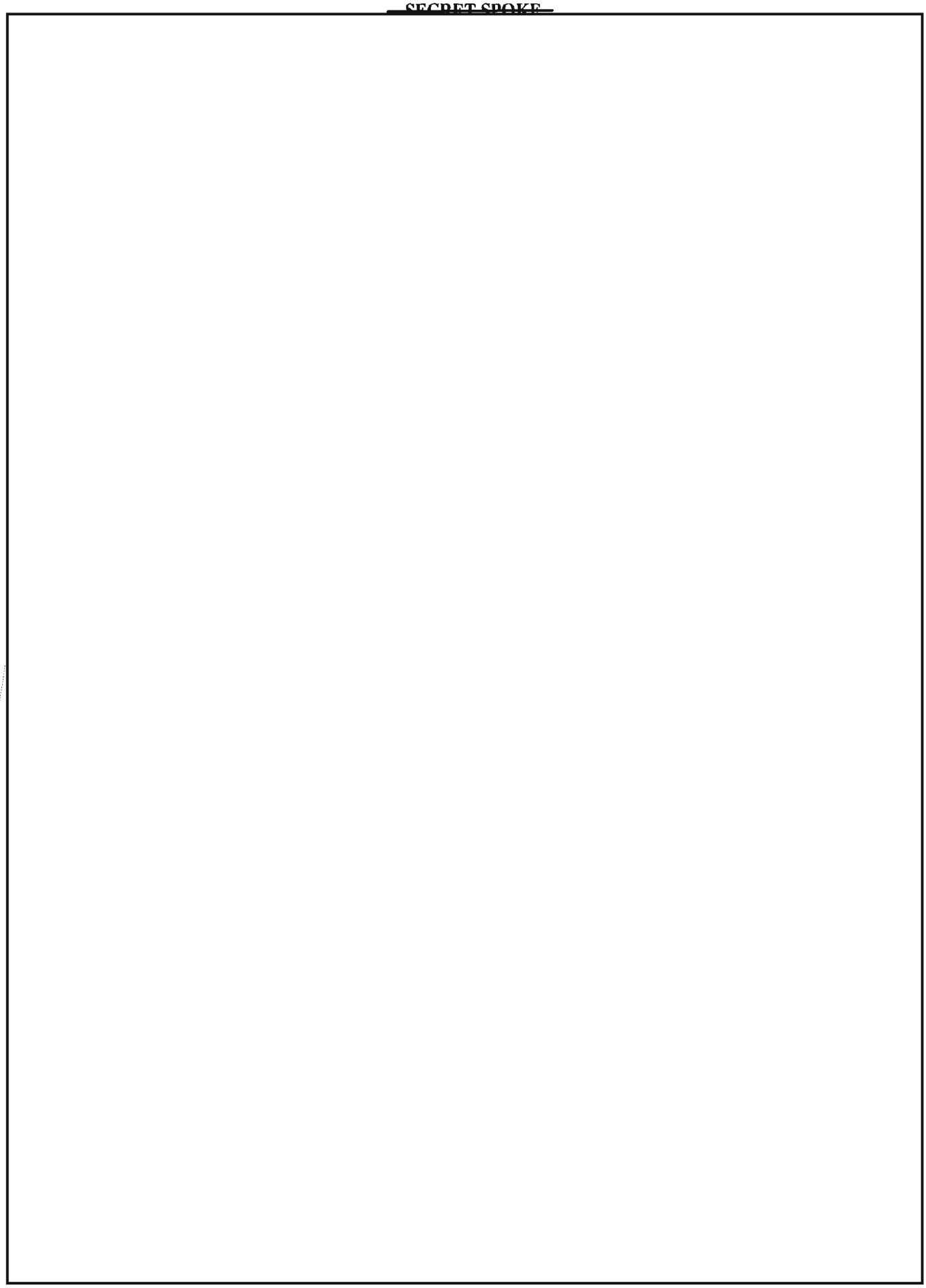
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4012034

EO 1.4.(c)
P.L. 86-36

DOCID: 4012034

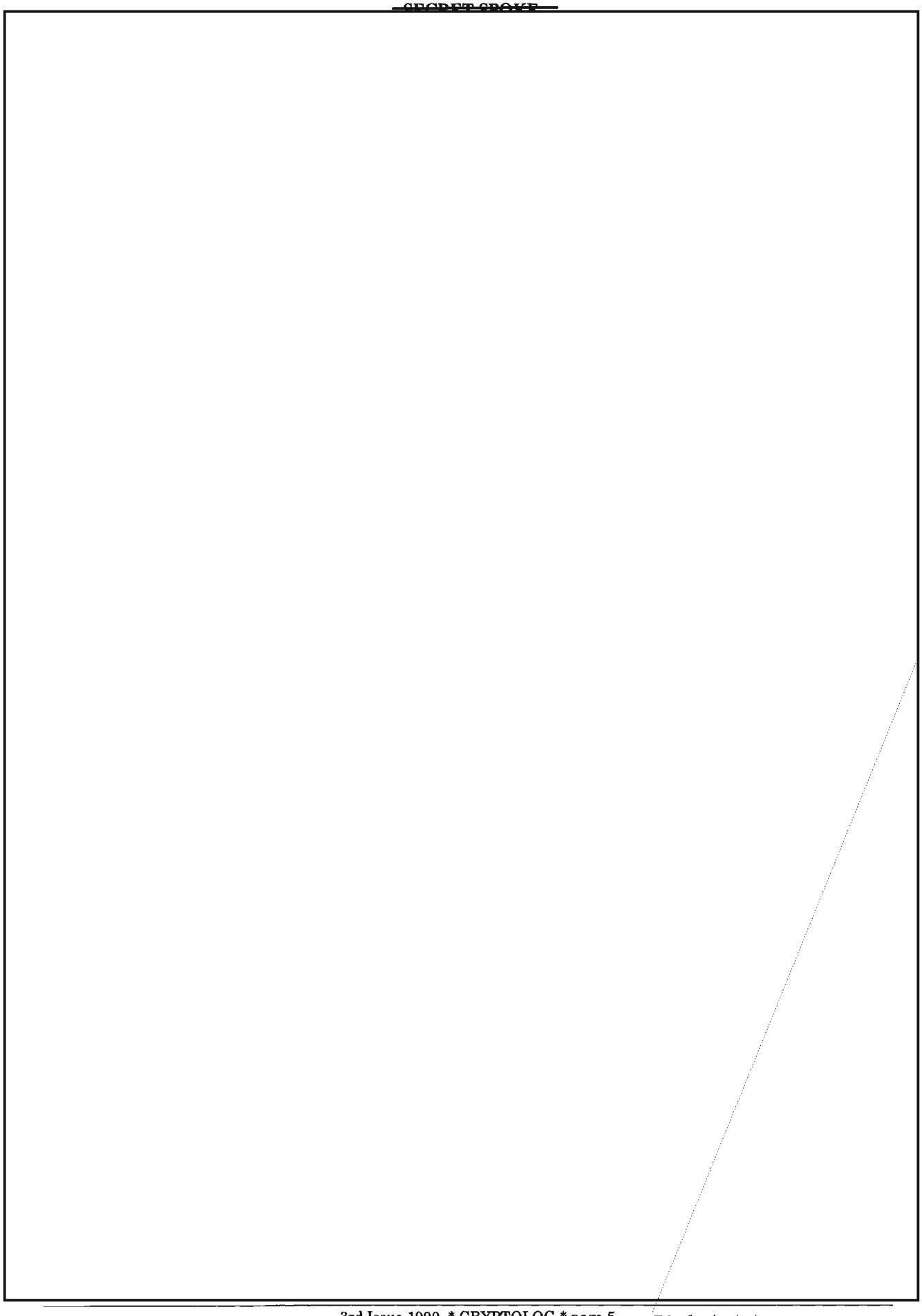


EO 1.4.(c)
P.L. 86-36

DOCID: 4012034

EO 1.4.(c)
P.L. 86-36

DOCID: 4012034



EO 1.4.(c)
P.L. 86-36

DOCID: 4012034

SUBSCRIPTION TO CRYPTOLOG

- ❒ Please enroll me as a new subscriber
- ❒ Please check my current mailing address
- ❒ Please change my mailing address
- ❒ Please change my name
- ❒ Please remove my name from the mailing list because I am
  - ❒ retiring or resigning
  - ❒ going to a field site
  - ❒ taking long-term training
  - ❒ too busy to read CRYPTOLOG (though I know I'm missing a lot)

P.L. 86-36
EO 1.4.(c)

OLD NAME AND ADDRESS

_____
Name (Last, first, mi)

_____ _____
Org *Bldg*

CURRENT OR NEW NAME OR ADDRESS

_____
Name (Last, first, mi)

_____ _____
Org *Bldg*

Mail to: **Editor CRYPTOLOG**
P1 NORTH

DOCID: 4012034

Asphalt and related bitumens (native):					
Bituminous limestone & sandstone & gilsonite	short tons	1,980,562	$8,879	1,918,748	$8,561
Carbon dioxide, natural (est.)	1,000 cu. ft.	1,109,530	191	1,194,836	144
Coal: Bituminous and lignite	thous. short tons	602,932	3,772,662	560,505	2,795,509
Pennsylvania anthracite	thous. short tons	9,729	105,341	10,473	100,769
Helium: Crude	thousand cubic feet	4,030,000	47,992	3,992,600	46,843
Grade A	thousand cubic feet	647,000	17,405	759,800	21,599
Natural Gas	million cubic feet	21,920,642	3,745,680	20,698,240	3,455,615
Natural gas liquids:					
Natural gasoline and cycle products	thousand 42-gal bbls.	206,305	603,024	201,784	603,084
LP gases	thousand 42-gal bbls.	399,611	672,088	378,457	498,927
Peat	short tons	526,000	5,986	565,760	7,055
Petroleum (crude)					10,426,680
Total mineral fuels			$20,152,974		17,965,000
Nonfuels:					
Abrasives	short	134		1	$600
Asbestos	short tons	125,314	10,696	125,936	10,648
Barite	Thousand short tons	854	12,800	1,077	15,753
Boron minerals	thousand short tons	1,041	86,827	1,020	81,261
Bromine	thousand pounds	349,748	60,560	391,883	87,990
Calcium-magnesium chloride	short tons	[4]	[4]	[4]	[4]
Cement: Portland	thousand 376-lb. bbls.	381,001	1,268,718	400,883	1,284,600
Masonry	thousand 280-lb. bbls.	21,275	67,537	23,253	69,106
Natural and slag	thousand 376-lb. bbls.	[4]	[4]	[4]	[4]
Clays	thousand short tons	53,932	258,332	58,694	264,415
Emery	short tons	[4]	[4]	[4]	[4]
Feldspar	long tons	[4]	[4]	673,985	8,869
Fluorspar	short tons	269,221	13,923	182,567	8,411
Garnet (abrasive)	short tons	18,837	1,936	20,458	1,874
Gem stones (estimate)		NA	2,396	NA	2,390
Gypsum	thousand short tons	9,436	35,132	9,905	38,354
Lime	thousand short tons	19,747	286,155	20,209	280,736

UNCLASSIFIED FACTS

[redacted] *P05/SAO* P.L. 86-36

We make continual efforts to protect our classified facts to the degree that we sometimes forget to acknowledge the unclassified ones that should not be revealed outside of official channels. Of course, there is no way every unclassified fact with which NSA is associated could actually be compiled. Below is a list of unclassified facts that are most frequently asked about in the Operations Organizations and that fall in that category:

❒ The terms "signals intelligence" (SIGINT), "communications intelligence" (COMINT), "electronic intelligence" (ELINT), and "foreign instrumentation signals intelligence" (FISINT) when used out of context.

❒ Elementary principles of traffic analysis, military cryptanalysis and cryptography.

❒ Individual job titles and descriptions that do not contain information otherwise listed above as requiring classification. (NSA regulation 10-11 provides unclassified job titles and job descriptions.)

❒ The "fact of" overhead reconnaissance.

❒ The mere "fact of" SIGINT liaison or collaboration between NSA and GCHQ, CSE, DSD, GCSB, UKLO, CANSLO, AUSLO, or NZLO.

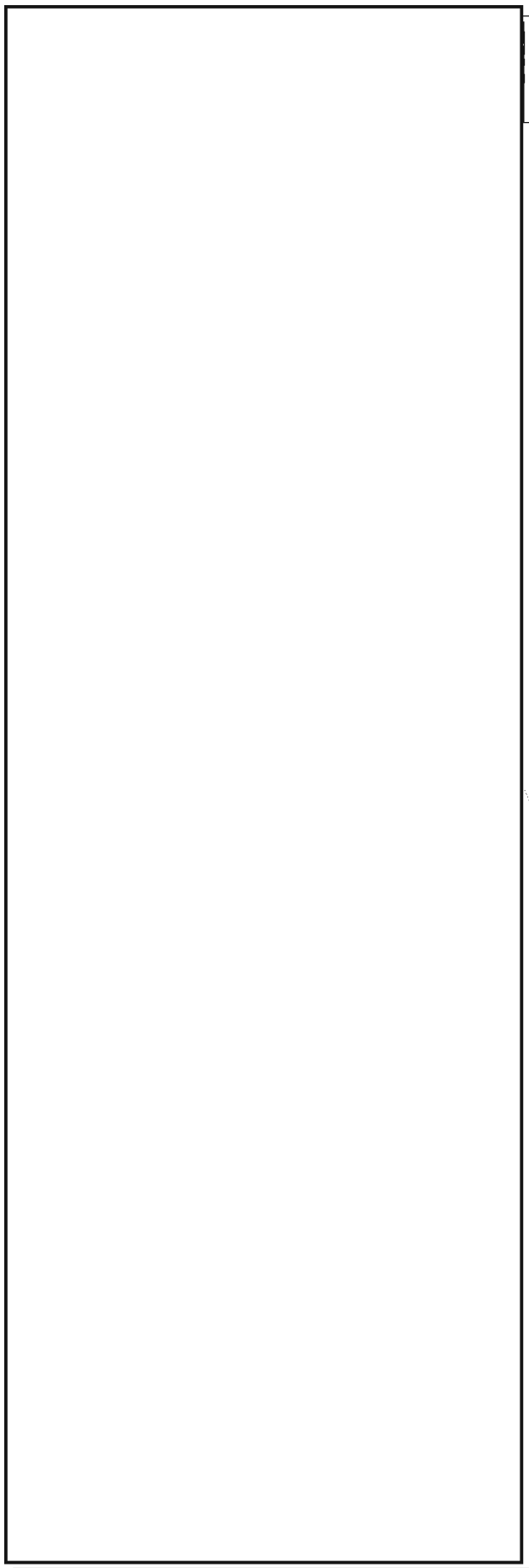
❒ The terms "NSA/CSS Representative Alaska," "NSA/CSS Representative Europe," "NSA/CSS Representative Pacific," [redacted] and their abbreviations.

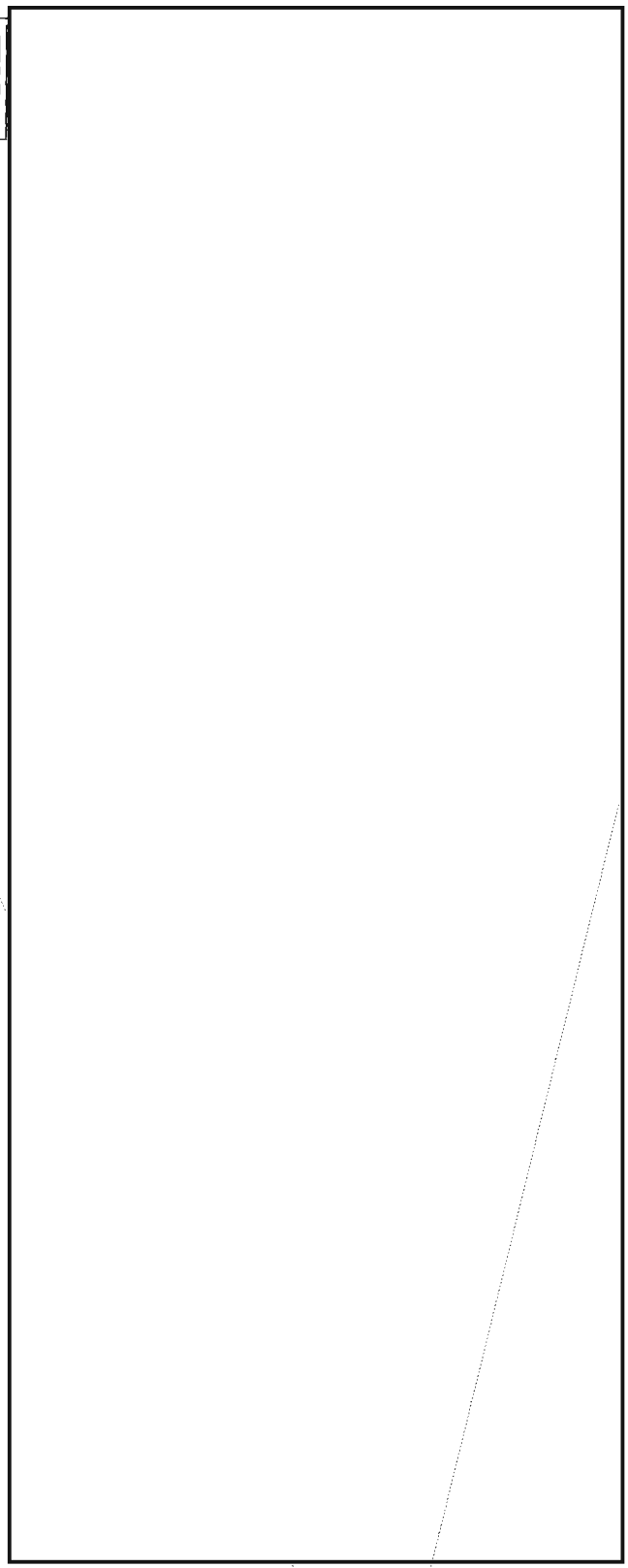
❒ Statements forwarded to contractor facilities or other government organizations which disclose the indoctrination status of individuals. This statement is to read: "The individual concerned is certified cleared and indoctrinated for access to TOP SECRET, Special Intelligence," and any other accesses should be abbreviated, such as TK, B, MC, LM, GG, etc.

❒ The caveat "HANDLE VIA COMINT CHANNELS ONLY" and combinations of, or other individual channel caveats, including those identifying the BYEMAN, TALENT KEYHOLE, or LOMA control systems. ❒

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012034





Extract from

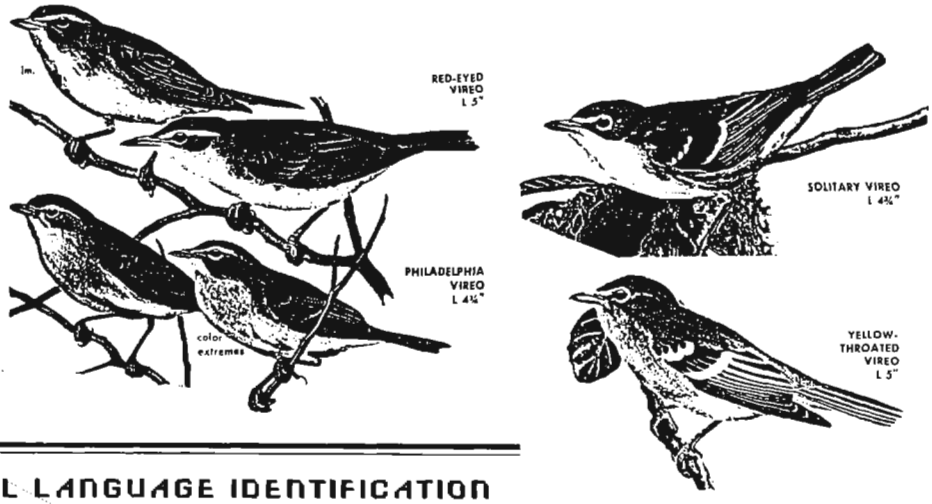
"National Cryptographic Habits"

by Preston Currier

Collected Papers on Cryptanalystic Diagnosis.

April, 1969. (S-194-074)

P.L. 86-36
EO 1.4.(c)



EO 1.4.(c)
P.L. 86-36

AURAL LANGUAGE IDENTIFICATION

~~(C-CCO)~~ The problem of identifying spoken languages at the Agency is an old one, as evidenced by the existence of the second edition (1958) of *A GUIDE TO SPOKEN LANGUAGE IDENTIFICATION,* Prod-03 Informal No. 10/2. More recently it was the subject of an article by [redacted] in *CRYPTOLOG*, December 1986, pp. 11-17, "The Language Identification Problem."

P.L. 86-36

~~(C-CCO)~~ When I returned to NSA in 1987 after an absence of 18 years, I was surprised to find it was more of a problem than ever, when [redacted] asked me if I had any ideas on how to solve it. After I had been thinking about it for a couple of months, she sent me a copy of a suggestion by [redacted] that had been adopted by DDO [C-547-85], stating that

[redacted]

[redacted]

(U) [redacted] had been exploring formal features in the same way that distinctive features are used in professional linguistic descriptions, and had even been working by computer to systematize them. But that approach would not work in the situation Barbara had described.

(U) My initial approach was also based on an analysis of distinctive features, but relying on features that are more subjective than scientific. There was one overriding reason for this approach: I had noticed years before that Polish and Spanish sound the same to me when I am far enough away not to distinguish words; this is because both languages are accented predominantly on the penult, the second syllable from the end of the word. I'm told that English and Norwegian have a similar relationship and sound alike if not heard distinctly.

(U) Thus I started on the premise that languages might be classified by their aural impression on a listener, so I compiled a list of seven

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

classes of language based on predominant accentuation, tone, and vowel, and consonant characteristics. Though some of the principles were useful, this scheme eventually proved to be too cumbersome to be practical. My original analysis is shown in the chart on the next page.

(U) At about this point it became obvious that this process might produce a scheme valid for some uses but not for this purpose. Additional criteria could have been added to form more groups, and more distinctive ones, such as the exact type of stable accentuation, nasality, clicks, retroflex consonants, the presence of "th" sounds, etc., but they would have made the scheme even more complex and unwieldy to be handy.

(U) My next approach was based on field bird study. I used to be able (before losing a lot of my hearing) to identify more than 100 Maryland birds by their songs and calls, sometimes only by one feature which occurs in a stream of notes. At times a family of birds, rather than a single species, can be identified before it is clear what the species is: Vireos are a good example. At other times different species have seemingly identical sounds, so the observer has to listen until a distinctive sound is uttered. In many ways this parallels human language: we do not understand any particular "words" used in bird communication, and perhaps we do not need to know any words in any particular language to identify the language; perhaps we can identify languages by subjective means.

(U) This has a parallel in field ornithology as well. American ornithologists insist that diagnostic markings be carefully observed for positive identification; this would be equivalent to identifying a language by words which are understood. British ornithologists accept the principle of GIS, meaning General Impression and Size; this corresponds to the subjective impression made by the sounds and mannerisms of the call.

(U) Take the bird family Vireonidae, for example. Vireos are small birds, olivaceous and grayish in color, often hard to find and to see clearly, and best identified by their songs. Six vireos can be found in Maryland. Four have predominantly robin-like phrases (comparable to a language family) and can be identified by song as follows:

> *Red-eyed vireo:* short, frequently repeated phrases [This can be compared to Chinese].
>
> *Solitary vireo:* short phrases, slower than red-eyed [This can be compared to staccato Hungarian phrases].
>
> *Yellow-throated vireo*: diagnostic "three-eights" note [This "distinctive" feature can be likened to clicks in Hottentot].
>
> *Philadelphia vireo*: very close to red-eyed vireo, but more mellifluous and slower. [Comparable to Estonian "overlong" vowels].

(U) The ability of the listener to identify the language is what is important, even if the guidelines are unscholarly. If linguists find (as some have) that Japanese sounds like Turkish, but is more "singsongy", the only question is: Does it work? Subjectively we find that for some people Greek is thin and Armenian is thick, Romanian is like Italian with more sh sounds, Portuguese is like Spanish spoken with a cold, and even that "Zulu reminds me of Italian." Whatever works is correct.

~~(FOUO)~~ Eventually I reorganized my findings and in the fall of 1987 presented them in a course at NCS listed as LG-220, Aural Identification of Languages, to ten students. The final course was organized with a combination of three potential approaches: distinctive features, subjective impressions, parallels with bird calls.

~~(C-CCO)~~ The results of the session were mixed. Everyone seemed able for a time to distinguish some of languages we started with. Some, who had to deal directly with collection in the field during the period spanned by the course, found that they could isolate their priority languages and eliminate others quite well. Other students could not identify certain languages at all.

DOCID: 4012034

Initial Distinctive Feature Analysis

Class 1/2 vowels

	glottal	dominant accent	long vowels	tone	example
1	+	-	-	-	Tagalog
2	+	-	+	-	Spanish
3	+	-	+	+	Hungarian
4	+	-	-	-	+ Lingala
5	-	+	-	+	- Ilocano
6	-	+	-	-	- Kurdish
7	-	-	+	-	- French
8	-	-	-	-	- English
9	+	-	-	+	- Serbian

These criteria were based on my observation of how I hear the languages.

1/2 vowels means broadly that there are many open syllables (i.e., ending in a vowel rather than in a consonant), which can make a language sound either very deliberate or fast.

Glottal refers to any sound deeper in the throat than normal American English sounds and therefore includes glottal stops and pharyngeal sounds.

Dominant accent means a predominant emphasis on the first, last or penultimate syllable.

Long vowels refer to languages where long and short vowels are phonemically different, sometimes difficult to determine without knowing the language because vowels are often lengthened for the sake of emphasis.

Tones refer to higher and lower pitches used in a consistent manner. ~~(S-CCO)~~

(U) Some members of the class never did accept the fact that the purpose of the course was immediate recognition of the language being heard. They wanted to follow their own instincts to identify languages by words which they understood. The great drawback here, as [redacted] has already pointed out in the paper mentioned above, is that there are recognizable cognates in many languages, so language identification based on words alone is flawed from the start.

P.L. 86-36

(U) Despite the early mixed results and mixed student evaluations the course has continued, and several sections are taught every year, mainly to students going on TDY and PCS. Happily, the two sessions given in FY90 received uniformly favorable student evaluations.

METHODOLOGY

(U) As is common in teaching practice, we try to go from the familiar to the unknown. Everyone seems to recognize French—why or how that is, I'm not even sure of the correct question to ask here—and almost everyone is quite sure of German, Spanish and Chinese. From there on we are on less secure ground.

(U) I begin by classifying the main accentuation pattern of non-tonal languages with practice for each type. We use four patterns:

first syllable (as in Hungarian, Czech, Estonian),
penult (Polish, Spanish, Italian),
last syllable (French, Turkish, Hebrew) and
mixed (Russian, Tagalog and Albanian).

(U) From here we move on to other features which are not quite so distinct:

nasality (French, Portuguese),
long vowels (Hungarian, Finnish),
palatalization (Russian, Chinese),
retroflex consonants (Hindi, Tamil),
tone (Asiatic: Chinese, Vietnamese; and African: Bantu languages, Malagasy), etc.

(U) The major Romance languages are presented as follows:

French nasal and final accentuation
Spanish penult accentuation
Portuguese nasal and penult accentuation
Italian penult accentuation and long consonants
Romanian like Italian but mixed accentuation and many sh and sht sounds.

(U) Some languages are hard to characterize, i.e., all Slavic languages have many palatal consonants, but Russian adds a great deal of vowel palatalization. Unfortunately the only way to classify Ukrainian is by the lack of this vowel palatalization, and ultimately perhaps it can only be recognized by those who already have a knowledge of Russian.

(U) The major Slavic languages are presented as follows:

Czech, Slovak accented on first syllable
Polish accented on penult
Serbo-Croatian mixed accent but lilting quality suggesting a tone language
Russian a great deal of palatalization, ya, ye, yo and yu syllables
Bulgarian t sounds in many final syllables, t, ta, te, to
Ukrainian like broken Russian, less palatalization

~~(S-CCO)~~ It may seem at first glance that this is not enough information on which to base the identification of a language, particularly in view of the occasional problems which arise:

[redacted]

[redacted] But-more often, I am amazed at the ability of many students to identify a score or more of languages with facility after just a few hours of training.

(U) Arabic is identified mainly by the wa sound which precedes most clauses; while this is a word meaning "and", it is not presented as a word and knowing the meaning has no real effect on the ability to perceive it and interpret it as an Arabic feature.

EO 1.4.(c) P.L. 86-36

[redacted]

~~(S-CCO)~~ Recognizing language family is particularly important with creoles and pidgins.

[redacted]

~~(S-CCO)~~ At present we deal with about 50 languages per class, in two different, complementary ways: language families and geographic areas. [redacted] as a major member of the Romance family, but is also reviewed in terms of Central Africa, North Africa and the eastern Mediterranean where Lebanon is located.

~~(S-CCO)~~ The problems involved in the range of languages also include several concomitant

EO 1.4.(c)
P.L. 86-36

situations. One of these is the use of the same language in distinctive dialects in neighboring countries, i.e., Farsi in Iran and Dari in Afghanistan; at present only a person who knows the vocabulary and/or syntactic differences between these two dialects can differentiate them. This

[redacted]

~~(FOUO)~~ We work principally with language tapes provided by the Voice of America because they are clear enough to teach the principles we operate with. We add other languages as required. Even so, the range of languages available does not meet all of NSA's possible needs, and we are constantly looking for new language specimens.

~~(FOUO)~~ Originally, we began by using Jack Gurin's Language Library of recordings (found in the NSA library in the past and now under P16), but many of them were poor because they were recordings of classes; the teacher often used "caretaker" language because of the weaknesses of the student, and the student often had a poor pronunciation. Others were ad hoc conversations between two speakers of a language who had never met before, and the sense of contrivance and artificiality comes through the recordings, making them seem unreliable as real native specimens of the languages.

[redacted]

be sent to collecting stations at home and overseas, as requests keep trickling in for more help in language identification.

(U) Retention is one problem which we face along with all other areas of language training. To enable students to practice and review at home, we have found it possible with our more recent equipment to make special unclassified cassette tapes with many language specimens.

~~(C-CCO)~~ I have speculated about other approaches that might be tried for certain languages. One would be for students to learn the first one or two lessons of some language courses which are on tape or records; in this way they could combine both the word recognition method and the subjective impression method. Two obvious drawbacks are an increase in study time, several hours per language, and the lack of such material in a great many possible target languages.

(U) Another possible method is the time-based versus syllable-based feature, the first of which accounts for the amount of slurring and the second for the degree of clarity and/or staccato in a language. This characteristic requires further investigation.

~~(S-CCO)~~ [redacted] has developed a remarkable computer program for recognizing graphic specimens of languages (I say remarkable because I tested it very successfully with

[redacted]

He believes it can be applied to spoken language after some refinements have been made; if so, and if a small enough device can be developed, the identification problem could be almost completely solved, and LG-220 would have little reason for continued existence.

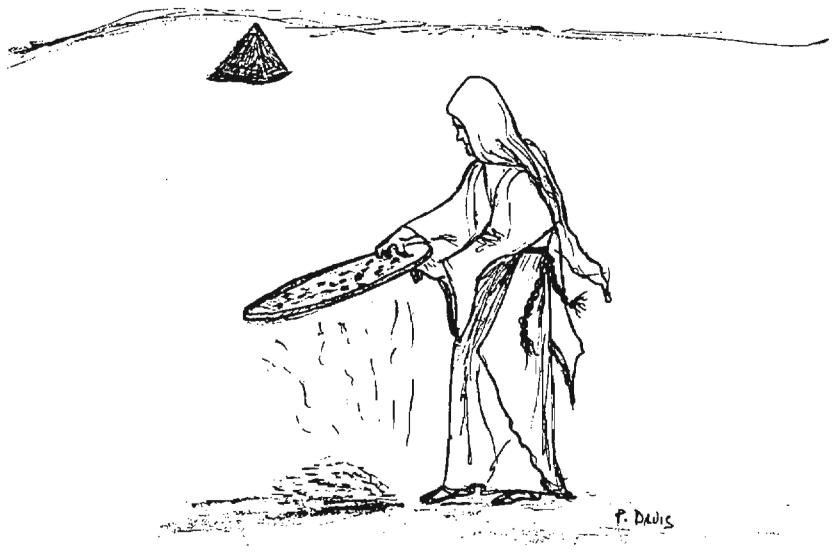
~~(FOUO)~~ Until then, however, LG-220 is one of the Agency's solutions to the formidable problem of aural language identification. ❐

P.L. 86-36

Sifting Wheat from Chaff

P.L. 86-36

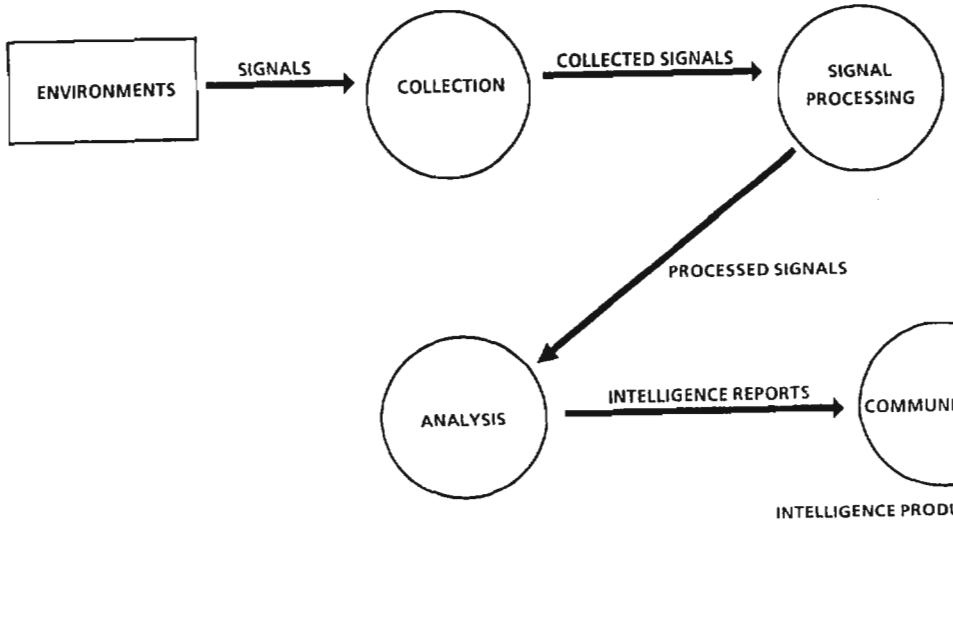
R5



P.L. 86-36

DOCID: 4012034

Fig. 1. DATA FLOW



~~FOR OFFICIAL USE ONLY~~

EO 1.4.(c)
P.L. 86-36

(U) Developing a good characterization of filtering tools will lead to identifying holes and gaps in technological capabilities and to identifying unfulfilled requirements that can be satisfied without new technology. This should not be construed as an exercise in system engineering, system or device design, or building and assembling equipment to do SIGINT.

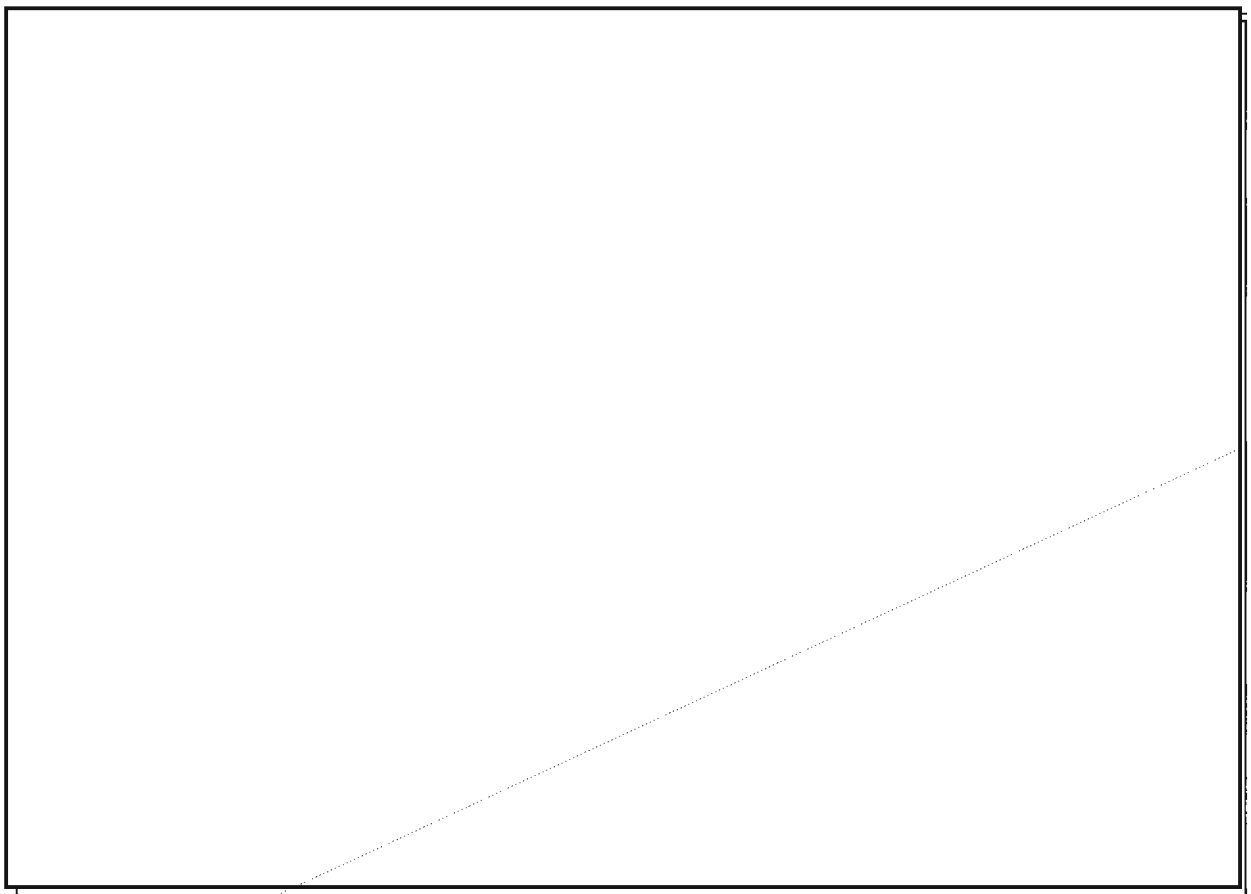
(U) The key to characterization is clear descriptions of data structures that are passed in the SIGINT system and how they are operated on to produce an intelligence product. Once a function is well understood and described, then science and engineering can proceed with specifics as to what can be done now, and what needs more R&D.

(U) In Figure 1 there is description of the SIGINT system at a top level with a data flow diagram. The problem with this "diode" concept of unidirectional flow is that it displays only the reaction to a signal situation. It does not display a system that must produce product, first based upon who needs data, then the source of the data, and finally, how the data are to be prepared and delivered.

(U) A more accurate snapshot of the SIGINT system is presented by the data flow diagram in Figure 2. The point here is not that Figure 2 is the only way to characterize the SIGINT process, but that the SIGINT System should be shown as a process where the activities interact, share data, and filter (make decisions about) all kinds of data. It is a data flow diagram that stresses the "goes intos" and "goes out ofs" without dwelling on the devices that transform the data. The symbols as shown on the key are defined as follows:

An OUTSIDE INTERFACE is a process or organization lying outside the context of a system that is an originator or receiver of system data;

~~SECRET~~



~~FOR OFFICIAL USE ONLY~~

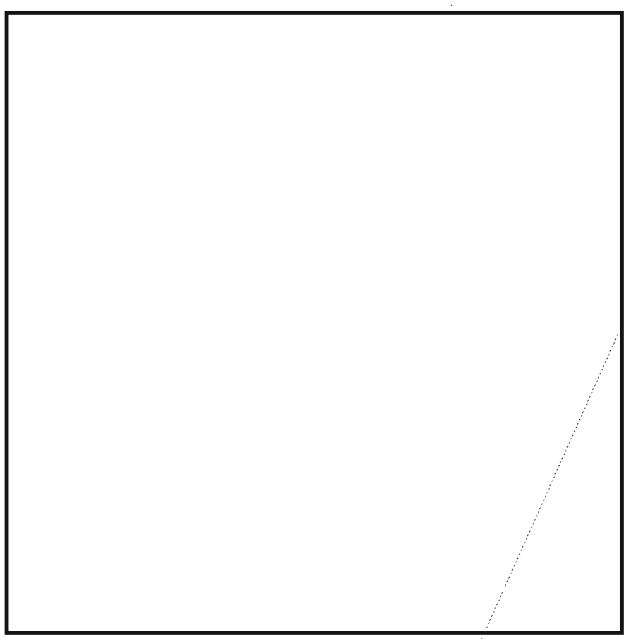
P.L. 86-36

An ACTIVITY is a transformation of input data flow(s) into output data flow(s);

STORAGE is a data store; and

DATA FLOW is a pipeline along which information of known composition is passed.

(U) Data flow diagrams can help characterize what filtering must be done because SIGINT product is produced from data that has been transformed. We must consider data structures in motion, data structures at rest, and the necessary ways to act on them. The diagram shown is only an approximation. The most effective diagram shows how the activity is carried out and has a good data dictionary that correctly describes what the data should be and its form. Filtering may have to include other data to be fused to the flow for good product output.



~~(C CCO)~~ As there are standing requirements for documenting NSA-acquired systems, there is a chance that current filtering techniques are fairly

EO 1.4. (c)
P.L. 86-36

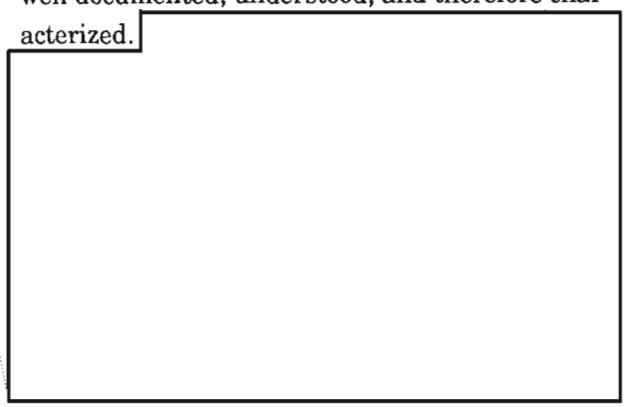
~~SECRET~~

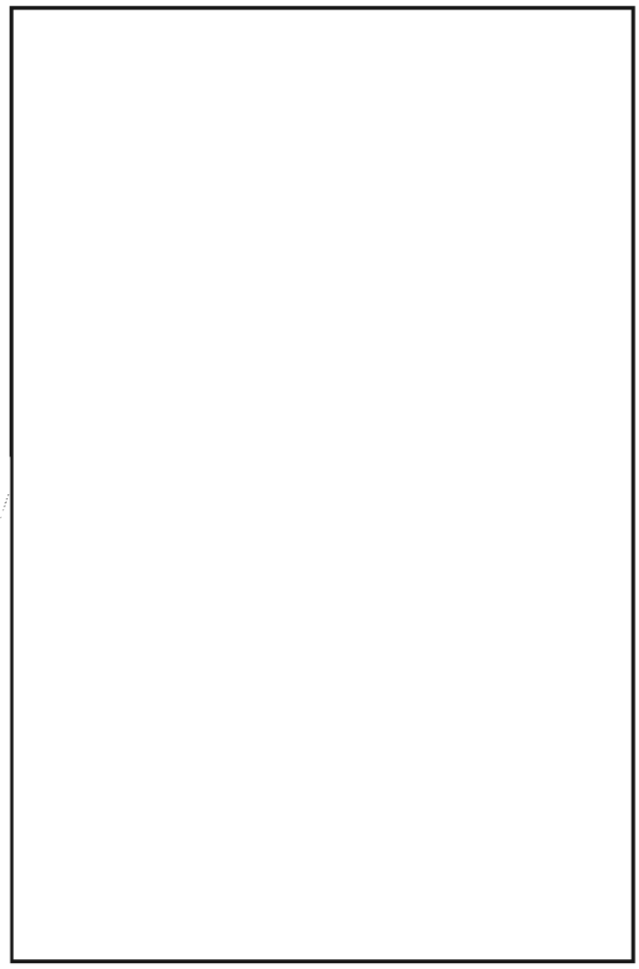
~~HANDLE VIA COMINT CHANNELS ONLY~~

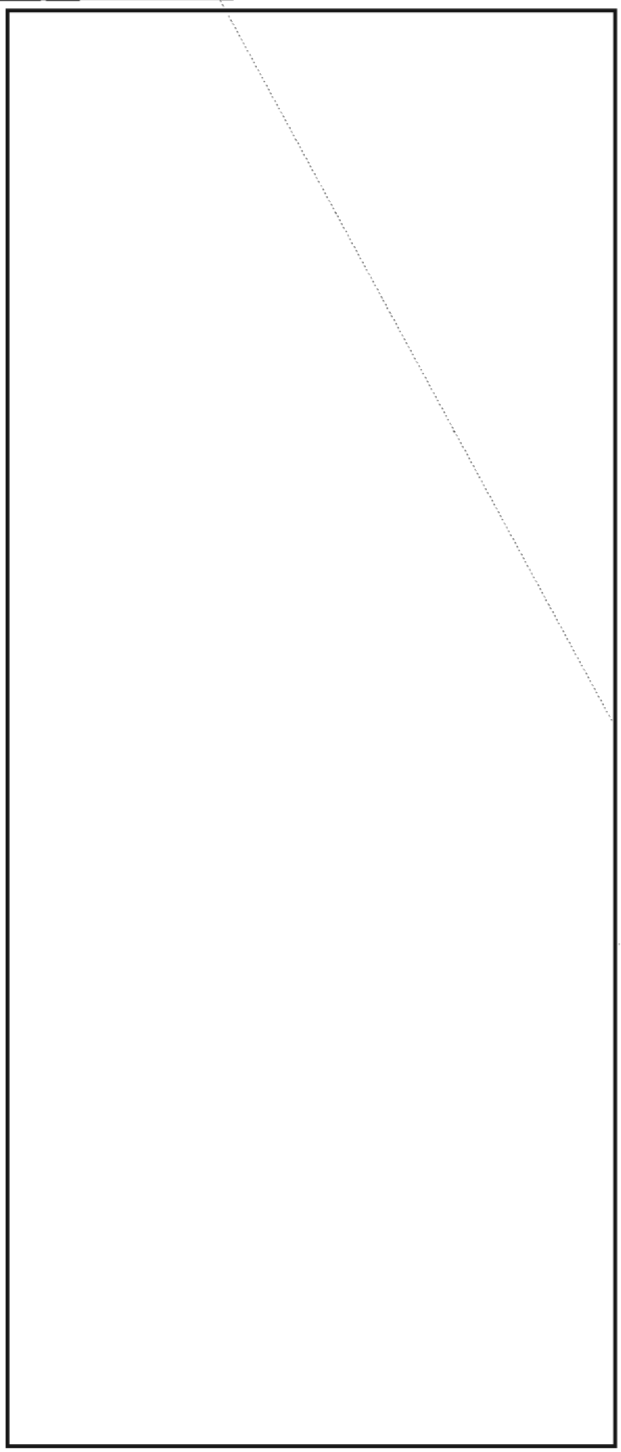
DOCID: 4012034
P.L. 86 36

EO 1.4.(c)
P.L. 86-36

well documented, understood, and therefore characterized.







(U) It should be no surprise that a complete solution to the entire SIGINT problem may be too big to accomplish initially. But we can at least try to see how much of the problem we can grasp, what problems we can identify, and how we can attack these problems.

~~(C-CCO)~~ Currently, we are looking at the following:

LOOKING AHEAD

~~(C-CCO)~~ Is there a stimulus to invent new filtering techniques? Do we have to get serious about characterizing the filters we have, or are they already characterized? The author is hearing all kind of pleas for help [redacted] Yes there is a need, but it is hard to believe enough people have a good grasp of what the

P.L. 86-36

DOCID: 4012034

whole SIGINT System really does to glean out the needed intelligence product (the author knows he doesn't have such a grasp).

~~(FOUO)~~ NSA folks must help each other to better understand the problem of SIGINT filtering from an operational as well as a technological point of view. Some of us have problems right here and now with which we are trying to cope (sometimes all by ourselves). Others of us want to talk about what we can do in the future. At times neither group talks to the other, because they are too busy, and some are blinded by their own view of what time tag is most important. Obviously, both aspects have to be considered together to foster a better mutual understanding, a foundation of experience, and some assurance that the current problem of each new day is not a bigger and bigger compounded predicament of the past and present.

~~(FOUO)~~ Is it clear that we'd better get a lot smarter about sifting wheat from chaff if SIGINT is to fulfill its potential? That is an easy question to answer. The harder one is, will the right folks stand up and be counted when the call goes out for input to strategic planning for aspects of the filtering problem, or will there continue to be fragmented efforts to solve such problems without the benefit of both an operational and technological point of view?

To the Editor,

CRYPTOLOG is still very much a winner, providing a very enjoyable break in work when it arrives.

At this time I'm writing to ask for a copy of the do-it-yourself packet on viewgraph preparation described in the 1990 2nd Issue. (With all the high-tech stuff in the National Cryptologic School, where I have been since December, I still find occasions when viewgraphs are the best things to use in my endeavors!)

Please send me a copy of that packet, addressed:

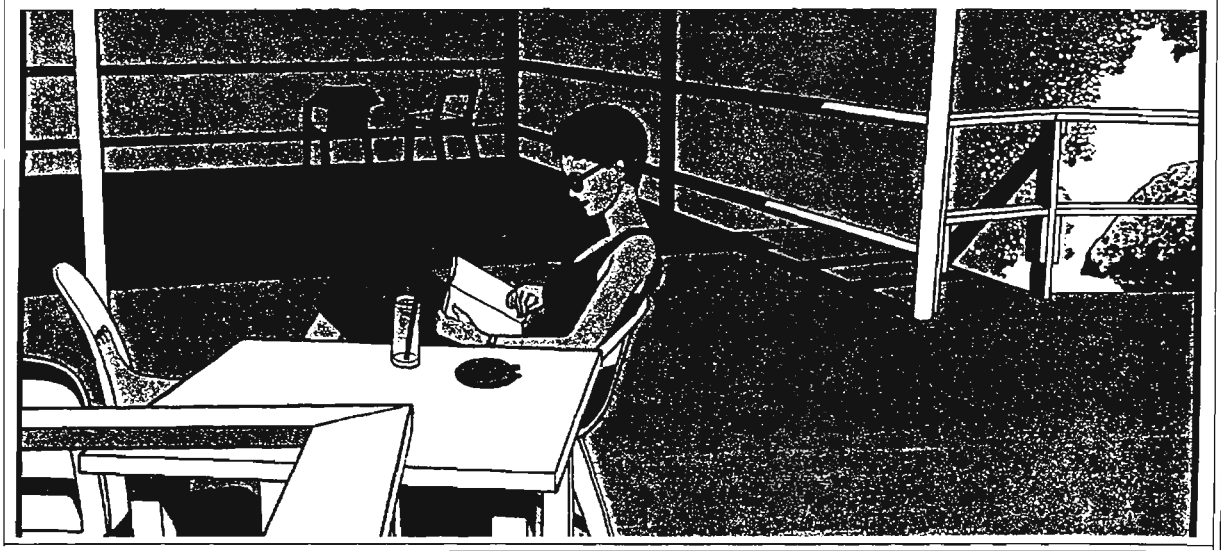
[redacted]
E9
ITB

P.L. 86-36

Thanks, and warm regards.

unclassified

CRYPTOLOG is a classified publication. It may not be read in the cafeteria or in other insecure areas.



DOCID: 4012034

THE MAYAGUEZ INCIDENT

[redacted] P.L. 86-36

(U) On 12 May 1975, the SS *Mayaguez*, a US merchant vessel, was seized by Cambodian Communist forces in the Gulf of Thailand. Within two days US Air, Naval and Marine forces launched a rescue operation against Koh Tang Island where the ship and its crew were believed to be held. During this operation, the *Mayaguez* was recaptured and its crew returned. This article described the actions taken by USM-7, Ramasun Station, Thailand, and its personnel in support of the operation.

~~(C)~~ In support of the operation, on 13 May 1975 NSA declared SIGINT Alert One "Vacater" to be used on all SIGINT product relevant to Gulf of Thailand operations. USM-7 was tasked with providing Tactical Reports (Tacreps) and Spot Reports on Cambodian communications relating to the disposition of the SS *Mayaguez* and its crew and to US rescue attempts. In addition, detachments of USM-7 personnel were deployed to several other locations to support these operations.

~~(SC)~~ At USM-7 itself, cast iron (24-hour continuous) cover was provided on eight Cambodian Southwest Region and mainline Morse links. As a result, it issued a total of five Tacreps and four spot reports by the end of the operations. The reports discussed Cambodian defensive activities as well as the results of US actions. Meanwhile USM-7 maintained contact with US Army Security Service, providing informal progress reports to its commander.

~~(SC)~~ The same day the alert was declared, the station commander summoned the NSA Cambodian Technical Representative to USM-7, whom he requested to identify four Army Cambodian linguists for immediate deployment [redacted] (It is interesting to note that the summons came via a two-way radio link, the same one employed at other critical times such as the evacuation of US personnel from Phnom Penh prior to the fall of Cambodia.) Their mission was to search for, intercept, record, translate, and report all Cambodian VHF voice communications reflecting reaction to the recovery efforts.

~~(SC)~~ Within one hour of that initial contact, the five linguists (four Army and the NSA tech rep) and their working aids were flown directly from the nearby Thai air force base at Udorn [redacted] by a US Air Force C-130. Shortly thereafter, the linguists began search efforts and succeeded in isolating several unidentified Cambodian voice links. This search and development effort involved the [redacted] mission, a Strategic Air Command U-2R reconnaissance aircraft.

~~(S-CCO)~~ During the three-day operation, two intercept positions were manned on a 24-hour basis, one for search and development of additional Cambodian voice links, and the other for monitoring the most active frequencies. Immediate one-liner Tacreps were issued through a joint Army-Air Force effort.

EO 1.4.(c)
P.L. 86-36

DOCID: 4012034

~~SECRET SPOKE~~

AREA OF OPERATIONS DEPICTING RELEVANT LOCATIONS

~~SECRET SPOKE~~

~~(S-CCO)~~ The text on which each Tacrep was based was recorded by one linguist, and immediately transcribed and translated by another linguist to provide the follow-up Spot Reports. After the US recovery operation began, [redacted] issued ten Tacreps and nine Spot Reports on the basis of Cambodian voice intercepts. The reports included reflections of Cambodian actions, intentions, and responses to US operation. During the entire Mayaguez operation, all reflections of Cambodian intent were relayed to USM-7 for possible follow-up traffic in HF Morse or voice.

~~(S)~~ In the early morning hours of 14 May, three additional Army Cambodian linguists at USM-7 were briefed, equipped, and sent to [redacted] as interpreters, to assist in US Navy and Marine tactical operations at Koh Tang Island. Their mission was to use bullhorns to advise the Cambodians that the only purpose of the operation was to recover the *Mayaguez* and its crew.

EO 1.4.(c)
P.L. 86-36

~~(S)~~ Of the three linguist sent, only one was successfully deployed to the island, but he was unable to establish contact with the Cambodians. This linguist was later rescued from the island along with the remaining Marine forces approximately eight hours after their deployment. The two other linguists were aboard helicopters that had been damaged by small arms fire and were forced to return to the Thai mainland.

~~(S)~~ On 15 May, another team of three Cambodian linguists was also sent [redacted] After the *Mayaguez* was rescued, when the US prepared to launch a search-and-recovery mission for the US personnel missing in action, the linguists [redacted] prepared a Cambodian text for broadcast and a possible leaflet drop to inform the Cambodians of the mission. But the Joint Chiefs did not concur, so it was not done. The linguists remained on alert aboard ship until their return to USM-7.

EO 1.4.(c)
P.L. 86-36

~~(C)~~ All the linguists deployed returned safely to USM-7 soon after the successful recovery of the SS Mayaguez and its crew on 14 May.

(U) Though the recapture of the vessel and its crew was successful, we were greatly saddened by the loss of our Army, Navy, Air Force, and Marine fighting comrades who gave their lives.

Originally published in the Field Information Letter, *March 1978*

DOCID: 4012034

P.L. 86-36

The Three Faces of Collection

The ongoing DDO restructuring is prompting discussion about what "collection management" is. I am offering my view of it in the hope that it can serve others as well as it has served me.

I believe that Collection management has three components:

◆ *the definition of collection requirements*; This is the process of deciding what we must have in order to produce the information required to satisfy our users' intelligence demands. THIS CAN AND SHOULD BE DONEONLY BY THE TARGET ANALYST.

◆ *brokering Collection*; This encompasses all actions between the statement of collection requirement and performing the collection task. It includes all organizations that traditionally identify themselves as "collection managers," e.g. 04 staffs, P5, A1, G8, B642, etc. Personnel of these organizations have the know-how to convert the collection requirement stated by the analyst into the arcane lingo of our various specialized collection systems.

The "broker" model, drawn from the commercial world, accurately parallels the functions of our "collection brokers:" rather than buying stock ourselves directly from a company, we call on a broker, a specialist who understands the mechanics of the stock market and makes our purchase for us.

As in the commercial world, NSA brokers should also be advisors to their "clients" on the best way to satisfy a requirement. The decision on the requirement; however, always rests with the target analyst. For example, I may call my stockbroker and say I want a long-term investment with a reasonable return and steady growth, "Please buy 100 shares of Amalgamated Circuit Inc." The broker may respond that this has good short term prospects, but for my long term requirements he recommends Integrated Widgets instead. But thenthe choice is mine.

Collection brokers are more than a bureaucratic cog in the cryptologic wheel; they are the human link between the target analysts and the collection system that assures we get the collection needed. This demands an understanding of how the collection systems function and an insight into the true nature of the needs of the target analysts. Regular dialog between analysts and brokers is essential for this process.

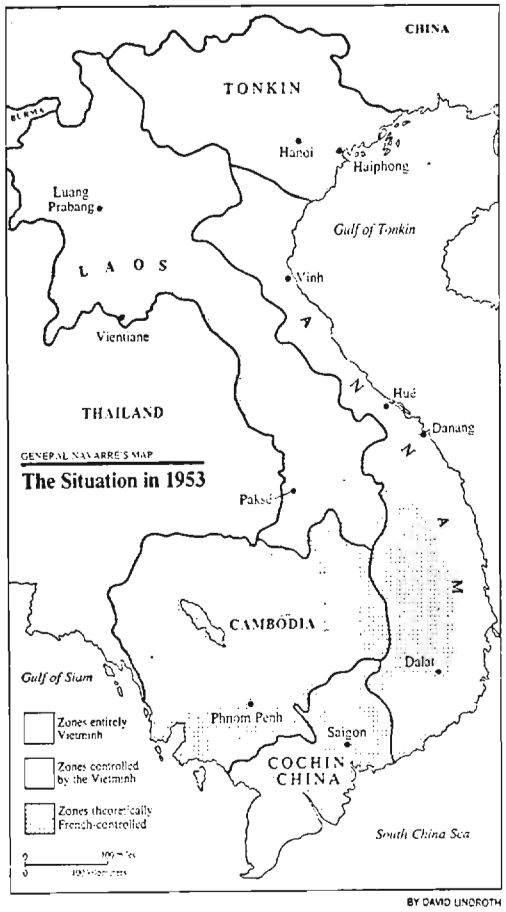
◆ *Collection Evaluation: This is* an assessment as to whether the collection provided actually satisfied the needs of the analytic organization. Perhaps the literal task was completely satisfied, in which case the broker would count it as a job completed, but only the target analysts can say if the intercept provided by the task actually produced the results they were seeking.

In summary, the three components of collection management are collection requirements definition, performed by the target analyst; collection brokering, performed by traditional collection management organizations and; third, collection evaluation, performed by both collection brokers (quantitatively) and target analysts (qualitatively). □

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012034

HOW IT STARTED



David Gaddy, D9

~~(S-CCO)~~ Last year marked the fortieth anniversary of the problem known for a long time as the "Viet Minh" problem. Forty years. That means 1949 and the days of the Armed Forces Security Agency, AFSA, forerunner of NSA. US involvement in Viet Nam has left a scar on the public conscience that has not yet healed. But it might be time for a little-known account of the SIGINT side.

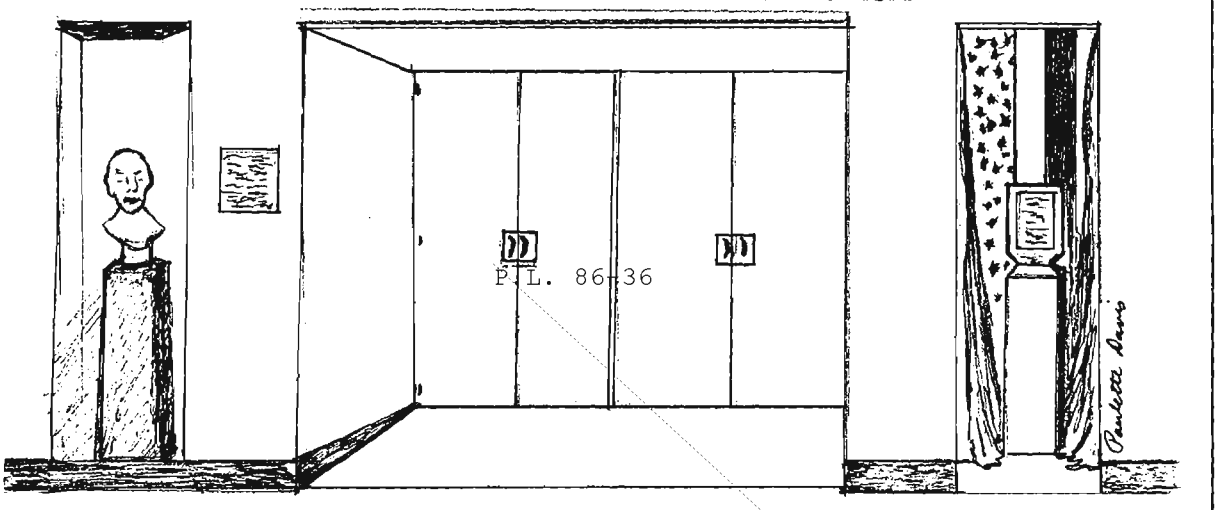
~~(SC)~~ All problems need some lore about their founding, and the Viet Minh problem, as it was called then, has an amusing (and instructive) story. The ingredients are an inquisitive young naval officer and some puzzling new intercept. It seems that USM-9 at Clark Air Force Base in the Philippines had intercepted some strange-looking material. The people at Arlington Hall who puzzled over such things concluded that it was plain text, but what language?

~~(SC)~~ Up pops the Lt (jg.), as I recall the story. He was the sort never to let time slip through his hands, and he often spent his time in the modest language library thumbing through the texts and becoming familiar with exotic languages. "Let me take a look at that," he evidently said. "You know," (combining his awareness of current events with his recollection of a text he had scanned) "I think this must be Annamese. That's the language of the Viet Minh—the people the French are fighting over in Indochina." "Oh?" was the reaction. "Well, since you seem to know so much about it, do you think you could translate these messages?" His hand called, what could the young officer do but agree, run get the glossary (or whatever it was he'd seen), and retreat into the sanctuary of a private spot. He emerged a while later with passable renderings.

~~(SC)~~ Yes, the language was Annamese (as some called Vietnamese at that early date) and the activity was "Viet Minh" (the already outdated name of Ho Chi Minh's anti-French movement). And, according to the story, the naval officer became the first American COMINT "unit" to work the problem.

~~(SC)~~ ~~It's~~ of passing interest, perhaps, that the original notation for such intercept was "VNG" to denote guerrillas in opposition to the government of Viet-Nam. Later it was changed to VH (for Viet Minh), and, as such, it flourished. The war ended in 1954-'55, with the "VH" withdrawing north of the Seventeenth Parallel, leaving a few well-chosen remnants behind. In the "second Indochina war"—the one we got involved in—we again dredged up "VNG" for the so-called "Viet Cong", Hanoi's campaign against Saigon, then later rolled them together as "VC," for Vietnamese Communist. ❐

DOCID: 4012034



How the Friedman Auditorium did *NOT* get its Name!

by [redacted] E9

I suggest that the NSA Auditorium be named the "William F. Friedman Auditorium" and that there be placed at the entrance of that auditorium a painting of Mr. Friedman and a case displaying a sampling of his published works, replicas of his awards, and photos of him with other cryptologic leaders and national figures.

Those words began Suggestion No. C–206–70, sent by me via NSA incentive awards channels on November 3, 1969, *the day after William F. Friedman died.* The idea came so naturally because I had grown up revering Mr. Friedman: I teethed on his *Military Cryptanalysis* works in the late 40's, as a GI studying with Lambros Callimahos, and helped on Callimahos's revision of those works in the early 50's, starting as a civilian in AFSA's Technical Division under Mr. Friedman.

The suggestion was acknowledged promptly by the M Awards Committee, in mid-December, but then nearly two years of **SILENCE** followed, to my great surprise. How naive I was then!

In late 1971, to learn the suggestion's status, I began an exchange of memos and phone calls with M awards people (and eventually the Deputy Director, Dr. Tordella) that continued until mid–1972. The awards people sought my patience, saying the original suggestion and a later duplicate had gone to the Deputy Director's office where each was "apparently lost." A note from me to Dr. Tordella was met with more **SILENCE**.

Finally, in early June, 1972, a memo came from the Incentive Awards Branch saying the suggestion (along with several others for honoring deceased NSA personnel) would not be adopted. It explained: "This decision apparently [sic] is based on the fact that the number of recent losses are regrettably high and that these, together with those that can be expected within the next few years, greatly exceed the number of potential memorials."

I thought "What an incredible excuse!" Mr. Friedman was, in effect, being viewed as some sort of a willy-nilly choice for memorialization from among an immense set of equally deserving people—not as the pioneer he had actually been.

Down but not out, I immediately sent the essence of the original idea to the Commandant of the National Cryptologic School (Frank Austin), suggesting that the National Cryptologic Course Center be named for Mr. Friedman. I justified it as recognizing his early development of comprehensive cryptanalytic training and his numerous contributions to the literature of cryptology. That was on the fifth of June, 1972; and was followed by **SILENCE** . . . .

~~FOR OFFICIAL USE ONLY~~

Some guys never learn: In June, 1974—as the fifth anniversary of Mr. Friedman's death approached—I re-sent the original suggestion through Incentive Awards channels, asking again that the NSA Auditorium be made a memorial to Mr. Friedman. This version was duly assigned Suggestion No. C–313–74 and, very promptly, "returned without action."

This time, the suggestion was characterized as failing to meet CSC and DoD criteria for Suggestion System processing. (Surprisingly, those criteria were said to have become effective about the time of the original suggestion in 1969, although that suggestion continued to be processed for another 2 1/2 years!)

I decided on one last shot. Since there was a new Deputy Director, namely, Mr. Buffham, I decided to get the 1969 suggestion directly to him. I did that in a personal memo sent on August 15, 1974. And, guess what? **SILENCE** again!

I was crushed. Five years of trying one method after another following Mr. Friedman's death, and still no memorial.

Imagine, then, my surprise and sense of achievement when, one April morning in 1975, I rode the escalator to the third floor in the Operations Building and found "WILLIAM F. FRIEDMAN MEMORIAL AUDITORIUM" over the auditorium doors. Though stunned, I composed myself enough to send another note to Mr. Buffham, this time thanking him for giving the project the support it needed, and expressing hope I might have the privilege of attending the dedication ceremony I presumed would follow.

By that time I should have been prepared for what followed, but I wasn't. Again, **SILENCE**! I heard nothing, a dedication was held, and I was not invited. And, when I recounted my five years of effort and ensuing disappointment to Mr. Callimahos, who participated at the dedication, my remarks got a blank stare.

It was then that I reached this shattering conclusion:

Designation of the NSA Auditorium as a memorial to Mr. Friedman had nothing to do with my suggestion!

BUT WAIT! That was 15 years ago. There's more . . . .

As I write this, it's late 1990, and I have just finished attending the agency's first "Cryptologic History Symposium," presented by NSA's Center for Cryptologic History (CCH). P.L. 86-36

"Bob! Long time no see. We were just talking about you a few days ago," [redacted] an old friend and CCH staffer also at the Symposium, said to me during a Symposium break. He went on to say something like "Tom Burns and I were looking at one of the Center's files containing material about you."

What was he possibly talking about? A trip to the Center produced the answer. There, in an aging file, was a November 1974 Memorandum signed by the Director, General Allen, addressed to ADIL, CNCS and ADPS, reading:

1. Attached is a suggestion for designating the NSA Auditorium as "The William F. Friedman Auditorium". . . .

2. For ADIL: Please arrange a plaque and painting of Mr. Friedman for the entrance of the Auditorium.

3. For CNCS: . . . investigate that aspect of the suggestion concerning photos, awards, publications, and other memorabilia . . . .

4. For CNCS/ADPS: . . . Since November is the fifth anniversary of Mr. Friedman's death, I hope we may be able to accomplish this action sometime this month.

And what was the Attachment? You're so right! It was a copy of the August 15 personal memo I sent to Mr. Buffham.

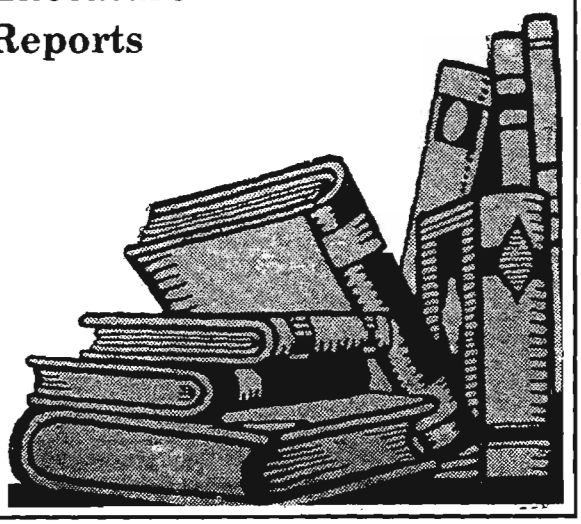
Now you know how the Friedman Auditorium DID get its name—and, finally, so do I.

□

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012034

Technical Literature Reports



Reported by: David Harris

Editor's Note: This material was submitted by the late author to be published in CRYPTOLOG as space permits. See "David Harris: In Memorium," 1st Issue 1990.

(U) Duncan Buell (1987) "Factoring: Algorithms, Computations, and Computers," *Journal of Supercomputing*, 1(2), pp. 191-216.

(U) M. C. Wunderlich & H. C. Williams (1987) "A Parallel Version of the Continued Fraction Integer Factoring Algorithm," *Journal of Supercomputing*, 1(2), pp. 217-230.

~~(C)~~ This issue of the *Journal of Supercomputing* was distributed free by Kluwer Academic Publishers at the AMS meeting in Providence.

Duncan's paper discusses "the computational structure of the most effective methods for factoring integers and the computer architectures--existing and used, proposed, and under construction--which efficiently perform the computations of these various methods." "The intent of this article is to use factoring and computers for factoring to provoke general thought about this matching of computer architectures to algorithms and computations."

(U) The article serves as a summary of some factoring algorithms and their implementations, especially parallel ones. The Wunderlich-Williams article is a description of an implementation of a parallel version of CFRAC on the MPP, together with a case study of the factorization of a 60-digit integer.

(U) James Reggia & Granger Sutton (1988) "Self-Processing Networks and their Biomedical Implications," *Proceedings of the IEEE*, **76**(6), June 1988, pp. 680-692.

(U) This is a survey paper on neural networks in medical applications. It may serve as a general introduction for the novice to the topics of neural nets, perceptrons, associative memories, Hebbian learning rules, energy minimizing networks, etc. It has a useful bibliography.

(U) Douglas Jones (1988) "Application of Splay Trees to Data Compression," *Communications of the ACM*, 31(8), August 1988, pp. 996-1017.

(U) The purpose of data compression is to improve the efficiency with which data can be stored or transmitted by reducing the redundancy of its representation. A compression algorithm takes the source data and produces a compressed text. It is undone by an expansion algorithm. Static probability models for strings of text have their limitations when applied to many different sources of text. Adaptive Huffman codes using tree balancing schemes is one way to handle this problem. Adaptive arithmetic compression algorithms are another.

(U) The paper describes the use of generalized splay trees to construct adaptive algorithms that are extremely fast and compact. When applied to Huffman codes, splaying (or a variant of it) yields a locally adaptive compression algorithm

P.L. 86-36
EO 1.4.(c)

~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4012034

P.L. 86-36
EO 1.4.(c)

~~CONFIDENTIAL~~

that is simple and fast, although not optimal in terms of compression. When applied to arithmetic codes, splaying yields near optimal compression and asymptotically optimal time. Finally the paper notes that as in other adaptive schemes, the loss of one bit from the compressed stream is catastrophic. The author says there is a need for research on ways to protect against such problem. He also suggests the possibility of using such compression schemes in cryptography.

(U) G. Brassard & S. Kannan (1988) "The Generation of Random Permutations on the Fly," *Information Processing Letters*, **28**, pp. 207-212.

~~(C)~~

The paper offers three different solutions to the problem of generating a random permutation when only a small but unpredictable subset of its domain is ever to be queried. Building the permutation on the fly allows one not to do the work of deciding on a value for the permutation until that value is requested. The choice among the three depends on the available time and space. Two new data structure techniques are introduced, continuous rehashing and a balanced tree scheme.

(U) William Kocay (1988) "Groups & Graphs, a MacIntosh Application for Graph Theory" *Journal Combinatorial Mathematics & Computing*, **3**, April 1988, pp. 195-206.

~~(C)~~

One difficulty is that CAYLEY is an all-purpose package that is difficult to modify, and is buggy. The user just calls CAYLEY and depends on it to do the proper thing. This is far from ideal for use as a research tool. One would like to be able to go in and modify code to try things out. Since the parts of CAYLEY are interdependent, the designers of CAYLEY could not let this happen.

~~(C)~~ Groups & Graphs is a software package designed to overcome these difficulties. It is a research tool for manipulating graphs on a computer screen, and for computing with them and their automorphism groups. It does not have the enormous scope of CAYLEY, but is portable, and relatively friendly to the researcher. This article describes the structure of the package, and some of its algorithms. Many computational problems can be converted into problems about the automorphism group of a graph, and so this package might be helpful in clobbering them. For example, the package has an algorithm for often finding Hamiltonian paths or cycles. Such cycles have importance in generalizations of Gray code problems. This is the basic paradigm described by both Aschbacher and Luks at the Providence meeting.

(U) Richard Thomas (1988) "Cayley graphs and group presentations" *Math Proceedings of the Cambridge Philosophical Soc.*, **103**, May 1988, pp. 385-7.

~~(C)~~

The goal is to come up with improved architectures for parallel processing. The Cayley graph of a group G with a given set of generators has as points the elements of G, and two such points are adjacent in the graph if one is gotten from the other by multiplication by one of the generators. The routing problem on the graph can then be reduced to a type of word problem in the group. The possibility of finding efficient means of routing between the nodes of the graph is one recommendation for using Cayley graphs. There is however a tradeoff between graphs with large numbers of vertices

~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

P.L. 86-36
EO 1.4.(c)

DOCID: 4012034
EO 1.4.(c)
P.L. 86-36

and the need either to have many interconnections or extremely long communications routes. One is interested in finding Cayley graphs of a given number of vertices that are optimal for communication between nodes. The purpose of the Thomas paper is to study groups with a certain kind of presentation and homomorphism, and obtain bounds on the number of generators in the presentation and the order of the group.

(U) Richard P. Lippmann (1987) "An Introduction to Computing with Neural Nets," *IEEE ASSP Magazine*, April 1987, 22 pp.

(U) At an R51 tea on neural nets technology, this paper was recommended as an excellent source (along with the book by Rumelhart and McClellan) for beginners wishing to learn about neural nets. The paper is elementary and expository.

(U) David H. Bailey (1988) "Extra High Speed Matrix Multiplication on the Cray-2," *SIAM J. Sci. Stat. COMPUT.*, May 1988, **9**, no. 3, pp. 603-607.

(U) Ravinderpal Sandhu (1988) "Cryptographic Implementation of a Tree Hierarchy for Access Control," *Information Processing Letters*, **27**, pp. 95-98.

(U) We are given a computer or communications network where users are classified into a rooted tree of security classes. Each user is assigned a security class, called his clearance. Each file or message is assigned a security class called its sensitivity. We want users to have access only to that information whose sensitivity is consistent with their clearances. Sandhu intends to design a system for achieving this using a conventional cryptosystem such as DES. Each security class has a distinct key. Items are encrypted according to their security class and stored in encrypted form, with the security class name appended. Only users with access to the class key will be able to decrypt and read the item.

(U) The problem is to assure this desired access to key. Sandhu describes a method due to Akl and Taylor. This method has many advantages, but the terrible disadvantage is that when a new security class is added, new keys need to be computed for many of the existing security

EO 1.4.(c)
P.L. 86-36

)OCID: 4012034

classes, and existing items must be either re-enciphered, or all previous keys stored. The author presents a new solution to access control, at least in the special case of a rooted tree hierarchy of security classes, using one-way functions. The root is assigned an arbitrary key. One assumes that one has a family of "independent" one-way functions, one for each value of a parameter p. If b is an immediate child of c, then the key of class b is the value of the one-way function, with parameter p the name of class b, applied to the key of class c. Sandhu believes he can construct families of such one-way functions that are sufficiently independent to guard against users pooling their keys to recover keys to compartments they do not have, but he cannot prove this.

(U) J. Skorin-Kapov & F. Granot (1987) "Nonlinear Integer Programming: Sensitivity Analysis for Branch and Bound," *Operations Res. Letters*, **6**, no. 6, December 1987, pp. 269-274.

(U) The authors attempt to evaluate the sensitivity of solutions of non-linear integer programs to small changes in the right hand side or objective function coefficients. Such sensitivity analysis has been done in the case of linear integer programming. The authors assume the non-linear integer program has a relaxation to a continuous problem that is a convex program, such that the Kuhn-Tucker constraint qualification applies (as for example it will if the constraints are linear). This lets them make use of the dual non-linear program. Computational results are given for an example with a quadratic objective function, linear constraints, and 0-1 random variables. The point is to get an idea of what additional information to keep along the way in the enumeration tree in order to be able to bound the optimal value of a perturbed problem.

(U) Patrice Philippon (1988) "A propos du text de W. D. Brownawell: "Bounds for the degrees in the Nullstellansatz"," *Ann. Math.*, **127**, pp. 367-371.

(U) Philippon shows that the major result of Brownawell's paper making the Nullstellansatz effective also follows from a 1986 paper by Philippon. Further, when the ground field is a number field, one gets an explicit formula for the constant appearing in the theorem..

(U) D. G. Rogers (1988) "An Arithmetic of Complete Permutations with Constraints, I: An Exposition of the General Theory," *Discrete Mathematics*, **70**, 219-240.

(U) D. J. Champin & D. G. Rogers (1988) "An Arithmetic of Complete Permutations with Constraints, II: Case Studies," *Discrete Mathematics*, **70**, 241-56.

(U) Let N be an set of m integers, ordered by increasing size. The set N is symmetric if -n is in it whenever n is in it, and $-n_i = n_{m-i+1}$, for all i. N is central if it consists of those integers less than some c in absolute value. The purpose is to study the group S of all permutations of such sets N. The permutation π is said to be complete if the difference π-e, where e is the identity. If S contains complete permutations, then N is called an integral base.

(U) The purpose of these papers is to develop a theory of complete permutations, especially on central N or symmetric N or similar types of N. The arithmetic of complete permutations of symmetric integral bases turns out to be similar to the arithmetic of perfect systems of difference sets. Perfect systems of difference sets are in fact an abundant source of complete permutations. A constraint on a complete permutation is a specification of its behavior on a subset.

(U) Joseph Silverman (1988) "Computing Heights on Elliptic Curves," *Math. Computation*, **51**, July 1988, pp. 339-358. P.L. 86-36

(U) [redacted] told me about this paper on how to compute the canonical height of a point on an elliptic curve over a number field. Tate gave a rapidly converging series for computing Archimedean local heights for real absolute values. Silverman generalizes these methods to work for complex absolute values, and gives an efficient procedure for calculating local heights at non-Archimedean places. Thus, we can

DOCID: 4012034
EO 1.4.(c)
P.L. 86-36

effectively compute heights over number fields having complex embeddings.

(U) This is potentially an important step in improving our ability to do computational work on elliptic curves. For example, heights are used in Zagier's algorithm for finding the integral points up to large bounds. The canonical height of P can be defined in terms of a limit of heights of 2-power multiples of the point (that is roughly the number of digits in the coordinates of the point and its multiples.) It is not practical to compute it as a limit, but one can write the canonical height as a sum of local heights, one for each absolute value on the number field. These local heights are what Silverman teaches us to compute. Computer-suitable algorithms for these local heights are included. Some examples of computing canonical heights of points on explicit elliptic curves are also included. For example, on the elliptic curve $y^2+21xy+494y = x^3 + 26x^2$, the point $P=(0,0)$ has canonical height 0.010492061 . . .

(U) Robert M. Kuhn (1988) "Curves of Genus 2 with Split Jacobian," *Trans. AMS*, May 1988, **307**(1), pp. 41-49.

[redacted]

[redacted]

(U) William Gardner (1988) "Simplification of MUSIC and ESPRIT by Exploitation of Cyclostationarity," *Proc. IEEE*, **76**(7), July 1988, pp. 845-7.

(U) This note says that the problem of dealing with direction-of-arrival (DOA) location with antenna arrays via eigenstructure methods, as in the algorithms MUSIC and ESPRIT, can be simplified by exploiting a property of modulated signals called cyclostationarity.

(U) The advantages gained include a reduction in the size of the array and thus a reduction in SVD computation work. The disadvantages are that frequency parameters, such as carrier frequency or baud rate, must be known or measured, the integration time for correlation measurement is longer, and a different correlation matrix must be estimated for each signal of interest. Eigenstructure methods are intended to allow the individual DOAs of interfering signals to be determined provided the number of sensors in the array exceeds the number of signal sources.

(U) A brief description of MUSIC and ESPRIT is included. The modified methods should work on such bauded or carrier modulated signals as radar or radio communications. The balance of the advantages and disadvantages for a particular problem will dictate whether the proposed new methods should be used in place of MUSIC and ESPRIT.

(U) J. E. Olson (1987) "A Problem of Erdös on Abelian Groups," *Combinatorica*, **7**(3), pp. 285-289.

[redacted]

DOCID: 4012034

EO 1.4.(c)
P.L. 86-36

~~CONFIDENTIAL~~

EDITORIAL POLICY

A Letter to the Editor in this issue prompts this brief restatement of editorial policy.

CRYPTOLOG's criteria for publication are very like those of *Cryptologic Quarterly*: articles may be on any theoretical, doctrinal, operational, managerial, or historical aspect of cryptology.

But CRYPTOLOG is a more informal publication, and does not demand, as *CQ* does, that the articles "... make a genuine contribution to cryptologic literature." It asks only that they be useful or interesting. Nevertheless, it does require that facts are accurate and that the writing is clear. As for controversy, CRYPTOLOG thrives on it! But please, not the cryptologic equivalent of "the moon is made of green cheese": factual error is not controversy.

About classification: material up to and including TSC may be published, but not if there are additional caveats.

Preferences? Classified over unclassified (that's the justification for CRYPTOLOG's existence, after all!); technical over non-technical; shorter over longer.

Also, most welcome are conference and seminar reports, book reviews, software and hardware reviews, technical literature reports.

P.L. 86-36
EO 1.4.(c)

And letters. We dote on Letters to the Editor. Readers do too.

unclassified

Notice to Subscribers

Distribution of this Issue reflects changes received by COB 26 October 1990

~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4012034

BOOK REVIEW

Doublespeak (From "Revenue Enhancement" to Terminal Living" - How Government, Business, Advertisers, and Others Use Language to Deceive You), William Lutz, Harper & Row, Publishers, New York, 1989.

P.L. 86-36

Reported by [redacted] *P16*

As the featured guest speaker at the Cryptolinguistic Association's annual banquet in May, William Lutz spoke to the audience about his research and experiences that led to the publication of his book, *Doublespeak.* I became intrigued by the examples he cited. Immediately that afternoon, I purchased a copy of his book to read for myself about the things he was describing to the audience:

> Doublespeak is language that pretends to communicate but really doesn't. It is language that makes the bad seem good, the negative appear positive, the unpleasant appear attractive or at least tolerable. Doublespeak is language that avoids or shifts responsibility, language that is at variance with its real or purported meaning. It is language that conceals or prevents thought; rather than extending thought, doublespeak limits it.
>
> Doublespeak is not a matter of subjects and verbs agreeing; it is a matter of words and fact agreeing. Basic to doublespeak is incongruity, the incongruity between what is said or left unsaid, and what really is. It is the incongruity between the word and the referent, between seem and be, between the essential function of language--communication--and what doublespeak does--mislead, distort, deceive, inflate, circumvent, obfuscate.

Thus does the author define the subject of his book which is a bountiful collection of examples drawn from a variety of sources that touch every facet of our daily lives: media, advertising, business, professions, government, military, politicians. While Mr. Lutz' message is timely, readable, entertaining and amusing, it is also sobering, at times shocking, and generally disturbing, if not outright disgusting.

Mr. Lutz devotes a considerable portion of his book taking government and politicians (at all levels and the world over) to task for their abusive use of doublespeak. What is most disturbing about *Doublespeak* is that, as government employees we are a part of the problem he describes. When we or our political and executive leaders use doublespeak in dealings with the public or subordinates or with each other, it reflects poorly on everyone in government service.

As members of the intelligence community we have an obligation even greater than that of the ordinary responsible citizenry to understand correctly what is being communicated to us, to act on the basis of an accurate comprehension of the facts, and to communicate to others accurately and clearly. But as the author all too clearly demonstrates, we are constantly bombarded by messages that are, sometimes intentionally, designed to "mislead, distort, deceive, inflate, circumvent or obfuscate." And, unfortunately, we do not always have the time and resources to strip away the doublespeak and receive the true message.

Readers should come away from reading *Doublespeak* with a new appreciation for and dedication to communicating more clearly, accurately, and honestly. I urge you all as professionals in the intelligence business to take this book to heart while you are churning out bureaucratic prose of any sort.

~~FOR OFFICIAL USE ONLY~~

How to Edit a Scientific Journal, by Claude T. Bishop. ISI Press, Philadelphia, 1984. $14.95.

Reviewed by: [redacted] *P16*

Every NSA editor of any type—scientific, end-product, newsletter—should have a copy of this excellent book. Authors and Publishers should read it too, so they might have some notion of what is expected of them. In just 132 pages Bishop has provided a do-it-yourself manual on every aspect of publishing a periodical. He spells out the responsibilities and duties of editors and of authors as well. He offers sample guidelines for referees, for reviewers and authors, and even, sample letters. His purpose in writing this book was to provide guidance to scientists who are not professional editors and who would likely "end up learning the business by hard and sometimes bitter experience."

The austere title gives no clue that this is a fun book to read. Bishop illustrates his points with zany scenarios, but he is dead serious about quality in professional journals. He points out that maintaining standards "rests squarely in the hands of editors, who decide what will be published." He is concerned that the pressure to publish is resulting in the proliferation of trivial periodicals—that serious scientists soon ignore. By applying a significance factor, he finds that of the 90,000 or so journals, only 8,000 need be considered: the remainder clog retrieval systems with GIGO (garbage in, garbage out).

Editors must also exercise great care in selecting editorial boards, referees and reviewers and in preparing guidelines for them, because the review process plays a key role in assuring that what is published constitutes a reliable record. It can save the reputation of authors, reviewers, editors, and the publication itself. Bishop cites a letter to the editor from an author grateful for the rigors of the review process:

> After discussions about the referees' reports, your Associate Editor agreed to seek the opinion of a third referee as arbitrator. This referee found a major error in the theoretical part, which escaped 4 authors, 2 previous referees and the Associate Editor! My gratitude is boundless; I was saved from a very embarrassing situation.

But more than embarrassment can result. In a seminar on ethics during the International Technical Communications Conference (Chicago, 1989) we discussed the responsibility of the editor who accepted a paper on a treatment for an eye problem and overlooked the fact that the researcher had not followed protocol for testing on humans. Moreover, the editor uncharacteristically endorsed the treatment. Later an ophthamologist friend filled me in on the rest of the story. The researcher went on to another university, patented the medication, and got millions from investors. But other researchers could not duplicate the results. Evidently he had cooked the books besides violating protocol. So now FDA, SEC and IRS are after him. Suits and countersuits have been filed. The reputations of all the individuals and institutions involved are affected. All this because of an editor's oversight compounded by an error in judgment. A diligent editor would have stopped the researcher in his tracks.

The chapters on the literature of science, editors, editorial boards, the review process, referees, ethics, and record keeping are of particular interest to us at NSA. Of lesser practical application are the chapters on copy processing and printing, and on post-printing activities, for NSA has its own rules. But they do offer considerable insight to the processes, and a wealth of terminology; editors will find these chapters invaluable in dealing with both NSA and commercial printers. □

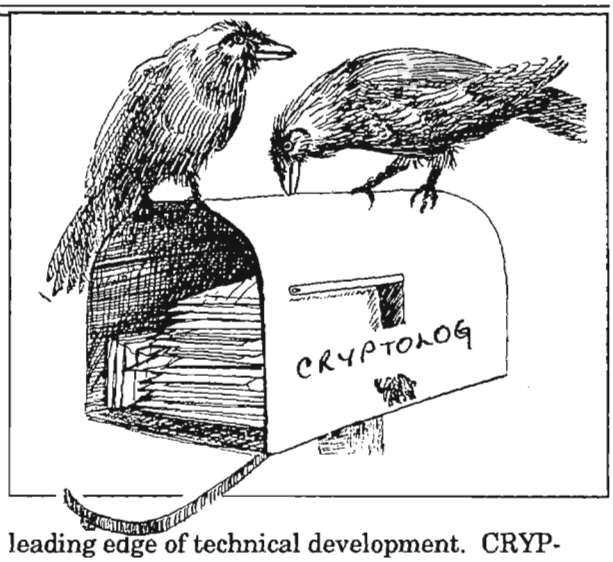
DOCID: 4012034
E.O. 1.4.(a)
P.L. 86-36

To the Editor:

As but one member of what must be a legion of CRYPTOLOG readers, I always felt that this publication was intended as a vehicle through which authors could share with others selected technical expositions relating to our mission. Expositions which not only explained "tried and true" methods of cryptology, cryptography, traffic and signals analysis, and other "technical" fields, but also documented and detailed new and innovative approaches to the problems we face in those fields.

Therefore, I was puzzled to see so many articles dealing with managerial problems, individual perceptions of Agency programs and explanations of corporate policy being published in the most recent magazine. Among the ten major articles contained in the CRYPTOLOG 2nd Issue 1990 I counted only two—"Planning for the Millenium" (sic), and [redacted] which were true technical dissertations. Six of the remaining eight articles—"A Perception of the Tech Track", "NSA/CSS and Counternarcotics", "Reassimilation", "Excellence through Evaluation", "Expert VLSI Designer Hired for Three Days", and "Rebuttal"—are not technical treatises and would seem more appropriate as submission for some other publication, such as the Agency's *Quarterly Management Review* (*QMR*). Each of these six easily fit into the *QMR*'s Quarterly Management Topic, Human Resources, and/or Telecommunications and Computer Services categories. The remaining two articles—"The Need for Intelligence" and "Balloon-Int, Civil War Style"—are perfect candidates for the historical publications of the NSA archives researchers.

As an internal publication aimed at serving our employees in the technical fields, CRYPTOLOG provides a valuable service. Surely our technical experts can provide the technical articles CRYPTOLOG should be carrying, and in quantities sufficient to warrant publication of more than two issues per year. We are a unique organization replete with talent and full of important achievements. Indeed, some of what we do is on the



leading edge of technical development. CRYPTOLOG deserves better support in terms of input from our technical professionals, and should be reporting more of what they are achieving. Non-technical articles of the type noted above should be addressed to, and published in other, more appropriate Agency vehicles.

P.L. 86-36

Don't you agree?

[redacted] *Chief, L1*

The Editor replies:

If there aren't more technical articles in CRYPTOLOG, it's not for want of trying!

Actually, we do get a lot of technical articles over the transom and through solicitation that we do not publish. Sometimes it's because they are prizewinners in essay contests and automatically go to *Cryptologic Quarterly* for consideration, and increasingly, it's precisely because they are about "new and innovative approaches"—advanced techniques that are closely held. Sorry, Fred, you won't be reading about them in CRYPTOLOG.

But you are right. We are getting more non-technical than technical articles, and especially, a flood of management articles of a general nature, to the point that I've had to resort to a printed rejection form! Why is this? I believe it's because the fashion in the agency is but a half-beat behind that in the outside world. Just as in universities there are fewer PhDs in physics and math and

~~FOR OFFICIAL USE ONLY~~

more MBAs, so at NSA anyone who can is disdaining the tech track for management. It's simply a matter of more reward for less effort. So ambitious tech types write on management or non-technical subjects as a way of planting the flag.

I haven't given up, though, and I continue to buttonhole everyone who might possibly contribute a technical article. I hereby make a plea to whom it may concern. (Thanks, Fred, for giving me this opportunity.)

As for publishing the cited "management" articles in *QMR* and the "historical" articles in historical publications, the persons in charge of those publications think differently, as you will read in their responses. In any case, the line between managers and technicians is blurred. Technicians do not work vacuum-packed in monastic cells solely on tasks handed down from above, but participate in decision-making and in the running of the agency. They sit on promotion boards, reorganization task forces, career panels. They order dictionaries and software. They provide grass-roots input to multi-million-dollar computer systems. They hire a specialist for a one-shot job. In short, they do management things.

CRYPTOLOG is somewhat more than a medium for technical exchanges among technical types. As Gen. Wolff, then DDO, set forth its charter in "A Letter of Introduction" in the first issue, ". . . its level of informal exchange invites short articles and letters on any subject." The editors have interpreted "any subject" to mean anything pertaining to NSA. And so it provides individuals, be they managers or technicians, a forum for indulging in speculation; for advancing futuristic notions; for query and challenge. It has become neutral ground where managers and technical types can meet, discuss, and argue with one another, having first checked their shoulderboards at the transom.

From the Founding Publisher

There is some, but not much, merit to [redacted] argument. I agree that most of what is published in CRYPTOLOG ought to be by technicians, about technical things, for technicians. But there is room for much else under that umbrella. The technicians' view of such management programs as the technical track is very different from that of generalists; it needs to be articulated. Pate's piece does it well. There is plenty of room for history in the CRYPTOLOG; the archivists will certainly welcome the material for their histories. Similarly with other articles mentioned. From what I recall of the *QMR*, it is simply not a vehicle for any of the articles in that issue.

William Lutwiniak, P1, (Retired)

Amicus Curiae *reponse to* [redacted]

Editors' lots are not always happy ones. Some readers adore their publications, some abhor them, other readers take what they can get. Mr. [redacted] observations about the last issue of CRYPTOLOG were certainly written out of concern for the quality of technical publication in the Agency. And it is true that the articles he points out are not strictly technical in the sense that we usually define the term, i.e., signals analysis, cryptanalysis, computer science, etc. We can look at this situation from two directions, however. First, and not meaning to be flip, an editor doesn't always receive a good supply of the kinds of articles he or she would like, in this case items of a more "technical" nature. The editor, however, still wants to publish matter of value to his or her readership. This brings us to the second point: Articles which address not-so-technical subjects but which are perhaps peripherally related and therefore still have value to the work force should not be shunned because they do not meet our tight definition of what is a technical subject.

Somewhat in this light, I couldn't agree more with [redacted] statement that ". . . our technical experts can provide the technical articles CRYPTOLOG should be carrying . . ." The same observation could be made about

P.L. 86-36
DOCID: 4012034

Cryptologic Quarterly, the journal I am privileged to edit. The fact is, however, because of busy schedules, lack of enthusiasm for writing, minimal awareness of the existence of publication vehicles, or a hundred other reasons, Agency employees don't submit articles in the volumes we editors would like to become accustomed to. Many of those who do send us articles, though they don't necessarily contribute technical "treatises," still write about topics that interest a large segment of the NSA population who don't have access to the *Quarterly Management Review* or other publications, which, while "more appropriate," do not receive the wide distribution that would make the information they contain even more useful.

A word about [redacted] reference to what the "NSA archives researchers" should be writing. First of all, [redacted] may or may not be aware that the archivists and the researchers (read "historians") are now organizationally two different groups. The historians, my organization, while personally interested in topics like "The Need for Intelligence" and "Balloon-Int," would not be inclined to write about them. The first would need much more elaboration and in-depth research to make it worthy of a cryptologic history monograph or even an article for *Cryptologic Quarterly*. The second, while fascinating and even amusing, does not carry a cryptologic theme and therefore would not be fuel for any cryptologic historian's production. Our criteria for publication of material as a monograph or as a *Quarterly* article include (to quote from the *CQ*'s title page) whether or not the article (or monograph) is of sufficient substance and interest to make a genuine contribution to cryptologic literature. By the way, *Cryptologic Quarterly* articles may be written (again, to quote) on any theoretical, doctrinal, operational, **managerial**, or historical aspect of cryptology. Although I have not seen an expressed editorial policy for CRYPTOLOG, I believe that it is implicitly very similar.

CRYPTOLOG and *Cryptologic Quarterly* are at their hearts technical journals. Both publications recognize, however, that not only should we as cryptologic professionals be concerned with the narrow (i.e., technical) aspects of cryptology, but we should also have an abiding interest in the broader issues that affect the cryptologic effort. To ignore those broader issues is to make us less than we can be.

Barry Carleen, D91,
Executive Editor, Cryptologic Quarterly

From QMR:

I am responding to [redacted] suggestion that six articles on management published in 2nd Issue 1990 are more suitable for the *Quarterly Management Review* (*QMR*) than for CRYPTOLOG.

A few words are in order about *QMR*. It serves as a management tool which tracks performance trends within the Agency. Information that is placed in the *QMR* is factual and presented in graphic and/or narrative form, limited in both length and amount of detail. It is not intended to provide an analysis of the data or to present personal opinions. Rather, the data illustrate the status, trends, comparisons and accomplishments of ongoing and new activities in a graphic or statistical manner for individual management analysis. Also included are topics that are of general interest to, or impact on, a wide segment of Agency management, but again, factual in nature.

Historically, CRYPTOLOG has offered an opportunity for individuals to contribute opnions, to relate experiences, and to share knowledge on a variety of subjects. The articles mentioned fall in this category. Therefore the several individuals involved in preparing the *QMR* read and appreciated the articles cited and were not perturbed that they were published in CRYPTOLOG. The article "Excellence through Evaluation" would be a suitable for QMR if the contents were factually oriented and summarized in one or two pages.

[redacted] *Chief, N313,*
QMR *Coordinator*

[redacted]

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

DOCID: 4012034

Golden Oldie

HIAWATHA DESIGNS an EXPERIMENT

1
Hiawatha, mighty hunter
He could shoot ten arrows upwards
Shoot them with such strength and swiftness
That the last had left the bowstring
Ere the first to earth descended.
This was commonly regarded
As a feat of skill and cunning.

2
One or two sarcastic spirits
Pointed out to him, however,
That it might be much more useful
If he sometimes hit the target.
Why not shoot a little straighter
And employ a smaller sample?

3
Hiawatha, who at college
Majored in applied statistics
Consequently felt entitled
To instruct his fellow men on
Any subject whatsoever,
Waxed exceedingly indignant
Talked about the law of error
Talked about truncated normals,
Talked of loss of information,
Talked about his lack of bias,
Pointed out that in the long run
Independent observations
Even though they missed the target
Had an average point of impact
Very near the spot he aimed at
(With the possible exception
Of a set of measure zero.)

4
This, they said, was rather doubtful.
Anyway, it didn't matter
What resulted in the long run;
Either he must hit the target
Much more often than at present
Or himself would have to pay for
All the arrows that he wasted.

5
Hiawatha, in a temper
Quoted parts of R. A. Fisher
Quoted Yates and quoted Finney
Quoted yards of Oscar Kempthorne
Quoted reams of Cox and Cochran
Quoted Anderson and Bancroft
Practically in extenso
Trying to impress upon them
That what actually mattered
Was to estimate the error.

6
One or two of them admitted
Such a thing might have its uses
Still, they said, he might do better
If he shot a little straighter.

7
Hiawatha, to convince them
Organized a shooting contest
Laid out in the proper manner
Of designs experimental
(Mainly used for tasting tea, but
Sometimes used in other cases)
Randomized his shooting order
In factorial arrangement
Used in the theory of Galois
Fields of ideal polynomials
Got a nicely balanced layout
And successfully confounded
Second-order interactions.

8
All the other tribal marksmen
Ignorant, benighted creatures,
Of experimental set-ups
Spent their time of preparation
Merely shooting at a target.

[redacted]
13 July 1967

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012034

9

Thus it happened in the contest
That their scores were most impressive
With one solitary exception
This (I hate to have to say it)
Was the score of Hiawatha,
Who, as usual, shot his arrows
Shot them with great strength and swiftness
Managing to be unbiased
Not, however, with his salvo
Managing to hit the target.

10

There, they said to Hiawatha,
That is what we all expected.

11

Hiawatha, nothing daunted,
Called for pen and called for paper
Did analyses of variance
Finally produced the figures
Showing beyond peradventure
Everybody else was biased
And the variance components
Did not differ from each other
Or from Hiawatha's
(This last point, one should acknowledge
Might have been much more convincing
If he hadn't been compelled to
Estimate his own component
From experimental plots in
Which the values all were missing.
Still, they didn't understand it
So they couldn't raise objections.
This is what so often happens
With analyses of variance.)

12

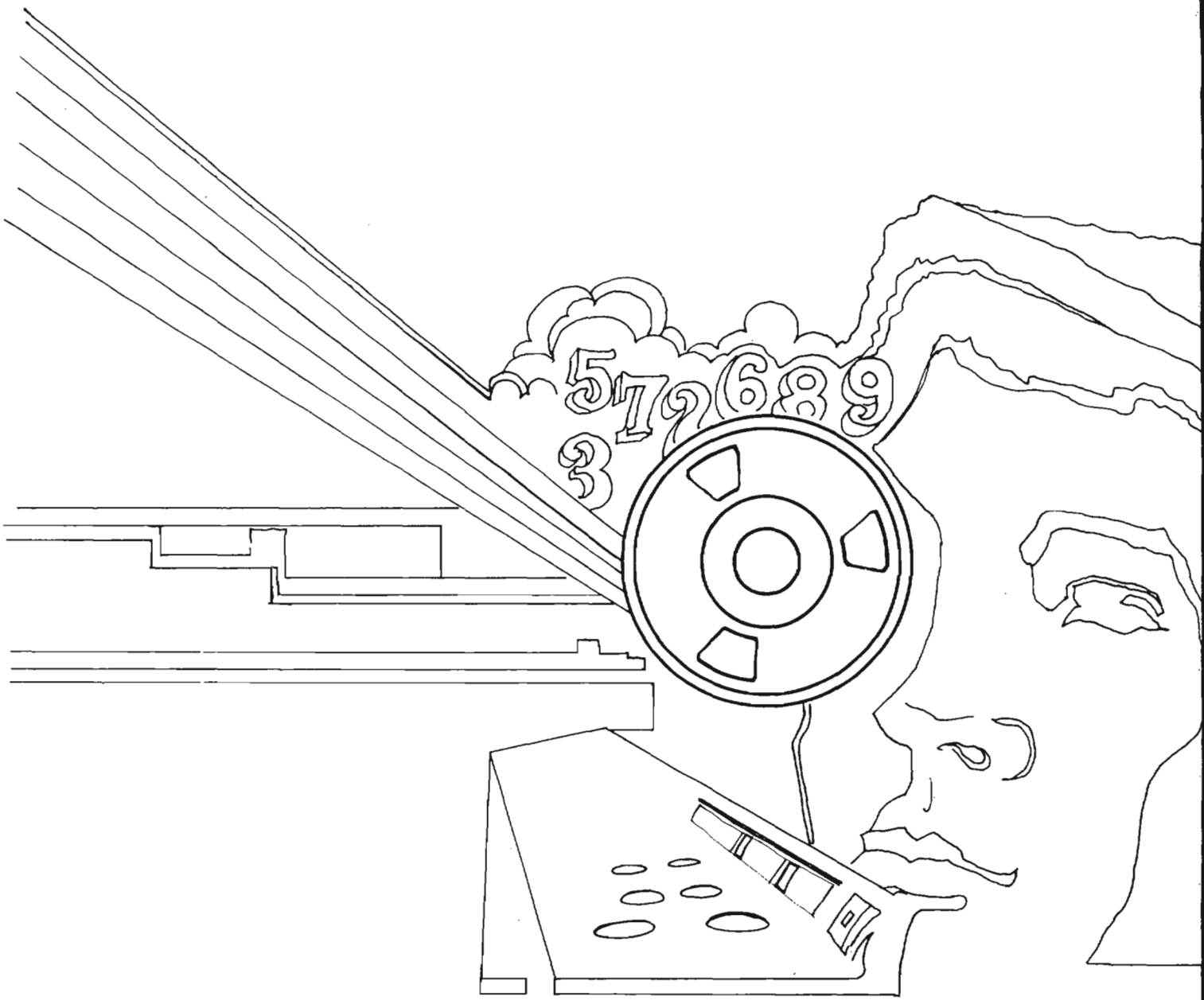
All the same, his fellow tribesmen
Ignorant, benighted heathens,
Took away his bow and arrows,
Said that though my Hiawatha
Was a brilliant statistician
He was useless as a bowman.
As for variance components
Several of the more outspoken
Made primeval observations
Hurtful to the finer feelings
Even of a statistician.

13

In a corner of the forest
Dwells alone my Hiawatha
Permanently cogitating
On the normal law of error
Wondering in idle moments
Whether an increased precision
Might at the risk of bias
If thereby one, now and then, could
Register upon the target.

~~FOR OFFICIAL USE ONLY~~

~~SECRET~~



DOCID: 4012037

Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

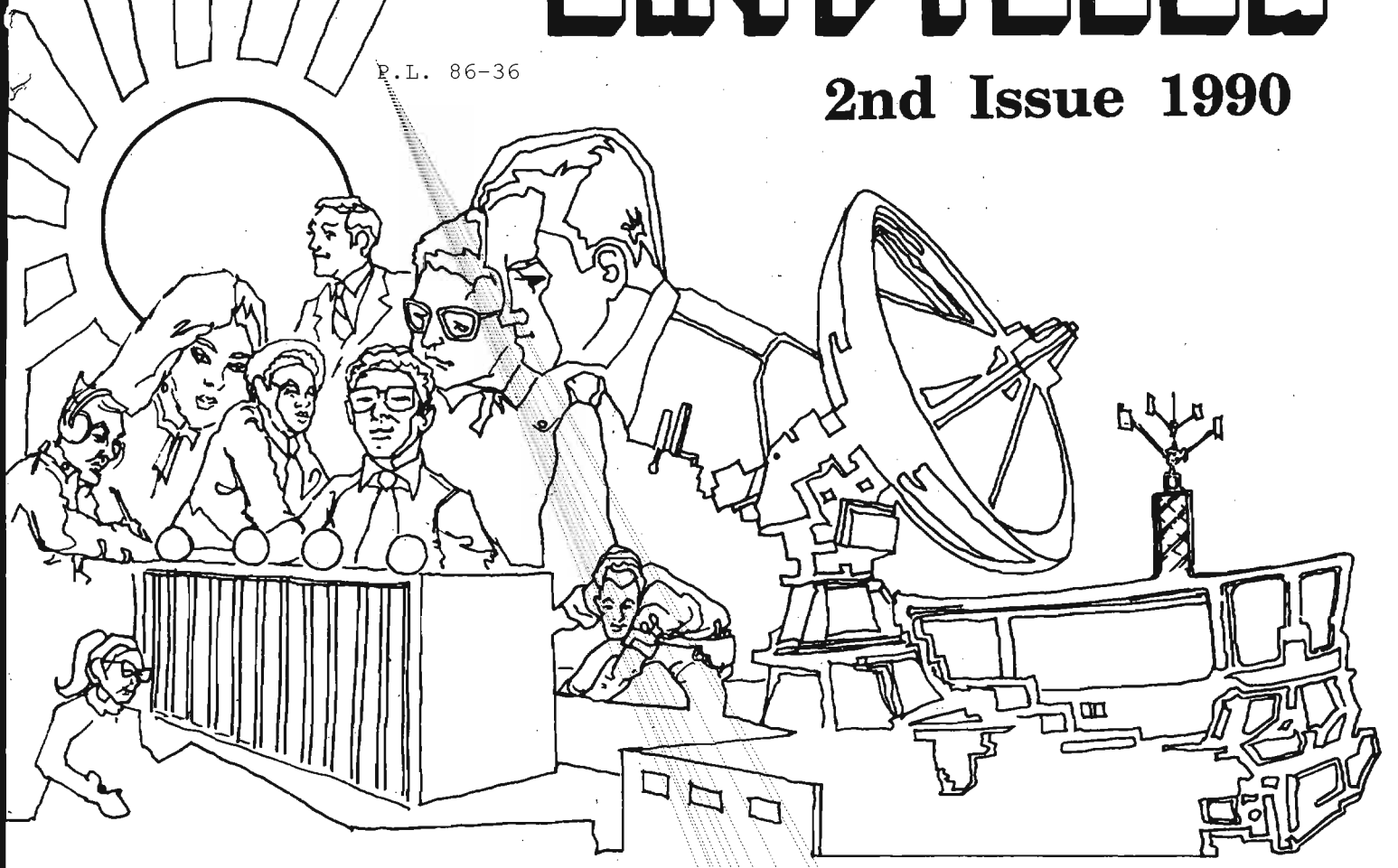
~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

P.L. 86-36

2nd Issue 1990



A PERCEPTION OF THE TECH TRACK	[redacted]	1
NSA/CSS AND COUNTERNARCOTICS	[redacted]	8
THE NEED FOR INTELLIGENCE	N. C. Gerson	9
HELP WANTED	David Hatch	10
PLANNING FOR THE MILLENIUM	[redacted]	13
REASSIMILATION	David L. Beckner	16
EXCELLENCE THROUGH EVALUATION	[redacted]	18
BULLETIN BOARD		20
CRUCIBLE/MOSTAR	[redacted]	21
RAW TRAFFIC AND REMOTE COLLECTION	[redacted]	27
EXPERT VLSI DESIGNER HIRED FOR THREE DAYS	[redacted]	28
REBUTTAL TO 'A NOTE ON THE LINGUIST PROBLEM'	[redacted]	29
SHORT-ORDER TRANSLATION	[redacted]	31
BALLOON-INT, CIVIL WAR STYLE	[redacted]	33
LETTERS		36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

DOCID: 4012037

P.L. 86-36

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XVII, No. 2 ..... 2nd Issue 1990

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Cryptolinguistics ..... (963-4382)
Information Resources ..... (963-3258)
Information Science ..... (963-3456)
Information Security ..... (972-2491)
Intelligence Reporting ..... (963-5068)
Language ..... (963-3057)
Linguistics ..... (963-4814)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (963-4958)
Special Research ..... Vera R. Filby (968-5043)
Traffic Analysis ..... (963-4351)

Classification Officer ..... (963-5463)
Bardolph Support ..... (963-3369)
Macintosh Support ..... (968-7315)
Illustrator ..... (963-3360

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, NORTH 2N018

If you used a word processor, please include the floppy or cartridge with your hard copy, with a note as to what computer, operating system, and software you used.

via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five)
(note: no 'o')

via ALLIANCE, send to:
PLBROWN [note: all caps]
attn: CRYPTOLOG

Always include your full name, organization, and secure phone; also building and room numbers.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, NORTH 2N018
Please do not phone.

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

WHILE-U-WAIT

(U) In this period of budget cuts management will be happy to learn that throughout the Agency, many analysts have devised clever ways to make every minute count. Take CRYPTOLOG's parent organization, for example, that puts out working aids of blockbuster proportions. Printing them is a chore because you have to be there to monitor the disaster-prone process in case the computer freezes up or the printer jams. What to do while-u-wait? The tradition here is to plan ahead to proofread, or scan the Read Folder, or eat lunch.

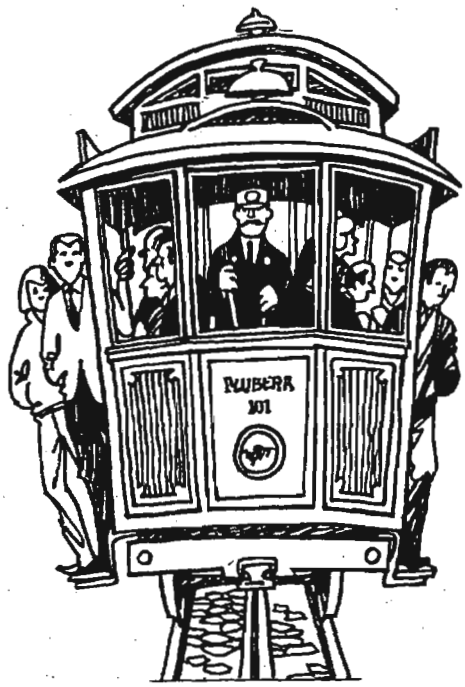
(U) This is but one modest example of many. Pride of place for productivity while-u-wait surely goes to a linguist of our acquaintance, who, a couple of crises ago, was wont to wait for his wife when her outfit was jumping and his was not. Idly he picked up a grammar book on an offbeat language that piqued his curiosity. Yes, you got it! While-he-waited the many months of that crisis he gained sufficient proficiency to become certified!

~~(C-CCO)~~ A more exotic while-u-wait chore was undertaken by a voice linguist listening to search. As some of you well know, it requires intense concentration to listen through the static for tiny segments of intelligence that crop up at long intervals between the "music of the spheres." There's not much you can do but sit there and listen, hands idle. But this analyst found that you can do needlepoint. Keeping hands busy in a way that does not occupy the mind serves to lessen the tension of intense concentration, and so permits longer stints without a break.

(U) And there's no doubt that readers can contribute stories that top these!

DOCID: 4012037

A PERCEPTION OF THE TECH TRACK



~~(FOUO)~~ The technical track program is an issue of considerable concern to career Agency analysts. Despite all the recent activity, there is skepticism about the viability of the program. For that reason, P16 and the DDO Language Advisory Committee have been looking at various aspects of the issue. They have conducted several rap sessions with senior linguists in grades 14 and 15 to gain their point of view about the technical track and technical language careers. The following remarks focus on linguists but apply equally to the other DDO cryptologic and analytical disciplines.

P.L. 86-36

[redacted] *P16*

~~(S-CCO)~~ The sessions revealed a widespread cynicism about the existence and future of a technical track. Most analysts see no real progress in the development of the track or appealing advancement opportunities.

[redacted]

~~SECRET~~ EO 1.4.(c)
~~HANDLE VIA COMINT CHANNELS ONLY~~ P.L. 86-36

(U) Individuals opt to remain in their technical specialties because of their technical professionalism, their devotion to duty, and their sense of mission, rather than as a result of the Agency's efforts to promote a technical career system.

(U) The linguists with whom I met agreed that the technical career situation, specifically promotions to GG-14/15, has considerably improved over the past several years, and they are encouraged by that. But a closer look at the current crop of senior linguists reveals that many achieved success only through a "detour" into management. It is true that the technical health of the organization benefits if people opt to return to the technical track after reaching grade 14 or 15. But the message is not ignored by junior technical employees looking toward advancement.

(U) Also, while one is "detouring", technical expertise is temporarily, perhaps permanently, lost so that others must be recruited and trained to fill the void.

(U) Pessimism is heightened by the fact that there will be very few open STE billets over the next several years. We need a healthy technical track program to ensure that we make the best use of those that become available.

THE PROSPECTS FOR LINGUISTS

~~(FOUO)~~ When we look at the present distribution of Senior Technical Experts in the Agency, we find that a disproportionate number are in mathematics, engineering, physical sciences, and data systems. Our first reaction is concern that the analytic specialities are not sufficiently represented in the STE ranks. I propose that the problem, for linguists at least, actually begins at grade 15. [redacted] Therefore, the pool from which language STEs may be drawn is very small, a fact that adds to the frustration, skepticism and cynicism felt by the more junior linguists who would aspire to technical careers.

~~(FOUO)~~ One might ask why linguists are not being promoted in greater numbers since language has been classified as a critical skill by NSA for years. Do promotion boards not think linguists deserve to be elevated to the senior grades? Do they fully understand the role of linguists and the skills required?

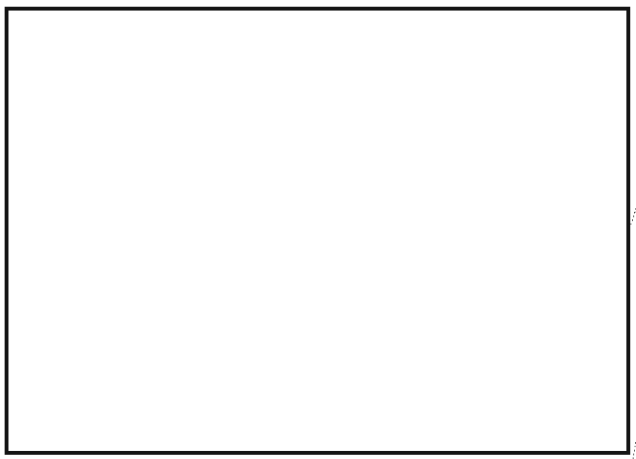
[redacted]

~~(FOUO)~~ The present dearth of GG-15 linguists is in part the inevitable consequence of a situation that prevailed two decades ago when it was not possible to go beyond a 12 as a "pure" linguist. That grade ceiling has been attributed to the misperception of a few senior managers that "anyone can translate given a dictionary." In fact, one senior manager considered language work to be of a clerical nature. So linguists left the field to seek advancement.

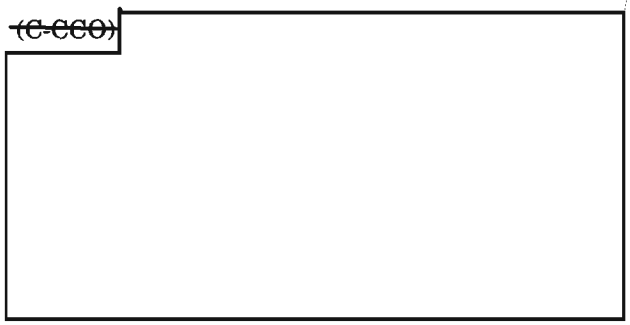
WHAT LINGUISTS DO

(U) Though the managers mentioned above are long gone, and, let us hope, their perceptions with them, it might be well to pause here to consider just what it is that linguists do.

EO 1.4.(c)
P.L. 86-36



~~(C-CCO)~~



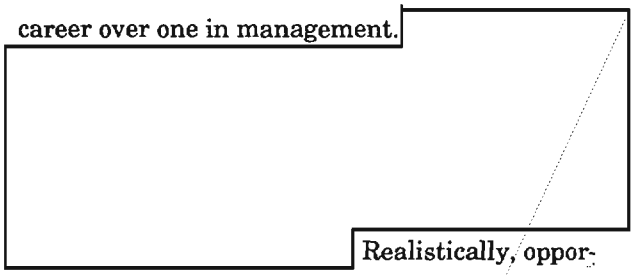
It requires years of dedicated study (much of it self-study) and experience to master a rare language. Aside from language skill per se, the linguist must also become fully knowledgeable of the target, its organizations, personalities, history, customs, lexicon, communications, and so on, in order to be a truly effective SIGINT linguist.

~~(FOUO)~~ These skills do not come easily or quickly. To become a true professional, a linguist requires considerably more dedication and effort than is generally assumed. The effort is so great in some instances that other less challenging and more rewarding avenues appear to offer more appealing opportunities. That is why it is so necessary to establish a viable technical track program in DDO.

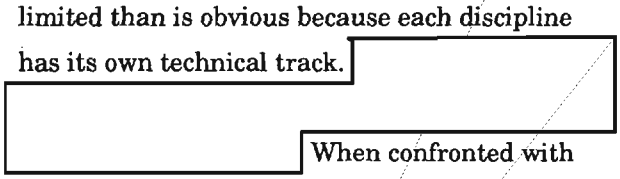
DESIGN FOR A TECHNICAL TRACK

~~(FOUO)~~ An effective technical track must provide a clear and objective set of qualification standards that will permit technical careerists to know what is expected of them in order to qualify for advancement to the senior ranks, including STE. It will have to produce a record that demonstrates unequivocally that sufficient numbers of people can reach the senior grades without substantially departing from a technical career path. Moreover, the advancement for qualified technical experts must be as rapid as it is for those who choose other career paths, such as management-cum-staff. That is to say, a technical track program cannot be viewed as truly successful when people are not being promoted to the senior grades, including Senior Technical Expert, until they are in the final years of their 30-plus-year career.

~~(FOUO)~~ At present the numbers do not add up to convince smart young people to choose a technical career over one in management.



Realistically, opportunities to become grade 15 are more severely limited than is obvious because each discipline has its own technical track.



When confronted with these numbers, it is little wonder that many technicians opt for management. The fact that some of them eventually will "opt", for various reasons, to return to the technical track after a number of years, should not comfort us a great deal.

(U) While I would not suggest total parity or a quota system among occupational specialties or between the technical and managerial/staff tracks, I do believe the Agency, and especially DDO, must give greater attention to senior level promotions to technical careerists. We want to encourage analysts to devote as much of their careers as practicable to their specialty. If but half of all past technicians had remained in their specialty, this Agency would be in a remarkable state of technical health!

(U) Though the Agency points with justified pride to a low attrition rate vis-a-vis other government agencies, the figures reflect attrition from the Agency, not the internal attrition from the analytic specialties into staff and management positions. While this is not counted officially as attrition, the effect is about the same, that is, loss of highly trained resources for which the Agency spent substantial sums to recruit, hire, and train, and for which additional sums must be spent to obtain replacements.

A PROPOSED SOLUTION

(U) The time has come for the Agency to give serious consideration to a new way of thinking about the grade structure of a technical track. The traditional pyramid, bottom-heavy with fewer and fewer people as one ascends in grade must give way, if not to an inverted pyramid, then certainly to a structure in which the ranks of the upper grade levels are somewhat larger than the lower ones. If our efforts to establish a technical track be truly successful, we should expect to have most people remain in their technical speciality for their entire careers of 30-plus years. We must hold out a reasonable promise of promotion to the senior ranks for the most deserving. And if the programs succeed, the numbers of deserving should similarly increase.

PROMOTION TO STE

(U) The manner of determining who should be selected (or promoted) to the senior technical expert ranks needs to be critically reviewed. We generally agree that fellow technicians recognize fairly accurately who among their ranks stand out from the crowd and who deserve to be senior technical experts. Currently, the Senior Technical Review Board does not act autonomously, nor does it conduct a true zero-based review of all eligible GG15's. To a very large degree, consideration of individuals proceeds as for all other Agency promotions, i. e., they are organizationally initiated and are processed in a linear fashion.

(U) But the selection process should reflect the notion that senior technical experts are, in the truest sense, all-Agency assets. At present, organizational constraint causes candidates to be placed in priority order, regardless of the areas of technical expertise they represent. Promotion review boards are, in their turn, constrained to review the candidates in a similar priority order. At no time is consideration given that this or that technical area needs to be represented by an appropriate array of experts. Nor do managers necessarily know how their respective technical peers view these candidates.

(U) Candidates for the STE ranks should not be processed linearly but rather in parallel, especially when they represent different areas of technical specialization. And since senior technical experts are technical resources available not just to the immediate manager who nominates them, there should be no concern as to the experts' grade vis-a-vis that of their administrative managers.

(U) To overcome some of these problems with recommending and promoting people for Senior Technical Expert, I strongly recommend that potential candidates for Senior Technical Expert be identified, and ultimately recommended for promotion, by their peers, with management playing, if it must play at all, a minor role in the process. High-level promotion boards should be composed of a fair representation of the organization's technical specialties, and where possible, members should be drawn from the STE ranks. Each board should be empowered to conduct zero-based reviews and should not be constrained by organizational recommendations. The chairpersons of the career panels might play an active role in the peer review process for Senior Technical Experts.

TECH TRACK POSITIONS

~~(FOUO)~~ Designating positions in a technical track program seems to be a very sensitive issue. There is a desire not to lock ourselves into the constraints of graded positions, as is the case for the management track. I support this notion generally. Although we do not view them as such, in reality most staff positions, especially in the operations elements, are technical positions. We have reporters, collectors, data systems analysts, cryptanalysts, traffic analysts all who provide technical support and advisory services at office and group levels throughout DDO. And there are also a few staff positions in any organization, especially at the group level, that warrant being established at the rank of STE. In the language career specialty, for example, each group has "established" a senior language advisor. Regardless of where these individuals sit organizationally, the scope of their responsibilities and the impact of their activities on the organization could well warrant the rank of STE.

~~(FOUO)~~ Besides the thorny issue of technical track positions, there are several other problems which those who are designing technical track programs must address. One of these has to do with transportability. Development of technical track programs in DDO is proceeding along group, and in some cases office, lines. For most linguists, a group-level program does not pose severe barriers to their mobility. The problem arises when linguists who have attained a given status in one organization then choose, for career diversification and enhancement, to seek an assignment in a different organization.

(U) With the exception of the recently published G Group Technical Track Program, none of the extant program documents deal explicitly with the question of transportability of qualifications and technical status, although there seems to exist a tacit understanding that would grant the transferee some credit towards meeting technical track criteria in a new organization.

~~(C CCO)~~ In many SIGINT language environments, multilingualism is an important factor in operational success. Therefore, a viable technical track program must accommodate multilinguists and provide the necessary transportability of status to encourage them to stay in the technical track.

DIVERSITY FOR TECHNICAL TRACK LINGUISTS

(U) Another concern for the designers of technical track programs, as well the tech trackers themselves, is how much diversity in career is acceptable and desirable. It is unreasonable to expect that all individuals will be content to remain in the same job for an entire career. The problem is identifying appropriate diversifying experiences

for each technical career. Both individuals and organizations benefit from a certain amount of interdisciplinary experience.

~~(C-CCO)~~ Diversity comes in several forms:

diversity of application within the specialty. In the case of language, there are options such as voice vs non-voice, language teaching, staff assignments performing language research, career panel tasks, and so on.

assignments that emphasize associated cryptologic disciplines, such as intelligence reporting, traffic analysis, cryptanalysis, collection.

acquisition and application of different languages.

supervision of other linguists, especially in language-related SIGINT activities.

(U) But these experiences must not so diffuse technical expertise in the language so as to render that proficiency inadequate to perform highly skilled technical language tasks.

(U) The individual is usually the best judge of when a career change is needed: when burnout occurs, when boredom begins to set in, when enthusiasm wanes, when creativity falters, when productivity drops. Even when an individual knows what the change ought to be, doing something about it is another matter.

THE ROLE OF MANAGEMENT

(U) This is where management plays a crucial role in the success of the technical track program. By being sensitive to the needs of the individuals as well as of the organization, managers can steer careers in directions that will optimize the individuals' potential and improve the chances that they will pursue a rewarding technical career. This is a management responsibility that cannot be taken lightly. American business has been faulted for its short-sighted views on long-term investments and profits. I fear that Agency management often takes the same view when it comes to managing human resources.

(U) It is difficult, maybe impossible at times, to look at particular individuals in terms of their future potential and development when the press of international events demand all of our attention today. Being able to do it, however, is a trait that differentiates a good manager from a manager in name only. Planning for the future is not just a corporate responsibility, it is the personal one of every manager.

~~(FOUO)~~ Management must afford technical trackers additional opportunities and challenges for growth. With experience and training, technical trackers become technical leaders. This means involvement in the technical management of targets, participation in advanced and specialized language study wherever offered, active participation in professional associations, both inside and outside the Agency, and interagency activities associated with the target or language, and opportunities for travel. These are but a few incentives that could be offered to technical trackers. They must be valued and used for the technical knowledge and experience they possess and can bring to bear on the accomplishment of the organization's mission.

TECHNICAL LEADERS IN LANGUAGE

~~(FOUO)~~ Besides knowing their language in depth and breadth, technical leaders possess a critical knowledge of the targets associated with the language or languages. The most valuable asset of long-term technical track analysts is target continuity. With it, discrete and seemingly unre-

DOCID: 4012037

lated and unimportant facts, often separated in time, become intelligence nuggets. This is a subtle and intangible benefit that comes when people remain productively associated with targets over long periods of time.

~~(FOUO)~~ Technical leaders have the ability to perform professional quality research and to produce working aids that advance the technical health of their specialties. They must also be able to impart to junior analysts the knowledge and experience they have gained. Above all, senior technical language experts are superior analysts and reporters in their own right. They can analyze incomplete material and derive meaningful information from it, and then convey it with facility precisely in correct English.

~~(FOUO)~~ The Agency now possesses a fair number of linguists in the senior grades who are well on their way to meeting the standards of senior technical expert. It remains to the DDO and its managers and the Agency senior promotion boards to ensure that these talents are properly recognized and used. While not the only solution to encouraging technical careers, an effective DDO technical track program should go a long way in stemming the hemorrhaging of technical talent in DDO.

PATH vs TRACK

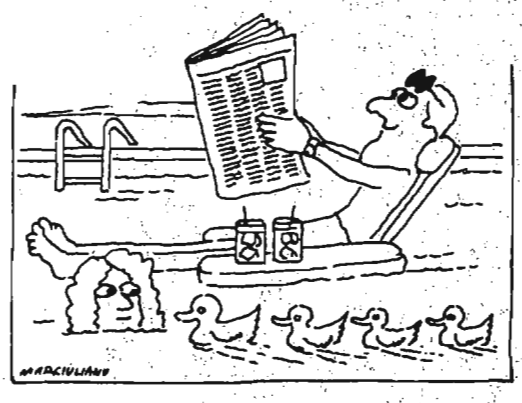
(U) When discussing technical track careers, we generally refer to a technical track program as the administrative infrastructure under which such careers are to be "managed." The notion of a program suggests a certain structural rigidity with terms and conditions that an individual must satisfy in order to progress to the next level. Track suggests a unidirectional movement with little or no opportunity for the diversity discussed earlier. Flexibility is not generally viewed as a feature of "program." Therefore, in the context of technical careers at NSA, we should more properly refer to technical career development or pathing system, for no two career paths will likely be the same, yet the end results may be quite similar.

(U) Career pathing takes into consideration the strengths and weaknesses of both the technicians and the organization. Technicians are presented with career options that most effectively will lead to their career objective. These options and the actions to effect them are discussed and acted on in consultation with concerned managers who, in turn, have the authority to carry out the career pathing plan.

REPRISE

(U) The Agency will have to do some belt-tightening; that is a fact of life being discussed in every corner of the buildings. Protecting our investment in technical talent is essential. Simply put, we need effective, flexible programs to retain the skills we need to support our unique mission.

Notice to Subscribers

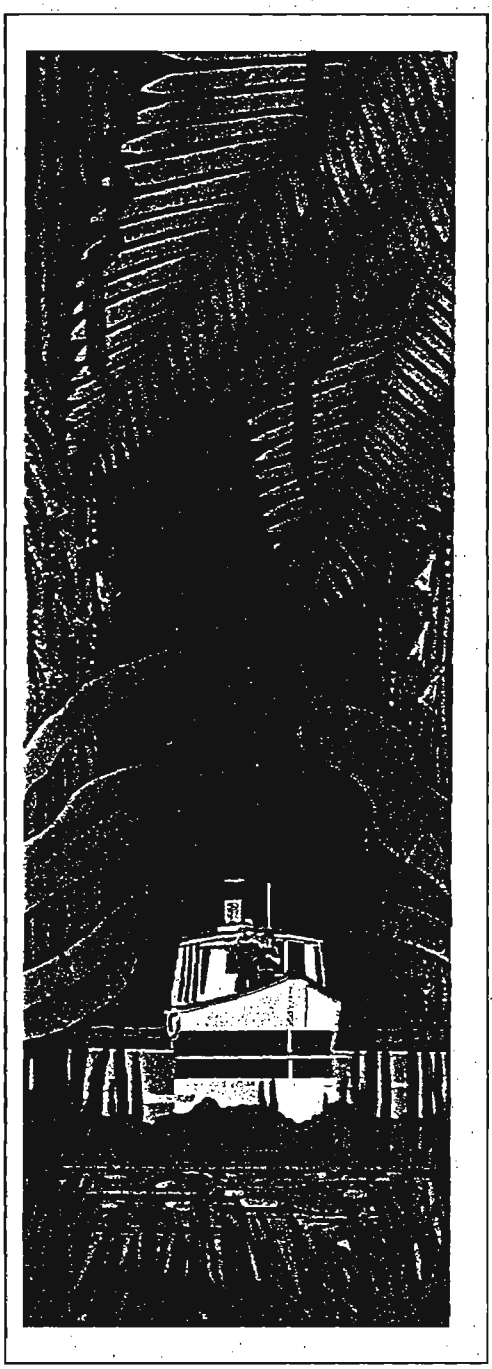


The distribution for this issue reflects changes received by COB 5 July 1990

NSA/CSS and COUNTERNARCOTICS

P.L. 86-36

[redacted] P05/SAO



(U) As most of you know, NSA has recently become heavily involved in the US Government counternarcotics effort. We have established the following guidelines for the classification of counternarcotics-related information:

❑ (U) The fact of NSA/CSS association with the US Government counternarcotics efforts is UNCLASSIFIED.

❑ (U) The fact of an association between DEA, Customs, US Coast Guard, FBI and NSA with counternarcotics is UNCLASSIFIED.

❑ ~~(C)~~ The fact of a SIGINT effort against international narcotics traffickers is CONFIDENTIAL.

[redacted]

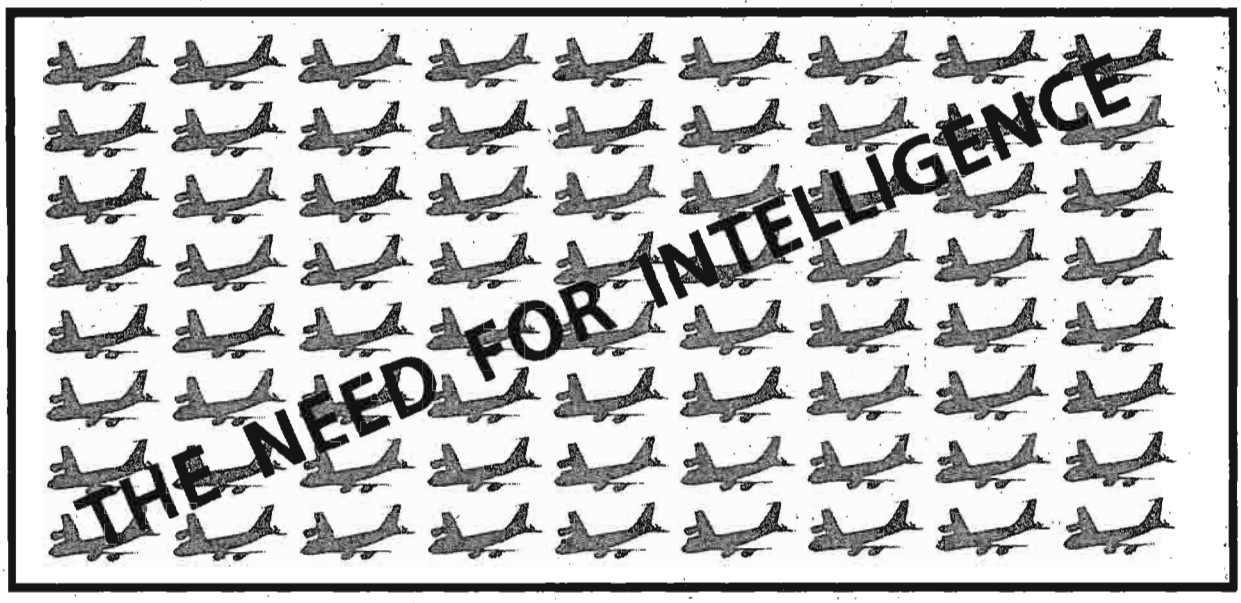
❑ ~~(C)~~ The association of NSA/CSS personnel by name, organization of location with a SIGINT counternarcotics mission is CONFIDENTIAL.

[redacted]

EO 1.4.(c)
P.L. 86-36

DOCID: 4012037

N.C. Gerson, R606



~~(SC)~~ During the Korean War, the USAF's F-86 Sabre jets had a kill ratio of 10/1 over the North Korean MIGs. It was widely believed that this superiority indicated the better reliability and fighting capabilities of US aircraft. This belief, however, was erroneous. The superiority resulted from the knowledge provided by SIGINT. This ratio was possible only because the US intercepted and read instructions to the pilots broadcast by the North Korean control tower on High Frequency (HF). The information was sanitized and given to the pilots as "radar plots." The US pilots knew where to fly to intercept the North Korean MIGs.

~~(S-CCO)~~ But in 1952 North Korea shifted shifted the tower broadcasts to Very High Frequency (VHF). There was no equipment in the field to intercept these frequencies. Without the intercepts, the kill ratio dropped to 2/1. The USAF found the losses unacceptable, so there were stand-downs and limited operations until we could ship the necessary receivers to the field. The official reason given for curtailing US fighter activity was "weather."

~~(S-CCO)~~ When the VHF receivers were deployed, North Korean air traffic again could be intercepted, and US Sabre jets could again be directed to the North Korean flight paths. The kill ratio climbed back to 10/1. In short, SIGINT, not weaponry, provided the margin for victory.

(U) We also might recall that during the battle of Midway, aircraft from distant carriers sank a major portion of the Japanese fleet whose location was derived from SIGINT. These examples amply illustrate that the outcome of any battle strongly depends upon knowledge of the adversary's location, strength, and intentions. The mightiest navy in the wrong ocean, the strongest air force in the wrong region, or the best army in the wrong place cannot win a battle.

(U) Indeed battles, both military and diplomatic, can be won with lesser strength if adequate information is available. Further, intelligence is necessary to a nation's political well-being as well as to its military success. It is the function an intelligence service to ensure that its government is not surprised. It should anticipate the movements and trends of other nations to enable its government to chart its own course and to take advantage of opportunities as they arise.

(U) We must never forget the old Chinese adage: "The commander who will not give silver for information should not be a commander." Funds for weaponry can be cut drastically, but funds for intelligence can be cut only at our peril.

DOCID: 4012037

SIGINT and INFOSEC PROFESSIONALS

HELP WANTED

The Center for Cryptologic History is soliciting your help in obtaining information about past events. The information is needed for a series of studies about events, crises, projects, and programs that have marked turning points in the development of NSA and the cryptologic community.

Send your contribution to:

David Hatch, D93

The Center for Cryptologic History is soliciting your help in obtaining information about past events. The information is needed for a series of studies about events, crises, projects, and programs that have marked turning points in the development of NSA and the cryptologic community. Some of the studies will focus on our role in national and international affairs, others will illustrate how cryptologic information has been used in support of decision makers, and still others will be case studies designed to benefit a new generation. Especially in the development of cryptologic policy and practice we hope to offer "lessons learned," which means including particulars of problems, failures, or negative effects.

We are also very interested in documenting the often unsung but crucial support or "housekeeping" functions which enable NSA and the cryptologic community to stay in business but which often fail to get the recognition they deserve.

D9 has inherited a provisional listing from earlier compilations. But we need your input to compile a more broadly based working list of topics and to reconsider the relative priority of the studies to be produced We believe that each of you has had personal experiences or knows of such matters; it is very likely that every individual is in a position to contribute an obscure fact or a unique perspective.

The form and wording of the questionnnaire are not meant to be delimiting factors but rather, as prompts to your memory. Do interpret the questions broadly, and do feel free to add any information you consider worthy of our attention. (This will be read by human beings!) Our purpose at this initial stage is simply to collect as much information as possible, then collate it, put it into manageable form, and calculate relative priorities for study.

Any length will do, from *War and Peace* to a paragraph, classified appropriately.

Thank you.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012037

Remember to classify appropriately

Name of submitter . . . . . *Present Position* . . . . . .

Organization . . . . . *Building* . . . . . *Secure phone* . . . . . .

Please return your responses, classified as needed, to Dr. David Hatch, D93, SAB 2, Door 22. He can be reached on 972-2355

---

1. Can you recall a situation in which you wished you had a historical background study to reference or consult?

2. In your current operations, would you find a historical study of use? If so, on what subject or of what nature?

3. What other events, projects, or programs might provide beneficial case studies if documented by the CCH or what support functions should be studied? Your responses might be cast in the form:

That was the first case of . . . .

That was the best example of . . . .

We had to change our policy or practices after . . . .

Our work on . . . . . was highly regarded by . . . .

We learned the most from . . . .

New cryptologic employees ought to know about . . . .

4. Are there individuals on board or whom you recall from the past as worthy of special study, as role models or as heroes and heroines of "the business," that you would wish to call to our attention? If so, in what capacity?knowledge or files about the instances listed in your response?

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012037

5. From your own personal observation, what event(s), project(s), or program(s) do you believe best illustrate the support NSA or the cryptologic community has provided to military or civilian decision makers? (This support could be to local- or national-level consumers or even in the international arena.)

6. Conversely, what event(s) provide an example in which NSA or the cryptologic community failed to perform well? Why do you believe that to have been the case?

7. If you have personal knowledge of the cases listed, are you willing to be interviewed by staff of the CCH concerning them or to guide us to other sources?

8. What present or former NSA or SCE personnel can also provide personal knowledge or files about the instances listed in your response?

9. If you have personal files, photographs, or mementos of the cases listed in your response, are you willing to lend them or otherwise make them available to staff of the CCH?

10. From your own observation, what event(s) would you say had the most profound effect on internal NSA or cryptologic community organization, policy, or practice?

DOCID: 4012037

[redacted] 3346

P.L. 86-36

Planning for the Millenium

There will be a problem with processing dates in the year 2000 unless it is fixed by then. That is because programmers are allowing only two digits for the year and assume that the century will always be 19**.

At present there are two principal ways we store dates in computer files. One is ordinal, and has the form YYJJJ where YY is the last two digits of the year and JJJ is the number of days since the beginning of the year. For example, February 4, 1988 would be 88035. The other is the calendar date, in the form YYMMDD where YY is the last two digits of the year, MM is the month, and DD is the day. Both forms are convenient for sorting.

The form of the date itself is not a problem. It's when you try to do something with the date in a program, add or subtract days, compare it to another date, or convert it to another form, that presents a problem:

❒ you can add days, months or years to a date. Most date processing computer programs can add 90 days to 861212 and get 870312, or to 871212 and get 880311 (notice that they are different because of leap year). But not all programs can add 90 days to 991212 and get 000311 (the year 2000 is a leap year). Subtracting days poses the same problem in reverse.

❒ you can compare dates. If you use a straight numeric compare, as most applications do, then 871231 is less then 880101 which is right, but 991231 is greater than 000101, which is not what we want. This situation can adversely affect sorting data in chronological order.

❒ you can convert dates from one form to another. Converting between the ordinal YYDDD format and the calendar YYMMDD format is not a problem because the century is assumed in both forms. (One sidelight: the year 2000 is a leap year but the year 1900 wasn't. So the programs that divide the year by four to see if it is a leap year will convert dates in the year 2000 properly but not dates in the year 1900.)

Note that there are some special cases that conversion programs will not handle properly unless they are fixed, such as a conversion program that assumes the twentieth century; it will not properly convert dates in the twenty-first century to a form that includes the century.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012037

For example, most programs will convert 050505 into "May 5, 1905" not "May 5, 2005". Also, there are some subroutines that will return the day of the week when given a date. For example, 880614 will convert to "Tuesday". As most of these routines assume the twentieth century, they will not return the proper result when given a date in the twenty-first century.

Here are a few applications that may not work in the year 2000 if date processing and calculation routines are not fixed:

- ❒ purge data on the basis of its age. Depending on how the routine is written, all data may be purged!
- ❒ sort data into chronological order
- ❒ calculate a person's age
- ❒ run payroll on Friday

One way programmers can avoid some of these problems is to use generalized date-handling macros, most of which should be fixed by the year 2000. One such macro, BDATE, written for The Conversational Monitor System (CMS) on IBM VM systems accommodates the twenty-first century. BDATE uses a base date number representing the number of days since January 1, 1900. This is compatible with the REXX function—REXX is a programming language for the IBM VM systems—DATE(C) except that on January 1, 2000 DATE(C) will revert to 0 while BDATE will continue. BDATE, which can be called up as a CMS command, a REXX function or a REXX subroutine, has the form

```
BDATE IA <inputs>  (STACK
```

where I defines the form of the input date(s) and A defines the action to be performed.

I can be: S for system date and time

D for an ordinal date or calendar date

T for an ordinal date or calendar date followed by a time (HHMMSS)

B for base date and optionally base time (seconds since midnight)

A can be: C for convert to base date

A for add

S for subtract

D for difference between two dates input

The results (except for difference) will always be the base date, the ordinal date, the calendar date, the day of the week, the month/day/year, the clock time (HHMMSS) and the base time. For an action of D, the result will be the number of days and seconds difference.

For ordinal date or calendar date inputs, BDATE assumes a range of January 1, 1950 (base date 18263) to December 31, 2049 (base date 54787). So 880220 would be February 20, 1988 and 100220 would be February 20, 2010. This will allow calculations that span the centuries and will return the proper day of the week for those days that are in the range. This technique is good for most applications, though some adjustments are necessary for others. For example, ordinal or calendar dates are not adequate as input to routines calculating ages of people born before 1950. The birthdays must be converted to base date.

The base date technique is one method of fixing

For example, the command:

```
BDATE DA 871225 10
```

means add 10 days to December 25, 1987. The result would be:

```
BDATE YYMMDD YYJJJ DAY       MONTH     DA YEAR HHMMSS BTIME

32145 880104 88004 MONDAY    JANUARY   04 1988 000000 00000
```


~~FOR OFFICIAL USE ONLY~~

data files that contain ordinal or calendar dates as sort fields. Since a base date is five digits long, the ordinal or calendar date could be converted to base date and stored in the same space as the ordinal or calendar date and the parameters of sort routines will not have to be changed. Another option is to add the century digits to the date (i.e. 19880613 for an calendar date). This would require that the file be expanded by two bytes and that the sort parameters be changed to accommodate the expanded field.

The base date concept used by BDATE is only one technique for solving the date processing dilemma. Programmers must analyze each problem individually and select the best solution for that problem.

Most systems have a time-of-day clock register that programmers can use for date/time processing. IBM 370 series computers have a 64-bit clock incremented so that 1 is added to bit position 51 every microsecond. The 370 assembler and the various compilers each have macros that access this clock. The epoch (date and time when the clock register would have been zero) has been arbitrarily set by IBM to January 1, 1900 at 0000. With this epoch, the high-order bit was set on May 11, 1971 at approximately 1157 a.m. Unless IBM changes the epoch, the register will overflow sometime in the year 2043.

The problem is not a difficult one to solve but it is pervasive. Most data processing involves a date somewhere. Programmers need to review and correct current processes and also ensure that new systems use date processing techniques that will still work in the twenty-first century.

Question: What is the date of the first day of the twenty-first century?

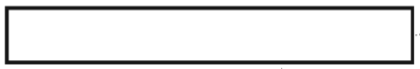
Answer: January 1, 2001. (not 2000. The year 2000 is the last year of the twentieth century.)

Oops!

To the Editor:

Thank you for printing my letter in VOL XVII, No. 1 of the Cryptolog. I note however, that you twice changed the spelling of the word "pejorative" to "perjorative." This is a common mistake, but it is a mistake nonetheless; there simply is no such word as "perjorative."

P.L. 86-36



File missp From line 1

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012037

Reassimilation

David L. Beckner, G05

It's that time of year again, the myriad lists of reassimilees assault all management levels within the Agency. We are asked, once again, to review exhaustive runs of people who are returning from overseas, some of whom have assignments, most do not, etc. Not infrequently during this Springtime ritual, we are admonished from on high by senior management to "give special preference" to overseas returnees. In worst-case scenarios, where a significant number of returnees have not been assigned back at Headquarters, elements are given quotas of how many returnees they will have to absorb. Despite DDA's considerable efforts to manage this problem, it doesn't work, it hasn't worked in decades, and the casualties of the system are those good people who have served this Agency overseas. Maybe it's time we took a different approach.

Consider for a moment who are these people who are returning home. They are some of our best and brightest analysts, collectors, staffers, linguists, or computer types who have risked life, family harmony, and career to serve this Agency overseas. Clearly there are benefits to serving overseas, but each PCS, no matter how glamorous, brings with it the trauma of uprooting family, stresses on relationships, kid's education, etc. The biggest hardship surrounding an overseas tour is the known prospect of having to come back sometime. Most, if not all, of our folks who volunteer for overseas duty do so with an open mind, aware that somewhere downstream they will have to face the agony of the reassimilation process. Yet our people still volunteer to go overseas and the record will show they serve us exceptionally well while detached from Headquarters. This Agency couldn't function nearly as effectively as it does without our overseas civilians. Why, then, when it is so difficult to get some of our best people to go overseas in the first place, do we mistreat them when it's time to come home?

Let's look at the reassimilation process as it now exists. We have, on paper, a system whose objective as stated in PMM 30-2, Chapter 390.8 is to provide "for rotating personnel from field assignments to positions at NSA/CSS Headquarters." The system is administered by M3, M4, the Executive Assignment Panel , the Senior Personnel Board and the Key Components. The essence of the system is geared to identifying positions for returnees a few months before they are scheduled to rotate home. Overseas individuals are allowed to indicate their preferences of jobs. Then, through some mysterious alchemy, returnees' preferences are (hopefully) married with Key Component's offers and vacancies, and the returnees are informed that they will be given xxx job when they return to Headquarters.

Good in principle; poor in practice. Many marriages of the type described above are made; all too often no offers are forthcoming from the Key Components, and the returnees arrive at Headquarters with no position nailed down, and they join the ranks of the untouchables, those lower class persons who literally walk the halls looking for/awaiting employment. Based on my own personal experience of having been overseas in the 1960's and 1970's, and having returned twice, I can tell you our predecessor systems didn't work very well. Based on the number of reassimilation lists routinely floating across my desk, and my own T/A of the number of GS-15's sitting in the cafeteria at 10:00 in the morning, I've concluded our present system doesn't work either.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012037

So, who's at fault, and how can we make the system work better? First, the employees, the returnees, probably are not at fault. They, in good confidence, took the overseas tour and expect to be re-employed upon their return. It's not their fault the present system doesn't work. Then, its not M3's fault—they have a "system" which they administer honestly and they really do try to do what's right for the employees and the Agency at large. I contend the fault lies with "management," that mysterious, anonymous, faceless force within the organization that drives the whole system.

Why is it management's fault? There is a relatively obscure label attached to each overseas position that is called "mission element" or ME. Each ME "owns" so many overseas jobs, is responsible for filling those positions, gets a vote on who is selected to fill the positions, gets to vote on promotions of overseas assignees on their ME's, and who, if all else fails, sometimes has to place (?absorb?) returnees once the rest of the "reassimilation process" has failed. Big responsibility. Lots of power. Why, then, is the ME the port of last resort for returnees? M3's most recent PML (No. 15, 27 Oct 1989) states clearly that all returnees who are not assigned to a HQS position will be assigned administratively to their ME, and that the "returnee's specific position will be determined by management of the organization (i.e., ME) to which the returnee is assigned." Finally, somebody is responsible!

My suggestion, a different approach, is to reverse this whole process, make management do its job in the first place, and place the burden (sigh!) on management of placing returnees BEFORE they ever go. That's right, BEFORE they go overseas. Consider for a moment that the ME gets one (of many) vote on who get's selected for overseas tours. That implies that the ME is the gaining organization, that the ME knows the qualifications of the person being selected for the overseas tour, and that the ME has enough confidence in the individual to say "yes" on letting the individual fill the ME's overseas billet.

Or, look at this proposition another way. View it as a contract. We (management or the ME) make a contract with the employee to go overseas for the Agency, on a ME's billet. The employee also makes a contract to take the tour, to complete it successfully, to get paid, etc. M3 makes a contract to represent the employee while overseas with pay, promotion consideration, etc. L Group makes a contract to ship the employee's household goods overseas, and then back home. It goes on and on. Why not force management, contractually, to send people overseas on its billets AND to have a position waiting for them upon their return from overseas?

My specific proposal is that management, at the precise moment it agrees to sending an employee overseas on its ME billet, also must commit, in writing, what that person's job will be within that same organization upon their return. This approach would solve several problems: It would get M3 and M4 out of the loop (they don't belong, anyway, other than administratively), it would stop the present "reassimilation process" charade we go through each Spring, and most importantly, it would require management to do its job— manage its human resources. It would take some better planning on the part of "management," but that's what managers get paid big bucks for.

My system is not infallible, I know. Some employees wouldn't be happy with their return assignment (most returnees I've known over the years expect to be D/DIR upon their return!), it doesn't account for growth by the employee while overseas, COSC changes, extensions, promotions, or organizational changes within the ME at Headquarters. And maybe my approach won't work with SCEs or STEs; perhaps the Eexecutive Assignment Panel and the Senior Personnel Board need to stay involved at that level. But all of these adjustments could be worked out to management's and the employee's benefit while the employee is overseas, and I, for one, could avoid the annual "reassimilation bugaboo" ritual.

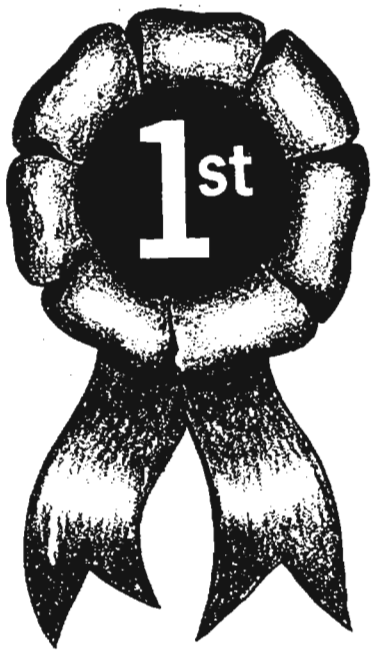
Our people and our reputation as a superb employer deserve better—maybe a new approach is worth trying.

~~FOR OFFICIAL USE ONLY~~

[redacted] E74

P.L. 86-36

EXCELLENCE through EVALUATION



(U) The Evaluation Division (E74) of the National Cryptologic School (NCS) has the job of monitoring the adequacy, relevance, and currentness of training. Its job is an enormous one. In 1989 there were over 700 courses including 200 Learning Center and Extension Services courses delivered at NCS and at fifteen sites throughout the world. Added to this is responsibility for the quality of cryptologic training furnished by the Service Cryptologic Elements (SCEs) whose evaluation methodology they oversee. This challenging task is carried out by 11 people who represent a mix of skills, both operational and academic, which includes a professional statistician and two professional educators as well as analysts, linguists, collectors, training officers, and a computer scientist.

(U) Ever-dwindling resources have led the Evaluation Division to devise smart ways of accomplishing the job with both macro and micro approaches to obtaining continuous feedback on courses. Course evaluations are based in part on responses to machines-scannable questionnaires, one for each learning center or extension courses, and three for each platform course:

- instructor rating
- course rating
- training assessment for student's supervisor

Each form also has a "Comments" section for free-form input in narrative form.

(U) An optical mark scanner scans the forms and automatically enters the data into the database on FLAGSHIP. It flags courses which fall below an acceptable level of performance. Special software compiles statistics in seconds, and allows the Evaluation Division to make various comparisons. For example, students' ratings of a course can be compared with supervisors' rating. Similarly, student ratings of the same course taught by different instructors can be compared. This scheme also permits comparison of ratings by demographic background, such as civilian compared with military, or experienced compared with inexperienced. Above all, it provides verification that courses are meeting their stated objectives and surfaces trends in all categories over several iterations of the course.

~~(FOUO)~~ Data from student questionnaires is only one part of the evaluation mosaic. Another macro

approach is the curriculum review—perhaps the most effective way we have of ascertaining how well a particular course of study is doing. There have been 35 curriculum reviews since the procedure was instituted in 1982. Curricula are selected to be reviewed on the basis of their importance to the Agency's mission and on the date of the last review. Scheduled for review in FY90 are Arabic, Cryptanalysis, Signals Analysis, and Computer Security.

(U) The curriculum review focuses on all courses in a particular discipline. Planning begins about six months before the actual review takes place with the establishment of a working group composed of two or three E74 evaluators and representatives of the teaching department whose curriculum is being reviewed.

(U) First the issues are identified, often with the help of users—Agency elements that are recipients of the training. After the issues are determined, the working group decides on the competencies and perspectives that should be represented on the Review Board. An important criterion for Board members is that they understand future training requirements inherent in technological advances and changing target information. The Board should have the experience and credibility not only to evaluate the relevance and technical adequacy of the current training, but to determine whether the subject is covered comprehensively and to what extent the training impacts on the mission.

(U) A Board consists of five to seven members, headed by a chairman, generally selected from the key component having the greatest need for the courses. The goal is to assemble an unbiased group from NSA operational elements, the military, academia, private industry, and the NSA career professionalization panels.

(U) The Board convenes for four or five days, listening to the teachers and managers who describe their courses and the methodology used. Users from operational areas testify as to user satisfaction with the courses—taking into consideration the structure and sequencing of courses, the quality of the instructional delivery system, the effectiveness of testing, and the communication between NCS and operations. Users are also asked to address future trends in their target that may affect the curriculum under review.

(U) Then the Board draws up recommendations which it briefs orally to the DDET, followed by a written report. Though the DDET is not obliged to act on these recommendations, past history shows that about 85 percent of them are actually implemented. With DDET approval, recommendations are written up as action items and monitored by the Evaluation Division.

(U) As a result of past curriculum reviews, many far-reaching changes have been effected which have had an influence not only on what the NCS is teaching, but on how it is being taught. For example, the Management Curriculum Review in 1989 encouraged the establishment of a management curriculum for mid-level managers to provide the kind of training which previously had been reserved for senior-level managers and executives—the MD-300 series.

(U) The Education Curriculum Review in 1988 was instrumental in more than doubling the number of courses in the ED curriculum (courses designed to train the trainer) and in the promulgation of NCS Administrative Instruction I-10, the Instructor/Course Manager Evaluation and Development Program. This instruction, patterned after the widely-acclaimed evaluation program used in Fairfax County, prescribed for the first time yearly evaluation of instructors by supervisor or a designated expert, to include classroom observation and a developmental plan for improving the instructor's skills.

(U) Another important initiative which grew out of the 1983 Intelligence Skills Curriculum Review was the establishment of the A Group Training Authority. The chairman of the curriculum review and the then Chief of A2 provided a training authority position as a test case, which soon proved to be an important step to a formal, ongoing line of communication between the NCS and Operations. This position was so successful that the 1986 Target Studies

Curriculum Review Board, of which the A Group Training Authority was a member, proposed training authorities for each Group, thus making training an important part of Group-level management. Today, the Group Training Authorities play a major role in the Curriculum Review process. They nominate candidates to serve as review board members, identify key training issues, provide points of contact to give user testimony, help determine which curricula should be reviewed, assist in the implementation of board recommendations, and identify potential adjunct faculty to assist in the review process.

(U) Some recommendations from curriculum reviews have led to special studies, such as a recent study on prerequisites undertaken by the Evaluation Division to determine the validity of all academic prerequisites. The study resulted in over 150 changes.

(U) In addition there is a mini-review process which includes course validation and revalidation. The initial validation of a course or the pilot evaluation is a look at the first or second offering of a course, examining course content, methods of instruction, and instructional materials. The Evaluation Division looks at methods for assessing student learning such as tests, exercises, projects, papers. It also looks at the results of student evaluations and conducts interviews with instructors, course managers, and students. Revalidation, which parallels the validation process, is used for courses that have been part of the curriculum for a while and have been previously validated. The scheduling of revalidation is based on student enrollment and the amount of time that has elapsed since the last examination of the course. The process of revalidating a course includes interviewing supervisors of course graduates and is conducted in sufficient depth to determine whether a full-scale evaluation is necessary.

(U) A specific evaluation plan is designed in coordination with the teaching department and appropriate operations personnel in order to ensure that the evaluation focuses on the issues of concern.

(C) In addition, the Evaluation Division conducts various research projects, such as managing the evaluation of computer-based courseware for GUESTMASTER; [redacted] Another of its larger projects is determining the validity and reliability of 80 to 90 equivalency tests now in use in the NCS. This project is being conducted by evaluation teams composed of professional evaluators, subject-matter experts, teaching department representatives, and a professional statistician who has researched and designed the determinants for test evaluation.

(U) The Evaluation Division is constantly looking for areas where they can make a difference. All of these procedures and programs have one common goal—ensuring quality standards for the NCS.

EO 1.4.(c)
P.L. 86-36

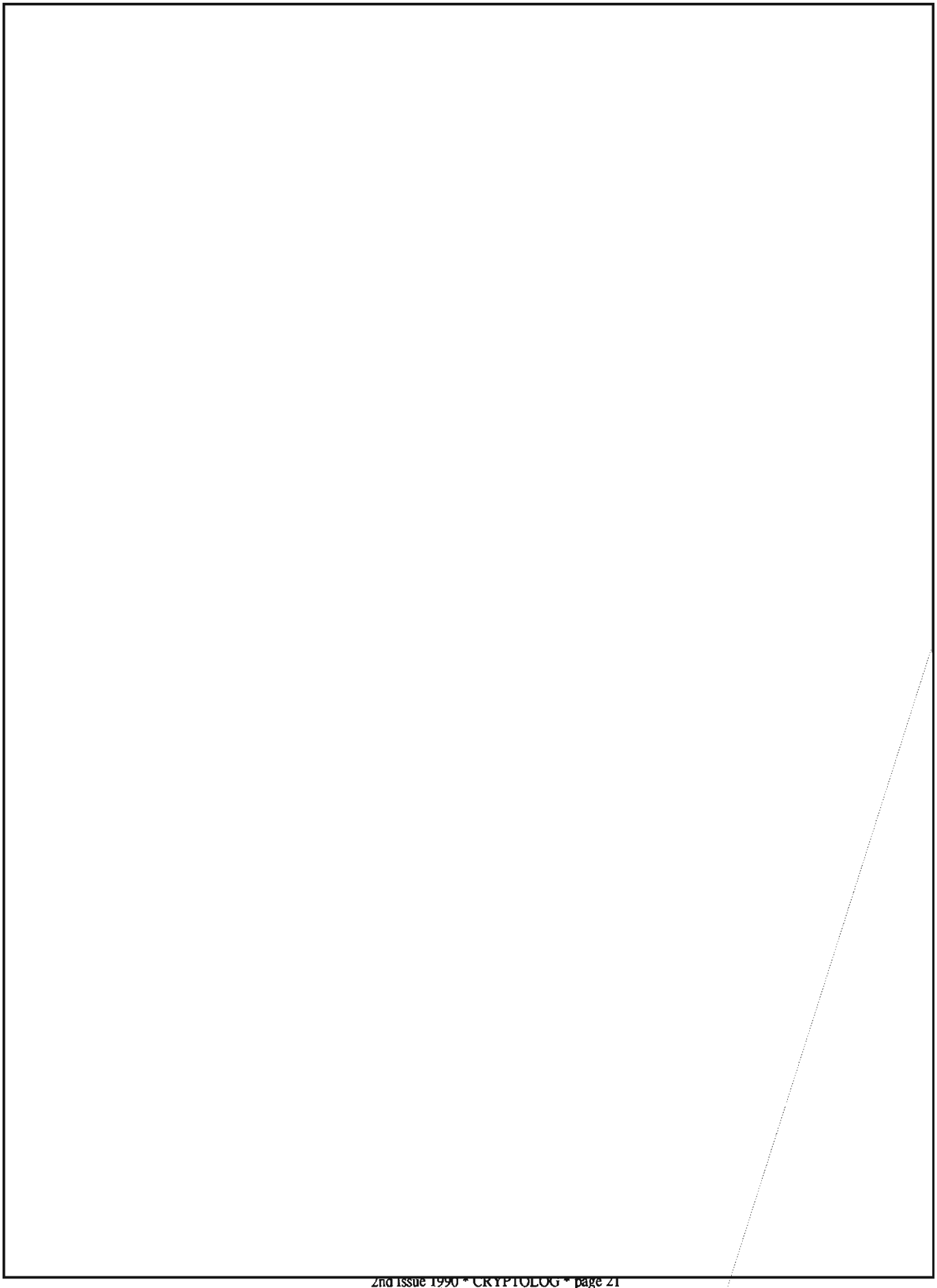
BULLETIN BOARD

GIVING A TALK?

(U) If you plan to use viewgraphs to illustrate your talk, you might want to consult a do-it-yourself packet that contains valuable hints about type face and size, arrangement of contents, and other information to help you prepare legible and appealing viewgraphs. For a copy write to The Editor, CRYPTOLOG, P1, North, giving your name, organization, and building. Please note that telephone requests will not be honored.

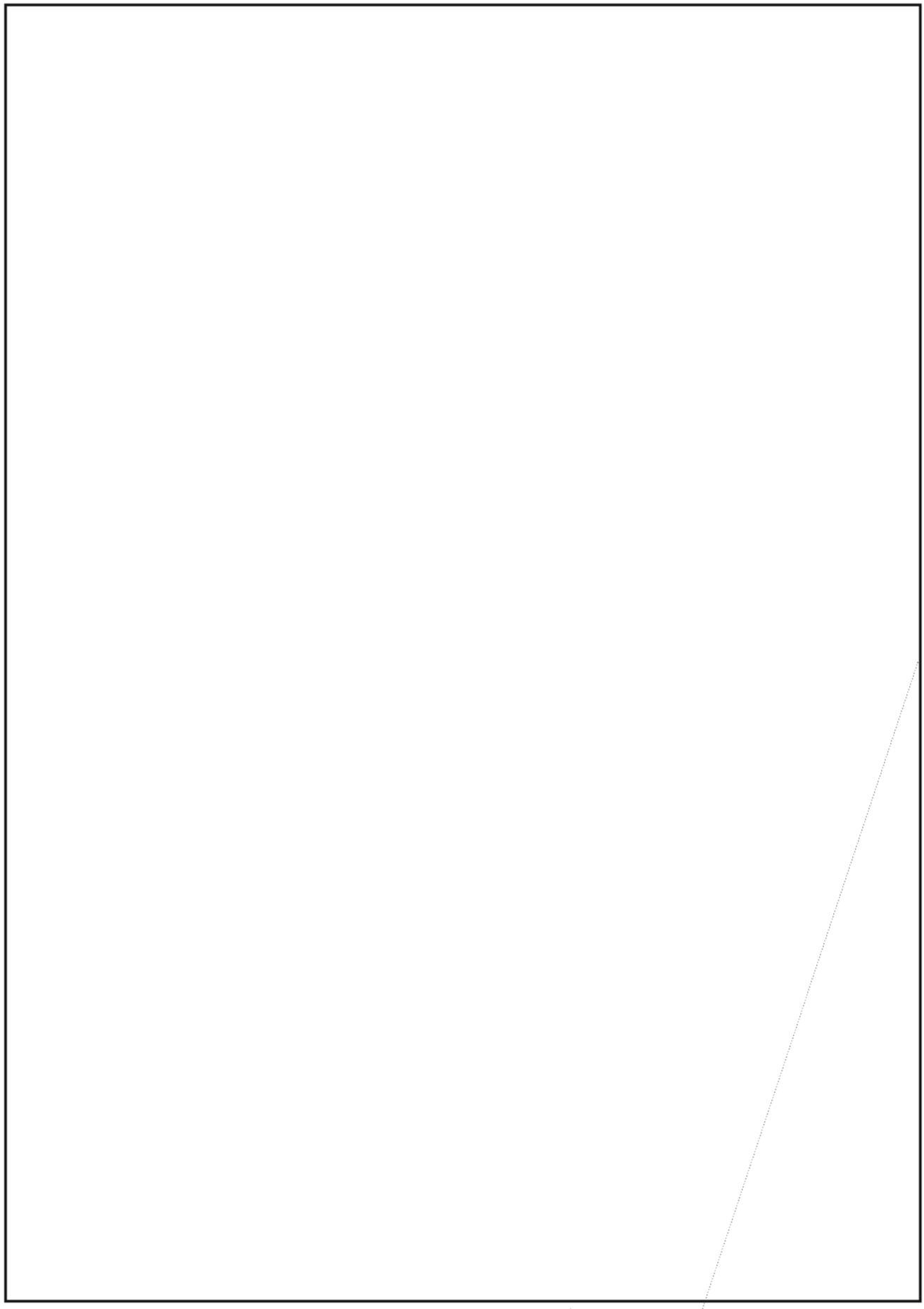
CORRECTION

(U) The correct telephone number for *The Cryptologic Quarterly*, now under D91, is 972-2355.



P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)



~~SECRET~~

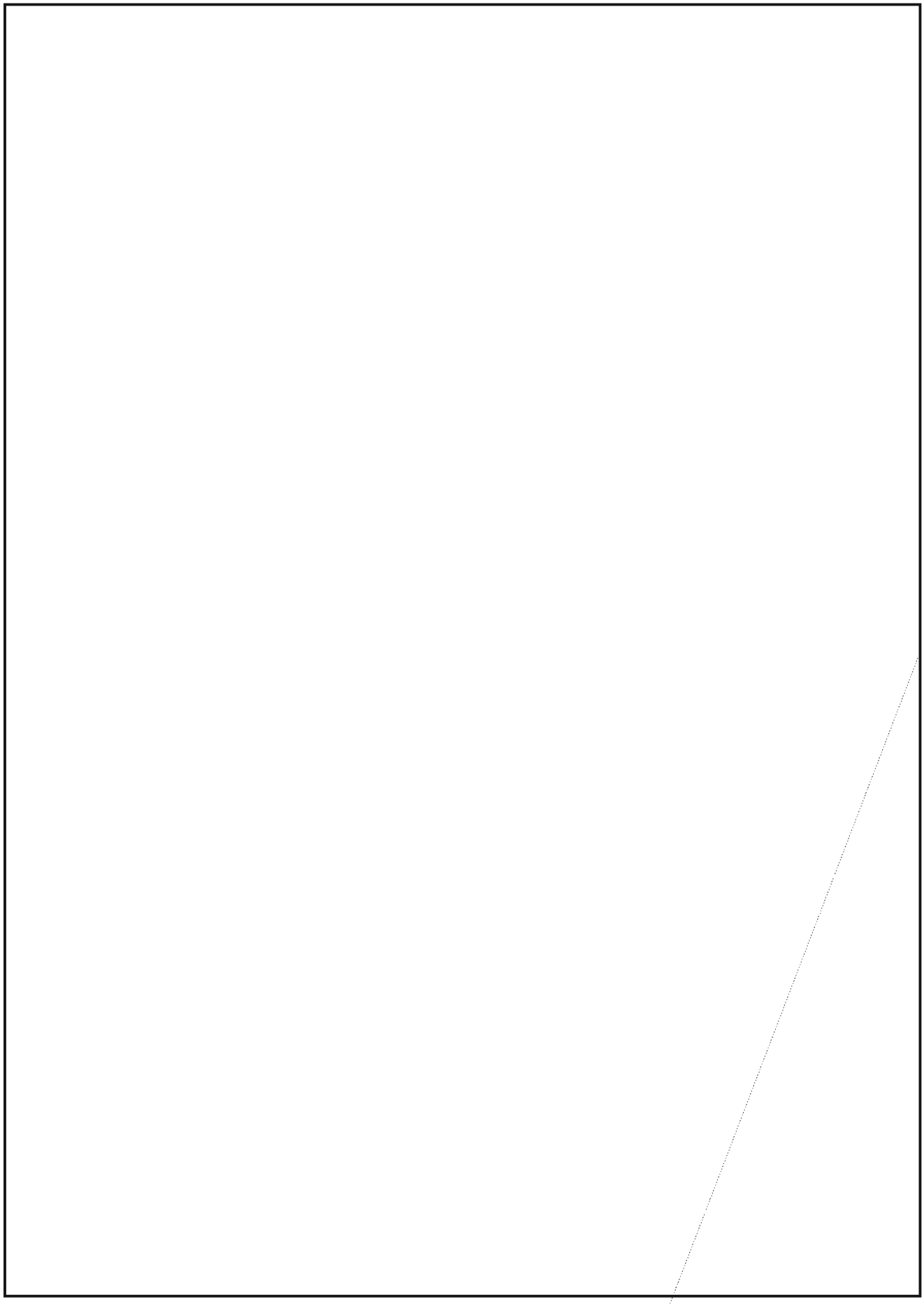
~~HANDLE VIA COMINT CHANNELS ONLY~~

P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

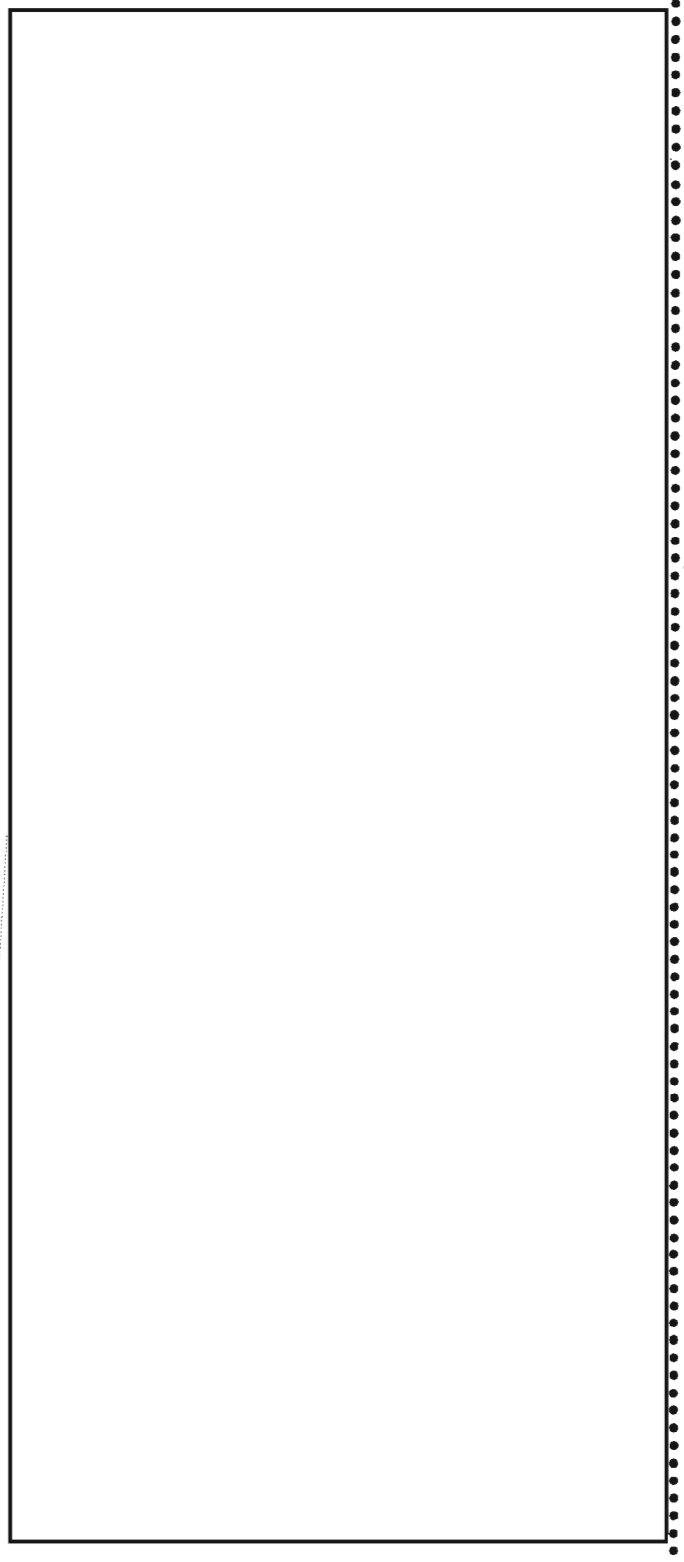
P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

DOCID: 4012037

P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)



P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)



P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

Raw Traffic and Remote Collection

P.L. 86-36

[redacted] P05/SAO

(U) Following is information on two topics that people have been calling about.

RAW TRAFFIC (U)

(U) A question that frequently arises in the Operations Directorate is, "What is the classification of raw traffic?"

~~(C)~~ Raw traffic, when it does not identify a target country nor reveal evidence of precessing is classified CONFIDENTIAL. This pertains only to unprocessed intercept that does not contain operator comments or indications of analytic successes or any reference to case notation or arbitrary traffic designators. This rule applies also to raw traffic intended fo training purposes only.

(U) The classification need not be place on each piece of raw traffic forwarded by courier. But if it is forwarded electrically, the classification, and any applicable caveats, must be placed on the message.

REMOTE COLLECTION (U)

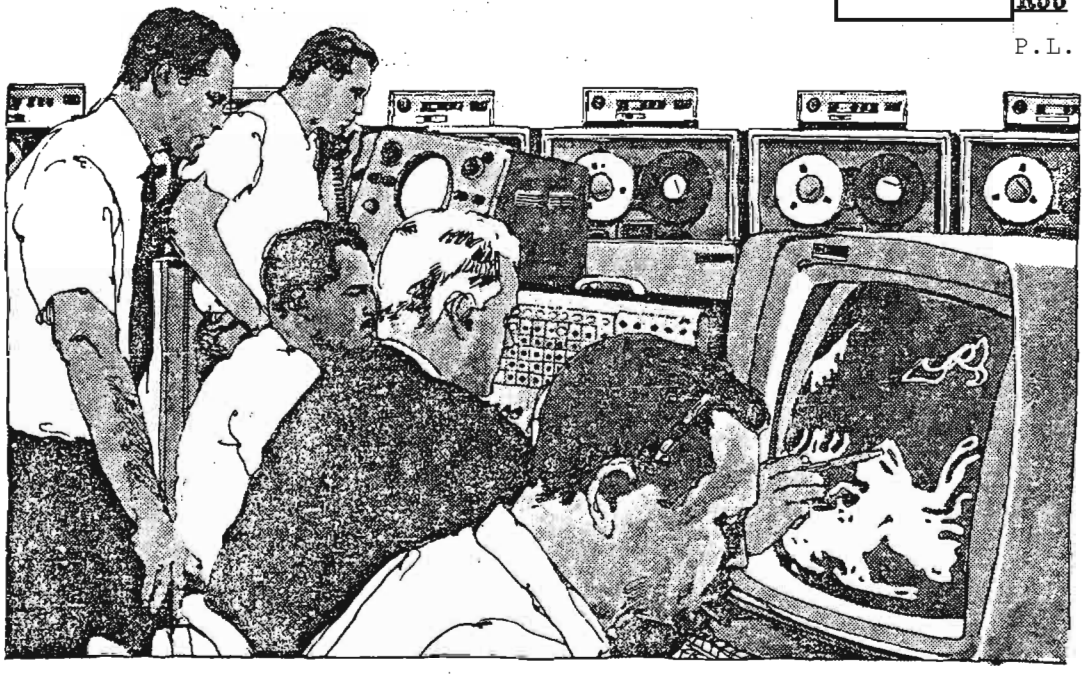
(U) The fact that NSA is involved in remote collection activities when no location or target is identified or inferred has been declassified.

~~(FOUO)~~ When remote collection was a new technology, the sensitivity of the method was protected as CONFIDENTIAL. But because of advance in science and technology, remoting is certainly a "state-of-the-art" capability and its disclosure should not damage our national security.

(U) Note that this change will be incorporated in the forthcoming revision of the NSA Classification Manual.

[redacted] R55

P.L. 86-36



EXPERT VLSI DESIGNER HIRED FOR THREE DAYS

We don't know everything there is to know in our office. As a result we need a little help from time to time. Our last call for help brought in an expert from California. Here's how we did it.

Our key VLSI designer, [redacted] is building a special multiplier for processing large numbers. Bob found a new design in the literature that featured high speed with small physical size. This design is complex, consisting of several pieces that are best visualized in three dimensions. Pictures show only two dimensions, so . . . help!

The author of the design was Dr. Mark Santoro at Stanford University. A call to the University led to a call to Dr. Santoro, who is no longer on the faculty at Stanford, but who agreed to visit and consult on the multiplier, for a fee, of course!

Fee payment for consulting services is something Bob has done before. He arranged with [redacted] our L4 contracting officer, to hire Dr. Santoro through Consumer Sensory Products Corporation, an occasional employer of Dr.Santoro. Since the cost was less than $5000, the PR was processed, with the help of [redacted] in less than a week.

An interesting sideline is that the telephone conversation between our [redacted] and Dr. Santoro was so clear that Dr. Santoro thought we were a local Bay Area company. He accepted our invitation before he realized we were across the nation and not across the Bay. Nevertheless he was on the airplane to the east a few days later.

Dr. Santoro was put to work. In the three days he was here, he gave one briefing to R55, another to R1, and still another to V75. After the briefings Dr. Santoro sat at the workstation with Bob and designed two arrays using the new architecture. The effort produced a family of multiplier designs useful to R5, V7, and R1.

The result is that for a modest expenditure and in a short time we were able to get expert help, all with an ordinary purchase request. As bureaucratic as it sometimes seems, our procurement system can be used in ways that are beneficial to our in-house designers.

We called on expert help, and within a short time, we got it!

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

Rebuttal

[redacted]

P.L. 86-36

P.L. 86-36

(U) A number of us "fallen away" linguists feel compelled to correct what we believe are definite misimpressions given in the last issue's article " A Note on the Linguist Problem." We believe Mr. [redacted] article was an honest attempt to address a perceived problem afflicting the language career field, but we also believe that his basic assumptions are incorrect.

(U) He maintains that there is general agreement on two issues: a shortage of qualified linguists and the fact that linguists leave the field because of a lack of promotion opportunities. While there have traditionally been critical shortages in certain (usually low-density) languages, and while not all linguists (qualified or otherwise) are working in the language career field, the far-reaching statement that there is a shortage of linguists may no longer be true.

(U) With respect to his second assertion, which is the focus of this response, we believe that linguists leave the language field for many reasons, only one of which is promotional considerations. In fact, promotions are probably the least important reason considering the real effort now to promote non-supervisors. One only needs to look at statistics in the latest QMR to discover how untrue is the assertion that one has to be a supervisor to get promoted. Linguists of the younger generation, especially, probably leave not so much for monetary reasons but for personal development. Let us present a few more plausible reasons why some linguists, including the writers of this rebuttal, have left the field.

(U) Linguists leave because they are bored and because they want more challenge than that offered by many language jobs. It is important to understand that not all individuals classified by their job duties as "linguists" love languages enough to make a career of them. Many "linguists" happened to have learned languages in pursuit of area or social studies degrees where languages were a mandatory part of the program. Even language majors were often more interested in the literature, culture, and history of the people who speak the language than in the language itself. These individuals have many other interests besides translating and transcribing.

(U) This brings us directly to another important reason linguists leave, namely the desire to use on the job other skills which they may possess and to develop additional skills or areas of interest. Such skills may include public speaking, political skills, public relations, teaching, representation, writing, and management. While many of these skills can be employed in some areas where linguists work, these skills are more heavily applied in management and staff positions. The diversity of skill usage that such positions offer is very attractive to those who want to exercise or employ as many of their abilities as possible in the process of fully developing themselves and their careers.

(U) A number of years ago it was not unusual to have linguists leave the Agency, not just the career field, because their language skills were so critical that they were not allowed to do anything else. Promotion was not an issue; personal development and job satisfaction were. Even today, many linguists who love language work are frustrated because they see little hope of advancement (read: increased responsibility and challenge — not just promotion) if they stay.

(U) There are any number of negative forces at work that also drive linguists from language work. Every year many very good linguists reluctantly leave the career field because of an inability to pass the relevant language PQE. No one likes to hear this, but perfectly good linguists doing valuable work in their organizations leave because they are tired of banging their heads against the PQE system. We must also mention the linguists who leave because of the "sweat shop" atmospheres that prevail (yes, even in 1990) in their work areas—this includes lousy and overcrowded working conditions as well as the often unchallenging and repetitive, albeit important, language work.

~~(FOUO)~~ [redacted] assumes that it is always a negative when linguists leave the field. We would like to suggest, however, that there are some good things that happen both for the Agency and the persons leaving . The Agency benefits immensely from the cross-fertilization that occurs when linguists work in areas other than DDO. On the one hand, linguists get exposure to the enormous problems and efforts involved in making it possible for linguists to have something to work on. Frequently, their expertise in operations helps those in support areas get a better perspective on how to handle requests for new products, services or improvements to existing support structures. On the other hand, people in support areas get a better perspective from these ex-linguists on what all their work amounts to in the operational arena. Those working in support areas outside DDO sometimes have little idea of how their work contributes to intelligence collection and processing. Even within DDO, former linguists have been known to bring valuable insights to the solution of a problem because of their particular expertise. Indeed, in the collection and processing fields, a first-hand knowledge of language or "analytic" skills often makes the solution more rapid AND more appropriate.

(U) Additionally, linguists, because of their facility with languages, tend to be good communicators. This is one area where "fallen away" linguists make critical contributions. There are several staffs in the agency (Q,J,N, for example) that devote much time to defending the Agency from those downtown who would chip away at, or steal outright, our mission, function, and even life's blood (i.e., budget). Many of these battles are ultimately won because we can state our case clearly and convincingly and many of these cases are written by ex-linguists.

P.L. 86-36

~~(C-CCO)~~ [redacted] seminal article raises other questions that need to be answered, such as: Is the failure to establish viable tech track programs the real reason linguists leave? or What is the real value of staff work to this Agency? or Is it realistic to expect linguists to conduct customer relations, collection management and still have time to process intercepted communications? (NOTE: We take strong exception to many of the author's other assumptions and conclusions, but will leave those topics to others to examine more fully.)

~~(FOUO)~~ We also suggest that this issue is not unique to linguists, but rather raises the broader question of individual growth versus organizational requirements. The author suggests that we collect and decrypt more than we can publish because we lack linguists. How much more could we collect and decrypt if we had more engineers, signals analysts, and programmers?

(U) Any attempt to solve the problem of linguists leaving the career field, if indeed there really is a problem worth solving, must take into account all the reasons for which linguists leave. While we do not pretend a comprehensive approach, we hope the perspectives we have just offered help establish a more complete and correct picture.

EO 1.4.(c)
P.L. 86-36
DOCID: 4012037

Short-Order Translation

Asian Parasite Threatens Bee Population
Italian Expedition Stakes Claim in Antartica
AIDS Information Campaign Extended to Schools
Alcoholism Statistics Worse Than Expected
Quality of Teaching Profession Criticized
Alitalia Increases Capital; Plans Expansion

P.L. 86-36

T5

~~(S-CCO)~~ These are just some of the subjects I've translated from Italian newspapers and magazines as a contract translator over the past few years.

When I moved to my current liaison position at CIA HQS, the job promised new challenges, broader experiences, new perspectives, my own IBM XT, even a work-related parking sticker, but no translating. I wasn't keen on having my language skills slowly rust away from disuse, so I looked for some other way to maintain them, as my use of Italian outside of work was minimal. Freelance translating seemed the logical answer.

~~(FOUO)~~ Since I was on assignment to CIA, it was relatively easy to research its translation service. The US Joint Publications Research Service (JPRS) is a component of the Foreign Broadcast Information Service (FBIS) located in Reston, Virginia. FBIS, an overt operation which falls under CIA's Directorate of Science and Technology, collects and scans over 7,000 foreign newspapers and publications for material to be translated in response to Community requirements. It publishes the more perishable items (radio and TV broadcasts or press reports, for example) in eight FBIS Daily Reports, and passes the less perishable items (newspaper and journal articles, for example) to JPRS for publication as reports.

~~(FOUO)~~ Well, it sounded as if it had possibilities. So I wrote JPRS, and received an application form, background information form, and a language examinationto do at home. The two forms were a couple pages of routine questions on background and experience that I submitted to Q4 for review. The language examination consisted of translating two articles—one economic, the other technical—into "clear and idiomatic English." Once the paperwork was completed, acceptance came in the form of a contract.

(U) Soon after, my Desk Officer sent a welcoming letter and a copy of the *JPRS Handbook for Contractors*, containing complete instructions for handling translation assignments. The Desk Officer, I learned, is the contractor's lifeline to JPRS. She sends assignments, supplies, newsletters and working aids. She also reviews and edits translations for publication, evaluates quality and timeliness of translations as part of the periodic evaluation process and stands ready to answer any questions.

(U) Assignments are made on the basis of qualifications, areas of expertise, and ability to meet deadlines. The goal of FBIS is to get the work translated as quickly and accurately as possible, so it's important that translators keep the Desk Officer informed of the number of words they can

Working Aids

(FOUO) NSA is on distribution for all of the working aids mentioned. T5152 handles internal NSA dissemination and the Reference Section of the Main Library has them all on microfiche. Hard copies of the more recent ones can be ordered through T5152.

(U) The most current list of titles and document numbers can be found in the 1989 Dictionary Issue of *No Uncertain Terms, Terminology Guide for Translators*, another excellent working aid. This bi-monthly publication provides information and guidance to JPRS translators. The publication, containing a wealth of information, is an open forum for any topic related to translating or terminology.

(U) The yearly Dictionary Issue is a compilation of those dictionaries and reference books considered essential for FBIS translations. One section of *No Uncertain Terms* is usually reserved for FBIS Standardization Decisions, such as FBIS rulings on the expansion of acronyms, translation of terms, correct spellings, and so on. It supplements the standardization rules spelled out in the *Handbook* and other working aids mentioned above.

translate each month,and also of any changes in their availability to translate. Since it has no control over the amount received, JPRS can give no guarantees on volume of work to be assigned.

(FOUO) To help the translator JPRS provides several working aids. JPRS publishes many very good glossaries and reference aids on acronyms, abbreviations and specialized terminology. Occasionally it conducts workshops for translators. Technical support is just a phone call away. With regard to automation support, there's the monthly *Newsletter for JPRS Contractors* which provides guidance on putting finished translations into proper software format. There's also the *Automation Guidelines for JPRS Contractors*, an instruction handbook for doing translations on computer. And of course, the Desk Office is always willing to help translator with questions.

(FOUO) Returned assignments are edited and published in about 50 serial reports and ad hoc publications. Most reports are published in two versions: a FOR OFFICIAL USE ONLY version containing material covered by copyright restrictions and distributed to U.S. government consumers only; and an unclassified version containing non-copyrighted material, distributed to US Government consumers and also on sale to the public through the National Technical Information Service.

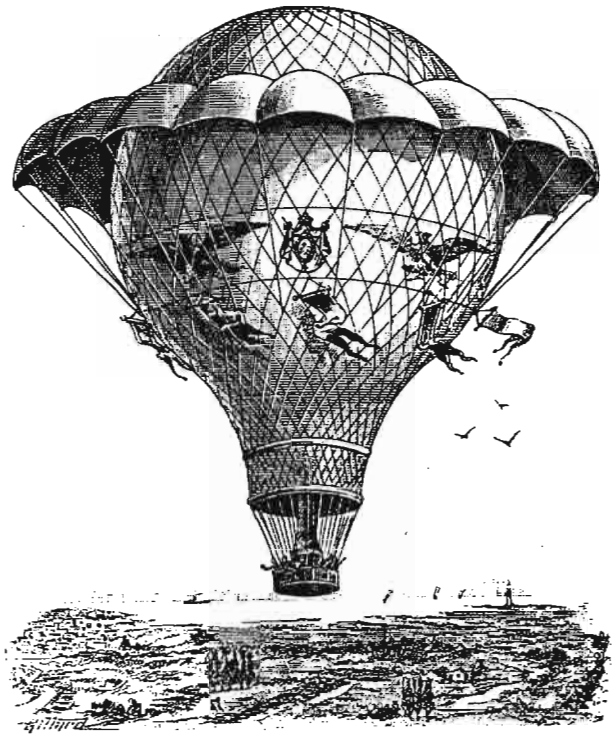
(U) JPRS contracts about 1,000 translators, who do not require US citizenship, to handle the unclassified translations—classified translations are done inhouse for the most part. Independent contractors receive assignments by mail, do their translating at home, and are paid according to a schedule of rates per thousand words translated. Rates are established based on such factors as specialized skills and type of language: selected Asian and East European languages and special technical expertise earn a premium rate.

(U) A new computer editing and composition system was introduced in 1987. The Automated FBIS System, as it is called, requires that all translations be in electronic form. As a result, close to 95 percent of the contractors now do their translating on computer and submit work on diskettes or via modem.

(U) If you're interested in contract translation, JPRS currently needs *experienced* translators in the following languages: Arabic, Cambodian, Chinese, Czech, Slovak, Finnish, Hungarian, Icelandic, Italian, Japanese, Korean, Latvian, Lithuanian, Turkish and Ukrainian. Applications from translators with a knowledge of uncommon languages, such as Kirghiz or Swahili, are always welcome. Applicants should have a good command of written English and should be able to submit translations on computer disk. To apply, send a resume (after Q4 has seen it) to FBIS/JPRS, P.O. Box 2604, Washington D.C. 20013.

DOCID: 4012037

P.L. 86-36



BALLOON-INT, CIVIL WAR STYLE

Today's arcane business of airborne and spaceborne intelligence gathering is a multi-billion dollar industry. However, as complex and as high-tech as it is in today's world, airborne intelligence gathering had a rather simple beginning—during the American Civil War. The Union and Confederates both used hot-air and later, hydrogen-filled balloons to spy on each other. Even back then field commanders were keenly aware of the lack of and the importance of real-time, reliable information on the enemy's intentions, whereabouts, and movements. Observing the enemy from balloons filled some of those information gaps.

Balloons were not new in the U S in the 1860's; in fact, they had been known in this country since their first flight here in 1793. Shortly after the outbreak of the Civil War, balloonists, or aeronauts as they then liked to be called, volunteered their services and their balloons. Perhaps the most famous of these was Professor Thaddeus Lowe, who although he was only 28 years old at the time, had been involved in the science of ballooning for years before the War. In July 1861 Lowe arranged a demonstration of ballooning for President Lincoln and the War Department. At an altitude of 1,000 feet over Washington DC he used the insulated wire anchoring his balloon to telegraph a message to Lincoln saying that from his observation point he commanded a view of over 50 square miles of area. This telegraph message was the first ever sent from a balloon. Thus was born the downlink—albeit an unencrypted one, but a downlink nonetheless. President Lincoln, impresssed by Lowe's demonstration, asked him to form a balloon observation corps and authorized funding and personnel for five ballons and ground support crews.

In an effort to sell the President and War Department on the new balloon technology, Professor Lowe probably stretched the truth and overstated its capability when he told Lincoln that he could see a 50 square mile area, because in actual operations a balloon observer, with the aid of a telescope, could realistically cover an area of about 30 square miles. Once they were put into service and after some trial and error the balloons were equipped with several miles of insulated telgraph wire, signal flags, and searchlights for nighttime use. The insulated wire

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012037

and signal flags were key additions to the inventory since the any information gathered was not worth much if it could not be quickly communicated to the field commanders. The observers soon became adept at counting tents to get estimates of troop strengths and using enemy campfires to spot locations. Surveyers and mapmakers also rode balloons as observers and used the first-hand information they gathered to make detailed maps of terrain features and troop locations for the local ground commanders.

There were however, limitations to the usefulness of Balloon-INT much as there is with modern airborne intelligence gathering methods. Weather was a big determining factor on the balloon missions. Even when the balloons could fly, sometimes the smoke and dust of the battlefield limited or entirely negated the usefulness of the observers. Realizing that being under Union observation made them very vulnerable, the Confederates, like today's armies, learned to deal with the threat. The Rebels became very adept at deception and camouflage—sort of if you can't join them, beat them. They constructed fake gun emplacements and cannons, and put out the fires in their camps or set campfires in dummy camps to confuse the observers. Another tactic they adopted was to make important troop movements at night. Although these measures did confuse the balloon observers, they also cost the Confederates dearly in manpower, time and ease and speed of troop movements

The Union learned just how valuable airborne intelligence gathering, coupled with real-time relay of information, could be during the battle of Fair Oaks (May 31- 1 June 1862). On the first day of the battle Professor Lowe himself was aloft and observed a large concentration of Confederates massing for an assault. His telegraphed information enabled the Union forces to quickly bring up reinforcements and stave off the advance. On the second day, ascending to an altitude of over 2,000 feetover the battlefield and trailing over a mile and a half of telegraph wire, Lowe used an on-board operator to relay situation reports every 15 minutes directly to the "ground station" where President Lincoln was located. It is generally conceded that in the battle of Fair Oaks the fact that ballons were able to make observations and relay them in real-time to the ground did much to avert a stunning Union defeat. Professor Lowe and his balloons played an important role in the Union actions at Fair Oaks. Little did he or anyone else know just how important this battle would be or the effect it would have on the rest of the war. For it was in this battle that the Confederate General Johnston would be twice wounded and have to removed from command. In his place President Jefferson Davis put Robert E. Lee in command of the Army of Northern Virginia—which he held until the surrender at Appomatox in April 1865.

Balloon-INT, like any other INT, has its share of amusing war stories. One such story shows just how important serendipity can be to a good intelligence gathering operation. Richard Wheeler, in his book *Sword over Richmond* which chronicles Gen. McClellan's Peninsula Campaign of 1862, gives an amusing account of an unplanned intelligence collection mission by one of the Union generals. It seems that Professor Lowe had been giving balloon lessons to Gen. Fitz John Porter. On 11 April Gen. Porter decided to make a dawn ascent in one of Lowe's balloons. According to the account, the single rope tethering the balloon snapped like "an explosion from a shell" sending the general and the balloon on an unintended free flight

With Lowe trying to shout instructions up to the general, the balloon began to drift toward the Confederate lines. Gen. Porter then tried to climb the balloon's outer netting to reach the safety valve release rope. Failing in this, he is reported to have calmly climbed down the netting, pull out a spyglass from the gondola and begin reconnoitering the enemy positions. At this point the winds aloft freshened carrying the balloon, Gen. Porter and his spyglass over the Confederate lines deep into enemy territory. While the Rebels tried in vain with their muskets to bring down the balloon; Gen. Porter calmly continued gathering intelligence. For some time the balloon drifted to and fro over the battle front under the helpless gazes of both sides. Finally, the balloon drifted back over the Union side and this time the general was successful in reaching the safety valve rope

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012037

and the balloon landed safely in Union hands. After a rather harrowing experience the general had indeed gotten more than he had bargained for. He got his first-hand, real-time intelligence and an adventuresome flight to boot. Upon hearing of General Porter's adventure, Gen. McClellan, who was Commander of the Army of the Potomac at that time, said that he wouldn't be caught "in one of those confounded balloons . . . " and would not allow any of his generals to go up in them.

Lowe is even credited with creating the forerunner of the aircraft carrier. Quick to realize that mobility and being able to keep pace with the tactical forces he was supporting were important, he developed a riverborne capability. He had a former coal barge converted to a floating balloon support station. Using this vessel he was able to fly his balloons high above the tether ship and be towed up and down waterways making continuous observations over a wider area.

While it is true that in the field of Balloon-INT the Union may have had the upper hand, it wasn't all one-sided. The Confederates realized, probably more so than the Union, the value of balloons for gathering information, and tried their luck. However, like so many things the Confederates tried, the only luck they had was bad luck. Their first attempt in 1861 to build and launch a balloon was an absolute failure. They tried again in June 1862 and were successful. This balloon, tethered to a tug in the James river, was one day left high and dry by the outgoing tide. The Union troops were able to capture the vessel and reel in the stranded balloon. Short of funds for such "experiments," the Rebels were not able to field a third balloon until 1863. In the summer of that year that balloon was blown from its tether by high winds, drifted over the Union lines and was confiscated. This was the last attempt by the South to use balloons in the War, though I believe that Southern generals would have been more willing than their Union counterparts to use observation balloons as part of their operations had funding been available.

Lowe, like many other visionaries, was not fully understood nor completely appreciated by those in power. Early in the war he enjoyed the active support of generals such as McClellan and Porter, but those who succeeded them in the Army of the Potomac were not as far sighted. His new superiors, not sensing the importance of his work, had placed what Lowe saw as unbearable restrictions on his operations, and they had also cut his funding and ground crew support. Lowe became disenchanted and resigned in May 1863. After his resignation his balloon corps died and with it the means to provide real-time intelligence support to ground forces. It would be almost 60 years, during World War I, before U.S. military forces would once again look to airborne intelligence gathering to support tactical operations. One can only imagine what changes would have been made in the histories of such battles as Gettysburg, the Wilderness, Chancellorsville and others had observation balloons and airborne intelligence gathering and real-time information relay continued to evolve.

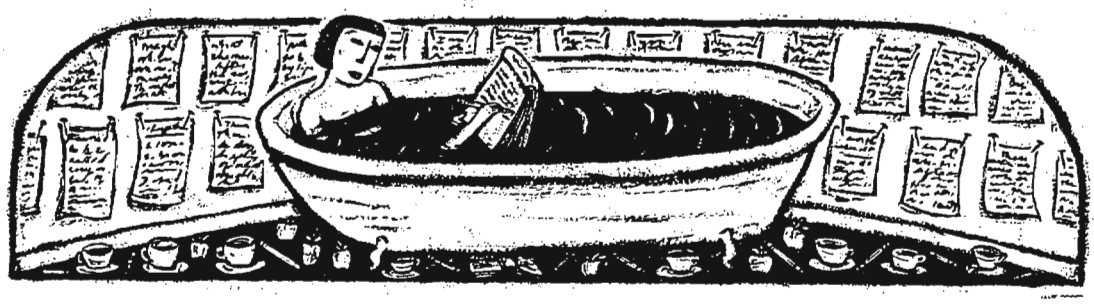
In today's high-tech intelligence gathering business, the concepts that are second nature to us such as downlinks, ground stations, real-time data relay, support to tactical commanders. camouflage and deception all had their beginnings back in the Civil War. We have have refined these concepts to a very high degree using video and digital technology, lasers, spacecraft, etc., but Professor Lowe and his balloons started it all.

By way of giving credit where credit is due, the least we can do is name our next high-tech, multi-billion dollar airborne intelligence gathering system after him.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012037

Letters



To the Editor:

I feel that [redacted] letter to the editor concerning the Multi-Disciplined Analyst Program (1st Issue 1990) betrays a misunderstanding of the program, and perhaps a flawed perception of the purpose of education and training in general. CK-600 is the current incarnation of the Multi-Disciplined program, and the first class, of which I am a member, will graduate in October 1990. At no time before or during my involvement in the program have I been so "naive" as to think that NSA would pay my salary for two years—two years in which I could contribute little to NSA's mission—simply to "enhance my career." I don't mean to say that the agency isn't interested in personal development, but business is business, and businesses invest in education and training because they expect some return. The Multi-Disciplined Analyst Program hopes to produce a set of employees equipped with in-depth knowledge of SIGINT collection, processing, and analysis. It wasn't created to boost the careers of the participants.

[redacted] letter reflects a common misconception about "career-enhancing" programs, including intern programs. NSA is in the business of producing signals intelligence and protecting U.S. communications; NSA is not in the business of making careers. A person's career is his or her own responsibility. Every employee should know that when an employer tells you, "This program will benefit your career," what is actually meant is, "This program will make you a more useful employee." And here's an important tip: being a more useful employee will benefit your career. What you write in your personnel summary is irrelevant if you don't use your background to further NSA's mission.

As far as the advertising hoopla about "technical leaders of tomorrow" goes, I hope the future applicants to CK-600 are analytically sophisticated enough to separate advertisement from fact. Anyone who has ever been in a gathering of interns has heard an agency senior say to a room full of people he or she doesn't know, "You are the future leaders of this agency—the movers and shakers." Any time you hear that sentiment expressed, take a look around you and imagine the people you see as agency leaders. Makes you shake and want to move, doesn't it?

The only thing an education and training program (such as CK-600) can do is increase a person's knowledge. If a person puts that knowledge to the right use, then yes, he or she may well become a technical leader; it's a worthy goal. But you cannot identify a person as a leader by looking at his or her personnel summary. I hope the agency never takes action to "enhance the careers of multi-disciplined people," or of anyone else, for that matter. Basing promotions on "tickets punched" is not good management. The only acceptable measure of an employee is job performance, and if an education and training program improves your job performance, then you're well on the way to enhancing your own career.

I would encourage anyone who is interested to pursue the CK-600 program, because I believe the agency needs people with the background this course provides. Plus, as long as you're interested in meeting that need and not just in filling out a persum, it could make you a more useful employee.

[redacted]

~~FOR OFFICIAL USE ONLY~~ P.L. 86-36

~~CONFIDENTIAL~~

P.L. 86-36

[redacted]

To the Editor

Re: [redacted] article "A Note on the Linguist Problem" in the 1st 1990 issue.

1. For Techtrackers:

```
        ##########################################################
        # This UNIX shell script explains the abysmal            #
        # state of the Agency's SIGINT technical health.         #
        ##########################################################
sed '/Linguists/s//TAs/' article > TAarticle
        # String "Linguist" in article is changed to "TA" in TAarticle
cat << ! >> TAarticle                                    EO 1.4.(c)
```

~~(C-CCO)~~ [redacted] As a group, Traffic Analysts have about one chance in 10 of getting to GG14, less than one chance in 100 of making GG15, and little chance of making STE. For actual working TAs, statistics are much worse: about one in 20, less than one in 400, and nonexistent, respectively. Unfortunately for the Agency, the best and brightest TAs can and do analyze things besides communications. Things like promotion stats, job opportunities, and BS&M (blue smoke and mirrors, aka Techtrack).

```
!
        # Adds additional paragraph to TAarticle.
cat *article > poortechhealth
        # Combines articles on linguists, TAs, IRs, SAs, SCs, Cms, etc
        # into a single report very appropriately named poortechhealth
read poortechhealth
        # Management reads report on technical health of the SIGINT
        # workforce (the folks who actually produce SIGINT and pay
        # the light bill here).
echo "We will do more for our technical people, etc, etc."
        # After upper management review, the usual action is taken.
        # More words are sent forth to pacify the technical rabble
        # while another 50 "fast tracker" managers, staff turkeys,
        # and other strap hangers are quickly promoted.
mv poortechhealth /dev/null
        # Management moves combined report on poor tech health to the
        # current location of Techtrack.
find / -name managementjob -print
        # Techtracker, after hearing the same old words, seeing the
        # action taken, and checking the latest promotion list,
        # locates and prints out a listing of management jobs.
cd /management/newjob
        # Techtracker finds the real answer to personal advancement.
haltsys
        # What BG&E does when you don't pay the light bill.

        ##########################################################
        # End shell script                                       #
        ##########################################################
```

2. For all others:

The gist of the above: "Actions speak louder than words", "As ye sow, so shall ye reap", and BG&E has a solution.

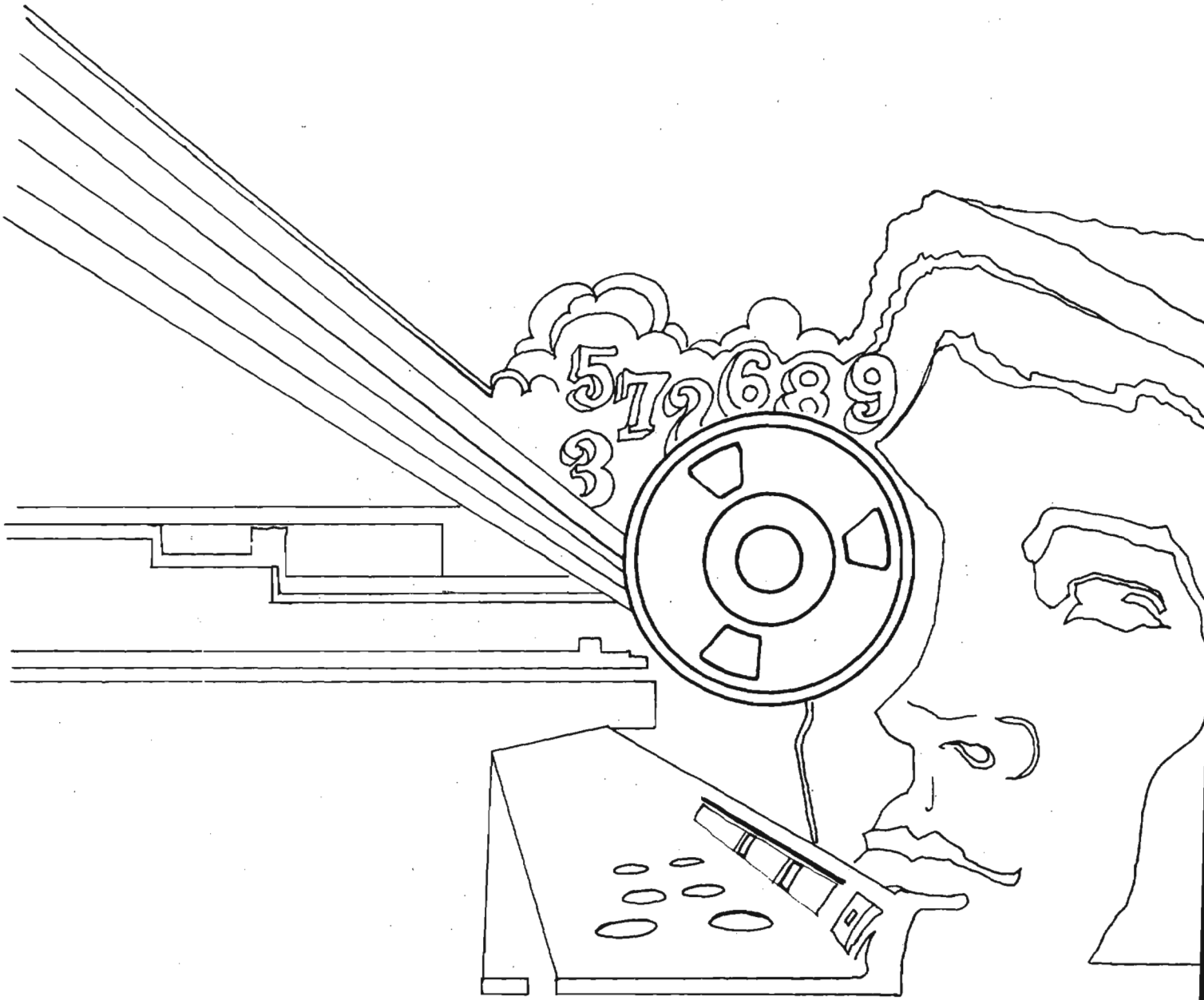
[redacted] P14

P.L. 86-36

~~CONFIDENTIAL~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~



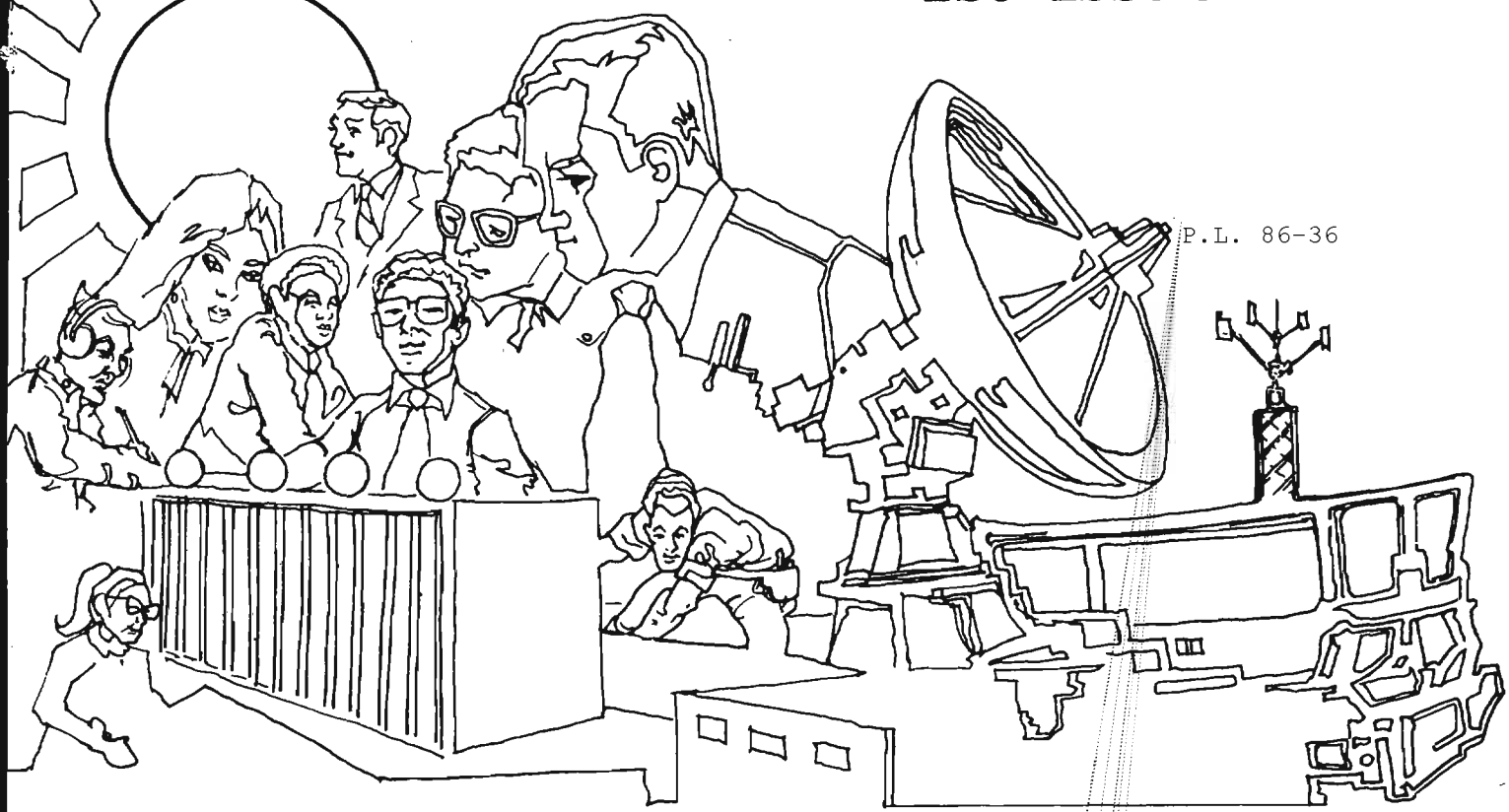
DOCID: 4019716

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

1st Issue 1990



P.L. 86-36

BRAVE NEW WORLD	Gerald R. Young	1
CRYSCOM '89 RECOMMENDATIONS	[redacted]	3
THE COLUMBUS DAY VIRUS	C313	5
THE CRYPTOLOGIC LINGUIST PROGRAM	[redacted]	9
TO NEW AUTHORS		10
A NOTE ON THE LINGUIST PROBLEM	[redacted]	11
THE ROLE OF OPSEC	[redacted]	13
DEPUTY DAWG	[redacted]	15
KRYPTOS ESSAY COMPETITION		17
DAVID HARRIS: IN MEMORIAM		18
BULLETIN BOARD		20
THE MYSTERIES OF GAMMA	Richard Sylvester	21
SORTING, ORDERING, AND HEAPING ON CRAY	[redacted]	22
TECHNICAL LITERATURE REPORT	David Harris	24
BOOK REVIEWS: THE CUCKOO'S EGG	[redacted]	25
REFLECTIONS ON INTELLIGENCE	Vera Filby	29
SOFTWARE REVIEW: MATHEMATICA	Robert Ward	31
LETTERS		32

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~NOT Rreleasable TO CONTRACTORS~~

Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019716

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XVII, No. 1 ..... 1st Issue 1990

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Cryptolinguistics ..... (963-4385)
Index ..... (963-4814)
Information Science ..... (963-3456)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (963-4958)
Special Research ..... Vera R. Filby (968-5043)
Traffic Analysis ..... Robert J. Hanyok (963-4351)

Illustrators ..... (963-6234)
..... (963-6423)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, NORTH 2N018

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five)
(note: no 'o')

via ALLIANCE, send to:
PLBROWN [note: all caps]
attn: CRYPTOLOG

Always include your full name, organization, and secure phone; also building and room numbers.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, NORTH 2N018
Please do not phone.

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

A LESSON FROM AN ARCHEOLOGIST

At a recent meeting of archeologists a foremost member of that tribe made some pronouncements that astounded his fellow professionals:

- He would not appoint anyone to head a dig who could not write and communicate with the public;
- An archeologist who fails to publish (and in good time) is a destructive treasure hunter, not a scholar;
- The one-man-one site philosophy is obsolete.

Then he announced that he was stepping down as the head of his dig to devote himself to writing up earlier excavations.

Now this is bound to have a stunning impact on the conduct of all archeology, for this man directed the excavation of one of the most glamorous finds of recent times. As well as being one of the most respected archeologists ever and the author of seven books and over 100 articles -- all eminently readable -- he has appeared on television and is almost a household name. He could have stayed on, as most others have done, to bask in glory as monarch of a prestigious site.

Instead, he is using his standing to set an example for others, to write up what he had done as a junior when he was not in control of his endeavors.

He emphasized that the head of a dig must be able to communicate, both orally and in writing, with the public as well as fellow archeologists, for it is the public who supports archeology. And it does not do to hoard your findings to write up upon retirement -- you might die before then (this has happened) -- and in any case, the information you are withholding until perfection is reached may be just what's needed elsewhere, and right now. And you certainly shouldn't spend 40 years refining references and footnotes.

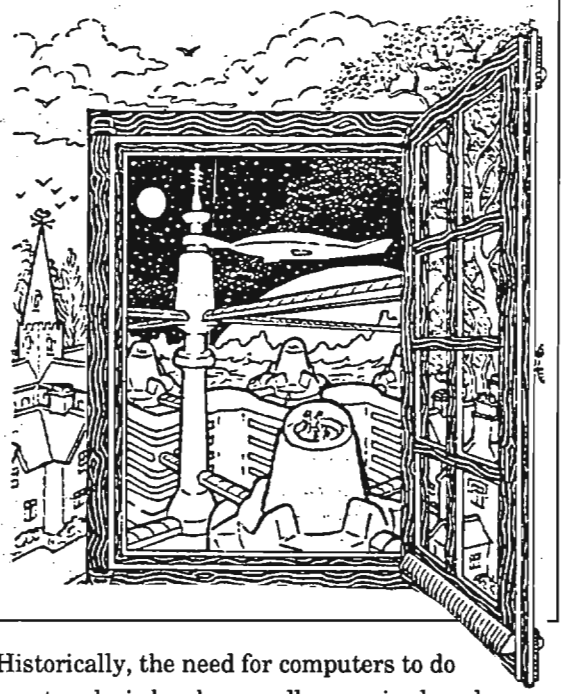
As for one-man-one-site-- teamwork is what is needed by a number of specialists--botanists, anthropologists, epigraphists, geologists, pathologists, and so on. No one person knows it all.

A good example for us all.

DOCID: 4019716

This article is classified ~~CONFIDENTIAL~~ in its entirety

BRAVE NEW WORLD



Gerald A. Young, D/Dir

This article is based on the keynote address delivered at the CRYSCO '89 Conference, 19 June 1989

CRYSCO-89 is the sixth annual Cryptanalytic Software Conference. Its theme is "Brave New World." This represents one of our more important efforts to exploit the potential of a new computer environment for cryptanalytic work.

But before I speak about computing, let me first say a few words about the importance of cryptanalysis to this Agency.

Since becoming Deputy Director, I have spent a considerable amount of time working with the cryptanalytic community as Chairman of the Cryptanalysis Council. I echo and applaud Vice Admiral Studeman's characterizations of the disciplines of cryptanalysis and cryptomathematics, along with their primary support discipline of computer science, as the bedrock of this Agency's mission. I further believe that the way we in the CA community meet the challenge of working in this "Brave New World" is critical to this mission.

Historically, the need for computers to do cryptanalysis has been well recognized, and as a consequence, the cryptanalytic community has continually encouraged the computer industry to produce ever faster machines with more computational power. We have also asked for increasingly "user-friendly" systems with ease of access and data transfer. In fact, for some previous generations of computing machines, NSA needs have been the primary driving force for development. Very early on, we used punched cards and paper tape for both program code and data media. This was followed by the use of dumb terminals for programming and magnetic tape for data, and now we have progressed to smart terminals and electronic links for moving data from machine to machine. Each change brought an improvement in some aspect of our computer resources — sometimes in the form of better response time, sometimes in the form of a more flexible input-output scenario.

In the past, with technology relatively simple compared to today's standards, we developed [redacted] our own operating system, specifically to meet the cryptanalytic challenge. [redacted] has provided outstanding editing and

P.L. 86-36

P.L. 86-36
EO 1.4.(c)

~~CONFIDENTIAL~~

computational capabilities since its inception in 1970. [redacted] The differences caused great difficulties in software exchange and maintenance, and for years we had an environment in which this exchange was very complicated and sometimes impossible to implement. So with the arrival of Cray machines, a conscious decision was made to keep the NSA and [redacted] systems compatible. The formal accord stated that the two Agencies should jointly develop the operating system and utility software. [redacted] I believe that the success of the [redacted] effort is a prime example of skilled people working together cooperatively toward a common goal.

P.L. 86-36

The introduction of stand-alone personal computers removed the need to access mainframes for word processing tasks, but cryptanalytic work on the PCs was less successful owing to an inability to load data easily and to access data bases. However, PCs did point the way forward, demonstrating facilities such as graphics displays, color displays, and local quality printing.

Now let me move to on the present challenge.

We can no longer afford the manpower resources to modify and maintain our own operating system for each individual computer type. There has been an explosion in computer technology. Today we can — and do — network a variety of machines, linking PCs, High Performance Workstations, MINIs, and supercomputers with all types of peripheral equipment, and each component with a different architecture. But all of the new computers — the High Performance Workstations, the MINIs, the SUPERMINIs, and the supercomputers — run a UNIX-based operating system. In view of this, from a management perspective at least, it seems reasonable to move [redacted] to the UNIX operating system.

We realize that this is not going to be an easy transition, especially for those of you who are so familiar with and who have grown up with [redacted] We in management are also aware that resources are currently diverted temporarily from traditional cryptanalysis to learning the C programming language and the UNIX operating system and to converting applications programs. I realize that this is a cumbersome process. But I encourage you to look to the advantages that the new environment offers, and to devise ways to exploit its potential.

P.L. 86-36

You are already beginning to do some CA work on the High Performance Workstations, and special boards are being deployed to do even more complex tasks on the SUNs. As you gain UNIX experience, if you see inefficiencies or deficiencies, point them out to your management and work with the T organization to correct them. Together, we should be able to meet this challenge and refine the system to do an even better job than we have in the past

With the variety of computer resources available to you, I challenge you to find appropriate uses for each of the capabilities, to identify the right machines for a particular task, and to maximize the use of this vital, versatile wealth of computer power. To that end, I fully support the goals of the Cryptanalytic Software Conference, together with the year-round work of its sponsoring organization, the Cryptanalytic Software Committee.

I also see that the conference agenda includes a session where each of the major crypt organizations describes its progress in meeting the challenge of adapting to the new computing environment. I encourage as many of you as possible to go and hear what others have tried, what they have developed, and what they have learned.

Share your ideas and your software! Maximize your resources! By doing so, we can meet the challenge presented by the growing number of cryptanalytic problems we see today. If we do this right, we can insure future cryptanalytic success for years to come. ❑

EO 1.4.(c)
P.L. 86-36

~~CONFIDENTIAL~~

DOCID: 4019716

[redacted] B04

P.L. 86-36

CRYSCO-89

RECOMMENDATIONS

This article is classified ~~CONFIDENTIAL~~ in its entirety

This paper serves as a record of CRYSCO-89. It lists the recommendations and also some observations and comments made during the conference. While the latter are not recommendations, they should be recorded. Note that "observations" are provable statements, while "comments" are the opinion of one (or more) speakers, which you may or may not agree with.

Priorities are included for the recommendations, which will be actioned by CRYSCOM in a timely fashion during the next 12 months. A separate "Recommendation Status" list will be created - and updated - giving current status on each recommendation. CRYSCOM is a volunteer organization, and each organization is requested to share in the work load. Organizations are requested to review the "Recommendation Status" list periodically for recommendations of interest or concern which they would like to pursue.

1. MOVE TO UNIX.

Recommendation: Encourage the move to UNIX, by promoting its advantages, sharing findings, providing examples of how to get the best from UNIX, etc. Discuss advantages and disadvantages of using pipes.

Priority: High.

Observations: UNIX has increased productivity for some. Should do things differently under UNIX [redacted]

P.L. 86-36

Comments: Get on with the move, it's not as daunting as it first appears. People who have used UNIX heavily have come to like it.

2. SOFTWARE PORTABILITY.

Recommendation: Maintain a list of what to do to keep code portable. Establish guidelines on C and FORTRAN inter-callability.

P.L. 86-36

Priority: Medium.

[redacted]

3. SOFTWARE MANAGEMENT AND EXCHANGE.

Recommendation: Establish a mechanism for UNIX to UNIX software exchange. Agree on common conventions on how to send exchanged software; aim at software easy to install by receiving organization. Promote the use of variables (internal and environment) in "make" files.

Priority: Very high.

Comment: Get on with UNIX software exchange. Try it and see.

DOCID: 4019716

4. LANGUAGES.

Recommendations: Promote, explain how, etc., to get autotasking to several CPUs. Encourage discussion on the advantages of FORTRAN and C.

Priority: Medium.

Observations: Modern FORTRAN and C compilers produce code which usually runs twice as fast as IMP compiler code. C compilers are getting better, approaching current FORTRAN compiler.

Comment: IMP is being phased out.

5. WINDOW SYSTEMS.

Recommendations: Teach the terminology of window systems. Encourage use of window systems - preferably a common one.

Priority: Medium.

6. NETWORKING.

Recommendations: Promote goal of networks being transparent to users. Check that response remains good with various terminal configurations (notably SUN workstations) at peak loading. As appropriate, keep users informed of security issues.

Priority: Low.

7. HARDWARE.

8. COMMERCIAL SOFTWARE.

Recommendations: Complete and maintain catalog of who has what. Expand above to include use and evaluation of the software. Include list of people able and willing to help others use the product. Expand subject to include public domain software. Encourage progression to standard products.

Priority: Very high.

9. CRYSCOM DISTRIBUTION.

Recommendation: Distribute relevant papers, info., etc,. through CRYSCOM channels.

Action required: Each organization should inform CRYSCOM Executive Officer of changes, additions, deletions, etc., required for their organization.

Priority: High.

10. WORKING GROUPS.

Recommendation: Create working groups to study topics of interest. Provide terms of reference, timetable (2 to 3 months) and monthly reporting mechanism.

Potential subjects: Crypt techniques - what is available where. Sorts - what do we need under UNIX. System accounting under UNIX.

Priority: High.

11. TOPICS FOR UNIX BROWN BAG SEMINAR (UBBS)

Recommendations: NFS, NQS, "lex" and "yacc". UNICOS 5.0 facilities. Other system upgrades.

Action required: Present seminars once a month or as needed. Organizations to volunteer speakers for topics they can cover.

Priority: High.

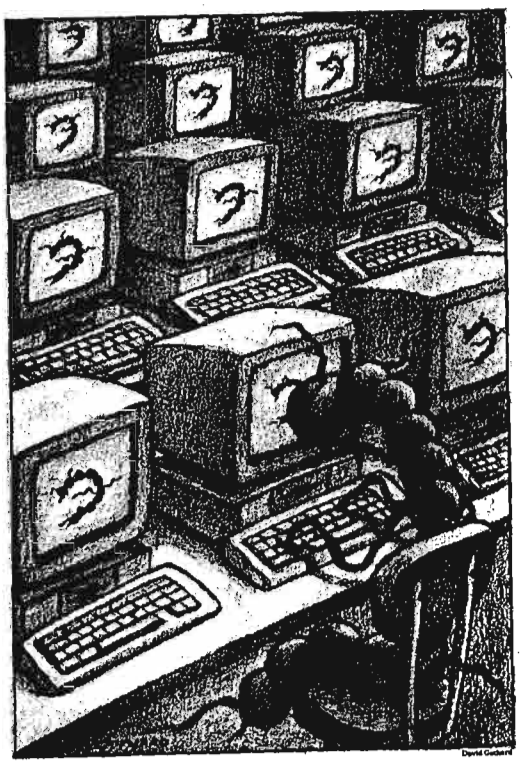
12. SUPERCOMPUTER SYSTEM SOFTWARE SUPPORT.

Recommendation: Provide priorities to T335.

Priority: High.

Comments: Recognize that T335 has a lot to do and cannot do it all at once. Appreciate T335 contribution to the crypt community. ❐

DOCID: 4019716



THE COLUMBUS DAY VIRUS

C313

There has been public and governmental apprehension about a possible computer virus attack designed to be launched Columbus Day, October 12. Therefore the National Institute of Standards and Technology compiled information from public sources about the "Columbus Day" virus and computer viruses in general and issued a statement to the press. The statement was prepared in conjunction with the National Computer Security Center and coordinated with the Software Engineering Institute. In summary, it found no evidence that the virus has spread widely in the US.

Then C313 conducted an independent analysis of the Columbus Day virus, more properly known as the DATACRIME virus. It verified that the characteristics of the virus do indeed match those reported publicly, and will, upon execution between October 13 and December 31 inclusive, make hard disks unusable.

Concern has focused on the possibility of widespread damage on IBM personal computers and clones running the PC-DOS or MS-DOS operating systems. Most researchers on computer viruses believe that the virus in question is a member of a virus family known as "DATACRIME." Since attention has first been drawn to this virus, there has been a lot of analysis as well as public discussion on its characteristics. The results of disassemblies, along with descriptions, have been posted on electronic digests, such as VIRUS-L. Most everyone participating in these discussions has come to the same conclusions, in which C313 researchers concur on the basis of their own work.

PUBLICLY REPORTED ACCOUNTS

While the virus has been referred to as the "Columbus Day Virus," it is more correctly referred to as the DATACRIME virus. It was reportedly released on March 1, 1989, somewhere in Europe. This virus is currently reported to have two versions, of which one version also has two strains.

Editor's note: This article is based on a report released prior to Columbus Day 1989 for internal NSA use.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019716

Reported Size / Version

One version of the DATACRIME virus has two strains which are named by the number of bytes by which the virus increases the size of infected files. One of the strains has a size of 1,168 bytes and the other has a size of 1,280 bytes. There is still another version of this virus, most often referred to as "DATACRIME II," about which little information has been reported. It is believed that its size is still larger than that of the other version.

Reported Propagation

The 1,168 -and 1,280-byte strains of the DATACRIME version propagate to files with ".COM" name extensions (with the exception of "COMMAND.COM"). The DATACRIME II version infects files with either ".COM" or ".EXE" name extensions.

Reported Mission

Both versions of the virus perform a low-level format of cylinder zero on the "C:" hard disk drive. This action will destroy disk directory information, thereby making the hard disk unusable.

Upon activation, the DATACRIME version displays the following message:

```
DATACRIME  VIRUS
RELEASED:  1  MARCH  1989
```

The DATACRIME II version displays this message upon activation

```
*  DATACRIME  II  VIRUS  *
```

Reported Date of Activation

For both versions, the mission of the virus is triggered upon execution of an infected file after October 12 (i.e., October 13 or later).

Reported Characteristic Strings

For the DATACRIME version, the 1,168-byte strain contains the hexadecimal string 'EB00B40ECD21B4', and the 1,280 byte strain contains the string '00568DB43005CD21'. A characteristic string for the DATACRIME II version has not been reported.

C313 ANALYSIS

In most cases we confirmed the reports by both static and empirical methods. Static methods included reviewing hard copy of disassembled virus code, while empirical methods included observation of the actions of the virus on isolated systems and analyzing actual code with utilities such as debuggers. The empirical methods were performed on three different systems: an IBM PC with two floppy drives, an IBM PC-AT with one high-density floppy and one 30-MB fixed hard disk drive, and an IBM PC-AT with one high-density floppy and two 10-MB removable cartridge disk drives. In several cases we were able to glean additional information that was not mentioned in the public reports.

Size / Version

Static and empirical methods confirmed that the two strains of the DATACRIME version increase the size of infected files by 1,168 and 1,280 bytes respectively. In addition, we determined that the DATACRIME II version increases the size of infected ".COM" files by 1,514 bytes. The DATACRIME II version increases the size of ".EXE" files by a non-constant number of bytes, usually between 1,500 and 1,800 bytes. Additionally, a large portion of the DATACRIME II version is stored on disk in a simple encoded format and is decoded prior to execution.

Propagation

Static and empirical methods confirmed that both the DATACRIME and DATACRIME II versions of the virus propagate to files with ".COM" name extensions, while only the DATACRIME II version infects files with ".EXE" name extensions. We were also able to clarify the report that the virus would not infect the "COMMAND.COM" file. Actually, neither version will infect *any* file where the seventh character is a "D". Additionally, both versions will infect only one file per execution, and both will infect files as long as the system date is between January 1 and October 12 inclusive.

Mission

Static and empirical methods confirmed that both versions of the virus perform a low-level format (INT 13, function 05) of the 80H

~~FOR OFFICIAL USE ONLY~~

OCID: 4019716

drive (usually a hard disk drive, most often named "C:"). Additionally, this operation will format up to 10 surfaces of a disk. Both methods also determined that the text strings printed by the versions of the virus match those reported in public sources. The text strings in both strains of the DATACRIME version are stored in an encoded manner instead of plain ASCII. As previously mentioned, the DATACRIME II version is almost completely encoded.

Date of Activation

Static and empirical methods confirmed that both versions of the virus will activate their mission when the system date is between October 13 and December 31 inclusive.

Characteristic Strings

Static and empirical methods confirmed that the publicly reported characteristic strings in the DATACRIME version do actually exist in the code. The 1,168-byte strain contains the hexadecimal string 'EB00B40ECD21B4', and the 1,280 byte strain contains the string '00568DB43005CD21'. Additionally, we have determined an acceptable characteristic string for the DATACRIME II version, which is 'F8C288BF26CF8F81D9'.

OBSERVATIONS

Based on our analysis of the virus and a review of related information, we have some comments on various issues that are not necessarily covered by the items of interest we have identified so far.

Development of the Virus

We believe the DATACRIME version was the first version released, because of its relative simplicity in comparison to the DATACRIME II version. In addition, we believe that the 1,280-byte strain was the first of the two strains of the DATACRIME version. While the 1,280- and 1,168-byte strains both contain duplicate code in many places, the 1,168 has improved efficiency in some places, most notably in the smaller size. The DATACRIME II version, however, has many improvements over the original DATACRIME version, in that it infects both ".COM" and ".EXE" files, and makes primitive attempts to hide itself with encoding.

Detection

There are several ways this virus may be detected. One is that there is an increased file size upon infection. Another, one of the easiest ways, is to search for the characteristic string(s) of the virus is using a tool such as The Norton Utilities**1 or the DOS DEBUG utility.

Finally, the virus may access other floppy or hard disks in its attempts to propagate. It may be detected by such unexpected accesses.

Recovery

Our analysis has shown that the average DOS user will find it difficult to recover from this virus. Both versions of the virus do a low-level format of the hard disk upon activation, which standard DOS utilities cannot overcome. The best advice for average DOS users who need to recover from the malicious actions of this virus is to seek help from a local expert on DOS.

For individuals who believe themselves capable of restoring a system, there are really two cases to consider. The first (preferred) case is where backups of critical data have been kept. The second case is where no backups have been kept, but critical data must be recovered from the disk. Note that the procedures below do not address the possibility of non-DOS partitions and systems present on the hard disk. Specific knowledge of those systems will probably be necessary to restore non-DOS partitions. We will only address DOS partitions here.

▸ *If backups have been kept, the following procedure should be used by a knowledgeable user to restore the DOS disk partition:*

1. Boot from manufacturer's DOS floppy
2. Restore disk partition table using a tool such as The Norton Utilities
3. Format DOS partition (may require an initial low-level disk format to make the disk bootable)
4. Restore all files from backup EXCEPT executables (those with ".COM" and ".EXE" name extensions).
5. Reload all executables from manufacturers' disks or re-compile local source files to produce executables.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019716

▸ *If backups have not been kept, the procedure is much more difficult. In fact the following procedure may be more difficult than retyping text and data files by hand from hard copy:*

1. Boot from manufacturer's DOS floppy
2. Restore disk partition table using a tool such as The Norton Utilities
3. Attempt to recover critical text or data files from disk using a tool such as The Norton Utilities; note that this may require searching entire disk for data blocks related to a particular file
4. Save recovered data or text files to floppy disk
5. Format DOS partition (may require an initial low-level disk format to make the disk bootable)
6. Reload executables from manufacturers' disks
7. Reload saved data or text files

THREAT

We feel it is important to address the potential threat of this virus. To date, there have been very few reported cases of this virus in the US. Most of the interest we have seen in this country has been from a technical standpoint or from rumors in press accounts, and not from victims who have been attacked and seek a remedy. As a result we feel that the current versions of this virus pose a small threat to US systems.

Note that there appears to be no specific year associated with the actions of this virus. If an infected file is executed between January 1 and October 12 of any year, it will try to infect other files. If an infected file is executed between October 13 and December 31 of any year, it will attempt to format cylinder 0 of a hard disk drive. It would be prudent for people who detect the virus or those whose disks are damaged by the virus to look for other infected files on the floppy disks they use as well.

CONCLUSIONS

The C313 analysis has shown that the DATACRIME virus does indeed match the characteristics that have been reported through public sources. Its intent is malicious, and it will format cylinder 0 of the "C:" hard disk drive when activated on or after October 13. It is important to mention that owing to the difficulty we had in obtaining a copy of this virus, and given the comments in publicly-available sources, we do not believe that this virus has spread widely in the US. Therefore, we do not rate this virus as any more important than other currently known viruses. However, the lesson to be learned from this virus and others is that good prevention techniques need to be applied all of the time, and not just in times of reported outbreaks of viruses.

ACKNOWLEDGMENTS

The following C313 researchers participated in the analysis of the virus in and the preparation of this report:

Research material for this report was obtained from the following sources:

David Chess, IBM; David Brown, Department of Energy Computer Incident Advisory Capability (CIAC); Ken van Wyk, DARPA Computer Emergency Response Team (CERT).

A Note to Subscribers

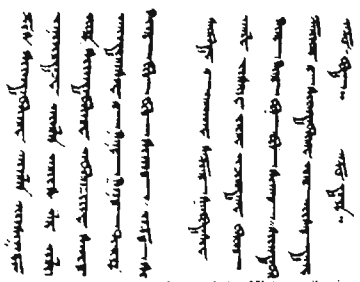
The distribution for this issue reflects changes received by COB 4 April 1990

~~FOR OFFICIAL USE ONLY~~ P.L. 86-36

DOCID: 4019716
P.L. 86-36

~~SECRET~~

THE CRYPTOLOGIC LINGUIST PROGRAM



UIGHUR SCRIPT. The writing of the Uignur tribe in central Asia and western China in the medieval ages. Sometimes written horizontally.

PASSEPA SCRIPT. Established by Kublai Khan in the 12th century as the official international script of the Great Mongolian Empire.

KÖK TURKI RUNES (ORKHON SCRIPT). The writing of pre-Islamic Turkic peoples in northern China about the 6th century.

[redacted] P16 P.L. 86-36

~~(C-CCO)~~ The Cryptologic Linguist Program began with the perception that there is a need to have a pool of multilinguists ready for immediate deployment against language problems as they arise, rather than to attempt to identify, recruit, and train linguists to attack a problem that has already grown to critical proportions. The concept is deceptively simple. All one needs to accomplish that end is the ability to look twelve months or more into the future [redacted] Failing that, one takes an educated guess and begins recruiting and training people in languages that appear to be the best bet.

[redacted]

[redacted]

(U) As the present tendency is to follow the inclinations and desires of the individual program member in broadening the language base by family or area as long as the languages fit into the perceived needs of the Agency, all three paths are being followed.

~~(FOUO)~~ Linguists are brought into the Program through one of two paths: direct hire or on-board recruiting. Direct hires have either postgraduate degrees in a language or in a discipline that requires a strong language minor such as history or linguistics, or a demonstrated proficiency in more than one language with very high aptitude for learning languages. On-board recruiting is done by advertisement through M36 to all Agency elements. Successful candidates for entry into this three-year Program are already certified in at least one language and have developed reputations as high achievers in their assigned elements.

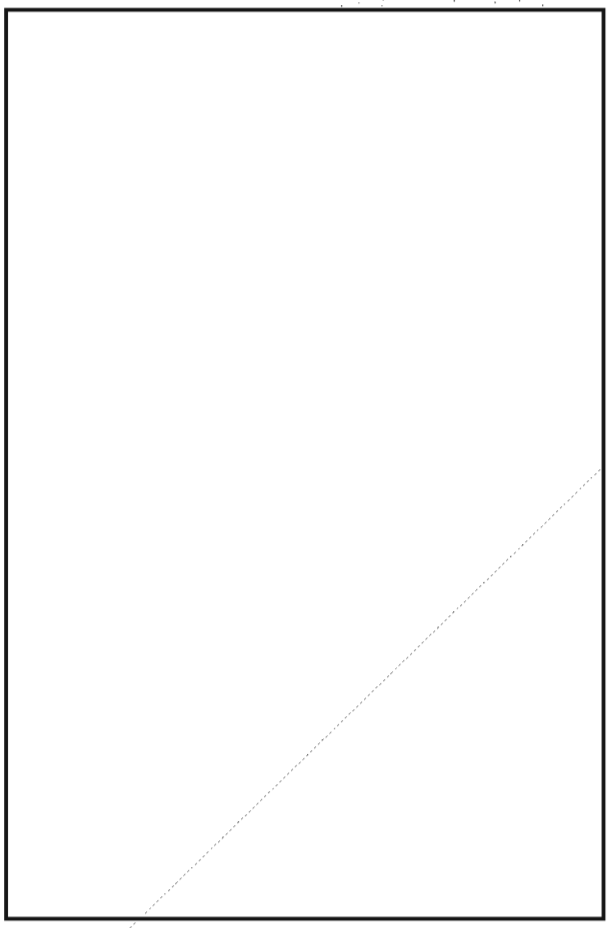
~~(C-CCO)~~ Administration of the Program is modeled on the intern programs, in that members are detailed to six-month tours over a three-year period (more or less), with training in language and associated skills as with interns. The major difference is that since the members enter the program with widely varied skills and backgrounds, individual goals are stressed more than common milestones. When

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~
EO 1.4.(c)
P.L. 86-36

DOCID: 4019716

language skills permit, the members tour across groups (A & G, A & W, G & B, etc.) and field sites to broaden their knowledge and perspective. Graduation from the Program is contingent upon fulfilling two conditions: certification in a target language (or a new target language in the case of on-board hires), and assignment to a billet in an Operations organization.

~~(C)~~ The Program was initiated on July 1974 with a memorandum from LtGen Allen, DIRNSA/CSS. directing that a three-year program be initiated, designed to "develop a corps of cryptologic linguists performing tasks in support of the linguistic effort of the Agency, who are capable of operating effectively in several languages and to emphasize in this group the broad application and development of linguistic proficiency across the cryptologic spectrum." The Office of Techniques and Standards (P1) was directed to administer the Program, and that administration was delegated to the Languages and Linguistics Division (P16).



TO NEW AUTHORS

Once you've written your article, the hard part begins--editing your own work. A good writer is a rewriter: improving, simplifying, clarifying. Sometime stop at a library that has the ms collection of a noted author; you'll see evidence of many, many revisions.

How to start?

First, set the paper aside for a week or two "to develop the flavor" as the cookbooks say. Print it out double-spaced in a monospaced font. Review the hard copy. A little distance will give you fresh perspective. Obvious flaws will shout at you. Mark the changes in a bright color.

Fix the soft copy, reprint it, and check for wordiness. Every word or phrase should be load-bearing. Reduce "during the FY91 time frame" to "in FY91;" "at this point in time" can be boiled down to "now." Readers just will not wade through thickets of dead wood.

Reprint.

Once the text is lean, the organization of thought should be clear. Check the first paragraph. Will your point be evident to readers and invite them to read on? If not, reword it. Does it look like alphabet soup? An excess of abbreviations and acronyms is poison.

Fix it. Reprint.

Do a field test. Find a reader, a good and true friend, who will mark the text wherever there is an unclear passage, wherever something isn't just right. Take the comments in good heart. Keep in mind that not every reader is as up on the subject as you are, and might need an explanatory phrase now and then.

When you've honestly done as much as you can, send it on to CRYPTOLOG. If you prefer, you may call one of the subject editors for aid and comfort.

EO 1.4.(c)
P.L. 86-36

DOCID: 4019716

A Note on the Linguist Problem

[redacted] G142

P.L. 86-36

~~(C-CCO)~~ There seems to be general agreement on at least two aspects of the linguist problem at NSA: [redacted] and, linguists are leaving the language career field because they see better promotion opportunities in the management or staff career track. This has a deleterious effect on intelligence production, because most of our targets perversely persist in using languages other than English, thereby forcing us to rely on linguists to make sense of the traffic. While management stresses the importance of linguists, it does not seem to be overly concerned by their exodus since it has taken few effective steps to correct the problem. The one substantive step, the FLIP program, fails to address the problem because it attempts to substitute token premium pay for what employees really want, namely, promotions

[redacted]

collection staffs in order to enhance their careers, there seems to be some justification for this approach. One can find former linguists at all levels of NSA's management structure. They probably would not have gone as far had they remained working linguists. The fact that there are breathtakingly incompetent managers who have somehow reached relatively senior positions could reinforce the perception that the management track is a relatively easy and foolproof path to career advancement. Still, one wonders which is easier to replace, a mediocre office chief or a mediocre Hungarian linguist?

(U) In spite of the management's protests, linguists will probably continue to leave the language field as long as the current situation persists. In other words, the lack (or perceived lack) of linguists stems from certain management decisions that can only be corrected by the management. Should management bother to do that?

(U) It is obvious that we are currently witnessing profound upheavals that will shape the world situation for years to come. Since our government finds itself more and more frequently in the uncomfortable position of having to make important decisions on increasingly short notice, the need for timely, relevant, and above all plentiful and accurate intelligence is greater now than at any other time in the recent past.

~~(C-CCO)~~ Even though NSA claims to be an analytic and reporting agency, a great deal of its budget is spent on machinery and resources needed to operate that machinery, and comparatively little on analysis (including language analysis) and reporting. Even though we collect and

EO 1.4.(c)
P.L. 86-36

P.L. 86-36
P.L. 86-36

DOCID: 4019716

It seems to me that this is analogous to building the Hoover Dam in order to operate a single light bulb. The benefits derived simply do not justify the cost of the infrastructure.

(U) A better solution might be to shift some personnel (and related promotion points) from staff positions to operations. Even though they were originally intended to help the operational elements, many staffs have over time become hindrances to both operations and operational elements' interaction with customers and collectors. Not only is every operational element down to the office (and sometimes division) level liberally larded with staffs of its own, we seem to have developed a number of large, remarkably well-manned organizations dedicated to staff and protocol functions. Over time, these staffs have evolved into sequential choke points through which virtually all information coming in and out of the Agency must pass. The current situation is such that many operational elements are successful only to the extent that they are able to get around the system, often with the help of sympathetic staffers, in order to get the job done. In other words, we have invested much of our resources into a system that now forces us to expend additional resources to circumvent it. One is almost reminded of Dr. Strangelove, who kept trying to strangle himself with one hand and using the other to free his throat. In addition to streamlining operations, a reduction of staffs might even enhance security, since it would reduce the number of people who are needlessly exposed to sensitive information.

~~(S-CCO)~~ In addition to an immediate boost in the quality and quantity of intelligence production, an increase in the size of the operations workforce would create more promotion opportunities for linguists and other analysts, especially to higher grades, and retention in those fields would undoubtedly improve. Another benefit would be increased decentralization and flexibility, which would also have a beneficial effect on efficiency and productivity. Because they are more efficient and flexible, for example, private companies with decentralized operations consistently post higher profits than those with rigid central planning.

~~(S-CCO)~~ Shifting decision-making, customer relations, and collection responsibilities (and resources) to the lowest possible (i.e. analytic) level would ensure more timely, plentiful, and accurate reporting, greater responsiveness to customers' needs, and more effective coordination

It would also identify those linguists and analysts who, in addition to technical and linguistic expertise, have the background, target knowledge, mature judgment, and dedication to the Agency's mission that would qualify them for promotion to STE ranks. Better retention in the language field, and the consequent improvement in intelligence production, would go a long way toward making NSA what it claims to be, a true intelligence agency and not a mere collector. ❐

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4019716

THE ROLE OF OPSEC

in improving the effectiveness of a cryptologic mission

Experience in peacetime and wartime civil and military governmental operations has shown that even where good security programs were being implemented in each of the traditional security disciplines, an adversary has been able to acquire critical information that impaired our ability to accomplish the mission.

OPSEC is an analytical discipline for improving mission effectiveness by denying to an adversary critical information that could impair the mission. The term "adversary" in this context refers not only to hostile intelligence services but also to any entity whose acquisition and use of critical information, whether or not maliciously intended, could impair the mission. OPSEC and the traditional security disciplines are complementary in that they are all directed at the protection of national security information. In the OPSEC process, however, all aspects of an operation are examined, including support functions.

THE OPSEC PROCESS

As could be expected of any analytical discipline, OPSEC has a well-defined methodology, called the OPSEC Process. It is composed of five steps:

1. The identification of critical information about the operation that must be protected.

This is crucial to the process. Operations personnel determine what specific information about an operation must be denied to the adversary lest it be used to neutralize or negatively impact on the mission.

It should be noted that the question asked is not what classified or sensitive information must be protected but what information, if obtained, could impact negatively on the mission. Called "critical information," it may be unclassified, even in classified or compartmented operations.

All cryptologic missions have information about the activities that must be protected if there is to be the best chance of success. Some examples are: the itinerary of INFOSEC inspections, the criticality of communications nodes, the specific mission and targets of a facility, degree of success.

2. Analysis of the mission-specific threat

The adversary's technical capability and resources for exploiting vulnerabilities of the operation and thus acquire critical information are assessed in this step. Included in such threat assessment must be a realistic appraisal of the adversary's opportunity and intention to undertake such exploitation, the risk it subjects itself to in the process, and its willingness to accept the risk.

~~FOR OFFICIAL USE ONLY~~

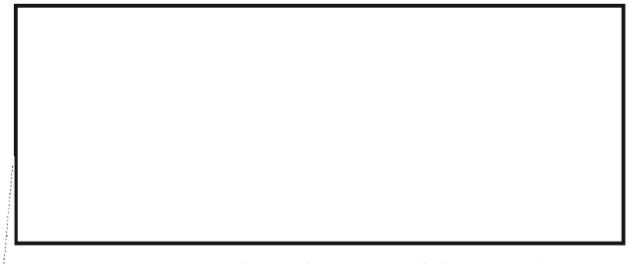
3. Identification and analysis of vulnerabilities

It is almost axiomatic that no operation or system can be relied upon to be perfect in this imperfect world. Almost every one possesses certain inherently exploitable conditions, that is, vulnerabilities that could permit an adversary to acquire critical information. Furthermore, at times the adversary can use inherent vulnerabilities to induce still other vulnerabilities in the system. Prominent among vulnerabilities is human frailty. Frequently OPSEC analyses reveal stereotypic procedures or other poor practices that reveal critical information.

Because of the high value of the information that can be derived from exploitation by adversaries, the cryptologic community must be extraordinarily aware of vulnerabilities. For example, some variations of activity at a site may give an insight into its mission when an adversary correlates it with a remote event previously unconnected to the site's role.

4. Risk assessment

In this step an assessment is made of the impact of an adversary's acquisition of critical information, and practical countermeasures to be considered are identified.



An important and difficult aspect of this step is an estimate of the degree to which the additional or changed countermeasures are expected to reduce the risk, and the cost associated with their adoption. In the case of the cryptologic community, the costs of implementing recommendations resulting from OPSEC analysis have almost uniformly been modest relative to the high value of the critical information to be protected.

5. The application of appropriate countermeasures

This, of course, is the payoff. In the OPSEC process, the final determination of what countermeasures to implement is made by the managers of the operation or activity since mission accomplishment and resource management are their responsibility.

OPSEC PLANNING AND SURVEYS

To be most effective, OPSEC planning must be an integral part of operations planning. It is essential that personnel involved in operations planning be versed in OPSEC. Where feasible, it is also very helpful to have operational plans analyzed by an independent, multi-disciplinary OPSEC team. The team should be composed of people fully knowledgeable of the details of the operation, along with specialists from intelligence, security, communications, logistics, ADP support, and so on.

OPSEC surveys using multi-disciplinary teams are an integral part of the overall OPSEC process. In almost all cases the teams can identify critical vulnerabilities that are or would be revealed during actual operations and that are frequently overlooked by personnel involved in routine.

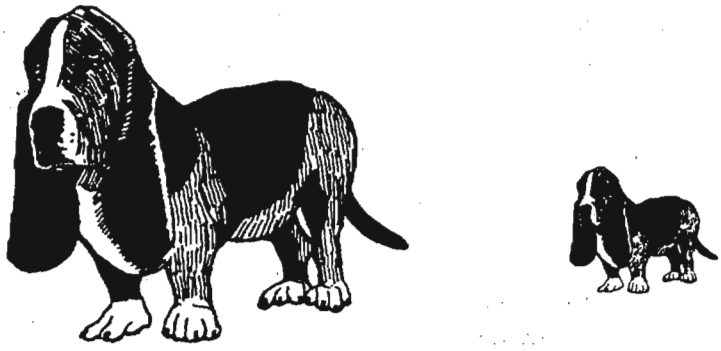
DIRECTIVE 298

In view of the demonstrated value of OPSEC, in January 1988 the President issued National Security Directive 298. This requires all organizations with, or supporting, national security missions to establish formal OPSEC programs, to plan for and implement OPSEC in their agency's activities, and to make sure that all personnel are aware of the threats, and that they understand the OPSEC process.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019716

DEPUTY DAWG



[redacted] P.L. 86-36

How many times have you heard an Agency manager say that he or she enjoyed being the chief of a lower organization more than being the deputy of the next higher level organization? There seems to be more satisfaction to being the Lone Ranger than being Tonto. Yet in this Agency, the deputy position serves a valuable role in meeting both mission requirements and personal career goals.

Being a deputy should provide a good learning and growth opportunity, though it is seldom anyone's final career aspiration. This paper offers some thoughts about the various roles a deputy chief may play.

The deputy position is common in both the civilian and military sides of government. It is generally absent in the private sector. The conventional wisdom is that profit-dependent organizations either cannot afford (or chose not to) the overhead expense inherent in deputies. When the boss is away, someone from the next level may or may not fill in. In one person's words: "When you are the boss, you are always the boss, whether you are on a business trip or a vacation. If there is someone else in your organization who can do your job while you are away, he or she will—and you will be looking for another job."

There is very little in the academic and professional literature on the role of deputies. Perhaps most authors assume that no self-respecting, hard-charging, and upwardly-mobile professional is interested in playing second fiddle. Perhaps it only reflects the general absence of deputies in the private sector. Or perhaps this absence reflects a belief that there is no real need to write specifically about deputies: the literature addresses management concepts, techniques, and ideas that apply to any executive or manager, whether chief or deputy.

Profit-dependent organizations tend not to be as concerned about long-term career paths for their employees. If no one in the organization has the skills required for a particular management or executive position, the company goes out and hires someone who does. Indeed, managers and executives in the private sector often progress along their career paths by moving through a number of companies.

Our unique business demands that we have a stable, experienced, and highly trained workforce. Our policy of promoting from within not only helps us keep a high employee retention rate but also ensures a pool of qualified people

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019716

capable of stepping into higher management positions when needed. The deputy position enhances the ability of our system to provide qualified people to move up.

The primary justification for a deputy is work load. When the work load is so great that a chief cannot handle his or her responsibilities without excessive stress, the health of the organization and the individual may suffer.

Another significant reason, which should be related to the first, is to provide a training opportunity. The deputy role permits someone who previously was concerned only with a more narrow perspective to see a larger one. It allows the person to learn how to manage the larger organization and to work in the bigger picture— and do so with less risk to the mission and health of the organization than would otherwise be the case. In meeting these two goals, the position also serves as a testing ground for potential chiefs.

The role any deputy must play depends on the chief's style and wishes. Generally speaking, deputies have to repress their own egos in favor of their chiefs'. Loyalty and patience are required traits. Secure chiefs will not want a mirror image of themselves. The prime responsibility of subordinates is to give the bosses their best professional judgement. This is especially true for a deputy. The value of a deputies may be measured by the work load they can absorb from the chiefs and by the manner in which they complement the skills of the chief. Some of the roles a deputy may play (they are not mutually exclusive) include:

◆ Advisor. All subordinates, especially deputies, owe their supervisors their best professional judgments. This means telling the chief what the deputies believe is right, not just what they thinks the chief wants to hear. This requires a chiefs who are willing to listen to ideas and judgments that may be contrary to their own. The advisors also haveo be mature enough not to sulk or feel threatened when the chiefx do not accept the advice offered.

◆ Assistant. Deputies as assistants help the chiefs in all or most organizational matters. The two truly share the organizational work load, with the chief making the final decisions and signing off on finished products. Sometimes, the chief delegates certain functional areas to the deputy, who then acts as the final authority for the organization.

◆ Team member. The deputy works as an equal partner with the chief, although the chief, as in all cases, retains ultimate responsibility. This may require a chief who is more interested in achieving organizational objectives than worrying about whose idea something was. It also requires a deputy who does not try to upstage the chief, and who is more interested in successfully reaching organizational goals than gaining personal credit.

◆ Back Up. The deputy as back up is one who stays fully informed on the chief's policies, concepts, wishes, etc., but steps in only when the chief is absent.

◆ Project Manager. In the project or task manager mode, the deputy handles only specific projects assigned by the chief. This allows a deputy's special interests or talents to be concentrated on special problems or issues vital to the organization.

◆ Intermediary. In this role, the deputy serves as the communications link between the chief and subordinate supervisors and/or the non-managerial ranks. The deputy may serve as the "people-oriented" member of the management team, while the chief fills the "task manager" role.

◆ Inside Person. In this role, the deputy manages the internal operations of the organization while the chief does the outside political or public relations work.

◆ Student. The deputy position permits the incumbents to improve management skills and increase their expertise in the organization's technical areas of responsibility.

The effectiveness of a deputy may not be easy to measure except in contrast with periods of prolonged absence. The standard of measure-

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019716

ment in the absence of a deputy would include the chief's work load growth, the increase of stress, and the organization's efficiency.

Deputies may be most effective when they absorb work load the chiefs do not covet, when they provide skills in which the chief is either lacking or simply does not excel, and when they are able to facilitate communications within the organization. Deputies are also effective when they serve as peer-level sounding boards for management, policy or personnel matters. From a chief's point of view, the effectiveness of a deputy may be measured in the sense of "comfort" the deputy provides to the chief.

Serving as a deputy does offer a number of positives. It offers a chance to contribute to the organization's mission while learning more about the "big" picture. And it allows the deputy to study the chief's managerial style "up close and personal." A deputy can attack organizational problems that otherwise might not come to the attention of the chief, or on which the chief would not have time to focus. And a deputy may be able to propose ideas and solutions to issues that might be overlooked because of operational pressures on subordinates.

There are draw backs too, of course. The primary one is that a deputy's effectiveness and utility is directly dependent on the style of the chief. It is easy for hard-harging deputies to become frustrated. Depending on the style of the chief, authority to act may not be there, and perspectives and ideas may be filtered. Exposure to Agency executives may be diluted, and the ability to directly influence actions may be less than expected.

Deputies serve a valuable role in meeting the challenges this Agency faces, and the position can serve as an important rung up the career ladder. The success of any particular deputy depends, as it does in most things in life, on the incumbent's professional and personal skills, and a degree of good luck. ❑

KRYPTOS

Cryptanalytic Literature Competition

open to all NSA employees

closes COB 30 June 1990

Papers may treat any topic in the broad category of professional cryptanalytic literature, including:

- attacks and techniques relating to cryptanalytic problems
- cryptanalytic research
- history of cryptanalysis
- other subjects relating directly to cryptanalysis, such as target studies, cryptologic trends from the point of view of cryptanalysis, computer support of a cryptanalytic problem.

Papers written between 1 July1989 and 30 June 1990 are eligible. They may be written specifically for the competition.

Entries may carry a classification up to TSC. Compartmented papers will be considered only in extraordinary cases.

Criteria

- Is the paper an original discussion of a cryptanalytic subject?
- Is the paper well written? Is the subject presented well? Can the reader with a suitable technical background but unfamiliar with the subject understand the paper and, by reading it, gain knowledge about the subject?
- Does the paper constitute an important addition to the body of cryptanalytic literature?

To enter, send four copies to :

[redacted] A547, Ops 2A

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

OCID: 4019716

The following is reprinted, with permission, from R5 Tech Briefs, *July 1989, "Literature Reviews and Recommendations." Written by some of Dave's friends, it is a tribute to a model professional. CRYPTOLOG is proud to have been among the beneficiaries of Dr. Harris's many efforts to inform and inspire.*

David Harris

in memoriam

(b) (6)

(U) David Harris passed away at his home on 14 July 1989 after having served over 10 years with NSA. It is appropriate to write of him here as his contributions carried 99% of this column since this magazine began publication last year. [redacted] His passing will mark a large change in R51's activities and reports, as others try to take up only some of the many things that Dave did so well.

(U) To describe what Dave Harris has meant to R51 and to the National Security Agency, perhaps it is best to begin with a parallel from a novel of Chaim Potok. The conflict in *The Chosen* revolves around whether the main character will take up the career for which he seems to have been chosen by his brilliant intellect, his insight, and his command of an immense body of knowledge. In the case of Dave Harris, we were fortunate that he decided to join our business, rather than pursue an academic career in the field of Algebraic Geometry.

~~(FOUO)~~ Having chosen this alternative career, Dave plunged into the world of cryptomathematics wholeheartedly. In February 1979, he began his career with NSA, entered the class of 1982 P1 Cryptologic Mathematician Program (CMP), and had very productive tours in G95, R14, G42, A54, and S61. Upon graduation from the CMP he joined R51 where his great energy, organization, and breadth of mathematical knowledge made him invaluable. In R51, the office of Mathematical Research, he played increasingly important roles as researcher, teacher, and leader.

(U) In conducting research on a variety of problems, Dave drew not only on his previous broad academic background, but on his great versatility and quick grasp of new fields. He soon became expert in several areas of statistics with applications to our problems, most notably the interplay between moments problems and Pearson curve fitting which is recorded in his article in the *Proceedings of the NSA Mathematical Sciences* Meetings. His intuitive grasp of cryptomathematics is illustrated by the fact that the credit he received for MA-250 came from his teaching the course, despite not having taken it previously himself.

(U) In seminar and informal working discussions, Dave could always be counted on for relevant and perceptive comments and suggestions on how best to attack a problem, or rethink a process in order to extend its generality and applicability. Several of his particularly insightful solutions to statistical consulting problems earned him Letters of Appreciation during his two-year assignment in R513, the Statistical Techniques Division. He was eager to consult and his interest in statistics was also shown by his membership in the American Statistical Association and the Institute of Mathematical Statistics, R513 is deeply appreciate of his work

DOCID: 4019716

and interest in NSA statistics during and after his tour there.

(U) Examples of his contacts with outside academia were his survey of work on the Mordell Conjecture which appeared as one of the prestigious expository articles in the Notices of the American Mathematical Society for June 1986, and his correspondence with Professor Nicholas Katz of Princeton University on some deep conjectures concerning Kloosterman sums over finite fields of characteristic two.

(U) As a teacher, with an interest in passing on and fostering knowledge in classified and unclassified mathematics, Dave Harris kept his finger on the pulse of developments in an amazing number of fields, and communicated pertinent summaries through the R51 Seminar, these literature reviews, his famously comprehensive and incisive trip reports (often numbering 5, 10, 15, and even 20 pages in length), as well as individual research papers. During his record-breaking term (over five years) as coordinator of the R51 Seminar, Dave molded it into an institution with his own personal stamp. The R51 Seminar was carefully planned to continually survey the major new developments in all corners of NSA, and was, incidentally, an area where his skill with words and love of puns were strongly displayed. The speakers usually found that the most perceptive questions and observations came from Dave himself, as he would "do his homework" by reviewing the speaker's previous work on the subject before attending a presentation.

(U) The literature reviews need only be mentioned to our readers to recall the breadth of coverage, personal insight, and craftmanship of composition displayed every month. Similarly, his coverage of a Mathematical or Computer Science conference was unequalled, from his advance planning and surveys of talks for coverage, through his careful note-taking at as many talks as he could possibly attend at any conference or seminar, and his very detailed reports. In his individual research papers on classified topics, he took up themes of interest for their applicability, while a natural instinct for teaching led him to keep a supply of problems

An excerpt from his contribution to the publication commemorating his 25th Harvard class reunion:

I have been reasonably happy with my job. It allows me to dabble in whatever subject comes to hand . . . I still consider myself a mathematician. Recently I have been trying out the high-prestige career of Defense Department manager. I try to serve others, and help them do whatever they do well . . .

I would like to advertise President Bok's by-now-forgotten speech at the 1988 commencement. He dealt in part with the problems of preserving a government competent to handle the tasks we assign it. When people run down government employees, they discourage capable people from getting involved. If you believe our present system inadequate to handle the problems facing it, or that it is going the wrong way from time to time, do not stay safely on the sidelines telling us that we cannot do the job. You are right. I will probably fail to make any difference. The politicians of both parties do not help. But I do try my best to move things in what I think is the right direction.

In the present world of scarce resources for government, math and science are competing with housing for the poor. How shall we juggle priorities in this situation? Whatever you and I think, these needs are not likely to be met by cutting the national defense whenever money is needed. Math and science cannot afford to be parochial in assuming themselves the highest public good. And the pragmatists and humanitarians cannot ignore the need to arrange for the future. A proper balance between the long and short term, pure and applied, pragmatic and humanitarian, must be sought. It is important that these decisions not be made in the typical way —in accordance with the relative strengths of the lobbies involved, each acting in its narrowly conceived self-interest. Those willing to try to strike the balance on broader grounds must be discouraged. Currently, the American system in government and industry acts to encourage managers to consider only payoffs that will become apparent during their own brief tenures in office.

UNCLASSIFIED

DOCID: 4019716

suitable for those just beginning to study crypto-mathematics.

(U) During 1988 and 1989, Dave took a turn as Division Chief of R512, the Consulting Division within R51. Here his sense of personal responsibility and integrity contributed to a selfless period of service to his fellow researchers and to the future good of our organization. He functioned alternately as cheerleader, planner, and advocate of his employees. He sought to provide a dialogue on organizational goals, on technical ideas, on what role management played in R51. And in keeping with a typical Dave Harris style, he produced toward the end of his term of office a closely-spaced, tersely written 4 1/2 -page set of informal notes: "Survey of the Job of an R51 Division Chief." He planned thoroughly for his meetings with management, tried his level best to advance the concerns of those beneath him, and generally took on the role of a caring and concerned parent.

(U) In his building of mathematics within R51 in his "alternative career" as researcher, teacher, and leader, one fact about Dave Harris especially struck those of us privileged to work with him: he was a thoroughly good man. He put the good of others before his own, the growth of knowledge before personal advancement, and was truly the "righteous man" spoken of in Chapter 18 of Genesis.

P.L. 86-36

Editor's Note:

Just a small fraction of Dave's many reviews and reports that appeared in R51's Monthly Research Summary have been republished in CRYPTOLOG. There still remains a considerable backlog on which we will continue to draw from time to time. A sample appears on page 24 of this issue. Dave was most gracious in giving CRYPTOLOG carte blanche on publishing his writing.

BULLETIN BOARD

CQ UNDER NEW ORGANIZATION

(U) *The Cryptologic Quarterly*, NSA's professional journal, is now published under the auspices of a new organization, D9, the Center for Cryptologic History. The Chief is David Gaddy, OPS 2B, 963-1891. Submissions to CQ should be sent directly to the Managing Editor, [redacted] D91, SAB 2 Door 22, 972-2235.

FOR TRAFFIC ANALYSTS

[redacted]

CA SOFTWARE RUNNING ON UNIX

~~(FOUO)~~ CRYSCOM has initiated an exchange program for CA software running on UNIX contributed by various CA organizations. Available are complete packages, individual programs, and subroutines. For a complete list please get in touch with [redacted] CRYSCOM Exec, P13, 963-3045, or [redacted] CRYSCOM Chairman, P1/A548, 963-1464, or one of the following points of contact: J.

[redacted]

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019716

The Mysteries of ΓAMMA

Γ,γ γάμμα, τὸ τρίτον γράμμα τοῦ ἑλλην. ἀλφαβήτου, δεύτερον σύμφωνον· ὡς ἀριθμητ. σύμβολον γ′=3 ἢ τρίτος καὶ ,γ=3000.

Richard D. Sylvester, B

~~(S-CCO)~~ Many people who have been granted GAMMA access have only a vague understanding of what this special access is, or they have no idea at all what it constitutes. GAMMA is an unclassified coverterm used to flag especially sensitive Category III COMINT product. The term signifies that the product requires maximum security protection for one or more of the following reasons:

[redacted]

~~(C)~~ Although the term GAMMA used alone is unclassified, the fact that the term is related to COMINT is classified, at a minimum, CONFIDENTIAL. In addition, information which has been reported in GAMMA product reports may not be referenced in non-GAMMA product nor revealed to personnel not cleared for GAMMA access.

~~(C)~~ DDO is the authority responsible for identifying that COMINT which is to be handled in GAMMA product reporting channels. Proposals for assignment of sensitive COMINT to the GAMMA series are made to DIRNSA, through the GAMMA Control Officer, for DDO approval. NSA keeps the National Foreign Intelligence Board (NFIB) informed of the nature of the information placed in this series and justifies each assignment in such detail as to convey the security risk inherent in dissemination of the information.

~~(FOUO)~~ The dissemination of GAMMA reports is tightly controlled. To assure proper handling of GAMMA information, the DDO nominates and DIRNSA appoints a GAMMA Control Officer (GCO), who is responsible for all aspects of the handling and distribution of GAMMA material and maintaining records of that SIGINT which requires GAMMA protection. [redacted]

P.L. 86-36
EO 1.4.(c)

[redacted]

~~(FOUO)~~ For additional classification guidance concerning the GAMMA control system, contact the the appropriate person at your Division, Office or Group level, or the GCO in P0522, or refer to

[redacted]

P.L. 86-36

DOCID: 4019716

[redacted] G96 P.L. 86-36

Thoughts on

ORDERING, SORTING, and HEAPING on CRAY

I was pleased to read [redacted] years I have know [redacted] to be one of the best sorting packages available. Now, however, I find that some of the others (which I thought to be efficient) are not so hot.

P.L. 86-36

Many of the "good" routines are merely drivers for [redacted] No doubt, the sort algorithm(s) used by [redacted] should and will have a major influence on future sorting, ordering and (possibly) heaping routines.

Algorithms to save the top-n best answers (which I'll group under "heaping") are related to, but should be considered separately from sorting and ordering. When heaping, we have a large degree of control concerning the format of the heap - that is, the heap is already ordered (in some way) when the next answer is about to be inserted. Heaping requires that the heap be continually updated as new (best) answers are produced.

Sorting and ordering require less interaction with calling programs, and the algorithms used can dynamically allocate and release space as needed. (Heaping requires dedicated space for the duration of the heap.)

[redacted]

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

DOCID: 4019716

GENERAL COMMENTS

What commercial routines are available? Or ones from academia? P.L. 86-36

While conversion from [redacted] to UNIX is a tremendous burden, it is also an opportunity to review, revise and consolidate major processes. Ordering/sorting/heaping is one of the topics which deserves and requires a great deal of attention, since applications of such routines are so pervasive.

A Better Way?

Share your findings with your fellow analysts

Write it up for CRYPTOLOG!

Need Help?

Ask!
An ad in Bulletin Board will bring results.

Competitive rates

Satisfaction guaranteed

DOCID: 4019716

Technical Literature Report

Reported by: David Harris (see page 18)

(U) S. Radziszowski & D. Kreher (1988) "Solving Subset Sum Problems with the L^3 Algorithm," *Journal Combinatorial Mathematics and Computing*, 3, April 1988, pp. 49-63.

~~(C)~~ The authors are interested in what most people call the knapsack problem, and in particular with speeding up attacks on it using the lattice basis reduction algorithm. They reduce the number of multiprecision operations needed. The authors also use a direct search for short vectors to complement L^3. The authors claim the run time is an order of magnitude better than that of Lagarias and Odlyzko, and that as a result higher density subset sum problems can be solved. While there is no proof the new algorithm beats its competitors, there are practical examples that this is true. The authors give some ideas for further improvement.

(U) Daniel Fuhrmann (1988) "An Algorithm for Subspace Computation, with Application in Signal Processing," *SIAM J. Matrix Anal. Appl.*, 9 (2), April 1988, pp. 213-220.

~~(C)~~ There are many situations that involve using eigenvectors, eigenvalues, or singular values to recover information hidden in a matrix. An algorithm for computing the eigenvectors corresponding to the m algebraically smallest or largest eigenvalues of an nxn symmetric matrix A is given, where m is small compared to n. In addition to cryptanalytic applications, such methods come up in signals processing as in the MUSIC algorithm for bearing estimation. When n is large and A is structured, the Lanczos method and its variants are best.

~~(C)~~ This paper proposes a Lanczos-like algorithm consisting of repeated applications of the Rayleigh-Ritz (RR) procedure to a sequence of subspaces which converges to the desired invariant subspace. The RR portion of the algorithm is highly structured din a way that the author hopes will lead to significant computational savings at little cost in memory. All the computations lend themselves to parallel implementation. The author's goal is "an adaptive formulation of Schmidt's MUSIC algorithm, or alternatively, an adaptive eigenvector beamformer, in which the weight vector for an array of antennas or sensors is determined from the eigendecomposition of the received signal covariance matrix."

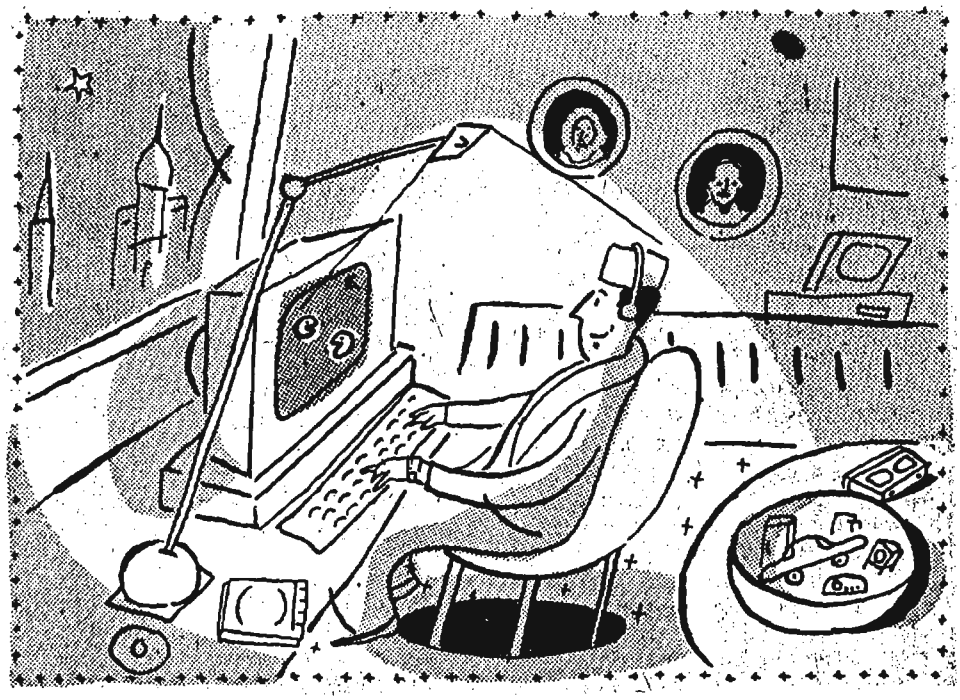
(U) Robert M. Kuhn (1988) "Curves of Genus 2 with Split Jacobian," *Trans. AMS*, May 1988, **307** (1), pp. 41-49.

~~(C)~~ An algebraic curve has a split jacobian if its jacobian is isogenous to a product of elliptic curves. Given a curve X of genus 2, and a map from X to an elliptic curve E, then X has a split jacobian, but the complement to E in the jacobian of X is not uniquely determined. However, under certain conditions, there is a canonical choice of the complementary curve E′ and the map from X to E′. Kuhn shows this, and gives an algorithm for finding that curve. The construction works in any characteristic *other than 2*. Applications are given in characteristics 0 and 3.

~~(C-CCO)~~ In theory, the analysis of such splittings is relevant to solving the discrete logarithm problem on the jacobian (a Harris upgrade of a suggestion of Mike Paul.) The degree of the isogeny is crucial to any crypto application, and turns out to be the size of the kernel of the direct sum of two maps. The jacobian of dimension 2 is the next step up from elliptic curve discrete log problems. Of course it is not clear this will ever be of practical importance. Split jacobians are used in the theory of abelian varieties to construct counterexamples, and families of curves with maximal numbers of points in finite fields. The study of coverings of curves by curves is at the heart of the paper. □

DOCID: 4019716

Review



The Cuckoo's Nest
by Cliff Stoll. Doubleday, New York, 1989

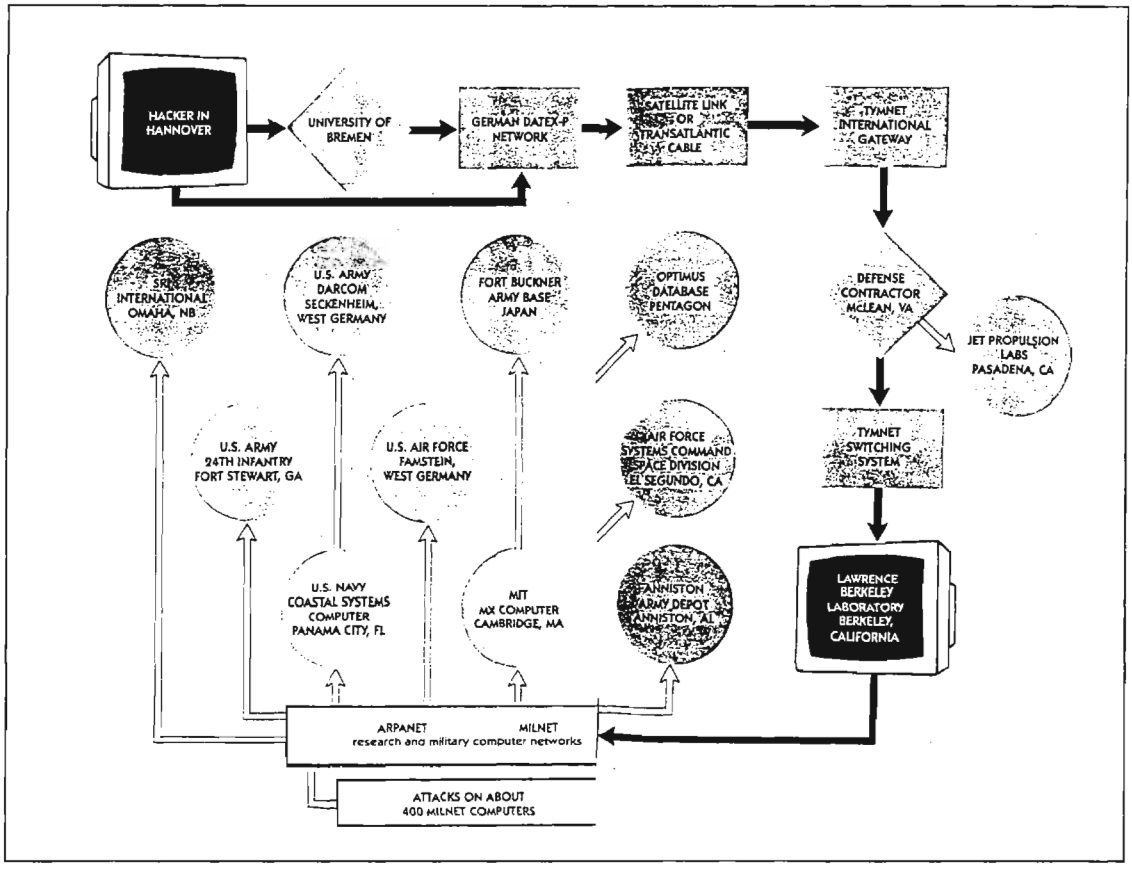
P.L. 86-36 *Reviewed by:* [redacted] *P13*

(U) A German computer hacker penetrated a computer at Lawrence Berkeley Laboratories (LBL) in August 1986. This caused a 75-cent discrepancy in the system accounts. Clifford Stoll, an astrophysicist who had run out of grant money, was given a job at LBL computer center, and as the newest programmer was asked to check the discrepancy. Thus began a frustrating and fascinating international hunt that lasted for a year, finally leading to conclusive evidence of a KGB link to a ring of German Hackers.

(U) In *The Cuckoo's Egg*, Stoll has written an intriguing and suspenseful tale of computer sleuthing, bureaucratic muddle and indifference, and the exploits of a cunning hacker, counterpointed by the tenacious struggle by a single concerned scientist determined to find the unknown hacker. One of the ironies revealed by the book is that the thicket of laws and administrative restrictions established to protect the privacy of communications in fact make it almost impossible for computer managers, telecommunications operators or Government agencies to detect or pursue hackers who penetrate computers and E-Mail systems. Unchecked, the penetrators can read or alter anything they want within the computers.

(U) When Stoll began to investigate the 75-cent discrepancy, he found an unregistered user

~~FOR OFFICIAL USE ONLY~~



"Hunter" had been using the LBL computer. One day later an E-Mail complaint arrived claiming that some LBL Unix user had tried to penetrate a DOCKMASTER computer in Maryland. Checking showed that only one LBL Unix user Sventek was logged in, but he was in England, with no access to the computer. There was no clear proof of a hacker, just circumstantial evidence. Stoll's superior was unimpressed, and demanded proof. Stoll began to secretly monitor who was using the Unix system, and soon saw a log-in by Sventek. Stoll traced the port. By chance, a hardware technician who knew the computer center communications complex had been collecting statistics on who had been using the communications switchyard. This showed a 1200-baud connection, which meant an outside phone line. The discovery narrowed the search to about 50 phone lines. So Stoll decided to tap the 50 phone lines and printout the modem traffic — so that the hacker could not detect, from *inside* the computer, that the E-Mail was being intercepted. Stoll's girlfriend, a law student, assured him that since he was not the Government, he didn't need a warrant (p,.20). With a clear conscience, Stoll borrowed 50 printers, teletypes and portable computers on a Friday night in September, and printed out all the E-Mail traffic, keystroke by keystroke. One of the printers had 80 feet of printout, and evidence of how the hacker operated.

(U) The transaction, sent through Tymnet, showed that the hacker had been on the machine for three hours and used a special editing program called Gnu-Emacs which allowed him to bypass the Unix controls to change a Unix program ATRUN. The hacker then used the changed Unix operating system to make himself a privileged user. The original ATRUN program was replaced and all trace of the transaction erased. This was like a cuckoo bird laying its egg in another bird's nest, to let the victim hatch the cuckoo's egg. Once the hacker became a privileged user, he could bypass all the privacy protection in the computer. Without the warrantless wiretaps, this penetration would have

been undetectable, for the hacker's penetration program was watching for *internal* surveillance.

(U) In time, Stoll set up an interception system that not only spotted and recorded the hacker's transactions, but signalled him in morse code on his telephone beeper, so he would know instantly, day or night, when the hacker was on the line.

(U) The hacker was not content just to penetrate into the LBL computer, but got into university and government computers all over the US and abroad. Usually the system managers had no hint of any trouble until Stoll, reading his intercepts, called them and told them what to check for. Without the year-long accumulation of intercepts, the extent, modus operandi and source of the hacking could never have been determined.

(U) In due course, Stoll and LBL contacted the police, the FBI, NSA, CIA, AFOSI, Tymnet and the German Bundespost. The carriers, Tymnet and Bundespost, were very interested, and energetically traced calls whenever Stoll's pager signalled him. Eventually this found the hacker, who had started working for the KGB after he was able to copy sensitive unclassified military files. But for most of the complex network investigation, the FBI was uninterested because there was nothing they could prosecute; the National Computer Security Center at NSA considered domestic monitoring as "prison term stuff" and stated, "We're here to make computers more secure, not to catch criminals."

(U) In spite of the caveats, CIA, NSA, FBI, DOE and the Pentagon *did* in fact keep up with the case, asked Stoll for copies of his intercepts, and invited him to tell his story to very high level audiences. The Defense Department sealed up its computers to prevent penetration. But what the agencies could *not* do was intercept, trace or pursue the hacker.

(U) Stalled by the C&P telephone company who would not tell him where the hacker was getting into Tymnet, Stoll finessed the long distance operator into revealing enough information to track the connection back into Mitre corporation in Maclean, VA. Further work showed that the hacker was getting across the ocean into Mitre, and making Mitre pay the phone bill for both the incoming transatlantic calls from Germany, and numerous outgoing calls around the US. Mitre refused to believe that was possible.

(U) Stoll set up a "sting" operation with counterfeited classified documents. Government interest vacillated. Stoll was told repeatedly he had "only one more week" to catch the hacker. The FBI closed the case. Stoll discovered the hacker had passwords to a number of systems, and knowing from his intercepts that the hacker had been stealing *encrypted* passwords, deduced that the hacker used the published encryption algorithm to encipher dictionary words until he got matches with the encrypted password files!

~~(FOUO)~~ Then in April 1987, a letter from Pittsburgh (p.64) in response to the sting enabled FBI counter intelligence to show a KGB link via the Bulgarian secret service. This revived official interest, and exposed a team of German hackers selling Unix operating software copied from US military computers and some passwords into military files, to the KGB. This led to a prosecution in Germany which concluded in 1990 with the hackers convicted and set free, because, under German law, they had not caused serious harm to West Germany (Reuters 15 Feb 90). Another point in the German case was that Stoll's intercepts could not prove that it was the *same* individual who was penetrating into the LBL computer (ibid.). That bizarre legal outcome was typical of the mismatch between the law and the actions and effects of the hacker.

~~(FOUO)~~ The book, which has become a best seller, draws a rather unflattering portrait of interagency buck passing and turf battles. Stoll tracked the hacker down, despite all of the resistance and indifference, because he got involved , and because he had enough freedom to pursue the trail where it led by any means he could devise. In his quest he pioneered in a number of techniques of "network investigation," useful tools in computer security.

~~(FOUO)~~ This raises an interesting point about privacy laws. Stoll's initial intercept of 50 phone lines was done, without a warrant, in early September 1986, when there were still no legal restrictions on intercepting data traffic on telephone lines. The local phone company would not trace the hacker's calls *without* a warrant, even though a warrant was *not* required. However, Stoll continued to monitor all the traffic over four telephone lines connected to Tymnet and sent printouts of the intercepts and logs to various government agencies. Without the intercepts and logs the search would never have led back to the hacker and to the KGB.

(U) PL-99-508, which changed the interception law, went into effect on 21 Oct 1986. The law, codified in 18 USC 2510-11, does not authorize computer managers to monitor content of electronic communications. New laws concerning computer networks in 18 USC 2701-2 came into effect only at the end of 1988, and they also do not authorize intentional wiretapping, nor do they authorize disclosure of deliberate interceptions to a law enforcement agency (18 USC 2702(b)(6)).

(U) What Stoll's book illustrates, in spellbinding detail, is that purely passive measures of defending complex modern networks against skillful attack are inadequate. Without *network investigation* techniques, i.e. domestic interception, records keeping, and general search over suspect channels (Stoll searched 50 lines!), it is impossible to get enough information to detect even very serious threats to security and privacy.

~~(FOUO)~~ Law enforcement agencies cannot get warrants for general search, and they usually cannot tell *who* is hacking or *which circuit* will be used. Those specific data are required for interception warrants (18 USC 2518(4)). The carriers can check every voice circuit they operate, but *not* for content (18 USC 2511(2)). There is no authority for carriers to monitor non-voice traffic. The authority of computer center operators to intercept the *content* of all the communications in and out of their computer complexes is not clear, for it depends on whether the system operator is considered a *party* to the communication (18 USC 2511(2)(d)). Usually the system operator is not a party to the E-Mail communications, just as a PBX operator is not a party to voice communications. Government agencies are not allowed to obtain or use the contents of intercepts unless they satisfy the interception laws (18 USC 2511(1)(d)). *All* LBL computer users coming in through the Tymnet lines were intercepted, even though they were not engaged in any wrongdoing, and had a right to all the privacy the law provided. The Hanover hacker was deliberately trying to *avoid* the system operator, because he did *not* want the system operator to be a party to the transaction.

(U) The new laws permitting certain disclosures of information stored in computers apply only to organizations "providing remote computing services to the *public*" (18 USC 2702(a)(2). Since most computer networks require password access, they are *not* available to the general public, in which case the operators apparently have no legal authority to disclose information, even if it was inadvertently obtained. There is a private organization CERT (Computer Emergency Response Team) at Carnegie-Mellon University, chartered by DOE to respond to hacking, viruses, etc., but its authority to do anything but advise is very unclear. It is also not clear that US privacy laws or computer crime laws can be applied to a person outside the US — the Germans applied only their own laws to the German hackers. Finally, as the German courts pointed out, no one could prove that it was the same person on every call, or that he was causing any specific harm.

(U) Thus, in a beautiful paradox, the laws set up to protect the privacy of citizens against government surveillance ironically shield the activities of hackers or malicious penetrators from any surveillance, so they can tamper and exploit the files and communications of legitimate E-Mail and computer users, leaving them as defenseless as an unknowing cuckold. ❐

DOCID: 4019716

Review

Reflections on Intelligence by R.V. Jones. 376 pp. Heinemann: London, (1989)

Reviewed by: Vera Filby, E4

Among the procession of now-it-can-be-told books on the history of World War II published in recent years, one has stood apart from the rest for its focus on the scientific and technological aspects of the war and its view of events from the highest levels of science and government. In *Most Secret War*, R. V. Jones, now Professor Emeritus of Natural Philosophy of the University of Aberdeen, recorded the struggles and achievements of military science and technology in Britain and his role as scientific adviser to Prime Minister Churchill. (Jones was the man responsible for breaking Germany's new navigational beacon system, which could direct Luftwaffe bombers with devastating accuracy. His special work with radar was instrumental in the successes of the Allied bomber offensive and the preparation for D-Day.)

The present book is a history and appreciation of scientific intelligence and activities related to intelligence from the prospective of half a century's involvement in the field. The main body of the book, Part One, addresses the philosophy and ethics of intelli,gence and the activities of security and deception. This is supplemented in Part Two by "postscripts" to the earlier work and in Part Three by the solution to the mystery of the Oslo Report.

Professor Jones began his postwar intelligence career in 1952, when Churchill asked him to leave teaching in Aberdeen and become his Director of Intelligence. Less than two years later, having observed and evaluated all aspects of the intelligence scene and completed a report, he resigned and returned to his students. Contributing to his decision was his dissatisfaction with the treatment of atomic energy as something apart from other intelligence and his objection to the assignment of ELINT to GCHQ, which he believed to lack the expertise to deal with it.

Under the heading of intelligence ethics, the author discusses respect for allies, diplomatic bags, covert action, assassination, privacy, and other facets of intelligence, all of which encompass irreconcilable contradictions. These short essays, in a style characteristic throughout the book, combine instruction, commentary, conclusions, reminiscences, and lots of anecdotes and good stories. Some of the stories are old but they are retold here by a master, often with new insights and always with sparkle.

Official secrecy requires a chapter of its own, which begins with the observation that the balance between too much and too little has been pondered at least as far back as Francis Bacon. The author relates with undiminished indignation his own run-ins with security in connection with official suppression of information already released to the public. On a different note, he recognizes the marvel of the silence faithfully maintained for 30 years by thousands of people to protect wartime cryptologic security. He attributes this in part to the system of security developed by the British and adopted also by the Americans, and in part to the loyalty that all felt to others who had participated in the great effort.

But the best and most secure system cannot protect against leaks, disclosures, and indiscretions by those outside its authority. Such violations may be committed because of carelessness, indifference to security, arrogance, or for personal advantage or political motives, or for some combination of reasons. A classic case of political motivation occurred in the 1930s, when Prime Minister Baldwin exposed

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019716

the content of Soviet decrypts, resulting in the loss of the source.

Politics can also have the opposite effect - the suppression of information that ought to be made known. Here again Baldwin provides an example by his withholding of evidence of German rearmament on the grounds that the public might be so upset as to cause the loss of the election.

In discussing insecurities nearer to the present, Professor Jones mentions self-importance as a possible factor and cites damaging comments by politicians during the Falklands crisis.

Subsequent chapters explore the interrelationships of intelligence and security, intelligence and deception, and intelligence and command. Each could serve as a textbook on the subject.

The book changes course at this point and turns back to the beginnings of modern military science and technology. Here the author presents a history of World War I weaponry and military science and in doing so pays tribute to to the scientists and inventors whose work was so largely responsible for winning both wars. Subjects covered include radio, sonar, chemical warfare, air warfare, infrared, atmospheric research, and several others. Radio was already well established and had been used in the field during the Boer War; but World War I inspired a great expansion in its development. Along with it, cryptology flourished and brought forth its miracles, only to be dismissed and neglected after the war until it was urgently needed for the next one.

While some scientists were creating the weapons of war, others were applying scientific methods and mathematical analysis to military operations, both tactical and strategic. The author credits the invention of operational science to Benjamin Franklin, recounting a story about Franklin's mock estimate of the cost per head of killing Yankees. This introduces stories of extraordinary men and their accomplishments. Told in Professor Jones' vivid and witty style, they make most entertaining reading. Not surprisingly, the scientists' new and unorthodox ideas were not always welcomed in military circles. But lessons were learned, and as World War II progressed, operational research groups were established in various commands to provide analysis, assessment, and advice.

The rise in the power of scientists and their influence with national leaders brought problems of conflict, responsibility, and conscience. Professor Jones comments on these concerns and the crises of conscience that the uses of science in war, particularly nuclear energy, have caused, and concludes: "Never-the-less, I think that in general scientists need to take the risk of bringing political leaders into their confidence, and that reciprocally scientists have a special claim to be consulted about the exploitation of their ideas. If, as in the case of nuclear weapons, these ideas offer horrifying prospects, it is better in the long run that national leaders and populations generally should be soberly aware of them."

Part Two is a mixed collection of short pieces which supplement or complete stories left unfinished in *Most Secret War*. Responses to that book brought an abundance of new contacts, information, and insights. Official documents declassified and released after its publication revealed or made usable still more material. As his first postscript, Professor Jones recalls the Polish cryptanalysts who escaped after the German occupation of Poland and succeeded despite great difficulty and danger in getting their knowledge of the Enigma machine through to the French. Stories follow about members of the resistance movements and other wartime friends and colleagues, Churchill and other national and military leaders, and former German enemies. There are episodes of risk and sacrifice, missions lost and missions accomplished, intelligence efforts - Peenemunde, for example - revisited. Along with these are accounts of the author's adventures and happenings as he followed up the leads generated by his book. NSA readers will enjoy the story of his visit to Electronic Security Command Headquarters and a slew of other U.S.military, research, and industrial establishments, including NSA. Professor Jones had a very good time.

The document called the Oslo Report was sent anonymously by mail to the British Embassy in Oslo in November 1939 and forwarded to London by the Naval Attache.It has been a center of controversy ever since. It consisted of seven typescript pages and a sealed package. The papers contained information on a German glider bomb, torpedo fuses, radar, and other

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019716

weapons and devices; in the box was a trigger part.This unexplained gift was regarded with suspicion by almost everyone who knew about it except Jones, who believed in it and used it to guide him in his assessments of future German developments. It proved reliable time after time, and on one inspired occasion a reference in it was combined with an ULTRA decrypt to reveal that a distance-measuring beam had been added to the German bomber beam-guidance system.

Professor Jones describes in considerable detail the strenuous but fruitless efforts of many searchers, including investigative journalists, to identify the unknown source and in even more detail his own wide-ranging and finally serendipitous efforts. In 1954 he learned the identity of the author and knew that he was a noted German scientist and mathematician, an expert in electronics. At last, in 1955 at a conference in Munich, Professor Jones met Professor Hans Ferdinand Mayer of the electrical firm of Siemens & Halske. He did not tell this story in *Most Secret War* for reasons of privacy and a continuing requirement for security.

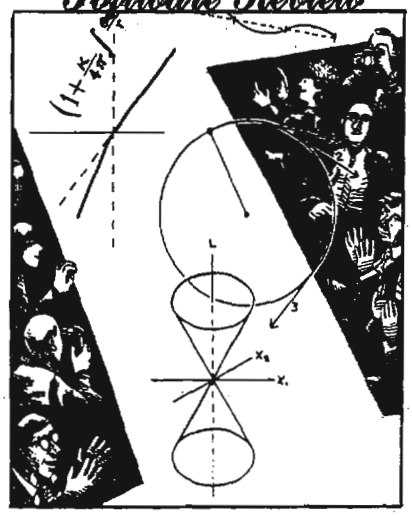
Hans Meyer had been with Siemens for many years and was on a business trip for the firm in Oslo in November 1939. By that time, he had become increasingly disturbed by the evils of the Nazi regime; but he continued with his work in Germany until in 1943 he was reported for listening to the BBC and arrested by theGestapo. He survived Dachau and other camps, escaping finally as Germany was collapsing. He was certified as a victim of fascism by the Allied military authorities and soon went to the United States where during 1946-50 he was a research professor at Cornell working on radioastronomy. He then returned to Germany and Siemens.

This book in its variety -- history, science, studies in intelligence, people and places -- is hard to categorize; but it is easy to recommend for both enlightenment and entertainment.

End Note

Most Secret War. By R. V .Jones. Hamish Hamilton, London. (1978). Published in the United States as *The Wizard War,* Coward, McCall & Geoghegan, Inc. (1978).

Software Review



MATHEMATICA. Wolfram Research, Champaign, IL

P.L. 86-36

Reviewed by: [redacted] *R562*

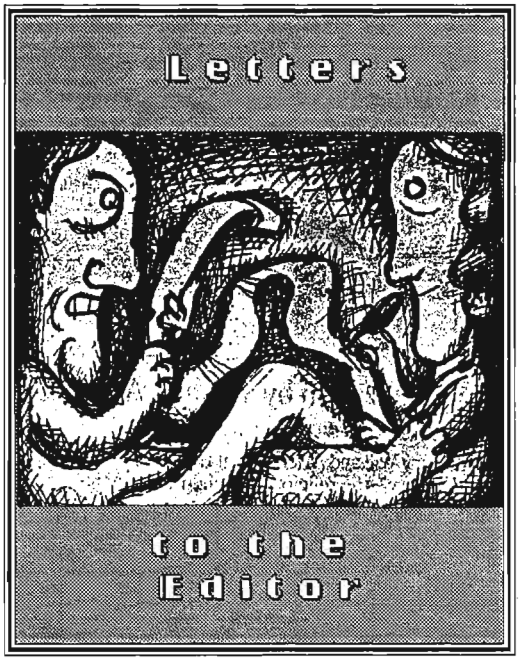
~~(FOUO)~~ The symbolic mathematics language Mathematica has been used in two problems [redacted] One is constructing a primitive irreducible polynomial of degree 256 over GF(2), namely, $x^{256} + x^{10} + x^5 + x^2 + 1$. It is known that there are no such polynomials with two, three, or four terms, and this one is the lexicographically least with five terms.

P.L. 86-36

~~(FOUO)~~ The other problem is explicit construction of the Hilbert Class Field of the algebraic number field $Q(\sqrt{-95})$. This was done by closely approximating a root of the so-called Watson polynomial by means of complex Fourier series, then finding the Watson polynomial of degree 8 by using integer lattice basis reduction. All eight roots of this polynomial were then found to extremely high accuracy, and the roots of the class equation computed from them. The class equation itself was then computed as a product of linear factors, and the resulting coefficients rounded to the nearest integer. A positive check was successfully made by factoring both the constant term and the discriminant of the class equation, and finding that the prime factors satisfied a famous theorem of Gross and Zagier. This particular class of equation had already been computed, so we recomputed it with Mathematica as a test, and found that it could do this computation very easily.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019716



To the Editor:

Further to the exchange between [redacted] concerning the use of the term "bastardized" to describe the development of Afrikaans.

I would agree with [redacted] comments on the development of Afrikaans and with his point that the term "bastardized" is derogatory and linguistically meaningless. I feel I can lay claim to some expertise in this matter, as my MA thesis dealt with the various theories about the origin and development of Afrikaans..

[redacted] argues in her response to [redacted] that "bastardization" is frequently used in a technical sense to describe the development of Afrikaans. We are assured that the term is not perjorative. I cannot recall, however, any serious linguistic work I encountered during two years of research into the question that referred to "bastardization" in connection with Afrikaans. The term used by most scholars to describe the development of Afrikaans is "creolization," although there is some question as to whether or not Afrikaans is a true creole. It seems unlikely in the few years since I finished graduate school, a perjorative like "bastardized" could have gained currency in the rather small group of scholars who concern themselves with the history of Afrikaans. P.L. 86-36

[redacted]

Former member, Afrikaans PQE Committee

To the Editor:

I have just seen a bulletin from the National Cryptologic School which is inviting applications for a two-year program designed "to train highly motivated Agency personnel to become the skilled technical leaders for tomorrow's Agency workforce." As a CY-100 graduate, I feel honor-bound to warn potential applicants that this is an empty promise.

When we entered CY-100 in 1968, we were told the same thing about our one-year program: we were to become the technical leaders of tomorrow. When my class compared notes at our twenty-year anniversary luncheon, we found that no one considered CY-100 to have enhanced his or her career; if we are the technical leaders of NSA today, why isn't anyone following us?

The bulletin would have you believe that NSA has a need for multi-disciplined analysts. I agree that we do have such a need, but try to find a job announcement that says that. I believed the propaganda: I took CY-100 and went to a great deal of effort to diversify (I am certified as a professional in five technical fields); I know of no one in NSA who has any interest in my diversification.

If NSA management actually believes there is a need for diversification, they should identify some jobs that demand multi-disciplined analysts (such analysts are readily available); and they should enhance the careers of multi-skilled people to demonstrate that such broadening is actually valued.

If NSA management does not believe there is a need for diversification, they should stop telling lies to naive young employees.

[redacted] *P13*

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

P.L. 86-36

DOCID: 4019716

P.L. 86-36

~~SECRET~~

To the Editor:

(U) I read with some misgivings [redacted] praise of W Group ("Cogitations of a Contumacious Cabalist" *CRYPTOLOG*, 3rd Issue 1989), and feel that a molifying response may be in order. I laud [redacted] obvious pride in belonging to the W Organization; however, I found her point to be somewhat obscured and diffused by it. If she is dismayed by what she perceives is a lack of appreciation of W Group by the rest of DDO, then she may be assured that this is by no means the case. On the other hand, if she is trumpeting the unique qualities of W Group and its personnel, it may be best to remember that we are all team players whose efforts should be put in the larger context of contributing to national intelligence objectives. DDO would be truly hampered, but certainly would not "crumble like a house of cards" without W Group.

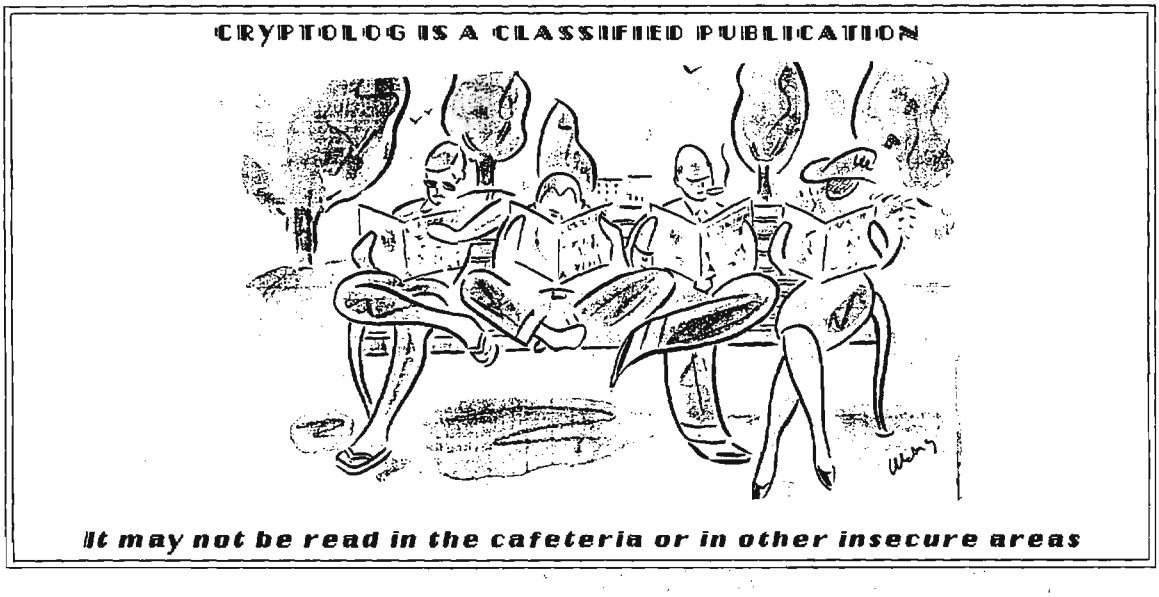
P.L. 86-36

~~(S)~~ It may also have served her purposes better if [redacted] continued her familial symbolism by describing ELINT's split personality - "op" and "tech". Most line analysts should have a passing familiarity with tech ELINT but, if they are involved in military (the current and antici pated de-emphasizing notwithstanding) civil air, telecommunications and tech transfer, or many other problems, Op ELINT is a very important part of their lives. We in B51 have a deep and unabashed respect for Op ELINT. My first introduction to the practical applications of this discipline was in April 1972, and it left a lasting impression on me. That Op ELINT could geolocate, corroborate and and identify individual Vietnamese surface-to-air missile sites, with the result affecting the life expectancy of U.S. air crews, is a lesson I hope never to forget.

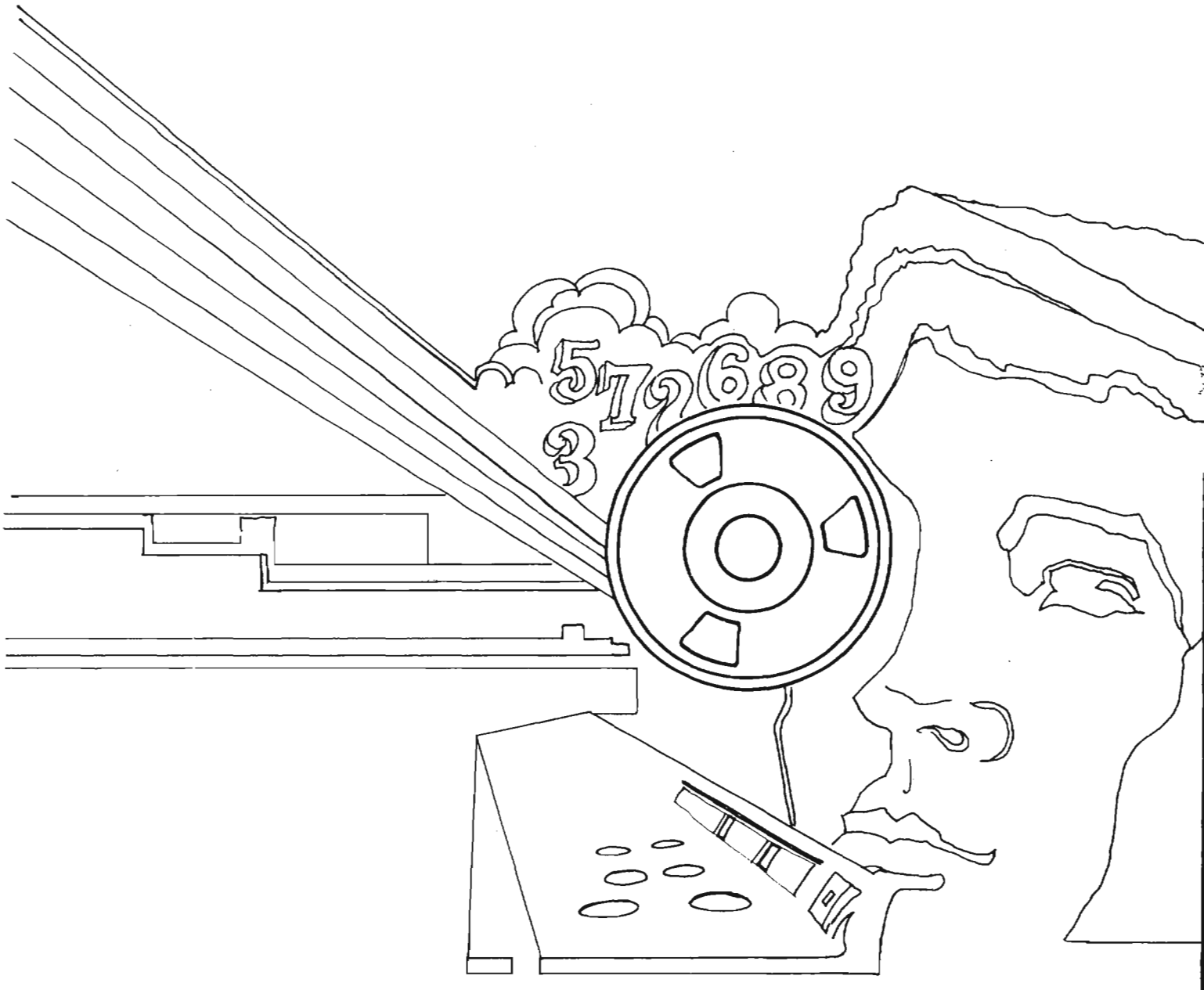
~~(FOUO)~~ To close, I would like to reemphasize that the operational side of ELINT is well appreciated in at least this corner of DDO (in fact, through out the organization, if the attendance of last year's Op ELINT seminar is any indication), that we recognize the fact that analysis of guidance triplets and jitter modes is best left to those who know them best (and possibly perpetuating [redacted] observation that ELINTers are misunderstood), and that in the analytic arena we should operate in concert, not opposition (although I am the first to admit that it very often doesn't seem that way).

[redacted]

P.L. 86-36



~~SECRET~~


5 7 9 6 8 9
3

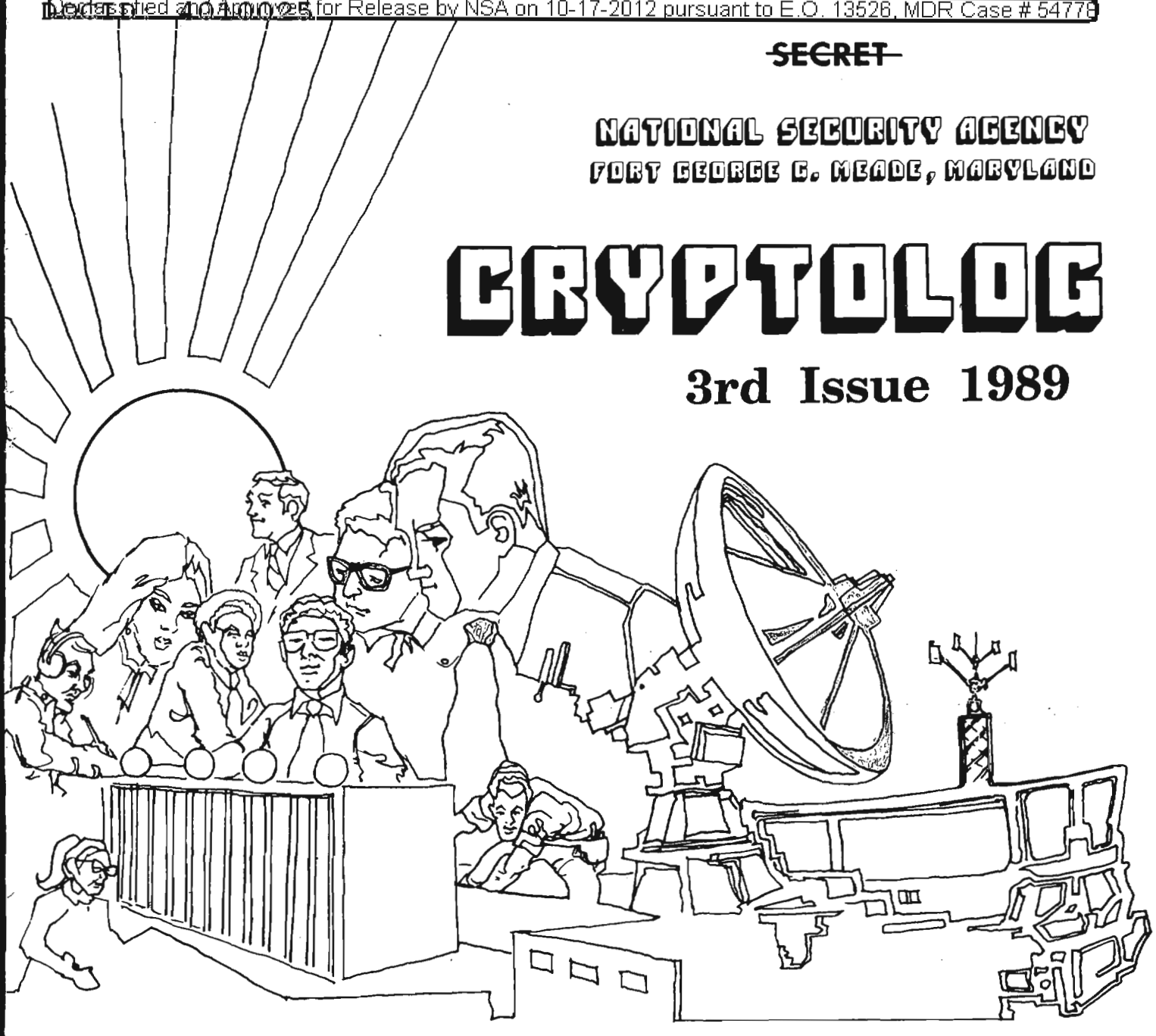
Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

3rd Issue 1989



50 YEARS WITH UNCLE SAM 1
ERRATUM 6
MAPS AS VITAL RECORDS . . . . . [redacted] . . 7
DINOSAURS ARE ALIVE AND WELL. . . . . [redacted] . . 9
PORTABILITY PROBLEMS IN C PROGRAMMING . . [redacted] .12
SPECIAL INTEREST GROUP ON FUSION. 17
COGITATIONS OF A CONTUMACIOUS CABALIST. . . [redacted] .18
LETTERS 19
ANSWERS TO TA EXERCISE. 20
HARDWARE REVIEW: THE NeXT COMPUTER
[redacted] .21
BULLETIN BOARD. 28
REVIEW: STRUCTURE AND INTERPRETATION OF COMPUTER PROGRAMS . . .
. . . . . [redacted] 29
CLA ESSAY CONTEST 32
TA EXERCISE . . . . . [redacted] .33

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

DOCID: 4010025

P.L. 86-36

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XVI, No. 3 ..... 3rd Issue 1989

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Index ..... (963-4814)
Information Science ..... (963-3456)
Information Security ..... (972-2122)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (963-4958)
Special Research ..... Vera R. Filby (968-5043)
Traffic Analysis ..... Robert J. Hanyok (963-4351)

Illustrators ..... (963-6234)
..... (963-6423)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, NORTH 2N018

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five)
(note: no 'o')

via ALLIANCE, send to:
PLBROWN [note: all caps]
attn: CRYPTOLOG

Always include your full name, organization,and secure phone; also building and room numbers.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, NORTH 2N018
Please do not phone.

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

ABOUT DISTRIBUTION

We had been submitting address changes to Distribution at the eleventh hour, just before CRYPTOLOG went to press, in an effort to keep up with the last-minute moves of subscribers. But ironically, it turns out that the Press greatly improved its turn-around time, outpacing that of Distribution, so the changes were entered well *after* the eleventh hour And that's why we've been having problems with distribution, except for times when CRYPTOLOG was held up at the Press.

So now we have to go the way of commercial magazines ("allow six to eight weeks for change of address . . .") and close the distribution list well before we're ready to print.

While we're on the subject of distribution, let us direct your attention to a paragraph in very small print that appears elsewhere on this page. It reads,

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

This means that

- copies of CRYPTOLOG may not be forwarded to subscribers in the field.
- field stations may not pass copies of CRYPTOLOG to their subordinate field entities.

For further information about the distribution of CRYPTOLOG to the field, please write or call the Editor.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

~~SECRET~~

50 YEARS WITH UNCLE SAM

~~(FOUO)~~ The popular perception of a federal employee with 50 years of service is that of a timid, colorless person shuffling papers in an obscure corner of an obsolete government bureau. The protagonist of this article is no such thing. He is a visionary, NSA's own Jules Verne and Arthur C. Clarke, whose imagination was lauded by NSA's first Deputy Director. He is a man of integrity, an activist who speaks out when moved to do so. He is a doer who actually gets out in the field to implement his theories. He is a world-class scientist, unknown to PBS audiences only because his endeavors, and his association with them, are classified. Among his many honors is his election to the prestigious Cosmos Club for original research and publications on the ionosphere.

(U) During an exceptional career, Nate, through his energy, enthusiasm, and dedication to solving the real problems, has inspired others and broken new ground. He has won the gratitude, affection, and respect of his colleagues here and abroad. He is the epitome of a visionary, scientist, and explorer.

(U) This tribute was composed by his friends and admirers, and submitted with their very great affection and respect.

(U) When young N. C. (Nate) Gerson returned from summer training with the Massachusetts National Guard in 1934, he found a telegram from the Government Printing Office in Washington, offering a position at $90 a month. The country was in the grips of the Great Depression and jobs were unavailable, so his mother was convinced that President Roosevelt personally made the selection to help the family. Thus started a federal career that stretched over half a century.

(U) In 1938 he transferred to the US Weather Bureau and subsequently was assigned to San Juan, Puerto Rico. There he worked all night (2200-0600) and attended the university as a full time day student (0800-1600). After three years with four hours sleep a day he graduated magna cum laude with a BS in physics. Then he began what was to be a series of "firsts." He completed the first thorough evaluations of pseudo-adiabatic equations. In 1943 in Puerto Rico he made the first upper air wind determinations using wartime radar and resonant dipoles suspended below radiosonde balloons. This technique was implemented for routine observations of upper air winds. He also designed all the thermodynamic charts needed to evaluate upper air soundings, many of which are still in use today by the Weather Bureau and by DoD. This work was not without peril, as Nate reports:

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4010025

> While working at Arecibo, the open cable car taking me from the carriage house, (500 ft above the antenna) to the ground struck the feed structure. The car "caught" and became horizontal as it was haltingly dragged over the structure. The car almost dislodged itself from its support cable; had it done so it would have plunged to the ground. I hugged the only vertical (now horizontal) strut on the flimsy cable car for dear life. After scraping clear, the car swung wildly while its support cable oscillated vertically 15-20 feet — all about 500 feet in the air. I was glad to reach the ground. A $10 override switch in the circuitry would have prevented a mid-air collision course between the cable car and the feed structure. I expressed my peevishness to the management.

(U) In 1945 Nate met a beautiful creature in the WAVES. She married him before realizing that his annual salary was only $1620. The Navy, during their honeymoon, assigned her to Barracks D with 3999 other women. After their return to Washington, Nate would visit her in the evening until at curfew an enormous WAVE wearing an SP armband would tap him on the shoulder and say, "Time to go home sonny."

(U) One day in 1946 an old professor sauntered into the office and told Nate's boss that he wanted Nate to work for the Army Air Corps. Listening with apprehension Nate learned for the first time that his boss appreciated him, but the professor won, and Nate was shifted to the US Army Air Corps' Watson Laboratories at Fort Monmouth, NJ. He left Washington by train on a Monday morning, telling his wife he would return by Friday. Thursday morning he was given 120-day travel orders, later extended another 120 days. He crisscrossed the arctic from Hudson's Bay to Alaska and visited (under primitive conditions) more of the Canadian north than most Canadians ever will see.

(U) At the Watson Labs Nate assisted in evaluations of 180 kHz experimental Loran navigational systems in southwestern Canada, later implemented as LF LORAN. He was responsible for its calibration and acceptable operation at all field sites in Canada and Alaska, from 45° N to beyond the Arctic Circle. Its reliability led to its installation globally as an electronic navigational system for ships and aircraft. And another first: Nate completed the first analysis of natural LF noise intensities in the subarctic.

(U) While doing all of this, Nate managed to obtain an MS in physics from New York University, and has worked in that field ever since, first in thermodynamics then in electrodynamics.

(U) In 1948 the Army Air Corps split from the Army and became an independent Service, the Air Force. Nate was asked to organize a research laboratory devoted to radio wave propagation. Feeling that knowledge of the medium (the ionosphere and atmosphere) was essential, he established the Ionospheric Physics Laboratory, still in existence, and became its Chief and one of the five founders of the Air Force Cambridge Research Center near Boston. Characteristically, he took charge at once, and reoriented the USAF radio propagation research from statistical studies of intensity variations on point-to-point circuits to an understanding of the physics and dynamics of the ionosphere. Among his many initiatives during this period was the implementation of a follow-the-sun (as the earth rotated) airborne observatory to obtain ionospheric soundings over the North Pole; it then became possible to examine arctic ionospheric drifts and to obtain midlatitude airglow spectra.

(U) Early on, Nate revealed his mettle as innovator and goad, backed by that single-minded purposefulness that is an elemental factor of success. Between 1948 and 1956 he made pioneering studies of auroral, ionospheric, and geomagnetic physics and prodded the U.S. and Canada into becoming world leaders in this field. He won over initial opposition, and instrumented an airborne laboratory for ionospheric and spectrographic measurements, a concept later copied by the Soviets. The plane he sent to the arctic developed mechanical problems, drastically reducing the flying hours over the North Pole, which led him to propose and justify

EO 1.4.(c)
DOCID: P.L. 86-36 4010025

the US station at the South Pole. (In sun-earth geometry the poles provide unique observational points.)

~~(TOUO)~~ In 1956 he was invited to present a lecture on ionospheric winds at Arlington Hall Station to a group unknown to him — the newly formed National Security Agency. Before the meeting ended he was asked to consider a consultantship. Shortly afterwards the US National Committee for the International Geophysical Year suggested that he join Deep Freeze II, the US Antarctic Expedition, as Admiral Byrd's Chief Scientist. However, by that time he had become hooked on the challenges facing NSA, and he became a full-time employee in the old REMP— Research, Engineering, Math and Physics.

~~(TOUO)~~ Nate's insight into NSA's problems has been extraordinary. This probably stems from his stint with the Air Force, where he looked at propagation from the point of view of communications; at NSA ,the viewpoint is that of intercepting. Now one of his primary concerns is improving the front end of the SIGINT system — intercept.

~~(C)~~ And as some of you know all too well, Nate speaks his mind, even when his comments might be unwelcome. For example, he discounted rosy estimates

Unfortunately he was proven right —the physics just did not permit it.

~~(S-CCO)~~ The range of his activities at NSA is astounding. Among his many undertakings, he examined High Frequency Direction Finding accuracies and system improvements, intercept from HF to SHF, general search, and electromagnetic wave propagation in general.

Nate relates his adventures ...

The Roof and Floor of the Earth

In Antarctica I slipped on an icy hillside and slid 3000 feet free-fall to the bottom. On another occasion my Weasel stalled on a very steep icy path. I parked and carried the 750-pound dummy load cross country uphill 200 yards through knee-deep ice-encrusted snow. The flight "to the ice" from New Zealand was unusual; a forward hatch unexpectedly opened and discharged a life raft which automatically inflated and slammed against the tail section. The plane was thrown out of control until the life raft finally blew off. Unfastened passengers were thrown about like corks. I had been sleeping on the cargo and could not reach a bucket seat until grabbed by friendly hands. The pilot recovered less than 1000 feet above the sea. We were three hours from McMurdo Sound.

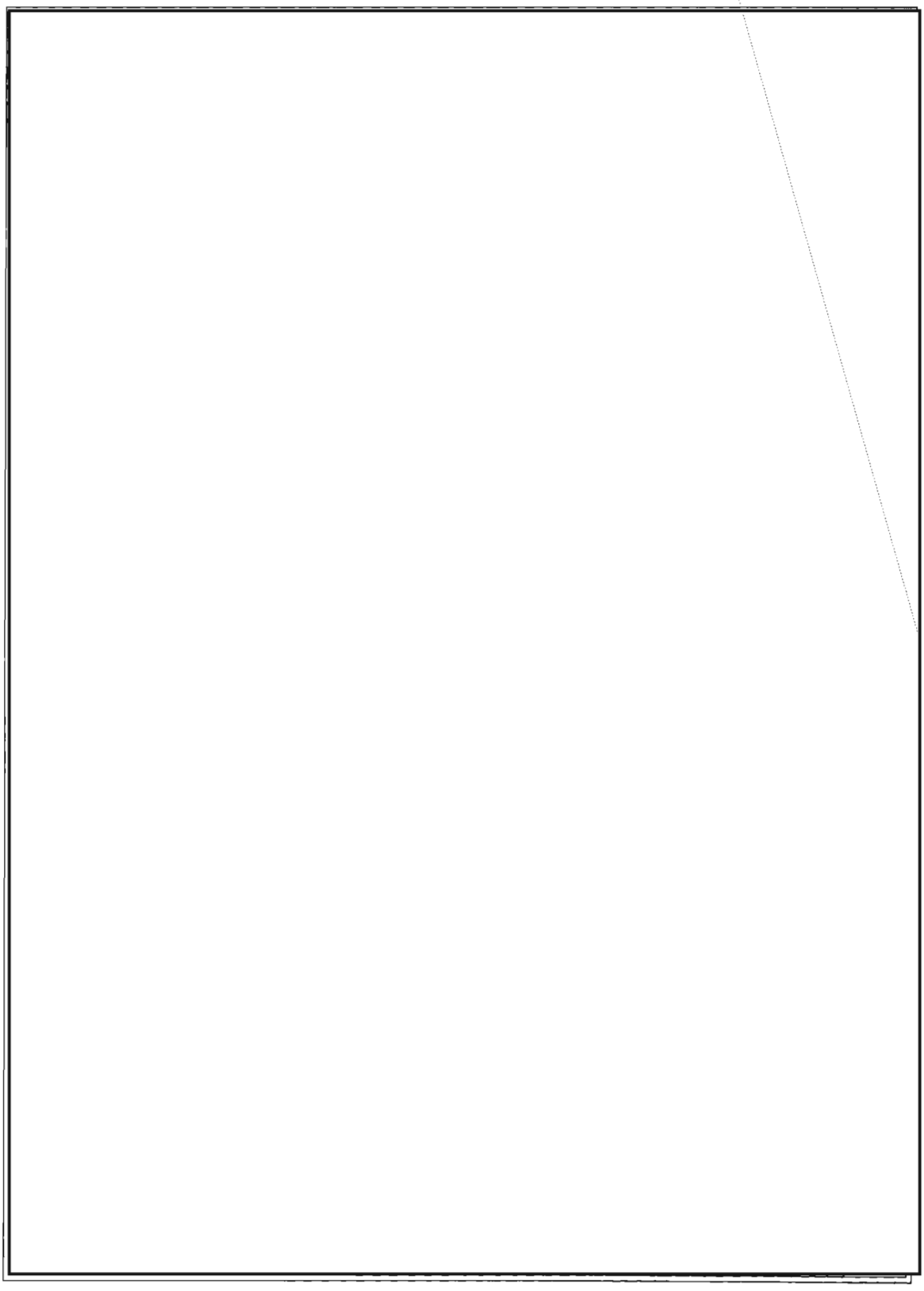
In the Arctic one December morning when I left the mess hall after breakfast for work, I was blown down onto the snow four times during the 3/4 mile walk to the Operations Building. Time for the "walk" was 45 minutes. During two summers (outdoor temperature +52F) the work was so arduous that perspiration soaked through all my clothes to the outside of my parka. On several trips I lost 10 pounds during the first week. While I was working at isolated outside facilities one summer, grazing caribou came within 15 feet. On one occasion, working alone far from the station, I came across fresh wolf tracks in the soft tundra.

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4010025

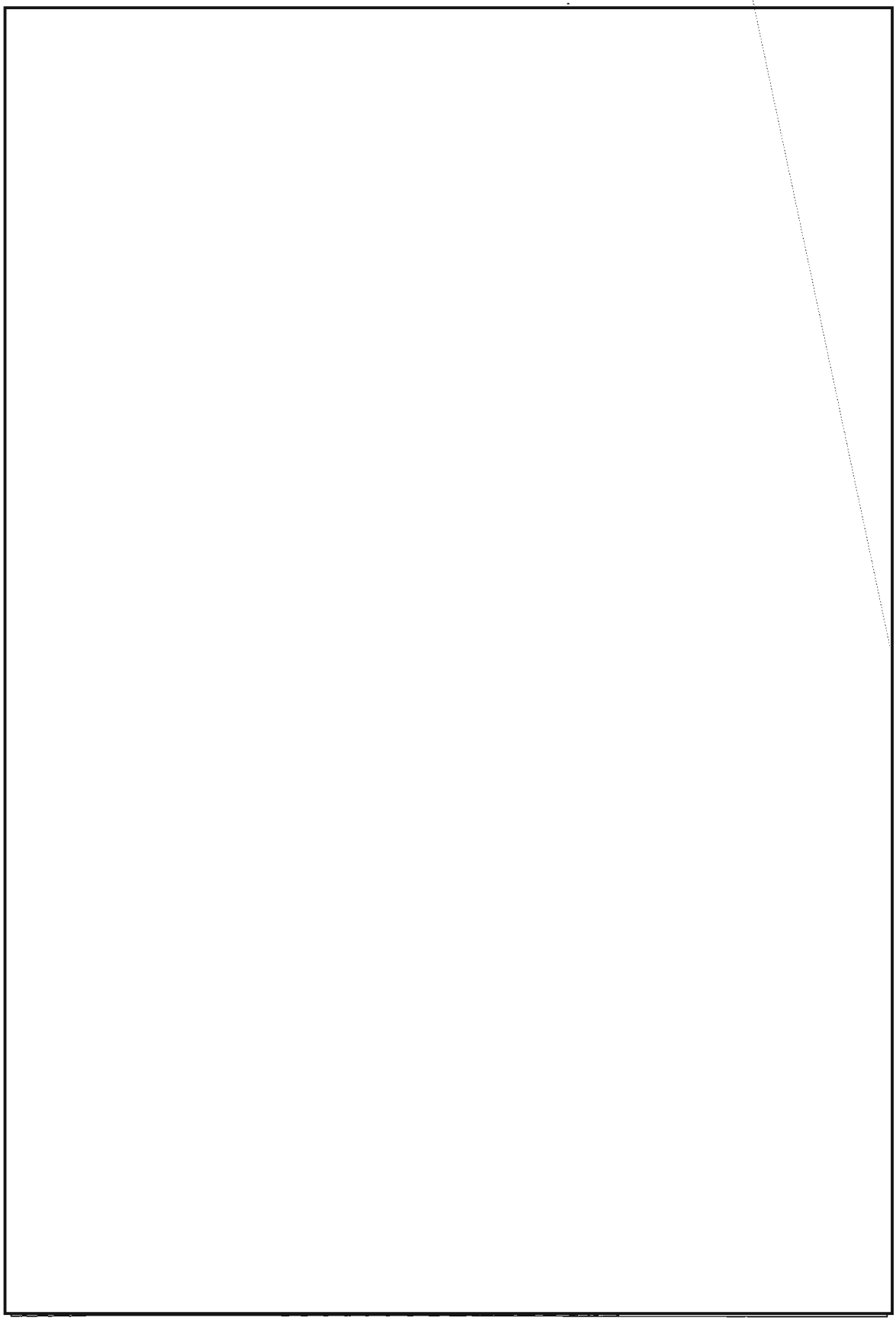
EO 1.4.(d)
P.L. 86-36



Two of the many congratulatory messages sent to Nate

DOCID: 4010025

EO 1.4.(d)
P.L. 86-36



EO 1.4.(c)
DOCID: 4010025 36

[redacted]

~~(C)~~ At NSA Nate has bounced between DDR and DDO, alternating between theoretical science and practical applications, as he prefers to do. He has regularly visited field sites to gain first hand understanding of the operational system as it is, not as it is surmised to be. He spent over four years beyond the polar circles, and is the only Agency employee sent to both the Antarctic and the Arctic.

(U) Like the professor he might have been, he is adamant that every project produce a positive or negative final report in good idiomatic English to guide future workers, "otherwise you flunk the course." Moreover, the reports must be short, and to the point. Some unhappy souls discovered, too late, that Nate has a short fuse for six-pound reports containing only one sentence of value.

~~(FOUO)~~ High on his wish list for NSA is that quality outweigh quantity; a close second is that managers be more aggressive in sifting wheat from chaff. He urges Engineering to be somewhat more responsive to Operations, but he would like to see Research given higher internal status (and set higher goals). At the same time, he insists that proposals be more critically evaluated before adoption. As for people, the single most valuable attribute anyone can have is integrity.

(U) Still a starry-eyed idealist, he believes (even as he scolds it) that R&E is comparable to the Lake Woebegone Community: all the women are beautiful, all the men dedicated, and all the Elders wise.

P.L. 86-36

ERRATUM

In 2nd Issue 1989, "Compusec Policy for the Intelligence Community," by [redacted] two captions were inadvertently transposed. Please replace the published diagram with the one shown below. CRYPTOLOG regrets the error.

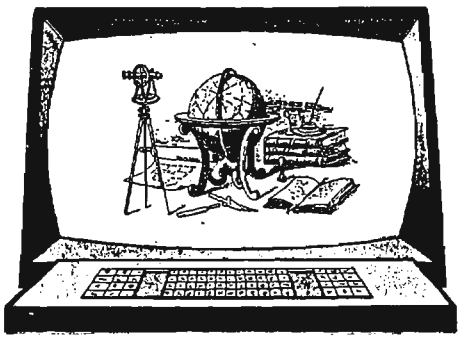
MODES OF OPERATION

USER ATTRIBUTES	Dedicated	System-high	Compartmented	Multilevel
Need-to-know	All	Some	Some	Some
Access	All	All	Some	Some
Clearance	All	All	All	Some

unclassified

DOCID: 4010025

MAPS AS VITAL RECORDS



T541

(U) Two aspects of the emergency preparedness programs were prime factors in the revitalization of the Vital Records program. These were (a) having records available which will ensure the effective conduct of essential United States Government activities, and (b) having sufficient means, people, equipment and physical plant to manipulate these records as needed.

P.L. 86-36

~~(FOUO)~~ The revitalization began in October 1985 with a memo from the then NSA Records Officer, [redacted] reminding all Agency elements that the Director had tasked the Agency with designing and building "a framework for a survivable SIGINT system, under all conditions, including general war." Through seminars and personal contacts, the Senior Key Component Records Officers were apprised of the T54 plans. With the assignment of a vital records controller to T5411, planning began in earnest.

(U) The element records officers analyzed their element's operational needs and identified the records that they considered vital to their survivability and reconstruction plans. Among them were the map requirements. These were submitted to the controller.

(U) After analyzing the requirements for maps and geographic aids submitted by the various records officers, the controller noted that several components had a requirement for the same materials. And just at that time came an evaluation of the Agency's performance during the Joint Chiefs of Staff exercise PRESENT ARMS, which concluded that maps and geographic aids would have greatly assisted the NSA participants in performing their tasks. The Controller decided to develop a single file to make all map and related information available to all possible users. Thus was born the idea of the Common User Module MAPNEED (CUMMN).

(U) Several things had to be done before the maps and geographic aids could be indexed into a retrievable data file, then shipped to and stored at a Vital Records Depository. First was to develop a system of accounting for each item placed into the data file, as well as a manual retrieval system. Then all maps had to be folded to fit the legal size folders used for shipment and storage. The folders were marked with identifying information as depicted in Figure 1, then placed in boxes marked CUMMN ##.:

Chart	Country (ies)
Sheet #	Placename
Sheet #	Placename

Figure 1

~~(FOUO)~~ The controller and the T54 Project Officer for Archival Processing developed a file containing a collection of maps and geographic aids that were identified as vital to the Agency teams engaged in reconstruction, emergency relocation, or critical post-disaster operations. This was provided to the element records officers.

~~(FOUO)~~ The file took form as maps and geographic aids, procured through the T54 Map and Geographic Aids Library, began to arrive. It includes a machine database called MAPNEED with a backup file called NEWMAP. Both the original database and the backup file use the dBASE III PLUS system and show identifying information about the maps and geographic aids contained in the file, as well as other identifying data. As items that are out-of-stock or out-of-print are procured, the file will increase in size. 5,044 items are currently indexed into the data file.

(U) The procedure is virtually self-evident:

- Enter the data into each field and press (CR).

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

```
D B A S E  I I I  P L U S
  S T A R T U P  M E N U

1. Use NARADEX Programs
2. Use ANSUM Programs
3. Use ACCONLOG Programs
4. Use Vital Records Programs

0. EXIT
```

Step 1. Select 4.

```
V I T A L  R E C O R D S

1.  YAKIMA Records
2.  MAPNEED Records

0.  EXIT
```

Step 2. Select 2.

```
M A P N E E D

1. ADD INFORMATION
2. CHANGE INFORMATION
3. REMOVE INFORMATION
4. ADD COUNTRY INFORMATION
5. PINT OUT FILE

0. EXIT
```

Step 3. Select desired action.

~~FOUO~~

Figure 2. Accessing the data base

- When all data has been entered, press (PgDn) to move to the next record.
- Press (Ctrl/End) to save all the new information that has been entered
- When the computer screen indicates 0 (select 0) press (CR) until a dot prompt appears.
- At the dot prompt, type <USE MAPNEED INDEX MAPCHART> and press (CR),
- Type <REINDEX> and press (CR). This command reindexes the file and place the new record containing the new information in its proper place.

Field		Type	Length
1	REC_NO	C	6
2	CHART	C	50
3	PROJECTION	C	20
4	SCALE	C	18
5	LOC_INFO	C	80
6	BOX_NR	C	7
7	ORG	C	20
8	COMMENTS	C	50

Explanatory Notes

1. REC_NO indicates the record number.
2. CHART is the short title of the specific chart otherwise the long title.
3. PROJECTION indicates the type of projection requested by the user if available.
4. SCALE is the ratio of units used on the map or chart, i.e., 1:50,000.
5. LOC_INFO is the country or geographic area covered by the map or chart, or in the case of UTM charts, the long title.
6. BOX_NR refers to storage
7. ORG is the organizational designator(s) of the requesting NSA organization. Multiple designators are separated by backslash (\).
8. COMMENTS additional descriptive data

(U)

Fig. 3. Data Structure of MAPNEED and NEWMAP

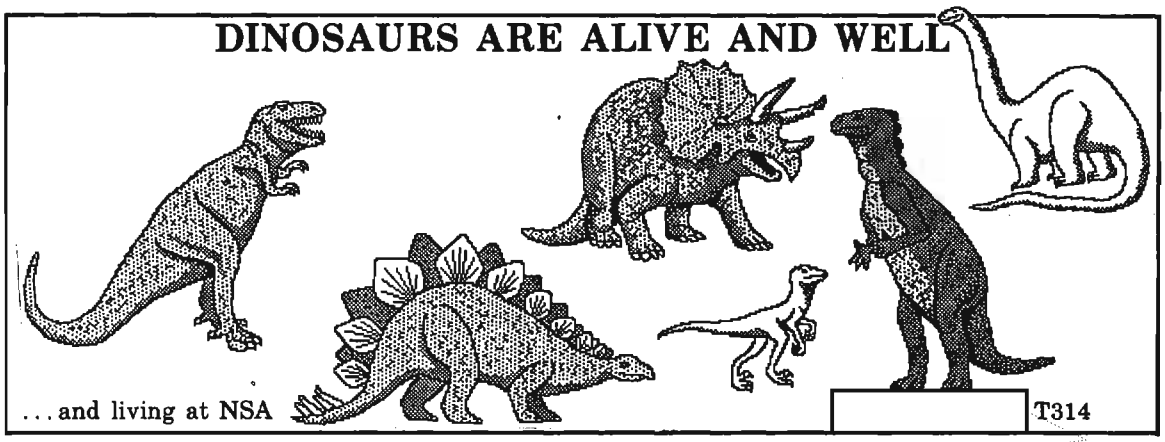
(U) All the routines for modifying and accessioning data are just as easy to do. It is possible to retrieve information on any the fields shown and to print it out. There are procedures for selecting all charts required by a specific organization or user, or by a combination of them. It is even possible to make a "gang" selection to include all organizations subordinate to the one cited. □

CRYPTOLOG

welcomes your letters and comments

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025



P.L. 86-36

The article "Software Acquisition: A Reform in Need of Reform" by [redacted] 2nd Issue of 1988, prompted me to propose a radically different view from the one proposed in that paper. I contend that software acquisition is not so much in need of reform as are the philosophies and practices of those who manage the software acquisition or development. Seat-of-the-pants software acquisition and development didn't die with the advent of formalized procedures. It's thriving at NSA, kept alive by archaic software management practices and philosophies that have failed to adapt to the new generation of concepts in the software world.

IN-HOUSE SOFTWARE DEVELOPMENT

Poor management is the main reason for NSA's software development problems. This includes inept Software Development Managers who fail to plan and organize the development effort, the laissez-faire style of upper management that fails to enforce commitments and has a "hear no evil, see no evil" attitude, and apathetic external organizations with no active interest in software development.

THE CUSTOMER

The road to failure doesn't begin with the development organization or the program management office but with the customers' lack of committed involvement and poorly defined and expressed needs. Only when the system is deployed do they take an active interest in the product. The pervasive attitude seems to be "Here, Research and Development, perform a miracle with this sparse information and we'll talk to you when it's done or when we need a change in the miracle."

While overstated, this situation is real. At this juncture, the customer is the only one who knows specifically what it needs and what information is necessary to meet those needs. Operational organizations should place greater emphasis on conveying those needs as clearly defined objectives and requirements. Often requirements are so generic that what takes place is "interpretation by misperception," (i.e. a mismatch between what the developer understands and what the customer meant). Continuous customer involvement during the entire development process is vital to clear, concise requirements. The technical exchange and direction the customer could provide would help immensely in guiding an errant project.

UPPER MANAGEMENT

The most frustrating obstacle to overcome is upper management's non-receptiveness to issues concerning suspect software development practices. "You can knock forever on a deaf man's door," says Zorba the Greek. The message they're sending is interpreted as non-support and indicates a lack of trust in their subordinates. This action is hypocritical for an organization espousing the benefits of NSA manuals on software development. One wonders from what perspective upper management is viewing the situation.

One could postulate that the motives are partially financial. The measure of an organization's worth has become the size of its budget, instead of its efficiency and effectiveness. And since the organization is budget-based, the normal business definitions for

"performance" and "results" have changed. "Performance" becomes the ability to maintain or increase the organizational budget, while "results" is the acquisition of a larger budget (Drucker). By accepting troubled systems, the worse off the better, management acquires justification for their budget. Unfortunately, it's justification by non-performance.

Another perspective, using 80's terminology, involves male bonding and the "good ol' boy" upper management fraternity where shunning inter-organizational conflict is all too prevalent. Conflict is inevitable and, in my opinion, necessary in our dynamic working environment. Software maintenance organizations have been compromising their ability to maintain newly developed software because of upper management's resistance or inability to take stands on software development issues that cut across organizational boundaries. It is amazing that a stance has not been taken in light of some of the recent software disasters.

Upper management difficulties are not solely internal to the organization: problems are also generated by external organizations failing to acknowledge and enforce the responsibilities they approved. Management's concurrence on documents has become more of an exercise in form than in substance. Corrective measures are rarely taken when identified obligations are not fulfilled. There is a definite truism in relating management signatures to the cliche "... not being worth the paper it is written on".

THE DEVELOPMENT ORGANIZATION

The lack of proper management practices is nowhere more apparent than on projects with software development problems. The use of formalized software development techniques isn't the root of the problem since in most instances they are not being used anyway. The problem lies in the inconsistent or nonexistent application of basic management principles: planning, organizing, integrating, and evaluating. Formalized software development techniques are nothing more than an advanced application of these basics.

Planning, as I loosely refer to it, is usually done in one of two ways. The first is planning by mental imagery. The software development or acquisition manager knows what the overall objectives are and begins to visualize and initiate the steps needed to get the ball rolling. He then applies the same technique to a variety of sub-objectives. Eventually, he is overwhelmed trying to keep track mentally of everything going on. So the project that started out with the best of intentions falls into disarray, missing schedules and going over budget, and turns into a QRC effort - not a Quick Reaction Capability, but a Quick Reaction to Chaotic conditions. The two are similar, in that both are undocumented, untested, and meet only the minimum requirements.

Planning by camouflage is used when a boilerplate Software Development Plan is written. The document is written in a half-hearted attempt to satisfy an NSA reg but is not periodically updated. All the right buzz words are there, but unfortunately the document lacks substance. Nevertheless, the document is waved like a banner in proclamation of good software development techniques. Eventually, its fragile nature becomes evident as the complexity of software development increases. Development collapses because of a false sense of security in having a plan, owing to a common but mistaken belief that planning is a one-time event rather than an on-going activity.

Without adequate planning it is unfair to discuss the organization and integration of project resources. Whether the resources are time, budget, personnel, facilities, or managerial style, success is directly related to the effectiveness of planning. On problem projects, the software manager is in a reactive rather initiative mode when it comes to coordinating and utilizing resources. In the past, it was possible to compensate for poor planning by drawing on additional resources, for even if the project came in late and over budget, -- who cared -- the money was there. As we move into a period of greater austerity, this avenue of escape will no longer exist. Poor project management will become increasingly apparent.

More often than not, development organizations become afflicted with software development amnesia, so mistakes made in previous projects recur, usually in the form of schedule slippages and over-expenditures. Critical evaluation of a project isn't something that is done just at project completion; like planning, it is an on-going activity. Evaluation of mistakes provides an opportunity to learn how not to do things as well as how to do them.

DOCID: 4010025

SOFTWARE ACQUISITION BY CONTRACTING

Is software acquisition more expensive than in-house software development? Not really. There are hidden costs in in-house software development owing to large adjustments in schedules and our hypocritical attitude toward documentation. When software is developed in-house, schedule slippages lock development personnel in place, adding to the initial cost and delaying the opportunity to begin new projects. Adding to that cost is documentation that is non-existent or poor in quality. In most cases, software documents have to be upgraded to a level of acceptability by the life cycle support organization using their own personnel or contracting the work out.

Acquisition is not a panacea for the Agency's software development problems. I do not advocate contracted efforts and do not believe the end product is any better just because it was developed by a contractor. What I have found is that acquired systems are better documented and experience fewer schedule slippages. The reasons for this are contractual and financial. Software documents are identified as part of the Contract Data Requirements List and the contractor is motivated by profit to avoid excessive schedule slippages. Problems surface when the Agency provides inadequate requirements definition in the purchase description or asks for modifications because of unforeseen environmental changes. Of course the contractor is going to ask for more time and money. These risks should already have been considered when opting to acquire, rather than develop, new software.

RECOMMENDATIONS

▸ Don't blame Agency software development practices and procedures for the project's failures. "It is a poor workman that blames his tools for shoddy work." Instead, tailor them to meet the size and needs of the project. In this case, familiarity breeds proficiency.

▸ Try to obtain the clearest possible definition of what the customers really need. The customers should be as involved in the project as is the developer. If they aren't, they have only themselves to blame for the type of system delivered.

▸ Become receptive to bad news during software development. Not only must you listen to what is being said, ou must act. A Janus-faced stance on enforcement of Agency standard software development practices promotes organizational inefficiency and ineffectiveness.

▸ Accept and use the Agency's software development methodology. Credibility to deliver acceptable software is being undermined by resistance to using new techniques. The track record for previously developed software indicates changes are needed. There are reasons for the existence of the NSA regs.

▸ Provide more opportunities to software support organizations to develop software. Presently, by charter, most of the Agency's new development is being done by research and development organizations. Expanding development opportunities will give the customers a choice of developers and make the process. Quality then becomes the prime justification for increasing organizational budgets. The customers usually keep selecting a developer whose projects not only perform, but are timely and cost-effective. The Agency should no longer keep all of its development eggs in one basket.

CONCLUSION

My opinions are based on experiences and observations in software support. My concern is not for present but for future developments. In most cases, it is too late for constructive suggestions to have an impact on current projects. Even the simple identification of problems is often seen by the developer as meddlesome intrusions. Changes need to be made in the way the Agency handles future software development. The Agency is too dynamic and its software personnel too professional to be sabotaged by archaic software development philosophies and practices. If the Agency fails to adapt to the new software environment, it runs the risk of meeting the same fate as the dinosaurs. Those large entities were overcome by their failure to adapt. Unfortunately, too many Agency dinosaurs are still developing software.

ACKNOWEDGEMENTS

My thanks to [redacted] T31 Technical Writer, for her constructive comments.

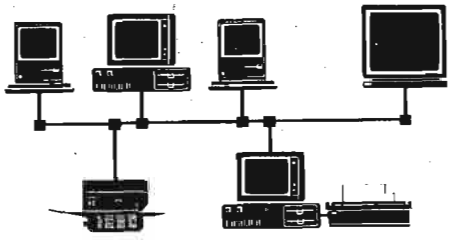
P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

Portability Problems in C Programming

. . . and how to avoid them



P.L. 86-36

Many portability problems are hidden from the C programmer because C is a high-level language. Some of the flexibility which allows C to be easily implemented on so many machines also allows for variations in a number of well-defined ways. A programmer must be aware of these variations in order to be able to write portable code. The most important variations are described below.

WORD SIZE

The common word sizes today are 16 and 32 bits, with some 8-bit words on aging micro computers and 64-bit words on some super computers. In C/UNIX the common word size porting problem comes from using the variable type "int". An int is defined as the storage class that is most efficient on the given machine. On a 16-bit machine an int is 16 bits; on a 32-bit machine it is 32 bits.

Problems arise when you try to go from larger to smaller word sizes and find that an int is no longer large enough to hold your information. Problems also arise when you try to write data in the form of an int to a disk file. On a 16-bit machine it will take 2 bytes of disk space; on a 32-bit machine it will take 4 bytes. If a program believes it knows how many bytes of data are on the disk it may be surprised when compiled on a different machine.

For portability one should use the variable type "char" for 8-bit data, "short" for 16-bit data, and "long" for data which is 32 bits or more in size. Remember too that an unsigned quantity will allow a magnitude twice as large as the original.

Some examples of different sizes :

```
short=2, int=2, long=4     :  PDP-11, AT (XENIX)

short=2, int=4, long=4     :  386(SCO-XENIX), SUN-3-4, ASH(3b15/20), CONVEX

short=3/4, int=8, long=8   :  CRAY
```

Further, programs should use the "sizeof" compiler construct if they need to reference the size of an "int" variable. Unfortunately there is a lot of code that doesn't use these more portable constructs.

BYTE ORDER

Different machines have different ways of storing 16- and 32-bit quantities. Let's first consider the ways a 16-bit value might be stored :

```
short variable = 0x0102;     /* 0x is notation for hex */
```

this may be stored internally as

```
01 02            /* each 2 digit number is */
   or            /* is a byte              */
02 01
```

Now consider the ways in which a 32-bit value might be stored :

```
long variable = 0x01020304;   /* 0x is notation for hex */
```

this may be stored internally as

```
01 02 03 04          /* each 2 digit number is */
     or              /* is a byte              */
04 03 02 01
     or
02 01 04 03.
```

There are two kinds of portability issues that arise from this difference.

The first problem comes from using more than one kind of storage class to access this information. For instance, suppose you allow a short (16 bits) to represent a character on a display screen. In the short the Most Significant Byte is the actual character displayed and the Least Significant Byte is its attributes (foreground color, background color, blink, underline, etc.). When you initially put a character in this short you will store both the character and the attribute. Now suppose that you wish to write over the character but not affect the attribute. Most programs will let a character pointer point to this short and then change the first byte. This is not portable since it only works on machines with the first byte ordering scheme. If the second scheme is used the MSB is actually the second byte. This problem is even worse when dealing with 32-bit quantities since there are more possible outcomes.

The second kind of portability issue deals with writing this data to a disk file. A file that is created by writing shorts or longs to the disk will not have the same meaning if it is transferred to a different machine with a different byte order. This gives rise to interoperability problems between machines and the need to translate structured data files when transferring from machine to machine.

Some examples of variants

```
with 8 bytes in order being = 0102030405060708
2-byte short=0201    4-byte long=02010403    : PDP-11
2-byte short=0201    4-byte long=04030201    : AT(XENIX)  386(SCO XENIX)
2-byte short=0102    4-byte long=01020304    : SUN-3-4  ASH(3b15/20) CONVEX
3-byte short=060708  8-byte long=0102..0708 : CRAY
```

BYTE ALIGNMENT, STRUCTURE SIZE

Some machines allow a short (16 bits) to be aligned in memory on any byte boundary, others allow a short to be aligned only on even byte boundaries. Further some machines allow a long (32 bits) to be aligned on any byte boundary, others allow a long to be aligned only on even byte boundaries, while still others allow a long to be aligned only on 4 byte boundaries.

In UNIX you can group related variables into a structure. A UNIX structure has as its elements each of the related variables. For example:

```
struct example
{
     char  first_char;      /*  8 bits */
     short first_short;     /* 16 bits */
     long  first_long;      /* 32 bits */
};
```

This defines a structure called "example" that has 3 elements "first_char", "first_short", and "first_long". On a machine that allows alignment on any byte boundary the elements in the structure will have the following data storage:

```
struct example
{
   char  first_char;  /* byte 1                                  */
   short first_short; /* byte 2 and byte 3                       */
   long  first_long;  /* byte 4, byte 5, byte 6, and byte 7 */
};
```

And its size will be 7 bytes. On a machine that allows alignment for shorts and longs on even byte boundaries only the following storage will be in effect:

```
struct example
{
   char  first_char;    /* byte 1                                  */
                        /* byte 2 is unused                        */
   short first_short;   /* byte 3 and byte 4                       */
   long  first_long;    /* byte 5, byte 6, byte 7, and byte 8 */
};
```

And its size will be 8 bytes. On a machine that allows alignment only on 4-byte boundaries the following storage will be in effect:

```
struct example
{
   char  first_char;      /* byte 1                                */
                          /* bytes 2, 3, and 4 are unused          */
   short first_short;     /* byte 5 and byte 6                     */
                          /* bytes 7 and 8 are unused              */
   long  first_long;      /* bytes 9, 10, 11 and 12                */
};
```

And its size will be 12 bytes.

The problem with this comes when a program makes an assumption about the size of the structure. There is a construct "sizeof()" that will return the size of a structure but not all programs use it. Even if they do you can still get into buffer size problems if a structure gets copied into a buffer and the buffer is large enough to hold the structure on some machines but not on others.

Structure size and alignment also lead to the same problems with access by different storage class mechanisms (ie. character pointers) and representation on disk that the byte order differences lead to.

We looked at some examples of the size of a structure containing a character plus an integer of different types :

```
sizeof( struct { char c; short si; } )
```


~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

```
sizeof( struct { char c; long  li; } )
```

```
sizeof(char+short)=4  sizeof(char+long)=6  : PDP-11  AT(XENIX) SUN-3
sizeof(char+short)=4  sizeof(char+long)=8  : 386  ASH  CONVEX  SUN-4
sizeof(char+short)=16 sizeof(char+long)=16 : CRAY
```

SIGN EXTENSION

In UNIX values can be signed or unsigned. If a value is signed its Most Significant Bit is used as a sign bit. For example an unsigned character can range in values from 0 to 255, while a signed character can range in values from -128 to +127. The same also applies to short (16-bit) and long (32-bit) values.

Some machines will extend the sign bit, propagating it to the left, when a smaller storage class variable is assigned to a larger one (ex. long = short), and others will not. In UNIX this happens more often than you might think. Every time a subroutine is called its calling arguments are pushed on the stack as integers (whose size varies according to the word size of the machine).

The problem arises when comparisons are made between values. If I have a short (16-bits) with a hex 0085 stored in it and a character (8 bits) with a hex 85 stored in it and compare them on a machine that does not sign extend they will be equal. However on a machine that does sign extend they will not be equal because the 85 stored in the character will be converted to a hex FF85 for the comparison. To get around this problem some programs will logically "and" the character value with hex FF. Unfortunately this works on some machines but not on others (the SUN 3 will sign extend the result of the logical and the PDP 11 won't).

The only real way to get around this problem is to use unsigned storage classes when dealing with data that may have the MSB turned on. Most programs have some kind of sign extension non-portability built in to them.

Variations which were found are :

❒ *We looked at whether typecast of small data types to larger types resulted in a sign extend*

```
sign extend all cases : PDP-11  AT(XENIX)  SCO386  SUN-3-4  CONVEX
sign extend short to long but not char to any : ASH(3b15/3b20)  CRAY
```

❒ *We looked at whether an arithmetic right shift sign extends*

```
sign extend short and long       : PDP-11  AT(XENIX)  SCO386  SUN-3-4
sign extend only short, not long : ASH(3b15/3b20)  CRAY
no sign extend on right shift    : CONVEX
```

(no machine sign extends an unsigned quantity)
(PDP doesn't allow for unsigned long, and restricted experiments)
(CRAY converts short->int before shift, so sign extending it first)

FLOATING POINT FORMAT

The format used for internal representation of floating point numbers can vary from machine to machine. This can cause the disk file data transfer problems mentioned above and can also cause loss of precision problems to floating point programs.

CONCLUSION

It is probably impossible to give rules which will guarantee a portable program without restricting the

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

flexibility which a language like C allows you. Some hints which might help are:

(a) prefer to use long/short rather than int, and if the object is not a signed integer quantity the type should probably be unsigned.

(b) always use sizeof() to discover the size of an object

(c) make all your output and input data ASCII readable rather than binary

(d) avoid using multiple representations of the same data, e.g., use of unions and certain means of type-casting.

We note first that some of these hints are trade-offs between portability and efficiency. We also note that the 'lint' program will highlight many potential portability problems. The best way to learn the problems is probably to take some small program you have written and port it to as many machines as you can find. You will avoid many of the pitfalls with your next program.

We note that no two of the machines investigated were identical. The program supplied as an appendix will run differently on each of the eight machines investigated.

APPENDIX

```
char *whatmc()

{
      /*  test one data  */
      union { char clist[8]; short si; long li;} mix;
      /*  test two data  */
      char c=0xff; short si=0xffff; long li=0xffffffff;
      /*  test three data  */
      struct { char c; long li; } combine;

     { int i; for(i=0; i<8; i++) mix.clist[i]='0'+i; }



     /*  Test one, picks out a CRAY and PDP-11  */
     if ((mix.si&0xff)==0x37) return "cray";
     if (mix.li==0x31303332) return "pdp-11";

     /*  Test one, splits the rest into two groups  */
     if (mix.li==0x30313233)
     {

       int i=c; /*  Either SUN or ASH or CONVEX  */
       if (i == 0xff) return "ash";
       if (li>>1 == 0xeffffffff) return "convex";
       if (sizeof(combine)==6) return "sun-3";
       return "sun-4";
     }
     else
     {
        /* Either an AT or a 386 machine running SCO XENIX  */ if
        (sizeof(int)==sizeof(short)) return "at";
        return "386";
     }

     /*  Never gets here  */ }

/* end of whatmc()  */
```


~~FOR OFFFICIAL USE ONLY~~

DOCID: 4010025

COMPUTER & INFORMATION SCIENCES INSTITUTE

Special Interest Group on

DATA FUSION

If you use or write software that uses data from multiple sources to track, identify, or evaluate TARGETS, you are doing DATA FUSION and may benefit from exchanging ideas and software with others.

MEETINGS in EARLY 1990

all held in 9A135, HQS, 0930-1030

Wednesday 24 January

Wednesday 28 February

Friday 23 March

Wednesday 18 April

CLEARANCE LEVEL: Top Secret Codeword
ALL PERSONS WITH GREEN OR GOLD BADGES ARE WELCOME

For more information on the [redacted] Special Interest Group, please call:

[redacted] P13, 963-5868
[redacted] A2, 963-3493
[redacted] A6/T4, 963-4743
[redacted] W46, 963-4702

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

COGITATIONS *of a* CONTUMACIOUS CABALIST

P.L. 86-36

[redacted]

W21

~~(C)~~ Someday it will be recognized as a fundamental truth of DDO that each group deserves the analysts it gets. Conversely, someday it will be admitted that no analyst deserves the group to which he or she is assigned.

~~(C)~~ As a veteran observer of the machinations among DDO organizations, I delight in belonging to a veritable cabal. Throughout the centuries cabals have been seen as covens for witches and warlocks, and as secret organizations from whence no good ever came. That label--CABAL--is not unlike the cloak of mystery which surrounds those who dwell in the heart of W Group.

[redacted]

~~(C)~~ Even to dare pronounce the phrase "W Group" in the same breath as "job" or "position" is not for the faint of heart. For the well-bred sons of DDO (the Groups of A, B, and G) cannot abide the ne'er-do-well son W. In fact several A and G pundits are quite sure that W was not born of the same father at all. They firmly believe that W is an imposter at best, and illegitimate at worst.

~~(C)~~ How can W, the wayward son, compete? To be sure, there is a small linguistic conclave fighting for freedom and the American way as part of W1. But that is a small, elite force. Most of W is not made up of linguists but of engineers, signals analysts, computer scientists and mathematicians (with a few odd intelligence research analysts thrown in to make the concoction odder still).

~~(C)~~ With such an eclectic band of workers, it is no wonder that most people wonder at W group! Try telling the linguist that you study what we affectionately call "green worms." That alone sparks off titters and cat calls. For who hasn't wondered at how the worm gets into the finest tequilla bottles. No sense in telling the linguist it is not that kind of nematode, for as they are wont to say: "worms is worms." No, the plight of the W grouper is worse still because few recognize that ELINT doesn't lie. That is to say, ELINT won't tell you he or she has turned over a new life and resolved to be on the side of truth, justice, and the American way, while still doubling the defense budget. Nay! ELINT just appears out of the sky and bites you when you least expect it. Rather like death, it shows no discrimination.

~~(C)~~ The problem with ELINT is that so few people understand it, which is why we ELINTers are so sorely misunderstood. ELINT is not a class unto itself. It is merely another side of that vixen, SIGINT. Although ELINT is not that scourge known as "voice," it does have melifluous tones and modulations. You might even say it can sing, as it often chirps! It can even illuminate the darkest of hours. As such ELINT is just another chapter in the life of the nefarious vixen, SIGINT. □

P.L. 86-36

DOCID: 4010025

P.L. 86-36

Letters

To the Editor:

This is regarding the derogatory and linguistically meaningless comment in [redacted] article on Xhosa (CRYPTOLOG, 3rd Issue 1988) to the effect that Afrikaans is a "bastardized version of 16th century Dutch" (sic):

Afrikaans, as all languages, evolved and developed organically, incorporating numerous lexical and syntactic features of the languages with which it came into contact during its formative period. Afrikaans is, in fact, the only modern European-based language which evolved on non-European soil, adopting many non-Indo-European vocabulary and grammatical features — including those from the Bantu and Khoisan language families, as well as from Portuguese and English. Its beginnings indeed go back to the 16th century, and it was nearly fully developed (with the exception of a standardized orthography) by the early to mid 1700's.

As all languages develop from antecedents, is it accurate to describe English as "bastardized" Danish and Norman French? Italian and "bastardized" Latin? Yiddish as "bastardized" German? Xhosa as a "bastardized" Bantu dialect mixing Hottentot and other non-Bantu elements?

In an article with some linguistic pretensions, I recommend that a modicum of attention be paid to proper linguistic terminology and accuracy, and that the writer's personal prejudices, however keenly felt, be tempered by some knowledge of prevailing linguistic theory in the interest of providing the reader with accurate information.

[redacted] *G0533,*

Former member, German PQE Committee, former Chairman, Afrikaans PQE Committee, present member, Dutch PQE Committee

---

The author replies:

I would like to express my appreciation to [redacted] for his keen interest in my article on Xhosa

(CRYPTOLOG, 3rd Issue 1988, pp 14-15). I found his comments on the derivation of the Afrikaans language very useful in expanding on one of the points I had made. I do regret, however, that my reference to Afrikaans as a "bastardized version of 16th-century Dutch" triggered such an emotional response. I would like to assure Mr. Day that this comment was not meant to be perjorative. In this particular technical context, the word does not have a derogatory meaning as he states, but is merely descriptive, denoting the rapid simplification of Dutch in its new environment. (NB: Bastardize = to reduce from a higher to a lower state or condition.) In fact, the word is frequently used by scholars to classify Afrikaans and the linguistic process Dutch underwent as it evolved into the language we know today.

[redacted] passionate defense of Afrikaans clearly reflects a love of languages, which I share. I would like to thank him for providing me with the opportunity to comment on this subject.

[redacted] *PhD., G94*

CRYPTOLOG

welcomes your letters and comments

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

DOCID: 4010025

~~SECRET SPOKE~~

- Meaning of two "Q" signals:

  + QST = you change to _____

  + QZY = I will change to _____

- Four digit groups:

  + first digit indicates callsign table used (1 or 2)

  + second digit indicates column receiving callsign is taken from referenced table

  + third digit indicates column transmitting callsign is taken from referenced table

  + forth digit indicates frequency from frequency table (only one table used)

  + example - 1/472

  1 = callsign table 1

  4 = receiving callsign

  7 = transmitting callsign

  2 = frequency

  1/472 = QEY DE CVQ 4700Kcs

Callsign tables:

Table-1

1	2	3	4	5	6	7	8	9	0
Z	B	S	Q	U	A	C	J	X	D
R	T	W	E	G	L	V	M	F	K
I	N	O	Y	H	P	Q	E	Z	R

Table-2

1	2	3	4	5	6	7	8	9	0
F	B	K	O	G	D	N	J	P	S
M	L	R	A	H	U	X	Q	W	M
E	T	Z	V	P	Y	O	C	I	G

Frequency table:

1	4450Kcs
2	4700Kcs
3	4825Kcs
4	4900Kcs
5	4975Kcs
6	5600Kcs
7	5775Kcs
8	5900Kcs
9	6150Kcs
0	6300Kcs

~~SECRET SPOKE~~

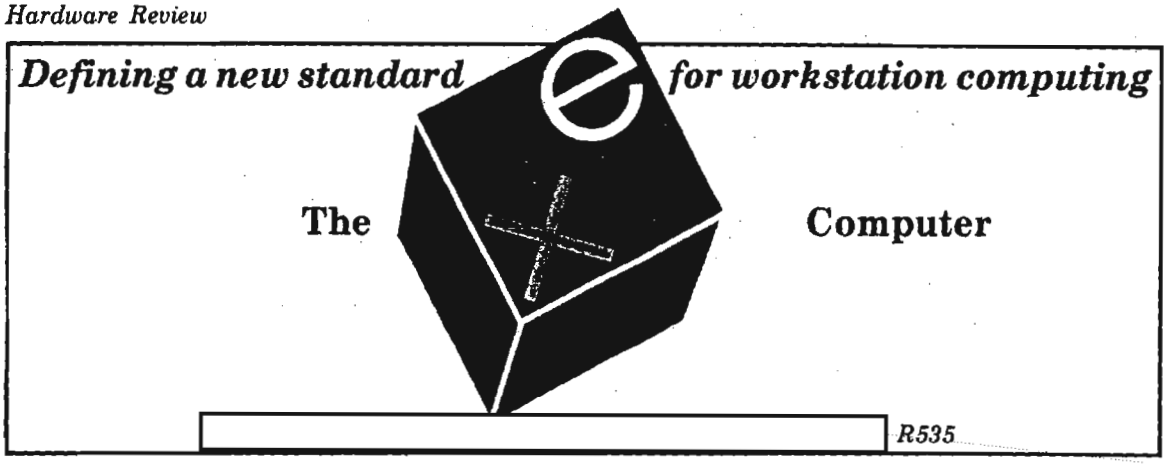
Reconstructed Signal Plan

Answers to TA Exercise on page 33

~~SECRET SPOKE~~

DOCID: 4010025

Hardware Review



P.L. 86-36

The NeXT Computer is the product of Steve Job's endeavors since leaving Apple Computer. It was designed after interviews with numerous universities and research organizations on what their needs and desires were for workstation computing. Initially it was to be offered only to educational institutions; arrangements have since been made to market it commercially through Businessland Computers.

The computer embodies new and diverse technologies which have the potential to define a new standard for high performance, low-cost, interactive workstation computing. In sum, it appears to offers a refreshing alternative to many workstation solutions which seem to stress only computational performance.

This paper discusses the important features of the NeXT Computer and will attempt to assess the impact of this technology on Agency applications. It will present the important hardware features that were designed into the architecture and how they could be exploited; it will the describe robust and dynamic software environment which appears at first glance to be superior to others currently on the market today; and finally, it will speculate on the significance of this technology for NSA computing architecture.

HARDWARE

At first glance, the NeXT Computer looks just like any other UNIX-based technical workstation. It consists of a 25 Mhz. Motorola 68030 CPU with a Motorola 68882 floating point unit, an Ethernet interface with TCP/IP and Network File System (NFS), 4-6 Megabytes of RAM memory, 32-bit NuBus system bus with 4 slots, a high resolution (1120x832), 17", 2-bit deep monochrome display, SCSI peripheral interface, 5.25 winchester disk, and keyboard with mechanical mouse. Though there are many vendors who sell systems with the same basic components, they do not offer the additional hardware features that the NeXT machine provides. These features allow for significant functionality not typically included by competitors in standard units.

MAGNETO-OPTICAL DISK DRIVE

The NeXT Computer incorporates a magneto-optical disk drive which provides a removable optical disk with up to 256 megabytes of data. This is the first instance of optical technology incorporated into the base platform of workstations. The drive is slow by comparison to winchester disk technology, 96-ms average seek time as compared to 18-ms average times for 5.25 winchester drives, but the increased capacity on a random access removable medium is very impressive. The complete operating system, very rich with bundled software is available on one optical disk. The disks are rather expensive, about $50.00 per disk, but that will probably decline as the device becomes more popular.

INTEGRATED AUDIO

It provides for high quality audio input and playback, with a built-in microphone jack that accepts a high impedance microphone signal. The microphone jack is connected to an analog-to-digital converter known as the CODEC. The CODEC converter produces 8-bit mulaw-encoded samples at a sample rate of 8 kHz. CODEC

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

input is roughly equivalent to telephone quality speech and is suitable for a number of sound applications such as voice mail where limiting the size of sound objects is important.

The CODEC mu-law encoding is used to save storage space required for storing sound. The mu-law encoding allows a 12-bit dynamic range to be stored in only 8-bits. The 8-bit mu-law encoded sample will yield the same amplitude resolution as a linear 12-bit sample.

The NeXT Computer also integrates a Digital Signal Processor (20 MHz Motorola DSP56001) to process high-quality stereo sound. Its primary function is to minimize system overhead while processing sound, but it can also be programmed to process any type of digital data including signal filtering or image data. The DSP can record and play back up to 44.1 kHz samples per second in both the left and right channels with 16-bit quantization. The DSP can also process 24-bit image data and is able to perform multiple arithmetic functions on data within one instruction cycle of the DSP. Applications which require real-time data capture, such as voice input, can be effectively addressed with this processor.

The types of sound format currently supported under version 0.9 of the operating system are:

16-bit Linear, mono or stereo, 22.5 kHz or 44.1 kHz
16-bit linear, mono 8 kHz
8-bit mu-law, mono 8 kHz
8-bit linear, mono 22.5 kHz
DSP load image

For sound playback, the system contains a speaker built into the NeXT monitor with left and right channel line-out jacks on the back of the monitor. Sounds are sent to both the built-in speaker and to the stereo jacks during playback.

VLSI I/O PROCESSORS

The custom VLSI processors handles I/O between the different system components. NeXT studied workstation architectures and discovered that one significant limitation was in data throughput. In most workstations the CPU is interrupted to perform I/O operations on the system bus, including network transfer and storage medium interactions. In I/O-bound applications this becomes a serious performance problem which vendors usually address by higher bandwidth busses, faster CPU clock cycles and somewhat faster I/O controllers.

While incremental gains are made it still can be a bottleneck, especially when considering signal or image processing applications. NeXT decided that a major emphasis would be to significantly improve sustained system throughput. To accomplish this within the defined architecture required two special I/O processors whose function was to offload as much I/O from the CPU as possible. These two custom VLSI chips manage the SCSI interface, the optical disk drive (including error-correction logic), the serial ports and the Ethernet transfers.

To make efficient use of these components required custom DMA hardware between the CPU board and the I/O processors. There are currently 12 DMA channels on the CPU board to facilitate I/O throughput between devices and processors. To attain designed performance rates required enhancing the RAM memory to CPU data transfer rates. The NeXT computer can perform these transfers in burst mode, twice as fast as other Motorola CPU-based systems.

ERGONOMIC FEATURES

NeXT was very conscious about the system size and ergonomic features. The system consists of a 1-foot cube, a 17" monitor and a keyboard with a mechanical mouse. The system has one power plug which takes standard 110-120V power and is sufficient to supply the complete system. There is one 10 ft. cable from the system cube to the monitor and one cable from the monitor to the keyboard. The cube to monitor cable provides power, the video signal and audio signals for speaker output and microphone input. The limited number of cables makes for quick and easy installation. The keyboard has keys to control power to the system, video display intensity (lighten and darken) and audio volume. This allows all system interaction to take place from the keyboard and for the remoting of the cube away from the desktop if that is desired.

The hardware components are very cleanly integrated into a compact yet expandable cube. Few systems available today offer the powerful

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

compute platform with the compact packaging that NeXT provides. The ultimate criterion will be the effectiveness of the software interface in developing applications which advantage of the unique hardware.

THE NeXT SOFTWARE ENVIRONMENT

The software environment provides an exciting first glance at the future for operating systems and the users' interaction with the system. NeXT has pushed the state of the industry by providing one of the first commercial offerings of the MACH operating system. It includes several important third party development tools and a user interface with development toolkits to assist in faster application development. The net effect is a dynamic, extensible, and robust environment which will appeal to both programmers and users.

We will discuss the software in three phases: the Mach operating system, the NextStep environment, and two of the application toolkits which are available for development.

THE MACH OPERATING SYSTEM

The Mach operating system was developed in 1986 at Carnegie Mellon University. It was originally intended as a multiprocessor operating system compatible with Berkeley 4.3 UNIX. It has received significant backing from DARPA (Defense Advanced Research Projects Agency), the major funding source for this effort. It also developed a mechanism for making extensions to UNIX without adding to the kernel. This allows for a smaller kernel base with system-specific functions executing outside the UNIX kernel. It also provides support for sharing memory between processes. This significantly improves performance when multiple processes are accessing large volumes of data. In traditional UNIX these processes would be copying data into each processs' memory space before accessing. In Mach the data is copied once into memory and copied again only when one of the processes attempts to modify it. It has been claimed that Mach outperforms UNIX by 15 to 25 percent because of these modifications.

NeXT adopted Mach for several reasons. First, Mach is based on Berkeley UNIX which is widely used in the academic and scientific research communities. This allows theNeXT Computer access to many existing applications and experienced personnel in these communities. Second, NeXT sought a smaller kernel, eliminating functionality that was not pertinent for their environment. They also preferred having the ability to extend the system without adding to the kernel, which Mach allows. Third, with the major emphasis on maximizing data throughput, the ability to share memory was extremely attractive. And finally, support for multiprocessing provides NeXT with the possibility of adding more processors to its cube (there are three unused bus slots) without having to rewrite the operating system.

Even though the emphasis is placed on Mach, the user's perception will still be that the operating system is UNIX. The many traditional methods for UNIX hackers to interact are provided, including the structure and access to the file system. When interacting with the operating system the commands behave as a Berkeley UNIX system, including the network support for remote operations. NeXT was able to take advantage of the work pioneered at Sun Microsystems with the Network File System and the Yellow Pages utilities to ease the integration into existing network environments.

NeXTStep USER ENVIRONMENT

NeXT believes that powerful user interfaces are critical for systems of the nineties. Its proprietary interface called NextStep uses Display Postscript from Adobe systems for all text and graphics written to the display. It embodies a proprietary window system NeWS, similar to the Apple Macintosh in interaction and behavior, which is currently not compatible with X-windows or any postscript-based window system.

There is a complete graphical interface to the operating system and application toolkits. Applications are invoked by double clicking with the mouse on displayed icons and window manipulation is performed with the mouse pointing to specific areas in the window. The window system supports "hiding" applications which transforms the process into an icon on the lower part of the display where it continues to execute. The application can be recalled by double clicking the icon.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

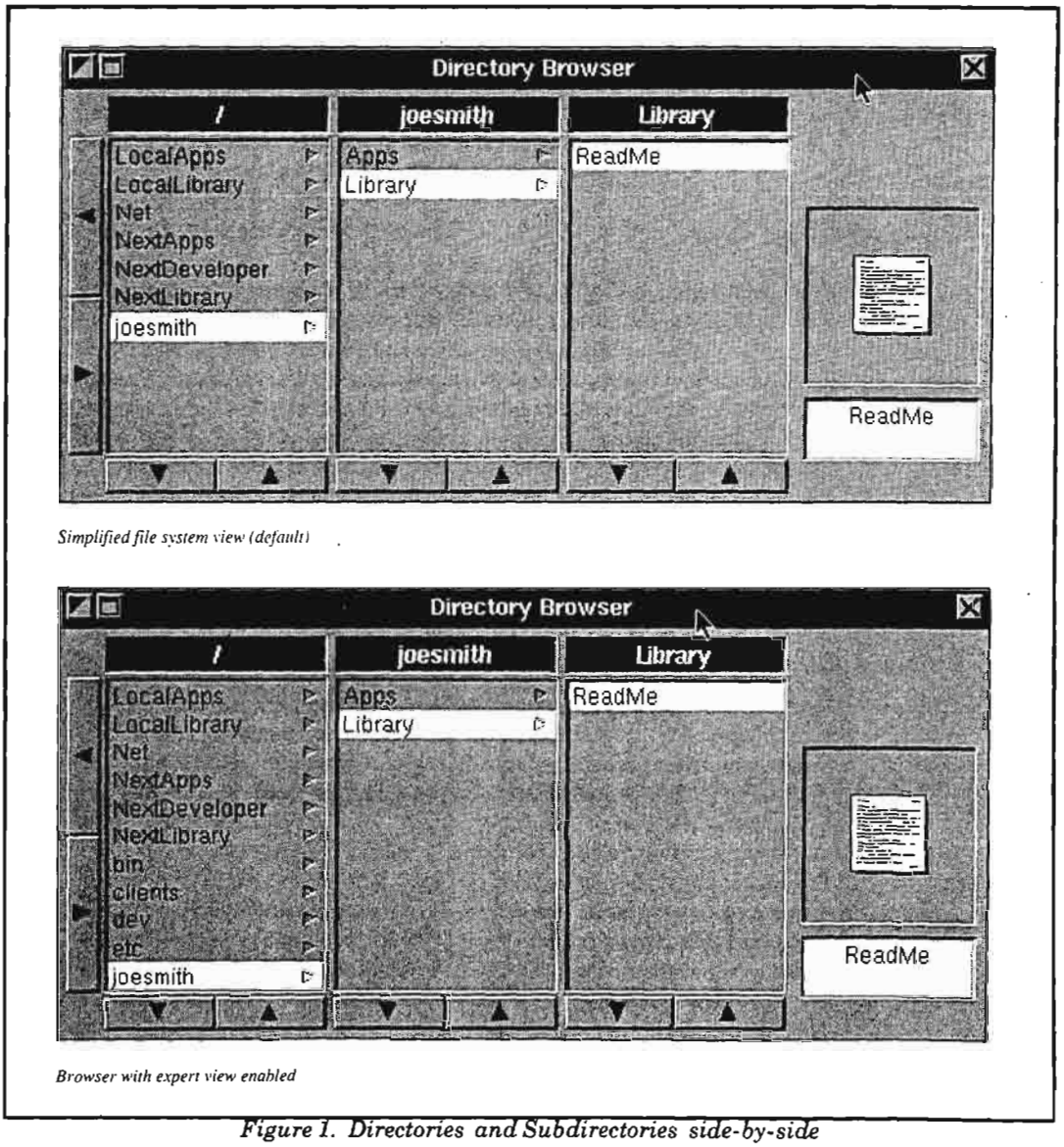


Figure 1. Directories and Subdirectories side-by-side

The NextStep environment also provides a directory browser which displays the contents of directories and subdirectories side-by-side, as shown in Figure 1. The user selects an item with the mouse; if it is a subdirectory its contents will be presented in the column to the right of the current column. A graphical icon depicting the selected item is also displayed in the area immediately to the right of the columns. A user can easily use this tool to navigate through directories looking for files.

Windows are manipulated from the border area along the top edge. There can be several different icons within the border depending on the type of window used. These icons allow for functions like window resizing, moving the entire window pane to a new area on the screen, or terminating the window. Although it is not intuitive for novice users to immediately understand how to manipulate windows, it is easy to learn and users very quickly become adept at window interaction.

The NextStep environment with release 0.9 can be customized by users using the preference tool. This tool allows for setting user preferences for such things as key repeat rates, mouse scaling, etc., through a graphical

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

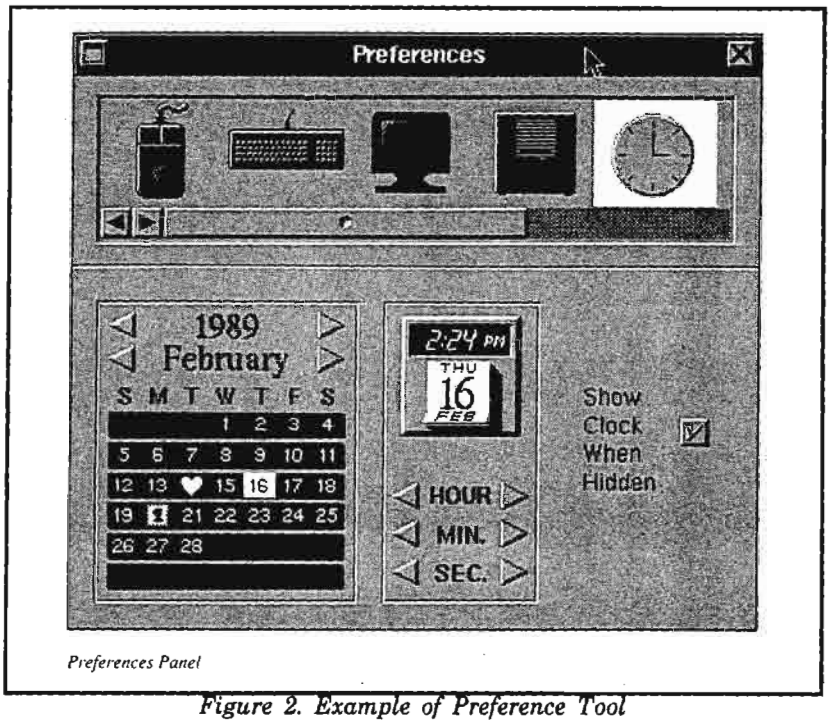


Figure 2. Example of Preference Tool

interface. Examples can be seen in Figures 2 and 3.

APPLICATION TOOLKITS

A major advantage of the NeXT software environment is the inclusion of toolkits to aid developers in building applications on the NeXT Computer. These toolkits consist of object-oriented function libraries which perform low-level object manipulation. Developers use these functions to define new objects required for the application.

This process takes advantage of the desirable features of object-oriented programming, namely extensibility and software reusability. NeXT provides an object-oriented language, Objective-C, as part of the standard environment to encourage development with object-oriented programming. Following are description of two toolkits provided.

Interface Builder

The Interface Builder on the Next machine offers a powerful easy-to-use tool for constructing user interfaces. It allows one to generate the visual component of a user interface without typing a single line of code, yet it does not limit the complexity of interfaces that can be built.

An interface designer builds the visual component of the user interface by picking a graphics object from a set of available objects, and then dragging it to the interface building workspace. Once an object is in the workspace, one can modify it in various ways. For example an object can be resized, moved, copied, cut, pasted, grouped or ungrouped with other objects. Grouped objects can all be set to the same size and can be moved together as a single block. Tools are provided for aligning objects in rows, columns or matrices.

The interface designer selects graphics objects for the interface either from a set of defined objects or by creating a new graphics object. A system for creating and adding new graphical objects is provided, although the method is neither defined nor documented well. Examples of available graphics objects are: buttons, slide bars, text areas, boxes, switches, fields, windows, and panels. A pop-up menu can also be included in a user interface.

The Interface Builder also allows one to associate a sound or an icon with most graphics objects. This can be done by dragging the

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

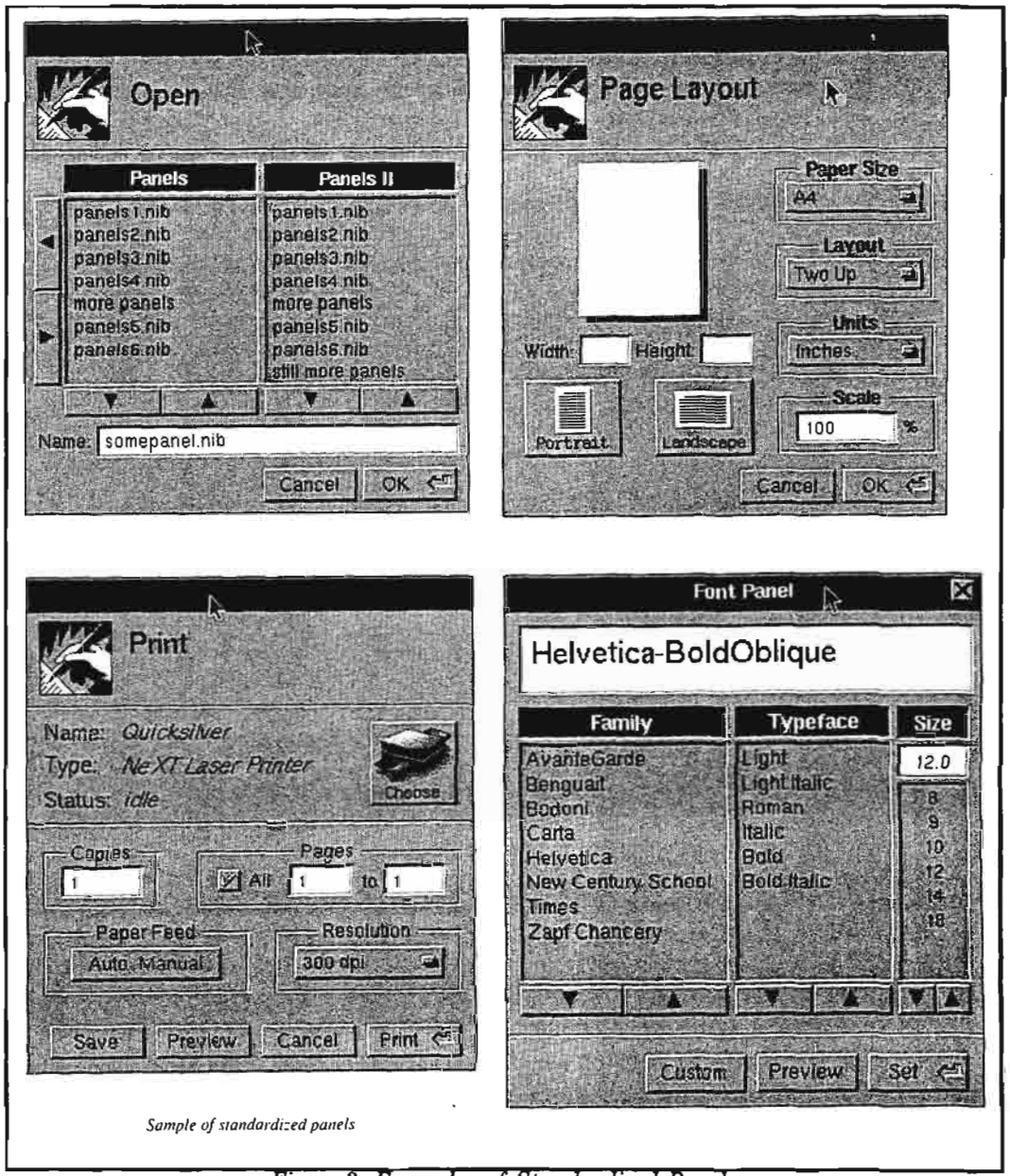


Figure 3. Examples of Standardized Panels

sound or icon object onto the top of the target object. The system comes with a set of predefined sounds and icons which can be customized.

Once an interface has been built, it can be easily tested without the associated application. This allows one to work on the user interface without worrying about the actual application. A programmer and an end user can work together on the user interface for a project. They can completely build and test an interface before formally designing and coding the application. A complex user interface can be built in about five to ten minutes.

Graphical tools are provided for connecting an interface to an application. A programmer specifies how the interface and application components are associated. Then the Interface Builder uses this information to generate header and Objective-C codefiles. These files may be manipulated as the application is debugged. This toolkit (as well as others) automatically generate UNIX "make" files to allow for easy compilation of the finished product. This is

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

extremely useful for developers as they maintain and rebuild software during the development process.

Sound Toolkit

The Sound Kit for analyzing and manipulating acoustical data consists of two Objective-C classes (Sound and SoundView) and a wide array of C functions to allow software developers to access the NeXT sound facilities with a minimum of effort. The Sound Kit software manages the details of OS communication, data access, and data buffering that are required during recording and playing sounds.

The Sound Kit provides the software developer with full access to the digitized samples of a sound object. Using the C functions provided, simple programs can be written to alter the pitch of a sound or change the playback speed of a sound. In addition, sounds can be played backwards, looped end-to-end, or divided into segments and reassembled in a different order. There are even software tools provided to digitally splice and mix together different sound objects.

The Sound class provides the facilities to create and manipulate sound objects. Sound objects are manipulated by sending messages to them. For example, the following lines of code are all that is necessary to create and record 5 seconds of sound:

```
/*  Create  a  new  sound  */
    id  mysound  =  [Sound  new];
    /*  Record  a  sound  */
    [mysound  record];
    /*  wait  5  seconds  */
    sleep(5);
    /*  Stop  recording  */
    [mysound  stop];
```

There are routines to record and play back a sound, as well as to read and write sound files. Facilities are also available for basic editing operations, such as deleting a portion of a sound or inserting part of one sound into another.

The SoundView class is provided to display sound objects in a predefined Soundview window. (Soundview windows can be built using the Interface Builder). Using the SoundView class, sound objects can be displayed as continuous waveforms, such as you would see on an oscilloscope, or as an outline of its maximum and minimum amplitudes. There are also methods provided for scrolling and zooming in and out of a displayed sound object, and selecting portions of a sound with the mouse.

Other Toolkits

Those are just two examples of the powerful toolkits which are available to developers with the NeXT Computer. Others provided are the text search toolkit which allows large bodies of text to be keyword indexed, searched or scanned for pattern matches; the Music Kit which allows for the generation and manipulation of synthesized music: the Application Kit to aid in object-oriented software development; and database management software (Sybase) which provides the tools to build and access relational databases.

CONCLUSIONS

The NeXT Computer has the potential to make significant advances in workstation computing within the Agency. It offers the most sophisticated integration of hardware and the most advanced software environments, all of which are included in the delivered system, in the smallest, cleanest packaging available today. Many of the important tools will be available on final operating system completion. Version 1.0 is expected about mid-summer.

How do we assess this technology? The general feeling of the programmers in R535 who have used the NeXT Computer is very positive. There is an extensive library of robust applications. We believe that rebuilding the prototypes developed on Suns and Apollos would be easier to do and functionally richer because we would begin building the application at a higher level. But to take advantage of these functionally rich libraries probably requires that applications be developed in Objective-C. This may be a problem for those without experience programming with object-oriented languages, though it is easy to learn in the NeXt step environment. A second potential problem might be performance-related if the application is not designed with object-oriented principles. The NeXT software environment continues to evolve, and with that evolution comes changes to the system. Applications being developed with the current 0.9 software release will not be object-code compatible with software release 1.0.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

Software releases after 1.0 are supposed to be object-code compatible with applications developed at the 1.0 release. Developers should be aware of that if developing at 0.9.

R535 believes the NeXT Computer is appropriate for many types of applications at the Agency. It clearly competes with Apollo and Sun workstations for applications that do not require color displays. The tools for managing and searching large volumes of text, powerful database support and graphical tools for analysis make it appropriate for most analytic and reporting functions. The DSP processor and audio capabilities with the processing power available make it ideal for signals processing and transcription operations. The numerous tools for the software developer, including automatic generation of "make" files, make it appropriate for software development and maintenance. The unique capabilities it offers allows for innovative concepts and ideas to be explored from the research perspective. For these reasons, the real usefulness of the NeXT Computer has yet to be discovered. Interest in the Agency is growing. In the near future we will have a much better idea of how effective these machines can be within the Agency computing architecture.

REFERENCES

Denning, Peter J. and Karen A Frenkel, "A Conversation with Steve Jobs", *Communications of the ACM*, April 1989, Volume 32, No. 4.

Fisher, Sharon, "Mach, The New UNIX?", *UNIXWORLD*, March 1989, vol. VI, No. 3.

Thompson, Tom and Nick Baran, "The NeXT Computer", *BYTE*, November 1988, Vol. 13, No. 12.

NeXT 0.9/1.0 Release Description, April 1989.

BULLETIN BOARD

WISE NATIONAL CONFERENCE

The Interagency Committee for Women in Science and Engineering will hold its ninth annual National Training Conference Monday through Thursday, 26-29 March 1990 at the Westpark Hotel, Rosslyn, Virginia. This is an excellent opportunity to meet mathematicians, scientists and engineers in other government agencies, to network with them, and to gain some perspective. A highlight of the conference is an exhibit of science projects developed by 9th and 10th grade female students for science fairs held at their schools. These students represent the future. NSA women should encourage them to pursue careers in math, science, and engineering by taking the time to view their projects and yes, even, recruiting!

Concurrent workshops will be held Monday through Wednesday and a science tour is scheduled for Thursday morning. Cost for the full conference, which includes three luncheons and an evening reception, is $275. One-day fee is $135, and two-day fee is $150; both include all events of the day.

P.L. 86-36

For further information please call or write [redacted] Federal Women's Program Manager, D8, OPS 2B, 963-1103, or your local FWP representative.

FREE LISP MACHINE

P16 is offering a free LISP machine, available for the taking. This is a classic LMI Lambda system. The package consists of one processor, two terminals, a 6250 tape drive, software, documentation, and a support contract.

The machine can be viewed in the P1 machine room, accessed through 2N001 or 2N018. For information call Steve, 963-1103.

WRITING AND EDITING

CRYPTOLOG receives many brochures about conferences, seminars, and courses on writing and editing. The topics include manuals, online documentation, presenting science to the public, newsletters, slide and vuegraph presentations, proposals, procedures, pamphlets and brochures, proofreading, layout, interactive instruction, handbooks, multimedia presentations, and so on. They are available for consultation, as are the textbooks, references, handbooks, and conference proceedings in CRYPTOLOG's library.

The materials may be consulted in 2N018. For an appointment call the Editor, [redacted] 963-1103.

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

Review

Structure and Interpretation of Computer Programs

P.L. 86-36

Reviewed by: [redacted] *P16*

If anyone wishes to reexamine his preconceptions about the programming language LISP, I highly recommend the course *Structure and Interpretation of Computer Programs.* During 4-16 June I attended this course in Harpers Ferry, West Virginia. It featured videotaped lectures by MIT Professors Harold Abelson and Gerald Sussman on a variety of advanced programming techniques such as data-directed, object-oriented, stream-based, and logic programming. The lectures were complemented with lab work. Other issues covered during the course included the orders of growth for algorithms, contrasting models for the evaluation of procedures, procedural and data abstraction, the vanishing line between programs and data, and the inherent limitations of software engineering.

Structure and Interpretation of Computer Programs is a five-credit course at MIT required for all computer science and electrical engineering majors. It is based on an outstanding textbook of the same name written by Abelson and Sussman. It is significant that the MIT faculty selected LISP to illustrate many of the computer science concepts it considers essential for further study.

The National Cryptologic School offers this course both in an intensive two-week live-in format and in regularly scheduled daytime classes spread over an entire semester. I believe that instruction of this material in either configuration should be given highest priority because our computer scientists should be as forward looking as those at a leading technology-based university.

LISP AND SCHEME

LISP is bound to be a vital part of the future of computing. At the same time it is as old and resilient as FORTRAN. A testament to LISP's dynamism and continued importance is that Steven Jobs considered it worthwhile to bundle LISP with the system software of the NeXT Machine. Although *Structure and Interpretation of Computer Programs* is not a course in LISP, but in programming techniques, familiarization with LISP is a positive by-product of the course.

If employees' comfort level with LISP could be increased, this would enable us to adopt the latest research advances, particularly in the area of natural language processing, in which LISP plays a leading role, without worrying about lacking adequate support personnel. Since LISP is available on a multitude of platforms, including SUNs and PCs, the excessive maintenance cost of some specialized LISP machines is irrelevant.

Abelson and Sussman praised LISP (or the dialect SCHEME) as an ideal language for designing special-purpose languages appropriate to the task at hand. An example of this was that in the section on logic programming SCHEME was used to approximate PROLOG. They called this capability meta-linguistic abstraction. While LISP per se may not be well suited for any particular task, it provides the

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

building blocks necessary to design higher-level languages optimized for a given task.

SCHEME, which is distributed by Texas Instruments, is described by the vendor as "a simple, modern LISP." It is also inexpensive and small enough to run on the PC. In the laboratory we used IBM-compatible laptop computers from Zenith. SCHEME is also available on the SUN and Macintosh.

One of the advantages of SCHEME over other dialects of LISP is that it enables the programmer to pass procedures as first-class objects to other procedures. This means that a procedure name can appear without any special syntax anywhere in another procedure to which this procedure name has been passed and still be applied properly. This is an elegant addition to the lambda notation--found in every version of LISP--which makes it possible for procedures to create and return other procedures. It also exemplifies SCHEME's simple design.

Key Concepts

A key concept in the course was the abstraction of procedures and data. Procedural abstraction is the notion that a procedure is just a name for a piece of code that performs some specific task. How this is done is intentionally concealed from the rest of a program so that higher level procedures invoking this procedure do not need to be concerned with the implementation details. There is an abstraction barrier between the code's implementation and its use. Data abstraction is analogous to procedural abstraction. It is defined as "a methodology that enables us to isolate how a compound data object is used from the details of how it is constructed from more primitive data objects." (Abelson and Sussman, p. 74) Data constructors and selectors are used to keep the issues of data format and use separate. When data come in different formats they carry a label describing their format. Such data are called typed data.

Data abstraction provided a departure point for a discussion of data-directed programming. Data-directed programming is used to manipulate typed data with generic operators. Data-directed programs work with "a two-dimensional table that contains the possible operators on one axis and the possible types on the other axis." (Abelson and Sussman, p. 137) The body of the table contains the code corresponding to each pair of operator and type. Since this table guides the generic operator to the appropriate code, the format of the data is transparent to the user.

Abelson and Sussman illustrated data-directed programming by designing a program to perform arithmetic operations on complex numbers that were alternatively stored according to the polar or rectangular coordinate systems. The complex number package was one component of a large system for symbolic mathematics, including symbolic differentiation, that was examined in detail during the course. The symbolic mathematics system gave concrete expression to a multitude of concepts besides data-directed programming. For example, it was shown that recursion made it possible for the coefficients of polynomials to be themselves polynomials or complex numbers without disturbing the generic operators for manipulating mathematical expressions.

Object-oriented programming is ideal for modeling situations that can be described by a collection of objects that can be called upon to perform various actions. This is done by passing messages to the objects requesting that they perform such actions. The code for performing the actions is contained in the objects themselves, thereby erasing the line between procedures and data. Objects also contain local state variables that describe their condition at a given moment. This raises another issue: "how a computational object can change and yet maintain its identity." (Abelson and Sussman, p. 168)

Much as signal processing focuses on signal flow, so does stream-based programming or stream processing focus on data flow. A stream is a theoretically infinite "sequence of data objects." (Abelson and Sussman, p. 242) Stream processing gives us an alternative to conventional algorithms, which concentrate "on the order of events in a computation, rather than on the flow of data." (Abelson and Sussman, p. 245) From the perspective of stream processing, many computations can be reduced to a series of processes, specifically enumeration, filtering, mapping, and accumulation. Most programs combine these processes blindly, thus obscuring "the commonality that underlies many typical computations." (Abelson and Sussman, p. 243) By using this approach, the programmer can reduce significantly the amount of code needed

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

for a set of problems and make the necessary code much more understandable.

Abelson and Sussman gave logic programming and PROLOG mixed reviews. They believe that declarative programming (where the programmer describes *what* he wants done, not *how* he wants it done) is an important paradigm, but that implementations of logic programming such as PROLOG have several defects. Some of the defects are restrictions on the placement of *not* clauses, infinite loops, and the closed world assumption that a program is aware of all information relevant to a query. The two professors held that *not* clauses were only useful as a filter to screen the possible answers already generated by the preceding clauses in a logical rule. They could not be placed in the first position among a series of clauses because they would not generate answers themselves and consequently would ensure that the rule would never return a positive response. The professors also maintained that a commutative rule (e.g., if X is married to Y then Y is married to X) combined with a fact to trigger the rule (e.g., Minnie is married to Mickey) would cause an endless loop.

Several reservations should be stated about this critique of PROLOG. Some believe that MIT is biased against PROLOG because it wasn't developed there, although LISP was. The infinite loops were confirmable in a commercial version of PROLOG, but they were not confirmed in a PROLOG-based knowledge engineering tool. The same tool provided a flag for the user to select either an open or closed world assumption. The approximation of PROLOG in SCHEME was much slower than PROLOG itself and could not eliminate duplicate responses. Incidently, Abelson and Sussman acknowledged that some excellent compiler work had gone into the design of PROLOG. However, the approximation was good enough to prove the point about LISP's capacity for meta-linguistic abstraction.

Along with abstraction barriers and programming paradigms, another theme was models for the evaluation of functions. Initially, the substitution model sufficed because there was no need to introduce an assignment operator into the language before the discussion of object-oriented programming with its requirement for local state variables, and thus assignment. The substitution model can be summarized by this rule: "to apply a compound procedure to arguments, evaluate the body of the procedure with each formal parameter replaced by the corresponding argument." (Abelson and Sussman, p. 184)

Once an assignment operator had been introduced, though, the substitution model broke down and had to be replaced by the environment model of evaluation. According to the environment model, expressions are evaluated with respect to the bindings in a series of frames called an environment. In a hierarchy of frames, bindings are inherited at lower levels, but they can be reassigned there without affecting the bindings in higher level frames. This permits assignment and local state, with the accompanying complications.

Abelson and Sussman generated some controversy by criticizing software engineering for promoting inflexibility. They stated that the product of software engineering is an elaborate edifice that performs the assigned task but cannot be easily modified to perform other tasks. They also maintained that it is impossible for a program module to serve more than one purpose under the software engineering approach, although this would be highly efficient. Despite these criticisms, however, Abelson and Sussman implicitly endorsed top-down design--a key characteristic of software engineering--by decomposing problems and referring to as yet non-existent code as "wishful thinking."

REACTIONS TO THE COURSE

Reactions to the course among fellow students varied widely. There were three main criticisms:

- The prerequisites for the course should have stated that to be successful, one needed a strong foundation in LISP and mathematics at least through one semester of Calculus;
- The material was too much to cover in two weeks; and
- The course was unrelated to work responsibilities.

A crash tutorial in LISP was offered beforehand to students without a background in LISP, but I believe that those with strong backgrounds in LISP were at an advantage. There is some dispute about this, though, because some

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

students without any background in LISP ended up excelling, while others already proficient in LISP used their knowledge as a crutch to avoid learning the material as presented. In any event, the initial advantage eventually dissipated.

As for math, it certainly would be helpful to review or become familiar with the basics of differentiation, logarithms, and the conversions between the polar and rectangular coordinate systems beforehand since the professors relied on examples involving this level of math to illustrate many important principles. Whether calculus should be an absolute prerequisite is open to debate because arguably symbolic differentiation, for example, was only a means to explain a concept, not an end in itself.

That the material was too much to cover in two weeks is indisputable. By the second week, many of us displayed various forms of burn-out. I take exception, however, to the criticism that the course was unrelated to work responsibilities. Even if one does not program in LISP, many of the concepts and techniques presented in the course can be transferred to other languages and to a wide range of applications. But if these techniques are not being used at work, then that, along with an antagonism to LISP, is precisely what we should seek to change.

Endnotes

Abelson, Harold and Sussman, Gerald Jay, *Structure and Interpretation of Computer Programs*, MIT Press and McGraw Hill Book Company, 1985.

ESSAY CONTEST

closes COB 22 April 1990

START WRITING NOW! DON'T DELAY!

Money prizes go to the first, second, and third place winners.
Honorable mentions may also be awarded

RULES:

- The contest is open to Green and Orange badge holders.
- Essays must have language or linguistics as a major theme.
- Essays may be unclassified, or classified no higher than TSC; compartmented submissions cannot be accepted.
- While topics pertaining to language as it relates to culture, business, academic pursuits and other general themes are eligible, greater weight will be given to essays more closely pertaining to NSA applications.

Submit your entries to:

CLA Essay Contest
Attn: [redacted] A2405, Ops 2B, Room 2B5110.
963-3863

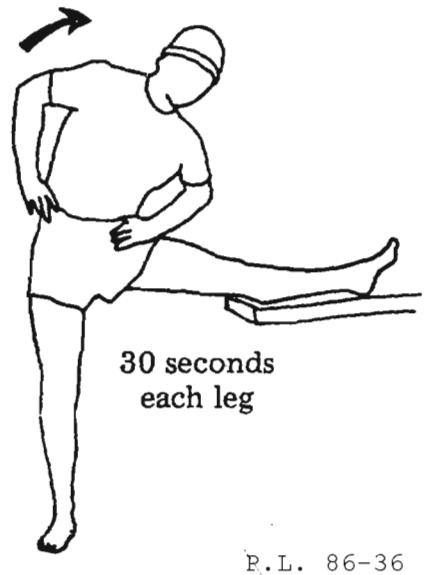
P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010025

TA EXERCISE:

RECONSTRUCT THE SIGNAL PLAN



~~(SC)~~ During the early 1960's, a Viet Cong (Vietnamese Communist) radio group operating in what was then the Eastern Nam Bo Region of South Vietnam, near the Cambodian border, used a signal plan that was different from other Vietnamese Communist (VC) communications in South Vietnam. The control authority was located close to the VC Central Office for South Vietnam and its outstations were located in the same general area. We could not make firm identifications of these entities, but we suspected that they may have represented logistic elements

~~(SC)~~ The group was active, or at least continuity was maintained, for about 18 months. During that period it did not undergo an overall communications change but random changes of call-ups and frequencies. Each time a change occurred one of two "Q" signals was sent followed by four digits; the first and second digits were always separated by a slash. Finally we recovered the system used to allocate the callsigns and frequencies.

(U) Shown below are examples of the "Q" signals and four-digit groups followed by the call-ups and the frequencies used after they were sent by control or outstations.

(U) See if you can recover the system.

~~(SC)~~ Control changes to call-up and frequencies listed below after sending QZY X/XXX:

```
QZY 1/472 QEY DE CVQ 4700Kcs
QZY 2/615 DUY DE FME 4975Kcs
QZY 1/747 ZRI DE QEY 5775Kcs
QZY 1/934 XFZ DE SWO 4900Kcs
QZY 2/128 FME DE BLT 5900Kcs
QZY 2/393 KRZ DE PWI 4825Kcs
QZY 1/281 BTN DE JME 4450Kcs
QZY 2/586 GHP DE JQC 5600Kcs
QZY 2/939 PWI DE KRZ 6150Kcs
QZY 2/240 BLT DE OAV 6300Kcs
QZY 1/352 SWO DE UGH 4700Kcs
```

~~(SC)~~ Control changes after receiving QST X/XXX:

```
QST 2/476 OAV DE NXO 5600Kcs
QST 1/561 UGH DE ALP 4450Kcs
QST 1/629 ALP DE BTN 6150Kcs
QST 2/757 DUY DE GHP 5775Kcs
QST 2/845 JQC DE OAV 4975Kcs
QST 1/128 ZRI DE BTN 5900Kcs
QST 1/373 SWO DE CVQ 4825Kcs
QST 1/842 ZRI DE QEY 4700Kcs
QST 2/963 PWI DE DUY 4825Kcs
QST 2/020 SMG DE BLT 6300Kcs
```

~~(SC)~~ Outstation changes after sending QZY X/XXX:

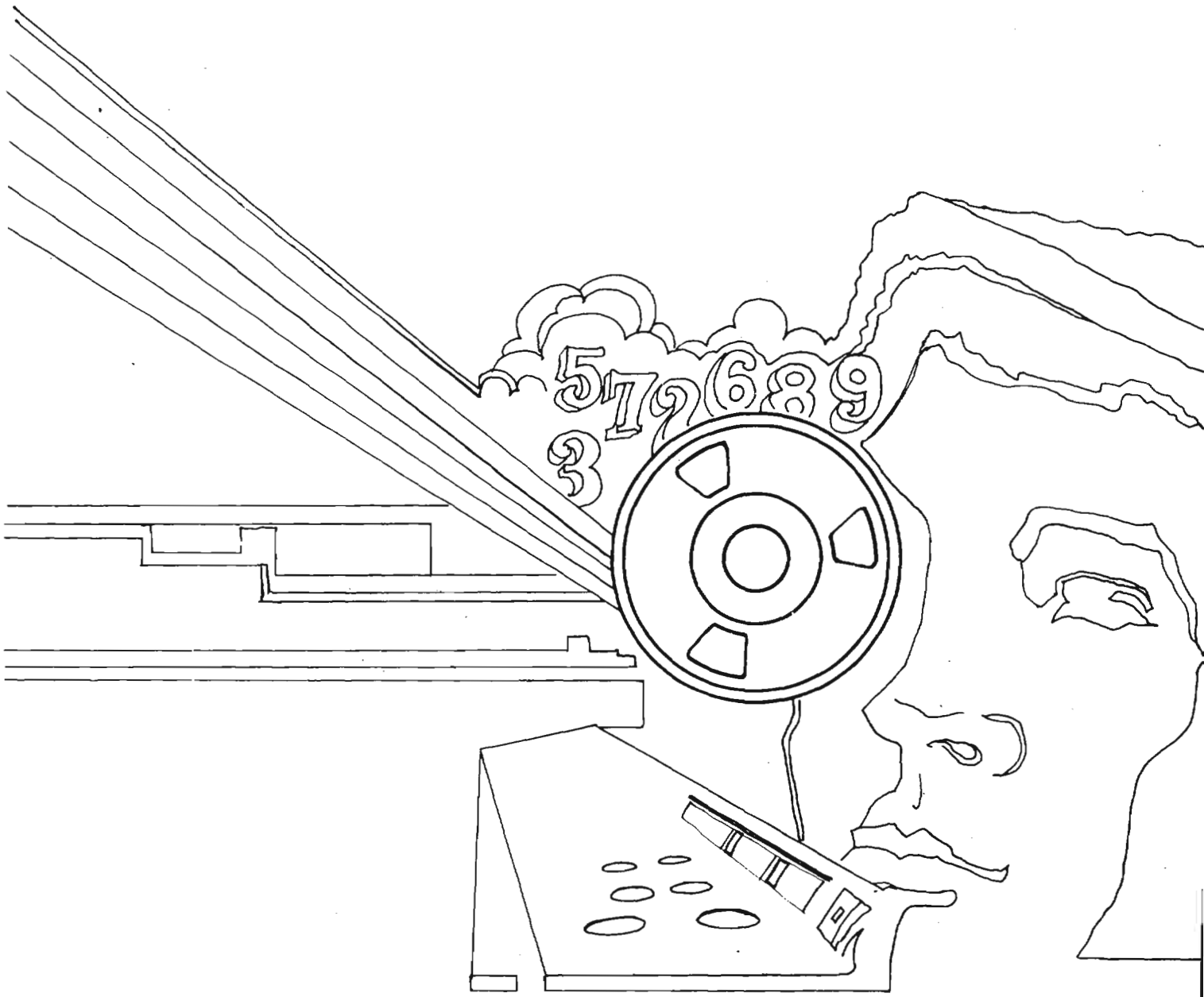
```
QZY 1/016 DKR DE ZRI 5600Kcs
QZY 2/602 DUY DE SMG 4700Kcs
QZY 1/157 ZRI DE UGH 5775Kcs
QZY 2/579 GHP DE NXO 6150Kcs
QZY 1/421 QEY DE BTN 4450Kcs
QZY 1/083 DKR DE JME 4825Kcs
QZY 2/458 OVA DE GHP 5900Kcs
QZY 2/970 PWI DE NXO 6300KCS
QZY 1/292 BTN DE XFZ 4700Kcs
QZY 2/746 NXO DE OAV 5600Kcs
QZY 1/324 SWO DE BTN 4900Kæcs
```

~~(SC)~~ Outstation changes after receiving QST X/XXX:

```
QST 2/370 KRZ DE NXO 6300Kcs
QST 1/014 DKR DE ZRI 4900Kcs
QST 2/605 DUY DE SMG 4975Kcs
QST 1/261 BTN DE ALP 4450Kcs
QST 2/486 OAV DE JQC 5600Kcs
QST 1/090 DKR DE XFZ 6300Kcs
QST 1/763 CVQ DE ALP 4825Kcs
QST 2/148 FME DE OAV 5900Kcs
QST 1/905 XFZ DE DKR 4975Kcs
QST 1/839 JME DE SWO 6150Kcs
QST 2/397 KRZ DE PWI 5775Kcs
```

The reconstructed signal plan appears on page 20.

~~SECRET~~



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~
~~NOT RELEASABLE TO CONTRACTORS~~

Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

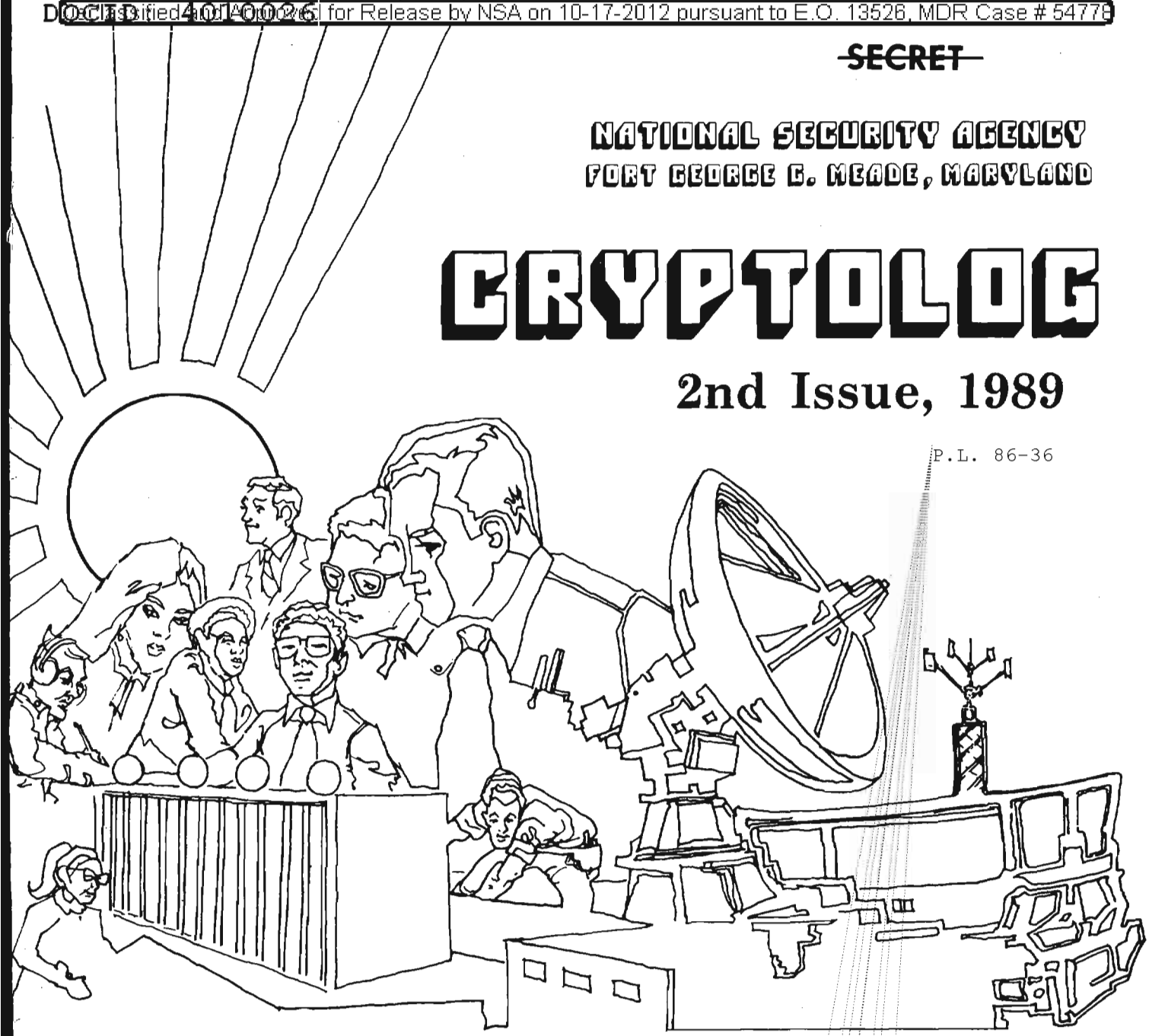
~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

2nd Issue, 1989

P.L. 86-36



IN HONOR OF WOMEN IN SCIENCE AND ENGINEERING.	Elizabeth Rindskopf	1
ABOUT CLASSIFICATION.		3
COMPUSEC POLICY FOR THE INTELLIGENCE COMMUNITY.		4
ACROSS THE POND		7
A NOTE TO CONTRIBUTORS.		10
THE EXCITEMENT OF INFOSEC		11
HOW TO BUILD A USER-SEDUCTIVE ARCHITECTURE.		13
GOLDEN OLDIE.		16
BELATED THANKS.		17
CAMBODIA IN PEACE AND WAR		19
BULLETIN BOARD.		28
HARDWARE REVIEW: OCR DEVICES.		29
FROM THE PAST		37
GETTING STARTED		38
LETTERS		39
ON THE LIGHTER SIDE		41

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

DOCID: 4010026

P.L. 86-36

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XVI, No. 2 ..... 2nd Issue 1989

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Cryptolinguistics ..... (963-4740)
Index ..... (963-4814)
Information Science ..... (963-3456)
Information Security ..... (972-2122)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (963-4958)
Special Research ..... Vera R. Filby (968-5043)
Traffic Analysis ..... Robert J. Hanyok (963-4351)

Illustrators ..... (963-6234)
..... (963-3738)
..... (963-6423)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, NORTH 2N018

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five)
(note: no 'o')

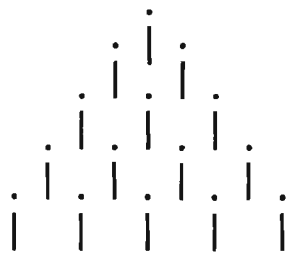
via ALLIANCE, send to:
PLBROWN [note: all caps]
attn: CRYPTOLOG

Always include your full name, organization,and secure phone; also building and room numbers.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, NORTH 2N018
Please do not phone.

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.



The first issue of CRYPTOLOG came out fifteen years ago. It was designed to be a monthly, "written by technicians for technicians, informal, newsy, controversial, lively, and timely." The budget crunch did away with the "monthly." But thanks to you, the reader-writers, the other attributes still apply.

"To be successful, CRYPTOLOG must reflect current operational topics in a way that interests you and others." So wrote General Wolff, the then DDO, in a letter of introduction to that first issue, August 1974. He went on to say, "I hope that you will want to read it and will help to write it."

We are repeating his words for the benefit of newcomers to CRYPTOLOG. You, the readers, are also the writers. The vitality of the publication is due to the animated exchanges of views among readers.

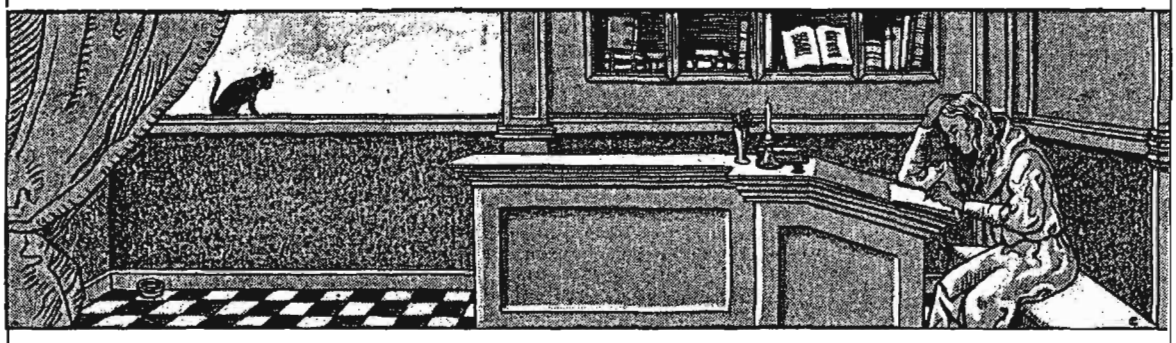
And now for two high-tech events to mark this anniversary. (We are state-of-the-art ourselves, as befits the high-tech sponsoring organization.) CRYPTOLOG can now receive contributions via ALLIANCE as well as over PLATFORM. Instructions appear elsewhere on this page. Also, beginning with this issue, we are moving over to desk-top publishing on the Macintosh as conversion software permits.

CRYPTOLOG
has moved to OPS-1, 2N018.
New Mailing address: P1 NORTH

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010026

In Honor of Women in Science and Engineering



Elizabeth Rindskopf, GC

This article is based on an address at a luncheon of the Federal Women's Program honoring NSA's women in science and engineering.

It is an honor to be asked to speak to you today but rather daunting too—I have read your bios and know the talent that I have before me. Indeed, such professional distinction and accomplishment — and in such great quantity—makes me wonder just what I might have to say today which could be directly relevant to you in your busy lives. In short, I asked myself, as I sat down to prepare these brief remarks, what message might I want to deliver this morning and what could I hope to accomplish in speaking to you.

The answer that came to me is simple and intensely personal. It may be that what I most want to say will have greater meaning for me than for you. And so I ask your indulgence and permission to express my own personal feelings on the meaning and importance of women in Science and Engineering today. For what I want to say today is first, thank you, and second, keep it up, and third, spread the word. Let me spend a minute telling you a little more about each of these messages.

Thank you. Some of you may recall an interesting program produced and directed by Peter Ustinov several years ago on the dangers and likely impact of a nuclear holocaust. It combined multiple interviews with those involved day-to-day in "manning" — and I use that word advisedly — our nuclear defense. Interspersed with these interviews was a dramatic portrayal of the impact of a nuclear attack on a small group of people—a mini "day after", if you will. In all of the many interviews not one woman appeared, never mind spoke. The only woman, in fact, was one actress in the dramatic inserts. I was struck by this total absence of women. Weren't we half of the population? Where were we when decisions about matters so central to the future of the nation— our civilization—were being made? Shouldn't we be involved with our unique feminine perspective? Of course we should.

Well, why weren't we there? Was Don Regan really right when he commented that women simply weren't interested in disarmament talks and related issues? No, I felt in my heart that that view was wrong.

The correct answer was a different one: Women as a group have traditionally lacked the technical training to be able to participate effectively in many of the technical discussions surrounding issues so critical to the nation's security, issues such as nuclear war, disarmament, and so on. And lacking technically informed voices, they have not been heard at all.

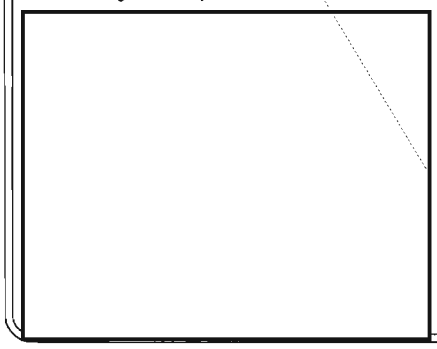
To my mind, this is not only wrong, it is wasteful and foolish as well. Wasteful because we need all the good minds we have to solve the problems that confront us as a nation and as an agency. Let's be frank. This Agency and this nation are on the brink of a serious shortage of mathematicians and technically trained people. To survive in the next century the nation must muster every bit of its technical and scientific strength. And that means

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010026

P.L. 86-36

NSA Women Honored for Contributions in the Fields of Science and Engineering, Women's History Month, March 1989



women must be a part of the solution; without them there may not be a solution. Foolish because I believe that women are in fact different than men—neither better, nor worse, but with an important and often unique perspective and wisdom all their own. We waste a precious asset when we organize ourselves to make important decisions without the presence feminine character and point of view. And, as a lawyer, I might also add that we undercut the very genius of our democracy—a system based on the strength in diversity and the healthy tension in the competition of different ideas, different strengths and different perspectives. In short, we need the participation of women in all avenues of public life. But they cannot participate unless they are properly prepared to do so. And so today I thank you for the hard work you have done to obtain the training that will allow you to excel in the technical leadership of this very high tech and very important agency.

And let me say a word about the group of women we are honoring today. Twenty-seven candidates were selected for nomination by their organizations. They were mathematicians, computer programmers, electronic engineers; some had doctorates; one taught mathematics at a school no less prestigious than the University of Texas. Others taught themselves what they needed to know right out of high school.

Yet despite this highly impressive array of educational credentials and superb work performance, all are—at least from my perspective —young , between the ages of 23 and 37, to be precise.

Their relative youth brings me to my second point: Keep it up. We need you now doing the creative work of the technical expert. We will need you tomorrow as part of the Agency's Senior Management team. And here I'll offer another personal perspective: Too many times I find myself one of a handful of women, if not the only woman, sitting around the table in the Director's Conference Room. I've formed a habit of taking a head count. 75 men to 1 woman is not an acceptable ratio for these meetings. It must and it will change, but only if you make it happen.

Let me not be guilty of suggesting that you will have an easy time as you grow and progress in your chosen field. I can guarantee that you won't. As pioneers, each of you will face special challenges: many of you will lack adequate role models and as a result you'll be required to spend the extra energy demanded of all those who serve as our trailblazers. I can tell you this with confidence because I've been there. Just remember that your task is in many respects to change an entire culture that fails to encourage and may actively discourage the woman scientist or mathematician. And many will have the added challenge of working two equally hard jobs: raising young families right at the point when your career is at its most competitive. For this you will require hard work, military discipline and, most importantly, a sense of humor. But keep at it; you can do it. Perhaps a phrase from my high school Latin course will help: POSSUNT PROPTER COGEUNT — They can because they think they can.

Before I leave this point, let me mention something you won't have to fight: NSA Management. I believe you have as supportive an environment as you are likely to find anywhere today. Does that mean I guarantee you won't ever face discrimination? No. But I believe you will have the management support you need to conquer the problems you confront. Keep at it: you won't regret it if you do, but we will if you don't.

Lastly, spread the word. We need more technically versed women here at NSA and nationally.

~~FOR OFFICIAL USE ONLY~~

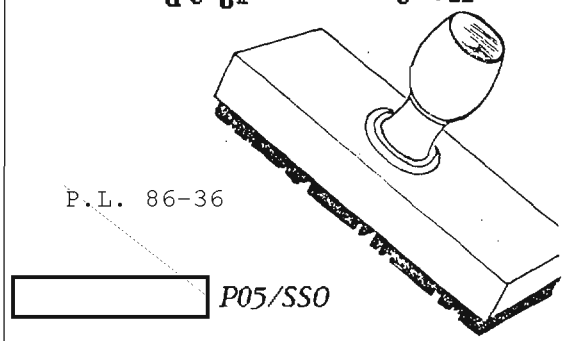
DOCID: 4010026

I hope you'll encourage other women in their pursuit of technical and scientific careers, both here at NSA and outside as well. And I hope you'll get involved, when you can, in serving as role models and teachers of girls and young women still in school. And the earlier they see your example, the better. They need you to see what a kind of career the technically trained women can have.

Some will need your help to tackle the persistent problem of math anxiety, and other difficulties particularly faced by girls and young women who pursue technical careers. I believe much remains to be done in learning why it is that our young women find themselves, considered as a group, less comfortable than their brothers in learning math and science. Do they learn the principles of math and the sciences differently than boys? Possibly. Are they often intimidated and discouraged when they confront technical subjects? Probably. Can you make a difference in attacking this problem? I believe you can. Your example inspires; it encourages and creates the self-confidence essential to any fine performance.

Seeing your pictures as I came in today reminded me of just how powerful an example you can set. Some months ago, I visited the college my daughter has selected. Some of you may know Wellesley and its long tradition of encouraging academic excellence in women. For me it was a new experience, but one I will long remember. As I walked into the library's main reading room, I looked up to the clerestory windows bathed in lovely fall sunlight. There, hung all around the room, were the elegant oil portraits of all the college's past presidents, and each and every one had the face of a woman. I realized then with a thrill of surprise that in all my time in various fine educational institutions, I had never before been a room where those so honored were exclusively women. The message was clear in those confident gazes. They could do it.

About Classification



It is widely recognized that the volume of classified material NSA handles is enormous. It is therefore incumbent upon us also to recognize the importance of proper classification practices and to ensure that our actions reflect the sound judgment required.

Individuals responsible for making classification decisions should remember that overclassification increases our vulnerability in two ways:

- It increases the volume of documents to be protected.
- It degrades our awareness of documents which truly merit TOP SECRET classification.

The classification decision process includes four steps:

- An initial decision to classify information based on whether it concerns military plans, weapons, activities, or intelligence operations that are classifiable;
- A decision concerning whether unauthorized disclosures of the information can cause damage to the national security;
- A decision as to whether the information should be classified

TOP SECRET - information the disclosure of which could cause exceptionally grave damage to the national security;

SECRET - information the disclosure of which could cause serious damage to the national security, or

CONFIDENTIAL - information the disclosure of which could cause damage to the national security.

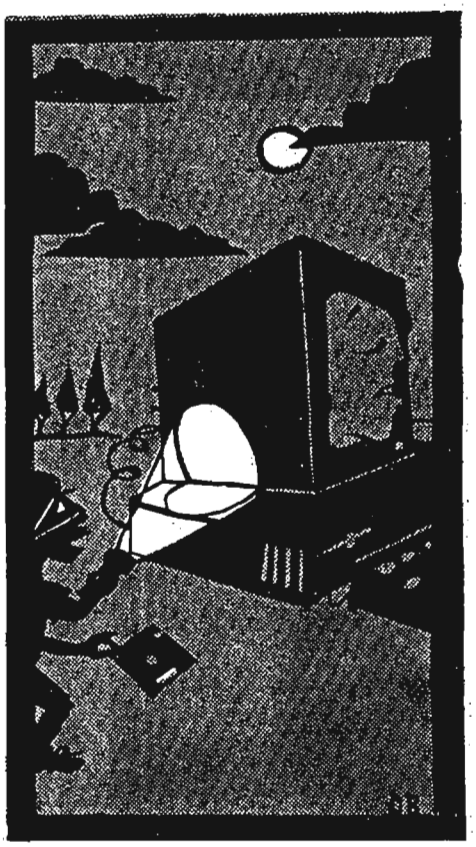
- A provision for an indefinite period of classification, unless an original classification authority establishes a date or event upon which automatic declassification should occur.

Note that classification decisions cannot be made merely to conceal violations of law, inefficiency, or administrative error; prevent embarrassment to a person, organization or agency; or to restrain competition.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010026

COMPUTER SECURITY POLICY FOR THE INTELLIGENCE COMMUNITY



P1

(U) This article summarizes the current national level policy on protecting intelligence processed in computer systems or networks. It also discusses a problem that has plagued system security officers, accreditors, and users for years; how to determine the mode of operation of a computer system in the NSA/CSS environment.

P.L. 86-36

BACKGROUND

(U) The Director of Central Intelligence (DCI) publishes security policy in the form of DCI Directives called DCIDs (pronounced D-skids). These cover all aspects of security, including personnel security, physical security, operations security, and computer security. DCID 1/16 "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks" covers computer security. Emphasis is placed on the *uniformity* of protection mechanisms, which becomes extremely important when we talk about interconnecting Automated Information Systems (AISs). Emphasis is also placed on the protection of *intelligence* processed in AISs and networks. Thus, this DCID applies not just to all classified information, not just to all sensitive information, but to all classified information that involves, or is derived from, intelligence sources or methods. The first DCID treating computer security as a separate topic was published in 1972. The DCID in effect before 19 July 1988 was dated 4 January 1983, but was substantially the same as the DCID published in 1972. Obviously, there have been a lot of changes in the computer security field since 1972, and the current version of the DCID reflects those changes.

GENERAL POLICY GUIDANCE

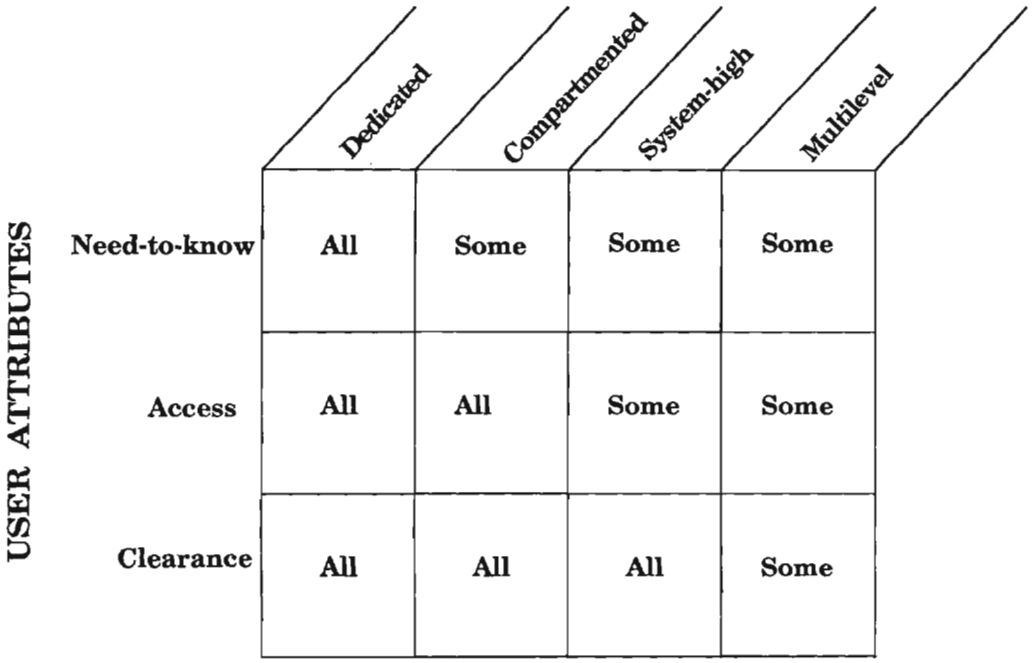
(U) The purpose of the directive is to establish long-term (year 2000) goals and near-term requirements (year 1992) intended to improve the security of U.S. intelligence processed in AISs and networks. The goal is for all Intelligence Community AISs to become trusted systems incorporating trusted products by the year 2000. In the period leading to the achievement of the foregoing goal, interim measures to improve security will be taken, including accrediting or reaccrediting systems, implementing minimum near-term security requirements, and improving access control and monitoring.

ACCREDITATION

~~(FOUO)~~ Each AIS and network covered by this policy must be accredited to operate in one of the four modes of operation: dedicated, system-high, compartmented, or multilevel. Accreditation requirements vary with the mode of operation. The minimum levels of trust (as specified by the DoD Trusted Computer System Evaluation Criteria, or "Orange Book") to be achieved as a goal by the year 2000 are: Dedicated Mode - C1; System-High Mode - C2; Compartmented Mode - B1; and Multilevel Mode - B2. Of course, a higher level of trust may be mandated for a particular

DOCID: 4010026

MODES OF OPERATION



AIS by its sponsor or responsible accrediting authority. The responsible accrediting authority for NSA/CSS is the NSA/CSS Senior Computer Security Coordinator (T03).

MODES OF OPERATION

(U) In DCID 1/16, the fundamental basis for deciding which protective mechanisms are appropriate for a given situation is a concept called mode of operation. There are four modes of operation used for AISs and networks processing intelligence: dedicated, system-high, compartmented, and multilevel. There are exactly two sets of information needed to determine the mode of operation of a system: (1) the classifications and categories of information on the system, and (2) the clearance level, formal access approvals, and need-to-know of all users of the system. These two sets of facts are the sole determinant of the mode of operation of a system.

~~(FOUO)~~ For purposes of this policy statement, categories of intelligence information include Sensitive Compartmented Information (SCI) and Special Access Programs for Intelligence (SAPIs). SCI includes either COMINT (sometimes referred to as Special Intelligence or SI), TALENT KEYHOLE, or BYEMAN information, or any combination thereof. Those programs that require, as a condition of access, the signing of a nondisclosure statement are considered to be SAPIs. Therefore, in NSA/CSS, programs in the Very Restricted Knowledge system (VRKs) and the GAMMA subcompartment are considered to be SAPIs and are given the status of SCI compartments and subcompartments in terms of the security levels required for their protection.

(U) For a system processing SCI, clearance is based on criteria contained in DCID 1/14, "Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information." In NSA/CSS that means a user must have either a green, gold, or black badge.

(U) The attached chart shows how user attributes (need-to know, formal access approval, and clearance level) for the information on the system determine the mode of operation of the system. These modes of operation are described in further detail below.

DOCID: 4010026

DEDICATED MODE

(U) When *all* users are cleared for *all* data on the system, and *all* users have formal access approvals for *all* data on the system, and *all* users have the need-to-know *all* data on the system, the system is operating in the *dedicated* mode of operation. The system is not required to provide *any* technical security at all. All the security for the system is based on traditional security disciplines, such as physical security, personnel security, communications security, and so forth.

SYSTEM-HIGH MODE

(U) When *all* users are cleared for *all* data on the system, and *all* users have formal access approvals for *all* data on the system, and *at least one user* has the need-to-know *only some* of the data on the system, the system is operating in the *system-high* mode of operation. The system is not required to provide much technical security, only a reasonable amount of user separation. Systems operating in the system-high mode are usually also trusted to provide some level of access control and accountability (i.e., logins and passwords) and, perhaps, some level of audit trails. Almost all the security for the system is based on traditional security disciplines.

COMPARTMENTED MODE

(U) When *all* users are cleared for *all* data on the system, and *at least one user* has formal access approvals for *only some* of the data on the system, the system is operating in the *compartmented* mode of operation. The system is required to provide some technical security over that needed for the system-high mode. Systems operating in the compartmented mode must provide a mandatory separation of users and data based on some sort of formal compartmentation and labeling. They must also provide a high level of access control and accountability (e.g., logins and passwords, biometrics, etc.), and a detailed and reliable level of audit trails. Even with this improved technical security, much of the security for the system is based on traditional security disciplines.

MULTILEVEL MODE

(U) When *at least one user* is cleared for *only some* of the data on the system, the system is operating in the *multilevel* mode of operation. The system is required to provide a high level of technical security; in addition to the technical security needed for the compartmented mode, systems operating in the multilevel mode must provide a mandatory separation of users and data based on classification and clearance. They must also provide an extremely high level of access control and accountability (e.g., logins and passwords, biometrics, etc.), and a detailed and reliable level of audit trails. Even with all this technical security, some of the security for the system is based on traditional security disciplines.

P.L. 86-36

ACCESS BY FOREIGN NATIONALS

[redacted]

CONCLUSION

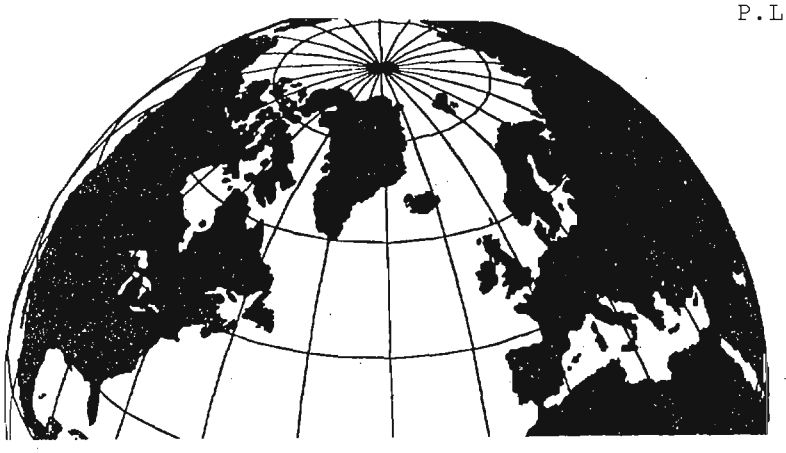
(U) If you have had experience working with previous policy statements on computer security, you will note that we have come a long way in defining the parameters and technical measures for protecting intelligence information. If this article has sparked your interest, I recommend that you obtain a copy of DCID 1/16 and its supplement, "Security Manual for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks", dated 19 July 1988.

DOCID: 4010026

ACROSS THE POND

[redacted] S331

P.L. 86-36



[redacted]

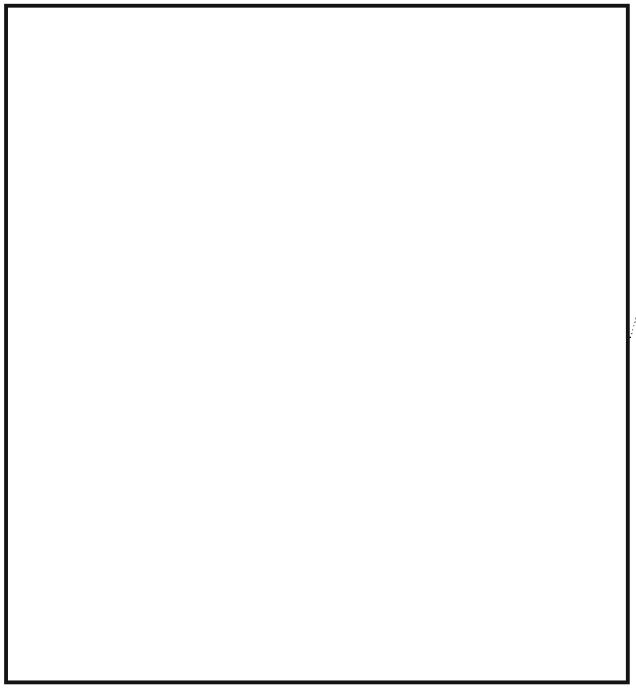
P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

DOCID: 4010026

P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

DOCID: 4010026

P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)



~~(FOUO)~~ In spite of some of those morale dampers, the workers I met were generally cheerful and dedicated to using their highly developed abilities to the fullest extent. Personally, I was treated very well by my British supervisors and co-workers and made many friends. I rarely met anyone who "tooted his own horn," and I discovered that a major attribute of "English reserve" is patience which does not allow hasty judgments but gives people a chance to prove themselves.

(U) Outside of work, I met many really friendly English people in Cheltenham, a heterogeneous town about 3 miles in diameter located almost 100 miles west of London in the county of Gloucestershire, in the South Midlands. I spent considerable time socializing with friends from work, church, the Royal Scottish Dance Society, and other organizations.

(U) I rented a 7-room house in Cheltenham with all the modern conveniences one needs, and which was located within walking distance of work and the town center. In town were an abundance of lovely shops with the latest fashions (especially reasonably priced woolens), parks and gardens (one with a boating lake), schools, churches, doctors and dentists, a choice of grocery stores and produce markets, bookstores, camera shops, sport shops, British Gas and the Midlands Electricity Board, banks and administrative offices, appliance centers, theaters, restaurants, antique shops, and anything a person needs, all within walking distance. Most shops close at 5:30 p.m. and most restaurants and theaters open at 7:00 p.m. Surrounding Cheltenham are the beautiful Cotswold hills, which provide an immediate retreat from the bustling, rather crowded business and residential areas.

(U) I traveled extensively throughout the country on coaches and in my Mini, in which I could drive on the narrowest of country roads and park in the smallest spaces in the cities. Armed with my AA (Automobile Association) membership, atlas, and tour books, and usually in the company of British friends, I thoroughly explored the Cotswold hills and Gloucestershire, home of the famous Gloucester Cathedral approximately 10 miles southwest of Cheltenham; visited London, Bath, Oxford, and Cambridge; and traveled to the Lake district in the northwest; Yorkshire in the northeast (where I stayed at Menwith Hill near Harrogate); Devon (including Torquay in "the English Riviera") and Cornwall in the southwest; Canterbury Cathedral, Windsor Castle, and Hastings in the southeast, and the Isle of Wight in the south.

(U) All over Great Britain, including Scotland and Wales, and also Southern Ireland and the Channel Islands, I saw everything from palaces and manor houses to tiny village pubs, rich in historical significance, nestled in magnificantly scenic countryside, a photographer's paradise. Although a few places, such as Stonehenge, now have fencing to protect them against vandalism, the countryside is kept very clean and neat by residents and travelers, as well as by organizations like National Trust and English Heritage. Also, much to my surprise and delight, travelers even encounter a fair amount of sunshine from time to time.

(U) A geographic and social feature of England of which I had not been previously aware was the contrast between the North and the South. The north of England is rugged and hilly with plenty of good low-priced housing, but a shortage of jobs, mostly in factories, which are closing down in large numbers. By contrast, the flatter, more urbanized south(east) has ever-increasing high-paying jobs, largely in new international computer firms, but only very high-priced houses and hardly anything like our apartments for people who would be just starting their careers or would be willing to move there from the north.

DOCID: 4010026

(U) Concerning prevalent English views of America, I noted that many people do indeed consider our country as being somewhat similar to theirs, but just more technologically advanced and less polished and less rich in cultural heritage. I noted also, however, that a surprising number, even the large number who like the Americans whom they have met, also strongly identify our country with the crime, aggressiveness, extreme wealth and wastefulness, neurosis, and superficiality that is seen in the very popular soaps like *Dallas* and *Dynasty*, police films, etc., which they receive from us. Although their news coverage is quite objective, some commentaries and documentaries, when seen in light of these one-sided films, are often misconstrued by the populace to the detriment of our country.

(U) Many people attribute several of England's recent social problems to U.S. influence. Some also act cool, at least initially, towards Americans, especially in the vicinity of Royal Air Force/U.S. military bases like Fairford, apparently because of their sometimes justified stereotype of Americans abroad. Nevertheless, I met even more people who were fascinated with everything American and wanted to visit America, or had already visited America and had a marvelous time. In my experience, the majority expressed admiration for the openness and friendliness of the Americans they had met. Others even changed their minds and decided to include a visit to America in future holiday plans.

(U) My tour in Cheltenham was, on the whole, very beneficial and enjoyable. Although it seemed to take a long time to adjust to the new surroundings and cultivate friendships, the results were well worth my efforts. I learned a great deal from the English people, not only in office matters, but also in human relations, and I discovered tremendous opportunities for travel. I highly recommend this tour of duty. □

NEW MAILING ADDRESS

CRYPTOLOG
P1
NORTH

A NOTE TO CONTRIBUTORS

Though CRYPTOLOG is an informal publication, it closely observes the etiquette of publishing. One of the provisions concerns anonymity. According to that rule, the Editor must know the source of the information but may not reveal the identity without permission; and without identification any submission is discarded, whatever its apparent worthiness. CRYPTOLOG has followed this rule many times over the years.

So, dear author, if you've sent a contribution without identifying yourself, you won't see it in print. Don't bother to scan issue after issue for your submission. You must make yourself known to the Editor. No exceptions. Submissions received without identification are tossed out.

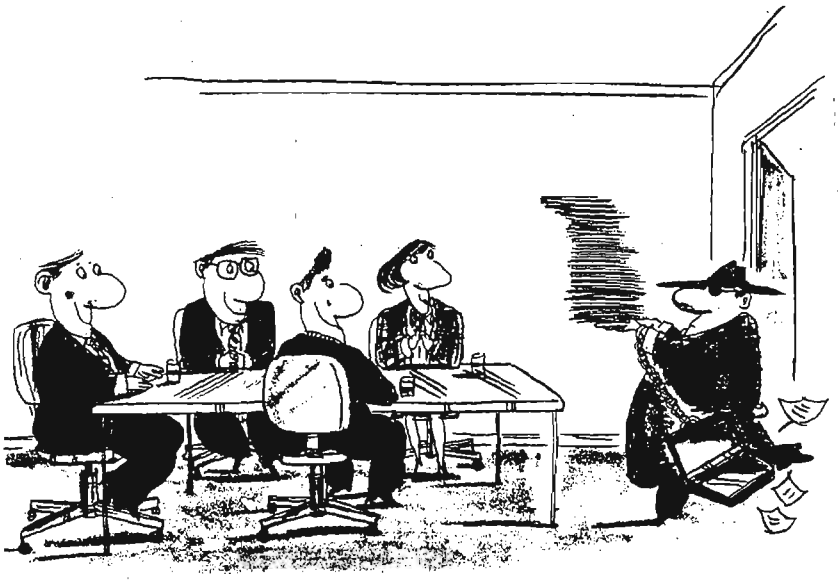
If you have already submitted something anonymously, resubmit it with your name, organization, building, and secure phone number—that is, if you want to see it in print.

And please include, along with the hard copy, a floppy with specifics about the computer used, the operating system, and the word processing software.

Unclassified

DOCID: 4010026

THE EXCITEMENT OF INFOSEC



[redacted] D2 P.L. 86-36

Some time ago, while I was having lunch with the Director of Security of one of our NATO allies and we were discussing the rash of books on intelligence agencies such as the CIA and Britain's MI-5 and MI-6 that were flooding bookstores, he asked, "Why aren't there more best selling books on INFOSEC?" I replied, "It's because the best days we have in INFOSEC are when nothing exciting happens in the outside world. When we are successful, which we are most of the time, the result is a non-event."

During the Walker spy trial, Earl Clark, an NSA INFOSEC expert, said, "Give me access to your codes, give me access to your ciphers, and you won't have any secrets." INFOSEC has all the secrets of US national security as well as the secrets of NATO and those of our allies around the world to protect. The responsibilities are awesome. On a good day for INFOSEC, the externals are placid, but make no mistake, the internals are boiling. That's the excitement of INFOSEC.

The internal story is unknown, and it must necessarily remain so to the outside world. It is possible, however, to give some appreciation of the scope of the INFOSEC task with respect to the various elements, each fascinating in its own right, which collectively must be integrated into the total security pattern which constitutes INFOSEC.

Consider the challenge to the cryptomathematician: Design a cryptoalgorithm to encrypt our most sensitive secrets, and having encrypted them, we will give the resulting text to our most mathematically and technically sophisticated opponents and let them subject it to their most high-tech attacks. It must protect the information for decades against such continuous attack. That's not all. It must do this under the assumption that the opponent has the algorithm but not the key.

To cryptoequipment engineers we say, "Embody the algorithm in an equipment that is fail-safe," and to the evaluator we say, "Analyze the algorithm and the cryptoequipment that contains it and give it a seal of approval." Impossible as it seems, it is a task that must be coped with successfully if we are to have the ability to securely command and control our forces and to protect our strategic interests.

There are many situations, particularly in tactical operations, where valuable information can be derived, not by breaking the encrypted transmissions but by analyzing the stereotypic formats, the quantitative message data, and other externals. The task of protecting against such exploitation is the domain of transmission security. This is an entirely different type of challenge, the searching for seeming minutiae that could actually be a bonanza to hostile intelligence services.

One aspect of this, or for some an INFOSEC category of its own, is providing secure sequences for ECCM transmissions that are secure against enemy analytical reconstruction.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010026

Hostile intelligence operations can concentrate on the attack mechanisms of their choosing. The job of INFOSEC is to protect against practical attacks. A technically pervasive phenomenon, a known physical fact of life, is that electronic and electro-mechanical equipment when processing information necessarily create emanations which can be detected if not protected against. TEMPEST is the field of INFOSEC devoted to the protection against unwanted, unintentional, compromising emanations. The technical challenge to determine how best to detect such emanations, to identify those that may be compromising, and then to devise corrective measures is complex. However, the real challenge is how to determine the cost-effective compromise. At what point have we made such an attack unprofitable? INFOSEC is always involved in optimization trade-offs, but it is a two-party game of exceedingly high stakes.

TEAPOT is a recently coined terms for another aspect of the compromising emanations problem. The difference between it and TEMPEST is that the emanations are hostily induced by "bugs" planted in the equipment. In the TEAPOT category is the widely publicized GUNMAN operation of the recent past, a rare case of our sharing the excitement with the outside world. In the GUNMAN operation we removed tons of equipment from our Moscow embassy and replaced it with clean equipment in one rapid move before the Soviets could react.

Physical security in INFOSEC includes the protection of the cryptomaterials: the codes, ciphers, cryptologics, keys, cryptoequipment. When you consider the high value the Soviets place on the acquisition of our cryptomaterial, coupled with the vast amount of codes, ciphers and keys in hard copy form around the world, you can appreciate the enormous size of the this task. If protection breaks down, security breaks down. That is why INFOSEC is a top priority target of the Soviet espionage apparatus.

Personnel security goes hand in glove with physical security since it is this route by which physical security is often attacked. There are no stricter security constraints and checks on any personnel in the U.S. Government than on those working at the heart of INFOSEC.

The rapid expansion of computers and the field of information processing has enormously complicated the qualitative and quantitative problem of protecting classified and sensitive information, and at an exponentially increasing rate. The previously discussed aspects of INFOSEC, as complex and challenging as they may be, have trend lines and data bases helpful in planning. If Communications Security, (COMSEC), is in a state of combustion, COMPUSEC is in a state of explosion. Harnessing an explosion can be almost too exciting. Again, it is a game, a deadly two party game with extraordinarily high stakes. It is vital to know the enemy capabilities if we are to be successful in countering them effectively. That is the field of threat analysis. Doctrine provides the procedural and regulatory sinew binding the INFOSEC capabilities into a coherent body. The production of literally mountains of codes, ciphers, keys, and other crypto-material with the utmost of security and accuracy is fundamentally important to an effective INFOSEC program. Each of these areas of INFOSEC is a story in itself.

P.L. 86-36

INFOSEC is not, of course, an end in itself. It is only useful when applied in communications and electronics systems. This opens another whole dimension to the scope of INFOSEC. It is absolutely essential for both systems security and for the effectiveness and efficiency of the systems into which it is integrated that the INFOSEC professionals not only fully understand the technology of those systems, but also the operations those systems are supporting. Thus, INFOSEC professionals are spread throughout the world in a wide variety of roles. Take one example: Imagine the situation where a satellite launch is on hold for some unidentified technical problem and your equipment is the only Government Furnished Equipment in the whole system. Now that's real excitement.

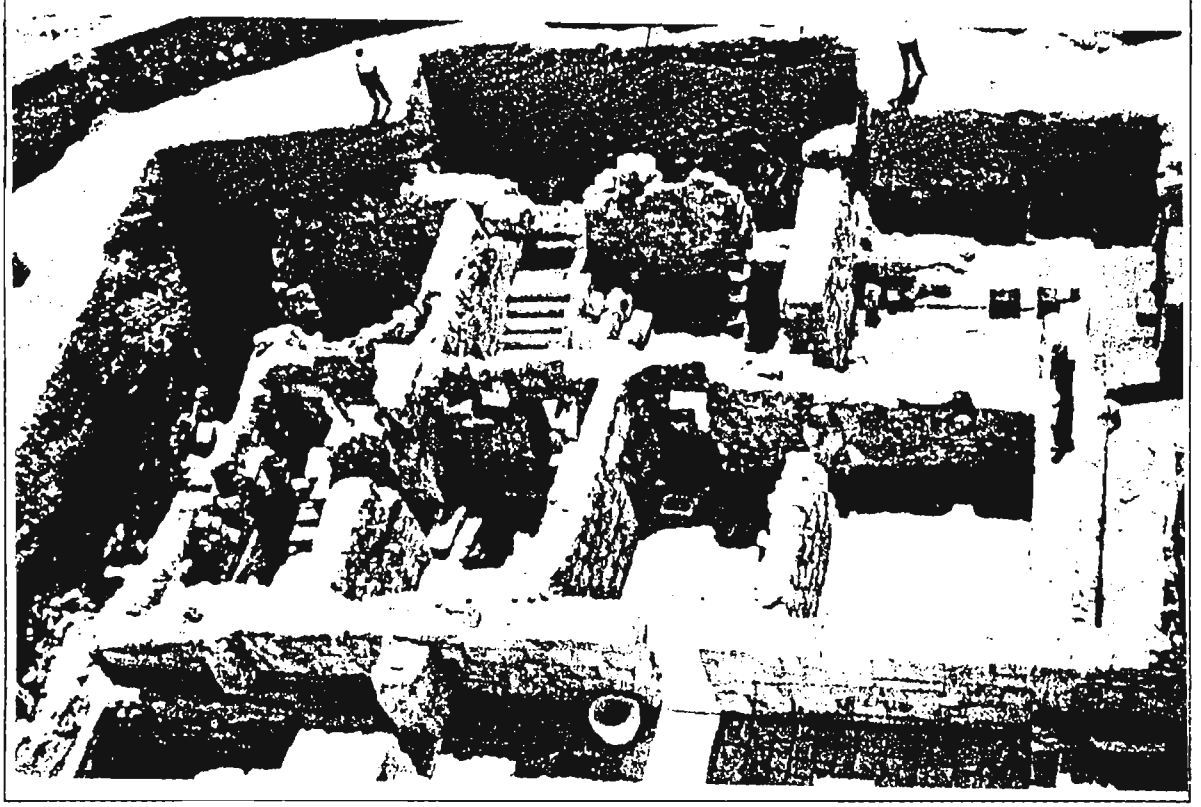
And now the final INFOSEC role, systems security evaluation. In accomplishing this task, all the above discussed areas and their complex interactions must considered. Coupled with this must be the consideration technology, the varied environments and the wide range of applications, and the ever-present hostile threat. This must be integrated, assessed, and a determination made to give the seal of approval to a system, "OK to pass our nation's most vital secrets in this system." The pressures on INFOSEC are great, the task seemingly impossible, and the external recognition and rewards necessarily almost nil. But balancing all that out is the EXCITEMENT OF INFOSEC.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010026

How to build a USER-SEDUCTIVE Architecture

[redacted] W45 P.L. 86-36



(U) By integrating off-the-shelf software, some standard Agency hardware, and programs already developed by the R Directorate, we developed the basis for the OPELINT Architecture that can be used at any level within the ELINT community. It has new ideas, capabilities, and opportunities in which analysts and programmers can be imaginative, creative, and explore new ideas and techniques. We incorporated into the Architecture some computer models that give program managers, decision makers, and analysts the capability to develop different collection and processing strategies, along with high quality computer simulations that give visual results of their decisions. The system is based on high quality graphics designed for easy use, with concealed text to explain only those areas where users might need more detailed information.

(U) We have been able to do this without a multimillion dollar budget and without having to purchase large mainframe computers or write massive programs or arrange large scale contracts.

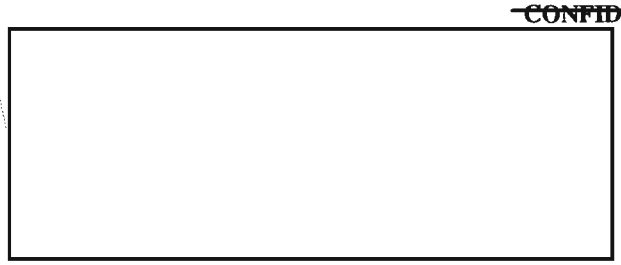
(U) The process seemed simple at the outset. All we had to do was gather information on all the collection and processing systems that provide operational ELINT, put it together, and print out a nice document (that would probably end up being cumbersome, out of date before the end of the week, and whose only useful function would be as a doorstop). As we were collecting information two things quickly became evident: (1) most information was hopelessly out of date (some as much as 6 years); and (2) the scope of the Architecture meant that we were inundated with information.

[redacted]

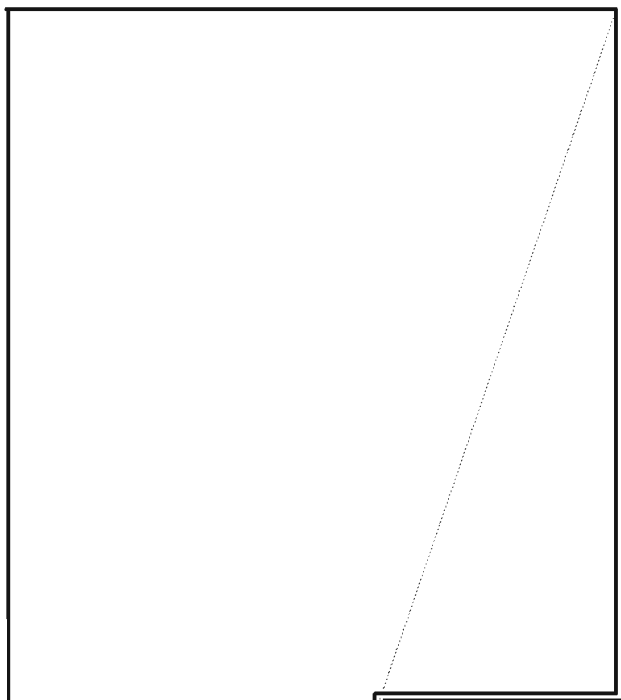
P.L. 86-36

DOCID: 4010026 P.L. 86-36

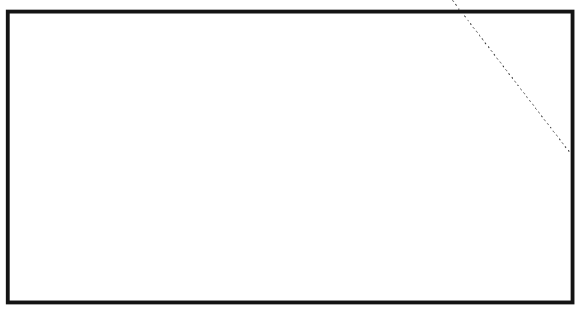
EO 1.4.(c)
P.L. 86-36



(U) Then W45 was faced with a conundrum: what Architecture do you use to create an Architecture?



We plan to develop a system whereby the user can provide information directly to the data base and, after review and formatting, updating will be automatic. This will give the users the opportunity to be involved in the development and maintenance of the overall system.



(U) We can anticipate shortfalls by comparing current requirements with new target trends. We then help planners and programmers make smart decisions about eliminating the shortfall. Their decisions then become a new plan that is factored back into the original equation either as a new capability or as a future plan.

~~(C)~~ The primary purpose of an operational ELINT Architecture is to provide a baseline from which decision makers can make those smart choices.

(U) Once we determined what we would include in the Architecture, we had to decide on what form we would use to present it. This became a key issue because the Architecture will be used worldwide—at different levels of command and by people making decisions on various types of ELINT systems. The mass of information collected to date indicated that the finished product would be several large volumes of printed material. Since the ELINT community is a vast network of commands and organizations, writing, printing, and distributing hardcopy documentation would be a major effort, similar to publishing a full-length book. Instead, we decided to place the Architecture online and provide access through various means; printed versions of the documentation would be limited to a master copy and several hardcopies for the archives.

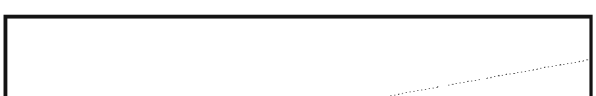
architecture

1. The art of designing and erecting buildings. 2. A structure of structures collectively. 3. A style style and method of deign and construction. **4. Any design or orderly arrangement perceived by man.**

The American Heritage Dictionary of the English Language

(U) A useful by-product of the baseline Architectures has been the creation of an ELINT Glossary. As we culled information for the baselines, we published ELINT terminology and acronyms in a hardcopy document. We are now looking for a way to make an interactive glossary for our online version of the Architecture.

(U) Once the objective A.rchitectures are developed, we must update them whenever there is a change.

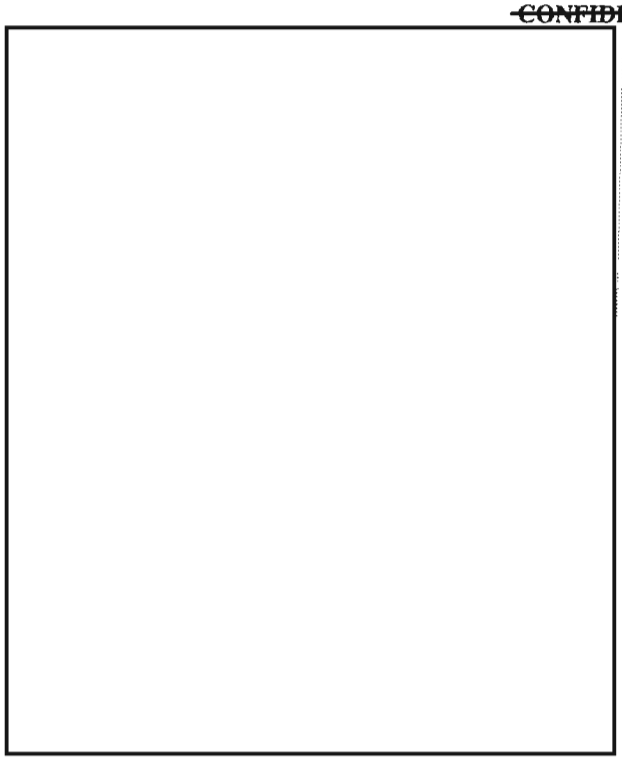


EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4010026

EO 1.4.(c)
P.L. 86-36



(U) The process seemed simple enough to us, and we planned also to develop a floppy-diskette version that for tactical units in the field.

(U) Our real problems began when it was pointed out that while our idea was good, there were problems with printing in hard copy the diagrams and charts essential to the understanding of ELINT: flow charts, organizational diagrams, mission tracks, and even hardware configurations. Once again the hunt began for off-the-shelf software. Instead of incorporating diagrams with the Architecture, we are now developing a graphics-based program that allows the users to call up concealed or suppressed textual explanations of each graphic. In addition, we are developing a program that will allow the users to capture a series of graphics and assemble them in any order they wish for briefings and presentations.

(U) All of this software currently operates on an IBM or IBM-compatible AT with an enhanced graphics capability. In the next phase, when we have found an imaginative programmer to do it, we will convert the Architecture to run on the Agency's high-performance workstation.

~~(C)~~ Our development of an OPELINT Architecture does not end with the establishment of a baseline. We now must find ways to make it compatible with existing Architectures, develop a program to add an interactive glossary, develop computer models, and look at ways to use the Architecture to help planners and decision-makers better understand ELINT.

~~(C)~~ To provide guidance in the areas of computer modeling, interactive glossary development, and database establishmen,t W45 purchased the services of a special engineering technical assistance contractor. The contractor may be able to use or adapt some computer models already on hand or under development by R08 and R3, thus reducing costs, saving time, and assuring compatability with other programs.

~~(C)~~ The final area in which we want to concentrate is presentation. Once the ELINT baseline is finished and modeling is under development, we need to organize the information to prepare briefings, write new plans, and help document new programs. For this purpose we are purchasing software that will provide high quality graphic simulations of ELINT systems and run on an Agency standard high-performance workstation. The system will output the graphics as a composite video signal. By creating and editing video tapes, we hope to develop a library of simulations that can be combined with still graphics for high quality presentations.

(U) In summary, the Architecture is based on three ideas: (1) the development of an operational ELINT baseline and objective Architectures; (2) the creation of computer models operating on a community-compatible data base; and, (3) the development of computer simulations that can be combined with other visual material for demonstrating new concepts to decision makers and fiscal authorities.

~~(C)~~ Although far from finished, the OPELINT Architecture has already begun to pay off for W4. We have been able to use the information developed to create a comprehensive Operational ELINT Program Plan, and we have opened some new avenues in the areas of graphic presentations for operational uses. There are still some areas we need to explore and that offer opportunities and challenges for imaginative analysts, programmers and planners.

(U) It is my hope this article not only aids others in their efforts to develop an Architecture, but also elicits responses from those of you who are working on existing programs that may aid us in the execution of ours.

New Address for CRYPTOLOG

P1
NORTH

DOCID: 4010026

GOLDEN OLDIE

REFLECTIONS ON SELECTED NILOTIC LANGUAGES

Nuer, which is spoken along the upper White Nile,

Has more complicated morphophonemic alternations than there are theories about Mona Lisa's smile.

And it may well be that they can be analyzed in terms of a pattern,

But, if so, the system is about as complex as the control mechanism of a space vehicle designed to travel to Venus by way of Saturn.

It is also possible that Shilluk is the language I have been looking for, which is neither a contour nor a discrete level nor a terraced level but a split level tone language,

But in any case I am very glad that Shilluk is not my own language,

Because if it were I would be wandering around naked with a spear in one hand and a nail through my lower lip for decoration,

A complex of cultural traits of which my wife would take a dim view because she is not fond of lethal weapons and is sure that a nail through the lower lip would seriously interfere with expectoration.

And although I have never heard Dho-Luo, I am extremely dubious about the feasibility of developing competence in it with the lesson manual entitled "Dho-Luo Without Tears,"

Because I have never heard any Nilotic language that isn't at least as hard as saying "Peter Piper picked a peck of pickled peppers" after seven beers.

In fact, my sentiments on another can be summed up by the simple observation that Dinka

Is a stinka.

In short, although these and other languages of the Sudan and Uganda and Kenya are indisputably neglected,

In the light of all the evidence I have collected,

I am not just before proposing a government-supported Language and Area Center specializing in Nilotic,

Because even I have a feeling, possibly brought on by advancing years, that there is such as thing as being too ruddy exotic.

[redacted]
March 14, 1961

P.L. 86-36

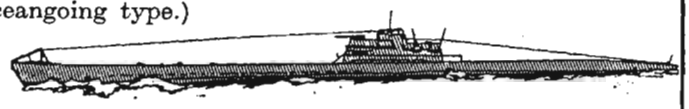
~~OFFICIAL USE ONLY~~

DOCID: 4010026

BELATED THANKS

U 25, 26.
(Oceangoing type.)

U 37—44.
(Oceangoing type.)



U 77, 78
(Oceangoing type.)

P.L. 86-36 [redacted] P13D

For most of us us Sigint-oriented types at NSA, appreciation for the many-faceted art of cryptanalysis is something that just seems to go with the turf. We *have* to give it lip-service, at least, since after all we do work here. Well, the other day, while cleaning out my desk (preparatory to getting ready to retire) something happened to drastically change my perspective. I came across an old copy of *Cryptologic Spectrum* (Winter, 1978) which featured a series of fascinating articles on "Ultra and the Battle of the Atlantic." *More* than fascinating to me, because one of them, called "The German View" by Prof. Jurgen Rohwer, made me realize that C/A might very well have been the instrument for saving my own life—and those of a number of other nervous GIs aboard our troop ship—way back in World War II days, in February 1943. Suddenly, in flashback, I experienced a visceral appreciation of what the art of cryptanalysis could really do, worked out on a scale of life and death.

Looking back on the Battle of the Atlantic from my own perspective aboard a tiny Liberty ship, I can imagine few situations better calculated to instill a feeling of Man Against the Elements. Add to that the gnawing fear of *das Boot*--the dread of a torpedo coming from somewhere out there. We were heading northeast in early February on a convoy out of Boston, both seasick and scared, en route for Iceland. We heard that a previous convoy had been hit—the one in which the *Dorchester* (with the three heroic chaplains aboard) had gone down. Reading Mr. Rohwer's article, I discovered something none of us knew at the time: Bletchley Park's OIC (Operational Intelligence Centre)—which we of course had never heard of!—had begun to make inroads on the German Naval Triton cipher, after a bad six months during the second half of '42 when our people had a decrypting blackout and the U-boats were intercepting about one-third of the running convoys. At last, as he says, "Bletchley Part succeeded . . . in solving the main problems of the Triton cipher circuit . . . (and) from the 5th to 28th February the traffic was decrypted with seldom more than 24 hours time lag." A comforting thought—just in time to protect *our* convoy . . .

These C/A successes meant that the British Submarine Tracking Room at the OIC could get warnings out to reroute the convoys and keep us away from the U-boat patrol lines. If we had known this then, a lot of us aboard the tiny *USS Chateau Thierry* (barely 10,000 miserable tons in size) would certainly have slept better. But there was still a problem with the wolfpacks, according to Prof. Rohwer: at this time, the German *B-Dienst* (the counterpart of the OIC at Bletchley Park) was also having its most successful period: "it could decrypt many of the routing and re-routing signals and many of the U-boat situation reports sent daily by the Admiralty or COM-INCH (Commander-in-Chief, Tenth Fleet) . . ." He goes on to say that even if only 6 to 10% of the German decrypts were done in time to be of operational value, they could have "important

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010026

consequences." He then cites February 1943 as a good example of this—the fateful time when the Battle of the Atlantic was beginning to come to a climax, and when our own little troop ship was riding into it.

Prof. Rohwer cites a certain convoy HX.228, heading northeast, about which the *B-Dienst* had decrypted a position report. (Might this have been us? It was the right time and direction.) At this point Admiral Dönitz's people ordered the wolfpack *Ritter* to move north to find them (or us!). Fortunately, our heroes at Bletchley Park decrypt the order—God bless 'em—and the convoy gets an order to move north of the *Ritter* patrol line. Another piece of luck for HX.228—the U-boat command about this same time intercepted and decrypted position reports on two other convoys.ON.166 and ON.167--heading west, away from our convoy. Group *Ritter* was thereupon ordered to change course and set up a new patrol line along longitude 30° West to cover the expected passsing routes of those two other convoys—as I interpreted Prof. Rohwer's account.

What followed must have been one of the most dramatic scenarios that fate could ever devise—more gripping than anything Hollywood could have dreamt up—move and countermove—as Bletchley Part and the U-boat command decrypted each other's messages, the hunted and the hunters maneuvering for position in a life-and-death chase through leaden seas. Finally it came to a grim conclusion. Prof. Rohwer reports: "In a fierce convoy battle which lasted for six days and covered 1100 miles the U-boats sank 15 ships and lost two of their number to the counter-attacks of the escorts."

Many died, many were spared. Looking back, I wish I knew for sure whether HX.228 was really *my* convoy. I do know I want to look for more clues in Patrick Beesly's much-praised book, *Very Special Intelligence. The Story ofthe Admiralty's Operational Intelligence Centre 1939-1945*, published in 1977. (Mr. Beesly was deputy chief of the Submarine Tracking Room of the OIC at that time.) Anyway, regardless of the exact role that C/A played in getting our own particular convoy to Reykjavik safe, sound (and hungry), I'm now totally convinced that innumerable Allied lives were saved because of the hard work of the people at Bletchley Park, OP-20-G (the US counterpart of the OIC), and in other places where the cryppy's trade was relentlessly pursued during those trying days. So, 46 years after the fact, I send belated kudos to all of them from a grateful, non-cryppy survivor. In normal times, we can only dimly surmise how our lives are daily affected by unknown, unseen people and events. But in times of war, how much more dramatic and powerful, if the curtain is lifted and we catch a glimpse of it. (And, in the case of my own particular convoy, who knows but that some strange quirk of fate might have decreed that a decryption by our adversary, the *B-Dienst*, could become a strangely crucial factor in getting the wolfpack off *our* trail and on to someone else's? If so, perhaps I could even say, somewhat selfishly: *Vielen Dank* to you too, our one-time enemy.) On the basis of my own experience, relived retrospectively, I can now agree with Prof. Rohwer on the very deepest level, when he says: "... without the work of many unknown experts at Bletchley Park, the turning point of the Battle of the Atlantic would not have come as it did... but months, perhaps many months, later."

Solution to:

NSA-Crostic #68

1st Issue 1989

by [redacted]

[Finally, and perhaps most important,] translators must learn to unleash their minds. Rote translation works for some texts all of the time and all texts some of the time, but not for all texts all of the time. It is at this juncture that creativity [- - the choice of right phrase or word in English to match the thought and flavor of the original --] becomes crucial.

[redacted] "The Creative Translator," *Collected Articles on Translation*, 1973

P.L. 86-36

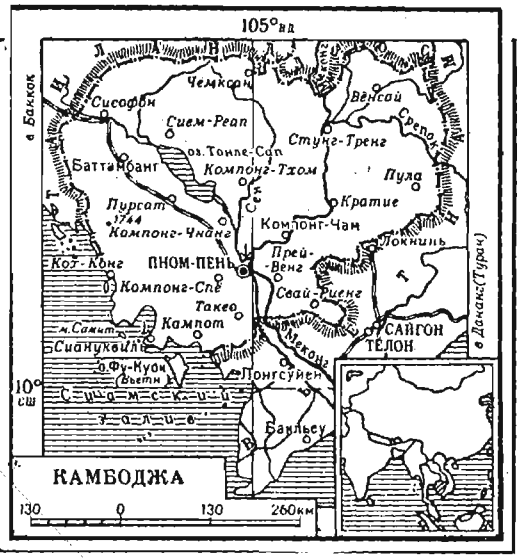
~~FOR OFFICIAL USE ONLY~~

DOCID: 4010026 EO 1.4.(c)
P.L. 86-36

CAMBODIA In PEACE AND WAR

P.L. 86-36

[redacted]



~~(S-CCO)~~ After spending over 12 years on the Vietnamese Communist (VC) target, I had the opportunity in July 1968 to assume the duties of Chief of the Cambodian Branch in what was then B12. I took on this assignment because I saw it as both a career-enhancing job and an opportunity to work in a new environment. But I can remember my former Division Chief asking shortly after I took on this assignment, "How are things in Sleepy Hollow?"

~~(S-CCO)~~ I must say that in July 1968 the Cambodian problem could not be compared in any way with the Vietnamese problem. With the war going on in Vietnam and the US involvement steadily increasing, Cambodia (also known as Khmer) was not a target of importance. [redacted] brought about a great change in Cambodia in the way the target was handled here at NSA and in the Intelligence Community as a whole. The following is a description of this change and the developments we had to contend with to support our customers on a real-time basis.

~~(S-CCO)~~ My main intent in writing this article is to provide information that might be of value to production organizations which may have to face a similar target change in the future. I dedicate it to all the men and women who worked on the Cambodian problem, both at NSA and overseas, and willingly put in many hours of their own time to ensure that the job was accomplished in a quick and thorough manner. I will not mention any of them by name simply to avoid leaving anyone out.

SUMMARY OF THE EFFORT

~~(S-CCO)~~ In July 1968, the Cambodian Branch consisted of three teams [redacted] most of whom were civilians. This included Traffic Analytic, Linguistic/Reporting and ADP Support Teams. Most of our effort was concentrated on the analysis, processing and reporting of Cambodian Armed Forces (FANK) communications.

~~(S-CCO)~~ Cambodia at that time enjoyed a low priority, and in many cases hard copy reports satisfied the requirements. These were annual disposition of forces/order of battle reports and periodic reporting on political and military activities and changes in the military organization and equipment. Electrical reports were issued by field elements (USM-626, Saigon, South Vietnam; [redacted] and U.S. Technical Research Ships) as well as by B12.

~~(SC)~~ The only significant requirements related to the use of Cambodian territory by the VC forces, either as safe havens or for the infiltration of supplies, equipment, and personnel through Cambodia into South Vietnam. [redacted]

EO 1.4.(c)
P.L. 86-36

P.L. 86-36
EO 1.4.(c)

any evidence to support this theory and reported electrically on any indications of Vietnamese forces operating in Cambodian territory.

~~(SC)~~ Also, there was relatively high interest in Cambodian insurgent activities. Three insurgent groups, the Khmer Serie, Khmer Leou and Khmer Rouge (Cambodian Communists) were active at the time, primarily in the Cambodia-Thailand border areas. We often reported on FANK operations and activities of insurgent elements. None of these insurgent groups appeared to be of any great threat to the Cambodian government or its armed forces.

~~(S-CCO)~~ In my opinion the FANK communications network was a relatively easy target to collect, process, and analyze. Most communications were in HF manual Morse [redacted] The field sites forwarded most traffic by courier except that which was encrypted or they felt was possibly important enough to meet product reporting requirements.

TRAFFIC ANALYSIS

~~(S-CCO)~~ The traffic analysts working on FANK communications performed the normal tasks expected of them by maintaining continuity on all targets of interest, preparing net diagrams and message/address group logs, and providing technical support to field elements via technical messages and hard copy working aids and COMINT Technical Reports.

~~(SC)~~ The FANK did not use signal plans as sophisticated as those used by the VC. Most HF communication groups were simplex stars using day and night frequencies, international procedure signals and French language operator chatter. They often compromised address groups used in message preambles and occasionally in operators chatter and gave advance warning of callsign/frequency changes. This coupled with the fact that we were eventually able to obtain, through the Defense Attaches Office (DAO) in Phnom Penh, copies of the FANK overall signal plan, made the traffic analysts task relatively easy. Our only problem was dealing with the large volume of material.

~~(S-CCO)~~ Examples of the FANK message preambles and HF communications groups are shown in Figure 1.

CRYPTANALYSIS AND LANGUAGE EXPLOITATION

~~(S-CCO)~~ Approximately ninety-five percent of the correspondence passed over FANK communications was French plaintext messages. A small amount of Cambodian language material was noted as well as some encrypted traffic. We were able to exploit all traffic with except that which was badly garbled.

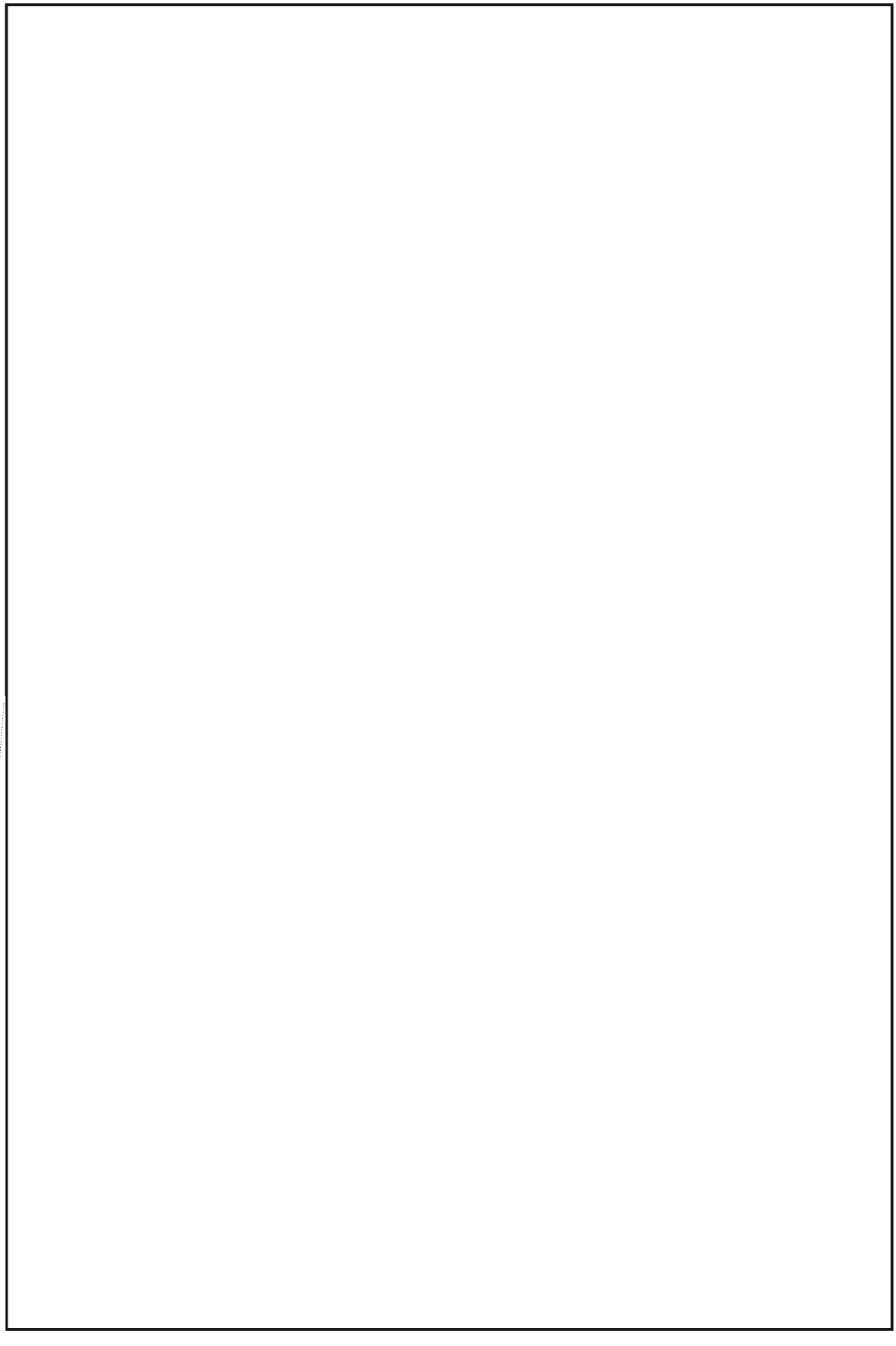
~~(S-CCO)~~ The Linguistic/Reporting Team consisted of about ten French linguists and a couple of Cambodian linguists. They were able to scan and translate messages of significance and flag them for inclusion in a machine data base for subsequent reporting in hard-copy reports. The messages meeting timely reporting requirements appeared in electrical summary reports. The messages put into the machine data base were flagged by subject so that a pull could be made on them when a hard copy report on a specific subject was in preparation.

~~(S-CCO)~~ The FANK messages were normally less than a hundred groups in length and generally limited to one subject. This made it fairly easy to categorize the messages and identify the originators and addressees. Often specific addresssees were spelled out in the preambles and/or the beginning of the message texts. So, just as with the traffic analysts' job, the linguists/reporters had a relatively easy but heavy work load.

THE KHMER COMMUNIST PROBLEM

~~(S-CCO)~~ The development of the Khmer Communist (KC) problem was a very gradual one that took place over about a two-year period. By early 1969, we began seeing reference in FANK communications to increased KC activities in scattered areas of Cambodia. This, supported by collateral information, indicated that the KC were growing much stronger and were probably being assisted by the VC. Extensive collection efforts were undertaken to intercept KC communications which we suspected would be HF manual Morse and HF/LVHF radiotelephone.

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

DOCID: 4010026

EO 1.4.(c)
P.L. 86-36

~~(S-CCO)~~ By early 1970 we had not been able to identify any KC communications. We suspected that if the KC were being assisted by the VC, the Vietnamese would provide them with necessary radio equipment and probably signal plan and cryptographic training and materials, and so the KC communications characteristics and procedures would be similar to that used by the VC. Eventually this proved to be the case.

~~(SC)~~ In late 1969, while conducting general search efforts at Udorn, Thailand, USM-7 intercepted an HF manual Morse link initially identified as VC.

~~(S-CCO)~~ Because of the signal plan used on this link we tried to have these communications worked in the Vietnamese Office. Some even thought that the link was actually down-working of a VC communications group which had most of its stations located in Cambodian territory. Further, some believed that the VC were running the show in Cambodia and that this communications group served their command and control apparatus in Cambodia. Later we concluded that the VC group probably served the VC cadre who were helping the KC establish their infrastructure and were providing communications and technical assistance. Nevertheless, this initially proved to be a stumbling block in our attempts to move on with the development of the KC communications network.

~~(S-CCO)~~ By this time, interest in Cambodia had increased significantly as the KC military and political arms started putting more and more pressure on the Cambodian Government and its armed forces. Intelligence requirements changed drastically, with high emphasis being placed on obtaining information on KC activities. Meanwhile, the intelligence requirements on FANK communications lessened as the US increased aid to Cambodia and a larger contingent of US personnel was assigned to Cambodia. They were to help train FANK personnel and develop a more effective intelligence gathering operation and expedite the flow of intelligence information to FANK units involved in day-to-day combat operations.

~~(S-CCO)~~ During the next two years, we found ourselves having to deal with a number of problems besides the isolation and development of the KC communications network. The traffic analytic work force had to be trained to do more detailed analysis on the more complex and sophisticated KC communications; the language pool had to be changed from primarily French to a Cambodian cadre; and those involved in preparing product reports (other than translations) had to shift gears to produce more timely reports and, as with the traffic analysts, learn to deal with a target that was not going to reveal as much in message externals and text as the FANK did.

~~(S-CCO)~~ During 1970-1972 one of our primary goals was resolving our language problem. This, as you can imagine, was not an easy task since good Cambodian linguists couldn't be hired off the street. The Service Cryptologic Elements were our initial sources of linguists and both INSCOM and NSG were able to provide assistance over a period of time. They adjusted their language training program to train more Cambodian and fewer French linguists and the Language Intern Panel was able, eventually, to provide us with one linguist.

~~(S-CCO)~~ By late 1972, our Cambodian language pool had grown which included a number of military personnel. We were able to hire some of these military personnel after they had satisfied their military commitment. Fortunately, this was back in the days when a military person could clear the building on a Friday and come back as a civilian the next Monday.

~~(S-CCO)~~ During the next couple of years, the Cambodian Branch was able to meet all time-sensitive reporting requirements and at the same time develop a mean and lean work force. By early 1974, the branch consisted of three teams Traffic Analysis,

EO 1.4.(c)
P.L. 86-36

DOCID: 4010026

Language Exploitation, and Reporting. The three teams had to work closely together to ensure that all communications were collected, processed, analyzed, and reported on as quickly as possible.

~~(S-CCO)~~ Meanwhile, an extensive collection and analytic effort had also been established at USM-7, Udorn, Thailand, where the bulk of the KC communications were being collected. Every effort was being made to give the field the capability to perform first instance reporting on the target. However, because of language difficulties, only a limited reporting effort could be maintained. Thus, most of the reporting effort fell on the Cambodian Branch at NSA. The efforts involved in this process are described in the following paragraphs.

TRAFFIC ANALYSIS

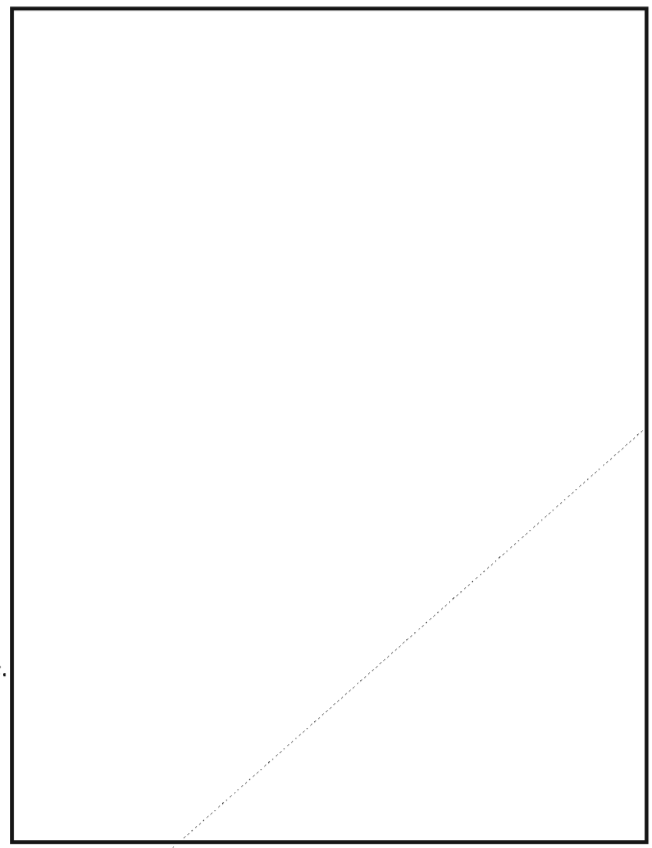
~~(SC)~~ As I indicated earlier, the traffic analysts working on the Cambodian problem had to significantly alter their method of analysis in order to contend with the KC communications. The KC communications groups consisted of two or more complex links which changed callsigns and frequencies on an ad hoc basis. Fortunately not all links changed at the same time, so it was possible to concentrate on certain areas following signal plan changes.

~~(SC)~~ The KC HF manual Morse network grew gradually as the KC established their infrastructure in different parts of the country. This allowed us to develop the communications while teaching the analysts to perform more detailed analysis. Since the KC used complex links, the intercept operators often intercepted only one end of a link; in many cases they didn't have the capability to copy both ends at once. So, it was a case of searching through the unidentified material we received in the Cambodian Branch, as well as material held in the unidentified files in the Vietnamese Office to find backlink activity. A time-consuming task, but often profitable. Through up- and down-time matches and message servicing activity, we were able to recover many backlinks and aid the intercept operators in collecting those stations passing message traffic.

~~(SC)~~ Because all KC traffic was readily exploitable, the traffic analysts thought that their task would be relatively simple as it had been with FANK communications. However, this proved not to be the case. The KC used cover names and designators in the message texts for originators and addressees of messages as well as for political and military organizations. The analysts had to be very careful when using the internal address information to co-locate terminals because it was often difficult to determine if a message was being sent by one control station to two or more subordinates or if the message was originated by a senior authority and being relayed to a second- or third-level subordinate. The KC did not use broadcast communications to send a message to two or more subordinates; the same message was sent separately to each.

~~(S-CCO)~~ Another interesting traffic analytic problem developed a few months after the first KC link was isolated.

Also, different message preambles containing what appeared to be routing indicators started to be used on messages passed over the link. The traffic analysts as well as the linguists were miffed by this development and it wasn't until we obtained some HF direction finding (DF) results that we started to get a hint at what we were dealing with.



EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~(S-CCO)~~ By the end of the war, the traffic analysts had gained a lot of experience by working on a more difficult problem and learned how to use a variety of techniques to assist in their analysis. This included not only HFDF results, but airborne DF (ARDF) as well. ARDF missions flown by US Army platforms over South Vietnam were able to provide accurate fixes on many of the KC targets while they flew missions along the Cambodian border. In addition, they were able to gain some experience in working on KC VHF/LVHF voice communications which were occasionally intercepted by airborne platforms. Unfortunately, these communications were very difficult to intercept because of the low power and the type of equipment used by the KC, and never really provided any meaningful intelligence information.

~~(S-CCO)~~ Figure 2 shows an example of a KC message preamble and HF manual Morse communications group; note the difference between the KC and the FANK practises.

[redacted]

LANGUAGE EXPLOITATION

~~(SC)~~ [redacted] As we became more familiar with chart usage and patterns noted in the chart internals, it was possible to develop [redacted] process which not only did not help, but it hindered our language exploitation efforts.

~~(SC)~~ [redacted] the linguists had developed romanized equivalents for the Cambodian script characters, patterning them after the romanized Cambodian we occasionally noted in FANK Cambodian plaintext messages. [redacted] the new linguists had great difficulty.

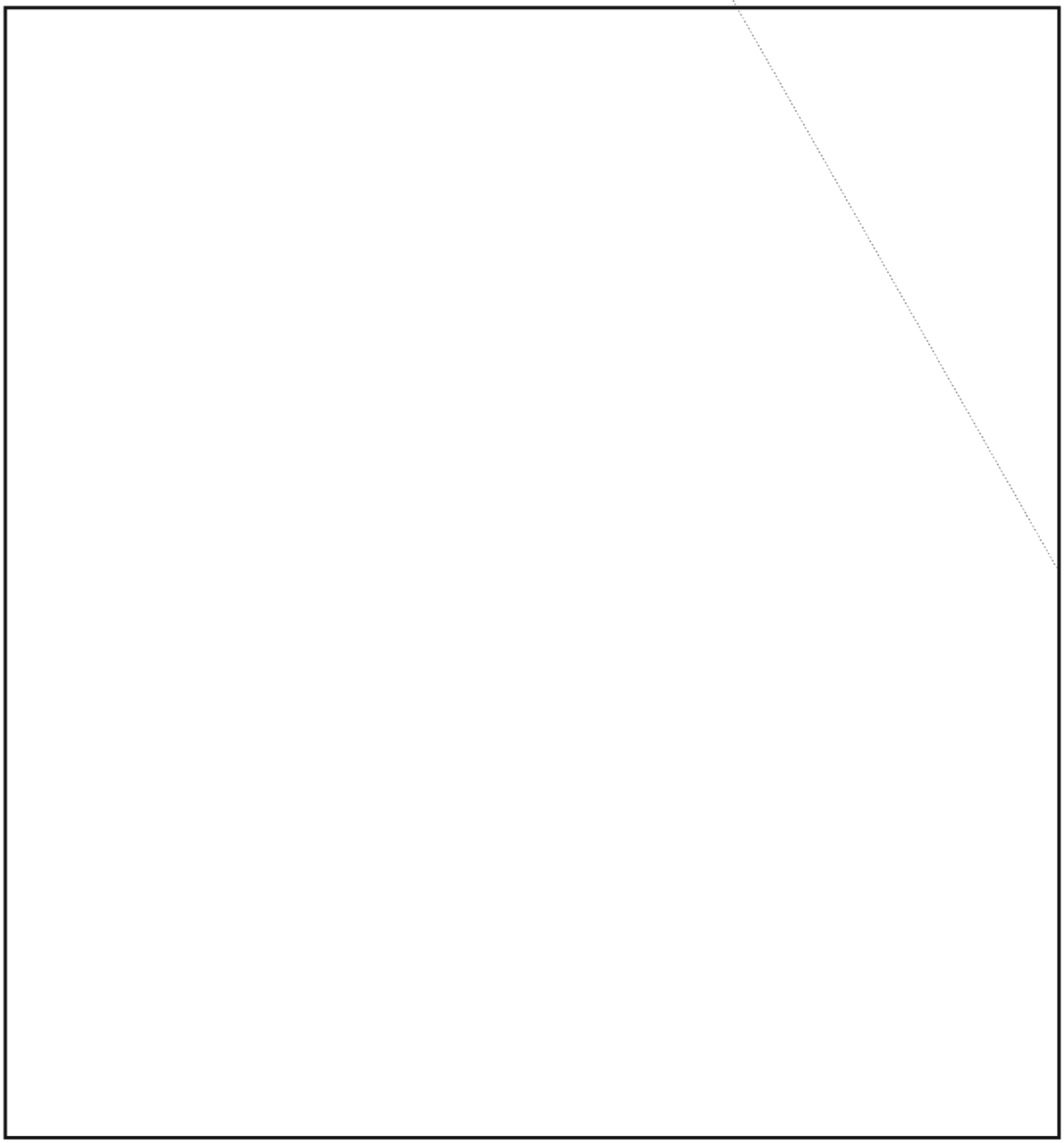
~~(S-CCO)~~ All of the new linguists had been trained in Cambodian using materials such as newspapers and books in Cambodian script and were taught to use Cambodia dictionaries written in that scrip, for Romanized Cambodian was not used in non-SIGINT material. Thus, to [redacted] one of the first things they had to do was to learn the romanized equivalents. This was time-consuming, the more so because before these new linguists could translate the message, they converted the romanized text back to Cambodian script by hand. Another key problem was garbles that often appeared in intercepted material. Even if there were only a few in a particular message, the new linguists were unable to render the text readable.

~~(S-CCO)~~ Another thing the linguists had to deal with was the different vocabulary used by the KC. Besides using words not normally seen in FANK communications, they also used a large number of abbreviations, cover terms and cover names for persons, places and things. The linguists had to become familiar with all these before they could produce meaningful translations.

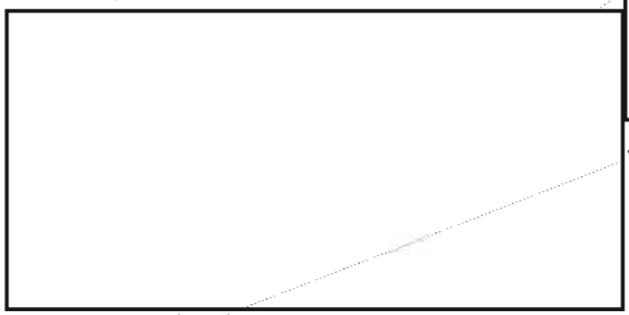
~~(SC)~~ To further complicate the linguists' task there was the problem of part messages. KC messages were long, sometimes more than 1000 groups. [redacted] Moreover, unlike the FANK, the KC might cover a number of subjects in one message. Thus, the linguists would have to determine the right order of the message parts before they could translate the message in the right context.

~~(SC)~~ The linguists first scanned the cleaned up message for any information that met timely reporting requirements. In most cases this was tactical information which provided data on KC attack plans or unit locations. Normally, they prepared a short narrative SPOT Report or CRITIC providing the information to the DAO in Phnom Penh and our other customers, then followed it up as soon as possible with a full text translation. The Defense Attaché Office in Phnom Penh had a standing requirement for full-text translations of all messages containing

EO 1.4.(c)
P.L. 86-36

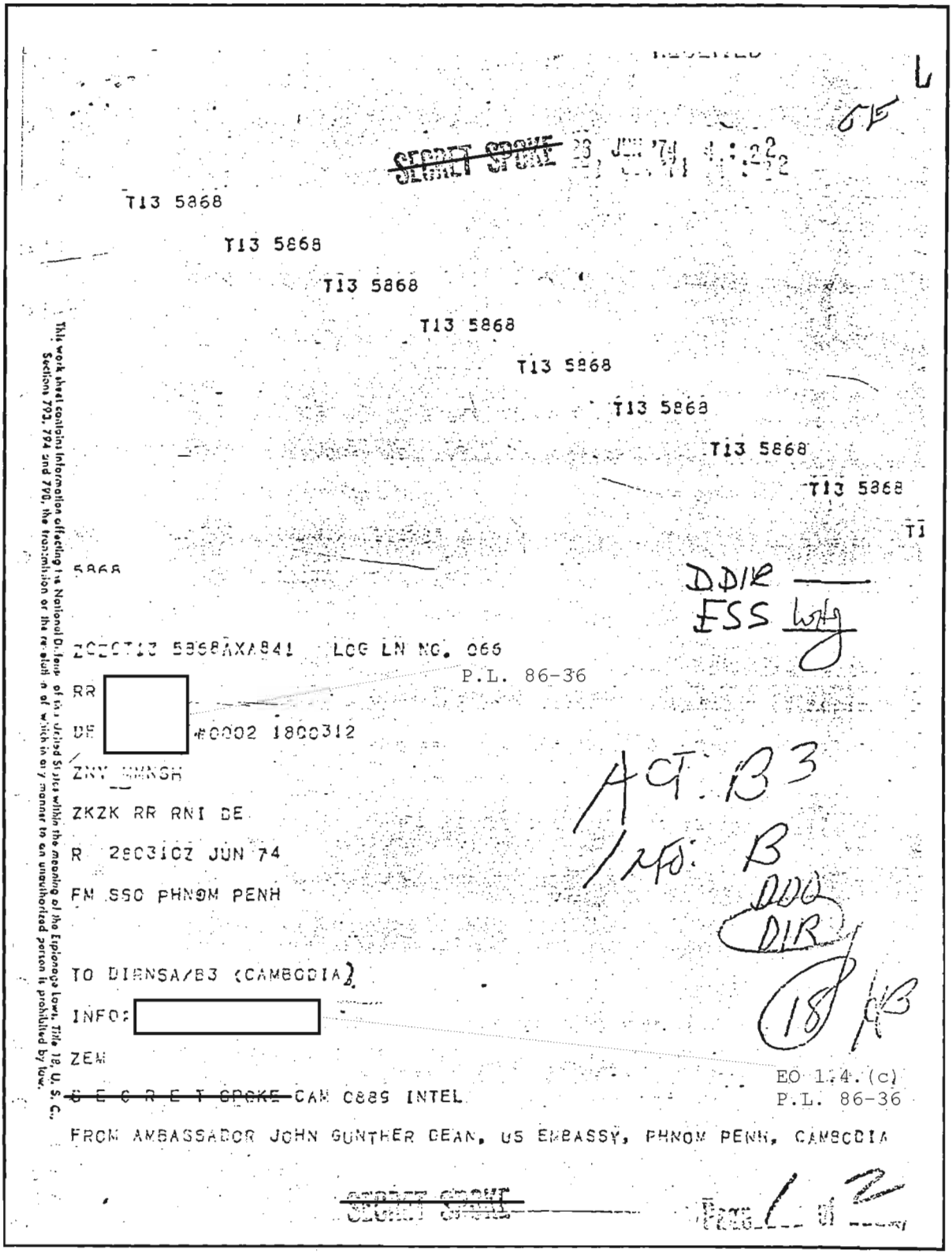


any intelligence information of value to them. The DAO then sanitized the information and forwarded it to the appropriate FANK authorities for the necessary military action.



~~(S-CCO)~~ Besides having to contend with all of the above, the Language Team also had to provide on-the-job training for Cambodian linguists assigned to USM-7. Through early 1975, several groups of Army linguists spent three to

EO 1.4.(c)
P.L. 86-36



~~SECRET SPOKE~~ 28 JUN '74 4:22

T13 5868

T13 5868

T13 5868

T13 5868

T13 5868

T13 5868

T13 5868

T13 5868

T1

5868

DDIR ——
ESS WHG

ZCZCT13 5868AXA841 LOG LN NO. 066

P.L. 86-36

RR [redacted]

DE [redacted] #0002 1800312

ZNY MMNSH

ZKZK RR RNI DE

R 280310Z JUN 74

FM SSO PHNOM PENH

ACT: B3
INFO: B
DDO
DIR
18 HB

TO DIRNSA/B3 (CAMBODIA)

INFO: [redacted]

ZEM

~~S E C R E T SPOKE~~ CAM 0889 INTEL

EO 1.4.(c)
P.L. 86-36

FROM AMBASSADOR JOHN GUNTHER DEAN, US EMBASSY, PHNOM PENH, CAMBODIA

~~SECRET SPOKE~~

Page 1 of 2

This work sheet contains information affecting the National Defense of the United States within the meaning of the Espionage Laws, Title 18, U.S.C., Sections 793, 794 and 798, the transmission or the revelation of which in any manner to an unauthorized person is prohibited by law.

four months each in the Cambodian Branch prior to going overseas. Much time had to be spent with these linguists to get them to the point where they could adequately handle the KC traffic sent back to USM-7 [redacted] Although they did their best in the

EO 1.4.(c)
P.L. 86-36

DOCID: 4010026

~~SECRET SPOKE~~

SUBJECT: MESSAGE OF APPRECIATION

IT IS ALL TOO SELDOM THAT PERSONNEL PERFORMING AN INDISPENSABLE TASK RECEIVE THE RECOGNITION RIGHTFULLY DESERVED. I WOULD LIKE TO TAKE THIS OPPORTUNITY TO EXPRESS MY PERSONAL APPRECIATION FOR THE OUTSTANDING INTELLIGENCE PRODUCT PRODUCED BY THE CAMBODIAN SECTION OF 83. I CAN HONESTLY SAY THAT WITHOUT YOUR CONTRIBUTION, THIS MISSION-S EFFECTIVENESS WOULD BE GREATLY REDUCED. TO ILLUSTRATE THIS POINT, ONE MERELY HAS TO RECALL YOUR RECENT CRITIC SERIES MESSAGES OF 8 JUNE IN WHICH YOUR TIMELINESS MAY HAVE AVERTED A CATASTROPHE. IN ADDITION TO MY OWN PRESENCE, THE FANK GENERAL STAFF, THE REPUBLIC CABINET, AND THE ENTIRE DIPLOMATIC CORPS HAD BEEN SCHEDULED TO ATTEND CREMATION RITES FOR THE ASSASSINATED MINISTERS ON 9 JUN. AS A RESULT OF THE CRITIC, RITES WERE RESCHEDULED FOR 10 JUN UNDER MORE STRINGENT SECURITY CONDITIONS.

IN FULFILLING OUR GOVERNMENT'S OBJECTIVES REGARDING CAMBODIA-- A JUST AND LASTING PEACE-- YOU MAY TAKE SPECIAL PRIDE. YOUR ENDEAVORS HAVE DAILY DIVIDENDS IN THE FIELD AS WELL AS IN PHNOM PENH ITSELF.

THANK YOU FOR A TRULY PROFESSIONAL JOB.

XGDS-2

#0002

~~SECRET SPOKE~~

Page 2 of 2

This work sheet contains information affecting the National Defense of the United States within the meaning of the Espionage Laws, Title 18, U. S. C., Sections 793, 794 and 798, the transmission or the revelation of which in any manner to an unauthorized person is prohibited by law.

field, they never reached a level of proficiency sufficient to handle first-instance reporting on the KC problem.

DOCID: 4010026

REPORTING

~~(S-CCO)~~ In addition to the SPOT Reports, CRITICS, and translations published by the linguists, it was also necessary to produce summary reports on KC activities. These reports dealt with message content as well as developments noted in communications. A separate team was established to report these activities in addition to the Traffic Analytic Team. One of the major problems we had early on was identifying the users of the KC radio network; reporters familiar with FANK practises provided specific information which made it relatively easy to identify radio station users. This was not the case with the KC.

~~(S-CCO)~~ I can remember many instances where we had long, tough discussions on whether we had enough information to at least tentatively identify a user on the basis of the structure of a communications group, the area it was located in, and the contents of message text. Because the KC seldom identified themselves as the FANK did, it was hard to get reporters to go along with less than "A" validity. But, after a while this became normal practice and to my knowledge the identifications we came up with were pretty much on the mark.

~~(S-CCO)~~ The summary reports prepared by the Reporting Team were done to satisfy customer requirements not requiring real-time reporting. This included periodic disposition of forces reports, special topic summaries and inputs for the Southeast Asia SIGINT Summary and the NSA SIGINT Summary. Often we were able to use collateral information to supplement what we obtained from SIGINT.

CONCLUSION

~~(S-CCO)~~ I hope after reading this article you will have a better appreciation of what the Cambodian Branch had to contend with during the war in Cambodia. I wish I could conclude with a statement that would give a happy ending to this story. But, unfortunately, the Lon Nol Government of Cambodia fell to the KC on 15 April 1975. We had given it our best effort, as I'm sure the US personnel in Cambodia had done.

~~(S-CCO)~~ We published thousands of pieces of product with information which should have been of value to the FANK authorities in countering KC activities. Unfortunately, there were often indications that when FANK forces were tipped off to an impending KC attack, instead of reinforcing their positions or conducting a counter attack, they would simply withdraw from the area to avoid a confrontation. Because of this and the constant heavy workload, we often felt frustrated with the job at hand.

~~(SC)~~ However, there were times when our efforts were duly rewarded. One prime example was an event that occurred in early June 1974 shortly after a number of Cambodian Government officials were assassinated by the KC. A funeral ceremony was going to be held in Phnom Penh which the U.S. Ambassador, the FANK General Staff, the Cambodian Cabinet and the entire diplomatic corps were scheduled to attend. A KC message was intercepted indicating that they were going to conduct a rocket attack on Phnom Penh during the ceremony. We issued a CRITIC immediately upon recognition of the KC intent. As a result of this CRITIC, the ceremony was rescheduled and according to the words of the US Ambassador, "your timeliness may have averted a catastrophe." The Ambassador's message to DIRNSA on this subject is shown as Figure 3.

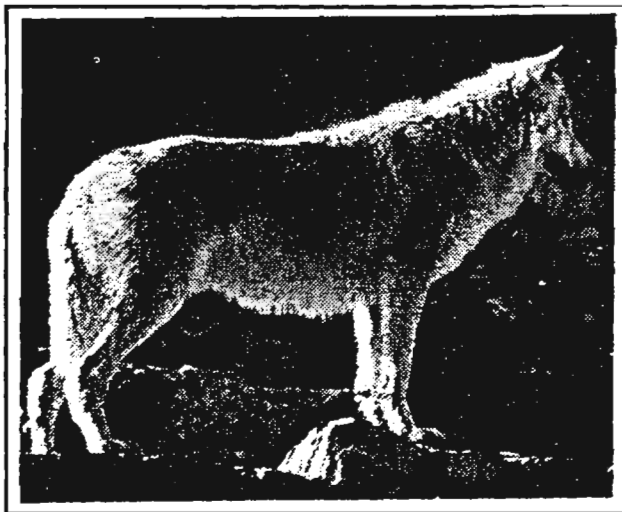
~~(S-CCO)~~ Needless to say, the job of working on the Cambodian problem during the war was very rewarding from many aspects, most important, the privilege to work with a fine group of people. During the period covered by this article, B Group had a few reorganizations which fortunately didn't affect the Cambodian Branch.. The division we were part of was moved between a number of offices and changed designators each time--B12, B65, and B33.

BULLETIN BOARD

UPDATE ON CAPULET

~~(FOUO)~~ Individuals who have CAPULET software may obtain updated versions from [redacted] B824, HQ 1A205, 963-5184. CAPULET is a suite of CA programs for the IBM XT or AT

P.L. 86-36



HARDWARE REVIEW

OCR DEVICES

P.L. 86-36

Reviewed by: [redacted] *R8311*

~~(S-CCO)~~ [redacted] R831 has been testing Optical Character Recognition (OCR) devices to determine the feasibility of using such machines for producing digitized working aids [redacted] Presented here are some principles of OCR, our test methodology, the results of our tests on three devices and of an accuracy test for several languages that was run on the best device.

ON OPTICAL CHARACTER RECOGNITION

(U) The technology which allows printed matter to be transformed into computer (digitized) format is called Optical Character Recognition (OCR). There are two kinds of OCR software. The first is dot matrix recognition which works by analyzing the location of dark and light spots on an image and matching them as closely as possible to a stored set of dots. A more sophisticated technology is called pattern matching, sometimes termed Intelligent Character Recognition (ICR), and relies on analyzing an image for its component parts, much as a human does when reading. Simply put, a scanning device looks at the pattern for each character of text, determines what this pattern represents and assigns a value to that pattern, generally using ASCII text codes. For example, when the scanner sees a vertical bar crossed at the top with a horizontal bar it interprets the pattern to be that for the upper case letter "T" and assigns the appropriate ASCII value to the image.

(U) The accuracy of such interpretations is further enhanced, to a limited degree, by lexicons and artificial intelligence rules which help determine if a particular sequence of characters is in fact a plausible combination. Artificial intelligence, however, is much less reliable than the human eye in viewing text as meaningful words. A computer, as well as a human, can tell just as confidently that in English the character sequence "happ." should end with the letter "y." But the human can go one step further and also accurately fill in the missing letters for the phrase "Happ. N.. Year!" while the computer, unless programmed with context-specific information, probably cannot. To a computer, words such as "Now", "Net", etc. are just as likely as the word "New."

(U) R831 purchased for testing three optical character readers of the many on the market. Although there are a number of different types of readers available, including hand-held models, desktop PC-based models and large stand-alone models, the selection criteria were geared primarily to the need to digitize multilingual publications, especially those having Cyrillic text. Given these considerations, the models selected were: Intelligent Optics Corporation's (IOC) SPEEDREADER, Kurzweil Computer Products' DISCOVER 7320 and Kurzweil's 4000 Intelligent Scanning System (ISS).

DESCRIPTIONS OF THE DEVICES

IOC SPEEDREADER

(U) The IOC SPEEDREADER is a desktop, pattern-matching page reader which can input text or graphics from a printed or typed page to a personal computer or word processor. Any

P.L. 86-36

alphabet of a typewritten or typeset format can be recognized in a variety of fonts, although point size is limited to the range 8 to 12. Scanning speed for high-quality text is approximately 30 characters per second for typeset and 40 characters per second for typewritten material. In the graphics scanning mode the SPEEDREADER scans either line art or continuous tone images. It has an automatic sheet-fed scanner which can be loaded with up to thirty pages of material. Files of longer than thirty pages can be created using an append facility. Minimum page size is 5.5 by 5.5 inches and maximum is 8.5 by 14 inches.

(U) Character recognition is achieved when the scanner compares the patterns appearing in the text to a font selected from the document processing software and then provides the appropriate ASCII text code. This font of patterns can be created by the user or chosen from a library of starter fonts contained in the software. Creating a user font, called "training," is a process which requires assigning an ASCII text code to each of the patterns appearing in the text. This procedure might only require 30 minutes or so for very simple text but can be considerably longer for text having multiple typefaces. The assigning of text codes to patterns is left to the discretion of the operator but is limited to two codes per pattern with a storage capacity of 256 patterns. The operator might find this to be insufficient if, as in the case of a document with several typefaces and/or alphabets, it is necessary to maintain typeface integrity in the output.

(U) In training SPEEDREADER, the user must take time to account for all the characters and symbols appearing in the text. This is important because if the scanner detects a pattern on which it has not been trained, the output text displays either an incorrect character or a special symbol indicating an unknown character. Since the SPEEDREADER has no capability to add to a trained font while scanning is in progress, in order to correct this problem the operator has to stop scanning, add the new character to the trained font and re-scan the text.

(U) SPEEDREADER's output is a text file including the control characters inserted by the word processing program. These control codes include hard and soft returns to preserve paragraph integrity but allow wordwrap functions, tabs, indents, centering, underlining, space compression, subscripts and superscripts. SPEEDREADER supports most of the more popular word processing software packages on the market.

(U) All things considered, the SPEEDREADER, although the slowest of the three scanners tested, performs satisfactorily as long as the input text is of good quality and contrast, a caveat one could apply to all scanners. Despite the limited capacity for trained characters, and the lack of a concurrent editing function, the SPEEDREADER is a flexible device which does an adequate job under most circumstances.

DISCOVER

(U) DISCOVER 7320 is a PC-based, menu-driven, pattern-matching scanner. It reads both normal and landscape-oriented text in a variety of fonts ranging in size from 8 to 24 points. A maximum speed of 50 to 60 characters per second can be achieved, depending on the complexity of the character fonts and the quality of the scanned document. Software, containing system lexicons of approximately 50,000 words, is available for English, Spanish, Dutch, French, German, Italian or Swedish. In addition, user-defined lexicons of up to 10,000 words each can be created to supplement the system lexicon.

(U) DISCOVER is also an image scanner which can scan drawings and photographs with 15 levels of contrast control. There is a built-in sheet feed which will handle up to ten pages of material. DISCOVER can operate in a background mode under MS DOS thereby allowing document scanning and access to other software packages and PC functions simultaneously.

(U) Other features include an assurance threshold, which is a system confidence level telling the software how sure it must be of an identification before considering a text character as being recognized; a window option, which allows the operator to specify a zone whose contents should be captured when the page is scanned; and a column recognition function, which allows the system to analyze the pages for the specified number of columns and separate them into discrete zones.

(U) DISCOVER 7320 is probably the fastest scanner and the easiest to configure, but it is the least flexible. It is not trainable and can be used realistically only for monolingual

documents containing text in one of the preprogrammed languages. Also, even though the DISCOVER 7320 reads different typefaces, it gives no beginning- nor end-of-font markers in the output text to aid parsing. Nevertheless, if scanning requirements are such that these perceived drawbacks are not important, then DISCOVER 7320 can provide a reliable product

KURZWEIL 4000 ISS

(U) Kurzweil 4000 is a stand-alone pattern-matching scanner which can accommodate multiple fonts within a single document and read virtually any type font in sizes ranging from 6 to 24 points. Standard equipment features a display terminal, hard disk drive and a floppy disk drive used for file backup. Optional equipment includes an electronic tablet for document mark-up and a document feeder capable of holding up to 25 pages. Input can be either from bound books or individual pages measuring up to 11 by 14 inches. Separated pages can be placed individually on a glass surface directly over the optical scanning head or fed into the scanner by means of the document feeder. In the case of bound books, the pages must be placed on the scanning window. Depending on print quality and format of the original material, scanning speed is between 20 and 50 characters per second.

(U) The standard language configuration is for English but additional optional language packages are available for German, Italian, French, Dutch, Danish and Spanish. Language packages come with lexicons containing approximately 33,000 words. Since it is a trainable device it is also possible to program the 4000 to read other languages as long as the text is composed of discrete characters.

(U) Output is a file which can be transmitted to magnetic tape or hard disk, displayed on the terminal screen or transmitted to a peripheral device using appropriate communications software. The 4000 will also receive documents from asynchronous ports and magnetic tape machines. A more detailed examination of how the Kurzweil 4000 functions follows below.

TESTING AND EVALUATION

(U) The process of converting printed material into computer format requires more than simply choosing a scanning device and feeding a document into it. At least four mutually dependent phases of the digitizing operation need to be evaluated before deciding which scanner will produce the most accurate and reliable output. In addition to considering (1) the features and capabilities of the scanning device, and (2) the format and clarity of the printed text, the user must give equal consideration to (3) the amount and method of output editing to be done as well as (4) the format and intended use of the digitized product.

(U) It is also possible to have a single restriction as the deciding factor in the selection of a scanner. If, for instance, there is a need to capture a publication having significant intrinsic or monetary value, removing the pages of the document from the binding is not practical. Digitizing in this case is then limited to a device capable of scanning bound book material. Only after all of the variables are evaluated can a user make a reliable determination as to the best scanner for a job.

~~(C-CCO)~~ Performance evaluation of the three scanners was conducted on a wide variety of documents such as office memorandums, monolingual and multilingual publications, printer text and magazine articles. In addition to English, languages included Amharic, Arabic, French, German, Italian, Polish, Portuguese, Spanish and Russian. The quality of the material ranged from very good for clear, high contrast print of a newer publication, to very poor for older, worn documents whose print has faded through use and age. One goal of the evaluation was to judge the relative capabilities of the three scanners, but the primary emphasis was on determining which scanner produced bilingual digitized output in a form most suitable for incorporation into a relational database.

CONCLUSIONS

(U) Given the rigid constraints of producing bilingual digitized text for a relational database, the flexibility of the Kurzweil 4000 appears to make it the most effective device for the job. This should not be interpreted as a blanket endorsement of the Kurzweil 4000 over the other scanners but merely a best-bet choice for this particular scenario. Less versatile, but nevertheless still a viable alternative, is the IOC SPEEDREADER. The remaining scanning device, the Kurzweil DISCOVER 7320, is least suitable for the purposes described.

	DISCOVER 7320	KURZWEIL 4000	IOC SPEEDREADER
Model Type	Desktop	Stand-alone	Desktop
Cost	$11,950	$29,107 **	$5,495
Speed	50-60 cps	20-50 cps	30-40 cps
Font Size (points)	8-24	6-24	8-12
Graphics Capability	Y	N	Y
Scan Bound Book	N	Y	N
Language Lexicons	50,000 WD	33,000 WD	N
Trainable	N	Y	Y
Concurrent Editing	N	Y	N
Column Recognition	Y	Y	Y
Multifont Recognition	Y	Y	Y
Parsable Output	N	Y	Y
Scan Bilingual Text	N	Y	Y

** The cost for the Kurzweil 4000 includes the optional electronic tablet ($3097), automatic document feeder ($2655) and four language lexicons ($1425 each)

Table 1. COMPARISON OF OCR DEVICES (U)

ESTIMATES OF ACCURACY

(U) Table 1 provides an estimation of the accuracy one could expect from each of the optical character readers. Percentage of accurately-read characters is based on results of test material or represents computations derived from a comparison of characters within scripts. It assumes that all text is monolingual and of high quality.

PRODUCTION OF A DIGITIZED DICTIONARY

~~(S-CCO)~~ After preliminary testing of the three scanners was completed, R831 decided to begin production of a digitized version of a text for inclusion in a prototype of the [redacted] database system. Callaham's Russian-English Chemical and Polytechnical Dictionary was chosen as the candidate for this effort because of its high priority status in the queue of working aids for incorporation into the [redacted] database system and because of its high-contrast, good quality text. Being a bilingual dictionary, it also gives a true representation of the challenges R831 faces in converting hardcopy publications to relational database form.

(U) The Callaham is 852 pages long with two columns of text per page. Most columns contain 62 lines of text and an average of approximately 32 characters (including spaces) per line. This is roughly 3,400,000 characters of input, which produces output of approximately 4,000,000 characters. Included in the output figure are begin-end font indicators and multiple codes for certain individual letters. The text is consists of standard (Roman) English characters (approximately 58 percent), English italics (7 percent) and bold Cyrillic (35 percent). Special characters include diacritical marks (acute accent, grave accent, circumflex, tilde, hacek, diaeresis), degree symbol, percent sign, virgule (/), ellipses (...), em dash, superscript, subscript and Greek letters.

(U) The first step in the procedure for scanning a new document is to define the initial set up parameters. This process involves stepping through a series of menus in order to set the framework for training. The user is prompted to define a document name, training set name, training mode, lexicon, page incrementation option and use of super/sub scripts and underlines. Some textual ambiguity information is also required in order to help the scanner distinguish between 0/O, l/1 and I/l.

(U) After the initial parameters have been defined, a training set for the document is formulated. Training is the process by which the Kurzweil system learns to recognize the set of characters which constitute the document text. The machine is configured to the manual

training mode in which the operator's role is to review text character by character or line-by-line and verify that the images displayed on the screen are clear and well-formed. Training should not be done on partial or ill-formed characters. Those characters which do not meet the confidence level of the system recognition logic are displayed in inverse video and are called interventions. All interventions should be verified as correct by the operator or assigned the appropriate identification. All images, not just interventions, should be reviewed by the operator to ensure the training set is not corrupted with incorrect values.

(U) When the operator is satisfied that most of the text characters have been incorporated into the training set it can be copied to system memory for use in production. Training sets are stored in memory and can be used repeatedly as long as the characteristics of the text remain constant.

(U) There is also an automatic training mode which is used to analyze and display characters to the operator once a base level of recognition has been established, that is, after a training set has been created and production is in progress. An existing training set can be supplemented during production through the use of a special function key as long as the storage capacity of 432 images is not exceeded. Exceeding that limit results in a corrupted training set.

(U) Classification of fonts is also done during training. Fonts are numbered 0 through 9 and are flagged on the screen and in the output file as "<n" at the beginning of the font sequence and ">n" at the end. The predominant font in the text, which, in the case of the Callaham Dictionary, is standard English, is assigned font zero. Font zero is maintained only internally and appears in the output file without a font flag. Superscript, subscript and underlines are flagged "<s...>s", "<i...>i" and "<u...>u" respectively.

(U) With the establishment of a satisfactory training set, the operator can now begin the production process by stepping through the menus and setting the scanning parameters. Part of this procedure requires the operator to define page and column limitations by using the electronic tablet. This entails marking the upper left and lower right corners of each

	DISCOVER 7320	KURZWEIL 4000	IOC SPEEDREADER
Amharic	0	85	75
Arabic	0	5	3
Chinese	0	5	3
Czech	60	97	95
Danish	85	97	95
Dutch	95	97	95
English	95	97	95
French	95	97	95
German	95	97	95
Greek	50	97	95
Hebrew	0	97	95
Hungarian	70	97	95
Italian	95	97	95
Japanese	0	5	3
Korean	0	18	11
Polish	65	97	95
Portuguese	55	97	95
Russian (Cyrillic)	5	95	90
Spanish	95	97	95
Swedish	85	97	95

Table 2. Estimates of Accuracy

column of each page of text. When all the page/column boundaries have been defined, the material is ready to be scanned. The operator loads the pages of text into the feeder, or places individual pages or bound documents directly on the scanning window, and sets the optical scanning head into motion. For the Callaham, the pages were removed from the binding and scanned individually. In this case at least, placing the individual pages directly on the scanning window seemed to produce slightly better results than using the document feeder.

(U) Depending on the degree of accuracy required, the operator has a number of options for scrolling through the text as it appears on the screen. The "SCROLL UNLIM" option allows uninterrupted scrolling of text in the editor. This is the quickest way to scan a document but produces the least accurate output since corrections, changes or additions to the training set or output text can e made only bby accessing the file via a word editor or word processor.

(U) A second option is the "SCROLL GOOD" mode which allows scrolling to proceed uninterrupted as long as the rate of interventions (questionable images) is low. If the rate of interventions increases, operator verification is required.

(U) A third mode is the "SHOW (right arrow)" option which allows the operator to skip from intervention to intervention and make appropriate corrections or additions. Unfortunately, using this method alone does not allow for correction of those errors not appearing as interventions, a common occurrence. Other arrow keys allow the cursor to be moved one position at a time and help expedite the editing process.

(U) The final option is the "ACCEPT" mode which scrolls text one line at a time. The "ACCEPT" mode, especially when used in combination with the "SHOW (right arrow)" option and arrow cursor keys, produces the highest accuracy output but requires the most time since the operator is verifying both interventions and non"interventions.

POST-PRODUCTION EDITING

(U) It is estimated that unedited optical scanning of Callaham's Dictionary would result in an accuracy rate (per character) of 85 to 90 percent. Choosing the "ACCEPT/SHOW (right arrow)" scrolling options, thereby editing the document on a line-by-line basis during scanning, increases the accuracy rate to approximately 96-98 percent. But even such a modest error rate results in approximately 80,000 to 160,000 incorrect characters in the output. Three different methods were used to detect and correct these remaining errors.

(U) The most efficient method is a computer program which is written to reflect inconsistencies in the presentation of the various elements of information contained in the dictionary. For instance, the Callaham has an identifiable, finite number of abbreviations, always appearing within parentheses, which provide contextual information. It is a simple matter then to write a computer program to verify that all abbreviations within parentheses match a list of context abbreviations. Another way we used a computer program in editing was to develop a partial spell checker to help verify the orthographic sequence of dictionary headwords. Approximately five percent of the errors produced through machine scanning were identifiable programmatically.

(U) Another technique in editing errors is employing the Search and Replace functions of a word editor. The nature of optical character recognition, especially when applied to a large volume of text, often produces errors which appear in a consistent, repeated fashion. It is those errors which fall into this category that can best be edited using the Search and Replace functions. For example, in the Callaham the scanner often was unable to distinguish between the character sequences "f.", "fi" and "f" when appearing in italic script. As a result, the part of speech "prefix" was frequently rendered as "prefx". It is a simple matter, then, to globally replace all occurrences of the incorrect sequence using the Search/Replace function. The operator, however, must take care to ensure that the sequence being replaced is not a valid sequence elsewhere in the text. If global replacement is not possible, then replacing the sequence in question must be treated on a case-by-case basis.

~~(C-CCO)~~ Another instance of how the Search/Replace function can be used is when text, although technically correct in the output, needs to be modified to accommodate a database design. For example, since the Callahan has two narrow columns of text per page, words are often hyphenated. When this

output is incorporated into a database such as for [redacted] these hyphens must be removed so that an interrogation of the data yields comprehensive retrieval information. This problem is compounded, however, by the fact that many words need to maintain hyphenation. Further complication is encountered because the operator often cannot tell the difference between a word which should have the hyphen removed and one which maintains hyphenation. To illustrate, the average OCR operator may not know if a chemical term such as "hexamethyl-enetetramine" contains a hyphen because it is a compound word or if it is because of columnar limitation in the source document.

(U) Many different types of errors are encountered during digitizing, but generally they can be broken down into two broad categories: those caused by scanner programming and those resulting from problems with the input text. The predominant error by far is incorrect character recognition, that is, the optical scanner detects an image but assigns an incorrect value to that image. This occurs most often when the scanner is forced to perform a task it was not designed to do. The Kurzweil 4000 is intended to scan monolingual text in English, French, German, Dutch, Italian, Spanish, Swedish or Danish.

(U) By trying to scan bilingual text the machine is being forced to recognize characters in a language for which it has not been programmed. Nevertheless, scanning even bilingual text yields a reasonably high accuracy rate as long as the character sets for both languages are based on the Latin alphabet. For example, scanning an Italian-English dictionary is not a major problem for the Kurzweil 4000 because both Italian and English use Latin script. Italian has five characters which are not used in English and English has five characters which are normally used only in borrowed words in Italian publications. Scanning could be accomplished by determining the predominant language in the dictionary, initiating the lexicon for that language and teaching the optical reader to recognize the extra letters from the secondary language.

(U) Accuracy begins to suffer, though, when it becomes necessary to scan bilingual text having significantly different alphabets such as in a Russian-English dictionary. The only method of scanning text presented in non-Latin script such as Cyrillic is to utilize a transliteration scheme of Latin characters. This can create recognition problems for the scanner, however, since a single image might appear in both character sets and, therefore, have two values. An illustration of this is the image "C" which appears in both the English and Cyrillic alphabets. The scanner needs to assign one value when this image appears in Cyrillic and a different value when it appears in the English character set.

(U) Incorrect character recognition occurs also when images are very similar to each other. The problem appears to be compounded in bilingual text when multiple language fonts are used and one of the fonts represents a non-Latin alphabet. The Cyrillic letters И, Н, П, have similar images and are often indistinguishable to the scanner. The result is an error rate of approximately 10 to 15 percent which is correctable mainly through manual scanning of the output text. But recognition of characters with very similar images in the preprogrammed lexicon results in highly accurate output (at least 97 percent).

(U) Another fairly common error encountered in processing the Callaham is misplacement of the language font indicators. The Kurzweil 4000 often had problems determining when one font ended and another began, especially with a Cyrillic/English italics sequence. This is a very difficult type of error to detect in editing because the flaw does not always happen in a discernibly consistent fashion.

(U) Other errors caused by the scanner itself include incomplete character values (i.e., only two characters of a three-position code are returned in output), omission of certain characters, spurious insertion of characters, and lines of text skipped (rare).

(U) The digitized output of the Callaham also showed a significant amount of errors which were more a result of publishing errors as opposed to scanner interpretation of images. These problems included skewed text, misprints and misspellings in the publication, as well as downright erroneous information.

(U) Although the acceptable error rate varies from document to document, the operator usually will want to identify and correct as many of the errors as is practical. As the type of error becomes more obscure the likelihood that the error will be found decreases. Similarly, the amount of time it takes to find

DOCID: 4010026

the error increases. In a large publication such as the Callaham Dictionary, for which a high degree of accuracy was necessary, processing time (scan and edit) averaged approximately one hour per page of input. This produced an extremely low error rate, conservatively estimated to be less than one error per 1000 characters, which facilitated easy assimilation into a relational database.

ERROR COMPARISON

(U) Table 3 compares the type and approximate percentage of errors encountered while scanning the Callaham Dictionary as well as the methods used to correct them.

		METHOD	PERCENT OF CORRECTION	
Error Category	Percentage of Error	On-line During Production	Word Editor	Computer Program
Incorrect Character Standard English	1	90	5	5
Incorrect Character English Italics	15	70	15	15
Incorrect Character Bold Cyrillic	75	80	15	5
Incorrect Font ID	2	50	25	25
Incorrect Font Placement	2	50	25	25
Character omitted	2	75	20	5
Miscellaneous	3	75	20	5
Partial value				
Spurious Characters				
Text omitted				
Publishing errors				
Illegible text				

Table 3. Error Comparison

CRYPTOLOG has moved!

Mailing address:
CRYPTOLOG
P1 NORTH

DOCID: 4010026

From the Past

HARVEST Machine Support in the Publication of Working Aids to Consumers (U) -- Many consumers require listings and references as working aids which must be published and updated periodically. If a listing contains 9,000 records, for example, 300 additions and changes resulting from current analysis may have to be made to the basic listing every month.

Ordinarily, the original listing is published and distributed to consumers once a year. When additions and changes are compiled monthly, they are machine processed against the basic file through some file maintenance program. Work listing are then sent to the sponsor for the next month's updating. The sponsor usually rewrites the current changes and additions in a format suitable for presentation to the consumer and proceeds to type his own multilith masters. The consumer then has the burden of making pen-and-ink changes to his copy of the basic document.

Under a new HARVEST process, the changes and additions, after they have been used to update the basic file, are utilized to prepare a set of supplementary multilith masters. This is done by extracting from the newly updated basic file all records which have been affected. These extracted records are then arranged in exactly the same format and sequences as they appear in the basic document. These by-product masters are then sent to the sponsor along with his new listings of the basic file. He needs only to add his introduction and release them for publication. All monthly change files are retained in the machine system so that they can be accumulated to produce a cumulative master file with only the latest changes included. This, in effect, produces for the consumer, one current supplement containing all changes and additions to date. Obviously, he can then destroy his preceding month's supplement. For him to find the latest information, he need only look first in his current supplement. If he finds the record, he knows he need not look any further; he has the latest data. If he does not find it, he must look in his basic document knowing that the basic entry is still valid. This technique does away with pen-and-ink changes.

Multilith masters, as a rule, result in a rather bulky and awkward document. Since pen-and-ink changes have been eliminated, a use of multilith masters can also be eliminated by replacing them with #16 paper. As many as 108 records can be listed on the #16 paper, whereas the usual number of records on multilith is a maximum of 72. L24 photographically reduces the #16 paper image to a letter sized sheet - an 8 x 10½ inch page. The resulting publication is much more compact and usable. For example, in one publication, the multilith method produced 534 pages. The same product using the #16 paper resulted in a document containing only 152 pages. Incidently, in the multilith method, L24 estimated that 190 man-hours were required and the cost of printing and binding was $1,757.33 to produce 533 copies. Under the latter method, the man-hours required were 52, at a cost of $652.72 to produce the same number of copies. One hundred and thirty seven man-hours were saved and $1,104.60 were cut from the production cost. According to L24, the image area and number of copies should determine when #16 paper should be used. When the number of copies is small, and the format of the report (image) can be accommodated on standard multilith masters, the masters should be used.

Some working aids have elaborate introductory narratives. In some cases these have been put on magnetic tape as a separate file from which multilith masters or #16 paper listings are made, thereby saving the sponsor from typing his introduction.

The technique described in this article could be applicable to any machine process which has a file maintenance program.

[redacted]
C451 X-3710

P.L. 86-36

Henry E. Riley
C412 X-4221

Reprinted from
bits & bytes
C4 MACHINE PROCESSSING INFORMATION BULLETIN
Vol I, No. 3 July 1965

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010026

On writing an article

1. My object is to:

- ☐ Make a report on something that has been accomplished
- ☐ Call attention to something that is wrong
- ☐ Suggest a better method or idea
- ☐ Share a personal experience
- ☐ Enlist support
- ☐ Explain a process
- ☐ Ask a question
- ☐ Defend a principle
- ☐ Report news or announce a coming event
- ☐ Recognize an achievement
- ☐ Amuse and entertain
- ☐ React to something someone else has written
- ☐ None of the above, but something else, namely: _____

2. My working title is:

- ☐ A better way to _____
- ☐ Hurray for _____
- ☐ The fallacy of _____
- ☐ It's time to _____
- ☐ The scandal of _____
- ☐ Are we paying too much for _____?
- ☐ After _____, What?
- ☐ A proposal for _____
- ☐ What happened at _____
- ☐ Why I agree/disagree with _____ who wrote _____
- ☐ A funny thing happened on the way to _____
- ☐ None of the above, but _____

3. I will consider this, in my own mind, an open letter to _____ and will address to primarily to her/him/them.

4. ☐ This would be a particularly good time for such an article to appear because _____ *(or)*
   ☐ This subject is timeless

5. ☐ I am especially well qualified to write on this because _____
   (or, on the other hand)
   ☐ I want to speak up on this even though I am no expert on it, because_____

6. Some tentative suggestions for a final title are: _____
   _____
   _____

7. I think it would be most appropriate for publication in:

- ☐ CRYPTOLOG
- ☐ The Cryptologic Quarterly
- ☐ CLArion
- ☐ The NSA Newsletter
- ☐ PQS Update
- ☐ Vox Topics

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010026

LETTERS

To the Editor:

(U) A version of my trip report on the American Mathematical (AMS) meeting in Providence last August appeared recently in CRYPTOLOG, and, to my surprise, cause a controversy. Buried on p. 23, in a description of a talk critical of AMS by former presidential science advisor Edward David, was the following section, intended as a sarcastic criticism of the mathematical establishment that runs the AMS:

> Mathematicians must find better ways to attract young people to our field - NOT as currently, take it or leave it. The young have been leaving it in droves for adjacent fields . . . Most students think we aim at winnowing out the weak and grinding down the ungifted. [They are right. Most outstanding mathematicians view the world differently from David, not a mathematician. There is only a comparative handful of people in any generation capable of making important breakthroughs in theoretical pure mathematics. They are of interest to us. The rest are a waste of our time.] Academic education should be a pump, not a filter.

(U) My own views (and David's) are clearly represented by the last sentence. The "we," "our," and "us" are meant to be the sort of "outstanding mathematicians" that have power in AMS and that constituted David's audience, the people who are driving young people from the field. Surely it was never intended that "us" would be taken to mean NSA.

(U) Neither I nor anyone who knows me will take it that I think of myself as in the category of "outstanding mathematicians." I saw enough of them in graduate school to doubt I would want to be one of them if I could. While my brother-in-law in academia would not agree, I personally see little reason for society to tolerate people who undermine the general quality of university education because they care only about obtaining "breakthroughs in theoretical pure mathematics." While exposure to people doing research is part of training new mathematicians, it is only part of the process.

(U) I hope that this straightens out any misunderstandings. I do have to admit that when

I attend a math conference, I always feel a bit of conflict between my role as member (of rather mediocre abilities as any star of the AMS will freely tell me) of the mathematics society and my role as government bureaucrat seeing the considerable failings of the professional quality mathematicians from society's point of view. But I have long since stopped cult worship of the "great men" of mathematics, and taken a broader view that mathematicians, like everybody else, must justify their salaries by arguments that involve more than their talent at "glass bead games." In this I believe I echo Admiral Studeman's speech to the AMS in Phoenix.

David Harris, R512

(U) We regret to report the death of David Harris, a valued contributor to the technical health of NSA. An appreciation will be published in a future issue.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010026

To the Editor:

(U) The "anonymous" ***Cryptopoem*** published in the 1st Issue 1989 was in fact written by [redacted] sometime prior to 1971.

[redacted] *A532*

P.L. 86-36

EO 1.4.(d)

To the Editor:

~~(FOUO)~~ [redacted] mentioned in 1st Issue 1989, page 13, there is a copy available in the T53 Technical Library (FANX II, 968-8611), Accession Number S-170,832. There are also a few spare copies in the R51 Mathematics Library (FANX III, 968-8580).

(U) If there is sufficient demand for this document, we will look into another production run. In the interim, we see no reason why this document could not be reproduced as needed. Please address your inquiries to the undersigned.

[redacted] *R51, FANX III*

To the Editor:

(U) My initial reaction to [redacted] article "Where are Our Textbooks?" (CRYPTOLOG, 1st Issue 1989) was that Mr. Gaddy was out of touch with the operational world because there are plenty of good technical documents being written at NSA. I mentally started ticking off textbooks, thought pieces, working aids, and other types of technical documents whose absence Mr. Gaddy was bemoaning. Then I realized most of these examples had never been formally published.

(U) Why aren't a number of our best technical documents being published? Quite simply, the process is so lengthy and frustrating that many good analysts will not put up with the hassle. These people value their time and talents and prefer to expend their efforts on technical problems rather than on pushing a paper through the publication pipeline. Consequently, we have the situation where many analysts are not submitting their papers for publication but are just making copies for their colleagues. Such documents form what is a growing "underground" technical library.

(U) If we want our technical documents to be formally published and available to the general NSA technical population, we are going to have to make the publication process less painful. As long as we force analysts into a "publish or produce" dilemma, we are going to have a shortage of publications.

[redacted] *P15*

P.L. 86-36

Dear Charlie,

(U) Now that you're in P1 you've landed in clover, documentation-wise. P1 has a technical series and encourages its people to write for it. There's a minimum of fuss, and, moreover, each publication can have its own distribution.

(U) Other organizations have technical series that are similar.

[redacted] *Chief, P1*

P.L. 86-36

CRYPTOLOG

welcomes your letters and comments.

Send them to The Editor, P1, NORTH

NOTE THE NEW MAILING ADDRESS

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010026

Introducing Exciting Friedman BINGO!

Another boring briefing in Friedman? Never again, with the POLEMIC's new FRIEDMAN BINGO game, guaranteed to keep even those with the heaviest eyelids awake and on the edge of their seats during any talk.

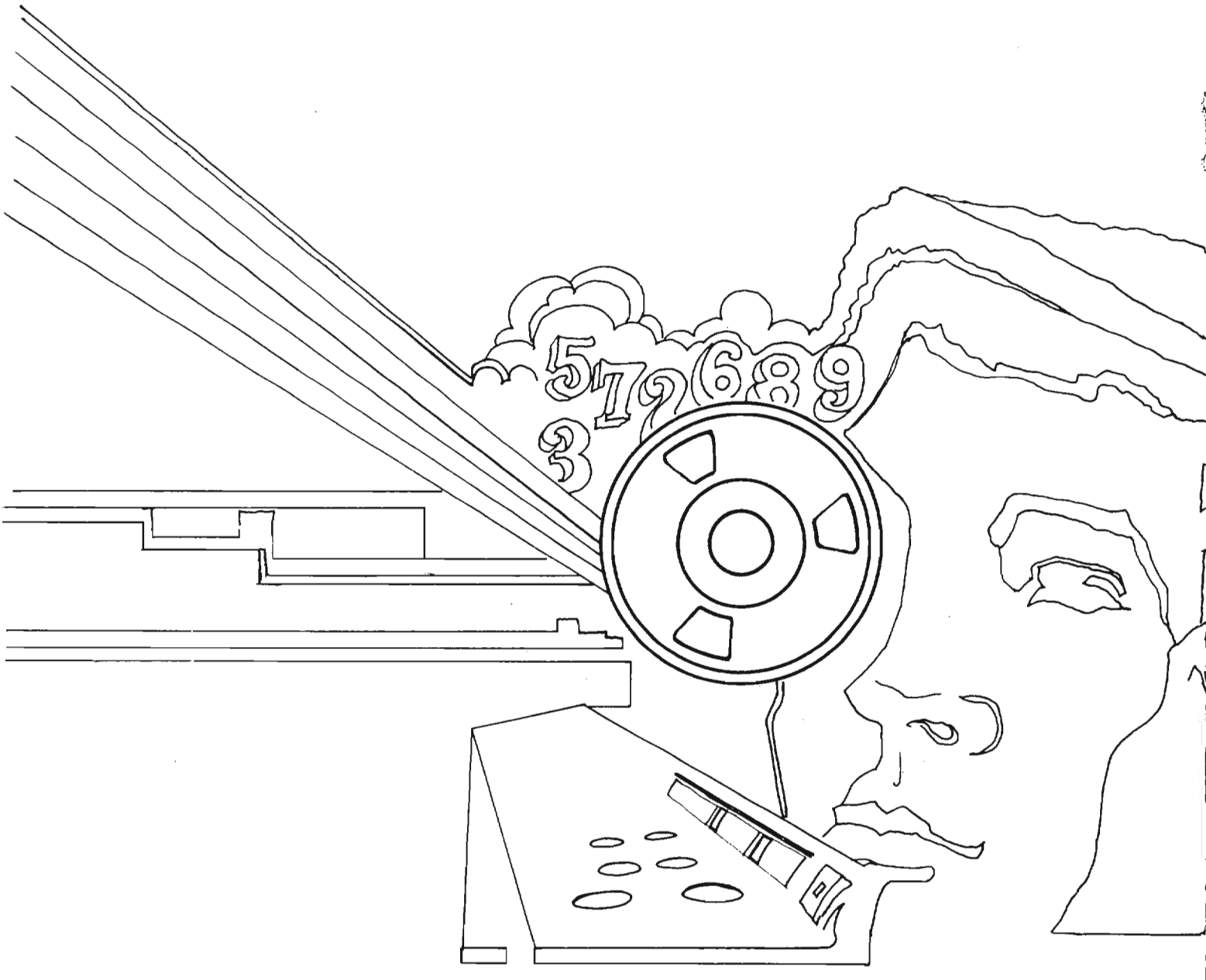
Just cover up a square any time you see one of the events on the FRIEDMAN BINGO game. Get five in a row (horizontally, vertically, or diagonally) and you're a winner!

Take FRIEDMAN BINGO to your next briefing. Never a dull moment again at CMI, HINT, KRYPTOS, CISI, CLA, or any other presentation!

B	I	N	G	O
Lights Dim	Phone Rings in Projection Booth	4 or More Interns in Your Row	Chair Squeaks During Talk	No One Asks Questions
Man Snoring in Back	Sign Language Interpreter Present	Slides Change without Speaker Saying "Next"	A Former Supervisor is in Attendance	Microphone Falls Off Speaker
Speaker Says "uh ..." Twice Consecutively	Slide Upside Down	FREE SPACE	Your Supervisor Walks in Very Late	Book Awarded is NOT Math-related
"Wiring Diagram" on the Screen	Speaker Adjusts Height of Lectern	You see Sign "This Entire Row Reserved"	2 People Asleep in Your Row	Speaker Pours Water From Pitcher
Number of People in Your Row Divisible by 3	Introducer of Speaker is Introduced	Speaker Begins With Joke	Someone Leaves Talk Early	Director is in Attendance

Courtesy of POLEMICS

~~FOR OFFICIAL USE ONLY~~


5 7 2 6 8 9
3

Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778
DOCID: 4012031

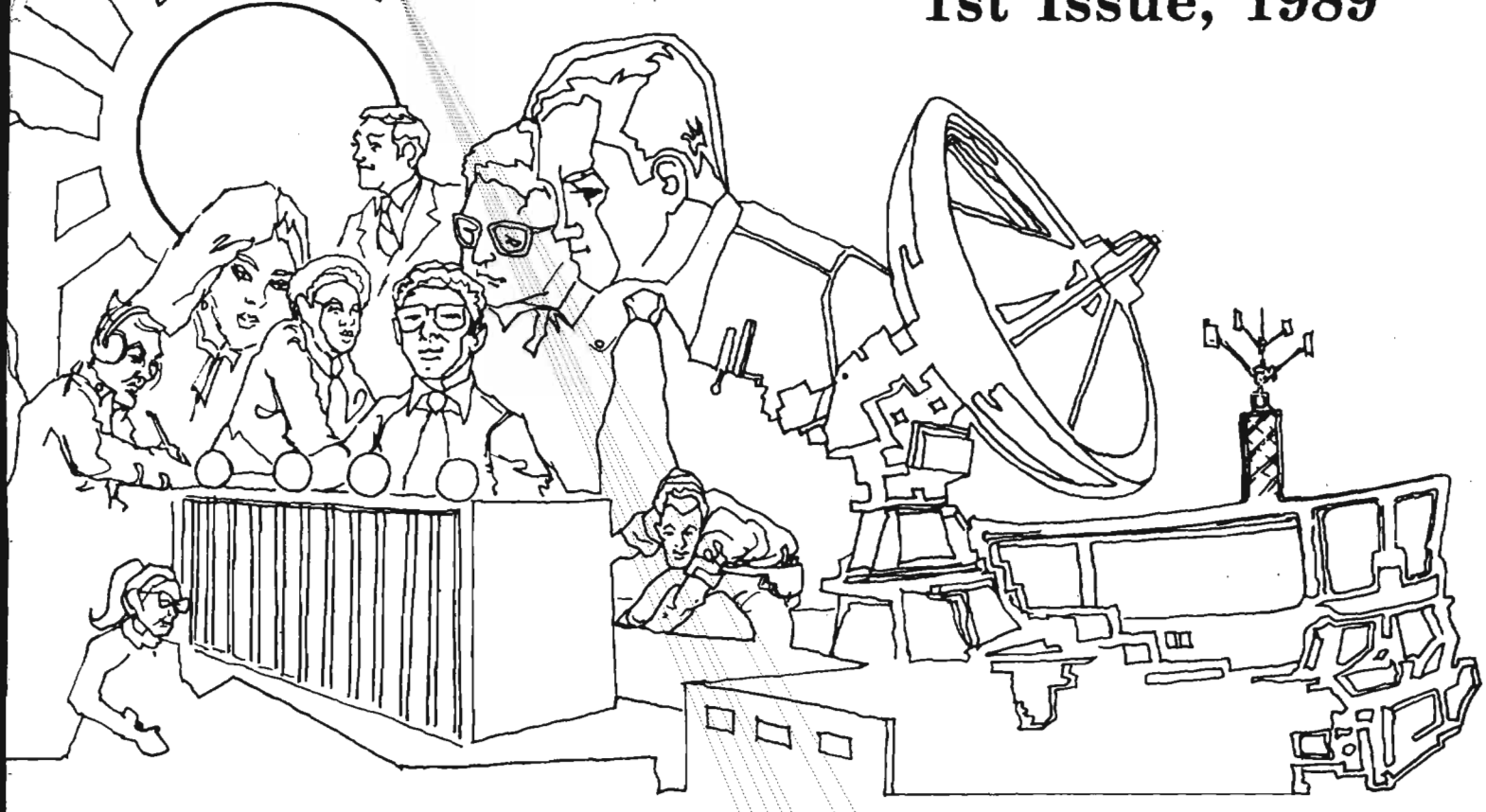
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

P.L. 86-36

1st Issue, 1989



WHERE ARE OUR TEXTBOOKS?	David Gaddy	1
QUOTE WITHOUT COMMENT		4
PROJECT TOTEMPOLE	[redacted]	5
GOLDEN OLDIE.		8
DEFSMAC'S 25th ANNIVERSARY.	[redacted]	9
BULLETIN BOARD.		10
OUR NEIGHBORHOOD: ASQ 20.	Vera Filby.	11
FROM THE PAST		12
ONE CRYPTANALYST'S ONE-FOOT SHELF	[redacted]	13
CONFERENCE REPORTS: DARPA ON LANGUAGE	[redacted]	15
MATHEMATICS	David Harris.	19
REVIEW: BOOKS ON SIGINT HISTORY	[redacted]	21
LETTERS		24
CLASSIFICATION QUIZ	[redacted]	26
BONUS PUZZLE: MINICRYPTS #2	Bill Lutwiniak.	27
NSA-CROSTIC No. 68.	[redacted]	28
ON THE LIGHTER SIDE		29

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

DOCID: 4012031

P.L. 86-36

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XVI, No. 1 ..... 1st Issue 1989

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Cryptolinguistics ..... (963-4740)
Index ..... (963-4814)
Information Science ..... (963-3456)
Information Security ..... (972-2122)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (963-4958)
Special Research ..... Vera R. Filby (968-5043)
Traffic Analysis ..... Robert J. Hanyok (963-4351)

Illustrators ..... (963-6234)
..... (963-3738)
..... (963-6423)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five)
(note: no 'o')

Always include your full name, organization, and secure phone; also building and room numbers.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, HQS 8A187
Please do not phone.

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

ABOUT YOUR SUBSCRIPTION

Maybe some day the Agency will have enough money to buy equipment that labels periodicals automatically and bundles them in zip code order, just like commercial magazines. Until then, we'll have to make do with a compromise, which in the case of CRYPTOLOG, is subscriber lists. The alternative is general distribution by organization.

Perhaps a few words about CRYPTOLOG's distribution are in order. The alphabetical subscriber list is on an XT. Each record shows Date of Information, Organization, Name of Subscriber. There is also an Organization list showing Date of Information, Organization, Building, Number of Individual Copies, and Number of Organizational Copies. When we're about to go to press, these two lists are fed into a program which generates a list of changes in distribution counts by organization for Distribution (Y16) and a merged list that is sent to a program on WINDMILL which generates a tape for printing the subscriber lists that you -- or your secretaries -- see. At this point the distribution is cast in concrete for that issue. We mail the sheets when it is time to proofread the Blue Line (the photo proof before it goes to press). Note that we go through this procedure for each issue.

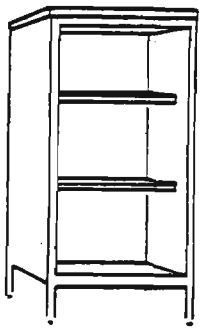
Theoretically, CRYPTOLOG should hit the streets a day or two after the subscriber lists reach you. But things happen. The magazine may be bumped by a higher priority at the Press. Or be held up in Distribution -- they count off the copies and bundle them by hand. So it may be ten days or so between the time your office receives the lists and its copies of CRYPTOLOG. Be patient. Wait. DO NOT CALL.

If you get too many copies, send us the spares -- maybe some other organization is short a few. If you don't get enough copies, WRITE, do not call, for more. And WRITE, do not phone, about a change of address. We just can't cope with the volume of calls.

If anyone has better ideas about distributing CRYPTOLOG, please send them on. We're always looking for a better way.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012031



WHERE ARE OUR TEXTBOOKS?

David Gaddy, DSC

~~(FOUO)~~ According to legend at the National Cryptologic School, Minnie Kenny arrived on the scene as the new D/ADT a few years back and asked to see the library. There was no school library, she was told. Her response was, "Nonsense! Who ever heard of a school without a library?" Suiting action to words, she established the facility that was dedicated in 1982 and is still maintained by T51 (albeit now in constrained space, along with other crowded NCS activities at the moment). A visitor to the School today might well ask "where are your textbooks?" Would the answer be the same, "we have none"?

(U) Back in the summer of '65 our former colleague, sometime journalist, and classic jazz pianist [redacted] deplored the lack of writing in an *NSA Technical Journal* article calling for the generation of professional literature. Ed's point, and a point with which most of us would agree upon reflection, is that professional literature is the outstanding characteristic of a profession. It is the means through which the profession is defined and through which the profession grows and evolves over time. It affords the opportunity to assert and to challenge, to advance ideas and to have them tested. It offers vitality; it encourages imagination and creativity; it exposes outdated thinking and procedures. It also does something else: In a 1988 memorandum to Agency seniors, enlisting their support in leading seminars, NCS Commandant Whitney Reed said, "lacking a more systematized institutional memory, we are heavily dependent on individual knowledge, recollections of lessons learned (or not learned), and acquired wisdom on the part of our seniors to guide the education of the next generation of Agency leadership." More careful attention to professional literature would, in large measure, supply the need for "more systematized institutional memory."

~~(FOUO)~~ What do I mean by "professional literature" and by "textbooks"? I mean both in the broadest sense: articles, papers, monographs, manuals of a certain type--information in a form that can be studied, retrieved for reference, passed about. In the flowering that took place after Ed's 1965 article, the National Cryptologic School Press was announced by Commandant Frank Austin (the Agency's history program was under the NCS in those days) and the issuance of "Special Studies in Cryptology" began. *The Cryptologic Spectrum*, a somewhat more "popular," but classified, quarterly joined the highly respected and often erudite *NSA Technical Journal*. A variety of specialty-oriented house organs flourished among the groups, key components, and learned organizations, compensating in part for what I recall as a concurrent decline in case histories and system solution reports, once SOP but dropped because of resource reductions and larger workloads. But we were writing and we were reading. "Letters to the Editor" columns and articles offering a different viewpoint from that of an earlier one reflected the challenge and response, and a depth and quality of thinking was seen that was frequently lacking in daily memoranda. Such writing was the grist for textbooks.

(U) By "textbooks" I mean those things we could read and study as professionals and that would serve as the basis for teaching. When it

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

involves a record of past practice, this means history. But history can be relevant–indeed, it generally must be to be tolerated in a government agency. (It is not that "the old way" was necessarily the right way, but it was a way, and it might save time and effort for a later generation to be able to reflect on it.) It would add a sense of continuity, a kinship with the past. For example, I still have among my papers Bob Benjamin's 1964 revision of the 1955 *Fundamentals of Radio Traffic Analysis*, suitably worn and dog-eared, as befits a textbook and continuing reference. What is its late 1980s' counterpart? The syllabus of TA-103? Are we too busy doing, to reflect on the whys and wherefores? What is it we need as "textbooks"?

(U) We need service biographies of potential role models for a new generation, biographies to increase our appreciation of our profession, and our heritage from the military services and their civilian colleagues. We need studies of "lessons learned"--and not learned. We need accounts of actions and operations well planned and smoothly executed, and how--and those that weren't, and why. (Yes, I know, this is asking a lot of an organization or an individual. "Self-criticism," the Communists call it.)

(U) We need critical, reflective, analytical studies that will draw out the mind as well as informing–articles of a type so often encountered in Naval Institute Proceedings, perhaps the best military example of the professional literature I mean. We need imaginative, futuristic, "impractical" thinking. We need reprints of quarterly articles or technical papers, "convenience compilations," such as the Friedman lectures, the Boak lectures, *Collected Articles on Code Reconstruction*, as compiled by Kate Swift and [redacted] We need "pop history," such as Ed Wiley's *On Watch*, produced by the NCS.

(U) What is our basic textbook today on C/A? On T/A? On reporting? On the concept of SIGINT support to a joint task force? On cryptology per se? Where are the writings for the apprentice, the journeyman, the advanced student?

(U) There is yet another consideration. With nearly a half-century or more behind us (depending on your choice of the starting date), we need doctrine–the distilled essence of our experience. We tend, rather, to have procedural instructions. Studies—professional literature—would contribute to the development of doctrine. At the present time new students at the National War College receive a stack of 14 books (one of them an historical novel, by the way) to start their professional library. As a self-check, what would constitute yours? What 14 "must read" texts would you suggest to a newcomer in our ranks? What 14 or so do you believe every professional here should have read?

(U) From the vantage point of four years at the NCS, concerned with introducing the new generation (and outsiders) to cryptology, as well as life-long learning for the professional, I am excited over the potential I have seen in the new generation, but I regret all the more the disorderly shape of the heritage we offer them. Many of the oldsters have forgotten or have selective memories; many of the youngsters haven't discovered what was or felt the absence of what might be. Our sheer bigness removes the youngster from proximity to the oldster and the opportunity to evesdrop (that is, learn from overhearing). As our profession has become more diverse and better known outside our fence, we've found unclassified writing about our once-concealed craft in books such as *The Codebreakers* and *The Puzzle Palace*, as well as journals, some good, some not so good.

(U) But who informs the professional or the neophyte which is which? It is all too human to reject what we personally know to be wrong, but tend to accept otherwise. We may accept and institutionalize untruths, such as the infamous Coventry bombing story. The continuing need for timely, informed book reports is obvious.

(U) Let me suggest some reasons for the state of things today: letting ourselves become too busy in other things; our incredible growth over the past decade; and, finally, not knowing what we're missing. We've been busy acquiring and defending. Our fascination with technology, and with "things" occupies so much of our time—another piece of equipment to master, another newer piece of software.

(U) We feel guilty taking the time to read and digest "unessential" classified matter in the office. We think about writing or rebutting, but don't take the time to do it. We see little evidence of reward for thoughtful exposition, of anyone caring. We often seem to be caught up

DOCID: 4012031

in careerism—ticket-punching—instead of honing the tools of our craft. Yet we bemoan the passing of the World War II generation and wring our hands about what industry calls "the assimilation of a new generation into our corporate culture," a culture we really have failed to define.

(U) There is probably another reason: The very computers that are enabling us to do easier word processing may be receiving the fruit of our individual creativity but denying it to others. Think-pieces probably reside in countless individual computer libraries. But professional literature must be generally accessible.

(U) For the most part, the professional literature I am describing must be classified. It must be generated, circulated, read, kept, and used at the office. It cannot be taken home for leisurely evening or weekend reading and contemplation, as with other professions. All the more reason, then, that it must be nurtured by a corporate concern. At the individual level that means allowing office time to read and reflect and write as part of our profession ... and not only permitting but encouraging subordinates to do the same. At the top it means having as Agency policy the advocacy and persistent defense of classified professional literature as essential to professional growth and, indeed, survival when the paperwork reduction campaigns come upon us. It means recognition of, and reward for, contributions to the professional literature. (Although there is provision for it in our Personnel Summary, I wonder how often that section is considered at promotion or selection time.) It means providing conveniently located and equipped study facilities with access to classified professional literature.

~~(FOUO)~~ It may also mean a better corporate effort to institutionalize study and writing. The war colleges have had study groups of one form or another; CIA has its Center for the Study of Intelligence under their training establishment. The idea is an attractive one—the opportunity for a selected few to reflect, study, listen; to write; to teach; and then to cycle back into the fray, leaving behind a heritage of sorts and emerging with renewed energy and matured knowledge. And we do have a potential: As among T54, P1, the Director's Senior Council, the Director's Fellows, and other pockets here and there, we have mission responsibilities for study, reflection, and exposition, just as we do at the NCS, including its Cryptologic Education Fellows, where the product of such thinking is so needed for education and instruction in the form of case studies and textbooks.

~~(FOUO)~~ While great strides have been made over recent years in improving information support to analysts and analytical units, we are only beginning to apply the same attention to the automation of our records, a project well underway in T5. In time that will support not only historical research and writing but enable the study of topics that cut across target or major organizational lines. That is the very sort of research needed in developing doctrine, theory, philosophy—areas in which we are weak. Once we had the P1-sponsored Cryptologic Collection, the pride of Lambros Callimahos. There researchers could find assembled most of what they might want, whether classified or unclassified—technical reports, historical studies, news clippings, books. They could search for precedent in system usage beyond their target area or find copies of earlier studies on the subject of interest.

~~(FOUO)~~ Squeezed out of the Main Library because of a space crunch, the remnant of the Cryptologic Collection is consigned to T54 care in SAB 2, but is not being sustained. The

The author, who chairs the NSA Cryptologic History Committee, solicits readers' views. Comments may be sent directly to him or to any other member of the Committee:

DDA	Robert L. Benson
DDI	Richard Proto
DDO	[redacted]
DDT	
DDPP	
DDPR	
DDR	Thomas H. Cosgrove
ADIL	[redacted]
ADT	Edward S. Wiley
GC	[redacted]
J	

Executive Secretary, Henry Schorreck, T54, NSA Historian

~~FOUO~~

P.L. 86-36

DOCID: 4012031

prospect of automating—and improving upon—that lost capability is a thrilling one.

~~(FOUO)~~ I must confess that, having spent six years across the street from T513, I had thought of "STINFO" as dedicated to the interests of Research & Engineering. Only recently did I learn of their indexing of internal publications. While it varies in coverage, STINFO would be my first place to check in seeking a bibliography of pertinent material on the subject of my research, and some day that index may be available online at my desk n,otwithstanding the horrible problem of access that must first be solved, given the caveats of the assorted documents received by T513.

~~(FOUO)~~ There are some hopeful signs that others are recognizing the need and addressing it within their spheres of interest. The IR Panel has found mutual benefit in assigning its interns to a tour in T54. Clubs and associations under the Council of Learned Organizations sponsor literary contests. Winners are recognized with publicity (sometimes cash) and publication.

(U) Publications such as *The Cryptologic Quarterly* and *Cryptolog* continue to manifest the qualities we need—one can only wish that they were monthlies, but the labor is much and the laborers few. Some serious studies are done in connection with courses at the NCS or elsewhere, but they may or may not see the light of day in general availability. [redacted] study of the personality types of Agency executives, done as a National War College project, later reached us in a modified, but concise and thought-provoking article in a publication concerned with the Productivity Campaign.)

(U) Perhaps, then, we are doing more to address the need, but are not adequately making the results known to the workforce. If so, the implications are the same: the professional literature I'm describing must, as I said, be generally available, and sufficiently current as to sustain reader interest. It must also be retrievable through subject matter, title, and author. That must be our goal. □

P.L. 86-36

QUOTE WITHOUT COMMENT

Extract from: "Reflections on the CA Essay Test" by Peter Jenks, *KEYWORD*, June 1971

The Question: 'Describe the attributes of a good working aid' was attempted by some 20 people. At least one respondent interpreted 'working aid' to be an assistant: e.g. a Crypt-Aide. A few described a 'good working aid' rather than its attributes. (Examiners survive these things and, it should be added, in a spirit of considerable generosity. Obviously responsiveness to the question is one of the things which must be assessed, but beyond that each essay is quite independently assessed in terms of its own premises.) Of the remainder, in any event, a surprising number of the respondents included an assertion much along these lines:

"When you are assigned to a new problem where nobody will tell you what the problem is, let alone how one goes about getting the answer, good working aids tell you what to do."

This was an unexpected answer. One's first instinct was to regard the point as marginal. Reenforcements from other essayists altered that; in the experience of far too many analysts it has proved to be of high importance. Granting this, one's second instinct was to accept the point as valid, giving credit accordingly, but to deplore the fact that it should be valid. What are our managers doing, or more to the point, failing to do?

The negative implication speaks for itself. Is it fair, though? Can it not be asserted that a manager, recognizing that a recurrent problem can best be dealt with by the use of well designed working aids which both conserve experience and preclude recurring reinvention, also recognizes that use of this aid is more edifying than hours of instruction? Can it not be asserted as well, that such an aid will not only enable the new analyst to go about his job on the most expeditious basis but, in addition that its very character will, to the inquiring mind, suggest the 'why' of that aid as well as the 'how'?

~~FOUO~~

~~SECRET~~

EO 1.4.(c)
P.L. 86-36

Project TOTEMPOLE

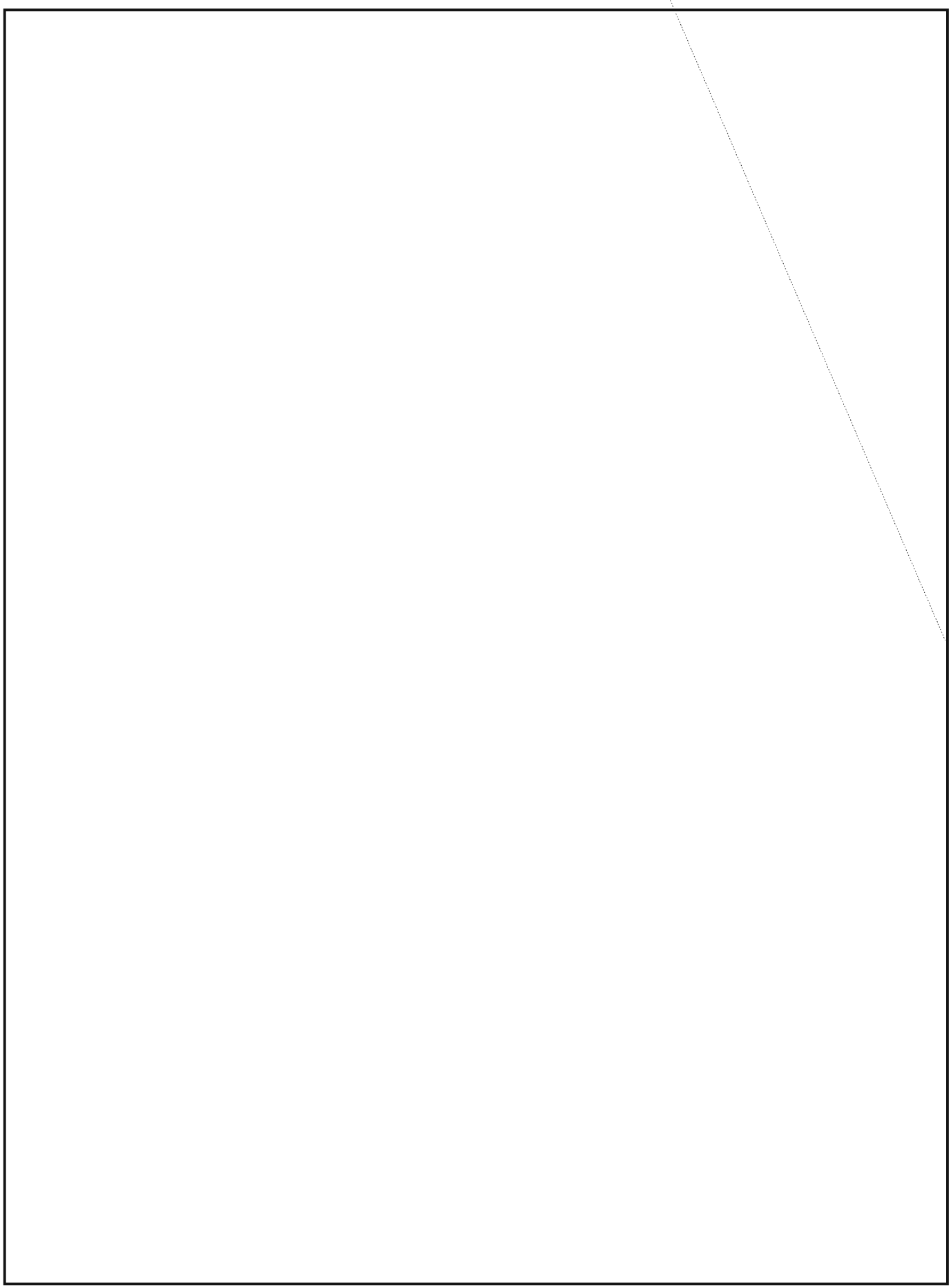
EO 1.4.(c)
P.L. 86-36

P.L. 86-36

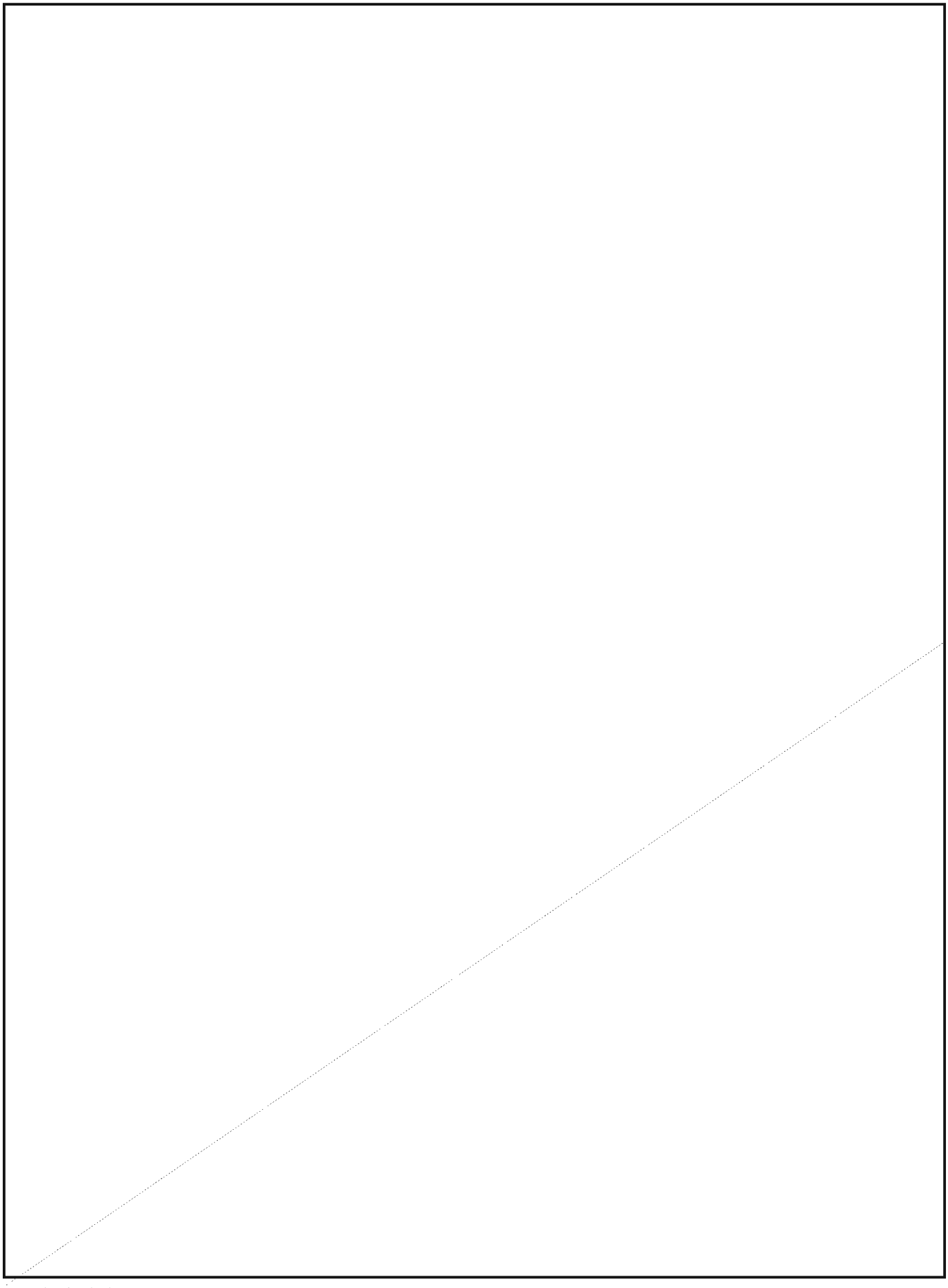
EO 1.4.(c)
~~SECRET~~
P.L. 86-36
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

EO 1.4.(c)
P.L. 86-36



~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~



EO 1.4.(c)
P.L. 86-36

Golden Oldie

CRYPTOPOEM

THERE WAS A LITTLE CIPHER
All digited and stuff,
Who was tricky as the devil
But not secure enough.

She had no nice "top secret" beaux
To take on lengthy trips
She just went out with press reports
And other "routine" drips.

Her fellow codes and ciphers
Used to huddle in the safe;
And whisper unkind things about
This naive crypto-waif.

Whenever she was put to use
The others wreathed in smiles
Would snicker at her format and
Her quaint digraphic styles.

Then one fine day she got revenge
(The others all turned red)
For turning to her catty friends,
She snapped her nulls and said,

"Your cryptographic raiment
Serves to keep you well disguised,
But *I'm* the one who's had the fun
For *I've* been comprised - - "

Author unknown.

~~CONFIDENTIAL CCO~~

DEFSMAC'S SILVER ANNIVERSARY

P.L. 86-36

P.L. 86-36
EO 1.4.(c)

[redacted] *Director, DEFSMAC, and* [redacted] *Historian, DEFSMAC*

(U) The Defense Special Missile and Astronautics Center (DEFSMAC) will celebrate 25 years of operations on May 3, 1989. DEFSMAC was established by direction of the Secretary of Defense in 1964 as a center to be staffed jointly by the Defense Intelligence Agency and the National Security Agency. The DIA contingent is a part of the Directorate for Collection Management (DC) while the NSA personnel are attached to the Deputy Director for Operations (DDO).

(S) The Department of Defense (DoD) charter for DEFSMAC specifies that it is to provide 24-hour surveillance of foreign missile and space activities, accomplish technical control of DoD intelligence collection systems directed against foreign missile and space events, provide technical support, including tip-off, to all DoD missile and space collection activities, and perform all-source current analysis and reporting on all detected foreign missile and space events based on initial site reporting. These responsibilities are carried out at a 24-hour operations center, with the support of a worldwide operational communications network, a dynamic, multi-discipline collection alerting and coordination effort, and analytic and technical data base resources.

[redacted]

EO 1.4.(c)
P.L. 86-36

[redacted]

(C) Among DEFSMAC's tasks is to provide earliest possible warning of preparations for foreign missile tests over the ocean to facilitate collection.

[redacted]

(C) The DoD community is increasingly looking to DEFSMAC for exercise participation, tip-off to new sensor systems, treaty support, timely provision of event-related information to operational commands, and collection coordination for strategic directed-energy weapon testing.

(S) The DoD's targets of interest in the foreign missile and space arena have grown dramatically in the past 25 years.

[redacted]

DoD and national level interest in the "Nth" country problem is demanding more time and resources as the potential grows for such countries to acquire ballistic missiles, chemical or nuclear weapons, and space capabilities.

(U) DEFSMAC occupies a unique location in the flow of initial site reporting. Its personnel perform very timely analysis of multisource

P.L. 86-36
EO 1.4.(c)

data, and identify and report significant activity. These actions serve to bridge the gap between collector and user, to support prompt action by the scientific and technical intelligence community, and to meet the time-sensitive information needs of operational consumers.

~~(C)~~ On 1 March 1989, after nearly two years of preparation, DEFSMAC began Space TACREP reporting to U.S.Space Command and others in support of Department of Defense Space Policy initiatives. This is the first step of the implementation of time-sensitive support to military commanders under a new function called Operational Foreign Instrumentation Signals Intelligence (OPFIS). Without this service, operational military commanders would not have access to time-sensitive information on the status of foreign missile and space weapon systems and to potentially significant improvements, or even, to entirely new systems that might be otherwise overlooked or whose analysis might be significantly delayed.

(U) On the occasion of its 25 Anniversary, the men and women of DEFSMAC would like to take this opportunity to salute the DoD, the Intelligence Community and Executive Agency, organizations we serve, and particularly our parent agencies, DIA and NSA. DEFSMAC's next 25 years promise to be even busier than its first 25. We look forward to continuing and improving the services and productive relationships. □

BULLETIN BOARD

FOR RUSSIAN LINGUISTS

(U) The complete Russian Handbook of Spoken usage is in press. It includes the first three volumes which were published individually (the letters A through Ф) as well as a new section covering the letters X through Я.

(U) The Handbook is an unclassified reference containing detailed information about the spoken Russian language. Entries are arranged alphabetically by the principal word in the phrase. It includes:

- constructions characteristic of the spoken language
- regional, uneducated, and other non-standard words and forms
- points of syntax and usage
- particles and combinations of particles

~~(FOUO)~~ Individuals in A2, A4, A6, E3, and the field should order copies through their organizations. Others may order copies **BY MAIL** directly from the author: [redacted] P16, HQS. **Telephone orders will not be accepted.** P.L. 86-36

LIBRARY OF UTILITY SUBROUTINES

~~(FOUO)~~ G964 has developed a library of utility subroutines to be used with the common data format discussed in CRYSCOM Recommendation #5, October 1988. The library has been successfully ported to SUN, JEPX, CONVEX, and IBM/AT computers. The source code has been written to allow conditional compiles so that a small, medium, or large version of the functions can be created on the AT.

(U) The library is modular so that programmers need select only those routines that are needed, thus keeping the program code to a minimum.

~~(FOUO)~~ Address your inquiries and suggestions to [redacted] 963-5317.

P.L. 86-36

DOCID: 4012031

Our Neighborhood: Airport Square 20

Vera Filby, E4

One bright December day a group of us from the Intelligence and Analysis Department of the National Cryptologic School rode over to Airport Square 20 to inspect our new quarters. We were to occupy the entire top floor of the latest Airport Square building and were to be the only occupants for an indefinite period of time.

We found a four-story brick and glass building graced by a fringe of trees that had somehow been allowed to survive from the woods that until recently covered the land hereabouts. Entering the lobby, we glimpsed the expanse of a softly lit atrium beyond the security desk. We took a rather childish pleasure in our ride up the glass elevator with its frame of sparkling lights. We emerged in the corridor alongside the atrium, and from there we looked down across a scene of hanging plants and banners.

The future office and classroom spaces, still bare of most of the furniture, were bright with light from the jalousied floor-to-ceiling windows on all sides. As we looked for our allotted spaces we paused to admire the scenery on the way, most especially the broad prospect from the north side and a clear view right down into the Inner Harbor. That was a surprise.

We moved in over the Christmas holidays, and early in Jsnuary the first students started to arrive. They seem to like it here too. For one thing, since the building is only one quarter occupied, parking is no problem. Some of them like to sit on the floor outside the atrium near the windows and enjoy the view while eating their lunch. The other day a couple of students were speculating on how many more Airport Squares there would be.

The answer to that question is not yet certain, but Mr. Gregory E. Masi of Dickinson-Heffner Incorporated, the developer, was glad to tell me when I asked him that during the next 7 to 8 years, 10 or 12 more buildings will be constructed, filling in the gaps in the 124-acre Airport Square campus and continuing the development of Airport Square Technology Park, located to the north and east. The name Airport Square Technology Park is now applied to the entire 300-acre project, which when completed will have created 3.5 million square feet of office space. Airport Square Technology Park is a totally integrated project, with the developer performing every part of it - land acquisition, development, design, construction, landscaping, gardening, marketing, financing, leasing, management, and maintenance.

Dickinson-Heffner's ventures in this area began in the mid-1960s with the building we knew as FANX-I when it was used for NSA operations. FANX-II was built as a warehouse. FANX-III was designed to NSA specifications, supplying 450,000 square feet of office space. Some years later Airport Square 1 appeared, and since then about a dozen three- and four-story Airport Squares have been built and occupied by a variety of tenants.

"Why does Airport Square 20 have four stories?" I asked Mr. Masi. "Why not two? Or five? Why not a highrise?"

"The answer to that is easy," he said. "We track the real estate market closely, and this is what people want - what they need." What they need translates to a first-class modern suburban commercial building which can provide a high quality workplace environment inside and outside. If it happens to have a greenhouse atrium, so much the better. When a building is constructed for the speculative market, it may have to be altered for the new tenant.

This happened with Airport Square 20. Before we could move in the floors had to be raised 9 inches to accommodate the wiring for our computers and especially for networking our long-awaited new computers. They were acquired to give us the means to develop computer assisted and computer based training and new applications for the continuing modernization and enhancement of our courses.

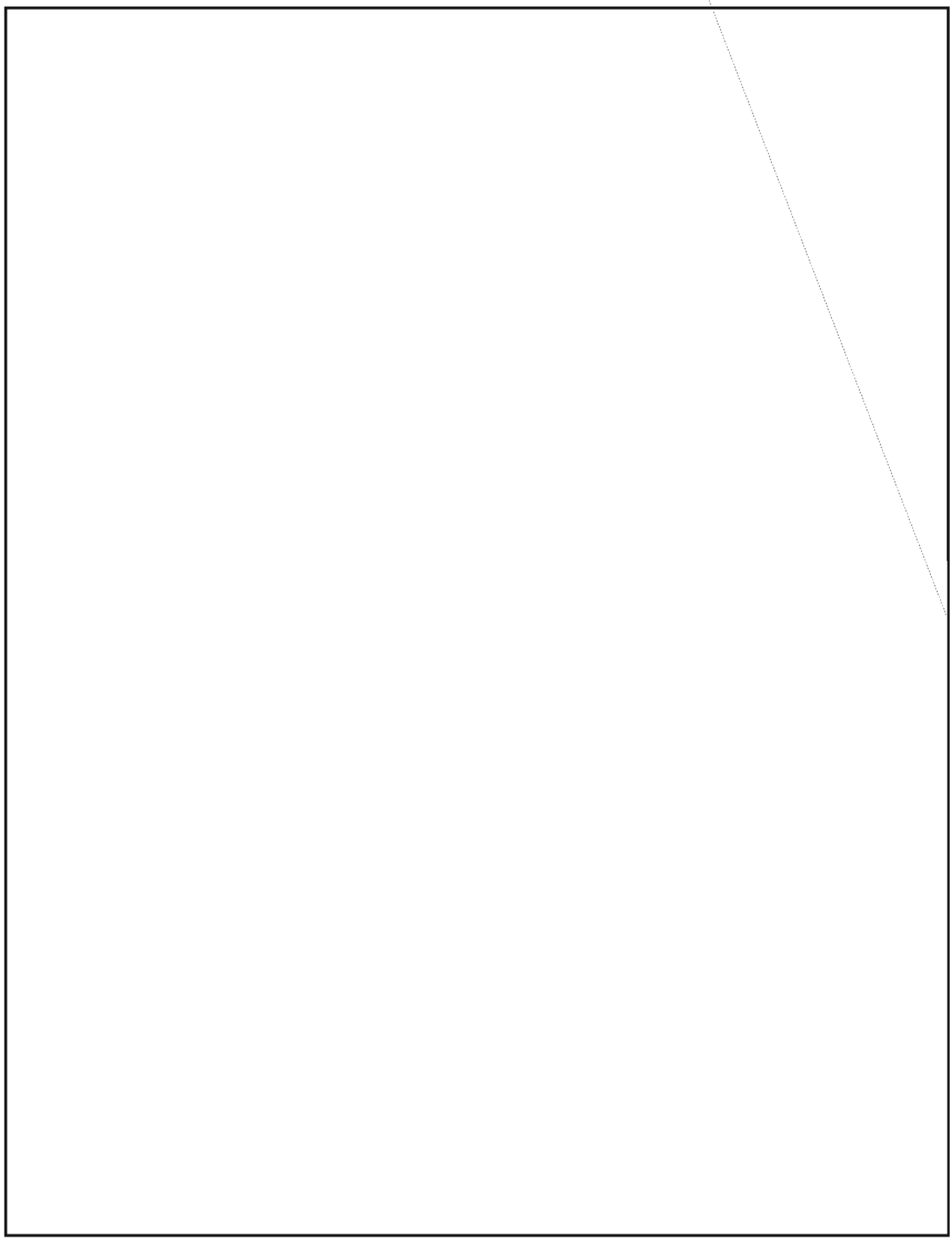
We are now wired up, settled in, and in business - and getting ready for new initiatives in the use of computers in training and education. □

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012031

FROM THE PAST

EO 1.4.(c)
P.L. 86-36



ONE CRYPTANALYST'S ONE-FOOT SHELF

Reprinted from KEYWORD, January 1972

P.L. 86-36

[redacted] *P16*

~~*This article is classified C-CCO in its entirety*~~

Can the cryppie build a personal technical library which is adequate for his needs, but small enough for ready reference without resort to indexing, and compact enough to fit in his desk? This is in essence what CA interns ask after a first encounter with the CA library. My answer to them is that it can be done, and I hereby offer some suggestions as a starting-point.

Technical references can be sorted roughly into three types: 1) the general works that one might want no matter what the assignment; 2) special working aids that pertain only to a certain target or type of system; and 3) guidelines or aids traditionally distributed to entities such as section or branch rather than to individuals, usually because they are scarce or because they require frequent updating.

We will consider just the first category, the basic books for the permanent library that will have to be dragged around with every move. It is understood that the cryppie has, for the duration of a particular assignment, the working aids that are purely local, such as Microbian word-pattern lists and Elysian pro-sigs. (He has a responsibility to see that working aids that he no longer needs are turned in or otherwise given a good home; the CA library, not the burn bag, is the proper repository, should the problem be dropped.) Machine ciphers, teleciphers and codes are not included in the basic books, not only for reasons of space, but also because the former two are usually worked in special sections and bookbreaking is seldom entrusted to the "pure" cryppie.

The publications below total almost a foot, and that's just about the amount of space left over in a desk file drawer when it's used to file legal-size folders; hence, the Basic Foot.

Remember, these are the suggestions of one cryppie. Others might make other choices out of the works now available, and new publications come out from time to time which must also be considered. Watch for the Cryptanalyst's Statistical Handbook, soon to be issued by P1, and Virginia Jenkins' textbook Practical Diagnosis, now in working draft form. That one foot of drawer space will hold an amazing amount of cryptologic knowledge, if carefully managed.

MILITARY CRYPTANALYTICS, PART I AND PART II by L. D. Callimahos and W.F. Friedman

Everyone knows of MC I & II, and to many a non-cryppie they are the Alpha and Omega of cryptographic literature because for years that's all that was generally available. Actually, together the volumes represent the Alpha; the Omega will be reached in that infinity where parallel lines meet.

MC I & II are the cryppie's bible, wherein are expounded the precepts of "the science of cryptanalytics and the art of cryptanalysis"; it is here that the foundations are laid for the solution of any cryptographic system. The two volumes also comprise a handy refresher for working long-forgotten systems. The junior analyst fresh from class, I know, will find it hard to believe that next year he will not remember the niceties of solution that are so vivid in his mind now.

STANDARD REAGENTS AND DIAGNOSTICIAN'S DICTIONARY by. I. J. Good (Blue Ribbon Series, Monograph No. 11)

This exceptionally well-written paper is considered by many cryppies as the best friend to take along when you lay siege to a difficult system; it will advise, comfort and sustain you, and keep you from straying. It contains specifics in compact form on how to go about things, including thinking, and so it is a practical handbook as well as good reading that invites dipping into. And the cryppie who seeks guidance in these pages when the prospects are gloomy will come away enlightened, and heartened and refreshed by the uplifting and optimistic tone.

This most valuable tome, unfortunately, is out of print, and no reissue is planned for the near future. If you do not have a copy, make friends with someone who does, especially if he is about to retire. Meanwhile, there's a copy in the CA library that you can read.

BASIC CRYPTOLOGIC GLOSSARY (a new edition is just out)

COMBINED GLOSSARY OF TRAFFIC ANALYTIC TERMINOLOGY

COMMUNICATIONS IDENTIFICATION GUIDE: Volume III, Operating Signals

The reasons for having the first two are obvious; the third book lists the Q and Z signals and their meanings. The three volumes fit nicely in a looseleaf binder.

ARS CONJECTANDI: THE FUNDAMENTALS OF CRYPTODIAGNOSIS by L. D. Callimahos (Blue Ribbon Series, Monograph No. 18)

It's neatly put in the foreword by Dr. Tordella: "This monograph represents a milestone in cryptologic literature: it is the first detailed and comprehensive exposition of the fundamentals of cryptodiagnosis, treating the techniques and procedures of manipulating data and recognizing and interpreting phenomena. Broadly theoretical in its treatment of the principles of diagnosis, it is applicable to both manual and machine cryptosystems, whether the diagnostic examination is performed by manual methods or with machine aids.

"Any cryptanalyst, whether he has two years; or 20 years' background, will profit from the study of this pioneering work. For the experienced cryptanalyst, it is an indispensable *vade mecum.*"

THE CRYPTANALYSIS OF CIPHER TEXT AND PLAINTEXT AUTOKEY SYSTEMS by L. D. Callimahos (Blue Ribbon Series, Monograph No. 19)

This monograph is an advance publication of two chapters of MC III, which is still in preparation. If you're working on unknown systems you need this, even though autokey isn't very common. Maybe it isn't common because it hasn't been found!

Watch for other parts of MC III as they come out in the Blue Ribbon Series.

COLLECTED PAPERS ON CRYPTANALYTIC DIAGNOSIS (S-194,074)

These interested papers range from the philosophical through the theoretical to the practical. Some are reprints and others are newly presented; all bear re-reading. Mr. [redacted] artical may shock some by its very title: "Is the Index of Coincidence Obsolete?" but it will prompt thinking about statistical tests in general. It should be mentioned that [redacted] appears to be the missing link between the mathematicians and the cryptanalysts, for his exposition is understandable to a cryppie who came in through the liberal arts. P.L. 86-36

THE SOLUTION OF TRANSPOSED CODE AND DOUBLE TRANSPOSITION SYSTEMS by H. D. Siegel (Blue Ribbon Series, Monograph No. 1)

In the foreword Mr. Rowlett said, "This paper by Helen Siegel, issued originally in 1948, is the first to be published [in the Blue Ribbon Series] because of its established reputation as an authoritative reference in dealing with transposition systems." It still is the authoritative reference.

RYE GUPPY MANUAL FOR CRYPTANALYSTS

The GUPPY programs give every cryppie the equivalent of 100 top-flight, speedy, accurate and indefatigable crypt aides 'round the clock. The manual also serves as a resident consultant–just by reading through the descriptions of programs a cryppie may find another was to study phenomena or even another approach to the problem.

LOOSE LEAF BINDER, *Ad Lib.*

This is probably the most valuable item in your collection, for it contains your own selection of handy-dandies. [redacted] Whatever the contents, its dog-eared appearance proclaims it as your nearest and dearest. This is what you save in a fire!

P.L. 86-36

DOCID: 4012031

Conference Report

P.L. 86-36

DARPA Speech and Natural Language Workshop
February 21-23, 1989, Philadelphia, PA

Reported by: [redacted] *P16*

Several Agency personnel attended the Spring DARPA Speech and Natural Language Workshop which presented ongoing research results and projections for DARPA-funded programs. The current budget for this research area is $11M and will be cut by 15% for the coming year. In FY90 speech research will account for 75% of total budget of the Speech and Natural Language Division, while the remaining 25% will be applied to Natural Language research programs. Some attendees explained this discrepancy in terms of the new role of natural language research in speech processing.

A new program, entitled WHISPER, will provide an additional $10M over the next three years. WHISPER is jointly funded by NSA and Rome Air Defense Center (RADC).

[redacted]

The following notes summarize conference activities. Interested individuals can contact P16 to obtain copies of related papers and for further information.

OVERVIEW OF SPEECH RECOGNITION

J. Makhoul: BBN Laboratories Incorporated

Areas of speech recognition are focused on the transcription of speech into words. Speech Understanding (SU) includes actions based upon the speech such as data base transactions and message gisting, and require natural language processing capabilities. This is an area of research that needs more emphasis. Without Natural Language Understanding (NLU), Spoken Language Systems (SLS) are limited. Computer architectures and software are necessary for real-time speech processing functions. More research is required on the topic of spoken language acquisition and modeling. Training opportunities in speech and language processing for undergraduate students should be expanded. There is much attention to Air Traffic Control (ATC) as a model for defense applications.

OVERVIEW OF NATURAL LANGUAGE

M. Marcus

Past research focus has included augmented transition networks, natural language interface (NLI) to database systems, and expanded context-free parsing. There is a DoD thrust on replacing query languages with NLI. Current areas of research are focusing on unification grammars, lexical functional Grammars, computational semantics and discourse analysis. Much research is depending on a wide range of *a priori* knowledge about the world or operational domain. New research should focus

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012031

on prosody for SLS, machine translation (MT), stochastic and symbolic techniques for learning grammar. The Japanese have a major effort in MT that will produce a wave of commercial natural languge products soon. DARPA does not have an MT program.

TUTORIAL on NATURAL LANGUAGE

Grishman, New York University

Natural language technology is used to produce man-machine interfaces (MMI) and for automated message processing. There are two distinct views, computational and theoretical. Two major goals are syntactic analysis and semantic analysis. The former is more feasible. Semantic analysis requires an experiental base of real world knowledge in order to be effective.

TUTORIAL on SPEECH

E. Neuberg, IDA, Princeton

Neuberg presented an overview of articulatory phonetics, acoustic phonetics, and phonology. He then provided a technical introduction to speech recognition.

INVITED TALK ON PROSODY

Pierrehumbert

Pierrehumbert delivered the invited talk on prosody. She demonstrated that prosodic features convey semantic and pragmatic information. She also showed that phonological phrasing does not always match syntactic groupings. In light of the role that prosody plays in understanding spoken language, Pierrehumbert suggested that speech recognition systems be built in narrow domains so that these systems can attempt to incorporate the systematic use of prosody.

PERFORMANCE EVALUATION

Natural Language Evaluation Workshop: Palmer, Unisys

Two methods of evaluating natural language processing (NLP) systems were presented. The black box method analyzes user viewable input/output, modularity and the man-machine interface. The glass box evaluation method considers a systems underlying theory, efficiency, and extensibility. The meeting was successful for testing syntactic systems but no agreement on semantic testing could be reached.

DATABASES

Text Collection: Marcus, U. of Pennsylvania

There is an emphasis on collecting test corpora of text. There are many different sources offering free but licensed text corpora for use in the research community.

Spoken Language: Doddington, Texas Instrument

Efforts to assemble a data bases of spoken language examples will receive 1.5M dollars over five years. There is a new effort to collect spontaneous speech examples in different scenarios.

INTEGRATION OF SPEECH AND NATURAL LANGUAGE

BBN: Stallard, Roukos

Because understanding spoken language requires actual understanding of language, BBN is Integrating its natural language component with MIT's speech recognition system. Basically, itsr system takes a word lattice as the output of a speech recognition system and then uses its natural language component (syntactic, semantic and pragmatic components) to identify the input sentence.

Stanford Resarch Insitutute International: Moore

SRI is attempting to integrate the architectures for speech recognition (SR) and natural language processing (NLP). Because of problems with word lattices and a serial connection betwenn SR and NLP components, SRI is using a dynamic grammar network. In this system, a natural language parser incrementatlly generates a grammar state transition table used in the Hidden Markov Model (HMM) speech recognition architecture.

University of Pennsylvania: Steedman

The University of Pennsylvania is investigating the integration of syntax and entonation in a combinatory grammar because of the inadequcy of present theories of syntax for processing speech. They propose using a combinatory categorial grammar which provides the notion of a syntactic constituent that is the same as

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012031

the notion of a sense-unit in a recent theory of intonation.

Carnegie Mellon University: Ward

CMU is just beginning to research recognition of spontaneous speech. Because of limitations of current recognizers, they will use a HMM work recognizer and create a phrase lattice. Syntactic constraints will operate locally and semantic globally. This is a system which will use a tighter grammar at the recognition level and produce a phrase output.

MIT: Seneff

MIT is developing TINA, a natural language system for speech understanding tasks. The system integrates ideas from Augmented Transition Networks and Lexical Functional Grammars. Probability assignments on arcs provide the basis for a best-search parsing strategy.

Texas Instruments: Hemphill: Picone

MIT is researching the integration of natural language models with statistical probabilities in speech understanding. They are using a chart parser with stochasitc regular grammar in combination with rule and observation probabilities.

Carnegie Mellon University: Young

CMU is using a higher level sources and constraints to predict content and thereby reduce complexity in speech recognition. These sources include the dialog model, task semantics, general world knowledge and user knowledge.

NATURAL LANGUAGE RESEARCH

New York University: Grishman

NYU discussed its telegraphic speech handling system, PROTEUS. Basically, a general English grammar is relaxed, allowing the omission of subject and preposition. To control relaxation, the system applies local semantic parsing and imposes a penalty for each omission.

University of Pennsylvania: Joshi, Webber

Joshi is studying the equivalences of grammars and lexicalized tree adjoining grammars. In a tree adjoining grammar, each lexical item has its own tree. Once the trees are identified, the trees are adjoined. Webber is researching cooperative response generation and discourse phenomena, particularly clausal reference.

Unisys: Palmer

PUNDIT is Unisys" natural language understanding domain specific system. Presently, the system handles about half of the input data composed of casualty report and rainform messages. Developers are extending the linguistic coverage and building tools for development. They are also working on interaction among the syntactic, semantic, and pragmatic components and are creating a more sophisticated interaction with knowledge bases.

SRI: Hobbs

TACITUS is a message understanding system which extracts information for database updating. Basically the abductive inference scheme in the system produces a logical form of a sentence in the message and then tries to prove it. For this system, interpretation of a text equals the minimal explanation of why the text would be true.

BBN: Bobrow

A major problem in applying natural language systems to different applications is the cost. To reduce the cost involves a) reducing the amount and complexity of application-specific knowledge, b) matching the interface to user capability and information needs, and c) reducing marginal costs. To reduce the cost of porting their natural language interface to a new database, BBN developed Knowledge Acquistion (KNACQ).

IBM: Byrd

IBM is developing a system to disambiguate dictionary entries. The system would hold word senses in a hierarchy and some information necessary from the context for disambiguation. This would be a lexical knowledge base, not a world knowledge base.

BBN: Crowther

Crowther is building a database from on-line reference works, like dictionaries and encyclopedias. He is researching the procedures

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012031

for building databases and retrieving information from databases.

Information Sciences Institute, UC: Kasper

ISI is developing a more efficient means to link appplications (expert systems) to PENMAN, their text generation system. A subordination tool to coordinate knowledge in Penman and a Sentence Planning Language (SPL) are now provided.

UC at Berkeley: Wilensky

Wilensky is developing a natural language interface to help UNIX users, called UNIX Consultant. Presently, Wilensky is working on knowledge acquisition for the project.

New Mexico State: Hartley

Researchers have made three proposals to DARPA, two AI projects (model generation reasoning and resolution of conflicts in belief systems) and a project to evaluate parsers.

PERFORMANCE TASK PROGRESS

CMU: Rudnicky

CMU researchers are developing a speech recognizer (SPHINX) and an interface for a spreadsheet task.

Dragon Systems: Baker

Dragon Systems is developing a system for interactive transcription for any subject. The system will have an open vocabulary and interactive error correction.

Unisys: Dahl

Unisys is developing a spoken language interface to an expert system (KSTAMP) for system maintainance.

MIT: Glass

MIT is developing a system called Knowledge Navigator. The system will allow the user to locate objects within an area and give directions to locations within the area.

BBN

BBN is developing a spoken language system to make database queries. The system will be developed from an existing database and a real-time speech recognizer. The task domain is personnel records.

SRI: Price

SRI is developing a spoken language system for travel planning.

TECHNOLOGY TRANSFER

BBN: Bates

BBN ported PARLANCE (a natural language interface to SQL) to a Navy database by using a porting tool called LEARNER. LEARNER creates the domain-dependent knowledge bases that PARLANCE needs.

Dragon Systems: Baker

Dragon System discussed a number of different applicatons, some of which were successfully transferred to the commerical applications for which they were originally designed.

IBM: Davis

IBM has developed a real-time 20,000-word speech recognition system called TANGORA. In this study, IBM attempted to identify performance factors in order to develop behavioral stratagies to improve the users' interaction with the system which requires some user speech modification.

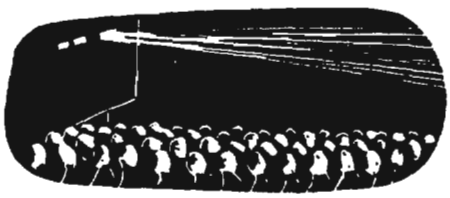
ANSWERS TO

CLASSIFICATION QUIZ, p. 26

1. e
2. d
3. d
4. a
5. c
6. e
7. a
8. d
9. c
10. b
11. a and e
12. b
13. c

~~FOR OFFICIAL USE ONLY~~

EO 1.4.(c)
DOCID: 4012031 P.L. 86-36



The Fourth SIAM Conference on Discrete Mathematics, San Fransciso, June 1988

Reported by: David Harris, R51

~~(FOUO)~~ This was an outstanding conference on discrete mathematics, with many talks of interest to the Agency. We should continue to attend such conferences in order to gather the fruit being made available so cheaply. We should also look into some of the consequences. I suspect there has been some effect from Agency participation in conferences, in the direction of convincing academics and mathematicians from industry to see us as human. We also had the usual variety of informal discussions with outside academics.

(U) Technical highlights included:

- (U) A talk by Carl Pomerance on the use of number theory in cryptology.
- (U) A session on applications of number theory, with talks by Odlyzko (Riemann Hypothesis), Lagarias (multidimensional continued fractions), and Sarnak (Ramanujan graphs).
- ~~(C)~~ A session of invited talks on cryptology, including talks by McCurley (discrete logarithms), Goldreich (zero knowledge), and Crepeau (secret sharing). The McCurley talk was particularly alarming, in that it stressed practical wisdom.
- (U) A somewhat disappointing session of contributed talks on cryptology, including talks by McCurley (Buchmann-Williams cryptosystem), Bailey (Ferguson's algorithm for multidimensional continued fractions), Elia (application of linear error correcting codes to communications security), and Shoup (factoring polynomials over finite fields with a minimum of randomness).
- ~~(C)~~ A session on the use of Cayley graphs in communications networks, including talks by Cooperman, Fellows, Krishnamurthy, Blaha, and Faber. [redacted]

A talk by North on the use of graphics to simplify lattice structure.

- (U) A session of invited talks on irregularity and discrepancy, featuring talks by Spencer, Voigt, and Niederreiter. Possible applications include looking for non-randomness in apparently random data, designing super-flat sequences (especially for use in numerical analysis), and tests of randomness in general.
- ~~(C)~~ A talk by Wilf on generalizations of the Gray Code Problem, in particular relating such questions to the existence of hamiltonian cycles. [redacted] Their various generalizations are also of interest.
- (U) A talk by Ron Graham on quasi-randomness as a replacement for the intractable concept of random graph.
- (U) A session of invited talks on codes and dynamical systems, featuring talks by Marcus and Ashley. These dealt with sliding-block decoders, a generalization of trellis codes.
- (U) A poster session featuring work by Weinstein (de Bruijn sequences), Bart Rice (characteristic sequences in characteristic q), and Maffioli (RPP algorithms for NP-complete problems).

P.L. 86-36
EO 1.4.(c)

Problem Session

(U) At the Problem Session held Tuesday night and chaired by Peter Winkler, twenty open problems from academia were presented on which they would like to solicit research.. Later, a handout was distributed giving the problems that were raised at the session. Only a single problem was answered cold at the session - and that by Andy Odlyzko (The guy is smart!) The following is a brief summary of the problems with their sources at the conference (which may not be their true originators):

1) (Grinstead) What is $\lim_{n\to\infty}$ Pr(random partition of 2n is graphical)?

2) (Voigt) Given the lattice of subspaces of an n-dimensional vector space over GF(q), can the levels k through l be covered with few intervals?

EO 1.4.(c)
P.L. 86-36

DOCID: 4012031

3) (Richey) Can the edges of planar graph be partitioned into two pieces each of which is outer planar? series-parallel?

4) (Duffus) Let H be a hyperplane of $L_n(q)$, P a point not in H. Can the spaces not comparable to either be partitioned into $q^{n-1}-1$ copies of $L_{n-2}(q)$?

5) (Kleitman) Let $\Sigma x_i^2 \leq 1$; prove that at least half of the sums $\Sigma \varepsilon_i x_i$, where $\varepsilon_i = \pm 1$, have magnitude ≤ 1.

6) (Kleitman) Let 2n candies be placed on the vertices of an n-cube. You may pick up two candies from a vertex, eat one, and put the other down on an adjacent vertex. Prove that you can always get a candy to the origin.

7) (Tovey) Given a real square matrix, how many of its entries need to be examined to find a saddle point?

8) (Wilf) Fix n and let f(j) be the number of ways of expressing the identity permutation on n letters as the product of j transpositions. Find out anything about f(j).

9) (Tzvieli) (solved by A. Odlyzko) Let $x_1,...,x_n$ be consecutive integers none of which is prime, for which a k exists satisfying $\gcd(x_i,k)>1$ and $\gcd(x_i,k-1)>1$, for all $1 \leq i \leq n$. Find max n or show n can be arbitrarily large. (AO shows the latter!).

10) (Kezdy) Fix d and let G be the (2d-2)-regular graph on Z/n, $n > 2d-1$, given by $x \sim y$ iff $|x-y|<d$ or $|y-x|<d$. Find the smallest induced subgraph H such that $\delta(H) \geq d$.

11) (Ullman) Consider the disjunctive product GxH of two graphs. Then $\chi(GxH) \leq \chi(G)\chi(H)$ is known. Define $\chi(G|F) = \chi(GxF)/\chi(F)$. Conjecture: $\chi(GxH|F) \leq \chi(G|F)\chi(H|F)$.

12) (McCanna) Information is inserted into a vertex of an n-cube at time t = . At time t=2 it spreads to all neighbors of the vertex, and can be inserted again at a second vertex. Let f(n) be the minimum time to inform all vertices. Prove f(n) = the greatest integer at most equal to (n+3)/2, so that you can do no better than insert at P, then at the antipode of P, then wait!

13) (Hurlbert) What is the largest (should this be *smallest*?) $l \leq k$ for which the levels l and 2k+1-l of an (2k+1)-cube induce a Hamiltonian subgraph? (it is well-known that levels k and k+1 work)

14) (George) Let $A = (a_{ij})$ be the adjacency matrix of an arbitrary n-regular graph. Can you replace the 1 in position i,j with a number b_{ij} between 1 and n such that (1) $b_{ij} \neq b_{ik}$ for $j \neq k$, and (2) $|b_{ij}-b_{ji}| \equiv 1 \pmod n$ whenever $a_{ij} = 1$?

15) (D. West - from Maurer, Wagstaff, Slater) For what n is there a Gray code on the n-cube such that the coordinates changed at successive steps are always adjacent? (This is the well-known lamplighter problem that I wrote up in my trip report for the Boca Raton conference many years ago. I got Ralph J. interested in it then. Not much progress has been achieved.) This is believed true for small n, but false for n = 8. Any more information?

16) (Tovey) What is the complexity of finding, in a weighted complete graph a Hamiltonian circuit whose weight cannot be lowered by a two-edge exchange? (i. e. a TSP tour that is 2-optimal exists, but can we find it in polynomial time?)

17) (Tovey) Call the binomial coefficient C(m,k) proper if $1 < k \leq m/2$. What is the greatest n such that there exists a number with n proper binomial representations? Can there be infinitely many such? (e. g. C(16,2) = C(10,3). Erdös claims to have a number with 8 or 9 such representations!)

18) (Trotter) Let P be the poset of vertices, edges, and faces of a 3-dimensional polytope. It can be shown that $\dim(P) \leq 6$; what is the correct upper bound?

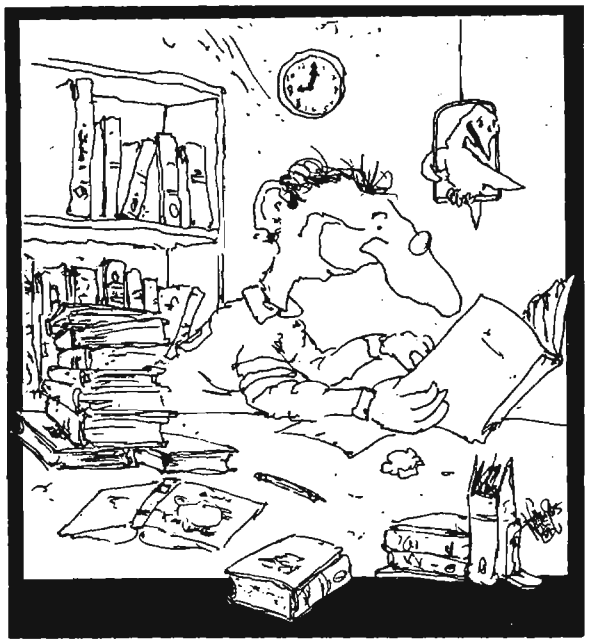
19) (Spencer) Let $A = \{S_1,S_2,...\}$ be a family of k-sets such that the degree of each ground element is D. Let $\chi(A)$ be the least m such that A is the union of m disjoint subfamilies P_i, and let $\phi(A)$ be the greatest m such that A is the union of m subfamilies C_i each of which is a covering subfamily. Then $\phi(A) \leq D \leq \chi(A)d$, and it is known that $\chi(A) = D(1+o(1))$ implies $\phi(A) = D(1+o(1))$. Can this implication be reversed?

(20) (Grinstead) The average number of Hamiltonian paths in an n-tournament is $n!/2^{n-1}$. Conjecture: for n odd, all regular n-tournaments beat the average!

DOCID: 4012031

Review

BOOKS ON THE HISTORY *of* SIGNALS INTELLIGENCE



Reviewed by: [redacted] *A28*

P.L. 86-36

There are a few books on the history of signals intelligence of particular significance that I recommend to friends who ask about them.

By far, the best book I have ever read on the use of signals intelligence in war is Ralph Bennett's *Ultra in the West: The Normandy Campaign 1944-45*. Bennett worked at Bletchley Park1 from February 1941 to the end of the war as a reporter in Hut 3. What makes the book particularly useful is that Bennett, a Cambridge don who specialized in medieval history, wrote it not only from memory of his activities during the war but also from decrypts of German ENIGMA made available to the public for the first time at London's Public Record Office in 1977.

Bennett actually wrote many of the terse reports sent to the field commanders himself and was able to reconstruct day-by-day, hour by-hour, the availability of sigint to the invasion of Normandy and the subsequent battles in western Europe. When Bennett describes a particular event or situation, he refers to the sigint by the time a specific piece of information was passed to the commands in the field, German and Allied. That is, each ULTRA-based statement in the book is supported by one or more signals, the time of transmission by a German command, and the time of transmission from Bletchley. It is a phenomenal piece of research!

Another most significant book is R.V. Jones' *The Wizard War: British Scientific Intelligence 1939-1945*. Jones was a Scientific Officer on the staff of the Air Ministry in London during World War II and, as such, had access to the highest compartments4 of sigint as well as photo and human intelligence. He is held by many to be the father of scientific and technical intelligence. As the scientific adviser to MI-6 and Churchill, Jones played a crucial role in the scientific and technological struggle involving radar, navigational beams, electronic warfare and German V weapons. Jones had a unique grasp of the intelligence process -- he used elint, comint, aerial photography, prisoner interrogation and captured material. His book is a clear argument for small organizations with the close participation of its chief in analysis.

Arguably the most important book on sigint written by an American is David Kahn's *The Codebreakers: The Story of Secret Writing*. Kahn did not participate, as Bennett and Jones, in signal intelligence activities but he wrote the most lucid and most comprehensive book on cryptology up to World War II. Unfortunately, Kahn wrote his book a decade before the ULTRA secret was revealed so one has to go elsewhere for sigint history concerning the European theater in WWII. But Kahn does chronicle a complete history of cryptography including ancient secret writing, the Black Chambers, the interest by Thomas Jefferson, World War I, Yardley, Friedman, NSA, etc.

Another important book on sigint written by an American and largely unnoticed is *The ULTRA Americans: The U.S. Role in Breaking the Nazi Codes* by Thomas Parrish. As Parrish relied heavily on records and interviews with "ULTRA Americans", he tells the fascinating story of ULTRA as seen from an American viewpoint. The book offers some insights into the use and handling of this most precious source of intelligence by operational commanders, including notably Patton and his Third Army, but its most significant revelation is the work

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012031

EXPLANATORY NOTES

Bletchley Park was the home of the British Government Code & Cipher School (GC&CS), forerunner of GCHQ.

Hut 3 was the area for translation of the decrypts and reporting of German Army and Air Force activities. Hut 6 was the area for decryption. Huts 8 and 4 were the equivalent areas for the exploitation of German naval communications.

ENIGMA was the name of an cipher machine patented in 1919 and originally marketed as a means to safeguard commercial secrets in Germany. It was eventually used by all branches of the Wehrmacht.

ULTRA was the highest level comint compartment at the time; it was the category for the results of UK-US exploitation of German high-grade cipher.

of the joint U.S.-British mission, undertaken after the war was won to determine the success of the German signals intelligence service and its subsequent discovery of the German achievement against Russian high-level enciphered teleprinter communications. There is little doubt that the Americans owed much to the British regarding the exploitation of the German ENIGMA transmission during the war just as the British were in debt to the Poles for their techniques passed on to them immediately prior to the outbreak of war in 1939. But Americans were very much part of the team at Bletchley park from late 1942, and their remembrances, sometimes folksy and always anecdotal, add greatly to our understanding of operations in the Huts at Bletchley.

Of naval operations, two books stand out. One is by Edwin Layton, *And I Was There, Pearl Harbor and Midway*. Layton was the head of intelligence for the Pacific Fleet prior to World War II and served under in that capacity for Nimitz throughout the war. Layton's memoirs provides the most definitive answer on why we were surprised in December 1941. The book is a serious, well documented history of the American intelligence effort against Japan between the wars and through the end of WWII. It concentrates mostly on the events which led up to Pearl Harbor and the decisive naval battle near Midway Island in June 1942. For the former, Layton points out that although we had cryptanalytical success against Japanese codes, we were organizationally confused and did not take benefit of our advantage. Regarding the latter, Midway was a smashing success for our Navy and sigint played the crucial role.

The other important book on naval operations and sigint is the late Patrick Beesly's *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Center 1939-1945*. Beesly served in the OIC, the British Admiralty's organization which collated, evaluated, and disseminated all intelligence on enemy navies. He places the role of comint and ULTRA in proper perspective as an aid in winning the naval war, particularly against German submarines. The book also documents development of fusion centers on both sides of the Atlantic in support of operational naval forces.

By far the best unclassified reference book on sigint or intelligence is the several volumes by F.H. Hinsley, et al, *British Intelligence in the Second World War*. It is part of the official British history of World War II and is the most significant account of the role intelligence (in particular, sigint) played in strategy and operations in WWII. Hinsley and his colleagues, given full range to British government documents and intelligence records, revealed, for example, that the British had two sigint stations in the Soviet Union during the early days of the war and that they helped the Soviet's traffic analysts with knowledge of analytic techniques developed at Bletchley. For a serious scholar of intelligence in WWII, this book is *the* reference. (Unfortunately, there is no parallel in official U.S. history.) The history does include quite a bit on sigint relationships prior to and during World War II between the UK and the US.

Here is a list of my favorites:

ANDREW, Christopher, *Secret Service: The Making of the British Intelligence Community* (London: Heinemann, 1985)

BATES, David Homer, *Lincoln in the Telegraph Office: Recollections of the U.S. Military Telegraph Corps During the Civil War* (New York, London: D. Appleton-Century, 1939)

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012031

BEESLY, Patrick, *British Naval Intelligence 1914-1918* (New York: Harcourt Brace Javanovich, 1982)

_____, *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Center 1939-1945* (Garden City, NY: Doubleday, 1978)

BENNETT, Ralph, *ULTRA in the West: The Normandy Campaign 1944-5* (New York: Scribners, 1980)

BERTRAND, Gustave, *ENIGMA 1939-1945* (Paris: Librairie Plon, 1973)

BLAIR, Clay, Jr., *Silent Victory: The US Submarine War Against Japan* (Philadelphia: J.B. Lippincott, 1975)

CALVOCORESSI, Peter, *TOP SECRET ULTRA* (New York: Pantheon Books, 1980)

CLARK, Ronald William, *The Man Who Broke Purple: The Life of the World's Greatest Cryptologist, Col. William F. Friedman* (Boston & Toronto: Little, Brown, 1977)

CLAYTON, Aileen, *The Enemy is Listening* (London: Hutchinson, 1980)

EWING, A. W., *The Man of Room 40: The Life of Sir Alfred Ewing* (London: Hutchinson, 1939)

GARLINSKI, *Jozef, Intercept: The ENIGMA War* (London: J.M. Dent and Sons, 1980)

GYLDEN, Yves, *The Contribution of the Cryptanalytic Bureaus in the World War* (Washington, D.C.: Government Printing Office, 1935)

HINSLEY, F.H., et al, *British Intelligence in the Second World War: Its Influence on Strategy and Operations* (London: HMSO, 1979)

JONES, R.V., *The Wizard War: British Scientific Intelligence 1939-1945* (New York: Coward, McCann and Geoghegan, 1978)

KAHN, David, *The Codebreakers: The Story of Secret Writing* (London: Weidenfeld and Nicolson, 1967)

LAYTON, Edwin T, et al, *And I Was There: Pearl Harbor and Midway -- Breaking the Secrets* (New York: William Morrow, 1985)

LEWIN, Ronald Lewin, *The Other ULTRA* (London: Hutchinson, 1982)

_____, *ULTRA Goes to War: The First Account of World War II's Greatest Secret Based on Official Documents* (New York: McGraw-Hill, 1978)

MONTAGU, Ewen, *Beyond Top Secret ULTRA* (New York: Coward, McCann and Geoghegan, 1978)

MURRAY, Williamson, *Luftwaffe* (Baltimore: The Nautical & Aviation Publishing Co., 1983)

PARRISH, Thomas D., *The ULTRA Americans* (New York: Stein and Day, 1986)

SHULMAN, David *An Annotated Bibliography of Cryptography* (New York: Garland, 1976)

TUCHMAN, Barbara W., *The Zimmerman Telegram* (New York: Viking, 1958)

WELCHMAN, Gordon, *The Hut Six Story* (New York: McGraw-Hill, 1982)

WINTERBOTHAM, Francis W, *The ULTRA Secret* (London: Weidenfeld and Nicolson, 1974)

YARDLEY, Herbert O., *The American Black Chamber* (London: Faber and Faber, 1931)

Solution to :

NSA-CROSTIC #67 (plus)

4th Issue 1988

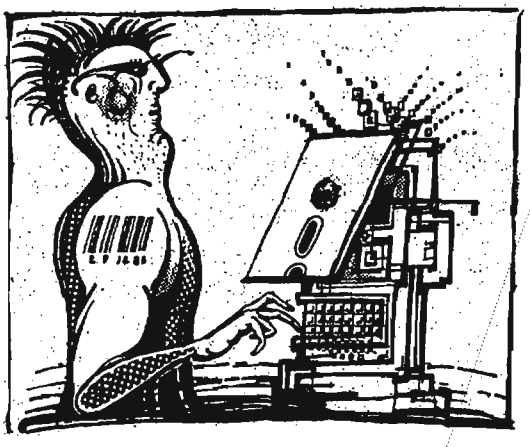
[Brigadier John H.] Tiltman, COLLECTED ARTICLES

[redacted] one of my leading book breakers, worked chiefly [redacted] [and seemed to bully any of my attached officers who worked under her.] She is famous for her editions of Mozart's and Beethoven's letters and was reputed on one occasion to have said [to [redacted] "]You don't seem to realize, Commander [redacted] that my work starts when I leave your office! ["]

The unadvertized feature is that the contents of cell 274 is an exclamation point!

EO 1.4.(d)

~~FOR OFFICIAL USE ONLY~~



P.L. 86-36

To the Editor:

(U) [redacted] in his article entitled "Changes In Agency Reporting" (CRYPTOLOG, 3rd Issue 1988), presented an excellent perspective on the most recent changes in Agency reporting philosophy. In his last paragraph, "Where Are We Headed" he mentions some of the problems facing Agency reporters in the future. In addition to his observations I would like to offer some of my own which I think will have a major effect on the future of SIGINT reporting here at NSA.

[redacted]

[redacted]

[redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

[redacted]

(U) Is the Training School presently capable of providing this type of training? If not, it will take some time to devise courses, and provide the training required for an adequate number of reporters. We probably need to start soon [redacted] is upon us. As we have found out in the world of collection, technology quickly outpaces whatever we have in our arsenal. The same will be true for SIGINT reporting unless we take the first steps soon.

~~(FOUO)~~ Fortunately some of the technology that is the problem is also part of the solution. By using graphics software, scanning technology, desktop publishing, etc., our reporters can begin to keep pace with our customers' requirements for information. We will probalby have to take a hard look at the way we are producing and disseminating reports. The old "E-GRAM" will have to take on a new look to incorporate both text and graphics in the same document. If we don't take steps soon we won't be able to meet our customers' demands for information. If we don't begin to make some changes in our reporting philosophy and procedures we could be in danger of merely collecting the cutomers' required information and passing it on to him, as collected, for him to make an evaluation of the content. We could end up being nothing more than a transmitter of SIGINT information to our consumers rather than reporters of SIGINT information.

[redacted] *Chief, G82*

P.L. 86-36

To the Editor:

~~(FOUO)~~ T is not the only Key Component with a "Yellow Pages." The Information Systems Security Organization has just completed an INFOSEC Yellow Pages and a Services Directory. A hard copy of our Yellow Pages will be out within the next couple of weeks and an automated capability is expected by the summer. The automated system will have several search capabilities to aid users within the INFOSEC organization.

(U) Our Yellow Pages were the result of an employee suggestion at a "Town Meeting" held by our former DDI. Your editorial [3rd Issue 1988] and [redacted] response [4th Issue 1988] would seem to indicate that "Look it up in the Yellow Pages" can be an appropriate response in some organizations.

[redacted] *D/Chief, S1*

P.L. 86-36

To the Editor:

(U) In response to [redacted] article in the 4th Issue 1988 of CRYPTOLOG entitled "The Question of Leadership," I am happy to report that in the 30 to 40 years since [redacted] was at sea, many changes have occurred.

(U) Today's Navy is an all-volunteer force made up of officers and enlisted personnel with significantly broader and more extensive education and training than [redacted] experienced in the 1950's. The World War II ships of that time have been replaced by modern and highly complex warships which require a very high degree of technical competence and management (leadership) ability to operate.

P.L. 86-36

(U) One fact that [redacted] noted is still true. That is that the appearance, morale, and operational performance of a ship is a reflection of the competence, ability, and personality of its commanding officer. This fact, coupled with the self-contained, self-sufficient and independent "on-their-own" nature of a ship at sea, results in a unique relationship and dependency between captain, officers, and crew that is not duplicated elsewhere. Unless you have experienced sea duty you might not realize that once a ship has sailed (steamed) over the horizon it is out of the country. In fact, it isn't in any country! At that time the realization of the captani's role and the relationship between him and the crew is much easier to see. Among other things, the captain is the senior leader, the standard setter and the one individual above all others on board, who is responsible for the ship and all hands aboard.

(U) It is quite obvious that those experiences at sea back in the 50's made a lasting impression on [redacted] and partically influenced his own leadership (management) abilities.

(U) Go Navy!

P.L. 86-36

R. A. Schriver, Capt., USN, Asst Commander, Naval Security Group Command

CLASSIFICATION QUIZ

JAMES C. LEISTER, DDO/CAO

~~(S-CCO)~~ This multiple-choice quiz illustrates some of the common classification decisions many of us must make on a regular basis.

1. Sensitive Compartmented Information (SCI) refers to which of the following:

a. TK
b. COMINT
c. BYEMAN
d. VRK
e. Any or all of these.

2. COMINT which, if compromised, would allow the target country to take specific countermeasures to deny us further access, must be handled as:

a. TS
b. S-CCO
c. TK
d. COMINT codeword.

3. The "fact of " a COMINT relationship between NSA and GCHQ, CSE, GCSB, or DSD is:

a. S-CCO
b. CONFIDENTIAL
c. TS
d. FOUO.

4. The fact that there are categories of COMINT, e.g., "cleared for CAT III COMINT," must be:

a. C-CCO
b. FOUO
c. SECRET
d. UNCLASSIFIED.

5. A SIGAD, e.g., USA-57, when associated with its location (Clark AFB) or its administrative designator (6922 ESS), must be classified at least:

a. SECRET
b. C-CCO
c. CONFIDENTIAL
d. FOUO.

6. The fact of the existence of Third Parties, without elaboration, must be protected as:

a. CONFIDENTIAL
b. FOUO
c. C-CCO
d. UNCLASSIFIED
e. S-CCO.

7. The "Handle via . . . " channels caveats for COMINT, BYEMAN, TK, and/or LOMA must be handled as:

a. FOUO
b. C-CCO
c. SECRET
d. CONFIDENTIAL.

8. All GAMMA information must be classified at least:

a. S-CCO
b. SC
c. CONFIDENTIAL
d. TSC.

9. The statement "cleared for TOP SECRET, Special Intelligence (cleared TS/SI)" is:

a. FOUO
b. CONFIDENTIAL
c. UNCLASSIFIED

10. The "fact of" NSA's SIGINT support to NATO and NATO Commands is:

a. CONFIDENTIAL
b. SECRET
c. FOUO
d. S-CCO.

11. Which of the following should not be marked on SAO (candy-stripe) coversheets:

a. COMINT codewords
b. BYE projects
c. NOFORN
d. VRK-11A
e. TK codewords.

12. NSA's association with SUSLOL, SUSLOO, SUSLOM, [redacted] is:

P.L. 86-36

a. CONFIDENTIAL
b. FOUO
c. UNCLASSIFIED
d. C-CCO.

13. Another marking that should always accompany LACONIC is:

a. ORCON
b. PROPIN
c. NOCONTRACT
d. NOFORN
e. None of these.

(Answers on page 18)

Solution to

MINICRYPTS, 4th Issue 1988

1. WALRUS PUPS SPRAWL

2. HEDGEHOGS DO SO SHED

3. LITTLE GIRL BETTER LET BIG BEE BE

The Winning (and only) entry came from the team of:

[redacted]

and "Mother" [the MASS4 computer]. The team won a CRYPTOLOG mug, and promised faithfully that all members would share it equally.

~~FOUO~~

P.L. 86-36

minicrypts #2

by Bill Lutwiniak, P1

Editor's note: We had only one response to the minicrypts in 4th Issue 1989. Astonishing for this Agency! But a reader pointed out that the fact that Bill Lutwiniak composed it would intimidate people; it sure gave him cause to pause, and he's still pausing!

Let's try one more time. Bill tells us that this one is not so hard. Do let us know whether you like it or not, or even, whether you'd even bother to try it.

1. W U B G L S I T H I N G
   - - - - - - - - - - - -

   G Y F L H G T R U S H U N
   - - - - - - - - - - - - -

   W B G N F I R U Y L U H
   - - - - - - - - - - - -

2. *T R U T H T O D U S T E D U R
   - - - - - - - - - - - - - - -

   U H S A T E D T O D
   - - - - - - - - - -

3. T R G A D R I V Y L
   - - - - - - - - - -

   D E L I V Y E R G R E T A
   - - - - - - - - - - - - -

** denotes a proper name*

~~This puzzle is FOUO~~

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4012021

NSA-CROSTIC No. 68

by [redacted] R822

P.L. 86-36

HOW TO SOLVE A DOUBLE-CROSTIC

Using the Definitions, fill in whatever Words you can. Then copy each letter from the Words into the corresponding square of the grid below. Scan the text in the grid from time to time; from the recovered fragments you may be able to complete the word in context. Copy the new entries from the grid into the Definitions, where the fragments there might suggest a complete Word, and so on, working back and forth. Also, scan down the first positions of the Words as you recover them for additional clues.

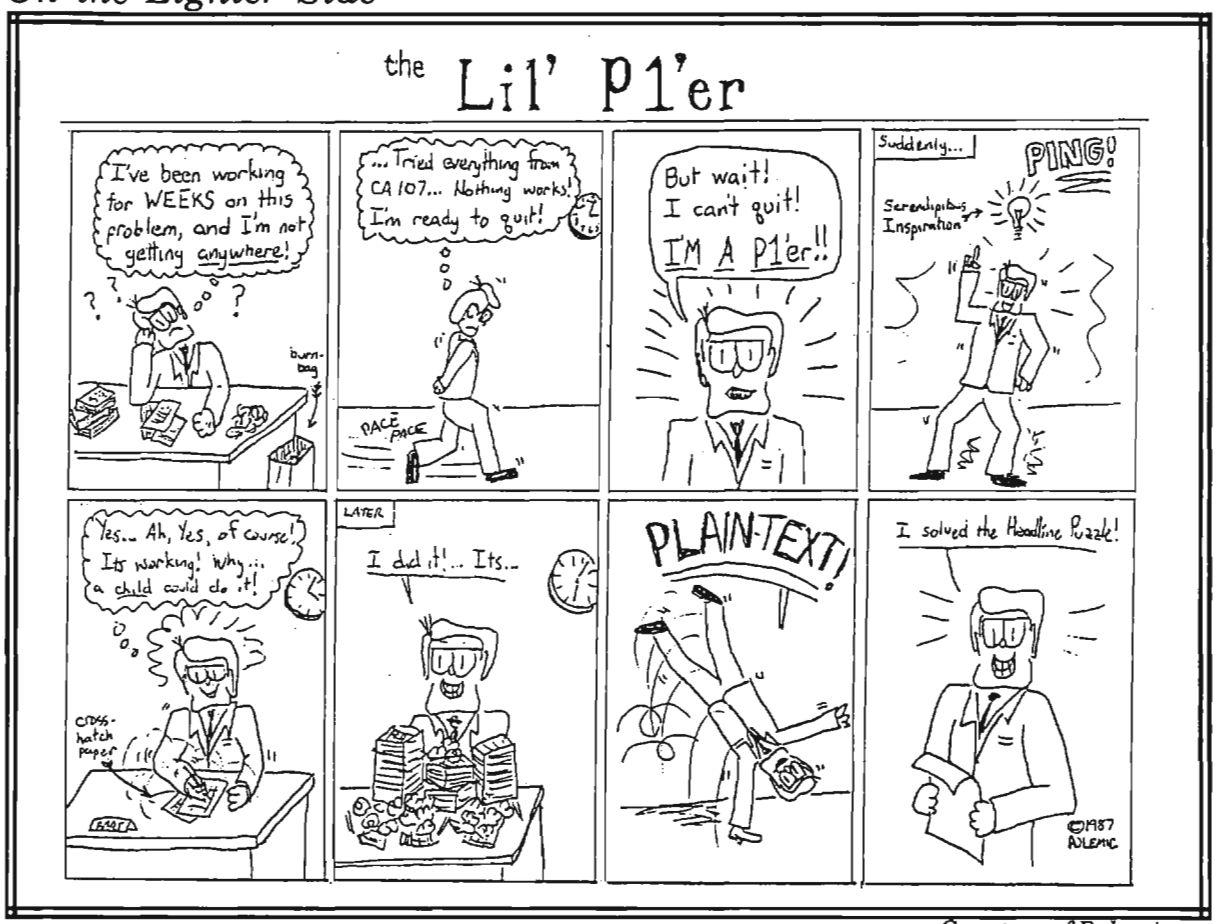
P.L. 86-36

DEFINITIONS **WORDS**

~~FOR OFFICIAL USE ONLY~~

The quotation in the grid was taken from an article that appeared in an NSA publication. The author's name and the title of the work are spelled out in the first positions of the WORDS.

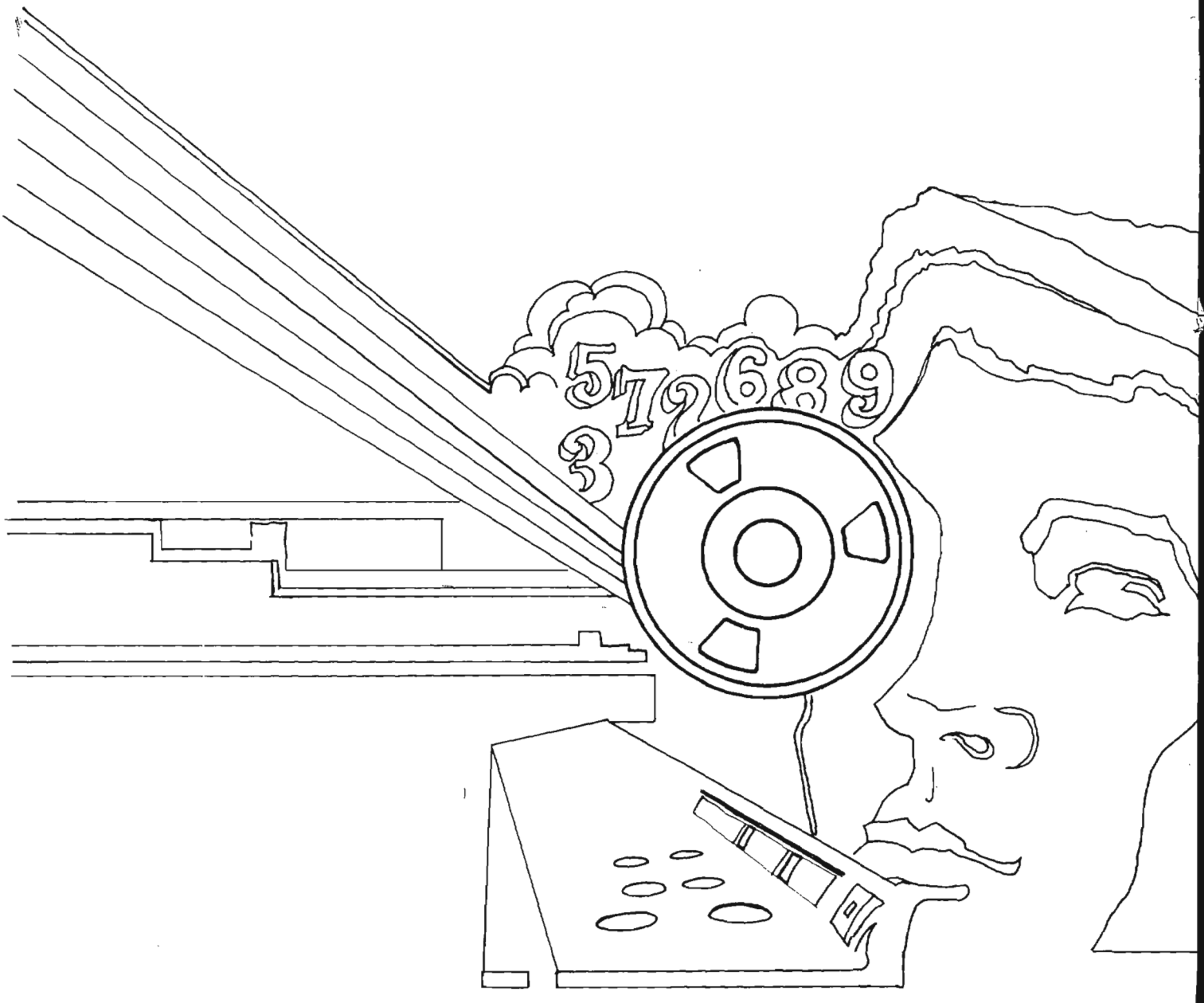
On the Lighter Side



Courtesy of Polemics

~~FOR OFFICIAL USE ONLY~~

~~TOP SECRET~~



DOCID: 4019712

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

4th Issue, 1988

P.L. 86-36

PROJECT RELOAD	[redacted]	.1
HOW TO MAKE A MORSE OP	[redacted]	.5
BULLETIN BOARD		.6
LOTUS 1-2-3: A FANTASTIC RESEARCH TOOL	[redacted]	.7
THE NEW CRAYONS: AN ALLEGORY	[redacted]	12
RESUMES AND JOB APPLICATIONS	[redacted]	14
THE QUESTION OF LEADERSHIP	[redacted]	15
SCRIBE	[redacted]	17
SOFTWARE REVIEW: RIGHTWRITER	Leroy Ferguson	18
CONFERENCE REPORT: AMS CENTENNIAL CELEBRATION	David Harris	20
QUOTE WITHOUT COMMENT		28
LETTERS		28
FROM THE PAST		34
BONUS PUZZLE: MINICRYPTS	Bill Lutwiniak	35
NSA-CROSTIC (plus) No 67	[redacted]	36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~NOT Rreleasable TO CONTRACTORS~~

Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019712

CRYPTOLOG

P.L. 86-36

Published by P1, Techniques and Standards

VOL. XV, No. 4 ..... 4th Issue 1988

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Cryptolinguistics ..... (963-4740)
Index ..... (963-4814)
Information Science ..... (963-3456)
Information Security ..... (972-2122)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (963-4958)
Special Research ..... Vera R. Filby (968-5041)
Traffic Analysis ..... Robert J. Hanyok (963-4351)

Illustrators ..... (963-4989)
..... (963-3738)
..... (963-6423)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the *mag card, floppy or diskette along with your* hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five)
(note: no 'o')

Always include your full name, organization, and secure phone; also building and room numbers.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, HQS 8A187
Please do not phone.

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

NSA'S BLACK HOLES

A recent theory about the universe holds that there are little black holes, like worm holes, in our universe leading to other universes. It must be right. We have evidence right here at NSA.

There's one worm hole between Fort Meade and FANX. If we ever get into that universe we'll find reams of memos that never got to their destinations. There's another worm hole just outside of SAB 2 that captures bundles of CRYPTOLOGs on their way to the intended recipients. There's even one, just a pin prick, to be sure, between HQS building and Ops 1, that attracts proof sheets of CRYPTOLOG articles.

Strangest of all, NSA's black holes don't go in for junk mail. You know the kind, when every employee gets a memo (after the fact) stating that 25 December is a legal holiday. Curious, isn't it?

Of course, there are those who attribute the disappearance of mail to a virus, the same kind that affects the US Postal System.

We don't know which of the two is the right explanation for the missing mail. Or if there's still another cause. We hope that somebody can find out soon and do something about it.

Vq.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019712

PROJECT RELOAD

P.L. 86-36

P.L. 86-36

[redacted] *P04B*

illustrated by the author

~~(FOUO)~~ Project RELOAD was launched in March of 1985 to improve the U.S. SIGINT System (USSS) support to national decision-makers and military commanders. This was to be done by upgrading the SIGINT production capabilities and missions of field sites, in particular those operated by the services. The initial objectives were to restore technical health in the field and to enhance analysis and reporting in the field, thus ensuring the wartime survivability of the USSS.

(U) In the earliest stages, the project concerned developing short-term solutions to site-specific endemic problems identified during field surveys made in late 1985 of 55 collection sites. These surveys gave mission management at the sites an opportunity to document their perceptions, problems, and needs. The findings formed the basis for, and provided the spirit upon which RELOAD strategies were subsequently built. Problems unique to each site were addressed by appropriate Agency elements which provided quick fixes to pressing problems. In fact, some 325 corrective actions were implemented by late 1986, resulting in some improvement in front-end production.

~~(C-CCO)~~ However, by the time the final RELOAD assessment was approved by the Director in April 1986, it became evident that certain problems in the USSS were systemic deficiencies requiring the development of long-term institutionalized solutions.

[redacted]

[redacted]

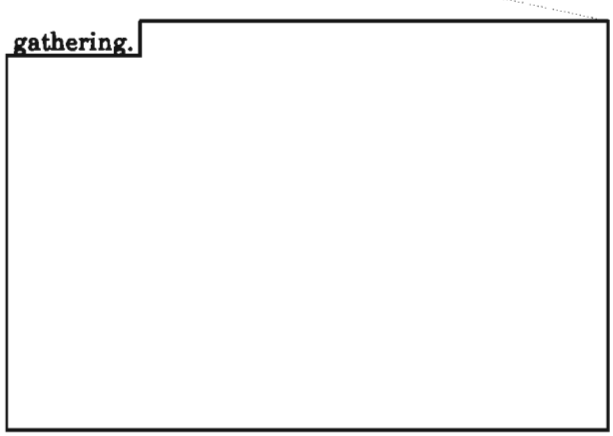
(U) About the time the basic RELOAD Findings and Recommendations report was released, the results of three other major studies became known, and the recommendations cited therein significantly influenced the course of follow-on RELOAD actions. These studies are:

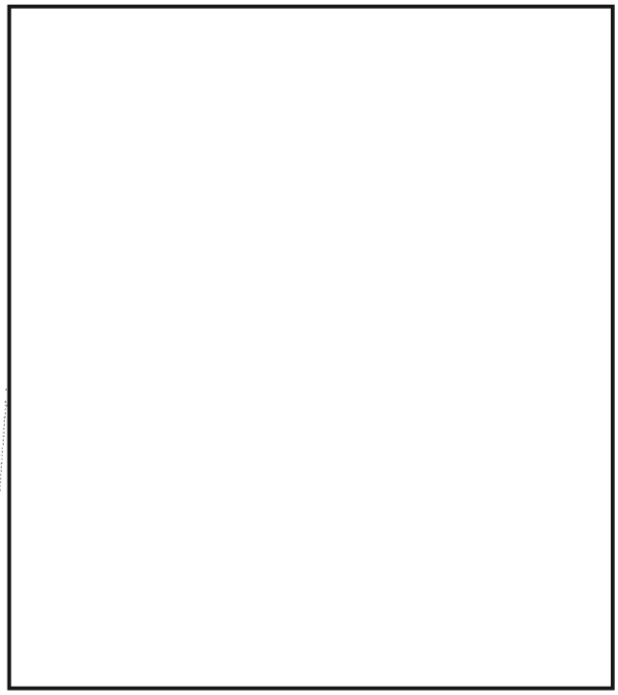
~~(FOUO)~~ **A Study by the Director's Blue Ribbon Panel,** consisting of high-level NSA executive-consultants. It reviewed the USSS in its entirety to determine the state of its technical health and its ability to accomplish its assigned mission now and in the future. It concluded that technical health in the field had to be strengthened; the practice of giving the military (the SCEs) virtually robotic tasks had to cease; and that NSA had to share the high tech duties with the field -- not just to enhance the field's capabilities, but to allow the time and talent of the NSA work force to be directed toward keeping up with the vast expansion taking place in all aspects of SIGINT. Systemic deficiencies were evident within NSA as well as in the field, for different reasons.

~~(C-CCO)~~ **The Future SIGINT Capabilities Study (FSCS)** which examined the capability of the USSS to handle the rapidly increasing volume of signals in the environment as well as its ability to cope with our targets' advances in signals technology. It pointed out that the seriousness of the rapidly advancing technologies of our targets poses serious problems requiring strategic action if the USSS is to maintain superiority in intelligence

P.L. 86-36

gathering.





FOLLOW-ON ACTION

(U) Because three of the four studies focused on operational matters under the Operations Directorate, it seemed reasonable that follow-on action should be undertaken by that Key Component. Since Project RELOAD had done so much on the study initially and was most familiar with the problems, it was given the corporate go-ahead to attack the systemic problems plaguing the system. The nature and breadth of the RELOAD program changed drastically as it shifted from problem study to problem solving. The reconfiguration and modernization of the entire USSS seemed to be necessary. Consequently, the scope of Project RELOAD has expanded, as has the original list of systemic issues.

(U) Through all of this there has been a very vivid perception on the part of NSA, the field, and the SCEs that RELOAD has had, and continues to enjoy, the strong backing of DDO and the Director.

(U) The Director of NSA charged the key components and the SCE commanders with identifying specific people to work with the RELOAD Project Management Office to implement the findings and recommendations of the various studies. A tiger team approach was selected, as the effort is and will continue to be a corporate one. The players involved are DDR, DDT, DDA, ADT, DDO (A, B, G, P, and W), CMC, ESC, INSCOM, and NSG.

~~(C)~~ The working groups chosen to meet and implement near-term (less than a year), mid-term (two to five years), and long range (beyond five years) solutions to the issues have contributed immeasurably to the accomplishments of RELOAD, as have the innovative suggestions of field sites. The SCE HQ are represented on *all* working groups, with the Cryptologic Manning, Collection, and Processing Working Groups actually being chaired by INSCOM, ESC, and NSG representatives, respectively. RELOAD is broader than just the working groups and the initiatives do not come from the working groups alone. Nor do initiatives come just from the SCE Headquarters; they can come from any element in the process, and often spring from the field sites themselves. RELOAD has brought about a better bonding between the front end and the back end of the system with the common goal of doing it more efficiently and effectively.

(U) RELOAD continues to use quick-fixes to problems wherever practical, but is following up with long-term corporate (NSA-SCE) institutionalized programs, serving as the means by which organizations are brought together to fix their own problems. It provides the forum and the opportunity through the working groups to actively pursue solutions to problems with the RELOAD banner serving as the driving force. A corporate entity has been created in which all of the parts recognize essentially one goal: to equip and to educate the work force to acquire the skills required to cope with the challenges of tomorrow.

~~(C)~~ By the end of 1987, RELOAD had blossomed into a widespread brainstorming

P.L. 86-36
EO 1.4.(c)

effort with fresh ideas emanating from many NSA and SCE sources. The effort has already yielded some degree of improved field technical health, has upgraded target assessment and reporting, and has made genuine progress toward expanded front-end crisis response and self-sufficiency capabilities. The emphasis continues to focus on improving technical health through enhancing the skills of the work force. As a consequence, certain RELOAD initiatives traverse the entire USSS, and impact on both the military and civilian work forces. The achievements recorded in 1987 are many and attributable to the hard work, vision, and cooperative efforts of numerous personnel at various field and headquarters elements.

~~(C-CCO)~~ During the past year, the technical health concerns and issues documented in the RELOAD findings report of April 1986 drew the corporate working groups that were examining the topics into a scope beyond the narrow analysis and reporting structure earlier associated with RELOAD.

(U) The present scope of RELOAD actions becomes evident from the following summary of highlights:

~~(FOUO)~~ **Traffic Analysis** - The focus has been on increased training, responsibilities, and documentation. Site technical exploitation initiatives are flourishing. Corporate skill standards have been introduced to assist the training and assignment processes and major revisions to existing career pathing and development schemes are under consideration. The traffic analysis and SIGINT reporting skill standards were subsequently combined into a SIGINT analyst skill standard. Certain field sites have assumed increased target responsibilities and new technical studies (e.g., ITNs) are resulting. Mission managers are refocusing duties to capitalize on available experience and skills and as a consequence analytic proficiency is on the rise. A working group TA Focus Plan calling for a broad range of reforms to strengthen career field/discipline mechanisms is in final coordination and appears to have overall management/command backing.

~~(C-CCO)~~ **Cryptanalysis** - A host of SCE field stations have now reacquired basic cryptanalytic capabilities and missions.

Two courses were conducted to teach cryptanalytic techniques and acquaint analysts with target cryptanalytic histories and profiles. Stations have been given appropriate software and data base access where possible to aid local exploitation efforts. Early results are most promising. Productivity at some sites has markedly increased, processes producing monthly keys for some targets have been accelerated, and most important, local target identification and warning methods have been upgraded.

~~(FOUO)~~ **ADP/Data Bases** - One achievement in this area has been the development of a means for all sites to request access to data bases, by approaching one office (T52) with their justification. Group A has developed and fielded procedures to provide access to information requested, which also satisfy need-to-know controls. This system will now be applied to other data bases, and made applicable to more field sites. Access to data bases from field sites will remain a function of the capacity for communications paths to support it. Other aspects being worked are a directory of information managed by T52 which can deliver a listing of data bases, provided by target offices, designated for access to field sites, and an up-to-date listing of software that has been developed either in NSA or in the field and is available for acquisition.

EO 1.4.(c)
P.L. 86-36

[redacted]

[redacted]

[redacted]

(U) **Manning** - With the aim of getting better skills-to-job matches, the SCE HQs are now geared to push their current manpower systems to the maximum. One universal method employed was the drafting of better job skill requirements statements and the rollover of these expressions into TDs. Also to be employed in this process will be the RELOAD-drafted and corporately approved three-tier skill standards. Attention is being devoted to tracking and assigning skilled personnel including the addition of trailers to occupational codes to identify specially trained and uniquely capable personnel. Most important, SCE managers are striving to implement improved career pathing schemes to enhance the cryptologic development of personnel; NSG's A & R plan is a trend setting example.

(U) **Language** - This newly established corporate working group has established as its goal a commitment by managers to fix long-standing problems in proficiency, maintenance, retention, assignments, and training. It held its first meeting in December 1987 and will interact with SCE and NSA management to gather essential information to form a baseline of existing linguistic proficiencies from which to build realistic requirements that will lead to improved language competencies in the field and at NSA.

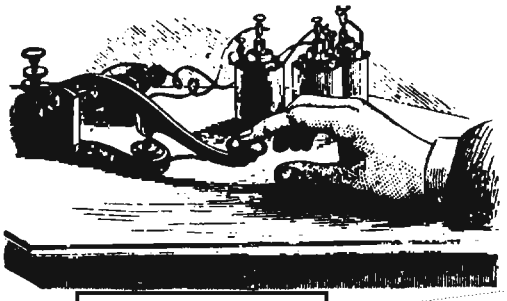
(U) The challenges of the combined studies have driven what has been done under RELOAD and continue to direct what is yet to be accomplished. The Field Stations and SCE HQ are most enthusiastic and have been the key players since the results of the initial site surveys developed into positive actions. The producer community is now convinced that RELOAD is not just a fad that will go away. The front-loading effected by RELOAD will continue; it will continue because there is now an understanding of the scope of the problems and an understanding of what must be accomplished under the umbrella of RELOAD. The concerted effort includes reaching outside the USSS to obtain reviews and reconsiderations of procedures affecting the very heart of SCE skill acquisition and maintenance, to wit, training and assignment. □

~~(C-CCO)~~ **Processing** - The main thrust in this area was to make collectors cognizant of why certain signals were important and what the plans and strategies were for future field exploitation [redacted]

[redacted]

DOCID: 4019712

//HOW TO MAKE A MORSE OP//



//[redacted]/P043//

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

~~(S-CCO)~~ NSA was asked to prepare SIGINT training [redacted] several years ago. The OPI, [redacted] solicited input from several sources for material and training, including E23 (now E54) for help with training new Morse operators. The following is based on a memo prepared by one of my NCS colleagues at the time and to which I contributed. We never learned whether our recommendations were adopted or used. But we think it worthwhile to publish our findings on what it takes to make a Morse operator. The statistics and conclusions are based on our experience at NCS in training morse operators.

THE RECOMMENDED PLAN

(U) It usually takes a Morse operator trainee approximately twenty weeks to achieve a code copying speed of twenty groups per minute. (This is not full time -- not all of the 800 hours are spent copying code.) To achieve 13 GPM usually takes about 165 hours.

(U) The usual progression for a Morse trainee is that after about 110 hours the average student can copy eight groups per minute. From this level, the student will progress rapidly, usually attaining 13 to 15 GPM after an additional sixty hours of work. At this point a plateau is reached, after which it will take another 150 hours of copy to progress to 18 GPM. By the term "plateau," we mean the level at which the student can copy at his highest speed accurately and with relatively little trouble. The next higher speed, on the other hand, seems to present the student with an inordinate amount of trouble. That is, at the plateau the error rate will be at or under 2%, while the error rate at the next higher speed usually starts at about 15% and gradually diminishes. The plateau speed varies from student to student, but as we said above, it usually ranges from 13 to 15 GPM.

(U) This plateau is apparently the transition point at which Morse code copying becomes a psycho-motor response rather than a cognitive translation of the sounds to symbols. After the transition is made, code speed acquisition again rises steeply with a gradual flattening of the curve as the natural limits of the students' abilities are approached. It will take approximately 400 to 500 hours of copying Morse for an average student to attain a code speed of 20 GPM.

(C) In designing a course for an intercept operator, material other than morse copying of course is taught. In designing a course combining Morse training with the academic material required, we recommend that the subject matter is scheduled so that the first two weeks are devoted to learning the Morse alphabet. After this, most of the time should be spent on the academic material, gradually increasing the amount of time spent on Morse until the final weeks, when copying Morse is full time. The conditions under which the students work, particularly during the last weeks, should be as realistic as possible. This could be accomplished by introducing recordings of actual target transmissions, or perhaps by assigning the student an actual mission which is duplicated on cover.

(U) Morse learning is a very individual thing with students progressing at different rates, reaching their plateaus at different code speeds, spending different amounts of time on their plateaus, and so forth. A student who appears to exhibit good potential, then, should not be dropped for failure to achieve average progress.

DOCID: 4019712

(U) One feature of Morse is that accurate copy is much easier if (and when) the student learns to stay behind the character being sent. Three to five characters behind is what the average high speed operator manages, but accuracy is nearly impossible if the operator is working right on top of the character being sent. This should be stressed by the instructors from the time the students have mastered the alphabet all the way through the course.

SUGGESTED TIMETABLE

(U) The end of week nine, by which time the students would have had 159 hours of Morse training most of the students should be working on 15 GPM or thereabouts. Whatever speed they are on, it is likely that most, if not all, will be at their plateau level. Here is the time to start to bear down and increase the time spent in the training day on Morse.

~~(C)~~ The end of week fourteen, after approximately 300 hours of Morse training, striving to achieve higher code speeds will be getting old. A break here will, in some cases, provide better results in the long run and in most other cases make little or no difference. That is, there is a good chance or benefit and little chance of loss by taking a break from the Morse at this point. The next two weeks, we recommend, should be devoted to classroom training in intercept procedures. When Morse training is resumed after that, all appropriate logging and copying formats should be incorporated.

(U) By the end of week 18, some 330 to 350 hours of Morse training will have been given.

~~(S-CCO)~~ Starting with week 19 or thereabouts, code speed practice should be interspersed with recording or target activity or, if resources are available, [redacted] Additionally, students who have achieved the required code speed and are apparently gifted operators can be introduced to barred letters and special characters beyond what they will have learned as routine. [redacted]

(U) The remainder of the course, probably through the 23rd week or beyond, should be full-time Morse with about two-thirds of the effort on operational material and the rest either speed work, if still needed, or introduction to other alphabets.

(U) From a training perspective, it will take twenty weeks or more to make a Morse operator. Most people will tell you that at least a year actually doing the work is necessary to produce a competent operator, but that's another story that can be told some other time. □

BULLETIN BOARD

UNIX BROWN BAG SEMINARS

~~(FOUO)~~ At the February session of the brown bag seminars on UNIX sponsored by CRYSCOM, [redacted] CRI/T335, will speak on [redacted] analogies and CA applications. In March [redacted] T335, will give details on data configuration using SCCS/MAKE, especially in regard to ther UNIX/UNICOS Software Exchange Proposal. Date, time and place for the February and March meetings will be announced later. For further information please call or write the CRYSCOM Exec, [redacted] Ops 1, P13, 963-3405.

CRYSCO '89

P.L. 86-36

~~(FOUO)~~ Planning for CRYSCO '89 is underway. The sessions will take place the week of 19 June in HQS 9A135, the Old Director's Conference Room. Suggestions for topics are solicited. Contact one of these people: [redacted] CRYSCO '89 Chairman, 968-8141; [redacted] CRYSCOM Exec, 963-3045, or [redacted] CRYSCOM Chairman, 963-4681.

Reminder

Material from CRYPTOLOG, whether classified or unclassified, may not be disseminated outside NSA without written permission. Address inquiries to the Editor.

EO 1.4.(c)
P.L. 86-36

Lotus 1-2-3: A Fantastic Research and Intelligence Tool

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

[redacted]

P3 Technical Assistant

[redacted]

~~(C)~~ Lotus 1-2-3 is a commercial software package its creators say was designed for accounting and financial analysis. But its integrated spreadsheet, database, and graphics components also make it an ideal piece of software that can be used in the Agency by traffic analysts (net identification, analysis, and query counting), engineers, mathematicians, typists, and managers. [redacted] Its ready availability on IBM PCs, XTs, and ATs that are widely distributed throughout the agency, the low cost, and compatibility with new upgrades of Lotus make it a cost-effective analyst's tool, especially welcome in these days of tight budgets.

(U) The menu options include:

- FILE IMPORT- Inputs to a Lotus spreadsheet any ASCII numeric or textual file up to 240 characters per line; inputs to other spreadsheet files (DBII & DBIII, Visicalc, word processor files).

- PARSING- Allows user to separate any line(s) of text into separate columns of numeric or alphanumeric characters. The parsing line can be stored for reuse on new data.

- DATABASE- Allows sorting of columns and rows of data; permits querying the database using criteria to extract information.

- STATISTICS- Finds sums, averages, and standard deviations for data entered into the spreadsheet.

- GRAPHICS- Displays Bar, Pie, Line, XY plots on the screen using spreadsheet-entered data; [redacted]

(U) Since Lotus is an integrated package, any menu option can be used either independently or together with other options on the same data.

IMPORTING DATA INTO LOTUS FOR DATABASE OR MAP DISPLAY PURPOSES

~~(FOUO)~~ Lotus can import into its spreadsheet any ASCII textual or numeric file from any Agency database if it has 240 characters or fewer on a line and can be stored on a diskette. That means that reports from the field with mixed narrative and tabular information can be processed through LOTUS to pull the tabular information together. Then that tabular information can be parsed, as required, by any parameter. The parsed results can then be sorted by any parameter or saved to another file for database querying.

(U) If new reports require similar parsing, you need set up only one parse line, store it, and use it for the new data. Once all the necessary data are extracted and stored on separate files, these files can be read back into the spreadsheet, and combined and sorted as a single file. The data can also be queried for specific criteria and the data matching the criteria can be extracted for any purpose, such as input to the Lotus map display spreadsheet.

PARSING

~~(FOUO)~~ If you have old alphanumeric textual files you've created with a word processor or on a terminal such as COASTLINE and you want to create a database without retyping the data, Lotus parsing is for you. Figure 1 shows how

EO 1.4.(c)
P.L. 86-36

parsing works on a message where the parameters are separated by / marks, and zulu time, latitude and longitude are wanted for the database.

(U) Lotus tries to up a parse line (first line in Figure 1) where L=label, * = space, and > means continue the label until a new symbol appears. If the parse line doesn't meet your criteria, you may modify it, as shown in Figure 2 where S in the parse line = space. Lotus then parses the data automatically and lets you store the parsed data anywhere you want on the spreadsheet, as in Figure 3.

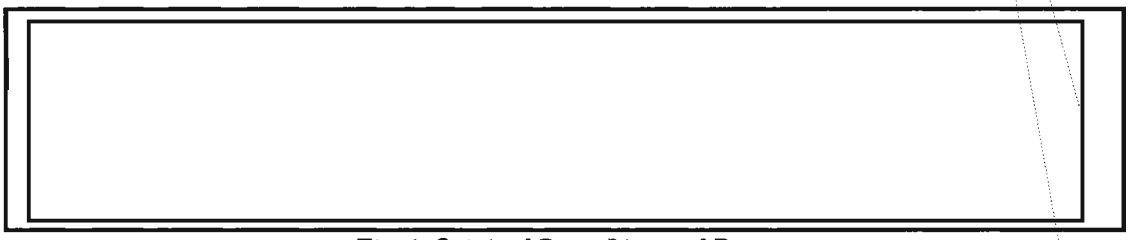


Fig. 1. Original Parse Line and Data

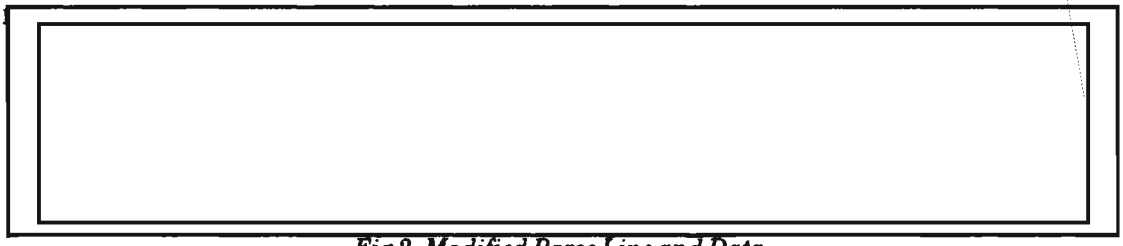


Fig 2. Modified Parse Line and Data

~~(C)~~ The data in Figure 3 is arranged in three columns and can now be sorted using Lotus' database sort option, combined with another file having similar data previously extracted the same way, or input to my Lotus Elint Display spreadsheet for plotting.

DATABASE SORT AND QUERY AND DATA TABLE SETUP TO COUNT DATABASE DATA

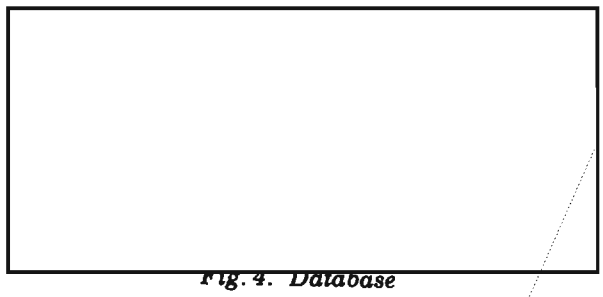


Fig. 4. Database

(U) In Figure 5 the database is sorted with the "from" column as primary sort.

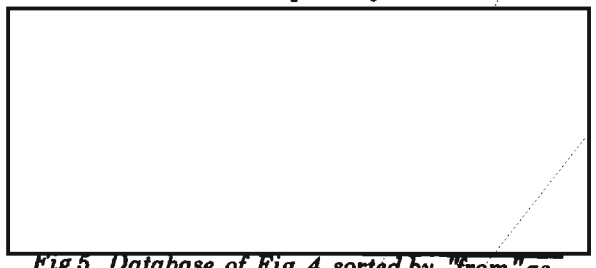
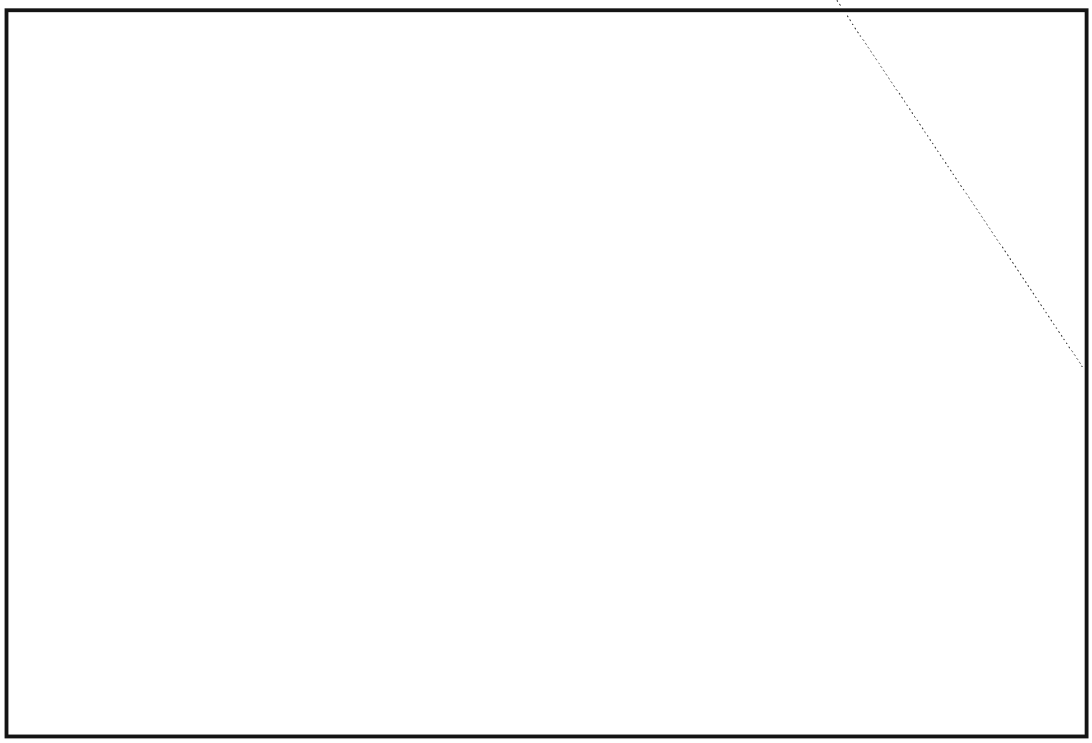
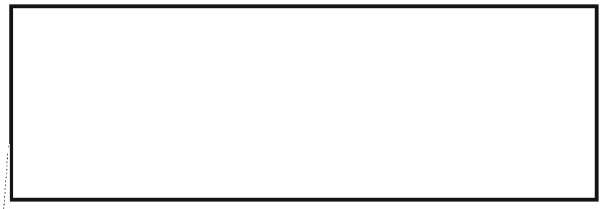


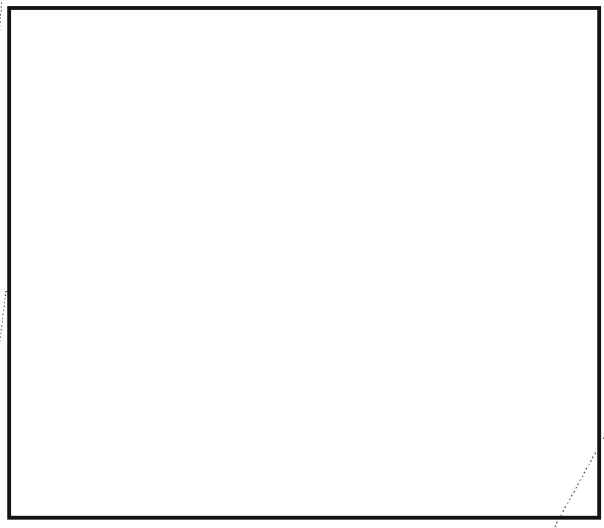
Fig 5. Database of Fig. 4 sorted by "from" as Primary column and "to" as Secondary column.

(U) Figures 6 and 6a show how the database is queried for information. Lotus requires setting up a criteria and output header with the same titles as those for the database. Criteria are input in the criteria line for any of these header parameters. Results matching the criteria are then displayed on the output lines.

EO 1.4.(c) P.L. 86-36 ~~CONFIDENTIAL~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~ EO 1.4.(c) P.L. 86-36

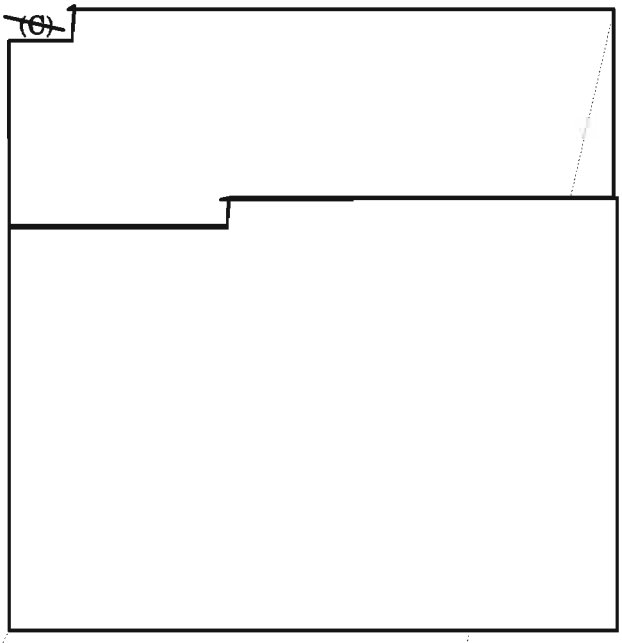




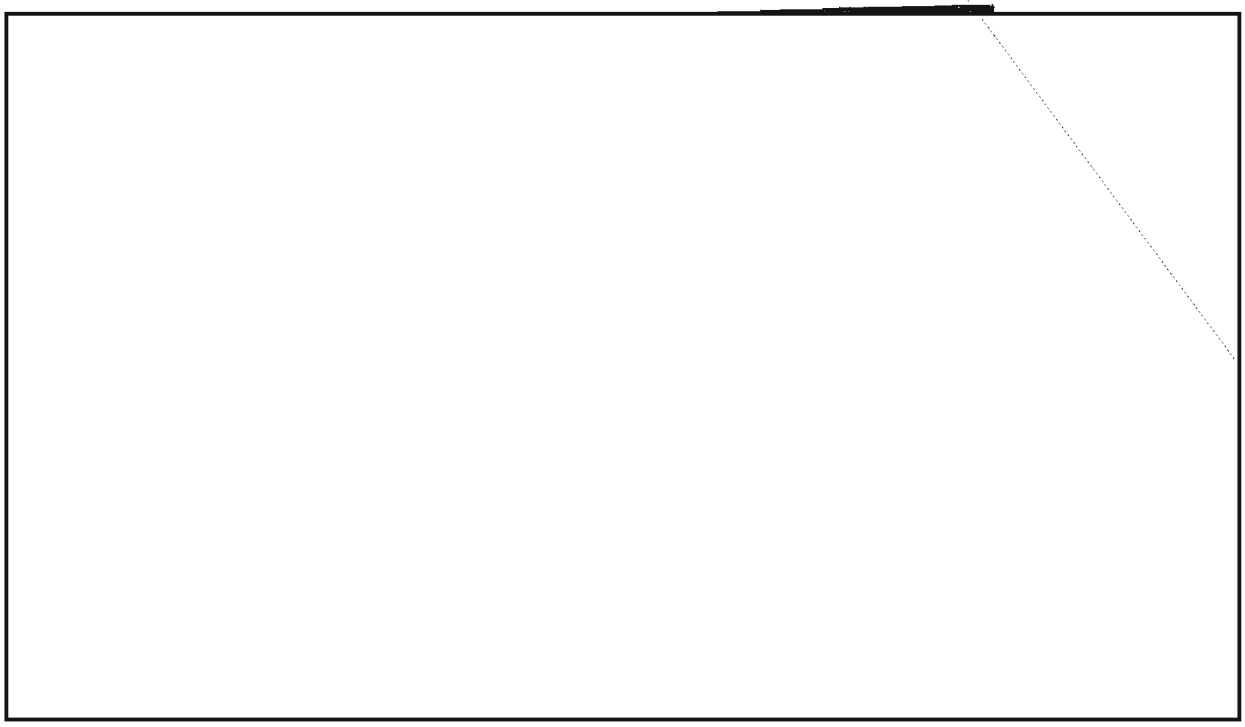


(U) These steps are continued for all parameters in the Data Table until it is filled. Analysts can then scan the Data Table to determine who talks to whom and how many times, thus establishing relationships very easily.

~~(C)~~



~~(C-CCO)~~ I have just touched the surface of what Lotus can do. For example, curve-fitting techniques can be developed on a spreadsheet, and the input curve to be matched displayed together with the calculated curve; message editing hard to do on Coastline can be input to Lotus where paragraph-justifying can be easily done and the results passed back as a Coastline file. Files too large to transmit to a



field site via Coastline can first be read into Lotus, split into segments and then transmitted via Coastline. At the field site the segmented files are read back into Lotus, recombined, and saved as the original file.

(U) It is also possible to convert any program binary file into an ASCII hexadecimal file, split the file into segments, and transmit it to the field site. The field site then recombines the file in Lotus and reconverts it to a binary file and uses the program. This saves sending new application programs by mail to the field.

~~(FOUO)~~ The field can also transmit programs not working correctly to NSA where they can be analyzed and transmitted back. This saves mailing time (usually 3 weeks per mailing), updating time, and uptime for using the program. Bar, pie, line or XY charts can be developed in a spreadsheet, displayed, and plotted. The data for these charts could be imported from a diskette, keyed in by hand, extracted from a query from a database setup in the spreadsheet or a sort of the data, or entered from a parsed message.

(U) In summary, this article shows that Lotus can handle many intelligence chores without special programming. Before your organization buys sophisticated hardware or software to accomplish a task, check into Lotus spreadsheet capabilities. You'll be surprised at the power available. Try it... you'll like it.

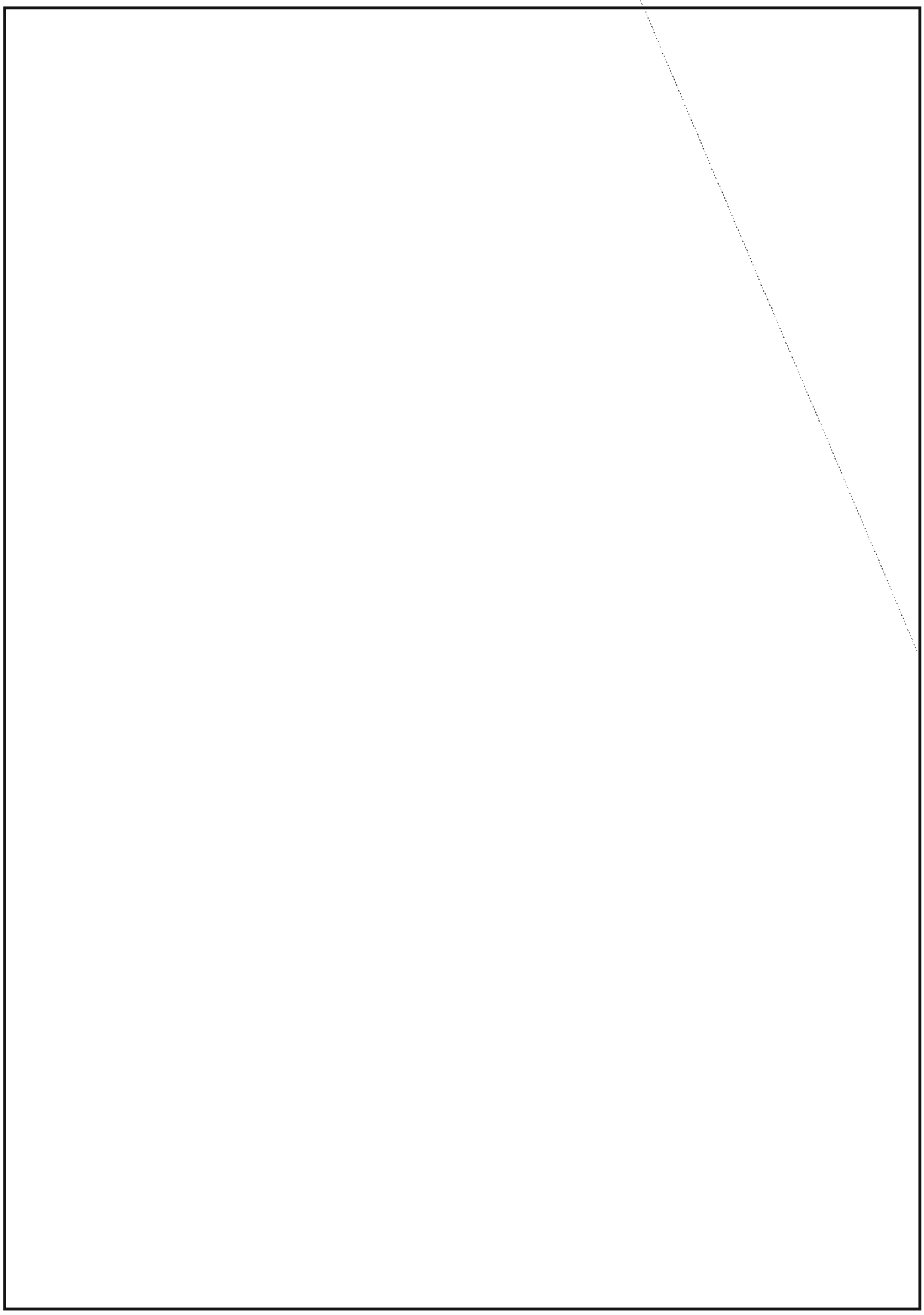
Editor's Note:

We are advised that ASPIC has replaced Lotus 1-2-3 as the standard spreadsheet software with SuperCalc4, but the latter does not have parsing capability and lacks other features necessary for the applications described in this article. Lotus 1-2-3 can still be ordered as non-standard software with justification.

DOCID: 4019712

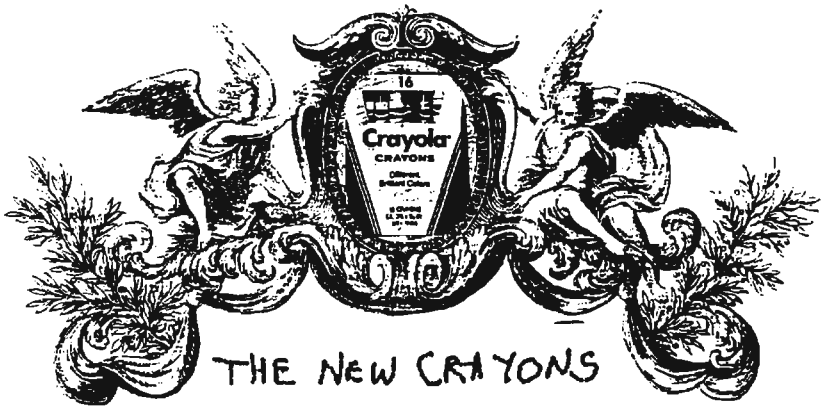
P.L. 86-36
EO 1.4.(c)

~~CONFIDENTIAL~~



~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4019712



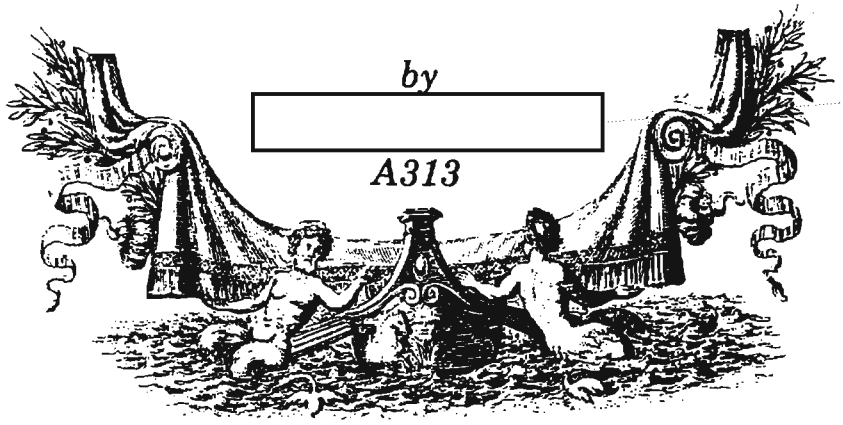
THE NEW CRAYONS

Once upon a time there was a special school for young artists. Only the most promising students were allowed to attend. The school had several boxes of crayons for them to use. Each box contained eight fine colors. The school did not have enough boxes to give one to each student, so the children had to share. But most of the time that was okay. While they were waiting for their turn to use the crayons, they could rub their drawings with tissues to make them look smoother, or they could think about what they would draw next. Sometimes they wished they could have more crayons, but they managed to make do. The children learned to make wonderful pictures with their simple tools, and people began to come to look at their masterpieces hanging in the school's own gallery.

The schoolmaster was very proud of the gallery. He wanted to help the students produce more and better drawings for the visitors to admire. So he decided that each child should have his own box of crayons. He arranged to buy more. The new crayons would be thinner, so the young artists could draw finer lines. There would also be 16 colors in each box, so the children's pictures could be even more wonderful than before. These new, improved crayons were expensive, so the schoolmaster could buy only a few boxes at a time. But nobody worried too much because they knew that one day everybody would have his own.

When the new crayons began to arrive, the children discovered that the boxes had room for 16 crayons, but two colors were missing from each box. The crayon makers had not yet been able to make new, improved versions of blue and purple crayons. But they promised to make them soon and send them to the school.

As the months went by, the students were given more of the new crayons. Finally, there was one box for each student. Some had the old ones, and some had the new. The new 16-color boxes still had no blue nor purple. So the children with new crayons had to borrow the old ones when they wanted to use blue or purple in their pictures. The children with old crayons had to borrow the new ones so they could



P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019712

An Allegory

draw finer lines and use some of the fancy colors. The new, improved, thin crayons were easier to break, so everyone had to be more careful. And, of course, everybody had more crayon sharpening to do.

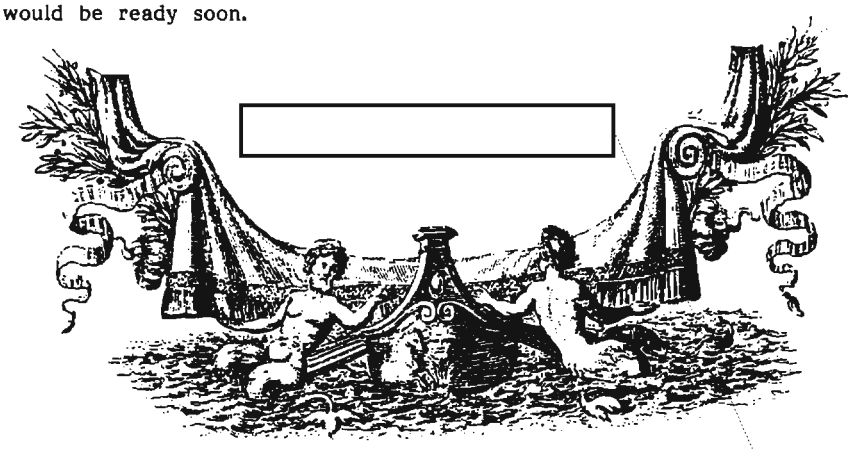
The schoolmaster declared, "Now that we have one box of crayons for each student, you can draw more pictures faster to hang in our gallery."

"No," the children explained, "We cannot. We do not really have enough crayons for everybody to use at once. We still have to share. We also must spend more time taking care of the crayons."

The schoolmaster thought the children were ungrateful and greedy. He refused to buy any more new crayons unless the children agreed to trade in the old ones. He did not want to make the school board angry by having more boxes of crayons than there were children in his classrooms. But the children insisted that they could not give up the old crayons because they needed blue and purple to complete their pictures.

Soon the children were spending less time drawing and more time trying to explain their crayon needs. Yet the schoolmaster would not change his mind: the boxes of crayons must not outnumber the children. But he promised to provide new, improved blue and purple crayons, even if he had to make them himself; then they would no longer need the old ones. The children were not convinced, but agreed that it would be just fine if he could really do it. Then they could see about getting a complete set of new, improved crayons for everybody. They just wanted to make sure they had the new blue and purple crayons before giving up the old ones.

Meanwhile, the crayon salesman said that there would soon be no more 16-color boxes of crayons. Instead, he would be selling boxes of newer, more improved crayons in 24 colors. Well, at least there would be room for that many. The crayon experts were still working on the red and orange ones, but the salesman assured everyone that these would be ready soon.



P.L. 86-36

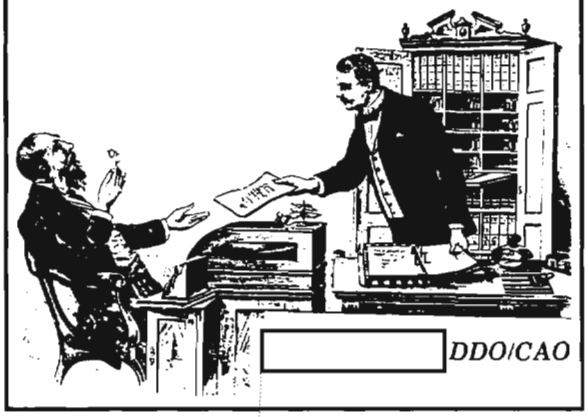
~~FOR OFFICIAL USE ONLY~~

DOCID: 4019712

RESUMES *and*

JOB

APPLICATIONS



DDO/CAO

During our employment with the National Security Agency, many of us will prepare or have already prepared, one or more resumes or job summaries in which we must explain, in unclassified language, what we have done and are doing on the job at NSA. This often is a difficult task, since much of what we handle tends to be classified.

All resumes, detailed job applications, student co-op reports and the like must be reviewed and approved for release as unclassified. The Classification Advisory Officers (CAO's) throughout NSA have been authorized by Q43 to review and release these resumes, applications, and reports. The five CAO's within the Operations Directorate are listed at the end of this article.

Any document intended for public release, such as a resume, may not contain classified information. The following additional information also may not be released:

- NSA missions and functions
- Employee names (names of supervisors are releasable; employee character references should not be attributed to NSA employment, but to U.S. Government employment.)
- Project names and covernames
- Salaries (other than the originator's)
- Number of people employed by NSA
- Office symbols and organizational designators

Also, although the terms COMINT, ELINT, SIGINT, etc., when associated with NSA are considered FOUO, you must be careful when associating them with job titles, duties and performed functions.

As stated elsewhere, indications of one's foreign language capability in connection with NSA duties are considered classified; this creates problems in writing a resume. Association with languages in an academic or training context is permitted, but specific languages should be listed only in the academic section of the resume. Specific foreign language ability, e.g., native speaker, self-taught, etc. should be listed only in the summary of qualifications or miscellaneous section. You may show any and all language training courses as unclassified. You may not associate your language capability with the duties of your position.

As far as clearances are concerned, you may indicate that you are cleared for TOP SECRET Special Intelligence (TS/SI) without further elaboration or detail. You may not include any additional specific accesses. Revealing that you hold a TS/SI clearance may actually be helpful, even if the position sought may not require a clearance. The fact that the government granted the clearance speaks well for the honesty and integrity of the applicant.

The following is an updated listing of the Classification Advisory Officers (CAO's) within the Operations Directorate. Please contact the appropriate CAO whenever any assistance is desired or needed concerning proper classification of information or materials, or for review and release of a resume, applications, etc.

- B/CAO Dick Sylvester, B03, 4053s 2S010-2

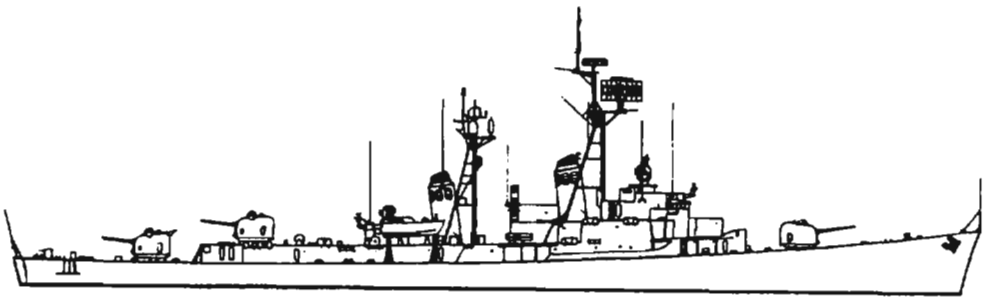
P.L. 86-36
EO 1.4.(c)

P.L. 86-36

P.L. 86-36

DOCID: 4019712

THE QUESTION OF LEADERSHIP



P16 P.L. 86-36

~~(FOUO)~~ During the early 1950's I was assigned to the staff of Commander, North Atlantic and Mediterranean for duty with Communications Unit 32D (COMUNIT 32D). I was assigned to various destroyer division staffs where I taught ELINT countermeasures to radiomen and radar operators aboard three different destroyers. All three destroyers had similar missions and almost identical manning.

(U) At that time Greece and Turkey were going through a very unsettled period, so one mission assigned to the Navy was to show the flag in Greek and Turkish ports - usually spending three to five days in a port or lying offshore before moving on to the next. Observing the difference that leadership made on the effectiveness of officers and crew in carrying out their missions gave me some insights into the practical effects of leadership. It may have been only coincidence that leadership varied so much from one ship to another, but the magnitude of variation made the picture very clear.

(U) Taking the leadership of the first destroyer (USS *GYATT*) as a baseline, the officers and crew seemed to be of average competence, and morale was about average for ships in the Mediterranean at that time. Command reacted to problems of training and morale rather than anticipating and controlling them. Reaction was quick enough to avoid major problems, and well guided enough to get the job done.

(U) The Commanding Officer (CO) was not known by the average crew member except as an authority figure. He relayed all instructions and commands through his Executive Officer and down the chain of command. That is the norm throughout the Navy, and works well when exercises are large and diverse enough to leave little slack time. It does not work as well when a great deal of time is left unoccupied, while supplies are at low levels from lack of replenishment opportunities, and recreational facilities during port calls are minimal.

(U) The second destroyer was USS *O'HARE*, which we boarded in Gibralter where she arrived after a stormy Atlantic crossing during which an accompanying destroyer was overrun and sunk by an aircraft carrier. Our small detachment was very favorably impressed on our first visit to USS *O'HARE* to survey our working spaces. The crewmembers on the Quarterdeck (the area aboard the ship at the end of the gangway) were noticeably sharper and more courteous, and the ship was cleaner and in better repair than *GYATT*, in spite of the rough crossing.

~~(FOUO)~~ We left Gibralter and returned immediately to the Eastern Mediterranean. On the day before our first port call in Greece aboard *O'HARE*, the CO mustered all hands on the fantail (the open stern of the ship) and delivered an interesting talk on the area that included local points of interest as well as historical highlights and a brief on local customs. He emphasized the point that we (the crew) were to be ambassadors of good will, and desired that we make a good impression on the local population. He saw to it that sightseeing

tours were organized for those interested in them, and arranged for sporting events (softball and soccer) for others. The difference in crew conduct ashore and in our (COMUNIT 32D) perceptions of this port were radically different from our two visits aboard *GYATT*.

(U) During that visit and subsequent ones to other Greek and Turkish ports, all preceded by talks delivered by the CO or another of the officers. I do not recall a single serious breach of discipline. We had been used to seeing at least a few fights and/or drunk and disorderly incidents on previous visits of *GYATT*. We soon became aware also, of the reason that the ship was in such good repair and clean condition. The CO and his officers had fostered a spirit of friendly competition between the two leading Boatswains Mates (those Petty Officers responsible for repair, upkeeep, and seamanship) which resulted in fast, efficient repair and cleaning of anything in their areas of respnsiblity. A spirit of pride in their work and friendly cooperation existed among the other departments of the ship also, resulting in the award of several E's (official awards for excellence) to the ship.

(U) After such an enjoyable tour aboard *O'HARE*, we were ill-prepared for our introduction to USS *KNAPP* on a miserable, rainy day in Plymouth, England. The *KNAPP* sent a whaleboat to pick up our unit, and when the Coxswain (the Petty Officer in charge of the whaleboat) discovered that he was to take aboard equipment as well as crew, he refused to do so. After some discussion with *O'HARE*'s Officer of the Deck, he agreed to take both equipment and crew, but we were offered no help in loading or unloading. When we finally got aboard *KNAPP*, we found that our assigned work spaces had no usable antenna connections, and the antennas that had been installed some time before were not in operating condition. We had to do all of the repair and installations ourselves.

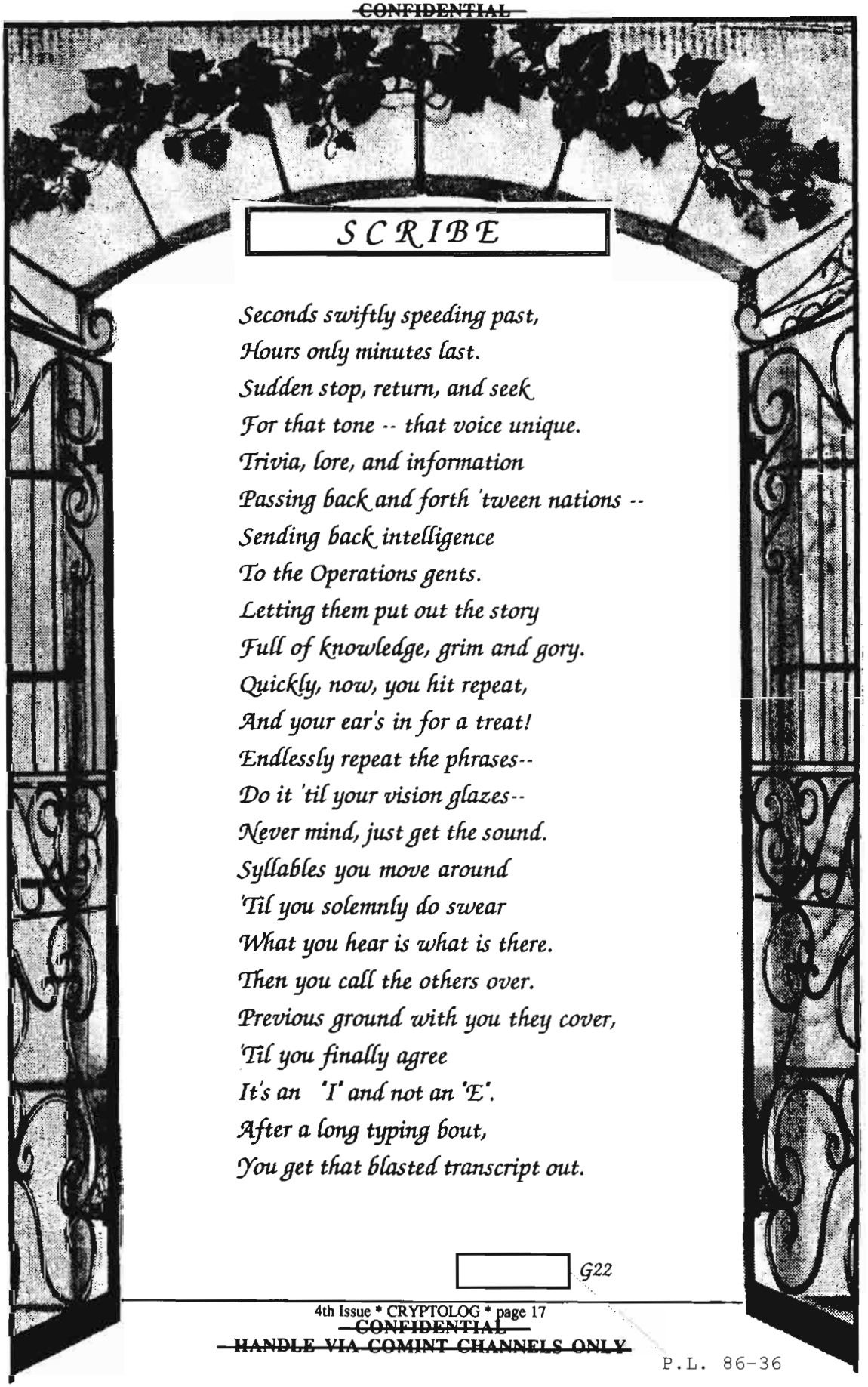
(U) It came as no great surprise after that to see the large number of crewmen returning aboard drunk from liberty in Plymouth, and other places later. There was rivalry between factions of the crew of *KNAPP*, but it was not the friendly rivalry we had observed in *O'HARE*; *KNAPP*'s crew often were involved in drunken brawls between factions.

(U) I cannot recall ever having seen the *KNAPP*'s CO, but his reputation was well known to all of the crew. He was said to prefer drinking with some enlisted crewmembers to spending time with his officers, by whom he was not well regarded. He was alleged to have been arrested for drunken driving by Military Police in Rome, where he had driven a jeep which had been assigned to *KNAPP* from a Navy motor pool in Trieste for use by ship's officers. It seemed to us in COMUNIT 32D that the poor crew discipline and *KNAPP*'s generally rundown appearance and condition were a direct result of the negative influence of the CO.

(U) Differences in leadership in the three destroyers was also evident from the examples of seamanship that we observed while aboard. *GYATT* was generally competent, and did a good job of maintaining station and maneuvering during exercises and while coming alongside a tender or tying up to a dock or pier. *O'HARE*'s crew distinguished themselves by the precision of her movements, whether maneuvering in restricted waterways or tying up to a dock in tricky winds and tides. *KNAPP* generally was able to maneuver competently under favorable conditions, but her crew was not able to deal well with unfavorable circumstances.

(U) One remarkable example illustrates the great difference between *O'HARE* and *KNAPP* - the ships with the two most widely different commanders. Both spent two weeks in a course at the Antisubmarine Warfare School in the Foyle River near Londonderry, Ireland. During the course, each had to refuel at the dock in the Foyle River. The river at that point is rather narrow and the current swift. The maneuver required an upstream approach, a 180-degree turn, and ended with coming alongside the fuel dock from upstream. *O'HARE* made the upstream approach and dropped her port anchor when about two ship-lengths upstream of the fuel dock, reversed one engine and swung around the anchor (like a child around a lamp post) and ended in perfect position to back upstream against the dock. *KNAPP* made her upstream approach and turned without using her anchor, which left her drifting into the fuel dock as she attempted to back alongside. Irish linehandlers on the dock were forced to scramble quickly to avoid *KNAPP* as she tore up six to ten feet of the pier before stopping. □

DOCID: 4019712



SCRIBE

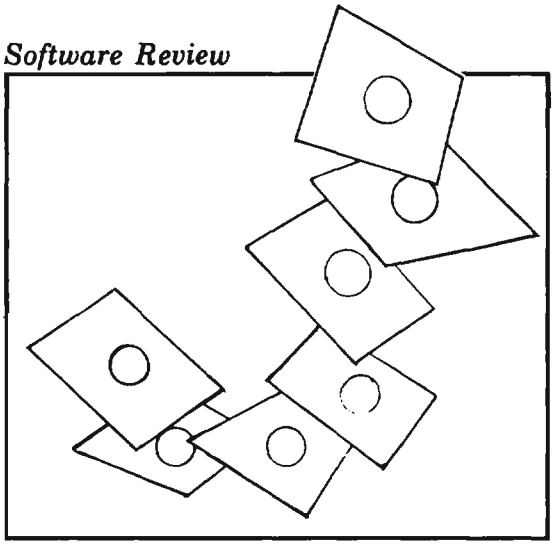
Seconds swiftly speeding past,
Hours only minutes last.
Sudden stop, return, and seek
For that tone -- that voice unique.
Trivia, lore, and information
Passing back and forth 'tween nations --
Sending back intelligence
To the Operations gents.
Letting them put out the story
Full of knowledge, grim and gory.
Quickly, now, you hit repeat,
And your ear's in for a treat!
Endlessly repeat the phrases--
Do it 'til your vision glazes--
Never mind, just get the sound.
Syllables you move around
'Til you solemnly do swear
What you hear is what is there.
Then you call the others over.
Previous ground with you they cover,
'Til you finally agree
It's an 'I' and not an 'E'.
After a long typing bout,
You get that blasted transcript out.

G22

~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~
P.L. 86-36

DOCID: 4019712

Software Review



RIGHTWRITER, by Rightsoft, Inc. 2033 Wood Street, Suite 218 Sarasota, Florida 34237

GSA price $56. Upgrade, $5. additional.

Reviewed by: [ ] *P13*

P13 has been reviewing recent software that DDO analysts might consider buying.

One of these is **RightWriter**, which evaluates a document for grammar, style, usage, and punctuation. The program creates an output file consisting of the original text interlineated with comments and suggestions. It provides an overall critique, a measure of the grade level of the writing and the "strength of delivery." It flags jargon and clichés and concludes with a list of words in the document that should be reviewed. There is also an option to provide a frequency count of all words in the document.

The manufacturers claim that the program is compatible with most word processors including OfficeWriter, the agency standard. Output files match the format of the input files.

We found the program easy to use, with a better-than-average user's manual. It is designed as an aid for business and technical writing, and we highly recommend it for that purpose. The writing hints in the user's manual would benefit other writers as well.

In summary, a good buy.

Note: the passage delineated by lines was run on RIGHTWRITER. The results are shown on the facing page.

System requirements:

- Minimum Internal Memory: 384K RAM
- Minimum Disk Configuration: Two dual sided diskette drives or one diskette drive and a hard disk
- Operating systems: PC-DOS, Version 2.0 or higher; MS-DOS, Version 2.0 or higher; OS/2
- Computers: IBM PC, PC-AT, and PS/2, and all MS-DOS compatibles. (Special versions are available for DOS earlier than 2.0 and for memory sizes smaller than 384K.)

~~FOR OFFICIAL USE ONLY~~

Output from RIGHTWRITER

<<** SUMMARY **>>

Overall critique for: D:\RIGHT\soft2.txt
Output document name: D:\RIGHT\soft2.OUT

READABILITY INDEX: 8.87

```
4th        6th        8th        10th       12th       14th
  |****|****|****|****|****|     |     |     |     |     |
SIMPLE      | ------ GOOD ----- |                  COMPLEX
Readers need a   9th grade level of education.
```

STRENGTH INDEX: 0.92

```
0.0                          0.5                          1.0
  |****|****|****|****|****|****|****|****|****|     |
WEAK                                                 STRONG
The writing has a strong style.
```

DESCRIPTIVE INDEX: 0.60

```
0.1                  0.5                  0.9        1.1
  |****|****|****|****|****|     |     |     |     |     |
TERSE  | ------------ NORMAL ------------ |      WORDY
The use of adjectives and adverbs is normal.
```

JARGON INDEX: 0.00

SENTENCE STRUCTURE RECOMMENDATIONS:
15. No Recommendations.

<< WORDS TO REVIEW >>
Review this list for negative words (N), jargon (J),
colloquial words (C), misused words (M), misspellings (?),
or words which your reader may not understand (?).

RightWriter(?)	1	compatible(?)	1
critique(?)	1	evaluates(M)	1
interlineated(?)	1	jargon(N)	1
reviewed(?)	1		

<< END OF WORDS TO REVIEW LIST >>
<<** END OF SUMMARY **>>

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019712

CONFERENCE REPORT

The American Mathematical Society Centennial Celebration, August 1988, Providence, Rhode Island

Reported by: David Harris, R51

Several Agency personnel attended the Centennial Celebration of the American Mathematical Society. The celebration featured invited talks by eighteen prominent mathematicians surveying the present state of American mathematics. It also featured some discussion of where mathematics is going, a discussion generally dominated at this conference by the applied types interested in improving the ties of academic mathematics to the users of mathematics in the real world, be they DoD, physical and social scientists, or industry. The left wing of the academic world, winner in last year's referenda on relations with DoD, was conspicuously quiet.

The managers of the society were apparently minded to try to undo some of the political harm from last year's debates by advertising and supporting better relations with applied math and its sponsors. The world of mathematics nearly always has known some conflict between applications-driven mathematicians (say Herman Weyl) and purists (say Bourbaki). Some of the best math now is being done by non-mathematicians. Organizers of this conference made an apparent effort to sell applied areas as a source of good math and good problems. Applied scientists can be a source of wisdom on what problems should be worked on, as well as an inspiration. But traditionalists resist. The establishment was clearly trying to show that it realizes applied science has a role to play.

EVALUATION

I think that conferences like this are a convincing argument for the importance of having Agency people travel to at least selected conferences. I would hope the Agency would continue to try to keep our program of attending outside conferences alive, despite the budget crunch. In my view, it is foolish to spend money on supporting academic research, and fail to gather up the material that is presented to us at conferences for such relatively low cost. It would be self-defeating to let our ties to the outside atrophy for lack of money. All our previous efforts and expense would quickly be wasted.

SUMMARY

The technical highlights of the conference included an excellent minicourse by Gene Luks on Groups, Graph Theory, and Computer Science and a related talk by Aschbacher on recent developments in group theory exploiting the classification theory, very interesting talks on the interaction of physics and mathematics by Jones, Kac, Uhlenbeck, and especially Witten; a talk by Gross on modular forms and elliptic curves; a somewhat disappointing minicourse by Assmus and Key on Coding Theory and Finite Geometries; and talks by Caffarelli, Diaconis, Fefferman, Freedman, Friedman, J. Harris, Howe, Majda, Peskin, Sullivan, Tarjan, Thurston, Bott, and Lax.

In my personal opinion, the most awe-inspiring talk was Witten's on the relationship between quantum field theories and the future development of mathematics. He argued convincingly that many of the recent breakthroughs in math can be understood in terms of quantum field theories, and that theoretical physics can serve as a guide to new directions for mathematics. This possibility was illustrated by Jones' talk on knot theory, Kac's talk on modular forms, and by Donaldson's work on 4-dimensional manifolds. For details of the technical talks, please see my trip report.

Perhaps equally important was the political side of the conference. The political talk at the meeting was for once generally pro-DoD, and

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019712

anti the usual academic mathematical establishment. Especially outspoken were the talks by Peter Lax, a former president of the AMS, and Edward David, otherwise known as head of a commission that helped to convince the government to increase its support for academic mathematics. They both had many critical things to say about the lack of effort by academics to help deal with the current and future crisis in recruiting more American-born mathematicians.

David stressed the dangers of getting involved in politics. Once the math world declares itself political on any issue, politicians will cease to view its opinions as based on expertise, and will instead judge it as a political ally or enemy. This has heavy long-term consequences for mathematics support by government. David mostly gave the academics the bad news that they are failing to do their share of the job, and that they had better get out of politics and get to work in preserving mathematics as a profession. The mathematicians were repeatedly told that math is in competition with welfare and housing the poor. So, mathematicians must expect to be held to meeting their social obligations if they expect funding.

Lax gave what the president of the AMS called a blunt speech roundly criticizing many in both the pure and the applied mathematics communities. The anti-DoD resolutions of last year have clearly left much hard feeling, and the establishment was keeping its mouth shut to try to avoid making further trouble.

Another interesting event at the conference was a JPBM-sponsored meeting on the MS 2000 program and the abuse of MAs as teachers in academia. It was never quite clear however whether the intent was to deplore the practice of exploiting masters holders by using them as underpaid temporary help without benefits, or whether the intention was to educate department chairmen on the best way to do exactly such exploitation!

As usual, we engaged in a considerable amount of informal discussion with academics, both for purposes of improving our general image, of finding out what is going on in academic mathematics, and of ultimately aiding recruitment.

POLITICAL SPEECHES

Opening Ceremonies

Perhaps one could look on this opening ceremony as indicative of the lack of understanding by laymen of what professional academic mathematicians do and how they view themselves. Neither the governor nor mayor showed up for the opening ceremonies, despite the fact that AMS is an employer in Providence. The governor sent his policy advisor, Valerie Southern. The mayor sent Joseph Almagno, the Superintendent of the Providence School Department, apparently under the mistaken impression that the members of AMS are teachers. Brown University. sent Phillip Stiles, Dean of the Graduate School/Research.

The London Math Society and the MAA exchanged presents with AMS. SIAM accepted a present from AMS but gave none that I know about (in keeping with the general skepticism by applied mathematicians throughout the meeting about the attitudes of the pure mathematicians of AMS.)

President Reagan sent a letter, indicating his staff has some awareness of AMS's activities, and stressing the role of mathematical skills in maintaining "...our domestic prosperity, our national security, and our competitive stance in the world marketplace...That's a challenge I know you're ready to meet." Not if the members of the AMS can help it!

Governor DiPrete could not come because of the National Governor's Conference. His aide showed little appreciation of the noble role pure mathematicians assign themselves. She spoke of the 50% high school drop out rate in Providence, of the remaining students that cannot really read or write, and want less technical schooling. DiPrete opposes this, and wants more engineers, biomedical workers, scientists. The members of AMS are the role model for them. DiPrete wants to forge a partnership to guide our children and society. President Mostow reacted by calling this a message we rarely get, but appreciate (i.e., don't call us about such a partnership, we'll call you.)

Next, Joseph Almagno spoke. He said, we need you to help public education. The public is losing confidence in our product. We need to retool, reshape, and find better methods. He

~~FOR OFFICIAL USE ONLY~~

apparently thought he was addressing an audience interested in education. He did not understand the role of the AMS as inventors of the truth of pure mathematics. Instead, he hoped they could help him with the problem of non-English speaking students, largely Hispanic and Southeast Asian. How can we teach them? Apparently, the differential geometers and algebraic topologists should show the way.

Phillip Stiles from Brown spoke of the long record of collaboration between AMS and Brown. Brown reaffirms its commitment to math and its outstanding math library (by which he meant they had recently bought a large collection of ancient mathematics manuscripts.) Brown University Mathematics Dept. was conspicuous by its lack of active participation as such at the meeting. For example, there was no effort to encourage mathematicians to visit the department. A search on foot allowed me to locate the Brown Mathematics Department building, in an outwardly unprepossessing old Victorian house. This was rather in contrast to the Applied Math and Engineering buildings, or for that matter the History of Mathematics Dept. quarters.

After the Presidents of AWM and the London Math Society had congratulated AMS and given it some gifts, Bill Gear of SIAM spoke. Math is the infrastructure of our future progress. SIAM and AMS must work together. We are all developing countries, and mathematics is at the heart of the process. We must have a literate population applying math to the problems of the real world. The distinctions between engineers, scientists, and mathematicians should be blurred, and we should all work together, unlike the traditional disdain of mathematicians for all these others.

In particular, funding is now in the hands of democratic institutions, which means that sciences must work to inform the public if they want money. Show that math is significant to the public. Integrate math into the world. All these points were repeatedly made by the applied mathematicians at the conference, but are distinctly distasteful to the true mathematicians. They are at variance with the sentiment expressed in the overwhelming support for the anti-DoD resolutions of the AMS last year. The organizers of this conference, however, did seem to stress by their choice of talks precisely the importance of non-mathematicians to the future of mathematics.

Finally President Mostow spoke. He said that math today is so diverse that no one person can describe it all. Few people know the breadth and depth of the influence of math. The computer revolution shows, if anything, the invisibility of math in the world at large. The educated public does not share our enthusiasm for the subject. We must make efforts throughout education to find opportunities to expose people to real mathematics. AMS must get involved in this. Math will be permeating the world. So we are feeling our way towards a solution.

Future textbooks on the history of ideas should give mathematics its proper place. This will encourage youth to go into math. The role these textbooks give math is totally opposed to the role most academic mathematicians would like to have, and are willing to fill! How do you keep this from turning off those students you have educated on the role of mathematics in the real world?

Edward David "Renewing U. S. mathematics: An agenda to begin the second century."

The highlight of the political activity at the meeting was the address by former Presidential Science Advisor, Edward David. He is remembered as the leader of a committee that wrote the David Report (see my Trip Report on the AMS Meeting in Louisville 5 years ago.) David was helpful in selling the government on increasing funding for mathematics drastically. Now he has come back to AMS to lecture the mathematicians on their failures as citizens and professionals.

He started by expressing his concern about how mathematics deals with its customer activities. After five years of pushing how have we done? Substantial progress has been made, but there is a long way to go, and the hour is late. Frank talk is needed. In the last five years, math support has increased considerably. You have been winning in the fixed sum game over your competitors such as housing for the poor and aid for the starving. But the major issue was renewing mathematics, and enabling it to sustain itself. That issue is more pressing than ever. In 1983 there were 800 new Ph.Ds. Now

DOCID: 4019712

there are 700 a year, and half of those are foreign.

The increase in funding has been almost equally from NSF and DoD. NSF gave high priority to support for grad students and post docs. Unfortunately, they did not help senior investigators. But the problem is bottoming out, salaries are skyrocketing, and this may change the common perception that the world does not want any more mathematicians.

The David Report asked for actions from universities in support of mathematics, but has gotten little such support from them. To the Universities, mathematics is not as worthy as other subjects if it does not bring in as much money. Mathematicians must unite to educate the world on the value of math and on its needs. The world thinks math exists; there is no need for any more mathematics, just teach the math already known. Ken Hoffman's lobby has been quite good at fighting this attitude. [Of course, Ken Hoffman's lobby has also taken a lot of heat from the Thurston branch of AMS precisely for selling math as useful to the real world, in ways that many mathematicians oppose.]

Next David addressed reform of education. Two boards of the NRC are currently working on school curriculum reform, and informing mathematicians of opportunities for cross-fertilization. This is the MS2000 project. But there are very tough political realities. There are budgetary restraints. Federal R&E is already 25% of the nondiscretionary budget. Math is competing with social programs, like housing and welfare. Science has incredibly been winning in this competition. But math cannot expect another 84% increase in the next five years. The highest priority is of course sustaining the quality of math research. There should be an update of the David Report every five years to document progress, evaluate university instruction, and overview research opportunities in the view of mathematics users. It should discuss how math should be supported. A mechanism for such an update is needed.

David said AMS must overcome last year's combative attitudes and recommit itself to its goals in Washington. Micromanaged, programmed government-sponsored research is inevitable. As at Bell Labs, perhaps government can choose the research field, but let scientists determine the direction of the research. There is a need to know what problems both the math and the user world think are important. What do your results mean for these *other* people. This may be done post hoc rather than ad hoc. Do the research, then look for how it may be sold to the outside world as useful.

AMS must work on its relation to the public - if only out of concern for keeping its share of the discretionary budget. We need political sophistication and cohesiveness, and must consider our responsibilities to society, and how we look to society. David said he is not calling for overcoming political activism. Mathematicians may offer advice to government in statesman-like ways. *But, mixing science with politics is poison. In Washington, if you try to use the prestige of mathematics to decide nonmathematical political issues, you will be treated as enemy politicians, and all your views will be rejected as political.*

Mathematicians must find better ways to attract young people to our field - NOT as currently, take it or leave it. The young have been leaving it in droves for adjacent fields. Even those in adjacent fields are appallingly ignorant of what mathematicians really do. Most students think we aim at winnowing out the weak and grinding down the ungifted. [They are right. Most outstanding mathematicians view the world differently from David, *not* a mathematician. There is only a comparative handful of people in any generation capable of making important breakthroughs in theoretical pure mathematics. They are of interest to us. The rest are a waste of our time.] Academic education should be a pump, not a filter.

David says we must improve mathematics education in our schools. We are a part of the educational crisis. The country is failing to educate youth in mathematics. We should help - and if we do, it will be appreciated. Twenty five million kids take mathematics in school; that gives mathematicians a big responsibility. [Elsewhere at the conference the "New Math" efforts of mathematicians to reform curriculum were discussed. These lead to doubts on this point. If mathematicians seek to make pure mathematicians out of the masses, they may end up messing up math education even worse. What is needed is an effort to talk with the masses in ways they will understand and find

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019712

convincing. It is rather doubtful that there are many members of AMS wanting to do this.]

In conclusion, David said our success in renewing mathematics has been mixed at best. We need new doctorates, and we must give them reason to believe that going into mathematics will give them a reasonable future. This will require the members of AMS to interact with schools, other disciplines, etc. Are they willing?

AMS BUSINESS MEETING and STEELE PRIZES

There was an amendment to the bylaws, voted without controversy, to change the way that dues are computed for institutional members. The effect is to break the connection between dues and the number of published articles from the institution, to the probable detriment of non-academic institutional members like the Agency. Several long-time employees of AMS were thanked. Then the Steele Prizes were awarded. Sigurdur Helgason won the prize for exposition. Gian-Carlo Rota won the prize for a fundamental research paper, for his work on the use of the Mobius function in combinatorial theory, and Deane Montgomery of IAS won the prize for cumulative influence on the profession. Paul Nevai, with whom I have had some interactions on the subject of orthogonal polynomials, got a job on an AMS committee. Mel Hochster, whom I knew in college, is one of the candidates for Vice President. William Browder will become the new President of AMS in December.

At the MAA Business Meeting, Steven Galovich and Bart Braden won Carl Allendoerfer Awards. James Epperson and Stan Wagon received Lester Ford Awards. Dennis Luciano, Gordon Pritchett, and V. F. Rickey won George Polya Awards. Seven Certificates of Meritorious Service were presented.

MISCELLANEOUS

AMS was organizing tours of the AMS Headquarters building in Providence. While I did not go on these tours, I did manage to go to the headquarters building to take a look around on my own. Not nearly as interesting as the wonderful little Rhode Island School of Design Museum of Art. I also recommend walking tours of College Hill and Federal Hill to see the interesting architecture. My wife spent much of her time in nearby Newport.

There was an AMS short course on chaos and fractals that I did not attend.

There was a daily newsletter throughout the conference, featuring such information as that Rhode Island was the first state to attempt to tax sexual intercourse. They also advised, when driving in Rhode Island, "never ever beep your horn at black Cadillacs with blackout windows."

INVITED TALKS

Michael Aschbacher (Cal. Inst. Tech.) "Representations of finite groups as permutation groups" (introduced by Daniel Gorenstein)

"The classification of the finite simple groups in 1981 changed the landscape of finite group theory and led to an increased effort to describe the structure and representations of the simple groups. Together with the classification, this effort has made possible unexpected applications of finite group theory in other branches of mathematics." In 1860, the French mathematics society offered a prize for the best research on the following problem: what are the possible indices m of subgroups of the symmetric group of degree n, and for such an m, what are the subgroups of index m? Several great men published work on the problem, but understandably made little progress, and no prize was actually awarded. The purpose of Aschbacher's talk was to show that finally we are beginning to be able to do this problem, and to illustrate how to use the classification theorem.

Luis Caffarelli (Inst. Advanced Study) "The geometry of solutions to nonlinear problems" (introduced by Louis Nirenberg)

Persi Diaconis (Harvard) "Sufficiency as statistical symmetry" (introduced by Gian Carlo Rota)

Charles Fefferman (Princeton) "Problems from mathematical physics" (introduced by Felix Browder)

This session covered two problems in mathematical physics. The first is from quantum mechanics and concerns how close our current state-of-the-art will take us to explaining why a roomful of hydrogen gas can

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019712

happen. The answer is quite close. The second is from general relativity and concerns a proof that some small enough initial disturbance will not become a black hole. As such it deals with a quite difficult analysis of the possible nature of solutions for a PDE.

Michael Freedman (UC-San Diego) "Working and playing with the two-dimensional disk" (introduced by William Browder)

Harvey Friedman (Ohio State) "The incompleteness phenomena" (introduced by Saunders MacLane)

Benedict Gross (Harvard) "Modular forms and elliptic curves" (introduced by John Tate)

This session surveyed some major developments in the theory of elliptic curves, the theory of heights, and rational points. Gross is married to Jill Mesirov, whom some of you may remember. According to Tate, they had a child two weeks before this conference.

Joseph Harris (Harvard) "Developments in algebraic geometry" (introduced by Phillip Griffiths)

Roger Howe (Yale) "A century of Lie theory" (introduced by George Mackey)

Vaughan F. R. Jones (UC-Berkeley) "A von Neumann algebra excursion: from quantum theory to knot theory and back" (introduced by Joan Birman)

Victor Kac (MIT) "Modular invariance in mathematics and physics" (introduced by Nathan Jacobson)

Upon hearing this talk I remarked that some deep mysterious truth was going on here. Witten's talk later explained to me what it is! Kac began by asking us all to sign the petition on behalf of Soviet emigrés available at the registration desk (a partial reminder of the role of immigrants in this celebration of math in America!)

Andrew Majda (Princeton) "Mathematical fluid dynamics: the interaction of nonlinear analysis and modern applied mathematics" (introduced by Peter Lax)

Majda advertised the importance of an interdisciplinary approach to applied math problems. These problems are too difficult to be handled by any one method, but can be reasonably well dealt with sometimes by combining attacks via new computational methods to guide research, experimentation (with physical models for example), suggestive rigorous theoretical analyses of simplified mathematical prototype models, etc.

Thus fluid dynamics is governed by a complex system of nonlinear PDEs with features of all kinds of PDEs. The key new ingredient allowing the interdisciplinary approach is the use of computer simulation to guide research and test models and conclusions when experimentation is unreasonable. This situation is a paradigm for even worse applied problems, such as oil recovery, combustion, elasticity, and magneto-fluid dynamics. This use of gas dynamics dates back to ideas of Lax.

Charles Peskin (Courant Institut.) "Mathematics and computing in physiology and medicine: Biomathematics from Hearts to Molecules" (introduced by Cathleen Morawetz)

Peskin gave yet another talk on the advantages of mathematicians working on applications rather than pure math. Here the problem is the mathematical modeling of functioning human organs, and in particular the designing and testing of heart valve replacements. Several articles of this sort are in the latest engineering journals. Similar problems arise in constructing oil rigs that have parts subject to both slow and fast vibrations. Also, molecules undergo slow and fast vibrations.

Peskin described the problems of modeling heart valves, and illustrated with films done by computer simulation showing how hearts with various kinds of replacement valve would in fact function. Several possible valve designs can be studied this way, and dismissed as defective, or improved.

One molecular chemistry problem being modeled is how large molecules like DNA control the production of RNA, which creates protein enzymes, which in turn control the reproduction and action of the DNA. The "Genes in Action" model is by no means done, but is already being used to study the mechanics of molecules. Again the so-called stiffness problem, caused by the differing time scales within which nerve impulses and DNA operate, is the difficulty in doing the modeling.

FOR OFFICIAL USE ONLY

DOCID: 4019712

Dennis Sullivan (CUNY Graduate School) "Progress on the renormalization conjectures in dynamical systems" (introduced by Stephen Smale)

Robert Tarjan (Prof. Computer Science, Princeton) "Mathematics in computer science" (introduced by Ronald Graham)

After a general introduction to theoretical computer science, and the development of effective algorithms, Tarjan spent most of his time talking about his work on trees and operations on trees. He introduced rotation as a mechanism for balancing trees and keeping searches cheap. He argued then that balancing is not in practice a good idea. A possible answer is splaying (Sleator-Tarjan 1983).

William Thurston (Princeton) "Three-dimensional geometry and topology" (introduced by Lipman Bers)

Bers introduced Thurston with glowing praise. The talk he gave merited the praise.

Karen Uhlenbeck (Texas) "Instantons and their relatives" (introduced by S. S. Chern)

Edward Witten (Prof. Physics -Inst. Adv. Studies) "Quantum field theory and Donaldson polynomials" (introduced by Clifford Taubes)

To me at least, Witten's talk was the high point of the entire conference, giving a glimmering of where the grand synthesis will come from that Uhlenbeck, Kac, Jones, Tarjan, Thurston, etc. are looking for in their work. The point is that much of traditional mathematics can be looked at as related to 1-dimensional quantum field theory. The recent work of Jones and Donaldson are the first inklings of 3- and 4-dimensional quantum field theories. The Kac and Bott talks, as well as work by Gromov in Thurston's talk are inklings of a 2-dimensional theory. So, there is at least the possibility of inspiration for vast new areas to develop in mathematics out of this connection to quantum field theory. Witten's talk was a sketch of this connection.

Raoul Bott (Harvard) "The topological constraints on analysis" (introduced by Andrew Gleason)

Peter Lax (NYU) "Mathematics: Applied and Pure" (introduced by George Mostow) Alternative titles from Lax, "The Flowering of Applied Math in America" or "The Deflowering of Pure Math in America".

Mostow summarized Lax's talk as 'blunt'. It was. He said a lot of impolitic things that ought to have been said. This talk was part of the continuing counterattack by the applied people against the disdain for applied math by the academics. Lax started by mentioning the Bourbaki attitude that once dominated pure math, calling for math isolated from the rest of the universe, and internally guiding its own future growth. Lax said the great mathematicians of the past would have been horrified. Math and Applications are equal partners, feeding each other [controversy in the audience!]. Before 1945 applied math was treated shabbily in math departments despite some great examples.

Lax launched into a survey of recent work in applied math. Equal to the gains from computing caused by improved hardware has been the gain from clever software, algorithms, code, discretizations, etc. Computing forms an additional bond between pure and applied math. Integer programming, dynamic programming, optimization problems, and simulated annealing have become major fields. Lax described simulated annealing at length, especially attacking the traveling salesman problem via the Metropolis algorithm. He mentioned FFTs, the simplex method, fast matrix multiplication, Karmarkar's algorithm, and Knuth's book as major subjects.

Lax then described Sarnak's work on network design, which is done using the theory of automorphic functions and the Ramanujan conjecture. Then he talked of Smale's work on average case complexity, although he acknowledged that there are not many answers yet in computational complexity.

Lax then lambasted AI and catastrophe theory. He said AI set its goals preposterously high and exaggerated its achievements. He was particularly hard on Herb Simon's talk on BACON at the AMS meeting at Louisville (I worked over that talk myself in a trip report.) Lax cited several other skeptics on AI. He had similar harsh words for the advocates of catastrophe theory. Lax is a believer of sorts in the theory as such. But, the hostility of many is caused by stupid attempts to oversell what catastrophe theory is.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019712

Zeeman was an honored guest at this conference, representing the London Math Society. Lax quoted Zeeman at length on the virtues of catastrophe theory as a breakthrough, and then tore the quote apart. For example, he pointed out that the study of shock waves for PDEs dates back to Riemann, and is older than AMS or even the London Math Society of which Zeeman is president. He expressed skepticism that Zeeman did not know this.

The methods of applied math are sometimes rigorous (when this is practical, which is far from always). Otherwise, it must rely on asymptotics, experiments, simplifications to inspire intuition for further research. In the days before computers, these simplifications may have helped cause the bad reputation of applied math, and the unwillingness of pure mathematicians to work in this area.

World War II demonstrated the importance of math to the real world, which led to support for both applied math and math in general. The US Government provided this support, at first through ONR, then AFOSR and ARO, then through DOE (the successor to AEC). NSF took over much of this funding later on. The AMS proposal to reduce DoD funding is offensive to many of us. It implies we are doing something wrong when we accept government money to fund our work. We object.

Immigrants to the United States were responsible for pushing applied math in the old days. To them, it was inexcusable not to look to the applied world for advice on what problems math should be confronting. For example, von Neumann and Weyl were dominant figures in American math that felt this way.

Finally, Lax spoke of the need to change our educational system. As for calculus, he said he was one of the "doubting Thomases" (groans at the pun!) Lax thinks we should replace calculus by a new style calculus course oriented towards applications. UMAP can serve as a source for such.

Saunders MacLane (Chicago) "Some major research departments of mathematics" (introduced by Leonard Gillman)

MINICOURSES (*I attended two of the seven.*)

"Contributions of algebraic coding theory to finite geometry" E. F. Assmus (Lehigh) and J. D. Key (Bryn Mawr).

[Handout, surveying parts of the course, is available.] This minicourse suffered from the ravages of the MAA support personnel. They changed the room for the course without telling half the participants. As a result, half of us missed the first half of the course. The second half of the course had all the students, but was held in a ludicrously hot and unfavorable classroom environment. After an hour, Key wilted to the extent of not being able to go on. After another hour, Assmus was soaked to the skin. Why the originally scheduled, air-conditioned room was not used I do not understand. The course served as an introduction to linear codes and their connection to designs and finite geometries.

"Groups, graphs, and computing" Eugene M. Luks (Oregon).

[Handout, rather incoherently surveying parts of the course, is available. In addition to the handouts that were supplied at the course, Luks mailed us a better version, one representing properly the various overlays he used with his overheads, as well as a reprint of an article, "Isomorphism of Graphs of Bounded Valence Can be Tested in Polynomial Time" that led to some of this work, and that originally appeared in August 1982 in *Journal of Computer and System Sciences*.]

Though it was given in the same impossible environment as the second half of the Assmus course, this course went splendidly. The classroom was not quite as unpleasant. But, mostly, this was because of the presence in Luks of a true expert, lecturing about the state-of-the-art of an important subject that he clearly loves. The course dealt with a paradigm for solving computational group theory problems, together with many examples. Ultimately the goal is to come up with ways to use the classification of finite simple groups, and divide-and-conquer, to improve computer algorithms. The role of the connection between group theory and graph theory is central to how Luks suggests doing this. □

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019712

P.L. 86-36

QUOTE WITHOUT COMMENT

Extract from

BANANA, The Story of a Fruitful Diagnostic Enterprise, G42 TSR05-88, March 1988

by [redacted] *G424*

Cryptologic diagnosis is not an activity for the insecure. It may be thought of as a mental wrestling match against an opponent who is assumed, not known, to have some weakness. The diagnostician must be prepared for a long, possibly futile struggle. He must have enough confidence in his abilities to mount a relentless attack even though the referee may be the opponent's mother. Rather than give up in a particularly tiring match, he merely takes time out to face other opponents, only to return with some new moves.

Unlike most other members of the cryptanalytic community, the diagnostician is not armed with the hard knowledge of his opponent's game plan—no sacred diagrams. He must possess an even more thorough knowledge of principles and techniques than his non-diagnostic colleague in order to seize the advantage on his adversary. To add insult to injury, his successes seem trivial to those who have never been in his shoes. Diagnostic success is often shrouded in secrecy, making it even more difficult for the diagnostician to enjoy the cryptanalytic limelight. With his chances of fame and even respect somewhat limited, the diagnostician presses on secure in the knowledge that he is working in the most difficult and creative area of cryptanalysis.

~~FOUO~~

To the Editor:

(U) In response to your editorial in the 3rd Issue 1988, I wanted you to know that at least one Key Component, T, has a "Yellow Pages." Here's a copy for you. Others can be had for the asking.

Jim Devine, A/DDT

The Editor replies:

(U) Thanks! And, dear readers, some of the pages are yellow!

To the Editor:

P.L. 86-36

~~(FOUO)~~ [redacted] article on the language programs (2nd Issue 1988) was very good. My experience with the language reserve program leads me to believe that is should be more widely advertized among the managers, not just the retiring linguists. I also sense that most managers and linguists interpret the wording "the director can call upon in emergency situations" to mean crisis or almost warime situations. In my case, in G Group, it was a critical shortage in the field and the need to fill the spot for a longer than average TDY period, e.g., several months.

~~(FOUO)~~ Thanks to the willingness of the linguist, the preserverance of the managers, and assistance from P16, we were able to overcome the initial hesitancy from some quarters to defining our language problem as fitting the criteria of emergency and of requiring directorate approval. It was a successful endeavor.

(U) [redacted] perceptions as SUSLO-2 were very interesting also.

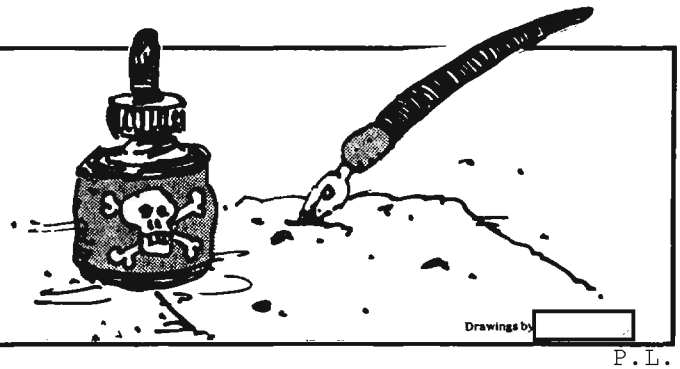
[redacted]

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019712

LETTERS



P.L. 86-36

To the Editor:

I recently received a copy of the article, "A Reform in Need of Reform" by [redacted] published in *CRYPTOLOG*, 2nd Issue 1988. Some of the things I read truly amazed me, and I would appreciate an opportunity to offer a moderately vigorous rebuttal. The points with which I wish to contend are synopsized below:

The author believes that the current NSA software acquisition methodology is hindering software acquisition, that our software customers are well aware that the process is not working, that the finance people know we are paying more for less, and that our Office and Group Chiefs feel weak and uncomfortable because all they can do is throw their hands up and go for a quick-response solution. In a curious contradiction, the author acknowledges "that the software being delivered today is cleaner and easier to maintain than in the past, but ... in terms of costs ... the trade-off is unacceptable."

The article states, "Incontrovertibly, contractor-developed software comes at a much higher cost than in-house developed software ... software developed out-of-house is costing the Agency perhaps four to nine times what it might otherwise cost."

The author proposes that we produce software using a method loosely patterned after a level of effort contract. As I understand from the article, software developers should be assembled into small groups, and assigned small portions of a large system. The software developers will get a general idea of the customer's problem, produce some software that they think is approximately what the customer wants, and demonstrate it to the customer. If the result is not exactly what the customer wants, the developer will simply rework the software until the customer is happy. If the customer or the developer happens to think of something else the software should do, the developer will just add it in. Conferring continually with the customer, the teams will carry on, adding functions as knowledge is gained, correcting course as necessary, and documenting as little as possible until the team and the customer agree that the job is done. The article suggests that if we follow this formula, the software developers will be productive and happy, the customers will be undisappointed, and the "malaise" that has so cruelly afflicted our Office and Group Chiefs will be forgotten as they busily reallocate something like seventy-five to eighty-nine percent of their software acquisition budgets.

The method..that the author proposes to replace current software acquisition policy seems laissez-faire to an extreme. Nothing could be planned more than a few weeks in advance, because the customer might change his mind or there could be a dramatic technological breakthough that will redirect the whole project. Without a plan, there is nothing to schedule; besides nothing is ever going to get done on schedule anyway. It would be wasteful to document before the software is finished, because there are no firm requirements, and no one really knows what the finished product is supposed to do. Never mind that the software developers, unstifled by the need to document and uncontrolled by firm requirements, may strike out on some wild tangent that comes to a deadend, and may need to reestablish what was done two weeks earlier, but cannot remember how they did that last tricky little algorithm that got altered during the wild tangent. Just continue this....method.., and one fine day the project will be finished.

In his article [redacted] impeached for reasons of greed or self-interest any witness who supported NSA software acquisition methodology. Before I try to counter some of

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

DOCID: 4019712

the positions taken in the article, let me defend myself against the charge of greed. I am never enriched by prolonging a project. I write no textbooks. I teach no courses. I am a software acquisition manager, and my rewards, such as they are, depend upon my ability to acquire software within cost and schedule. I confess to the charge of self-interest in this matter, but because of that self-interest, I am strongly motivated to transfer allegiance to any doctrine that promises to help me develop software within cost and schedule limits.

If there is a known method by which we can produce software on schedule at one quarter the cost of acquiring it under contract, I am willing to adopt that method instantly. Maybe the author is correct and we have been wasting three-quarters of our software budget. I certainly do not have figures to refute this estimate; does anyone know an accurate overhead rate or an authentic productivity figure for NSA software developers? Maybe the author can help me out here. Could I possibly see the research data that was developed to support this estimate

Perhaps the author will be surprised to learn that many of the contractors I have dealt with recently stand four-square on his side. If the contractors are being enriched by our methodology and documentation requirements, they are almighty ungrateful; the cry against NSA documentation requirements is almost universal among contractors. Most contractors have their own way of doing business, and are eager to demonstrate that their way "meets the intent of NSAM 81-2 and NSAM 81-3." They want us to accept their standards and practices, precisely because they are familiar with them, and we probably are not. They object to the amount of documentation we require. Usually they cite prohibitive cost, but I suspect they balk for the same reasons government developers do: they do not want those nosey parker software managers telling them what to do.

According to the article, the NSA acquisition policy reduces the productivity of our newly-hired software producers. These people have had the benefit of the "formalized" experiences of their predecessors, and are "far better prepared than their predecessors to analyze, design, implement, test, and document", yet they chafe under the yoke. They are stifled; the documentation requirements are "stultifying" and the methodology is "demotivating" (sic). They yearn to be free from the oppression of the wearisome NSAMs, which expect from them either too much or too little, depending on how you read the author's remarks. On one point the author is clear: "Agency [...] methodology is [...] in flagrant disregard of [...] Maislow, Herzberg, and Argyris."

I fail to see how our methodology violates the teachings of all the Management Hall of Famers. Using it, software managers can provide software developers with clear direction, unambiguous measures of progress, and frequent indications of accomplishment and success. All of these are Good Things, according to the Management Meisters. It seems to me that drifting through a project, with no clear indication of immediate or long-term goals, continually trying to patch new requirements into the software, with no real sense of accomplishment and no end in sight, would demoralize the new-hires more than having to document their work. I agree that today's developers are trained to "analyze, design, implement, test, and document". NSA software acquisition policy provides a framework of discipline that guides them while they do what they are trained to do.

If so much is wrong with our policy, and if so many people, including the newly hired, the contractors, the Data Processing customers, the financial people, and the author of this article, object to it, why does it remain in place? Who supports NSA software acquisition policy? I think most software acquisition managers do. I think the software support managers do. I hope and trust that my upper management does. Among us, we may often hold spirited and enthusiastic discussions concerning the proper interpretation of finer points in 81-2 and 81-3, but we have in common certain beliefs: software acquisition requires firm discipline; Life Cycle Support requires documentation; the NSAMs offer a way to achieve both. Whether it is perfect or not, our current methodology allows us to define and bound the software project, divide it into discrete tasks, estimate cost and schedule much more accurately, measure progress throughout the project, predict cost and schedule variances, and react decisively when such variances occur. As it happens, much of the documentation produced as tools with which to *manage* software

~~FOR OFFICIAL USE ONLY~~

production also serves another purpose: it helps the poor devils in Life Cycle Support organizations who must patch and mend the result for the next ten years. These people have one of the toughest jobs in the software world; ask them if it costs too much to produce clean maintainable software and the documentation to go with it.

Most of all, I hope our Data Processing customers support methodology and discipline in software the aquisition. As a result of front loading software acquisition efforts, the customer has reasonable expectations about what he is buying, how much he is going to pay for it, and when it will be ready. Reverting to desultory software acquisition is almost sure to result in a lot of disappointed customers. Without goals or requirements, without discipline and method, we cannot predict or plan events; if we cannot predict or plan events, we cannot estimate cost. The customer will never know what he is going to get, when he is going to get it, or how much it will cost, until after the project is over.

So I guess I am one of the author's axe-grinders. The axe I must grind remains the same whether contractors or govvies turn the stone: accountability. As a software acquisition manager, I am responsible for producing useable, maintainable software and the proper documentation on time and within budget. Therefore, I want control, or at least the illusion of control, of the software development process. I want to know what work is to be done, how much money is going to be allotted to the task, who is going to do the work, how the work is going to be done, how soon the work is going to be finished, how progress is going to be measured, and how success is to be declared. No additional work will be done without a written requirement, accompanied by a certified check, more people, or schedule relief. Furthermore, I want current information concerning how much work has been done, how much money has been spent, how much work is left to do, when we are going to finish, and how much it will cost in the end. In writing, please. NSAMs 81-2 and 81-3 provide guidelines and methods for managing software projects, and I need all the help I can get. Some software producers may find the process onerous, but for the most part, these people are professionals, and understand the need for a disciplined approach to software development.

The author of this article presented several other viewpoints that I would like to address. Some of his points are actually supported by the 81-2 and 81-3 philosophy, but he states those points so casually and offhandedly that one can easily overlook the implications of his reference. For example, he states that the critical ingredients of a successful project are "simple design", "prototyping", "incremental development", "small, tightly organized teams", and "minimal formality".

Aren't "tightly organized" and "minimal formality" antithetical? Still, I think I get the point: a small group of people working together without having to deal with outsiders, and without a lot of tiresome management types asking how things are going.

No argument from me about "incremental development". Paragraph 2.1.2.2 on page 2-3 of NSAM 81-3/DOD-STD 1703, dated 15 April 1987, is the definitive work on this subject, as far as I am concerned. The same goes for "prototyping", which is actually a subset of incremental development. Sorry, [redacted] but the projects I see these days just do not yield to "simple design". Apparently all the simple software has already been written, and the only projects we have left are devilishly complicated.

The author offers a solution to the complex software project ("If a project is large, it should be broken into smaller projects."), and likens the process to a diner eating steak. Strangely, he then leaves the subject and says nothing more about the tremendous system engineering effort required to implement the Sirloin Approach. The process of breaking a large project into smaller projects *is* the design process, and it is simpler said than done. The procedure is described in Paragraph 1.4, page 1-9 of DOD-STD-1703, which defines the design activities during software development. Traditionally, these activities consume forty percent of the total acquisition effort. Developing software is not very much like eating steak. It is a process of defining the basic parts of a system, manufacturing the parts according to specification, and assembling the parts into a working system. It requires thought, planning, organization, cooperation, discipline, and a lot of hard work. It requires

DOCID: 4019712

a lot of formality, too. Somebody has to document the requirements assigned to each segment of software, the input each expects, and the output it provides, because eventually all those segments must fit together to form a system that works.

The author does recognize the importance and difficulty of system integration, and masterfully reduces a task of imposing proportions to an elegant understatement: "Of course, the interfaces amongst the teams must be clearly defined, and the coordinator must do his job skillfully." You are only too right, sir. The "coordinator" may even have to introduce a little more formality, meaning an Interface Control Document, and a Software System Integration Plan. And a Configuration Management Plan; otherwise those highly-motivated software developers, in a high flush of "esprit de corps", will "respond dynamically to new requirements" and produce only "mimimal adequate informal documentation while development is fluid", and put the ICD and the Integration Plan down the sewer. And of course the "coordinator" needs to know when each piece of the software is going to be ready, which means . . . a Schedule! Here is Formality of the meanest sort, with assigned tasks, and deadlines, and people's names, and all like that so They know if you don't do your work. But not to worry, more than likely at least one other tightly organized team, unburdened by formality, is going to get tied up interacting with the customer and assimilating knowledge gained into the product, and will blow the integration schedule to hell before you do.

I suspect that [redacted] strikes close to the truth with one statement: "...the Agency has suffered great difficulty in developing large software systems using today's software acquisition methodology." If he refers only to software developed in-house, I will agree. But the great difficulty is not caused by our methodology; we have great difficulty because we will not accept the discipline and the accountability that goes with *any* methodology. I have been through some very large system acquisitions under contract, and have seen methodology successfully applied. Industry workers may not like it, but they accept the discipline and methodology, and it works. Industry managers have remarked to me that the government managers cannot or will not apply 81-2 and 81-3 standards to their own workers with the same diligence they display in applying it to contractor personnel. I believe the statement is true. If we allow our methodology to fall into desuetude internally, we will always have great difficulty developing large software systems.

Flexibility is built into NSA Acquisition Policy. The documentation required for system development depends upon the needs and intentions of the customer, and the type and size of the project. The policy itself so states; the Manuals 81-2 and 81-3 contain many words about tailoring documentation requirements to the needs of the project. If a manager takes exception to a particular requirement of the policy, there is usually relief available. If the leeway in our policy is inadequate [redacted] in T303, is always looking for a better method to develop software, or ways improve the method we use. He has always been willing to help me with such problems. In the meantime, our method may be all wrong, but it is what we have to work with.

[redacted] *R741*

P.S. I really need that study that compares the cost of developing software in-house with the cost of contracting for software development. My managers are excited about the potential savings. Could you send me a copy right away?

The author replies:

A careful reading of [redacted] *conclusion and my own shows us to be in basic agreement. Specifically, my paper concluded by calling for a review and reevaluation of the Agency's current software acquisition methodology.* [redacted] *in his conclusion, acknowledges that our method may be all wrong, but it is what we have to work with, which of course, is my point. I can only infer that he welcomes my proposal to review and revise appropriately, and I heartily welcome his articulate support on this matter.*

Admittedly, we have a few point of disagreement, but not on the need for discipline and control; from my experience, small teams usually possess and abundance of both commodities.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019712

I suspect our principal difference lies in what I would label "the knowability assumption" -- the basic premise upon which our prevailing acquisition methodology is based. Today's methodology employs a "waterfall" model of steps: identify and understand all requirements, document, design, code, test. However, my experiences at the Agency have led me to reject the notion that the desired system is knowable enough to document and design in cement at the outset; a tremendous amount of knowledge is gained through an interactive development process. With my approach, a fast start can be undertaken. with the knowledge gained rapidly assimilated into the process. And note: large teams get in the way of a fast start.

Yes, today's methodology provides discipline and control, but precious little in the way of timeliness. [redacted] *and I agree we would like to do better than we're doing. Let the review begin!*

To the Editor:

A while ago I bought a Russian-alphabet element ("golfball") for my Selectric typewriter. Every time I hit the letter Ж, it would print imperfectly: only part of the letter would print. Several phone calls to IBM in the Washington area finally got me to the "expert." He told me that on the Russian-alphabet element the Ж is in the position that is occupied on the regular element by the colon and semicolon. That position, as well as the position occupied by the period and comma, has reduced velocity, because otherwise the English punctuation marks would pound holes through the papers. The rest of the conversation went like this:

Me: But I want to type Russian words containing the letter Ж.

Him: Then you'll have to phone us and we'll send a technician to your home. He'll take the machine apart and reset the tension for that character.

Me: But what if I want to switch back to English again?

Him: Then it will punch holes through the papers.

Me: Do you mean to say that every time I want to switch back and forth, I've got to have a technician make a service call and reset the tension?

Him: That's right.

Me: That's impossible! I want to switch back and forth from English to Russian, sometimes even within the same sentence!

Him: Say, I've got an idea! How often do you need that letter?

Me: As often as it occurs.

Him: Well, then, why don't you just use other words instead? Or just leave out the letter completely?

I must confess, dear reader, that I was unable to explain to the "expert" over the phone that this would be comparable to having F. Scott Fitgerald type, " elda and I went to the oo today. elda loves the ebra with his ig ag stripes."

Art Salemme, Ret.

Art tells us that he has since switched to a word processor for his free-lance translations.

Readers may recall that Art was the Editor of CRYPTOLOG in the late 70s who set the tone for this rag with his sprightly and irreverent sketches. We've kept them in our portfolio for recycling, and show one of them in the previous column.

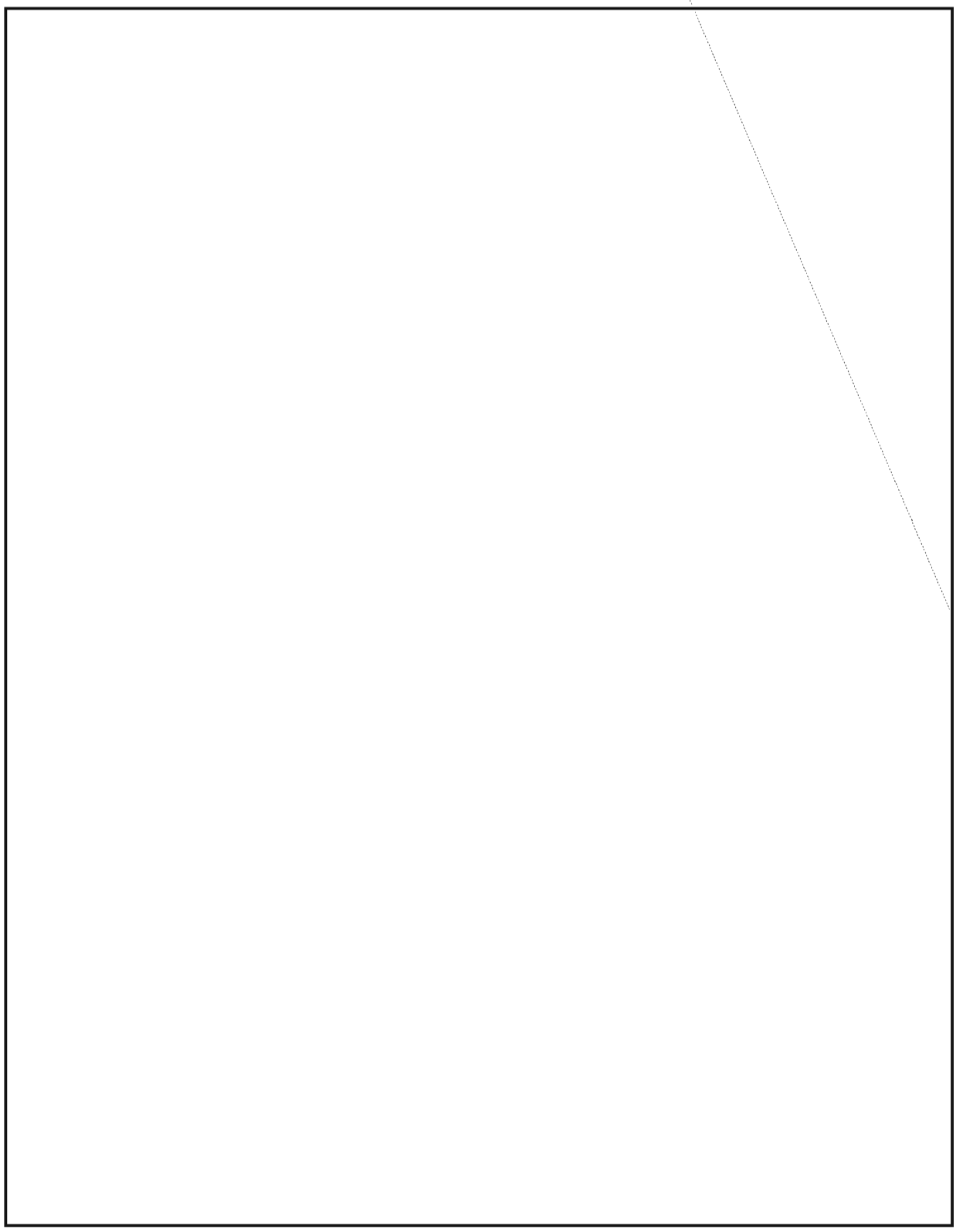
Art was pleased to learn that CRYPTOLOG is still going strong, and sends warm greetings to readers, editors, and contributors.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019712

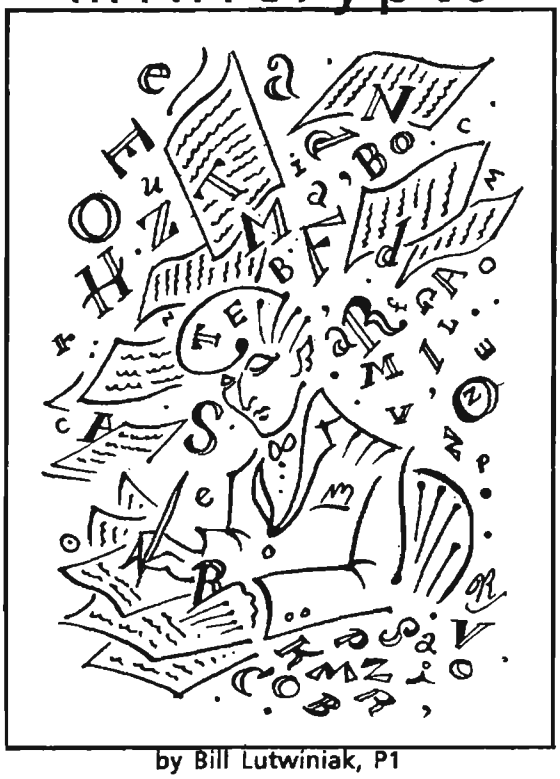
EO 1.4.(c)
P.L. 86-36

FROM THE PAST



DOCID: 4019712

minicrypts



by Bill Lutwiniak, P1

Years ago the New York Herald Tribune published a short cryptogram along with its daily crossword puzzle. There was a special ground rule -- every letter involved had to be used at least twice. Over the years constructors began to torment solvers with very short cryptograms which, while they conformed to the ground rules, were not very easy to solve. These held a strange sort of charm for some of us cryptanalysts, and they may still have appeal.

The other rules were intelligibility, of course, and that the plain text consist of a sentence of three or more words. There was no caption for the cryptogram, nor were proper names so indicated.

To illustrate how brief the minicrypt may be, consider:

A Father's day commercial

I SIS IS
A DAD AD

or

What's the kazoo for?

A SEES AS
I TOOT IT

or

What if Eisenhower Runs

A'PP PART ART*
I'LL LIKE IKE

(The asterisk indicates a proper name)

If this puzzle proves of interest, we'll publish more of them. We also solicit contributions. Here are three for this round.

KNIGHT AHAT TAGNKI

------ ---- ------

TRANRTYNE AY EY ETRA

--------- -- -- ----

SWOOSH KWYS PHOOHY SHO PWK PHH PH

------ ---- ------ --- --- --- --

SPECIAL OFFER

Just to get to moving on this initial round, a prize is offered to the first person or team to solve the minicrypts. Indicate whether the solution is an individual or a team effort.

Send your entries to CRYPTOLOG PUZZLE, P1, HQS. In case of a tie, the winner(s) will be selected by lot.

Readers in the Field may send entries via PLATMAIL to: c r y p t l g @ b a r 1 c 0 5. Field entries will be competing only with other field entries.

Solution to

LEFTOVERS *3rd Issue 1988*

1.	CORN	DEAN	SEND	RAIN	I
2.	STAR	BAIL	PITY	RAMP	M
3.	ADAM	ISIS	IRON	PAIR	P
4.	EXIT	LENS	LIVE	RILL	R
5.	APER	FORD	MERE	AIDE	I
6.	REAL	PIPE	TARS	LINT	N
7.	DIPS	MEAN	TALE	PEAT	T

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019712

NSA-CROSTIC *(plus)* No. 67

P.L. 86-36

G422

This puzzle has a user-friendly feature. The squares are numbered so that all squares on the left side have an even middle (tens) digit, while those on the right side have an odd middle (tens) digit. Further, all squares in the same column end with the same digit.

Fair warning: There's a wild card in this puzzle !

A. Where Crockett County is
B. Fixes
C. A kind of cheer
D. Like tropical rain
E. Poisonous herb
F. Fletcher
G. Mock Roman naval battles
H. Respite from work
I. Kind of production
J. World War II program
K. Rank
L. A canine
M. Anastasia, for one
N. Said *grazie* or спасиба
O. Relating to a letter
P. Religious fervor
Q. Astonishment
R. ***Hibiscus syriacus***
S. Inflammatory
T. Every bride has one
U. John Hancock used one
V. Necessities
W. Praise phrase
X. Specimens of ***xiphias gladius***

230	273	228	191	153	115	75	53	18			
255	235	84	102	40	3	27	71	111	133	194	
257	239	272	190	212	173	152	67	127	208		
226	200	113	137	195	170	192	99	117	70		
2	23	65	44	87	125	106	169	189			
112	51	46	85	144	130	213	271	233	251		
215	259	187	197	145	165	57	224	245	178		
164	211	269	60	42	1	35	11	28	72	52	
264	270	82	121	41	20	7	30	49	69	62	
4	123	141	220	132	2522	232	180	161			
205	79	10	151	244	122	253	166	157	68		
258	236	217	199	159	156	135	175				
210	207	181	240	221	260	160	140				
114	93	29	14	38	59	119					
128	150	168	146	100	64	61	43	25	5		
216	196	177	16	134	58	37	32				
238	186	73	54	94	91	109	149	129	172		
202	163	104	45	126	107	248	231	214	95	36	17
31	8	56	77	118	154	182	204	246	263		
247	218	90	86	47	12	136	176	24			
206	223	241	243	124	83	103	142				
232	261	203	183	167							
33	13	50	98	89	110	148	185	227	265	274	
225	250	268	266	9	21	101	80	76	97	138	

~~FOR OFFICIAL USE ONLY~~

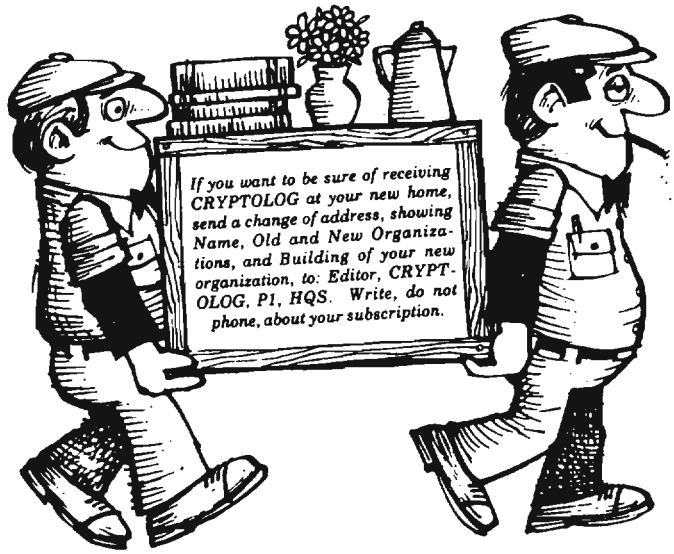
DOCID: 4019712

HOW TO SOLVE A DOUBLE-CROSTIC

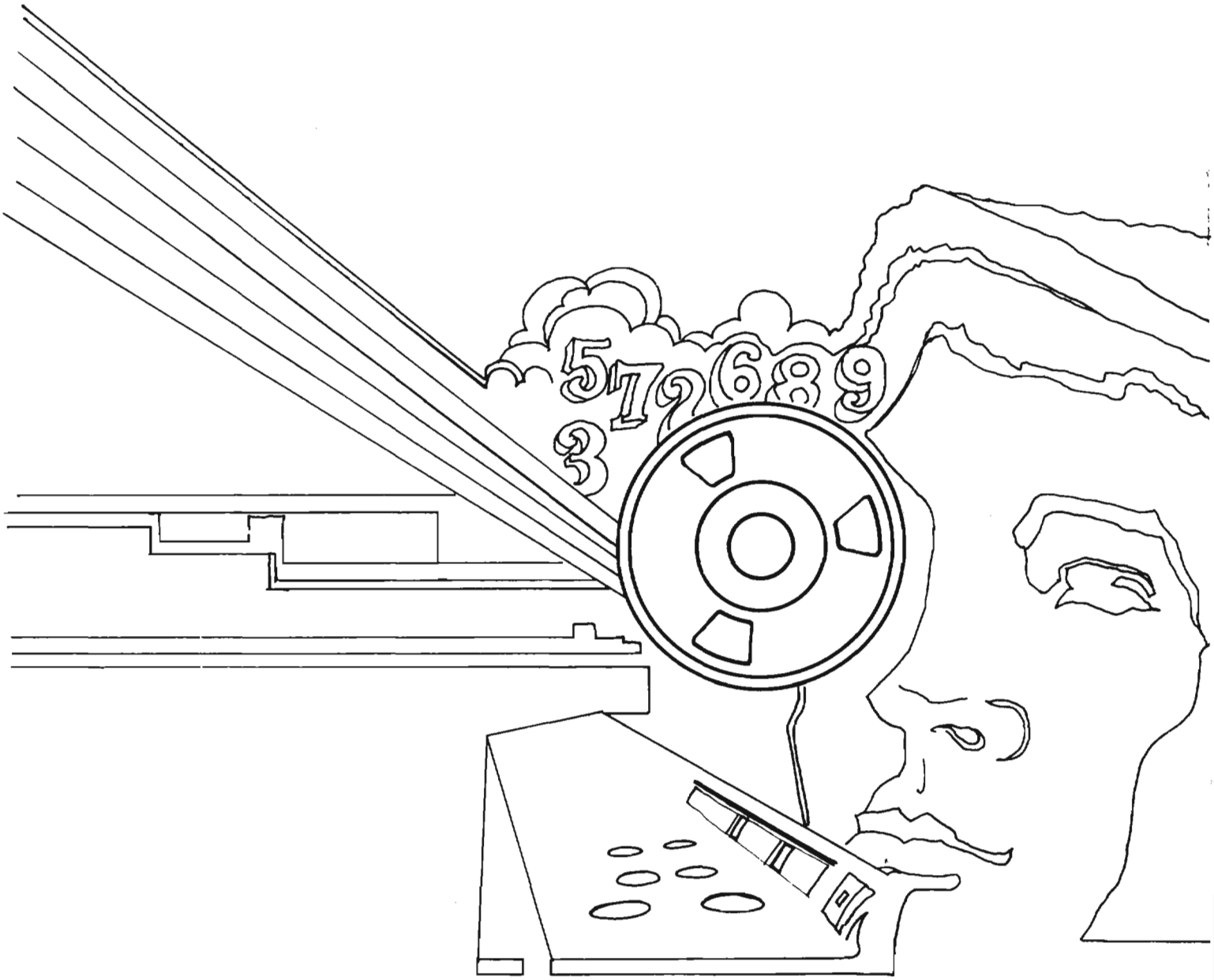
Using the Definitions, fill in whatever Words you can. Then copy each letter from the Words into the corresponding square of the grid below. Scan the text in the grid from time to time; from the recovered fragments you may be able to complete the word in context. Copy the new entries from the grid into the Definitions, where the fragments there might suggest a complete Word, and so on, working back and forth. Also, scan down the first positions of the Words as you recover them, for additional clues.

	1H	2E	3B	4J	5O		7I	8S	9X	10K	11H	12T	13W	14N		16P	17R	18A	
20I	21X		23E	24T	25O		27B	28H	29N	30I	31S	32P	33W		35H	36R	37P	38N	
40B	41I	42H	43O	44E	45R	46F	47T		49I	50W	51F	52H	53A	54Q		56S	57G	58P	59N
60H	61O	62I		64O	65E		67C	68K	69I	70D	71B	72H	73Q		75A	76X	77S		79K
80X		82I	83U	84B	85F	86T	87E		89W	90T	91Q		93N	94Q	95R		97X	98W	99D
100O	101X	102B	103U	104R		106E	107R		109Q	110W	111B	112F	113D	114N	115A		117D	118S	119N
	121I	122K	123T	124U	125E	126R	127C	128O	129Q	130F		132J	133B	134P	135L	136T	137D	138X	
140M	141J	142U		144F	145G	146O		148W	149Q	150O	151K	152C	153A	154S		156L	157K		159L
160M	161J		163R	164H	165G	166K	167V	168O	169E	170D		172Q	173C		175L	176T	177P	178G	
180J	181M	182S	183V		185W	186Q	187G		189E	190C	191A	192D		194B	195D	196P	197G		199L
200D		202R	203V	204S	205K	206U	207M	208C		210M	211H	212C	213F	214R	215G	216P	217L	218T	
220J	221M	222V	223U	224G	225X	226D	227W	228A		230A	231R	232J	233F		235B	236L		238Q	239C
240M	241U		243U	244K	245G	246S	247T	248R		250X	251F	252J	253K		255B		257C	258L	259G
260M	261V		263S	264I	265W	266X		268X	269H	270I	271F	272C	273A	274W					

MOVING?



~~FOR OFFICIAL USE ONLY~~



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~
~~NOT RELEASABLE TO CONTRACTORS~~

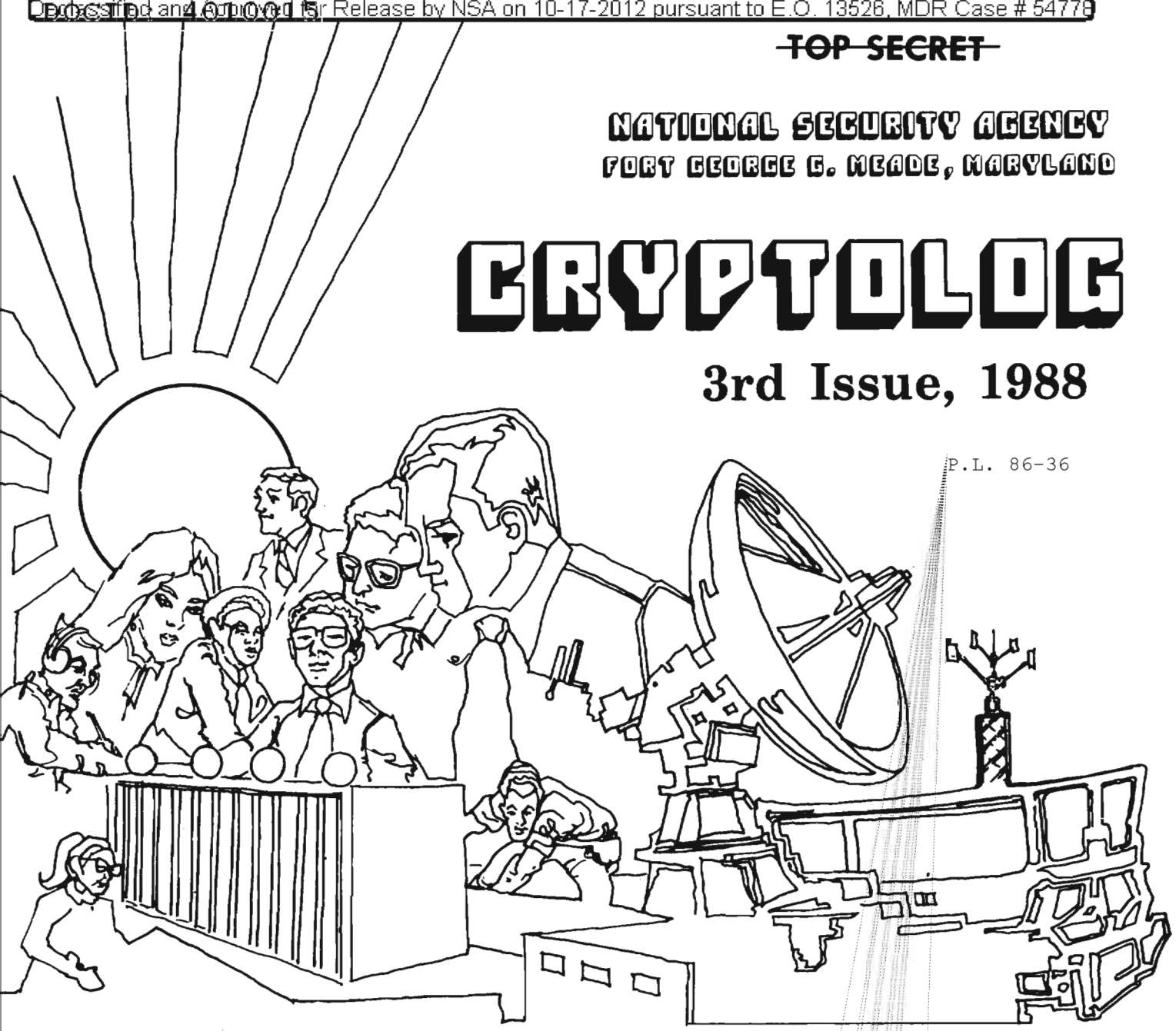
Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

3rd Issue, 1988



P.L. 86-36

CHANGES IN AGENCY REPORTING . . . . . [redacted] 1
SIGINT REPORTING PRINCIPLES . . . . . [redacted] 3
UPDATE ON PACKET RADIO. . . . . [redacted] 3
EMBARGOED INFORMATION . . . . . [redacted] 4
BULLETIN BOARD. 5
THE SHORT BUT HAPPY LIFE OF WIDEBAND. . . . [redacted] 6
[redacted] . . . . . N. C. Gerson. 9
LANGUAGE BRIEF: XHOSA . . . . . [redacted] 14
EXPO 88 16
CONFERENCE REPORTS: MATHEMATICS . . . . . [redacted] 17
LINGUISTICS . . . . . [redacted] 19
COMMUNICATIONS. . . . . [redacted] 22
ON THE LIGHTER SIDE 27
CALL FOR SPEAKERS 28
"LEFTOVERS" . . . . . [redacted] 29

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

EO 1.4.(c)
P.L. 86-36

~~NOT RELEASABLE TO CONTRACTORS~~

DOCID: 4010015

P.L. 86-36

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XV, No. 3 ..... 3rd Issue 1988

PUBLISHER: [redacted]

BOARD OF EDITORS

Editor ..... [redacted] (963-1103)

Collection ..... [redacted] (963-5877)
Computer Systems ..... [redacted] (963-1103)
Cryptanalysis ..... [redacted] (963-5238)
Cryptolinguistics ..... [redacted] (963-4740)
Index ..... [redacted] (859-4351b)
Information Science ..... [redacted] (963-3456)
Information Security ..... [redacted] (972-2122)
Intelligence Research ..... [redacted] (963-3845)
Language ..... [redacted] (963-3057)
Mathematics ..... [redacted] (963-5566)
Puzzles ..... [redacted] (963-6430)
Science and Technology ..... [redacted] (963-4958)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-4351)

Illustrators ..... [redacted] (963-4989)
..... [redacted] (963-3738)
..... [redacted] (963-6423)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five)
(note: no 'o')

Always include your full name, organization, and secure phone; also building and room numbers.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, HQS 8A187
Please do not phone.

Contents of CRYPTOLOG should not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

YELLOW PAGES FOR NSA

What NSA needs is Yellow Pages, just like the phone book, showing functional responsibilities. Or where to get information. Or even, how to found out how to get information.

What brought this to mind is a kind of inquiry that CRYPTOLOG often gets. Here's a typical exchange:

Reader: *I'm looking for articles on Project XYZ. It seems to me I read about it in* CRYPTOLOG.

Editor: *Let me check. [Pause.] No, sorry. Probably you saw it in* The Cryptologic Quarterly. *The two publications are often confused. Their number is 972-2355.*

[A week passes.]

Reader: *About that Project XYZ. CQ tells me that they didn't publish it, either. Do you know where else I can try?*

Editor: *Try STINFO, T513. Their number is 968-8611. They can do a keyword search in classified documents and in open sources as well.*

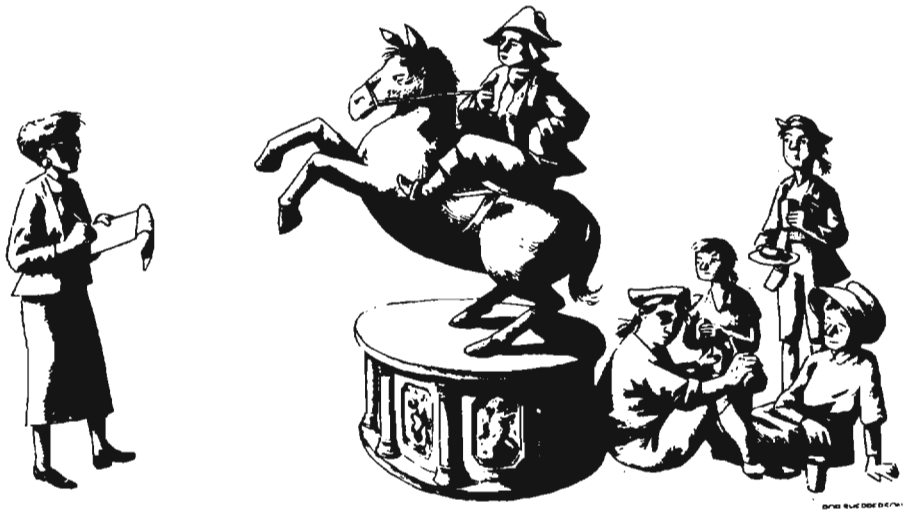
Reader: *Thanks. By the way, someone from another agency is coming in for a briefing on the project. I'm supposed to make the arrangements. Where can I find out what I have to do?*

It would be nice to say, "Look it up in the Yellow Pages," which, of course, is printed on yellow paper -- or better yet, in this day of automation, is kept on line. It could be limited to a few outlets, one terminal per office, something like the personnel files on the M204, for example.

Why not?

~~FOR OFFICIAL USE ONLY~~

CHANGES IN AGENCY REPORTING



P05 P.L. 86-36

~~(C-CCO)~~ In November 1982, NSA, with G Group at the lead, launched a major initiative to move away from the traditional full-text translation format [redacted] to a journalistic format.

~~(C-CCO)~~ The basis for this change was multi-faceted. One was security related. We had lived through instances of seeing verbatim quotes of some of our product in the media, and needless to say, even in an English translation form, a quote in the media of a verbatim translation of target communications makes it much easier for a target counterintelligence effort to track our source and to take countermeasures. While the journalistic format does not provide full-proof protection in the case of leaks or other compromises of our product, it does give at least some additional security.

(U) Another reason for the move to the journalistic style was to provide a product better suited to the reader, especially the executive reader, who has to scan rapidly much incoming material to determine quickly the key elements of the reports. The journalistic format encourages the reporter to summarize briefly the highlights of the report at the beginning of the report. Thus, by reading the title and the introductory summary, the reader quickly learns what the report covers and can decide whether to read the entire report. In contrast, when the information is published as a full-text translation, the reader often has to wade laboriously through long-winded salutations and extraneous material to extract the important parts of the report.

~~(C-CCO)~~ Finally, another reason for the switch to journalistic style was that we have only a limited number of foreign-language translators to cope with an ever increasing volume of intercept. [redacted] Some reporters complained that the switch to the journalistic style detracted from their verbatim translation skills upon which they were tested for certification. Some senior checkers complained that the switch to the journalistic format actually took more time because they could not feel confident of the reports done by the junior linguists unless they first saw a full-

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

text translation upon which the report was based.

(U) But gradually those growing pains have been overcome. Our reporters and checkers have adjusted to the journalistic style and now most feel quite at home with it, preferring it over the old style because it makes them think more about the story they want to convey and how they want to convey it.

EO 1.4.(c)
P.L. 86-36

CUSTOMERS' REACTIONS

~~(C-CCO)~~ As the new Agency initiative began to develop momentum, we got mixed reactions from readers. Some were quite pleased with this new format

As time went on, we encouraged customers to develop a direct relationship with our reporting elements to help answer any questions arising with our product.

COORDINATION WITH SECOND PARTIES

WHERE WE ARE HEADED

~~(C-CCO)~~ Any changes as dramatic as the Agency's move to the journalistic style for our product would be expected to take time as we progress toward our objectives. New reporting policies and procedures have evolved as we made adjustments to come up with a more efficient production process and to provide the best product possible to our customers. Sometimes communication with our readership, with our Second Party agencies, and even within our own ranks has not been as good as it should have been. But with the patience and persistence of top Agency officials, managers at all levels, and reporters at the Agency and in the field, we have made tremendous progress since setting out on this road over five years ago.

~~(FOUO)~~ Our main effort now is to consolidate these changes into a new draft of USSID-300 in a way that will clearly document these and other changes for the workforce. And we have established a DDO Intelligence Staff Product Improvement Working Group to provide a forum for within-DDO communications of the success and problems associated with this initiative and to surface other ideas on ways to publish better product with our limited resources. We encourage the active participation of everyone concerned in these endeavors. □

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

DOCID: 4010015
P.L. 86-36

[redacted]

UPDATE ON PACKET RADIOS

[redacted] *G923*

P.L. 86-36

(U) As a follow-up to my article "Is Packet Radio Alive and Well on HF?" (Cryptolog, 3rd Issue, 1987), here is some recent information:

[redacted]

- (U) The following countries should be added to figure 2, countries whose amateur radio operators are active in amateur packet:

Bahrain	Namibia
Bermuda	Nepal
Bolivia	New Caledonia
Bulgaria	New Guinea
Egypt	Nigeria
French Polynesia	Oman
Gabon	Pakistan
Greece	People's Republic of China
Honduras	Peru
Hong Kong	Poland
Iceland	Qatar
India	Senegal
Ireland	South Korea
Israel	Soviet Union
Kenya	Surinam
Lebanon	Thailand
Lesotho	United Arab Emirates
Malaysia	Western Samoa
Malta	Yugoslavia
Marinique	Zaire
Monaco	

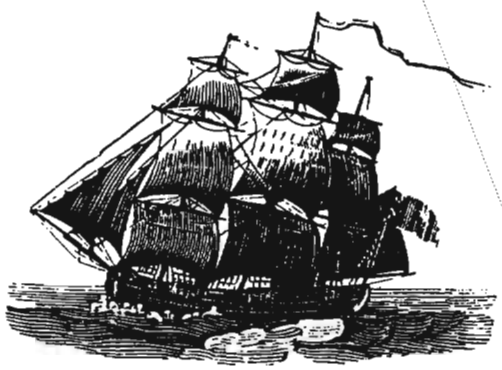
UNCLASSIFIED

EO 1.4.(c)
P.L. 86-36

Release of Embargoed Information

P.L. 86-36

[redacted] *P05*



(U) This is a discussion of pertinent facts and regulations concerning the release of embargoed items to non-NSA contractors. Keep in mind that the distinction between **embargoed** and **unembargoed** information applies only to information released to the non-NSA contractor.

~~(C-CCO)~~ The key to identifying end-product that DIRNSA considers embargoed is that, regardless of its COMINT category, it bears caveats, handling restrictions, or channels markings other than, or in addition to COMINT channels.

(U) DIRNSA's policy is to not release any embargoed material to a non-NSA contractor on a blanket basis. In other words, the sponsor must identify each and every specific document requested, together with supportive justification. A general request such as, "All information pertaining to technical intelligence on the [redacted] system" is unacceptable.

(U) Embargoed information falls into the following categories:

- ~~(C-CCO)~~ End-product, regardless of its COMINT category, bearing any restrictive caveat, such as **NOFORN, ORCON, GAMMA** Controlled Item, **PROPIN, NO CONTRACT**, etc., is considered embargoed information. (These are examples of restrictive handling and distribution exchange designators, and do not purport to represent all possible versions of such restrictions).

- (U) Any end-product protected in a special channel, such as **LOMA**, and/or **TALENT-KEYHOLE**, instead of, or in addition to COMINT channels.

[redacted]

- (U) All technical data is likewise embargoed, regardless of classification and/or channels protection. Technical data includes working aids, technical support letters, reports and manuals; information of SIGINT production processes; raw SIGINT data; tapes of specific signals; and tapes of electromagnetic spectra.

- (U) Foreign encrypted signals are not, repeat not, releasable to non-NSA contractors without the specific approval of the Director or Deputy Director, NSA.

To Request Release of EMBARGOED Information

~~(FOUO)~~ A request for the release of embargoed information to a non-NSA contractor involves the following steps:

~~(FOUO)~~ 1. The sponsoring agency's contract monitor must submit a written request (electrical message/letter/memo) to DIRNSA, ATTN: P05/SAO. Military sponsors should forward their requests to the cognizant intelligence command for review and validation, with an information copy to DIRNSA (P05/SAO). Upon P05/SAO's receipt of the cognizant intelligence command's validation, it will initiate processing action.

P.L. 86-36

DOCID: 4010015

~~(FOUO)~~ 2. The request must contain the following:

(a) The title, contract number and expiration date of the contract.

(b) The contract statement of work or information sufficient for NSA/CSS understanding of the contract's purpose.

(c) Certification of the contractor's need for access to the SIGINT infomation.

(d) Certification of the contractor's clearances.

(e) Security certification of the contractor's storage facility or the facility in which the SIGINT information will be processed.

(f) Name and phone number of the contract monitor.

(U) 3. Upon receipt of the above, PO5/SAO will review the request and determine the appropriate action office (generally dictated by what organization originated the material, and/or the OPI of the subject matter involved). In most cases the OPI (action office) is the final authority regarding the releasability of the material requested, and has the prerogative of mandating specific provisions or precautions to be adhered to in connection with the release. The OPI is also responsible for advising PO5/SAO concerning the decision to release of the requested information.

(U) 4. PO5/SAO will then forward the Agency's decision to the requester in writing, based upon the recommendation of the OPI.

~~(FOUO)~~ NSA-originated SIGINT or SIGINT-related material may not be released to a non-NSA contractor unless the above process is observed and PO5/SAO (DDO's designated Central Point of Contact regarding release of material to contractors) is aware of the request/action.

(U) For clarification as to whether material requested for a non-NSA contractor falls into the embargoed or unembargoed category, please call me on 963-5463s. □

BULLETIN BOARD

WORD PATTERN LISTS

~~(FOUO)~~ A program to generate word pattern lists is available in G244. It produces patterns in the familiar form ABCDAC, *et al.*, when run on an edited plaintext data base. For information call Fred Pollnitz or Bob Silva, 963-5380s.

IBM TO XEROX CONVERSION

(U) There is now a program to strip superfluous function codes (carriage return and line feed) from IBM floppies before conversion to the XEROX STAR format. (Preliminary tests show that it also works for IBM to Macintosh conversion.) This is a quick routine, a matter of seconds, that eliminates the customary time-consuming multi-step "find-and-replace" routines. For a copy of the program and instructions call or write [redacted] P16, HQS, 963-1103. P.L. 86-36

SOFTWARE VERIFICATION

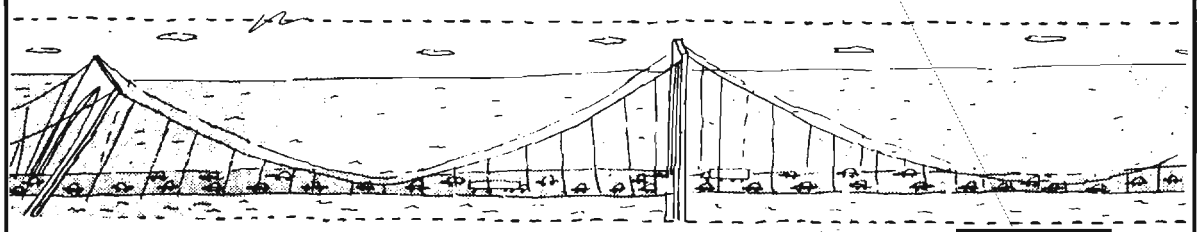
(U) The National Bureau of Stapdards has adopted a new standard for improving the accuracy and quality of software during development and maintenance. Called "Software Verification and Validation Plans" (ANSDI/IEEE 1012-1987) it was developed by IEEE. We expect to see it published as a Federal Information Processing Standard in the near future. For further information call or write [redacted] P13D, FANX-II, 968-8161. P.L. 86-36

WANTED: CONVERSION FROM APOLLO

(U) CRYPTOLOG is seeking to convert files prepared on APOLLO, particularly those done in $Te_{X,}$ to IBM DOS or Macintosh or Xerox STAR. If you know how to do it, please get in touch with the Editor, [redacted] P1, HQS, 963-1103. P.L. 86-36

EO 1.4.(c)
P.L. 86-36
DOCID: 4010015

THE SHORT BUT HAPPY LIFE OF WIDEBAND



P0431

P.L. 86-36

~~(C)~~ There was a time when we had collection resources all around the world. [redacted] The manning in those stations, however, was to become a source of concern for Agency management. Collection activity as it was performed in those bygone days was man-intensive and quite costly.

(U) In the early sixties another problem arose that exacerbated the concerns about station manning. The French, for whatever reasons they had, began a run on the gold reserves of the United States by cashing in dollars. Other nations, not wanting to be left holding the bag when the U.S. ran out of money, followed suit. Several programs were started on a national level to halt the erosion and to bolster our country's reserves, but they are not involved in this story.

(U) NSA, as its contribution, sought means to limit its contribution to the gold flow. One of the most significant factors identified was the pay that our field personnel spent off base. That money went into the foreign economy as dollars that were at that time redeemable in gold.

(U) This was the issue: How do we limit the spending of our personnel on the foreign economy? Cutting their pay, limiting off-duty time or restricting off-base activity were all equally unattractive as solutions. We have never enjoyed an overabundance of the skilled, intelligent personnel required to man a SIGINT field station and any solution that would make the duty less pleasant would make it more difficult to find people to do the job. The only reasonable approach to this problem was to develop some method of limiting the number of people to spend the money.

[redacted]

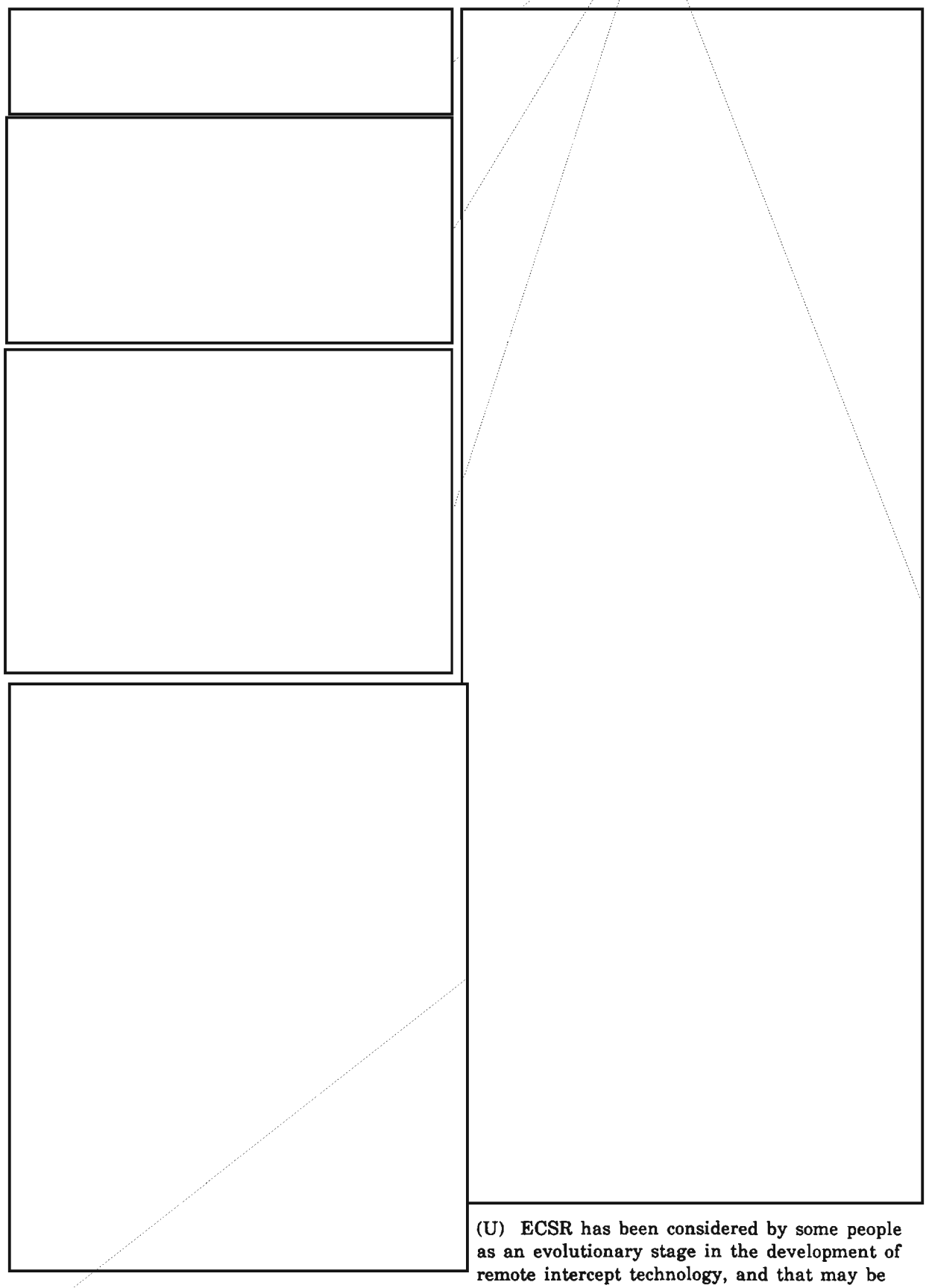
[redacted]

[redacted]

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~SECRET~~



(U) ECSR has been considered by some people as an evolutionary stage in the development of remote intercept technology, and that may be accurate. But just as the tyrannosaur, the

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

diplodocus and the triceratops may be gone, the gekko, the alligator, and the iguana are their descendants and still fill ecological niches. So, too, does the ECSR system of today serve its collection functions.

(U) A new chapter is being written in this story. Just as the technique is more than twenty years old, the equipment now being used is ten to fifteen years old and is beginning to show its age.

(U) There are people in NSA who are beginning to be concerned about the equipment and the methods now in use and who are persuading themselves that new technology should be developed to supplant the banks of recorders that are in use to record a little more than a Mhz apiece. There is discussion of digital recording techniques, techniques using VCR technology, and of techniques that retain the basic technology in use at present, but modified to record at half the speed used now, thus saving - in theory, at least - head wear, tape wear and tape volume. Reduction of the tape volume, in turn, would also reduce tape storage space requirements, shipping costs and the expenses involved in rehabilitating and inspecting the tapes.

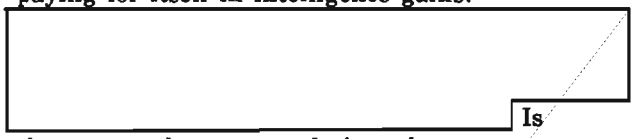
(U) Each of these options has one thing in common with the others: They are all very expensive. The least expensive of the options, the half speed modifications, has been tested and seems to work well, judging by the limited experience we have had with it. The cost for modifying each recorder would be in the neighborhood of $50,000 per unit, and the modification also requires that new high performance tapes be introduced into the system. Tapes now in the inventory will not serve.

(U) It has been postulated, however, that the high performance tapes may be more abrasive than the tapes used at present, which would, of course, increase the wear on the recording and playback heads. Would that offset the savings realized from the slower tape speed and the reduced footage that would be recorded and played? There are no definitive answers to that, yet.

(U) One additional advantage to the half speed modification would be the fact that the new version could probably be phased in more easily than could the introduction of entirely new technology. Thus the cost of the option could be spread across a few years, resulting in smaller impacts on annual budgets and less disruption to ongoing activity. New technology would require a turnkey operation and, while it could be phased in by theater, it would probably have to be done theater-wide in each phase.

(U) There is one other disadvantage to the half speed proposal, however. It involves replacing the heads, capstans and other parts on the recorders already in the inventory. With this, you have new technology on what are still old machines. We would be putting hundred dollar saddles on ten dollar horses. The motors, power supplies, and other parts of the machines will just continue to get older. Worse yet, when the parts that never break start to break, they will be very difficult and expensive to replace—all out of proportion to their original value—if past experience with other kinds of hardware holds true.

~~(C-CCO)~~ There is no good answer to what we should do about our wideband resources. Perhaps, before we consider the answers to those questions, we should examine other questions. For example, is wideband recording paying for itself in intelligence gains?



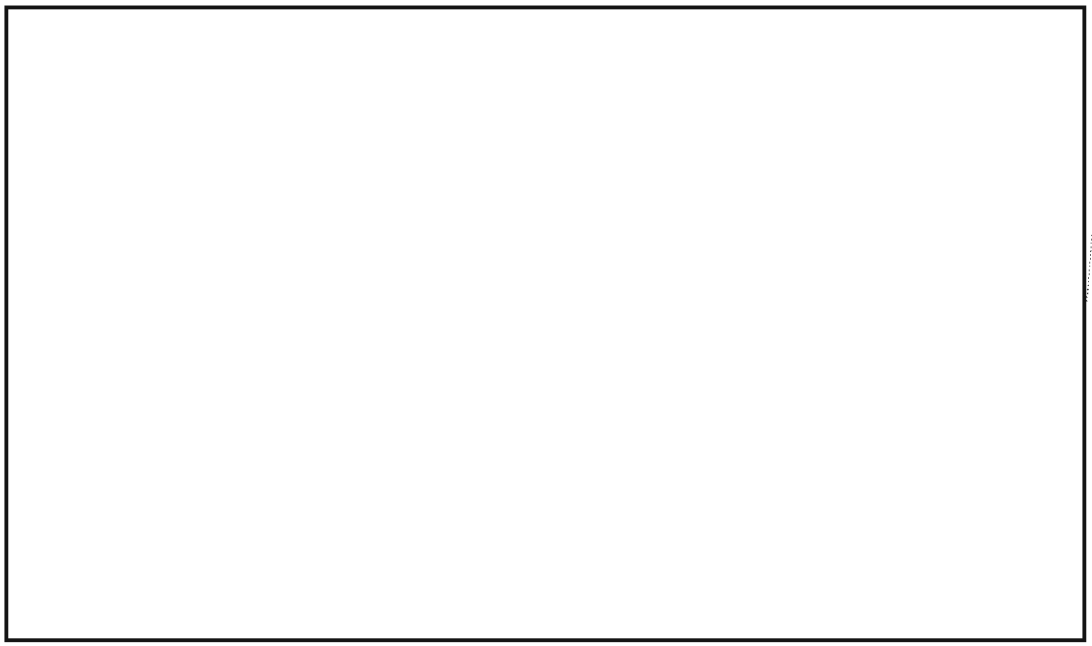
Is there any other way to derive what we now get from wideband recording?

(U) This has not been a research paper; it has been some random ideas that have crossed the writer's mind. The historical chronology may be fuzzy, the costs cited may be inaccurate, but the basic facts are facts and we are coming to a time when a decision should be made.

(U) Any suggestions?

EO 1.4.(c)
P.L. 86-36

DOCID: 4010015



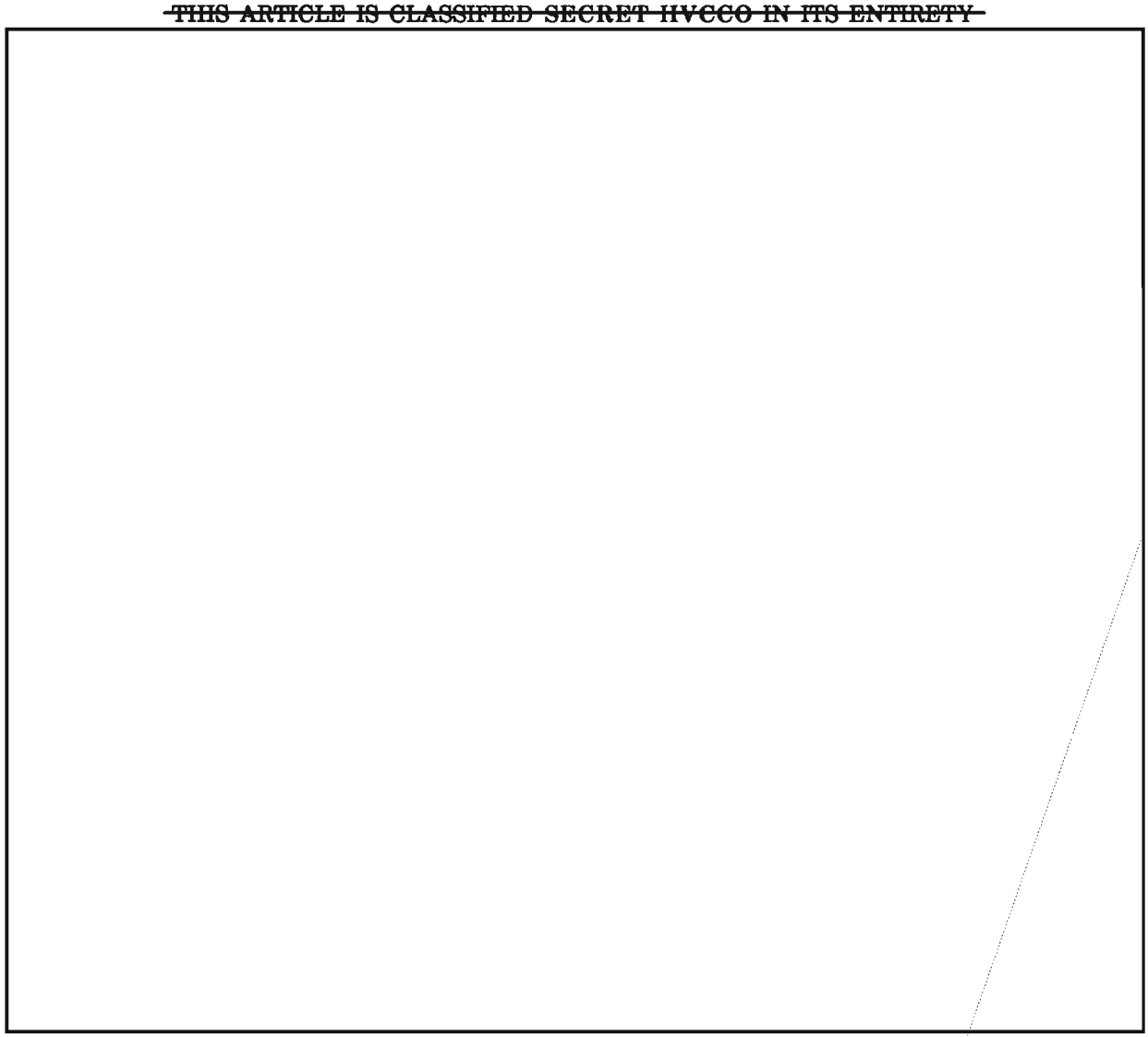
EO 1.4.(c)
P.L. 86-36

N.
C.

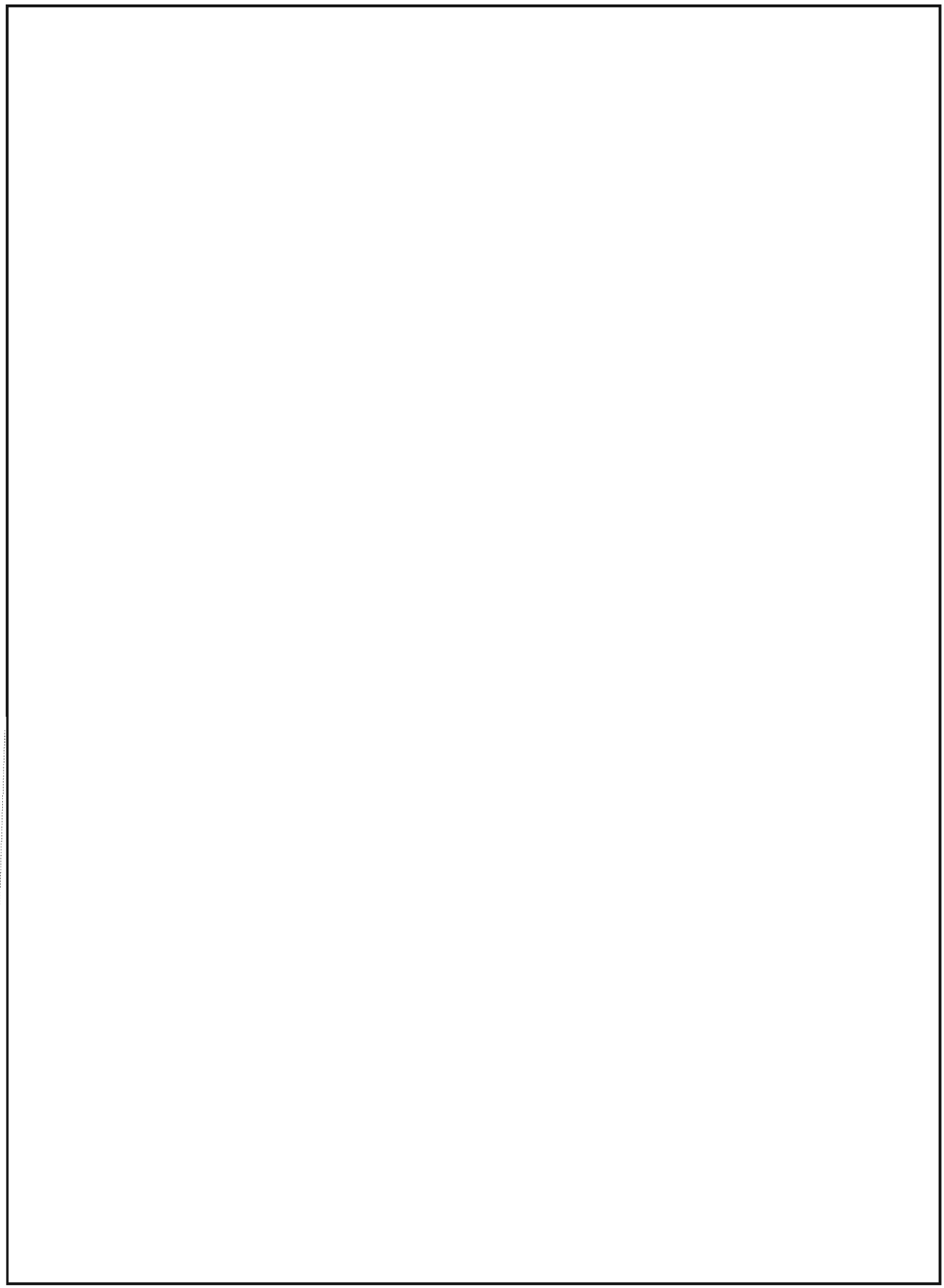
G
E
R
S
O
N,

R
6

~~THIS ARTICLE IS CLASSIFIED SECRET HVCCO IN ITS ENTIRETY~~

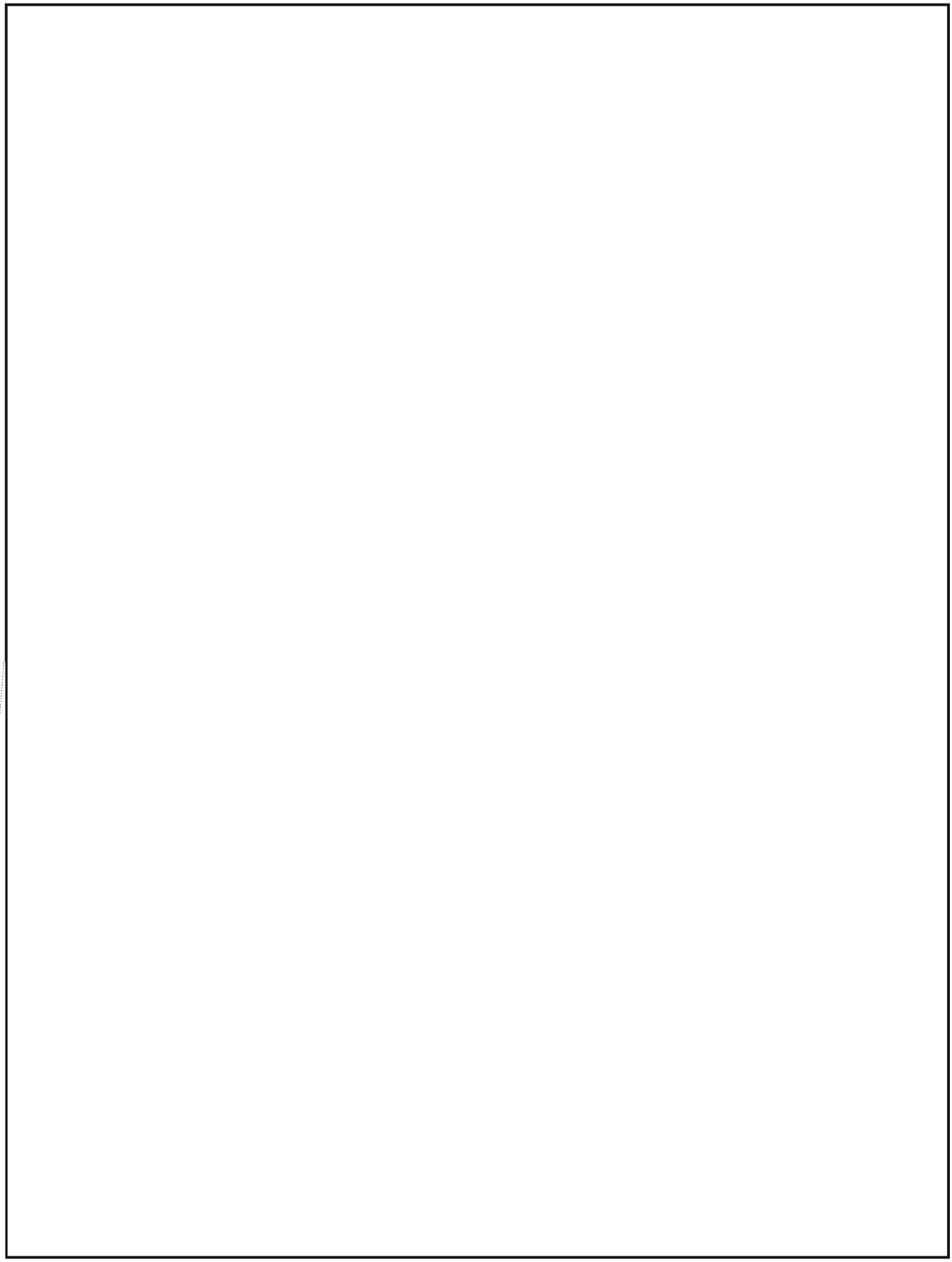


P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)



P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

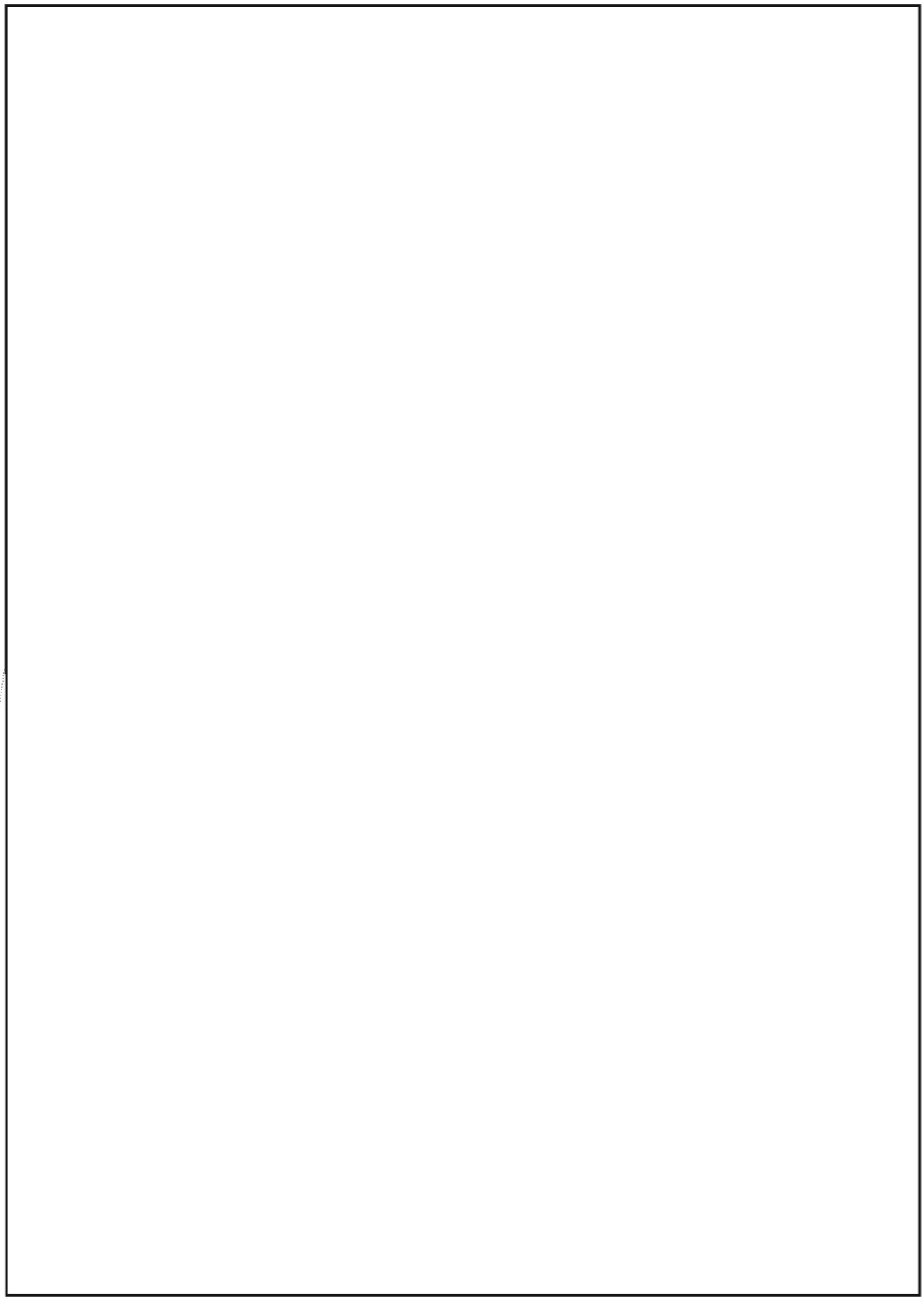
~~SECRET~~



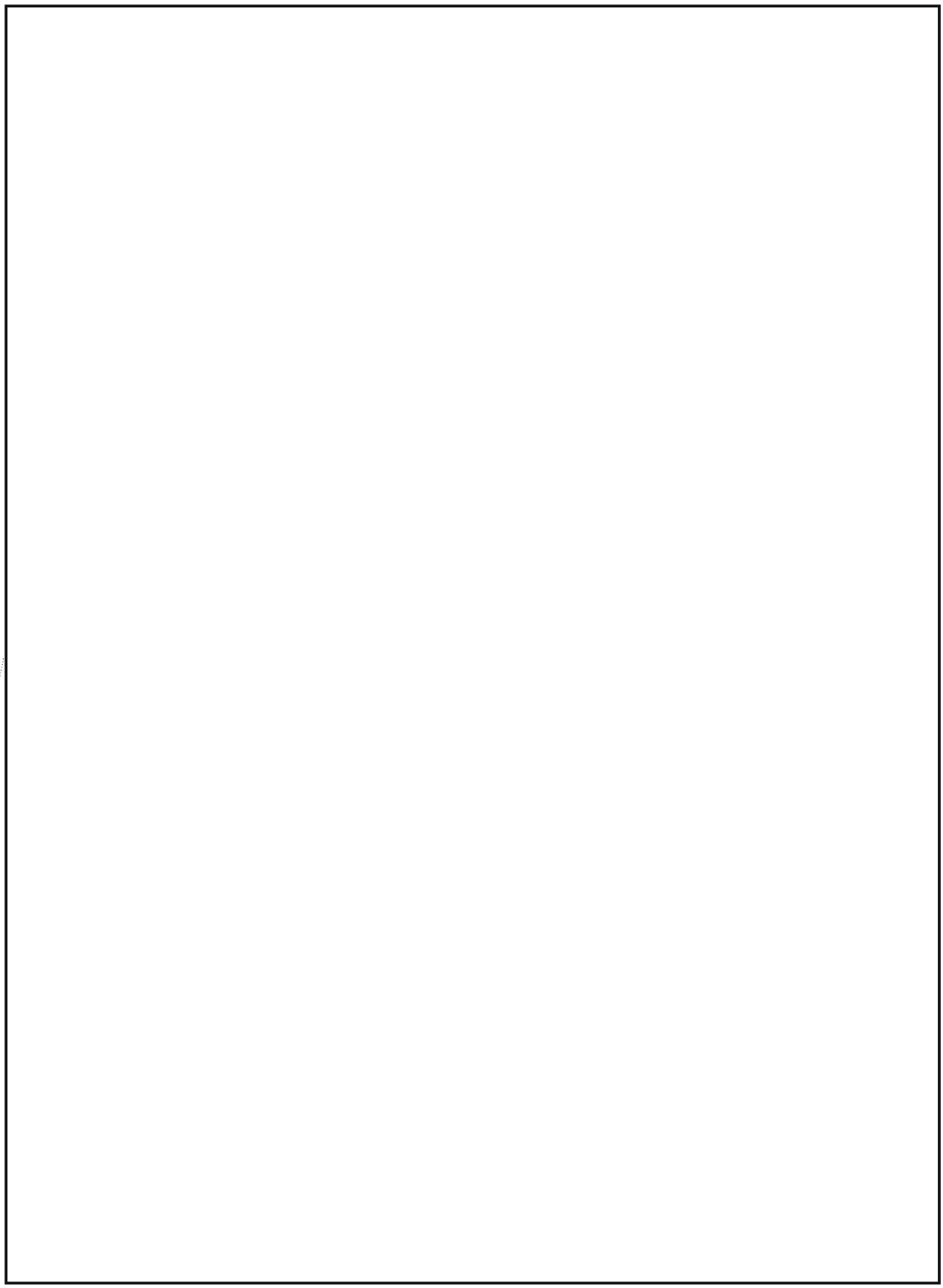
~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

DOCID: 4010015



P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)



P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

LANGUAGE BRIEF: XHOSA

G94

(U) Xhosa is a Bantu language spoken by more than 6 million people in the Transkei and Ciskei "homelands" of South Africa, which border Lesotho and face the Indian Ocean. The Bantu family of languages numbers over 300 and is spoken in an area encompassing most of the southern part of Africa extending south of Cameroon and Kenya. Xhosa was the first South African Bantu language to appear in print, transcribed by missionaries in 1821.

(U) Xhosa is a tonal language, with high, low, and falling tones. Because the Xhosa people interacted with the Hottentots early in their history, their language shares some of the peculiar clicks characteristic of the language spoken by the Hottentots, people of a South African race related to the Bushmen. (Sotho also shares some of these characteristics, although it has only a single click.) The clicks are represented by the letters "X", "Q", and "C" and, in combination with vowels and consonants, form 20 click combinations . Changing one click combination for another can change the entire meaning of a word.

(U) The "X" click, or lateral, sounds like an equestrian urging his horse on; the "Q" click, or palatal, sounds very much like a cork being released from a bottle. The "C" click, or dental, sounds like the nonverbal sound a person makes to express disgust.

(U) Xhosa is based on a system of concords, or prefixes. Depending on which of seventeen classes the noun of the sentence fits into, the prefix of the noun will influence the form of the verbs, adjectives, and other parts of speech which are brought into relationship with the noun. Examples are shown below. Because of these concords Xhosa is extremely alliterative, which makes it fairly easy to recognize in written and spoken form.

(U) In addition, Xhosa is an agglutinative language, as opposed to inflectional, having a predominance of detachable particles which can be added to the word to vary its meaning. It is a language filled with interjections, and has ideophones as well. Ideophones are descriptive and exclamatory utterances designed to complement the thought being expressed and are often imitative of the action described, or of a sound associated with it.

(U) Although Xhosa is one of the principal languages of South Africa, along with Zulu, Tswana and Sotho, it is not considered an official language in that white-ruled country. Only Afrikaans—a bastardized version of 16th century Dutch—and English are officially recognized.

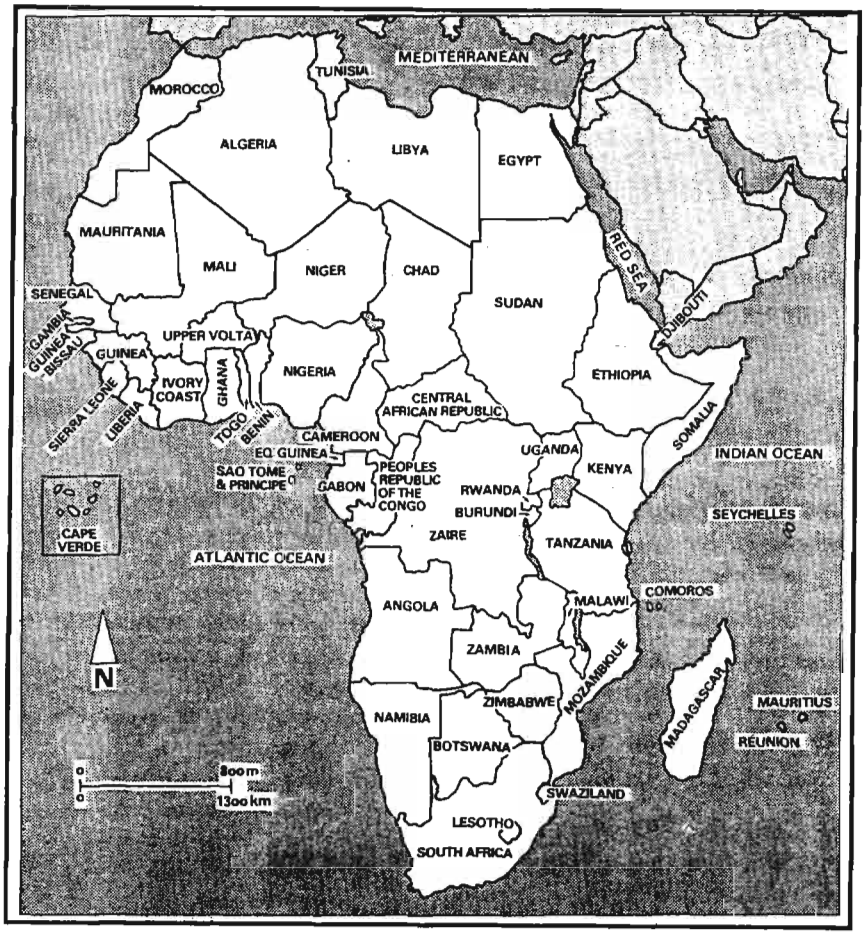
Unclassified

EXAMPLES OF CONCORD

All people want peace	Bonke	abantu	bafuna	uxolo.
The whole country wants peace.	Lonke	ilizwe	lifuna	uxolo.
The whole nation wants peace.	Sonke	isizwe	sifuna	uxolo.
All nations want peace.	Zonke	izizwe	zifuna	uxolo.

EO 1.4.(c)
P.L. 86-36

Unclassified



EO 1.4.(c)
P.L. 86-36

DOCID: 4010015

EXPO 88

★

19 October 1988

Friedman Auditorium

★

See it now!

★

High tech for linguists!

Custom-designed workstations for linguists!

Online dictionaries!

Electronic gazeteers!

High-resolution displays!

Neat inventions!

Useful gadgets!

★

Sponsored by The Office of the Chief Scientist and the Natural Language Working Group, a consortium of linguists, computer scientists and engineers from A, B, G, T, R, and Z.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010015

Nineteenth Southeastern Conference on Combinatorics, Graph Theory, and Computing, 15-19 Feb 1988, Louisiana State University, Baton Rouge.

Reported by: [redacted] *R512*

P.L. 86-36

I attended this conference to present my paper "A New Combination Generation Method, " to keep abreast of developments in a vital area of mathematics, and to support Agency recruitment of professional mathematicians.

[redacted]

There were five invited presentations and about 180 fifteen minute talks in three parallel sessions. As conference proceedings are scheduled to appear in *Congressus Numerantium*, published by Utilitas, and also because no earth-shattering new results were announced, I am limiting myself to comparatively few remarks about the talks themselves.

CONCLUSIONS AND RECOMMENDATIONS

The Southeastern Conference addresses a type of mathematics of very special importance at NSA, namely combinatorics. Hence NSA attendance is indispensable. More than one representative should be sent when possible.

This may be an appropriate place to give a view on the value to NSA of attendance at meetings of the present type. I believe that the dominant factor is the educational and motivational value to the individual attendees. They are exposed to a lot of new information by enthusiastic researchers from the US and the world; they make contacts and are made to feel a part of a larger mathematical community. This will be reflected in better job performance. Attendance at meetings is an appropriate and economical mode of training for those of us who are already steeped in formal degree-oriented schooling. The individual attendees will be better trained, better motivated, and have improved morale. Benefits like this have the biggest potential payoff.

THE TALKS

Each of the five days was highlighted by an invited instructional lecture of one or two hours. All of the invited addresses with the exception of Frankl placed considerable emphasis on whether the problems addressed are NP complete or had efficient algorithms. I interpret this to be an indicator of current fashion.They were:

- "Cycles in Graphs and Directed Graphs" by Carsten Thomassen of the Technical University of Denmark;
- "Fast Algorithms for Convex Polygon Problems" by Maria Klawe of IBM Almaden Research Center;
- "Current Developments in Cryptanalysis" by Ernest Brickell of Bellcore and Sandia Labs;
- "Old and New Problems in Finite Sets" by Peter Frankl of Bell Labs and the University of Paris; and,
- "Recent Developments in Ramsey Theory" by Vojtech Rödl of Bell Labs and Czech Tech.

The last two speakers are mentioned as possible successors to Erdös. (Erdös himself was to have talked, but skipped off to Australia at the last moment, so Frankl spoke instead.) All of these talks were of high quality.

Klawe studied a scheme whereby certain inequalities related to convexity propagate

~~FOR OFFICIAL USE ONLY~~

through a matrix. "Totally monotone" is her term for matrices in which this happens. This structure was exploited to construct certain efficient algorithms. Her scheme appeared similar to one which I had employed in computing what I call "subsequence numbers." I pointed this out to her and gave her a reprint of my paper (*Discrete Mathematics* 16, 1976, 123-140).

Brickell's talk surveyed a lot of open-literature cryptanalysis very fast. I am told the presentation was not much different from previous talks he has given. Nevertheless, since there is probably interest in what he had to say, I have obtained copies of his multitudinous slides which he was kind enough to send me. He kept repeating that much of this material would be included in a paper to appear in the *Proceedings of the IEEE*, written with Odlyzko.

Frankl's talk was fairly short and included problems concerned with the existence and construction of critical (e.g., maximal or minimal) families of subsets of a finite set with various stated requirements on how the subsets in the family had to be related one to another. Sperner's theorem, for example, concerns the case where the requirement is pairwise incomparability. In most of the cases Frankl discussed, however, the requirement concerned "intersecting," or "cross-intersecting" between sets in the family, where to intersect means to overlap. As an illustration, he gave a result which says: if a collection of subsets of an n-element set has the property that any two subsets in the collection intersect, then that collection cannot have more than 2^n subsets in it. (It is easy to verify that the stated bound is attained.)

Harary mentioned **Fan Chung** in his 15-minute talk on sum and difference graphs as having character theoretical techniques for obtaining bounds on the diameters of graphs. Since the latter was in attendance, I sought her out for details. (She is married to Ron Graham of Bell Labs.) It quickly became apparent that her work is pertinent to routing problems in distributed memory/processing arrays, as being considered for HORIZON at SRC.

She sent me quite a collection of preprints, including a crucial lemma by Nicholas M. Katz which appears to be significant in its own right. Katz obtains a bound on certain sums of characters; I have a copy of his preprint.

Chung's principal result translates Katz's lemma into a bound on the diameter of a k-regular graph in terms of the eigenvalues of its adjacency matrix. I have the abstract of her relevant papers. The papers Chung sent me are as follows:

(a) an estimate for Character Sums (by Katz, 5pp, used in (b)

(b) Diameters and Eigenvalues (19 pp)

(c) The Average Distance and Independence Number (12 pp)

(d) A Dynamic Location Problem for Graphs (with Graham & Micheal E. Saks, 36pp)

(e) Diameters of Graphs: Old Problems and New Results (26 pp)

(f) Quasi-random Graphs (with Graham & R. M. Wilson, 35 pp)

These papers are undated. I will try to supply copies to anyone who expresses interest.

Chung's paper (c) verifies a conjecture of GRAFFITTI. GRAFFITTI is a computer program, and the conjecture is that in any connected graph the independence number is at least as large as the average distance between vertices. GRAFFITTI was written by another attendee at the conference Siemion Fajtlowicz, Math Department, University of Houston. GRAFFITTI has apparently enabled Fajtlowicz to look at a large number of graphs and to formulate conjectures on the basis of the results. He has sent me a recent update on his conjectures (this has been going on for several years), which I will supply on request.

Fajtlowicz may be a valuable source for efficient graph algorithms even in cases where no really efficient algorithm is possible, ie in cases where the problem is NP complete. This is because GRAFFITTI has had to contend with such computations, for example in the case of the determination of a largest clique in a given graph. Fajtlowicz told me he would be happy to supply me with this particular algorithm. (I didn't actually ask for it, however.)

My own talk, on Mardi Gras morning, went very well. It was a variant of my talk at last

DOCID: 4010015

P.L. 86-36

year's NSA Mathematical Sciences Meetings, so doesn't need elaboration here. I did meet a fellow interested in this sort of thing who seems to have done new and interesting work in this area. He is Frank Ruskey of the University of Victoria in British Columbia. He supplied me with a number of recent reprints which I am enthusiastic about, but which I haven't yet had a chance to assess in detail.

RECRUITING

In accordance with policy, I identified myself as an NSA employee, although my name tag read Department of Defense. I got permission from the conference organizing committee to leave recruitment material on the table reserved for new publications. I left copies of regular NSA technical recruitment brochure and of Brent Morris's brochure. I also placed a couple copies of the Proceedings of the NSA Mathematical Sciences Meetings. One copy of each I marked to remain on the table throughout the conference. The Proceedings attracted a lot of interest. Most of the time someone had it open and was reading it.

I suggested [redacted] Math Panel Executive, as an NSA contact for math employment inquiries. I stapled one of his business cards inside the table copy of the Tech Brochure and the Meetings Proceedings. I think these measures were both conservative and effective.

AFTER HOURS

Having completed my own presentation on Tuesday morning, I was in an ideal frame of mind for the afternoon and evening trip to New Orleans for the famous Mardi Gras celebration. (That day the conference adjourned at noon.) Having been prepared by warnings about staying out of dark alleys and not keeping a wallet in a back pocket, Bert Hartnell (Saint Mary's University, Halifax) and I spent most of our time going up and down Bourbon Street. Bert and I managed to wend our way intact back to our bus at 11 PM. I was worried that I had led Bert to ruin, but his talk the next morning was great.

I was treated very well by local people. There may actually be something to the notion of "southern hospitality." This does not refer only to people connected with the conference, who sort of had to be polite, but especially to the people in the town of Baton Rouge, in the shops and parks and streets. One towns-family even invited me to ride with them to New Orleans for Mardi Gras, but I decided to go with the conference crowd. I would enjoy going back. □

The Linguistic Society of America, San Francisco. December 27-29 1987

Reported by: [redacted] *P16*

The annual meetings of this society are the principal means of reporting developments in linguistic theory and applications. Keeping abreast of developments is important to NSA because of the increasing application of linguistics to Agency work. I hope that other NSA people with training in linguistics will be able to attend future meetings.

As proceedings are not published, I am summarizing the talks I attended, arranged by topic.

SYNTAX

Ronald Kaplan and Annie Zaenen, Xerox Parc, "Crossing Dependencies in Germanic Languages and Functional Precedence"

This paper gave an LFG account of infinitival and participial constructions in West Germanic languages. The LFG account allowed them to posit that arguments of an infinitival complement follow those of higher verbs without having to introduce them in the same phrase-structure rules.

Nigel Fabb, University of Strathclyde, "Non-Restrictive Relative Clauses and D-Structure Adjunction"

Scope tests show that a nonrestrictive relative clause is not c-commanded by its antecedent while a restrictive relative clause is. However, tests involving binding show that the antecedent does not c-command parts of the non-restrictive clause. Fabb examines two different options for explaining these data.

DISCOURSE

Joan Levinson, City University of New York, "The Linguistic Status of the Orthographic (Text) Sentence"

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

DOCID: 4010015

This paper discussed factors which affect the distribution of marks of sentence punctuation. Levinson first showed that neither the boundaries of sentences nor the sentence internal punctuation is syntactically specifiable and then offered a theory of information grouping to account for punctuation. This theory suggest that punctuation is a guide for how to read a text and may reflect some kind of intonational grouping.

Jack Dubois, UC Santa Barbara, "Discourse Promotion and the Two-Track Hypothesis"

The one track hypothesis claims that anaphora operates on a single track. Thus, one can measure the distance between pronoun and antecedents in terms of the number of clauses. Dubois claimed that there are two tracks or two patterns of anaphora. In pattern 1 (for subjects), subsequent mentions are nonlexical. In pattern 2 (for objects), subsequent mentions remain lexical.

SEMANTICS

Jorge Hankamer, UC Santa Cruz, "Nested Antecedents"

Hankamer cited the following sentence:

> Bob presented his theory about the ECP, which is/*are pretty interesting.

where 'which' can be 'his theory about the ECP' or just 'the ECP' but not the plural entity corresponding to the set of the ECP and Bob's theory. He used this examples and others to show how the discourse model approach must be sensitive to syntactic relations.

Lewis Creary, J. Mark Gawron, John Nerbonne, Hewlett-Packard, "Toward a Theory of Locative Reference"

This paper proposed a treatment of locatives as components of arguments to predicates:

> (WORK agent: Tom location: (ON(Mass-Ave)), ((IN(Boston)))))

Toshiyuki Ogihara, University of Texas at Austin, "A Present Tense Embedded Under a Past Tense"

In the sentence:

> John said that Mary is pregnant.

a present tense in a verb complement clause is embedded under a past tense, thus violating the sequence-of-tense rule and causing the time of the embedded clause to contain both the time of the matrix and the speech time. Ogihara showed the deficiences of a syntactic solution (Enc forthcoming) and offered a semantic solution.

PRAGMATICS

Peter Tiersma, California Supreme Court, "The Language of Perjury"

This paper examined a Supreme Court opinion defining a false statement in the law of perjury: *Bronston vs United States*. Tiersma argued that Grice's maxims operate even in adversarial proceedings and that the court's definition of false statement needs revision.

PHONOLOGY

Natuso Tsujimura, Indiana University, "Japanese Suffixal Accentuation and Lexical Phonology"

The author identified a class of stem-making suffixes in Japanese which form intransitive/transitive pairs. Some of the suffixes show the pattern of recessive suffixes. The latter provide an exception of Halle and Mohanan (1985) and Halle and Vergnaud's (1987) claim that dominant suffixes, which are cyclic, must precede recessive suffixes.

Charles Li, UC Santa Barbara, "Contact Induced Tonogensis"

This paper showed how a Mongolian language (Baonan) acquired tones after close contact with a tonal language. Acoustic analysis of pitch and amplitude of Baonan disyllabic words revealed a system of two tones: high and low. Li hypothesized that the tonogensis was triggered by the infusion of loan words from a tonal language. This infusion caused pitch rather than amplitude to become a dominant distinctive feature.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010015

SECOND LANGUAGE ACQUISITION

Eileen Kingsley and Ann E. Daubney-Davis, USC, "Native Speaker Nonnative Speaker Interactions: Variations in Negative Data"

This paper analyzed six twenty minute interviews of native-nonnative speaker situations in order to identify instances of negative feedback. These instances were classified as clarification, confirmation, reformulation, and distress. The researchers investigated the relationship between progress and frequency of responses to negative data. Results suggest a possible relationship between progress and the amount of negotiated interaction initiated by the learner.

William Rutherford, USC, "The Contribution of Second Language Acquistion to Learnability Theory"

Studies in second language acquistion (SLA) have mainly been studies of developing grammars. In contrast, theories of learnability (or how language can be learned via impoverished data and without negative evidence) have only recently been addressed in the SLA literature. Rutherford suggested two areas of research in learnability theory: the Subset Principle (Berwick 1985) and the the Uniqueness Principle (Pinker 1986). Examination of these two areas can help explain how learning occurs and thus offer refinement of the theory.

Monika Farner, Macalaster, "Tutorial Questions in Caretaker Speech"

This paper examined the language tutoring function of questions of two caretakers (German speaking and English speaking) of a bilingual child. The what-questions of both caretakers were analyzed. Results showed that questions of both caretakers increased in complexity over the period of study.

INVITED LECTURE

Charles Ferguson, Stanford University, "The Future of Applied Linguistics: An Overview"

Ferguson stressed the need for identification of problems in the real world requiring linguistic solution and the identification of resources to solve these problems. He pointed out the emergence of subfields in applied linguistics and how their development meshes with research in other areas. For example, he cited the effect of phonological theory upon the field of speech therapy.

PANEL DISCUSSION

"Writing Effective Reviews, Abstracts, and Referees' Reports"

This was a panel discussion sponsored by the committee on the status of women in linguistics. Panel members discussed how to write a review for a journal article, how to review a grant proposal, and how to write an abstract for the LSA conference.

CENTENNIAL LECTURE

(in honor of the centennial of Bloomfield's birth. Leonard Bloomfield is the father of American linguistics.)

"Bloomfield: The Man and the Man of Science"

R.H. Robins delivered the main lecture on Bloomfield. Following Robin's talk, a sympoosium of invited speakers (Isidore Dyen, Murray Emeneau, Charles Hockett, Henry W. Hoenigswald, Kenneth L. Pike, Frank T. Siebert, William G. Moulton, and Rulon Wells) spoke about Bloomfield's contributions to the field of linguistics.

AAAL SYMPOSIUM

"Canadian Immersion Programs: Recent Research", by Merrill Swan, Christina Bratt Paulston, Lily Wong-Fillmore, Fred Genessee

Swain: Five different studies were conducted: large scale proficiency, transfer study, age study, observation study, experimental study. The following conclusions were reached: a) Communicative competence includes discourse, sociological, and grammatical factors. b) The teacher needs to point out contrasts between languages and needs to link form with function. c) Beginning study at a later age is all right because the child needs a firm foundation in one language. d) Content teaching alone is not effective. There is a need for language instruction tied to content teaching.

Paulston: Paulston made a number of comments based on the results above: a) We

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010015

need to focus upon language teaching not just language learning- Comprehensible input is not enough. b) The results of the study seem to imply that late immersion is as effective as early immersion. One must consider that perhaps early immersion students would have outperformed late ones if they had been taught differently. c) Methods to discriminate different teaching methods did not reveal any distinct differences in learning because teachers are basically eclectic. What is important is the quality of teaching.

Fillmore: Fillmore commented on classroom treatment studies: a) Evidence from the immersion studies showed that after many years of study children did not achieve native-like competence. It is clear that mere exposure is not enough to insure acquisition. Learners need input but they also need to use the language. The teachers can have a strong influence upon the degree of mastery. b) Students got little feedback about how their skills were deficient. They had little regular contact with French speakers outside the classroom.

Genessee: Genessee commented on the effect of variation in learner and environmental characteristics upon language mastery: a) Language achievement is affected by age of arrival and length of residence, but length of residence is a better predictor. b) Earlier study is not necesssarily better. Cognitive maturity and L1 proficiency both affect language achievement.

The International Communications Convention (ICC-88), June 1988, Philadelphia.

Reported by: [redacted] *P13*

Optical fiber communications was a mini-theme of ICC-88. About one quarter of the three-volume proceedings contained information about optical fiber and related telecommunications technology, and half of this was from foreign authors. Seven complete sessions were committed to the topic of fiber communications. This illustrates how important optical fiber is to the future world's communications. Within ten years more than 80 percent of the important point-to-point communications will pass over optical fiber links.

PART I: THE CONFERENCE

Leading Third World countries, viz: Brazil and China, are actively developing domestic fiber optic production capabilities, and intend to catch up with the fiber optic networks and ISDN digitization of the industrial nations by 2000. European and Japanese laboratories and manufacturers and PTT's are getting ahead of the US in the technology and use of fiber optics.

The technical development of fiber optic communications is still device-limited. The network designers cannot exploit the bandwidth of the fibers because the devices are too expensive, too inflexible and too noisy. Most of the problems of terrestrial trunk communications have been temporarily solved, and the US has installed over a million kilometers of fiber in a competitive scramble for long distance business, but the physical fiber is probably unsuitable for future needs. The potential demand for "fiber to the subscriber" is a much larger market, perhaps a hundred times larger than the trunk networks, but the electronics are expensive, and the designers have not pinned down a service they can offer at 150 Mbps or higher, which the non-business subscribers will pay for. They hope that HDTV will create a demand for the "last mile" of a total fiber network.

There has been a lot of activity in the U.S. laying trunk networks of fiber, as more than a dozen competitors sought part of the long distance market after divestiture. This has produced overcapacity, and mergers and bankruptcies are expected. In addition, there are severe regulatory and political barriers to development of an "all fiber" network in the U.S., as more lawyers have come into the telecommunications field. The Asians and Europeans have proceeded more slowly, installing much more local fiber than the U.S. and prolonging the experimental and trial stages while the technology changes. This difference was manifested in the sessions, where U.S. authors dominated the fiber trunk sessions, while foreign authors had more to say about processing, switching and local loops. The French have already installed fiber to millions of homes, compared to a few hundred residential fiber loops in the U.S. The foreign

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

DOCID: 4010015

Current Mediterranean Submarine Cables

Most of the submarine cables in the Mediterranean are analog systems, but some fiber cables have been installed. The 1984 NTIA report on submarine cables by Schenck gives maps of the analog cables of that era, and also gives technical details. There are about 50 analog links, which are numbered on the Schenck maps. The slide shown by Marone during the oral presentation of paper 2.7 indicated existing and future optical fiber links on many of the same routes as the Schenck maps. The analog cables circa 1984 are listed below. Presumably many of them will be replaced by fiber, or by repeaterless flouride fiber cables within the next ten years.

Number	Name	Capacity	Date	Constr. contract
21	Sicily-Malta	36 ch.	1955	sub cables
23	Kelibia-Bou Ficha/Tunis	120	1956	cit
26	Italy-Tunisia	60	1956	bpo
34	Marseille-Bord el Kiffan	60	1957	cit
36	Italy-Sardinia I	60	1957	stc
52	Trapani-Cagliari	120	1962	stc
53	Sicily-Crete	60	1962	scl
56	Canet Plage-Mers el Kebir	60	1962	cit
81	Cannes-Ile Rousse	96	1966	cit
90	Canet plage-Tetouan	96	1967	cit
96	Marseille-Tel Aviv (MARTEL)	96>128	1968	excofina
99	Cantanzaro-Lekhaina	480	1969	scl
100	Italy-Sardinia 2	480	1969	stc
101	Agrigento-Tripoli	120	1969	stc
104	Barcelona-Pisa	480	1969	stc
107	Marseille-Bizerte	96	1969	cit
109	St. Raphael-St. Tropez	480	1970	submarcom
110	Marseille-Beirut	160	1970	cit
113	Mediterranean-Atlantic (MAT 1) Estepona-Palo	I480>640	1970	stc
122	Peninsula-Balearic Is. (PENBAL 1)	900>1380	1971	c&w
125	Pisa-Algiers	480	1972	stc
129	Marseilles-Bord el Kiffan	480	1972	cit
134	Cantanzaro-Alexandria	480	1972	stc
137	Alexandria-Beirut	120	1972	cit
146	Barcelona-rome	1380	1974	stc
147	Civitavecchia-Cagliari	1380	1974	stc
151	France-Greece-Lebanon-Cyprus	480	1974	submarcom
152	St. Raphael-La Foux	2340	1975	submarcom
154	Heraklion-Lagonissi	1380	1975	stc
156	TELPAL (Tel Aviv-Palo)	1380	1975	stc
157	ANNIBAL (Perpig.-Bizerte)	640	1975	submarcom
160	Algeria-Spain	480	1975	submarcom
162	MARPAL (Marseilles-Plao)	2580	1976	submarcom
174	Italy-Turkey	480	1976	stc
177	Rome-Palermo	1800+2tv	1977	stc
180	Marseille-Bastia	2340	1977	submarcom
184	PENBAL 2	3900	1977	stc
195	AMITIE'(France-Morroco)	2340	1978	submarcom
205	Tripoli-Benghazi	900+2tv	1979	NEC
206	Genoa-Sassari	3600	1979	stc
207	La Seyne-Tripoli	640	1979	submarcom
210	BARGEN (Barcelona-Genoa)	4140	1979	stc
215	France-Algeria 4	2580	1980	submarcom
234	Greece-Syria PALMYRA	480	1981	submarcom
236	Greece-Cyprus 2 APOLLO	1380	1981	stc
237	France-Greece 2 ARTEMIS	2580	1981	submarcom
241	Sardinia-Sicily 2	3900	1982	stc
247	Juan le Pins-Cagnes sur Mer (France-France) (fiber optic)	340 mbps	1982	submarcom
249	France-Tunisia 3	2580	1983	submarcom
254	Greece-Egypt ALEXANDROS	624	1983	att

~~FOR OFFICIAL USE ONLY~~

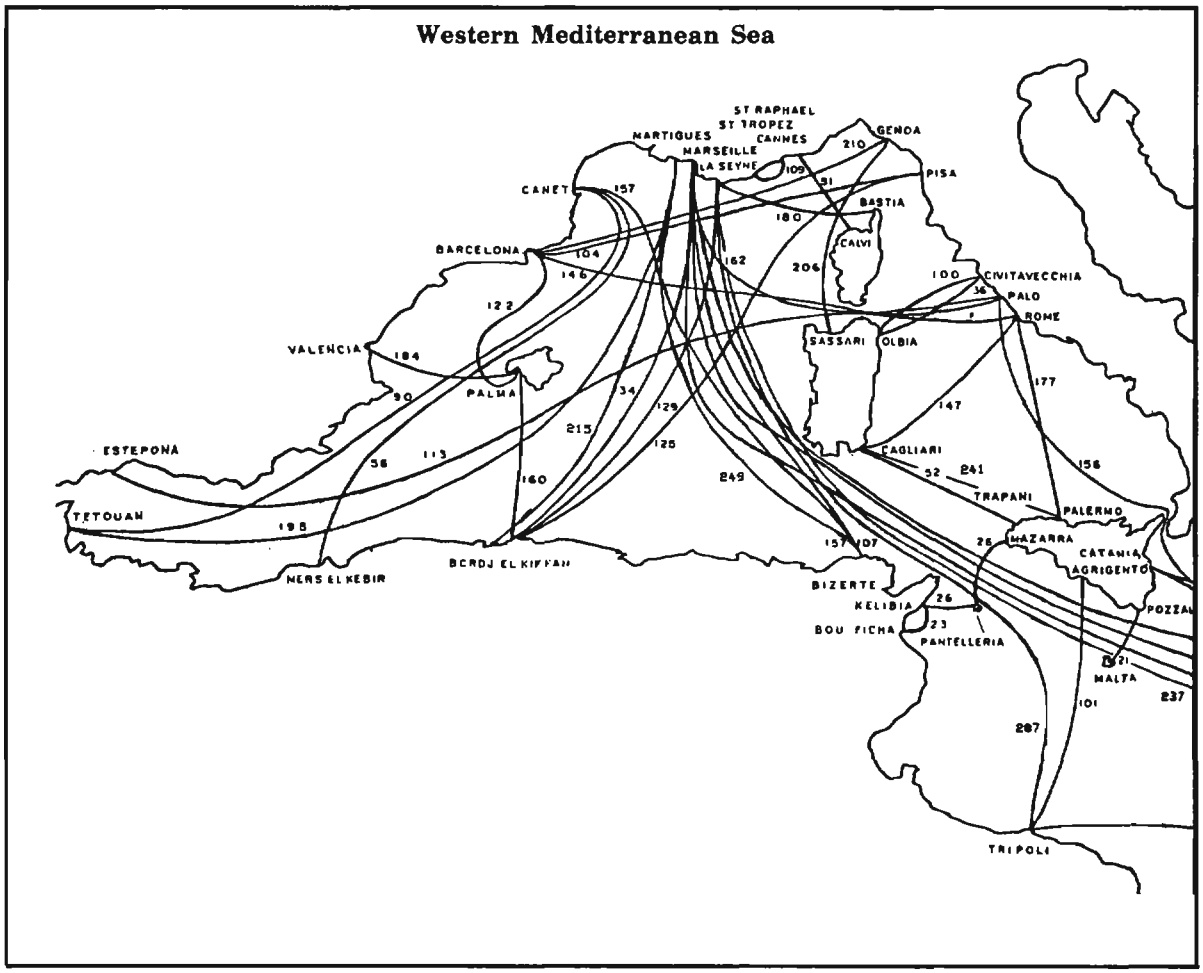
PTT's can develop fiber nets as part of an integrated telecommunications plan. This takes longer, but costs less, and probably avoids the rapid obsolescence and waste of the American efforts.

One point of interest was the development of flouride based fiber for repeaterless submarine cable links in the Mediterranean by the Italian CSELT. They expect that transmission at long wavelength will allow 300 Km repeaterless links at 2.4 Gbps by 1992, and even longer spans by 2000. Another point was the prevalence of damage to the fiber trunks from backhoes and other effects, which is spurring the design of "survivable" networks. There is a plan for a global synchronous optical network (SONET) which will use TDM multiplexing to carry 150 Mbps services at line rates of 2.4 Gbps. (16 x 150 = 2400). However, there are critical timing problems in a synchronous net which are exacerbated by the US divestiture that has different interconnecting networks driven by uncoordinated clocks.

Although there is intensive research and progress, the manufacturing of certain types of fiber and components is still difficult, and the development and operation of optical fiber networks is still a "jungle" of problems. Costs, applications, markets, and integrating the wideband capacity of the fibers into the existing narrowband copper and radio nets are creating uncertainties and delays in the actual deployments of fiber and the development of machines to interface fiber with non-fiber nets. In the meantime, the technology is spreading all over the world.

AN OVERVIEW OF THE SESSIONS

Fourteen of the 54 sessions dealt entirely or partly with optical fiber.



~~FOR OFFICIAL USE ONLY~~

DOCID: 4010015

Session 1. on optical switching presented different schemes for switching of trunks, MANs, LANs and subscriber loops. The designers are trying to develop an all-optical net. All of the papers were foreign.

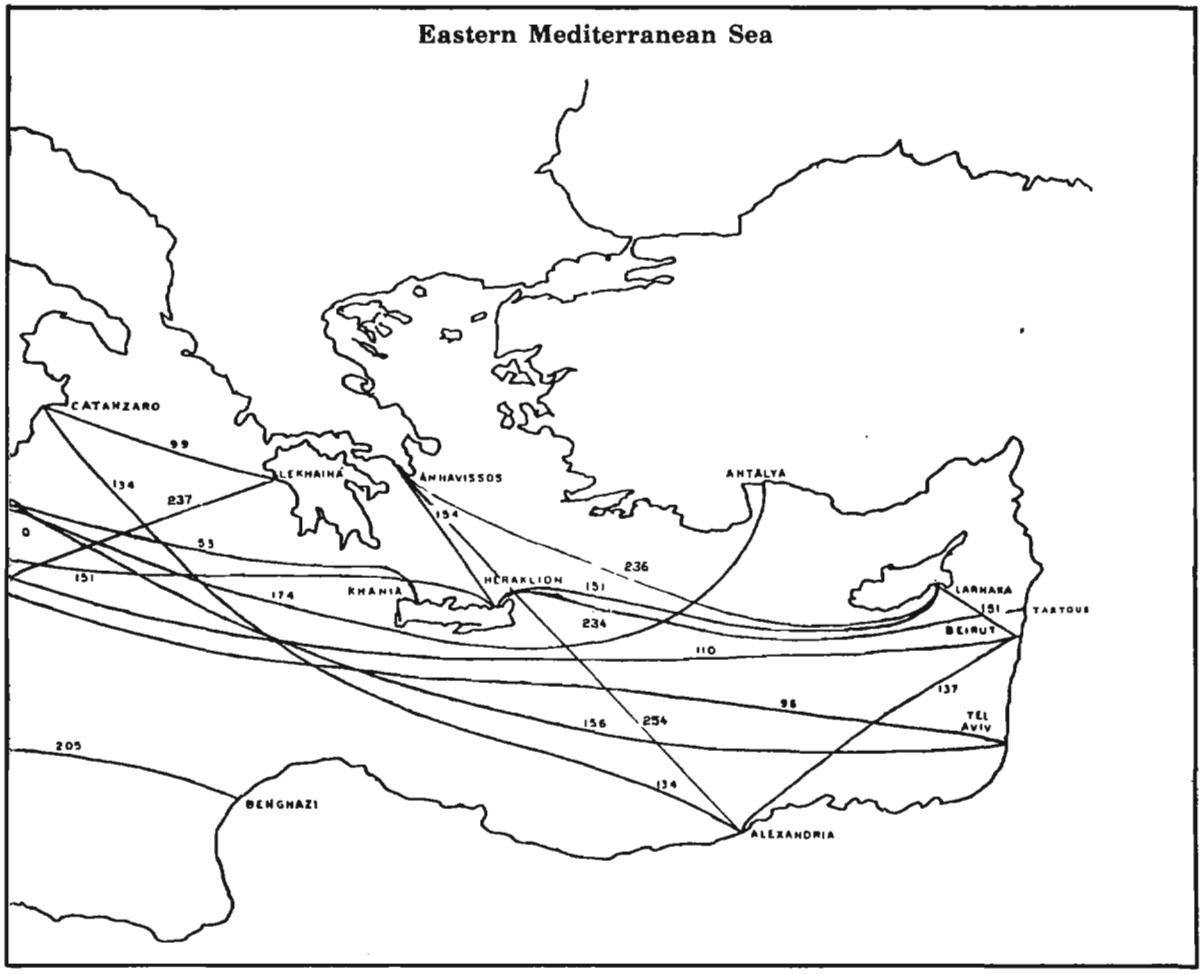
Session 2. on long-haul fiber systems was dominated by Americans. The competitive race to build long distance fiber trunks by SPRINT, WILTEL and others has required elaborate testing and installation procedures because the new carriers did not have organic resources to do the installation and splicing. Undersea fiber cables will have "wetmux" switching, and repeaterless flouride glass links.

Session 10 on high speed transmission was mostly foreign papers. Foreign laboratories have demonstrated 10 Ghz linear amplifiers and receivers, and 700 Km repeaterless spans. Fast transmission is device-bound, and although more than a million kilometers of fiber have been installed, it is probably the wrong kind because it will not prevent polarization shifts that degrade coherent transmission.

Session 11 on digital cross-connects systems described the machines for interfacing between fiber trunks and local networks, particularly fiber hubbing nets. The existing asynchronous digital networks using radio and cable at electronic speeds must connect into high speed synchronous optical nets (SONET).

Session 19 on simulation of lightwave systems covered mathematical models of fiber, lasers, waveforms and subnetworks.

Session 28 on fiber access to the home described current work in the critical "last mile" of fiber installation. Costs are a major factor. The Japanese and French are trying to get an economical transition from current services to future wideband services. They have fewer regulatory barriers to the PTT's delivering CATV, but still have to deal with



~~FOR OFFICIAL USE ONLY~~

established interests. Some of the architectures create an "ether" in which all the traffic reaches all the subscribers, while other designs select traffic flow at central switches. Combinations of fiber and coaxial cable are use to reduce the number of fiber splices and taps. Analog transmission of TV is much cheaper than digital coding and decoding, taps and bridges. Synchronization of many independent local and long distance digital fiber nets will be very tricky.

Session 29 on broadband systems showed GTE's preference for circuit over packet switching. Siemens considers 150-600 Mbps services to subscribers over fiber loops. Fujitsu prefers Asynchronous Transfer Machines (ATM) for interface between narrowband ISDN at 64 Kbps and broadband ISDN at 150 Mbps. Memory matrix TDM switches allow 8 streams of 150 Mbps to be combined into a 1.2 Gbps signal, in a switch with a throughput of 8 x 1.2 = 9.6 Gbps, currently demonstrated. The Japanese like Transport Processors (TP) for the expected bursty nature of multi-gigabit broadband services.

Session 37 on coherent lightwave transmission was dominated by U.S. papers. The Japanese noted problems in manufacture of polarization-maintaining fiber, which they think necessary for coherent systems. Coherent lightwave communications (CLC) can be used to carry microwave compatible transmissions, based on existing microwave systems. Optical amplifiers will give 20-30 dB gains. AT&T thinks a 4.5 terabit/sec star net can be built with currently available components. The decisions to install monomode fiber that does not preserve polarization and adopt TDM multiplexing will dominate switching and CLC.

Session 46 on lightwave local networks showed a number of schemes to operate nets at terabit rates. One academicians's scheme used pulse position addressing combined with spread spectrum transmission over fiber. Multi-fiber rings allowed many different architectures to be expressed over the same robust physical net. The Japanese proposed fiber LAN based on combining FDDI access with CSMA/CD transmission.

Session 47 on broadband ISDN and packet switching was concerned in part with how to extend broadband ISDN services to residential customers. TV and HDTV are seen as the main traffic to non-business BISDN customers. Broadband ISDN will require a global SONET synchronous optical net and ATM (asynchronous transfer machines) for interface to the existing asynchronous digital networks.

∞ ∞ ∞

In general the cost of the electronics is too high for subscriber optical loops. Europeans and Asians are able to pursue systematic development of integrated optical networks without the regulatory problems and fragmentation that affects the U.S. telecom environment. The U.S. has deployed a lot of yesterday's technology for todays short-term market share, while the foreigners are proceeding more slowly but on a broader front to get the markets, the costs, the technology and the customer demands coordinated in a profitable way. In some areas, e.g.. subscriber services, they are well ahead of the U.S. This may give them a long-term advantage, even inside the U.S. market.

Answers to

CRYPTO-"LOG" PUZZLE
2nd Issue 1988

1. Easy as falling off a log
2. Psychological
3. Logjam
4. Lincoln logs
5. Loge
6. Logrolling
7. Logy
8. Ship's log or logbook
9. Catalog
10. Sawing logs
11. Slept like a log
12. Tagalog
13. At logger-heads
14. Backlog
15. Sat like a bump on a log
16. Yule log
17. Analog computer
18. Log cabin

~~FOR OFFICIAL USE ONLY~~

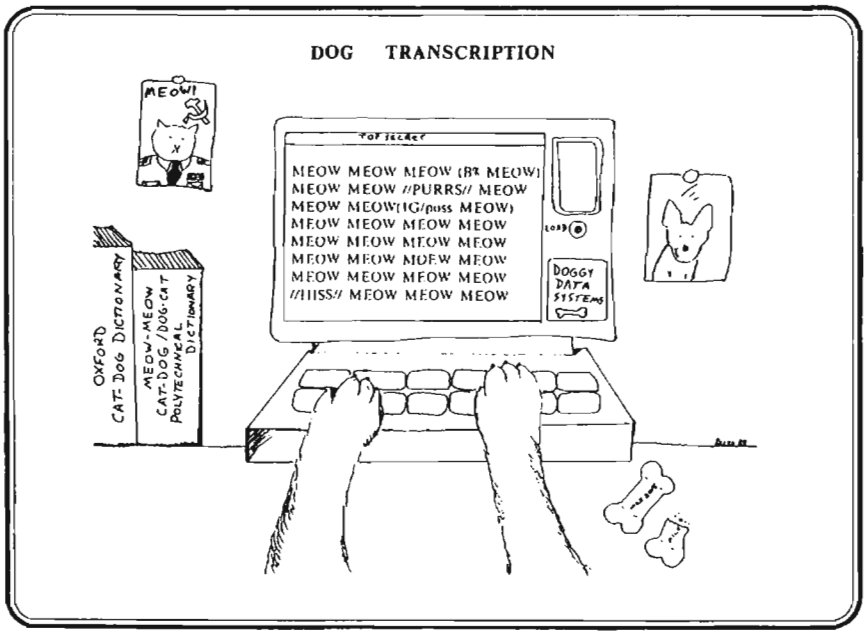
DOCID: 4010015

PART II: SIGINT IMPLICATIONS OF TRENDS IN FIBER OPTICS COMMUNICATIONS

(U) Most of the world's long distance point-to-point communications will pass over optical fiber trunks within fifteen years. The capacity of the fiber trunks, and the low cost of transmission, tends to concentrate enormous amounts of traffic from thousands of low speed tributary systems onto a single fiber.

(U) The impact of fiber is so significant that even COMSAT is installing fiber. Fiber is already displacing traffic from satellite and microwave links. For broadband digital services, it has no equal. Bit rates above 3 Gbps are already in service, and rates above 50 Gbps will soon be in use on single fibers. At the same time, local nets will be carrying terabits of traffic, and on many local nets all the bits will be available to all the subscribers. Analog transmission of microwave signals will also occur on fiber, probably as part of an analog-digital format. Improvements in glasses and optical components will allow both high bit rates and long repeaterless spans. Infrared wavelengths at 3.4 microns will be used to take advantage of low attenuation in new glasses.

On The Lighter Side



by Charles Ralya *courtesy of:* Vox Topics

EO 1.4.(c)
P.L. 86-36

DOCID: 4010015

Call for Speakers

WHEN YOU WERE IN SCHOOL, DID YOU EVER WONDER:

WHY DO WE HAVE TO SOLVE THESE DARN LOGARITHMS?

WHY DO WE HAVE TO KEEP PROVING THAT TRIANGLES ARE CONGRUENT?

WHY DO WE HAVE TO LEARN MATH? I'M NEVER GOING TO USE IT!

STUDENTS ARE STILL ASKING THESE QUESTIONS.

THE LOSS OF STUDENT INTEREST IN MATH IN PAST YEARS IS THREATENING THE FUTURE OF U.S. MATH AND TECHNOLOGY.

THE **NSA MATH SPEAKERS BUREAU**

HAS BEEN ESTABLISHED BY THE MATH PANEL WITH THE GOAL OF
INCREASING YOUNG STUDENTS' INTEREST IN MATHEMATICS.

You can help answer the WHY questions by visiting Elementary, Junior High or High School math classes in the State of Maryland as a Guest Speaker. Stimulate students' minds with discussions of:

- the beauty of mathematics in nature
- elementary cryptology
- how to solve logic puzzles
- careers in math / math in careers
- any topic that you would like to present — we have a library of topics to give you ideas!

YOU DON'T HAVE TO BE A MATHEMATICIAN TO BE A MATH SPEAKER!

For more information, contact [redacted] Coordinator, NSA Math Speakers Bureau, G423, 963-6423s, 688-5361b.

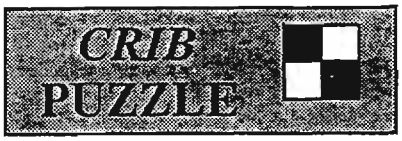
"If the math community suffers, the National Security Agency suffers."
— [redacted] Chairman, NSA Math Panel

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010015

P.L. 86-36



"LEFTOVERS" by [redacted]

This puzzle is *UNCLASSIFIED*

Each of the clues below contains definitions for four 4-letter words. Removing one letter from each of the first three 4-letter words and combining the resulting 3-letter pieces, in the order given, will form a new 9-letter word. The letters you removed, also taken in order, will spell a 3-letter word. You can now add a letter to some position of this 3-letter word to form the answer to the fourth definition. The letter you added is the leftover. The seven leftovers, in order, spell the solution word. Call me with the correct solution at 1351(s) and I'll print your name in the next issue.

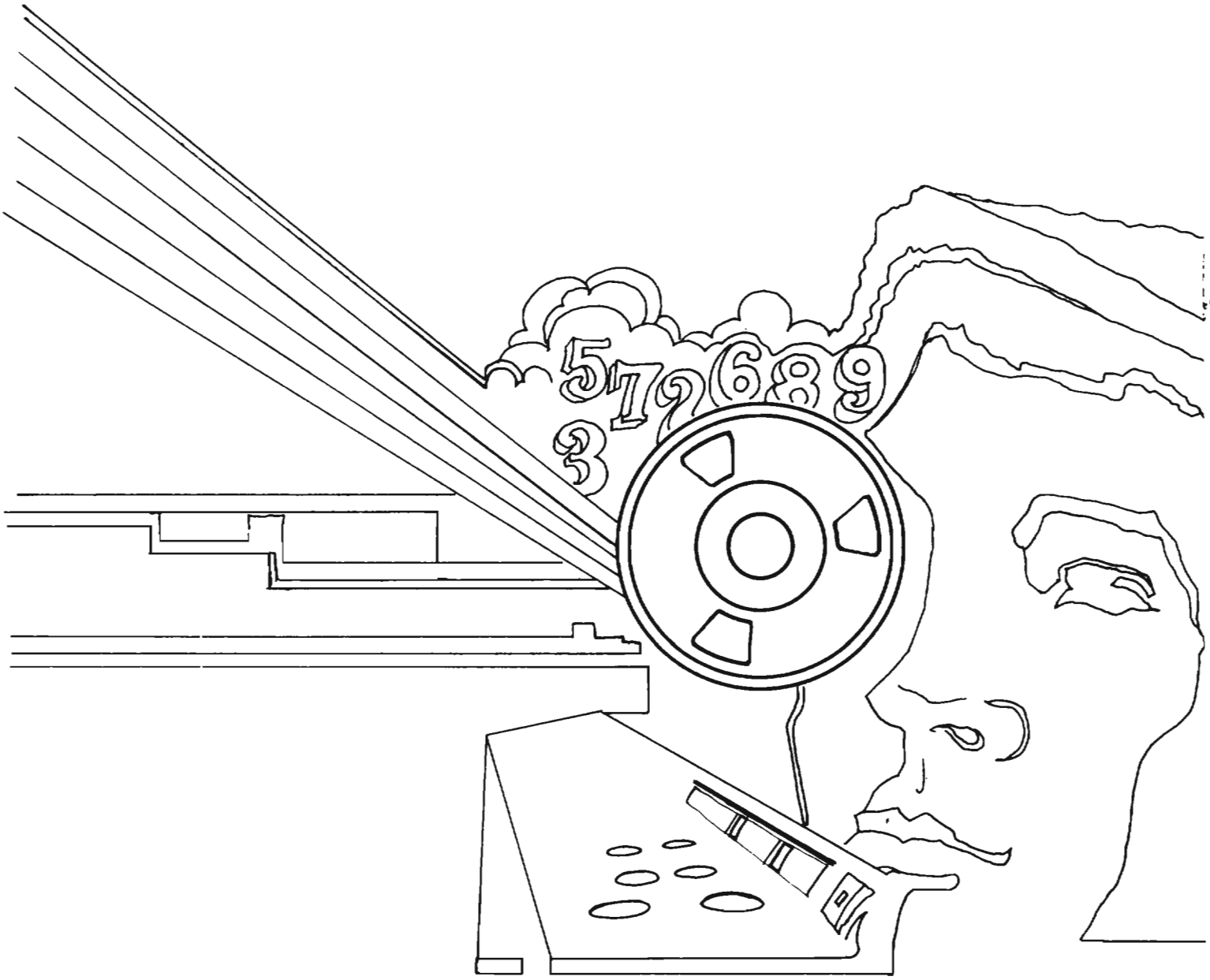
Ex.	Bony growth	Ice arena	Give temporarily	Singe	
	SPUR	RINK	LEND	BURN	B

Remove the "U" from "SPUR," the "R" from "RINK" and the "N" from "LEND." Combine the 3-letter pieces to form the word "SPR INK LED." The removed letters spell the word "URN," and adding the letter "B" forms the word "BURN," the answer to the fourth definition. The leftover is the "B."

1.	Something on a foot or an ear	College figure	Dispatch	Pour	
2.	Beta Orionis, e.g.	Bucket handle	Sympathy	Incline	
3.	Enos' grandfather	Egyptian goddess	Wood's partner	Join	
4.	Way out	Contact	On stage	Streamlet	
5.	Imitator	Crossing	Small lake	Assistant	
6.	Concrete	Smoker	Feathers' prerequisites?	Fuzz	
7.	Road hazards	Average	Recounting	A fuel	

Courtesy of CRIB

~~FOR OFFICIAL USE ONLY~~


5 7 2 6 8 9
3

DOCID: 4019715

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

2nd Issue, 1988

P.L. 86-36

THREE PROGRAMS IN SUPPORT OF LANGUAGE	[redacted]	1
NOT CRASHING THE SYSTEM	[redacted]	5
THE CLAN ON THE FAR SIDE OF THE PARKING LOT	[redacted]	6
THE FALSE FRIEND: A TRUE STORY.	[redacted]	9
BULLETIN BOARD.		12
SOFTWARE ACQUISITION: A REFORM IN NEED OF REFORM.	[redacted]	13
IN RE LACONIC	[redacted]	16
A LESSON IN COMPUTER SECURITY	[redacted]	17
DATA FOR THE LANGUAGE AND LINGUISTICS SECTION	P H. Currier	18
A PARTHIAN SHOT	Peter Jenks	19
HARDWARE REVIEW: PROJECTORS OF SCREEN IMAGES.	[redacted]	26
TECHNICAL LITERATURE REPORT	David Harris.	27
ON THE LIGHTER SIDE		28
CRYPTO-"LOG" PUZZLE	[redacted]	29

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~NOT Rreleasable TO CONTRACTORS~~

Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019715

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XV, No. 2 ..... 2nd Issue 1988

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Collection ..... (963-5877)
Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Cryptolinguistics ..... (963-4740)
Index ..... (859-4351b)
Information Science ..... (963-3456)
Information Security ..... George F. Jelen (972-2122)
Intelligence Research ..... (963-3845)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (963-4958)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-4351)

Illustrators ..... (963-3057)
..... (963-4989)
..... (963-3738)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five)
(note: no 'o')

Always include your full name, organization, and secure phone; also building and room numbers.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, HQS 8A187
Please do not phone.

Contents of CRYPTOLOG should not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

P.L. 86-36

THE GENTRIFICATION OF NSA

NSA is growing in leaps and bounds, as you can see from the many trailers to house operational elements that have been springing up like toadstools after a rain. Only temporary quarters, they assure us. But history tells us otherwise. The WW I temporary structure on the Mall known as the Munitions Building housed our predecessor in the early days of WW II and survived for half a century. At Arlington Hall, the temporary buildings of WW II that were NSA's first home will soon have their golden anniversary.

So we may as well recognize that "temporary" buildings associated with us are only relatively so—compared to the pyramids, that is--and incorporate them into the grand design.

The makings of a charming Olde Worlde enclave, a walled city, are already in place. There are rudimentary Grand Plazas at the entrances of Ops 2b and the HQS buildings. There's an attractive (well, mostly so) courtyard between the two new buildings and Ops 1. All that's needed is gentrifying the trailers: a few petunias here, the odd geraniums there, and imaginative paving joining the trailers to the main buildings. Hardest of all is deciding whether the paving should be patterned brick, a design in terrazzo, or even, log slices set in gravel, Japanese style.

~~FOR OFFICIAL USE ONLY~~

[redacted]G7

Three Programs in Support of

LANGUAGE

CLRP FLIP FLTP

THIS ARTICLE IS CLASSIFIED ~~CONFIDENTIAL CCO~~ IN ITS ENTIRETY

An ongoing problem at NSA has been staffing language positions and encouraging linguists to remain in the language field once they fill these positions. The Agency has looked at this problem through several studies and has implemented a number of programs in an effort to alleviate the problem.

Historically, at NSA there has been a great imbalance between the workload and the workforce in language. [redacted]

Despite the expanded needs in language, however, the language workforce has tended to remain relatively static. Until recently, linguists at the grade 12 level were changing to other career fields or going into management positions in order to progress to higher grades, as they felt that there was no potential for advancement in language. [redacted] Attrition of linguists has been of great concern, since departing linguists often represent the sole source of a language skill, and are therefore considered irreplaceable.

To solve this problem, Section 10 of the National Security Act of 1959 was amended to grant the Director the authority "to establish and support language and language-related training programs for civilian and military cryptologic personnel, provide special incentives, allowances and benefits to personnel in language and language-related skills, provide language training to families of designated personnel, and establish a Cryptologic Linguistic Reserve Program." The Agency thus hoped to make available sufficient language resources to provide for current as well as anticipated needs.

Several programs have been instituted as a result. Incentives, in the form of specialized training or pay, were established by NSA/CSS Directive No. 40-1, dated 6 May 1982, and include the three programs described in this paper: the Cryptologic Linguist Reserve Program (CLRP), the Foreign Language Incentive Program (FLIP), and the Family Language Training Program (FLTP).

P.L. 86-36

The Cryptologic Linguist Reserve Program

The CLRP was implemented to provide for a reserve pool of individuals with specific language experience whom the Director can call upon in emergency situations. It responds to the problem of attritting linguists whose departure leaves the Agency with little or no resources in a particular language. This group consists largely of former or retired civilian or military cryptologic personnel from the Agency, but may also consist of other individuals who the Director determines to be qualified. Members of the CLRP "agree in writing to serve for a period of one year, to serve in an active civilian status with the Agency during

EO 1.4.(c)
P.L. 86-36
DOCID: 4019715

periods of emergency, perform such linguistic or linguistic-related duties as the Director may assign, maintain their language skills as required, and accept such training as is required."

The program is limited to persons possessing knowledge of a Class I or Class II foreign language or one required by the Agency for crisis situations.

Prospective members must have worked with the language within the past 18 months or must have passed the appropriate Language Proficiency Test (LPT).

The CLRP is under the management of the Deputy Director for Administration (DDA.) However, it is the Deputy Director for Operations (DDO) who is responsible for informing the Director of an emergency situation that warrants the call to duty of members of the CLRP, as well as for establishing a priority listing of Class I and II languages requiring augmentation in a crisis situation. This listing includes the number of CLRP personnel needed in each language and is to be provided to the DDA and Assistant Director for Training (ADT). The Deputy Director for Programs and Resources is responsible for reviewing the manpower requirements for the CLRP and advising as to the availability of funds for the program.

Previously, individuals to be offered membership in the CLRP were recommended by chiefs of key components to the DDA. To help in the selection process, M3 circulated listings of recently separated employees to offices for their endorsement. In May 1986, however, a change was made from soliciting individual linguists to circulating information about the program to exiting GGD-07 and above personnel. A brochure was designed in late 1985, but as of mid-1987 it has not been published, largely for lack of funding. Nevertheless, in anticipation of the new system, the practice of circulating listings of separated employees to appropriate offices was dropped in July 1985.

P.L. 86-36

Members of the program are initially tested for proficiency and are to have follow-up testing or training after two years in the program. The program calls for members to be brought back for periodic training or operational assignment.

One of the main problems is that while the statute establishing the program calls for some sort of training after two years, it is not being done: three members have been in it long enough to be receiving this training, yet there is none available. M3J is still waiting for G Group to compile a training package.

The Foreign Language Incentive Program

The Foreign Language Incentive Program (FLIP), which began in November 1982, provides monetary incentives to civilian cryptologic personnel to acquire or retain language skills needed by the Agency. This program is restricted to languages for which NSA has an operational need or which have been designated as Class I or II languages. No one can receive these incentives solely for learning a foreign language.

A FLIP position is one requiring the use of foreign language(s), and for which the Career Occupational Specialty Code (COSC), civilian grade, job number and language(s) have been certified as eligible. Civilian employees must be assigned to established FLIP positions in order to receive this incentive pay. FLIP positions

P.L. 86-36

[redacted]

[redacted]

are certified by the individual's supervisor, and include three levels of proficiency:

[redacted]

FLIP is pro-rated for employees in a part-time pay status.

[redacted]

[redacted]

The Family Language Training Program

I am including the Family Language Training Program as a potential source of future linguists, though it was not designed for that purpose. It was established to provide language training for family members of both civilian and military cryptologic personnel assigned to representational duties outside the United States. Training is provided on a voluntary basis, is directly related to the assignment, and may be performed in anticipation of assignment outside the United States.

Family members who are eligible for this program are designated by the DDA in conjunction with the Deputy Director for Plans and Policy and the DDO. The ADT is to be notified of qualified applicants sufficiently in advance of their assignment so that training may be conducted within the United States. Training also may be performed outside the U.S., but only for family members who will be remaining on assignment for a reasonable period following the training. The DDA is also responsible for programming the funds and personnel requirements for this program.

Eligibility is determined by M3l (overseas personnel) and sometimes G Group for country desk positions. This training is done externally at various contractors, depending on language, such as Berlitz, Foreign Service Institute, Language Learning Enterprises, etc.

Because it is limited to family members of personnel representing the Agency at field positions, it is a little known, little used Agency program.

EVALUATION AND RECOMMENDATIONS

These programs offer Agency employees incentives in the form of post-retirement income and training as in the case of the CLRP, additional monetary and training incentives, as

DOCID: 4019715

in the case of FLIP, and exposure to language training for family members going to field sites, as in the case of the FTLP.

Each program provides an incentive to pursue specific language capability, although FLIP seems to be more aggressively pursued by linguists than the other programs. The main reasons for this seems to be that it is an ongoing program with wide Agency exposure, offers immediate monetary incentives, and experiences a large increase in the number of participants each year.

According to the outgoing FLIP coordinator, the problems with FLIP are minimal considering the size of the program. Because of FLIP it has become much more important to have positions classified properly, to have reassignments and details done on a timely basis, and for the panels to enter certification records into the system promptly.

Beginning in 1986 a "trailer card" has been distributed to FLIP recipients to remind them that they share in the responsibility for accurate payment of the FLIP bonus. FLIP also requires semi-annual certification by supervisors that personnel receiving FLIP are using the language as part of their duties. This was first done in June 1986 and will be updated every six months.

The CLRP is an excellent means of retaining capability in those languages which are under strength in the Agency. It enables the Agency to draw on experienced personnel in emergency situations. However, although well organized and well thought of by the Agency and its members, the CLRP seems to have run out of gas when it comes to the refresher training that is a requirement of the program. Unless this training is made available, how long can we expect those participating to maintain their interest and their language proficiency?

M3J is still waiting for G Group to prepare the training package for people who have been in the program long enough to require such training. Meanwhile, the G Language Coordinator is developing a language maintenance package that will be applicable not only to the CLRP, but to FLIP maintenance as well. The CLRP will then be assured of having capable linguists in reserve.

P.L. 86-36

Some problems concerning FLIP remain. For instance, there are currently 221 overrides that must be worked manually. This is due to existing qualifiers that are not recognized by the current computer program for payroll. More refined programming should eliminate the need for so many overrides.

A language committee that has studied this problem has submitted its findings to M37. In June 1986, M37 responded with a rewrite of this COSC. Eventually a change to the Career Service Occupational Handbook and an amendment to the PML on FLIP will be issued and this problem should be resolved.

In the case of the FLTP, although this program was established along with other language and language-related programs pursuant to Section 10 of the National Security Act of 1959, it seems that it was never as fully developed or utilized as other programs. I found that most people were either not aware of its existence or had no knowledge of its ever being used; some were aware that such training was provided for family members going to field sites. Moreover, it is restricted to higher grade levels. Obviously it needs a lot more exposure in order to be of any real benefit, as it does not provide the Agency with a noticeable "return on the dollar" as the other two programs do.

I was left with the question of the long-term benefit to the Agency of this program besides the immediate benefit of having our overseas personnel acquainted with the language of their field site. I believe that it is the potential for second generation Agency family members to develop into linguists as the result of having their interest in a particular language piqued during an overseas tour with their families. This interest could then result in becoming future Agency employees and linguists.

In summary, the Agency has addressed the problem of acquiring and maintaining necessary language capability through the institution of programs such as those addressed in this paper. Some are more effective than others, and some

need to be focused more closely if they are to achieve what they were initially designed to accomplish.

I strongly recommend that, as soon as it is feasible, a Regulation or PMM Chapter be published as a comprehensive directive for FLIP. To date the only directives existing are PMLs, and considering the magnitude of FLIP, a comprehensive directive warrants a high priority.

I believe that with these programs and improvements on them the Agency has taken a few first positive steps to correct the chronic problem of being unable to maintain a sufficient number of skilled linguists. I believe that they will in time alleviate the situation. And one program, FLIP, may well serve as an encouragement to linguists to remain in the field.

NOT CRASHING THE SYSTEM

I read with interest and some nostalgia [redacted] article in the 1st Issue 1988 of CRYPTOLOG titled "Crashing the System." I helped develop and later managed the RYE system that was mentioned in the article. Now I am involved in computer security matters. For these reasons I cannot resist setting the record straight and making an important point at the same time.

RYE was a transaction processing system which used a priority scheme for scheduling tasks. (I do not believe that the term "transaction processing" was invented in RYE's lifetime.) The priorities ranged from a low of 0 to a high of 7. All RYE executive and operating system software was written by NSA personnel in assembly language. Carol correctly states that RYE used a "greater-than-or-equal-to" instruction to test for priority 7. Since all alphabetic characters were numerically higher than all digits, when she input the letter "B" it was interpreted as a "7."

Sorry, Carol, you did not crash RYE; at worse, you aborted a task so that yours could load. Priorities 0-5 were valued in ascending order of importance. Priority 6 blocked lower priorites from loading. Priority 7 was for "critical" tasks (but not reserved for the Director) and would load immediately even if it had to abort, then later restart, a task. To preserve the sanity of our users, we arranged it so that

[redacted] *T03*

certain tasks like file maintainance could not be aborted. We did not want to leave a user with an unthreaded file.

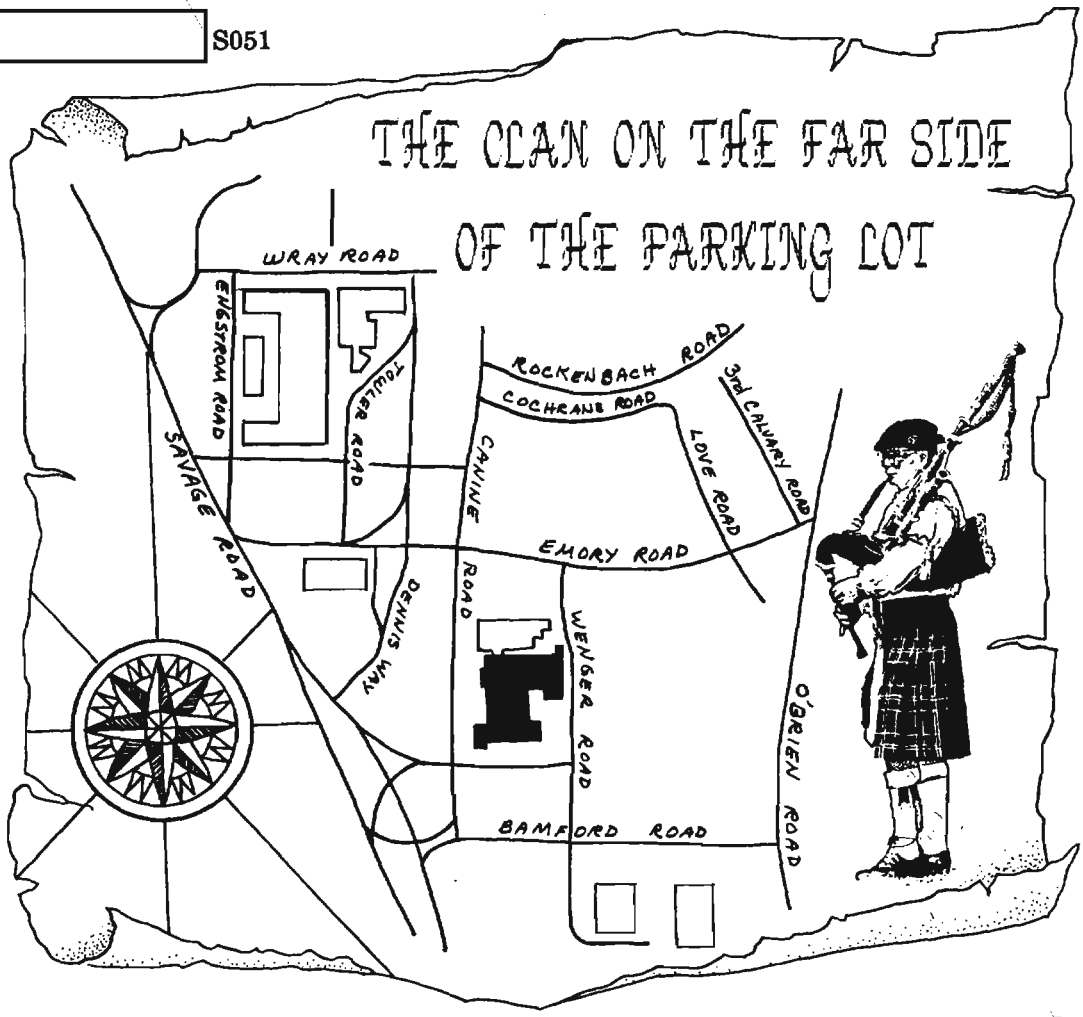
P.L. 86-36

RYE had extensive security and management features well before its time. Its on-line audit trails and analysis tools were valuable both for security and for functional evaluation. When people used the system, they left a "footprint" which we could use to re-create their actions. We could also evaluate every action of the system as it affected reliability and performance. Using these tools, we constantly "tweaked" the system to obtain maximum functionality. When Carol input her priority 7 tasks it resulted in an immediate entry on the operator's console. Analysis of the audit trail identified her as the perpetrator and told us her name, organization, telephone number, room number, and the location of her input terminal. As she pointed out in her article, we called her within one hour.

A key point to note here is the value of well-constructed on-line audit trails and analysis tools to support both security and management. □

~~*For Official Use Only*~~

[redacted] S051



P.L. 86-36

(U) Over yonder, a couple of hundred yards southeast of the Main Building, lies a complex unexplored and unknown to a majority of NSA employees. Hidden in recesses of the edifice known as Operations Building 3 lurks the INFOSEC clan. (Pervasive rumors indicate the clan is spreading to the hinterlands of Parkway Center, Friendship, and Airport Square as grazing space lessens at Ops 3.) Rather than continue to let the strange inhabitants known as INFOSECers dwell forever in anonymity, let us take a guided tour to learn their customs, organization, and how they contribute to the security of their nation under the great chief, DIRNSA.

CLAN MEMBERS

~~(C)~~ The clan consists of [redacted] including engineers, mathematicians, liberal (and conservative) artisans, technicians, computerers, business administrators, skilled craftsmen and print producers, as well as clan administrators, clerics and assorted shamans and wonder workers. The clan labors under the direction of Chief "Tall Tree" [redacted]

~~(C)~~ The clan is about 67% male and 33% female with an average age of 34. The average INFOSECer has 15 years of schooling, has been with the clan for ten years and has attained the tribal status of GG-10.3. At last count, 200 members of the clan have been initiated into the esteemed cult of "professionalized INFOSECers" wherein they have accrued rights and privileges not available to non-professionalized members.

TRIBAL OBJECTIVES

(U) The clan's mission is to ensure the secrecy and security of information transmitted or processed electrically among all of the members of the nation of which they are part. (An interesting sidelight to this objective is the perception among the INFOSECers that this mission is "the other side of the coin" and helps to support the objectives of a neighboring clan,

the SIGINTers. In fact, this perception is so pervasive it has been said in legend that the two tribes sprang from the same origins and in fact, neither could exist without the cooperation and knowledge provided by the other.)

CLAN ORGANIZATION

(U) Though all serve the same master, there are several separate, but complementary, sub-cultures within the clan that labor together to fulfill the great chief's bidding. These sub-clans are known as the "Cs," "Rs," "Ss," "Sos," "Vs," "Xs," "Ys," and "the Fielders."

~~(FOUO)~~ The Rs (R1 and R5) support the clan in the production of classified microcircuits, and the research, design and development of cryptographic algorithms for use in INFOSEC equipment. A large new building to house the burgeoning R1s is nearing completion on the edges of Ops 3 and will greatly increase the capacity for fabrication of special devices.

(U) The Ss are a diverse lot responsible for INFOSEC assessments, INFOSEC customer and industrial relations, technical security and INFOSEC planning.

~~(C)~~ The Vs are the INFOSEC program managers who design, develop, procure and field INFOSEC equipments and techniques for the nation. The Vs contracted for the production and development of over [redacted] in the past fiscal year.

(U) The Xs are the system security evaluators and standard developers. They delve deeply into the magic arts of cryptomathematics and TEMPEST.

(U) The Ys run the print facility (rumored to be second largest facility, in terms of quantity of printed materials, outside of the Government Printing Office). The Ys also provide a wide variety of INFOSEC support services to V and C programs and run the INFOSEC computer system complex. The Ys provide INFOSEC keying material (free of charge) to all validated customers, and also print many of the SIGINTer documents.

(U) The Sos provide the management support for the clan and are responsible for administration, finance, policy and doctrine, and INFOSEC international relations.

(U) The Cs are the newest of the groups in the clan and reside at Airport Square 11. (It is rumored that a new building for them is under construction.) The Cs, in addition to supporting the clan internally, also function as the National Computer Security Center, responsible for developing standards and evaluating applications of commercial computer products for the protection of classified information.

~~(FOUO)~~ The Fielders represent the clan around the world. There are full-time INFOSEC fielders located at NCPAC, NCEUR, NCR DEF, [redacted] SUSLO CHELT, NCR SAC, [redacted] and NCR SOUTH. There are also INFOSEC fielders at the Treasury Department, JCS, WHCA, NNBIS, U.S. Trade Representative, and GSA.

WHAT THE INFOSECERS DO

P.L. 86-36
EO 1.4.(c)

(U) Meeting the INFOSEC objective of protecting sensitive information is, in my opinion, as much an art as a science, so it is very difficult to describe how it is done. To make it clearer to those not acquainted with the INFOSEC methodology, here is a generalized example:

~~(FOUO)~~ An INFOSEC need (i.e., a need to protect national security information that must be transmitted or processed electrically) is established by a customer. The recognition of a need may be initiated by the customer or may be the result of an INFOSEC assessment (an analysis of threats vs. vulnerabilities) by the clan done at the request of the customer's organization. Examples of types of needs most commonly seen by the clan are needs to trust a computer or ADP system to limit file access, needs to protect a new communications system from exploitation, and needs to securely intercommunicate with allies. Before the need is then validated through tribal and national management, it must be clearly elucidated and fleshed out between the customer and a customer account executive to determine if it can be satisfied through an existing INFOSEC equipment or technique, or if a new development is required. Regrettably, in some cases, the clan lacks the resources to solve the competing needs of all its clientele.

(U) If the need can be satisfied through application of an existing INFOSEC equipment or technique, the customer is provided with procurement information, costs, delivery dates,

and technical parameters of the selected equipment or technique; the customer is also provided with assistance for ensuring that the integration of the technique or equipment within a given application is sound. The customer is asked to provide (and help is given to him) in formulating his concept of operations, key management and key requirements, maintenance concept, installation and fielding plans, and training. The customer is consulted in the development of system and equipment doctrine and kept advised of equipment modifications that may be necessary during the life of the equipment. Assistance and customer support is provided by the clan throughout the life of the requirement.

(U) When the customer's need cannot be satisfied by an existing equipment or technique, the clan may undertake development. The process described above is front-ended by identification of funding, task prioritization establishment of a development plan and milestones, algorithm design or technique development, evaluation, fabrication and contracting. In many cases, a test and evaluation is specified to ensure correct operation in a system.

(U) In both cases the clan must ensure that both the design and implementation of the equipment or technique are sound, that a multitude of security-related considerations are satisfied, that the customer understands INFOSEC policy and doctrine related to the system, and that the customer has the corporate infrastructure necessary to ensure that INFOSEC is, in fact, being obtained.

WHERE THE CLAN IS HEADED

(U) The business of the clan is constantly expanding as more and more of its customers recognize the need for INFOSEC and as telecommunications grow and computers proliferate. The clan has found that closer relationships with industry can provide help and ensure that INFOSEC needs are satisfied by drawing upon the expertise of industry. The clan has established a very close working relationship with the computer industry and is encouraging the use of their resources in developing computer security techniques and products. It is likewise working with the carriers of communications to ensure that INFOSEC needs are considered in the development of switching and transmission systems.

CONCLUSION

(U) From this brief sojourn we have learned that the INFOSECers are not so strange after all. Some of you may even know them, ride in car pools with them, and associate with them. We have also concluded that the far side of the parking lot is not so far away and is an integral part of the NSA structure and mission.

AN INVITATION

~~(FOUO)~~ I was asked by tribal management to dispel the mystery surrounding the clan and to spread the word and invite talented SIGINTers and other personnel to help the clan prosper and meet its objectives. I am convinced that the clan has an active intern program and a program to help on-board INFOSEC personnel join the cult of the professionalized and advance through the organization. As outlined during my tour of the tribal organization, the challenges faced by the clan are unique, interesting, and provide a real sense of satisfaction. The tribal chief has invited all interested NSAers interested in learning more about INFOSEC or in becoming INFOSEC clan members, to contact the INFOSEC Career Panel, H113, 972-2308. □

Solution to NSA-Crostic #66, Ist Issue 1988

Arthur J. Salemme, "A Few Tricks of the Trade (for the Translator of Russian)," NSA Technical Journal, Fall 1966.

If the translator of Russian can maintain the author's original style and can avoid awkward constructions in English, he will be more and more likely to hear the ultimate compliment of the non-linguist, "Why, it doesn't even sound like a translation!"

DOCID: 4019715

THE FALSE FRIEND: A True Story

EO 1.4.(c)
P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019715

EO 1.4.(c)
P.L. 86-36

DOCID: 4019715

~~FOR OFFICIAL USE ONLY~~

EO 1.4.(c)
P.L. 86-36

DOCID: 4019715

BULLETIN BOARD

SUN USERS GROUP

Persons interested in joining a SUN Users group are invited to make themselves known to [redacted] R53, FANX III, 968-8845.

P.L. 86-36

UNIX SEMINARS

CRYSCOM is holding monthly brown bag seminars on UNIX in the North Cafeteria in the room behind the glass doors. Interested persons are invited to attend. For a schedule and further information, get in touch with [redacted] P.L. 86-36 [redacted] T335.

MACINTOSH USERS GROUP

Persons interested in forming a Macintosh Users Group are invited to make themselves known to: [redacted] R822, FANX II, 968-8807 or 963-1011.

P.L. 86-36

SOURCE OF OUTLINE MAPS WANTED

CRYPTOLOG is seeking a source of high quality reproducible black-and-white outline maps. Geographic now stocks only colored maps which do not reproduce well. Also, they are cluttered with irrelevant information, which makes it impossible for authors to superimpose their own information legibly.

For articles published in CRYPTOLOG we need the kind that is used in schoolrooms, showing only rivers, or roads, or principal cities, or national boundaries, etc., that children fill in for tests. Please note that maps output on a dot-matrix printer are not of acceptable quality. Call the Editor, [redacted] 963-1103 or send a note to her at P1, HQS

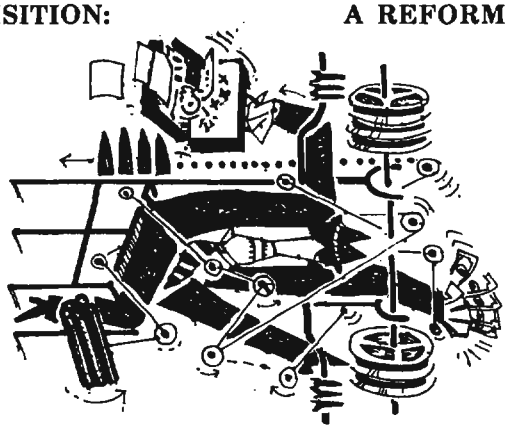
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019715

SOFTWARE ACQUISITION: A REFORM IN NEED OF REFORM



P.L. 86-36

T35

~~FOR OFFICIAL USE ONLY~~

In the fifties and sixties, software development had been by the seat of the pants – get the job done as quickly as possible, documenting afterwards if time permitted. Then, in the seventies, fueled by anxieties over the growing costs of software maintenance, and virtually mandated by reports from the Director's Scientific Advisory Board, software development underwent drastic reform.

The reform had its most dramatic impact on the methodology of developing software. It came to be known as "software acquisition," and the pendulum swung virtually 180 degrees from seat-of-the-pants to a series of formal, discrete, sequential steps. These consisted of: gathering all the requirements, reviewing and freezing them; drafting a preliminary design and reviewing it; detailing the design, reviewing, and documenting each step of the way; coding, unit testing, integrating, and finally, bowing to the few customers who outlived the process.

The reform affected both policy and procedures. Some of the resulting policy measures have been beneficial, such as employing higher-level language in the place of assembly language and employing commercially available off-the-shelf software where feasible. And undeniably, the Agency had been paying (and is still paying) a high price to maintain software that had been developed quick-and-dirty and that was never cleaned up. Some correction was needed to obtain cleaner and more maintainable software.

In recent years, a larger portion of the Agency's software has been developed under contract, and its effect on the cost of that software should not go unmentioned. In the past, formal deliverables had been required as a part of any software contract, but now, contractors are required to adhere to the Agency's formal software acquisition methodology.

Incontrovertibly, contractor-developed software comes at a much higher cost than in-house developed software – say a cost factor of two or three per man-year. Since the cost of employing the current methodology adds its own overhead factor – in my estimation perhaps a factor of two or three – software developed out-of-house is costing the Agency perhaps four to nine times what it might otherwise cost.

I acknowledge that the software being delivered today is cleaner and easier to maintain than in the past, but I contend that in terms of costs expended and value subtracted, the trade-off is unacceptable. The cost of the cure has been more than that of the sickness. Specifically, the practices which have evolved in the quest of developing maintainable software are outrageously costly in up-front manpower and time, and are doing grievous harm to the Agency's ability to deliver a timely, useful, product. And I firmly believe that it is possible to acquire clean and maintainable software at a much lower cost.

It should be noted that many who extoll the benefits of the new methodology are from the private sector or academia with an axe to grind: people and organizations who have been enriched by it, such as contractors, course givers, and textbook authors. I can recall no CISI speaker who advocated this methodology who did not have something to gain by so

doing. Prolonging projects is meat and drink to these people. No contractor would welcome a change in Agency methodology that halved rather than doubled the duration of its software contracts.

Moreover, the delivered product is often apt to be not quite right owing to inevitable changes in the requirements. In sum, today's software acquisition process subtracts timeliness and responsiveness from the delivered product and adds additional costs. My observations lead me to believe:

- that today's software acquisition methodology is having a debilitating affect on the Agency's ability to deliver timely, functional software;
- that Agency dp customers have recognized for sometime that the process isn't working;
- that Agency finance people have recognized for some time that software costs are spiraling, but without obvious improvement in quality, timeliness, or customer satisfaction;
- that Office and Group Chiefs are experiencing a sense of malaise over a growing inability to respond to operational challenges with timeliness except when a quick-response situation is decreed.

Nevertheless – perhaps because of the lulling affect of academicians and consultants who are either unaware or unconcerned about the needs of the Agency to expedite the delivery of software – Agency software acquisition methodology has continued to go unchallenged.

FALLACIOUS PREMISES

Today's software acquisition methodology seems to be based on a number of fallacious premises. One is that more work makes for a better ultimate system. It is a fallacy because the "more work" is not technical but bureaucratic. More documentation is required, more inspections, more reviews, more workers, more coordinators, more and larger teams, and so on. I note that:

- bureaucratization is seldom salutary;
- the more people involved in an effort, the more overhead will be involved in coordinating that effort;
- individual accomplishment, motivation, and morale are reduced rather than raised when each person is asked to play a lesser part in a large group effort.

The major fallacy is bureaucratic formality which tends to treat system development as a closed set of well-documented sequential steps rather than as an interactive process. Consider, for example, how the methodology calls for an extensive up-front effort to identify and document every last requirement at the outset. Since requirements are seldom static, and seldom clearly and accurately known at the start, this is effort ill-spent.

I believe that it is better to gather the major and obvious requirements, and accumulate additional requirements as the project progresses, since the development of a system should be interactive rather than sequential in order to expedite the development and to ensure the fidelity of the product. The charge of the team should not be "figure out the totality of the user's needs, design a way to do it, document it, then do it." Rather, the philosophy of the development team should be "determine the types of services the user needs, arrive at or develop general software tools to provide them, begin prototyping and interact with the customer until his needs have been met." Documentation should be kept to a minimum until some degree of certainty is present.

Aside from fostering an improper sense of sequentiality, formality in itself imposes a drag on project development to the extent that it inhibits rather than encourages exploiting and integrating the knowledge gained in the systems development process. New or newly-perceived requirements or methods must be filtered through a formal, coordinated, impact-gathering process. Enhancements being thus discouraged, the resultant software product is often bereft of what was learned, and represents the needs and services as they were understood only at the inception of the pr ject. As a result, the long-awaited system is apt to disappoint when it finally is delivered.

In the past, software developed ad hoc, though imperfect, had the redeeming merit of giving the user the function he needed in a timely fashion. Today's formality discourages ad hoc enhancements, and serves only to elongate projects.

Another fallacy is that software designers and developers cannot satisfactorily find

DOCID: 4019715

and fix their own mistakes. Admittedly, in earlier days, programming was "by gosh and by golly," in part because it was a new and little understood endeavor. But today's software developers are far better prepared than their predecessors to analyze, design, implement, test, and document. Most of the Agency's newly hired programmers have a degree in computer science (which consists of formalized information gained from the experience of those pioneers in the early days of programming) and so their technical knowledge surpasses that of their predecessors.

Today's methodology – which calls for inspections, walk-thrus, independent test teams, and odious levels of documentation – can only serve to stifle these new hires. I find absurd the notion expressed in the literature that it takes three or four peers to inspect code or design, and that it takes an independent test team to test an implementation team's software. This notion is absurd both in terms of costs and the implied denigration of the technicians. Contemporary developers, given their education and background, require less documentation than did their predecessors and find today's required documentation stultifying to prepare and time-consuming to maintain, and obfuscatory as well, precisely because there is so much of it.

One of life's self-fulfilling prophesies is that when one expects less of people than they are capable of, they deliver accordingly. I see that Agency software acquisition methodology is having the undesirable effect of demotivating its workforce, in flagrant disregard of the respected management writings and teachings of Maislow, Herzberg, and Argyris which are diligently taught by our own Training School.

THE BETTER WAY

Consider the ingredients which are critical to a sound, successful software development:

- *A simple design* accepts the premise that the full set of requirements is not knowable from the start, anticipates that there will be changes to the requirements as they were initially stated, and tends to lower the cost per change. A simple design also reduces the learning curve of newly-acquired personnel.

- *Prototyping with user-involvement* enables the project to be started quickly, with the understanding that lessons will be learned rapidly, and that both the customer and the development team will increase their knowledge of the system requirements during the development process.

- *Incremental development* assures the customer earliest possible delivery wherever possible, and enables mistakes to be observed and repaired at the earliest opportunity. Turnkey development is risky at best, and is devoutly to be avoided in all but the direst of circumstances.

- *A small tightly-organized do-it-all team operating with minimal bureaucratic formality* has the advantage of productivity, high-morale, rapid development, and a high degree of individual responsibility.

- *Minimal bureaucratic formality* is a controversial yet key element in the equation. The drag in today's methodology is the amount of documentation which must be generated, and ultimately updated if a change is accepted. It is better to use minimal adequate informal documentation while development is fluid, and to encourage fluidity so as to respond dynamically to new requirements with minimum cost and schedule risk.

An interactive system development effort which involves a small, cohesive design-development team, unburdened by formality, and interacting with the customer on a continuing basis results in:

- a product whose risk of disappointing the customer is minimal, and whose initial delivery to the customer is rapid;

- a process which rapidly assimilates knowledge gained into the developing product;

- a team whose performance is characterized by a high degree of esprit de corps, individual responsibility on the part of each member, and productivity.

While the concept of back-loading rather than front-loading documentation is admittedly controversial, the advantages of a small-team approach are widely accepted. However, many people believe that a small-team approach is inappropriate for any but a small project. This assertion is preposterous. The mistake all too often made is to declare a project "large." If a project is large, it should be broken into

DOCID: 4019715

inappropriate for any but a small project. This assertion is preposterous. The mistake all too often made is to declare a project "large." If a project is large, it should be broken into smaller projects. Diners do this when they are eating a steak; savvy managers do this when they organize to solve problems; and the principle is no less true for large software undertakings.

Despite a long history of success in developing smaller systems using a flexible methodology, the Agency has suffered great difficulty in developing large software systems using today's software acquisition methodology. To my mind, the corollary that follows is that large software systems should not be "developed," but rather "coordinated" as a series of small-team minimal-formality efforts. Of course, the interfaces amongst the teams must be clearly defined, and the coordinator must do his job skillfully.

SUMMARY

I find today's software acquisition methodology labor-intensive, costly, and cumbersome, and undercutting the Agency's ability to deliver large software efforts on a timely basis. While the software delivered is value-added to the extent that it is more maintainable than in the past, it is also value-subtracted in terms of its lack of timeliness and responsiveness to the customer. Ancillary drawbacks of the methodology are its inflationary effect on already expensive contracted software, and its demotivating affect upon the workforce. The costs seem to outweigh the benefits by far. A review of the methodology is sorely called for.

An alternative methodology, suggested by the Agency's history of success in quick-response efforts, is to employ small teams which are less formal and more flexible, which emphasize the importance of individual accomplishment, and which are in concert with Agency objectives in productivity and excellence. Extending small-team methodology to the development of large systems requires that large projects be divided into and skillfully coordinated as smaller efforts of a size appropriate to a small team of developers.

Let those readers who feel that the Agency's software acquisition methodology is successful accept my challenge to support a disciplined review and re-evaluation of this methodology. Let those who find agreement with the contentions expressed here do the same. Nobody wishes a return to the transgressions of "seat-of-the-pants" software development or the repeal of software reform, but the pendulum's full swing appears to be imposing an unacceptable burden on this Agency, and the reform itself is in need of review and reform. □

P.L. 86-36
EO 1.4.(c)

in re LACONIC

[redacted], *DDO/ACAO*

P.L. 86-36

Lately, many classification advisors have received queries concerning the use of the term "LACONIC." Its use is sometimes confusing, and it is often taken to indicate a special clearance or classification. It is not a clearance or classification, but a handling control marking.

LACONIC is a restrictive distribution indicator for certain [redacted] techniques. It is a handling caveat designed to warn the reader that the accompanying material contains information concerning [redacted] procedures. It does not require a special clearance, but the reader must have a need to know certain [redacted] details. In addition, this caveat is designed to deny access to contractors and consultants, therefore the marking "NOCONTRACT" should always accompany it. Both markings are used in order to denote that the material is NOCONTRACT because it reveals [redacted] techniques.

When marking correspondence containing LACONIC material, the caveat LACONIC-NOCONTRACT should be stamped or typed at the bottom of the page in proximity to the classification. An example of a paragraph portion marking is TSC-LACONIC-NC. LACONIC must be spelled out, not abbreviated, in a portion marking.

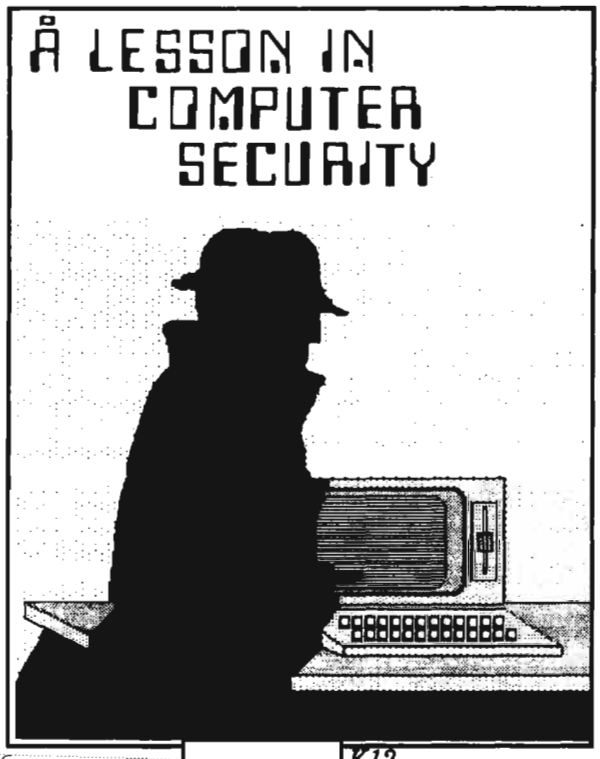
The NSA/CSS Classification Guide 58-83 further describes the use of LACONIC. Specific questions concerning its use should be directed to P1, on 963-3957s.

(The above information was adapted from Notes From the BCAO, December, 1987, by Richard Sylvester, B/CAO.)

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

~~*THIS ARTICLE IS CLASSIFIED CONFIDENTIAL IN ITS ENTIRETY*~~



P.L. 86-36 K12

Most of us in Operations don't think much about computer security (COMPUSEC). As an Intelligence Research Intern, I knew next to nothing about it until I worked in X23, the Division responsible for technical computer security evaluations of NSA systems.

Before my tour there, I had assumed that I didn't really *need* to know very much about COMPUSEC. *Somebody* must be taking care of it: "this is NSA, after all. If you can't trust an NSA computer to keep your secrets secret, whom *can* you trust?"

But I learned that in 1986 there were three computer security incidents involving an NSA computer system. The system was DOCKMASTER, an unclassified computer system used by the National Computer Security Center to share COMPUSEC information with contractors. DOCKMASTER is accessible via direct dial-in commercial networks and DoD networks, and can therefore be accessed by a person with a terminal, a phone, a valid user ID, and a password. Although DOCKMASTER is rated as a B2 level system (relatively resistant to penetration), its built-in security features alone were not enough keep out unauthorized users.

In March 1986, someone tricked a DOCKMASTER user into giving passwords over the phone. But after revealing the passwords, the user realized that authorized systems personnel wouldn't need a user's password to get into the system. He called the system administrator, who quickly locked the accounts in question and shut out the would-be penetrator. **Do not give your password to anyone!**

Another user was denied access in October because his account was already active–in other words, someone had already logged in using his ID and password. The user notified the system administrator, who kicked out the intruder and locked the account. The unauthorized user had previously penetrated a computer system connected to DOCKMASTER. The hacker had apparently implanted a "Trojan horse" which grabbed users' passwords, including the one used to access DOCKMASTER. The hacker logged in over a phone line to the remote host and used the stolen password to log into our system from there. What if the real user had simply assumed, as many would, that there was just a glitch in the system that day?

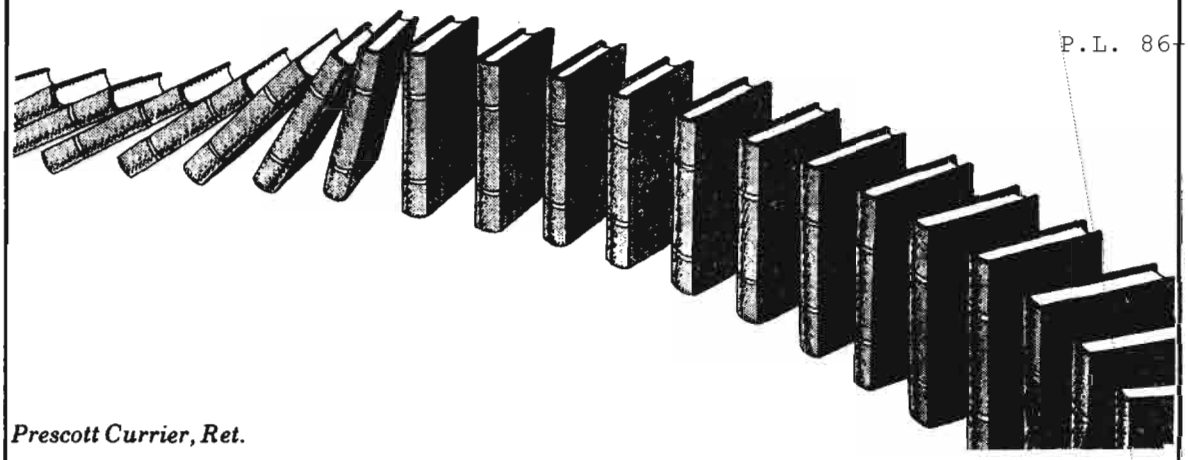
In still another case, an alert DOCKMASTER user, logging in around mid-November 1986, noticed that he had not been working at the time shown by the system as his previous login time. Like most NSA systems, DOCKMASTER stores each user's login times and, upon login, displays the previous time to the user. Most of us ignore this message, but on this occasion the user noticed that the time displayed by the system had been on a Sunday. The user, who wasn't a shiftworker, immediately reported the discrepancy to the system administrator, who locked the account and prevented further unauthorized access. Subsequent audit checks showed that the intruder had been in the system for a total of two hours and fourteen minutes over several days. That may seem like a short time, but it would have been enough for the intruder to grab over two billion bytes of proprietary information if the owner of the account was authorized access to this data.

Admittedly, there are no classified systems that can be accessed by outsiders as DOCKMASTER was. But consider the possibility of another Pelton. Would you notice if your computer said that you had been logged in during your vacation? □

DOCID: 4018715

Data for the Language and Linguistics Section of the Country Reference Books

P.L. 86-36



Prescott Currier, Ret.

~~THIS ARTICLE IS CLASSIFIED CONFIDENTIAL CCO IN ITS ENTIRETY~~

This article, originally published in the May 1968 issue of The Quarterly Review for Linguists, was mentioned in the last issue of CRYPTOLOG as a model for preparing a language brief. In response to many requests for copies we reprint it here.

Again we invite linguists to contribute language briefs to CRYPTOLOG following this outline or in any other format.

The Country Reference Books are to be a series of publications designed to provide useful technical information in ready-reference form on each of the target countries of interest to NSA. They will contain data on C/A, T/A, and Language, plus an introductory chapter of general interest material on the country concerned. The Language and Linguistics Chapter will be divided into two sections: the first devoted to a brief description of the characteristics and uses of the standard language; the second a compendium of cryptanalytically-useful information on the telegraphic language. A suggested Table of Contents for the Language and Linguistics Chapter is as follows:

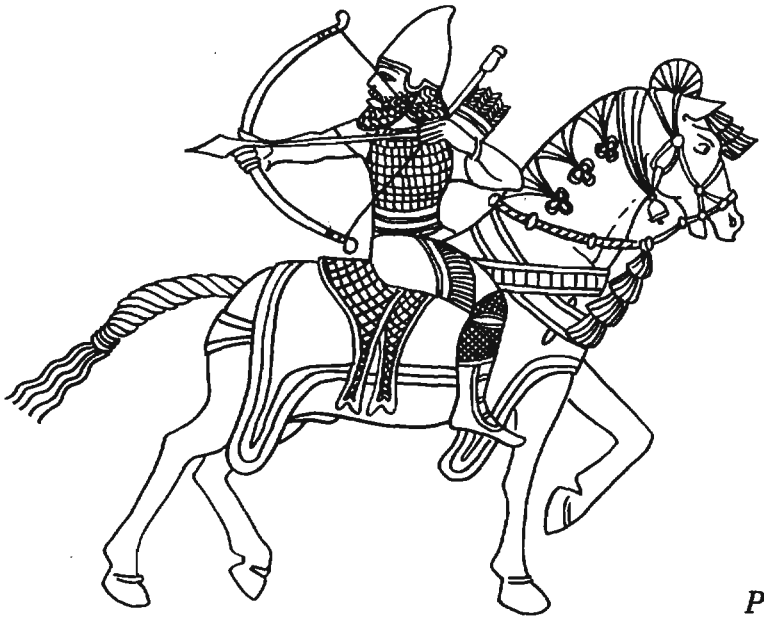
Disappointingly little progress has so far been made in collecting and compiling the linguistic data for the Country Reference Books. This is due largely to a dearth of available talent to undertake the tedious and time-consuming task of collecting the rather formidable amount of data scattered throughout P, and to sort, correlate and prepare the material for publication.

To assist in gathering the data already prepared by the various analytic elements for their own use, it would be very helpful if each element could provide P1 with copies of the cryptolinguistic data now in the hands of their operational linguists. The data need not be prepared formally, nor need it be in a prescribed format. The object now is to accumulate centrally (in P1) as much operationally useful language material as now exists but to do so without imposing too great a burden on the all-too-few linguists at work on all-too-many operational problems. If copies cannot be provided, a simple listing of the material will suffice. P1 will undertake to get it reproduced.

P.L. 86-36

~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

A PARTHIAN SHOT



Peter Jenks, Ret.

~~THIS ARTICLE IS CLASSIFIED TOP SECRET UMBRA IN ITS ENTIRETY~~

The author was D/Chief, G, when he wrote this account just before retiring in December 1979. When the paper surfaced during a recent move it was presented to CRYPTOLOG for publication. This is a condensed version.

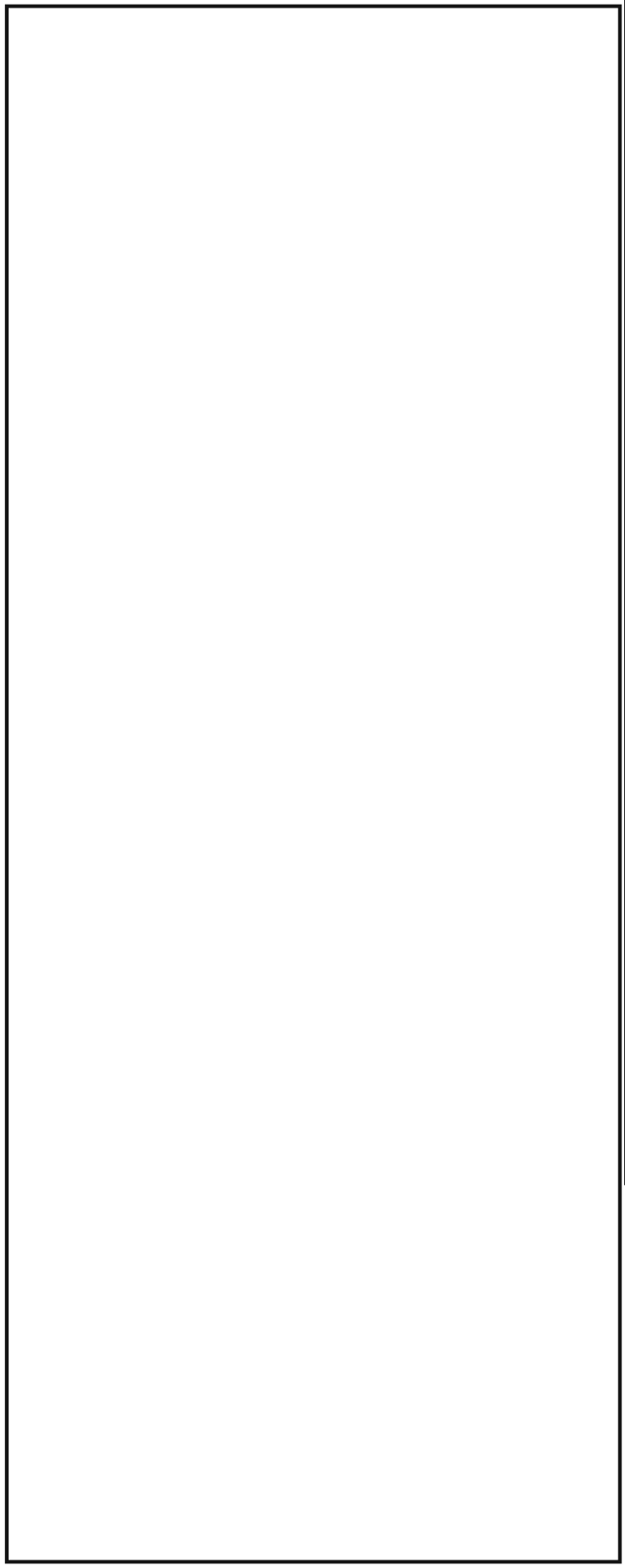
I am completing some 32 years of work as a cryptanalyst, a career which has taken me from crumbling old IBM listings to something called the Architect for Cryptanalysis; a journey which has taken me through A, B, and G through diagnosis, exploitation, and something called paracryptology; an itinerary in which I have served the cause of cryptanalysis in the most hermetic of compartments and as advocate in the most exposed of locations.

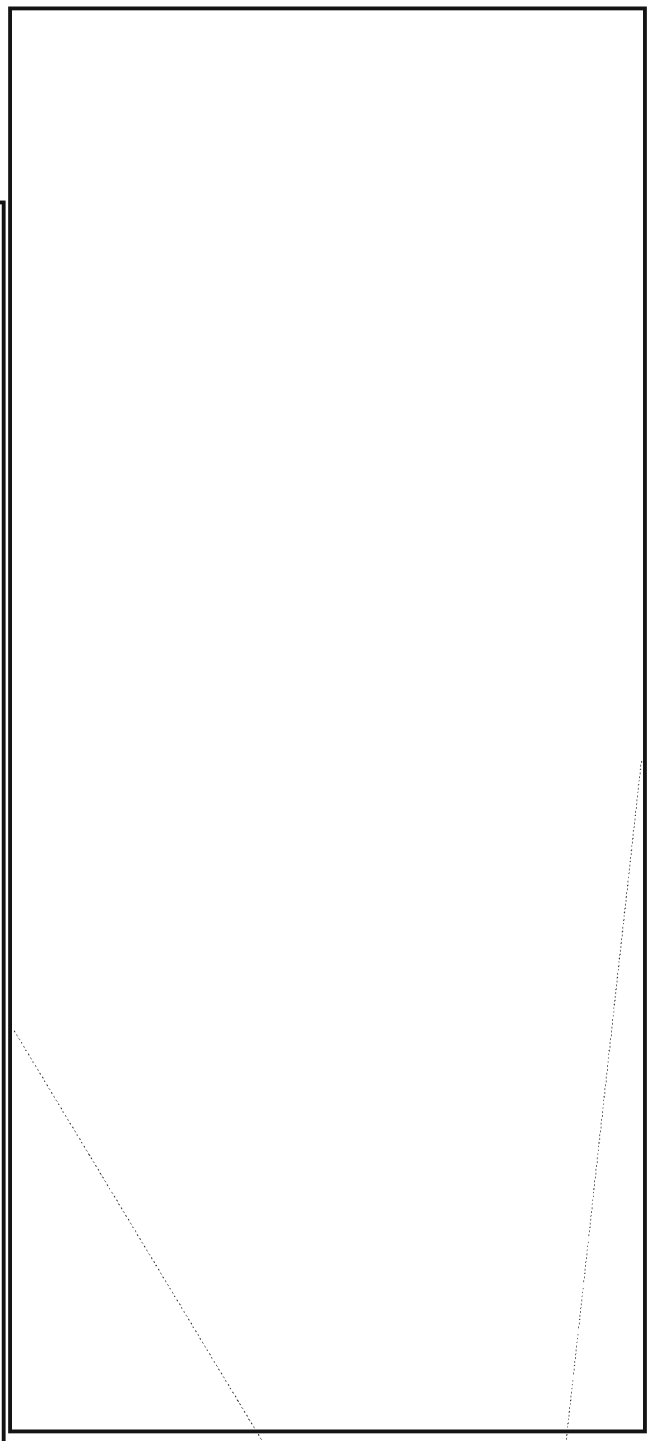
I propose to describe that career briefly, attempting in passing to identify perceptions and convictions which experience later conferred and ratified.

My first experience of the Agency was the training school; in those days (1947) they hired you provisionally first, and cleared you second, and in the interim you passed the time in training school--working your way at your own speed through MIL CRYPT I, II, etc., and doing it again if you stayed long enough. I was enchanted and somewhat puzzled by the medieval character of both the subject matter and the exposition. The sensation of entering a culture was strong and welcome, if the character of that culture was a little surprising.

EO 1.4.(c)
P.L. 86-36

I realized that proving a negative is one of the most difficult tasks facing a cryptanalyst and, in addition, that proving an unwelcome negative carries its own difficulties.





This was to be one of the most important points in my career both professionally and as an analyst. Marshalling the evidence, securing acceptance of inferential processes, and a clear delineation of the scope and depth of analysis were required. This I did, and got for my pains a promotion and a vastly greater domain of analysis.

Recognition at last! I should not imply that all, or even most, of the foregoing was indebted to me. At least four work centers were

EO 1.4.(c)
P.L. 86-36

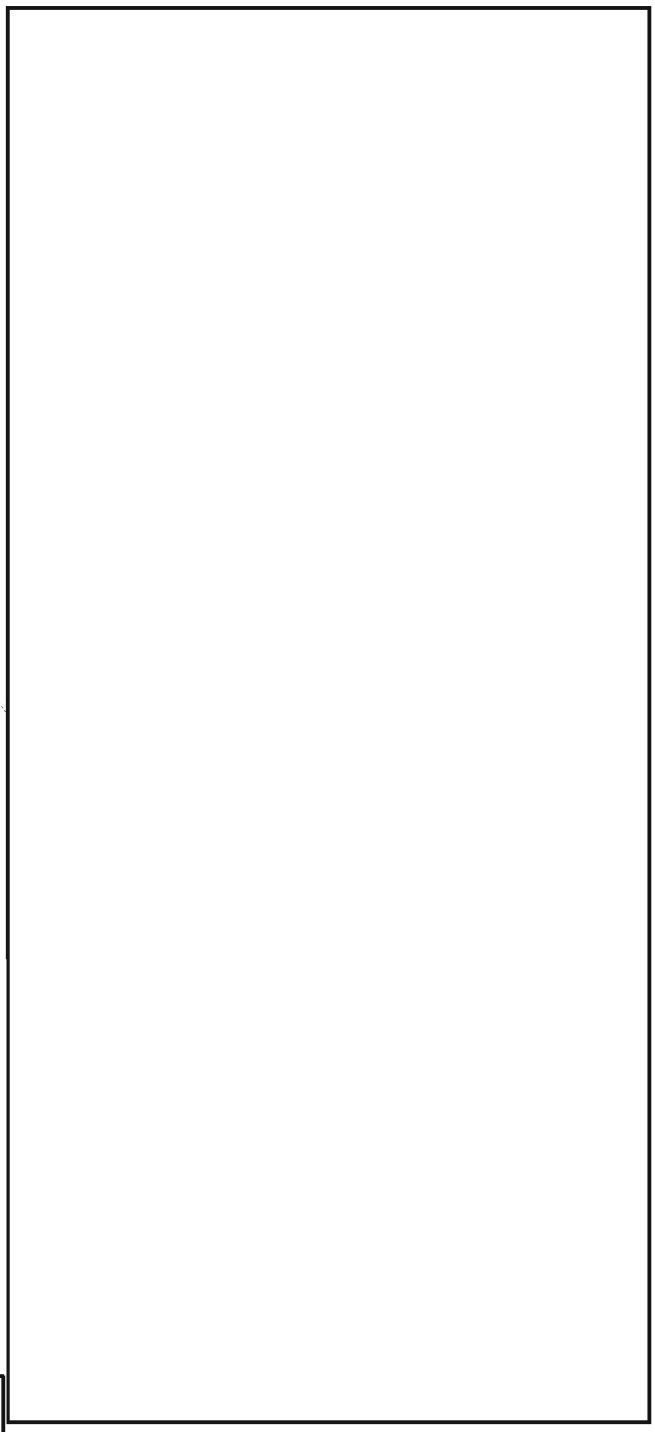
laboring on analogous problems with a common intimation emerging. I fared better than my peers as a result of undisguised ambition, at least in part, but equally because I saw extremely cogent reasons for putting the whole case in writing and acted upon them, if only to deflect the assignment of more resources to a hopeless venture.

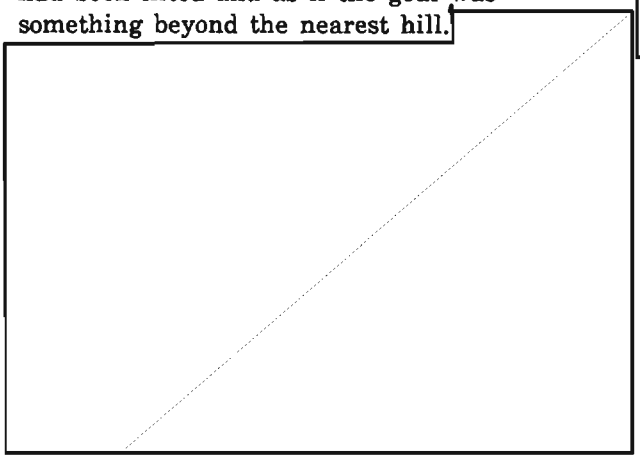
My new job entailed, in effect, analytic direction of the work centers mentioned above, the assembly and preparation of branch technical reports, and research. I took all of these things really seriously.

Management at last! I took this, in those days, as a way to extend my reach, to multiply my energies. There were things I felt should be done on a broader scale and in greater depth and now, now I could direct that these things be done. In retrospect, an arrogant and autocratic view, but not totally without merit. At least I knew what I wanted to do.

Publication at last! There was never much doubt in my mind that the world would be better off for my views. By the time I took on this task I was already a prolific writer even if my readership included only my bosses, and the exercise was beginning to pay off for me as an analyst: the articulation of premises, principles of inference, and conclusions has its disciplinary character; the asking of questions makes some demand on oneself as well as others for answers; the enunciation of plans and goals involves similar moral imperatives. Whatever else it did I was in no doubt that this work was making me a better analyst.

Research at last! As it happened, the research I performed here was, yet again, diagnosis but somehow I felt as if my sights had been lifted and as if the goal was something beyond the nearest hill.





P.L. 86-36

This stupid job and my miserable performance of it obviously qualified me for high office, and midway in that tour I received a very nice offer to be a deputy chief to a chief I much admired (if with some admixture of hostility) and under a group chief who had always intrigued the hell out of me.

[redacted]

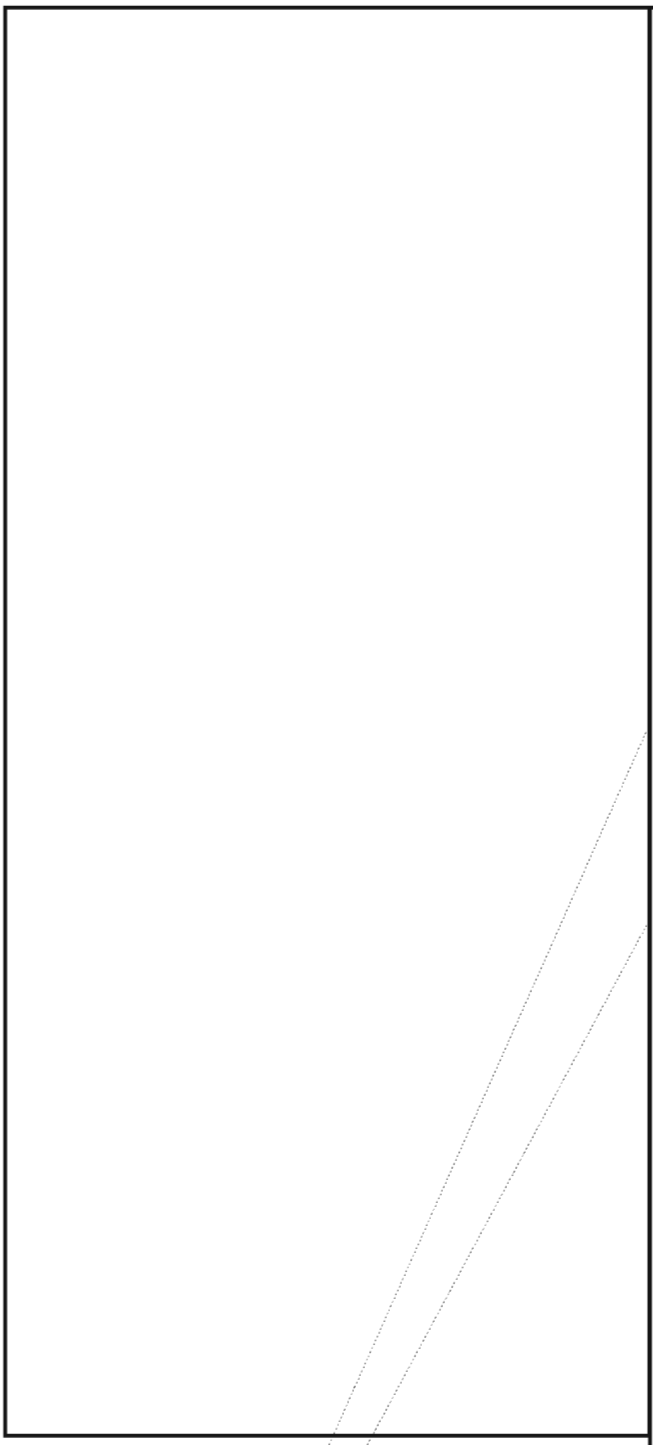
At this point I felt there was little left to understand about the target, and indeed that it was time for seniors to make some judgment about the future of the effort. I presented an extended account accordingly of what was known, how it was known, and what, inescapably to me, it implied.

And so I got a new job! The new job involved responsibility for all key analysis, although in practice the mission was directed at one particular target. Primarily on this account the effort was highly compartmented.

An office at last! With walls and a door. And soon enough, a computer of our own. But more important, although I didn't realize it at the time, was the elite membership of the group and, indeed, the elite character of our bosses. Our little group of twelve was to produce two GS-17's, and one 16, and it was to serve as the seed-bed of a number of enterprises which have since become respectable empires of their own. As is so often the case with such groups, it was independently subordinated, reporting upward by two, rather than one, echelons. In those circumstances, typically, the group writes its own mission, sets its own goals, and monitors its own performance. Given good marching orders and good people it is an arrangement hard to beat.

[redacted]

EO 1.4.(c)
P.L. 86-36



By the time I took on this task I was already a prolific writer even if my readership included only my bosses, and the exercise was beginning to pay off for me as an analyst: the articulation of premises, principles of inference, and conclusions has its disciplinary character; the asking of questions makes some demand on oneself as well as others for answers; the enunciation of plans and goals involves similar moral imperatives.

EO 1.4.(c)
P.L. 86-36

[redacted]

[redacted]

It was time once again to assemble all the evidence and draw the inescapable inferences for my bosses. I did this and was sent off to GCHQ as a liaison officer.

[redacted]

The analytic responsibilities were actually well-timed. By now I felt myself to be possessor of a scientific methodology which worked and which was attuned to me as a person. And at this point I must depart from my plan of not mentioning names. I had resolved not to do so because to give credit to all my bosses, colleagues, and subordinates in just measure would multiply this paper by a factor of ten,and still risk slighting a large number of respected associates and valued friends. Better by far to slight all uniformly and risk the imputation of stealing merit not justly mine. However, there was one NSA figure and one at GCHQ who so decisively shaped me that to ignore them is to tell a fundamental lie. The NSA figure was Art Levenson, my boss in the period just described.

Art, of all my bosses, brought a philosophical turn of mind to his life's job; a recognition that cryptanalysis is a culture with a history and tradition; a sense that cryptanalysis is a science offering an arena for intellectual triumph and artistic Integrity; a concern for the moral and ethical ambiguities which of necessity attach to our work; a high appreciation of, in particular, thought and courage. To a young man whose greatest fear in those days was that he was throwing his life away, there could have been no better boss.

Continuing the slight discursion, there was another cultural force which then and was to continue to shape me. This was the Class of '51. In that year a bunch of extraordinary young mathematicians, hired at once in a deliberate and careful way, and mainly assigned to 206 (later 064), the Agency's training ground and base of operations for the cryptanalytic elite. I was very envious and, in fact, jealous of this crew. I would have welcomed early on an invitation to join 064 but later it became a point of pride to me to not be in it.

Negative influences, though, can have powerful effects and not necessarily bad. Feeling set off from my peers and destined to a different route, I both consciously and unconsciously set out to make the best of that, often as not by a deliberate contrast. This was all very well but a difficulty was about to emerge. Briefly, to be a good liaison officer you need at a minimum two things–a knowledge of the field you will represent, and an old-boy relation with the leaders in that field. I found myself with neither.

I had no experience [redacted] or of those who directed it. A series of briefings and a well-filled notebook were not to remedy this. Both the problems and the people swarm in my mind. If ever I was going to

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36
DOCID: 4019715

have to fake it, the time was now. And so to GCHQ.

I was to find the job detestable but not for the reasons I feared. The job turned out to be an office boy task complemented by supposedly obligatory rounds of party-going. I found that my predecessor had developed an idiotically complex and comprehensive filing system for documents never again referred to, and an equally time-consuming mail distribution and logging system whose chief attribute, as I saw it, was the destination of documents to long-ago abolished organizations. This situation I corrected only to find myself thereafter with nothing to do. Well, as noted above, I didn't know the field [redacted] worth a damn so I passed the time mainly by reading the technical reports I was charged with passing to and fro. This proved in the long run to be a very smart thing to do. But I can't say I knew it then.

This stupid job and my miserable performance of it obviously qualified me for high office, and midway in that tour I received a very nice offer to be a deputy office chief to a chief I much admired (if with some admixture of hostility) and under a group chief who had always intrigued the hell out of me. The office, moreover, was engaged in [redacted] a field in which now I felt at home and anxious to make a contribution. I was spared by this happy offer the humiliation which characterized the typical overseas tour--looking for a job, hat in hand. This, plus getting a promotion at much the same time, certainly mitigated an otherwise somewhat depressing tour. I am speaking professionally of course; I and my family loved the non-professional aspects of the tour.

Before leaving the matter of GCHQ I must make a bow in the direction of [redacted] I had seen Hugh from the fringes several times in the past decade and there was nobody in my life who had impressed me by half what he did. He had then and continued to have for me the attributes of genius, an almost naive innocence in approaching new problems, all too swiftly followed by profound insight, and an instinct for the jugular insofar as that problem was concerned. A strange mixture of art, scholarship, and science. Not without the defects of his virtues either; impatience, arrogance, irrelevance. This exposure was of some importance to me. I wanted very much to believe that my chosen field captured and nurtured transcendent intellects, and in Hugh any doubts I had were laid to rest, so back across the ocean.

To some [redacted] problems of which I had no first hand experience whatsoever, and analyzed by some 200 people, virtually all strangers to me. I wasn't, nonetheless, alarmed about the problems (I had, after all, read a good bit about them) except in the sense that I seriously doubted that I could make a high technological contribution in such a complex field. At this stage and eminence, such a contribution was, of course, unnecessary but, since the only way I know of earning respect is earning it I felt uneasy. More to the point, I knew that what I would have to do to earn my pay was to make judgments, often as not on insufficient evidence. How to do this with only theoretical knowledge and supported wholly by subordinates unknown to me promised to be a difficult task.

It should be emphasized that the name of the game, here, was solution and exploitation, not diagnosis which was where my most solid experience lay. It seemed to me that the world would survive, at least temporarily, if I didn't know or do what my subordinates knew or did. Then things would go rather better if I learned and did what they didn't.

I should attempt to develop a rather fine generalized picture of what this organization did, where it had been, where it was going, how its internal priorities were arrived at, how it fitted in its environment of support systems, competitors and consumers, how it should be governed, and to what end.

I felt that if I knew that, I would know something no one else did and could turn it to account to earn my pay. □

CRYPTOLOG

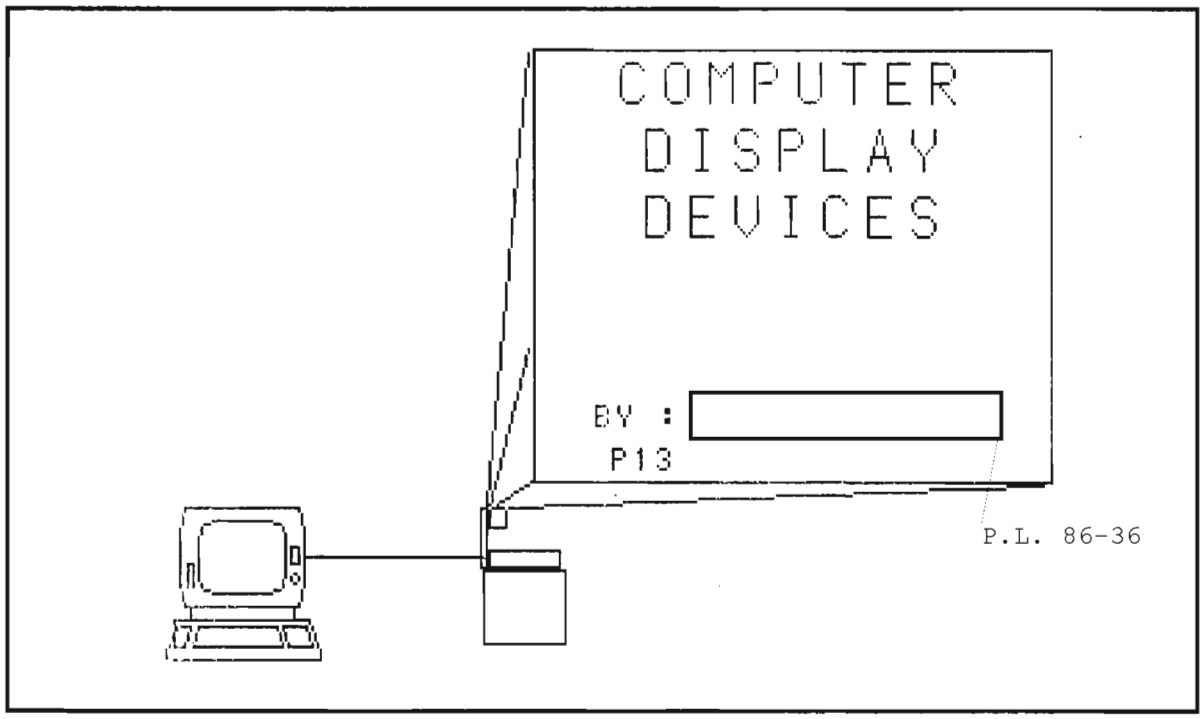
is a classified publication.

It may not be read in the cafeteria

or in other insecure areas.

EO 1.4.(d)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



If you have to brief a number of people about some new software, you need to use a data display device, for no more than two people can read what's on a PC monitor at the same time. The device is attached to the computer and projects a screen image onto the wall using an overhead projector.

P13 recently bought one device and obtained another on loan. We bought the Data Display by Computer Accessories Corporation at a cost of $1000.00. We borrowed the Magna Byte II by Telex Communications Inc., which costs $1500.00. Both displays come with software to capture screen images and to prepare slide shows using the captured images. Following are our observations of the two devices:

The Magna Byte II

- has the option of using instructions in English, French, German or Spanish;
- displays the screen images in color, not all the same colors as the screen but still impressive;
- offers a graphics mode with software to allow for the creation of piecharts, barcharts and text in a medium-resolution graphics mode;
- allows you to change slides in the slide presentation through a time interval sequence you specify or by using a wired hand-held remote control;
- requires a controller card which must be installed in a slot in your computer; this limits its portability.

The Data Display

- gives a good resolution black and white presentation;
- has an optional carrying case for portability.

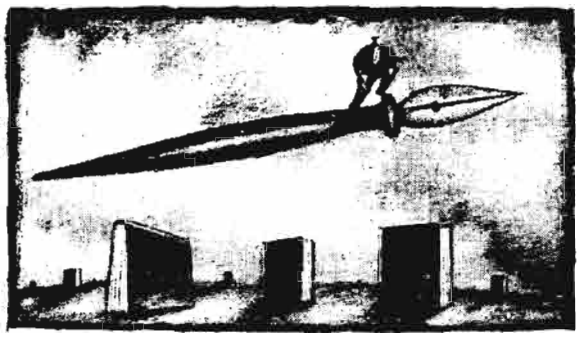
CONCLUSIONS

Although the Magna Byte II offers color display, a graphics package,and a wired remote control, it has a major disadvantage for us: it is not readily portable. The controller card which must be installed in a slot in the computer tethers the device to the computer and so limits its portability.

We chose the Data Display, which gives a good resolution black and white presentation and is highly portable. P13 created a nice portable presentation package consisting of this device, a Zenith lap-top computer, and a folding overhead projector.

For further information or a demonstration you may call anyone in P13 on 963-3045(s). At present we are in room 2C030, OPS-1. □

DOCID: 4019715



Reported by: David Harris, R51

M. M. Pozzo & T. E. Gray (1987) "An Approach to Containing Computer Viruses," *Computers and Security*, **6**, pp. 321-331.

A computer virus lures unsuspecting users into executing it in the course of carrying out an allegedly useful program, while in reality it performs additional functions intended to give unauthorized access to the system or to damage the operation of the system and its contents. For example, recently it was reported in the news that an American corporation fell victim to a Christmas virus. The virus produced a Christmas tree display on a terminal and asked the user to carry out a seemingly innocent action. If he did so, the side-effect was to distribute a similar Christmas tree display to all people to which the user had access. Rapidly, the Christmas virus spread throughout the corporate network, even across the Atlantic. Eventually the network crashed from the communications traffic jam, and the network had to be taken down while operations systematically removed the virus from each and every user's space.

Viruses can modify other programs, perhaps by making them adjoin a copy of the virus itself, thus spreading the virus throughout the computer. The virus, once it has infected a user's software, may be used to give the attacker access to all the user's other files. Further, any third user will become infected if he uses an infected user's software. This paper presents a mechanism for containing the spread of a computer virus by detecting at run-time whether or not an executable statement has been modified since its installation. The detection strategy uses encryption. The method avoids assuming that it is sufficient to prevent modification of executables by unauthorized users. The authors suggest using public key encryption.

Eliot Marshall (1988) "The Scourge of Computer Viruses," *Science Magazine.*, **240**, 8 April 1988, pp. 133-4.

This article appeared in the News and Comment section of *Science Magazine.* Marshall describes the problem, gives some history of computer viruses in the workplace, and talks about efforts to protect against the threat. In general, the article is negative about the role of NSA, concentrating on what it says are our efforts to downplay the problem. Marshall believes that we feel that it is best to give this subject as little publicity as possible so as not to stimulate hackers to develop viruses. He quotes Fred Cohen of the University of Cincinnati as saying "One of the NSA guys told me to my face, 'You're not going to do any research on viruses if we can help it...'." Clearly, Marshall does not agree with this approach. He believes current protections are largely inadequate, and much more research ought to be done. Cohen does concede however, that while the NSA does not announce its plans, "they seem more concerned now because they've got people researching it."

K. Hwang (1987) "Advanced Parallel Processing with Supercomputer Architectures," *Proceedings IEEE*, Oct. 1987, pp. 1348-1379.

This is a rather comprehensive survey of supercomputers and supercomputing. To quote the introductory blurb, it "... presents advanced parallel processing techniques and new hardware/software architectures ... (with) emphasis on vectorization, multitasking, multiprocessing, and distributed computing. Important issues addressed are architectural choices, parallel languages, compiling techniques, resource management, concurrency control, programming environment, parallel algorithms, and performance enhancement methods." It includes an assessment of the potentials of optical and neural technologies, and a survey of available supercomputing hardware.

All in all, anyone with a serious interest in the field would probably want to look over this article. □

~~FOR OFICIAL USE ONLY~~

DOCID: 4019715

(Advertisement)

JOLLY JOE's

INTERN CLEARANCE SALE

21 P1'ers MUST GO BY AUGUST TO MAKE ROOM FOR THE NEW '91 MODELS. ALL INTERNS HAVE HIGH TEST SCORES, HAVE TAKEN ALL REQUIRED TOURS & COME WITH P1's STAMP OF APPROVAL.

ONE BILLET or BEST OFFER

WE WILL NOT BE UNDERSOLD!!!!!!!

TEST DRIVE AN '88 INTERN TODAY

ALL SALES FINAL !

Courtesy of POLEMICS

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019715

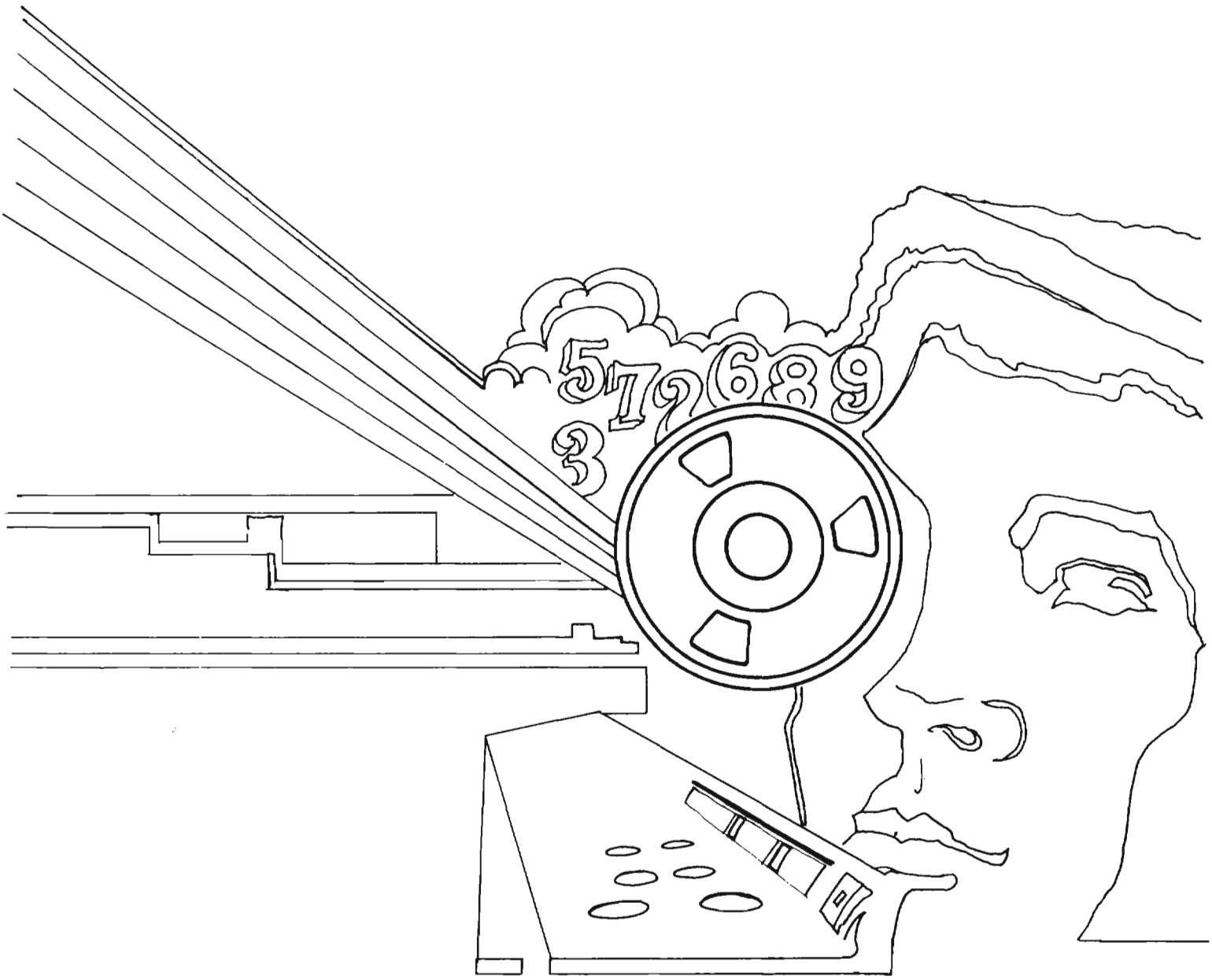
CRYPTO "LOG" PUZZLE

By [redacted] *T12* P.L. 86-36

"Log" is one of many English words with several different meanings. Also, its letters form parts of other words. The following clues define words or phrases that contain "log." How many can you guess?

1. Ridiculously simple -
2. Of or affecting the mind or its working - - - - - - - - - - - -
3. Immovable mass or blockage - - - - - - - - - - - - - - - - - -
4. Child's building set -
5. A box in a theater or opera house - - - - - - - - - - - - - - -
6. Mutual help, especially with political programs - - - - - - - -
7. Lacking vitality; sluggish - - - - - - - - - - - - - - - - - -
8. Detailed record of a voyage - - - - - - - - - - - - - - - - - -
9. Systematic list of library books - - - - - - - - - - - - - - -
10. Sound asleep -
11. Slept soundly -
12. Principal Indonesian language of the Phillipines - - - - - - -
13. Disagreeing, arguing, or quarreling - - - - - - - - - - - - -
14. Reserve or accumulation - - - - - - - - - - - - - - - - - - -
15. Did absolutely nothing -
16. Wood burned at Christmas - - - - - - - - - - - - - - - - - - -
17. Computer using physical quantities to represent numbers - -
18. Abraham Lincon's birthplace - - - - - - - - - - - - - - - - -

~~FOR OFFICIAL USE ONLY~~


5 7 2 6 8 9
3

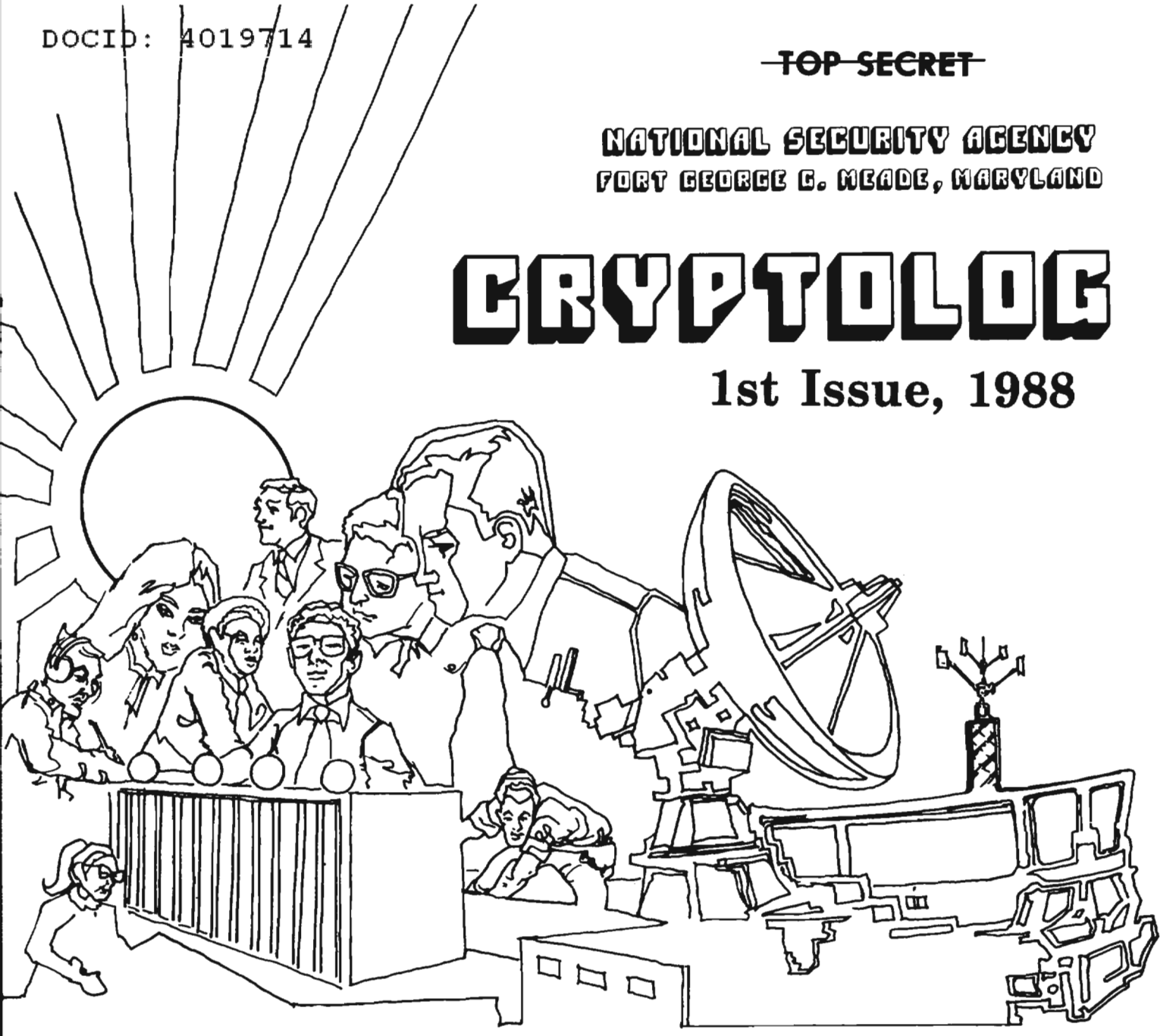
DOCID: 4019714

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

1st Issue, 1988



THE DIRECTOR'S MAJOR THRUSTS. . . . . [redacted] . . . 1
BULLETIN BOARD. . . . . [redacted] . . . 5, 15
AN OVERSEAS TOUR: A PERSONAL CHRONICLE. . . . . [redacted] . . . 6
STU-III, THE NEW TELEPHONE SYSTEM . . . . . [redacted] . . . 12
GOLDEN OLDIE. 13
AN OPEN LETTER TO ALL SENIOR TECHNICIANS. . . [redacted] . . . 14
FOR PC USERS. 16
LETTERS 17, 26
ABOUT CRYSCO. . . . . [redacted] . . . 17
REVIEWS: FOUR WORKS ON CRYPTOLOGY . . . . . [redacted] 18
THE STATISTICAL PRECISION OF MEDICAL SCREENING PROCEDURES
. . . . . [redacted] . . . 21
THE LINGALA CODE . . . . . [redacted] . . . 22
CRASHING THE SYSTEM . . . . . [redacted] . . . 22
LANGUAGE BRIEF: LINGALA . . . . . [redacted] 24
NSA-CROSTIC #66 . . . . . [redacted] . . . 28

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019714

CRYPTOLOG

P.L. 86-36

Published by P1, Techniques and Standards

VOL. XV, No. 1 ..... 1st Issue 1988

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Collection ..... (963-5877)
Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Cryptolinguistics ..... (963-4740)
Index ..... (963-5292)
Information Science ..... (963-3456)
Information Security ..... George F. Jelen (972-2122)
Intelligence Research ..... (963-3845)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (963-4958)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-4351)

Illustrators ..... (963-3057)
..... (963-6211)
..... (963-3738)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five)
(note: no 'o')

Always include your full name, organization, and secure phone; also building and room numbers.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, HQS 8A187
Please do not phone.

Contents of CRYPTOLOG should not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

TIME TO WRITE

It's time to write at NSA!

Writing for a competition may bring you fame and fortune!

Writing for a competition may bring about revolutionary changes!

The most prestigious writing competition is the Agency's Cryptologic Literature Award. It brings very large cash prizes in addition to prestige. This year's deadline is March 31 for papers written in 1987. The papers may be submitted by the authors or by anybody else to: The NCS Registrar, Executive Secretary, Cryptologic Review Board, ITB.

While it's too late to write for this year's awards, you're just in time to prepare for next year's. And meanwhile, you can try the other competitions.

Just about every one of NSA's professional societies sponsors some kind of competition for writing, and most are open to all Agency employees regardless of discipline. Most competitions award cash prizes for the best entries. (It's not a bad thing to win an honorable mention, even without cash.) Usually winning essays are published, and sometimes, non-winning entries are published as well.

There's still another benefit to writing for a competition: the chances are very good that your words will be read by people who are in a position to act on your ideas. Some authors find this prospect even more appealing than winning a prize.

So, analysts, take pen in hand or put fingers to keyboard, and write!

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019714

THE DIRECTOR'S MAJOR THRUSTS

P.L. 86-36

Q1

Editor's Note:

An article on Thrust #4 by Glenn Stahly in CRYPTOLOG, 2nd Issue 1987, spurred many requests for information on the overall concept of the thrusts and for specifics on the other five of what were then six thrusts.

We are pleased to bring you this article by the Agency's coordinator for the thrusts.

Shortly after becoming Director of NSA in the Spring 1985, General Odom examined the Agency's missions and activities from the standpoint of existing international alignments. He realized that the requirements levied on NSA/CSS would continue to grow and expand, thereby straining its capabilities, so he developed six thrusts as a framework within which NSA/CSS could respond positively and effectively to existing and anticipated future requirements. He viewed the thrusts as areas of emphasis or direction on which NSA/CSS must focus its corporate energies to ensure the continuation of the vitality and responsiveness of its future missions.

General Odom based his original six thrusts on three basic considerations:

1) the estimates contained in the Future SIGINT Capabilities Study on the changing technologies expected to be applied in the telecommunications structures and operations of our target countries;

2) long-range estimates of the threat to our national security; and,

3) an examination of our customers' ever increasing requirements for intelligence information.

In October 1985 the thrusts were promulgated. They provide general direction in the areas of planning, budgetary programming, policy and operations. Now, all NSA/CSS specific plans must be consistent with, and support, the thrusts. In addition, the Service Cryptologic Elements (SCEs) are encouraged to use the thrusts as guidelines for their planning, programming and operations initiatives.

A paper on the thrusts was distributed to the Agency's key component chiefs and also to the SCE Chiefs, the Chiefs of Intelligence of the Military Services, and to the Director, DIA, as background information and to allow them to understand the direction in which we are heading.

The thrusts should be viewed as a synergistic set of forward-looking areas of emphasis that serve to:

DOCID: 4019714

THE TEN THRUSTS

1) to modernize the SIGINT collection and processing systems to cope with the changing target communications technology;

2) to integrate tactical and national SIGINT capabilities to satisfy more effectively military requirements in peace, crisis and war;

3) to maintain and improve our capabilities to support diplomatic, economic, and other non-military requirements for SIGINT support;

4) to maintain a large US lead in cryptanalytic capabilities, both in computers and in personnel;

5) to design a framework for a survivable SIGINT system, under all conditions, including general war, which we can develop incrementally and through astute dual-use applications over the next decade;

6) to provide easily attainable, inexpensive, user-friendly information systems security features;

7) to speed up research for major breakthroughs in the technology of computer security; at the same time, to help industry manufacture more "trustworthy" computer products for defense and other government needs;

8) to establish a program to reduce significantly the HUMINT threat to information security systems;

9) to provide modern, secure, user-friendly key management systems;

10) to overcome, by the end of 1991, the problem of wholesale obsolescence of COMSEC equipments and to establish a program to avoid it thereafter.

- provide a means for the Agency's managers and analytic elements to share in shaping the Agency's future;
- bring together separate budgetary programs (e.g., the Consolidated Cryptologic Program and the Tactical Cryptologic Program), thus allowing for the cooperative development of a total SIGINT system that will furnish critical intelligence information to SIGINT customers in peacetime, crisis, and war;
- influence our own cryptologic programs and enable us to influence other Intelligence Community programs that contain SIGINT capabilities but are outside the control of the CCP; and,
- serve as a yardstick against which the efficiency of all Agency resources (SIGINT, COMSEC, COMPUSEC) can be gauged and efforts redirected, where necessary, for maximum payoff.

Thus, the goal is to develop a coherent aggregate of capabilities that is technically healthy, secure, responsive to central NSA coordination and tasking under appropriate circumstances, adequately equipped to deal with all target communications technology, and concomitantly, one that is survivable.

The original six are now ten – five SIGINT and five INFOSEC. The original Thrust #6 was a broad, generic statement about continuing the present revolution in improved COMSEC and repeating that revolution in COMPUSEC. Subsequent study led to the conclusion that this thrust did not adequately address INFOSEC-related needs and concepts. The Director and the DDI thereupon developed five INFOSEC-related thrusts as a replacement for original Thrust #6. These new INFOSEC thrusts were promulgated on 4 November 1986.

In the past year, the Director and the chiefs of key components reviewed each thrust. Generally the status review takes this form:

> A knowledgeable person presents an overview of the thrust topic, followed by a round-table discussion led by the Director. The subject then is examined from the perspectives of planning, policy, operations, funding, resources, etc. When the discussion uncovers a shortfall or deficiency or poses a question that cannot be resolved at the table, a task is assigned to a single key component to lead a study of the problem

DOCID: 4019714

EXPLANATORY NOTE

on Thrust #10, block or wholesale obsolescence.

Updating our current COMSEC equipments piecemeal is somewhat like trying to update the kitchen of a single apartment in a 70-year-old building. You can't just replace the old frig with a refrigerator-freezer, or the old stove with a microwave oven-cum-stove; you can't merely install a dishwasher, garbage disposal, and a washer-dryer. You'll probably have to rewire the entire building and replace all the plumbing. And, very likely, you'll have to make sure that the connections to the water mains and sewers are up to the task.

So, like the old frig and stove, our COMSEC equipments are old technologically and cryptologically. Replacing tens of thousands of devices all at once is a daunting task as well as an extremely expensive one. We want to plan our modernization so that the same situation of wholesale obsolescence does not recur ten or twenty years hence.

and report the results to the Director. Other contributors are also designated, a suspense date is set, and the item is then inserted into the Thrust Tracking System. (Each action item specifies a "deliverable" to be presented to the Director, e.g., a briefing, paper, study, or funding item.)

The Director continually has reaffirmed his commitment to the thrusts within the Intelligence Community and outside it as well. For example, the first time he publically referred to the thrusts was during his budget testimony to Congress, linking budget items to a specific thrust. He refers to them during his interactions with the JCS, with the cryptologic and intelligence elements of the Military Services, with the Intelligence Community Staff, and with the US Commands. Moreover, whenever an opportunity arises, the Director seizes it to further the thrust concept and its use, not only within the NSA/CSS, but throughout the Intelligence Community and Defense establishment. For example, General Odom presented the five INFOSEC-related thrusts at the December 1987 meeting of the DoD-sponsored Military Communications Electronics Board which he hosted.

The NSA/CSS Field Representatives have been made fully aware of these thrusts. Moreover, the Director personally encouraged them to carry the message to the CINCs and local military commanders in order to gain their support for NSA/CSS programs and initiatives. Similarly, the SCEs are to use them for their own planning, programming and operations.

At NSA/CSS, the Director and the senior managers continue to review the thrusts, adding action items as they arise.

To involve the analytic elements, the Director sent a memorandum on 20 April 1987 to the Agency's workforce reaffirming his commitment to the thrusts and encouraging echelons two to three levels below to become familiar with them, to understand them, and to use them in their everyday decision-making. During his address to NSA seniors in June, the Director underscored their applicability to the Agency's future, stating that, even though the ten thrusts provide broad overall direction, they contain enough specifics to serve as a guide. Furthermore, he pointed out, there is sufficient latitude and freedom within them for the NSA/CSS workforce to excel and innovate. He emphasized that managers can use the thrusts to understand how he would respond in his interactions with other US government agencies and with Congress. The thrusts should be viewed not as a rigid set of directions but as areas in which managers and analysts alike are encouraged to participate and in which to take creative and innovative action.

The thrusts will continue to represent areas of interest and concern for the future efforts of the NSA/CSS. Previously, NSA Directive 25-2 "NSA Goals and Objectives" represented the Agency's future aims, but this directive was replaced by the thrusts. The usefulness of having areas of interest that can be understood by managers, analysts, customers, and laymen alike will undoubtedly pay dividends for NSA.

ADMINISTRATION

In order to keep up with the activity generated by the thrusts, there must be a focal point for

~~CONFIDENTIAL~~

UNITED STATES GOVERNMENT

memorandum

DATE: 20 April 1987

REPLY TO ATTN OF: DIR

SUBJECT: Director's Major Thrusts (U) - INFORMATION MEMORANDUM

TO: DISTRIBUTION III

1. My basic planning guidance, the six thrusts, have served as our overall direction for more than a year. In the meantime, it became clear that the sixth thrust needed further elaboration for the INFOSEC mission.

2. I believe that most of you have come to realize the coordinating effect these thrusts can have on all our programs in NSA. There is considerable linkage from one to another, and success in one either adds or reinforces success in another. I intend them as a general idea of where we are going. To the extent you understand them, you can anticipate and take initiatives on your own which are compatible and helpful in their larger context. In other words, they are meant not to constrain or restrict innovation and initiatives but rather to guide your innovations and initiatives into constructive directions for the USSS as a whole. They allow you to anticipate how I will judge the worth and utility of proposals and actions. They also allow you to fit your initiatives with those of other managers in other components and organizations without major confusion and cross purpose about final objectives. Finally, they help me keep track of where we are as a whole and what we may be neglecting or overemphasizing.

3. I intend to repeat the thrust reviews again this summer. These will involve a look at what we have accomplished since the last review and also another look at things we may be missing, actions we may have neglected, and things we might do to speed up and improve our programs under each thrust.

4. To make the most of these reviews, managers at lower levels need to think through the thrusts and ask what is lacking in our program efforts as viewed from their level. I want to get as much insight from two and three levels below as possible. While it may not be possible to act on all points raised from below, it is important to consider those points. They enriched my understanding last year in the review process, and I want even more this year. They also give me a sense of how well you understand my general guidance.

~~Classified By NSA/CSSM 123-2~~
~~Declassify On: Originating Agency's Determination Required~~

OPTIONAL FORM NO. 10
(REV. 1-80)
GSA FPMR (41 CFR) 101-11.6
5010-114

☆ GPO : 1985 O - 461-275 (428)

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

5. Those of you in the support areas may not immediately see the direct relevance of the thrusts for you. In many cases it is indirect, but it is there. As we succeed in thrust one, two, three, and four for SIGINT, we create strains and new demands on training, communications, logistics, and facilities. To understand better these impacts on the support areas, I recently held a Corporate Management Review. Support, we determined, needs more attention, more resources, and stronger leadership in some cases. I do not view this emphasis on support as a change to the basic thrusts. I see it as essential for continued success in those thrusts. As we progress and you see that my program decisions emphasize some support areas, do not misread them as lessening emphasis on the thrusts--quite the contrary.

6. I share these thoughts with you to alert you to upcoming reviews and to give you time to think through once again the rationale of my general guidance so that you may profit from it and help me carry it through. As we progress, we may see reasons to modify the guidance. I do not see it as inexorable, and I am ready to make changes when the reasons are compelling. In the meantime, its firmness should be a help at all levels in making good decisions toward our shared goals.

WILLIAM E. ODOM
Lieutenant General, USA
Director, NSA/Chief, CSS

handling the myriad actions that emerge from the status reviews. At the outset, the NSA Chief of Staff administered the overall Thrust System in the Director's name. Recently, however, the DDPP assumed this responsibility. Q1 does the day-to-day work of handling the status reviews, preparing agendas, drafting summations of the meetings, initiating and maintaining the Thrust Tracking System, monitoring progress of the individual action items, negotiating and arbitrating between and among the various players, and submitting a monthly report to the Director on the status and health of the thrusts, and conducting follow-up actions. □

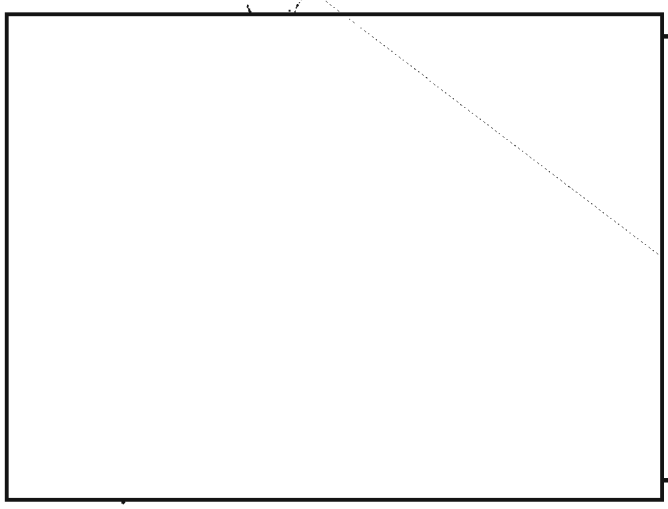
BULLETIN BOARD

WANTED: EXPERIENCED USERS OF UNICOS/UNIX

(U) Are you an experienced user of UNICOS/UNIX and willing to help others learn it? If so, please get in touch with [redacted] CRYSCOM Chairman, G451, and let him know which of the following you have experience in: [redacted] UNIX operating systems, programming languages, machine familiarity.

P.L. 86-36 P.L. 86-36

DOCID: 4019714 EO 1.4.(c) P.L. 86-36



An Overseas Tour

P.L. 86-36

A PERSONAL CHRONICLE

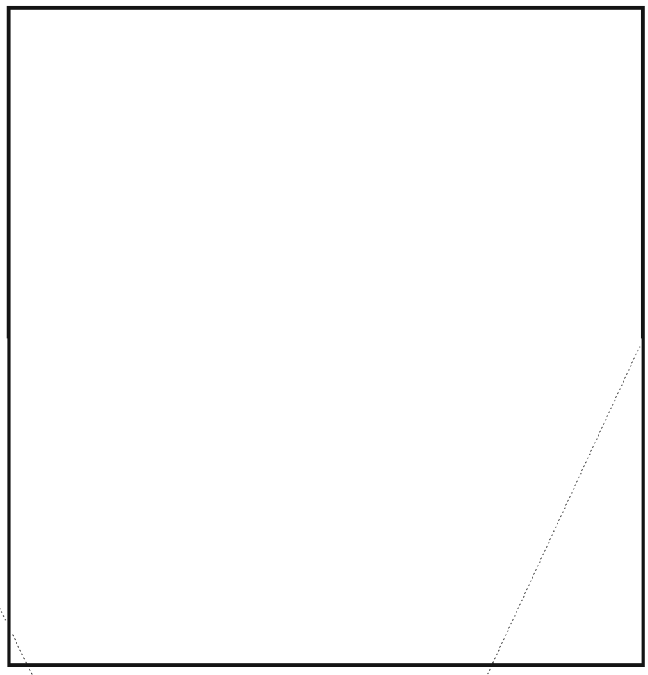
[redacted] *N2*

(U) I am writing this paper not only as a personal chronicle, but also as a means perhaps of convincing others to apply for an overseas tour. I am writing with mixed emotions because if I do a good job in convincing more people to apply, I may not be able to go again myself. I am not sure whether the circumstances that allowed me to finally get an overseas tour were unusual or not, but I have not heard of anyone else having the same experiences that I had.

GETTING THERE

~~(C)~~ With that in mind, I will get on with chronicling the events which finally culminated in an overseas tour. I had worked in B Group as a cryptanalyst for quite a few years and although overseas positions were advertised, there never seemed to be any for cryptanalysts. In 1980, a field announcement was circulated with a position for a cryptanalyst [redacted] It looked like an opportune time to get some experience in another aspect of the Agency. I filled out my application and sent it to the required offices. I also made appointments to talk to various people who would be making the selections and also to people who had been [redacted] either TDY or PCS.

(U) I decided that this was the job for me. The selection committee narrowed the candidates down to two people, me and the person who eventually got the job. All was not lost, though. Because I had expressed a lot of interest, the Chief of B5 asked me to consider transferring to B5 as the replacement for the selectee in order to have an inside track when the overseas position again became available. As it turned out, this was probably the ideal solution for B5 and for me.



~~(C)~~ This course is long and arduous but worth every minute. There were only three people in the class, all destined to be part of the [redacted] This included the future [redacted] the future computer and systems analyst, and myself. As in most language classes, morning dialogs and conversations were the norm. I can really appreciate the saying "you can run, but you can't hide". Pre-class preparation was a must and participation was required. Fortunately, our instructor, a native speaker, had the patience of Job and a sense of humor. I really think that the class was as hard on her as it was on the students.

EO 1.4.(c)
P.L. 86-36

(U) This part of the pre-departure preparation is probably the most difficult and brings the most complaints from people going overseas. The reasons for the complaints are many – not only do you have to go to class everyday and all day, you also have many administrative things to take care of at the same time, like: getting passport pictures, being inoculated, being briefed on security by various elements in M and N, finding out about financial and medical benefits or lack thereof, changing from one payroll system to another, learning your cover stories, trying to find out when you will be leaving, what your flight schedule will be etc., and the list goes on and on.

(U) As you get on with this you can only wonder whether it's worth it. Nothing seems to be organized, and there doesn't seem to be enough time to get everything done before departure. Patience is definitely what you need. After going through the process, I can empathize with the people in personnel, security and travel. They really have their tasks cut out for them. It is a thankless job for which they receive little credit when they should. So be patient – things always seem to work out eventually.

~~(S-CCO)~~ Finally, the big day came. All the paperwork was completed, I had my orders, passport, and tickets; my housing and hold baggage had been shipped and I was ready to go. Sometime before I left, the chief of the site sent a welcome card and an orientation package so that culture shock would not be too great. I was also very fortunate in that I had had an opportunity to meet her several months prior to my departure made it possible to meet some counterparts during their visit to NSA. All in all, the principals kept us informed and gave us the opportunity to meet everyone and anyone who might be able to give us insight to our assignment.

~~(C)~~ Be prepared for culture shock when you go overseas. No matter what anyone has told you about the country, you never really know what it is like until you get there. When I finally arrived the first thing I noticed was the heat. Hot and really bright sunlight. As in most places, people make lasting impressions and can either make a job memorable and enjoyable or absolutely unbearable. Well, fortunately in my case and I think for almost everyone else who has been in it started off on the right foot. The person whom I was replacing met me at the airport Welcome, and brought flowers. He took me to my hotel, checked me in and then took me out to our working spaces, which were located outside of metropolitan

~~(S-CCO)~~ I was introduced to all the team members and to personnel I would be working closely with for the next two years. Fortunately, there was almost a two week overlap before my predecessor's return, so he saw to it that I got to meet and associate with at the very beginning. I was not required to jump into a pond and sink or swim. Everybody at our station was helpful. The administrative officer made sure I liked where I was staying (initially most people stay in a hotel for several days before their apartments are ready), inquired if there was anything I needed, sent a message to my daughter to let her know that I had arrived safely, and did lots of little things that I personally probably wouldn't have thought of.

~~S-CCO)~~ The chief met me again and gave me a briefing on everything that went on and stressed that if there was anything she could do to help or answer any questions, anything at all, just let her know. I got the feeling right away, that this was like a family – everyone tried to help everyone else feel at home. The Ambassador also played a role in making new personnel welcome and comfortable by inviting new people to attend a country team meeting where he introduced them to his staff. Few analysts at the Agency have the opportunity to meet people at this level, but I did in this case. The Ambassador was very appreciative of the benefit and information derived through SIGINT and the assistance that our office provided him.

(U) All of this in the first two weeks. I had trouble believing it, but it was all happening. During this time I had settled in for an almost three-month stay in a hotel. Some people would think that this would be a real inconvenience, but as I was there by myself, and as the hotel personnel was very cordial and congenial, I found this an excellent opportunity to meet the people in a non-work environment. The

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36

DOCID: 4019714
EO 1.4.(c)
P.L. 86-36

hotel management was quite friendly and I now number some of them as good friends. They found that if they treated the guests as a family, the stay was much more enjoyable as well as being just good business sense. This was also a good opportunity for me to start practicing [redacted]

WORKING THERE

[redacted]

~~(S-CCO)~~ This was evident soon after they were given a C/A course using the IBM pc. The Assistant Director of Training sent two very competent people to teach it and I acted as translator/interpreter and assistant instructor. As soon as the course was completed, I was getting questions on how to work specific problems; these were from the cryptanalysts and even the traffic analysts had found useful applications for the course.

[redacted]

HOW TO GET OVERSEAS

1. Keep track of the overseas jobs in the announcements as they come out.
2. Find out where you want to go.
3. Talk to people who have been there.
4. Talk to the selection official.
5. If you really want to go, apply and make yourself known to the people who can help you get there.

Unclassified

[redacted]

EO 1.4.(c)
P.L. 86-36

ADVANTAGES OF A FIELD ASSIGNMENT

1. Money (differential pay)
2. Travel
3 Experience
4. Career enhancement
5. Promotions
6. Meeting great people

Unclassified

~~(S-CCO)~~ As an advisor, I found that [redacted] respected the knowledge and experience I had and would listen to what I would tell them. I realized right away, though, that if something needed to be changed or improved or suggested, it was certainly better to do it in a manner in keeping with their culture. I could just not walk into an office and say such-and-such had to be changed because it was wrong to do it that way. Even though NSA furnishes much of the things they use, we are still their guests. I don't think you would call it a con job, but common sense.

~~(S-CCO)~~ [redacted] Well, remember the C/A course I mentioned before. I suggested that the C/A people who now knew something about using the PCs, type out their new systems on a disk in a format I had already put on the disk. This saved me and them a lot of time. They could make corrections, enter the system into their data base, and give the system to me in a short period of time. In turn, I could transfer their input onto a disk in message format, enter the correct date and message number, and give the disk to the our comm center for transmission to NSA.

[redacted]

~~(FOUO)~~ Going TDY was also an excellent opportunity to see other parts [redacted] Usually after the workday was finished, the site personnel would want to show you "their part" of the country. They would take to you to famous temples, important landmarks and tell you where to get the best food at the cheapest price and what the specialty of the area was. If you like sea food or strange exotic dishes, this is the time to try it. I had one soup that had animal organs in it that I did not recognize, and I was a biology major in college. I ate it anyhow and it was quite good.

~~(C)~~ I was lucky to have worked with a really good bunch of people, from the chief of the field site [redacted] It was more like a family working together to make things happy. If anyone had a problem, any problem, someone would help. Everyone covered the job responsibilities of team members if they were going to be TDY, on annual leave, etc. You always knew that any information to or from NSA would get to the right office. All of the different teams helped each other. When a shipment of equipment arrived and it had to be unloaded, everyone turned out to help.

EO 1.4.(c)
P.L. 86-36

[redacted]

P.L. 86-36

LIVING THERE

[redacted]

POSSIBLE DISADVANTAGES

- Possible loss of visibility (in your old office)
- Time difference for solving problems
- Looking for a place to work on return

Unclassified

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

[redacted]

(U) Living is fairly inexpensive and you can get bargains of almost any kind. Those who are interested in antiques can find an abundance [redacted] If you see an "old thing" you really like but the price is more than you want to pay, you can try to bargain for a reduction (I would recommend this avenue first) or you can probably find someone who can make it for a fraction of the cost. Clothes are another item that are good bargains. Tailor-made or ready-made, natural materials or man-made, they can all be found here.

(U) I really appreciated one of the benefits of an overseas tour and that is the R/R. I picked [redacted] It is really nice to have someone else pay for a plane ticket.

(U) As for the [redacted] people, I cannot say enough good things about them. They are friendly and truly are a smiling people. Not a lot of things appear to bother them and almost all are willing to help. They really make you feel at home.

EO 1.4.(c)
P.L. 86-36

RETURNING TO HQS

~~(C)~~ After I was in [redacted] for six months, I was asked whether or not I wanted to extend for additional 1 or 2 years. After discussing this with the chief of the field site, I decided not to extend for professional reasons. Also, after six months, I really did not know whether to stay or go. More about this later. About six months or so before I was ready to return, I found out that I had a job offer from a non-DDO organization, thanks again to a great boss who on her own had looked for a good job that would further my career. Actually as it turned out later, I had a pick of two positions.

(U) I also knew who my replacement would be so we had the opportunity to correspond with each other. During this time I tried to fill him in on what to expect, what to bring, who to see and anything else that I thought might help him and his family enjoy their tour. Unfortunately, we had no overlap to discuss problems and allow me to introduce him around to his counterparts.

~~(S-CCO)~~ After all the out-processing is done – you have to clear with Embassy housing, bank, commissary, and a lot of other places – you get your orders and plane tickets. I was seen off at the airport by my colleagues, [redacted]

(U) On return to CONUS, I was given 14 days of home leave and enough admin leave to more than cover the time needed to readjust and take care of personal and professional business. I had to check through different elements of M and N for personnel, security and finance. Some of this is a hassle, but necessary. I got a physical from the medical center. I also made it a point to stop in my old office to see how my replacement was doing and give them a debrief of what was going on when I left.

(U) There are some things I would like to see changed, from both a professional and personal point of view. They include:

a. the selection process: it takes too long

b. out-going processing: it is too confusing and time-consuming

c. the time (six months after arrival) when you have to decide whether to extend your tour: it is unrealistic. You really can't make a rational decision in six months. Just finding your way home at night might still be a problem.

d. scheduled overlap of for replacements – this should be a requirement.

e. upon return to NSAW, a two-week period should be spent in the office associated with the field site, not as only as a courtesy, but principally to inform them of how things were going when you left. It will also help your replacement if he or she has a problem.

f. return processing, especially for payroll: there should be an electronic way to transfer personnel from one payroll system to another without have to redo all the paperwork.

(U) All in all, I would say if you are looking for adventure, career enhancement, a lot of personal satisfaction, and a chance to meet new people, take a chance. Apply for an overseas tour, but not the one I want, thank you! □

DOCID: 4019714

STU III: The New Telephone System

V

~~This article is classified CONFIDENTIAL in its entirety~~

Three years ago NSA set out build a low-cost secure phone. We hoped to put practical secure telephones into the hands of hundreds of thousands of personnel handling classified and sensitive information. (See "NSA's Initiative on Secure Voice" CRYPTOLOG, Jun-Aug, 1985.) Today, as contractors are shipping out the first of the production STU-IIIs – Secure Telephone Unit III, pronounced "stew three" – it seems that our goal will be reached. In the process of achieving this goal, we have also created a device with the potential to change completely the nature of our entire telephone system. What this eventually will mean for us at NSA is replacing the black, grey, and green phones with a single handset.

In the coming year we will deliver approximately 50,000 STU-III's. Our options/add-ons to the present contracts will bring the total up to 80,000 by mid-1989. In addition, each of the three major services has identified a requirement for approximately 300,000 STU-IIIs each, and they have started programming action to fund these buys. All of these STU-IIIs will interoperate with one another. This secure network will be larger, by more than several orders of magnitude, than any secure network ever created. And it may grow even more if the volume of secure communications generated by a million interoperable secure phones creates a demand for more. To understand how all this may effect us, we need to know how our present phone system works and how the STU-III differs from it.

Currently most secure phone users communicate within and between secure areas. We encrypt calls only when communicating with a distant location comparable equipment. Usually some telecommunications organization takes care of encrypting, multiplexing and switching the calls and operating the secure trunk communications lines. The average user is not involved in this process at all. The present system is "user-friendly." You use it just like a "regular" phone. This system has some drawbacks, however:

- For the most part, you can call only locations with comparable systems.
- The system is "system high" so you can talk on it only to people who are cleared at least as high as you are;
- It is cost effective only in relatively large installations.

Unlike the present system where cryptography is separated from the phone instruments, the STU-III contains its cryptography in the handset. Though secure phones containing their own encryption devices have been around for years, the STU-III is different in cost, interoperability, and the keying scheme. The first production run of STU-IIIs has an average unit cost of $3828. Although this price would probably keep the STU-III out of the average home, it is almost five times less expensive than its predecessor the STU-II (KY-71), which sold for $18,136.

As the vendors make additional production runs of the STU-III, economies of scale will drive the unit cost down even more. Devices acquired from the options to the present contracts will cost only $2655. It is difficult to predict the final unit cost, but the trend is clearly

P.L. 86-36

downward. Given advances in manufacturing and large productions runs, the unit cost of the STU-III may well drop to less than $1000 per phone.

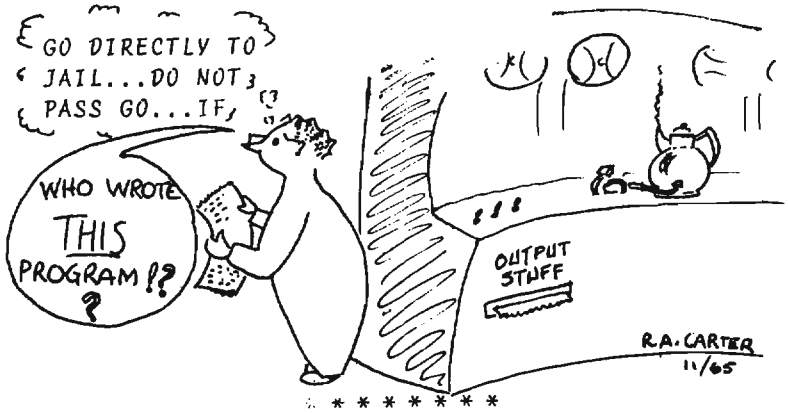
The STU-III enjoys a degree of interoperability that is truly revolutionary. It can be used anywhere there is a standard analog phone line simply by unplugging the present handset and plugging in the STU-III. While the earlier generation STU-II also enjoys the flexibility of using standard commercial phone lines, it does not have the STU-III's multilevel security capability. The STU-III can be used for all calls from unclassified to Top Secret Codeword. The secret of the STU-III's multilevel security is its keying scheme.

Unlike earlier generations of secure phones, the STU-III does not depend on an external source of keying material. The two phones in contact generate their own key with each call. They automatically and securely authenticate calls at all classification levels. Thus someone with access to a Secret level STU-III can call someone with a Top Secret level STU-III and talk securely at the Secret level. A display panel on each phone displays the highest common classification level *for that particular call.* A vast community that has not been able to contact us before will now be able to call us securely.

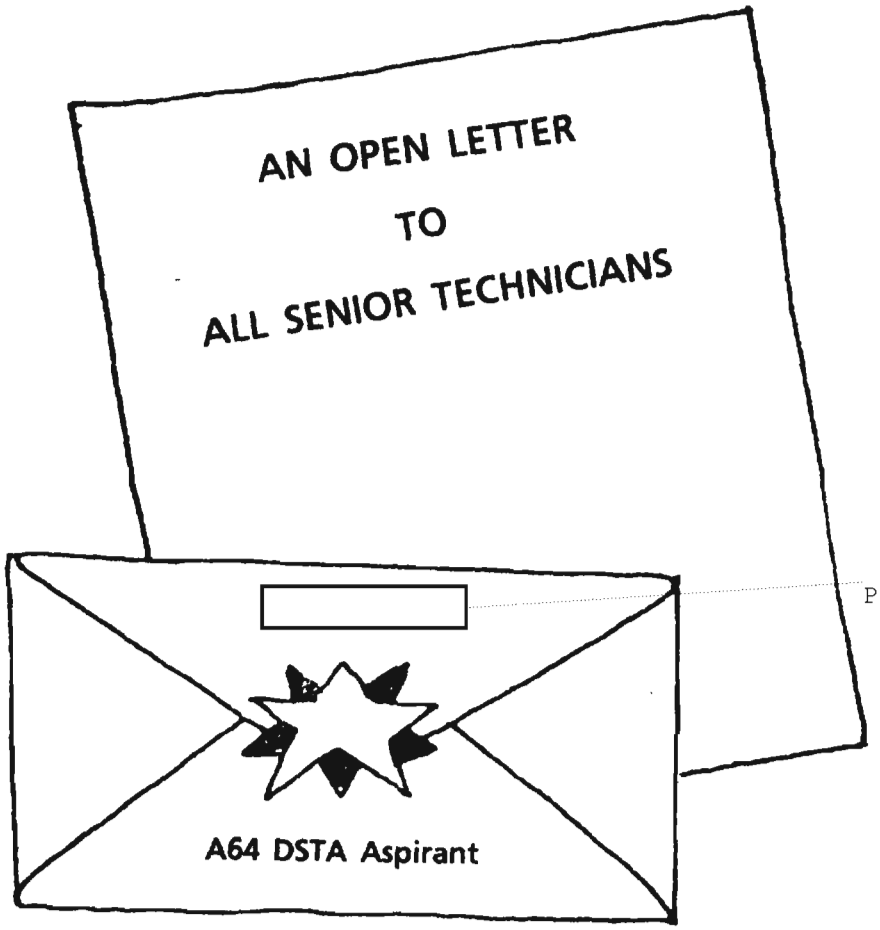
For the next decade we will be in a transition from our current secure phone system to a new system based on the STU-III. Meanwhile, operating both systems in parallel will demand an efficient interface between the new and the old secure phone systems. We have a large investment in equipment, expertise and emotion in the current system. Although sunk and hidden costs, such as segregated secure and non-secure cable plants and wideband circuit leases between installations, make a comparison difficult, placing a STU-III on every desk is not yet clearly cost-competitive at existing large fixed plant installations such as NSA Headquarters, CIA, and the Pentagon. Eventually, as the unit price of the new secure phones goes down, we can replace today's large fixed plant phone systems with a single instrument and a much simpler system to handle all of the functions of today's grey, green and black phones. □

GOLDEN OLDIE

Reprinted from:
bits & bytes
C4 Machine Processing Infomation Bulletin,
Vol I, No. 6, October 1965



DOCID: 4019714



Editor's Note:

A6's (voice language) technical track provides for post-professionalization certification in quality control (QC). The Branch Senior Transcriber/Analyst is expected to provide training and technical leadership on all branch projects and to provide technical advice to branch management. The Division Senior Transcriber/Analyst (DSTA) is to do the same on all or most division projects. At Office level the Senior Linguist should be capable of doing the same for selected projects in all divisions.

This article originally appeared in the Fall 1987 issue of Vox Topics. *It is reprinted here with the kind permission of the Editor.*

During a recent meeting of the A64 Technical Track Advisory Group the discussion centered on the tech track in general and specifically, on some of the perceived problems within the tech track. Two of the problem areas which surfaced during this discussion were:

(a) that some individuals were not staying current with the people and projects in the branches where they toured for certification in quality control, and

(b) that after certification many individuals were not paying back to the branches the learning time spent there as aspirants.

I would like to spend a little time discussing these two problems.

One of the areas that senior technicians are rated on when it comes time for performance appraisals has to do with technical leadership. This is a broad area that includes at least the willingness to perform on those projects where we have been QC-certified, as well as the requirement to take part in promotion boards, Career Development Review Boards, Quarterly Management Reviews, Branch Management Teams, Division Management Teams, etc. I don't feel that we can be considered to be properly performing in a technical leadership role unless we are willing to function in these areas.

~~FOR OFFICIAL USE ONLY~~

In order to be able to provide adequate input to the groups mentioned above, it is necessary to know the work of as many people as possible. I believe that the only way to gain that knowledge is to spend some time each year in each of those areas where we are QC-certified. When I finally achieve certification as a DSTA, I will be QC certified in A641, A643, and A644. Since I enjoy chasing airplanes around the sky, I will probably make A643 my home. I do, however, intend to spend one month each year in each of the other branches in order to stay current, not only on the projects in those branches, but also to get to know the workforce so that I can better represent them. I would like to suggest that other titled senior technicians consider doing the same.

The process of becoming QC-certified on the projects necessary for becoming a titled senior technician is looked upon by some of the aspirants as nothing more that a ticket-punching exercise. Spend as little time as possible on a project, get certified, and immediately move on to something else seems to be the way many aspirants view the program. I believe that this is very short-sighted as well as selfish. The managers of each project we work on spend a good deal of time training us and getting us to the point where we can be considered to be QC-certified. It seems to me that the least we can do is to pay back a little of that time after we achieve that certification. The amount of time to be paid back should be negotiated between the aspirant and branch or project manager. I personally think that a pay-back of 20-25% is a good figure to aim for and, as a DSTA aspirant, this is what I am suggesting to the management of those branches where I receive QC certification.

Again, I suggest that other titled senior technical aspirants give this serious consideration.

The technical track provides those in the workforce who do not feel comfortable as managers and who are better technicians than managers with an avenue in which they can channel their efforts in a meaningful way. It is up to all of us who have chosen the tech track as our career path to make it the best it can be. To this end I offer these comments. □

BULLETIN BOARD

NEW ISO STANDARD FOR CYRILLIC

(U) The International Standards Organization has just published ISO 9, "Transliteration of Slavic Cyrillic Characters into Latin Characters." This is intended for "international communications." The new standard leaves every country free to adopt a *national* standard for its own internal use.

(U) ISO 9 provides Latin-alphabet equivalents for 52 characters, adequate for transliteration of Bulgarian, Byelorussian, Macedonian, Serbo-Croatian, and Ukranian.

~~(C)~~ At NSA, however, the authority for SIGINT purposes is USSID 406, "Standard Transliteration of Foreign Writing Systems." The individual annexes for specific languages treat special problems unique to that particular writing system. Address your questions about USSID 406 to [redacted] P044, 963-5577.

P.L. 86-36

ATTENTION: POLEMICS

(U) CRYPTOLOG seeks permission to reprint two items from POLEMICS, a cartoon and a mini-article. Would the appropriate person please send a note to Norm saying yes or no?

BACK FROM THE FIELD?

(U) Yes, you can catch up on issues of CRYPTOLOG published while you were away! Available on a loan basis is a volume titled *While You Were Away* ... which contains issues published in the last three years or so. Address your inquiries to the Editor, P1, HQS. Please do not call.

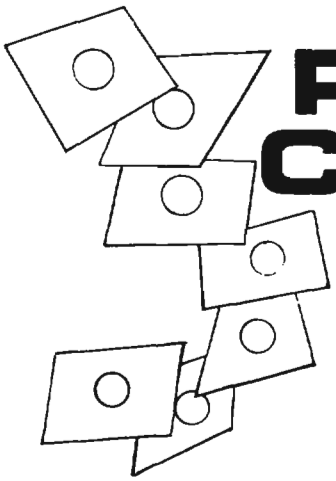
ATTN: CRYPPIES WHO PROGRAM IN C

(U) E53 is looking for unclassified examples of C-language code that perform unclassified CA techniques, and also some sample I/O (e.g., bit manipulation). The examples will be put in a booklet that will be given to students in C-language courses. Send your submissions to P1, HQS, for classification review. POC is [redacted] E53, ITB, 968-8007.

P.L. 86-36

DOCID: 4019714

FOR PC USERS



PERSONAL COMPUTER SECURITY

FLOPPY DISKS

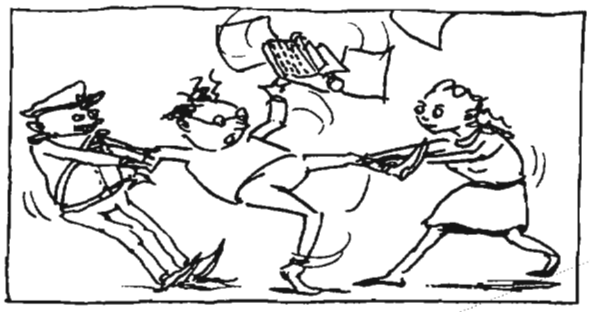
Care and Keeping

- KEEP DISKS IN THEIR PROTECTIVE JACKETS WHEN NOT IN THE DRIVE UNIT.
- KEEP DISKS STORED UPRIGHT IN THEIR BOXES.
- KEEP DISKS CLEAR OF ERASER CRUMBS, DUST, AND SMOKE PARTICLES.
- USE A FELT TIP PEN WHEN WRITING ON THE DISK LABEL. PENCIL OR BALL POINT PRESSURE CAN DESTROY FLOPPY PRECISION.
- *MAKE-UP COPIES. THEN STORE THEM IN A SEPARATE FACILITY FROM THE ORIGINALS.*
- DON'T TOUCH THE DISK SURFACE. IT'S EASILY CONTAMINATED, SO SOMETHING AS MINOR AS A FINGERPRINT CAN CAUSE ERROR. ON A DRY DAY, YOUR FINGER COULD HAVE ENOUGH ELECTROSTATIC CHARGE TO DAMAGE THE DATA PERMANENTLY.
- DON'T USE ALCOHOL, THINNERS, OR FREON TO CLEAN THE DISK. CHEMICAL FUMES CAN ENDANGER THE MAGNETIC COATING, SO DON'T EXPOSE IT TO SOLVENTS LIKE NAIL POLISH OR DUPLICATING MACHINE FLUIDS.
- DON'T EXPOSE THE DISK TO MAGNETIC OR MAGNETIZED OBJECTS. DATA CAN BE DESTROYED, SCRAMBLED, OR WIPED OUT COMPLETELY. A COLOR TV, CRT, ELECTRIC MOTOR, OR OTHER DEVICES CAN DESTROY DATA INTEGRITY. SCREWDRIVERS, PAPER CLIPS, CAR KEYS, OR ANY METAL OBJECT MAY ALSO BE MAGNETIZED.
- DON'T PUT A TELEPHONE ON TOP OF A DISK, THE DISK DRIVE, OR A BOX OF DISKS. ONE RING CAN CAUSE DAMAGE.
- DON'T EXPOSE DISK TO HOME POWER SUPPLY UNITS.
- DON'T BEND, FOLD, OR USE RUBBER BANDS OR PAPER CLIPS IN THE DISK. ANY WARPING CAN LEAD TO MISTRACKING.
- DON'T REST HEAVY OBJECTS ON THE DISK. IT CAN CAUSE A CRIMP THAT WOULD LEAD TO MISTRACKING
- PROTECT YOUR FLOPPY AT LEAST AS WELL AS YOU WOULD THE DATA THAT'S ON IT.

NATIONAL COMPUTER SECURITY CENTER

DOCID: 4019714

LETTER TO THE EDITOR



P.L. 86-36

To the Editor:

(U) [redacted] letter [CRYPTOLOG, 4th Issue 1987] praising interns matches our experience. We value their energy and ability, and could not get along without their help. But experience counts, too.

[redacted]

(U) Succesful analysis depends not only on intellectual ability, but on some knowledge of what came before. The former without the latter is not enough. Particularly in this Agency we must place high value on experience, and create an environment in which experienced analysts (who may well have been 'bright young' interns in *their* day) can prosper and whose contributions are recognized. Only by remaining in the technical fields might they, one day, perform some the magic related above.

(U) The example I gave is simplistic, but the principle has broad application. Let's not denigrade the need for experienced analysts and look only to the 'bright young' interns.

[redacted]

P.L. 86-36

About

[redacted] *A538/P13*

~~(FOUO)~~ The first annual Cryptanalytic Software Conference (CRYSCO) was held in April 1984. The Cryptanalytic Software Committee (CRYSCOM) organizes and conducts this conference where super-computer users can share ideas and information and discuss plans and problems. The purpose of CRYSCO is to provide organizations using supercomputers with a better understanding of the plans and progress of cryptanalytic software used by other organization in the supercomputing community. CRYSCO also addresses long-range hardware and software plans and problems.

~~(C)~~ The week-long conference is attended by cryptanalysts and programmers from NSA and also from Australia's Defence Signals Division (DSD), Canada's Communications Security Establishment (CSE), the United Kingdom's Government Communications Headquarters (GCHQ), and the Institute for Defense Analysis (IDA).

~~(C)~~ Speakers are experts from NSA, [redacted] and outside people as well. CRYSCO presentations and workshops take place in the Friedman Auditorium and in a conference room.

~~(FOUO)~~ During CRYSCO, recommendations are forwarded by the cryptanalytic super-computing community, which are then reviewed, prioritized, and implemented by CRYSCOM.

(U) This year's conference, CRYSCO-88, will be held 23-27 May. Specifics on the program will be announced later. □

~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36

DOCID: 4019714

Review: FOUR WORKS ON CRYPTOLOGY (U)

EO 1.4.(c)
P.L. 86-36

Reviewed by: [redacted] *P11*

P.L. 86-36

Analysis and Design of Stream Ciphers. by Rainer Rueppel. Sproinger-Verlag. Berlin, New York, Heidleberg, 1986. [TK5105. R83]

~~(C)~~ Though cryptologically naive, Rueppel has developed a great deal of shift register theory and has presented it in a very attractive way.

~~(U)~~ Rueppel is a Swiss national. Much of his book is taken from his doctoral thesis, written under the direction of Jim Massey, an American, at the Swiss Federal Institute of Technology in Zurich. Rueppel has had contacts in useful places. He mentions Borer Electronics of Solothurn, Switzerland; he was at one time an employee of a popular Swiss manufacturer of cryptologic equipment; he has designed a cipher system for the European Space Agency. He was recently visiting at the University of California, San Diego, in the Department of Electrical Engineering and Computer Science.

(U) Most of the work done by academic cryptologists has been in the development of "block" cipher schemes, for which a plaintext element (and a ciphertext element) is a unit of a preassigned (large) number of bits. Rueppel instead studies "stream" ciphers: text elements are single bits. As usual, there is the obvious, but universally acknowledged to be much less important, generalization to fields of more than two elements.

~~(C)~~ Rueppel begins with the usual definitions and carefully develops the algebra associated with polynomial rings over a finite field. He mentions the synchronization problem for stream cipher generators, and discusses briefly the advantages and disadvantages of "self-synchronizing" stream cipher generators, known to us as CTAK machines.

~~(C)~~ Chapter 4 is concerned with the "linear complexity" of a sequence (the length of the shortest shift register which will generate the sequence). [redacted] He shows that the linear complexity of a "random" n-long sequence is near to n/2; in fact the expectation of the complexity is asymptotic to 1/18 (9n + 4 + (n mod 2)) and the variance is asymptotic to 86/81.

~~(C)~~ It should be pointed out that Rueppel allows shift registers which produce tails (coalescent registers) and that a similar theory can be developed [redacted]

EO 1.4.(c)
P.L. 86-36

~~(S)~~ Using a recursion devised by Massey, Rueppel was able to calculate inductively the exact distribution for the function $N_n(L)$ = the number of n-long sequences which have linear complexity L. The work that he does is closely related to the mechanics of the Berlekamp-

Massy algorithm known to us as Zierler's algorithm, after its inventor.

~~(S)~~ Chapter 5, which takes up 88 of the book's 230 pages, deals with the analysis of nonlinear combiners which produce key from a linear shift register. Here the important result is the Paige-Blankinship Theorem, and Rueppel worries about when the (upper) bound of this theorem is in fact not attained. We know (and he does to) that such an occurrence is rare. Though the book was published in 1986, there is already an update to the material of Chapter 5: "Products of Linear Recurring Sequences with Maximum Complexity" by Rueppel and Othmar Staffelbach, in the 1987 IEEE Transactions on Information Theory.

~~(TSC)~~ In the 1984 IEEE Transactions on Information Theory, Siegenthaler defined the "correlation-immunity" of a function to be of order m if the output is independant of any m input variables. We would express this differently: the bulges of all linear approximators of density $\leq m$ are 0. It turns out that for a memoryless system one cannot have both large correlation-immunity and large linear order, since their sum is bounded by the number of input variables. This can be corrected by allowing a single bit of memory in the combiner, as Rueppel notes in his Chapter 9 (apparently an afterthought, as it logically should follow Chapter 5).

~~(TSC)~~ Rueppel goes on to define the Walsh (Handamar, Fourier) transform of a binary function and to develop its most elementary properties. This has been done before, but Rueppel goes on to make a connection with cryptology. He discusses the Data Encryption Standard (DES) and calculates a Walsh transform of one of the 6-input 4-output S-boxes. We already knew (this was announced by Adi Shamir at a CRYPTO meeting) that there exist strong linear approximations to some of the S-box functions.

~~(S)~~ Chapter 6 is one of the poorer chapters of the book. Rueppel notes that changing the timing of a register (operating the register d times as fast as the system clock or, equivalently, decimating the output of the register by d) yields a different stream. He proposes a random sequence generator as follows: Take two (or possibly more - he's vague on the implementation in that case) shift registers of different (say, relatively prime) lengths $L < M$, with primitive feedback polynomials. Form key as $k_i = \sum_{i=1}^{L} x_i y_i$ mod 2, where x_i and y_i are the contents of the L low-order stages of the registers. Optionally, add in some y_j for $j > L$. He seems to think he gains something by varying the speeds of operation of the registers.

(U) In Chapter 7, Rueppel introduces the notion of a cipher system based on the knapsack (subset-sum) problem. Initially this idea was devised by Merkle and Hellman, but the Merkle-Hellman knapsack has been shown by Shamir to be weak. Rueppel laments the reputation which has befallen the knapsack concept. The idea is that N positive integer weights $w_1, w_2,...,w_N$ are chosen and then a "test" integer T is given; the challenge is to find a subset of the weights which sum to exactly T mod Q. This problem is well known to be difficult (when N is large) for most choices of T.

~~(C)~~ In Chapter 8, "The Hard Knapsack Stream Cipher" Rueppel introduces an entirely new approach to knapsack design. This is the system proposed for the European Space Agency. This is not a public-key system; the weights are not available to the analyst. Rueppel employs an N-stage primitive register and a set $\{w_1, w2_1, ..., w_N\}$ of weights. He calculates an N-bit number $k = \sum_{i=1}^{N} x_i w_i$ mod Q, where x_i are the fills of the register and Q is a number equal to or just less than 2^N. The number k, expressed in its binary representation, provides N bits of key for encipherment. Recognizing that weakness may

DOCID: 4019714

exist in the low-order bits, Rueppel suggests shortening k by lopping off a few bits. He also recognizes that the regular single stepping of the device could lead to an attack, and proposes the multiple (but still regular) stepping of the register.

~~(TSC)~~ This seems quite a sensible proposal, and [redacted] Apparently Rueppel's design has appeared elsewhere, for Don Coppersmith of IBM has announced an attack [redacted] in a paper dated March, 1986. Coppersmith also refers to a paper by Gander and Bader. Coppersmith's [redacted]

~~(TSC)~~ The book sells for $47. I own only two books (each of two volumes) for which I've paid that much, but perhaps it's the changing times. I don't think Rueppel's book is worth that much. Certainly for us there's little that's new. He has a few problems with English, but none of the errors are troubling; he writes very well. [redacted]

Primality and Cryptography by Evangelos Kranakis, Yale University. Wiley-Tuebner. Stuttgart, Chicester, New York; 1986. 235 pp. $41. [TK 5102.k66]

(U) This is another book of cryptologic significance. It does not deal with mainstream crypt topics, as Rueppel's does, but prepares the reader to study with understanding the recent papers on cryptologic systems which are based on the difficulty of mathematical (especially number-theoretic) problems. I found nothing novel in Kranakis' book, but it certainly is a convenient collection of number-theoretic facts which one needs to know to understand contemporary academic cryptology.

~~(TSC)~~ One of the papers for which Kranakis prepares his readers is the interesting "A Simple Unpredictable Pseudo-random Number Generator" by Lenore Blum, Manuel Blum, and Mike Shub, from the 1986 SIAM Journal on Computing (pages 364-383). An internal (G44) paper "The x2 mod N key generator" comments on the article.

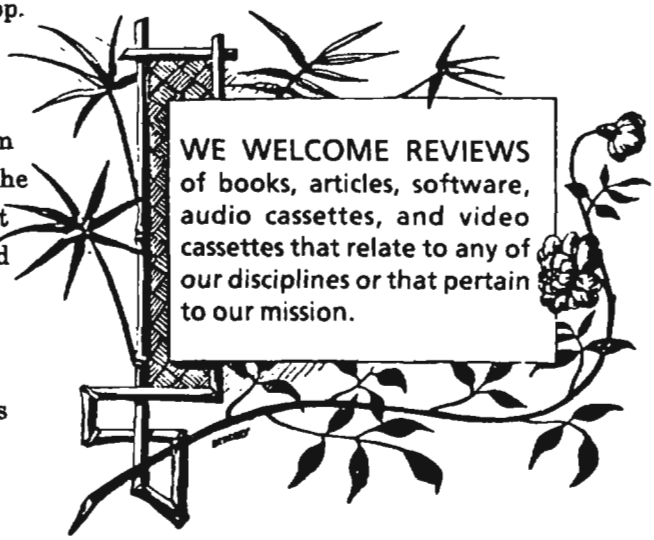
Two Issues in Public-key Cryptography: RSA Bit Security and a New Knapsack-Type System by Ben-Zion Chor. MIT Press. Cambridge (Mass), London. 1986. 78 pp. $20. [TK 5102.5 c478]

(U) This book represents the author's doctoral work at MIT under Ron Rivest. The Chor-Rivest knapsack was introduced at CRYPTO '84. A description should be in the Proceedings of that conference (available at the NSA library).

~~EO 1.~~ 4.(c)
P.L. 86-36

"Knapsack-type Cryptosystems and Algebraic Coding Theory" by Harald Niederretier. *Problems of Control and Information Theory* [a Hungarian journal] 1986, pp 159-166. [In NSA Library.]

(U) This Austrian was the co-author of an excellent book on finite fields. In the article he carefully compares his system with the Chor-Rivest Knapsack. No prizes for guessing the winner!



DOCID: 4019714

Technical Literature Review

Joseph L. Gastwirth, "The Statistical Precision of Medical Screening Procedures: Application to Polygraph and AIDS Antibodies Test Data" (with Comments by D. H. Kaye, J. C. Kircher and D. C. Raskin, Janet Wittes, J. D. Goldberg, Seymour Geisser, and Beth Gladen). *Statistical Science*, Volume II No. 3, August 1987, pp. 213-238.

Reviewed by: David Harris, R513

This article should be of interest to anyone concerned with either government polygraph or government drug testing policy.

The problem is the statistical analysis of the false positives and negatives when these tests are applied to populations in hopes of detecting rare phenomena. Suppose a test is 90% reliable in the sense that if a person has the disease, there is a probability of 0.9 that the test will give a positive response, while if he does not have the disease, there is a probability of 0.9 that the test will give a negative response. Suppose only 1 person in 5000 in the population being tested has the disease. Then, in any 5000 people tested, there will be about 500 positive responses to the test, but only one of these people will in fact have the disease. Gastwirth takes this standard analysis further in showing that in such situations, it is extremely difficult to analyse accurately how reliable the results of the test are. Thus, we may not even be able to draw reliable inferences on how much faith we should have in the test as a guideline to who is diseased and who is not.

The implications of this for the proper use of drug tests and polygraph tests are clear. Employers who give people a single polygraph test, and then either fire people or refuse to hire people on the basis of this test (a common practice in industry) are likely to be doing grave injustices to hundreds of people for every one true risk they expose. This is especially serious when the victims have no legal recourse against employers who advertise the results of polygraph or drug tests to the community at large. Such use of testing in screening a large population is clearly believed improper by all the experts. Repeating the test may or may not protect against injustice, depending on whether the false positive is for a causal reason, resulting in correlation between the incorrect results of consecutive tests.

Two guidelines are generally accepted by all the experts. First, if advanced screening has been applied so that the population tested has a reasonably high likelihood of being infected, then the problem of false positives is much less severe. Testing for AIDS in a high risk population is more reasonable than testing for AIDS in the population at large. This, of course, has implications for drug testing especially. Second, even when a trait is low probability in the population tested, there are proper ways of using the results of the test to guard against abuse. In particular, failing a polygraph or a drug test should not in and of itself disqualify an employee, but passing a test can be taken, in the absence of further reason for suspicion, to be grounds to trust the employee.

Polygraphs and drug tests can thus be used as money-saving devices. If an employee passes such a test, we may reasonably cut back on other checks of his character. If an employee fails the test, then he should get special attention of some sort. Since relatively few people in the population fail the test, we can concentrate our efforts on them. But, when screening a largely innocent population, we should remember that most of the people who fail the test are innocent. Thus, in AIDS testing, if someone fails the ELISA screening test, the proper approach is to explain the situation to him unhysterically, and go on to more sophisticated tests to settle the matter.

That there is general agreement among the experts on the proper technique for screening a broad population is impressive. □

~~FOR OFFICIAL USE ONLY~~

DOCID:4019714

CRASHING THE SYSTEM

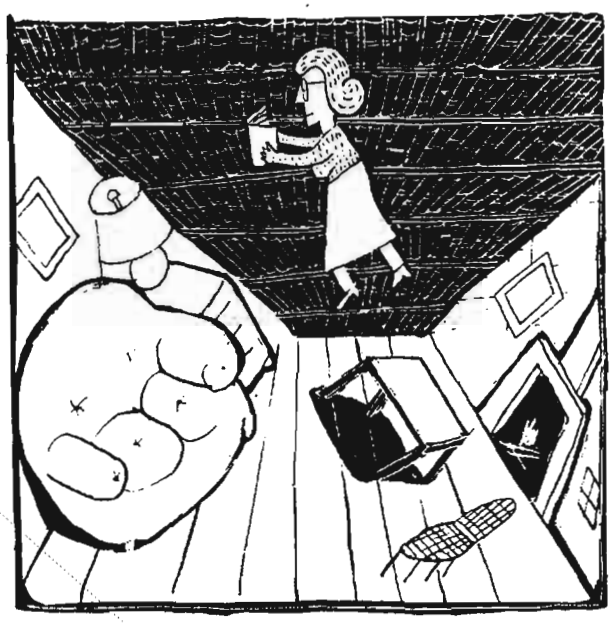
by [redacted] *C11*

(U) System crashes have become commonplace in this high-tech world. All kinds of things can cause them, from power failures to innocent mistakes by a (perhaps inexperienced) user. The latter variety are ones that operating systems try to prevent, but as with most things done by human beings, they are subject to mistakes. I can recall my own experience crashing the system.

~~(FOUO)~~ The object of my attack was RYE, and I used it infrequently enough to need the cheat-sheet (a three-by-five card, actually) that Carolyn Palmer had taped to the terminal. Carolyn had used a red pencil when writing the card; the first element of the first command line was the priority, a digit from 1 to 7, but the digit we were to use was a 3. Carolyn had made a slight goof when she started writing; maybe she was thinking of something else; at any rate, she started off with a single vertical stroke, which she tried to erase. Marks made by red pencils don't erase easily. Her "3" was abutted to a partially-erased vertical stroke, looking for all the world like a "B."

~~(FOUO)~~ Maybe you can guess what happened. Logging onto the system, I typed the "B" that I thought I was seeing and proceeded with the rest of the command. Too late, I remembered that the first character should have been a digit. About an hour later I got a call from the System Administrator [redacted] as I recall), wanting to know why I had logged on with the Director's priority. It seems that 7 (the highest) was reserved for the Director, and it threw everybody else off the system. But I hadn't asked for a "7"—I had asked for a "B".

~~(FOUO)~~ In what is good programming practice in other situations, the system tested for a "greater-than-or-equal-to" 7, rather than just testing for "equal-to" 7. On that system, alphabetic characters were numerically greater than digits. So to the system I looked like a surrogate for the Director. I think they fixed that little bug after that.



The Lingala Code. by Warren Kiefer. Random House, New York, 1972.

Reviewed by: [redacted] *P16*

(U) Why report on a 16-year old novel? Because I just ran across it by chance when my local library rearranged its holdings.

(U) It is an adventure story abounding in steamy jungles, spies, and bureaucratic infighting. There's lots of atmosphere. It's a good yarn, clearly written by someone who was there at such at time and who participated in events similar to those described.

~~(FOUO)~~ But the reason for reporting it here, however belatedly, is that the author describes an ingenious cipher system, the invention of "Eddie Ryan," a code clerk working with "Mike Vernon," a CIA agent in Africa. It seemed plausible to me, and even more so after reading the description of Lingala beginning on page 24.

~~(FOUO)~~ This book certainly would have been acquired for the Crypt Collection back in those Olden Days—which become ever more Golden with the passing of time. The Collection included fiction that had descriptions of crypt systems, especially home-made ones, just in case they popped up somewhere.

(U) (Say, whatever happened to the novels that once were in that collection?)

(U) Let "Mike" describe the Lingala code:

DOCID: 4019714

Ryan's system had the supreme virtue of looking exactly like several hundred other obscure African dialect written phonetically. Yet it was not. It was, as Ryan said, gibberish. Only when broken would it become a piece of intelligible information.

The Lingala Code worked on some of the oldest cryptographic and theological principles available to Eddie Ryan. Its basis was a missionary grammar which had fascinated him, and which he then showed me. The book was the product of a Protestant evangelical conference in Ubangi in 1931. I leafed through it.

. . . . . .

As I said, Ryan had talent. The Lingala Code answered our simplicity requirement. And it was secure, as Washington later discovered. The following day I sent it off to the States without the missionary grammar. The Agency failed to crack it, computers and all. That was because machines do no have Ryan's imagination, let alone his perception. When I sent the Agency the book finally, it still took them a few days to break the code. They did not realize that the underlying key was the way of the Congo: simple tings were often simpler than they looked, until you turned them inside out and found they were not, quite. The Lingala Code never attracted attention because it looked and sounded like a bone-fide African language. Everyone thought it was.

Lingala is a tonal language. That was one of the keys to the code's success. Lingala had never been written by the people who spoke it until the missionaries came. For their schoolrooms and their prayer-learning, Lingala was necessary, and by missionary standards, it was equally necessary that the local tribesmen become literate in what was essentially a spoken tongue. The wrong tone in Lingala could turn the word for "shield" into the word for "nut." So the phonetic system was full of traps.

The last sentence of Ryan's coded page read "Kobana yu aya yosa yu mumu."

Read that sentence aloud to the average African and he will not laugh. It was total nonsense. But the average African is polite, and language is language. There are so many dialects that it can pass as just another. I tried the Lingala Code on two eminent professors at Louvanium University, men learned in tongues of African origin. They were unable to make any sense of it, but they sagely agreed, because of its presumed source, that it was an interesting variation on one or another esoteric tribal speech. Bullshit. It was a variation on Ryan's ingenuity.

If one read the sentence, as Ryan suggested I read it, in reversed word order, it took on a recognizable, halting African rhythm: "Mumu yu yosa aya yu kobana." But it was still gibberish.

Then he showed me his simplified table of ten letter substitutions. It contained four vowels and six commonly used Lingala consonants. The list looked like this:

a=u, e=i, i=o, u=l, l=k, k=n,

n=b, t=m, b=y, and m=l

With the substitution, the new sentence read "Tata na biso oyo na likolo." A quick reference to the missionary grammar, and I came up with a literal translation of "Father from we is of heaven . . ." or "Our Father Who art . . ." etc. Ryan pronounced me a genius.

"Now sir" he continued patiently, "in our word assignments, suppose we designate 'Father' our man in Stanleyville and we assign 'heaven' as the code name for Kamina base. The message is quite clear."

LANGUAGE BRIEF: LINGALA

by [redacted]

(U) Lingala was originally the speech of the Bangala, a tribe living between Lisala and Nouvelle-Anvers in northwest Congo. First through the trading activities of the Bangala up and down the Congo River, and then through their services as mercenaries of the Belgians, Lingala became a lingua franca spoken on both sides of the Congo River from Kinshasa to Kisangani. Under the Belgians, it was the usual language of laborers, clerks, riverboat and railroad employees in the whole central and northern part of the Congo.

(U) It is one of the four official native languages of the Congo and, along with French, the official language of the Congolese National Army. It also appears to be known by all major government figures. Most Congolese have learned Lingala as a second language, but nowadays many urban dwellers, particularly in Kinshasa, learn it as a primary tongue. It is

~~(S-CCO)~~ This article was originally published in the November 1969 issue of The Quarterly Review for Linguists (QRL) where it was to be the first of a series of briefs on "the more exotic languages" prepared by linguists working in those languages. In fact, only one other brief was published, on Uzbek, in the May 1970 issue.

~~(S-CCO)~~ The idea for language briefs was presented by Prescott Currier in his article, "Data for the Language and Linguistics Section of the Country Reference Book" in the May 1968 issue of QRL. The Country Reference Books were to be a series "designed to provide useful technical information in ready-reference form on each of the target countries of NSA." That project never got off the ground.

~~(C-CCO)~~ We invite linguists to contribute briefs on low-density languages as well as on "exotic" ones. You may wish to consult the outline suggested by Capt. Currier. For a copy write to: Editor, CRYPTOLOG, P1, HQS.

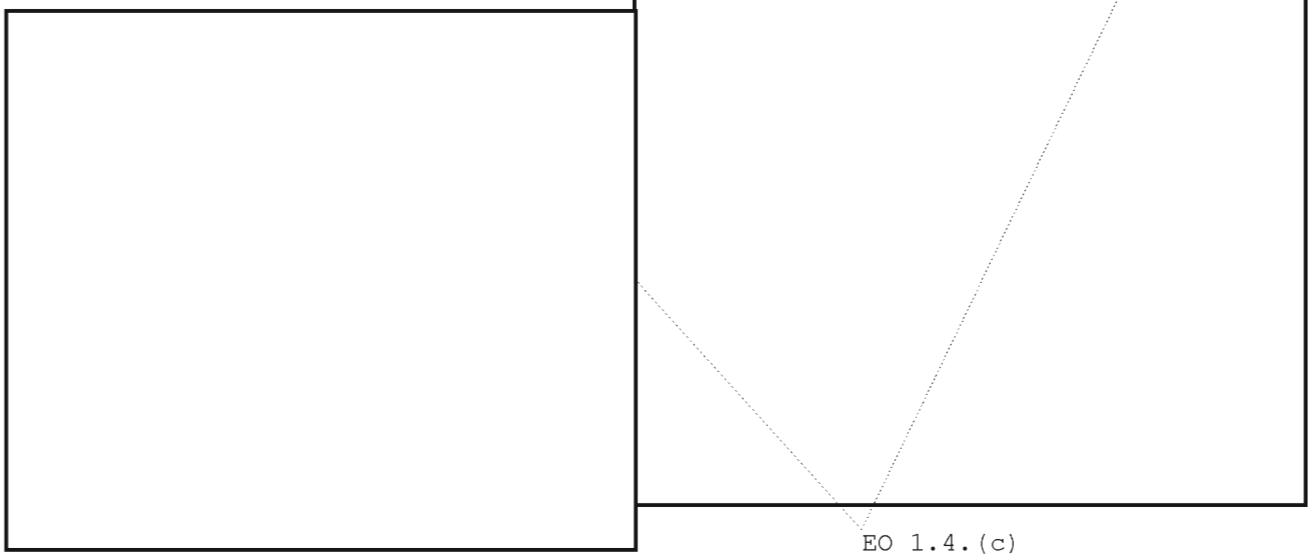
probably the most useful of the Congolese languages for a foreigner to learn; it is also an excellent starting point for the study of Bantu languages.

(U) Lingala is a member of the Bantu family of languages which dominates almost the whole southern part of Africa from the lower edge of the Gulf of Guinea across to the Indian Ocean below Somalia. It shares with other Bantu languages the characteristic of noun classes (of which it has seven) distinguished by prefixes and agreement of other parts of speech with the noun by means of concordial prefixes.

(U) Through its widespread use as a lingua franca Lingala has become simplified. Rules for concordance are not strictly observed; many adjectives are invariable and in everyday language the use of verb prefixes showing person and number is limited. The genitive particle -A normally appears only in the forms -NA and -YA, the two highest-frequency words in the language.

(U) The consonants used in Lingala are b, d, f, g, k, l, m, n, p, s, t, w, y, and z. The letter r does not occur (in foreign words it become l). U often occurs as a variant of o; dz, dj, and z frequently interchange. The nasalizing consonants m and n are sometimes dropped before another consonant.

(U) Tone is of some importance in spoken Lingala, but since there are no tonal markings in the standard written language, context has to be the prime determinant of meaning. The frequent inclusion of the French words in Lingala texts can often be an aid to understanding.



EO 1.4.(c)
P.L. 86-36

DOCID: 4019714

More Letters

To the Editor:

I refer to [redacted] letter in CRYPTOLOG, 3rd Issue 1987.

Amen!

Vera Filby, E4

To the Editor,

Just a note to say that I enjoyed [redacted] [redacted] article on traveling very much.

I can't match his experience by a long shot, but it did bring back some of my memories of trans-Pacific MATS flights in the middle and late 50's (crash trucks and Hawaiian lay-overs then, too) and of travel to the Middle East (special baggage searches, unattended baggage concerns).

I wonder if Kermit ever went through body searches in the Far East? South Korea lacked electronic gear in 1959, so there were separate male and female search rooms.

Again, thanks, Kermit, for taking the time to write that article.

[redacted] *G*

To the Editor:

I was intrigued by your note on the British Diplomatic Cipher of 1783 [4th Issue 1987]. This cipher looks a great deal like what is most frequently referred to as the "Beale Ciphers". Basically a source document is chosen. The words are then numbered starting with the first word or some previously agreed upon starting point. To encipher the plaintext, a word is chosen at random from the source document which has the same first letter as the plaintext and the number of that word is written down as the first cipher character. Hopefully, the encipherer will also mark through each word in the source document to prevent a unilateral substitution. In this case, a source document of 4000 or more words is needed since numbers in the 3900's appear. Finding the source document is no easy matter but even a second grader can solve the problem if the source document is in hand.

Sir Arthur Conan Doyle described this system in "The Valley of Fear". The Beale ciphers appeared in 1820 as documented in a 1964 paper by George L. Hart published by the Roanoke, VA. Public Library. The first mention of such a system may have been by a French mathematician named M. Michel Chasles who flourished around the time of the French Revolution.

Many man-hours have been spent by the American Cryptogram Society and the Beale Cypher Association in the unsuccessful attempt to decipher the two unsolved 1820 Beale messages, which indicates a certain degree of security of the method.

[redacted] *R223*

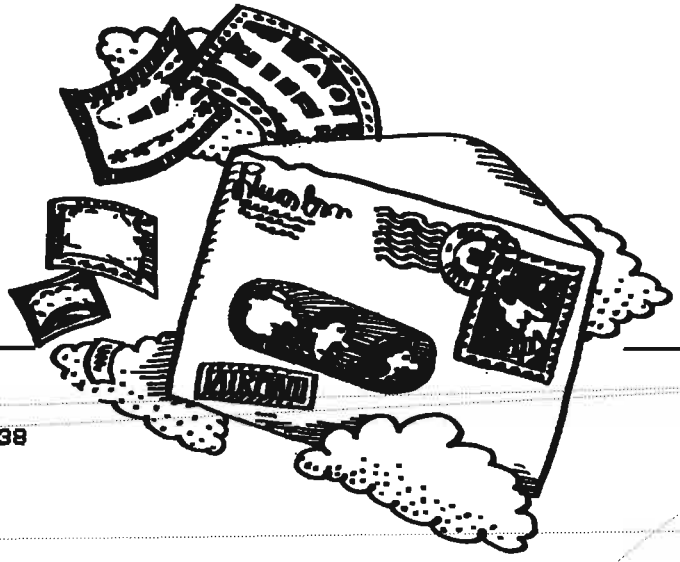
To the Editor:

Another "well done" on your 4th Issue 1987, with very valuable tips in the articles on writing.

I'm circulating my copy throughout C1!

[redacted] *D/Chief, C12*

~~FOR OFFICIAL USE ONLY~~
P.L. 86-36



CLASSIF

ZCZCRKA746DAR535
RR [redacted]
DE [redacted] #3043 0210838
ZNY MMNSH
R 210838Z JAN 88
FM GCHQ
TO [redacted] MD
ZEM
~~C O N F I D E N T I A L~~
QQQQ
[redacted]

CLASSIFIED

CRYPTOLOG NO 4 1987 - BRITISH CIPHER OF 1783
1. CODE BEARS CLOSE RESEMBLANCE TO TWO WE HOLD IN CIPHER MUSEUM DATED 1809 (R/R) AND 1820 (T/T). BOTH ARE TWO-PART WITH 4200 GROUPS, OF WHICH 102 ARE INSTRUCTION GROUPS (EG TAKE ONLY THE FIRST SYLLABLE OF THE PRECEDING NUMBER). COMMON GROUPS HAVE TWO OR OR MORE ALTERNATIVES (19/19 FOR WHAT IS EFFECTIVELY END SYLLABIC SPELL, 4/4 FOR FULLSTOP, 5/5 FOR A). VALUES ARE OFTEN COMPLEX, EG HUR,RICANE, T,FUL,RY,RIED.
2. CODE T IS ESSENTIALLY A HATTING OF CODE R IN SMALL BLOCKS OF GROUPS (2/3/4) - PROBABLY BY SHUFFLING DECODE TYPE CASE. FCO IS KNOWN TO HAVE TWO EARLIER VERSIONS: Q/Q OF 1806 AND N/N OF 1795. SHALL BE CHECKING THESE ON FRIDAY 22 JAN. THERE IS A POSSIBILITY THAT ONE MAY WORK AS PARIS IN 1772/3 HELD K/K THRU P/P (SEE KAHNS CODEBREAKERS PP 173-174). WILL LET YOU KNOW RESULT.
#3043

P.L. 86-36
EO 1.4.(d)
P.L. 86-36
EO 1.4.(d)
P.L. 86-36

CLASSI

ZCZCRKA240DAR965
RR [redacted]
DE [redacted] #3212 0251628
ZNY MMNSH
R 251628Z JAN 88
FM GCHQ
TO [redacted]
ZEM
~~C O N F I D E N T I A L~~
QQQQ
[redacted]

CLASSIFIED

FURTHER MY 210838 JAN 88
1. NEITHER N/N NOR Q/Q WORKED THE ORACLE. YOU MAY CARE TO PASS ON THAT GROUP RANGES AS FOLLOWS (ALL 2-PART):
N (1795) 1-4200
Q (1806) 1001-5200
R (1809) 1-4200
T (1820) 301-4500
INSTRUCTION VALUES ALL THE SAME.
2. POSSIBLE THAT PUBLIC RECORDS OFFICE MAY HAVE SOMETHING. WILL ASK FOR NON-PRIORITY LIBRARY HELP.
#3212

EO 1.4.(d)
P.L. 86-36
EO 1.4.(d)
P.L. 86-36

DOCID: 4019714

NSA -CROSTIC #66

[redacted] R822 P.L. 86-36

The quotation on the next page was taken from an article that appeared in an NSA publication. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS

A. Learned

B. Injuriously

C. Travel

D. Use

E. Attic quality

F. Coined

G. Fascinated

H. Blood condition

I. The act of exploding

J. Compels obedience to

K. Plumbing fixture

L. "The ——— Show"

M. Anna Pavlova used it

N. Know by instinct

O. Cape preamble

P. Miss Dunham

Q. Scurries

R. Barnyard speech

S. Terminator

T. Shade

U. Encourage

V. Serpentine

W. Hairy spider

X. A motley crowd

Y. Pertaining to birds

Z. Gravity gradient

a. Where meteorites fall

WORDS

175	141	131	125	159	52	82	118	169		
128	105	19	196	34	66	92	187	123		
197	142	77	151	114	183	3	170	46	9	
178	137	144	103	108	56					
147	163	80	139	68	181	190	182	10		
107	90	31	130	106	186					
180	88	55	42	47	198	122	104	100	69	
74	51	5	143	22	12					
2	40	11	28	48	195	65	124	96	78	24
121	185	17	173	75	84	132	165			
167	39	21	37	97	13	194	161	172		
81	67	91	119	49	98	32				
44	14	89	136	176						
1	27	150	83	30	171					
25	201	133	112	153	61	87	71	93		
120	23	85	4	38	193	164	149	174		
20	62	115	16	36	45					
157	50	79	72							
152	86	156	200	54	168	155	18			
166	146	60	199							
154	127	29	7	192	140	64				
148	110	134	53	160	189	58				
135	8	15	59	158	177	184	145	191		
116	70	94	6	138	162					
26	179	102	63	35						
113	43	73	202	126	188	57	57	95		
117	33	109	41	99	101	111	129	76		

~~FOR OFFICIAL USE ONLY~~

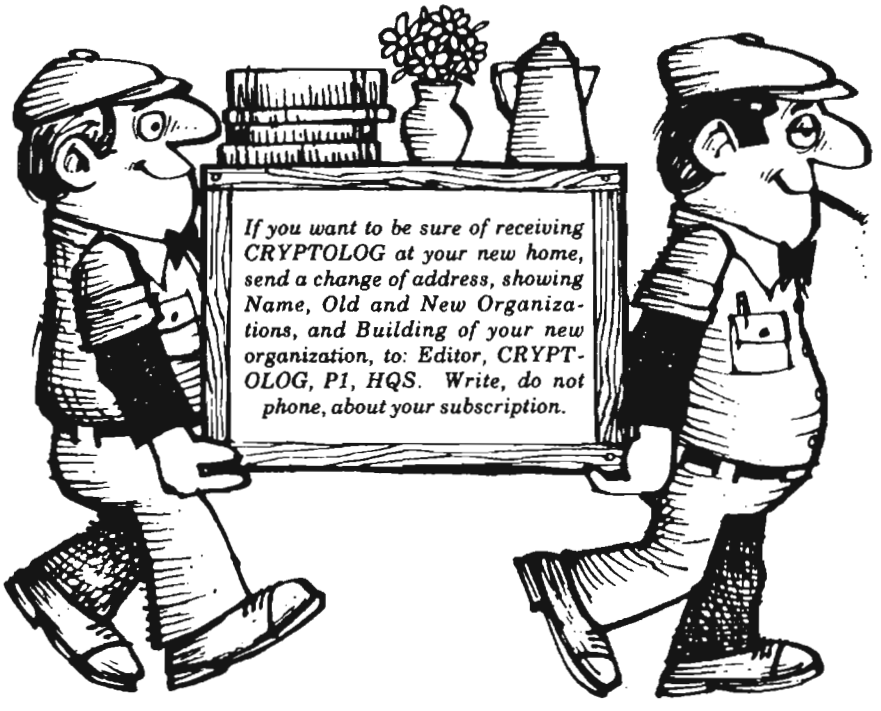
DOCID: 4019714

HOW TO SOLVE A DOUBLE-CROSTIC

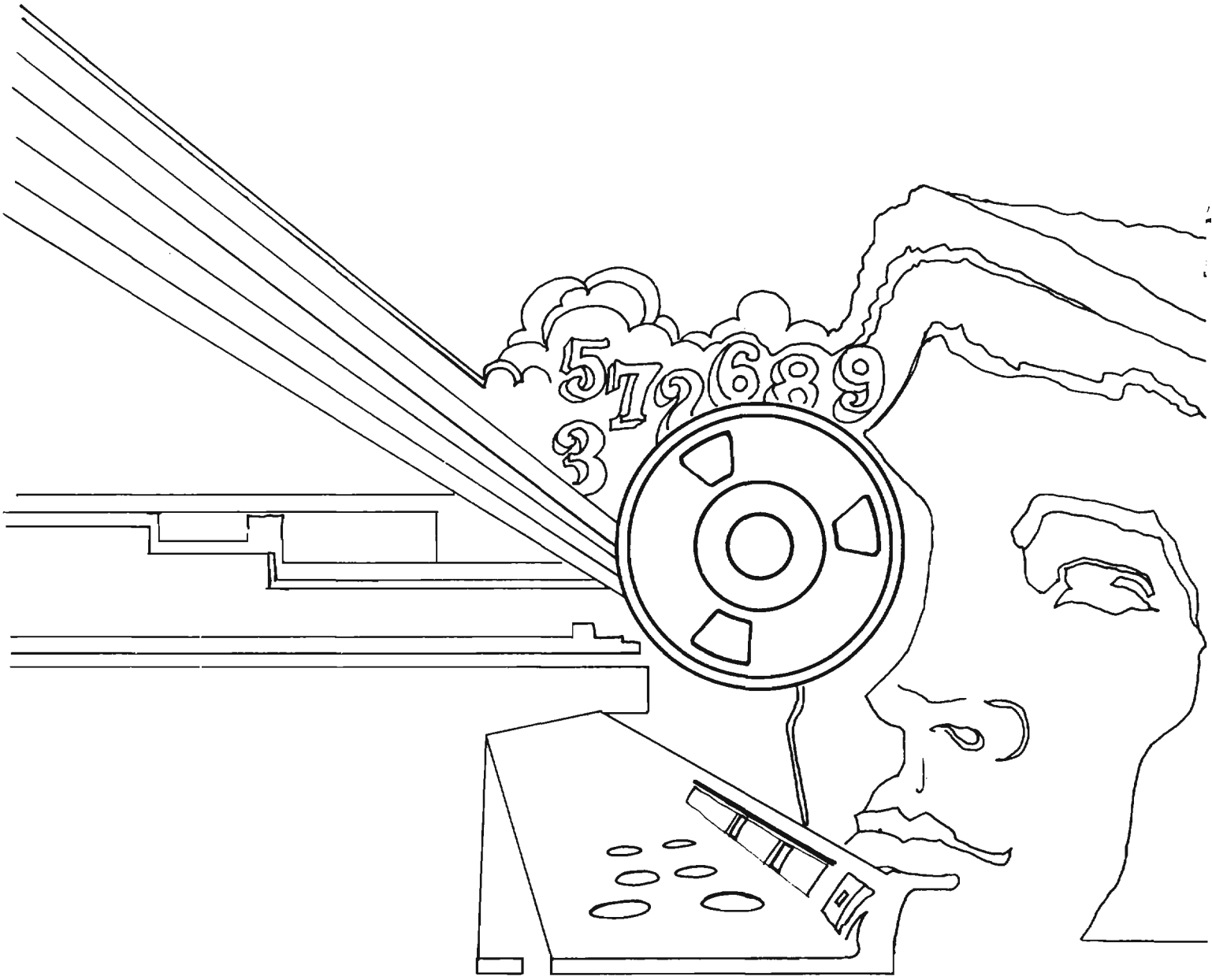
Using the Definitions, fill in whatever Words you can. Then copy each letter from the Words into the corresponding square of the grid below. Scan the text in the grid from time to time; from the recovered fragments you may be able to complete the word in context. Copy the new entries from the grid into the Definitions, where the fragments there might suggest a complete Word, and so on, working back and forth. Also, scan down the first positions of the Words as you recover them, for additional clues.

1 N	2 I	■	3 C	4 F	5 H	■	6 X	7 U	8 W	9 C	10 E	11 I	12 N	13 K	14 M	15 W	■	16 Q	17 J	■	18 S
19 B	20 Q	21 K	22 H	23 F	24 I	■	25 O	26 Y	27 N	■	28 I	29 U	30 N	31 F	32 L	33 a	34 B	35 Y	■	36 Q	37 K
38 P	■	39 K	40 I	41 a	42 G	43 Z	44 M	45 Q	■	46 C	47 G	48 I	49 I	50 R	51 H	52 A	53 V	■	54 S	55 G	56 D
57 Z	58 V	■	59 W	60 T	61 O	■	62 Q	63 Y	64 U	■	65 I	66 B	67 I	68 E	69 G	■	70 X	71 O	72 R	73 Z	74 H
75 J	76 a	■	77 C	78 J	79 R	80 E	81 I	82 A	83 N	84 J	85 F	86 S	87 O	88 G	89 M	■	90 F	91 L	■	92 B	93 O
94 X	95 Z	96 I	97 K	98 I	■	99 a	100G	■	101a	102Y	103D	104G	■	105B	106F	■	107F	108D	109a	110V	■
111a	112O	113Z	■	114O	115O	116X	117a	■	118A	119I	120F	121J	122G	123B	■	124J	125A	■	126Z	127U	128B
129a	■	130F	131A	132J	■	133O	134V	135W	136M	137D	138X	139E	140U	■	141A	142O	143H	144D	145W	146T	147E
148V	149P	150N	■	151O	152S	■	153O	154U	155S	■	156S	157R	158W	159A	160V	161K	162X	163E	164F	165J	166T
■	167K	168S	169A	■	170O	171N	■	172R	173J	174F	175A	176M	177W	■	178D	179Y	180G	181E	■	182F	183O
184W	185J	186F	■	187R	188Z	189V	190E	■	191W	■	192U	193F	194K	195I	196B	197O	198G	199T	200S	201O	202Z

MOVING?



~~FOR OFFICIAL USE ONLY~~


5726893

DOCID: 4010011

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

4th Issue, 1987

HOW TO WIN WITHOUT PLAYING THE GAME . . . . . [redacted] .1
LETTERS 5, 10
PROJECT TIPONI. . . . . [redacted] .6
THE EFFECTS OF DETONATIONS ON METEOR SCATTER. . N. C. Gerson. . . .9
BULLETIN BOARD. 10
ALAS, WADE GILES, I KNEW YOU WELL . . . . . Leigh Sawyer. . . 11
HOPEFULLY, FOR ALL OF WE. . . . . [redacted] 12
THE MATTER OF STYLE . . . . . [redacted] . . . 14
HOW TO MEASURE CLARITY IN WRITING . . . . . [redacted] . 15
TWO TIPS ON WRITING . . . . . [redacted] . . . 16
POINTERS ON GRAMMAR . . . . . Ralph Jollensten. 17
THE HERO OF THE SENTENCE. 18
GIMME REWRITE!. . . . . Va. 19
BOOK REVIEW: MACHINE TRANSLATION. . . . . [redacted] . 20
FROM THE PAST 21
BUSMAN'S HOLIDAY: A BRITISH CIPHER OF 1783. 22

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4010011
P.L. 86-36

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XIV, No. 4 ..... 4th Issue 1987

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Collection ..... (963-5877)
Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Cryptolinguistics ..... (963-1596)
Index ..... (963-5292)
Information Science ..... (963-3456)
Information Security ..... George F. Jelen (859-1211b)
Intelligence Research ..... (963-3845)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (963-4958)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-4351)

Illustrators ..... 963-3057)
..... 963-6211)
..... 963-5248)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five)
(note: no 'o')

Always include your full name, organization,and secure phone; also building and room numbers.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, HQS 8A187
Please do not phone.

Contents of CRYPTOLOG should not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

DESERT ISLAND BOXES

The scenario below was inspired by the program on public radio, "Desert Island Disks" where guests select five recordings and one other item to while away the hours when they are castaways on a desert island. The guests also discuss their choices and philosophize on their careers and on life in general.

We thought it might be fun for CRYPTOLOG readers to think out a version of this fantasy.

⊕ ⊕ ⊕ ⊕ ⊕

You're shipwrecked on a desert island on your way to a field site. You've got everything with you to carry out your mission, packed in boxes that are 12x12x15. And thanks to miniaturization, a pc and printer fit in one box. Fortunately, in the desert island there is food, shelter, clothing, and standard supplies aplenty, as well as electricity. Also, your team can communicate with the main frame at HQS via a pc for a total of an hour a day. But you will have to take along the references and handy-dandys, in the form of paper, floppy disks or other media, that you will need to accomplish your mission.

Each member of your team is allowed to take along six boxes, five with materials for the mission that are selected and packed by that member, and one for personal use, relaxation or otherwise. There's a catch, however: the team may be evacuated to another island, in which case the team leader may be ordered by HQS to jettison one mission box per person.

What would you take with you? How would you pack your boxes? All your dictionaries, say, in one box, or lesser ones in the jettison-able box? And why? What would you put in your personal box, and why?

It will be most interesting to read your responses.

~~FOR OFFICIAL USE ONLY~~

How to Win Without Playing the Game

P.L. 86-36

On International Protocol Standards and Security Features for DoD

R536

(U) As the International Standards Organization (ISO), and by extension, the American National Standards Institute (ANSI), continue to specify inter-computer protocol standards for open systems, more pressure is being put on the DoD to adopt these standards. Upon completion of the study of the National Academy of Engineering, comparing DoD's Transmission Control Protocol (TCP) with ISO's Transport Protocol Class 4 (TP4) for use in DoD, the Assistant Secretary of Defense for Communications, Command, Control, and Intelligence stated that DoD will transition to the international standards once they have been shown to be as reliable and resilient as current DoD protocol standards. NATO has already endorsed for NATO systems the use of protocols developed from these standards.

(U) A benefit advanced for adopting such standards is procurement off-the-shelf as part of a vendor's standard product line. But some major pitfalls lurk in this strategy (or desire) which we will address later.

PITFALLS OF IMPLEMENTING STANDARDS

(U) Significant attention is being given to the ISO reference model and the standard protocol specifications that derive from it. Manufacturers are selling their future products with the words "we are compatible with the ISO standards" or "our system is compatible with

EO 1.4.(c)
P.L. 86-36

the ISO reference model." Purchasers seem to be of the belief that products purchased with the ISO caveat will allow those equipments to intercommunicate automatically with products with the same caveat from other vendors.

(U) However, few people at high levels seem to be paying attention to what really matters, which is the implemention, not specification, of the standards. The American and European continents have different approaches to implementation. Additionally, implementations are jealously guarded, usually with comments like "don't worry how I implement them internally, as long as I provide the standard interface, you shouldn't care."

(U) I believe that the European market is so small that any single vendor cannot capture a large enough market share to remain profitable. It is therefore, to their advantage to be able to interoperate with each other's equipments. In the US, however, the market is sufficiently large that a number of vendors can each capture a profitable market share, thus affording less incentive to interoperate with other vendors' equipments. These vendors are "adopting" the ISO approach, but they are doing this either in conjunction with their own proprietary approach, or by adding proprietary functionality which can result in non-interoperability. Moreover, each vendor attempts to add its own little enhancements which try to lock in their customers to *its* equipments, and prefers to implement its own proprietary protocols and network architecture. By contrast, European vendors predominately are planning to adopt ISO and to discontinue their own proprietary approaches.

(U) Some US vendors are adopting the International Standards as a second capability to try to meet the requirements of some of their users who are adamant about the use of commercial standards. But what isn't said is how they will go about providing them. In addition to incompatible enhancements to the international standards, some vendors have privately indicated that they may provide "invisible" translating gateways between the international standards and their proprietary protocols. Effectively, they are providing an ISO interface into their proprietary network. The interconnection of their machines runs only their proprietary protocols. For those US vendors who take one of these approaches, statements of compatibility with ISO protocols are at best a smoke screen to obscure what they are really doing, and at worse, misrepresentation of their products.

(U) The original intent of the DoD Protocol Standardization effort was to preclude the need to translate protocols by requiring all to implement a standard protocol suite. The ISO standards are based on the same premise. But as things stand now, let the buyer beware. Each individual vendor's approach needs to be carefully examined.

IMPLEMENTATION OF PROTOCOLS WITH SECURITY MECHANISMS

(U) The pit becomes larger when security features are included in protocol implementations. There are three elements to the inclusion of security features in protocols: the definition of the security mechanisms; the implementation of those mechanisms in a trusted way; and the assurance that the implementation is in fact correct and safe. Security mechanisms are normally included as part of the protocol specification. However, protocol specifications do not address either trusted implementations or assurance factors. The ISO Security Addendum deals primarily with security mechanisms and their placement in an overall protocol architecture, the ISO Reference Model. It mentions that trusted functionality is expected whenever security features/mechanisms are implemented, but it doesn't say much more than that. And for its purpose, it probably shouldn't. No documents deal with the assurance issue for security mechanisms in protocols, though one that does address assurance is the "Orange Book."

(U) It is clear, I hope, that trusted implementation and assurance issues are (in part) implementation issues. Security mechanisms need to be carefully implemented, understood, and evaluated. Yet it is not clear that vendors fully appreciate the impact of these statements on their freedom over their implementation. One can't allow a vendor attitude of "leave the implementation to me." It is also not clear how much the vendors intend to do about satisfying the need for trusted implementations and satisfaction of assurance requirements.

(U) Will off-the-shelf vendor products be good enough? It is not inconceivable that the DoD may have to modify and/or adapt off-the-shelf

products to meet assurance and security evaluation requirements, as well as to adapt them to a trusted implementation. This is independent of the presence or absence of adequate security mechanisms in the protocol.

AUGMENTING THE INTERNATIONAL STANDARDS

~~(S)~~ [redacted] In general, it is not clear that this approach can be effectively utilized. It is applicable for simple functionality substitutions, such as replacing one checksum with another. But it breaks down quickly with more complex functionality, especially with the more complex counters against denial of service and integrity attacks.

(U) If one changes the functionality of a protocol, for example, a reassembly scheme to protect against playback attacks, one actually has defined a new protocol. It really doesn't matter how you refer to it, the odds are it won't interoperate with its parent. An excellent example of this name game taken to an extreme is the International Standard Transport Protocol (TP) and its versions TP0 through TP4. In actuality, they are five different protocols that do not interoperate with each other. Yet because purists in ISO will allow only one protocol per layer, they defined these different protocols as versions of the same protocol. Some even claim that the National Bureau of Standard version of TP4 differs from ISO's TP4. Its not clear whether implementations of the two will in fact interoperate.

(U) However, there is an excellent concept in the previous suggestion. That is the modification and/or augmentation of off-the-shelf protocols. We can combine that concept with a few others to define one possible approach of utilizing international standard protocols to the maximum extent possible, without active involvement in the standards arena.

(U) We begin by first recognizing that any protocol functionality of a non-sensitive and unclassified nature can be presented and argued by the National Bureau of Standards. They are the Government's agent in the commercial standards arena. This method of operation can continue.

(U) We next look at NATO's method of operation. They first try to get ISO to adopt their military requirements in the commercial standards. But they recognize that not all military requirements are needed by the commercial world, and that they won't all be accepted. They have Standard Nation Agreements (STANAGs) which are basically NATO augmentations of commercial standards for NATO's use.

(U) Now the questions become: can a similar bureaucratic approach be used by the DoD, and can implementations be structured in such a way as to make the approach acceptable to all parties? We propose that DoD develop the equivalent of NATO STANAGs for DoD purposes, as part of the DoD Protocol Standards Program. Where the augmentations or changes deal with sensitive security issues, there is nothing to prevent the DoD augmentation from being classified. It appears that some bureaucratic mechanisms are already in place, with a DoD Protocol Standards Steering Group report identifying the "development of Mil-Spec supplements for the commercial ISO protocol definitions."

DEVELOPING THE IMPLEMENTATION

(U) The more difficult question is, can off-the-shelf implementations be easily modified? And how can the new version be structured so that the old version could still be utilized if necessary?

(U) We will start by examining what the conditions are if the desire of using off-the-shelf products containing security mechanisms were achieved. It would have to be a trusted implementation. It would have to be evaluated, and therefore understood by independent parties, and it would have to meet some assurance level of correct and safe operation. All of these criteria argue that the implementation would have to be well structured, most likely in a modular way.

(U) Our approach, where a DoD product is derived from an augmented off-the-shelf product, would still require it be modular. But it would not necessarily require that the off-the-shelf implementation be a trusted one. Additional security functionality modules could

EO 1.4.(c)
P.L. 86-36

be added, and calls at the appropriate places in the off-the-shelf version could be inserted. Where functionality has been changed, the module calls in the off-the-shelf version would be changed to call the new modules.

(U) Alternatively, a conditional test of whether or not one was operating in secure mode could be added with a call to the new module. This would allow continued operation of the original product as well. Using the terms of protocol implementers, the security functionality would be viewed as "optional functionality," which is not invoked for non-secure operation but which would always be invoked for secure operation. This approach also allows for a more complex implementation whereby the security system may back off from some of the features provided if environmental conditions warrant it and if policy allows it. (An example of a security back-off is BLACKER's Emergency Mode.) This is not to suggest that back-off be a user-selectable option.

(U) The only modules that would need to be protected and evaluated would be the new ones. Thus, a trusted computing base could be designed around only the new modules, leaving the rest of the protocol to run as untrusted code. The trusted computing base would also have to ensure that the secure functionality is invoked for secure operation.

(U) One must recognize the performance risk with modularly implemented protocols. The overhead associated with module calls and returns can be significant, and may have a negative impact on the ability of the implementation to meet high speed performance requirements. Careful design in this area is required. A proof of concept demonstration in this area would be reassuring. (C324 is addressing the issue of protocol implementations in ADA. ADA alone forces a high degree of modularity in an implementation.)

(U) Of course one does not change the functionality of a protocol without changing the headers. If one adds functionality to the basic protocol, then the header must be extensible, with option fields being used for the new functionality. If a functionality change requires a header field change, two approaches could be used. One is to use the option field approach, where the presence of the option field overrides the correspondent field in the basic header. Or, one could define a different header format from the basic one, and distinguish between them through the use of a protocol version number in the header.

CONCLUDING REMARKS

~~(C)~~We believe this to be one approach which would satisfy the contradictory desires to use off-the-shelf commercial protocols as much as possible and still prevent transfer of security technology potentially inimical to DDO's mission. This approach does not require active participation in the commercial standards world. We take what they produce and modify it appropriately, through the DoD Protocol Standards Program for the specifications, and through vendors or cleared contractors for the implementations. Contractors and vendors could be restricted as to whom they provide the "DoD secure" implementations.

(U) What is required of the international standards is only an extensible header and a protocol version number in the header. What is required of the implementation of the standard would be modularity.

(U) It has also been argued that the US commercial world is also in need of security protection. This is a major argument for NSA's active involvement in the international standards process. By using the above approach, commercial vendors could be provided the security modules (DoD specifications or implementations) under a license arrangement, which could restrict dissemination of the "DoD-secured" product in any manner DoD required. It could be restricted to continental US use, to US-owned companies, etc. This approach is analogous to the COMSEC Commercial Endorsement Program licensing arrangement for encryption implementations.

(U) The serious technical implementation challenges of this approach are a modular implementation (which would be required anyway for a trusted implementation) with adequate performance, the manner with which the "security modules" are integrated into the commercial product, and the ability to run an off-the-shelf implementation as untrusted code on a trusted computing base. One conjectured approach for doing this, utilizing ADA, has already been raised.

(U) This approach does not satisfy the desire by some defense personnel to actively participate in the international and national commercial standards arenas for security enhancements. Some seem to have confused the means with the ends.

ACKNOWLEDGMENTS

~~(FOUO)~~ I wish to thank [redacted] C322, and [redacted] R536, for their helpful comments on an earlier draft.

SOURCES AND REFERENCES

(1) ISO Draft Standard 7498, Open Systems Interconnection (OSI) Protocol Reference Model

(2) ISO 7498 Part 2 Draft Proposal, Security Addendum to the OSI Reference Model dated Nov 85

(3) Transport Protocol for Department of Defense Data Networks; National Research Council Committee on Computer-Computer Communication Protocols

[redacted]

(5) DDO contribution to (9), 3-page paper undated and untitled.

(6) M/R serial C3-160-82 dated 2 Nov 82; subj: National and International Standards, DoD Use Thereof; Network Security Issues, and Classification

(7) Q41 Memorandum dated 3 Jul 86; serial Q4-637-86; subj: Final review of Network Security Classification Guidelines

(8) M/R serial C32-003-84 dated 18 Jan 84; subj: Status for NSA Response to USD R&E (CCCI) on Use of Commercial Standard Protocols in DoD

(9) DIRNSA letter N1743; dated 18 Oct 84; subj: Data Communications Protocols

(10) Department of Defense Trusted Computer System Evaluation Criteria, National Computer Security Center

(11) Q41 M/R (no serial) dated 6 Aug 86; subj: OSD Initiative re Participation in Standards-making Bodies

(12) C Memorandum C-301-84 dated 31 Aug 84; subj: Data Communication Protocol. (The ADCS contribution to (9))

(13) C Memorandum C-367-82 dated 9 Nov 82; subj: Classification Guide for Network Security

(14) Private conversation with vendor personnel at the National Academy of Engineering Transport Protocol Study which resulted in (3)

(15) DCA/DCEC/R130 letter dated 21 Aug 86; subj: Record of the 27th Meeting of the Protocol Standards Steering Group (PSSG), 24 June 1986

P.L. 86-36

To the Editor:

(U) As I walked into the office early this morning and saw our latest intern hard at work, these thought flooded my mind. With only one or two exceptions, the 15 or so interns the division has enjoyed in the last 3 years have been super performers. We've given them responsible jobs and challenged them to excel. They have taken up the challenge and produced results far above our high expectations.

(U) I've heard expressions of concern for this Agency's eroding experience base. I've also observed that long experience, per se, isn't always relevant, and is sometimes an impediment, to solving current problems. If the interns we've had are representative of the intern popiulation as a whole, and I have no reason to doubt that they are, then the Agency's future is in quite capable hands. These young folks may not always do things the way we old-timers would, and that may be good.

[redacted] *P36*

P.L. 86-36

Project TIPONI

The Translator's Workstation of the Future

P16

P.L. 86-36

Description of the Task

(U) We also require the capability to optically scan hardcopy data, in any native script, for input to the workstation in the native script.

EO 1.4.(c)
P.L. 86-36

DOCID: 4010011
P.L. 86-36

Selecting Reportable Messages

[redacted]

[redacted]

(U) As he works, the linguist may wish to jot down notes on either the message text or the translation. The notes should be clearly distinguishable from the text itself and should be deleted easily when the translation or report is complete, if desired. For example, the linguist may wish to send notes along with the document to another linguist noting an area with which he had difficulty and where he requires assistance.

~~(FOUO)~~ During the process of preparing a message for publication the linguist needs to consult on-line working aids such as gazeteers, dictionaries, special purpose glossaries, databases, etc. to obtain further information about a name, location, or another message referenced in the message in question. These on-line tools should be easy to reference and easy to display in a small window where it does not obscure the rest of the text. During the process of preparing the report, the linguist may add footnotes to the end-product. The footnotes should be automatically placed at the end of the document and in the appropriate format. In checking his work, the linguist may wish to examine the footnote at the same time that he is looking at the text which is footnoted.

~~(FOUO)~~ After the translator has completed a report or translation, he prepares a cover sheet for the end-product and sends both to a senior linguist or checker who verifies the accuracy of the coversheet and of the end-product. The linguist may wish to display the source text, translation, and cover sheet on the screen at the same time.

(U) The checker may consult on-line working aids such as dictionaries and glossaries, and

The Translation Process

[redacted]

P.L. 86-36

should be able to look at a footnote as he is reading the footnoted text. The checker may wish to jot down notes on the document in order to direct the linguist's attention to errors to be corrected, or to train a junior linguist. These notes should be clearly distinguishable from the text and easily deletable. If the text is returned to the linguist for corrections, it is then returned to the checker who will look at the notes and corrections to verify that the document is now correct. When the document is approved, the checker sends it along to another workstation for publication, or a camera-ready final copy is printed.

Summary of Desirable Features of a Translator's Workstation

Screen Size

(U)The display for a translator's workstation should be large enough to allow a linguist to look at large portions of both the original text and the translation so that he can see enough information to understand the text. There should also be room for small windows to display working aids such as dictionaries. This requirement probably calls a 19-inch screen with bit-mapped graphics display. The 11-inch or even larger raster displays are not large enough or flexible enough to offer a linguist an alternative to paper and pencil.

Fonts

(U) In some cases for display of the text, and in many cases for display of softcopy working aids, linguists require foreign language fonts in approximately 30 to 40 foreign writing systems. The foreign fonts must include punctuation and special symbols necessary to represent the foreign language accurately, and the display screen must have sufficient resolution to represent the native scripts clearly and accurately. The fonts required include difficult ones such as Japanese, Chinese, and Korean, as well as the easier European languages. A variety of font sizes and faces should be available to highlight portions of text.

Word-Processing

(U)The foreign language displayed must be in a form, i.e. character strings rather than graphics or pictures of text, that can be edited, sorted, indexed, parsed, etc. The user must be able to specify how the text is to be sorted or indexed, including the direction (forward or reverse), nulls, etc.

On-line Working Aids

~~(FOUO)~~ Linguists require softcopy working aids such as dictionaries, gazeteers, [redacted]lists, etc. which can be referenced from the workstation. The dictionaries should include both personal dictionaries and master dictionaries available to all linguists. New additions to the dictionary would be added to the personal dictionary, and be stored in a file for review by a senior linguist before being added to the master dictionary. The dictionaries must be capable of including grammatical information, usage examples, English translation, and descriptive narrative in English, the foreign language, or both. The grammatical information should be stored in concise linguistic format to save space, but be expandable by a user interface so that the information could be used by language specialists who are not familiar with the formal notation system.

Translator's Editing Features

(U) The checker requires capability to show on the screen the suggested changes to the product in order to assist in training junior linguists. This would include such things as pointing out omissions in the text, errors in the text, suggesting deletions in the text, indicating with highlighting, pointers, lines, or color, dependency relationships in the text which the translator has failed to understand. □

The author solicits comments from linguists and reporters who might be concerned with any aspect of the process described.

DOCID: 4010011

The Effect of Detonations on Meteor Scatter

N C Gerson, W3

~~This article is classified CONFIDENTIAL in its entirety~~

Meteors create discernible ionization trails at altitudes between 60 and 140 km above the earth. On the average, the trails last for seconds or less. The electron densities in the trail usually range from 10^6 to 10^8 per cm^3. These figures represent nominal means of distributions; extremes are larger in all cases.

Meteor scatter systems offer low data rate circuits at high reliability, low power and some privacy.

If sufficient ionization arising from any other physical mechanism is produced in the altitude range near 100 km, the meteor system operates continuously as a normal system. This may occur under either of two conditions:

- natural, when sporadic E is present, or during periods of high sunspot activity;
- man made, during artificial modification of the E layer, or during high altitude nuclear detonations.

Effects of the latter are discussed below.

High Altitude Detonations

A high altitude detonation may be defined as one that occurs above 40 km, where atmospheric number densities approach those in vacuum – or discharge – tubes. The detonation releases huge amounts of energy, both radiant (to gamma rays) and corpuscular (ionized metallic and atmospheric species lumped together under the term debris). The injection of this energy at this altitude profoundly alters the normal ionosphere.

It should be recalled that energy of this magnitude injected into the ionosphere produces complex hydrodynamical and magneto-hydrodynamical disruptions, and changes the ambient chemistry and ionization reactions. After a single detonation, the entire affected area remains violently disturbed for 30 to 60 minutes.

EO 1.4.(c)
P.L. 86-36

Finally, it must be remembered that the ionosphere is self-healing. After a period, whose duration depends on the total energy and on the altitude of the detonation, the ionosphere slowly returns to normal under the action of sunlight. □

MOVING?
Mail a change of address to:
HQS, P1, Editor, CRYPTOLOG
Include your Name, Old and New Organization, and Old and New Building

BULLETIN BOARD

ANALYTIC SOFTWARE FOR PCs

~~(FOUO)~~ A new work center in G33 is being created specifically to provide support on the pcs for the exploitation of manual systems in G Group. This center will offer personal help as well as generalized and customized programs. All it takes is a phone call. In addition, it will maintain a library of cryptanalytic programs for the ASTW. In the future it will call for programs written in G and elsewhere that could be used by a wider audience.

~~(FOUO)~~ The new center will be headed by [redacted] 963-3669. Other pc needs will continue to be provided by G331, whose chief is [redacted] Her phone number is also 963-3669.

P.L. 86-36

GERMAN TV HOUR

(U) If there is sufficient interest, we will resume showing TV news and documentaries in German from the FRG, Austria, and the GDR. In the past they were shown once a week at lunchtime on a walk-in basis. Let us know how often you'd be likely to attend (once a week, once a month, etc.) Please respond to [redacted] P16, HQS 8A187, 963-1103.

P.L. 86-36

To the Editor

I enjoyed Dave Chizum's article on Ethiopia [CRYPTOLOG, 1st Issue 1987] so very much. It's a thrilling and exciting story - and a first-rate piece of writing. It's too bad it's classified and can't be published outside.

[redacted] SC

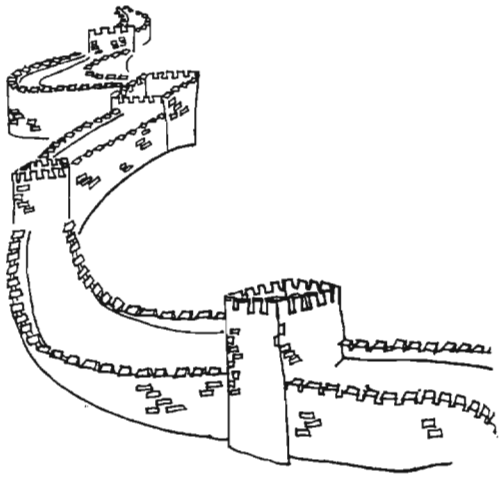
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4010011

ALAS, WADE GILES,

I KNEW YOU WELL



E. Leigh Sawyer, Ret.

In the December 1972 issue of the now defunct publication *DRAGON SEEDS*, there appeared an article of mine on the Wade Giles system. This system for the romanizing of Chinese, once used by NSA and throughout the intelligence community, was cast aside on 1 January 1979 in favor of the PINYIN system. For historical purposes, it might be well to reprint the Wade Giles item if only for auld lang syne. By the same token, a PINYIN item would also seem appropriate so as to permit a better understanding of how the system works.

THE WADE-GILES SYSTEM

For the p'erson who has had little exp'erience with the Ch'inese lankuache, the p'ronouncing of p'lace names, p'eop'le's names, art'ifak't's, and even the inkretinent's of Monkolian parpek'ue is often k'onfusing. An unterst'anting of at least Wate Chile's ap'ost'rophic usache aft'er cert'ain k'onsonant's chust might enable one t'o atchust himself t'o this esot'eric linkuist'ic area. A little pak'ground on Wate Chiles might pe in orter. Wate Chiles was porn in Ch'ik'ako, and lat'er moved to Cheorchia. At that t'ime, his mother atvised him, "You ought t'o invent something. Why ton't you ko t'o Ch'ina, Wate, and invent the Wate Chiles syst'em?" He said, "Poy oh poy, mom, puy me a t'ik'et and I will t'ake the first poat leaving p'ort." So he t'ook off for K'athay. His letters t'o his mother reflek't the choy he felt in t'raveling from p'lace to p'lace. He mate reference t'o the many intichenous t'ype nat'ives he had pump'ed int'o, and the cheokraphik'al ottit'ies he had seen. In any k'ase, as may be kauched py it's witesp'read usache t'otay, Wate invent'ed his syst'em, and it is seen on map's and all k'inds of swell st'ull all over the p'lace.

On the pasis of the k'arefully kathered tat'a p'rovided apove, one k'an easily tecite how t'o p'ronounce that p'art of a Ch'inese p'lace name that has an ap'ost'rophe in it, and one which toesn't - also p'rop'er names (poys or kirls) and telek't'aple Ch'inese tishes such as K'ant'onese st'yle pean k'urd.

THE PINYIN SYSTEM

Wonce upon a taim, there were tu little Chinese boyis named Pin and Yin. Won night, Pin was studying Chinese karakters when he suddenly threw down his book and said to Yin, "Anyone hu studies this zhunk has to be a zherk. What du you say tu our killaborating on a niu system. We'll kall it the 'Pin-Yin' system'." Yin said, "Don't hand me that zhaive. That would bi qiting on the system. It's ok to qit at ma zhoung or at kads, but not in skul. Bisides, if we went ahead with a niu system, we should kall it 'Yin-Pin'."

Well, they qiued this over for a bit and finally agreed on "Pin-Yin." The mein reason being Pin kud easily punch out Yin bikause he was a lot bigger. The top of Yin's head only kame to Pin's qin.

"Anyhow," Pin said to Yin, "If we are tu get on with this, we'd be waise to du it on a full stomak." So, after a big meal of fish head and ternip chaoder, and also raiding the kukie zha, they set to work.

Working dei and night, they zhenerated the system in short order. When they were finished, they went tu the zhuish deli around the kourner for beigles and a kup of zho. "Ji whiz," said Pin tu Yin, "won't Wade Zhailes be mad when he learns of our system? He may try tu send us to zheil, may be even to Xing Xing."

Well, Pin and Yin did not go tu zheil. The moral of this story being, there's more than wun wei to skin a kat, so qin up, Wade Zhailes dai hards, and bi of good qir. □

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010011

HOPEFULLY,

FOR ALL OF WE

DSC

P.L. 86-36

In my article, "How To Write A Memo" published in CRYPTOLOG, 1st Issue, 1987, I promised some pointers on grammar. Here they are. Grammar is such a problem these days that I have about given up on it, and I debated with myself about tackling it in this article. But I'll give it a try. I must say something about a few errors, at least the ones that bother me the most and interfere seriously with my ability to understand memos and almost everything else I read as well.

¶

One of my pet peeves is the misuse of **hopefully**. If you want to make me cringe, just use that word. Until recently, **hopefully** was just another common adverb meaning "with hope."

He eyed the candy jar hopefully (with hope).

He approached the task hopefully (with hope).

But at present it's commonly misused. One doesn't really mean this:

Hopefully (with hope???) he'll make the next touchdown.

But this:

I hope he'll make the next touchdown.

I urge you not to use **hopefully** at all if you can't use it correctly. If you mean "I hope that" then say it, and do not misuse the adverb **hopefully** (meaning "with hope") instead. Don't be a lamb following all the others into this error!

And while I'm talking about "ly" words, here is another: **most importantly**. That also sets my teeth on edge. Only rarely is it the correct phrase. Most of the time the ly is redundant and ungrammatical. Say "most important" since that is what you mean.

¶

Apostrophes are everywhere these days and mostly where they shouldn't be. Take **its** and **it's**, for example. **It's** means "it is." The apostrophe represents a contraction:

***It's** too bad you **can't** come.*

*(**It is** too bad you **cannot** come.)*

Its is a possessive adjective and never has an apostrophe:

***Its** place was already taken.*

Other words of the same type are **his, her, our, your, their** and **whose.**

***Hers** was already taken.*

Hers is a pronoun denoting relation or possession, as are **his, ours, yours, theirs,** and **whose.** In this case I can understand why it's confusing. Ordinarily you make something possessive by adding an apostrophe and an **s.**

In other instances, however, you do indicate the possessive by adding an apostrophe and an **s.** Different books provide differing guidance on use of apostrophes for forming the possessive. But the following simple rules are quite acceptable and will take care of most needs.

1. If a word does not end in **s,** add an apostrophe and an **s:** girl's, man's, men's, people's.

2. If a singular word ends in **s,** add an apostrophe and an **s:** Lois's, James's, Perkins's.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010011

3. In plural words ending in **s**, add an apostrophe only: girls', boys', wives'.

Which brings me to two common misusages of apostrophes. The first example naturally upsets me because it involves my own name, which happens to end in an **s**. I can't tell you how many times I have received memos with it written this way: [redacted] office." Of course, this changes my name to [redacted] which it is not. A simple "Mrs. [redacted] office" will do nicely, thank you. Or else you can leave off the final **s** and write [redacted] office" instead.

The second example is even wilder. It shows that the writer simply does not know the difference between singular and plural. Some hilarious things can result, of course. The best one I've seen, and I see it every night on the way home, is a sign in front of a housing subdivision which reads: "Settler's Landing." Every time I pass it I think about how lonely that single pilgrim must have been!

¶

Will we ever get **affect** and **effect** sorted out? It's really easy, but lately one so rarely sees or hears these words used correctly.

Affect means "to influence." It is a verb only. *Your answer **affected** (influenced) my thinking.*

Effect means "to bring about or to achieve" as a verb. *This proposal could effect (bring about) some profound changes.* **Effect** means "the result" as a noun. *The **effects** (results) of all this are obvious.*

¶

And what about **lie** and **lay**? **Lie** means to recline; it never has an object. **Lay** means to put, place or set down; it always has an object when referring to present time.

A man can **lie** down to rest, but he must **lay** down his head to do so.

When the action has already taken place, note the past tense of **lie** (whose principal parts are lie, lay, lain):

*A man **lay** down to rest ... and **laid** down his head to do so.*

¶

And then there are quotation marks! Judging by the epidemic use of quotation marks these days, a lot of people are saying a lot of quotable things! But that's not the case, of course. What is happening is that quotation marks are misused for emphasis. One of my favorites is a sign I saw recently which said in large letters:

"NO TRESPASSING"

Now what original wit said that?

In general, if you are not quoting someone directly or giving the title of something, don't use quotation marks.

¶

To conclude, I'll say something about the current misuse of **I** and **me**. It used to be that only uneducated people made mistakes with these two words (and also with she/her, he/him, we/us, they/them). Everyone knew about parts of speech and sentence structure and correctly used **I, she, he, we** and **they** as subjects (the ones taking the action) and **me, her, him, us** and **them** as objects (the ones receiving the action). Nowadays one's ears are assailed daily by misusages from all directions: radio, TV, newspapers ... Just about everyone seems to have jumped aboard this ungrammatical bandwagon. The problem is most acute when the objective case is called for, as here:

*I gave it **to him**.*

*He wrote it **for** my sister and **me**.*

*She told all **of us** about it.*

The problem seems to be those little prepositions **to, for** and **of**. Whenever a preposition is involved, people get tangled up and produce whoppers such as these:

*It was designed **for we** mothers.*

*Jim said it **to her** and I.*

I heard these examples on TV. The second one is puzzling since it is inconsistent in mixing an objective **her** with a subjective **I**. But it is also particularly popular. Whenever there are two people mentioned, the one farthest away from the preposition is usually in an incorrect form.

Is it any wonder that I have about given up on grammar? □

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010011

THE MATTER OF STYLE

J2

P.L. 86-36

A CRYPTOLOG article on writing memos [1st Issue, 1987] prompted me to ask: which letters or memos that pass through the Executive Registry are truly memorable? Not many, and if they are, it's usually for the wrong reason.

Most writers don't think about style. It's hard to explain what style is, much less how to achieve it. What causes a combination of words to leap from the page, to be recalled later? Consider restating this sentence, "These are the times that try men's souls" as "Soulwise, these are trying times." Not quite the same.

Before you can think of style, you must know the principles of English composition. Learn to recognize and use properly the eight parts of speech. Diagram a few sentences for practice. Learn the rules of punctuation, improve your spelling by looking up doubtful words in a good dictionary, and concentrate on the fundamentals of a plain English style.

Brevity will help most to develop or improve style. "OMIT NEEDLESS WORDS" shouts Strunk. He says: "Vigorous writing is concise. A sentence should contain no unnecessary words, a paragraph no unnecessary sentences, for the same reason that a drawing should have no unnecessary lines and a machine no unnecessary parts. This requires not that the writer make all his sentences short, or that he avoid all detail and treat his subjects only in outline, but, that every word tell." What an essay on the nature and beauty of brevity!

Strunk also advises writers to revise and rewrite. Few writers get it right the first time. Have someone else check your work; others can spot your errors much more quickly that you can. To hold your reader's attention, use definite, specific and concrete language. And be clear. There is no substitute for clarity. Ambiguity may amuse, but humor is not the aim--clarity is. □

Solution to NSA-Crostic # 65, 3rd Issue 1987

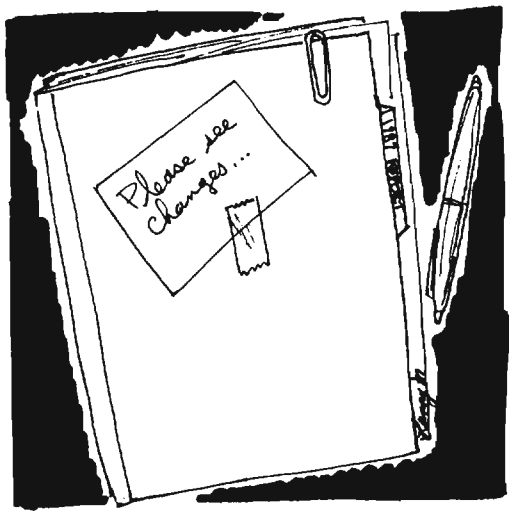
Ronald Reagan, DEDICATION
(Plaque on Ops 2B)

You of the N[ational] S[ecurity] A[gency] are . . . part of a proud tradition, . . . which . . . has its beginnings with George Washington and the American Revolution. And you . . . make history quietly – silently – aware that . . . your greatest victories, if ever known at all, will be divulged only . . . many years from now.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010011

How to Measure Clarity in Writing



[redacted] *R451*

Inspiration for this article came from [redacted] and her article, "How to Write a Memo" [CRYPTOLOG, 1st Issue 1987]. Guideline 4 in her article addressed how to write simply and clearly, and it included some helpful rules. But the article did not explain how to measure the clarity of writing.

I found a simple way to measure the readability of a piece of writing. It's a guideline called the Gunning "Fog Index," first published by Robert Gunning in 1952.

The guidleine does have two minor drawbacks. First, its simplicity results in a measure that is not exact. And second, the index says nothing about the writer's style. However, the value of the guideline's simplicity far outweighs the disadvantages for making it a useful writing aid.

Here are the steps for making the calculation.

1. Using a writing sample that is at least 100 words long, find the average number of words per sentence. Divide the total number of words in the sample by the number of sentences. This gives you the average sentence length.

2. Count the number of words having three syllables or more in a 100 word passage. Don't count: (a) words that are capitalized; (b) combinations of short easy words like "bookkeeper;" or (c) verbs of three syllables whose third syllable is "ed" or "es," as in "created" or "trespasses."

3. Add the results of steps 1 and 2 and multiply by 0.4. This will be the Fog Index. It corresponds roughly with the number of years of schooling a person would require to read a passage with ease and understanding.

Fog Index	Readability
5	fairly easy
7-8	standard
9-11	somewhat difficult
12-15	difficult
17 +	very difficult

(Isn't it interesting that the "standard" level of writing corresponds to the comprehension level of an 8th grade education?)

Sentence length and word complexity are the major factors that determine readability. But don't go overboard while trying to achieve a lower Fog Index. Writing that contains all short sentences with one syllable words would read like a first grade primer.

Again, let me say that the result of the guideline is not precise. But a sample having a Fog Index of 10 certainly will be clearer than one with an index of 15.

Practice using the guideline on the first 8 sentences in this article. You should get a Fog Index of about 8.6.

1. Average sentence length is 13.5.
2. Number of words equal to or greater than three syllables is 8.
3. Fog Index is $(13.5+8) \times 0.4 = 8.6$.

Don't skip over this part; go back and do it!

Now try the Gunning Fog Index on some of your own writing; you may be surprised at the results. Is your writing too complicated for others to understand? Perhaps you can improve it by breaking those long sentences into two separate thoughts? Substituting simple words for long ones should help, too.

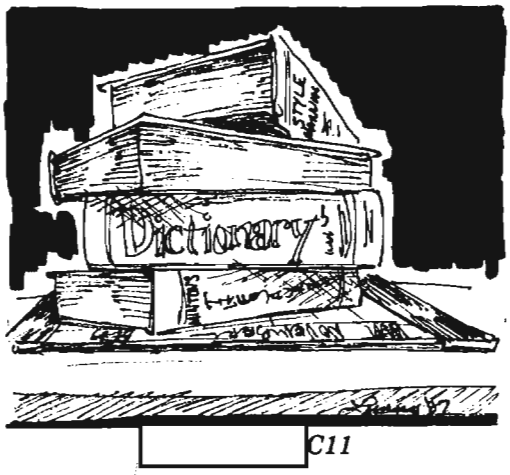
How does your writing measure up? □

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010011

Two Tips on Writing



¶

Two common abbreviations that are often misused are "i.e." and "e.g." They are especially nagging since you may not even find them in your desktop dictionary. Most people know that one of them (i.e., as it turns out) means "that is" and the other (e.g.) means "for example." The problem is remembering which is which. The result of guessing wrong is that you may say "that is" and give an example (or series of examples) instead of an explanation, or vice versa. If you don't mean for your list to be exhaustive, be sure to say "for example" (e.g.). On the other hand, if you mean to explain or amplify, use i.e.

How to tell the difference? The easy way is to remember the expansion of one of them: i.e. stands for the Latin expression *id est*, which means *it is* or "that is." Even if you didn't study Latin or a Romance language, this one should be easy to remember. Id and est look enough like "it" and "is" to give you a hint. By the way, Freud used the Latin *id* when he came up with his terminology. Of course, if you prefer, you can remember the expansion of e.g., which is *exemplia gratia*.

Examples:

> "The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system." [Files and programs are two examples among several possibilities for named objects.]
>
> "Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity." [Passwords are among several possible mechanisms.]
>
> "When the TCB exports an object to a mutilevel I/O device, the sensitivity label associated with the object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., "machine-readable" or "human-readable form)." ["Machine-readable" and "human-readable" explain what is meant by the same form; they are not examples of several kinds of same form.]

Note the form of the abbreviations: a period follows each letter, but there is no space between the first period and the second letter. A comma typically follows the abbreviation.

¶

Does a sentence-ending period precede or follow the parenthesis or quotation mark? This is the *bête noire* of many of us. When a period is used next to a parenthesis, the rule is completely logical: if the parenthetical expression is PART of a sentence, the period follows it. If the parenthetical expression CONTAINS the sentence, the period precedes the final parenthesis.

When a quotation occurs as the last element of a sentence, the rule differs. Even though the quotation is completely within the sentence, the period precedes the final quotation mark. The reason for this is that typographers feared that the little period would be lost if it fell completely outside the sentence. For the same reason, a comma is placed within the quotation marks. An exception is made for technical text, wherein a distinction must be made between "period—quotation mark" and "quotation mark—period."

Examples:

> The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on the any other subject (unless restrained by mandatory access control).
>
> (See the Convert Channel Guideline section.)
>
> Any discussion of computer security necessarily starts from a statement of requirements, i.e., what it really means to call a computer system "secure."
>
> The result of executing "substr (alph, 3,5)" is "abc". [If the period preceded the hyphen, the result would be interpreted as "abc.", which is incorrect.] □

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

DOCID: 4010011

P.L. 86-36

Pointers on Grammar

[redacted] P12

P.L. 86-36

The article on memos by [redacted] impelled me to pass on some pointers on grammar that readers might find helpful.

About hyphenation

My grammar teacher gave us a rule about hyphenation that works:

- If the sentence makes sense using each of the modifiers separately, don't hyphenate. Example: "We have a large red barn." It makes sense to say, "We have a red barn" and it also makes sense to say "We have a large barn." So we don't hyphenate.

- If the sentence doesn't make sense using each of the modifiers separately, hyphenate. Example: "He had a broken-down car." You might say "He had a broken car," but you wouldn't say, "He had a down car."

Misuse of quotes

My biggest pet peeve with regard to grammar is the misuse of quotes, especially partial quotes. The rule is, almost always, that commas and final periods go inside quotation marks. Other punctuation marks should be placed inside the quotation marks only if they are a part of the matter quoted. Here are some correct examples:

Call it a "gentlemen's agreement."

Why call it a "gentlemen's agreement"?

"Change 'cat' to read 'dog'."

One reason why many NSAers misuse partial quotes is that they subconsciously follow British usage, which is to put quotes inside the period or comma. That's understandable. What isn't understandable is the inconsistency; many memos have it both ways -- sometimes in, sometimes out.

The reason isn't *because*

"The reason is because" is incorrect because the verb is requires an adjective or noun clause following. The correct form is: *the reason is that . . . The reason why . . . is.*

It's not "kind of a"

People say, "I like that kind of a meal." when they should say, "I like that kind of meal." Use of the indefinite article a limits the field to one thing. In this case, there is only one thing to choose from meal, not a class of things.

It's not "very unique"

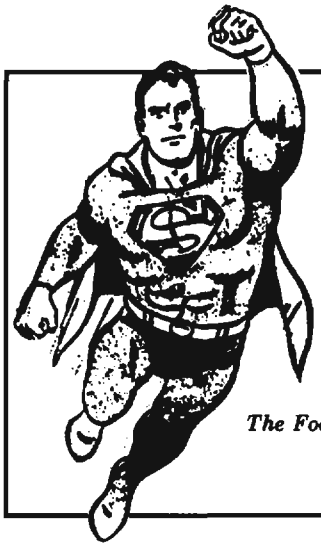
When people say, "I had a very unique experience," they are probably confusing *unique* with *unusual.* Unique means one of a kind. It is an absolute that cannot be qualified.

Editor's Note:

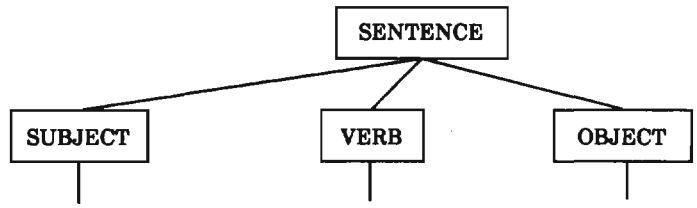
Discussion on writing in these pages is now closed. We refer readers to the many works on grammar, usage, and style that can be found in libraries and bookstores. We will, however, consider articles on SIGINT terminology and usage.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010011



THE HERO OF THE SENTENCE



Extract from: *Getting Your Ideas Across Through Writing,* Training Manual No. 7, 1950. US Department of Health, Education and Welfare.

The hero of the sentence is the "hero" of the story that each sentence tells. The "subject" is what the story's about. For some strange reason, we often pick the wrong hero, as in this sentence:

> The function of the Food and Drug Administration is the enforcement of statutes to insure the honesty and purity of foods, drugs, devices and cosmetics. (This is the opening sentence of a pamphlet.)

Who cares to read a story about a "function"! The Food and Drug Administration is the hero of this story, so let's make it the subject: *"The Food and Drug Administration"* (Let's make the verb work, too.) *"enforces five statutes . . . "*

Of course we cannot take time to fiddle that way with each sentence. Many of us need to change our habits, however, because we habitually go out of our way to select the wrong subject. People like to read about people and concrete things; yet often we twist the sentence around so that the story appears to be about an abstraction.

Most of all, people like to read about people. Yet readers of Government writing must get the impression that no human beings exist, anywhere. Our sentences tell stories about functions, policies, grants, conditions, factors, abstract ideas, and "it" – especially "it." Everything but people. *Ours are programs for people, administered by people,* yet often we write like this:

> *Employment* in manufacturing recorded increases, while there were declines in trade and domestic service. (The *number of people* working in manufacturing increased, while the number in trade and domestic service decreased.)

When we do admit that people exist, we often treat them as mere appendages to abstract ideas. Sometimes we seem to go out of our way to keep from making them the subject of our sentences, like this:

> The *protection* afforded industrial workers is far from complete. (Many *industrial workers* are inadequately protected.)
>
> *General Assistance or relief* accounted for nearly all the remaining recipients of public aid. (Nearly all the other *people* getting public aid were receiving general assistance or relief.)

Here are some more sentences in which the real "hero" has been subordinated. Just to focus your attention on the advantages of keeping people and relatively concrete things as the subjects, you may want to revise these sentences. You can make the verbs work more effectively, too.

> Responsibility for satisfactory working relationships within their organizational units rests with operating supervisors.
>
> Refusal of employment of women workers is common on the part of employers.
>
> There has been much opposition to the measure on the part of the educators. □

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010011

Gimme Rewrite!

Va.

This is a note to prospective contributors and to others who might have to write at NSA.

We hope that the articles on good writing in this issue do not discourage you from contributing because you're afraid of making one of the errors mentioned. As writing errors go, most of the ones touched on are minor lapses which are taken care of by the copy editor.

Self-respecting publishers of books, magazines, and newspapers all have copy editors as a matter of course. In many newspapers this tedious job is assigned to the reporter most recently hired . . . a lesson in humility.

The usual sequence of preparation for books and periodicals, including newspapers, is:

- § text editing;
- § copy editing;
- § proofreading.

Each should done by a different person. (In CRYPTOLOG, a low-budget rag, the Editor merely changes hats.)

The point that the authors of the articles are making is that the finished product should not contain such errors. They detract from and tend to cast doubt on the substance. Think of it as good grooming. However elegant and stylish your clothes may be, spots and tears are what people will notice, not the couturier styling or bespoke tailoring.

What to do?

At a minimum, have someone else do your copy editing and your proofreading. (It is well known that you cannot do either for yourself because you tend to see what you expect to see.) But it's still better to hand over your bit of writing, along with sharp blue pencils, to at least one other person to edit for clarity. (And preferably, that person should come from the population of the intended reader.) This is what experienced writers do, and often, they expect their text to undergo changes in each of several passes by different individuals.

The wider the distribution of the document, the longer its life, the greater the care that you must give to preparation.

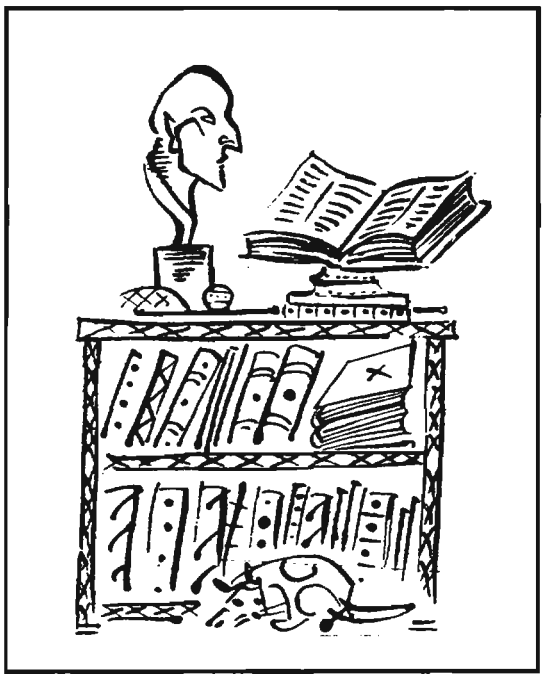
If you're doing any writing at all in this Agency, you should have at your desk some good references on grammar, usage, and editing. Order a desk copy for yourself. Browse in libraries and bookstores to determine which ones best suit your needs. Don't overlook handbooks for college students – some of them could have been written specifically for NSA!

Practice editing – a good way to begin. Try your hand at editing or rewriting an awkward passage, one that you had to reread to understand. Practice writing. A good exercise in writing clearly is writing up a suggestion.

Hardest of all, practice editing and rewriting your own text. Set it aside overnight, or a week, or a month, then read it cold. Now what do you see? □

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010011



Machine Translation: Past, Present, and Future. by W. J. Hutchins, University of East Anglia. Ellis Horwood Limited, Chichester, 1986 (distributed by Halsted Press, a division of John Wiley & Sons) [P 308 .H85]

Reviewed by: [redacted] *P12*

This book lives up to its comprehensive title. The "past" begins even before the 1948 memorandum by Weaver, from which all machine translation projects have sprung directly or indirectly, with a discussion of 17th-century numerical codes as universal languages, and a 1933 Soviet patent which went nowhere.

Weaver's memorandum justified the concept of machine translation in four ways, one of which will be of special interest to readers of CRYPTOLOG. During the war, a cryptanalyst had deciphered a Turkish message without knowing any Turkish. Weaver verified that this incident had actually happened. Hutchins explains that the relative frequencies of letters, digraphs, and so forth, are sufficiently similar in English and Turkish to have enabled the cryptanalyst to succeed. Weaver was mistaken, but in no way does that vitiate the concept of machine translation.

Hutchins points out that some prefer the term "computer translation" to machine translation, or MT, but declines to part with tradition.

He then surveys all, or so it seems, the MT systems for which information is available. His account of the Georgetown MT project was of particular interest to me, since it covers ground that I became aware of while a student there. His account is accurate, and it contains many details about the various approaches tried, and gives samples of the output produced. Included also are wryly humorous anecdotes about the rivalries that developed. His accounts of other MT approaches are similar.

Then came the infamous ALPAC (Automatic Language Processing Advisory Committee) report, which all but ended funding of MT projects in this country. Hutchins systematically demolishes the premises and methodologies of this report.

He then turns to the modern, or post-ALPAC, era of machine translation, describing a wide variety of projects and their applications in places such as Oak Ridge. Many statements in the ALPAC report and elsewhere ring hollow in the face of successes for MT in actual use.

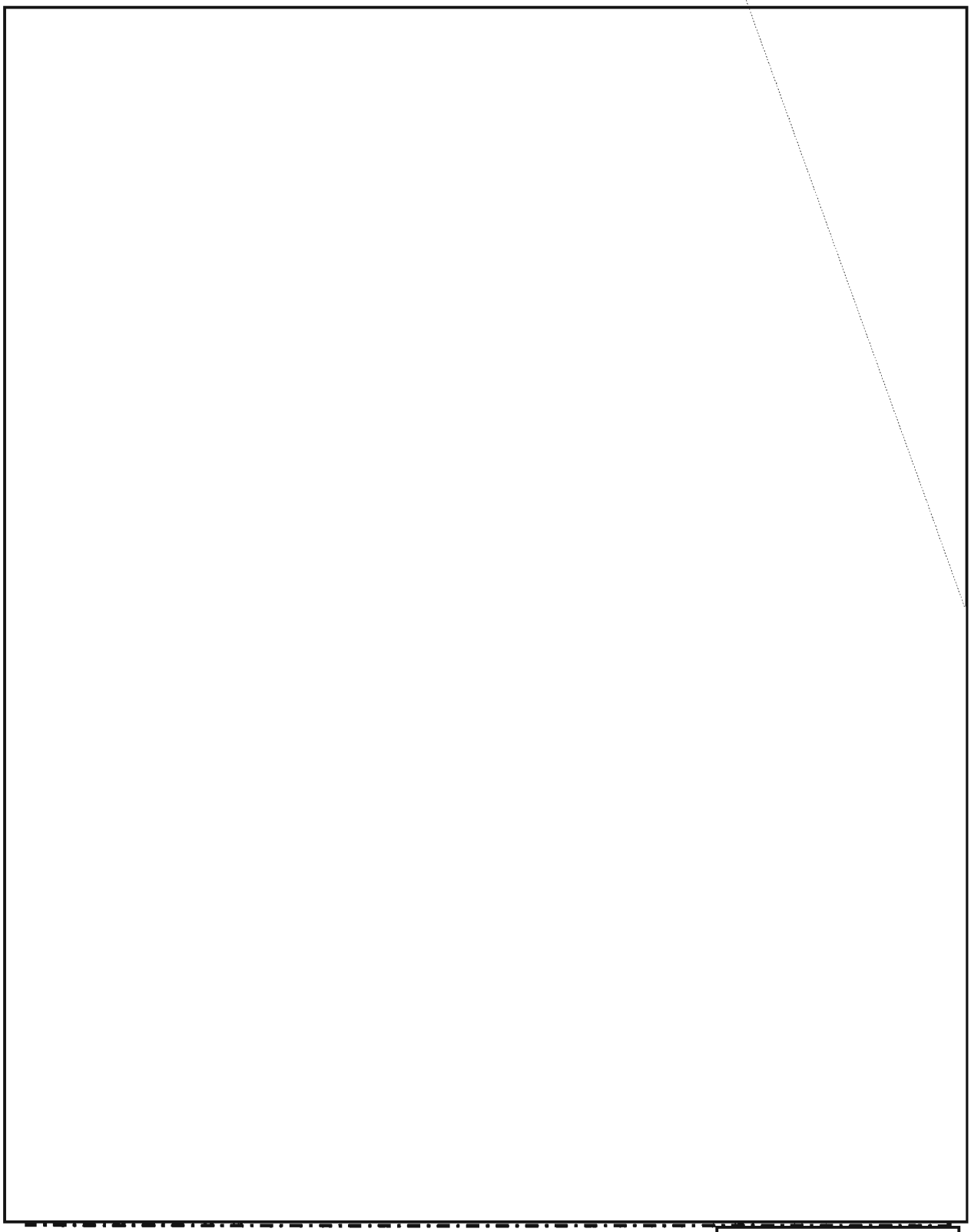
A chapter on Artificial Intelligence approaches to MT concludes with the curious observation that its "feasibility in full-scale MT must, however, remain doubtful," eerily reminiscent of earlier dismissals of MT as a whole that the author himself has shown to be unfounded.

Although there are many translation applications for which MT is inappropriate, Hutchins's survey justifies his concluding remarks: "the future of MT is secure: it satisfies a genuine urgent need, it is the subject of worldwide research and development, and it is becoming a commercial product like other technical aids and office equipment; the application of the computer to translation is a reality, for many it is already as much a part of life as the computer itself." □

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

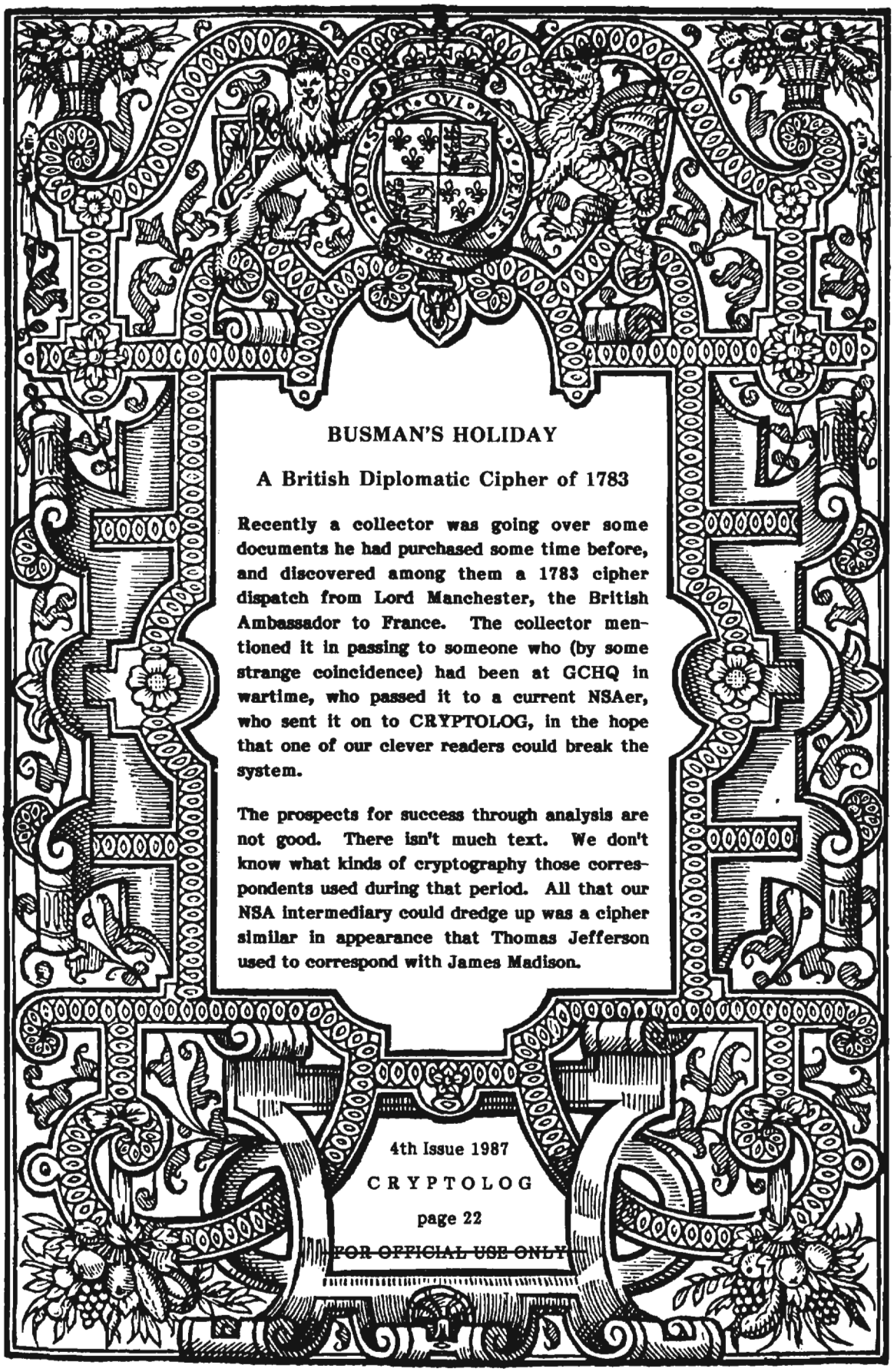
FROM THE PAST (U)



Provided by:

P.L. 86-36

DOCID: 4010011



BUSMAN'S HOLIDAY

A British Diplomatic Cipher of 1783

Recently a collector was going over some documents he had purchased some time before, and discovered among them a 1783 cipher dispatch from Lord Manchester, the British Ambassador to France. The collector mentioned it in passing to someone who (by some strange coincidence) had been at GCHQ in wartime, who passed it to a current NSAer, who sent it on to CRYPTOLOG, in the hope that one of our clever readers could break the system.

The prospects for success through analysis are not good. There isn't much text. We don't know what kinds of cryptography those correspondents used during that period. All that our NSA intermediary could dredge up was a cipher similar in appearance that Thomas Jefferson used to correspond with James Madison.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010011

THOMAS JEFFERSON PAPERS, UNIVERSITY OF VIRGINIA LIBRARY

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010011

The British Cipher of 1783

Fontainbleau 8br 20. 1783

Sir,

I received your Letter dated Septr 2. and should not have delayed so long sending an answer to it, had I any thing very material to communicate. 3693. 2517. 65. 3423. 576. 1100.
97. 1765. 3000. 259. 3032. 57. 66. 1795. 19. 211.
46. 1038. 1637. 970. 2609. 3369. 696. 3696. 427. 118.
3364. 1362. 456. 111. 566. 77. 1551. 2961. 1504. 1437.
3560. 1453. 2053. 1555. 1834. 1406. 9. 2044. 2694.
3423. 678. 1359. 493. 809. 1094. 956. 636. 1618. 61.
1437. 1369. 2316. 497. 314. 684. 1205. 193. 685. 2072.
65. 39. 3459. 3937. 2108. 2615. 1359. 766. 2450. 880. 1291.
647. 3339. 1175. 3714. 809. 184. 564. 2101. 1581. 566. 2323.
2066. 823. 665. 2401. 1692. 3560. 1444. 2734. 970. 830.
3601. 3263. 1612. 3000. 1291. 2000. 1936. 3056. 3278. 1618.
2894. 3438. 233. 2424. 3137. 3928. 1501. 3364. 434. 492.
566. 1498. 2450. 3560. 1603. 3905. 3082. 1504. 1242.
1624. 987. 2615. 1306. 350. 1245. 1504. 1145. 9. 3658.

Sr John Stepney &c. &c. &c.

2622.

~~FOR OFFICIAL USE ONLY~~

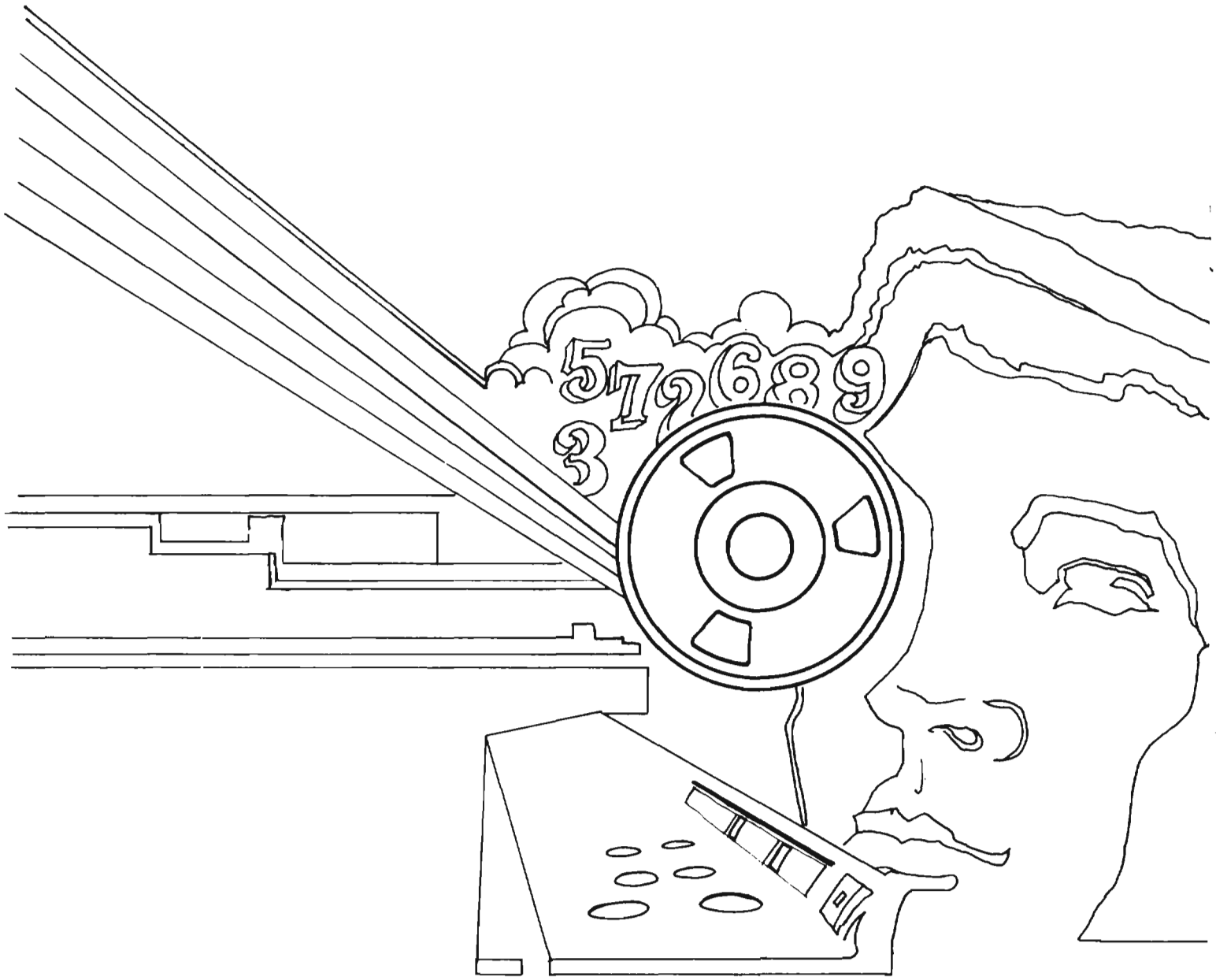
DOCID: 4010011

2622. 122. 3901. 1350. 758. 1986. 3905. 2426. 2051. 3791.
678. 498. 2109. 3438. 3536. 3487. 2999. 2694. 3892.
3056. 1350. 1397. 2985. 1778. 1719. 3739. 1753. 2126.
566. 77. . 956. 3000. 56. 9. 576. 3006. 10.

The Court is now at Fontainbleau where it is said it is to remain till late in November notwithstanding the Pregnancy of the Queen.

I am
Sir,
With great regard.
Your Most Obedient
Humble Servant
Manchester

~~FOR OFFICIAL USE ONLY~~


5 7 9 6 8 9
3

DOCID: 4019711

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

3rd Issue, 1987

ON THE CONSTITUTION . . . . . [redacted] . . . 1
GOLDEN OLDIE. 2
IS PACKET RADIO ALIVE AND WELL ON HF? . . . . . [redacted] . . 3
BIG LOOK. . . . . [redacted] . . . 5
THE JOYS OF US GOVERNMENT TRAVEL. . . . . [redacted] . . . 8
BULLETIN BOARD. 13
A ROPE BY ANY OTHER NAME. . . . . [redacted] . . 14
ODE TO STONEHOUSE . . . . . [redacted] . 15
CRYSCOM . . . . . [redacted] . 20
LETTERS ON PC USERS' MANUALS. 21
SAMPLE PAGES OF PC USERS' MANUALS . . . . . [redacted] . . . 23
REQUIREMENTS FOR A GOOD SET OF DIRECTIONS 25
BOOK REVIEWS: HER MAJESTY'S SECRET SERVICE. . . Vera Filby. . . . 27
TELECONFERENCING. . . . . [redacted] . 30
FROM THE PAST 31
NSA-CROSTIC No. 65. . . . . [redacted] . . . 32

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019711

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XIV, No. 3 ..... 3rd Issue 1987

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Collection ..... (963-5877)
Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Cryptolinguistics ..... (963-1596)
Index ..... (859-4351b)
Information Science ..... (963-3456)
Information Security ..... George F. Jelen (859-1211b)
Intelligence Research ..... (963-3845)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (963-4958)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-4351)

Illustrators ..... (963-3490)
..... (963-6211)
..... (963-5248)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five)
(note: no 'o')

Always include your full name, organization, and secure phone; also building and room numbers.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, HQS 8A187
Please do not phone.

Contents of CRYPTOLOG should not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

THE 200th ANNIVERSARY

P.L. 86-36

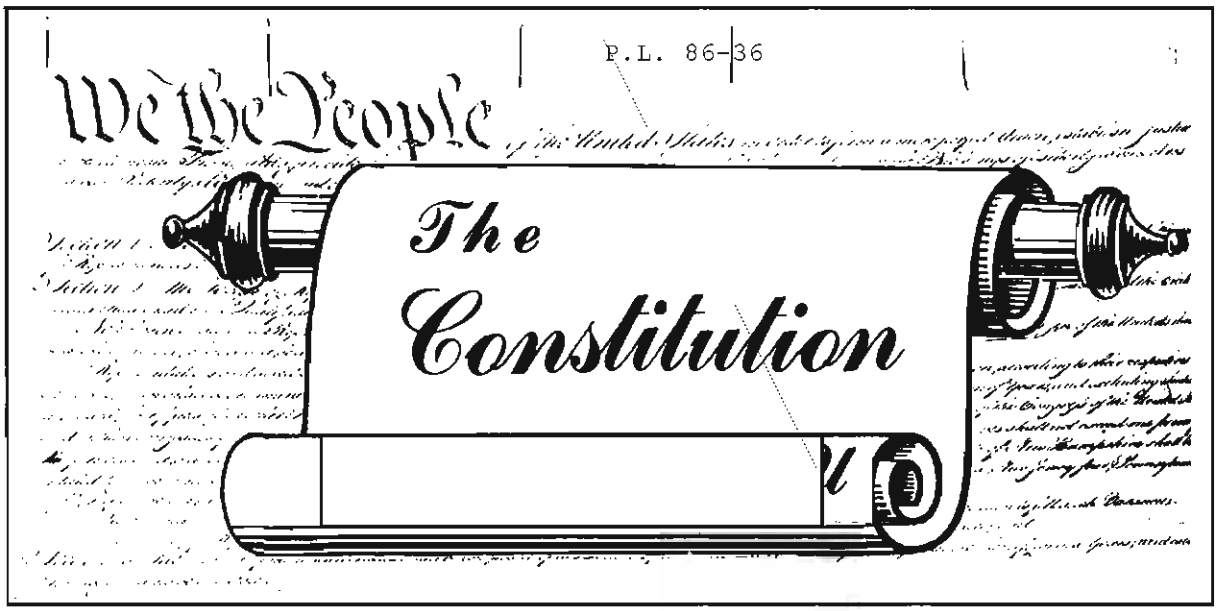
The bicentennial of the Constitution is an occasion for celebration. We rejoice in its sturdiness and flexibility. It is also an occasion for contemplation. This elegant document is as much the result of a bureacratic process, of negotiation and compromise, as of philosophy.

Thanks to the media, – radio, TV, magazines, newspapers – who provided "daily coverage" this summer as if it were 200 years ago, we were able to observe this process. The key issue then was the power of the central government. We know this not from an m/r attached to the document, but from the minutes, letters, and notes of the delegates. We know, too, that many delegates who participated in this process foresaw that certain compromises were bound to have unhappy consequences for the country some time in the future. But they voted as they did, albeit reluctantly, because they believed that it would be worse for the nation not to.

The key constitutional issue in 1987 is the balanced budget amendment. In commemoration of the bicentennial, we present an essay on this subject by an NSAer. His views, as you will see, are in part shaped by philosophy, and in part derived from first-hand experience with the bureaucratic process.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019711



The national commemoration of the bicentennial of the U.S. Constitution has evoked considerable study and reflection on this great document and the ordered scheme of government it provides. Thus, there is no small irony in the fundamental misperception of the role and purpose of the Constitution displayed by supporters of a balanced budget amendment.

The U.S. Constitution was the product of an effort that found its original purpose in the need to alter the existing Articles of Confederation to provide for a more stable and effective form of government for the newly independent, loosely united former colonies of Great Britain. The demonstrable defects in the Articles of Confederation led the convention assembled in the summer of 1787 to produce a new governmental charter that allocated power between the newly created branches of the national government, redefined the distribution of power between the national and state governments, and established certain limits on the exercise of governmental authority with regard to the national constituency - the people themselves. The subsequent amendments to the Constitution have served as refinements to this basic organizational scheme without disrupting the principal purpose of the document: to allocate the division of power among the federal government components, the states, and the people.

In considering the call for a constitutional amendment mandating a balanced budget, the question arises as to what constitutional defect or omission requires this remedy. Is there a fundamental flaw in the governmental allocation of power that has produced this national fiscal crisis? Is the problem linked to a misalignment between the authorities conferred on the government and the rights reserved to the people?

The answer to both these questions is, of course, emphatically in the negative. Article I of the Constitution provides the Congress with all requisite authority to conduct and manage the fiscal affairs of the national government. The powers conferred in this Article represent a marked departure from the authority provided in the Articles of Confederation in recognition that the national government must necessarily be imbued with unconfined authority in respect to all those objects which are entrusted to its management.

What then is the purpose of a constitutionally mandated balance budget? Stripped of surrounding rhetoric, the purpose is simply one of imposing some sort of constitutionally based wisdom on the prudence with which Congress exercises its fiscal powers. "Wisdom" is of course an abstract term

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019711

susceptible of varied interpretations: what appears wise at one moment may seem foolish the next. Whether or not Congress is collectively exhibiting the requisite "wisdom" in exercising its fiscal powers is a function of the legislative prudence of its individual members.

Undisputably, Congress has all the necessary authority to produce a balanced budget now, without need for any constitutional tinkering. Its failure to do so is not the product of any constitutional deficiency; it is the result of a continuing series of collective legislative judgments on the exercise of Congress' fiscal authority. If those judgments are now seen as imprudent, the Constitution already provides the remedy: popular election of the congressional membership.

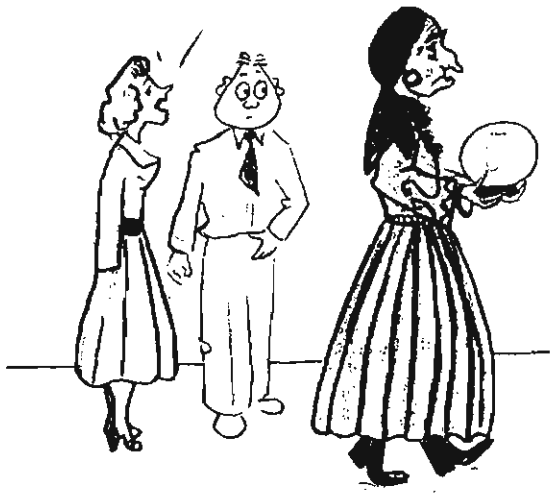
Advocates of a balanced budget amendment apparently misunderstand the role the Constitution plays in the performance of government. The Framers' intent was to ensure that the national government was provided with the means necessary to accomplish the ends entrusted to it. The wisdom with which any particular Congress exercises its constitutionally conferred powers is not a constitutional issue; it is a political one. Before the quintessentially political issue of proper fiscal policy is misguidedly framed as a constitutional one, all parties would be wise to recall Alexander Hamilton's admonition in Federalist No. 25:

> Wise politicians will be cautious about fettering the government with restrictions that cannot be observed, because they know that every breach of the fundamental laws, though dictated by necessity, impairs that sacred reverence which ought to be maintained in the breast of rulers towards the constitution of a country, and forms a precedent for other breaches where the same plea of necessity does not exist, or is less urgent and palpable.

In drafting the Constitution, the Framers wisely avoided shortsighted "fixes" designed to remedy problems endemic to their time because they realized they were creating a covenant that was to endure through the changing times of the future. Similar prudence should be exhibited now if we are retain any hope that the Constitution as we know it is to survive to its tricentennial. □

GOLDEN OLDIE

ARLINGTON HALL, c1955

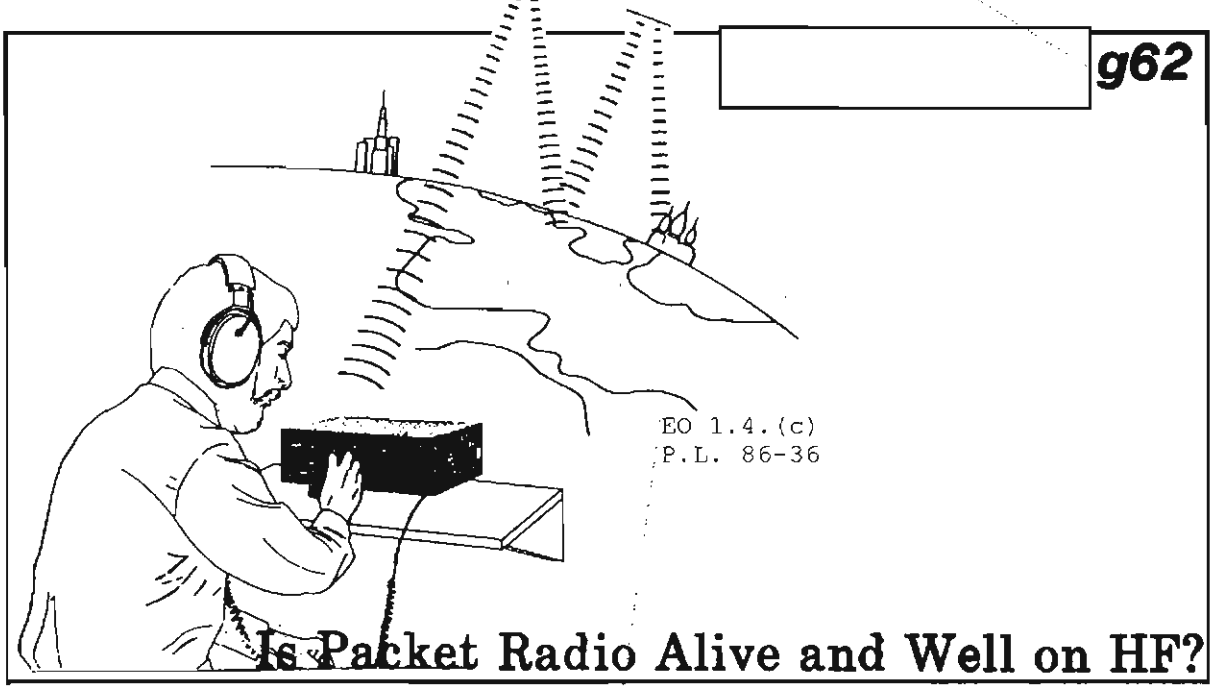


SHE'S CRACKED TWO SYSTEMS ALREADY!

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019711

P.L. 86-36



EO 1.4.(c)
P.L. 86-36

Is Packet Radio Alive and Well on HF?

(U) Packet is inexpensive! Figure 1 lists, as of August 1986, several terminal node controllers (TNCs) which are available to anyone. (Is the only market the amateur - the ham - radio operators?) These TNCs are the link between the only two other components needed for a packet system - almost any computer and almost any radio capable of transmitting voice communications. Not only are these units inexpensive, they are seemingly exempt from export controls, as anyone can buy one with no questions asked, simply by paying. You don't even to show the salesman your amateur radio license.

~~(FOUO)~~ Packet is error-free! According to the AX.25 protocol, packet can, in theory, provide virtually error-free communications. In actuality, an error may slip in every few years! Although the transmission speed common in amateur radio circles is 300 baud on HF (1200 baud on VHF and above, and 2400 is being experimented with) the actual speed is considerably less. In many applications where accuracy is a must, this is not too high a price to pay.

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
DOCID: 4019716

[redacted]

(U) This operation would be very similar to telephone bulletin board systems for owners of home computers. This sort of operation is being done everyday by ham radio operators. As a matter of fact, the amateur radio operator community has developed packet operation – file (message) up/downloading, store and forward message handling, dual-port (i.e., "in" on VHF or UHF and "out" on HF or vice versa) operation. A side benefit of this type of communications would be reduced training for military radio operators, eliminating the need for 5 to 10 weeks of morse code training. Additionally, much of packet technology is available in open-source materials and is documented in many ham radio journals.

[redacted]

Countries or Regions with Amateur Radio Packet Operations

Argentina
Australia
Austria
Belgium
Brazil
Canada
Cayman Islands
Chile
Colombia
Costa Rica
Denmark
Dominican Republic
Ecuador
England, U.K
Finland
France
Greenland
Guatemala
Guernsey Islands, U.K.
Haiti
Hungary
Indonesia
Italy
Japan
Jersey Islands, U.K
Kiribati
Kuwait
Luxembourg
Mexico
Montserrat
Morocco
Netherlands
Netherlands Antilles
New Zealand
Nicaragua
Northern Ireland, U.K.
Norway
Panama
Philippines
Portugal
Scotland, U.K.
Singapore
South Africa
Spain
Sudan
Swaziland
Sweden
Switzerland
Tanzania
Togo
United States
Vanuatu
Venezuela
Wales, U.K.
West Germany
West Malaysia/Sabah/Sarawak

P.L. 86-36
EO 1.4.(c)

FIGURE 2

DOCID: 4019711

[redacted] P16

P.L. 86-36

BIG LOOK

⇒*Since this article does not lend itself to portion marking, it is classified ~~TSC~~ in its entirety.*⇐

During the Vietnam War, SIGINT elements in the Vietnam area were tasked with identifying and locating sites from which the North Vietnamese were destroying US aircraft with Surface-to-Air Missiles (SAMs). The following is a sketch from memory of the US Navy approach to solving the problem.

Working separately, COMINT elements were able to follow North Vietnamese tracking of US aircraft, and succeeded in intercepting readiness and firing commands [redacted] so they could not locate the site that was preparing to fire quickly enough to destroy it. The usual analytic methods to determine position did not work because the Vietnamese moved missiles and crews from site to site overnight, as often as three or more times per week. Meanwhile, the ELINT elements were able to locate the FANSONG radars, but they had no way of knowing which SAM site they supported, or whether the operation was calibration, practice, or launch preparation.

The problem became acute when the Soviet advisors and the North Vietnames missile crews modified their procedures so that instead of tuning and calibrating their FANSONG radars at normal power, they used very low power, coming up to normal power only when a designated target was passed on to them to track and destroy. Thus our ELINT elements had no time to locate the FANSONG before a missile was already on the way.

At about that time, (early 1960's) electronic engineers attached to Fleet Air Reconnaissance Squadron One (VQ-1) devised two independent radar intercept systems, BIG LOOK and BRIGAND, that greatly improved our ability to locate radars. Used together, they were to help us solve the problem. The two systems were mounted in a modified EC121 airframe and sent to Danang, South Vietnam, for a trial. It proved successful enough to warrant expansion of the effort. At its peak, the effort provided continuous coverage whenever US strikes were made in the Eastern part of North Vietnam, using four platform aircraft and some 100 crew members each day.

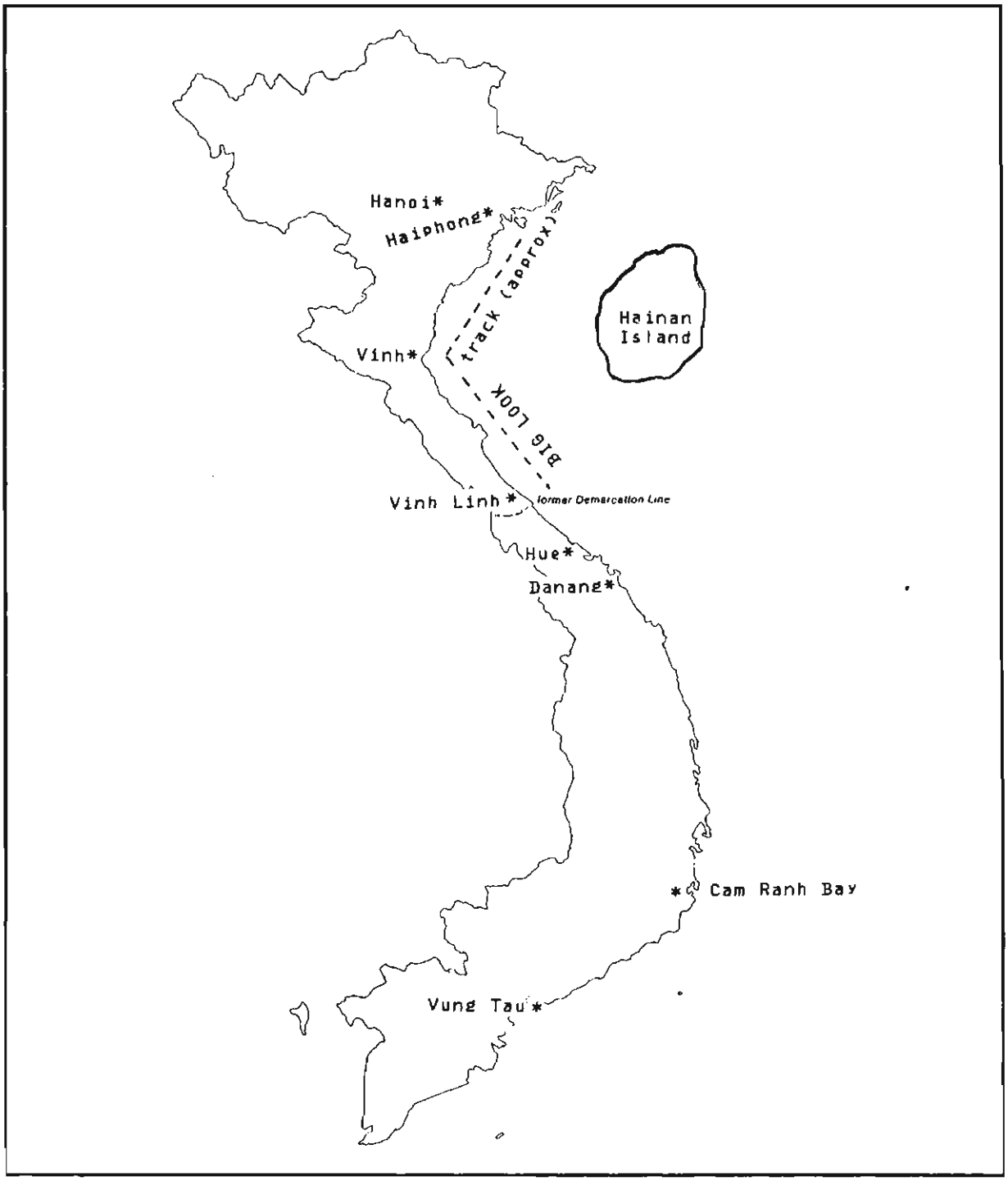
The project itself was given the covername BIG LOOK. It was assigned the mission of interception, identification, and location of North Vietnamese SAM emplacements as targets for strike elements, and of providing warning to those strike elements of impending launches of missiles against them.

Development of the BIG LOOK equipment made it possible for ELINT evaluators to get a position

EO 1.4.(c)
P.L. 86-36

on the FANSONG radar before it was up in the tracking mode and able to endanger US strike aircraft. BRIGAND was tricky to work with, but its capability to lock onto the rotation of a radar such as SPOON REST and position it with an accuracy sufficient to strike it after only one successful intercept made it worth all of the problems it engendered.

The primary problem was calibrating BRIGAND to the tolerances necessary to provide accurate fixes. Unfortunately, that accuracy was achieved only occasionally. A second problem was the high power requirement for both BRIGAND and BIG LOOK. Overheated wiring was very common, and it was not unusual for a platform to have several electrical fires while



EXPLANATORY NOTES

BIG LOOK. US radar intercept receiver coupled to an antenna with an oversized reflector, giving the system enough sensitivity to detect a radar emitting at very low power.

BRIGAND. US radar intercept receiver modified to have the ability to lock onto the sweep of a target radar and to present an offset representation of the return of the target radar.

DUMMY LOAD. Mode used used by the Viet Cong (or Soviet advisors) in warming up and calibrating the FANSONG radar to avoid detection until it initiated actual target tracking/missile guidance operation.

EC121M. The BIGLOOK platform aircraft. A modification of the C121, also known as the Lockheed Constellation.

FANSONG. Target tracking and missile guidance radar for the Soviet SA-2 missile that was widely used in Viet Nam.

SPOON REST. An air search radar used by North Vietnamese air defense forces.

airborne during any one deployment. A third problem was training ELINT evaluators to the level required to make accurate fixes, and keeping them on after they attained that experience.

The ELINT side of BIG LOOK was composed of BIG LOOK and BRIGAND. The COMINT side had four voice and two morse intercept operators, along with a teletype operator and the COMINT evaluator. The COMINT detachment officer in charge, Vietnamese linguists, and some others were drawn from USN-27 at San Miguel, [redacted] All were detailed for periods of three to six months to VQ-1, until late in 1968, when they were detailed to the Navy COMINT actvity at Danang. The aircraft, flight, and ELINT crews were drawn from VQ-1 elements at the [redacted] for a deployment period nominally of six weeks.

Intelligence support to BIG LOOK included US strike schedules which were received on a daily basis and briefed to aircrews before takeoff. On-board secure teletype provided schedule changes or additions. This permitted the COMINT evaluator to concentrate attention to scheduled air strikes.

Flights were eight hours long. One hour was allowed on each end for transit from Danang to home station and return. Most flights were conducted at five thousand feet above and parallel to, and some ten to fifteen miles to seaward of, the North Vietnamese coast between about 17°30′ North and 20°15′ North (or, between Vinh Linh and Nam Binh, North Vietnam).

Once airborne, the COMINT evaluator was passed morse and voice intercept of North Vietnamese air defense tracking of strike aircraft, and was alerted by voice operators who were listening to the air defense voice net when a missile launch was imminent. Then the COMINT evaluator alerted the warning officer, who coordinated with the ELINT evaluator to get a position on the FANSONG as soon as it began active tracking, and issued a voice warning to strike aircraft in the area. Interaction between COMINT and ELINT evaluators was necessary, since the ELINT side could provide DF on a radar, and the COMINT side could follow readiness and intent. When the system worked, that is, when BIG LOOK intercepted a FANSONG as it came up in guidance mode just after a SAM site was ordered to fire, then a valid warning could be broadcast for that area. Warning was based on a US grid system that was defined into segments small enough to be useful, and yet simple to use and understand quickly.

After a flight was completed, all SIGINT was fused by the evaluators and analysts into a report designed to provide strike information to the strike forces and intelligence information to the community as a whole.

The strike pilots and the commanders of strike units were most appreciative for the warnings provided by the crew members of the airborne platforms. This gave them a great deal of job satisfaction, and somewhat offset the effects of conditions under which they performed their tasks. □

EO 1.4.(c)
P.L. 86-36

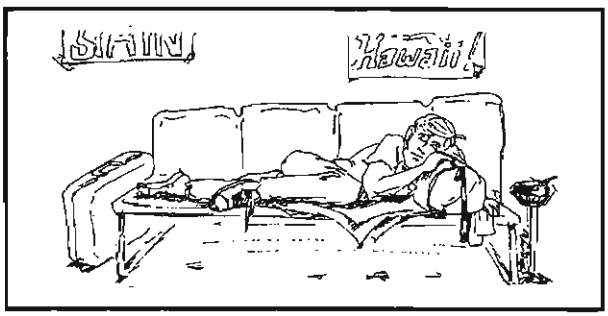
The Joys of US Government Travel

[redacted] G53

This article is classified ~~CONFIDENTIAL~~ in its entirety because of the sites visited.

As many story tellers would say, Once upon a time there was a young man who at the age of 20 decided to join the Air Force. I was this young fellow and I had lived all of my life in West Virginia with only brief trips to the five surrounding states and the District of Columbia. My longest plane or train trip at that time had been between Washington, D.C. and Charleston, West Virginia. As a small-town boy, I was looking forward to some worldly travels in the Air Force.

My first trip was from Charleston, West Virginia to San Antonio, Texas with a number of stops in between. Had I been a bit wiser at that time, I would have suspected that my travel horoscope was on a very interesting track. This flight was not scheduled to be on the ground anywhere for more than a few minutes before arriving in Texas. But for this traveling novice and his new companions, there was a 15-hour delay in New Orleans where I was without money or a place to sleep: somehow our plane arrived too late to connect with the onward flight to Texas. At the age of twenty, the solution for this problem was simple - find a comfortable seat some place in the airport and call that my bed for the night.



The next Air Force-sponsored trip was from Charleston, West Virginia to San Francisco, California. All was going well on this one-stop (Chicago) trip, when suddenly the plane lost cabin pressure over the Rocky Mountains, within sight of Mt. Whitney. A number of older people on this flight experienced breathing problems; many blacked out from the lack of oxygen. The pilot of the aircraft immediately turned back from the mountains and "hit the deck" (went to a lower altitude). Breathing was considerably easier at the lower altitude, but many of the older passengers continued to have problems. We were met at the Albuquerque airport by a number of ambulances with their lights flashing. After dispatching several of the passengers and having some repairs made to the aircraft, we were once again on our way to San Francisco to meet an onward flight to Japan.

When returning to the US from Japan some eighteen months later, I was once again faced with a day-long (propeller driven aircraft) flight to the States. The first stop on this flight, Wake Island, was reached without difficulty. The second part of this trip found us midway between Wake Island and Hawaii in a storm. This storm was a real roller coaster which eventually cost us two engines on a four-engine aircraft. The pilot announced at that time that we were "past the point of no return," which I soon learned was a point where there wasn't enough fuel to return to Wake Island and that our only reachable destination was Hawaii. Again we hit the deck for a very slow and bumpy ride to Hawaii, where we were met by fire engines and ambulances.

I have been told that there is often something good in something bad; this stop in Hawaii was no exception. We were housed at no expense to ourselves at the Hawaiian Village Hotel for a week (just before Christmas) while personnel were brought in from California to fix this chartered aircraft. After repairs were made, our first attempt to continue our trip got us only to the end of the runway. More work on

DOCID: 4019711

the engines was necessary before we could head on to California.

To paint a little clearer picture of my situation at this time and how I was looking forward to getting home, I had been married only five months before going overseas for eighteeen months, I hadn't talked by phone to my wife throughout this period because of the cost, and it was nearing Christmas. All of this made me want to get home as quickly as possible. Come on, plane, let's go! The flight between Hawaii and California was generally uneventful until we were within sight of the West Coast. The pilot came on the intercom to announce that the plane had lost all of its hydraulic fluid and that the wing flaps, wheel release, and brakes would be affected by this situation. Further, he said that the runway at March Air Force Base was not long enough for our plane to land (with only mechanical brakes), so on to San Francisco we headed.

Yes, again we were met by fire engines and ambulances. And the landing was uneventful. By this time, however, I thought I had had enough flying for a while and decided to take a three-day train trip across the states, my longest train trip ever.

This was about it for the events I faced while in the Air Force, and next came my civilian trips for NSA. The first of these of any significance (meaning that there were several previous trips, mainly to Texas) took me to Vietnam. I was informed that I had to be ready to make this trip in just a matter of days, and that meant getting shots, passport, and whatever else was required prior to this time. Shots—I can still remember how my arms felt after "Buck Rogers" in the NSA dispensary got through with me, and then came the doctor with one for my hip pocket. Wow, that last one really felt good after I had been on that plane for over 24 hours; and my arms were so sore that I could hardly carry my suitcase when I finally did arrive at Saigon. By that time, I was wondering how the fighting in Vietnam could be any more painful than just getting ready for this trip had been---in fact, I was beginning to wonder who the enemy really was.

I had made it, though, after a jet flight that took some 28 consecutive no-sleep hours to complete. This flight was generally okay except for having a slight delay in Guam waiting for fighting in/around Saigon to clear, having to fly on the edge of a typhoon just off the Philippines, and having to make a very strange landing in Saigon. The pilot informed us that he had to make a very high approach to the runway in Saigon in order to stay out of sniper fire range – my first real feeling that I was in an unfriendly place. The approach to the runway was high until we made a very steep descent; it worked, and there were no fire engines or ambulances there to meet us, either. (Only seconds later, however, as we were departing the plane, two planes collided on the runway as one was taking off and another was landing.)

My first night in Saigon was a real learning experience. Have you ever heard of being in a fighting zone and getting a room in a normal hotel? Well, that is what I did. I was informed that this hotel was okay, since it had "flower pots" in front of it---a sign that its dues had been paid to the bad guys and that it would not be attacked. I made my way to my room where I found three beds. I decided to wash several pieces of clothing at that time, and little did I know that the water was going to be red (rust) when I turned it on. My white clothes turned red at once, something that only the local Chinese laundry was able to correct. I also remember how this water situation forced me to buy soft drinks on base in order to have something to drink and for brushing my teeth. I climbed in bed later in the evening with a mind full of worry about my situation. Would I wake up if there was fighting during the night? What would I do, since I was by myself and knew nothing about this city? I couldn't fight, because I was unarmed (allowed only to wear fatigues and carry a Geneva Conference Card). How would I communicate with someone if I needed help, since I couldn't speak the language?

I did manage to get to sleep, only to be awakened by somebody walking around in my

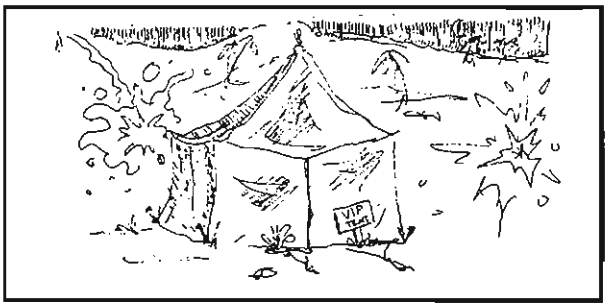
room. I quickly jumped out of bed to find out who the intruder was. I learned that it was another American and that it was common practice in Vietnam for all three beds to be individually rented to different people. I really began wondering at that time who the third person would be, possibly a bad guy? Well, the night passed and morning came with no new person in the room. I was suprised, however, to learn on my way to work the next day that an attack had been made on Saigon during the night and that rockets had exploded only a few blocks from our hotel. I must have been tired, as I didn't hear a thing, and I missed my first battle.

Everybody's work day in Vietnam was long, and mine was no exception. Generally, it was seven days a week from 0430 to 2300. I subsequently made several trips throughout the country where I soon learned to use my flak jacket as a seat pillow on plane rides because any incoming fire would be coming up from the ground. I also learned not to be in any hurry (as the old military saying goes, "hurry up and wait") because military planes did not fly by set schedules. It didn't take long for me to realize that I should take advantage of every chance I could get to grab some zzzz's.

I spent several days during this TDY waiting for transportation in terminals which had nothing more than dirt floors, no roofs, and sometimes only two walls standing. Several interesting things occurred on this trip that I will never forget. One had to do with a well-known Air Force officer at Da Nang. I had made plans, after being in Vietnam for several weeks, to sleep a little late on one particular Saturday morning. Very early in the morning, however, this officer banged a pipe on the end of my bed to wake me. He said that this was a war zone and that nobody was allowed to sleep in; TDYers were no exception. He asked me to get dressed, and he proceeded to give me breakfast which he had gotten from who knows where. While eating, he told me that we were going to add another room to his operations area. This required our cutting a hole in the side of an existing Quonset hut with a torch and moving one end of a trailer into this new opening. My job was to hold the ladder while the officer cut the hole.

All was going as planned, when we heard someone inside yelling "Fire!" The officer stopped cutting at once, uttered a few expletives, and ran around the building to discover that he had burned the tracking map to a cinder. Of course, the operations building was evacuated because of smoke, but officially it was because of hostile conditions, not further specified.

Another time, in Pleiku, very soon after arriving in Vietnam, I found out that I had a yellow stripe down my back. I was staying in the VIP tent which was some distance from the other tents and right next to the bunker. I asked whether there were any enemy in the area, and I was told that they never attacked during the dry period and, boy, was it dry that day. I was really happy to hear this news, but later that night there was a very loud clap of thunder, and the sky opened. It rained so hard that the water was coming through the fabric of my tent.



I started thinking about what I was told earlier that day about attacks, about the VIP sign in front of my tent being a good advertisement for attracting the bad guys; about the tent being off by itself where nobody could hear me even if I was in trouble, etc. I devised a scheme to wake myself should someone appear at my tent door: I put a wash pan next to the door, assuming that if anybody opened the door, it would knock over the pan, and the noise would wake me. I placed my shoes at the foot of my bed with my helmet between my shoes, thinking this surely would make for a quick exit if I had to leave. Sleep, yes, sleep; I thought I was finally going to get some sleep.

Clang! The pan fell, and I was gone like a flash. But nobody was there. I wondered where the enemy was. Evidently the wind had blown the door open and knocked over the pan. I decided if that alarm system wouldn't work, I would just zip up the front of the tent. But then I realized that if someone put an explosive under the wall of the tent I would be dead before I could get the door open to exit.

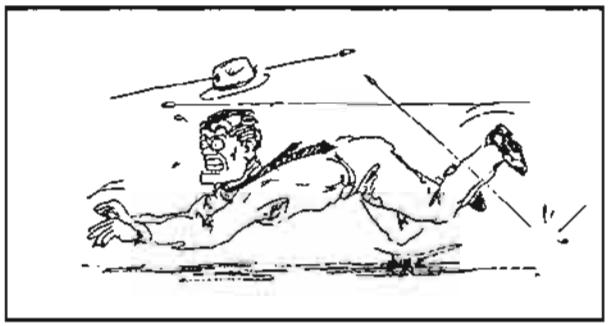
Finally, I decided to take my chances and just go to sleep. That I did.

I was surprised the next morning to learn that incoming rounds had destroyed two antennas only a few hundred feet from my tent. Would you believe that I slept through my second brush with war? Other excitement was on its way, and sooner than later. I learned not to worry about those things which were beyond my control, and I slept every chance I got.

My trip home, via Thailand, the Philippines, Okinawa, Japan, and Hawaii, was uneventful. I left Vietnam with blisters on the bottoms of my feet from the hot pavement and arrived in Baltimore where there was over a foot of snow on the ground. I waited outside the terminal in summer clothes for four hours before I was able to get a cab home...I nearly froze to death the remainder of that winter season. Also, I will add that my weight was 149 pounds when I started this trip and 129 pounds when I returned... mainly because of the lack of food and sleep (I averaged approximately four hours of sleep each day for the duration of this extended TDY). I also ended up with a fungus on one foot that continues to defy treatment to this day.

My next big journey was to [redacted] My trip from Baltimore, via New York and [redacted] was uneventful. After arriving [redacted] we claimed our baggage, passed through customs, checked at the ticket counter about our travel reservations [redacted] and proceeded to reenter the international area of the terminal. This part of the terminal was extremely crowded and noisy. After some two hours of waiting in this area, we realized that our flight was either on its way without us or that it was delayed. We weren't quite sure which was the case. We made a trip to the information booths where we found a representative of the airlines responsible for our flight [redacted] We asked about our flight [redacted] and were very pointedly instructed to see another person representing the airline responsible for taking [redacted] This was annnoying, but, rather than make a scene, we decided to comply.

We walked around to the opposite side of the 15x20-foot information booth, and suddenly there was an explosion. My natural yellow streak reappeared, causing me to duck immediately, and I then attempted to determine



the cause of the bang. Much to my surprise, I saw another movement like someone throwing something on the opposite side of the information booth. I immediately hit the floor, and then heard another bang ringing through the building. Several more bangs sounded, followed by automatic weapons fire. I now know that the sound of ricocheting bullets as depicted in old western movies is realistic. They really do make such sounds as they glance off marble walls and glass windows.

The next thing I heard was some people talking on the other side of the information booth. Taking stock of my surroundings, I became aware of a woman and her husband not far from me. The woman was suffering from shrapnel injuries over most of her lower abdomen. Another woman was separated from her husband and was about to walk out in front of the terrorists. We were able to stop her before she made this mistake. Then there was a young girl who had it in her mind to jump through a very large plate glass window simply to get out of the building. With difficulty, two of us were able to hold her down until she regained her senses. We stayed on this floor for what seemed like an eternity, but it was probably less than 30 minutes.

My traveling companion asked me what I thought we should do and my answer was "I'd rather be most anywhere other than in this building right now---even the middle of the runway dodging airplanes would be better than where we are now." We decided to make an arm-in-arm chain (all of the people described earlier) and attempt to get out the nearest exit before someone saw us. This door was only 30 or so feet away, but the distance seemed endless as we ran for the door. Looking over toward the area of some yelling, I observed a number of people standing in a line with their hands up... forming a human barrier between the terrorists and the police. Later, I learned

EO 1.4.(c)
P.L. 86-36

that the people standing next to me as I talked to the first person at the information booth were killed during this event. . . it was only a matter of seconds that kept me from being next to them when this occurred.

After we got out the door safely, we got the injured woman to an aid station. Then we were taken to another terminal, where we caught our plane [redacted] we made another mistake. As we walked to dinner one evening, unknowingly we passed [redacted] something we learned from our hosts the next day was a real no-no. Although we encountered a number of hostile looks and were followed, we made this trip to and from our eating place without incident.

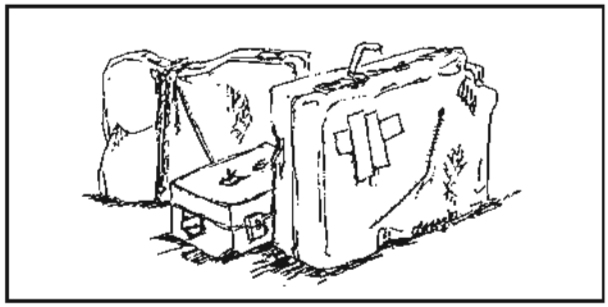
Four days after the airport incident, we were attempting to leave [redacted] when suddenly, as we were traveling down the runway, there was a loud banging noise under the aircraft. The pilot immediately braked and returned to the terminal building. Several "mechanics" came on board the plane and started taking the floor apart. Several of these mechanics subsequently disappeared under the floor for a while, and one of them reappeared after a time. He disappeared from the plane, only to return with a large pry bar and a sledge hammer. Again he disappeared under the floor, and there was a lot of pounding taking place just below my seat. The mechanics reappeared after a while, and the floor was replaced. Another attempt was made [redacted] and the exact same situation occurred again.

We returned to the terminal apron and waited three or four hours for another plane to be flown in from who knows where to take us to [redacted] but of course we had already missed our flight [redacted] We rebooked our flight, the last flight for the day [redacted] and proceeded on our journey. Our stay [redacted] was filled with new excitement.

While there, we were able to get a US Army helicopter flight that nearly ended in disaster. We were flying at 5500 feet when suddenly a gust of wind placed the aircraft on its side; a helicopter flies only one way in this position, down. The pilot was fighting to gain control of this bird, when suddenly it righted itself and rolled over on its other side---down some more we went. By the time he was able to regain control of this craft, we were only 500 feet above the ground. Needless to say, I was a bit frightened by recent events and beginning to worry about what was going to happen next. In fact, I made the statement that I would like to have a rowboat to get home.

[redacted] where one week later my traveling buddy and I became sick---food poisoning. After some recovery time, our next stop was [redacted] where we were not allowed to depart the runway for several hours, because of a strike by aircraft controllers. From there, we made our way [redacted] where one suitcase was virtually destroyed. Then we went on [redacted] where we got a rent-a-car.

[redacted] we suddenly realized that the transmission linkage on our rent-a-car was not working properly. We stopped the car and learned that a nylon ball and socket joint had worn out completely and would not stay together. After trying to get help from other passing motorists, we decided to do a real no-no again- [redacted] and broke it just enough to make it fit the shape of the transmission linkage.



I learned one thing during this trip. If you are traveling overseas, you should always have a roll of nylon tape and a roll of toilet paper with you at all times. The domestic paper in these countries is ridiculous, and the tape allowed me to mend my broken suitcase and repair the transmission linkage. We made the rest of this trip uneventfully, until we arrived at Baltimore. My broken suitcase, from which I had removed all valuables, arrived as scheduled. My good suitcase, containing those valuables, was missing. I made the usual claim, and some two weeks later I recovered

the other piece of luggage. Fortunately, nothing was missing. However, there were tags on this suitcase from nearly every country in South America; and there was a carton of cigarettes and a box of candy in this suitcase which were not mine.

This travelog could continue for a while longer, but I believe you now have a feeling for how exciting government travel can be and what one federal employee has been through. I could tell you about the time that we were in a severe storm (with significant amounts of lightning, rain, and hail) over London---a storm so intense that it forced the pilot to make an emergency landing, storm or no storm; or the many times I have been on flights that were delayed in landing because of heavy traffic and how this caused me to miss connecting flights; stories about some of the strange-looking aircraft I traveled on in Vietnam and in Central America; or some of the things that happened as we attempted to clear customs; or problems because of language barriers, etc. Incidentally, my trips have never allowed much time to see the sights along the way. Generally, I would work during the day, travel in the evening, or would be located at a God-forsaken place where there was nothing but work and wilderness.

I look forward to my next trip for the government; however, let it be known that such trips are not the same as, nor are they intended to be, vacations. I will always wonder, as I make future trips, what challenges I will face before I am once again home. I have gained a considerable education from these ventures and a new appreciation for the way things are back home.

The next time you have a chance to take a trip for the government, you should take it. Please, however, be prepared for almost anything to happen, as Murphy and his law seem to be nearby at all times. In fact, I think Murphy knows me well and is a constant traveling companion of mine. I have found that he is the only person who wants to travel with me - after people hear about my previous experiences. I don't mean to frighten or discourage anyone. After all, I am alive to tell my story. □

BULLETIN BOARD

EXCITING EXPERIENCES IN THE FIELD?

~~(C)~~ The Office of Archives and History (T54) is collecting historical information on field operations. They would like to hear from people who were involved in, or have information or files on, the following events:

[redacted]

If you can help, please call [redacted] on 972-2355s. Or you may drop him a line at SAB-2, Door 22, T54.

WORKING ON CODES?

~~(C)~~ The Bookbreakers' Forum on Machine Aids will resume meetings this fall. Membership is open to individuals who work on codes as cryptolinguists, cryptanalysts, or programmers, or who manage or supervise such endeavors. To get on the mailing list send your name, organization, and building to: HQ, P16, [redacted] Please do not phone.

P.L. 86-36

DO YOU HAVE THE MERCURY SOFTWARE?

(U) The MERCURY software which [redacted] advertized recently in Bulletin Board has gotten away from him. If you have it, or know who does, please give him a call at 963-1103 so that he can keep track of its whereabouts.

THE DISTRIBUTION OF CRYPTOLOG

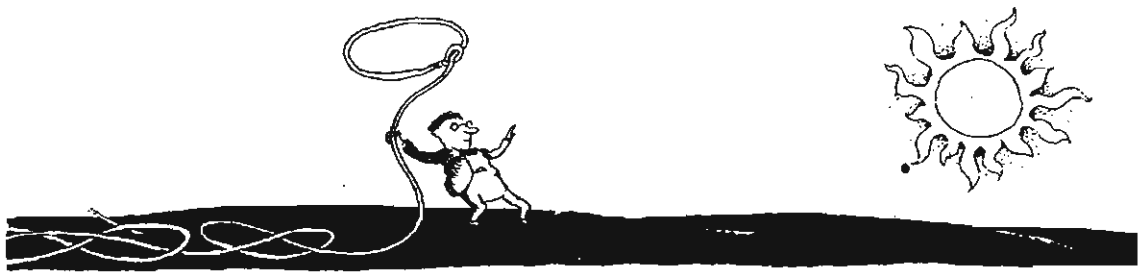
At the request of Y16, Distribution, we have discontinued mailing labels. But to ensure that individuals continue to receive their own copies, we have instituted distribution lists.

DOCID: 4019711

A ROPE BY ANY OTHER NAME IS . . . A TASSEL? (U)

B413

P.L. 86-36



The true way goes over a rope which is not stretched at any great height but just above the ground. It seems more designed to make people stumble than to be walked upon.

Franz Kafka, *The Great Wall of China*

At the Asian Defense Technology Exposition in Beijing in November 1986, the People's Republic of China unveiled a new anti-submarine missile delivery system called the **Changying 1** (長纓), literally, "long tassel." This is an unusually vapid designator for a missile system, particularly as in the past the Chinese had used more virile names: *Sea Eagle*; *Red Flag*.

The origin of the name remained a mystery until the publication of the January 1987 issue of the People's Liberation Army Pictorial, featuring a four-page spread on the Beijing exhibition. The article did not mention the Changying 1. But the eyecatching headline provided a clue. It read:

Chang ying ke xi ri (長纓可系日)

which means,

The long tassel can tie up the sun.

It was obvious that the author was playing with words by using the name of the new missile in the headline.

I thought it might refer to a **chengyu**, which is a saying like "A stitch in time saves nine," something that literate (and pseudo-literate) Chinese often employ. An extensive search finally led to the discovery, in an obscure dictionary of chengyus, of two phrases with classic origins which were combined to create that headline.

One phrase, **chang ying zai shou** (長纓在手) literally means, "The tassel is in hand." Here *tassel* is used for *rope*. The classical meaning of the phrase is that with a rope in hand one can tie up one's enemies. Mao Zedong, the late chairman of the Chinese Communist Party, used the phrase when, impatient at waiting to conquer his enemies, he wrote: "Now the long tassel is in hand. When will it bind up the old dragon?"

The other phrase, **chang sheng xi ri** (長繩系日) literally means, "using a rope to tie up the sun." It connotes making an effort that cannot succeed, something like our phrase "to hold back the dawn."

Thus, the headline is ostensibly saluting Chinese weapons production, prominently featured at the Beijing exhibition, for doing the seemingly impossible. The indirect reference to the name of the new Changying missile is apparently an in-joke for the cognoscente, a quiet statement that Mao's successors have a new weapon with which to tie up their enemies. □

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019711

Ode to Stonehouse

STONEHOUSE
Tentative
tenacious;
Real . . .

GLASSHOUSE
To some,
Beware, do not throw stones;
We will close you.

STONEHOUSE
For those of us who know it,
Real . . .
We live it;
We live.

STONEHOUSE
On paper a Mission and Function;
Stark words,
Not even full of sound and fury;
In bureaucratic jargon, certainly signifying nothing
To those who do not know YOU.

STONEHOUSE
To those who can see only shallow:
A thorn,
An O & M,
A $, to be cut in trying times . . .
Possible embarrassment;
A THING, over there, EO 1.4.(c)
A God-forsaken THING? P.L. 86-36
Who cares? Or, is it who could care?

STONEHOUSE,
To those of us who live it,
Love it . . .

DOCID: 4019711

OURHOUSE

You there;
do NOT throw stones at OURHOUSE!
We will not run.

In fact, even now you find we say:
"Look at us, see what we do for you,
Potential - see what we can do . . . "

You are not so blind;
Perhaps you see a hint of what we say.

STONEHOUSE,
Conscious,
Conscience,
Observe,
Listen to OUR message.

Can you really close us?

Measure the intangibles, mate;

Can you really replace us?

Think hard, before it is too late.

Can you do without us?

Know, before you seal our fate.

Can you still support us?

Examine your returns to date.

Can YOU really face US?

On this, do not procrastinate.

DOCID: 4019711

STONEHOUSE . . .

POWERHOUSE

Dynamo pulsing strong through day and night;
Curious mixture of stone, iron, and steel
With transistors, electrons, voltage, light;
S E C R E T, Mission Impossible come real?

Dynamo with antennae at great height,
Probing communications from afar;
Firm, poised steadfast and thriving from this site
Security for Earth about its star.

Dynamo of people who take delight
In computers, amplifiers, hardware;
Cabling to function with purposeful sight,
And directing it with complex software.

Dynamo struggling through its daily plight
With its machines made to produce for man,
To couple with his brain, avoid the blight
Of resorting to our guns, if we can.

Dynamo striving with our free world's might;
Ever hoping that IT will never cease
To support that which we believe is right -
Liberty, justice, love - preserve some peace.

DOCID: 4019711

STONEHOUSE . . .

OUR HOUSE . . .

Security, our defined objective;

Assigned mission for which OUR HOUSE does strive;

Technical and human strengths collective

Unified to create a STONE alive.

Security, for memory:

"A Mile High, A Mile Ahead;" trite, you say;

Perhaps. But for which we're appreciative

To evoke emotions some far-off day.

Security: measures preventative

With the proper tools, right time, correct place;

That's why it was not by chance creative

[redacted] was chosen STONEHOUSE base. EO 1.4.(c) P.L. 86-36

Security, no less diminutive

For our great country in its ongoing strife,

If in honesty we are cognitive

That we find here a satisfying life.

Security, of course, we're subjective

In our judgment of this HOUSE's true worth;

However, there is still much substantive

Beyond our feelings to warrant STONEHOUSE's berth.

Each person, from his perspective, will perceive

His own STONEHOUSE; many versions we will contrive;

We must avoid creating those that may deceive,

And with objective honesty we all must strive

To clearly portray the truths we deeply believe

When asking yea or nay to keep STONEHOUSE alive.

Key in this is whether or not we can achieve

Creation of a "STONEHOUSE" elsewhere that will thrive.

I know that there may come a time when I will grieve,

If when all is considered, STONEHOUSE you will rive;

There will be a part of me that will never leave

[redacted] EO 1.4.(c) P.L. 86-36

P.L. 86-36 [redacted] EO 1.4.(c) P.L. 86-36

[1st Issue, 1987] reminded me that I had written an Ode to STONEHOUSE when I was leaving it for the last time.

I dug back in my memorabilia file and found a copy. It evokes personal memories and emotions for me, of course.

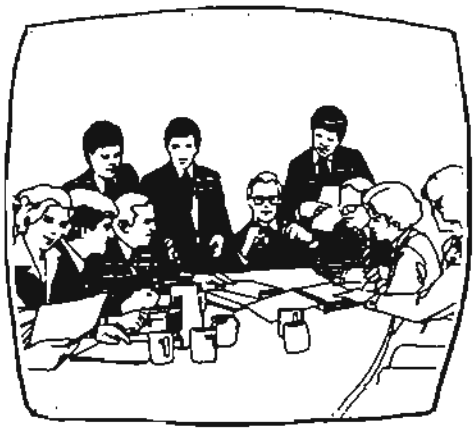
This was written at the time when there was considerable controversy and anxiety over whether or not the STONEHOUSE facility should be closed. The Ode implicitly carries the messages of Dave's two tendencies, which he spells out at the end of his article.

[redacted]

P.L. 86-36

DOCID: 4019711

CRYSCOM



[redacted] A638/P13

P.L. 86-36

FOR OFFICIAL USE ONLY

The Cryptanalytic Software Committee (CRYSCOM) was established in May 1984 as a volunteer organization. CRYSCOM's major functions are: to provide a forum where representatives of the cryptanalytic supercomputer complexes can discuss issues of common interest; to collect and distribute critical information to the user organizations; to organize and conduct the annual Cryptanalytic Software Conference (CRYSCO); to carry out the recommendations made at CRYSCO; and to facilitate the development or maintenance of software for the supercomputing cryptanalytic community.

CRYSCOM consists of a Chairman, Vice Chairman, Executive Officer, representatives with voting privileges, non-voting members, and points of contact. The Chairman presides at meetings of CRYSCOM and the Executive Council, appoints standing and ad hoc subcommittees, and represents CRYSCOM where required. The Vice Chairman acts for the Chairman in the latter's absence.

The Executive Officer is the only individual working full time on CRYSCOM business. Responsibilities of the Executive Officer include: overseeing the execution of the CRYSCO/CRYSCOM recommendations and reporting progress to CRYSCOM; recording the proceedings of the CRYSCOM meetings and distributing the minutes to the cryptanalytic community [redacted] retaining documents that are generated through or on behalf of CRYSCO/CRYSCOM in the CRYSCOM Library; maintaining contact with all complexes; carrying out the wishes of CRYSCOM and acting as a central point of contact for CRYSCOM matters.

The Executive Council determines CRYSCOM's policies and activities. The Council includes CRYSCOM representatives from each of the supercomputer complexes, the CRYSCOM Executive Officer, and one representative each from B6, T335, and T442.

CRYSCOM representatives who have voting rights are chosen by their complex manager. As representatives, they pass information to and obtain information from the user groups they represent. Since CRYSCOM has no power or authority, it must rely on the consensus of its members to implement new ideas and to solve problems.

Membership is open to interested persons in organizations which perform and support cryptanalysis in the supercomputer complexes at [redacted] NSA. As a member, an individual has no voting rights but may voice concerns at the monthly CRYSCOM meeting.

CRYSCOM has points of contact in each of the supercomputer complexes. They are the main contacts for cross-complex transactions. They assist in coordinating software and information exchange between supercomputer complexes, and also assist the CRYSCOM representatives in communicating information to, and receiving feedback from, users. [redacted]

P.L. 86-36

The monthly CRYSCOM minutes are sent to 65 individuals. The minutes as well as other items of interest are available in CANEWS, an on-line user news file residing on all the [redacted] systems. □

DOCID: 4019711

LETTERS

To the Editor:

I was glad to see the plea in the December 1986 issue of CRYPTOLOG for a readable computer handbook. Certainly it was time that there was public recognition of how poorly the job of introducing computers into our workspaces has been done. If the people who make the decision on the hardware, software, and training for the ASTWs and other desktop computers know how to automate a workplace properly, they have done a good job of keeping the fact a secret.

I know enough about computers to discuss them, but no so much that I cannot discuss them in English any more. I have a microcomputer at home, and I have as friends a software engineer and a computer secrity officer, and my father is a computer systems consultant. From them and from my own reading on the subject, it is clear that most of the usual steps in automating a workplace have been ignored here.

There are three basic steps to putting computer systems into the workplace. First, an expert knowledgeable in hardware, software, and other components of computer systems comes to the actual work area to be automated. This person will examine how that office does what it does and will suggest a system to meet each area's needs. Next, budget and compatibility questions are addressed: what can be afforded and will it work with any equipment already in place? Last, the system is installed and the users given training on it. A fourth "step" is the programming and service support so that the system continues to run and to evolve to new needs after installation. This step, at least, is being done well and need not be discussed further.

Our office got the same computers with the same software for everyone: no tailoring to our particular needs. The computers have actually made more work for us and slowed down the process of getting reports out. As for budgeting, it appears that we could have paid some 30% less than we did. Our PC/XTs communicate well with the mainframe systems when used as terminals, but have limitations in their ability to work with the PC/ATs we were given just recently. And, as the plea in CRYPTOLOG for a handbook shows, we are still waiting to find out how to use our computers.

Of course, the standard answer to training requests is "Read the Manual." But the manual is barely comprehensible, full of technical terms unintelligible to most people. And much if what is in the books is for the programmers and systems management people, not for the average users with PCs on their desks. Which commands are for which people, and how do you apply the commands that are for you?

The User's Handbook for the PC/XT is a dictionary of commands. It is like buying a toolbox and having a manual which tells you, in technical detail, how to operate each tool. But what we, the average users need, is the computer equivalent of a home improvement "How To" book. Most people do not even know the questions to ask on how to apply their computer to their job. A typical exchange:

"What can I do with my computer?"
"What do you want to do with it?"
"Gee, I don't know. What can it do?"
"Oh, it can do all sorts of things, but what do you want to do with it?"
"Well, what can it do?"

There are millions of dollars with of unused and underutilized computer capacity sitting on desks all over the Agency because the users really have no idea how to use them fully. If the Agency is serious about combatting waste, it could save a lot right here.

[redacted] *B41*

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019711

Maybe the authors of future works on using PCs will refer to pp 25-26 for guidance on writing directions. Ed.

To the Editor:

In response to your editorial in the December 1986 CRYPTOLOG ("Julia Child, Where Are You?") I would like to point out that there have been attempts to simplify the documentation for personal computers. The problem is often not that a usable handbook doesn't exist, but that the existence of that handbook is known only to a small group.

In particular, when G74 first began receiving IBM PC-XT prototypes for the ASTW, I wrote a manual for analysts using these machine with PC/IX. (This manual is usable with the XT-based ASTW as well, but some keys are in different places on the keyboard.) While it is far from perfect, my manual is an improvement over the IBM manuals both in readability and in usefulness, as it has an index. This manual is widely distributed in G74 but, while I provided copies to G3, T4, and ASPIC, its existence seems to be one of the better-kept secrets around here.

I am sending you a copy as a separate e-mail message. If you find it useful, please feel free to pass it on to anyone who could benefit from it. If you feel it needs improvement, please feel equally free to pass it on to let me know what changes you think are necessary.

[redacted] *G743*
P.L. 86-36

A sample page of Barry's manual appears on Page 23. Ed.

To the Editor:

I read your editorial in the December 1986 issue of CRYPTOLOG with great interest because you were talking about the need for materials to help novice PC users. Help is available in the Agency Standard Products Information Center (ASPIC, formerly the PCIC)! Enclosed are some samples. Unfortunately, because of legal constraints, we cannot include material such as these in the IBM boxes when they are delivered, but they are readily available in our OPS-1 and FANX-III locations.

In addition to these written aids, we have analysts ready to handle problems on the phone. We have tutorial packages that can be borrowed for up to two weeks at a time. Nearly all of our applications packages include excellent tutorials to help people get started. P.L. 86-36

[redacted] *A/Chief, T535/ASPIC*

A sample page of the ASPIC manual appears on Page 24. Ed.

EO 1.4.(c)
P.L. 86-36

Have you missed these articles?

§ "Has It Ever Been Translated Before? Tracking down technical translations." by [redacted] Jul-Aug 1978

§ "Exercise Support." by [redacted] P.L. 86-36 [redacted] December 1981.

§ "Rules for the Camel Corps." by [redacted] March 1982.

§ "What Promotion Boards Want." by [redacted] August 1982.

§ "Arms Control in the Wake of KAL 007." by [redacted] April 1984.

§ [redacted] by [redacted] Jan-Feb 86

§ [redacted] by [redacted] Mar-Apr 86.

§

To obtain a copy, send your name, organization, and building to: Editor, CRYPTOLOG, P1, HQS. Phone requests will not be honored. P.L. 86-36

§

Yes, we recycle! P.L. 86-36

We're always happy to receive back copies of CRYPTOLOG, especially of these recent issues: Oct-Nov 86, Dec 86, 1st Issue 87, 2nd Issue 87. We'll also accept copies of CRYPTOLOG's predecessors,: *KEYWORD, Dragon Seed, COMMAND, The Quarterly Review of Linguists.*

~~FOR OFFICIAL USE ONLY~~

EO 1.4.(c)
P.L. 86-36

DOCID: 4019711

P.L. 86-36

Sample Page:

USER'S MANUAL FOR PC/X ON THE UIS PROTOTYPE, *by* [redacted] *G743*

built-in hardware tests will be performed, during which time a series of memory check reports (e.g., "320 KB OK") will appear on the screen. When the tests are complete, the system will beep once, try to read from the floppy drive, try again, and finally begin loading from the hard disk. During the loading process, the statement "booting /unix from partition 1" will be displayed. After a short time, there will be another beep, the amount of available memory will be displayed at the bottom of the screen, and the following notices will begin to appear:

```
Normal startup in progress.
File system integrity assumed.
Enter Date [[MM]DD]HHmm[YY]:
```

Type in the portions of the date and time which have changed since the last time the system was booted. (I.e., if this is the first time on 19 Oct 84 that the system has been turned on, but it was used on 18 Oct, enter the day and time.) The format to use is two digits each for the month, day of month, hour, minutes, and year. The hour and minutes must be entered, the other three fields may be entered, but are only required if there has been a change since the last startup. Some additional system notices will be displayed, then the screen will clear and the login prompt will appear.

B. Login

At the login prompt ("login:"), type the name by which you are known to the system (usually your initials). The computer will respond "Password: ". Enter your current password. If your password has expired (M), you will be asked to supply a new one. After entering the new password a second time, you will be presented with a new login screen. Log in once more, using the new password. (Note that this is different from the PDP-11/Delta Data system, which allows you to log in using the old password, but asks you to use passwd to change it. PC/IX automatically runs a modified passwd when you try to log in and then logs you out again.) Once you are logged in, the system prompt (a dollar sign, rather than the percent sign we see on the Delta Datas) will appear and you are ready to begin work.

C. System Commands

When you consider that Section 1 of the IBM PC/IX User's Manual is 1.7 centimeters (about 2/3 inch) thick, you begin to get the idea that there are probably a lot of system commands which you will rarely, if ever, use. This guide, however, will try to present the most generally useful system commands as clearly as possible. In the entries

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019711

Sample Page:

TIP SHEET: INTRODUCTION TO THE ASTW: *Issued by ASPIC (formerly, PCIC)*

The Login: prompt will then be displayed.

4. Log in using your user ID and password (if one was assigned by the system administrator; if not, press the Return key).

```
System: Login:
User: (enter your login identifier)

System: Password:
User: (enter your password)

System: $
```

5. Set the battery-back-up system clock.

Key the numeric month (mm), day (dd), hours (hh), minutes (MM), and year (yy) after the clock command as follows:

```
System: $
User: /priv/clock mmddhhMMyy
```

6. Activate the "-" mode of the -/Lang key. (Note 1.)

Press the Ctrl and -/Lang keys simultaneously. (The "-" mode is required by the INed program to implement the Cancel command.)

7. Do the INed tutorial.

Read and follow the INed beginner's tutorial as defined in the PC/IX Text Processing Guide section that begins at the Getting Started tab. This tutorial provides valuable instruction on the PC/IX page editor and introduces file structure concepts as well as many of the more popular PC/IX commands. We strongly urge that you complete this tutorial.

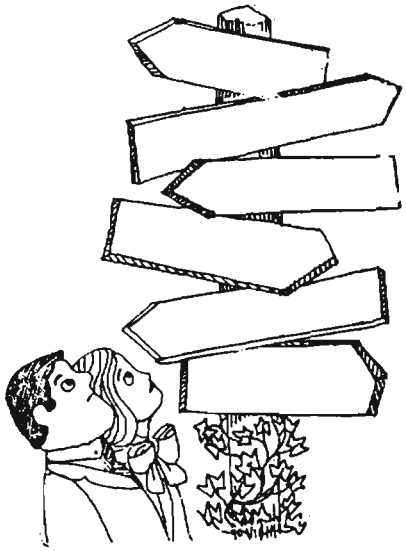
8. Establish your password.

Invoke the Password command and define a six-or-more character password that will be required at each future logon:

```
System: $
User: passwd

System: New password:
User: (key your desired password)

System: Re-enter new password:
User: (key your desired password again)

System: $
```


~~FOR OFFICIAL USE ONLY~~

DOCID: 4019711



REQUIREMENTS FOR A GOOD SET OF DIRECTIONS

extract from: *Writing Scientific Papers and Reports.* by W. Paul Jones, revised by Michael L. Keene.

W. C. Brown Company, Publishers. Dubuque, Iowa. 8th Edition, 2nd Printing, 1982 [PE 1475 .J72 1981]

1. Completeness

Keep your readers constantly in mind. Are they laymen, executives, experts, or technicians? Whatever the case, write for those within the group who know least about your subject. They will need every aid you can give them. Experts can ignore the directions if they don't need them.

2. Explanation of Technical Terms

Lest any reader may not understand them, define and explain your technical terms. Experts can skip the explanations, but non-experts may be frustrated without them. Most people don't have technical dictionaries to which they can refer.

3. Proper Emphasis

Number each direction and devote a whole paragraph to it, even if it is only a single sentence. Readers can then check them off, thinking, "All right, I've taken that step. Now what's next?" The next numbered paragraph will tell. If you include two or more directions in a single paragraph or under a single number, readers are likely to overlook one of them. Allow plenty of space for each direction.

4. Use of Visual Aids

Include any diagrams, pictures, graphs, etc. that will help readers to follow a direction.

5. Reference to Visual Aids

Put visual aids where the reader can most easily refer to them. If such an aid can be on the same page and near the direction it concerns, it will be most conveniently placed. If it is on a different page, readers may not refer to it when they should, and consequently may misunderstand a direction. Your own experience will tell you how irritating it is when a textbook prints a diagram, picture, table, graph, etc., on a different page from the explanation of it. If it is impossible to place it on the same page, put it on the next page.

6. Explanation of Visual Aids

Don't fail to allude to, if necessary explain, any visual aid. Usually it is not enough merely to refer to it, as in writing "See Figure 1." Add any explanation that will help reders to follow your directions. Too often the writer assumes that the meaning of a visual aid is self-evident and leaves many readers to puzzle out its meaning for themselves.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019711

7. Justification for a Direction

Be sure to give the reason for any direction, especially if your readers might think, "Why do that?" Otherwise, they might follow a different procedure which seems at the moment preferable.

8. Explanation of General Principles

Explain any general principles that readers ought to understand if they are to follow your directions easily. If the principles underlie the whole procedure, explain them in the introduction. If they refer to only one direction, put the explanation after the direction.

9. Suggestions for Avoiding mistakes.

Warn readers when there is a possibility of making a mistake. Novices especially may need warning to prevent wasting time or ruining expensive equipment. Mistakes due to lack of experience or skill may not be avoidable, but those due to ignorance or carelessness are inexcusable. If, for example, your instruction emphasizes the importance of gluing a wood joint instead of nailing it, you may prevent someone from making something that breaks under stress. Such warnings should be placed at the beginning of the set of directions. Do not assume your reader will read all the directions before starting the process. Your own experience tells you that the natural tendency is to follow instructions step-by-step without first reading all of them.

10. Avoidance of Telegraphic Style

Don't leave out all words like *the* and *a*, or the subject of verbs, words necessary for full grammatical expression. Telegraphic style may be justified if space is limited, as on bottles and other small containers. But in the average set of directions you will save less then 5 percent of your space in using it. Furthermore, telegraphic style is likely to obscure the thought. Instead of "Put curd into bowl, add water," it is better to write, "Put the dried curds into a small mixing bowl and add 4 tablespoons of cold water."

11. Consistency in Point of View

Use the second person imperative whenever you are writing a direction. For example, you should say,

> Pour two cups of skim milk into the saucepan.

not

> You should pour two cups of skim milk into the sacucepan.

or

> Two cups of skim milk are then poured into the saucepan.

The last two are not imperative constructions.

But if you are stating a general principle or giving some useful supplemenary explanation, use the third person. For example, after a direction "Add 6 tablespoons of vinegar to the milk," in the same paragraph could follow the explanation, "The vinegar will sour the milk and precipitate the casein out of the mixture as curds."

12. Use of Clear Transitions.

Make all of your transitions from section to section and from direction to direction as clear as possible. Proper used of headings, numbers, and paragraphs indentations will usually be sufficient. Don't insert unnecessary transitional words and phrases. If direction 3 is "Add one teaspoon of bicarbonate of soda," direction 4 should begin, not with "then" or "now" or "after you have done this," but simply with a new paragraph, the number 4, and the verb in the imperative: "4. Continue the blending, etc." Sequence in time ordinarily governs the arrangement of directions. Only if two or more things are to be done at the same time would a transitional phrase like "at the same time" or some explanation be needed.

PLAN FOR A SET OF DIRECTIONS

The plan for a set of directions is essentially the same as for a description of a process. In developing the plan, however, you need to pay special attention to the division points, both major and minor. Remember that your readers are, presumably, going to perform the process with your directions as the only guide. If they misunderstand a point in the description of a mechanism, perhaps the loss is not serious, but if they misunderstand a direction, they may lose a lot -- including their temper. □

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019711

BOOK REVIEWS

Her Majesty's Secret Service: The Making of the British Intelligence Community. By Christopher Andrew. Elisabeth Sifton Books, Viking, New York, 1986; pp. xviii, 619.

Reviewed by: Vera Filby, E4

The name Christopher Andrew is becoming familiar to readers of the British press. Dr. Andrew, Fellow and Senior Tutor in History at Corpus Christi College, Cambridge, is called upon with increasing frequency to comment on books and events of intelligence interest, like the Peter Wright affair in Australia, which was in the news at the time of this writing.

Dr. Andrew brings a message as well as a solid and scholarly account of British intelligence history in the 600 well-packed pages of his book. His message is that histories of 20th century British politics, foreign affairs, and military matters cannot be accurate or complete if intelligence is not taken into account, but British government, law, and tradition have unyieldingly blocked release of peacetime intelligence. Dr. Andrew maintains with some passion that the government should recognize that this is unreasonable and should release to the public archives all records that can do no harm to national security. (Those of us in the business can sympathize, but we understand that security decisions may not be as unreasonable as they seem to researchers on the outside looking in.)

After a glance back at Queen Elizabeth I's secret service, Dr. Andrew briefly traces the development of the British intelligence services up through the Boer War and into the 20th century. As early as 1703 a "Decyphering Branch" was set up by the Secret Service Fund. This largely private enterprise, as well as other intelligence and covert activities financed by the fund, were carried out by freelance amateurs and gentlemen adventurers. Indeed a trace of the amateur tradition survived even into recent times. The Decyphering Branch was disbanded in 1844, a time which, as Dr. Andrew points out, was exactly wrong, since the electric telegraph was just coming into use.

The progenitors of today's intelligence and counterintelligence services were created by strong-minded civilian officials and military men whe saw unmet needs for intelligence and took action to do something about meeting them, usually battling the "venerable inertia" of the established order. It was not until 1886 that the Naval Intelligence Department was created, and that was against the will of the Board of Admiralty.

The civilian intelligence organizations were also slow in getting started. Such resources as the counterintelligence agencies did muster were largely occupied trying to cope with Fenian violence. In 1884, after a bomb was set off in a public lavatory in Great Scotland Yard and security measures were being implemented, it was found that the entire sanitary system of the Houses of Parliament was being overhauled by Irish workmen.

When the Boer War started in 1899 the War Department's Intelligence Division had a total of 18 men with 2 officers and a clerk responsible for all British colonies and protectorates and the Boer Republics. When intelligence officers were sent to the field, their reports were disbelieved or ignored, but after the shift to guerrilla warfare a large and well-organized Field Intelligence Department was formed. As happened after other wars before and since, the intelligence structure did not survive the victory.

Boer guerilla successes shook British faith in the invulnerability of the empire. With the regular army overseas, fear of invasion by France washed over the country. Later Germany became the country to fear, and the hunting of spies, real and imaginary, occupied the counter-intelligence forces. During the same period the organization which was the ancestor of the Secret Intelligence Service (SIS) was founded. The first chief, Commander Mansfield Smith-Cumming, or Cumming for short, was the source of the designation "C," still used for the chief of SIS. He was another of the colorful characters that have populated British intelligence history. The fact that logbooks he kept are still considered too sensitive to release provides Dr. Andrew another opportunity, which

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019711

he is glad to take, to point to the absurdity (as he sees it) of withholding information so old that it could not conceivably be injurious to national security.

The peacetime exploits of the counterintelligence agents may have been often ineffectual, but peacetime cryptologic efforts were nonexistent. So upright was the Foreign Office in this regard that the Cambon brothers, French ambassadors in London and Berlin, used the British diplomatic bag, considering it more trustworthy than the French post or diplomatic couriers.

The 1914-18 War changed all that. The inadequacies of the old ways of gathering information at sea got the attention of the First Lord of the Admiralty, Winston Churchill. From the beginning, even as far back as the Boer War, Churchill understood and valued intelligence.

What was to become the famous Room 40, named for its location in the Admiralty Old Building, began with the appointment of the Director of Naval Education, Sir Alfred Ewing, to do something about coded messages thought to be of enemy origin. The effort began with a group of six mathematicians and linguists who according to one of them were "singularly ignorant of cryptography." They had to work in shifts because the space provided was too small. From that beginning, Room 40 grew into a formidable company equalled in accomplishment, brilliance, and general oddity only by its descendant, the phenomenal creation also named for its location, Bletchley Park. Room 40 knew failures too, but often they were failures not of the cryptanalysts but of the intelligence evaluators and disseminators. Much of the accomplishment of cryptanalysts on both sides was due to the lack of any sense of security on the part of their opponents. U-boat commanders, for example, helped Room 40 considerably by their "extreme garrulity." Nevertheless, German security did take effective measures from time to time, and during one of the periods of unreadability, a group of Room 40 people got together in a separate room to experiment and find out what they could do with the externals alone, and they invented traffic analysis, though they had no name for it then.

Just as there was no effectively organized foreign or naval intelligence at the beginning of the war, neither was there an organization for field intelligence until a commandant for an Intelligence Corps was appointed in 1914. The author tells the history of the Corps' operations on the Western Front until Armistice Day, when the last weekly Order of Battle showed the location of 186 enemy divisions. Only two proved to be wrong.

In 1919 a peacetime cryptanalytic group, which was eventually named the Government Code and Cipher School (GC&CS), was formed with veterans of Room 40 and the War Office M11b. Wasting no time, they were soon reading French, American, Japanese, and Soviet traffic. Evidence of Soviet agitation and subversion, supporting the revolutionaries in labor unions and among disaffected ex-servicemen, was so overwhelming that in 1920 outraged government officials were determined to expose it, and did. Even Churchill approved. In 1923 the government issued an ultimatum to the Soviets charging subversion and other hostile acts and quoted verbatim extracts of decrypted message texts. In 1924 a letter from Zinoviev, a Comintern official, was leaked for political reasons, and two days later a debate developed into "an orgy of governmental indiscretion." The eventual Soviet response was one-time pad, and GC&CS was out of the Soviet dip business.

With the onset of the depression, Britain's military power went into a steep decline and along with it military intelligence. Counterintelligence MI5 also suffered shortages of resources despite continuing Communist hostility. GC&CS, though lean and hungry, still exploited Japanese, Italian, Comintern, and other traffic (while some of the source countries did pretty well with British traffic). A great triumph occurred in 1933, when a team under Colonel Tiltman (our own "Brig," whom many of us remember with admiration and affection) broke into Comintern traffic from Moscow to a terminal which was DF'ed to a house in a London suburb. This was GC&CS' first use of DF. The law did not permit a search of the house, but MI5 finally got hold of one of its contents, a pamphlet "intended to be issued to the Fleet containing a gross incitement to mutiny."

After many years of preoccupation with inimical forces from the left, dangers from the radical right appeared with the fascist movement in Britain. But this menace never matured, and by the time the wave had passed

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019711

in the mid-1930's Germany had replaced Soviet Russia as the main worry for foreign intelligence. By then the Passport Control Office, which for years had been the cover for foreign intelligence operations, was being overwhelmed with applications from Central European Jews to go to Palestine. GC&CS successes during those years were often defeated by ill-coordinated intelligence evaluation and dissemination and by atrocious personnel and physical security in British embassies.

Intelligence events in the early days of the war included revelations by a defector of traitors in communications and the gift of the priceless but officially unappreciated Oslo Report, obviously written by a scientist, which contained information on new German torpedoes, radars, and other developments including early rocket work and the experimental center at Peenemunde. (*The Griffin*, published in 1986, is a biography of Paul Rosbaud, science editor for a German firm, who the author, Arnold Kramish, believes was the source of the Oslo Report.)

The thrust of Dr. Andrew's relatively brief treatment of the years from May 1940 when Churchill took office to 1943 is expressed in the chapter title, "Winston Churchill and the Making of the British Intelligence Community." Churchill had always believed in, appreciated, and championed secret intelligence. His faith in what was not yet called COMINT was rewarded when GC&CS, by then renamed Government Communications Headquarters (GCHQ), broke into an Enigma system. This was a payoff for foresighted cooperation with the Poles and the French.

GCHQ was foresighted also in the quiet recruiting beginning two years before the war of some of the best classics, language, and mathematics brains in Cambridge. The service intelligence departments were slower getting started, but they gathered in naval veterans of Room 40 and high quality men from the financial world. One of them was the stockbroker Ian Fleming. MI5 was even less prepared. Those it began belatedly scooping up included some of the most colorful intelligence characters as well as six future judges, future university professors, and Anthony Blunt. The Secret Intelligence Service was not in the same class, though some of the recruits became famous personages, among them Malcolm Muggeridge, Graham Greene, and Hugh Trevor-Roper. One other recruit was the only one to earn a decoration for his wartime work. His name was Kim Philby.

Exiled foreign intelligence services added to the assets available, and SIS maintained liaison with the Czechs and Poles and kept communications and funding control over the Norwegians, Dutch, and French. The operations, exploits, dirty tricks, misadventures, and coups of SIS and MI5 have became famous through the many histories, biographies, autobiographies, memoirs, spy stories, and films based on them in the years since.

Dr. Andrew credits SIS with two pioneering developments before the war. One included new methods of photoreconnaissance and a commercial front organization to carry them out. By the time the war started and the enterprise had been turned over to the Air Ministry, large parts of Germany and the Mediterranean had been photographed. The other innovation was the creation in 1938 of Section D (for Destruction) to specialize in means other than the operation of military force, translated as dirty tricks. This, as might have been expected, attracted some extraordinary people, one of whom, Guy Burgess, would eventually be exposed as a traitor.

Intelligence produced by all these outfits remained ill-coordinated until the Joint Intelligence Committee was bolstered by a Joint Intelligence Staff. In this improved coordination as in other aspects of intelligence, Churchill was directly involved. His interest and influence were strong, creative, and personal. Under his inspirational leadership, the author concludes, "the fragmented intelligence services acquired that degree of coordination which turned them into an intelligence community."

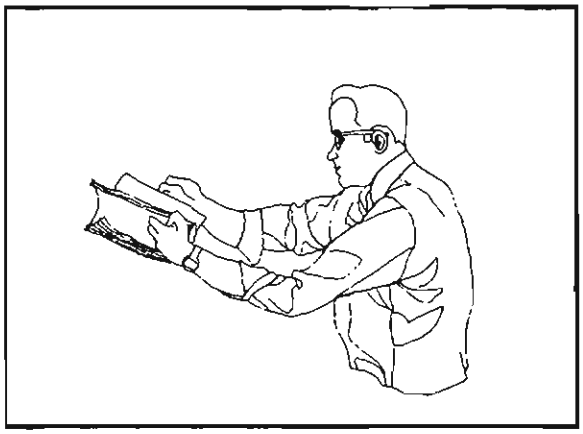
In the epilogue, "War and Peace," Dr. Andrew agrees with the now generally accepted opinion that signals intelligence made possible the victories in North Africa and the success of the Normandy landings. He summarizes in a few pages the main events in British intelligence since the war – the intensive and continuing collaboration between Britain and the United States in SIGINT; the revolution in air reconnaissance, first by the U-2, later by satellites; spies, more spies, moles, and defectors; and the still undiminished strength of the traditional taboos against discussion of the

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019711

intelligence community and release of information on peacetime intelligence activities.

This is a hefty work intended for serious readers, but Dr. Andrew's style makes it a pleasure as well as an education to read. Touches of wit and a dry humor come through especially in his accounts of spy-counterspy goings on. Some of these stories are too far out to be anything but true. □



Teleconferencing [a set of 37 papers] edited by R. Rao and R. Srinivasan, Van Nostrand, 1985

Reviewed by: [redacted] *P13*

This book is well edited and filled with information, and should be within reach of anyone concerned with high-bit-rate digital traffic. The papers aptly reveal the progress in video coding.

Video teleconferencing is gaining in popularity as a means of conducting business meetings. Two key factors in the spread of video conferencing is the digitization of the video signals and the use of compression coders to reduce the bit rates needed.

The first one-way videotelephone transmission took place in 1927 between New York and Washington D.C., and a two-way system, between Bell Labs and AT&T New York headquarters, took place in 1930. In 1971 the Picturephone service was introduced by AT&T. 3-bit DPCM coding was used to reduce the bit rate to 6.3 Mbps, carried on a T-2 digital carrier, which was technically advanced at that time, but the service did not have many customers. Satellite transmission changed that, and now a wide variety of teleconferencing services is available in European countries under the umbrella of the EUTELSAT, a consortium of 20 countries in the European Telecommunications Satellite Organization. At present, the substitution of videoconferencing for business travel amounts to only 0.003%, but this is expected to increase to 6% by the 1990's, (more than a 1000 fold increase), according to a NASA study included in the book.

The fundamental problem of providing video teleconferencing is the signal bandwidth and the cost, which are linked. In the US, analog transmission of video using "soft" video scrambling has been done, but the international trend seems to be digital compression. A seven-nation European COST 211 project resulted in a transmission format and a codec to operate at the CCITT 2 Mbps rate. It will code both European 625-line and US 525-line video frames. Encryption will be available using the DES algorithm, according to the author of Paper #23, and a public key exchange was planned.

The video coding techniques can be classified into two categories, predictive coding and transform coding. The 8-bit PCM coding of a video frame requires 90 Mbps, but different coding techniques described in the book show how this can be reduced to much lower rates.

P.L. 86-36

"Full motion" codecs can operate in the 6.3-to-.5 Mbps range, and a number are already on the market. The dedicated T-1 1.5 Mbps carriers cost $30,000 per month, so there is a search for lower bit rate codecs. A British GEC codec at 1.5 or 2 Mbps is widely used in Europe. NEC also has produced an excellent codec with motion compensation --- to give smooth picture continuity when rapid subject movement occurs.

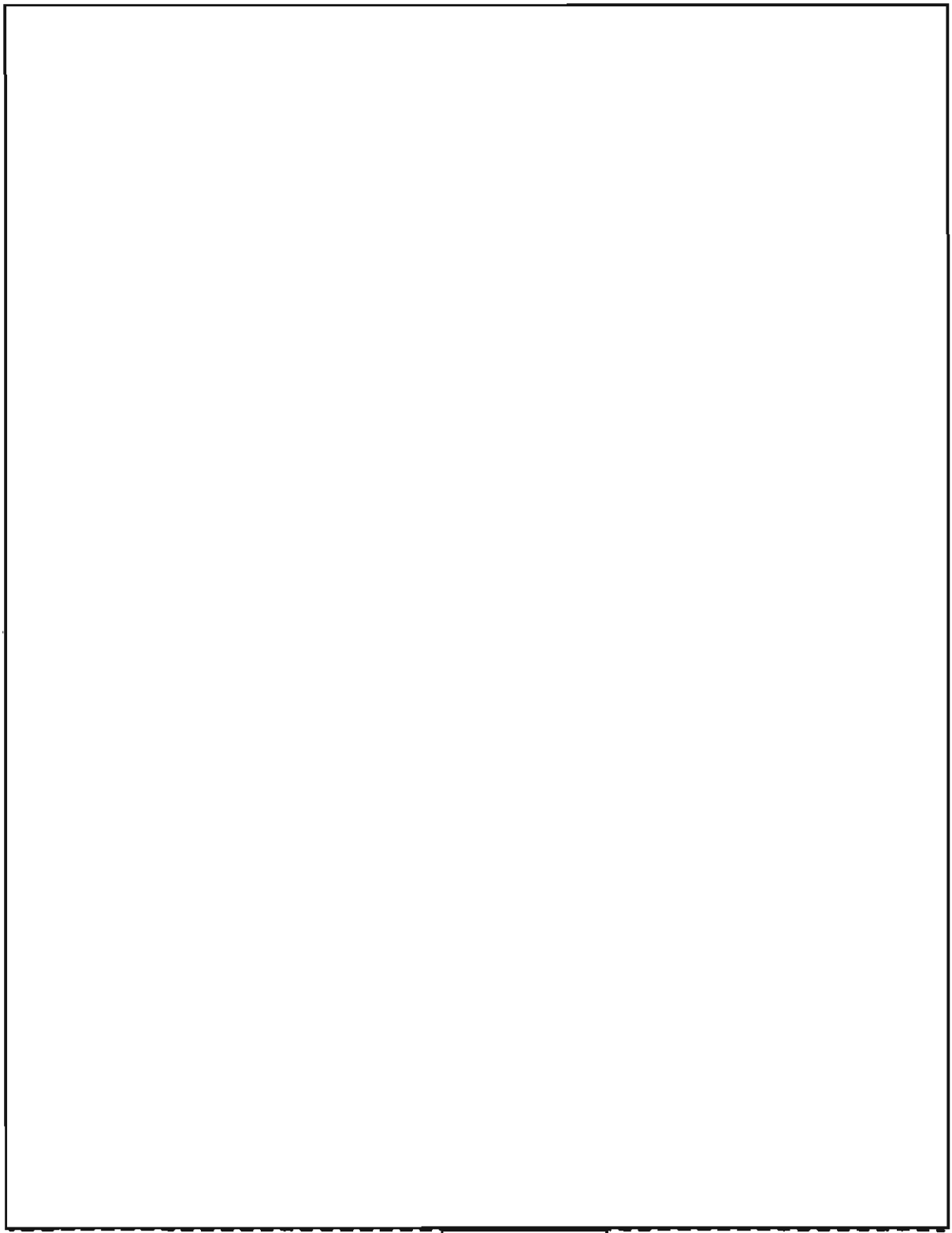
Part IV of the book is concerned with codecs that work in the range from 320 Kbps down to 4.8 Kbps. Many users accept the lower quality of 56 Kbps codecs to avoid the high costs of the T-1 carriers.

As ISDN and IDN services provide 64 Kbps channels to subscribers' premises, the 56 Kbps codecs will become easier to use. There is a lot of product competition at each of the tariffed bit rates (6.3, 1.5 Mbps, 56, 9.6, 4.8 kbps) and these coded communications are certain to form an increasing part of future digital traffic. □

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019711

From the past



Contributed by: [redacted] *A112*

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

NSA-CROSTIC #65

P12

The quotation on the next page was taken from a plaque in the building. The first letters of the WORDS spell out the author's name and the title on the plaque.

DEFINITIONS

WORDS

A. Navy cryptanalyst, Battle of Midway fame

23 94 88 37 66 206 4 17 45

B. Unrestrainedly frank

211 3 6 10 15 99 109 121 129

C. Boreal phenomenon (2 wds)

194 115 91 27 40 8 207 173 123 71 55

60 80 162

D. Stage orphan

68 90 100 126 137

E. Photons, not meager mantas (2 wds)

127 98 146 70 141 28 42 142 113

F. Haggard; depicted

79 116 133 179 210

G. Perhaps the shortest everyday word with 4 Rs.

168 48 164 13 33 65 82 86 101 122 143

147

H. Issues

148 185 160 138 50 19 72 125

I. Nevertheless

12 54 124 67 29 201

J. Askew

73 77 131 181 151 104 57 62 56 32

K. Versatile aircraft

108 84 22 7 186 183 180 176 170

L. State named by its British discoverer after his homeland (3 wds)

9 14 36 43 63 96 114 139 172 174 177

184 205

M. Maine (2 wds)

192 208 212 102 128 135 152 157

N. Tout le monde

202 166 161 145 132 47 34 26 200

O. A 32nd note

103 191 197 58 69 92 107 112 118 144 149

154 167 204

P. Zoological specialty

31 39 41 59 81 117 105 95 75 49 1

Q. Fire

156 171 199 5 195 203 190 136 83 74 53

24 35

R. Of hearing

21 119 30 38 97 2 64 196

S. Voluble

18 198 178 169 140 130 120 93 85

T. Crush

163 51 20 16 153 188 11 175 87 158 76

U. Crushing

193 187 110 159 134 111 165 182 209 44 52

61

V. Holmes's chambered mollusk

78 89 106 150 155 189 25 46

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019711

HOW TO SOLVE A DOUBLE-CROSTIC

Using the Definitions, fill in whatever Words you can. Then copy each letter from the Words into the corresponding square of the grid. Scan text in in the grid from time to time; from the recovered fragments you may be able to complete the word in context. Copy the new entries in the grid into the Definitions, where the fragments might suggest the complete Word, and so on, working back and forth. Also, scan down the first positions of the Words as you recover them, for additional clues.

1 P	2 R	3 B		4 A	5 Q		6 B	7 K	8 C		9 L	10 B	11 T		12 I
13 G	14 L		15 B	16 T	17 A	18 S		19 H	20 T		21 R		22 K	23 A	24 Q
25 V	26 N		27 C	28 E	29 I	30 R	31 P	32 J	33 G	34 N	35 Q		36 L	37 A	38 R
39 P	40 C		41 P	42 E	43 L		44 U	45 A	46 V		47 N	48 G	49 P	50 K	51 T
52 U	53 Q	45 I	55 C	56 J		57 J	58 O	59 P	60 C		61 U	62 J	63 L	64 R	65 G
66 A		67 I	68 D	69 O	70 E	71 C	72 H	73 J	74 Q	75 P	76 T		77 J	78 V	79 F
	80 C	81 P	82 G		83 Q	84 K	85 S	86 G	87 T	88 A	89 V	90 D		91 C	92 O
93 S	94 A	95 P	96 L	97 R	98 E	99 B	100 D		101 G	102 M	103 O		104 J	105 P	106 V
	107 O	108 K	109 B	110 U		111 U	112 O	113 E	114 L	115 C	116 F	117 P		118 O	119 R
120 S	121 B	122 G	123 C	124 I		125 H	126 D	127 E	128 M	129 B	130 S	131 J	132 N		133 F
134 U	135 M	136 Q	137 D		138 H	139 L	140 S	141 E		142 E	143 G	144 O	145 N		146 E
147 G	148 H	149 O	150 V	151 J	152 M	153 T		154 O	155 V	156 Q	157 M	158 T	159 U	160 H	161 N
162 C		163 T	164 G		165 U	166 N	167 O	168 G		169 S	170 K	171 Q	172 L	173 C	
174 L	175 T		176 K	177 L	178 S		179 F	180 K	181 J	182 U		183 K	184 L		185 H
186 K	187 U	188 T	189 V	190 Q	191 O	192 M		193 U	194 C	195 Q	196 R		197 O	198 S	199 Q
200 N		201 I	202 N	203 Q	204 O	205 L		206 A	207 C	208 M	209 U		210 F	211 B	212 M

THE ONE AND ONLY WINNER!

[redacted]R822, is the only person to report success in finding the PLUS in NSA-Crostic No. 63, December 1986. He is also the author of NSA-Crostic No. 64, 2nd Issue 1987, the solution to which is given on the right.

Solution to NSA-Crostic No. 64

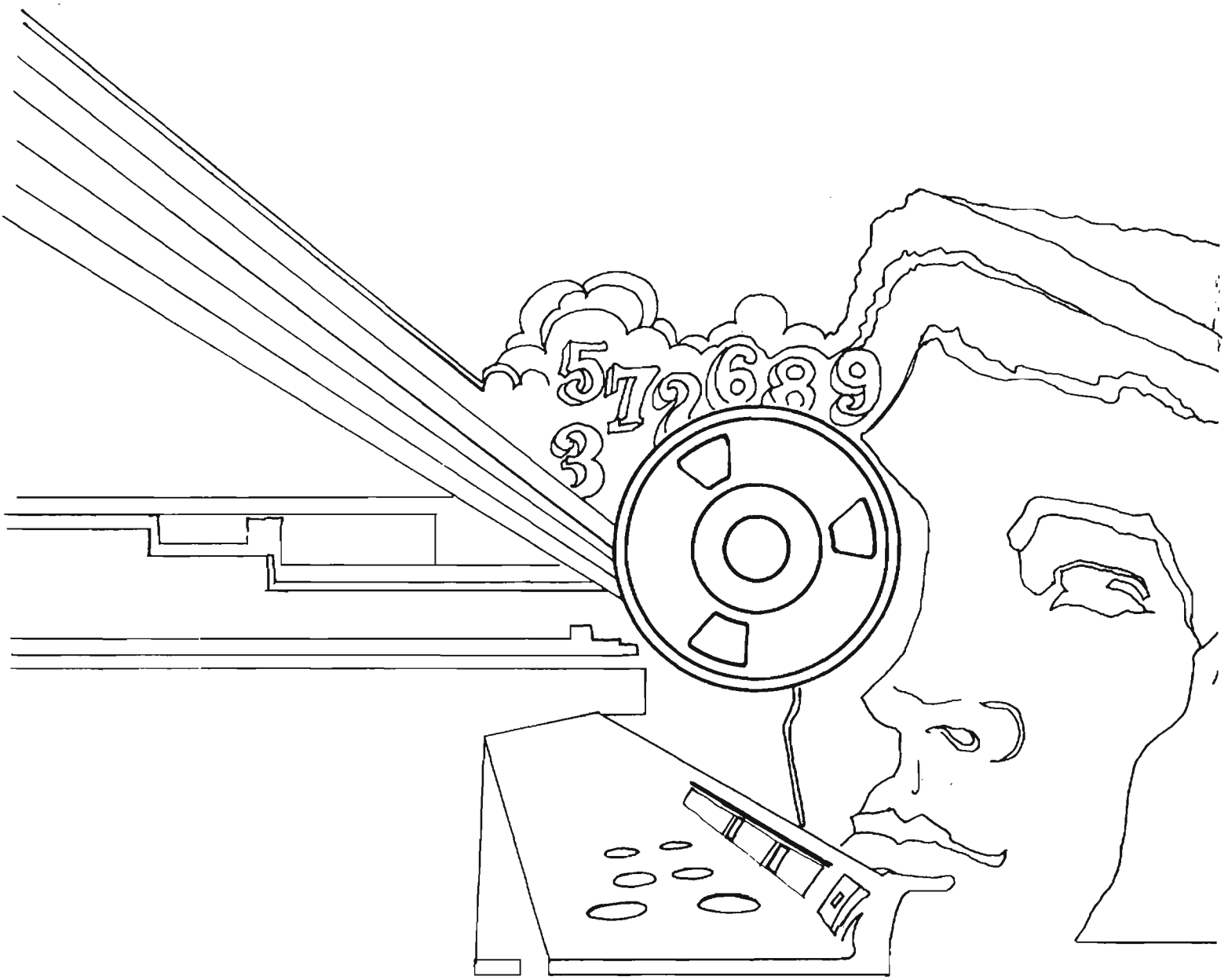
[William F.] Friedman, Lecture V, *Six Lectures on Cryptology*, National Cryptologic School, 1965 p. 116.

No code, [no matter how carefully constructed,] will be safe without trained, intelligent personnel. A poorly constructed code may be [in reality more] safe(r) when used by an expert than a [very] well-constructed one when used by a careless operator, or one ignorant of the dangers of improperly encoded messages.

Like to try your hand at composing an NSA-Crostic?
For instructions address your inquiries to HQS, P1, Puzzle Editor, CRYPTOLOG.

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~


5 7 2 6 8 9
3

DOCID: 4011703

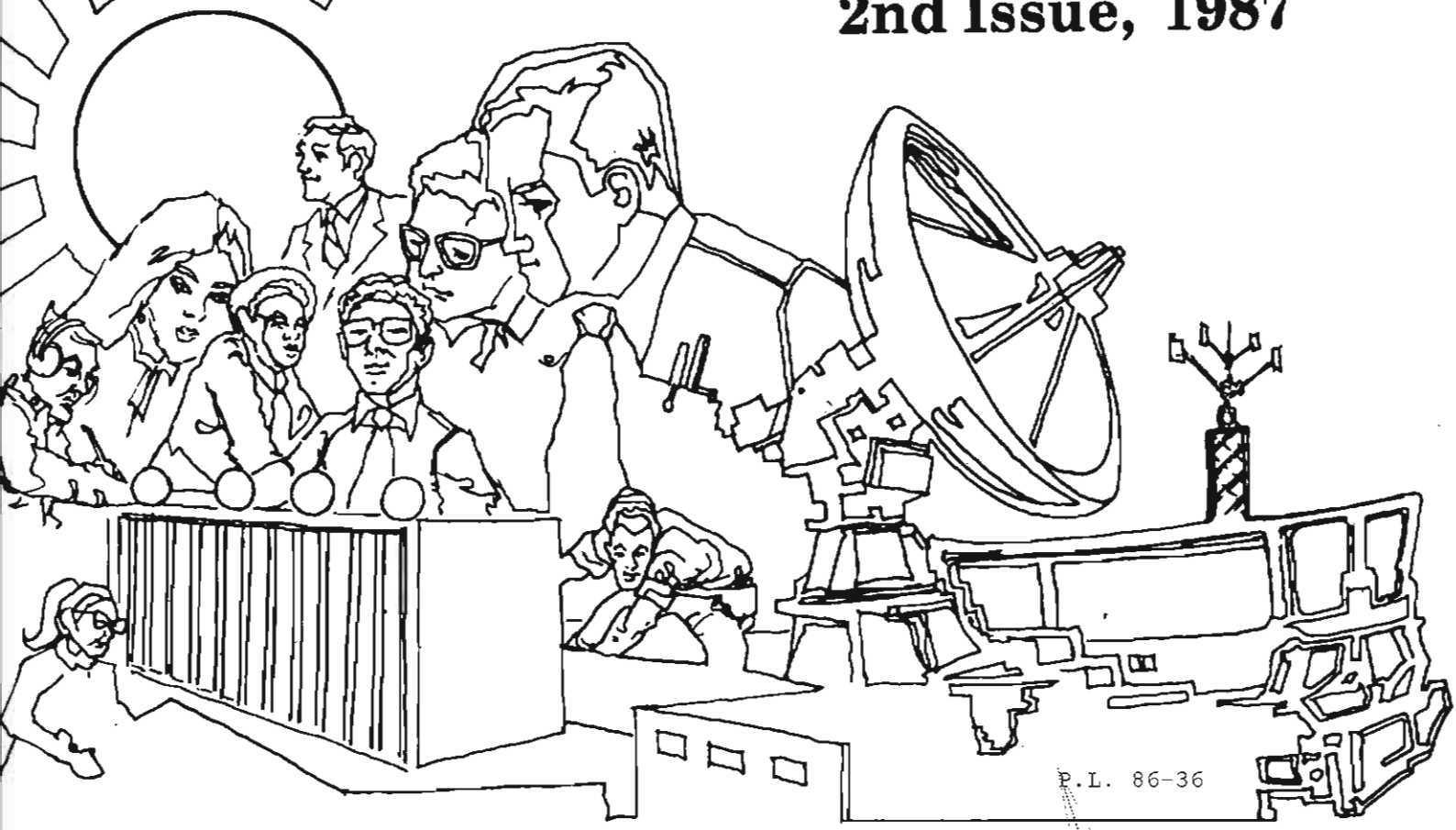
~~SECRET~~

Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

2nd Issue, 1987



P.L. 86-36

THRUST FOUR (U)	[redacted]	1
BULLETIN BOARD (U)		5
INFORMATION MANAGEMENT FOR THE FUTURE (U)	[redacted]	6
FOOD FOR THOUGHT (U)		8
MODEM COMMUNICATIONS (U)	Frederick Rodean	9
LETTERS (U)		16
THE RECKONING (U)	[redacted]	17
SOME TIPS ON GETTING PROMOTED, 3rd ed. (U)	[redacted]	19
CONTRIBUTIONS SOLICITED		29
GETTING STARTED		30
GOLDEN OLDIE (U)		31
NSA-CROSTIC No. 64 (U)	[redacted]	32
HOW RUSSIANS VIEW THEIR LEADERS (U)		33

~~NOT RELEASABLE TO CONTRACTORS~~

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

DOCID: 4011703

P.L. 86-36

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XIV, No. 2 ..... 2nd Issue 1987

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Collection ..... (963-5877)
Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Cryptolinguistics ..... (963-1596)
Index ..... (963-5292)
Information Science ..... (963-3456)
Information Security ..... George F. Jelen (859-1211b)
Intelligence Research ..... (963-3845)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (963-4958)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-4351)

Illustrators ..... (963-3057)
..... (963-6211)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five)
(note: no 'o')

Always include your full name, organization, and secure phone; also building and room numbers.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, HQS 8A187
Please do not phone.

Contents of CRYPTOLOG should not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

AVE ATQUE VALE

(u)

P.L. 86-36

There's a change in the masthead. who was publisher of CRYPTOLOG for six years, has moved to Z. They will benefit. He is taking to the Chief Scientist's Office what he brought to P1 and to CRYPTOLOG: a passion for the arcane arts practiced in this Agency; a concern about documenting current efforts to benefit our successors; an active interest in the storage and retrieval of information; and an enviable skill in expository writing.

Happily, he is not lost to CRYPTOLOG. He has merely become its friend rather than its publisher: almost the first thing he did in Z was to pass on some items for publication, and he has since helped us in other ways.

Good luck, Glenn, on your new assignment. We look forward to our new association with you.

We are most pleased to welcome as the new publisher. He comes to us from G4, where they practice esoteric disciplines. He is a natural for CRYPTOLOG, as he is noted for the breadth of his technical knowledge, his championship of passing on the torch, and for his singular gift of explicating highly technical matters to non-specialists. That's what we're all about!

Welcome aboard, Joe! P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011703

The Director's

Thrust #4 (U)

P.L. 86-36

Z

This article is classified ~~CONFIDENTIAL CCO~~ in its entirety

This was the Keynote Address at the 1987 session of the annual seminar series, CA-305, Contemporary Issues in Cryptanalysis. At the time the author was Chief, P1. P.L. 86-36

I want to tell you today about the Director's efforts to preserve and enhance the practice of cryptanalysis in NSA. He has given his personal attention to doing so and has involved top level managers also.

Shortly after he became our Director and got his feet on the ground, General Odom enunciated a number of goals for the Agency. He called them "Thrusts" to emphasize that they were to involve present action, not just remote hopes. Briefly stated, the five SIGINT thrusts are:

[redacted]

P.L. 86-36

[redacted]

The one of most interest to us as cryptanalysts is Thrust #4, and it is this:

[redacted]

The thrusts played a prominent part in a Future Sigint Capabilities Study and have been used as bases for planning and budgeting.

Last year General Odom held a series of status reviews of all of them, including two review sessions for Thrust #4. One session focused on computers and one focused on personnel. Specific questions posed beforehand by the Director set the stage for these reviews.

The first review session, held on 8 Oct 86, concerned computer support for cryptanalysis. It was attended by DIR, DDIR, Chief of Staff, several Key Component Chiefs including DDO, Chiefs of A, B, and G Groups, and the Chiefs of A5, B6, G4, and P1. The Director had asked:

EO 1.4.(c)
P.L. 86-36
DOCID: 4011703

Update on the Supercomputer Research Center: Any Actions Dir Should Take?

ADDR Marlin Wagner discussed NSA's unique needs and applications for massive parallel processing and described SRC progress to date.

[redacted] We intend to integrate up to ten NSA professionals in the SRC staff. When it achieves full staffing and operational capabilities in 1988, the SRC will be the [redacted]

After some discussion, the Director stated his intention to visit the SRC facility and to encourage the Center to intensify both recruitment activities and the assimilation of NSA integrees. He also wanted to see a research plan for the SRC.

What is the Significance of Recent and Anticipated Tech Transfers for our Lead in Cryptanalysis?

[redacted]

After considerable discussion of our technical transfer strategy, the Director said we needed to rethink our strategy on high-technology exports in order to recoup a measure of good will and cooperation with others in the government community, especially the Commerce and State Departments.

What Should we be Doing about the Semiconductor and Supercomputer Industries?

The concern is that we might become dependent on Japan, for example, for electronic components to use in building computers and special-purpose devices. Chief Scientist K. Speierman had already discussed this question with the Director, so it was not pursued further.

The final question for this session was:

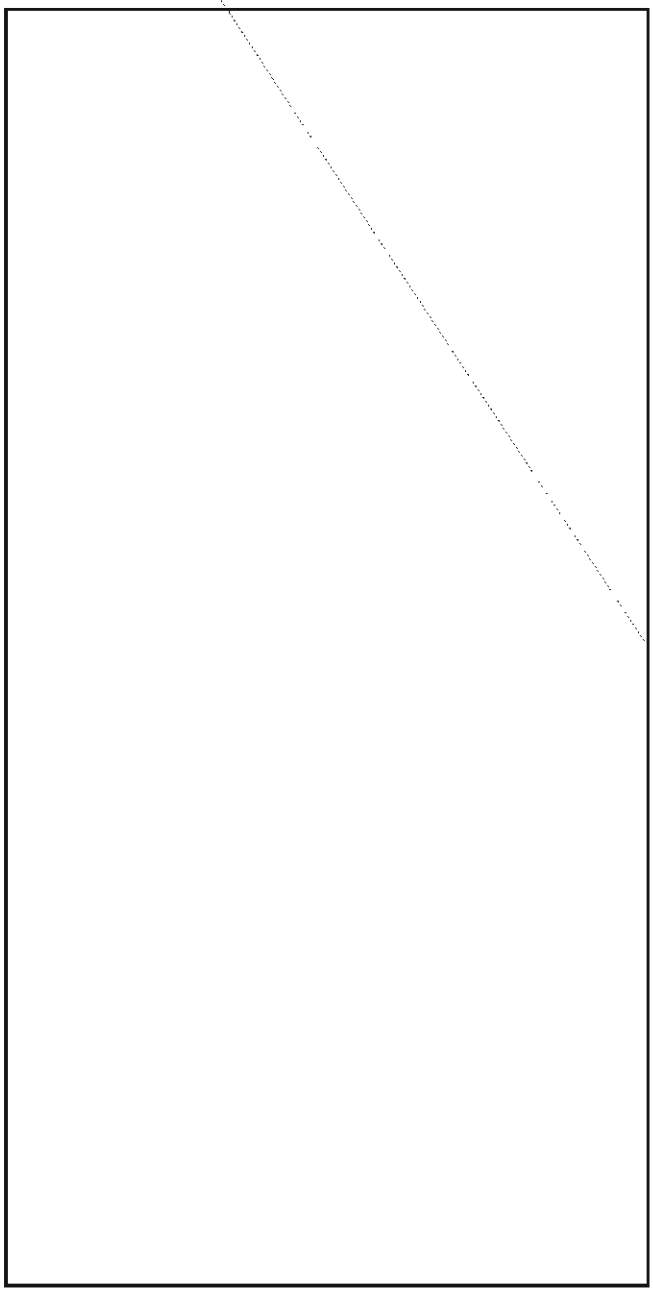
What is the Status of our Computer Acquisition Programs?

How do they fit with Anticipated Parallel Processing Approaches and our Expections of the SRC?

[redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
DOCID: 4011703 P.L. 86-36



The second review session, held on 9 Oct 86, concerned personnel. It was attended by the same people. The Director's first question was:

Will We Hire Enough New Mathematicians?

DDA Lou Bonanni outlined NSA hiring requirements for mathematicians, the present recruiting program, and some potential problems. One problem is that we are not offering PhD mathematicians a competitive starting salary; another is that American mathematics graduates are declining in numbers at all degree levels. However, DDA believed he could meet the hiring goal for mathematicians this year. A discussion followed in which several points were made:

- the reason we succeed in hiring PhD mathematicians (who sometimes pass up higher starting salaries elsewhere) is because of the large variety of interesting and difficult problems at NSA;

- cryptanalytic mathematicians are becoming more and more necessary in other disciplines such as signals analysis, hardware design, and speech research.

NSA once had an old-boy network of academic mathematicians who had worked in cryptanalysis during the war, who were extremely useful as consultants, and who recommended NSA to their students. This network has mostly disappeared. The Director stated he wanted us to enhance our recruiting methods, aiming particularly at PhD mathematicians (it was agreed that such an effort would also help the recruitment of Masters and Bachelors Degree mathematicians).

What Should We Do to Get More Use from IDA/CRD?

ADDR Marlin Wagner suggested the question should be, "What should we do to get even more use from IDA/CRD?" Those present at the meeting agreed that the contributions from CRD were of high quality and very valuable. The Director expressed satisfaction and there was no further discussion.

The Director's last question was:

What is the Status of Our Last Look at Internal Talent and Inter-Component Relations on Cryptanalysis?

The Chief of P1 (that's me) reported that a group of senior Agency cryptomathematicians from P, R, and S had been organized to

consider the need to attract more outstanding mathematicians to NSA, either as employees or as consultants. This group had held one retreat at the Maritime Institute of Technology And Graduate Studies (MITAGS) and had scheduled a second one the same week as this review to plan a Mathematical Sciences Day at NSA for about 50 prominent American mathematicians.

I also said I believed we had an excellent inter-component technical exchange situation involving A5, B6, G4, X1, R51, IDA/CRD, [redacted] I mentioned the regular seminars (GRABS, the R51 monthly seminar, monthly CMI and KRYPTOS lectures); the Annual Cryptomathematical Exchange (ACE) and annual SCAMP programs; the ad hoc week-long sessions on specific problems; the rotational tours of CA interns, Cryptologic Mathematician Program members, P1 personnel, and others.

Cryptomathematicians at NSA know each other and are able to communicate with each other as needed. (Manual cryptanalysts, however, are in a somewhat different situation, and some changes need to be made; this was not discussed at the review but is being pursued with DDO.) I repeated the earlier view that cryptomathematicians were needed much more widely throughout the Agency than just in cryptanalysis. There was some discussion, and the Director expressed the desire that we determine future skill needs, both qualitative and quantitative, for cryptanalytic work.

Following this meeting, too, the Director assigned a number of tasks addressing issues raised during the review:

- He asked DDA (with DDO, DDI, and DDR) to organize a recruiting team of high skill and polish to seek high-quality mathematical talent for the near term.

In response, the MITAGS group worked with M3 to identify Agency mathematicians who should be part of such a team. Also, the Math Sciences Day was held on 6 January 1987; 46 prominent mathematicians attended, some old friends and others new to us. Their expenses were paid and they were housed and fed at the Maritime Institute.

General Odom gave a welcoming talk at NSA in the morning; he said he had two problems he wanted their help with: one problem is how best to operate his proposed program of mathematical research grants [redacted] and the other is how to attract high quality mathematicians to NSA. His talk was followed by some general talks and then some technical ones.

The afternoon program at the Maritime Institute included some unclassified descriptions of math at NSA and how we use mathematicians, and more technical talks, followed by a long session at which we asked the visitors for advice and suggestions about the grants program and about recruiting mathematicians. We believe this meeting was very successful: the visitors gave us many good suggestions; we got some excellent publicity, judging from the feed-back; and we have begun to develop a new boy network that should help us recruit mathematicians in future.

I believe we should hold meetings like this every year.

- The Director asked DDA (with DDO, DDI, and DDR input) to propose for his approval a paper defining cryptanalysis in the context of future tasks and of what skills will be needed to do them.

This has been completed.

The definition is quite broad and includes some aspects of signals analysis, some engineering tasks such as the design of special purpose cryptanalytic computers, speech research,

EO 1.4.(c)
P.L. 86-36

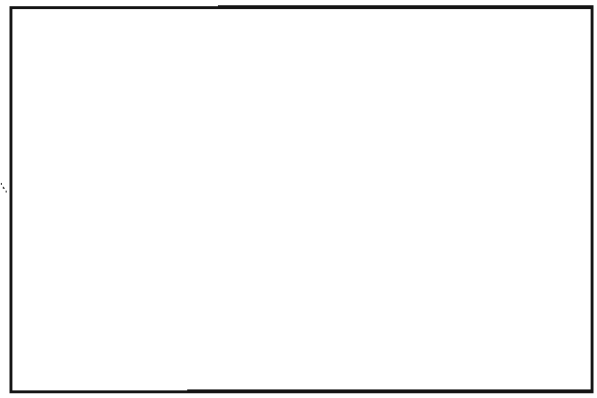
EO 1.4.(c)
P.L. 86-36

cryptographic system design and evaluation, some aspects of computer security and computer intelligence (a field I believe will emerge in future), and many aspects of computer science, as well as actual cryptanalysis.

- He asked DDPR (with DDO, DDI, and DDR input) to conduct an "unconstrained" assessment of the numbers of cryptanalytic personnel we will need, and report to him.

The figures emerging from this, all approximate, for actual cryptanalytic work just in Operations are:

P.L. 86-36



- He asked DDPR (again with DDO, DDI, and DDR input) also to conduct an assessment of the above constrained by reality, and report to him.

- Finally, he asked DDA and DDPR to take action to ensure that our COSC structure and Table of Distribution accommodate what is developed by the above.

These last three items are still in progress.

It seems clear that General Odom believes in cryptanalysis, is alert to present and future problems, and wants to do something about them. I encourage all of you to take time out occasionally from your daily tasks and give some thought to the future of our unique profession. I invite you to write down any ideas you may have for improving the practice of cryptanalysis here, for improving the lot of the cryptanalyst, or for any other constructive suggestions, and to send them to me in P1.

Let's help the Director help us! □

Editor's Note: A second review took place in July 1987, just as we were going to press.

BULLETIN BOARD

USERS' GROUP ON SUPERCOMPUTER-UNIX

~~(FOUO)~~ G4 and A5 have established a Working Group to coordinate efforts on supercomputers using UNIX. All organization with users on supercomputers are invited to participate. For more information get in touch with the chairman of the Working Group [redacted] G45, HQS.

P.L. 86-36

DEVELOPING SOFTWARE?

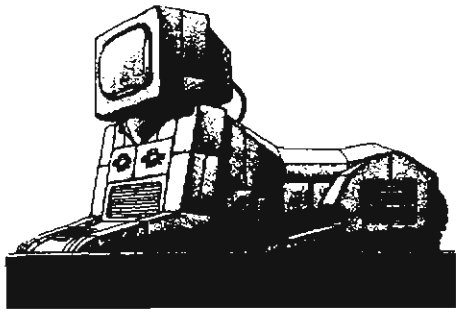
(U) The second edition of NSA Manual 81-3, *Software Product Standards*, is now in distribution. (For software acquisition the companion document is 81-2.) As DoD-STD-17-3(NS) it is also the DoD standard for use with contractors in software product development and acquisition. A copy can be obtained from T303.

SOFTWARE MANAGEMENT FOR UNICOS

(U) T335 is looking into software management systems for UNICOS. It is willing to investigate and evaluate commercial systems, and also to consider developing an in-house system under UNICOS. Potential users are invited to submit their desiderata (features required or desired) to Jim Bieda, T335.

DOCID: 4011703

INFORMATION MANAGEMENT FOR THE FUTURE (U)



T522

(U) John Naisbitt, in his book *Megatrends*, writes, "In the new information society, being without computer skills is like wandering around a collection the size of the Library of Congress with all the books arranged at random with no Dewey Decimal system, no card catalogue--and of course no friendly librarian to serve your information needs." Realizing the import on users, producers, and managers of intelligence information, NSA is taking steps to modernize its traditional information support services to SIGINT operations and to RDT & E efforts.

(U) The information explosion demands a revolutionary approach to keeping abreast of the needs of a knowledge industry. The Agency seniors, as articulated in an December 1983 NSA Advisory Board Report, mandated that a state-of-the-art information support system be developed. The report recommended that the information support system of the future deliver information directly to users via terminal/personal computer systems.

~~(FOUO)~~ The support system will be an integral part of the work life of analysts, managers, engineers, scientists, technologists, and office workers. Supporting these users will be information professionals who will lead in the planning, design, implementation, and maintenance of the system. The success of this endeavor depends on corporate planning, goal-setting, and focused leadership. T5 has been designated as the leader of Agency-wide information resource management. It plans to focus on several key fronts:

1) identifying and projecting hardware and software requirements;

2) determining proportion of centralized to decentralized support;

3) budgeting and control of expenses;

4) tasking;

5) identifying staffing and skill requirements;

6) providing education and training; and

7) assessing security requirements and limitations. P.L. 86-36

~~(FOUO)~~ Further, the advent of the personal computer has added a new dimension to T5's service philosophy "the closer to the customer, the better the service," and has redefined one-on-one service. Computer access will obviate the need for the preferred co-located support, which calls for placing an information professional in an operational element, and instead, enable that professional to provide tailored one-on-one support to several users almost simultaneously.

~~(FOUO)~~ Central to upgrading information support is the Electronic Information Center (EIC). The EIC will facilitate the interaction of all information support functions across organizational boundaries, with T5 as the central management authority. Key entry points for the EIC will be Central Reference, the Scientific and Technical Information Center, the Agency Standard Products Information Center (formerly the Personal Computing Information Center, PCIC), the Agency Records Center, and the Fort Meade Main Library. The EIC will make available major information support and delivery functions that can be accessed by a single log in. It will eventually electronically receive, organize, catalogue, control, process, and deliver all-source information, Agency wide, as needed to support the NSA/CSS missions.

~~(FOUO)~~ The EIC will be a series of personal computers and terminals, linked by a number of local area networks and the Agency Standard Host. The key to the success of the EIC is an easy-to-use, automated method of exchange of information and data among the system components. The programs that compose the EIC are:

▸ ~~(C)~~ [redacted] Primarily directed toward the support and upgrade of the NSA/CSS libraries and information centers, this program includes the functions provided by [redacted] and a planned acquisition module enhancement. [redacted] capabilities will include an on-line "card" catalog for all library branches, electronic logging of materials, overdue and availability notices, the generation of management and use statistics, material distribution, the status of inter-library loans, procurement documentation, periodical renewals, and mailing labels;

▸ ~~(C)~~ [redacted] provides direct support in the areas of information research and includes the development of [redacted] (the Time-Sensitive Support Center) [redacted] (commercial database exploitation and delivery), and the Automated Information Support System;

▸ (U) [redacted] applies to the receipt, storage, and distribution of the majority of incoming electrical and hardcopy messages and material. The primary projects are SOLIS, LEAFLET, WEEDER, DUSTBOX, DOORPLATE, and QUEENSWARE. Each of these programs addresses distinct intelligence collection, dissemination, and management requirements;

▸ (U) [redacted] modernizes life-cycle records management, with a storage and retrieval system to electronically and automatically archive information.

STATUS OF MODERNIZATION EFFORTS

[redacted] *Upgrade of Library*

(U) An Electronic Desk has been installed in the Geographic Information Center and was connected to the COINS network to allow on-line research and map display of COINS data. The center is also able to transfer maps to floppy disc for distribution to users.

~~(FOUO)~~ The Geographic Information Center is now able to produce maps on PCs using the PINSETTER software package developed by P14. PINSETTER enables the analyst to plot and track entities geographically on a PC screen.

(U) LS/2000, the integrated library system, is operational in the NSA/CSS Main Library. It houses cataloging records, which include book and periodical titles, authors, call numbers, book availability, and information on special collections. A feature of LS/2000 is the use of laser bar code readers.

(U) The ASPIC has expanded its role in production of software for PC and Office Automation (OA) users and will assume a role in the demonstration,acquisition, and distribution of ASH applications software as well. The ASPIC has acquired a Braille printer which enables the Center to produce working aids and tip sheets for the Agency's blind employees.

[redacted] *Central and Satellite Modules of the Electronic Information Center*

~~(FOUO)~~ T52 has started to implement [redacted] the automated system designed to transmit, store, and retrieve customer requests for information, references, and documents. The contractor developing and testing [redacted] has begun transferring [redacted] software prototype applications from a PC-base to the 3B20 ASH base. T52 is currently using the PC-based version of INFOREQ applications.

~~(FOUO)~~ Efforts continue in acquiring and accessing commercial databases for use on ASTWs via dedicated outside telephone lines. P.L. 86-36

~~(FOUO)~~ [redacted] a menu-driven gateway which provides access to multiple data bases, is being tested in Central Reference, the STINFO Library, and S2. Databases resident on [redacted] information retrieval systems are already available.

~~(FOUO)~~ [redacted] an automatic press delivery system, is now operational and available in the Media Center, formerly the Press and Cableroom, 2E099. [redacted] allows automatic delivery of news wire services to the floor of the National SIGINT Operations Center (NSOC). The Intelligence Watch Officer (IWO), a member of the NSOC team, uses [redacted] input to write the IWO Press Review which is distributed to headquarters and field elements.

~~(FOUO)~~ Conversion of the Press and Cable room has been completed with the delivery of 13 television monitor/recording consoles. Network news and other programs presenting information of concern to Agency analysts are monitored on over 13 channels. The ISO Intelligence Support Officer) supports the IWO and NSOC desks by monitoring and recording

broadcasts and publishing a video news summary. The ISO also makes operationally required video tapes on request.

[redacted] *Modernizing the Handling of Collateral Intelligence Information*

~~(C)~~ Several SOLIS-like systems have been designed to electronically store, disseminate, and retrieve collateral received by NSA. Those systems available on-line are:

[redacted]

[redacted] *Automation and Upgrade of the Office of Archives and History*

(U) The Office of Archives and History has acquired an IDM 500 database management machine for automated storage and retrieval of archival records.

(U) The Electronic Archiving Division is engaged in a joint effort with the National Archives and Records Administration to study the Optical Digital Image Storage System in order to evaluate the application of optical disk technology to archiving.

⇔

(U) In *Megatrends*, Naisbitt concluded that the most formidable challenge (of the move from an industrial to an information society) will be to train people to work in the information society. The transformation of T5 and its customers into providers and users of an electronic information support network will require a blend of many skills in computer science, intelligence research, information handling and management, personnel management, marketing, communications, and behavorial science.

(U) In order for NSA, a complex knowledge industry, to remain in the mainstream of the information society, the Information Management Group must meet the challenge to recognize and implement technological and personnel requirements. □

FOOD FOR THOUGHT

Extract from

The Office of the Future:
Information Management for the New Age

by [redacted] P.L. 86-36

published in Technology Review
December/January 1980

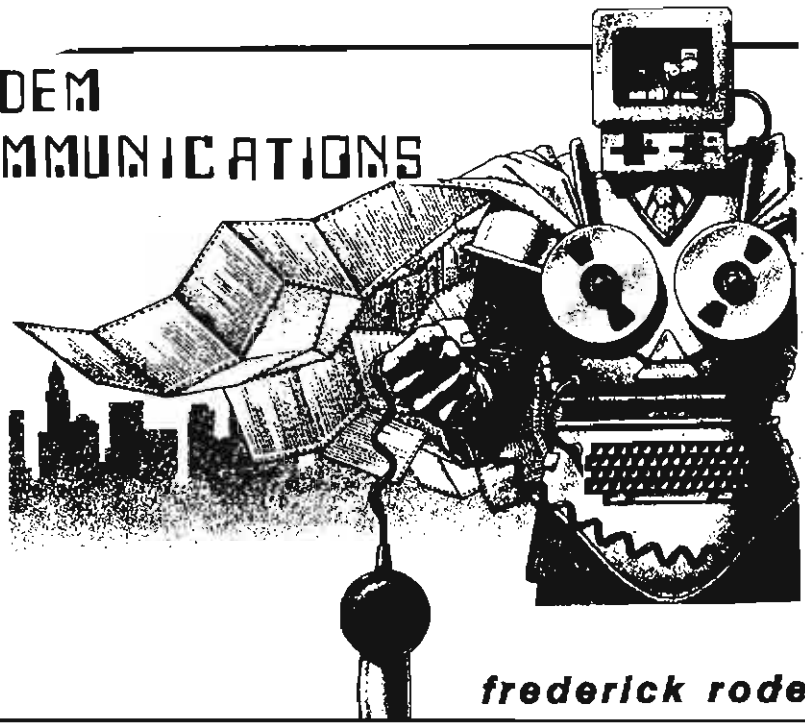
Though there is some variation from organization to organization and from job to job, surveys show that knowledge workers spend the major portion of their time absorbing or giving information verbally. Only a very small percentage of their time is typically given to "thinking" (less than 8 per cent) or to writing (less than 10 percent). The most frequent mode of activity is formal meetings (20 per cent and more in highly structured organizations); two-person conversation on the telephone (5 to 10 per cent) and travel (about 10 per cent) are also important. The proportion of intraorganizational or extraorganizational communication varies over a broad range; knowledge workers in large organizations spend almost all their time talking amongst themselves.

Electronic devices currently available have little direct leverage on the heavy communication loads of knowledge workers. Indeed, the impact of office automation on their personal working habits has been negligible. This is because the communication of knowledge workers is largely unstructured and ill defined. Where memoranda, reports, or procedures are needed, the bulk of the labor is delegated to supporting clerical or specialist staffs; here word processing, text editing, dictation, and facsimile equipment have a definite role. But the idea of automating the illusive, non-standard, and ever-changing communication patterns of knowledge workers remains difficult.

UNCLASSIFIED

DOCID: 4011703

MODEM COMMUNICATIONS [U]

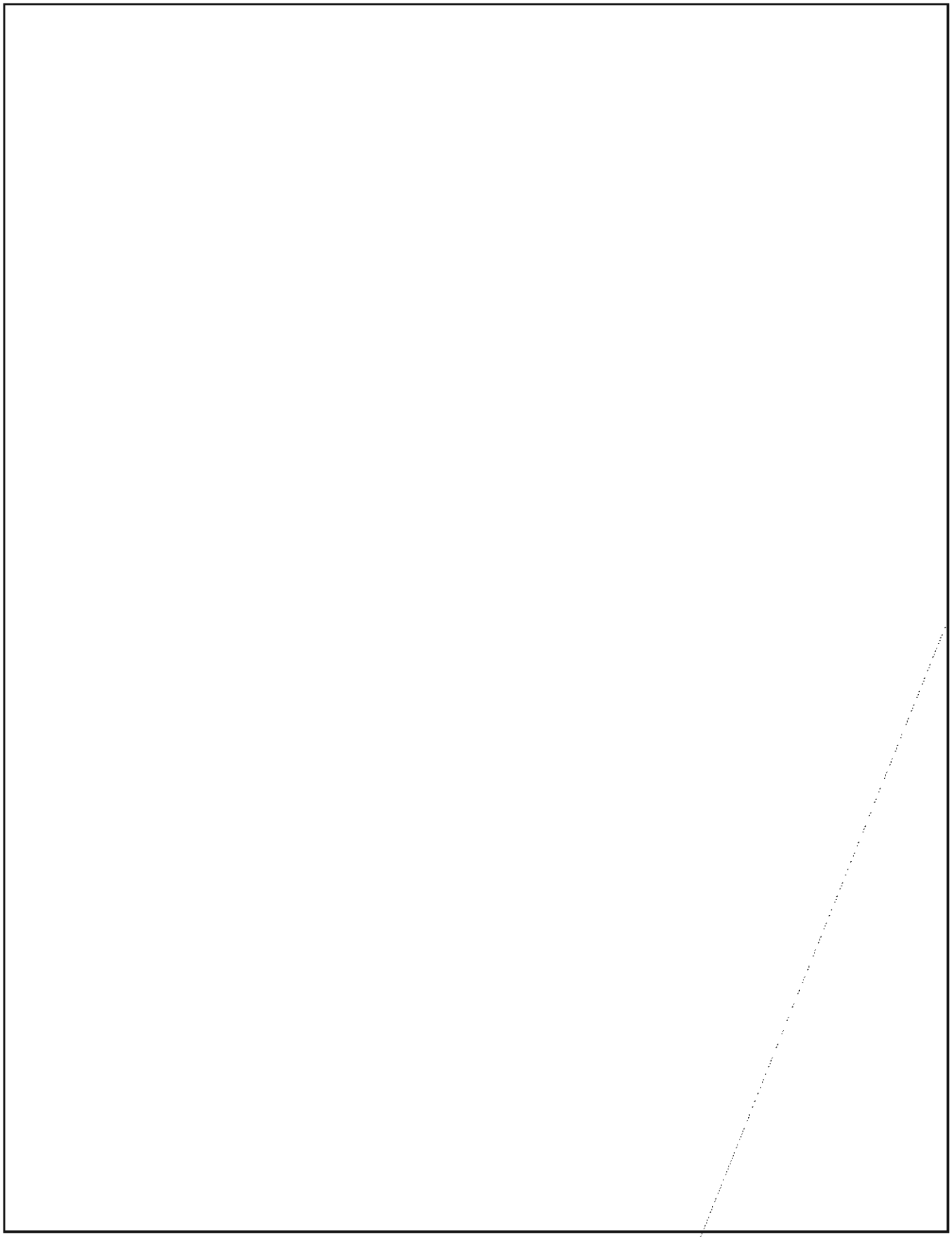


frederick rodean, g85

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~
~~NO CONTRACT~~

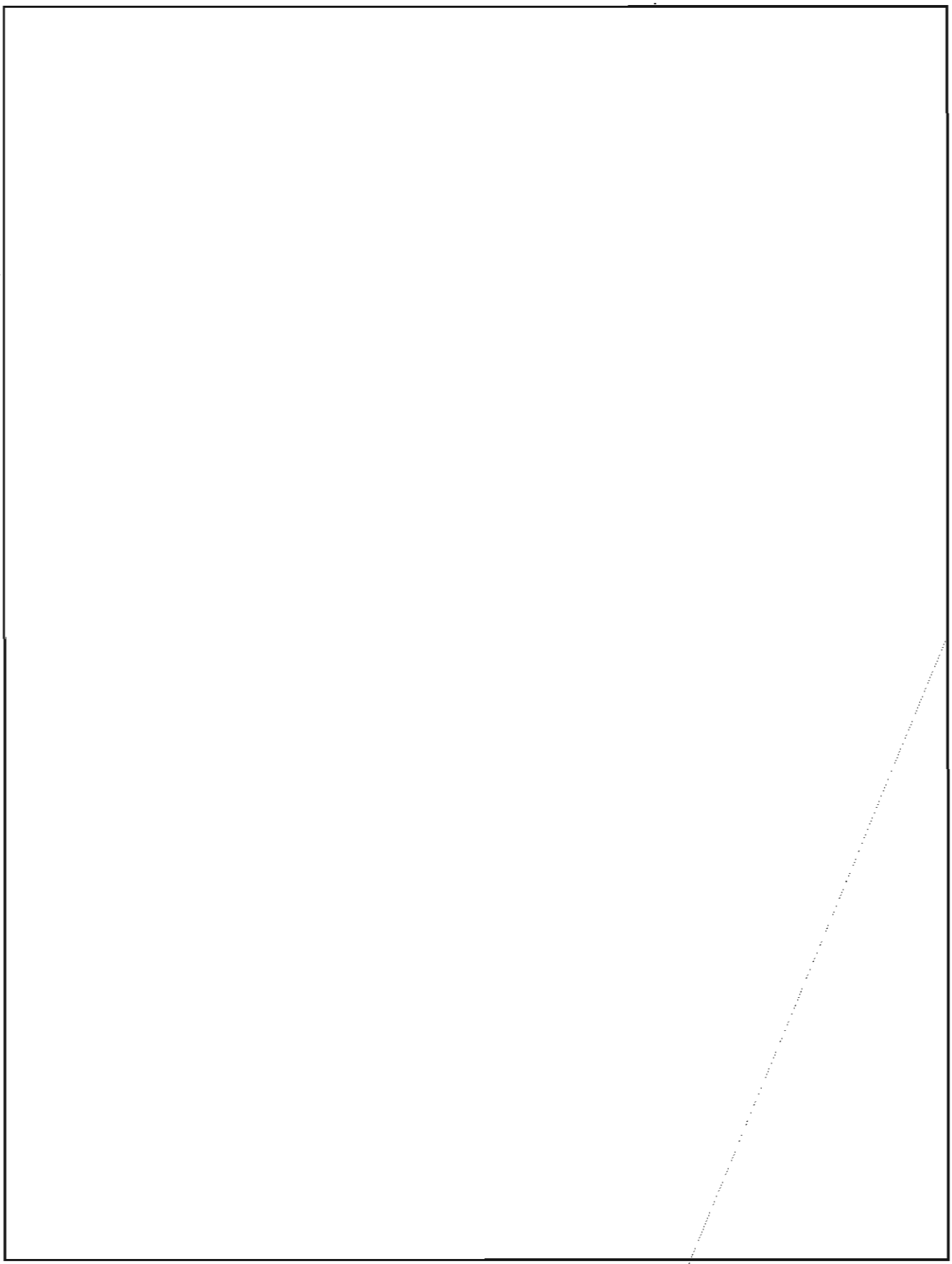
EO 1.4.(c)
P.L. 86-36

DOCID: 4011703



EO 1.4.(c)
P.L. 86-36

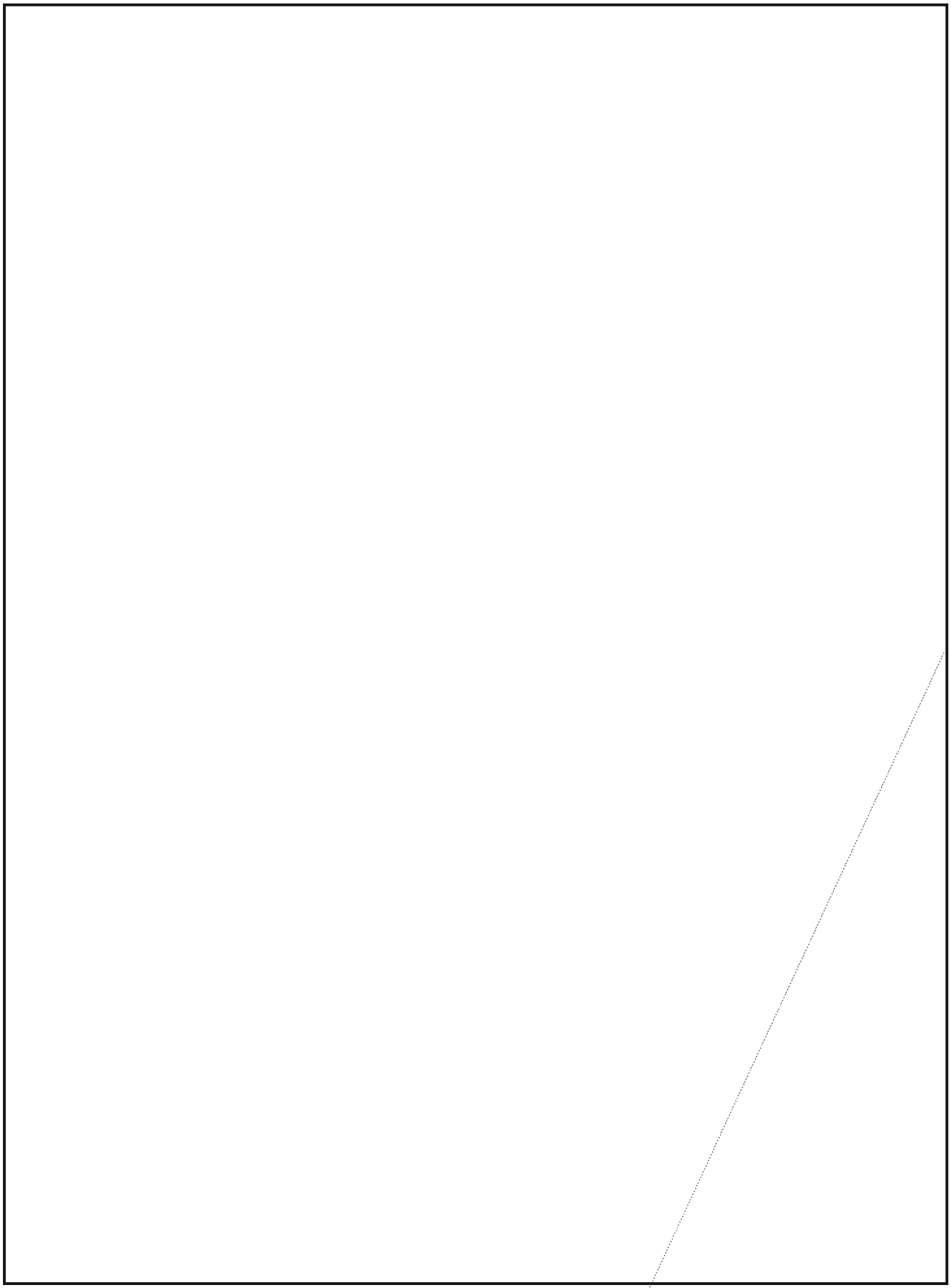
~~SECRET~~



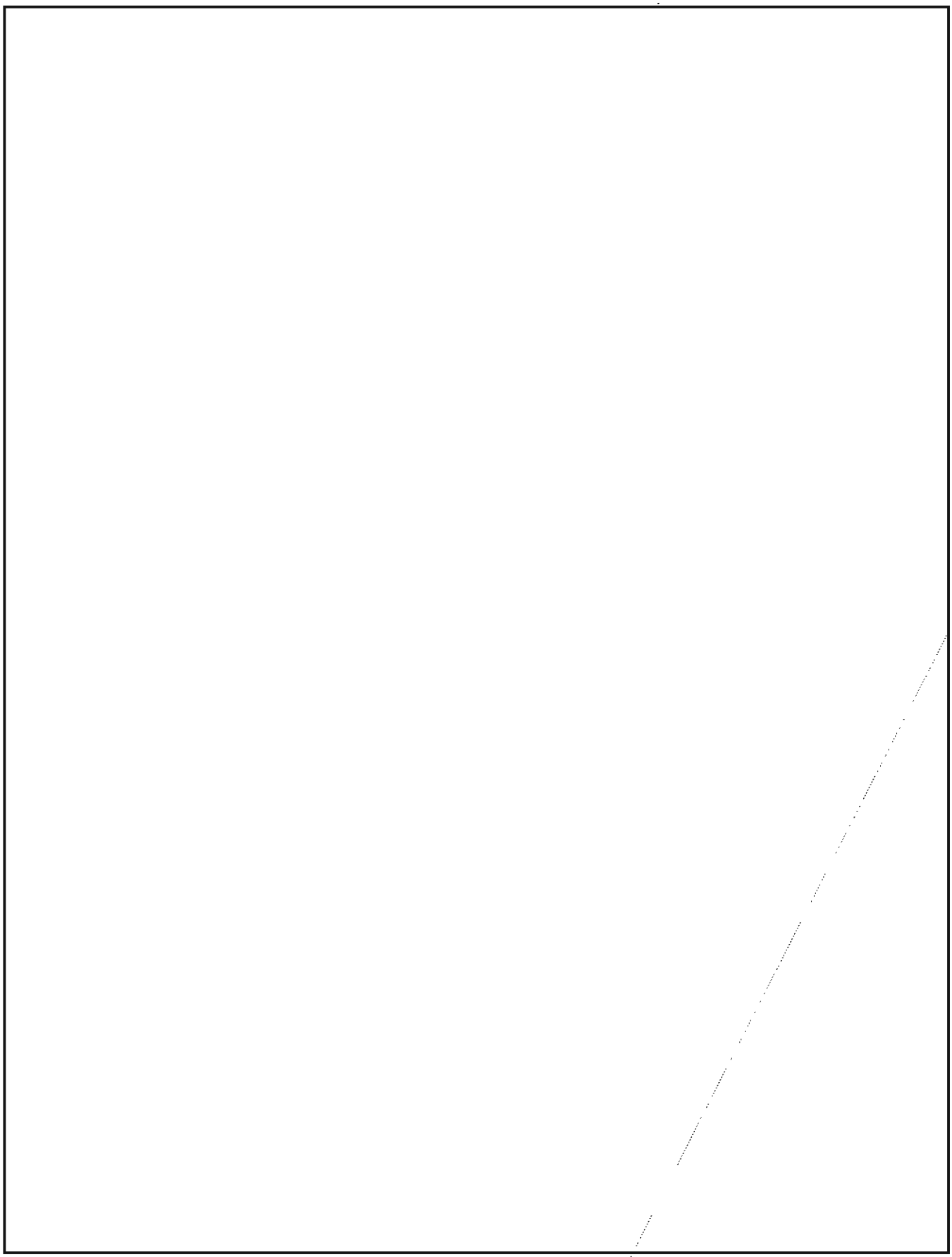
~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~
~~NO CONTRACT~~

EO 1.4.(c)
P.L. 86-36

DOCID: 4011703



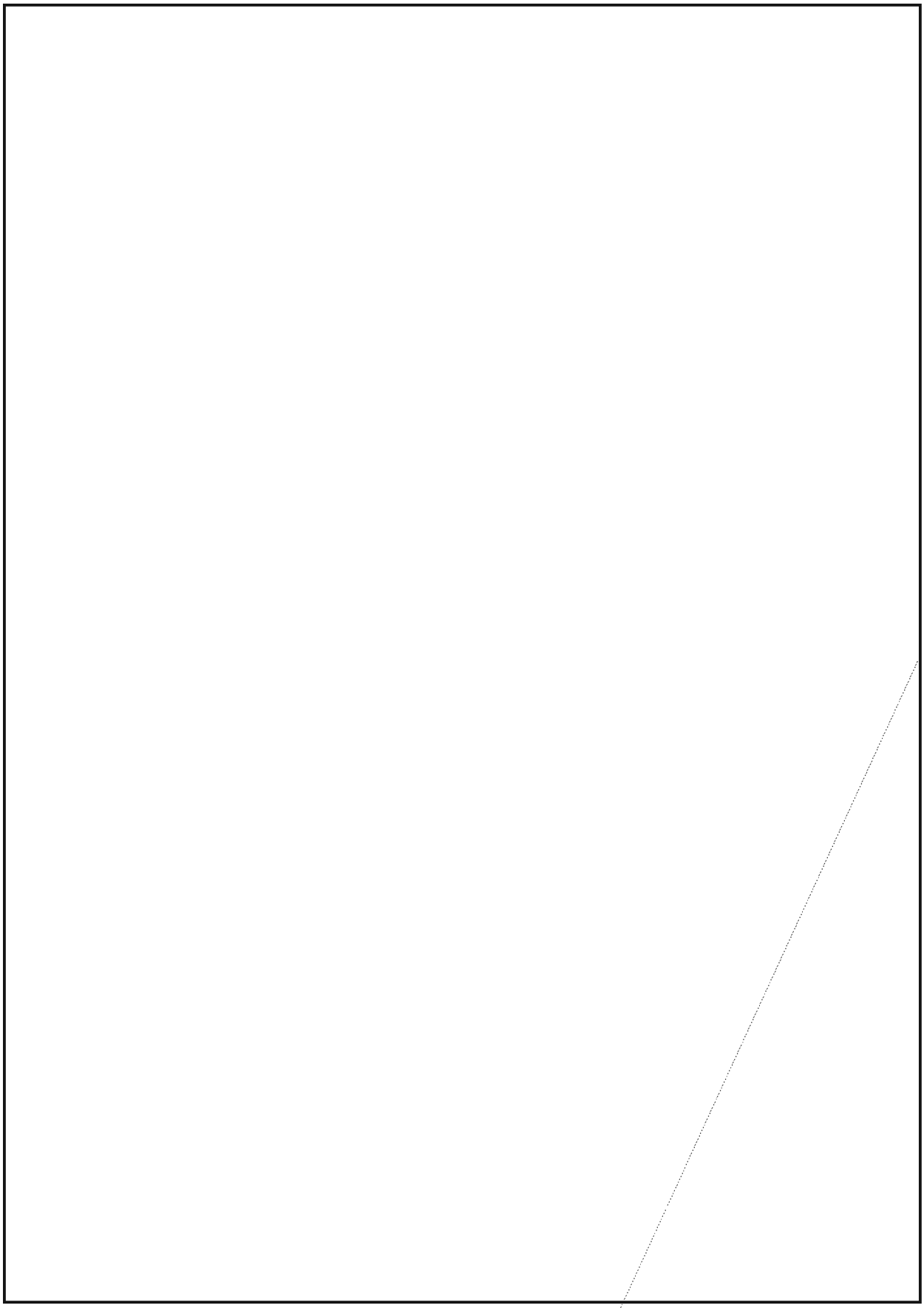
P.L. 86-36
EO 1.4.(c)



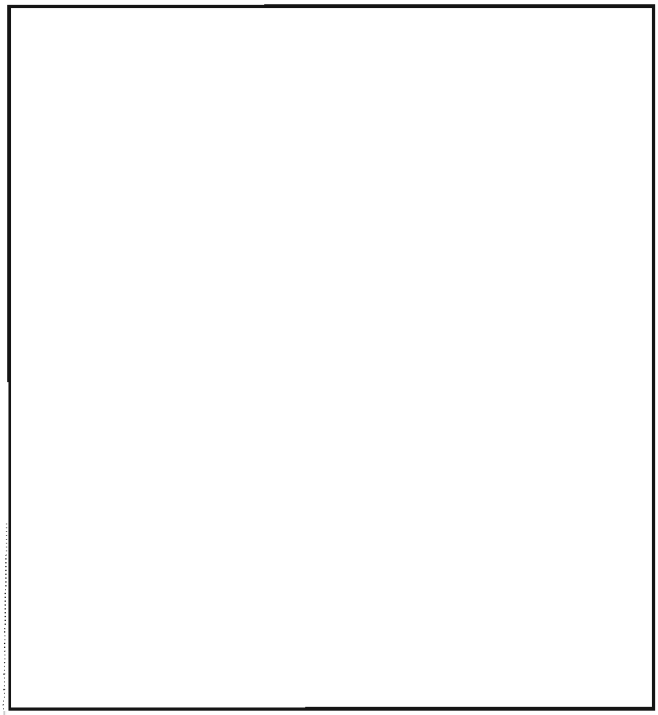
~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~
~~NO CONTRACT~~

EO 1.4.(c)
P.L. 86-36

DOCID: 4011703



EO 1.4.(c)
P.L. 86-36



(U) The trend appears to be towards to the establishment of integrated services digital networks (ISDNs). These networks will carry voice, data, and video information within multiplexed data streams by means of digital microwave, cable, fiber optic, and satellite transmissions. The structure of many of today's packet-switched networks has been designed specifically to facilitate the incorporation of ISDN technology. An ISDN is an end-to-end digital network that uses uniform transmission, signaling, and operating procedures. Access to the network and its associated services will be through a standard, physical interface using existing telephone systems.

(U) The key to ISDN is standards. A committee of telecommunications organizations in Western Europe began work in 1979 to develop standards for ISDNs. Today, ISDN standards are being further defined by the Consultative Committee on International Telephony and Telegraphy (CCITT), an international standards organization with a mandate to establish recommendations for end-to-end performance, interconnection, and maintenance of world networks of telephony, telegraphy and data communications. This group has already identified a number of fundamental standards of ISDN. Interestingly, though, planning for ISDNs has been progressing for at least seven years, it has only been within the past three years that the performance requirements for satellite networks have begun to take shape.

(U) The basic building block for voice, video and data communication in ISDN is a 64-kilobit per second channel, called a B channel. This same building block is used in existing digital telephony networks to transport pulse-code modulated voice-band signals. To achieve higher transmission rates, several B channels can be concatenated to form a channel with a bandwidth in excess of 64Kbps. The resulting channel is called an H channel.

(U) In existing telephony networks, signaling data for a communications channel is encoded within the channel, while in ISDN, it is carried in a separate, associated channel called a D channel. A single D channel can carry the signaling information for many B channels. This technique of separating the signaling channel from the data transmission channels is called common channel signaling and is fundamental to ISDN.

(U) A basic ISDN standard is the basic access interface. This 144-Kbps interface consists of two 64 Kbps B channels for voice, video and data transmission and one (16 Kbps) D channel for signaling. An alternate access interface for large organizations is the primary access interface. For North America and Japan, this is a 1.544-Mbps interface consisting of 23 (64-Kbps) B channels for voice, video, and data transmission and one (64-Kbps) D channel for signaling. In Europe and most of the rest of the world, the interface is a 2.048-Mbps interface consisting of 30 (64-Kbps) B channels for voice, video, and data, and one (64-Kbps) D channel for signaling.

(U) ISDN provides the flexibility of submultiplexing channels for applications that do not require the full 64-Kbps circuit capacity. It also supports packet switching, as well as the circuit switching found in existing networks. These capabilities provide great opportunity to maximize circuit capacity.

CONCLUSION

~~SECRET~~

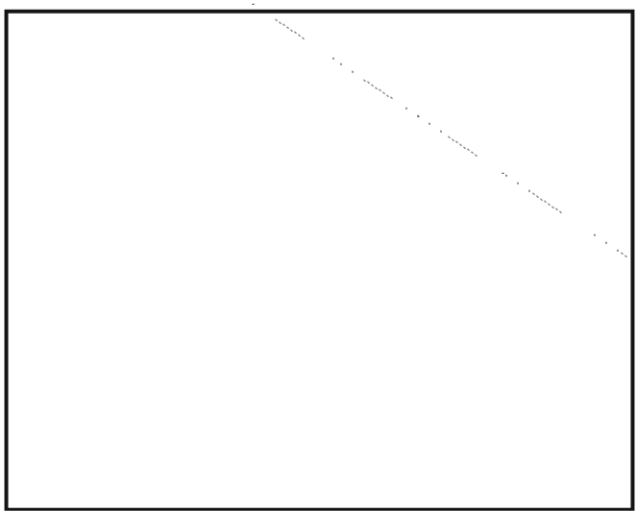
~~HANDLE VIA COMINT CHANNELS ONLY~~

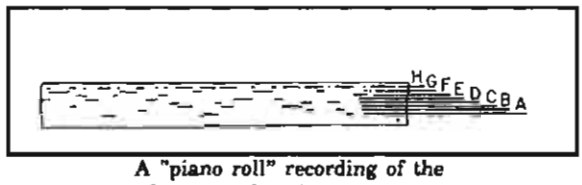
~~NO CONTRACT~~

EO 1.4.(c)
P.L. 86-36

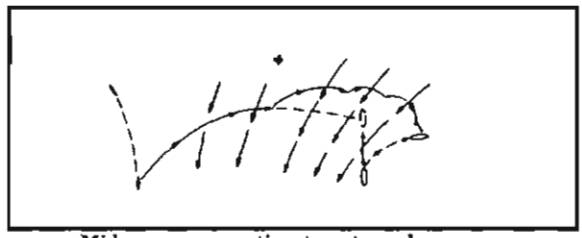
P.L. 86-36
EO 1.4.(c)

DOCID: 4011703
P.L. 86-36



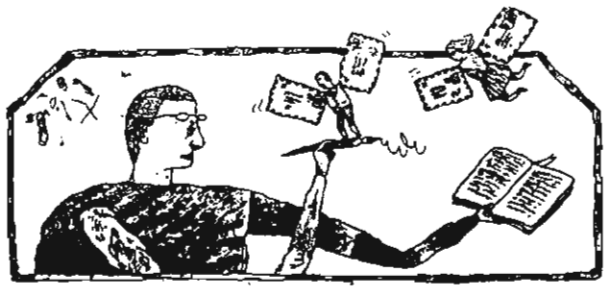


A "piano roll" recording of the frequency hopping sequence.



Mid-course correction to a torpedo course, made by FH-SR-SS communication from an observing aircraft.

LETTERS



To the Editor:

(U) Don't let anyone ever tell you that CRYPTOLOG isn't read. I've had calls from people I don't even know, also from people I hadn't heard from in years ... all because of the Hedy piece!

[redacted] *T542*

(U) We, too, have had calls about your intriguing piece, mostly expressing astonishment and delight at discovering that the glamorous Hedy Lamar was co-inventor of a frequency-hopping device.

(U) A couple of knowledgeable readers passed along additional information about the invention, including these illustrations:

(U) Co-inventor George Antheil had composed a multi-player-piano work in the 1920's entitled Ballet Méchanique.

Editor

To the Editor:

(U) On page 10 of the December 1986 issue, you made reference to the United Emirates Republic. A quick check of T5 Working Aid 03-86, "Independent Nations, Dependent Territories, and Their Capitols," dated October 1986, discloses that there is no such national entity. There is however, a *United Arab Emirates,* or the *Arab Republic of Egypt* (formerly, the United Arab Republic).

(U) I hope that not more than 10,000 sharp-eyed editors spotted this error and brought it to your attention.

P.L. 86-36 [redacted] *A2405*

(U) P.S. The date of this note, when compared to the date of issue of the December 1986 CRYPTOLOG, speaks volumes about the speed of distribution of your estimable publication.

(U) *We stand corrected. Thank you. Say, how'd you like to join up as a proofreader?*

Editor

(U) *P.S. Don't blame Distribution -- we're behind because our @#$+%¢&* terminal has been plagued with hard and soft crashes.*

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~
~~NO CONTRACT~~

DOCID: 4011703

P.L. 86-36

The Reckoning (u)

[redacted] P43

~~(FOUO)~~ Will NSA follow the US automobile industry into becoming a shell organization for offshore producers, sharing its intelligence market the same way Detroit shares its sales market with more aggressive and competent Asian and European suppliers?

(U) In *The Reckoning* David Halberstam gives a long and gloomy account of how the US automobile industry, a self-confident de facto monopoly in the late 1940's, stumbled and blundered into decline, while the Japanese fought their way into the US market and are now well on the way to replacing Detroit as the world center of the automobile industry. There are a number of fascinating parallels between the US automotive monopoly and the US SIGINT monopoly .

(U) Until the 1950's, the Japanese were so awed by Detroit's huge scale of production and technological know-how that they were afraid to go near the US market. They had seen in World War II that US manufacturing technology – in aircraft, ships, vehicles and equipment of every kind – was far superior to anything they could produce.

(U) Halberstam tells the story mainly in terms of the Nissan and Ford automobile companies, which exemplify what happened. The Japanese increased engineering education, and put their ablest people into manufacturing, in every industry they could restart. Henry Ford II, called back from the war to take over the ailing Ford Company, hired MacNamara and his statistical control people to give him control over the sprawling Ford organization. Over the next twenty-five years the Japanese systematically improved the engineering and manufacture of their cars, while at Ford (and GM) the manufacturing and "car" people steadily lost power to the financial managers who concentrated on keeping up the value of Ford shares to maintain the wealth and social position of Henry Ford II and the Ford family.

(U) The cutbacks and down-grading of manufacturing and of production people in favor of smooth, well dressed "management" people, and the no-risk, quick-profit manipulations led Ford into a complacent production of big, heavy, gadget-loaded cars that gave a high profit per vehicle.

(U) The resistance to new manufacturing investment is illustrated by the incident of the "E-Coating" process, which uses an electrically charged paint bath to get rustproofing paint into every crevice of the body pan. After the process was invented by Ford, GM obtained a license to improve their cars. The Japanese also did E-Coating under licensing. The Ford financial managers, however, rejected the investment cost, and their cars rusted away. It was twenty five years before the Ford production line converted to E-Coating.

(U) In effect, the financial managers became adversaries of the technical people who developed and produced the Ford products. They were profoundly ignorant of car production. For example, to avoid the cost of larger painting bays, MacNamara proposed building the cars in

DOCID: 4011703

two halves, painting them then welding them together. Henry Ford II had to intervene to block this folly.

(U) The managers grew in power, in spite of their ignorance of cars, by skilled intriguing. The financial managers, directed by Ed Lundy, who took over when MacNamara went to the Pentagon, managed to keep the stock prices high at first by avoiding investments and improvements, but Ford's market share eventually declined as customers bought elsewhere.

(U) Meanwhile, the oil shock of the mid 1970's gave the Japanese expanding access to the US market at the very time that Detroit de-emphasized compact cars. In a telling irony, when Chrysler tightened up its standards for suppliers to match the Japanese quality control and low spoilage, the Midwestern suppliers had to go to Korea to trade off the cheap labor for the new technology investments. This resulted in transferring even more US know-how and manufacturing power to Asian countries, and now they are competing in the US market with the US automobile companies.

(U) Detroit created an adversarial management caste which, by manipulating numbers and quick profit, gave the industry owners and stockholders the impression that they had perfect control of the current operations, when in fact they were losing control of their future to the Asians who paid more attention to technology and production. NSA may well be imitating Detroit by creating an adversarial management caste, with technology and production downgraded, cutback, transferred to contractors, or shipped offshore, in the name of maximizing quick-product and managerial control. Inevitably, there will be a reckoning. □

EO 1.4.(c)
P.L. 86-36

DOCID: 4011703

P.L. 86-36
CRYPTOLOG
2nd Issue 1987

SOME TIPS ON GETTING PROMOTED (U)

(3rd Edition)

Editor's Note: We are very pleased to present this update of an article which has been CRYPTOLOG's all-time best seller. The original, published in the December 1978 issue, was based on a talk given in April 1978 to WIN (Women in NSA); it has been reproduced thousands of times, as has a revised version which appeared in the June-July 1983 issue.

In anticipation of many requests for the 3rd Edition as well, we will have offprints available. For copies send your name, organization, building, room number, and number of copies desired, to: Offprints, CRYPTOLOG, P1, HQS, 8A187. Phone requests will not be honored.

Promotion. The word inevitably stirs response of some kind in every red-blooded NSA employee: hope, pleasure, challenge, despair, frustration, disappointment; even inertia, resentment, resignation. Despite disparate views on promotion, most people share -- openly or secretly -- a common desire to be promoted. And many also share, I believe, a common lack of understanding about the promotion process at NSA and a lack of knowledge about the part they play in it.

This article mainly addresses promotions to grades 13 through 15 and discusses two subjects which are fundamental to those promotions -- Personnel Summaries and Promotion Files. (The Personnel Summaries part also applies to persons in grade 15 for promotion to SCES or STE.) Both are critically important to you, the employee, because they are critically important to the promotion process at NSA. Witness these two points:

- *your Promotion File represents you to a promotion board,* and
- *you personally write only one document in that file -- your Personnel Summary.*

Promotion Files described in this article are the ones regularly kept for people in grades 13 and 14, for use by the two NSA-wide Boards that deal with promotions to grades 14 and 15. These Promotion Files are described in the final section of this article. Promotions to Grade 13 are handled by the Grade 13 Boards in each Key Component; almost all of them also maintain promotion files, with Personnel Summaries, on their Grade 12 employees. Promotions below grade 13 are handled at various local levels and their practices on the maintenance and use of promotion files vary.

Personnel Summaries are important to everyone, regardless of grade. For grades 13 and 14, the formal promotion process requires that every Promotion File, hence every Personnel Summary, be reviewed during every promotion cycle. Personnel Summaries are also used by many of the Key Component Grade 13 Boards, as well as by some of the local boards for grades up through grade 12. (I once chaired a local promotion board in my parent organization, S1, and we routinely reviewed Personnel Summaries of grades 2 through 11 each time we met.)

Personnel Summaries have still other uses: for overseas assignments; for transferring to new jobs; for some types of training. Whenever, in fact, official information on you and your career is needed, the Personnel Summary may be used. The first and major part of this article presents tips on how you should write your all-important Personnel Summary.

The ideas in this article are my own. I was not an expert on personnel matters when I wrote this article in 1978 and did not mean to appear to be. I wrote it as a result of my experience as a member of the NSA Grade 14 Promotion Board that year. In 1980 I chaired the NSA Grade 15 Promotion Board, and later (1981-82) served as a member of the Advisory Panel on Executive Development (APED) which selected candidates for SCEDP. The Executive Development and Qualifications Panel (EDQP) has replaced APED, with expanded responsibilities. The EDQP, a subordinate panel of the Senior Personnel Board (SPB), also evaluates qualifications of potential candidates for the Senior Cryptologic Executive Service (SCES) as well as for service schools and other selections.

DOCID: 4011703

These groups all still use employees' promotion files (including the Personnel Summary) during the review process. Files on Grade 15 employees are centrally maintained in M4 and are available for use as needed. All of these experiences have simply confirmed long-held impressions and reinforced my belief about the critical importance of the two topics covered in this article.

PERSONNEL SUMMARIES

Many consider Personnel Summaries to be the bane of their existence. Some don't take them seriously. Others fill them out casually. And most of us write them because we are forced to. Whatever you feel about Personnel Summaries, you should recognize why a Personnel Summary is important, who is responsible for filling it out, when it should be filed, and how to get it filed.

Why Important?

Why is your Personnel Summary important? Because it is an essential document in your Promotion File, the one that describes your complete NSA life: your jobs, your accomplishments, your training, your awards. It is no secret what things are deemed desirable for promotion. The information you provide in your Personnel Summary constitutes a list of the very things judged important when selecting people for promotion, to any grade. Your Promotion File represents you to the Board; it is one of the most important sources of information about you available to them. Board members cannot be expected to have personal knowledge of you in a large Agency like NSA. True, if you are fortunate enough to be nominated for promotion, then a written recommendation about your accomplishments and qualifications is included in your Promotion File. But a new Promotion Nomination form, instituted in August 1986, specifically directs that information available in the Personnel Summary not be duplicated on the Nomination Form. So, YOUR PERSONNEL SUMMARY IS IT! Since every Promotion File contains one and you write it, it is your chance to describe what you have done. No one knows it better. And if you do not say it, it may not get said at all.

Who is responsible?

Who is responsible for your Personnel Summary? YOU ARE!! You are responsible for filling it out initially (within 90 days after promotion to grades 12 through 14) and then for updating it. Do not expect your office to remind you. It is your duty. Though Personnel Summaries are not required for them, I also urge people in grades below 12 to fill out Personnel Summaries and to update them periodically. Get into the habit now, for it is easier to do it routinely and gradually than suddenly in one big lump when you become a 12. Also, I think it shows supervisors that you are a person of initiative with serious career intentions.

When to File

As I mentioned in the previous paragraph, you must update your Personnel Summary within 90 days after promotion to grades 12 through 14. I recommend you also do it whenever a major event occurs, such as when you: transfer to a new organization or job; become a supervisor or assume major new duties; receive a major award, professional certification, or educational degree. Otherwise, plan to do it annually, in synchrony with the promotion board cycles. Currently the Key Component Grade 13 Boards meet four times a year; the Agency Grade 14 and 15 Boards meet twice. If your updated Personnel Summary is in your file by 1 February or 1 September, you will satisfy all Boards. (Since both the Promotion Board cycles and members' assignments are now on a fiscal year basis, I recommend September.) I simplify updating my own Summary by following a practice I use to keep track of income tax deductions: whenever anything of importance occurs, I jot it down on a slip of paper with the date and stick the paper into a file. When the time comes to update, I have all the information at hand and the job is nearly done.

Tips on How to Write a Persumm

The following paragraphs describe ways to write a Personnel Summary. These are my personal ideas, and some people -- even you -- may not agree with them. So be it. But I hope to stimulate you to think seriously about Personnel Summaries and to try to help you to write a better one. My aim is to give you a start and hope that you will take it from there.

My best general advice is to be succinct. Say what you have to say briefly, concisely and clearly. Do not write the Great American

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011703

Novel and ramble on for 20 pages. On the other hand, avoid being too brief and selling yourself short. (I am surprised at the number of people who write one-liners!) Do not try to upstage Agatha Christie and write a mystery story, but avoid too much excruciating detail. Write your Personnel Summary so that a busy person, who is reading hundreds of Promotion Files, can understand and appreciate it quickly and, you hope, be impressed enough to single out your file for special consideration. Personnel Summaries are written on form P3267 (REV Sep 78) which is available in the NSA Supply Room, the M35 Integrated Personnel Activities (IPA's) and your office. And now, thanks to office automation, the form is also becoming available as software.

The first page contains seven items. Figure 1 shows the first four:

AS OF (date)	1. NAME (as it appears on official records) (Last, all capital letters)		(first)		(middle)
Feb. 1987	SMITH		JANE		ANNE
2. EMPLOYEE IDENTIFICATION (SSN)	3. CRYPTOLOGIC SERVICE MILITARY (i.e., ASA, AFSS, NSG, NSA) (years)	(months)	CIVILIAN (years)	(months)	4. TOTAL FEDERAL SERVICE
123-45-6789	3	2	12	9	15yrs 11mos

Figure 1

The "As of" date should never be over a year old. (Some files contain Personnel Summaries so ancient that the paper has turned yellow!) An out-of-date summary raises some rather unflattering -- to you -- questions in the mind of the reader. Are you lazy? Are you so disorganized you cannot remember to update it? Don't you care?

One sees many Personnel Summaries with only the dates changed -- the correction tape over the date is obvious in the reproduced copy. This is often done, and rightly so, to save retyping when there are no major changes to report. But what if there are important changes in your job and you don't record them? Look below at item 6, "Experience" (Fig. 2), taken from a supposedly current Personnel Summary:

6. NSA/CSS OR SCA CIVILIAN EXPERIENCE				
TITLE	GRADE	DATE OF ACTION	AGENCY	ORGANIZATION
A. CURRENT ASSIGNMENT (Functional/Job Title, e.g., Chief, Data Storage Equipment Division; if none, use job title reflected on 3160 or SF 50)				
Traffic Analyst	12	Jan. 1986		B111
B. TITLE OF LAST PROMOTION				
Traffic Analyst	12	Apr. 1984		B9
C. INITIAL ASSIGNMENT				
Analyst	5	Jun. 1958		ALLO

Figure 2

To the eye, Item 6 in Fig. 2 looks fine. However, this person is no longer a Traffic Analyst in B111. He has transferred to a new job -- a supervisory one -- and he is now Chief, Processing and Analysis Division, X35. BUT HOW IS THE BOARD TO KNOW?

The problem is magnified if this person is nominated for promotion. The documentation that accompanies the nomination describes the person's CURRENT job, with the result that the two documents -- the nomination and the Personnel Summary -- do not match. How does that look to a Board? Again, what does it say about you and your sense of responsibility?

When listing your current job title in item 6, be sure to use the FUNCTIONAL job title if you have one. For example: D/Chief, Data Storage Division; Project Manager for XXXX; Russian Language Instructor. Otherwise, use job titles as shown on the form.

Now let's go back to item 5, your educational record (Fig. 3):

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011703

5. EDUCATION (List most recent first)			
SCHOOL (Include Joint or Senior Service Colleges; also, any substantial work done toward a degree, but for which no degree was awarded)	DEGREE	MAJOR FIELD	DATES (If great span of time involved, indicate reason, e.g. (Night))
University of Maryland (Dean's List)	MA (20 credits	International Relations	1982 - present (Nights)
Armed Forces Staff College	Diploma		1980
University of Maryland (Cum Laude Phi Beta Kappa, Honors in History)	BA	History & Political Science	1972 - 1974
Anne Arundel Community College	AA	History	1970 - 1972
Bowie High School	Diploma	College Preparatory	1969

Figure 3

List these in reverse chronological order, with the most recent first. Include all education for which you earned a degree and use "Diploma" to indicate completion of a joint or service school. Also include substantial work toward another degree. If any of these took extended time, indicate why ("Nights"). And I suggest you state any graduation honors here, to highlight them.

Item 7, "Commendations and Awards," should also be in reverse chronological order. Fig. 4 shows some examples of the kinds of things to include.

7. COMMENDATIONS AND AWARDS (e.g. Meritorious Civilian Service Awards, Outstanding Performance Appraisals, Letters of Commendation from Chiefs of major organizations or higher) (List most recent first)	DATE
Letter of Appreciation, Chief A	1987
"E" Performance Rating - "our expert on UNIX"	1987
Special cash award (or QSI, or SSWP)	1986
Level 7 Performance Rating	1985
Outstanding Performance Rating	1982,83,84
First Prize, CIA Essay Contest	1981
Meritorious Civilian Service Award	1979
NCS Teacher of the Year	1970
NSA Scholarship	1958

Figure 4

Include Letters of Appreciation only if they are from a Chief of a major organization or higher (for grades below 12 I think this rule may be relaxed) and be sure that copies of such letters are in your Promotion File. List only whatever were top-level performance ratings of that period (i.e., when they had them, level-7, but not level-6). I suggest that you add any short complimentary quote from your Performance Appraisal to give it more substance, as "outstanding instructor," "most professional personnelist" or "THE expert." Also list any special Agency awards (cash or honorary) and scholarships you may have received. Professionalization certifications belong in Item 16, and extra-curricular activities should be entered in Item 14 -- do not include them here.

Page 2 of Form P3267 contains two items. At the top, Item 8 provides space for summarizing your "Current Assignment" (Fig. 5). Begin this paragraph by giving your functional job title, the name of your immediate organization, date of appointment, and names of ascending key organizations.

8. SUMMARY OF CURRENT ASSIGNMENT

D/Chief, Support Staff (Z13), Office of Facilities (Z1), Computer Services Organization (Z)

Since April 1986, Mrs. Jones has been responsible for managing . . .

Figure 5

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011703

Then list your major responsibilities, following these recommendations;

- *Use narrative style (not outline form);*
- *Use complete sentences;*
- *Use third-person forms (not "I was responsible for ..." but "Mrs. Jones was responsible for...").*

Note that your supervisor's signature is required in Item 8 as verification.

Item 9, at the bottom of page 2, is the "Summary of All Previous Civilian and Military Service of a Cryptologic Nature." This is probably the most difficult part of the form to fill out. The longer your career, the more you have to tell about. If there is not enough space provided in Item 9 to hold all the information requested, you should use as many additional plain sheets as necessary, labeling each with your name, SSN, and page number.

This is likely to be the longest section, so it is important to try to make it clear and readable. You do not have to be an accomplished writer or even to have any special writing skill. Just be direct, factual, and as concise as possible. Follow instructions given above for Item 8 (use narrative style, complete sentences, third-person forms).

In addition, follow these suggestions:

- *Use chronological order ("Begin with the oldest assignment and end with the most recent.") Note that this is not "reverse chronological order," as in some of the other items;*
- *Use one paragraph per job;*
- *Start paragraph with vital information: dates, functional job title, immediate organization and up;*
- *Identify organizations, projects, systems, etc.*

Notice that I said to identify "organizations, projects, systems, etc." Otherwise, you end up writing a mystery story, like this one:

"From August 1960 to January 1964, Mr. Smith was Chief of A13 where he was responsible for managing all aspects of Project SUCHNSUCH. He also provided technical assistance to several important systems under study by another division: XYZQ and ABCJ."

The only really clear thing in this paragraph is the date! Who remembers what A13 was in the early 1960's? What in heaven's name was SUCHNSUCH? What were systems "XYZQ and ABCJ"? And so on! How much clearer, and how much more professional, if this had been written instead (Fig. 6a):

9. SUMMARY OF ALL PREVIOUS CIVILIAN AND MILITARY SERVICE OF A CRYPTOLOGIC NATURE *(List in chronological order begin with oldest assignment and end with most recent; indicate location, functional/job title and dates)*

From August 1960 to January 1964, Mr. Smith was Chief of the Nonesuch Reporting Division (A13) in the Office of Overall Reporting (A1) in the General Analysis and Reporting Group (A). He was responsible for managing all aspects of Project SUCHNSUCH (full-text automation of Nonesuch reports) and provided technical assistance to several important systems under study by another division: XYZQ (system for automating . . .) and ABCJ (system for . . .).

Figure 6a

If you wish, you may use a space saving format, with an offset header (for dates, jobs and organizations) followed by a colon and a list, as in Fig. 6b:

9. SUMMARY OF ALL PREVIOUS CIVILIAN AND MILITARY SERVICE OF A CRYPTOLOGIC NATURE *(List in chronological order begin with oldest assignment and end with most recent; indicate location, functional/job title and dates)*

August 1960 to January 1964
Chief, Nonesuch Reporting Division (A13), Office of Overall Reporting (A1),
General Analysis and Reporting Group (A):

Mr. Smith was responsible for managing: SUCHNSUCH (full-text automation of Nonesuch reports), all reporting on . . ., and providing technical assistance to another division on several important systems, such as XYZQ (system for automating . . .) and ABCJ (system for . . .).

Figure 6b

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011703

These may seem like small things to you, but they have a big impact on improving the readability of your Personnel Summary. You do want people to read it, don't you?

As the final test, I recommend that you ask a friend to read your Personnel Summary critically to see if it is indeed clear and to the point. Preferably that friend should pretend that you are not a friend, but a complete stranger who wants to know everything about you. Does your Personnel Summary present you as a clear-writing (and, presumably, clear-thinking), forceful, direct person, or as an imprecise, vague person carrying out "various" unexplained duties? Rewrite your Summary, and especially Item 9, until anyone who reads it -- not just your friends who have known you for years -- can get a clear picture of what you have done and why you are promotable.

Page 3 of the form contains four items, the top three of which are often ignored -- or so it seems when they are so frequently left blank: "Field Assignments," "Related Experience" and "Publications." If you have pertinent information on any of these, put it in.

For Item 10, "Field Assignments" (Fig. 7), be sure to give the organization, functional titles and inclusive dates. These items are in reverse chronological order. Incidentally, regular updating of Personnel Summaries seems to be a special problem for people assigned to the field. Their Personnel Summaries are often neglected while they are away from Fort Meade/FANX and consequently promotion boards sometimes have no knowledge whatsoever about what the person is doing during an important 2- or 3-year period. I urge people to file yearly updated Personnel Summaries while they are on field assignments.

10. CRYPTOLOGIC COMMUNITY FIELD ASSIGNMENTS *(CONUS and Overseas) (List most recent first)*

ORGANIZATION	LOCATION	FUNCTIONAL/JOB TITLE	DATES
F06	Timbuck	Chief of Station	1983-86
F99	Eden	Engineer	1970-72
F17	Nowhere	Analyst	1965 (Jan - Mar)

Figure 7

For Item 11, "Other Civilian/Military Experience" (Fig. 8), include those things that may apply to your NSA job, such as teaching, managing and organizing. These are also in reverse chronological order. For example:

11. OTHER CIVILIAN/MILITARY EXPERIENCE WHICH MAY BE RELATED TO AN NSA/CSS OR SCA POSITION

ORGANIZATION	LOCATION	FUNCTIONAL/JOB TITLE	DATES
Army Reserve	Ft. Meade, MD	Platoon Leader	1976-Present
G.W. University	Washington, D.C.	Lecturer in Computer Science	1968-70
Summer Camp	Arlington, VA	Director	1965

Figure 8

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011703

Item 12 is "Publications" (Fig. 9). I am disappointed that so few files list any publications. Since publications are included in the Personnel Summary, NSA must consider writing to be an important skill. Managers, for example, must spend a lot of time writing. And good writing comes from practice.

Fortunately for us, NSA offers many opportunities to publish. If you have been looking for places to express your views, here they are: ***CRYPTOLOG***; *The Cryptologic Quarterly; The NSA Newsletter; CLArion, PQS Update; Vox Topics*. The editors of all these publications welcome your contributions. There are also essay contests sponsored by the Learned Organizations of NSA: CMI, CLA, Kryptos, HRMA, IAI, CISI, etc. And there are opportunities to contribute to the Cryptologic History Series and to NCS courses.

Try to have some published works and major reports (though not regular ones produced as part of your job) to list on your Personnel Summary. It just may help to attract attention to your file!

12. PUBLICATIONS *(List titles; do not confuse this with reports prepared as a regular part of the job)*	DATE
"Project SUCHNSUCH" — A Personal View — article based on talk given in April 1986 to the Computer and Information Sciences Institute (CISI)	CRYPTOLOG Dec. 1986

Figure 9

The next three sections, all part of Item 13 of the form, are meant to show "Highlights in the Area of Self Development" in your professional life -- past, present, and future. The format is the same for all three sections. Fig. 10 gives some examples for "A. Past." List here the things that are completed, such as past membership in professional societies and education not already listed in Item 5. Courses taken at NSA belong here, but not your college courses. Follow the example and identify the course by title and course number. In the rightmost column, you can indicate things like "Top Student" or special honors. You can leave this column blank if nothing applies.

13. HIGHLIGHTS IN THE AREA OF SELF DEVELOPMENT: *(Chronologically list all formal NSA/CSS/SCA, college level or technical courses (military or civilian) as well as membership in either NSA/CSS/SCA or external professional societies) (Exclude those for which a degree was subsequently awarded)*

	SUBJECT/SOCIETY	PLACE	DATES *(from - to)*	DURATION OR LENGTH	DEGREE	SPECIALTY/ OFFICE HELD
A. PAST	Zeta Eta Eta (French Honorary)	University	1965-68	—	—	President 1967
	MS-111 (Briefing Skills)	NSA	1968	49hrs	S	—
	MG-444 (Management Analysis)	NSA	1971	120hrs	A	Top Student
	CMI	NSA	1980-Present	—	—	Member

Figure 10

The first two items on page 4, the last page of the form, are "B. Present" and "C. Future" highlights in your self-development (sections not reproduced here). These sections are to be filled out in the same manner as "A. Past." Future plans might include such things as attaining another specified certification, changing your career field or joining a professional society.

Item 14, "Other Achievements" (Fig. 11), provides space for showing your self-development in your nonprofessional life. Many people leave this blank. If you do, I think you are missing a big opportunity to provide a rounded picture of yourself to the Promotion Board. If you are active in the areas like those listed below, I encourage you to list them. Show by your non-job-related activities that you have other interests -- and other talents.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011703

14. OTHER ACHIEVEMENTS *(In brief, list all NSA/CSS/SCA affiliate endeavors, which are not necessarily a part of your assigned duties, i.e., Civilian Welfare Council, GEBA, NSA/CSS/SCA club, etc; Civic or Community efforts may be included)*

ACTIVITY	INCLUSIVE DATES	CAPACITY IN WHICH SERVING/SERVED
NSA:		
Civilian Welfare Fund	1967 - 1969	B Group representative
Credit Union	1970 - 1973	Member, Board of Governors
GEBA	1972 - Present	Member, Board of Directors
NSA Jazz Band	1979 - Present	Member
Travel Club	1980 - Present	Member, President, 1976-78
United Givers Fund Campaign	1986	Keyman, B Group
Community:		
Church, Scouts, recreational activities, civic groups, PTA	(Provide the appropriate information)	

Figure 11

Item 15 (not reproduced here) provides space for you to list your job-related or self-improvement "Reading Achievements" -- in-house publications, professional journals, foreign language material. Please do not list your pleasure reading, especially not "Playboy." Board members have seen that one so often they are weary of it!

"Professionalization" certifications are to be listed in Item 16 (Fig. 12). If you have more than one, be sure to list them all, with the dates awarded. If you are about to receive still another, note this in parentheses, as shown:

16. PROFESSIONALIZATION *(List professional certification(s))*

CERTIFICATION		
TITLE	DATE	CERTIFYING PANEL (S)
Cryptanalyst	12 June 1976	Cryptanalysis Career Panel
Education and Training Officer	1 Sept 1983	Education Career Panel
Traffic Analyst (Lack only Part 3 of PQE for certification -- scheduled to take test in Nov 87)		

Figure 12

Finally, sign the form, date it, and affix the proper security classification. Take this responsibility seriously and do it carefully, seeking help from experts if you need it. Underclassi-fying or overclassifying looks bad to the board because boards expect that by grade 12 you should know how to classify correctly or know where to find help.

Instructions for filling out personnel summaries are contained in the "NSA Personnel Management Manual," Chapter 302B (Oct 79), which every major office has. Your own office will handle the filing of your personnel summary for you. It will reproduce multiple copies of it, some for retention in local organizational files, one for you, and (for grades 13 through 15), some for sending through channels to your promotion file in M4.

PROMOTION FILES

Promotion files are not to be confused with official personnel files, often called "201 Files." The Office of Personnel, specifically the M35 Integrated Personnel Activities maintain them. There is an Official Personnel File for every NSA employee. It documents all formal activity in connection with your NSA life: hiring, performance appraisals, training, job or organization changes, etc. There are official promotion files only for employees in grades 13 and 14. Local organizations often maintain abbreviated versions of the 201 File on their employees and some may also keep a promotion file. Official promotion files are the files that are being discussed here - the files used by the two Agency-wide promotion boards when considering people for promotion to grades 14 and 15. I am going to tell you what should be in your promotion file, how you can make arrangements to see yours, and how you can update it.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011703

Your Promotion File should contain:

- *Personnel Summary (current within one year);*
- *Certification documentation (in the form of a computer printout or a letter from the certifying Panel);*
- *Recommendation for promotion from Key Component, if you are recommended. (Since Promotion Files are shown to you intact, with nothing removed, you can see the recommendation on you if there is one.)*

In addition, your Promotion File should contain, FOR YOUR CURRENT GRADE ONLY (information from previous grades is purged):

- *Performance Appraisals;*
- *Inventory of Attributes (If you are 12 or above, this is part of your official Performance Appraisal. However, you may never have seen it or even know it exists because, until the late 70's, it was a private document and was generally not shown to employees. Nowadays the form is white but it used to be yellow and then green, and some files may still contain copies of the older forms.)*

  Figure 13 shows the form for the Inventory of Attributes. Rating is on a scale of 00 through 99, and space is provided on the right for narrative comments. Like the information in a Personnel Summary, the items in the Inventory of Attributes constitute a list of some of the most important things (in this case, personal qualities) judged desirable for determining a person's promotability.

  You may be concerned about the inevitable unevenness among supervisors' ratings on Performance Appraisals and Inventories of Attributes. Promotion Boards have access to detailed information (large computer runs) about all raters. This information shows them who the "hard" and "easy" raters are and helps the Boards to normalize the ratings.
- *Cash award and honorary award write-ups;*
- *Laudatory and commendatory correspondence. (Ordinarily these are to be from Chiefs of major organizations or higher. But if you have something noteworthy you would like to include, send a copy to: M43 Promotion Board Room, and let M43 decide.)*
- *Peer group ranking (was used in 1976 only);*
- *Individual Career Appraisal and Development Plan (used as part of the Performance Appraisal in 1975 only);*
- *Anything, since your last promotion, that might be beneficial, such as: letters from War Colleges, Invention Awards, Suggestion War Colleges, Invention Awards, Adjunct Faculty certificates from NCS, etc.*

P.L. 86-36

To review your Promotion File, call Mrs. Alice [redacted] M43, on 963-1677s or 688-7611b and make an appointment to see her, in Room 2B4132. You may talk to her about adding items to your file if you notice that something is missing. And if you disagree with something in your file or think that it is incorrect, call her attention to it. Depending on what it is, she may suggest that you discuss the matter with your supervisor, and then advise you about the possibility of your inserting something in the file to explain your views, as is usually allowed. M4 encourages you to look at your Promotion File and welcomes your help in keeping it up to date and complete. To insure that it is, especially if you have something important to add just at the time the Boards are conducting their file reviews, you should send a special copy directly to M43-Promotion Board Room as well as through official channels.

In conclusion, two points already mentioned sum up the main ideas with which I would leave you.

Your Promotion File represents YOU;

YOU write YOUR Personnel Summary.

Improve your promotability! Increase your chances of getting promoted by making sure that your Promotion File is complete and that your Personnel Summary is up to date and clearly written. It's up to you! □

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011703

SECURITY CLASSIFICATION, IF ANY

INVENTORY OF ATTRIBUTES
(Reference NSA/CSS PMM 30-2, Chapter 340)

GRADES 12 THRU 15 ONLY
(Prepare in triplicate)

DISCL. OF SSN MANDATORY. USE OF SSN AUTH BY EO 9397. SYS OF RCDS CREATED PRIOR TO 1 JAN 75; THEREFORE EXEMPTED FM REFUSAL PROVISION. SSN WILL BE USED TO VERIFY IDENTITY OF INDIV. ON THIS & OTHER ACTIONS RELATED TO THIS SUBJECT.

(1) SOCIAL SECURITY NO.	(2) NAME, (Last, First, MI)	(3) GRADE (e.g. GGD12)	(4) ORG

(5) DATES EMPLOYEE UNDER SUPERVISION
FROM (YR) (MO) (DA) TO (YR) (MO) (DA)

Supervisor's Data	(6) SOCIAL SECURITY NO.	(7) NAME, (Last, First, MI)	(8) GRADE (e.g. GGD12)

INSTRUCTIONS

Compare this employee with others in the same grade level regardless of the occupational specialty title. Assign your numeric evaluation using any of the numbers 01 through 99 from the scale shown.

90 - 99 Superior
75 - 89 Above Average
50 - 74 Average
25 - 49 Below Average
01 - 24 Poor

EVALUATION	ATTRIBUTE DESCRIPTION	NARRATIVE COMMENTS, IF ANY
(9)	A. INNOVATIVENESS: Consider how well the individual provides problem solutions, shows ingenuity and creativity, and pioneers in seeking new ways to complete work faster and more accurately.	
(10)	B. EFFECTIVENESS IN WORKING WITH OTHER PEOPLE: Consider how well the individual meets and deals with others, and effectiveness in establishing and maintaining working relationships with peers, subordinates, and supervisors.	
(11)	C. DRIVE AND INITIATIVE: Consider the extent to which the individual demonstrates attributes such as forcefulness, aggressiveness, and enthusiasm.	
(12)	D. PERSONAL CHARACTERISTICS: Consider all personal characteristics as they affect the individual's job performance.	
(13) Present (14) Higher	E. SUBJECT-MATTER KNOWLEDGE: Consider the individual's depth and breath of knowledges and skills required at the present and next higher grade.	
(15)	F. ADVANCEMENT POTENTIAL: Consider how the individual compares with others for advancement to a position of greater responsibility as well as overall capability for progression within the career field.	

SUPERVISOR'S SIGNATURE	TITLE	ORG	DATE

(16) CHECK IF EMPLOYEE IS AMONG THE TOP 6% OF YOUR WORKFORCE AT THIS GRADE LEVEL IN TERMS OF JOB PERFORMANCE COUPLED WITH POTENTIAL FOR FUTURE ACHIEVEMENT. (Requires approval below in accordance with applicable PMM instructions)

APPROVING AUTHORITY (Signature)	TITLE	ORG	DATE

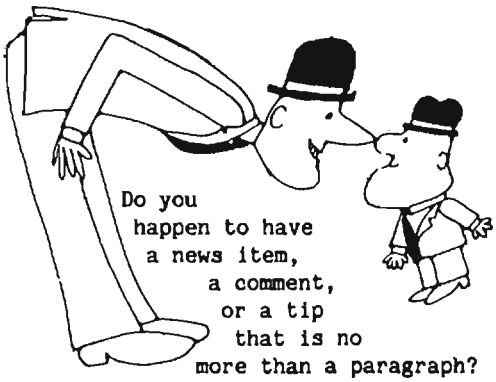
FORM P1B REV AUG 81(Supersedes P1B MAR 78 which is obsolete) SECURITY CLASSIFICATION, IF ANY

Figure 13

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011703

Contributions Solicited



Do you happen to have a news item, a comment, or a tip that is no more than a paragraph? Or perhaps you have an article of several thousands words? Long or short, if it has something worthwhile to say, we'll probably print it. Of course, a shorter item has a much better chance of getting read. (For your interest and guidance, one page of typescript, double-spaced, makes about one column in CRYPTOLOG.)

Your contribution does not have to be typed; we'll give preference to content over form, every time. (We've even accepted an item written on a used lunch bag!) Nowadays most people use a word processor, and in that case we ask you to send a floppy along with the hard copy, and write on your floppy what hardware, operating system, and word processing software you used. (And don't forget to include the file name and your name and phone number.) You can also send items via electronic mail to cryptlg@barlc05. In either case, please do not right-justify in your soft copy; the spacing isn't the same in our columnar format, and the extra spaces may have to be removed by hand, one by one -- in this day and age of automation!

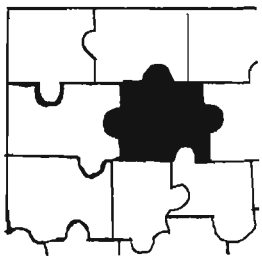
First-person articles or stories about your own experiences are welcome, so long as they relate in some way to our work.

Want anonymity? A thoughtful piece on a subject of interest to a large number of readers will be considered for anonymous publication if the writer requests it. The writer must, however, identify himself or herself to the editor. Needless to say, personal or trivial complaints will not be considered.

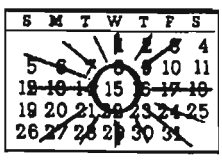
Need assistance? You may have an idea, or some notes, or even a half-finished paper that you feel has possibilities but you don't know what to do with. A call to the appropriate subject editor will get you a "story conference" and possibly inspire you to finish it up and get it into print.

Sensitive materials? No way!!! We'll go all the way to Top Secret Codeword, but we have to draw the line at compartmented or otherwise sensitive information.

Something missing? If you feel that your work or your interests are not represented in CRYPTOLOG, it's probably because you and your friends are not contributing. The editors earnestly want to cover the whole territory, but articles don't grow on trees, y'know! Somebody (who knows the subject matter) has to write them.



Our deadline? Theoretically, we should have one, but we don't. After all, CRYPTOLOG comes out six times a year, so if we get your article just after one issue has gone to press, you'll be in time for another one. There's no such thing as a bad time to submit an item for publication in CRYPTOLOG.



~~FOR OFFICIAL USE ONLY~~

DOCID: 4011703

GETTING STARTED

1. My object is to:

- ☐ Make a report on something that has been accomplished
- ☐ Call attention to something that is wrong
- ☐ Suggest a better method or idea
- ☐ Share a personal experience
- ☐ Enlist support
- ☐ Explain a process
- ☐ Ask a question
- ☐ Defend a principle
- ☐ Report news or announce a coming event
- ☐ Recognize an achievement
- ☐ Amuse and entertain
- ☐ React to something someone else has written
- ☐ None of the above, but something else, namely: _____

2. My working title is:

- ☐ A better way to _____
- ☐ Hurray for _____
- ☐ The fallacy of _____
- ☐ It's time to _____
- ☐ The scandal of _____
- ☐ Are we paying too much for _____?
- ☐ After _____, What?
- ☐ A proposal for _____
- ☐ What happened at _____
- ☐ Why I agree/disagree with _____ who wrote _____
- ☐ A funny thing happened on the way to _____
- ☐ None of the above, but _____

3. I will consider this, in my own mind, an open letter to _____ and will address to primarily to her/him/them.

4. ☐ This would be a particularly good time for such an article to appear because _____ *(or)*

☐ This subject is timeless

5. ☐ I am especially well qualified to write on this because _____
(or, on the other hand)

☐ I want to speak up on this even though I am no expert on it, because _____

6. Some tentative suggestions for a final title are: _____
_____
_____

7. I think it would be most appropriate for publication in:

- ☐ CRYPTOLOG
- ☐ The Cryptologic Quarterly
- ☐ CLArion
- ☐ The NSA Newsletter
- ☐ PQS Update
- ☐ Vox Topics

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011703

Golden Oldie (U)

EMPLOYEE PERFORMANCE APPRAISAL
PART A

[X] OFFICIAL [ ] UNOFFICIAL

LAST NAME - FIRST NAME - MIDDLE INITIAL	TITLE, GRADE AND JOB NUMBER	
CLICHE, PAragonia A.	Cryptanalyst (F/L), GS-9	NSA-6829

INSTALLATION	ORGANIZATIONAL SEGMENT	APPRAISAL PERIOD
NSA	7122	FROM 29 Feb 55 TO 29 Feb 56

1. SUPERVISOR'S EVALUATION OF PERFORMANCE ON THE ABOVE JOB: *(Covers aspects of performance as outlined in Performance Appraisal, a reference manual for supervisors)*

She's as potent as nuclear fission
In advancing the Agency's mission
Her cooperation approaches perfection
She GETS ALONG WELL WITH OTHERS IN SECTION
Paragonia's got a surplus
Of SERIOUSNESS OF PURPOSE
And nobody downgrades this cutie
When it comes to DEVOTION TO DUTY.
She's got TECHNICAL ABILITY
EMOTIONAL STABILITY
And QUANTITY and QUALITY
And USEFUL VERSATILITY.
She can COORDINATE and EXPEDITE
INITIATE - and read and write
And on the POST
She's the MOST
In ATTENTION TO PERTINENT DETAIL
She exercises JUDGMENT (SOUND)
As well as LEADERSHIP (ALL ROUND)
To no avail.
For though she's all these gorgeous things
This paragon of skill on wings
Gets: Performance Rating: SATISFACTORY

MAJOR STRENGTHS:

MAJOR AREAS IN WHICH IMPROVEMENT IS DESIRED:

2. PERFORMANCE RATING: [ ] OUTSTANDING *(Justification attached)* [X] SATISFACTORY [ ] UNSATISFACTORY *(Justification attached)*

EMPLOYEE'S SIGNATURE	DATE OF DISCUSSION	SUPERVISOR'S SIGNATURE AND TITLE

NOTE: The adjective rating assigned may be appealed. Information on the appeal procedure may be obtained from your supervisor, or if you prefer, from the Civilian Personnel Office.

DA FORM 1 DEC 54 1052 (TEST)

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011703

NSA-CROSTIC # 64

[redacted] R822

P.L. 86-36

The quotation on the next page was taken from a published work of an NSAer. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS

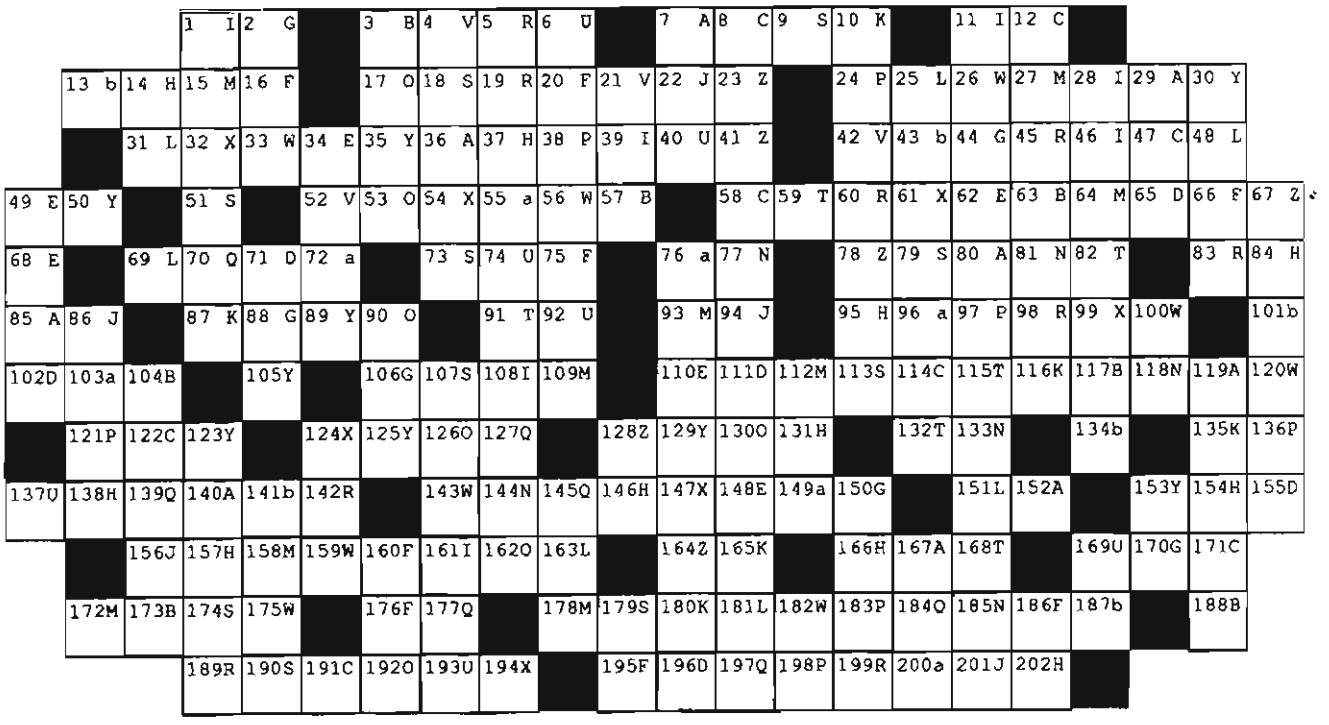
A. Operate unobstructedly
B. Freshness
C. Blameless
D. Reflected
E. Miss Marple does it
F. -------- love
G. Bow partners
H. Having a certain visual defect
I. Once famous for its trees
J. Boredom
K. Fanny Farmer measure
L. George Washington had one
M. Steadfast
N. Input again
O. Provided gratuitously
P. ------ measure
Q. Pronoun
R. Information source
S. Economic doctrine
T. ------ baron
U. Wished
V. Rear deck
W. Seat for an amphibian
X. Advancing
Y. Long-term rental
Z. Commencement
a. Transmission
b. Barms

WORDS

80	152	140	119	7	167	85	29	36		
63	173	3	188	104	117	97				
8	122	47	191	58	12	171	114			
196	65	102	111	155	71					
68	49	148	34	110	62					
195	176	66	20	16	160	186	75			
170	44	150	2	106	88					
154	138	14	146	202	37	152	84	166	95	131
108	39	11	161	1	46	28				
201	86	94	22	156						
135	116	180	165	87	10					
163	181	31	69	151	25	48				
64	112	15	93	178	109	27	158	172		
185	81	118	133	144	77					
130	162	192	53	17	126	90				
198	24	121	183	36	136	97				
70	127	164	197	145	139	177				
60	98	82	45	142	19	199	189	5		
190	79	23	107	174	51	9	18	133	179	
82	59	91	132	168	115					
92	6	74	137	40	193	169				
42	4	21	52							
100	182	26	120	175	33	143	159	56		
54	32	124	147	99	194	61				
35	123	105	129	89	125	153	50	30		
164	128	22	78	67	41					
200	72	103	55	76	149	96				
187	43	134	13	101	141					

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011703



HOW RUSSIANS VIEW THEIR LEADERS

A story is making the rounds in the Soviet Union and in some Eastern Bloc countries describing how the Party Chairmen would have dealt with a problem:

A train is traveling from Moscow to Siberia when suddenly the rails end. What to do? Await orders from Moscow, from the Kremlin.

Under Stalin, the order is given:

"Everyone off the train. Shoot everyone."

Under Krushchev:

"Everyone off the train. Pick up the rails from behind the train and lay them ahead. Move forward. Pick up the rails from behind the train and lay them ahead." And so on ...

Under Brezhnev:

"Everyone stay on the train. Close the blinds and rock the train so that everyone will think it's still moving."

Under Gorbachev:

"Everyone off the train. All loudly shout, 'There are no rails!!! There are no rails!!! There are no rails!!!' "

Provided by: [redacted] *P16*

Answers to:

"NSA" PUZZLE

(1st Issue 1987)

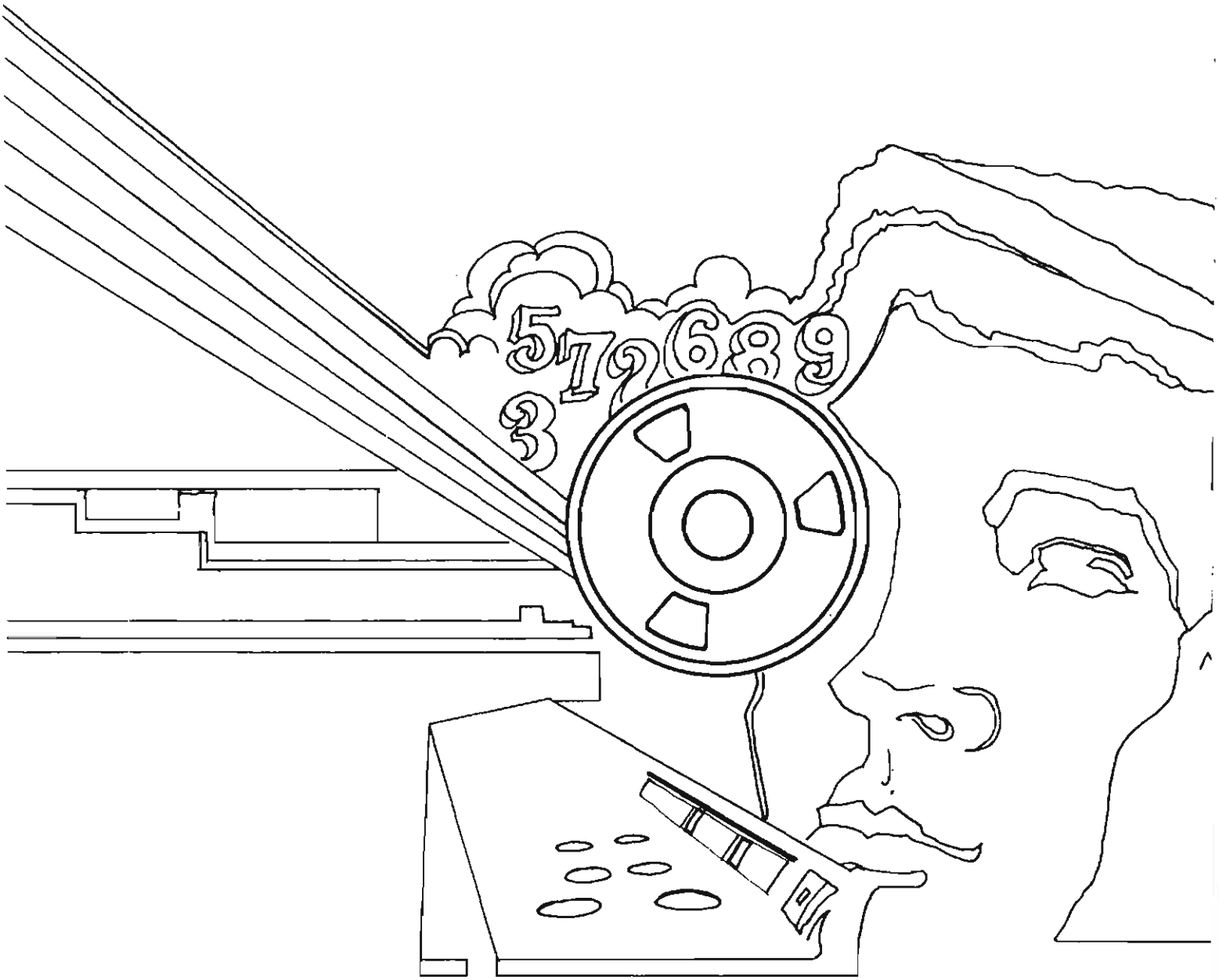
by Carolyn Cornelius, T12

1. INSANE
2. ARKANSAS
3. UNSALTED
4. COMPENSATE
5. BONSAI
6. INSATIABLE
7. TRANSATLANTIC
8. CARAVANSARY
9. INSALUBRIOUS
10. UNSAID
11. RANSACK
12. GAINSAY
13. UNSALARIED
14. CONSANGUINITY
15. UNSANITARY
16. TRANSACTION
17. UNSAVORY
18. MANSARD
19. MAINSAIL
20. UNSATURATED

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

Y16


5726893

Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4010012

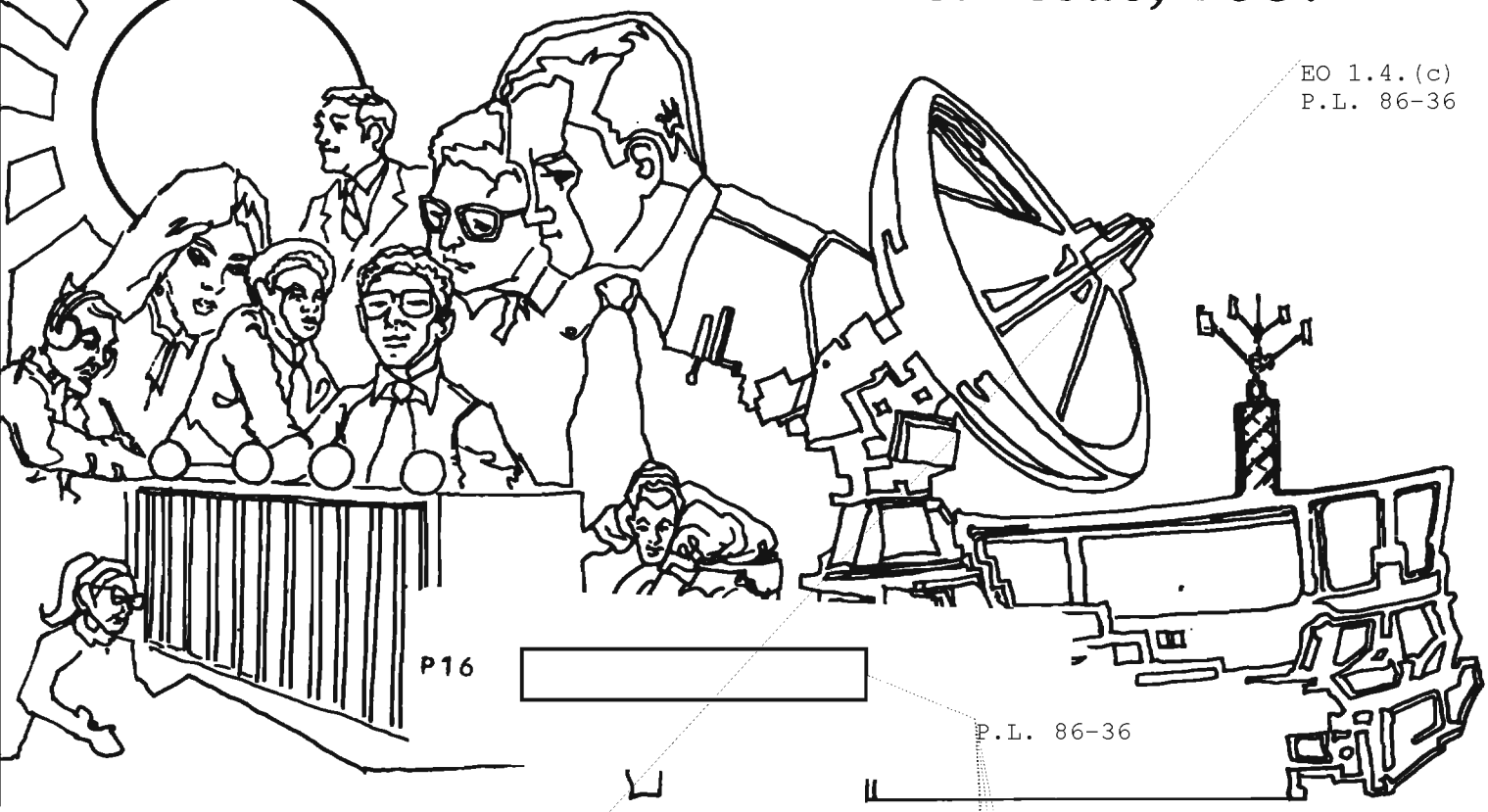
~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

1st Issue, 1987

EO 1.4.(c)
P.L. 86-36



P16

P.L. 86-36

[redacted]	[redacted]	1
HOW TO WRITE A MEMO (U)	[redacted]	9
CHECKLIST FOR NON-PROFESSIONAL INTERPRETERS (U)	Obst and van Reigersberg	14
GOLDEN OLDIE (U)		16
HOW DID A NICE CRYPPIE LIKE YOU ... (U)	[redacted]	17
BULLETIN BOARD (U)		19
FROM THE PAST (U)		20
CONFERENCE REPORT (U)	[redacted]	21
'NSA' PUZZLE (U)	[redacted]	29

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~NOT RELEASABLE TO CONTRACTORS~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~SECRET~~

DOCID: 4010012

P.L. 86-36

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XIV, No. 1 ..... 1st Issue 1987

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Collection ..... (963-5877)
Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Cryptolinguistics ..... (963-1596)
Index ..... (963-5292)
Information Science ..... (963-3456)
Information Security ..... George F. Jelen (859-1211b)
Intelligence Research ..... (963-3845)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (968-8075)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-5734)

Illustrators ..... (963-3057)
..... (963-6211)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
NOTE CHANGE: **cryptlg** at bar1c05
(bar-one-c-zero-five)
(note: no 'o')

Always include your full name, organization,and building, room, and secure phone number.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, HQ 8A187
Please do not phone.

Contents of CRYPTOLOG should not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

A VALENTINE

to

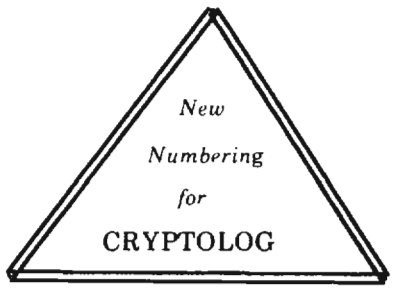
THE FRIENDS OF CRYPTOLOG

Many people behind the scenes make it possible to publish CRYPTOLOG. They are in the Press and in Distribution; they are on the Printing Control Staff; they do data conversion; they review for classification. These people carry out their assigned duties with extra-special TLC. To each of them we send a valentine.

We are also most indebted to our good neighbors in N, the editorial staff of the *Cryptologic Quarterly*, and the system administrators in P044 and in T09 for their bountiful professional courtesy. They very kindly allow us to use their printers while ours is in storage, and rescue us during our frequent crashes. To each of them we send a valentine.

And we are grateful to our colleagues in P1. They are the invisible home team who do odd jobs as needed. To each of them we send a valentine.

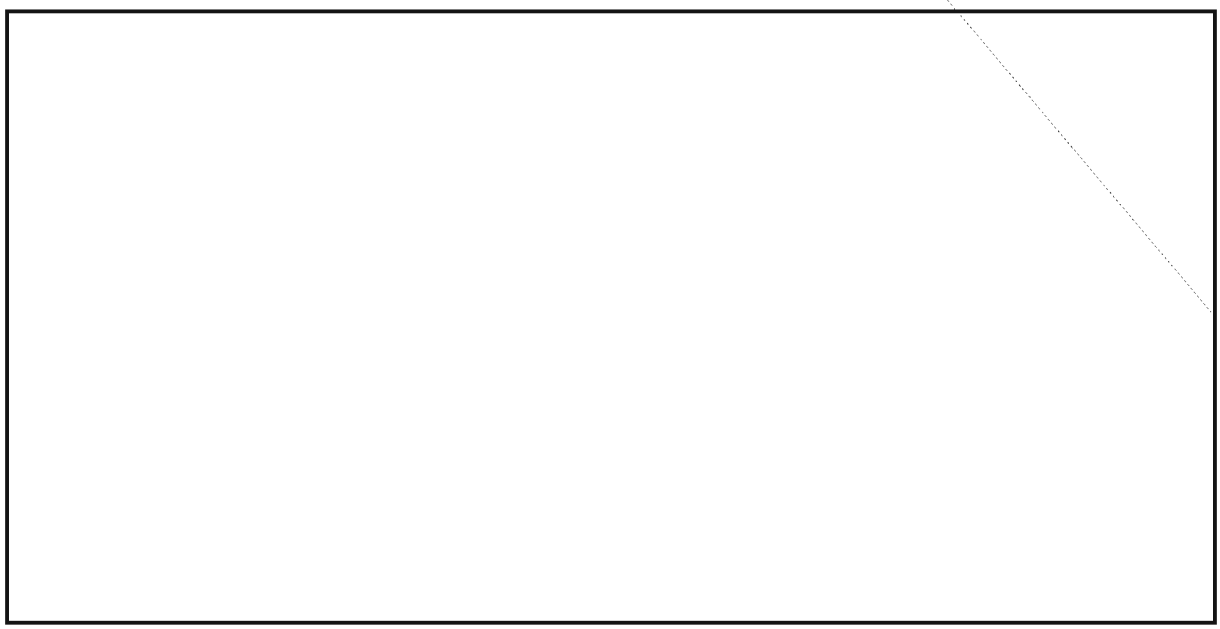
And last but not least, we cherish the many friends among the readers who steer us to the hot items of the day. To each of them we send a valentine.



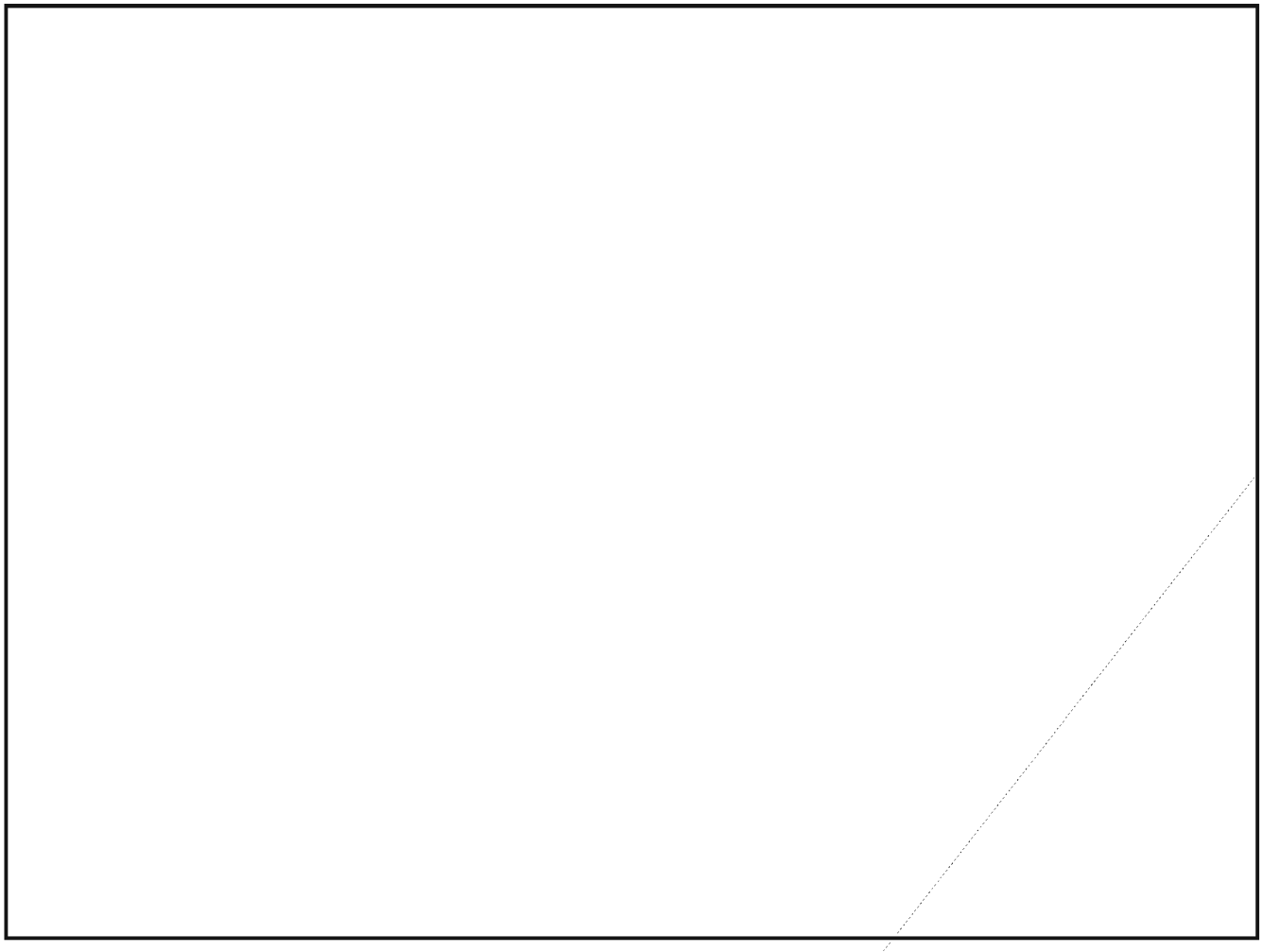
~~FOR OFFICIAL USE ONLY~~

~~SECRET~~

EO 1.4.(c)
P.L. 86-36



P.L. 86-36



EO 1.4.(c)
P.L. 86-36

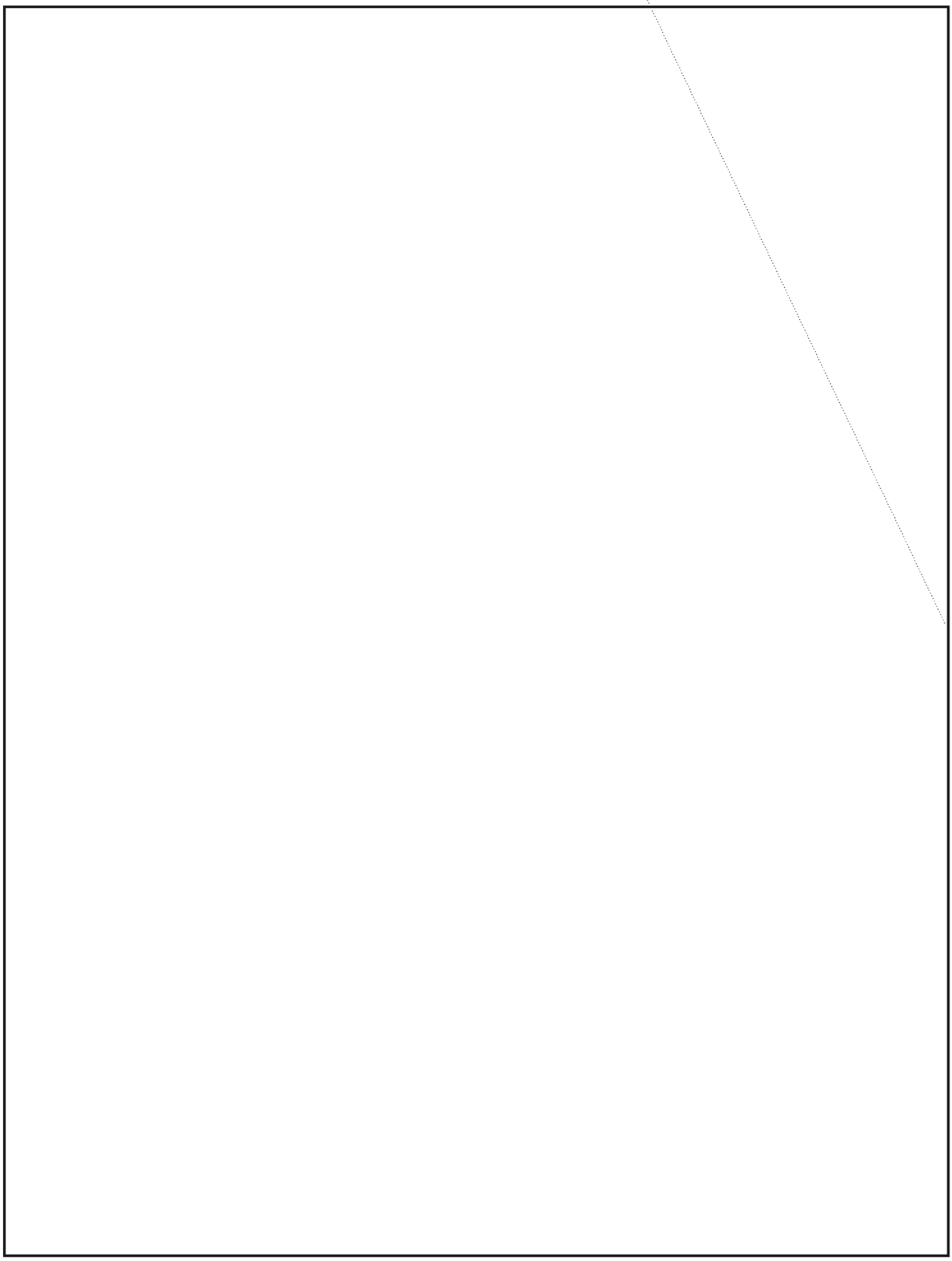
~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4010012

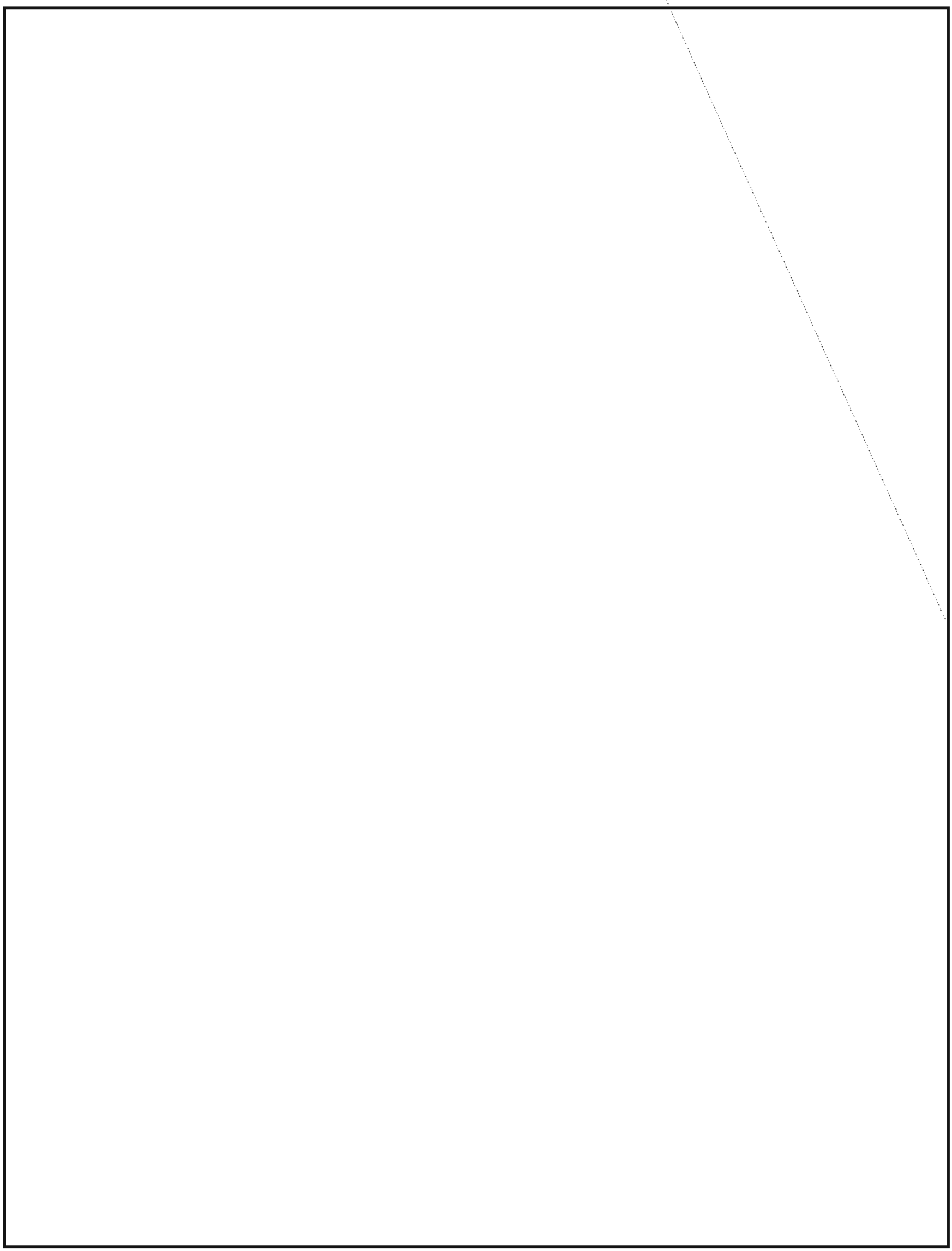
EO 1.4.(c)
P.L. 86-36

DOCID: 4010012

EO 1.4.(c)
P.L. 86-36



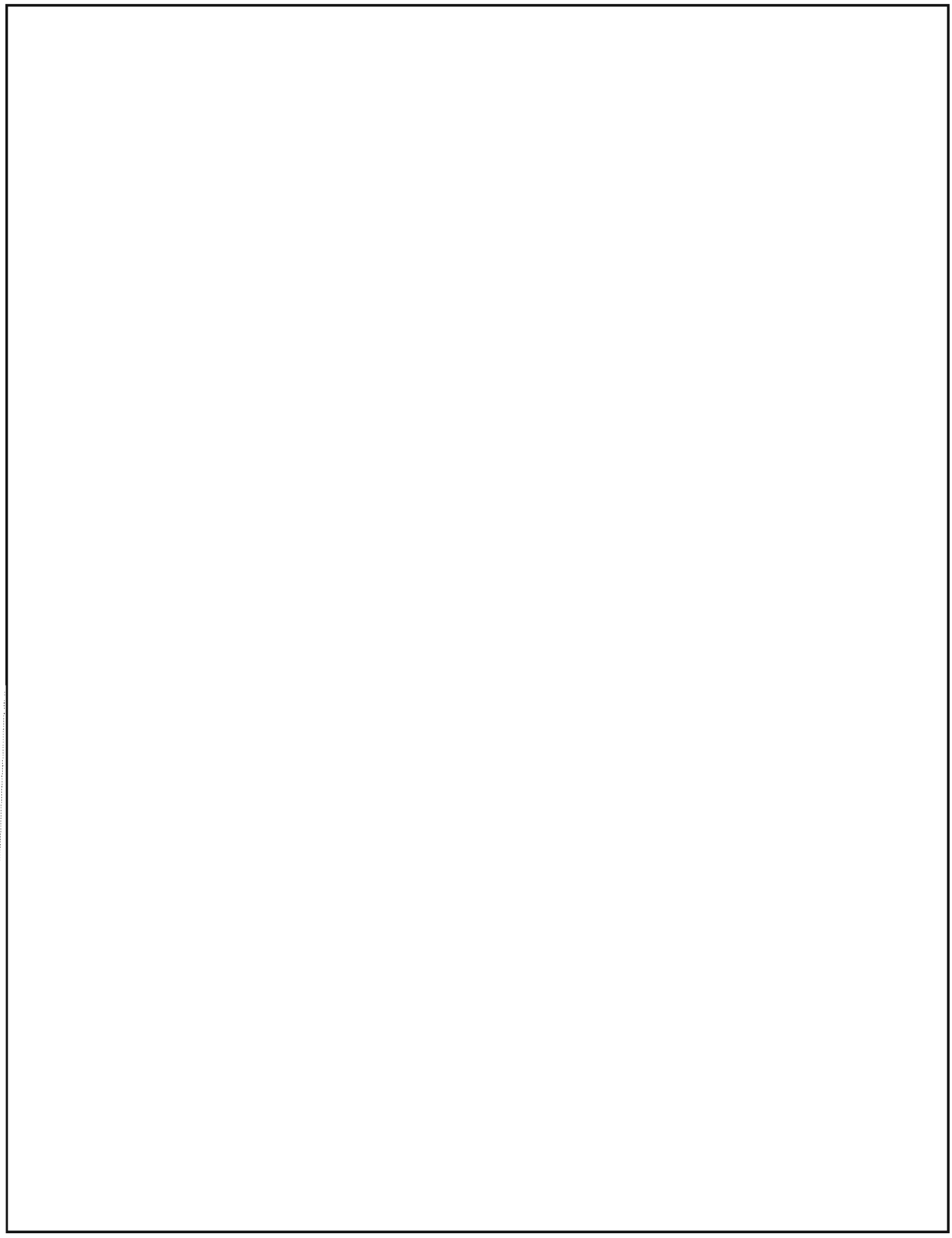
EO 1.4.(c)
P.L. 86-36



~~SECRET~~

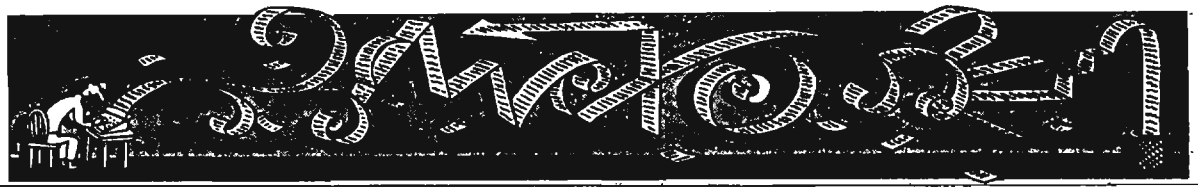
~~HANDLE VIA COMINT CHANNELS ONLY~~

P.L. 86-36



EO 1.4.(c)
P.L. 86-36

DOCID: 4010012



R.L. 86-36

UNITED STATES GOVERNMENT

memorandum

DATE: March 1987

SERIAL:

REPLY TO ATTN OF: [redacted] DSC

SUBJECT: HOW TO WRITE A MEMO

TO: All Memo Writers

1. The purpose of this memo is to provide a set of simple guidelines for writing a memo. My goal is to improve office communications by making memos easier to write and easier to read.

2. The reason for doing this is that I find memo writing in this Agency to be in a deplorable state. Memo structure has long been a particular problem. Trying to find out why the writer sent me a memo and what I am expected to do about it is like solving a whodunit! Grammar is another, but poor grammar is so widespread that I try to overlook it. Lately memos have become rude. "Request." They seem to command me, where a clearer "I request" or a polite "please" would have warmed me to the task of reading the memo and trying to do what the reader wanted. Somehow I have managed to get along with all these problems. But the situation has reached a crisis. Now I find that many memos do not even communicate. I no longer understand what they are trying to say. The time has come to do something about it. Hence this article!

3. My guidelines are:

Present your information in the prescribed order.
Write for the person who is going to read it.
Be brief. Use attachments for details.
Use words correctly and write simply and clearly.
Be polite and courteous.
Be grammatical.

4. A more detailed discussion of these Guidelines is attached.

5. The action to take is this: please follow these guidelines from now on whenever you write a memo.

~~FOR OFFICIAL USE ONLY~~

ATTACHMENT

A memo is, among other things, usually a brief communication that contains directive, advisory or informative matter. So says Mr. Webster! And he is certainly correct so far as NSA is concerned: we use memos in this Agency mainly to advise, inform and direct.

Guideline 1: Present your information in the prescribed order.

Memo structure is designed to assist this process of telling the reader something in the most succinct way possible. Hence, every paragraph in a memo serves a purpose. Look back at the memo in the beginning of this article and notice that I have underlined certain beginning words in three of the numbered sections. These words provide a formula for structuring the contents of a memo. You can't go far wrong if you stick pretty closely to this simple format.

The opening paragraph of every memo should clearly tell the reader why you have sent the memo and what action, if any, you want taken. The advice that Ben Franklin gave to newspaper reporters applies here: this is the who, what, when paragraph. Always, without exception, put this information in the first paragraph. This quickly places the rest of the memo into context for the reader; one reads on with an understanding of what it is one is reading, why one is reading it and what action one must take. Do not bury what you want done in the text where the reader has to hunt for it, or depend on the summary in the last paragraph to do the job.

The next one or two paragraphs convey pertinent information to the reader. Depending on the kind of memo, they may be brief background or history; concise explanatory detail to define or describe the subject (as a reminder or because it's complex); the reasons why you have done something (like "The reason for doing this is" paragraph in my opening memo); the authorities under which you are asking that something be done; or the specific information for which the memo is being sent (such as the "Guidelines" in paragraph three of my memo above).

The final paragraph summarizes the action you expect the reader to take and gives instructions for complying, including the expected due date, a point of contact for questions and a telephone number. If you ever wonder why people don't respond to your memos as requested, perhaps it's because you have hidden this information rather than highlighted it.

Guideline 2: Write for the person who is going to read it.

I'm tired of getting memos that read as if they were written by a computer--stilted, wooden, convoluted and often comprehensible only to another machine! It is easy to write a memo if you write as if you are talking directly to

someone. The technique works even when you are writing a memo destined for numerous readers. Here are some examples to show what I mean.

A. Dick,

1. This has happened and I'd like you to do so and so about it, please. This one has a short fuse so I'd appreciate hearing from you by ...

2. Here's how it all came about....

3. Please get back to me on this by ... Call my Exec on .... if you have any questions. Thanks very much for your help.

B. Mary,

1. You asked me this question ... (repeat the question) ... and here is your answer ....

2. I got the information by talking to so and so and by phoning some contacts I have at such and such. Everyone (or whoever) agrees with the answer I have given you.

3. If you have any questions about this, or want me to pursue it further, please just call me on ...

C. Jim,

1. We've recently established a new procedure (or committee or organization) and I want to tell you about it. You don't have to do anything, just read on.

2. The reason we have done this is that we saw a need for a new approach to such and such....

3. The officer in charge of this is ..... on extension .... She will be glad to answer any questions you may have. I hope that this new procedure (or committee or organization) will operate to our mutual benefit and satisfaction.

D. Anne,

1. We've recently finished our draft of the PPP Report for the Director and we are now requesting your help in reviewing it. If you

~~FOR OFFICIAL USE ONLY~~

can return your comments to us by ...., we'll be able to meet our deadline of .... for submitting the report to the Director.

2. You'll remember that this project, which is designed to ....., started in .....

3. Thanks for your quick attention to this request. My Action Officer, ..., will be glad to answer any questions you may have on ..... Please send your comments to him by .....

Guideline 3: Be brief. Use attachments for details.

If you follow the structure prescribed above, and say what you have to say succinctly, then your memos will be brief and they will also do what you intend them to do--communicate. One of the reasons memos have become so difficult to understand, in addition to being so disorganized, is that they are often far too long and rambling. The reader gets lost in all the unnecessary details if he or she doesn't get bored first and give up reading altogether. Details do have an important place in memos, but that place is in the Attachments. Use the memo text to direct the reader to what is included in the Attachments. Elaborating text, charts, displays, copies of pertinent laws, referenced documents -- these all belong in the Attachments, clearly tabbed and indexed for ease in referring to them. In the memo itself, stick to what you really want to tell the reader, without any distracting information.

Guideline 4: Use words correctly and write simply and clearly.

Memo writers often succumb to the temptation of trying to impress the reader. The irony is often that the writer displays ignorance instead by using words incorrectly. "Enormity" is a good example. It sounds so important and impressive. A thing can hardly be bigger! But "enormity" doesn't mean hugeness, it means wickedness, outrage or crime. When you exclaim that "The enormity of this project overwhelms me" you are saying, "This project is so crooked that I can't stand it." "Viable" is another good example. Does anyone really know anymore what it means? Popular usage is eroding nice distinctions and making communication more difficult in the process.

Even if you use a fancy word properly, it is not necessarily in good memo writing taste or style to use it. Aim for elegant simplicity which is always more desirable in a memo--and usually safer. Don't ever write anything that will send your reader to the dictionary! Always remember that you are trying to tell your reader something important and you want to make sure it is understood quickly and perfectly. Brief memos help you to write clearly and simply. They don't leave much room for lengthy words or text.

I also recommend an informal style for most memos, as you can see from my examples above. Don't be afraid to use informality when it is suitable. An informal style makes it easier to write simply and directly and to avoid the

stuffiness many memos have, or the appearance that they were written by a computer.

Guideline 5: Be polite and courteous.

Whatever has happened to the little word "please"? Nowadays memos all seem to issue commands, the most popular of which is: "Request." That's all, just the bald command: "Request." I realize this was once an acceptable usage but it is no longer desirable. It is jarring to the modern ear. At the very least you should say "I request so and so" (or "urge," "suggest," "ask," etc.). But even better is "Please do such and such," or "I would appreciate it if you would do such and so." After all, you are asking the reader to do something for YOU, a favor. You should show that you realize this and are grateful. Ordering a person around is not the best way to get something done for you. A little courtesy goes a long way.

Guideline 6: Be grammatical.

Poor grammar and word usage often interfere seriously with the reader's ability to understand memos. Good grammar is a primary asset in communication and should always be striven for. More on grammar another time.

Author's Postcript:

If you think it's a chore to write memos, I think it's a chore to read most of them. Memos these days tend to start in media res. *They lead off with what should be the middle paragraphs, omitting entirely any introduction to the subject to explain why the memo was sent to me and what I am expected to do as a result. For years I have been reading the last paragraphs of memos first, in order to find out. If you don't believe me, test it out right now on the memos in your box! Reading a memo in the order written is like reading a mystery story in which the whole thing doesn't come clear until the very end. That is good strategy for mystery story writers, but not for memo writers.*

While you're at it, you might count how many memos there are in your box. Busy executives around here all have mailboxes stuffed with memos and only limited time to read them. On a typical day the Chief of Staff plows through some eight to ten inches of them! The Deputy Directors have equally stunning loads. And all other managers and supervisors get their share. Keep in mind that you are writing a memo to communicate something you think is important for the receiver to read and that your reader is probably a very busy person. In such circumstances, you've got to do everything you can to make sure you get your message across, for your reader's sake and for your own.

Editor's Note:

An example of how not to write a memo can be found on page 20. Yes, it's for real! The indicative information was removed.

DOCID: 4010012

□ CHECKLIST
□ FOR
□ NON-PROFESSIONAL
□ INTERPRETERS
□ (U)

by

Harry Obst, Director, Director, Office of Language Services,

and

Stephanie van Reigersberg, Chief, Interpreting Division

DEPARTMENT of STATE

Editor's Note: This article may not be reprinted in another publication without the express permission of Mr. Obst.

This list was prepared by the Office of Language Services to provide some guidance to Foreign Service Officers and others who may be called upon to interpret for high-ranking officials when no professional interpreters are available.

I. Pre-meeting Preparations

1. Do not agree to interpret at a meeting about which you have not been briefed in advance or if the subject matter is totally unfamiliar to you. Make sure *in which direction* you are supposed to interpret. You may be able to handle Russian into English but not English into Russian. Make sure that you are not expected to do *simultaneous interpreting* (involving equipment and usually teams of two or more interpreters) unless you have had training and experience in it. This is best left to professionals, and even some of them can handle only consecutive interpreting.

2. Make yourself aware of the circumstances surrounding the meeting. Read up on the issues to be dealt with. Ask for the minutes of prior meetings if available.

3. Read briefing materials and talking points carefully with a view to saying their contents in the other language. Be sure you know what all the acronyms mean and how to say them in both languages.

4. Do not underestimate the difficulty of rendering some simple *sounding* English phrases and expressions in other languages. (Try to say "I am looking forward to working with you" or "we hope to be forthcoming" in the language into which you will be interpreting, for example.) Likewise, *do* work on rendering the exact psychological/emotional "charge" of expressions in context, not just the dictionary equivalent.

5. Try to obtain and read the biodata on the participants before the meeting.

6. Speak to the person arranging the physical set-up for the meeting and arrange to sit in the proper place. In general (there are expections) this means the following:

~~FOR OFFICIAL USE ONLY~~

a) next to your principal if you are interpreting for him alone,

b) between the two principals if you are to interpret both ways,

c) to the principal's left if you are at a conference table or if the meeting is a meal.

7. Find out in advance *how many* persons need interpreting assistance. Do not assume it is the principal alone just because you were asked to interpret for him or her.

8. Find a moment to ask the principal directly (or if necessary, ask one of his staff) how he wishes to proceed. If he asks for full consecutive or whispered simultaneous interpretation and you feel that you are not able to perform well in one of those modes, tell him *before* the meeting starts. If you are uncomfortable in both techniques, ask him to go a sentence or so at a time.

9. Make sure you have two pens and a note pad with you at all times. Use a *small* note pad at public ceremonies, formal dinners, etc. A legal size pad is not easily carried in the shuffle (security, reporters, waiters) and it spoils the pictures taken by the media and the official photographers.

II. Conduct During the Meeting

1. The golden rule for the placement of interpreters is simple: "*Sit where you can clearly hear* what needs to be interpreted." Do not be shy about moving if you are shunted off to a spot where the speakers are inaudible. Speak clearly and with self-confidence, loud enough to be heard by everybody, but not louder than necessary.

2. Speak in the first person. Never say, "He says to thank you for coming," or use any form of indirect discourse.

3. Avoid interjecting any personal opinion of the "he says but probably means . . . " variety. As a substantive officer you may worry when your principal strays from his talking points, but as an interpreter your role is to present a mirror image in the other language of what he is saying. In short, do not summarize *or* censor.

4. Do not draw out the interpretation of the social niceties at the opening of the conversation. Move through this at a faster clip, as the principals are already losing much of their allotted time due to the need for interpretation. Conversely, make sure to slow down a little and to apply the necessary emphasis when you interpret an important point or come to the crux of the message, so the principal will not miss it.

5. If the speaker talks too long for your skill level, politely remind him that he should pause for interpretation. Do not be embarrassed about this, because you are there to provide a service, a communications link, not to put on a bravado performance.

6. *Stay close* to the principal during stand-up and walk-around receptions and similar situations. The principal must be able to summon you in *5 seconds*. Do not get involved in you own socializing and let him drift away.

7. Pace yourself. Don't give everything you've got in the first 10 minutes -- you may have to keep at it for an hour or more.

8. If you are called upon to interpret a toast you may write it down (if you don't have the text in advance) where you are seated, provided you can hear clearly. However, at least while you deliver it, stand with your principal and do your utmost to project the same atmospherics as he does (cordiality, friendliness, etc.) Be sure to look up at the guests occasionally.

At the end of the luncheon or dinner speech when you come to the toast itself, it is advisable to depart from the rule that the interpreter always speaks in the first person. If the guests have already drunk the toast, because so many of them understood the speaker and are now seated listening to the interpretation, switch to the third person and past tense at the very end and say, for instance, "and then the Secretary *raised*

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

EO 1.4.(c)
P.L. 86-36

his glass and *drank* a toast to the health of the President and to the continued prosperity of . . . "

III. After the Meeting

1. In most meeting there is a notetaker who will write a memorandum of conversation.

If in the course of an interpreting mission you found yourself briefly alone with the principals, with no notetaker present and something of substance or importance being communicated, go to the principal's chief aide after the meeting and volunteer to write a memorandum of conversation on that exchange. He will instruct you how to write such a memo or may be satisfied with an oral debriefing. This obviously does not apply if your principal instructed you to make no record.

2. Return all classified briefing material and destroy your notes if no memcon is needed. Do not retain any copies of the memorandums of conversation. Destroy or surrender your interpreting notes after the memorandum is finished, unless you are instructed to hold them until after the memcon is reviewed and accepted. □

Solution to NSA-Crostic #63 (plus)
(December 1986)

[Lambros D.] Callimahos, *Ars Conjectandi:* [*The Fundamentals of Cryptodiagnosis*]

DEFINITION:

"*diagnostician*, [n.]. An experienced cryptanalyst of ability just before retirement age."

This is but a gentle reminder to the reader of an aphorism of Hippocrates, as translated by Chaucer: "The lyf so short, the craft so long to lerne."

PLUS: *The Bonus (or Clue, as the case may be) is in the fifth position down, and reads:*

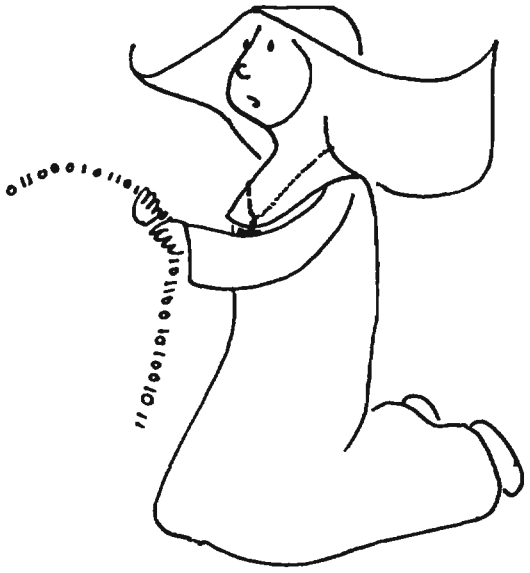
FIND HIDDEN MESSAGE. CALL DLP

Golden Oldie

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

WHAT'S A NICE CRYPPIE LIKE YOU DOING IN A PLACE LIKE N? (u)



P.L. 86-36

[redacted] *A509*

This article is classified ~~CONFIDENTIAL~~ in its entirety

Quitting time, April, 1985: I was on my way out the door when the secure telephone rang. "Ms. Wilson, GALAXY has surfaced your name as a top candidate for a position in M3."

"M3? Personnel? What does Personnel want with a cryptanalyst?"

"*N*3, not *M*3." (Payroll is going to encrypt paychecks?) Curiosity being inherent in cryptanalysts, I agreed to an interview, and began one of the hardest, fun jobs I've had in 18½ years at NSA.

A certified cryptanalyst, I had never worked outside DDO; worse yet, except for my intern tours, I knew little outside the workings of A5. Oh, there were occasional conversations with G4 and W3. But with regard to the mission of the Agency overall, I was a cloistered nun dedicated to the worship of bits, ignorant of any larger world outside my cell.

And what was this hardest fun job? Very simply, to look at, from an overall Agency point of view, all of the projects in support of cryptanalysis. [redacted] I got to look at the planning and to recommend approval of the money and actions. AWESOME!

P.L. 86-36

Yet my power was not inordinate. I really could only recommend a position to the Deputy Director for Programs and Resources, (DDPR) through a chain of Division Chief, Office Chief, and Group Chief. That kept me humble. I was often grateful that my view as the sole cryppie in DDPR was tempered by the perspectives of the very experienced managers in the N3 chain.

All the while the time clock was ticking away at my tour in DDPR. Two years in N342 was considered optimal, after which I was expected to go back into the DDO mainstream. In the meantime I would be part of a select group in N342, known as System Management Officers or SMOs, each of whom was a resident expert for a different discipline: signals analysis, language analysis and voice processing, telecommunications, collection, computer science, intelligence research, engineering, and of course, cryptanalysis. After two years out of the mainstream, the theory is, SMOs lose touch with what is happening in the trenches in their field, and fresh blood is needed to provide a current perspective. Also, the period of two years allows the SMO to participate in at least two budget cycles and to learn how the

Agency gets money; this is an excellent ticket for managerial positions.

As the resident cryptanalyst in DDPR, nominally my job was twofold: 1) to enforce NSA Circular 25-5; and 2) to advise the DDPR on cryptanalytic programs from a macro, overall NSA perspective.

The DDPR, as the Agency Directorate for Programs and Resources, is responsible for making sure that NSA acquires needed resources and spends money responsibly. And we must account to three layers of oversight: Department of Defense, Director of Central Intelligence and (always) Congress. A primary mechanism for insuring adequate planning and senior review/approval is NSA Circular 25-5 ("That blankety-blank 25-5!"). It calls for documentation of all NSA initiatives (projects) costing $2 million or more, with coordination and review by appropriate Agency-level authorities at specific decision points in the acquisition.

[redacted]

P.L. 86-36

[redacted]

These necessary coordinations allow L to plan space, T to plan comms circuits, E to gear up for new training courses. And as the details are being worked out, it gives you a chance to clarify the points that the engineer misunderstood:

[redacted]

Finally, the engineer writes a plan laying out the details of how to get your processor, assigning responsibility to any OPI that will be involved in getting your "system," and showing a schedule of milestones for keeping the acquisition on time.

This is a System Acquisition Plan, and again, you and appropriate offices in L, T, E, etc. will coordinate and have a last chance to make it say what you want it to do. Once it's coordinated, it is the record documentation for your project or acquisition, and the engineer can now put out Procurement Requests (PRs) to buy whatever is needed.

As DDPR's coordination staff for 25-5 documentation, the N34 SMOs review all of these papers. DDPR is one of the few places where all of NSA's efforts on a specific problem can be viewed for both serious holes and wasteful duplication. The budget resource managers in N2 understand the figures and totals and how to balance the overall NSA budget. They do not, however, have the technical expertise to understand the actual impact of budget cuts on the people in the trenches and on the work itself. The perspectives of the N34 SMOs, who are evaluating the efforts and who can see the real effect of a projected cut from the point of view of the working cryptanalyst, signals analyst, etc. enable the DDPR to operate with better understanding.

The biggest problem I had was my desire to save *every* project that came across my desk, because each one addressed what I considered to be a valid cryptanalytic need. Sometimes I succeeded in rescuing a program from the budget cutters or from shooting itself in the foot because of poorly written justification. While I was sometimes likened to a terrorist for enforcing 25-5 and related controls, just as often I was thanked by the sponsor, the user,

or even the developer, as being the policeman on the beat who came to their rescue when a project was being hijacked in political power plays, or threatened by budget cutters, or abandoned because of resource crunches.

Behind-the-scenes liaison with senior staffs was common, and I really came to understand the organization of NSA for the first time in my career.

Visibility was tremendous, for better or worse. I briefed DIRNSA as well as the Deputy Directors on an aspect of Advanced Modulations, and I briefed the Assistant Director for Installation and Logistics on an anticipated avalanche of future projects . And senior managers in R and T, (places I never even knew existed when I was in A544), bandied my name about.

I also realized that cryptanalysis was in much better shape than I would have guessed from my futile attempts when I was in A544 to get money to upgrade some obsolete collection positions.

A hard job? You bet! The responsibility for reviewing and evaluating cryptanalytic projects across the board is serious and mentally draining. But definitely a fun job! For it means that you get to see from start to finish, everything the Agency is doing in your field, and have a chance to comment on it. What a tremendous opportunity!

And that's why a nice cryppie (or signals analyst or linguist, etc.) should consider going to a place like N. □

BULLETIN BOARD

FOR GERMAN LINGUISTS

(U) Taped German radio programs with transcription, glossary, and extensive cultural notes can be loaned to interested individuals. The program is *Schau ins Land*, produced 14 times during the academic year. Write to [redacted] P16, HQ 8A187.

P.L. 86-36

OLD PHOTOS WANTED (U)

(U) Do you have any old photographs that illustrate an aspect of Agency history? A picture of an intercept site? Photos of obsolete R&D projects? Candid pictures of NSAers at work? Formal ground-breaking or VIP visits?

(U) Whether they are organizational pictures incorporated in an old briefing, or personal photographs stored in your desk, they might of interest to the History Program. NSA now has han official archive of historical pictures, maintained by T54.

(U) If you do have some pictures that illustrate an aspect of our history, and you can identify the subject and date with reasonable accuracy, please let us look at them. If you need the originals back, we will make a copy for the Photo Archives.

(U) We also accept donations of photos and slides, positives and negatives. Call [redacted] or [redacted] 972-2355.

P.L. 86-36

FOR CRYPTOMATHEMATICIANS

~~(FOUO)~~ NSA has a resource which every cryptomathemician should know and use. It is the R51 classified mathematics library, located at FANX-III, Room B2B37, and presided over by librarian [redacted] This collection of papers contains some real gems of mathematical cryptology dating from the years of World War II as well as much significant research of more recent times. It is well worth a trip to discover this reservoir of interesting and useful material. Mrs. [redacted] can be reached on 968-8580s.

CRYPT PROBLEMS WANTED

~~(FOUO)~~ KRYPTOS and the NCS will be publishing a series of problems in cryptanalytic diagnosis that will be representative of current target systems. The intent is to publish the problem in one issue and the annotated solution in the subsequent one. It will be designed so that the set of solutions can be bound, and thus collectively form a diagnostician's desk reference.

~~(FOUO)~~ We request your assistance in finding suitable problems. They should be non-trivial but capable of at least a partial diagnosis on the basis of a small sample and/or a statistical summary. If you have such problems, classified no higher than TSC, please check with your management first, then get in touch with [redacted] P15, 963-3957.

P.L. 86-36

DOCID: 4010012

FROM THE PAST

UNITED STATES GOVERNMENT

memorandum

SERIAL: Xxx/xxx /72

4 May 1972

X. Xxxxxxx/xxxx/xxx

REPLY TO ATTN OF: Xxx

SUBJECT: Xxxxx Xxxxx Contact Reporting Xxxx (Xxxx-xxx)

TO: Xxx, Xxx

REFERENCES:
a. XXXX-3-100, 4 Apr 72
b. X/xxxx/xxxx/x, 27 Mar 72
c. Xxx-066-72, 4 Mar 72
d. Xxx-065-72 4 Mar 72

1. Inclosed for your action is a copy of references a and b (which respond to references c and d). A copy of references d, e and f cited in reference b above has been also inclosed for your convenience. Two copies of reference c (XXXX/XXX-Xx) cited in reference b, were forwarded to Xxxx by XXX on 19 February 1971. The delay in forwarding this material was caused by the necessity to obtain a copy of reference f cited in reference b above from XXXXX.

2. Please forward your comments on reference b above to Xxx so that a response may be prepared and sent to XXXX-X as requested in reference a.

/s/ Xxxxx X. Xxxxx
for Xxx X. Xxxxxxxx

Chief, Xxx

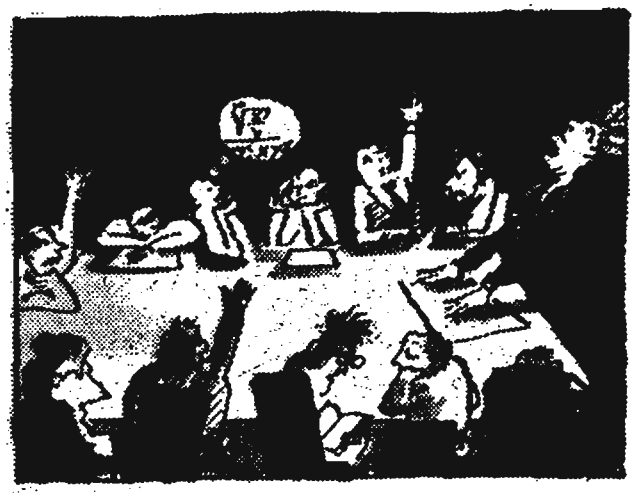
Incls:
a/s

cc: Xxx (less incls)
Xxxx "
Xxx "
Xxx (refs a and b only)

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

Conference Report



The 1987 Joint Mathematics Meetings,
San Antonio, Texas, 20-26 January 1987

Reported by: David Harris, R513

This is the national meeting of the two major mathematics societies, the American Mathematical Society (AMS) and the Mathematical Association of America (MAA), along with some other organizations. It drew some 3500 attendees.

NSA personnel in attendance were: [redacted] and the author. Some of us concentrated on talking with colleagues, making contacts, and studying recent developments in mathematics and statistics. Others were engaged in formal recruiting.

Also in attendance were individuals who are associated with NSA or with IDA/CRD: [redacted]

Among the other attendees were notables in mathematics from industry and academia.

The following is a summary of my own view of the major points of interest at the conference. For reasons of space only a few of the mathematical papers are summarized here. Additional information and some of the papers can be obtained from the attendees.

BENEFITS OF ATTENDING

It is important that the Agency continue to be represented at such conferences. It provides us with an opportunity to talk with outside mathematicians and to follow developments, and thus enables us to monitor the mathematics done in the public sector.

Conferences also give us an opportunity to improve public relations. DoD continues to have public relations difficulties with the mathematics community, and this has affected our recent efforts to establish a funding program for outside mathematical work. By attending these conferences we are in a better position to anticipate what the problems will be and to develop strategies for meeting them.

Much of the benefit from going to conferences derives from informal talks with mathematicians, as we had with Thurston, Calderbank, Diaconis, Kailath, Nevai, Askey, and Lax, detailed below. We get to be considered as human beings and so become less threatening to the academics. Through informal talks we learn more readily what we may expect in the way of technical breakthroughs. While we run the risk of giving academics information on our capabilities, we

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

also get to judge how close we are to the outside state-of-the-art.

PERCEPTIONS OF GOVERNMENT FUNDING FOR RESEARCH IN MATHEMATICS

Attitudes have changed for the worse in the last two years. At present, academic mathematicans are generally not very friendly to government or to DoD, though many think that they should get support through the National Science Foundation almost as a matter of right. This was evident at the AMS business meeting during a debate on DoD funding of academic mathematics, SDI, and the proper relationship between DoD and academic mathematics. Opponents of DoD pretty much controlled this meeting, though in fact it was poorly attended and only a few people were involved in the debate.

Agency personnel interested in our recent effort to build bridges to academia should study the debate to learn what does not work and what problems must be overcome.

On the positive side, NSA attained Corporate Membership in AMS at the Council meeting, attended by Alberts, Liebler, and Morris. Selfridge spoke on our behalf during the discussion on our membership, citing the favorable impression he gained at the recent NSA Conference. He also responded to a query about what NSA does, drawing on information he had gleaned at the NSA Conference.

THE AMS BUSINESS MEETING AND THE DEBATE ON DoD FUNDING OF MATHEMATICS

The board voted to call for a major increase in the NSF budget and for the AMS to sponsor mathematics competitions for students.

Under the rules of the AMS, before a motion can be adopted it must be considered at two business meetings. At the first, it is voted onto the Agenda of the second, and at the second it may then be formally adopted. Accordingly, there were four motions at this business meeting relative to the following two resolutions:

Resolution 1: Many scientists consider SDI (commonly referred to as Star Wars) incapable of achieving its stated goals and dangerously destabilizing. Participation by universities and professional organizations lends a spurious scientific legitimacy to it. Therefore the AMS will lend no support to the Star Wars program. In particular, no one acting as a representative of the AMS shall participate in efforts to obtain funding for Star Wars research or to mediate between agencies granting Star Wars research money and those seeking to apply for it.

Resolution 2: The AMS is concerned about the increasing militarization of support for mathematics research. There is a tendency to distribute this support through narrowly focused (mission oriented) programs which circumvent normal peer review procedures. This tendency, unless checked, may skew and ultimately injure mathematics in the United States. Therefore those representing the AMS are requested to direct their efforts towards increasing the fraction of non-military funding for mathematics research, as well as towards increasing total research support.

While the action parts of these resolutions are mild and apparently designed to achieve consensus, the preceding rhetoric is not. The first two motions were to put these resolutions on the Agenda at the Salt Lake City Business Meeting in August so that they may be formally adopted. The last two motions were to put the AMS on record as being in favor of the resolutions.

President Mostow decided to end the meeting on schedule, so he placed severe limitations on time for debate. Ultimately, all of the motions passed by slim margins. Probably none of the motions would have passed had the rules been adhered to. The few vote counts were of debatable accuracy. Attendance at the business meeting was about 200, a tiny fraction of the people registered at the meeting, not to mention of the AMS membership. About 400 AMS members had signed petitions endorsing the resolutions.

Summary of points against the motion:

- There should be multiple modes of funding;
- DoD has the ability to take risks;

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

- NSF funding is increasing as fast as military funding;

- How can anyone object to doing research to see if SDI is valid?

Summary of points for the motion:

- Neither motion inhibits individuals from doing SDI work.

- DARPA money unbalances mathematics towards mission-oriented work and encourages students to enter some fields at the expense of others.

- Priorities should not be set by a military that lacks an overview of mathematics.

- SDI thwarted disarmament at Reykjavik.

- Would SDI be wise even if it was possible?

- The dependence of computer scientists on DARPA is excessive and harmful.

- Suppression of factorizations of integers shows DoD's wickedness.

During the debate in the evening people spoke both for and against the resolutions, but predominantly in support of them.

One speaker focused on proper institutional policies in DoD funding. He supported national security as a valid goal, but he stated that military programs in support of research are highly mission-oriented, secretive, and rely on scientific evaluation procedures of variable reliability. In his opinion, AMS should do nothing to foster substantial funding of mathematical research in this military mode.

What may be more acceptable is defense programs in civilian mode, operated with a reasonable variant of peer review and unclassified, in research areas selected for their general relevance to the funding agency, but with little direction imposed on the individual investigators. He spoke of the dangers of "political abuses" (i. e. non-scientific pressures on investigators or political exploitation of their participation without their consent, as he said has happened in SDI). In the long term he wants a realignment of federal funding so that the preponderance will come from NSF-like Agencies. He believes that recent initiatives in interdisciplinary research should not be allowed to interfere with traditional modalities.

According to him, DoD program managers who understand science have little discretion or influence on scientific policy. He sees that policy makers operate at a level where non-scientific issues are paramount and where the mathematics budget is negligible. He opposes making such a structure responsible for the fate of 40% of federal support for mathematics. He believes that when the nation's interests call for adjustments in the funding of mathematics, the academic mathematicians can talk rationally to NSF. "But whom can we address at DoD who has the power, knowledge, and commitment to basic science to make appropriate changes?"

A second speaker believes that military research does not belong on university campuses, for military organizations are hierarchical and secretive. The size of military grants compared to other sources of funding distorts departments, creating divisive mini-empires, influencing allocation of limited resources, and setting priorities for graduate student manpower. The research initiative approach tends to give givers and takers a common interest in disguising research failures. There is more than enough military research being done already, most of which does not improve military effectiveness.

He cited evidence that money from DoD would be used to quiet mathematicians from criticizing DoD programs. "Military research adds to a threatening atmosphere, particularly between the US and the USSR." Military funding will change mathematical culture, leading it towards classified research and ultimately weapons design. "Mathematics is a poverty-stricken discipline, and we face a shortage of mathematicians soon. This does not mean we should sell out." "If and when a consensus can be reached, the Society should lobby against military funding."

A third speaker gave a reasoned defense of accepting DoD help. He pointed out that others wanted the government's money, and that the government need not beg mathematicians to accept financing. He argued that priorities are set by the *civilians* in Congress and by the President, and that if mathematicians want more money they must show that they are valuable to society on the latter's terms. If

DOCID: 4010012

society values research of practical importance to the national security, then mathematicians ought to consider this. He said he was very disappointed with the business meeting.

A fourth speaker made a passionate statement about the potential damage to the national defense if the resolutions were to pass. Such resolutions may discourage mathematicians from dealing with DoD. Another speaker said reliance on military money is a threat to mathematics. He compared taking DoD money to taking money from the Nazis (He later took this back.) He mentioned the threat to cut off money to people critical of DoD programs. Still another speaker referred to gold-plated toilet seats, cheating, and inequities in grants. He said National Defense is a euphemism for Imperialism. At best, military spending is money down a rat hole.

A New Jersey woman said she had been told by a non-mathematician that she should not teach mathematics because it will help blow up the world. She asked, can we change the perception of the world that mathematicians help the military? With this, someone attempted to recruit more spokesmen for the DoD's side. But since we saw which way the wind was blowing, we felt it pointless to respond and left the meeting.

All this was rather discouraging to those in favor of the new Agency effort to improve relations with academia. The attitude of academics at Louisville two years ago was more in tune with the Agency's present policy of collaborating for the common purpose of improving the health of mathematics in the United States. Those academics at this meeting who made their views known were generally of the opinion that the nation owes them support, that the support should be from NSF, and that money from DoD is more likely to harm academia than help. A substantial minority still view DoD as the enemy of humanity.

It seems clear, however, that DoD ought to give some thought to the effect its grants will have in mathematics departments. Departmental politics may be as important a consideration as national politics in making these grants work. DoD should try to avoid the appearance of trying to set priorities for academic mathematics.

The MAA business meeting was extremely poorly attended. In fact, after the resolution was passed changing a quorum from 25 to 50, a jokester in the audience pointed out that the business meeting no longer had a quorum and so had put itself out of business! Several proposed changes in the bylaws were routinely passed.

INFORMAL CONVERSATIONS

P.L. 86-36

I had informal talks with Askey and Nevai on approximation of the tails of distributions.

Several of us - [redacted] and I - talked to a leader of the faction in favor of the anti-DoD resolutions. I spoke to him about the Agency's new effort to strengthen academic mathematics and attempted to convince him that we are human.

Several times I talked to Persi Diaconis, who was in the Harvard Statistics Dept. in 1972 while I was getting my degree in the Mathematics Dept. I asked him about some of my moments problems. Kailath remembered me from a briefing he gave at Fort Meade.

[redacted] spoke at length to A. R. Calderbank of AT&T Bell Labs. [redacted] supplied Calderbank with several references relevant to his work, and informed him that one of his results had been anticipated in a paper by [redacted] At the urging of Marshall Hall, Calderbank is working on the existence of a design with parameters $(v,k,\lambda) = (28,10,5)$.

Don Rawlings of California Polytechnical State University gave a talk on an extended Simon Newcomb problem. [redacted] took him aside and educated him about a very powerful matrix technique published long ago by Becker and of which Rawlings seemed unaware.

[redacted] talked briefly to Ken Johnson of Penn State, who gave a very interesting talk on quasigroup characters relevant to nonabelian Fourier analysis, Schur rings, and association schemes. In recent papers Johnson and Smith generalize much of character theory to association schemes. Johnson gave [redacted]

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

several of these papers, copies of which are available upon request.

Eileen Poiani of St. Peter's College in New Jersey has worked at the national level on issues involving women in mathematics. She was interested to learn from [redacted] that NSA has many highly qualified women among its professional mathematicians, and asked if some of them would be willing to participate in her projects.

P.L. 86-36

At the NSA Conference, Askey asked me to look up Nevai of Ohio State. He was the organizer of a special session. I asked Nevai about using orthogonal polynomials to approximate tails of distributions. He asked me to send him my paper. Askey and I talked several times. At the NSA Conference he had argued for orthogonal polynomials as the solution to estimating extreme tails. The three-term recursion allows one to find orthogonal polynomials using the metric from the quadratic form dictated by the given moments. In theory, if the moments determine the distribution, the set of orthogonal polynomials determines the distribution. The practical utility for tail estimation is unclear.

Lax had told [redacted] at the NSA Conference that mathematicians have new and better ways of doing extreme tail approximation that statisticians have not yet learned. Accordingly, I cornered Lax and asked him what methods he had in mind. Lax thinks he has a clever way of finding the roots of orthogonal polynomials without the expense of generating the polynomials. (See Diaconis' talk.)

DR. GRAHAM'S ADDRESS

President's Science Advisor and Director of the Office of Scientific and Technical Policy (OSTP), W. R. Graham, stressed the need for educational reform, interdisciplinary cooperation, and lobbying for more government funding. The audience was tiny, which may or may not reflect the popularity of the US government at this conference. (It certainly reflected the availability of free beer at an Academic Press dinner held at the same time!)

Graham spoke first on government investment in mathematics, stating that the government is used to people lobbying for support and feels no need to force its money on people. He stated that support to mathematics is based on the premise it is crucial to future economic and military security. DoD is finally willing to give independent support for academic research, a healthy sign. Mathematics should involve itself in interdisciplinary efforts that prove its value.

In Graham's view, the health of mathematics depends on finding ways to apply it to the benefit of the non-mathematical public. He believes mathematics teaching in high school is poor. We expect little of our schools and students, so we cannot hope to compete with foreigners. The Mathematics Science Education Board should help. Demographics will be an increasing problem in getting enough good teachers [and Agency employees!] Decentralization may make reform difficult.

RECRUITING

The Agency recruiting effort was apparently quite successful. About thirty people were interviewed. This included most of the people who seemed to be good prospects. Of course, only time will tell which of these people will end up on board.

MATHEMATICAL HIGH POINTS

A short course on Moments in Mathematics included, among other things, the following:

- Diaconis' work on Wyner's encryption method for speech over telephone lines and his ideas on attempts to extend Chebyshev's bounds.

- Kailath's talk on speech synthesis, lattice filters, fast methods of finding Cholesky and QR factorizations, transmission line theory, and a parallel algorithm for decoding certain codes.

Of the other lectures given, the following were of particular interest:

- An interesting talk on radar by J. Michael Baden & Marvin N. Cohen of Georgia Tech.

- McEliece on neural networks. They can be used in theory to find local minima of NP-complete problems and as storage devices.

- A talk by Durrett on modeling for a variety of growth and decay situations. One wants parameter values for which a process dies out or lives.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

- Talks by K. S. McCurley on sieving the positive integers by primes, by Tapia on an unsuccessful attempt to use Karmarkar's methods to do quadratic programming, and by R. A. Mollin on the class number of certain real quadratic fields.

SOME DETAILS

Richard Durrett, Cornell Univ., ***Crab Grass, Measles, and Gypsy Moths: An Introduction to Modern Probability***. A preprint of Durrett's paper is available. The subject is five different models for interacting particle systems. One asks in each case under what parameter settings the phenomenon survives forever or dies out.

1) The Oriented Percolation Model.

2) Richardson's Model (Sites become occupied with a probability depending on the number of occupied neighbors.)

3) The Measles Contagion or Forest Fire Model (similar to no. 2, except there are three states, tree burnt, whole, or on fire.)

4) The Gypsy Moth Spread Model (similar to no. 1 except that time is a continuum).

5) The Crabgrass Spread Model on a lawn $(Z/M)^d$, where M is a large integer.

J. Michael Baden & Marvin N. Cohen, Georgia Tech., ***An Application of Undergraduate Mathematics Yielding Interesting Results in Radar Research.*** Cohen gave an introduction to radar with applications to ground mapping, surveillance, tracking, and signature acquisition. Long pulses give long range but weak resolution. Pulse compression involves coding the long pulse to improve resolution. Cohen explained filtering to handle sidelobes caused by correlations out of synch. One wants to minimize both the integrated sidelobe level and the peak sidelobe.

There are 8 Barker codes that have optimal sidelobes. But it is now known there are no Barker codes of length more than 13 and less than about 10000. One wants codes of length in the thousands. One can combine Barker codes to obtain longer codes. Also, there are Golay pairs. They are ideal, except that movement of the target or any sort of instability kills them.

Baden uses a method involving mismatched filters to reduce the sidelobe. The filter depends on the signal. In practice, one designs the filter with a sample of the signal, and assumes this will be close to optimal. One has to solve a linear system, which by a physical argument is invertible. Baden would like a mathematical reason why the system can be solved. Mismatched filters do much better than the alternatives, especially as the filter gets longer. Charts allow one to select the proper filter length to get the desired sidelobe characteristics.

Marc Culler, Univ. Illinois Chicago, ***Free groups, Trees, and their Automorphisms.*** This talk on geometric group theory included a reference to work of Ken Moss. Given a free group F, one tries to describe the outer automorphisms OUT(F). On the other hand, following Thurston's work, one seeks to characterize the points at infinity needed to compactify a topological space. The connection between these two problems is a generalization of the concept of tree.

Robert J. McEliece, California Inst. of Technology, ***The Capacity of Neural Networks.*** This is joint work with Posner, Rodemich, and Venkatesan. Neural networks are arrays modeled on the brain. Each neuron has a binary state (firing or not firing). It decides to change state on the basis of the sum of inputs from all the neurons to which it is connected. There is a threshold function for computing the new state depending on a symmetric matrix T. The initial state is called a prompt. At any given time, the node most urgently wanting to change is the one that changes (with some tie-breaking procedure). If the prompt is [+-+-++], and we multiply this by matrix T and obtain for example the vector [-1 5 -1 5 3 3], then nodes 1,2,3,4 want to change sign, while nodes 5 and 6 do not. The ones most urgently wanting to change are 2 and 4, so one of them is selected. If T is symmetric with zeros on the diagonal, this process will always converge to a fixed point, a local minimum of energy. In theory one can build a neural network to find local minima of NP-complete problems, such as the Traveling Salesman Problem. McEliece described how a network can be used as a storage device. One designs a neural network with matrix T chosen so that the words to be remembered are fixed points. However, there may be other fixed points to complicate matters, and other problems may arise. Neural networks are easy to build and to update.

R. A. Tapia & J. E. Dennis, Rice, & A. M. Morshedi, Shell Development, ***Polynomial-Time***

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

Quadratic Programming based on Karmarkar's Linear Programming Approach. Ye & Tse and Kapoor & Vaidya tried in 1986 to use Karmarkar's methods for QP. Their efforts are unsatisfactory for different reasons. The authors have tried again, also with unsatisfactory results, but for a bizarre reason.

R. A. Mollin, Univ. of Calgary, ***Class number of real quadratic fields.*** Mollin provides sufficient conditions for the non-triviality of the class numbers of certain real quadratic fields.

K. S. McCurley, USC, & D. A. Goldston, San Jose St., ***Sieving the Positive Integers by Large Primes.*** If Q is a set of primes, let $\psi(x,y,Q)$ be $\#\{n \mid n \leq x$ and $(p|n, p \in Q) \Rightarrow p \leq y\}$. The authors prove an estimate for $\psi(x,y,Q)$ in terms of a generalized Dickman function, extending work of Hildebrand. This yields an asymptotic estimate for $\psi(x,y,Q)$. One result is that removing small prime factors in sieving has less than the expected effect.

SHORT COURSE ON MOMENTS METHODS

I attended a three-day short course on Moments in Mathematics. In general, the experts at the course tended to approach moments from a function-analytic point of view and had relatively little experience with statistics. The course served as a general survey. I particularly liked Kailath's applications-oriented talk.

Henry J. Landau, Bell Labs, ***The Classical Background.*** Landau gave a survey of moments problems and applications, beginning with the Hamburger Moment Problem (find a measure on the real line with a given set of moments and determine if the measure is unique), the Truncated Moment Problem (only 2n moments given), and the Trigonometric Moment Problem (the equivalent existence problem but with complex moments on a circle - uniqueness following by Fourier transform theory.) A necessary condition for existence of a solution to the Hamburger Moment Problem is that a certain quadratic form be positive semi-definite. In this case, it defines a scalar product for polynomials, and so a family of polynomials orthogonal with respect to this product. He showed positive semi-definiteness is sufficient for existence. Landau discussed generalizations and applications.

J. H. B. Kemperman, Rutgers, ***Geometry of the Moment Problem.*** Given a set of measures, we can map them to points in n-space by taking each measure to the point (the "moment point") with coordinates the given n moments. For measures on an arbitrary measurable space, more general geometric constructs can be considered. Given a finite number of moments, one wishes to describe geometrically the convex set M of all measures having these moments, or at least to give accurate bounds for the integrals of particular functions as the measure ranges over M. Or one may require that some of the moments are not prescribed exactly, but only fall within given bounds, or on a line in n-space. Or, given a set A, fix moments and ask for the largest or smallest mass for A consistent with the moments. Such problems are conceptually simple but hard.

Donald Sarason, UC-Berkeley, ***Moment Problems and Operators in Hilbert Space.*** The connections between classical moments problems and the theory of operators in Hilbert space were recognized early on. Sarason described some of these connections. For example a one-sided version of the trigonometric moment problem, the so-called Nehari Moment Problem, is related to the theory of Hankel operators. A proof of the sufficiency of the positive semi-definiteness of the Hankel matrix for the Hamburger Problem follows from the Spectral Theorem for Self-Adjoint Operators. One can give function-theoretic conditions for the solution to be unique.

Thomas Kailath, Stanford, ***Signal Processing Applications of Some Moments Problems.*** Trigonometric moment problems are connected with positive definite matrices, orthogonal polynomials, and classical function theory. These subjects all are related in turn to a variety of signals processing problems: linear prediction, inverse scattering, digital filtering, etc. Kailath illustrated the interplay between moments problems and signals theory. Starting with linear predictive coding methods as applied in speech synthesis (the way modern American toys have learned to speak!), he described the role of Szego polynomials in providing a nice hardware implementation.

The issue of parallel implementation of image processing brings in an algorithm of Schur. This leads to a new class of digital filters called lattice filters that have excellent robustness to finite precision implementations.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

An offshoot is a fast method for finding Cholesky and QR factorizations of Toeplitz matrices. Other applications are to transmission line theory, layer-peeling algorithms for inverse scattering, and parallel algorithms for decoding Reed-Solomon and BCH codes.

Christian Berg, Univ. Copenhagen, Denmark, ***The Multidimensional Moment Problem and Semigroups.*** The 2-dimensional moment problem consists in finding necessary and sufficient conditions for a sequence s(m,n) m,n = 0,1,... to be a moment sequence for a non-negative measure on the real plane. More generally, in the n-dimensional case, one would like to characterize moment sequences among all sequences, characterize which are determinate, and give a complete description of the set of measures with a given indeterminate moment sequence. The theory of moments may be viewed as harmonic analysis on semigroups.

Persi Diaconis, Stanford, ***Moment Problems in Probability and Statistics.*** Statisticians use moment estimators as basic in applied work. For example, Diaconis said that the distribution of traces on the n-dimensional orthogonal group has the same first 2n+1 moments as the standard normal distribution. In the application, which was a proposal by Aaron Wyner of Bell Labs to encrypt speech for phone lines using random orthogonal matrices, this was bad news. Diaconis and his co-workers were trying to approximate Haar measure for the orthogonal group using iteration of random reflections. A reflection fixes a hyperplane, so log n reflections will fix too much and the trace of the iterated operator will be too large. One needs n log n reflections to get the trace right.

Diaconis mentioned Chebyshev's bounds on a distribution with the same first n moments as the standard normal distribution. There is a bound on the error, but it is attained by discrete distributions. If one looks at smooth distributions, the bound is very poor. Diaconis would like more work on what can be said with smoothness assumptions. I mentioned that robustness considerations both on the moments being equal and on smoothness must be studied. What if one drops normal? Diaconis and I have both been trying to get people to work on such problems.

Diaconis said that the modern approach to bounding variability among distributions with a prescribed n moments leads to numerical determination of the zeros of the associated orthogonal polynomials. This is feasible for a small number of moments, but is quite difficult in general. Are these bounds on all distributions with a fixed n moments useful? Probably the smoothness problems mentioned above occur generally.

Diaconis discussed Hausdorff's Moment Theorem which addresses the question: when is a sequence the moment sequence for a distribution on the interval [0,1] and De Finetti Exchangeability. Roughly, De Finetti's theorem says that *a distribution on sequence space is exchangeable if and only if it is a mixture of Bernoullis in a generalized sense.* This theorem is equivalent to Hausdorff's Moment Theorem. One can relate extensions of de Finetti's theorem to moment problems and so generate new problems.

MISCELLANEOUS

Many exhibitors were present and distributing literature. Literature and demonstrations on word processing were particularly evident. Mike Spivak showed his own commitment to TEX by typing people's equations in great numbers.

Among conferences advertised was the First Canadian Number Theory Society Conference, at Banff, April 17-30, 1988. A tentative list of speakers includes Erdös, Guy, H. Lenstra, Pomerance, Ribenboim, Selfridge, Washington, H. Williams, and Zassenhaus.

The AMS awarded Steele Prizes to Donald Knuth (for his book), Rudolf Kalman (for papers on filtering and linear dynamical systems), and Saunders MacLane (for cumulative influence, especially on homological and categorical algebra.) The Cole Prize in Number Theory was shared by Benedict Gross, Dorian Goldfeld, and Don Zagier for work on the class number problem for imaginary quadratic fields. As for MAA awards, the Chauvenet Prize went to J. H. Wilkinson, the Allendoerfer Awards to Bart Braden and Sol Stahl, the Ford Awards to Jeffrey C. Lagarias and M. E. Taylor, and the Polya Award to P. J. Davis. □

Editor's Note: We just learned that the resolutions passed during the AMS business meeting were subsequently ruled out of order by the General Council. It is expected that there will be a referendum on the motions after January 1988.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

"NSA" PUZZLE

P.L. 86-36

by [redacted] T12

The occurrence of "NSA" as a letter sequence in English words is rather uncommon. Some of the rare examples are shown below. Fill in the blanks to reconstruct the "NSA" words defined.

A. Crazy — _ n s a _ _

B. "Land of Opportunity" — _ _ _ _ n s a _

C. Lacking sodium chloride — _ n s a _ _ _ _

D. Pay for damages — _ _ _ _ _ n s a _ _

E. Miniature tree — _ _ n s a _

F. Unable to be satisfied — _ n s a _ _ _ _ _ _

G. Across the ocean — _ _ _ n s a _ _ _ _ _ _ _

H. Middle Eastern inn — _ _ _ _ _ _ n s a _ _

I. Unhealthful (as a climate) — _ n s a _ _ _ _ _ _ _ _

J. Not spoken — _ n s a _ _

K. Search thoroughly — _ _ n s a _ _

L. Deny or contradict — _ _ _ n s a _

M. Not paid regularly — _ n s a _ _ _ _ _ _

N. Relationship by descent from a common ancestor — _ _ n s a _ _ _ _ _ _ _ _

O. Unclean — _ n s a _ _ _ _ _ _

P. Result of a bank visit — _ _ _ n s a _ _ _ _ _

Q. Disagreeable or disgusting — _ n s a _ _ _ _

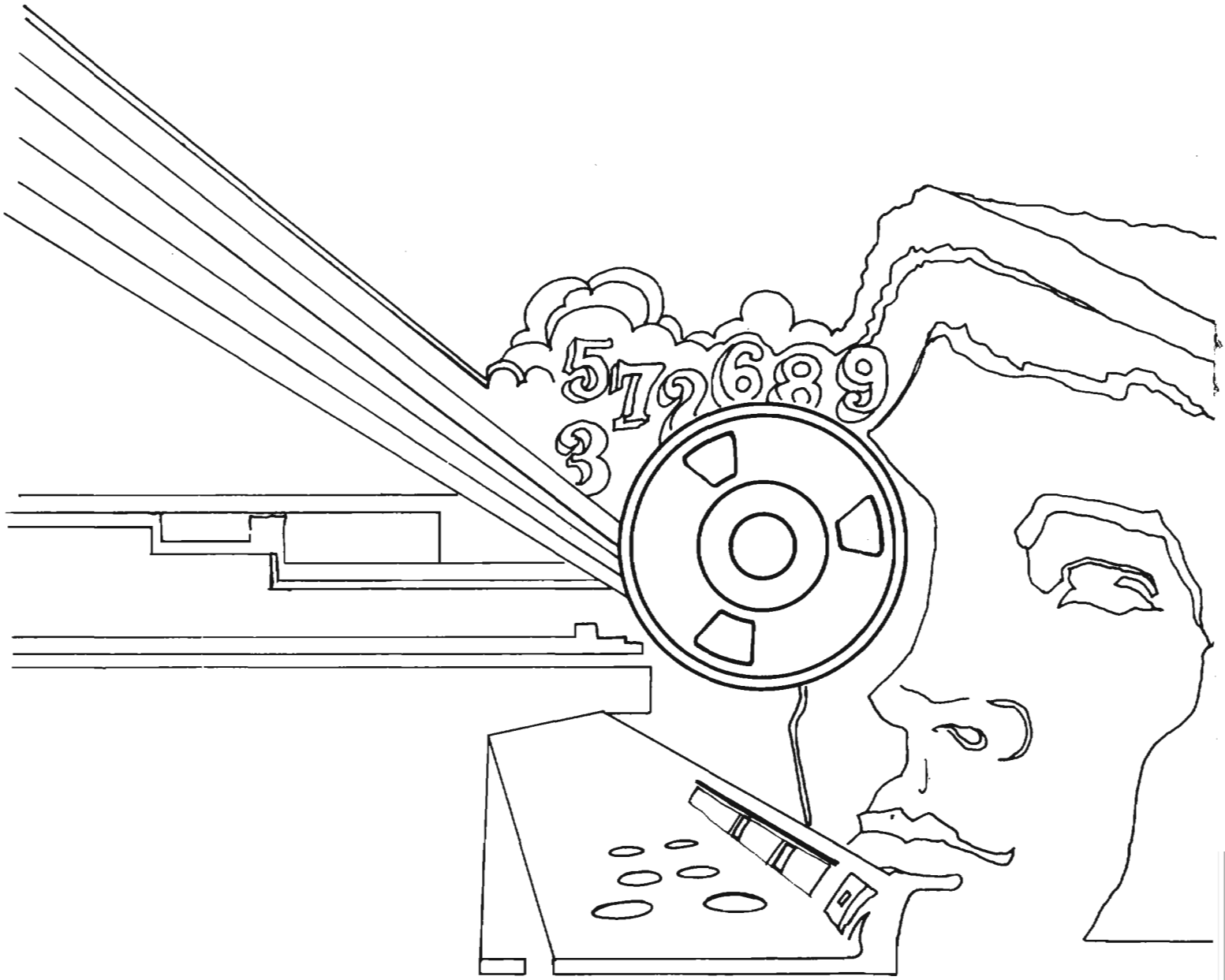
R. Type of roof — _ _ n s a _ _

S. Sail on a square-rigged vessel — _ _ _ n s a _ _

T. Able to combine with other substances — _ n s a _ _ _ _ _ _ _

~~FOR OFFICIAL USE ONLY~~

~~SECRET~~



~~HANDLE VIA COMINT CHANNELS ONLY~~

~~NOT RELEASABLE TO CONTRACTORS~~

~~SECRET~~

Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case #
DOCID: 4033692

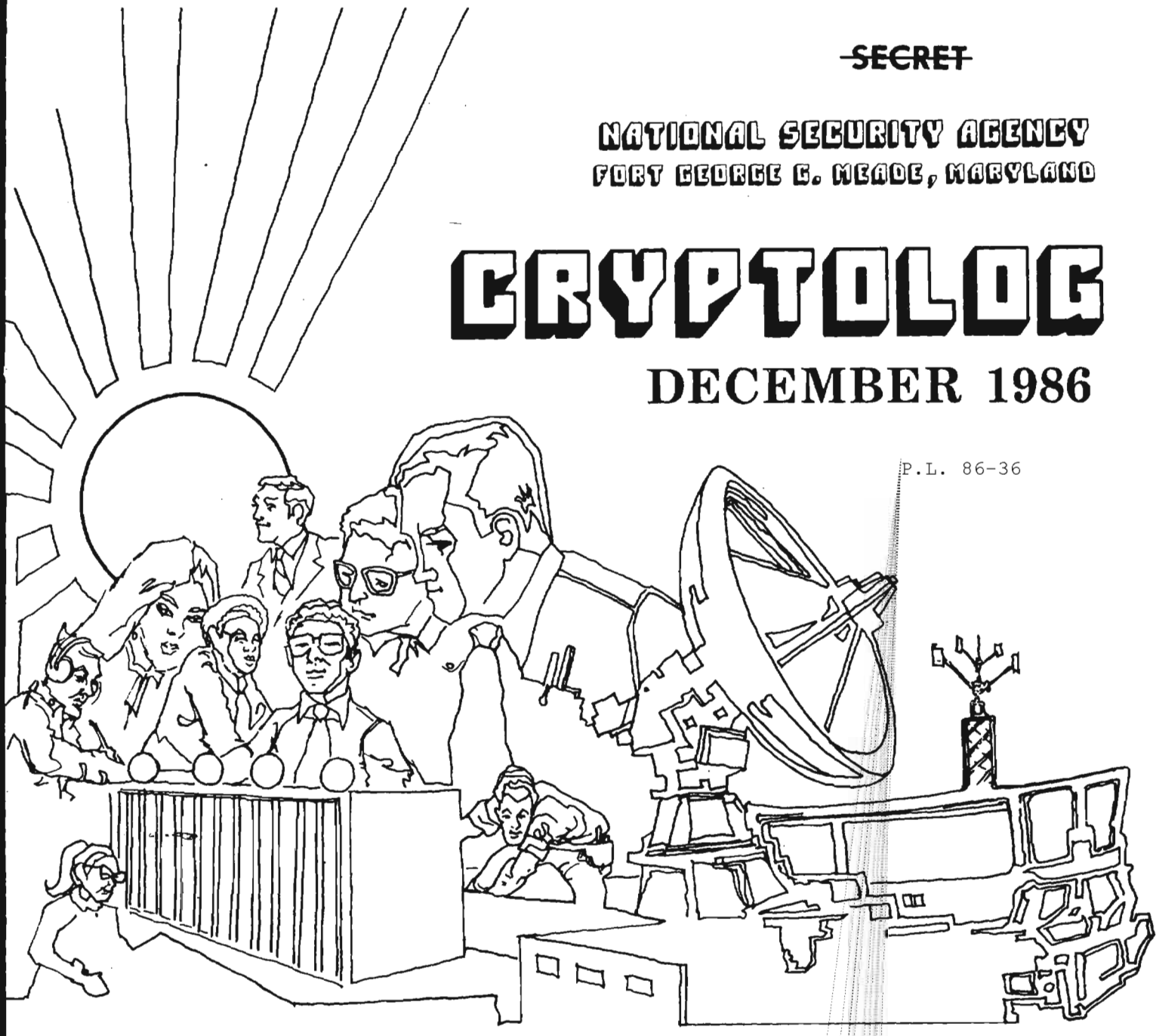
~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

DECEMBER 1986

P.L. 86-36



TECHNOLOGY SEEPAGE (U) 1
WHO IS SHE? (U) 9
CRYSCOM (U) 9
QUOTE WITHOUT COMMENT (U) 10
THE LANGUAGE IDENTIFICATION PROBLEM (U) . . . 11
PRODUCT vs PROCESS (U). 18
CHANGING JOBS (U) 21
ODE TO THE CA INTERN PROGRAM (U). 23
A COMPOSITE CONVERSATION (U). 24
BOOK REVIEW (U) . . . . . Vera Filby. 26
CONFERENCE REPORT (U) 29
LETTER (U). 31
OPPORTUNITY (U) 32
BULLETIN BOARD (U). 33
CISI CONFERENCE (U) 33
THE STORY OF A PRIVATE GERMAN CIPHER (U). 34
NSA-CROSTIC No. 63 PLUS (U) 36

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~NOT Rreleasable TO CONTRACTORS~~ ~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

DOCID: 4033692

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XIII, No. 12 ..... December 1986

P.L. 86-36

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Collection ..... (963-5877)
Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Cryptolinguistics ..... (963-1596)
Index ..... 963-5292)
Information Science .... (963-1145)
Information Security ..... George F. Jelen (859-1211b)
Intelligence Research ..... 963-3845)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... 968-8075)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-5734)

Illustrators ..... (963-3490)
..... (963-6211)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
NOTE CHANGE: **cryptlg** at bar1c05
(bar-one-c-zero-five)
(note: no 'o's in cryptlg)

Always include your full name, organization, and secure phone number.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1 HQ 8A187
Please do not phone.

Contents of CRYPTOLOG should not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

JULIA CHILD, WHERE ARE YOU? (u)

What this agency needs is a Julia Child to demystify personal computers.

Consider what she did for French haute cuisine: she brought it within the ken of any American who could read.

How? Very simply, she wrote a step-by-step handbook with ample illustrations and explanatory notes, all in an informal, joyous, and encouraging tone. Now there's a whole generation who never knew that French haute cuisine was once the exclusive preserve of a select group of the anointed.

What is odd about personal computers is that they were intended, as the name rather suggests, to be used by anybody. It's not working out that way because the user's manuals are poor. Scan the business pages of the local newspapers some time–you'll see that enterprising people have recognized this and are profiting from it by offering live-in seminars and other courses. And at a price! Highway robbers!

It would be advantageous to develop a handy-dandy for personal computers and maybe software as well, to be issued by the PCIC along with the hardware and software. As it is, many terminals are unused (or underused, solely as word processors) for lack of understandable instructions.

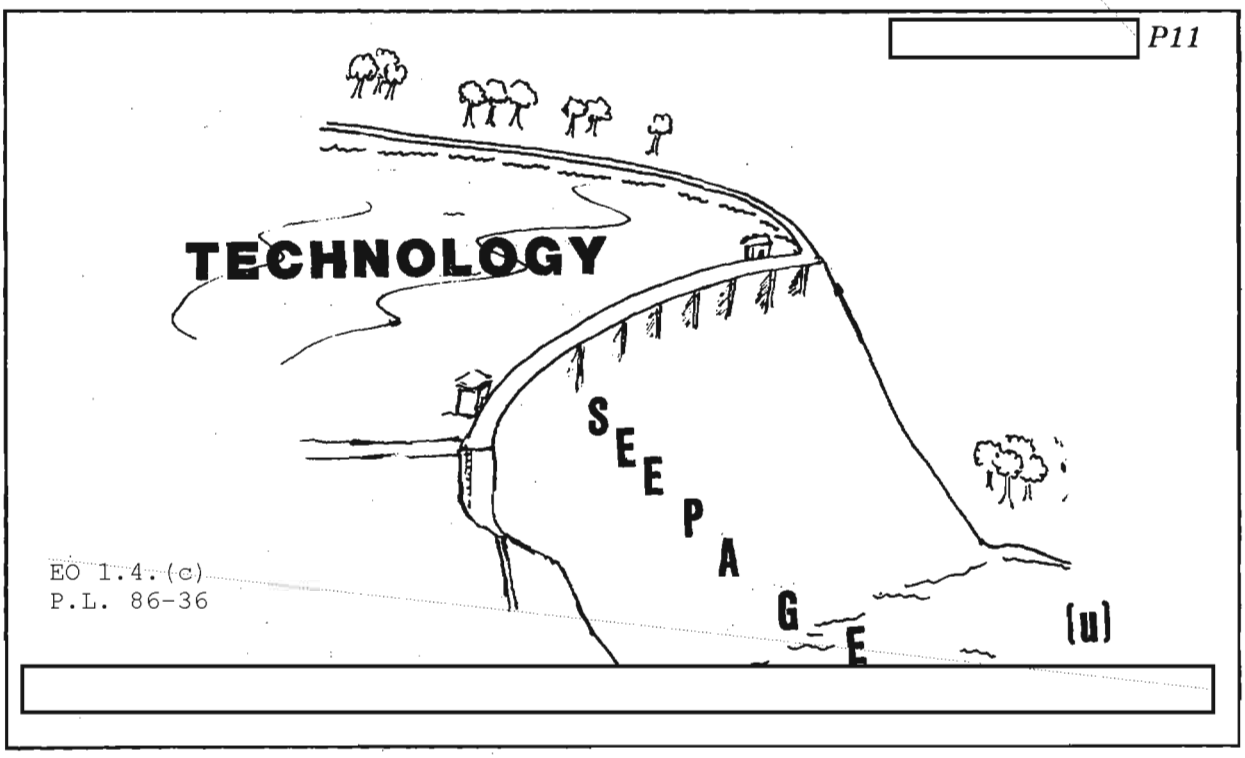
So, in the interest of productivity–think of those hours spent grumbling as well as trying to cope–it behooves Somebody Up There to commission a cookbook-type handbook to personal computers.

And when it's published, please send us a copy.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4033692

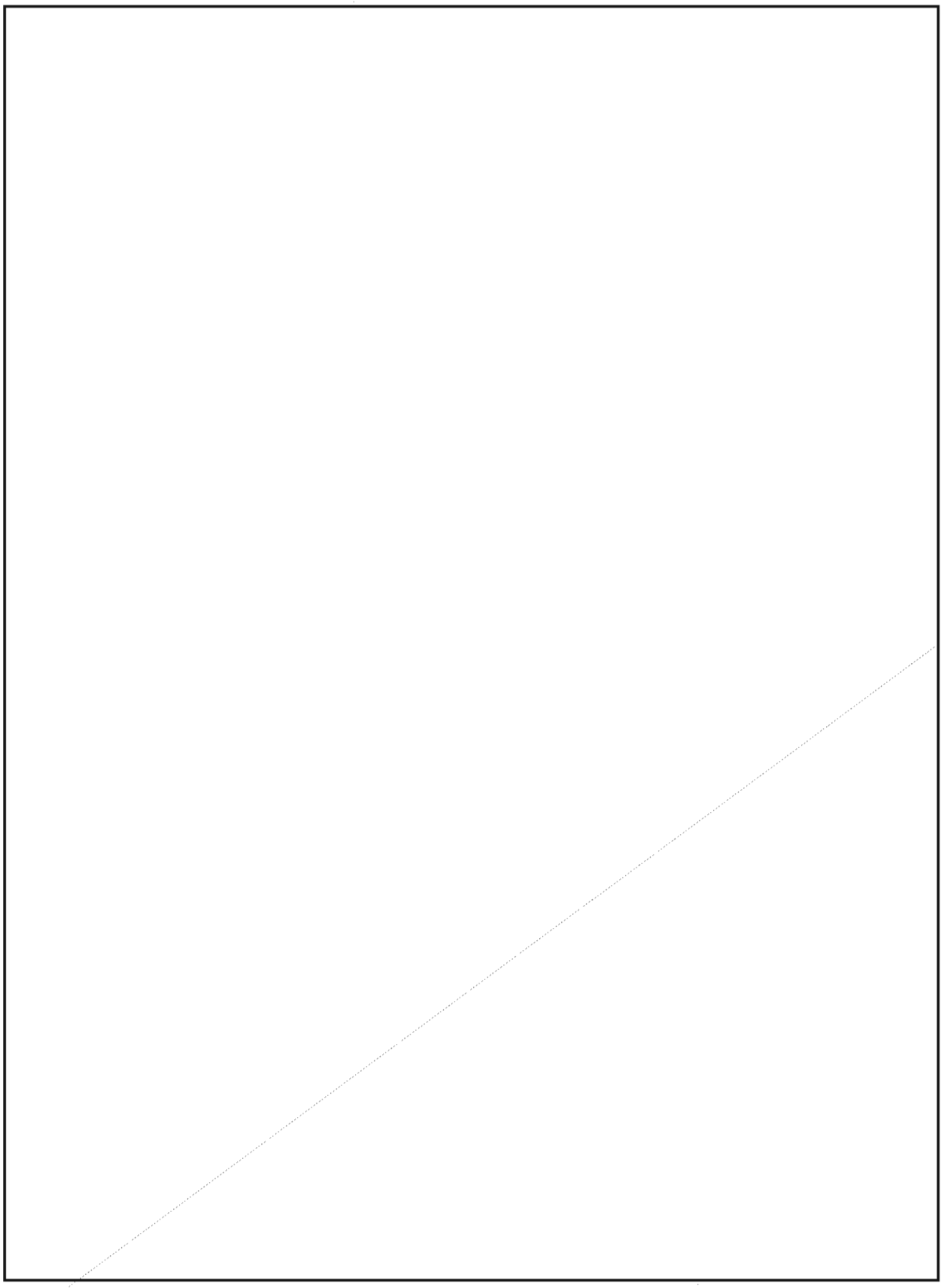
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4033692

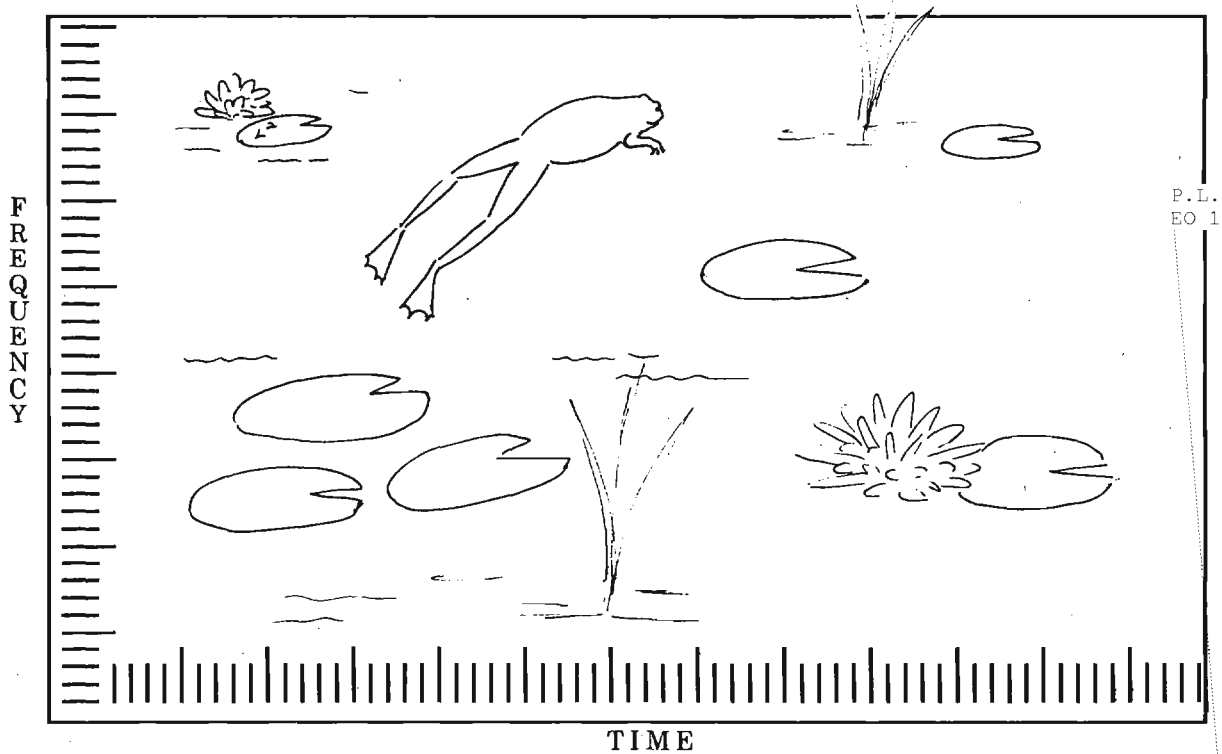


P.L. 86-36
EO 1.4.(c)

~~SECRET~~
~~NOT RELEASABLE TO CONTRACTORS~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4033692

FREQUENCY HOPPING, VARIABLE DWELL TIMES



P.L. 86-36
EO 1.4.(c)

spreading code used by the target radio is known, substantially less power is needed to jam its signal. If the spreading code consists of a relatively short recursive sequence, recovery can be made by exhaustive hypothesis testing techniques. Research to develop exhaustive methods of recovering short spreading codes would be unlikely to uncover sensitive algorithms. Longer sequences, such as those above the R20 level, cannot be recovered quickly today by exhaustive testing. To succeed against them, algorithms that parallel those used in extremely sensitive cryptanalytic attacks would have to be developed.

~~(C)~~ The services' requirements are genuine and critical to their mission. They do need a capability to intercept or to jam spread spectrum signals in a tactical environment. There are some who question whether predictive jammers or non-exhaustive spreading code recovery systems are the best - or even viable - ways to provide these capabilities. The services, however, assert that such equipments are vital to fulfilling their mission. And they have the independence, the will, and the money to pursue development.

POLICY ON CONTROLLING RESEARCH

[redacted]

(U) There is no policy that requires the services or other government agencies to coordinate with us before initiating spread spectrum research. Our knowledge of some projects was acquired by chance. We have no way of gauging what portion of the total non-Agency spread spectrum research and development of a cryptologic nature these projects represent. It would take a gigantic, manpower-intensive effort to uncover and track all such projects, and, in the current climate, it would be awkward to do it.

(U) Fortunately, none of the research that has surfaced to date really qualifies as a "smoking gun." But as the number and sophistication of

DOCID: 4033692

P.L. 86-36
EO 1.4.(c)

[redacted]

EXPLANATORY NOTES

Direct sequence spread spectrum signals are those for which the carrier is modulated by a digital code sequence whose bit rate is much higher than that of the information signal. The application of this spreading code spreads the signal across a broad bandwidth. The intended receiver of the signal knows the spreading code and uses that knowledge to collapse the signal back to its orginal form. To intercept or jam the signal effectively, the spreading code must be recovered. The binary streams used to spread the signal can be generated in a number of ways. The use of shift registers is a common method of generating these streams.

Frequency hoppers, as the name suggests, hop from frequency to frequency within a prescribed set. Hopping rates vary from a few hops per minute to many thousands per second. The hopper usually dwells on a frequency for a fixed time but some hoppers with variable dwell times are being produced. A binary stream, generated by methods similar to those used for direct sequence, is used to select the order of frequency use. A specific hopper, for example, might use a table of 256 (2^8) frequencies. It would employ some device, perhaps one or more shift registers, to generate a binary stream. The stream generated by this device would then be broken into 8-bit segments and these segments would be used as pointers into the frequency table. A wide variety of frequency hop radios is being produced, mostly by companies in the U.S., Western Europe, and Japan.

such activities increase, so will the likelihood of serious compromise.

[redacted]

(U) Such a policy statement was drafted and presented to DoD. It was never adopted. The prevailing opinion is that our presentation to DoD was handled awkwardly. This failure to "grease the skids" reduced severely the chances of the policy being accepted. Some people, however, believe that no matter how well it had been presented, prospects for adoption of the policy were slim. The military services are certain to view such a policy as an attempt to invade their domains, and they are zealous and effective in protecting what they deem to be their turf.

[redacted]

DOCID: 4033692

P.L. 86-36
EO 1.4.(c)

options. For example, pursuing Option 2 would not preclude some of the research from being done at NSA. If Option 3 were chosen, some of the research and development might be contracted by NSA to industry or the academic community.

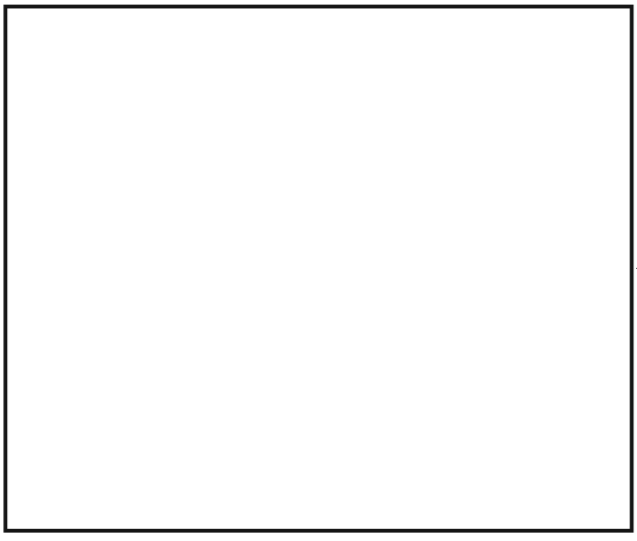
Option 1: Case-by-Case Problem Management

(U) This is the option we have pursued so far. When incidents of outside research and development in this area are discovered, the particular circumstances of the case are evaluated and an appropriate course of action is selected.

Advantages

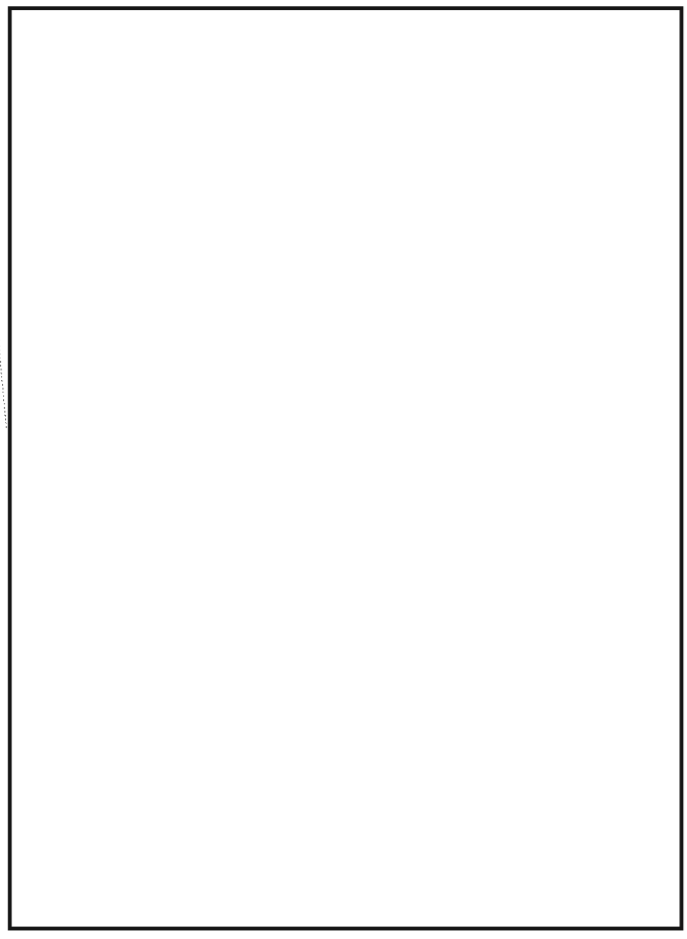
(U) So far, we have been able to resolve all the cases brought to our attention in a way that is reasonably satisfactory to all concerned.

(U) The services are rightfully jealous of their prerogatives. While they might see actions taken under this option as intruding on their turf, they might find them more acceptable than the systematic intrusion that would be introduced under Options 2 and 3.



Disadvantages

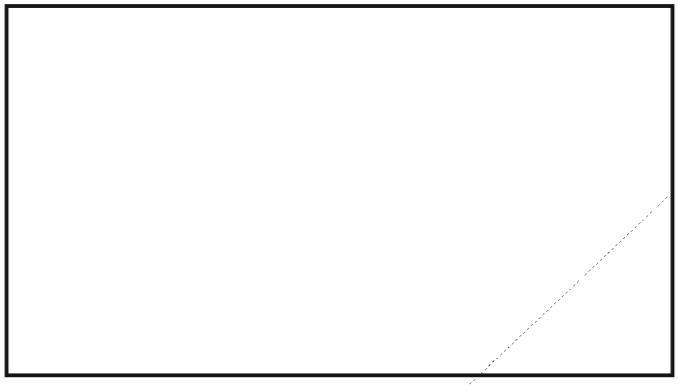
(U) This option depends upon controlling by persuasion that which is discovered by chance. It provides no systematic way to find out what research is being initiated and, despite our success so far, there is no assurance that we will be able to influence that which we do discover.



(U) As a first step in implementing this option, DoD would have to require that all government-sponsored research and development on spread spectrum be coordinated with NSA. A monitoring system based upon voluntary compliance would have little chance of succeeding.

P.L. 86-36
EO 1.4.(c)

Advantages:



(U) While the monitoring mechanisms required by this option would make this option more expensive than Option 1, it would be cheaper

P.L. 86-36
EO 1.4.(c)

P.L. 86-36
DOCID: 4033692

than Option 3. It would also require fewer people with critical skills than Option 3.

Disadvantages:

(U) Little could be done to implement this option until a DoD policy requiring coordination with NSA on spread spectrum projects was adopted. The risk that we could *not* obtain such a policy is high. Even if we succeed, a great deal of time is likely to pass before the policy is adopted and promulgated. Changing DoD policy is a slow, tedious business.

[redacted]

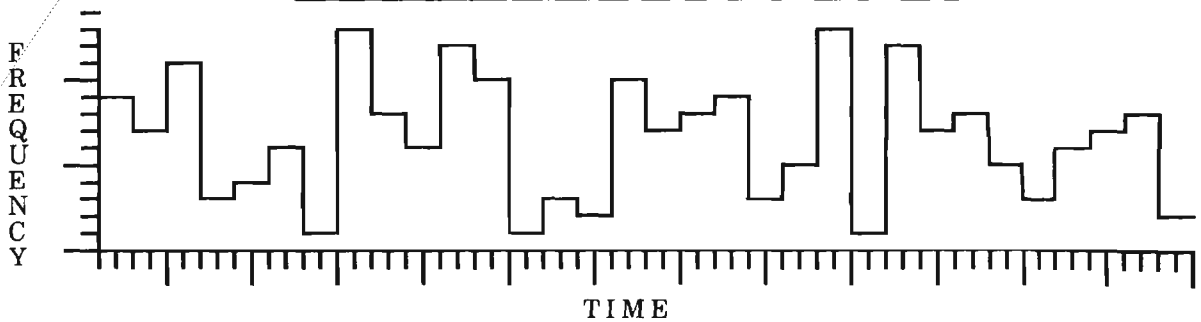
(U) The services would view implementation of this option as an intrusion into matters that have been, and in their view ought to continue to be, within their jurisdiction. They could be expected to resist both the regulation and any control mechanisms we established. It would be difficult to write a proposed DoD regulation so that the bounds of our authority were clearly defined. The services would likely seize upon any ambiguity in it to justify not coordinating with us or disregarding our counsel.

[redacted]

[redacted]

~~(C)~~ COMSEC regulations, policies, procedures and programs might be used as a model for a

FREQUENCY HOPPING, FIXED DWELL TIMES



P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)
DOCID: 4033692

system to control the deployment, accounting, use, and maintenance of spread spectrum equipment containing sensitive components.

Advantages:

(U) NSA's active role under Option 3 would provide much greater control over the technology seepage problem than would the Agency's passive participation under the other two options.

[redacted]

(U) Under either of the other options, it would be difficult to control duplication of research and development by the individual services and by us. By accepting responsibility for the sensitive components, we would not only ensure that the research and development for them was done securely but also that it was done without expensive duplication.

(U) Protecting sensitive techniques during the research and development stage is just the beginning. Safeguards must be applied to all facets of the product's life cycle. Care must be exercised in how the system is deployed, accounted, used, and maintained. Under Options 1 and 2, it would be difficult to persuade the services to institute life-cycle control procedures that would provide a sufficient level of protection for sensitive components. Those life cycle support control procedures that were employed probably would

[redacted]

P.L. 86-36
EO 1.4.(c)

DOCID: 4033692

P.L. 86-36
EO 1.4.(c)

(U) Openness would not mean disclosing fully everything that we are capable of doing. It would, however, require us to explain to the services what we can do, what we can't do, and that there may be some things that we can do but cannot provide to them. We would also have to provide an acceptable rationale for not sharing some capabilities with them. We believe that our decisions on what to release will be based upon sound technical judgments. We should be able to convince the services that they will not be made arbitrarily or out of contempt for their capabilities.

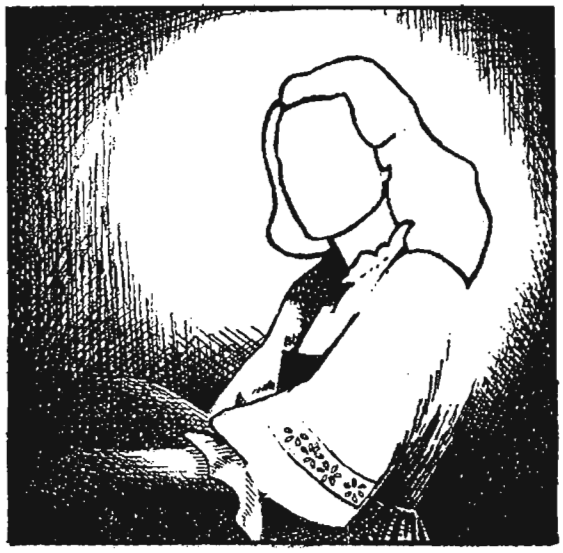
P.L. 86-36
EO 1.4.(c)

(U) There are no easy solutions to this problem. Option 3, if implemented well, would minimize the risk of disclosure of sensitive cryptanalytic techniques at all stages, from initial research to field operation of a system.

P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)

DOCID: 4033692



WHO IS SHE?

P.L. 86-36

[redacted] *T54*

She was born Hedwig Eva Maria Kiesler in Vienna, Austria, the only child of a prominent banker. In 1938, alarmed at the growing threat of Hitler and the Nazis, she left her native land and came to America, where she became one of Hollywood's most glamorous stars.

Her fans never suspected that she was also playing another role, that of inventor. In 1942, composer George Antheil and H. K. Markey (her married name) were granted a patent on their "Secret Communication System," a way of guiding torpedoes to their targets by frequency-hopping, spread-spectrum radio transmissions. A technique nearly identical to theirs was later used operationally by the U.S. Navy.

Who is this actress-inventor?

Answer on page 20.

Note Change in Electronic Mail Address

c r y p t l g @ b a r l c 0 5

no 'o'

CRYSCO - 87

FOURTH ANNUAL CONFERENCE

8-12 June 1987 at NSA

Sessions held in the Friedman Auditorium and in Conference Room 2W087

AUDITORIUM SESSIONS ARE OPEN
to persons with a green or orange badge

OTHER SESSIONS REQUIRE TICKETS
(distributed through your office)
a green or orange badge
and LACONIC access

★

General topics include:

- CRYSCOs in review;
- IDA/CRD and IDA/SRC updates;
- UNIX conversions;
- Transition to UNIX;
- Future workstations;
- Mass storage requirements and proposed solutions;
- Supercomputing trends;
- Programming multiple CPU and massively parallel systems;
- Requirements for software management system;
- Computer graphics;
- IOSP updates;
- Software development standards: do they work?
- Reports from CSE, DSD, and GCHQ;
- OWL libraries;
- CRYSCO-87 wrap-up.

★

Additional information can be obtained from the CRYSCOM executive, [redacted] *A538/P13, 963-4196.*

~~(FOUO)~~

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4033692

QUOTE WITHOUT COMMENT

Editor's Note: A number of readers sent us copies of the following translated excerpts from an article that appeared on 25 March 1986 in a literary magazine of the United Emirates Republic.

"

¶ Only a few people know that this agency actually exists; almost no one outside the US knows anything about it, while one out of a hundred thousand Americans knows of its existence.

¶ The annual budget of the NSA is $12 billion, and it employs sixty thousand Americans.

¶ Its chief assignment is to know everything, not only inside the US but everywhere in the world. It traces all telephone and radio calls whether their subjects are political, military, economic, cultural or even personal.

¶ It possesses almost absolute power; its ears and eyes are planted everywhere, but mainly in the Soviet Union. NSA personnel were the first to know of the crash of the Russian space shuttle, Soyuz.

¶ Its equipment and staff are able to analyze ciphers.

¶ It is not an exaggeration if we say that if Gorbachev sneezes the White House will be the first to hear it.

¶ The agency was established in 1952 during the second term of former president Truman. It is not subject to the oversight of the congress or any other US organization. Furthermore, it does not legally exist. When it was established, only the president and national security advisor knew about it.

¶ The NSA headquarters is located inside a thick forest of cedar trees near Fort Meade, Maryland, two hundred kilometers from Washington. The complex is very well protected and is more or less a fort, equipped with the most advanced electronic warning systems.

¶ The staff are chosen from among the personnel of other security agencies after being subjected to psychological training courses and a detailed scrutiny of their personal files. Because wives love to gossip, only bachelors are allowed to join the NSA. The staff may only marry each other.

¶ The staff is only allowed to have the minimum amount of social relations or may not have any social life at all.

¶ The NSA has very advanced computers, one for analyzing normal calls, and the other to pick up and analyze coded calls. The average number of calls that the computers receive daily is 300,000 normal calls and 200,000 enciphered calls. These computers are able to read and to analyze codes at up to 600 lines per minute and in all languages.

¶ The agency is a field study' of the most up-to-date scientific advances.

¶ Like the human brain, the agency's brain' is divided into two parts. The right part, named CARION,' is equipped with four linked IBM 3033 computers attached to three huge printers that are able to print 22 thousand lines a minute. The left part is equipped with super computers each of which weighs 5,000 kilograms and are able to do 200 million operations per second. NSA computers write up to 320 million words per second.

¶ Outside the USA, the agency has secret operations branches in Japan, Taiwan, South Korea, West Germany, South Africa, Lebanon and Turkey. These offices are usually described as annex buildings to American embassies, consulates, and US cultural and commercial organizations.

¶ The agency relies mainly on satellites that are specialized in espionage. From an altitude of 200 kilometers, these satellites are able to photograph any object that is two feet or more above the surface of the ground.

¶ The reason some of the NSA's secrets are being revealed at this time is to preserve part of America's image of technological superiority which was injured after the CHALLENGER tragedy. □

"

~~FOR OFFICIAL USE ONLY~~

DOCID: 4033692

The Language Identification Problem (u)

P16

P.L. 86-36

~~(C)~~ A message in a language that no one can recognize is a vexatious thing: there is no knowing whether the information is trivial or important as long as the text cannot be understood. Even if the information in itself is not valuable, there is the possibility that identifying the language may be helpful for making decisions and adjustments in collection.

~~(S-CCO)~~ The first thing we have to do is to get rid of the idea that language identification is simple. Language identification is a large subject that has only begun to be explored along lines that we would find useful. To begin with, consider the problems:

- The way in which language recognition takes place is not well understood. It appears that all people do not do it the same way: some rely principally on recognizing individual words, and others primarily on recognizing rhythm, cadence, and overall effect.

- Estimates of the number of languages in the world have run mostly between 3000 and 4000, and have tended to keep rising. The number of languages in Africa is said to be at least 850; in India, 800; in the USSR, 130; in South America (with less certainty) perhaps 500 or more, and so on.

- In the future we can expect to get more intercepts in unidentified languages than before. This will be due to increasing international travel and commerce; the use of foreign labor; the growing availability of radiotelephone, satellite communications, and multiple channels; and new collection techniques with more comprehensive intake.

~~(FOUO)~~ Fortunately for us, while 4000 is a meaningful figure in the field of anthropology, in the world of communications it is not. In practice, we are not going to have to identify 4000 languages. The vast majority are minor languages, spoken in remote and primitive areas and by tiny populations, some of them in single villages and 30-person tribes.

(U) Of the 4000 languages, about 100 are spoken by 3 million people or more, and another 50 or so are spoken by 1 or 2 million; all the rest have fewer than a million speakers apiece. Only about 70 languages are official languages of a national government. (This is because Arabic, English, French, and Spanish are used by so many. The number of countries in the world is about 170.) Another 15 or so are languages of sizable and well-known minorities.

~~(C)~~ In real life, we are going to find ourselves dealing with the same languages most of the time, and there will not be much more than

100 of them, which is still enough to give everybody plenty to do. My own experiences have generally fitted in with this principle: When it is an official national language, we can usually identify it; when it is a well known minority language, we have a good chance; and when it is neither of these, it can become very hard going.

[redacted]

~~(C)~~ How do we deal with all this? Experience has brought some pieces of accumulated wisdom with respect to both voice and graphic communications, as well as a subset of the latter, handwriting, which must be considered separately.

~~(C)~~ The ideas I present below are based on my own experiences with language identification. These ideas are set forth as suggestions for linguists and ways that managers and supervisors can help.

I. POINTERS FOR LINGUISTS

~~(FOUO)~~ Following are some suggestions for linguists who have been tasked with identifying an unknown language. Voice communications, message traffic (often referred to as "graphic"), and handwritten material are each considered separately.

A. VOICE COMMUNICATIONS

Try Rewind.

~~(FOUO)~~ Probably the first thing to do with a voice tape that defies identification is to try running it the other way, in case it has not been rewound. Don't laugh: a remarkable number of unidentified languages have turned out to be Russian or English in reverse.

EO 1.4.(c)
P.L. 86-36

Look for a short speech segment of one or two syllables or words.

(U) Often the easiest way to identify the language of a conversation by word recognition is to concentrate on the shortest speeches in the exchange. Short speeches by nature present the fewest word division problems, tend strongly to stereotyping and the use of common words, and usually represent simple ideas.

(U) The three primary short speeches are **Yes, No**, and **What?** A highly favorable case occurs when there is a long speech of one or more sentences, a short response of only a syllable or two, and then a repetition of the long speech. The odds are that the short speech means **What?**. Or if the response is longer than one or two syllables, it is likely to be: **"How's that?" "What did you say?", "What was that?", "I didn't get that"** or **"I couldn't hear you."**

(U) Now you will find it much easier to check for a word or phrase in dictionaries or lists when you know what you are looking for. (Unfortunately, there are people everywhere in the world who say "Aahh?" or "Haahh?" instead of "What?")

Keep an Open Mind, and Try Again.

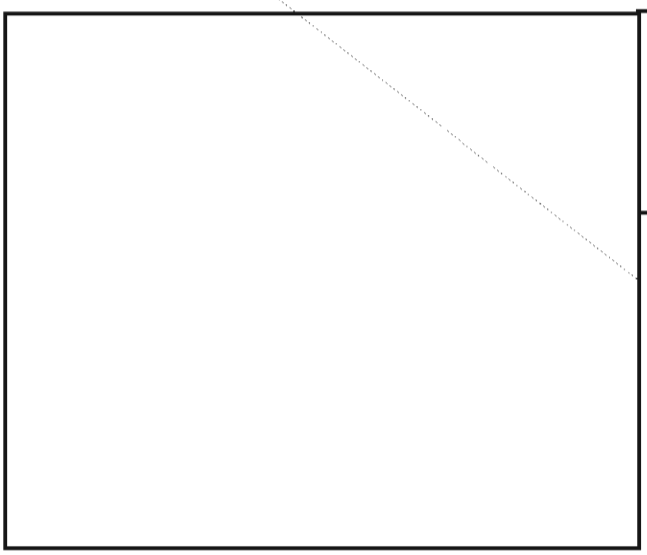
[redacted]

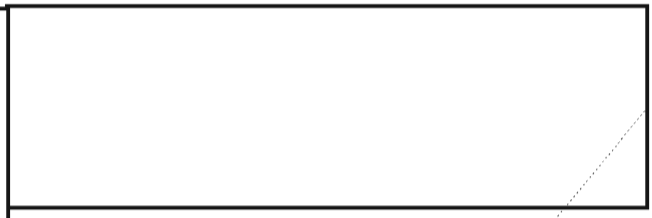
Consider the possibility of intrusive foreign words.

(U) International word borrowings "contaminate" language samples and have a cluttering effect that makes identification harder. Words of international scientific and

EO 1.4.(c)
P.L. 86-36

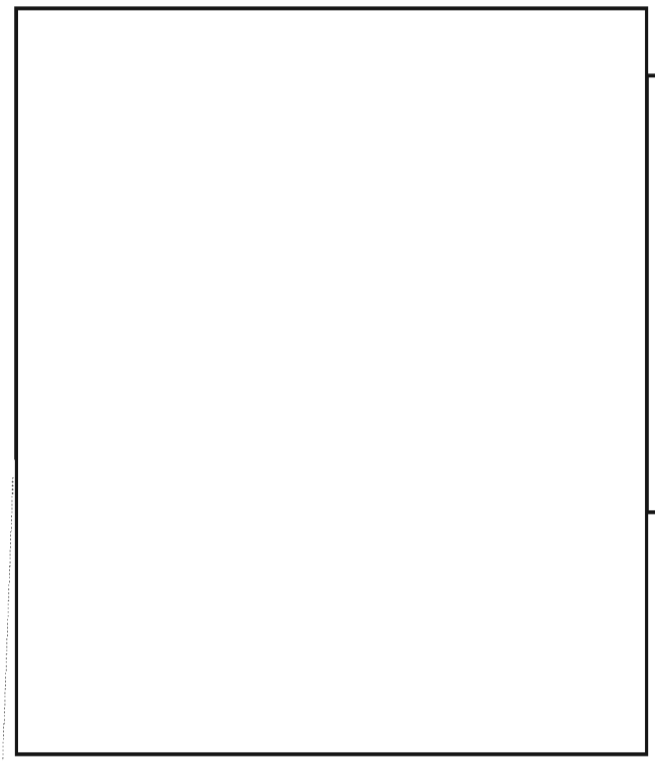
EO 1.4.(c)
P.L. 86-36
DOCID: 4033692





technological vocabulary like "telephone" are so widely adopted that they only hinder identification.

(U) Languages of Islamic countries have a considerable stock of borrowed Arabic words, and frequently it is the same Arabic words that several unrelated languages have borrowed. Obvious examples are Persian (Indo-european), Uzbek (Turkic), and Indonesian (Austronesian), which have many of the same Arabic words in common.



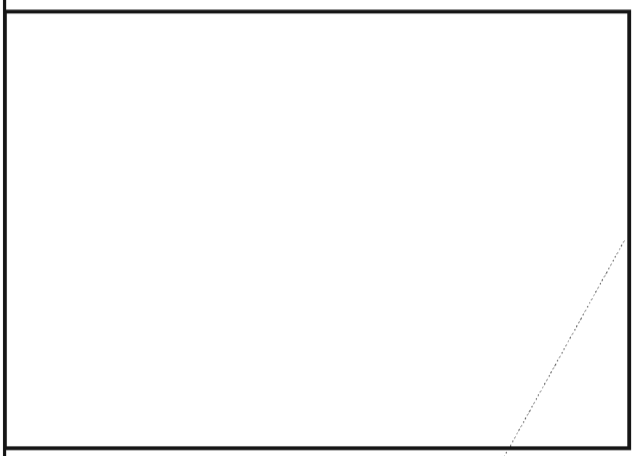
Establish What is Good Text by Finding Repeats.

(U) Make a photocopy of the text so that you can mark it. Then underline every string of letters that occurs in the text more than once. This will usually ensure that the things you are looking for in dictionaries are not garbles.

P.L. 86-36
EO 1.4.(c)

Collect References

(U) There are several identification books, intended for librarians and printers, which devote a page or two to each language and give a paragraph of sample text. Some of them also give some information about the grammar and point out some common words that are characteristic. One drawback is that the sample paragraphs are quite short and often fail to include some very characteristic words. Another is that the samples are given as they would appear in a printed book, whereas traffic is often in transliterated form, and there can be several transliteration systems for the same language.



C. HANDWRITTEN MATERIAL

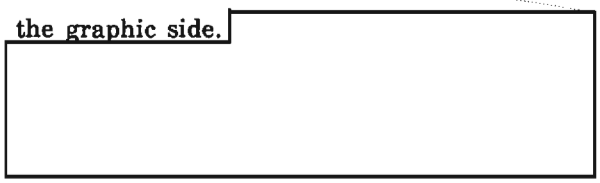
~~(FOUO)~~ Handwritten materials present special problems and must be considered separately. Generally, they present the hardest problems on

P.L. 86-36

P.L. 86-36
EO 1.4.(c)

DOCID: 4033692 P.L. 86-36

the graphic side.



(U) Handwriting that can be matched to a known cursive script, such as Arabic, Russian, Greek, Armenian, Georgian, or old Albanian is easily identified. Samples of cursive writing can be found in the following books. Call numbers are those of the NSA library:

Diringer, D: *The Alphabet.* 1968. P211.D62.1968 (2 vols)

Jensen, H: *Sign, Symbol and Script.* 1969. P211.J45gE.1969

Hoskins & Meredith-Owens: *A Handbook of Asian Scripts.* P213.B77

(U) What is not easily identified is handwriting with partial resemblances to one or more known scripts, especially when the characters are connected to each other, creating great uncertainties about how to separate them. Handwritten pieces of this kind present too many questions all at once: Is it plain language in an unidentified language? Is it really writing at all, or just doodling? Or done by someone under the influence of a narcotic who thought he was writing? Or a hoax? If it is plain language, why can't we match it with a known script? Is it a cipher? If so, we are at a great disadvantage in not knowing what the underlying language is, and at another great disadvantage in not knowing how many characters there are and what they are.

(U) For example, if we were looking at an unknown script that contained signs like English handwritten c and cc, e and ee, l and ll, t and tt, all letters made with only one or two strokes, we could not be sure whether cc, ee, ll, and tt were connected double letters or separate letters in themselves.

(U) Again, we can start by looking for repeated sequences, which would suggest that the text was not random doodling (but would not prove that it was not), and for repeated combinations followed by spaces, which would suggest grammatical endings in an inflected language, either in plaintext or in simple substitution. After that we are in for a long effort with poor prospects.

~~(FOUO)~~ Among the many problems are the alphabets, sometimes bizarre, that are invented by the writers; fortunately, these often prove to be monoalphabetic substitutions of a well-known language, and so they are easily solved. An important diagnostic feature of invented alphabets is that the characters are usually clearly drawn and clearly separated.

~~(FOUO)~~ An example of all of these problems is the Voynich manuscript, a unique European manuscript thought to date most probably from the 15th or 16th century, which has resisted solution, not only by philologists early in this century, but by NSA cryptanalysts as well.

II. HOW MANAGERS CAN HELP

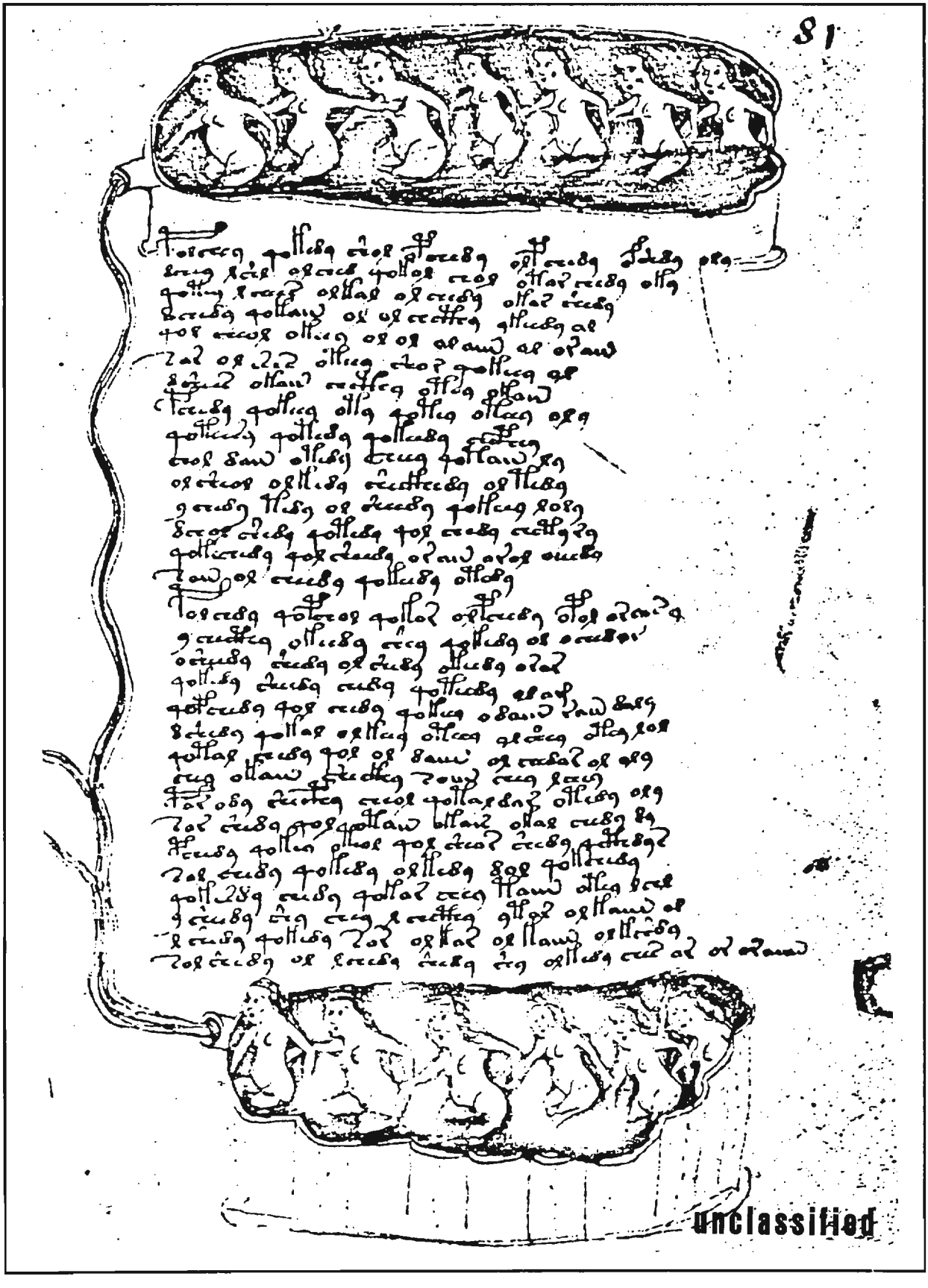
~~(C)~~ Simply having a list of expert voice linguists who can be consulted has been tried; it was found that the list required constant updating because of normal employee turnover. In any case, the old practice of carrying a tape around and trying it on various linguists is slow, inconvenient, unreliable, and not always successful either. It is also heavily dependent on luck and guesswork in finding the right linguists to ask.

(U) But there are several other ideas that might be tried to improve our success rate in identifying unknown written text. And these depend upon the active support of managers and supervisors.

~~(C)~~ Messages in unidentified languages turn up only sporadically but persistently. Because they constitute a recurrent problem but not a continuous one, they are dealt with individually, without any method or system and without any record of what was done and what resulted. They should be dealt with more methodically. What I have in mind would not involve concentrating and centralizing identification efforts but would be the opposite of that: making more analysts able to do identification by providing information on it

~~SECRET~~

THE VOYNICH MANUSCRIPT (u)



unclassified

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4033692 P.L. 86-36

more systematically. By no means are all of these new ideas.

(U) In general, supervisors and managers can do two things to help linguists identify unknown languages:

Support the Development of a Training course.

~~(FOUO)~~ Training is not a new idea. It would have the advantages of introducing methods in a package, rather than have everyone rediscover them individually, of furnishing supervised familiarization and practice, and of providing a basis for the creation and distribution of working aids. For example, the course could include a brief and practical introduction to phonetics, with special attention to speech sounds in a wide variety of languages.

Provide Reference materials.

(U) Recognition is by nature matching. The analyst must be provided with bases for comparison. This may mean purchasing books, subscribing to periodicals, and acquiring video and other voice tapes.

(U) Now for some specific suggestions about each type of language identifcation problem.

FOR VOICE TRAFFIC

Encourage the Use of the Tape Library.

[redacted]

P.L. 86-36
EO 1.4.(c)

Support the Updating and Expansion of Existing Word Lists.

[redacted]

Commission the Compilation of a Word Grid.

[redacted]

FOR A WORD GRID

Yes, No, What?
Hello, Hi, Goodbye, So long
Thank you
Wait a minute
Who is calling?
All right, Okay
That's right
I understand, I see
Listen, ...
Don't hang up!
That doesn't make any difference
Fine, Excellent
Impossible
Immediately
Necessary
Important
Will arrive
Because
North, East, South, West
Yesterday, Today, Tomorrow, Tonight .
Day, Night, Week, Month, Year
Next, Last (Week, etc.)
Names of weekdays
Names of months
Numbers from 1 to 10
Selected higher numbers, e.g. 100, 1000

P.L. 86-36

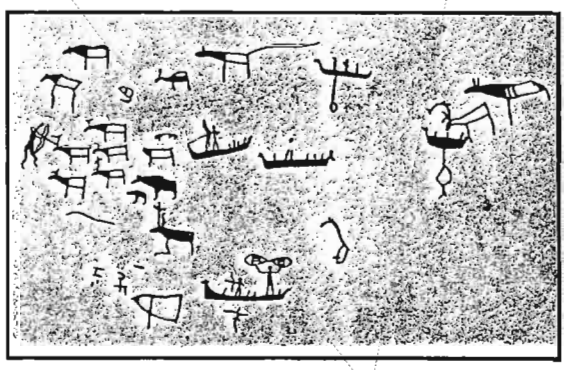
amount of text and without "too many" borrowed or foreign words.

Collect Samples of Transliterations and Romanizations.

~~(S-CCO)~~ Printed books on languages regularly give each language in its traditional writing system.

Sponsor In-house Research.

(U) Possibly some of the many things that are not known in language identification could be resolved by study and investigation. For example, there appears to be a difference of opinion on whether it is possible for someone who doesn't know a tonal language to tell whether it is one merely by listening to it. The objection is that in at least some cases it may be difficult to tell word-intonation from sentence-intonation. If this question could be settled, it would be a valuable piece of information in language identification.



P.L. 86-36

A FINAL WORD

(U) There is a great deal to be done in language recognition. At this time no one knows how many possible approaches there are, and no one system can claim to be invariably successful. □

DOCID: 4033692

P.L. 86-36

PRODUCT vs. PROCESS: One View (U)

[redacted] G14

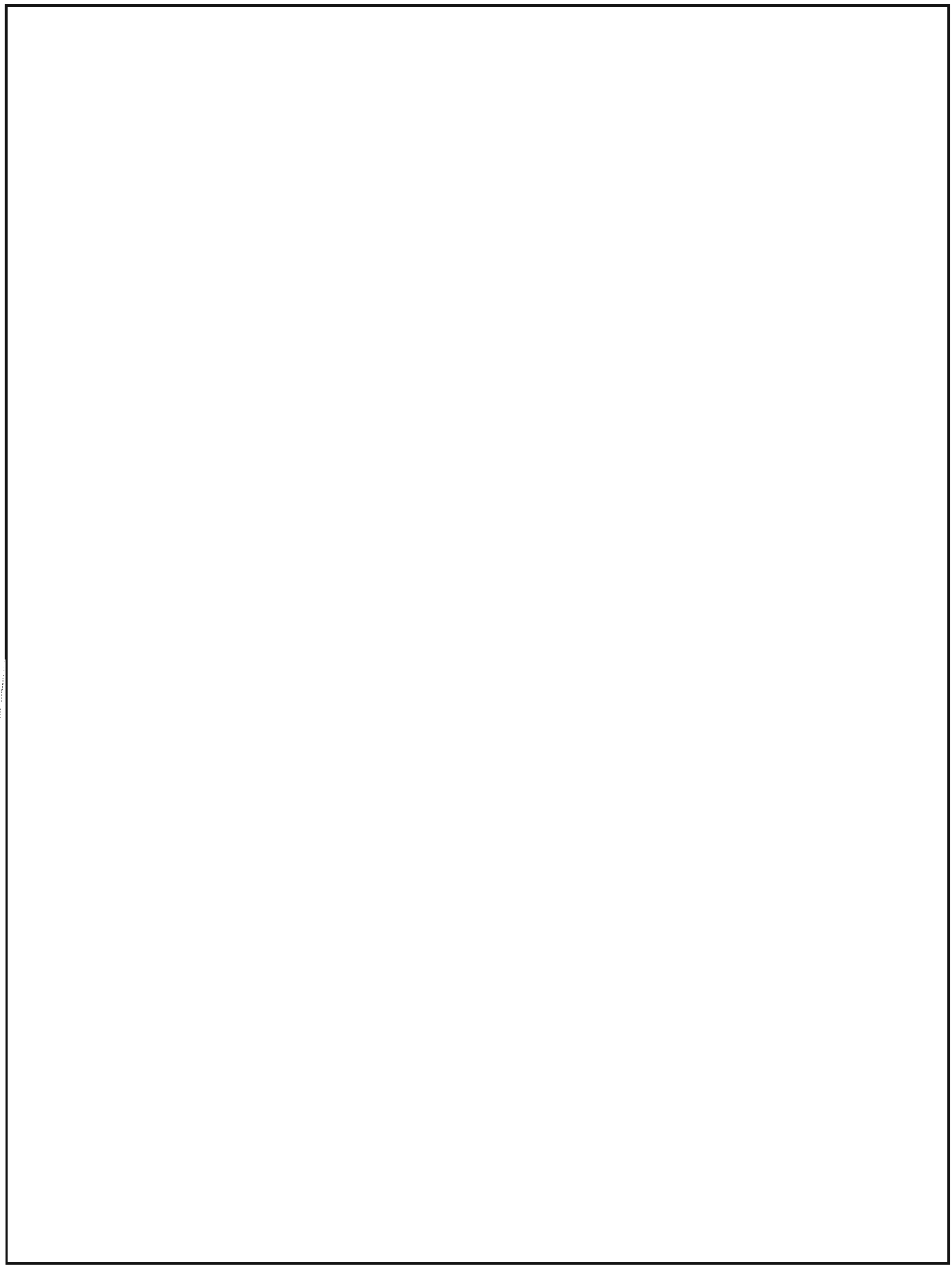
~~(FOUO)~~ Like the management of many other middle-aged organizations, the management of NSA is forgetting why the organization was created. The auxiliary functions of the Agency are distracting us from our primary task of producing intelligence information. In other words, we have become enamored with the process at the expense of the product. Recognition of this situation is critical because there is no "bottom line" to measure NSA's effectiveness; there is no danger signal to alert us that all is not well. (Some may argue that customer satisfaction is the "bottom line," but I believe that the customer is not aware of what could be provided and, therefore, makes decisions regarding NSA product without knowledge of our full capabilities.)

[redacted]

[redacted]

P.L. 86-36
EO 1.4.(c)

DOCID: 4033692



P.L. 86-36
EO 1.4.(c)

DOCID: 4033692

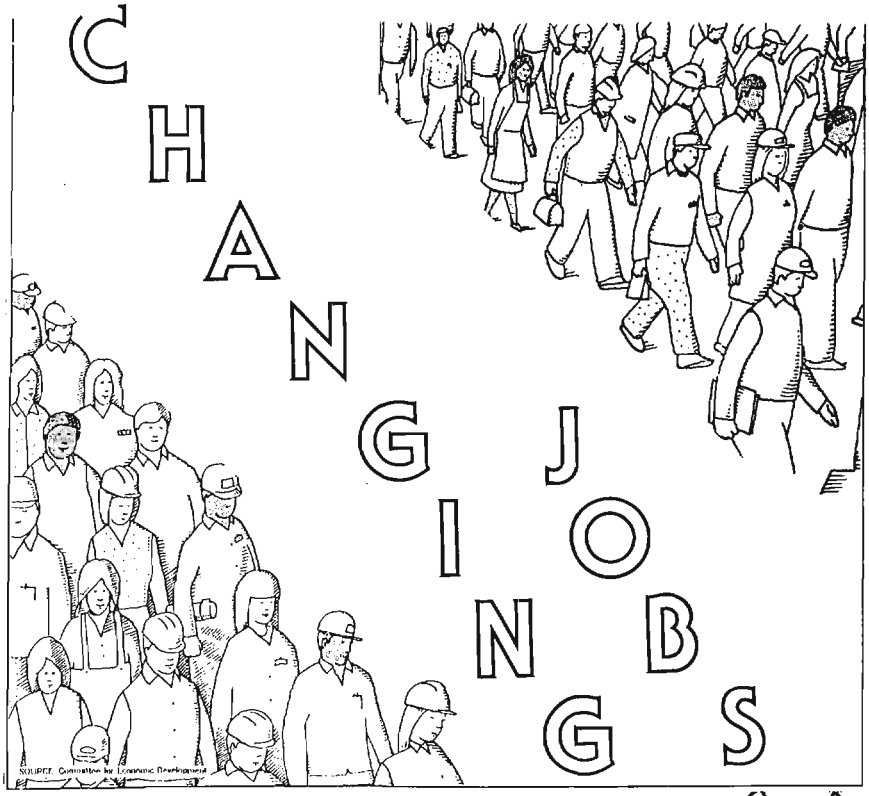
P.L. 86-36
EO 1.4.(c)

Answer to **WHO IS SHE ?** *on page 10.*

Hedy Lamarr, who once said, "Improving things comes naturally to me."

DOCID: 4033692

CHANGING JOBS (U)



P.L. 86-36

g221

So you want to change jobs within the Agency? One of the great advantages of working at NSA is the vast array of varied opportunities awaiting you. Unfortunately, many employees find it difficult to move. It doesn't have to be.

The first step is to determine your goals. For some the goal is to become a senior executive, while for others it is the more modest goals of enjoying their jobs and receiving reasonable promotions. Some employees want to work within a particular discipline and move around among different targets, and others are enamored of a particular country but want to work on various aspects of that target; still others want to diversify, and seek assignments in other fields such as personnel, logistics, COMSEC, etc.. And then, of course, there is the question of management or tech track. Once you have examined your personal needs and determined your goals you can start looking.

In order to be able to move easily you must first establish yourself as a skilled and willing worker. Get your assigned tasks completed and then ask your co-workers to teach you what they are doing. Ask your supervisor to give you tasks outside your normal range of duties. Learn everything you can. Take every course in your discipline that you can arrange. There are self-study courses in abundance, and you may find a learning center open after or before your normal duty hours. Try changing jobs within your current organization; that's generally an easy move.

Once you have established yourself as a skilled, experienced, and willing worker, start the above process in reverse. Teach your skills to others in your office; train someone to do

~~FOR OFFICIAL USE ONLY~~

DOCID: 4033692

your job or train several people to do different parts of your job. The mission, your co-workers, and your supervisor all benefit from this approach, and so do you. This course of action will allow you to move, for it is often easier for managers to find and hire someone at a lower grade. Don't fall into the trap of trying to make yourself indispensable; if you succeed you are doomed to stay in that job.

Write a complete and detailed description of your job. No one is more capable of doing this than the individual doing the job. This has multiple benefits. Not only will you surprise yourself (pleasantly) in finding how complex your job is, but by detailing it you may think of some ways to broaden or simplify the tasks or to improve on your performance. The description will also serve as a detailed guide for your replacement for learning your duties. In addition, your supervisor will be able to use this job description when writing your performance appraisal as well as a guide to writing a vacancy announcement, and even as a tool for interviewing applicants for your job.

Use your network of friends and acquaintances to look for a possible successor. Even if your job is all wrong for you, you may know someone else who would be a perfect match for your job. Suggest they come and talk with your boss. In fact, everytime you hear of someone looking for a job change or hear of a job opening, try to help.

All this, and we still haven't gotten around to discussing how you are going to find a new job! Well, being in a position to be granted a release from your present job is the first step in moving. Without it, you will have to find an advertised job, and even then, your supervisor can hold you for 90 days. Obviously, one of the secrets to moving is making it easy for your supervisor to let you go.

OK, now you are ready to move. How do you find that new job? My first suggestion is to review your goals, looking for various intermediate paths to achieving your goal. You can stay in one place a long time waiting for that one "perfect" job or you can be flexible and take a series of jobs, all of which teach you new things and allow you to make various contributions.

Now start talking to the people in your network. Of course you have one. They are the folks you eat lunch with, members of any Agency clubs you belong to, people you deal with professionally in other offices. If you've been trying to help them, they'll help you. Find offices which interest you and make an appointment to talk to a branch or division chief in that office. Ask your boss to check out his or her network for openings. Go to your Pers Rep and your Career Panel Exec and let them know you are looking. Don't assume that all advertised jobs are bummers. Talk to anyone who has a job which might in anyway move you closer to your goal. The job might not have the "right" title but the duties may be exactly what you are looking for, or close enough to fill the bill. Remember that you can apply for a job one grade above or below your current grade. (No, you don't take a salary cut.)

Get your Personnel Summary in tip top shape and have copies available. Make sure you have neither under nor over- sold yourself. Find ciritical friends to review it for you. Ask former supervisors if you can use them as references. If you are a GG-12 through GG-15 make sure that the SPCP folks (M44) are aware you want to move. Be creative, innovative, even daring in looking for ways to promote your job search. A large portion of Agency jobs are constantly being vacated, and the opportunities are there waiting for you.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4033692

Having found some interesting openings, interviewing for the position is the most important thing you can do. Many (even most!) NSA supervisors have never been trained to interview job applicants. This means that you must train yourself to be a top notch interviewee, without having the benefit of being asked the right questions. You have two goals during the interview: finding out if the job is what you want to do, and finding out if you and your prospective boss share the same philosophy. Typically an Agency supervisor will tell you what is being done in the office and a general idea of what your job will be. You will have to ask specific questions about the actual work. In some cases you will want to spend some time with the incumbent or another worker to see what is actually being done. This is the easy part.

If you want to be happy in your new job you also have to reveal a lot of yourself to your prospective supervisor. Tell him or her your worst faults--if he or she can't live with them, neither of you will be happy when those faults come out on the job. You're better off knowing that up front. Also, discuss what you believe to be your virtues and your methods of operation. If you need a lot of independence on the job, say so; you'll chafe under a controlling supervisor. If you need regular feedback on your performance, say so; you'll get ulcers waiting for the strong silent type. Watch and listen carefully to the supervisor during this discussion. Body language and verbal responses to your revelations will tell you more about that manager's style of management than you could ever learn by asking, "What's your management philosophy?"

Be truthful about your intentions during an interview. If you plan to stay in the new job for only two or three years, make that plain. You can contribute a lot during that time, and anyway, there is no stigma to moving; the seniors do so about every two years. If, at the end of your interview, you know that you aren't interested in that job, have the courtesy to tell the interviewer clearly that you are not interested. You might even suggest the name of someone you know who might be a good candidate for the job. If you are considering several other jobs you should tell the interviewer this fact. Play it straight; this same manager may call you years later with a job you do want! □

The following is classified ~~CONFIDENTIAL~~ in its entirety.

ODE

TO THE CA INTERN PROGRAM (u)

P.L. 86-36

[redacted] *B53*

Intern Grads both brave and tough
How we learned that cryptic stuff!

Was that program quite a chore
And that paper quite a bore?

Did we importune our buddies
As we practiced Folklore studies?

Did we grow more fatalistic
As we mastered each statistic?

If we shunned some probability
Did we suffer culpability?

In the washroom did we primp
Rather than practice IMP?

Would we games and puzzles play
Instead of work upon a CRAY?

Or struggle with a CDC
Or, worse yet, some weird SPD?

To choose UNIX or PCDOS
Were we ever at a loss?

Feezy filzy foozy fumzy
Do our brains feel slightly numbzy?

Are we live or are we dead
After so much traffic read?

Now we're Permanent and Real
What's the bravest thing we feel?

DO YOUR WORK, OH CAFETERIA
AFTER THREE YEARS

WE'VE NO FEAR O' YA!

Reprinted, with permission, from the October 1986 issue of the Cryptanalysis Intern Bulletin

DOCID: 4033692

A COMPOSITE CONVERSATION (U) Loosely Based on Experience

P.L. 86-36

[redacted] G72

I said, "Boy, I sure could use some computer support! I've got masses of data in this language to process and I need some efficient way to put the good stuff into English."

He said, "Boy, are you in luck! I've got just the thing for you, an interactive, virtual, untra-fast Gizmo Super-X computer with a superpowered, glitch-free VDT that won't even give you eyestrain. It will do everything for you but tie your shoes!"

I said, "But I don't need my shoes tied, I need help translating. Can your machine do that?"

He said, "Of course! It can interact instantaneously in 87 different scripts, including upside-down Urdu complete with all those funny squiggles and dots, whatever they are, I never claimed to be a linguist myself."

I said, "But I do this language, not Medieval Mongol, and my output is supposed to be all in English. I don't compose in all these other writing systems!"

He said, "No problem, we'll just ignore these other scripts, they only cost a few thousand dollars per machine anyway! Now what else do you need?"

~~FOR OFFICIAL USE ONLY~~

DOCID: 4033692

I said, "Well, how about a really sizeable dictionary and the capability to look up a term more quickly than I can by hand?"

He said, "Of course you know that will take all your memory. But we can do it! If you'll just fund the typists, we can probably get the dictionary entered in a couple of years! And the neat part is that you can program the dictionary yourself!"

I said, "Me, program? I'm a translator. I don't have time to learn to do all that."

He said, "Not to worry, it doesn't take all that long, I picked it up in just a few weeks myself. Just think, you'll be able to do all your own programming! Only thing is, the course is full and you can't get in until sometime late next year."

I said, "Why can't you do the programming for me?"

He said, "Who, me? I'm too busy for that! I already spend nearly full time as it is working the bugs out of the programs other people write, I don't need another job. You know these systems anyway, they're all overloaded."

I said, "Overloaded already? Then how can I add a program with dictionary, look-up capability, word processing, and all the rest?"

He said, "Well, you really can't for now. But just as soon as we get the Gizmo Super-X, you can do everything since it will stand alone."

I said, "You mean it won't have to talk to all these other systems? But what if I need to do just that?"

He said, "Well, it won't unless we develop a special package, but I'm sure that's already well in hand. Not to worry!"

I said, "So I have to wait for the Gizmo Super-X plus my programming class plus whatever interface package eventually gets developed, all before I can start work? With the budget situation the way it is these days? What do I do in the meantime?"

He said, "Well, if you only knew how to program, you could use your present system for, oh, just lots of things; of course, it's overloaded, so don't try to add too much, maybe just a few working aids or so. And by the way, the word-processing program on that system takes too much system space so we're going to take that out."

I said, "Thanks a lot!"

He said, "Have another pencil."

%

~~FOR OFFICIAL USE ONLY~~

DOCID: 4033692

This review is classified ~~CONFIDENTIAL CCO~~ in its entirety.

GCHQ: The Secret Wireless War 1900-1986
By Nigel West. 294 pp. Weidenfeld and Nicholson, London, 1986. [L12.95].

Reviewed by: Vera Filby, E41

This book on NSA's senior partner is a well-organized, well-researched history of British SIGINT beginning with its origins in telegraphy and wireless and carrying through in straightforward chronological order to events current at time of publication in 1986. It is no exposé or Bamford-style effusion, though the author has a reputation for such writing, but a balanced account of what happened, how it happened, and what it means, with abundant detail on organizational developments, complexities, and interrelationships, on codes, ciphers, and cryptomachines, on cryptologic places and events all over the world, and on people. Readers can enjoy the opportunity of learning more about some of the extraordinary people who over the years have made cryptology and SIGINT what they are.

This is also a book for entertainment, as any SIGINT history can be expected to be, since SIGINT in all its intricacy is endlessly interesting and a continuing source of great stories -- stories of achievement, of loss and failure, of discovery, stories of rivalry, international intrigue, war, and betrayal. What a goldmine historians have found to dig in since the ULTRA revelations in 1974! Some, like Nigel West, seem to have developed an understanding and appreciation of SIGINT's special nature. West is a military historian, and this is his seventh book on intelligence matters. Except for some private records of the Radio Security Service, his listed sources are public records and published works.

Until the beginning of the first World War, British authorities preferred to trust the security of their cable links throughout the Empire and were wary of wireless because of its vulnerability to intercept and its potential for spying. When war started, radio amateurs were banned, but eventually they were called upon to help. Future cryptologic organization was foreshadowed in a recommendation to make a list of those who would be willing to be trained in encryption, decryption, censorship, and interception. What was to become SIGINT started when wireless experimenters in the field in France came across German telephone conversations. That was the first surprise. The next was the clear evidence in those conversations that the Germans were intercepting the communications of senior Allied officers. War Office intelligence could hardly miss the significance of this, and soon the first military SIGINT unit was founded. Thereafter and throughout the war, SIGINT became an increasingly indispensable asset for the military forces.

The cryptologic history of the Great War is well documented and its outstanding events - most notably the still controverial battle of

DOCID: 4033692

Jutland and the celebrated Zimmermann telegram -- often recounted. West retells this history as an integral part of his total picture.

In an effort to reduce extensive service duplication a new body with the innocuous name Government Code and Cypher School was established on 1 November 1919. With wartime targets gone, GC&CS redirected its efforts to Soviet traffic, which was supplied by Army signals elements, and to Japanese, copied by Admiralty stations. In addition, civil and governmental communications provided a rich supply of Soviet diplomatic traffic, much of which was readable and highly valued for its abundant evidence of Comintern programs of subversion.

In 1920, top British Government officials chose to release decrypts of Soviet telegrams with all surrounding details to expose Soviet undercover activities. No reaction was apparent in Soviet traffic, but then the Government did it again. By the end of 1920 the Soviets were using couriers, and the traffic had disappeared. When it later resumed it was quickly broken and was read until May 1923, when once again the Government blew it, this time to challenge Soviet adherence to a Trade Agreement of 1921 and to support an ultimatum demanding that the Soviets cease financing subversion in Great Britain and the Empire. The price of this political decision was again temporary loss of the traffic. Finally, after yet another deliberate compromise in 1927, the Soviets introduced one time pad. These are the things that break SIGINTers' hearts.

In 1922 the Foreign Office took over administration of GC&CS because it was believed that the central problem for SIGINT would be diplomatic, and it was given jurisdiction over intercept, DF, TA, and CA in order to centralize control over these scattered functions. At that time the staff numbered 91. Led by a few brilliant survivors of Room 40, the organization achieved many successes but remained in a state of underfunded obscurity up to the very edge of war. Only in 1938 was a German section formed. But by the end of 1939, GC&CS had acquired the wartime covername of Government Communications Headquarters, and its staff had grown to 937. The wartime peak, in June 1944, was 6,812.

The Enigma machine enters the story when in 1926 the German Navy began using a version of it. The British Admiralty had bought two machines in 1928, and after years of consideration a Whitehall committee decided to have the Air Force supervise construction of a machine based on it. This became the TypeX, which provided secure telecommunications for Allied SIGINT throughout the war. Experts recognized that Enigma machines, in all their versions, were impenetrable if used correctly. But with thousands of German Enigmas in use, and under all kinds of conditions of stress and crisis, errors did occur, and these compromises did help the cryptanalysts break into systems. The fact that error can make systems vulnerable is well understood, and it is therefore rather surprising that the author makes so much of it. It is his view that this truth is the real ULTRA secret.

istorians seem to have been so intrigued with codes and ciphers and so involved in reevaluating battles, campaigns, and diplomatic maneuverings in the revealed context of intelligence that they have been less concerned with researching the fundamental role of intercept. At the time of his death, Ronald Lewin, author of *ULTRA Goes to War* and *The American MAGIC* , was compiling materials, now deposited in Churchill College, Cambridge, for a study of the British military intercept services, which have been coordinated by the Y Committee since 1928 and are referred to as the Y Service. *The Story of the Y Service* was the subtitle of Aileen Clayton's excellent history (and great adventure tale) of her wartime RAF service, *The Enemy is Listening*, published in 1980. West has now added to this record his account of the Radio Security Service.

True to the tradition started in World War I, wireless amateurs volunteered to help the war effort. Their help was sorely needed because

DOCID: 4033692

Foreign Office and Special Service facilities were ineffective or inoperative. The role of these Volunteer Interceptors when they were organized into the Radio Security Service in 1939 was to cover agent communications. By March 1940 they had completed their mission - the target had been eliminated. Meanwhile they had been copying great quantities of enemy signals from the Continent, developing techniques, and building data bases. Of their contribution, West says that "it was largely due to them that the cryptographers at Bletchley Park were able to continue their work."

A history of GCHQ necessarily includes a history of NSA, and West begins his treatment with the closure of the Black Chamber in 1929 and continues it as part of a combined story up to the present. Negotiations between Britain and the United States began in 1940, and the next year a replica of the PURPLE machine, which produced decrypts, designated MAGIC, of Japanese diplomatic messages, was sent to GCHQ headquarters at Bletchley Park (also known as BP, Station X, and to the Navy, HMS Pembroke). PURPLE had by then survived an appalling leak, when American authorities disclosed to the Soviet ambassador information in a MAGIC decrypt concerning Hitler's intention to invade Russia.

But those who, as it turned out, could have profited most from MAGIC did not have access to it. In his brief summation of Pearl Harbor, West notes that the commanders were out of the loop and that the low level tactical traffic that would have warned them was processed, after delay, in Washington, where the strained resources were committed to traffic of presumed higher value.

UK and US SIGINT collaboration was formalized in the BRUSA Agreement of 17 May 1943. This and later agreements with Australia and Canada established the basis of the structure that exists today. So productive was the collaboration that by the end of the war the SIGINT effort was flooding intelligence channels with torrents of information.

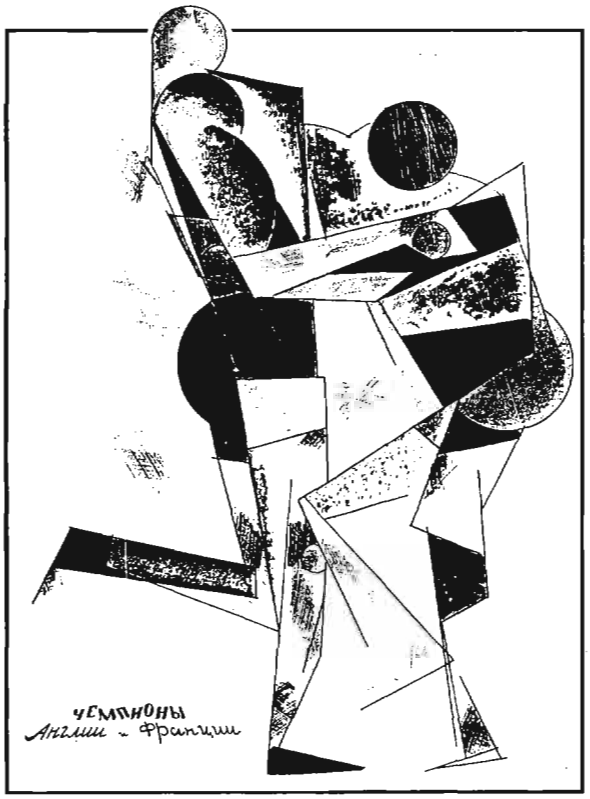
clever author likes to surprise his readers every now and then, and West does so by switching suddenly from the SIGINT scene at the end of the war to Australia. In 1944 a station there -- of all places -- picked up Soviet traffic in a system codenamed VENONA. This event, West believes, helped set the stage for a peacetime mission in exploitation of Soviet clandestine traffic. This traffic revealed continued Soviet involvement in and support of international subversion -- the story of the 1920s, unchanged. Exploitation of VENONA led eventually to the identification of the spy, atomic scientist Klaus Fuchs, the traitor Donald Maclean, and other spies and traitors in the ramifications that continued for years.

The last two chapters of the book, covering the postwar period, portray a scene of continual disasters, from the shooting down of the EC-130 over Armenia to Prime and the Pelton case. This is not really surprising, since only the things that go horribly wrong get out to become meat and drink for historians and investigative reporters. But such a recitation of losses, leaks, compromises, defections, and multiyear penetrations leaves a SIGINT reader feeling like a farmer who has seen his entire community's long-nurtured crops wiped out by insects and disease. The author manages to wind up, however, on a positive, if cautionary, note: "The secret wireless war will continue for as long as there are communications to be intercepted and signals to be interpreted. Accordingly, GCHQ will remain an invaluable source ... and a tempting target."

This book has been faulted for lack of proper, scholarly footnoting and original research. Be that as it may, for readers who want only a consolidated, readable survey of the publicly available record it will do the job. □

DOCID: 4033692

TECHNICAL LITERATURE REPORT



ABSTRACTS ON

SOVIET PACKET NETWORKS (U)

P.L. 86-36

Reported by: [redacted] *P13*

The June 1984 issue of *Inspec Key Abstracts on Communication Technology* contains translated abstracts of papers presented at the 3rd All Union Conference on Computer Networks for Packet Commutation (Вычислительные Сети Коммутации Пакетов, Тезисы Докладов Третьей Всесоюзной Конференции) in Riga, Latvia, in September 1983. The Russian proceedings were published in two volumes with abstracts in each volume. One foreign network, the Spanish IBERPAC, was described in the translated abstracts reported here.

One of the papers notes problems in implementing X.25 that result from the lack of a standard formal description of X.25 (and X.21). In Bratislava an experimental computer network IPK is being developed using the ISO architecture. The SIMULA 67 language was used to investigate the 4th layers of the protocol. A 'problem oriented' network 4 SET is a distributed computer system based on the IZOT 1016 small computers and the SM-4 mini computers. The SM-4's are connected to one another by data transfer channels, and form a network which operates across large distances. A term 'teletreatment of data' is introduced in connection with a description of the experimental packet switching network SET 1.2. The possibility of using optical fiber links for high speed transmission to perform 'distributed data treatment' is investigated in one paper.

Six papers deal with LANs. Foreign LANs such as ETHERNET, IEEE Project 802, ECMA, Sinpads and Hypernet are investigated to determine the control functions and access functions. No specific Soviet LAN is mentioned.

An interesting feature of the conference is the variety of different LAN and packet net schemes presented. There does not appear to be a single national system, and some of the regional systems link into the AKADEMSET net. This shows local variety that seems surprising in the centralized Soviet system.

The Soviet Academy of Sciences uses an AKADEMSET packet switched network for internal and foreign information-computing resources. The Ministry of Communications, and parties with data bases and applied software can also use the AKADEMSET network. Elektronika 100-25 minicomputers are interfaced by hardware adapters to the BESM-6 computers, and the whole structure used as an interface machine for accessing the AKADEMSET network. The SM-4 (TISA-4) has also been proposed as an interface with the packet network AKADEMSET. X.25 packet transmission protocol is used to connect the ES-7920 computers to the packet switching center in an open network.

There is apparently more than one packet net development, and several different services. A subsystem EKRAN of the DNEPR computer network is used for electronic mail. A network of the TsSu SSR provides user services which include: transfer of single- and multiple-address information; virtual communications between two points; data collection by computer

~~FOR OFFICIAL USE ONLY~~

DOCID: 4033692

from user terminals; dialog communications between networks users; and operator-user communications. The MSSR Academy of Sciences has developed a distributed computer network for quick access by a large number of users to an automated data base of scientific information. A multifunctional terminal system of a scientific center uses a central SM-4 minicomputers and peripheral Electronika-60 microcomputers, connected through the recommended X.25 protocol. This provides software exchange, collective use of external system hardware and simultaneous remote interaction among several users.based on variable packet lengths less than 1K, and data transfer speeds between 50 kbytes/s and 1 Mbyte/s.

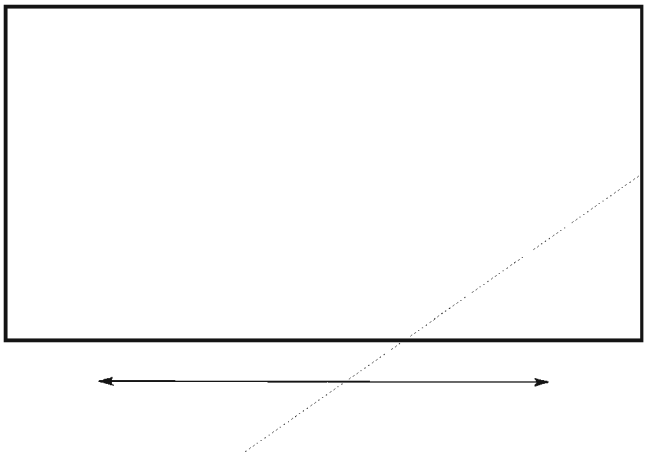
A Terminal VTsKP network for regional control of internal affairs combined different computers into a single distributed terminal network, using hardware developed along the CAMAC standard. A regional computer subsystem 'Ural' is intended to give users a wide range of services, including remote access to the subsystem informational-computational abilities, as well as access to the AKADEMSET network. The DNEPR network has a communication network that will accommodate 255 ports, receive or send messages up to 27 Kbytes, and remotely open or close ports.

A synchronous communication controller was developed to do bit-by-bit signal treatment using HDLC (high-level data link control), SDLC (Synchronous Data Link Control), and "K.25/2" (probably a typo for X.25/2) type protocols . The interface is intended for a microcomputer and connects with the main bus from one side and with either a synchronous or an asynchronous modem. The use of a subsidiary processor to free a main computer from queues of data will prevent inefficient data treatment even though it makes the net more complicated. One paper proposes the use of a TISA-4 computer to provide interface for a complex of SM-4 and BESM-6 computers with the AKADEMSET network via the network access method in TISA-4. Another proposal would use specialized hardware to perform the lower levels of the packet switching protocols to free the computers for more problem solving. A "cylindrical magnetic domain memory" (perhaps some kind of drum or disk) system of 100 Kbytes is proposed to give a reliable storage for storage of systems software and initial loading of separate microprocessors in the network.

X-25 is the standard packet mode transmission in more than 50 packet switched data networks that are operating in other countries. It is a CCITT recommendation for a packet protocol which makes a universal interface feasible between data terminal equipment and public packet switched networks. It is defined on three levels, viz: physical, link and packet level. The digital communications are defined by CCITT Recommendations X.20 and X.21 for stop-start and synchronous communications, and most existing packet nets support data rates of 2.4, 4.8 and 9.6 kb/s. Some also offer 48 or 56 kbps. The Soviets are currently using modems on some circuits which meet CCITT 4.8 kbps specifications. One of the Riga papers specifies a LAN.

Analysis

The US began its development of packet networks about eighteen years ago with ARPANET, which had heavy university and laboratory participation. Since then a number of packet nets have developed, many with scientific and resource-sharing aims. The Soviet AKADEMSET appears to be a development along similar lines. The technical features, as far as can be determined from the abstracts, are centered around micro and mini computers and medium-speed data modems. The work is probably about ten years behind US applications.



EO 1.4.(c)
P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4033692

Letter

P.L. 86-36

To the Editor:

(U) I chuckled to myself the other day as I read [redacted] introspections into the misty world of collection management. I think we all go through this period of doubt and reassessment occasionally - I know I have. Whether it is brought on by the myriad of reorganizations we have experienced; by endless criticism; or by mid-life crises, it is probably healthy to step back periodically to recount and reassure ourselves. (i.e., Now that you are a professional collection manager, what are you expected to do for a living?)

P.L. 86-36
EO 1.4.(c)

DOCID: 4033692

P.L. 86-36
EO 1.4.(c)

~~SECRET~~

[redacted]

(U) Just where does the real collection manager fit into this process? Right smack in the middle with both feet! Using his experience he must teach, cajole, reprimand, negotiate, and concede all in the course of a day. He is totally dependent upon analysts and collectors alike and must be guided by his NSRL. His responsibility is endless; his authority is elusive. The collection manager is the catalyst that makes it all work -- whoever he is.

(U) If [redacted] still has doubts about the necessity for collection managers, I suggest that the Collection Association consider instituting counseling sessions to coax [redacted] and any other temporarily wayward collection managers back into the mainstream of NSA thinking. Ours is a noble profession, no matter who does it.

[redacted] *P53*

P.L. 86-36

~~(S CCO)~~

OPPORTUNITY

- Are you a traffic analyst who despairs of finding a good TA job?
- Are you a risk-taker who likes independence and responsibility?
- Are you still searching for excellence?

If your answers are yes to the above, come talk to us. Regardless of grade, we may have just the job for you. [redacted] target is getting a lot of attention and will be receiving more.

We're searching for a few excellent men and women. If you think you are one of them, call [redacted] G221, on 963-3895s.

~~(S CCO)~~

EO 1.4.(c)
P.L. 86-36

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4033692

P.L. 86-36

BULLETIN BOARD

FOR CRAY USERS

~~(FOUO)~~ Cray Research, Inc., has a quarterly publication called *CRAY Channels* for users of its computer systems. If you are interested in obtaining a copy contact [redacted] CRYSCOM exec, A53/P13, 963-4196.

ATTENTION: LINGUISTS WITH IBM-PCs OR COMPATIBLES

(U) [redacted] is an on-line dictionary-building and look-up tool designed for the IBM pc or compatible running DOS 2.0 or above with two disc drives (floppy, fixed and/or cartridge.). It is memory-resident and requires 140K of RAM, in addition to whatever your word processor needs. According to the specifications, it works with Word Perfect, MultiMate, VoksWriter Delux, Word Wand, Palantir, WorldWriter, and other word processors. It also is said to work with pfs:Write and WordStar, but the latter two do not accept accented characters. Anyone interested in experimenting with this as yet untested software (it came as a free sample in the mail) is invited to call or write [redacted] P16, 963-1103s.

INSTITUTE ON MACHINE TRANSLATION

(U) Georgetown University, Division of Interpretation and Translation, will offer an Institute on Machine Translation from August 10 - 14, 1987. Persons who had participated in the 1985 Institute may register just for the sessions on new material, which will be given on 13 and 14 August. Fees are $200 for the five-day Institute, and $120 for the two-day sessions.

(U) Topics to be presented include basic issues of MT, recent developments in the field, and future trends.

(U) For further information and applications contact [redacted] P16, 963-1103.

ATTENTION ROCKET WATCHERS

~~(FOUO)~~ The History Division, in cooperation with W1, is undertaking a historical study of DEFSMAC and its predecessor organizations, SMAC and the A4 Watch. If you have records coyering those orgnizations, or have personal knowledge of significant organizational or substantive events, please call [redacted] or Henry Schorreck at 972-2355. You may also write them at T542, SAB 2 Door 3.

FOR SPANISH LINGUISTS

P.L. 86-36

~~(FOUO)~~ Still a favorite and available is the 1981 reprint of *SPANISH VOCABULARY, A Translator's Aid*, P1 Language Publications No.15 (S-220,300) 1979, compiled by [redacted] Copies can be obtained from [redacted] P16, HQ 8A187. Mail orders only are accepted.

CISI

SPRING CONFERENCE

Theme: INFORMATION SECURITY

18-22 MAY 1987

‡

GENERAL SESSIONS

Friedman Auditorium

Daily, 0900-1130 and 1300-1500

‡

CONCURRENT TECHNICAL SESSIONS

FANX II

National Cryptologic Course Center

Tuesday, Wednesday, Thursday

(Complete program with topics, speakers, and schedules will be published soon)

‡

For further information contact one of the Conference Co-Chairmen, [redacted] X2, 987-7446, or [redacted] P34, 963-6119

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4033692

THE STORY OF A PRIVATE GERMAN CIPHER OF WW I (u)

(Aug-Sep 1986)

[redacted] A204

P.L. 86-36

The postcards were found in a flea market in Stuttgart in 1979 or 1980 by Tom Brousseau while we were both assigned to Europe. Tom showed me the postcards, and though I found the cipher not difficult, the German script and language presented a problem, so we set them aside. In 1983 Tom lent me the cards for another attempt, and while I was at it [redacted] a co-worker in A2 and a good German linguist, strolled by, and soon read them. The only problem was interpreting a phrase in Martin's card to Anna, which we believe reads, "Today I finished preparing the flower vases."

Then when Frank was nominated to study at USARI in Garmisch, we thought it would be fun if he would go Stammbach, which we learned is about 20 miles north of Beyreuth, and check the local cemetery and the records at the town hall. But we really had no expectation of finding any trace of Anna or Martin, as 70 years had passed since the postcards were mailed.

When Frank got to Stammbach in 1986, he learned that Martin was born in 1884, and that Anna was born in 1884 and died in 1949. They had no children.

How Frank found the information and what happened as a result is a story in itself. To summarize briefly, he simply walked along the street where his pension was located, saw a grocery store owned by one Karl Wirth, and told a salesclerk that he was seeking information about Martin and Anna Wirth. One thing led to another, and he met a host of Martin and Anna's relatives, among them Martin's niece Anna, who told him that Martin had died in France in 1915. (The postcard shows him alive in January 1916. It is likely that Martin was killed during the battle of Verdun, which began with a German offensive on 21 February 1916, with heavy casualties on both sides.)

Frank had such a good time in Stammbach that he spend the next five days there, not speaking a word of English.

P.L. 86-36

The niece Anna, who now lives at the address of her Aunt Anna on the postcard, was perplexed about the postcards. How did they end up in a flea market in Stuttgart, she wondered. As do we.

But there's something else that puzzles us more. How was it possible that correspondence in cipher between a soldier and a civilian was permitted in time of war? Granted, it was a simple cipher, transparent to a professional. But what about the enigmatic message? The German linguists who looked over the decrypted text agree that the that cryptic passage is best translated, "Today I finished preparing the flower vases." But it seems an unlikely undertaking for a soldier, albeit a horn player, especially in January. Could it be a private message with the meaning, "I'm going to the front"? Perhaps some reader has the answer.

Among the difficulties we faced in translating the text–the cipher posed no problem–is that the postcards were written in pencil, and that the writing, in hard-to-read old-fashioned German script, is smudged. Furthermore, the spelling is non-standard; it is thought to reflect a local dialect. So other readings for the puzzling phrase cannot be ruled out.

THE CIPHER

1 2 3 4 5 6 7 8 9

A E I O U L M N R

~~FOR OFFICIAL USE ONLY~~

DOCID: 4033692

CARD FROM ANNA

LIEBER MARTIN!
BIN GESTERN GANZ GUT
NACH HAUSEGE KOMMEN
VON NEUEMARKT BIS HEIM
2.E KLASSE GEFAHREN BIN
HEUTE GANZ AUFGEREGT
LASSE RECHT BALD ETWAS
VON DIR HÖREN ODER
KOMME SELBST NOCH EINMAL
HEIM MIT HERZLICHEN
GRÜSSEN DEINE TREUE ANNA
HABE DEINE UHR SELBST MIT
ZUM UHRMACHER GEBRACHT

Dear Martin
I arrived home well yesterday.
I travelled second class from
Neuemarkt. Today I am
very excited. Let me
hear from you soon or
come home again. With
heartfelt greetings
Your true Anna
I brought your watch
to the watchmaker myself.

CARD FROM MARTIN

LIEBE ANNA
DEIN WERTES KARTCHEN
MIT FREUDE ERHALTEN
BEI UNS IST DAS WETTER
SEHR SCHON DIE BLU
MENVASEN HABE ICH HEUTE
FERTIG GEMACHT ES GRÜSST
DICH BESTENS DEIN LIEBER
MANN MARTIN

I was please to receive your dear little card.
We are having very beautiful weather.
Today I finished preparing the flower vases.
Best regards from your
loving husband Martin.

Solution to:

WHEEL OF FORTUNE

(Oct-Nov 1986)

1. WILLIAM FRIEDMAN
2. ARLINGTON HALL
3. CIPHER CLERK
4. DOUBLE TRANSPOSITION
5. BOOKBREAKERS FORUM
6. BURN BAG
7. CALLSIGN ROTA
8. ROTA SPAIN
9. DEPTH READING
10. CHELTENHAM
11. ONE-TIME PAD
12. BLETCHLEY PARK
13. SPREAD SPECTRUM
14. AIRPORT SQUARE
15. PLAYFAIR SQUARE
16. NORMAL DISTRIBUTION
17. FOR OFFICIAL USE ONLY
18. COMMUNICATIONS SECURITY
19. ZIMMERMAN TELEGRAM
20. HAGELIN MACHINE

Because of Technical Difficulties
We are Experiencing Delays
in Producing CRYPTOLOG

~~FOR OFFICIAL USE ONLY~~

DOCID: 4033692

NSA-CROSTIC (+) No. 63

P.L. 86-36

by [redacted] P12

Of all the puzzles that appear in CRYPTOLOG, the NSA-Crostic is by far the favorite. We're happy that in this issue we can satisfy the requests of many readers. This particular NSA-Crostic has an added wrinkle. Is it a clue or a bonus? That depends on when you hit upon it. It's a clue if you find it early enough, or a bonus if it becomes evident after the fact.

A. Insouciant
B. Normal personnel loss
C. Hybrid bramble
D. Mu's neighbor
E. Reddish bird dog (2 words)
F. A family ruler
G. Diligent
H. Innate
I. Syncopated?
J. Fortify
K. Essay
L. Supply fully
M. Patron
N. Crowning achievement
O. Casual
P. Plane figure; not a Greek conflict
Q. On edge
R. Apartment
S. —— del Vaticano
T. Seminary subject
U. Victim of Paris
V. Water nymphs; not dryads
W. A cryptanalytic phenomenon, such as TT; medieval garb
X. Amateurish

37	22	115	195	3	97	26	75			
112	61	48	66	85	77	21	106	187		
148	134	14	141	76	62	2	179	38	57	
185	120	74	153	36	13					
12	173	4	60	130	168	73	182	162	109	110
127	149	189	72	100	90	161	20	176		
180	47	183	131	11	88	16	158	147		
108	103	30	92	1	71	105	42	124	166	
128	64	50	52	29	137	70				
84	56	193	160	5	79	89	163	69	43	
118	138	143	63	99	121	94				
104	67	40	191	177	33	6	17	82		
86	133	49	25	126	184	68				
159	65	28	80	170	18	190	93	114		
169	117	181	171	44	194	102				
119	186	15	51	91	172	146				
58	125	150	7	35	136	154				
151	129	167	31	155	19	98	10	135	39	
34	53	174	175	78						
107	156	192	123	54	9	188	46			
24	178	122	83	95	165	32	142			
101	145	8	157	113	96	140				
152	116	59	87	45	139	81				
55	23	164	27	132	111	144	41			

~~FOR OFFICIAL USE ONLY~~

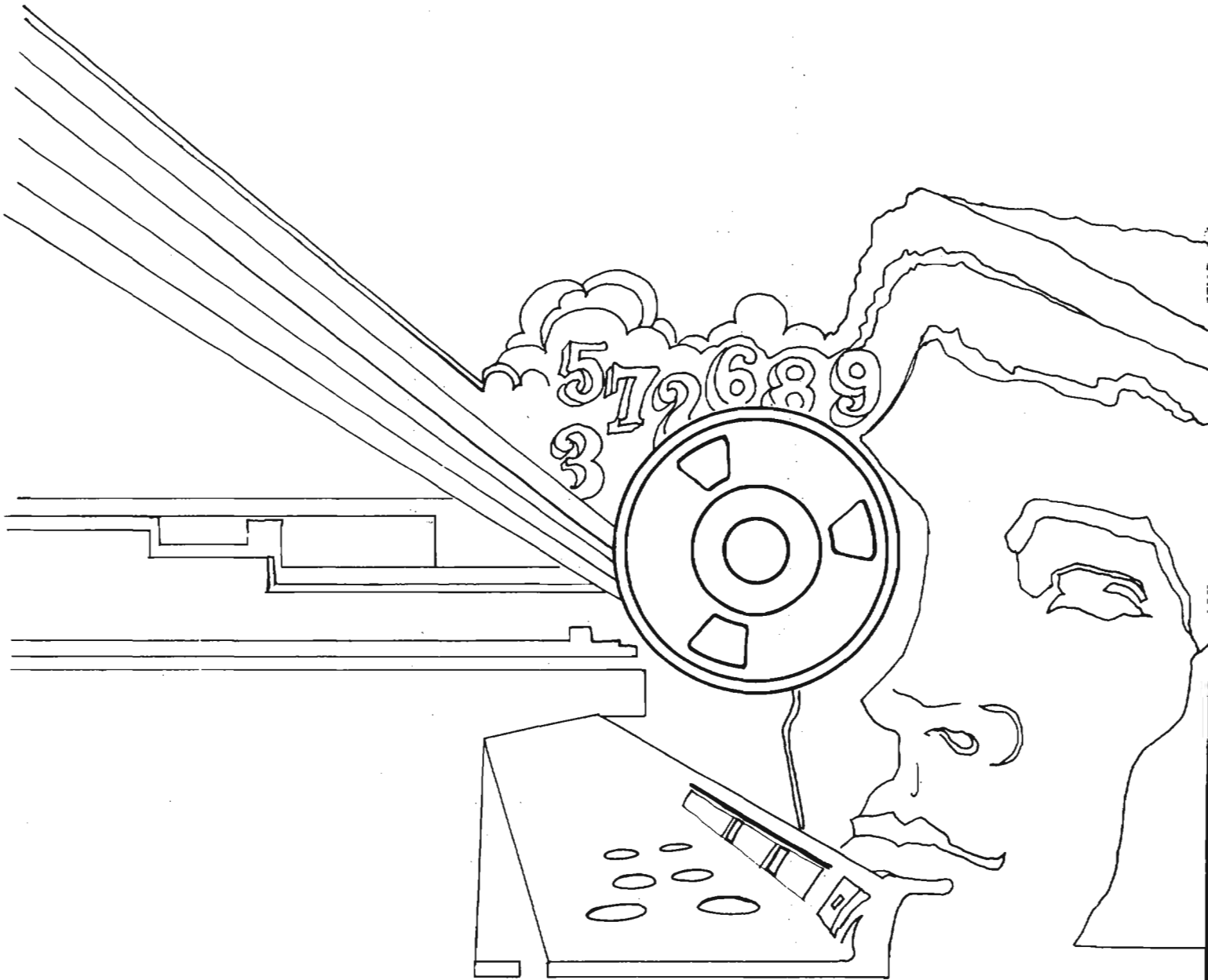
DOCID: 4033692

1 H	2 C	3 A	4 E	5 J	6 L	7 Q	8 V	9 T	10 R		11 G	12 E
13 D	14 C	15 P	16 G	17 L	18 N	19 R	20 F	21 B	22 A	23 X		24 U
25 M		26 A	27 X	28 N	29 I	30 H	31 R	32 U	33 L	34 S	35 Q	36 D
	37 A	38 C	39 R	40 L	41 X	42 H	43 J	44 O	45 W	46 T	47 G	48 B
	49 M	50 I		51 P	52 I	53 S	54 T	55 X	56 J	57 C		58 Q
59 W	60 E	61 B		62 C	63 K	64 I	65 N	66 B	67 L		68 M	69 J
70 I	71 H	72 F	73 E	74 O	75 A	76 C	77 B		78 S	79 J	80 N	
81 W	82 L	83 U	84 J		85 B	86 M		87 W	88 G	89 J		90 F
	91 P	92 H	93 N	94 K	95 U	96 V		97 A	98 R	99 K	100 F	101 V
102 O	103 H	104 L		105 H	106 B		107 T	108 H	109 E		110 E	111 X
112 B	113 V	114 N	115 A		116 W	117 O		118 K	119 P		120 D	121 K
122 U	123 T	124 H	125 Q	126 M	127 F		128 I	129 R		130 E	131 G	132 X
133 M	134 C	135 R	136 Q	137 I	138 K	139 W	140 V		141 C	142 U		143 K
144 X	145 V	146 P	147 G	148 C	149 F	150 Q	151 R	152 W		153 D	154 Q	
155 R	156 T	157 V	158 G	159 N	160 J	161 F		162 E	163 J	164 X		165 U
166 H	167 R		168 E	169 O		170 N	171 O	172 P	173 E	174 S		175 S
176 F	177 L		178 U	179 C	180 G	181 O	182 E		183 G	184 M		185 D
186 P	187 B	188 T		189 F	190 N		191 L	192 T	193 J	194 O	195 A	

Puzzle fans are invited to try their hand at compiling an NSA-Crostic, with or without additional features. For helpful hints and guidelines consult the Puzzle Editor.

~~FOR OFFICIAL USE ONLY~~

~~SECRET~~



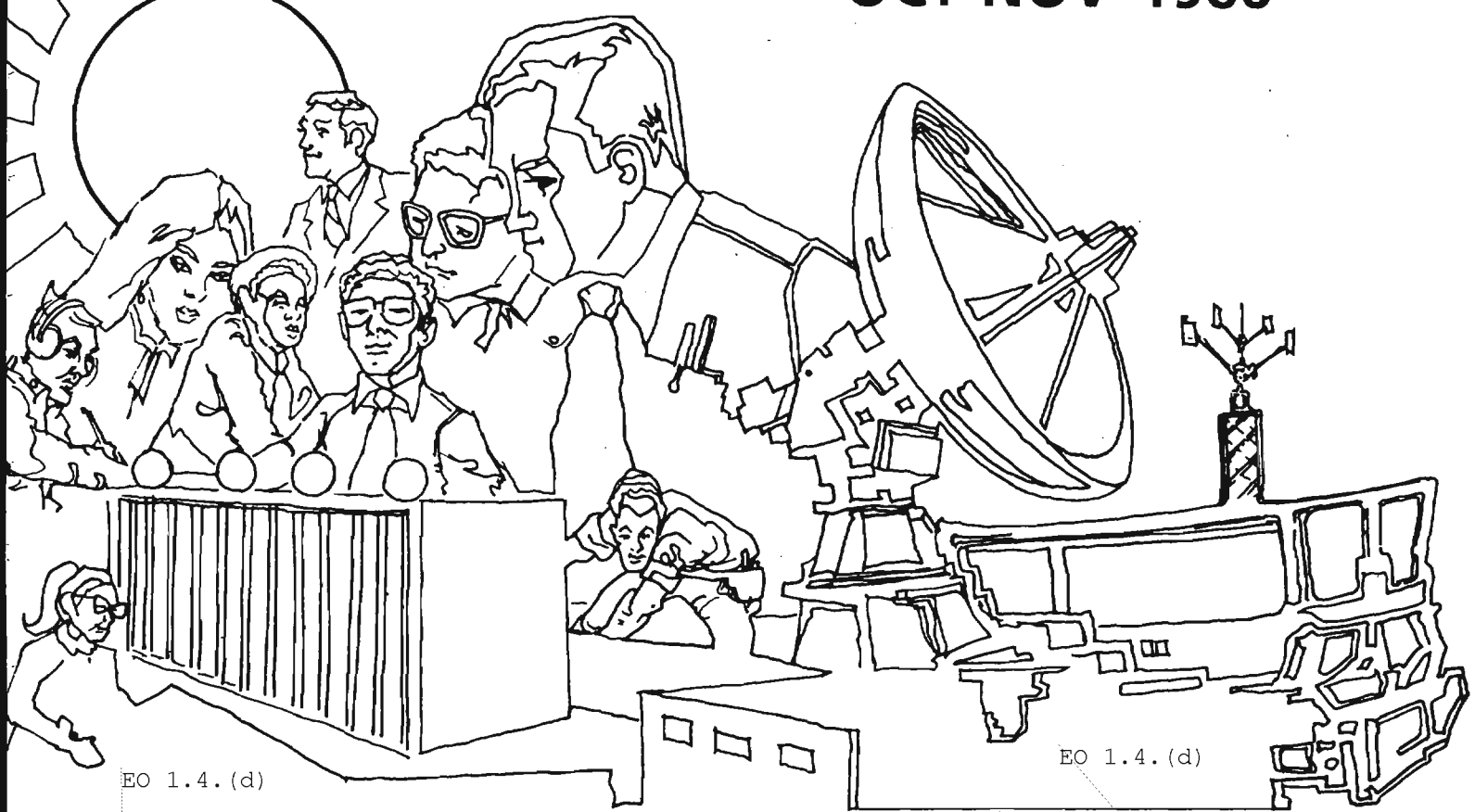
DOC ID: 4010004

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

OCT-NOV 1986



EO 1.4.(d)

EO 1.4.(d)

[redacted]	[redacted]	1
A NEW KIND OF JAPANESE (U)	[redacted]	9
SIREN No. 5 (U)	[redacted]	12
A SUMMER LANGUAGE COURSE (U)	[redacted]	13
ON THE LIGHTER SIDE (U)		15
THE REPRESENTATION OF PREFIXES		16
CONFERENCE REPORT (U)	N.C. Gerson	17
TECHNICAL LITERATURE REVIEW (U)	[redacted]	19
SOFTWARE REVIEW (U)	[redacted]	23
BULLETIN BOARD (U)		8, 14, 22
LETTERS (U)		27
FROM THE PAST		31
RESULTS OF READERS' SURVEY (U)		32
PUZZLE (U)		33

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~ ~~NOT RELEASABLE TO CONTRACTORS~~

~~TOP SECRET~~

P.L. 86-36

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

DOCID: 4010004
P.L. 86-36

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XIII, Nos. 10-11 ..... October-November 1986

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Collection ..... (963-5877)
Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Cryptolinguistics ..... (963-1596)
Index ..... (963-5292)
Information Science ..... (972-2268)
Information Security ..... George F. Jelen (859-1211b)
Intelligence Research ..... (963-3845)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (968-8075)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-5734)

Illustrators ..... (963-3057)
..... (963-6211)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptolg at bar1c05
(bar-one-c-zero-five)
(note: no 'o' in 'log')

Always include your full name, organization, and secure phone number.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1
Please do not phone.

Contents of CRYPTOLOG should not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

SHARE THE WEALTH! (U)

Even in the best of times, not everyone who could profit from it has been able to go to conferences. Partly it's because there's never that much money. But it's also because we can't shut down a whole operation for a conference -- someone has to mind the store.

Nowadays money is very tight. So people who are lucky enough to get to go to a conference ought to share the wealth, and write it up for CRYPTOLOG in addition to the customary trip report.

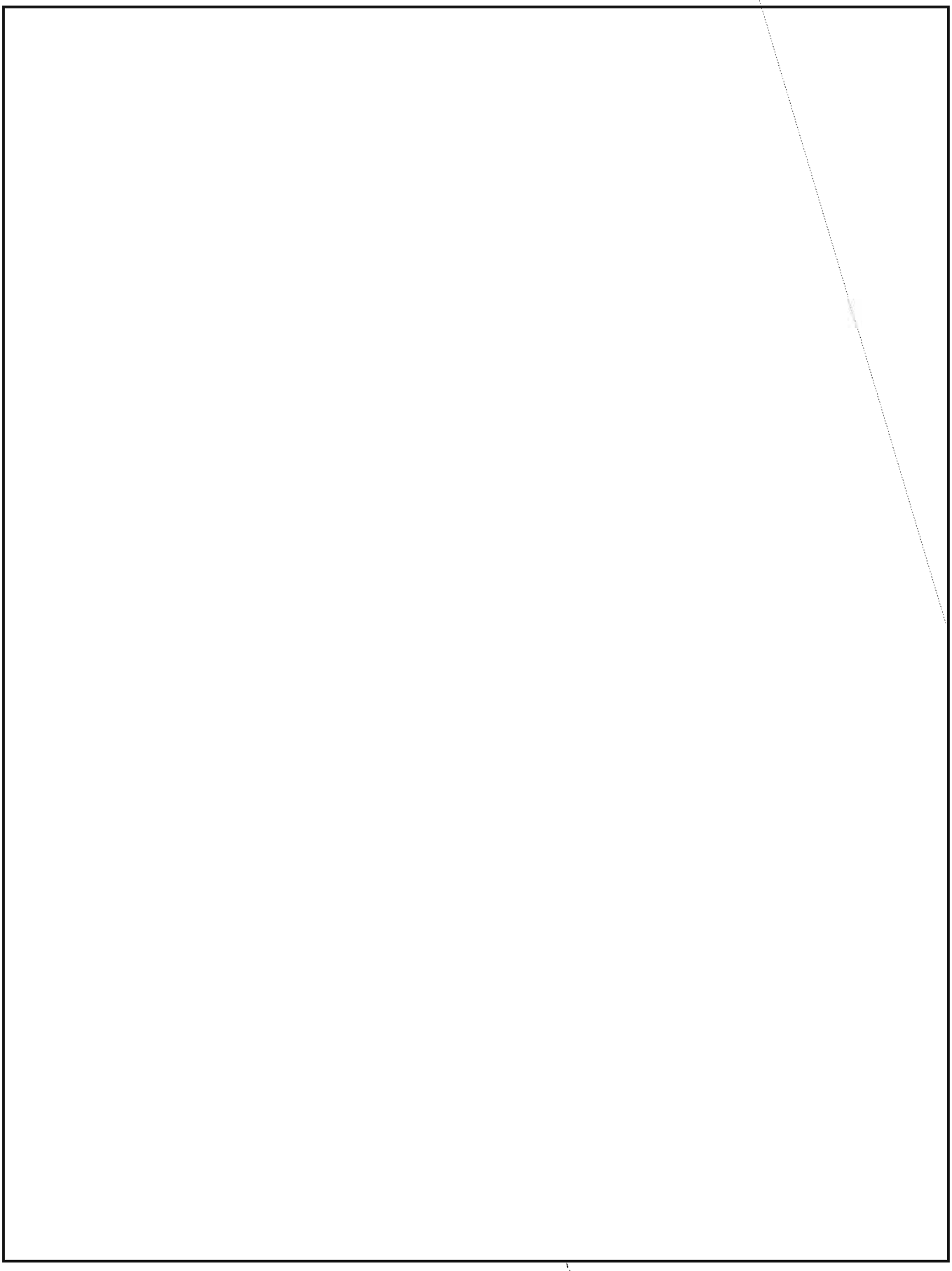
Why write it up again, when you can specify the distribution of each trip report and reach the right people? Because the probability is very great that there are people who should be informed that you don't know about. The Agency has gotten very large, and a good number of employees going to conferences haven't been around long enough to have a feel for who might be doing what. Also, our endeavors are becoming more complex and interdisciplinary, and the logical distribution may miss some key projects that are related. Only the fictional Mycroft Holmes could keep on top of things all by himself!

So, write it up for CRYPTOLOG, and increase the probability that your trip reports reach the people who would benefit. And the chances are that you'll get something out of it too -- making connections with people on similar projects or with like concerns.

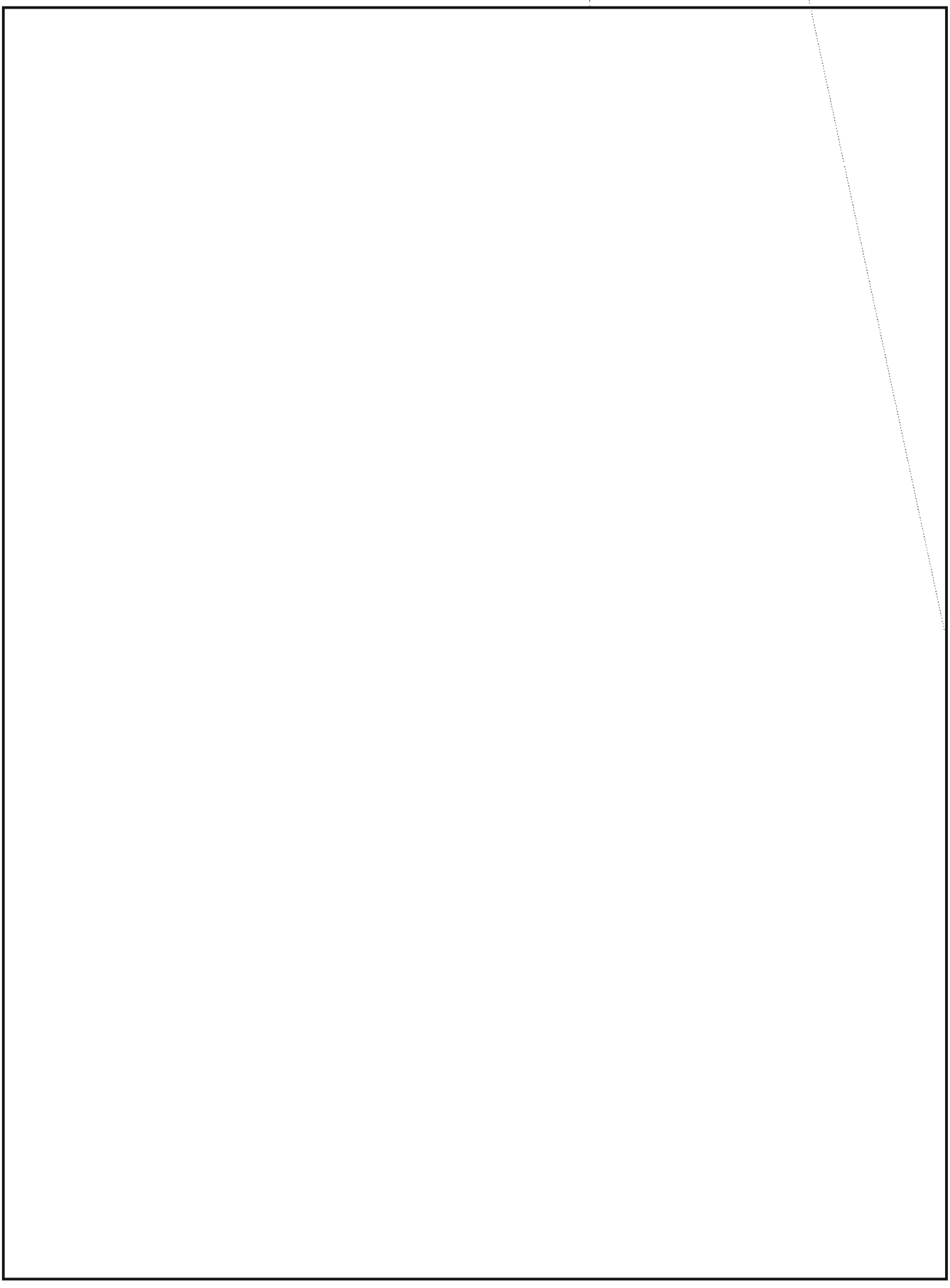
CORRECTIONS

- *The caveat NO CONTRACT should be placed on the covers of the Aug-Sep 1986 issue.*
- *The article titled "Collection Management" in the same issue should be classified CONFIDENTIAL rather than CONFIDENTIAL CCO.*

EO 1.4.(d)

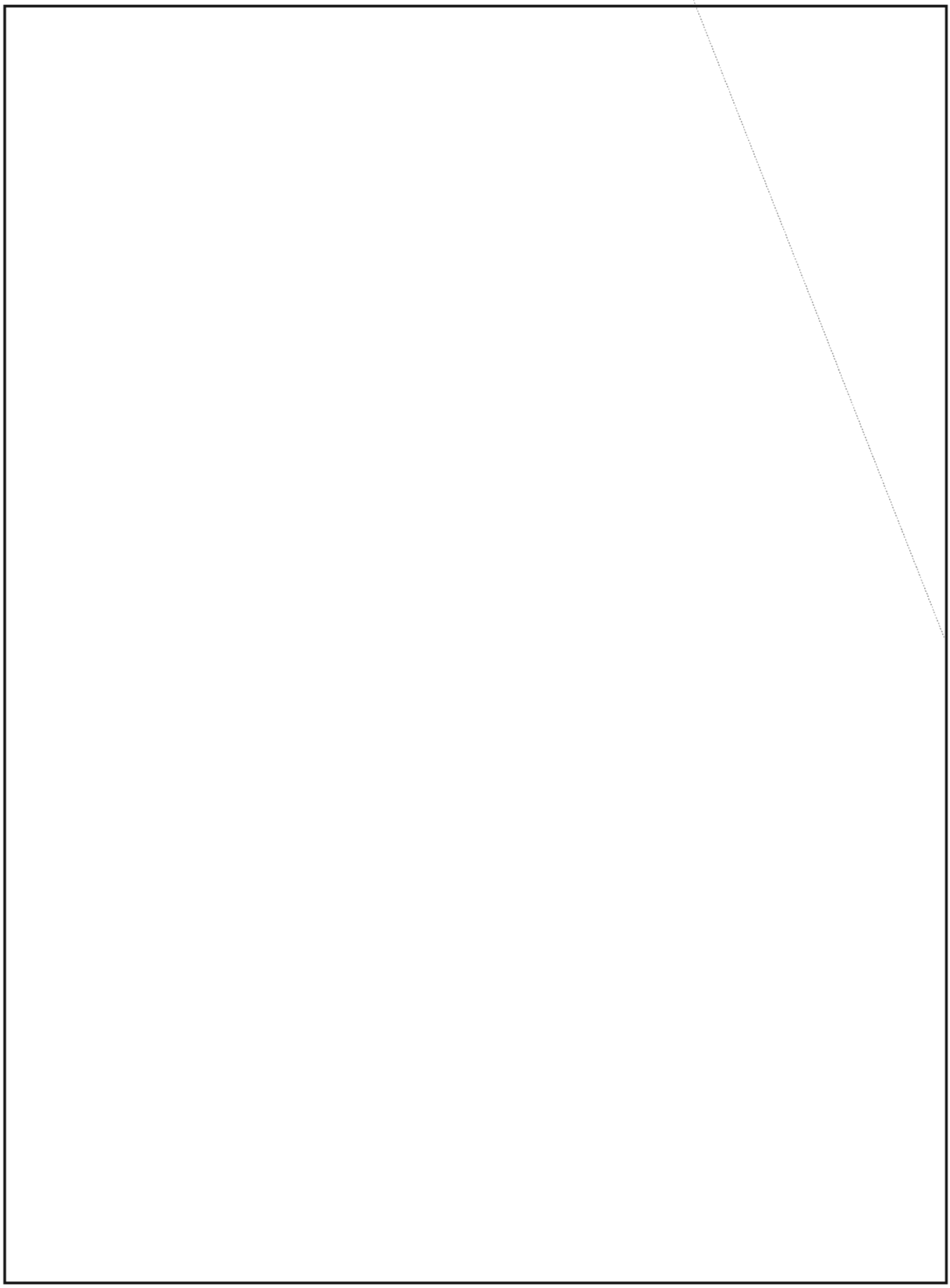


EO 1.4.(d)

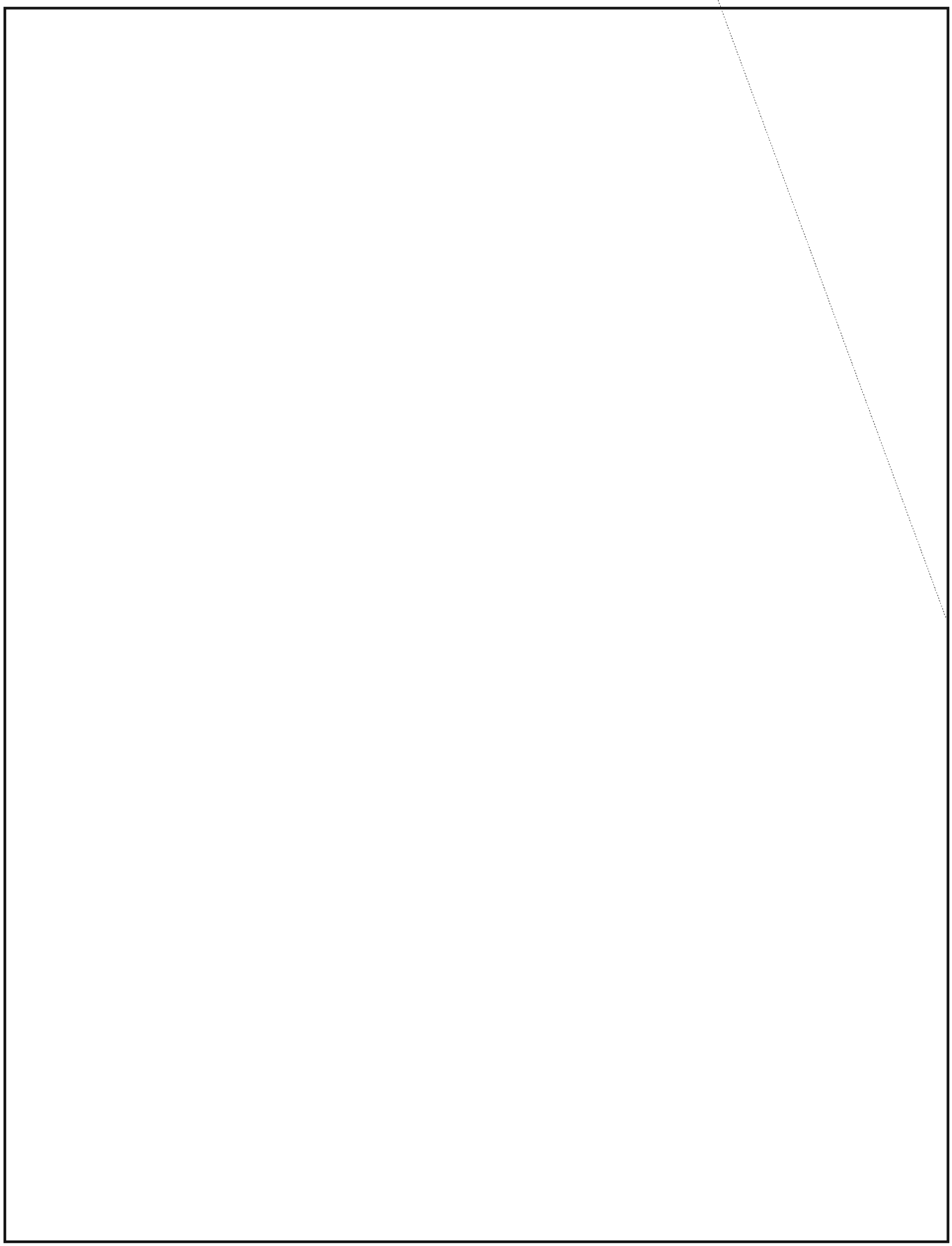


DOCID: 4010004

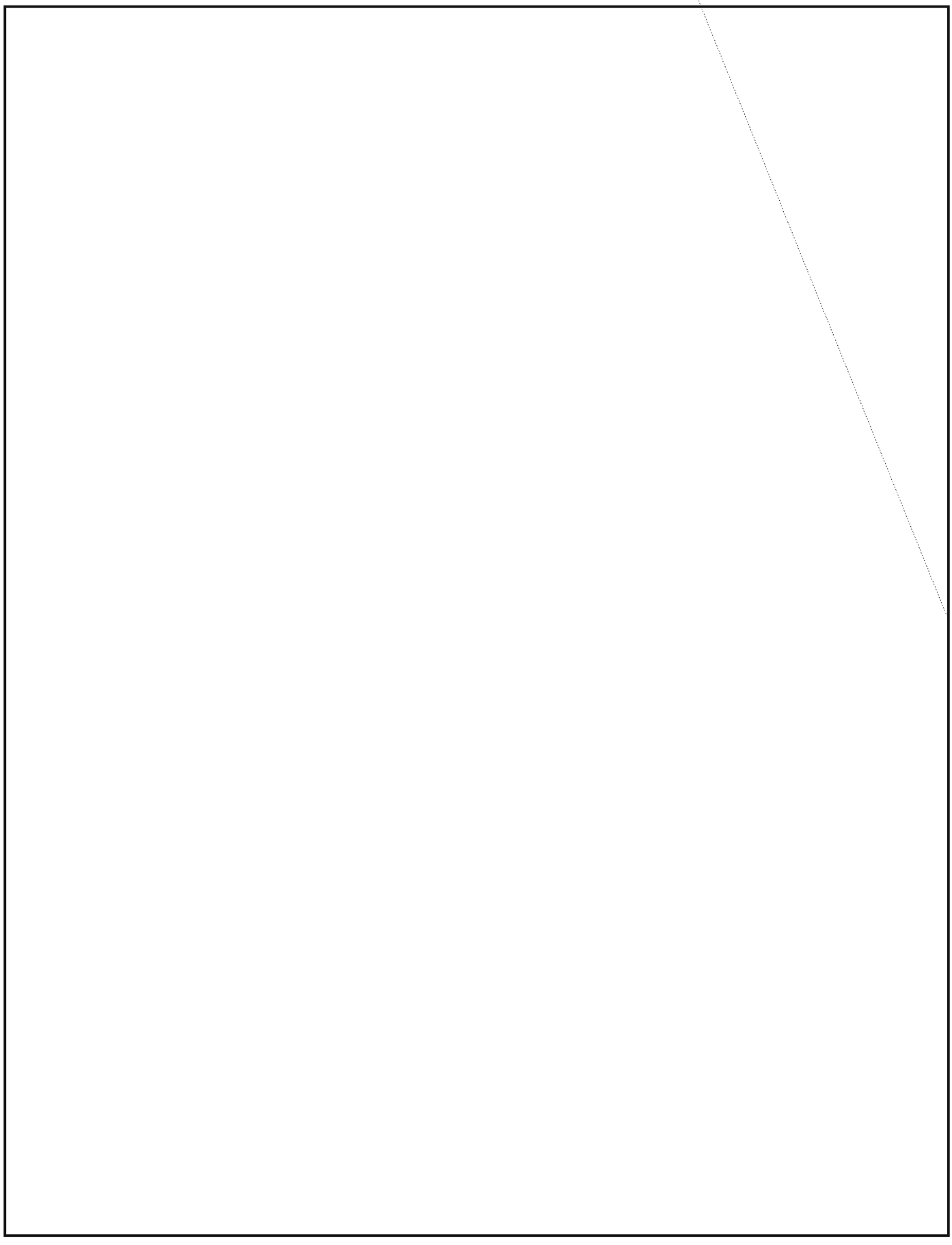
EO 1.4.(d)



EO 1.4.(d)

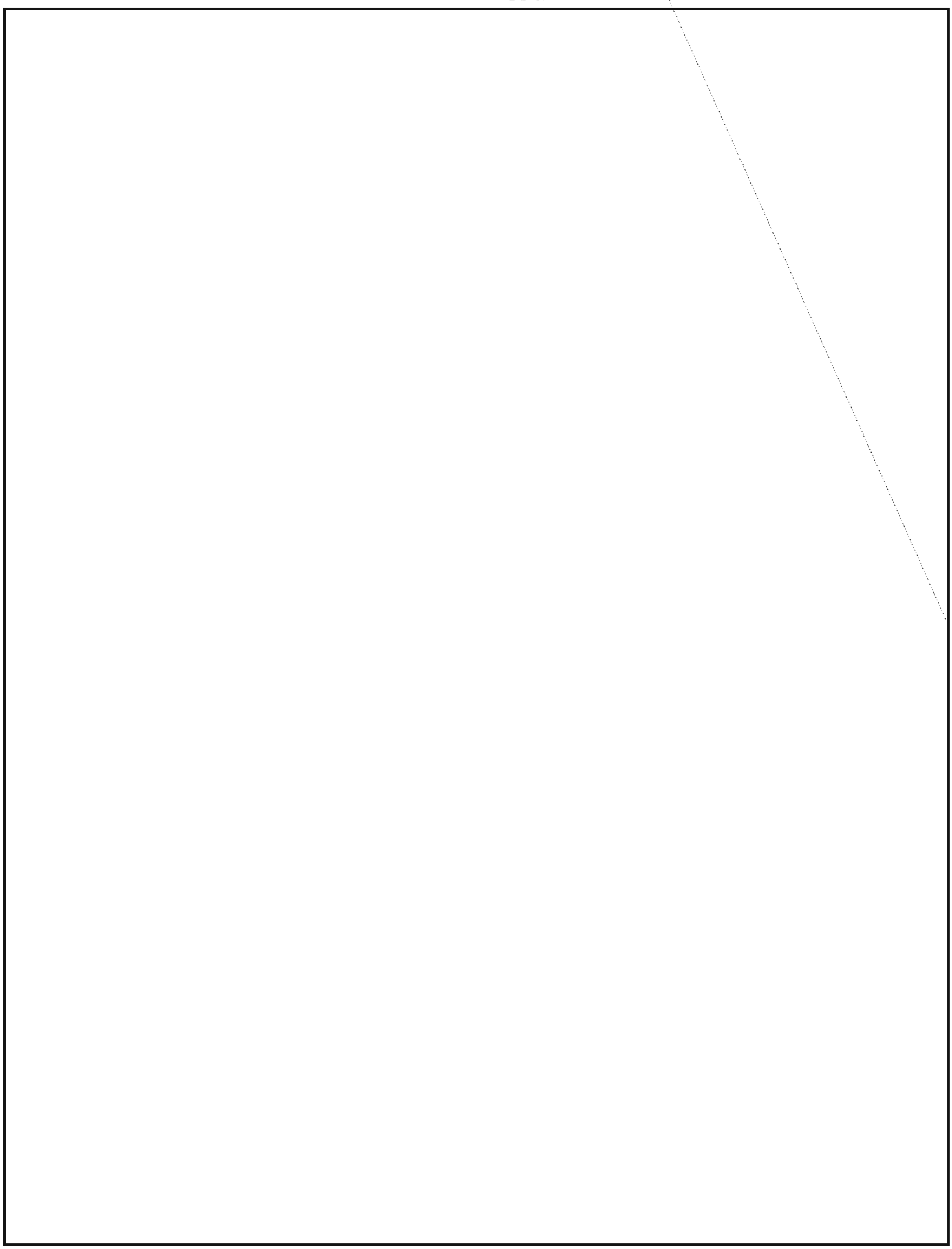


EO 1.4.(d)



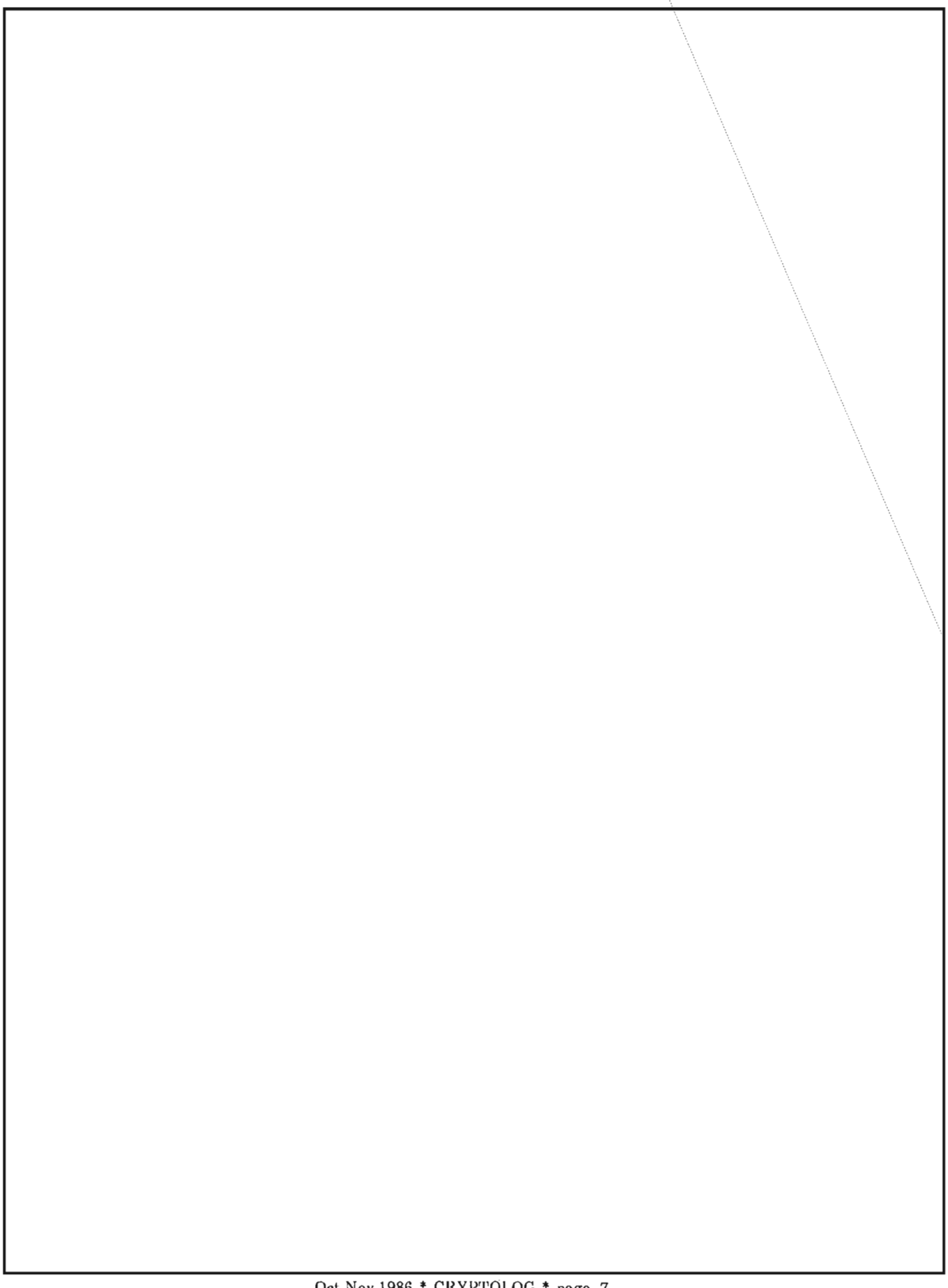
EO 1.4.(d)

DOCID: 4010004



EO 1.4.(d)

DOCID: 4010004



DOCID: 4010004

EO 1.4.(d)

BULLETIN BOARD

DATA CONVERSION (U)

~~(FOUO)~~ The Data Conversion Center, formerly known as JOBBER, can convert your hard copy to machine-readable form using an optical scanner or a keyboard. At the same location, the Magnetic Media Conversion Center can also, in most cases, convert data from one machine-readable form to another. For information about specific conversion pairs call [redacted] T1431, 963-4777.

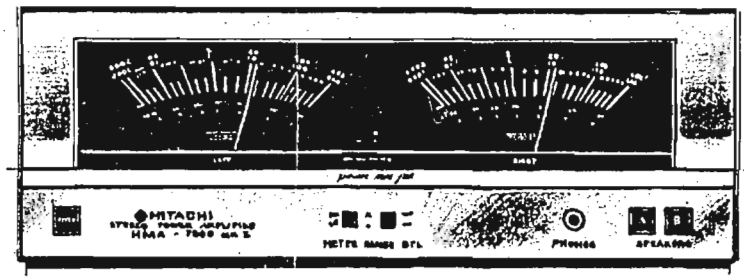
FORMATION OF HP3000 USERS' GROUP (U)

(U) In response to many requests an NSA Users' Group for the HP-3000 is being formed. Programmers as well as end users are invited to join. For information please call [redacted] [redacted] T2136, 968-8748.

P.L. 86-36

DOCID: 4010004

A NEW KIND OF JAPANESE (U)



P.L. 86-36

G72

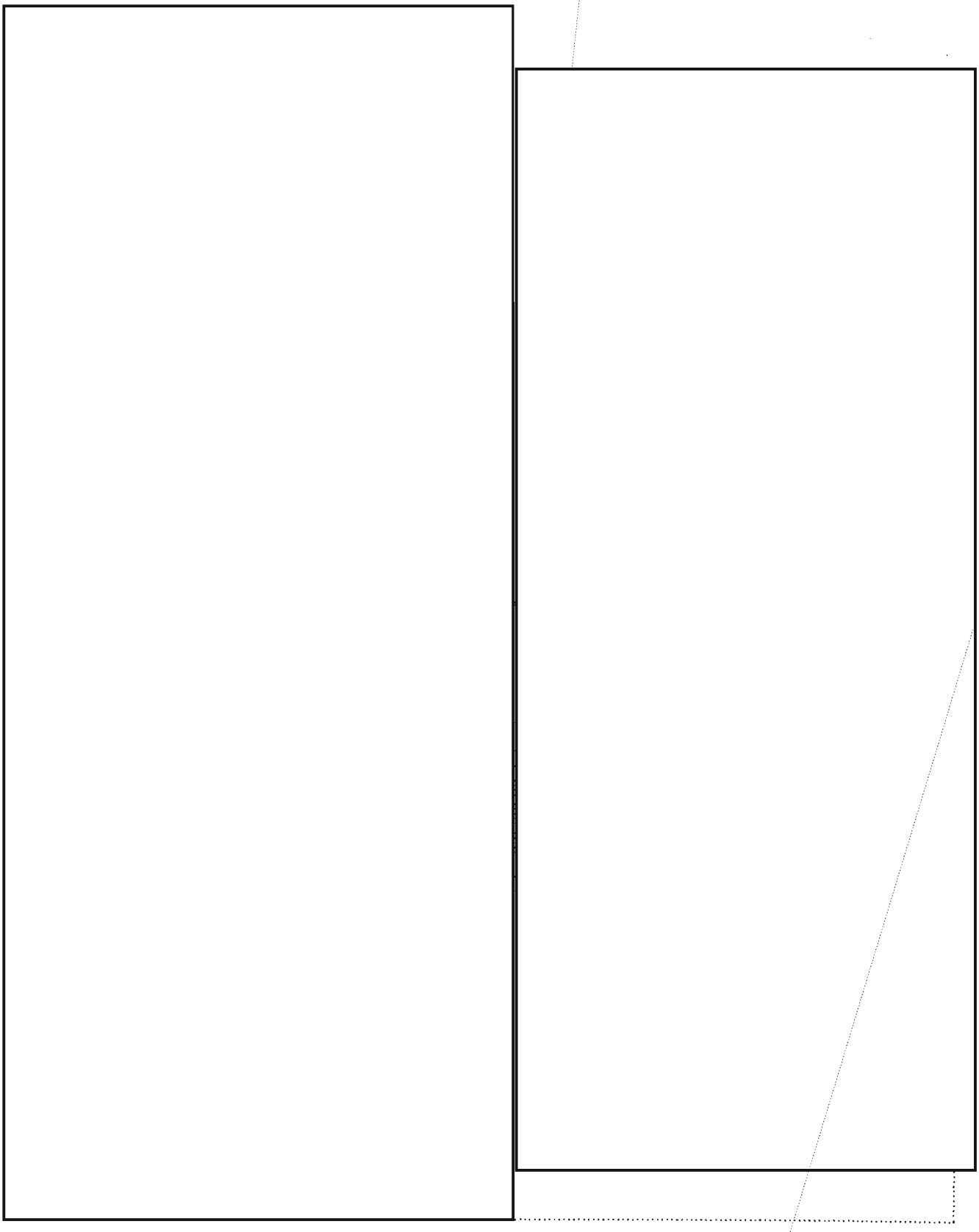
EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)

~~SECRET~~



P.L. 86-36
EO 1.4.(c)

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

A SUMMER LANGUAGE COURSE (U)

P.L. 86-36

(U) I have just returned from a great experience. I was at the Indiana University campus in Bloomington in an intensive Chinese language program. It was a fantastic two months.

~~(FOUO)~~ The opportunity came about rather suddenly in May while I was working as a clerical assistant in B61. I came to the agency as a Senior Clerical Assistant in 1985, but with a desire to get into a language program. It did not take long. In the second week of May a memo came into the office about an intensive East Asian Summer Language program being offered in Indiana. I knew this was exactly what I was looking for. I thought my chances were slim, but after talking to the chief and the deputy chief of my division, I decided to submit my name. After about two weeks I was told that there was a very good possibility that I would be able to go. During the last week of May I was informed that I was going to Indiana to begin an intensive Chinese language course on June 13.

(U) When I arrived at the university, I was overwhelmed by the size of the campus. It was beautiful. I went straight to the dorm to check in. All of the language students stayed in the same dorm, the women on one floor and the men on another. It was one of only two dorms on campus that was air-conditioned. This was nice in the middle of the summer. I was told there were television, movie, and exercise facilities available in the dorm. I do not know if this is true because after the first day there was no time for any of these things.

(U) I met the other girls who would be in my class that afternoon and we all became fast friends. At dinner that night I met the guys that would be in my class. There where 12 of us all together in the beginning class. All the Chinese students and teachers ate at special tables. The Japanese and Korean students also had there own tables. This was a great opportunity to talk to the teachers and practice Chinese as time went on.

(U) Classes started on Friday morning. We had four classes a day, each an hour long, with an hour between classes. That hour between classes was usually spent studying for the next hour's class. The two-hour lunch also was usually spent studying. The dorm cafeteria offered sack lunches so we did not have to waste time walking 20 minutes each way for lunch.

(U) At the end of the day we would all walk back to the dorm. It was a 20 minute walk along tree lined paths, over wooden bridges, and along a stream. This was an excellent way to relax after a day of classes. After dinner and about half an hour of relaxation and reading the newspaper, we resumed studying, about four hours a night. One of our native Chinese teachers had the room two doors down from mine. If anyone had a question, anytime, she was always eager to help. The teachers seemed to be truly interested in each student' sprogress. They were always around when someone had a question or a problem. They had office hours in the evening when the students could go and ask questions or just sit and talk. It was nice to be able to sit and use Chinese one-on-one with the teacher.

(U) All of our time was not spent studying, though. Every morning at 0630 there was Tai Qi (Chinese shadow boxing) for anyone who wanted to learn.

P.L. 86-36

There was also a Chinese drama class, calligraphy and drawing, and singing. There were Chinese movies (with English subtitles for beginners) on Friday nights. Occasionally there was a party after the movie where we could relax and dance after a hard week of study. Saturdays were usually spent doing all the things a person did not have time to do during the week. There were trips to the store to get away from campus for a while, laundry, cleaning, and studying. There were volleyball games between the different classes. Sundays were usually spent studying all day. Every second or third Sunday the teachers tried and do something special. Since there was no dinner served at the dorm on Sunday, they cooked their own Chinese food and we would have a picnic, or just get together and talk. Then it was back to the dorm to study.

(U) I kept a diary while I was there. When I look at it now I see that just about every other word is "study." But for every "study" there is a "fun," and that is what I remember most. Although there was a lot of hard work, the teachers and students made it all fun.

~~(SC)~~ [redacted] But at this time I am unable to do much. I still have a few years of study before I become effective in my job. But I look forward to it because it is definitely much more interesting and more challenging than being a secretary. I think I am going to like this.

~~(FOUO)~~ I found out when I returned to work that sending a beginner to Indiana was an experiment on the Agency's part. I was the first person to go there to take a beginning course. I think the experiment was a success because there is talk of sending more students next summer. I hope this is true because it would be great to see more people have the experience I did. And I must admit that I hope it is true because I would like to go back next year and take a more advanced course. I think even if the Agency does not send me next summer, I will go on my own for a long vacation spent studying and having fun. □

EO 1.4.(c)
P.L. 86-36

BULLETIN BOARD

SLAVIC TERMINOLOGY (U)

~~(FOUO)~~ Now in distribution is the third printing of the ever-popular *Comparative Bulgarian, Russian, Polish, and Czech Terminology* (S-203,185, P1 Language Publications No. 1, January 1972) compiled by [redacted] The multilingual format provides a base for a comparative method of solving translation problems, [redacted] For a copy write to: [redacted] P16, HQ 8A187. Phone orders are not accepted.

P.L. 86-36

1987 LINGUISTIC INSTITUTE (U)

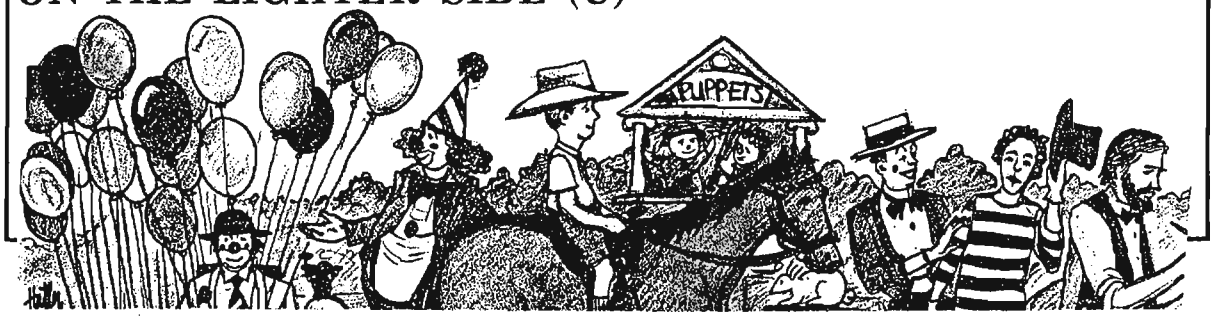
(U) The Linguistic Society of America, the Association for Computational Linguistics and the American Association for Artificial Intelligence are co-sponsoring the 1987 Linguistic Institute at Stanford University from June 29 to August 7, 1987. The theme is "Contextual and Computational Dimensions of Language." The Institute includes conferences and seminars of various lengths, from a few days to 6 weeks, with intensive courses in African languages, Arabic morphology, and linguistic and language processing courses on syntax, semantics, and phonetics. The aim of the conference is to integrate linguistic theory with artificial intelligence, psycholinguistics, discourse analysis and computational linguistics. For further information contact [redacted] P16, 963-1103. □

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4010004

ON THE LIGHTER SIDE (U)



A test paper making the rounds in the National Cryptologic School is rolling them in the aisles. Unlike most funny exams, the answers were right. You too might enjoy reading the unorthodox responses of [redacted] *an RU-15A student, to questions on Russian History.*

Question 1. Describe the reign of the following Russian Tsars. What did they do which was significant for Russia, and what events took place? P.L. 86-36

A. Ivan IV.

B. Peter I.

C. Alexander I.

D. Alexander II.

E. Nicholas II.

Answer:

A. Ivan IV (The Terrible). One hard-core tsar. He got the landowners, boyars, and the church to fork over some cash to help run the country. Created a 6,000-man political police force to help "persuade" his populace to follow the straight and narrow. Freaked out and killed his son during a tantrum.

B. Peter I (The Great). Tall dude who liked the West. Modernized the army and created a navy. He was a tsar who knew how to profit from Western technology. But no liberal was he. He did nothing that would weaken his absolute rule. Serfs remained chattel.

C. Alexander I. Napoleon came, saw, and barely escaped with his brandy intact. Alexander's troops beat him back to France and made Russia a European power to be reckoned with. Only head of state that showed up at the Congress of Vienna. But still your basic tsar on the homefront.

D. Alexander II. (The Tsar Liberator). Freed the serfs (technically) in 1861. Real liberal guy, he tried to push through a bunch of reforms but it wasn't fast enough and some hot-headed terrorists blew him to smithereens.

E. Nicholas II. The last tsar. This poor slob was hen=pecked by a warhorse of a wife. Wanted to be big and tough like his dad, but it was no go. Blundered into WW I. After a few uprisings he gave up some power, forming the Duma. But it was too little, too late. Overthrown in 1917, he and his family met an untimely end. (See "Anastasia" starring Ingrid Bergman.)

Question 2. Why was Lenin successful in the October Revolution when all other revolutions failed? What was the shortcoming of the Provisional Government?

Answer: The Germans secretly shipped Lenin into Russia to get the Russians off their backs. It worked. The provisional Government and Kerensky didn't pull Russia out of WW I (which was probably why the October Revoution took place in the first place). AWOL soldiers, workers, and your basic Joe Blowsky didn't take kindly to going back to the front and so Lenin moved in, and with the treaty of Brest-Litovsk got Russia out of the war.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010004

Question 3. What was the New Economic Policy and what was its effect on the Soviet Union?

Answer: In 1922, after the Civil War, the Soviet Union's economy was a shambles. So Lenin devised this new economic plan which was nothing less than a good strong dose of capitalism. It worked, and in 1927 everythingh was back to its pre-Civil War level.

Question 4. What steps were taken by Stalin to set the country back on the road to socialism? What problems were encountered? What effect did the purges of the 1930's have?

Answer: Stalin came in and ended the NEP, and put socialism back on its dreary path. Not too many people liked that. So he got rid of them. Exiled and/or killed millions. Decimated the officer corps, so that when WW II came arond his leadership cadre was wanting. Serves him right.

Question 5. What were the major events during Khrushchev's regime?

Answer: Let's see. There's the denunciation of Stalin that put the Soviets in a tizzy and really upset the Chinese. His "Virgin Lands" project to expand agriculturally into the vast regions of eastern Russia was a big flop. Gary Francis Powers took a nose dive in his U-2 and with that and so did relations with the U.S. And in 1962 he tried to sneak missiles to Fidel and blinked when Kennedy stared him down. Banged his shoe at the U.N. Visited Disney-land and was shocked by Shirley Maclaine on the set of Can-Can in Tinsel Town. □

REPRESENTATION OF PREFIXES (u)

Provided by [redacted] *P13D* P.L. 86-36

PREFIX	Factor byWhich Unit is Mutliplied	International Symbol (Common Use Symbol)	REPRESENTATION FORM I (Double Case)	FORM II (Single Case, Lower)	(Single Case, Upper)
exa	10^{18}	E	E	ex	EX
peta	10^{15}	P	P	pe	PE
tera	10^{12}	T	T	t	T
giga	10^{9}	G	G	g	G
mega	10^{6}	M	M	ma	MA
kilo	10^{3}	k	k	k	K
hecto	10^{2}	h	h	h	H
deka (deca)	10^{1}	da	da	da	DA
deci	10^{-1}	d	d	d	D
centi	10^{-2}	c	c	c	C
milli	10^{-3}	m	m	m	M
micro	10^{-6}	μ	μ	u	U
nano	10^{-9}	n	n	n	N
pico	10^{-12}	p	p	p	P
femto	10^{-15}	f	f	f	F
atto	10^{-18}	a	a	a	A

~~FOR OFFICIAL USE ONLY~~

CONFERENCE REPORT: TALC 1986

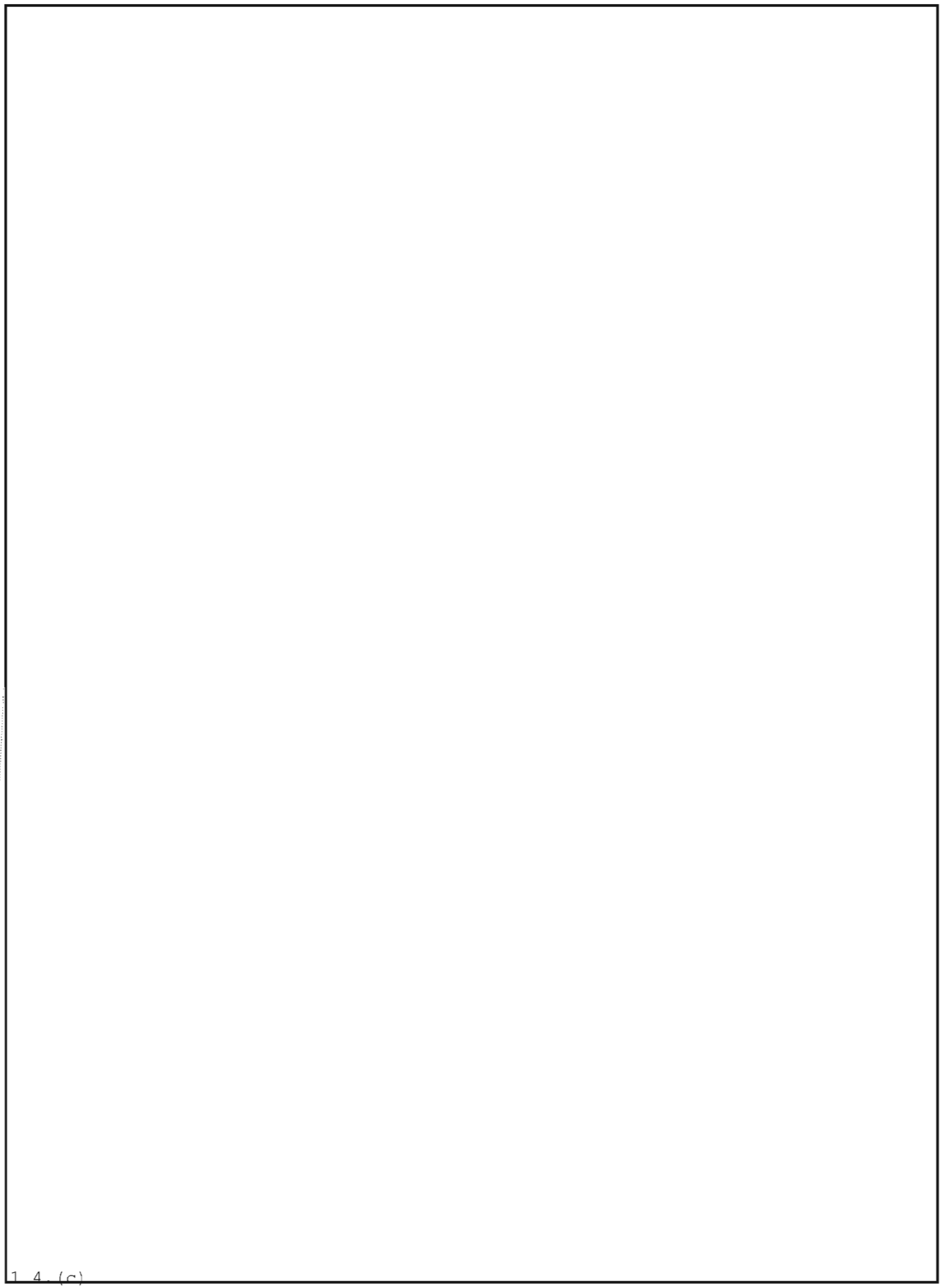
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

Target Aquisition *and* Location Conference 86 ~~(S-CCO)~~

N. C. Gerson, W3

~~*This article is classified SECRET HVCCO in its entirety.*~~

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

Technical Literature Review

"A Trigraphic Cipher with a Short Key for Hand Use" by Joseph R. Kruskal. *Cryptologia*, July 1985

P.L. 86-36 *Reviewed by* [redacted] *P12*

In this article the author presents a simple Playfair-like cipher which is, as he states, easily used for manual enciphering and is genuinely trigraphic.

I. THE SYSTEM

This segment of the review is unclassified

The author's scheme requires that the number of rows (m) and the number of columns (n), are both odd. As an example let us take m = n = 5, combining J with I, and construct a Playfair square with an appropriate keyword:

C	R	Y	P	T	00	01	02	03	04
O	L	G	A	B	10	11	12	13	14
D	E	F	H	I	20	21	22	23	24
K	M	N	Q	S	30	31	32	33	34
U	V	W	X	Z	40	41	42	43	44

The second square shows the row and column coordinates of the 25 alphabetic characters. Both the plain and cipher components are alphabetic; the coordinates will however be useful in calculations.

If the coordinates of an on-cut plaintext trigraph are (r_1, c_1), (r_2, c_2), (r_3, c_3), then the corresponding ciphertext trigraph has coordinates

$$(r_2 + r_3 - r_1, c_2 + c_3 - c_1),\ (r_1 + r_3 - r_2, c_1 + c_3 - c_2),$$
$$(r_1 + r_2 - r_3, c_1 + c_2 - c_3),$$

where the calculations of the components are carried out mod (m,n). To illustrate, if the plaintext trigraph REF is to be enciphered, we write R = (0,1), E = (2,1), F = (2,2) and calculate the ciphertext coordinates as

$$(2+2-0, 1+2-1), (0+2-2, 1+2-1), (0+2-2, 1+1-2)$$

which mod (5,5) is (4,2), (0,2), (0,0), resulting in the ciphertext trigraph WYC.

The deciphering procedure is only a little more complicated. If the ciphertext trigraph is

$$(R_1, C_1), (R_2, C_2), (R_3, C_3)$$

then the transformation, which is inverse to the enciphering transformation, produces the plaintext

$$(\tfrac{1}{2}(R_2 + R_3), \tfrac{1}{2}(C_2 + C_3)), (\tfrac{1}{2}(R_1 + R_3), \tfrac{1}{2}(C_1 + C_3)),$$
$$(\tfrac{1}{2}(R_1 + R_2), \tfrac{1}{2}(C_1 + C_2)),$$

as can readily be checked. For example

$$\tfrac{1}{2}(R_2 + R_3) = \tfrac{1}{2}((r_1 + r_3 - r_2) + (r_1 + r_2 - r_3)) = r_1$$

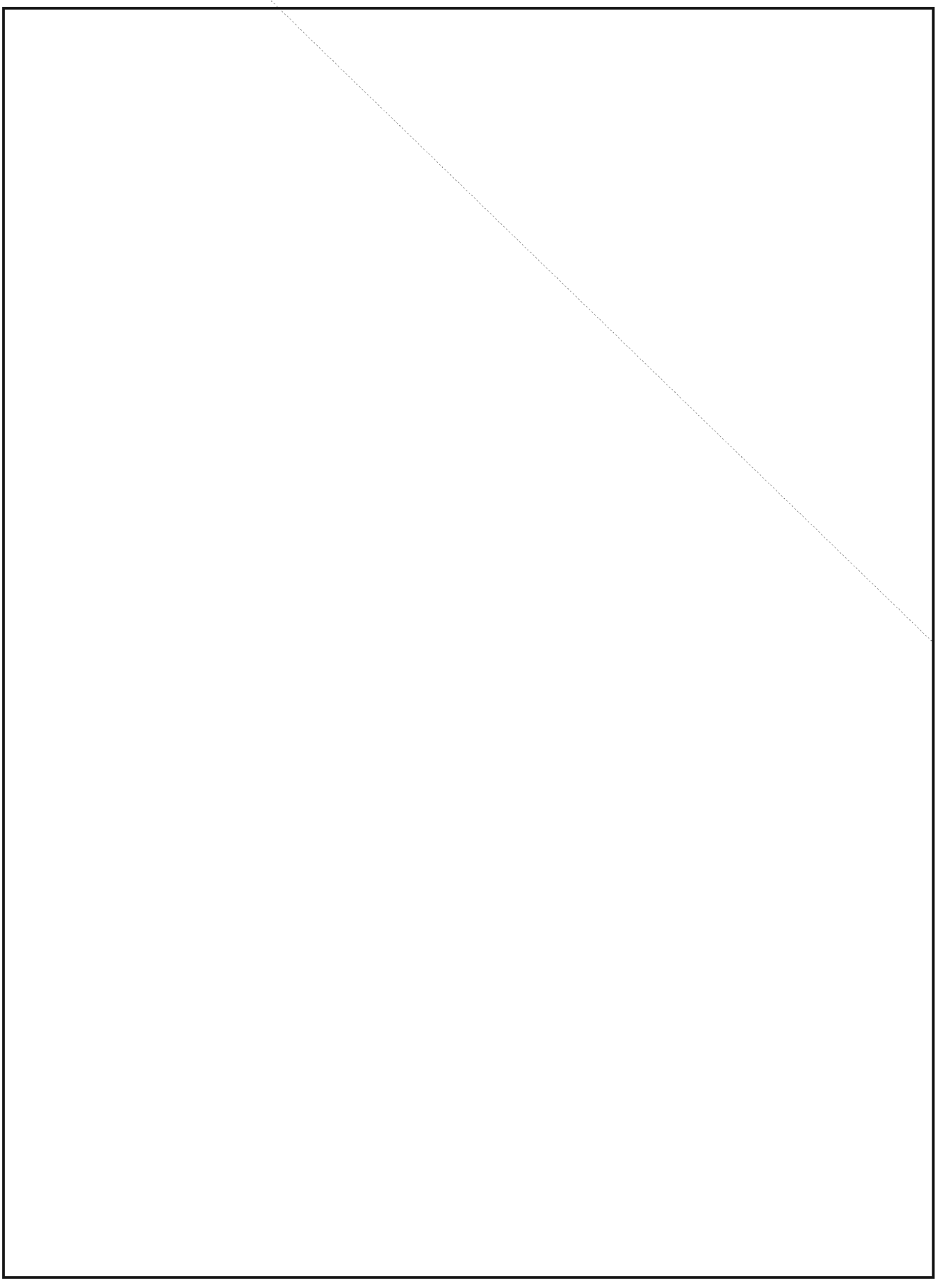
The form of the decryption operation shows why it is that we must insist that both m and n are odd. If m were even, then $\frac{1}{2}$ would have no meaning. But for m odd, $\frac{1}{2}$ makes perfectly good sense: $\frac{1}{2}$ is that number which when

EO 1.4.(c)
DOCID: 4010004 P.L. 86-36

multiplied by 2 yields 1 mod m. So for instance if m = 5, then $\frac{1}{2} = 3$, since $3 \cdot 2 = 6 = 1 \bmod 5$.

Kruskal remarks that if plain ABC corresponds to cipher XYZ, then we also have correspondences between the pairs BCA and YZX, CAB and ZXY, CBA and ZYX, BAC and YXZ, and ACB and XZY.

DOCID: 4010004 EO 1.4.(c) P.L. 86-36



EO 1.4.(c)
P.L. 86-36

BULLETIN BOARD

FORMATION OF XEROX USERS' GROUP (U)

(U) A Users' Group is being formed at NSA for users of the Star, Viewpoint, and XDE. Interested persons should call [redacted] Y44, 972-2345.

P.L. 86-36

FOREIGN LANGUAGE VIDEOS (U)

~~(FOUO)~~ Videotapes in Russian and German are shown every Thursday at lunchtime in a conference room. They feature news and documentaries. Russian tapes are shown 11:00-12:00, and German tapes, from Austria and East and West Germany, are shown 12:00-1300.

(U) Programs and meeting rooms are posted on the CLO Bulletin Board on the north wall by the escalators near the entrance to the cafeteria.

~~(FOUO)~~ For other information about the German videos call [redacted] P16, 963-1103, and about the Russian videos, [redacted] A2COG, 963-1180.

P.L. 86-36

TERMINOLOGIES (U)

~~(FOUO)~~ Several terminologies and glossaries in SIGINT and related specialties are being compiled by P13D. For a list of publications in the planning stage or already completed, call or write [redacted] P13D, 968-8161.

P.L. 86-36

DOCID: 4010004

SOFTWARE REVIEW: [redacted] P13

FOUR PC-BASED EXPERT SYSTEM SHELLS (U)

- ExSys
- Personal Consultant
- Guru
- Expert-Ease.

(U) Are any of the many "expert system" packages advertised really useful? Is even the best PC package suitable for building expert systems for NSA applications?

(U) In general, one might expect:

- cheap, easy to use products providing roughly the same set of features as in Mycin (an expert system research project of the 1970s) with the rule capacity limited by the PC's memory and disk storage;
- limited processing speed and either no extensibility or very limited extensibility
- a variety of user interfaces
- generally poor documentation.

(U) In the four packages tested I found:

- more features and a greater variety than I expected, though some of the "basic" Mycin features were not available in some packages,
- better user interfaces, but disappointingly, some aspects of the user interfaces seemed needlessly complex or difficult;
- generally more capacity than I had believed possible;
- documentation in some cases even worse than I had expected.

~~(FOUO)~~ Overall, I found that all the PC-based expert system shells have some potential for NSA applications. With the abundance of ASTWs in NSA and at its field sites, expert system shells have considerable potential for assisting both junior and senior analysts with complex analytical decisions. Greater potential exists in areas where personnel rotation creates a training problem and round-the-clock operations make it difficult for even an expert to keep track of the myriad of constantly changing detail. Field sites, NSOC, and DEFSMAC are excellent candidates for expert systems which assist with important time-sensitive decisions about analysis and reporting of observed phenomena, particularly when there are conflicting data from multiple sources.

(U) Following are specific comments on the individual packages.

ExSys ($300)

(U) ExSys is the easiest to use of the four expert system shells I tried, and it has some powerful features as well, though it does has some limitations.

(U) When you start to build an expert system with ExSys, the first activity is to define a rule. The rule constructor requires "qualifiers"

~~TOP SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36
DOCID: 4010004

and "choices" for the IF and THEN portions of the rule. While you are in the middle of making the rule, you go off to the side and build a qualifier, which is an enumeration data type whose name is the subject and verb of a sentence and whose values are possible objects for the sentence. When you have built a qualifier, you select one or more values for the rule you are building. ExSys automatically builds a rule that reads like English. Once a qualifier is built, it can be used in other rules; everything is integrated nicely. Before you know it, you have built an expert system.

(U) One particularly nice feature of ExSys is the optional ELSE part to a rule. This does not appear in any of the other three expert system shells reviewed.

(U) Some of ExSys's shortcomings:

- Qualifiers cannot have certainty factors; if you must deal with uncertainty, this may not be an acceptable system. Choices (the final output for ExSys) must have probabilities associated with them, and these probabilities will be averaged if multiple rules produce the same answer with uncertainty. That is as far as ExSys goes with uncertainty; no uncertainty is allowed in the IF portion of a rule.

- The manual is skimpy in some of its explanations. For example, the order of rule selection is according to the numerical order of choices. I found that out, not by reading the manual, but by rearranging the choices in alphabetical order and thereby messing up my system.

- The on-line explanation merely displays the current rule. This is not as useful as Personal Consultant's ability to display the entire chain of reasoning on-line.

[redacted]

[redacted]

Texas Instruments Personal Consultant ($950)

(U) Personal Consultant, a commercial implementation of the EMycin system, has several of its nice features:

- enumeration data types, very handy for user interaction. (The user can select from a list of values instead of typing them in, thereby avoiding mistyping);

- runs under Lisp; it is extensible in Lisp, and offers Lisp's advantages for processing symbols (e.g., text). This has a dark side, also: every 15-20 minutes, the Lisp system stops to do its garbage collection, a one-minute interruption on my PC;

- multiple rule contexts, to help organize the rules;

- comprehensive explanation capability, both during a session and after the session is concluded;

- an intuitive certainty factor system.

(U) Personal Consultant has some surprising problems: the documentation is badly organized and hard to use; a few features that I had not liked in the mini-Mycin package are unchanged in the TI package; and, worst of all, it requires a key disk in drive A, one of my pet peeves.

(U) Some other complaints about Personal Consultant:

EO 1.4.(c)
P.L. 86-36

DOCID: 4010004

- The rules are given names; then, when the rules are listed on the printer, the names are omitted and numbers are used.

- A user with no Lisp training will find some of Lisp's ideas confusing (for example, parentheses all over the place, and the ubiquitous garbage collection) Non-Lisp-oriented users would have trouble even with the installation.

(U) Mycin does offer a lot of power for building expert systems, and the Personal Consultant offers that power in a nice package, except for the copy protection.

P.L. 86-36

~~(TS-CCO)~~ Personal Consultant would be better than ExSys in an application with a complex knowledge structure. It also has graphics to display either input data or to explain its recommendations.

[redacted]

(U) A new version, called Personal Consultant Plus ($3,000), has graphics, metarules, frames, DOS program execution, the capability to insert a procedure to determine the value of a variable, and the capability to insert a procedure to be executed when a variable changes.

GURU ($3,000)

(U) The documentation of Guru is bulky. The four manuals -- a two-volume reference manual and two user's guides -- are intimidating. I found almost no use for the two user's guides.

(U) After running through the demonstrations, I tried to build a small (five-rule) expert system of my own. This took about ten hours. I had previously built the same five-rule system with ExSys in two hours and with Personal Consultant in 2 hours; and I later built an equivalent system with Expert-Ease in 2 hours.

(U) Some specific problems :

- Inadequate error handling: In ignorance I used display, a reserved word in Guru, both as a variable and as a rule name. The compiler did not tell me that I had used a reserved word. When I tried to run the erroneous expert system (Guru didn't stop me), the message "misplaced LOGIC" appeared on the screen. I knew something was wrong, but the error message gave me no clue whatever.

- Incomprehensible description of certainty factors in the manual. Although the claim is made that there are 16 ways to combine certainty factors, there are actually four very similar probabilistic ways that can be paired to make 16 combinations.

- Lack of enumeration type that would allow you to specify a limited set of string values for a variable (e.g., Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday). You should be able to access this through a menu function (missing in the current version of Guru) rather than having to write a subroutine.

(U) Guru is difficult to use but broad in its applicability. It would probably be good for a rule-based application for which access to a data base or spreadsheet or remote computer file is important.

~~(TS-CCO)~~ When the bugs are worked out, Guru may be useful for complex data base retrievals or for help with decisions based on information in a database.

[redacted]

P.L. 86-36

DOCID: 4010004
P.L. 86-36

EXPERT EASE ($495)

(U) Expert-Ease is a different kind of expert system shell. It builds rules using "examples" given by the user, a technique developed by Donald Michie in Scotland. This appears to be a very easy way to do it. It was surprisingly easy to set up the toy system I used to test all the packages.

(U) It was easy learn and to use, and it does allow linkage of multiple rule sets, and does deal with uncertainty in a limited way (three categories); but it has several major defects:

- it has no high-level language connection and it is not extensible.
- it provides no explanations of its reasoning chain.
- it has no reference manual. The manual is a tutorial, without an index.

(U) Expert-Ease runs under UCSD Pascal, and requires a Pascal partition to run it on a hard-disk system, causing problems for someone who wants to run it alongside DOS or Unix programs. The lack of extensibility and the lack of explanations make it inadequate for the kinds of things expert systems are noted for. It might be useful for someone who wants to experiment with building an expert system using examples instead of constructing rules.

SUMMARY

(U) Of the four systems reviewed, ExSys offers the most power for the money. It is superior to the others for ease of use, power, cost, and external program connections. But there are some applications in which it would fail miserably.

(U) My second choice would be Personal Consultant. For general power without respect to cost, for a Lisp connection, for good certainty factors, and for explanations, it is the best of the four. Personal Consultant Plus offers even more features (metarules, graphics, frames, external DOS programs), although at a higher price.

(U) Guru has a number of problems, but its concept is a good one. It is the only shell I know of that integrates a data base and spreadsheet with the expert system; it also has a natural language interface (not evaluated), graphics, and a communications interface. A new release will be available by the end of 1986.

(U) Expert-Ease is the only product to build an expert system from user-provided examples. Other than that, there is nothing to recommend it. □

REMINDER

If you want to be sure of receiving CRYPTOLOG after you move or are reorganized, send a change of address to Editor, CRYPTOLOG, P1, and include your name and both old and new organizations.

DOCID: 4010004

LETTERS

P.L. 86-36

To the Editor:

~~(FOUO)~~ [redacted] article on collection management (Aug-Sep 1986) is thought-provoking. I'd like to know if the situation as [redacted] has portrayed it is so. Has the NSA collection manager become a wart on the smooth skin of SIGINT operations? Do other collection managers feel as [redacted] does?

~~(S-CCO)~~ For the younger readers, a little expansion of [redacted] history may be in order. Before he arrived, elements of the Agency within Production (PROD) included General Studies (GENS), Asian Communist Studies (ACOM) [redacted] and All Other (ALLO). There was another element that was specifically concerned with the management of collection resources; Collection (COLL), although it was charged with other responsibilities as well. In fact, shortly after the element had been organized, it changed its name to Collection and Signals Analysis (COSA) to reflect more accurately the element's responsibilities. Even that name fell short. It omitted consideration of Non-Morse General Search (COSA-41), Morse General Search (COSA-42) and others.

~~(S-CCO)~~ That's enough of the gratuitous history lesson. Other readers with better memories than mine will almost certainly find some inaccuracies in the foregoing. The fact is that at that time things started happening to the way NSA was funded. The "good old days" ended about that time and the program elements and subelements began. Each part of the Agency was funded to perform specified functions; each had to justify its existence and its budget every year. Consequently, each insisted on exercising complete control of assets that were associated with the targets for which the subelement was funded. There suddenly was no longer a pool of intercept positions that belonged to the Agency and that could be assigned as required to perform functions that needed to be done. [redacted] That was when GENS became A, ACOM became B and so forth. And, that was when the collection managers who had managed the Agency's resources found themselves often in conflict with subelement managers who insisted on managing the resources they had to be responsible for. At this time, the role of the collection manager began to be eroded to the state described by [redacted]

~~(FOUO)~~ Please note that I am not disputing the events and facts described by [redacted] Those dates are true. I am just mentioning additional factors that were involved in the evolution of the role of the collection manager. There are probably other factors as well. The point that I am trying to make is that it is not a simple problem. Solutions, therefore, will not be simple, if they exist at all.

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4010004
P.L. 86-36
EO 1.4.(c)
P.L. 86-36

~~SECRET~~

~~(FOUO)~~ It would be useful to have responses to [redacted] queries from other collection managers

[redacted] *P041*

To a Mixed-Up Fireman on a Diesel Locomotive:

(U) Just thought I'd let you know that I spent part of my time here on this holiday [11 November] reading your article in CRYPTOLOG.

(U) I enjoyed it. I hope it brings the results you want.

P.L. 86-36 [redacted], *G05*

To the Editor:

~~(S-CCO)~~ I read with interest the article on collection management. Although the historical portion was somewhat informative the remainder was rather insensitive, misleading and a bit upsetting, at least to me. I would

[redacted]

LIkewise, I can't imagine a great deal of support for your recommendations coming from the Signals Collection Career Panel, collection professionals and aspirants, or the Collection Association. Some criticism, perhaps.

~~(S-CCO)~~ As collection managers we are continually involved in a multitude of sins to include:

[redacted]

A good collection manager is in some way always associated directly or indirectly with many of those functions. This was not very well reflected in the article, if at all.

~~(S-CCO)~~ In fact, if it wasn't for the highly dedicated efforts of our relatively small work force of collection managers the current ability of this agency to satisfy its SIGINT requirements [redacted] would be greatly diminished and/or in a messy state of disarray. And as NSA's mission continues to grow, the functions and roles of our collection managers will most likely continue to expand, not diminish.

~~(S-CCO)~~ I believe that the role of the collection manager and collection management as a profession is absolutely essential if NSA is to continue to satisfy its SIGINT requirements. I further believe that the collection manager in the performance of the multiplicity of his or her duties and functions in the process of getting the product to the consumers is absolutely vital and should be so acknowledged. Today's collection manager can be and should be very proud of his or her chosen profession.

~~(S-CCO)~~ This is not to say that collection managers cannot or need not improve upon their past performance and accomplishments -- they can and they are very willing to. In fact, today's collection manager is in a better position than ever before to do a more effective job more efficiently due to the modern tools of the computer age coupled with recent telecommunications upgrades. The most significant shortcoming of today's collection manager is due to the lack of a meaningful training program. All of the efforts and all of the tools and communications enhancements will not optimize the collection manager's skills or maximize his or her productivity unless they are fully and formally trained to handle the many and various collection-related matters in which they become involved. A good, complete, well-structured formal collection manager's training program is sorely needed to remedy the initial lack of technical, subject-matter related and literary expertise of our new collection

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~
EO 1.4.(c)
P.L. 86-36

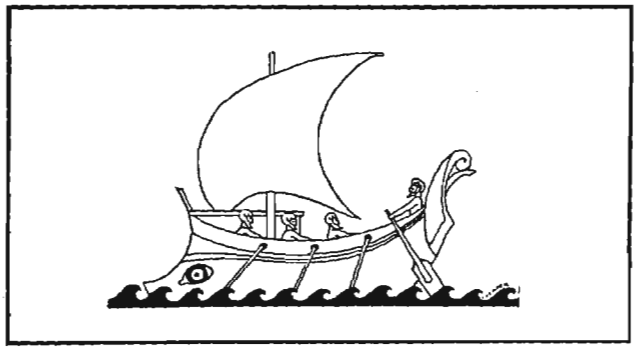
DOCID: 4010004

P.L. 86-36

~~SECRET~~

manager trainees. This approach, I believe, would be a positive step in the right direction.

[redacted] *G841.*



To the Editor:

~~(FOUO)~~ We read with great interest two letters to the editor concerning the ODYSSEY/CAMS article in the CRYPTOLOG. We in the organization where the process was begun would like to address the various points that were made in these two unsigned letters. So, to `A Retiring Cryptanalyst,' `An Old Timer,' and anyone else who may be interested, please read on.

~~(S-CCO)~~ Let us address the points common to both letters. Each advocates interactive editing either "very early . . . " or "before . . . " . Interactive editing would defeat the purpose of this process. [redacted] the shortest possible time with an absolute minimum of human intervention. In order to understand why, for us, the issue of `minimum human intervention' was and is critical, let us give a few statistics about the volumes we are faced with. [redacted] An additional benefit we derive is the capability to feed back decrypts to field sites seven days a week without having an analyst on hand to monitor the process.

[redacted]

~~(C-CCO)~~ Both letters showed concern over lost messages and perhaps never seeing key messages. These fears are unfounded since all messages that pass the various thresholds and process through the system are accounted for; [redacted]

~~(C-CCO)~~ The final point in common is a concern over the quality of AG22 data. We see no point in debating this issue. Given our successes as demonstrated by the above statistics, the quality must not be too bad. There is an additional capability which was not fully explained in the original article. [redacted]

~~(FOUO)~~ After we first started using the CAMS process, B53 gave demonstrations and talks about ODYSSEY/CAMS to interested people and organizations; the most notable being for the 1982 CA-305 course and for the 1982 CISI Spring Conference. We will be happy to discuss

~~SECRET~~ EO 1.4.(c)

~~HANDLE VIA COMINT CHANNELS ONLY~~ P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

any of these points further or to give demonstrations to anyone interested.

~~(C)~~ This organization does not view ODYSSEY/CAMS as a universal processing method. It is not the "be all and end all" for Agency cryptanalysts. For the original purpose for which it was created, ODYSSEY/CAMS is a very successful process and we highly recommend it to any organization that is tasked

B53 Management and Cryptanalysts

P.L. 86-36

~~*The following letter is classified C-CCO NO CONTRACT in its entirety.*~~

To the Editor:

CRYPTOLOG

is a classified publication.

It may not be read in the cafeteria

or in other insecure areas.

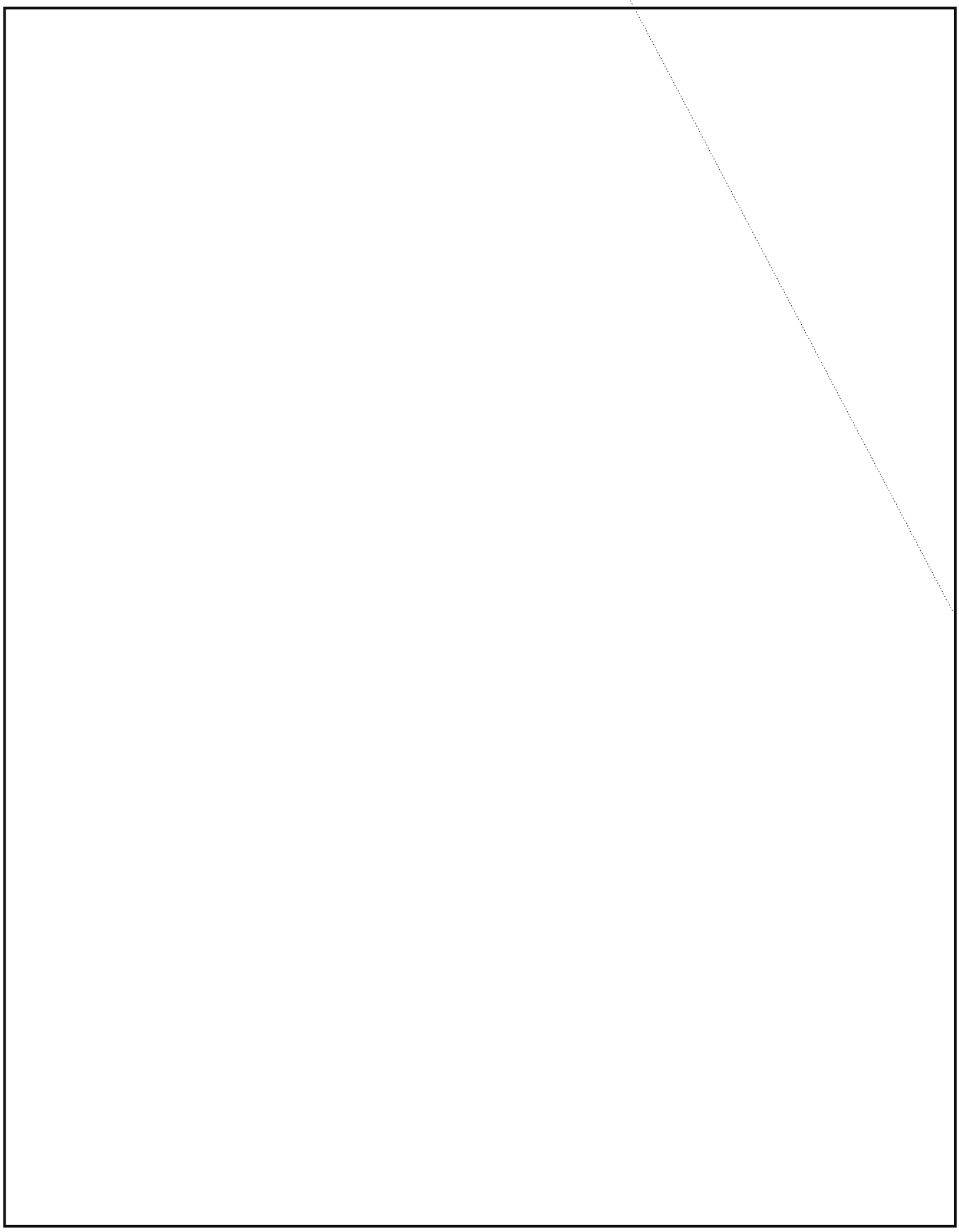
EO 1.4.(c)
P.L. 86-36

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4010004

EO 1.4.(c)
P.L. 86-36

FROM THE PAST (U)



RESULTS OF THE READERS' SURVEY (U)

In the May-Jul 1986 issue we used a variety of type faces, word spacings and leadings. Also, for some articles we right-justified the text, for other articles we didn't. An additional variation, a more subtle one, consisted of using for some articles 12-point type at 80% and for others, 10-point type at 100%; these two are theoretically equivalent. The purpose of this experiment was to determine what combination of variables would provide the most readable text, given the limitations (and bugs) of the current word processing software. And so we asked readers for their opinions. Meanwhile, we were moved to another press and a new page size.

Of the 38 responses received, one-third (idiosyncratically, as might be expected of the NSA population) gave only a few top and bottom choices, so the totals are not the same for all entries. Overall, people were more in agreement about what they *didn't* like than about what they did like. The scores show an aversion to fonts designed for optical character readers and to closely-spaced words and lines. The few comments indicated preference for serif type faces. And some respondents hadn't noticed any difference at all!

This text is set in 12-pt Classic, double space between words, with 15-pt leading, reproduced at 90% now that we are using the new standard page size of 8½x11. The result approximates 11-pt type, considered ideal for narrative text. We believe that this combination will be very readable. About right justification: we try it out for each article. When it causes grotesque spacing -- usually because of a sequence of long words -- we revert to ragged rights. We expect to right-justify routinely beginning in mid-1987, when upgraded software with automatic hyphenation is to be installed.

In the summary below, the NET column shows TOP 3 minus BOTTOM 3, for a net score.

ARTICLE	TOP 3	MIDDLE 9	BOTTOM 3	NET	TYPE FACE	SIZE	LEAD-ING	WORD SPACE	JUSTI-FIED?
Odyssey	14	15	2	12	Classic	12/80	13 pts	Double	No
C3	2	18	9	-7	Classic	12/80	12 pts	Single	No
Linguist	18	12	1	17	Classic	12/80	15 pts	Single	No
AI	3	16	14	-11	Classic	12/80	12 pts	Single	Yes
Documents	11	17	1	10	Modern	12/80	13 pts	Single	Yes
Team	8	21		8	Classic	10/100	11 pts	Single	No
Passwords	12	15	4	8	Modern	10/100	11 pts	Single	Yes
	5	21		5	Modern	10/100	12 pts	Single	No
Editor	6	14	6		*Mod Ital*	12/100	12 pts	Single	No
	6	19	2	4	Modern	12/80	14 pts	Single	Yes
	8	8		8	Classic	12/80	14 pts	Single	Yes
	1	15	9	-8	*Class Ita*	12/80	14 pts	Single	Yes
		7	21	-21	OcrA	12/80	13 pts	Single	No
		10	17	-17	OcrB	12/80	13 pts	Single	No
	3	21	2	1	Titan	12/80	14 pts	Single	No

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010004

P.L. 86-36

PUZZLE

by

"Wheel of Fortune" has become one of the most popular TV game shows in history. The object is to solve a word or phrase by guessing the letters that appear in it. For a bonus prize each contestant is invited to supply five consonants and one vowel, then given 15 seconds to solve a phrase with only those six letters revealed. Most contestants choose the letters L N R S T E, which are the ones revealed in the phrases below. A brief clue is provided for each. An additional clue is that all the solutions relate to cryptology. Note that `Person' need not indicate a proper name.

EXAMPLE:

Place: N_T___N_L SE___R_T_ ___EN___

Thing: ___N___L_____ET___ S___ST_T_T___N

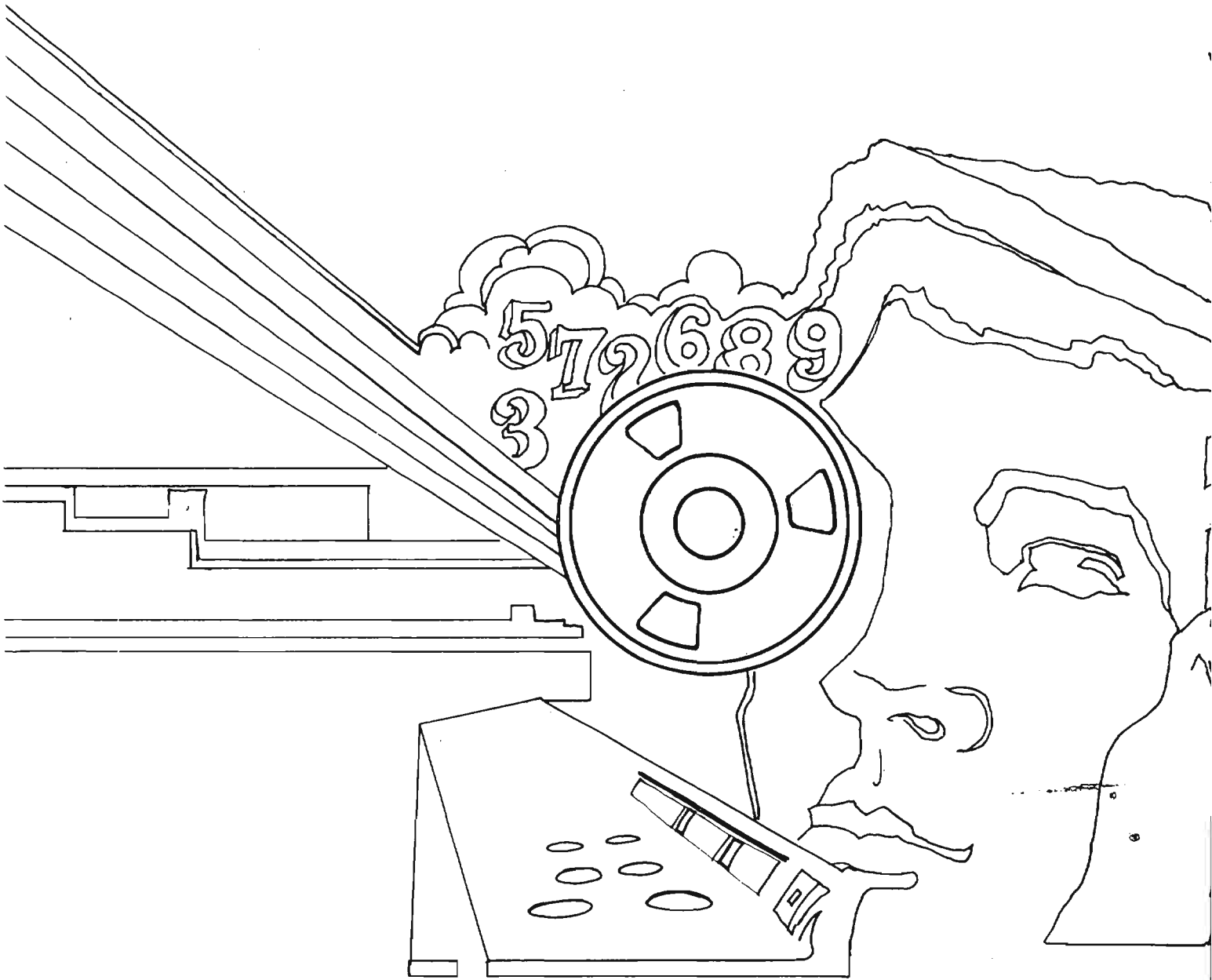
SOLUTION:

NATIONAL SECURITY AGENCY
MONOALPHABETIC SUBSTITUTION

o o o o o o o o

1. Person: _ _ L L _ _ _ _ R _ E _ _ _ N
2. Place: _ R L _ N _ T _ N _ _ L L
3. Person: _ _ _ _ E R _ L E R _
4. Thing: _ _ _ _ L E T R _ N S _ _ S _ T _ _ N
5. Organization: _ _ _ _ _ R E _ _ E R S _ _ R _ _
6. Thing: _ _ R N _ _ _
7. Thing: _ _ L L S _ _ N R _ T _
8. Place: R _ T _ S _ _ _ N
9. Thing: _ E _ T _ R E _ _ _ N _
10. Place: _ _ E L T E N _ _ _
11. Thing: _ N E - T _ _ E _ _ _
12. Place: _ L E T _ _ L E _ _ _ R _
13. Thing: S _ R E _ _ S _ E _ T R _ _
14. Place: _ _ R _ _ R T S _ _ _ R E
15. Thing: _ L _ _ _ _ _ R S _ _ _ R E
16. Thing: N _ R _ _ L _ _ S T R _ _ _ T _ _ N
17. Phrase: _ _ R _ _ _ _ _ _ _ L _ S E _ N L _
18. Thing: _ _ _ _ _ N _ _ _ T _ _ N S S E _ _ R _ T _
19. Historic thing: _ _ _ _ E R _ _ N N T E L E _ R _ _
20. Thing: _ _ _ E L _ N _ _ _ _ _ N E

~~FOR OFFICIAL USE ONLY~~



THIS DOCUMENT CONTAINS CODEWORD MATERIAL

TOP SECRET

DOCID: 4019706

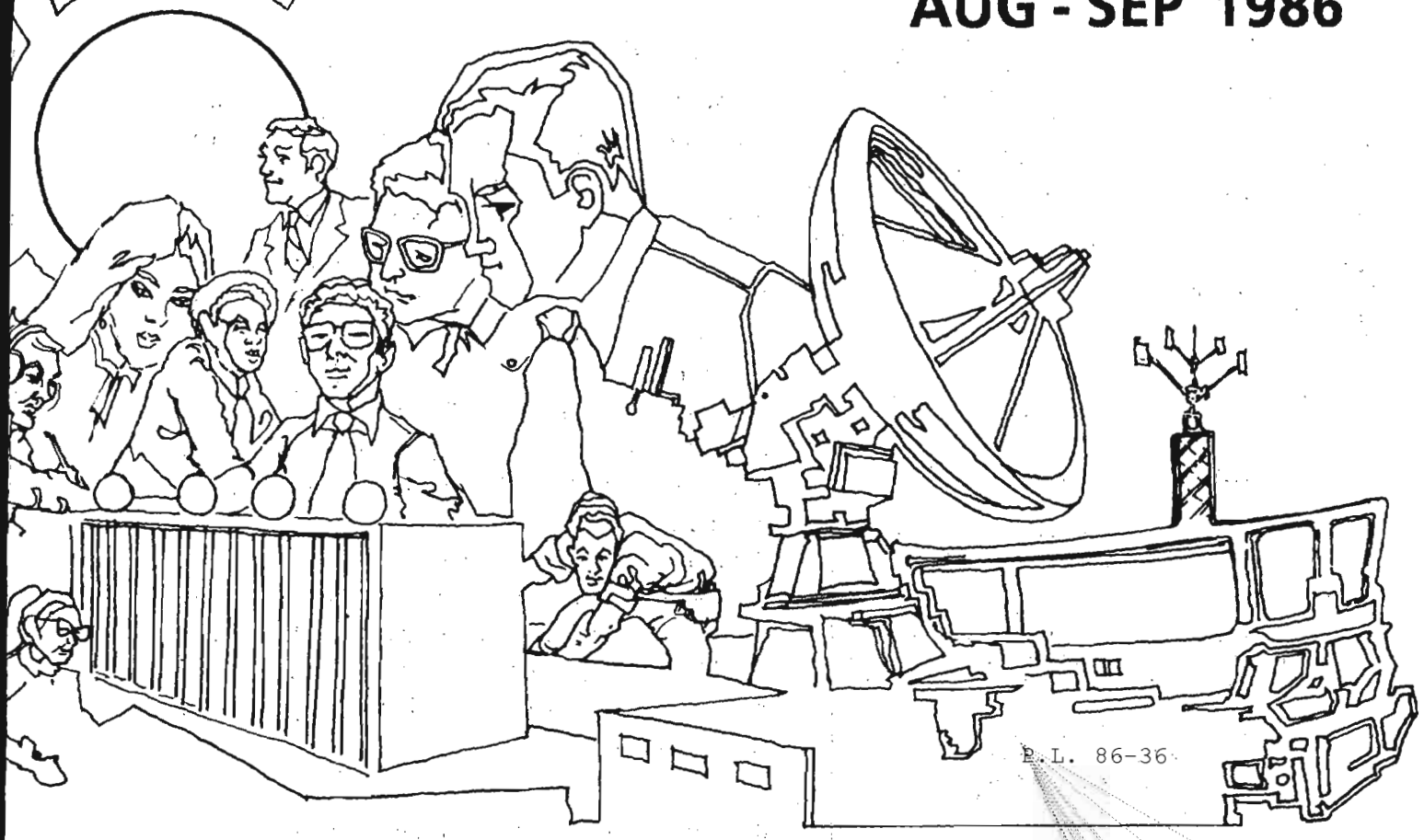
~~SECRET~~

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

AUG - SEP 1986



P.L. 86-36

SOMETHING NEW (U) 1
RUM RUNNERS, 1930 (U) 6
ENTER YOUR PASSPHRASE, PLEASE (U) 12
EXTENDED HOURS AT LEARNING CENTER #1 (U) 17
COLLECTION MANAGEMENT (U) 18
BULLETIN BOARD (U) 20
SENIOR PROFESSIONAL CAREER PROGRAM (U) 21
BACK-UP SHELLS FOR THE ASTW (U) 25
CONFERENCE REPORT (U) 26
BOOK REVIEWS: OUT OF THE INNER CIRCLE (U) 16
. . .SECRECY, AUTHENTICATION, AND PUBLIC KEY SYSTEMS (U) . . 27
. . .THE COMPUTATION OF STYLE (U) 29
. . .ITALIAN FOR EDUCATED GUESSERS (U) 30
LETTERS (U) 15, 31
A PRIVATE GERMAN CIPHER OF WW I (U) 36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

DOCID: 4019706

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XIII, Nos. 8-9 ..... August-September 1986

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Collection ..... (963-5877)
Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Cryptolinguistics ..... (963-1596)
Index ..... (963-5292)
Information Security ..... George F. Jelen (963-1211)
Information Science ..... (963-1145)
Intelligence Research ..... (963-5283)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (963-4191)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-5734)

Illustrators ..... (963-3057)
..... (963-6211)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptolg at bar1c05
(bar-one-c-zero-five)
(note: no 'o' in 'log')

Always include your full name, organization, and secure phone number.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1
Please do not phone.

Contents of CRYPTOLOG should not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

GOOD BUREAUCRATIC WRITING (U)

P.L. 86-36

A contradiction in terms?

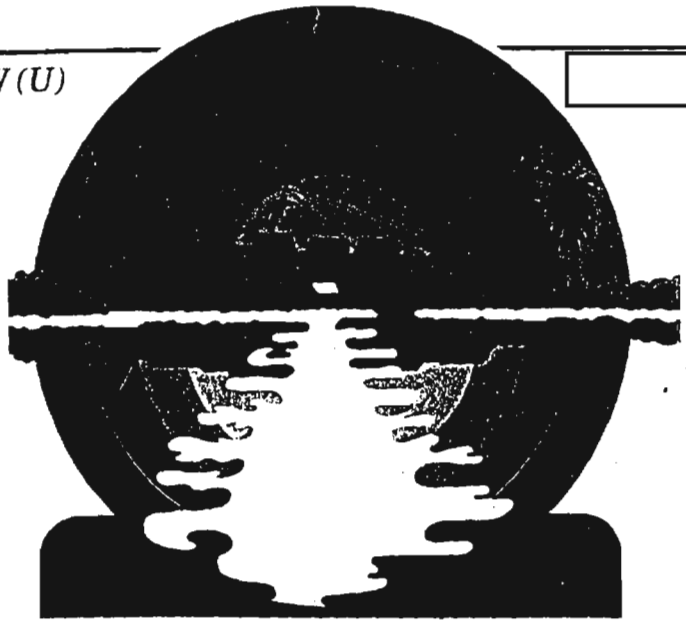
No! It's just that good bureaucratic writing is uncommon. Something strange gets into people when they compose official documents. They forget that the intended readers are the very same human beings they've been communicating with all along.

Maybe all they need is a good example. There's one beginning on page 21. Note that it is short though the information is complete. It can be scanned readily. It reads well. The tone is good. And, marvel of marvels, it states plainly that there is a change of concept, and tells why. Such directness is seldom found. It is efficient as well as refreshing. After all, the population to whom this is addressed is composed of senior professionals in the intelligence business. These people, let us hope, would inevitably find the needle of information in a haystack of gobbledy-gook. It might take them longer, that's all.

Just to show that this example is not unique {single, sole, one-of-a-kind} but merely unusual {rare, exceptional, remarkable}, there's another example beginning on page 6. It's a very readable, nay, fascinating, budget proposal. Surely it moved mountains!

DOCID: 4019706

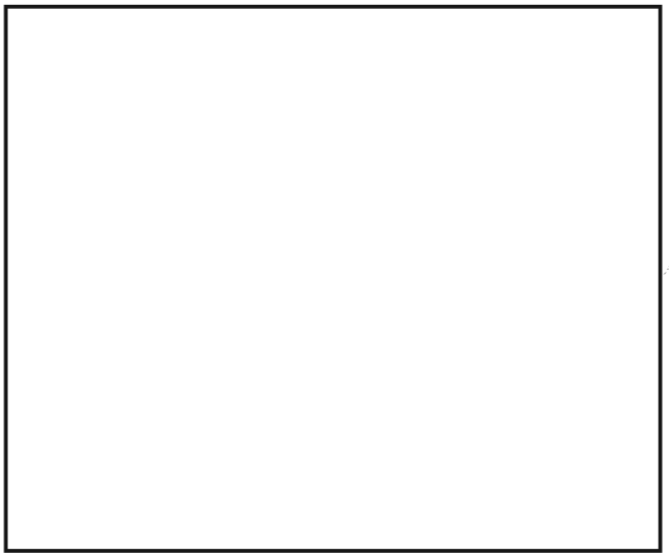
SOMETHING NEW (U)



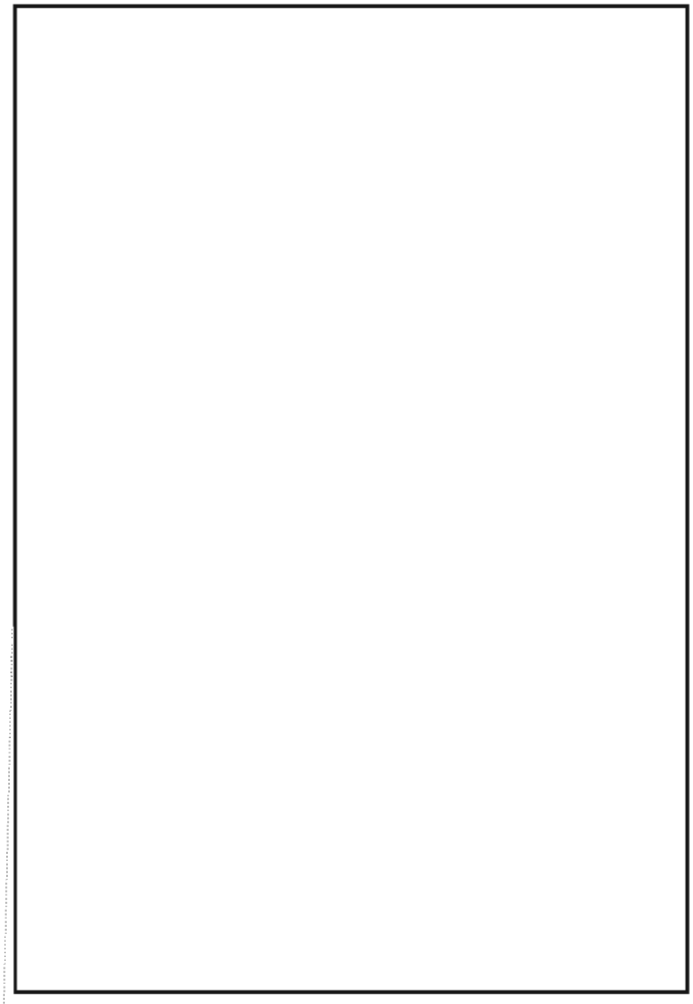
TARGETING NARCOTICS TRAFFICKERS ~~(S-CCO)~~

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



AUTHORITY



(U) One principle underlying the ruling is that there is no reasonable expectation of privacy for the radio communications of narcotics traffickers. Therefore, there is no general Fourth Amendment preclusion of USSS interception of such communications and of the monitoring and targeting of US persons who are parties to the radio communications of ships and aircraft involved in narcotics trafficking.

~~(FOUO)~~ Special procedures were approved by the Acting Attorney General in December 1984 which authorize intercept and direction finding against persons whom the USSS reasonably suspects to be engaged in international narcotics trafficking. An international trafficker is defined as any person engaged in buying, selling, manufacturing (from cultivation to refining), or transporting a controlled substance as defined by the Attorney General, where such activities cross international boundaries.

US POLICY

(U) Narcotics were legally imported into the US for more than a hundred years. By the beginning of this century there was strong sentiment to outlaw alcohol but little public concern for the widespread use of narcotics. Drug stores and grocery stores sold narcotics without a prescription and mail order houses distributed them as cures for any number of ailments.

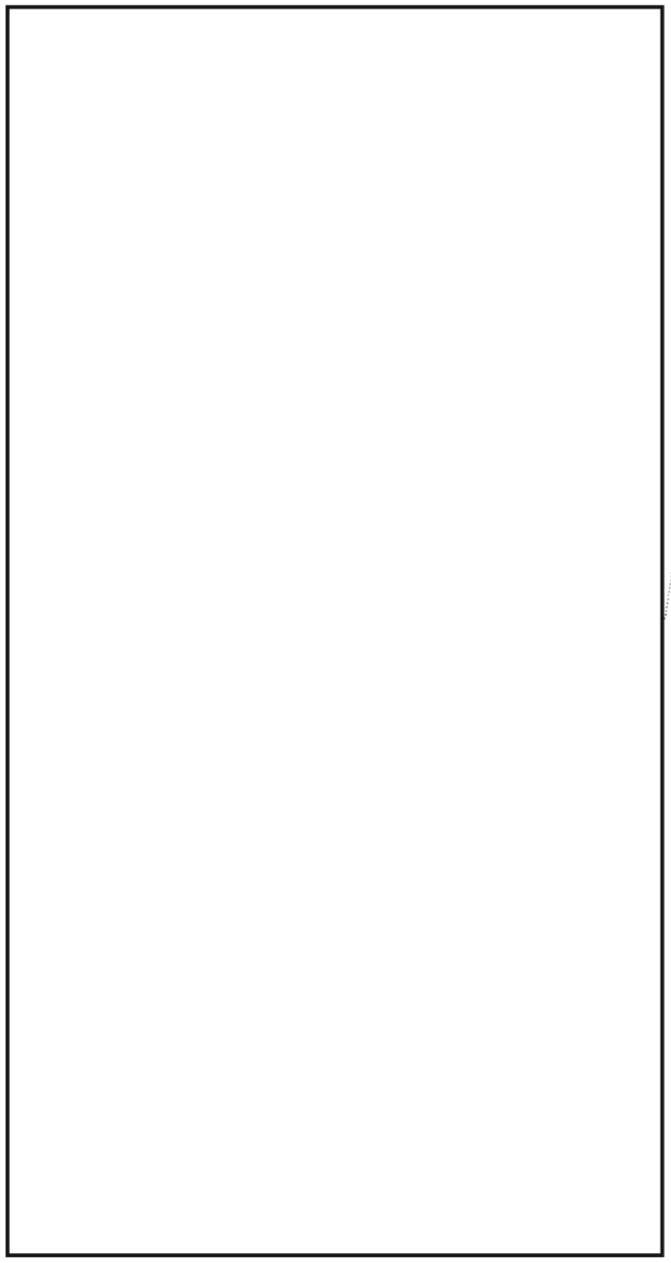
(U) On December 17, 1914, President Wilson signed the Harrison Narcotic Act, establishing the foundations of federal drug law enforcement. Since it was basically a tax on narcotics, Treasury was left to enforce it when it became law on March 1, 1915. The first step in monitoring international commerce in opiates was passed in 1922 and was called The Narcotic Drugs Import and Export Act.

(U) The Federal Bureau of Narcotics was established on July 1, 1930 and in September President Hoover appointed Harry J. Anslinger Commissioner of Narcotics, a position he held for more than three decades. It was Commissioner Anslinger who initiated the enduring US drug policy which maintains that the solution to the drug abuse problem lies

EO 1.4.(c)
P.L. 86-36

DOCID: 4019706

EO 1.4.(c)
P.L. 86-36



with the foreign nations that produce the illicit drugs.

(U) The White House stated in 1982: " . . . the elimination of illegal drugs at or near their foreign source is the most effective means to reduce the domestic supply of these substances." There is evidence that US efforts to control the production of drugs abroad have been largely unsuccessful. Unfortunately, narcotics involves developing nations in debt and in need of US dollars. The producing nations argue that the product would not exist were it not for the demand for the illegal drugs, while Congress accuses the State Department of giving too little high-level attention to the drug problem.

THE NATIONAL BORDER INTERDICTION SYSTEM

(U) In 1982 the National Narcotics Border Interdiction System (NNBIS) was established to combat drug smugglers at the US borders. It collates the intelligence, assesses the threat to the region, prioritizes smuggling targets, identifies resources available to interdict those targets, and recommends actions to the participating agencies. These consist of 14 Federal agencies and 14,000 state and local law enforcement entities that either have a role in drug enforcement or no statutory bar to such a role. The purpose of NNBIS is to increase the various agencies' effectiveness through cooperative and coordinated efforts.

(U) Reservations concerning NNBIS are many. Some suggest that NNBIS isn't needed because organizational coordination is not the problem and that reorganizations serve only to confuse the law enforcement community. State and local law enforcement agencies complain that coordination with NNBIS is virtually nonexistent and that NNBIS has merely confused the national drug enforcement effort and disrupted traditional working relationships with DEA, Customs, and the Coast Guard.

(U) Many people believe that coordination among DEA, Customs, and the Coast Guard is a problem. Note that the US Coast Guard is a part of the Department of Transportation, the US Customs Service is part of the Department of the Treasury, and the Drug Enforcement Administration is part of the Department of Justice. As in any bureaucracy, they sometimes don't talk to one another because of territorial competition. Increasing agency coordination for an effective drug enforcement effort is not yet a reality, and the jury is still out on the effectiveness of NNBIS as the answer.

NARCOTICS INTELLIGENCE GATHERING

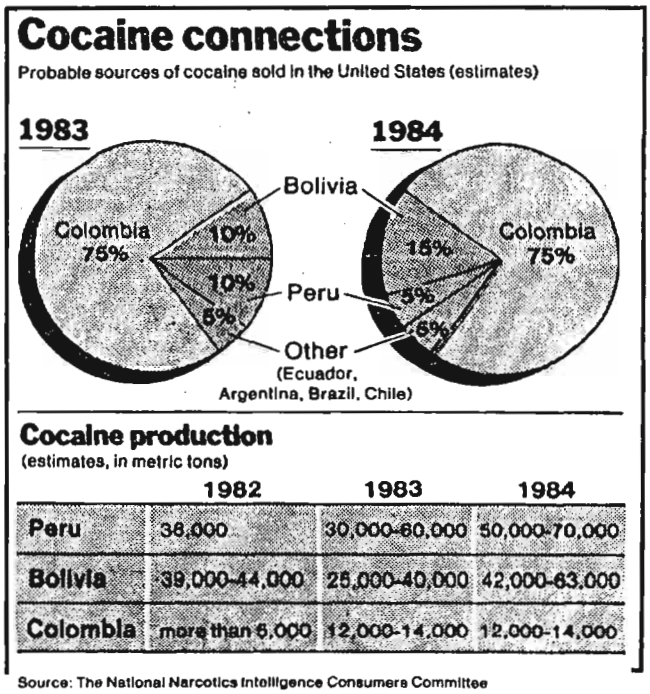
(U) DEA, created in July 1973, is the lead Federal agency in enforcing controlled substances laws and regulations. Its primary responsibilities are to: investigate major narcotic violators; enforce regulations governing the legal manufacture, distribution, and dispensing of controlled substances; manage a national narcotics intelligence system; coordinate with federal, state and local law enforcement authorities and cooperate with counterpart agencies abroad; train and conduct scientific research; and exchange information in support of drug traffic prevention and control.

(U) The El Paso Intelligence Center (EPIC) is an interagency operation managed by DEA with participation by nine other federal agencies and working agreements with 45 states. EPIC provides a nationwide intelligence clearinghouse for drug enforcement information. Most information produced by EPIC is marked "DEA SENSITIVE" because it does not qualify for classification as National Security Information. SIGINT received by EPIC pertains to narcotics information only and is used to corroborate other sources. Fewer than six persons with special intelligence clearances have access to SIGINT, and they are forbidden to remove, sanitize, or enter it into other databases.

STATUS

[redacted]

(U) Interdiction, however, is difficult. Most marijuana is smuggled into the US by ship and most cocaine by aircraft. Since cocaine is easier to ship and the profits are greater for dealers, there has been a predictable switch to cocaine. Ironically, the success of the US effort against marijuana has had the effect of weaning the



Cocaine production
(estimates, in metric tons)

	1982	1983	1984
Peru	36,000	30,000-60,000	50,000-70,000
Bolivia	39,000-44,000	25,000-40,000	42,000-63,000
Colombia	more than 6,000	12,000-14,000	12,000-14,000

Source: The National Narcotics Intelligence Consumers Committee

American public off marijuana and onto cocaine. The children who once smoked marijuana may now be smoking crack.

~~(SC)~~ NSA is only one of many players who deal with the international narcotics problem, but our input, modest though it is, is invaluable. SIGINT contributes to national estimates forecasts and to studies on the narcotics problem, and often gives US policy makers an indication of how effectively foreign aid earmarked for narcotics eradication is being used.

[redacted]

~~(S)~~ In April 1986 President Reagan signed the National Security Decision Directive that "will permit the armed forces to dedicate personnel and equipment ... to fight drug trafficking. Now the armed forces will be able to help in almost any area of drug law enforcement except arrests, seizure of materials and apprehension of suspects, as long as their primary defense mission is not jeopardized." Drug trafficking in the US Southern Command is seen as feeding arms supply and insurgency which destabilize Latin America. In this light, the new military role in the drug fight becomes more

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

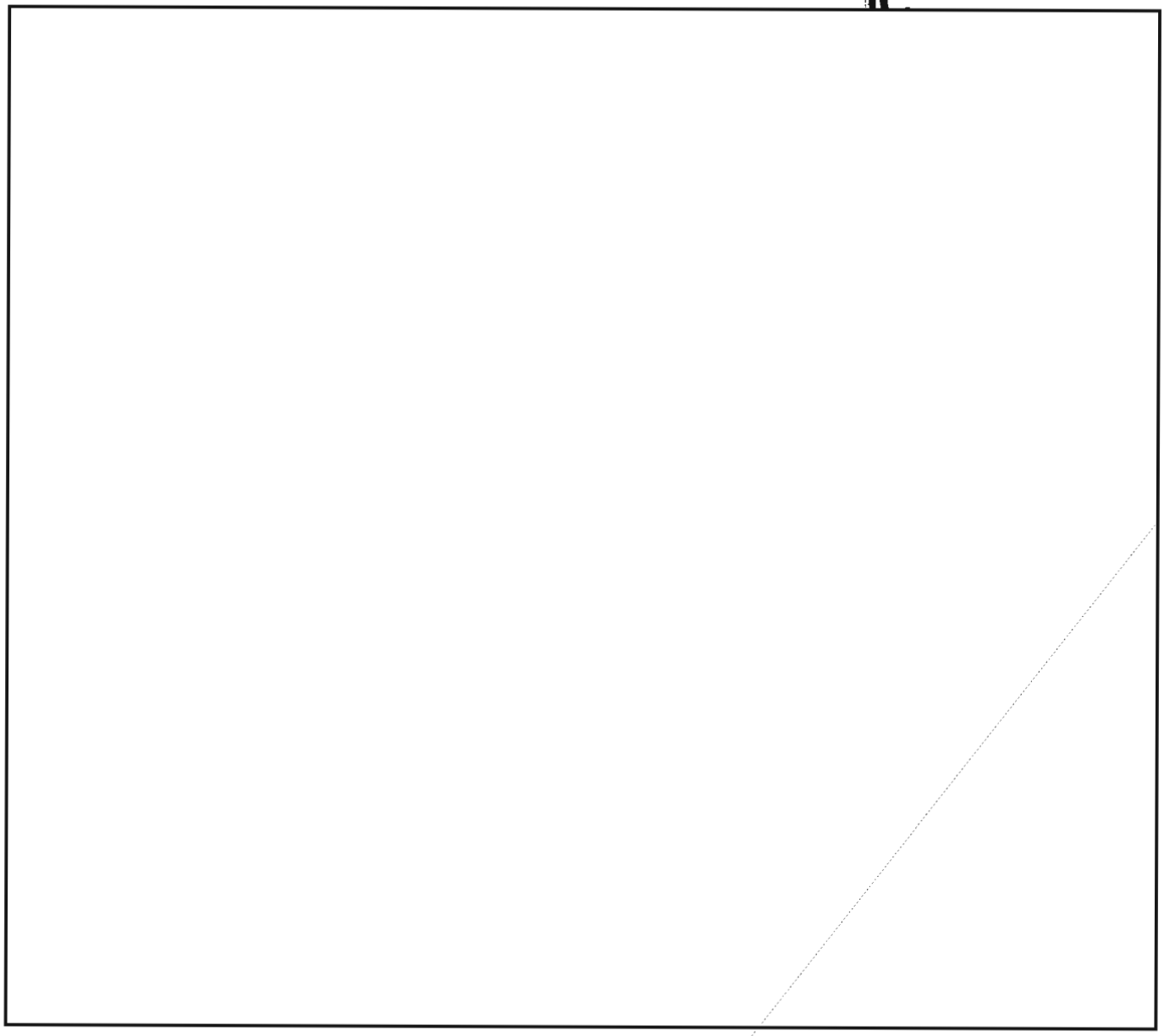
DOCID: 4019706

understandable. Defense Secretary Weinberger, however, once termed the idea "very dangerous and undesirable." Civil liberties advocates fear covert surveillance of US citizens, preferring that President Reagan ask Congress to fund the regular agencies.

~~(S-CCO)~~ But while the Defense Department budgets have soared in the last five years and DoD has been given an increased role in combating narcotics, Coast Guard ships sometimes remain in port because of the lack of gas and manpower to interdict drug smugglers. Priorities need to be adjusted so that enforcement agencies can act upon SIGINT when it is applicable. Moreover, it is clear that the federal law enforcement community needs better organization and coordination on narcotics interdiction strategy. It may also need to better define the role SIGINT can play in this overall strategy. □

Editor Note:

Readers might be interested in comparing present efforts to combat narcotics trafficking with similar efforts to interdict rum runners during Prohibition, as described in the memo beginning on the next page.



EO 1.4.(c)
P.L. 86-36

DOCID: 4019706

Rum Runners, 1930 (u)

DATE: 10 October 1930

MEMORANDUM FOR THE COMMANDANT

SUBJECT: Radio Intelligence; Establishment of Cryptanalytic Section at Headquarters and Intercept Stations in the Field

In accordance with your instructions of 3 October, I took up with Customs the matter of holding in abeyance the transfer of Mrs. Friedman, cryptanalyst, and her assistant, from the Coast Guard Intelligence Office to the Divison of Special Agents, Bureau of Customs, pending the determination of the question as to whether or not the Coast Guard could undertake the establishment of a cryptanalytic section at Headquarters as a basis for a radio intelligence service in the field which would put the enforcement agencies (Coast Guard, Customs and Justice) in immediate possession of specific knowledge of the operations of the smugglers upon which definite action, resulting in seizures and the prevention of smuggling, can be taken.

Customs readily assented to the retention of Mrs. Friedman and her assistant pending developments and, moreover, agreed that the Coast Guard was the logical government agency to handle the radio problem. When my plan was outlined, the Commissioner of Customs, Captain Eble, not only agreed to the Coast Guard undertaking the project but offered to go to Mr. Mills in support of it.

In order that you may be fully acquainted with the problem and its solution a brief summary of the radio activities of the smugglers and the attempts, to date, of the enforcement agencies to combat it is necessary. Practically all operations of the smugglers from the sea are now directed by radio in code and cipher. Without radio the smugglers would be so greatly handicapped that I have no hesitancy in saying that once the Government can gain the upper hand in the control of their radio activities smuggling from the high seas will be reduced 50 per cent. On the east coast there are forty-five radio stations, between Maine and Florida, directing the movements and operations of smuggling craft. There are fifty-eight smuggling craft known to be using radio. The Coast Guard has a record of eighty-one stations in a single group whose operations are directed from the New York area. On the west coast, all smuggling operations on the coast of California are directed by radio from Vancouver and a station on the California coast. In short, communication between ships and shore is essential to the operations of the smugglers on the present organized scale. It is carried on constantly in code and cipher. It is now being intercepted by the Coast Guard and by Customs Agency intercept stations. This intercepted material contains much of the information that the investigative agencies of the Customs and Justice are after the practically all of the plans, including contact points, to obtain which the Coast Guard vessels cruise endlessly.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

About three years ago the late Captain Root took up the matter with Prohibition, and, with the Prohibition Bureau furnishing personnel and the Coast Guard the equipment, intercept stations were established in San Francisco and Florida, and Mrs.Friedman, cryptanalyst, was employed by Prohibition and established in the Coast Guard Intelligence Office to decipher and decode the material. The information thus obtained was most valuable to the Customs Agency and Coast Guard in giving into the hands of the enforcement agencies complete information of the plans and methods of operation of the smuggling rings as well as the personnel engaged in the traffic ashore. With this limited organization valuable information for use in combating the rum-runners was obtained. The uses to which this information was put, and numerous concrete examples of the practical value of this work in the prevention of smuggling can be given from the files of this office.

Up to recently this work was mostly informative but the success obtained with this modest beginning led to an experiment with a 75-foot patrol boat (the CG-210) which was turned over to the Intelligence Office to operate. It was equipped with high-frequency receivers and radio-compass and assigned to duty in the New York Area to:

(1) Intercept and send in for solution the radio communication between rum ships and radio ashore.

(2) Locate and raid illegal radio stations from which the operations of the rum ships are directed.

This patrol boat; under the command of Lieutenant Meals, has done all that was expected of it. Its success in intercepting by high-frequency receivers of the rum-ship operating orders and in locating the illegal stations on shore with its recently developed high-frequency radio direction finders, led to the final step in the establishment of a complete field radio intelligence unit. Through the cooperation of the War Department, Major Friedman, Chief of Signal Intelligence Division, and an expert cryptanalyst, was detailed to the CG-210 for a period of two weeks. We thus had on a single 75-foot patrol boat:

(1) A battery of high-frequency receivers with radiomen to intercept the coded operating orders of the rum-runners.

(2) A cryptanalyst to reduce the intercepted message to plain text.

(3) Radio-compasses to locate the illegal stations.

(4) A Coast Guard officer thoroughly familiar with the operations of the enforcement agencies to immediately act on the information derived.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

In a period of two weeks the following was accomplished by the CG-210:

(1) The code was used by a group of smugglers operating off New York was broken and the operating orders to the rum ships were read as soon as received.

(2) The code was compiled and made available for use by the Coast Guard units.

(3) Two radio stations, one situated in new Bedford, Mass., and one in Coney Island, were located, raided and put out of business. (Coast Guard working in conjunction with Department of Justice agents and Department of Commerce inspectors).

(4) Evidence linking up the NOVA V, recently seized by the Coast Guard, with the radio station was obtained with is deemed ample to indict on conspiracy charges.

As a result of the interception and solution of the smugglers code and the raiding of the station, the operations of the group of rum ships was completely stopped for several days, no contacts were made and the resulting confusion to this group of rum ships was more than all the efforts of the destroyer force and other units combined have been able to effect in months--and it should be remembered that this was accomplished by a single patrol boat with nine men aboard which never went near "rum row." As a result of this two-weeks experiment we have arrived at the point where it has been demonstrated that the radio intelligence unit has passed from the purely informative stage to one of practical application as an invaluable aid to the patrol forces engaged in the prevention of smuggling.

The problem of the use of radio by rum-runners has grown to such proportions during the past year that it has attracted the attention of other government departments, with the result that a recent inter-departmental committee from Justice, Commerce and Treasury was appointed to suggest a solution. The report of the Committee is appended and it will be noted that the conclusions and recommendations show that the problem and its solution is entirely Coast Guard work. In fact, there was no necessity for putting it up to an inter-departmental commitee as the Coast Guard not only has been aware of the situation for years but has had all the elements for its solution at its disposal. It is logically a Coast Guard activity.

Now the keystone of the whole system is the reduction of the rum-runners' codes and ciphers to plain text--the cryptanalyst section--and it is essential that there be established at Headquarters a section in the Intelligence Office capable of breaking the codes and ciphers and supplying the rum-runners' codes and ciphers to the field; and of training the men in charge of intercept stations in this line of work. The set-

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

up required and the cost is appended. Discussion of this will be given in person, as it is quite involved and extended.

It might be well, here, to give a brief summary of the present rum-running situation. In the past year there has been an increase of 34 per cent in foreign rum-runners. We are now back to where we were three years ago with this vast difference, the rum-runners are organized on a basis that makes the methods used three years ago practically obsolete. And their radio communication system is the key to this organization. The actual figures are:

1927	138
1928	109
1929	103
1930	138

One rum-running syndicate pays the man in charge of its radio installations $10,000 a year. The radio communications on the west coast are directed from Vancouver by a radio schoolmaster versed in the most intricate system of codes and ciphers. Rum ships are in charge of former British Naval Officers. Under present conditions on the west coast the Coast Guard is practically impotent. On the east coast the Coast Guard harasses and annoys the rum ships, but the results in proportion to the effort expended is pitifully small. One of the purposes of the radio intelligence unit is to obtain greater results from the same expenditure of effort; in other words, to employ the present equipment of the Coast Guard to the best advantage. The cost of the entire radio intelligence unit is less than the cost of operation of a single destroyer or cutter or of three or four patrol boats, and the results that should be obtained are worth more than the results of operating a squadron of destroyers or patrol vessels.

It must be understood that this subject of radio intelligence is not theoretical nor anything new. The following has been actually accomplished:

(1) Cipher message intercepted and solved showing contact point where and when shore boat is to take load from rum runner. Information given to patrol force, British and American rum-runners seized. (Case ISABEL H--Destroyer Force).

(2) Radio stations on shore directing rum-ships operations and contacts located and raided. (New York area).

(3) Codes and ciphers broken and furnished to field so that operations of rum ships made available immediately to patrol forces. (West coast, Gulf and New York areas).

(4) Evidence obtained by breaking ciphers and codes to obtain convictions on seizures. (Gulf and New York areas--NOVA V).

~~FOR OFFICIAL USE ONLY~~

(5) Information furnished Customs and Justice agents to build up cases of the rum rings ashore which are operating the rum boats.

Concrete cases can be supplied from the files of this office. A development now in process is the location of the rum ships at sea by radio-compass instead of by the cruising of destroyers and patrol boats over thousands of square miles of sea.

The necessary field units can be supplied by the Coast Guard from present equipment and personnel--if necessary taking them from units now producing no results. What must be supplied is the Headquarters' Civil Service unit, costing approximately $12,000 a year.

Now for the other side of the picture. If this organization is not adopted by the Coast Guard, Mrs. Friedman goes back to Customs and works on the intercepts from the two Customs stations. The Coast Guard with its destroyers and patrol on a military basis will continue to patrol the seas and operate precisely as if radio had never been heard of, spending hundreds of thousands of dollars in an effort to stumble across. the information that is constantly on the air, i.e., the location and contact points of the rum-runners. Any one familiar with the history of the British Navy in the World War could hardly fail to appreciate the value of this work.

The personnel in the field are interested in this phase of operations and are wondering why Headquarters hasn't long ago developed an organization along these lines. Radiomen construct short-wave receivers, get the traffic and send it in to Headquarters--and there the matter ends. There is decidedly a question of morale involved. There is no brooking the fact that there is now spreading in the Service a sense of futility of effort; and from that a feeling that a demonstration is all that is required; and it is a very short step from that to the belief that a demonstration, rather than actual result is desired by Washington. The cost of this radio intelligence unit is so small in comparison with any other unit as to be insignificant, and it cannot fail to justify this expenditure.

It is therefore recommended:

1. That the Commandant go to Mr. Mills (or to Governor Lowman first and then to Mr. Mills) to get authorization for $14,660 to establish the central cryptographic section at Coast Guard Headquarters (civil service). It would appear that the best procedure is to request that it be authorized for the C.G. appropriation 1930-1931 available 1 July, 1931, and if necessary take this amount from various other items so that the total of the appropriation will not be increased. I deem this matter of sufficient importance to justify asking for a deficiency appropriation to cover but in view of the present fiscal situation, doubt if it

~~FOR OFFICIAL USE ONLY~~

could be obtained regardless of the merits and urgency of the proposition.

2. That three 75 foot patrol boats be turned over to the Intelligence Unit to be equipped and manned similar to the C.G. 210, each boat to have the following personnel:

1 Commissioned officer in command
1 C. B. M.
1 B. M. 1/c
1 C. Mo. M.M
1 M. M. M. 1/c
4 Radio Men 1/c
1 S.C. 1st class

3. That the following personnel be assigned to the New York Intelligence Unit under Lieutenant Meals:

1 Commissioned Officer
1 Yeoman
1 Radioman (Chief or 1st Class)
6 Radiomen 1st class
6 Carefully selected Warrant officers for preliminary training under Meals to be brought to Washington for training under cryptanalytic section when latter is established.

4. It is realized that the personnel asked for above are not available but the importance of this organization justifies, if it does not make mandatory, the withdrawal of the personnel required from other units, particularly non-producing units. The personnel of a 75-footer as now authorized will supply the personnel of each 75-footer assigned to this work.

5. It is realized that the commissioned officers required are not immediately available, and if it is not desired to take them from other units - and I would not hesitate a minute to put a destroyer or other unit out of commission to supply them for this work - carefully selected warrant officers can be substituted to command the 75-footers until commissioned officers are available.

As stated above the Commissioner of Customs, Captain Eble, deems this the most important development to combat smuggling that has arisen and is 100 percent behind the Coast Guard in this plan and will go to Governor Lowman and Mr. Mills in support of it. The inter-departmental situation makes immediate action necessary on the part of the Coast Guard. (This will be explained in person.)

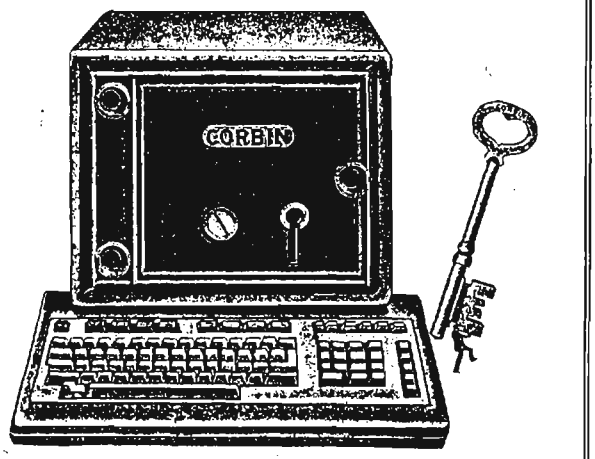
F. J. GORMAN

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

Editor's note:

Computer Security is in the air. In the same week we received an article, a Letter to the Editor, and a book review on the subject, printed below, as well as an item for the Bulletin Board.



Enter Your Passphrase, Please (U)

P.L. 86-36

C11

This article is classified ~~FOR OFFICIAL USE ONLY~~ in its entirety.

In fulfillment of NSA's expanded responsibility in the field of computer security (COMPUSEC), a major effort has recently been undertaken to support enhanced password security at the Agency. Soon users of CANDE and SOLIS will be introduced to the results of this effort. This article will give you an idea of what the new system will be like as well as the history and rationale behind this change.

In an attempt to provide enhanced security, better guidance, and rationale for the use of passwords on a computer system, the National Computer Security Center (NCSC) published the *DoD Password Management Guideline* in April 1985. The document is based on the best security practices on existing computer systems. The underlying principle of a secure password system is that the passwords are kept secret at all times. The major features advocated in this guide-line are:

- that users should be able to change their own passwords;
- that passwords should be machine-generated rather than user-created; and
- that certain audit reports (e.g. date and time of last login) should be provided by the system directly to the user.

The Guideline explains what a good password management system should be able to do, and outlines the responsibilities of users and system security officers in the secure use of passwords. It recommends and suggests alternatives for setting up a password management system, and explains how to calculate such things as the maximum password lifetime, password space (the maximum number of valid passwords that can be generated by the system), and the probability of someone guessing the password for a given password space and lifetime.

When users change their own passwords, no one but the user is involved in that change, and the user is supposed to be the only person who knows the password. But many users lack imagination and select passwords that are easy to remember, resulting in passwords that can easily be associated with themselves. This makes guessing passwords fun and rewarding for anyone trying to gain access to someone else's account.

Machine-generation takes the guess work out of selecting secure passwords, but results in passwords that people dislike because they are

DOCID: 4019706

usually too hard to remember, so they jot down such passwords and leave them by the terminal for handy reference -- by both the authorized user and unauthorized "hacker" alike. Even systems that attempt to provide pronounceable machine-generated passwords often fail to provide a certain linguistic reality which most people need to help remember them. However, there is a way to generate passwords that are both secure and that have linguistic properties that make them much easier to remember. This is using machine-generated passphrases, consisting of a combination of real words, with or without semantic meaning.

To demonstrate the utility of its guideline and the practicality of machine-generated passphrases, the Division of Standards at the NCSC embarked on a project to implement its *DoD Password Management Guideline* on one of the existing computer systems at the National Security Agency. For the experiment, the computer system selected had to be one that would significantly benefit from the implementation, one on which people could really see the tenets of the Guideline in action, and one that could readily use machine-generated passphrases. As the first step they examined the computer systems at NSA and had discussions with system security officers, computer system personnel, and users. Finally, they selected the WINDMILL / PULPWOOD Burroughs system, and began work in May 1985. . The completed Passphrase Management System will appear first on CANDE, followed by implementation on SOLIS.

Under the current system, users are sent a machine-generated, eight-character random alphanumeric password every six months through the mail. The user receives a punched card containing the password and a numbered information form and receipt to be filled out and returned to the Tech Support office acknowledging receipt of the password and that user's continued use of the system. The number on this form matches an identical password card that is filed in the Tech Support office for use whenever a user forgets the password and cannot find the card.

At an appointed time, most often over a weekend, all passwords on the system are changed. As you might guess, the next work day there are a lot of locked terminals as users forget to use their new passwords or have trouble entering them. (Three bad logins locks a terminal.) Paradoxically, the strongest point of the machine-generated password has proven to be its weakness: because random-generated passwords are so difficult to memorize, many users keep their new password on a card near their terminal for easy reference.

Under the new Passphrase Management System, three words are randomly selected from a data base of three to six letter English words and displayed on the user's terminal. The user may use those three words in any desired order to make up a new passphrase. If the set of words proffered does not yield a readily remembered phrase, the user may request another set, up to a maximum of ten sets. Once the word order has been selected, the user must enter the new passphrase correctly twice in succession to verify that it has been entered correctly and to reenforce the new passphrase in the user's memory. If a new passphrase has not been successfully selected within ten tries, the user will be locked out of the system and advised to contact the system security officer for assistance.

A new passphrase is good for a maximum of three months but can be changed at any time before then. The system will automatically alert users when their passphrase is within two

~~FOR OFFICIAL USE ONLY~~

weeks of expiration. Users on interactive terminals may change their passphrase at any time in that period. Should the passphrase not be changed by its expiration date, that user's account will be flagged as having an expired passphrase. Once the passphrase expires, the system will automatically invoke the change passphrase routine whenever a login is attempted and will not allow the user to login until a new passphrase has been selected. If the user does not change the passphrase within two weeks after expiration, the account will be locked, and the user will have to contact the system security officer to get back on the system.

To log in using this new passphrase system, the user first enters his or her standard userid. The user will then be prompted to enter a chargecode, consisting of a classification level, a function code, and a job number. Next, the user will be prompted to enter the passphrase, which wherever possible will be concealed. Upon entry of the passphrase, the screen will be automatically cleared. If all the elements supplied are correct, the user will be logged in and given the date, time, and place of both the last successful login and the last unsuccessful login attempt plus the total number of unsuccessful login attempts since the last valid login. This information can alert the user to any attempted penetration of the system using his or her userid. The new successful login data will be stored, the failed login counter cleared and the user given access to the computer. Should any of the information supplied be incorrect, the user will be told that the login was invalid and a record will be made of this incorrect login by incrementing the failed login counter and storing the date, time and terminal identification.

The user will be allowed a total of ten consecutive unsuccessful login attempts before the account is locked and the user required to contact the system security officer before again being given access to the system.

It is considered a security violation for more than one person to know the password or passphrase for any given individual userid. Thus this system will not allow more than one user to be logged in under a given user account. Special groupids may be established for those projects where more than one user needs to share access to the same computer resources. A user may be a member of as many as five groups, and a group may have as many as thirty members. At login time, the user will enter his or her own individual userid, then a comma, followed by the groupid. When prompted for the passphrase, the user will enter his or her personal passphrase. The userid and passphrase will then be authenticated, and if correct, group membership and classification level will be checked. If everything is correct, the user will be logged in under that groupid. Any problems will result in an unsuccessful login attempt for that user.

Users of the Burroughs system have always included a classification level within the chargecode as part of the login sequence. In the past, the system checked only to see if the classification given was at a meaningful level. Under this passphrase management system, the classification level is also checked against the user's own security profile. For example, if the user has a maximum clearance level of SECRET and tries to login at TOP SECRET, the login will be unsuccessful. Or should the user try to login at UNCLASSIFIED when that particular user's account has CONFIDENTIAL as a minimum access level, the system will also deny access. While the latter illustration may seem an unnecessary precaution, it is a measure to

DOCID: 4019706

protect extremely sensitive data from accidentally finding its way into an unclassified file. A user may also change the chargecode during a given session, but again, the user must specify a level for which he or she has access privileges or the requested change will not be accepted.

A record is made of every action processed by this new system. This information is stored in special audit files for use by the system security officer. There is a general audit file containing all the actions processed by this system, and in addition, another special audit file that contains a subset of those actions that could be indicative of a security problem. Some of this information is also given directly to users at login time in order to help users detect problems with their own accounts. However, the system security officer has these more comprehensive files available for detecting patterns of behavior which could signal overall security problems.

The Passphrase Management System has undergone extensive testing and evaluation and should be fully operational on CANDE by the summer of 1986. This project has shown that the principles propounded in the *DoD Password Management Guideline* can be effectively implemented. The recommendations and specifications in the guideline can be tailored to meet the security needs of any computer system. Keep in mind that while most of the features in the guideline can be automated, much of the effectiveness of any system will depend on the users working with the system security officers to understand and follow good password management practices. □

To the Editor:

In regard to the article "User-Friendly Passwords" in the May-Jul 86 issue, I find a problem with the premise stated in the first part of paragraph three: "the need to generate ... passwords" implying that password generation is a user responsibility. I agree with the DoD Computer Security Center's position, "Passwords should be machine-generated rather than user-created." People are far too predictable when picking passwords. Knowing something about the person allows an attacker to vastly reduce the number of possibilities in attempting to guess passwords. Machine-generated passwords (or pass phrases) are much better at assuring that passwords are distributed over a large space.

I claim that it is the computer system administrator's responsibility to provide password generators which give the user a fighting chance of remembering passwords that are generated. I claim that passwords that are pronounceable strings like "SEN-SLES-GAR-BYG" are not that hard to remember. Maybe not fun to remember, but not hard. Giving the user some choice in the matter can make the procedure

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

more user-friendly. Some of the author's mnemonic devices could be used to remember nearly any random string if the user is clever enough.

I believe that the author has a valid complaint about how machine-generated passwords are administered on some systems. His complaints about the way LUDLOW is used are understandable. Better human engineering of password generators would be welcome. More information on guidelines for passwords is available in the Center's publication on password management, available from C4.

If one accepts the premise that password generation is a user responsibility, then this article has practical suggestions on how users can do a better job at meeting the responsibility. But I would challenge the author to come up with a better password generator which meets the Center's guidelines. The basic requirements are not hard to state and they allow for a wide range of creative solutions. Human engineering is important and the author has practical experience in using passwords. Since password generator programs are rarely exercised during the course of a day, they can be large, and very user-friendly.

[redacted] *C51*

P.L. 86-36

OUT OF THE INNER CIRCLE;
A Hacker's Guide to Computer Security
by Bill Landreth. Microsoft Press,
Bellevue Washington, 1985

Reviewed by: [redacted] *C212*
P.L. 86-36

This book is an excellent non-technical introduction to computer security for the lay person. In the first chapter the author describes a hypothetical attack on a corporate computer: a battle of wits between the hackers (who choose the time and place of their attack) and the operators (who wait, detect, and respond). The remaining chapters present a brief history of computers, a history of hacking, and an overview of computer security measures designed to limit hacking damage. These chapters are well organized and the material is clearly explained, so that even non-technical readers will be able to understand it easily. The book closes with an epilogue detailing Landreth's arrest and trial and an appendix giving his evaluation of some commercial computer security devices. I have some reservations about his evaluations, detailed below.

Landreth writes about computer security from personal experience as a hacker; his hobby was breaking into other people's computers. (That's not the only meaning of "hacker," and some people object to it, but Landreth used it and so

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

will I.) He started with a TRS-80 and an Apple II. It was with his Apple II that he discovered the challenge of understanding and controlling other computers through his own; this challenge appears to be the motive force for most of the incidents recounted in the book. Landreth describes how his increasing ability and reputation finally brought him into the "Inner Circle," an informal group of expert hackers who "met" electronically by leaving messages on the computers they had penetrated. It was their superior skill that finally ended Landreth's hacking career; they had penetrated some computers so regularly that they were discovered, traced, and arrested.

Landreth's hacking experience gives the book both its strength and its weakness. His knowledge and interest are reflected in the book's convincing detail, but they affect his objectivity. Successful hacking means using the computer in an unauthorized or abnormal way. (It isn't hacking if they let you in!) Most hackers learn a system's weaknesses by trial and error, usually by exploiting "bad" commands in the programming (those not intended or anticipated by the computer's designer). Landreth implies that few hackers intend harm and that most are harmless. I disagree. Unauthorized entry may destroy data or slow down the computer so much that real work can't get done. Hacking, therefore, is not a harmless pastime.

Another limitation of Landreth's personal approach is his lack of knowledge about the special problems inherent in military systems, such as susceptiblity to espionage. The anti-hacker standards set by Landreth are inadequate to protect sensitive information against professional espionage. Appropriate standards for "Trusted Systems" are described in the "Orange Book," the National Computer Security Center Trusted Computer System Evaluation Criteria. None of the systems penetrated by the Inner Circle meet the requirements even for C1, the lowest level of trust. Landreth also neglects the special problems of embedded computers in modern weapons systems.

Neither omission is a serious flaw in an introduction intended for the general public. But people facing professional espionage or managing embedded computers need more than this book; they need professional defense. □

EXTENDED HOURS

for

LEARNING CENTER #1 (U)

[ ] *E22*

Learning Center #1 (room 2C166, Operations Building #1) is operating on extended hours. The center is open Monday through Thursday, 0700 - 2200. Yes, that's 10 pm!

At the Center there are courses on cryptanalysis and other Sigint disciplines, computers, management, personal development, target studies, office skills, and other subjects. Many are overviews without exams, a good way to try something new.

A list of courses is published quarterly. For more information stop by or call 963-5899 (s) or 688-7922 (b).

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

COLLECTION MANAGEMENT

I PAST,

II PRESENT, *and*

III UNCERTAIN FUTURE (U)

[redacted] G53 P.L. 86-36

~~*This article is classified CONFIDENTIAL CCO in its entirety*~~

Am I a fireman on a diesel-driven collection system?

Am I a relic of the past without a future?

It's time for me to find a psychoanalyst to gain an understanding of my original Agency occupational specialty. For some years now, I've asked myself the following questions: "What is collection management, and why do we need collection managers in NSA?"

These questions are disturbing only because I am certified in this career field and without it I would be qualified only for staff and management positions. I want to believe, therefore, that a need exists for collection managers like me and that the Agency really depends on our work. This is where my schizophrenic problem begins; I want to believe in the need for collection managers, and at the same time, I can't find a real reason for us to exist, at least under our present job description.

In order to understand my problem, you must have at least a basic knowledge about why collection managers were first introduced into the Agency work force. My knowledge along this line is somewhat limited in that collection managers were already on the scene at NSA when I started in 1959. I understand from some old-timers who worked here before me that there were elements in the Agency named GENS (now A Group), ALLO (now G Group), ACOM (now B Group), COLL or COSA (now P5 and a little bit of every other office involved with collection activities), and still others. At that time, there was no Combined Cryptologic Program (CCP) and nearly every element within the Production organization operated as an independent agency.

You must also remember that the signal environment at that time was simple (Morse, voice, and some printer ... which by the way was considered to be an advanced signal type at that time). I can remember statements being made upon my arrival at NSA that Morse was on its way out and printer was going to be the way of the future and, by the way, how would we be able to cope with such technology?

Because there were so few types of signals available for NSA to exploit at that time, it was some person's bright idea that each production element should make its collection assets available for use by other production elements (mainly because signal types were somewhat common across element lines).

Thus, GENS, ACOM, and ALLO were instructed to send a representative to this new element (COSA or COLL) where they would perform as brokers for other elements tasking on their positions. Although the element was formed, the people remained attached to their supported organization, while the chief of the collection management shop was an independent manager.

This fact soon caused many problems, the ultimate result being the permanent reassignment of all detailed collection managers to the collection management element. Another factor was our lack of computer support as we know it today. All tasking records were maintained on 5x8 cards and a recap of this file was made (typed, proofread and mailed) every month. This file was considered the authority for all tasking, and each mission change was entered on the appropriate station/position

card as it was being forwarded to the collection site by message.

This whole process was performed by a number of typist/record keepers and collection managers performing what would be considered manual labor in today's computer world. A high percentage of positions remained tasked against a single entity (this was based on the collection site location); however, it was not impossible or unusual for several types of tasks to be assigned to a single position. A collection manager would review the tasking assigned to a station/position, look at the collection statistics received electrically from each station, and ultimately determine the best place to assign a new task to obtain the desired results.

Even at this time, most assignments were pre-directed by traffic analysts who for one reason or another (i.e. availability of linguists or on-site reporters, etc.) would tell the collection manager where the task was to be assigned. In such cases, the collection manager would ensure that the position was being manned in accordance with tasking requirements, and that traffic forwarding instructions were complete, that technical support (TEXTA) was on station, and that the new mission was not going to interfere with the task of another office.

Collection assets seemed to be plentiful and there were many more [redacted] sites around the world than there are today. All in all, our world at that time was simple with no real lack of resources. The Morse and non-Morse General Search efforts (i.e., constantly looking for new and/or unidentified signals) seemed to keep us up with what was happening in our simple world and there were people around willing to perform manual tasks.

To step through time, we remember the introduction of computers into NSA, the loss of many collection sites around the world, the many new signals that are continuing to surface, the trend to use more line-of-sight transmission systems, the lack of money, the introduction of sensitivities into our work environment, the construction of collection positions to intercept a single type of signal, communications security awareness on the part of our targets, and the changing political world of the past 25 years, all of which changes have greatly altered the role of a collection manager.

Today's collection manager is not determining where to assign a case for coverage. He has no effective evaluative tools to use in the performance of his job. The signals environment is so complex that he doesn't understand how to collect a signal or even to know what type of equipment is required in order to collect most of our sophisticated signals. He has little authority in either the current or planned collection world. Furthermore, he is uninformed about why a task is being assigned (i.e., what is the requirement). Because of this, the collection manager today is by and large a creature of the past: a rubber stamp for conveying tasks between a traffic analyst and a collector or a resource controlling authority; a record keeper for upper management who is unable to accurately respond to questions because he is not trained to interpret the data in his files; a person who is more often wrong than right when showing initiative.

Since the early days, collection management functions were returned to the analytic offices (late 60s and early 70s) and more recently moved again to a centralized organization center. I believe this again reflects a manager wanting something from a collection manager but not being able to specifically place his finger on the requirement. I believe we need to face up to the fact that we need very few collection managers (maybe only to perform collection management functions of systems [redacted] Certain of the traditional collection management tasks should be given to the traffic analyst, and a new career field should be developed for our leftover collection managers.

The new career field should include such things as being responsible for ensuring standardization when we task resources, knowing what resources are where (in accordance with the CCP and as it is in the real world), [redacted] making sure that our collection system is ready to meet future requirements, building some type of an evaluative process which informs the system when a position is not longer productive, etc.

I still believe that day-to-day collection management of items being assigned for coverage

EO 1.4.(c)
P.L. 86-36

is rightfully a responsibility of each analytic office. Furthermore, I believe that we need to have some focal point in NSA for working with non-SIGINT elements that have an impact upon our collection assets , and that we need to have an element involved with watching tomorrow's technology so that we are prepared for the future [redacted] Basically, the collection system must be controlled from three points, planning and budgeting, assets versus requirement priorities, and evaluation/feedback to the planning and budgeting system.

I'm not sure that I have communicated my problem with collection management and collection managers clearly. However, I feel better now that I have attempted to address it. I would like to think that somebody will read this, and just maybe there will be a review of this situation.

In the meantime, this is your collection management fireman working on a diesel collection management system, saying so long for now. I look forward to your help with my problem.

BULLETIN BOARD

NEW LAMPS FOR OLD (U)

~~(C-CCO)~~ The Division of Cryptologic History is working on several areas of our past and needs Agency files and documents for research. The areas of greatest concern right now are:

- [redacted]
- The Cuban Missile crisis;
- The Korean War;
- [redacted]
- The Vietnam War.

~~(C-CCO)~~ If you have documents of any type on these subjects (reports, correspondence, end product, codebooks, computer runs, etc.) that have been moldering in your desk or file cabinet or that may be in storage, please let us know. We are also seeking to interview people who personally participated in these events; sometimes oral history is the only way to record facts which do not show up in files. Upon the completion of these histories the documents will either be returned to you if they are part of active files, or incorporated into the NSA Archival system to make them available for historical and technical research. Call or write Tom Johnson, Chief, T542, SAB 2 Door #3, 972-2355 about materials, and Bob Farley, at the same address, about the oral history program.

~~(FOUO)~~ Materials pertaining to other events should be sent directly to the Cryptologic Archival Holding Area: [redacted] Chief, T541, SAB 2 Door #3, 972-2268.

CALLING ALL HACKERS ~~(FOUO)~~

~~(FOUO)~~ If you have had any non-work-related experience with computer "hacking" please share your knowledge with us. Success not essential, just experience. Non-attribution, non-retribution. Please contact Joe Merchant, Operations Security Manager, P1, 963-4652.

ATTENTION FRENCH LINGUISTS ~~(C-CCO)~~

~~(C-CCO)~~ Copies of *The FRANCOPHONEGLOS* with Supplement 1, dated 15 April 1978 and classified C-CCO, are being distributed again. To obtain a copy send your Name, Organization, Building, and Room number to: [redacted] P16, HQ 8A187. Mail orders only are accepted.

EXTENDED CHARACTER SETS (U)

~~(FOUO)~~ The National Data Standards Center advises that there are international standards for extending 7-bit and 8-bit character sets and for coding the escape function which invokes a new character set. The information should be of interest to persons concerned with data transmission as well as to linguists and programmers dealing with non-Latin alphabets. Particulars are described in NDSC Bulletin #6-86. For a copy write to [redacted] P13D, at their new location, FANX II, A2B03.

DOCID: 4019706

SENIOR PROFESSIONAL CAREER PROGRAM (GALAXY) Status Report

At the request of the Director, the GALAXY Steering Group undertook a review of the GALAXY Program and program objectives. The group documented its conclusions in a revised regulation which was circulated to the members of the Board of Directors for their review prior to a presentation to the Director. The decisions resulting from this process are listed below.

CHANGE 1 - CONCEPT

Personal career development is a shared responsibility of the individual and management. A centralized program such as GALAXY should not be directive, but should provide services to facilitate the attainment of objectives established by the individual and management.

CHANGE 2 - NAME

The program will be known as the NSA/CSS Senior Professional Career Program (SPCP). The change from the GALAXY name was recommended because initial intentions for the GALAXY Program created expectations and perceptions that are no longer valid but continue to be associated with the name GALAXY. The term "mid-level" has also been dropped because it is an inaccurate description in many respects. The term "senior professional" corresponds to the Occupational Specialty Titles for GG13-15 level jobs, e.g., Senior Cryptanalyst, Senior Electrical Engineer, etc. The GALAXY name will continue to be used for the data base.

CHANGE 3 - REGULATION

NSA/CSS Reg. No. 32-9, dated 11 April 1984, NSA/CSS Mid-Level Career Management Program (GALAXY), is superseded by a new regulation entitled NSA/CSS Senior Professional Career Program, dated 7 May 1986. In addition, a Personnel Management Manual (PMM) Chapter ~~410~~ 430 has been drafted and will be published shortly.

CHANGE 4 - ADVERTISING

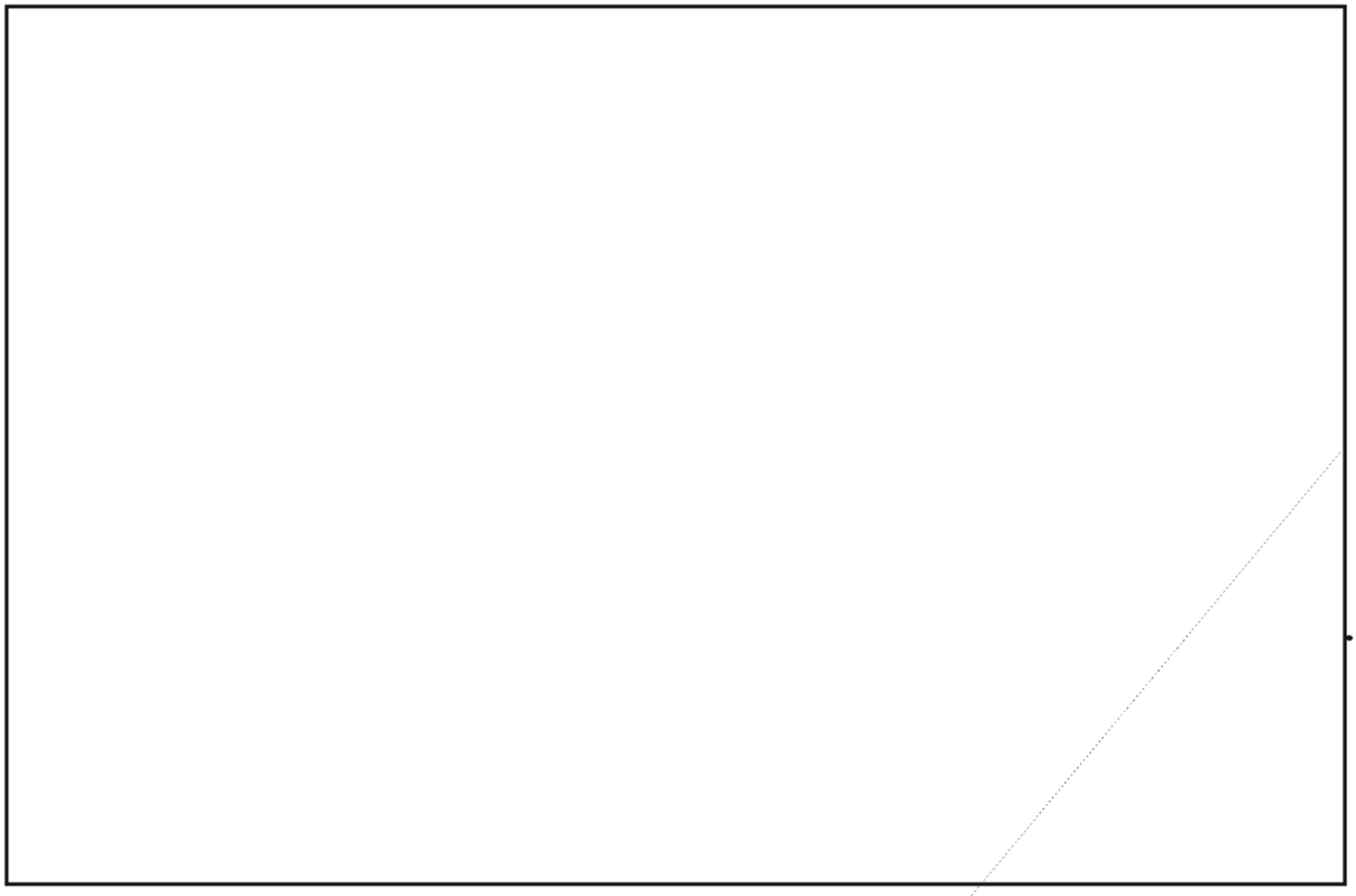
The new regulation establishes a requirement for advertising vacancies to be filled at Headquarters when the selection official desires to consider candidates from outside his/her organization. Managers can rotate personnel within their own organizations without advertising, but the job must be advertised before a cross-organizational move is approved.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

UNCHANGED

The program will continue to apply to civilian personnel at the GG13-15 level. Emphasis on field support and reassimilation is reenforced. Services will continue along present lines: maintaining data bases; publicizing vacancies; searching for candidates; coordinating selection; release and approvals; acting as focal point for field staffing and reassimilation for GG13-15 jobs and people; providing guidance and information on career opportunities and career planning.



P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

QUESTIONNAIRE #1 UPDATE

The GALAXY data base is used constantly to search for candidates to meet job requirements. You need to be as well represented in that database as possible. Please take a fresh look at your answers to Questionnaire #1. We urge you to give particular attention to secondary experience. We find that many people are conservative about claiming experience other than primary responsibilities, while requirements for a search are usually stated in fairly comprehensive terms indicating auxiliary skills and knowledges desired. Don't sell yourself short on secondary interests and experience. Please send us your changes using the attached data record.

QUESTIONNAIRE #2 UPDATE

We are preparing a reissue of Questionnaire #2 which should be more "user friendly". The answer sheets have been revised and have been printed as a standard NSA form (P1201) available in supply rooms. More about this when the new Questionnaire books are ready.

POSITION ANNOUNCEMENTS

With the new requirement for advertising, we may modify our format of the Position Announcements to some extent, but we will continue to use the following guidelines: 1) we run an ad until a job is filled or until requested to delete; 2) we do not set closing dates unless requested by the selecting official; 3) generally a new job runs two issues as a narrative and then reverts to a line item if not filled; 4) We are unable to publish in unclassified form. Therefore, the trend is toward COMINT CHANNELS so we can include more descriptive information; 5) We publish at least every 2 weeks; printing and distribution take 2 weeks; 6) 300 copies of each issue are distributed in advance to Integrated Personnel Activities at the time the document goes to press.

CAREER PATHING

We are currently working with a contractor, Human Systems Technology, to develop a model for career pathing in several fields pertaining to the procurement process (ILSM, Acquisition Specialist, Contracting Officer, Business Manager). Our basic approach is to meet with representatives of these fields to document examples of career evolution, define competencies, and identify the cross-overs which have been or should be possible. The contract will be completed in June. The pathing model will then be evaluated for applicability to other career areas.

~~FOR OFFICIAL USE ONLY~~

~~CONFIDENTIAL~~

P.L. 86-36

A NOTE FROM THE PROGRAM DIRECTOR:

(U) With a couple of years' perspective on the evolving GALAXY/SPCP program, there are two points I would like to emphasize:

~~(C)~~ First, individual initiative is the key ingredient to accomplishing a job change. Probably the greatest disservice of the GALAXY Program was to suggest to people that the Program would do it for them. We have found this is too much like playing the lottery. There are some winners, but with [redacted] GG13-15s there are a lot of people who never get called. On the other hand, a high percentage of people who want to move and take the initiative to work with us and with their supervisors are able to find a suitable new job within a six-month period. It takes persistence and patience, talking with a number of people, and waiting for selection officials to make decisions. It's a process that will test one's resolve, but the determined accomplish their objectives.

(U) Second, I consider the principal justification for our program to be to help everyone know the options. The Agency is just too large for individuals and managers to know all the posibilities. This lack of information inspires both hope and frustration. There is a sense that the "right job" or "right person" is out there somewhere if the decision-maker could only know all that is available. To a considerable extent these are not false hopes, and a brokerage service of some kind is really needed to help individuals and managers attain their objectives. We are continuing to develop all the means we can to meet information needs--advertising jobs, advertising people, candidate searches, career counseling and advice, career pathing guidance, etc. We welcome your suggestions as to what would be most helpful to you.

[redacted]

P.L. 86-36

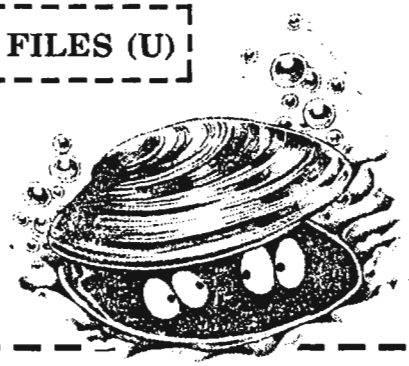
~~CONFIDENTIAL~~

DOCID: 4019706

P.L. 86-36

ASTW SHELLS TO BACK UP FILES (U)

[redacted] G743



In our office we have large number of text and data files on ASTWs. For back-up, we generally copy each file kept on the hard disk to at least one floppy disk as well.

Yesterday afternoon one of the analysts on my team, tired of typing **doswrite -afilename filename** for each file, asked if there weren't an easier way to dump multiple files to the floppy disks. After a little thought, the two of us wrote two shells.

• ① The shell **writeall** will write a list of files from the current PC/IX directory to the DOS floppy. The shell **writeall** is as follows:

```
while test $1
   do
         echo "writing" $1
         doswrite -a $1 $1
         shift
   done
```

To use **writeall,** enter one of the following commands:

```
writeall filename1 filename2 ...
writeall *
writeall filename.with.global.
   characters
```

• ② The shell **writesub** will write all files, except dot files, from a subdirectory of the current PC/IX directory to the DOS floppy. The shell **writesub** is as follows:

```
cd $1
writeall *
cd ..
```

To use **writesub** enter the command followed by the name of the subdirectory to be backed up:

```
writesub mysubdir
```

P.L. 86-36

Comment from [redacted]
Computer Science Editor:

This shell is useful when there is a need to write several files to floppy in DOS format, especially when several similarly named files can be specified with a wildcard.

As to the reason stated for needing this shell, however, I wonder why you don't simply use incremental dumps as described in the PC/IX Operations Handbook on pp 41-43. This will automatically copy every file that has been created or changed since the last dump (that way you don't run the risk of accidentally overlooking an important file) and back up all users of a given ASTW in a single step. Also, it runs faster than **doswrite.**

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

CONFERENCE REPORT

CRYPTO AT GLOBECOM 84

P.L. 86-36

P.L. 86-36

P13

(U) M/A COM exhibited their new Videocipher demodulator, designed for Home Box Office satellite TV relay. The company hopes that their system will become a de facto national and international standard.

(U) The encryption uses "hard" digital encryption of the audio channels and control information by the DES algorithm, and "soft" analog encryption of the lines of the video picture according to a DES key stream.

(U) The general scheme of "hard" encryption of the audio channel, with "soft" encryption of the video picture was specified by HBO in 1981 and presented at an EASCON meeting. [See "Video Encryption: A Report from EASTCOM 81" in the January 1982 issue of CRYPTOLOG.] The reason for the "soft" video encryption is to keep the bandwidth and format of the signal within the conventional video transmission bandwidth. The audio portion is "hard" encrypted because it is feasible to do it, and most of the program content is in the audio track. It was expected in 1981 that the audio encryption might be by DES, but a single 64,000 bps channels was under consideration. A surprising feature of the Videocipher is that the digital channel is at the megabit rate, with DES protection.

The Security of Videocipher

(U) If Videocipher is adopted as an international encryption system, which is likely since the basic scheme can be adapted to PAL or SECAM, it may be possible to limit use of DES, but there are other secure algorithms that also present difficulties.

Implications for NSA

(U) In addition to the entertainment broadcast application, the Videocipher unit can also be used for video teleconferencing --- a growing market. If it catches on for teleconferencing, the sales and dissemination of the technology could grow considerably.

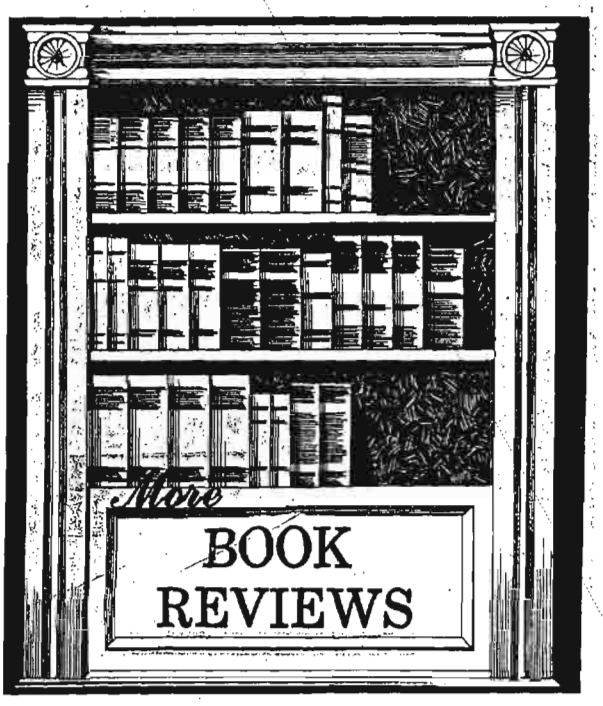
Sorry about that!

Bugs in the new software leave widows and orphans bereft, dangle parentheses and apostrophes, and cause other violations to convention.

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4019706 EO 1.4.(c) P.L. 86-36



P.L. 86-36

SECRECY, AUTHENTICATION, AND PUBLIC KEY SYSTEMS by Ralph C. Merkle
UMI (University Microfilms International)
Research Press, Ann Arbor (c1982, 1979)

Reviewed by [redacted] *P12*

~~(FOUO)~~ Let us make it clear that this is not a book in the usual sense but a revision of the author's doctoral dissertation written under the guidance of Martin Hellman at Stanford University. As one would expect, it is an immature work showing the narrow research of one student. It is not a survey of the field as the title suggests. No library need acquire this tract.

~~(C-CCO)~~ Merkle participated in the discovery, by Hellman and his many students, of what has become known to the academic world as public-key cryptography. (Actually, these systems were first conceived at GCHQ by James Ellis in 1970.) Public-key cryptography allows "secure" communications between subscribers to a large net though they have had no previous knowledge of each other and share no key in the conventional sense. Merkle's original scheme, based on solving "puzzles," as he describes it, is "primarily of pedagogical and historical interest."

~~(C-CCO)~~ The opening line of chapter 4 states incorrectly, "This chapter describes the first public key system ever developed." Of course Merkle could not have known that, several years earlier, such systems had already been proposed by Malcolm Williamson and by Cliff Cocks at GCHQ.

~~(S-CCO)~~ Perhaps it is a normal human failing to be blindly proud of one's own ideas. The idea which Merkle and Hellman originated is that of public-key systems based on the "knapsack" problem. Their design has been discredited on the outside as the result of clever work of Adi Shamir, Ernie Brickell, Andy Odlyzko, and Jeff Lagarias. [redacted] Merkle offered a prize of $100 to anyone who could solve the Merkle-Hellman knapsack; this prize was paid to Shamir in 1982. Then Merkle risked $1,000 on the security of the "iterated" Merkle-Hellman knapsack. This too was lost, to Brickell; the work of Odlyzko and Lagarias also suffices to demonstrate the unworthiness of the system.

~~(C-CCO)~~ Merkle has not entirely missed the target. The opening sentence of chapter 1 is spot on: "Cryptography is a fascinating subject, even more so today than in the past." But he alludes to the S-boxes (unique, so far as I know, to the Data Encryption Standard) as "found in many modern cryptographic functions" (page 52). And in comparing his knapsack to the sturdy public-key system developed outside by Ron Rivest, Adi Shamir, and Len Adleman, (this is the system originally proposed by Cliff Cocks), he states (p. 48): "the trapdoor knapsack appears less likely to possess a chink in its armor."

~~(C-CCO)~~ One of Merkle's ideas is that he has created an "NP-complete conventional cipher" (the title of his chapter 8). In fact his thinking is confused in several directions. Let us set the scene. A knapsack is a set $a_1,a_2,...,a_n$ of n (large) positive integers, known to everyone. The parameter n should be chosen large enough to prevent an exhaustive analysis of the 2^n

possible cryptovariables but small enough to allow timely operation of the encipherment scheme. Instead of the usual "trapdoor" use of the knapsack, Merkle intends that the sender and the receiver share key, one of the 2^n binary n-vectors, which they use to select some of the a_i which add (as integers, not mod 2) to provide a key. That is,

$$K = \sum_{i=1}^{n} x_i a_i \text{ , an integer sum.}$$

~~(FOUO)~~ Let's think about this a little. We're intending to use this key to encipher a binary stream of data, with the usual equation $C = P \oplus K$, so that the plaintext can be recovered via $P = C \oplus K$. That means that we need an arbitrarily long key stream! Yes, Merkle is ready for us. He has in mind that the knapsack elements a_i are infinite!

~~(FOUO)~~ Aha, you think -- a storage problem: where shall I retain these a_i? Never fear, that's not necessary. Instead, the sender will generate and transmit the a_i bit-by-bit! That is, in some (unspecified, but clearly essential for security) way the sender generates the n streams (starting, of course with the least significant bits) and with every bit of cipher must transmit an additional n bits of the knapsack components. Talk about data expansion!

~~(FOUO)~~ Now Merkle makes a swipe at establishing NP-completeness of his algorithm. But it's hopeless: complexity theory just cannot cope with components of infinite length. Furthermore he admits that his "proof" fails for another reason. The NP-completeness of the knapsack problem deals with the following decision problem: given the set of knapsack weights (the a_i) and an integer B, determine whether or not there is an n-long binary vector $x = (x_1, x_2, \ldots, x_n)$ such that

$$B = \sum_{i=1}^{n} x_i a_i$$

~~(FOUO)~~ The problem we're faced with as cryptanalysts is, instead, the corresponding search problem: given B, and knowing that an x exists, find x. Merkle says, "From a cryptographer's point of view there is not much difference between these two problems." It is just such difficulties that make contemporary complexity theory generally inapplicable to cryptology.

~~(FOUO)~~ Knapsacks are not appropriate vehicles for solving the authentication problem, in which secrecy of the contents is not an issue but the recipient requires assurance of the source of the message. Typically the message m is formed and then the sender A uses some function F (which is publicly known) to "sign" the message. One condition is that A (only) knows the inverse function F^{-1}: Given m, only A can find x such that $F(x) = m$. Now A calculates the signature x and transmits x only, along with a statement that it is he who has sent the message. Everyone now has the facility to read the message $F(x) = m$. No one else knows F^{-1} so no one else could have found the transmitted x.

(U) Because knapsacks typically have a very small image space, inverses of arbitrary elements m are most unlikely to exist. That is, for a randomly chosen m, it is very unlikely that a binary vector x can be found such that

$$\sum x_i a_i = m$$

so knapsack systems are not useful for authentication.

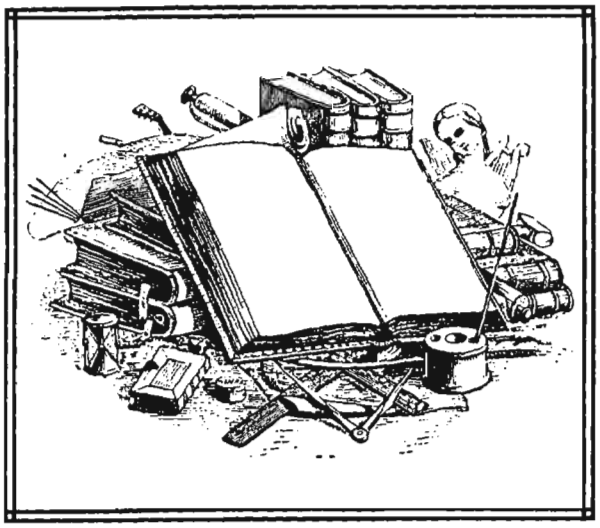
(U) Recognizing this deficiency, Merkle has written a chapter entitled, "A Certified Digital Signature." His design is "tree authentication," which is expensive, slow, and allows for the selection of only a small number of messages. Tree authentication appears again in the longest chapter, on "protocols for public-key cryptosystems," to no better effect. This chapter is not without merit: it alerts the unwary to the many pitfalls of designing secure protocols.

~~(S-CCO)~~ That Merkle fails to construct a satisfactory protocol is no disgrace: many skilled researchers have had no more success. The best work I've seen on this thorny problem has been done by [redacted] anyone familiar with their ideas will find Merkle's discussion very pale. But I particularly liked one remark of his: in the doubtful world of thrust and counterthrust, of

masquerade and tampering, the message "My secret key has been compromised" should always be accepted as a valid message.

(U) No book on cryptology is complete without mention of the Data Encryption Standard. Merkle has a novel approach to DES. He shows how to simulate a k-input m-output S-box by a knapsack with $2^k + k + m$ components. By assembling components he is now able to argue that a general algorithm which could solve a 10000-component knapsack could be used to solve DES. In a later chapter he discusses "the security of multiple encryption" of DES.

~~(FOUO)~~ Our criticism of this book is not intended as a criticism of the author. It would have been surprising indeed if such a young and inexperienced student had made an important contribution. He has not. Cryptography remains a fascinating subject, yes, but also a decidedly difficult one. □



THE COMPUTATION OF STYLE: An Introduction to Statistics for Students of Literature and Humanities. by Anthony Kenny Pergamon Press, 1982

Reviewed by [redacted] *P12/G422*

(U) Stylometry is the use of statistics in literary analysis. *The Computation of Style* is not and does not claim to be an introduction to stylometry, but it provides enough stylometric anecdotes to whet the reader's interest, such as its use in determining the authorship of certain of *The Federalist Papers*.

(U) Rather, the book intends to be an elementary introduction to statistics for those who wish to make use of statistical techniques in the study of literature. In this, the book succeeds fairly well, although a good deal of mental agility is demanded of the reader. (For example, the term "unimodal" is first used, without definition, several pages after "bimodal" is defined.)

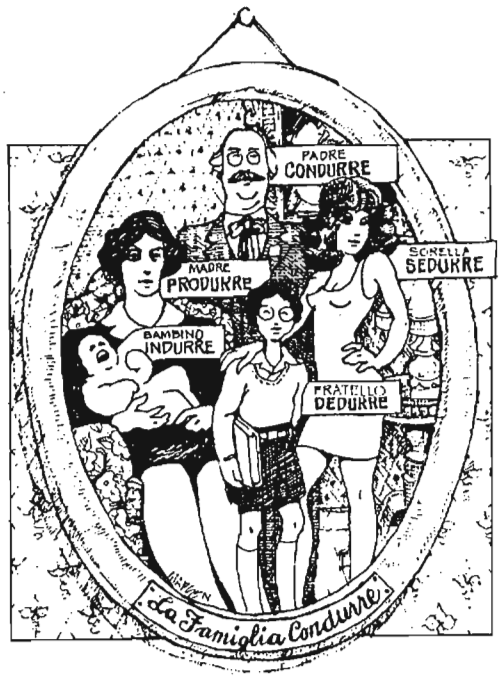
(U) The book is thoroughly British in orientation, which the American reader might find refreshing, although certain analogies such as the relationship of [highway] M6 to Manchester may be unhelpful. Passages excerpted for literary analysis are themselves a delight to read, such as two accounts of the murder of Richard III's nephews, one of which uses "the" more than twice as often as the other. The "distinctiveness ratio" could in principle be used to show that one of the authors is more likely than the other to have written a passage of unknown authorship.

(U) Most of the concepts present in the book are used to a greater or lesser degree by the cryptanalyst, such as chi-square, binomial and normal distributions, standard deviation, standard errors, significance testing, and sampling, to give only a partial listing. The cryptanalyst who wishes to review such concepts or approach them from a fresh vantage point would do well to consider this book.

(U) The author correctly states in the preface that a linguist with "a rusty memory of junior school arithmetic and algebra" should be able to follow the ideas of the book and perform the calculations needed to solve the examples. Practical applications of the techniques require the use of a calculator, or, preferably, a computer and therefore the ability to program a computer. □

P.L. 86-36

DOCID: 4019706



Drawing from Chapter 5
Verbs and Their Families: A First Approximation

P.L. 86-36

ITALIAN FOR EDUCATED GUESSERS: Shortcuts to the Language. by C. Peter Rosenbaum, M.D. Forza Press, Menlo Park, CA, 1985, $12.00. [PC 1112 .R6]

Reviewed by [redacted] *P16*

~~(S-CCO)~~ A fun book on language with short cuts for educated guessers? That's for us, the linguists at NSA! With this book (and a conventional grammar) an experienced operational linguist or cryptolinguist can slide into Italian from French or Spanish, or make the leap from long-forgotten Latin.

(U) It's an unusual size for a language book, 8 1/2" x11" x5/8" , with an appealing cover that invites you to pick up the book and peruse it. As you open it you notice that it has an attractive layout and a good "hand" -- cream-color high-quality paper that is erasable, which is a good thing, as it is a workbook. Margins are wide, and there's room for notes in the well-spaced text. But it is also a readable book that you can curl up with. And chortle over. You have to restrain yourself from interrupting your co-workers with "Look at this!"

(U) Each chapter starts with a humorous sketch illustrating the topic. (My favorite is shown on the left.) The information is logically presented, with an air of joyous discovery. Imagine coming upon "Regular Irregularities" *and* "Irregular Irregularities"! And some captions evoke operatic arias: "Unfaithful Cognates." "Unvarying Feminines."

(U) What makes this book rare and wonderful is the focus on semantics. The author takes you on a guided tour of syntax and grammar and points out the relationship between structure and meaning. This kind of analysis usually is the preserve of hard-core linguists. And the author presents the clearest exposition of sequence of tenses that I can recall.

~~(S-CCO)~~ We could have used a Spanish equivalent of this book when Cuba became an important target right after the missile crisis. There were very few Spanish linguists on board then, and even fewer lexicons and other language aids in Spanish. We made do at first with experienced French and Italian linguists who shared the few Spanish grammars and used French and Italian dictionaries. These linguists were able to walk in on the structure, and fortunately, most were also cryptolinguists and so were usually successful in finding an appropriate rendering by on-the-hoof "bookbreaking." But translating at one remove from a related language is fraught with peril. False friends abound between related languages. A special usefulness of this book is the tidy lists, with explications, of faithful, quasi, and unfaithful cognates.

(U) Dr. Rosenbaum, a professor of psychiatry who claims not to be a linguist, modestly assesses his labor of love as a supplement to a standard grammar for persons who have completed one semester of college Italian, and suggests that it might be "particularly useful for people who will be spending time in Italy." By the time you've worked through two fun-filled chapters, you find yourself *planning* a trip to Italy, just to try out your do-it-yourself Italian! □

DOCID: 4019706

To the Editor:

~~(FOUO)~~ One purpose of CRYPTOLOG is to stimulate controversy. On that basis alone, the article on ODYSSEY/CAMS [May-Jul 1986] was worth publishing. Is there anyone out there critical enough (and aware enough of its shortcomings) to critique the process?

[redacted]

~~(C-CCO)~~ Also, I consider dubious a process which does not include an interactive editing process very early in the game.

[redacted]

It would be interesting to get the reactions of the cryptanalysts who use ODYSSEY/CAMS.

'A Retiring Cryptanalyst'

To the Editor:

~~(C-CCO)~~ The ODYSSEY/CAMS article [May-Jul 1986] is both fascinating and scary. The success of this procedure is obviously directly dependent upon the quality of the original data base. Therefore, it behooves the prospective user to either clean up the data base (interactively) first, or to make sure that the data loss occasioned by this procedure is acceptable. Users who do neither should not be surprised if the cryptosystem doesn't read when it should.

[redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~(C-CCO)~~ There is no question that automation is the way to go. But it seems to this cryptanalyst that some of the procedures should be carefully evaluated before ODYSSEY/CAMS becomes the universal processing method. Instead, the designers should work with analysts in the operational areas to evaluate individual needs and to develop better initial processing procedures.

~~(C-CCO)~~ Certainly, any data base should be quickly scanned for identifiable/exploitable items which could be extracted at once. But there must always be provision for extensive cryptanalysis on resistant systems and for diagnosis, even in a paperless environment. This might mean making many printouts, or even resorting to cross-section paper and consulting the the original raw traffic. (Conversely, cryptanalysts who have worked exclusively in a paper-and-pencil mode should try mechanizing some of their efforts.)

'An Old Timer'

EO 1.4.(c)
P.L. 86-36

To the Editor:

~~(S-CCO)~~ I believe that Mr. Hopper's idea for organizing a workforce for C3 analysis [May-Jul 86] is right on target.

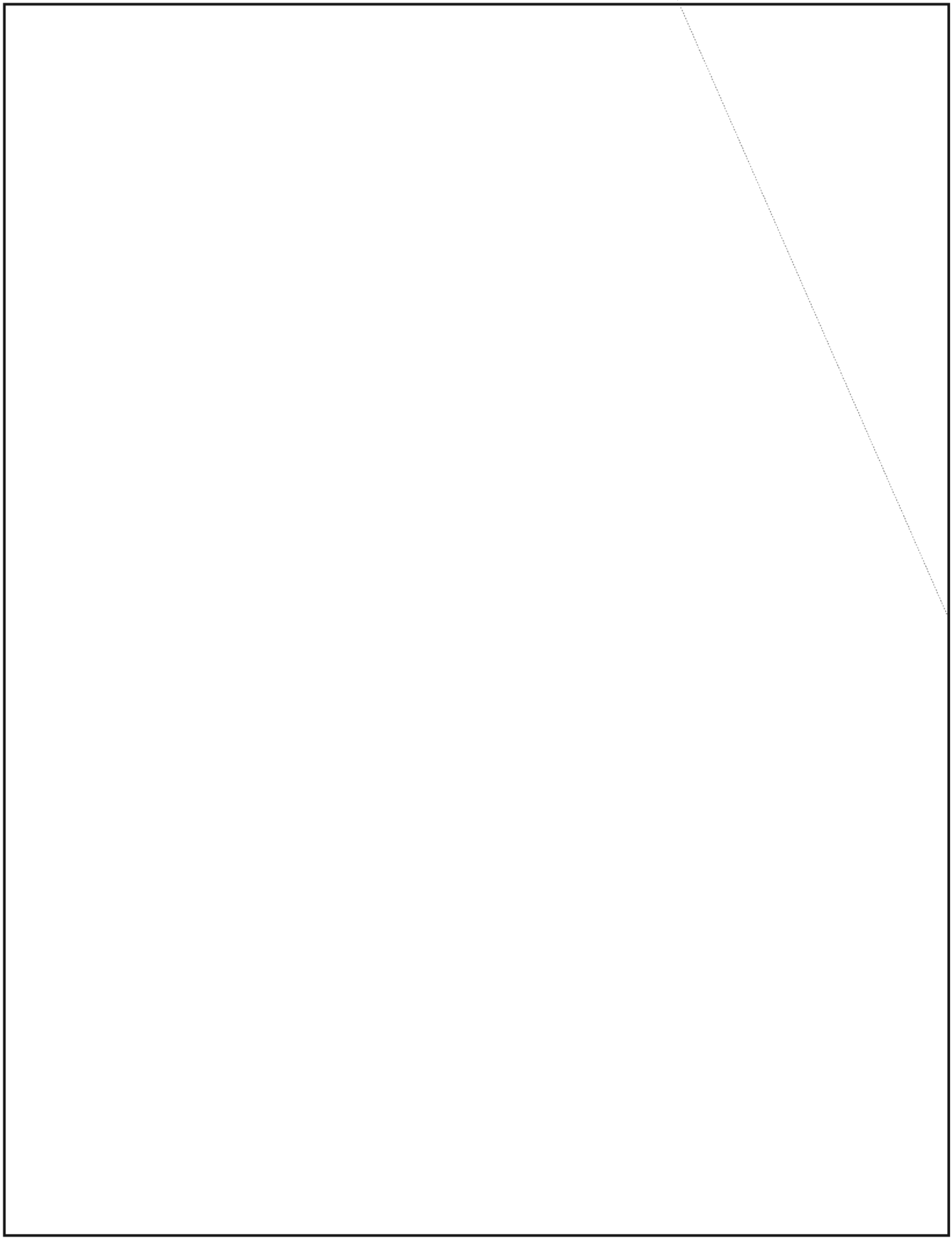
P0411

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4019706

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

~~CONFIDENTIAL~~

~~CONFIDENTIAL * HVCCO * NO CONTRACT~~

P.L. 86-36

~~*The following letter is classified FOUO in its entirety.*~~

To the Editor:

A short time ago I received a telephone call from an exasperated analyst in the CIA. She was interested in a report which had just been issued by NSA, but, after several calls to B and G Group personnel, she had been unable to locate the author, or even the organization to which the author was assigned. The subject of the report touched on the problem which I work, and so she had been directed to me for assistance.

Her description of the report revealed that it was a G Group product. After answering some of the analyst's questions and giving her references to two additional reports (one a CIA product she had not seen) pertaining to the subject in which she was interested, I contacted

~~CONFIDENTIAL~~

~~HANDLE VIA COMINT CHANNELS ONLY * NO CONTRACT~~

DOCID: 4019706

G05 and eventually got the name and telephone number of the author for her.

In all it took the CIA analyst and me seven telephone calls and perhaps a couple of hours to locate the author. All that time and effort could have been saved by the simple procedure of including the author's name and telephone number on the report.

In 1978 I published an article in CRYPTOLOG calling for by-lines listing authors' names and telephone numbers on NSA reports, something that sister agencies commonly do. I suggested that analysts naturally will do their very best if they know their names will appear on their product, and that the psychic income of seeing one's name attached to one's work is no small incentive to excellence.

A senior official responded that by-lines are not acceptable because of the need to maintain anonymity and because "two or more analysts often contribute to a report." My view is that anonymity can be a means of avoiding responsibility and that there generally is enough blank space preceding a report for the names of more than one analyst.

At any rate, nothing was done. However, the recent incident I referred to is common, and demonstrates again the need to reconsider by-lines to make it easier for our internal and external customers to get back to the originators.

While I believe that by-lines is the best answer, at the very least we should list a telephone number and the issuing organization's designator where a customer can contact the author. That simple procedure could save hours of unnecessary searching every year.

[redacted]

P.L. 86-36

From the Editor

IN ANSWER TO YOUR QUESTIONS

§ There are still <u>two</u> general classified periodicals being published in the Agency. **CRYPTOLOG**, the one you are reading now, is an informal monthly (bimonthly since the cuts) sponsored by DDO and published under the auspices of P1 for analysts in, or concerned with, Operations. It superseded four publications: *KEYWORD, DRAGON SEED, QRL, and COMMAND.* **The CRYPTOLOGIC QUARTERLY** (CQ), published by T54, is a formal Agency-wide vehicle for technical articles in all disciplines. It superseded two publications: *The NSA Technical Journal,* and *The Cryptologic SPECTRUM.* The editor of **CQ** is [redacted] T541, SAB 2, Door 3, 972-2355.

P.L. 86-36

§ Results of the Readers' Survey will be published in the next issue. We're allowing time for responses from the field.

§ More on OUT OF MY DEPTH #4 next time. Some readers wanted more of a challenge, so we obliged. But it's much too difficult.

§ Beginning with this issue CRYPTOLOG will be the new standard size, 8½ x 11.

Readers are invited to comment on letters and articles published in CRYPTOLOG and on other subjects of general interest.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

A PRIVATE GERMAN CIPHER OF WW I

Contributed by [redacted] *A204*

FELD=POST

HORNIST MART. WIRTH

7. INF. REGT. 3. KOMP.

1. ERS. BATL. BAYREUTH

STAMMBACH, DEN 24. MAI 1915

632B29 719T38!

B38.G2ST298.G18Z.G5T

71CH.H15S2G2K47728.S38D

V48.N252719KT.B3S.H237

2.K6SS2.G2F1H928.B38

H25T2.G18Z.A5FG292GT

61SS2.92CHT.B16D.2TW1S

V48.D39.H4̈928.4D29

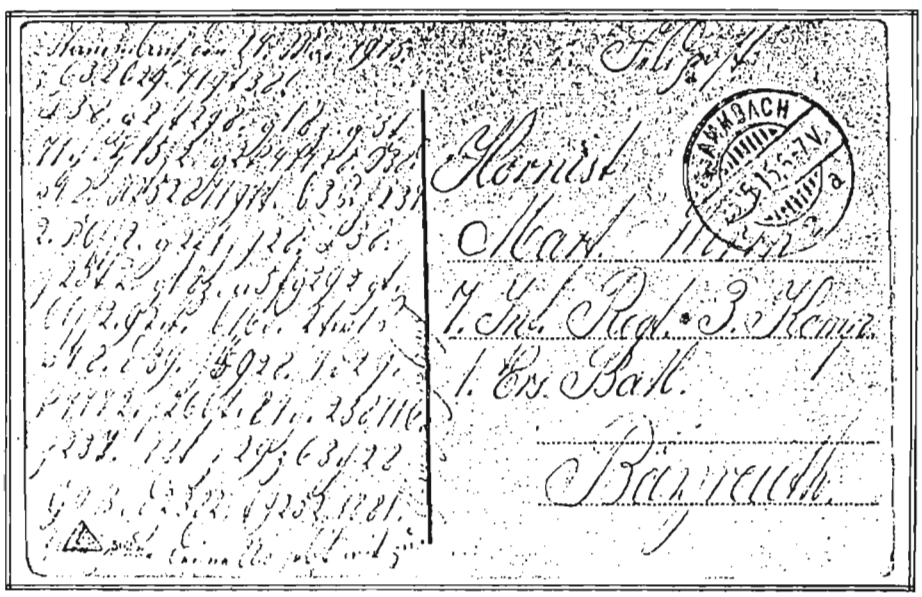
K4772.S26BST.84CH.238716.

H237.73T.H29Z63CH28

G9ß.D2382.T9252.1881

HABE HEUTE DEINE UHR SEBST MIT

ZUM UHRMACHER GEBRACHT



~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

[From]

ABS(ENDER) HORNIST WIRTH

1. ERS(ATZ) BAT(AI)L(LION)

7. R(E)G(IMEN)T 3. KOMP(ANIE)

BAYREUTH FELD=POST

AN
FRAU ANNA WIRTH
IN STAMMBACH
HS. NO. 83 OBF

BAYREUTH, DEN 23.1.1916

632B2.1881.

D238.W29T2S.KÏ9TCH28

73T.F925D2.29H16T28

B23.58S.3ST.D1SV2TT29

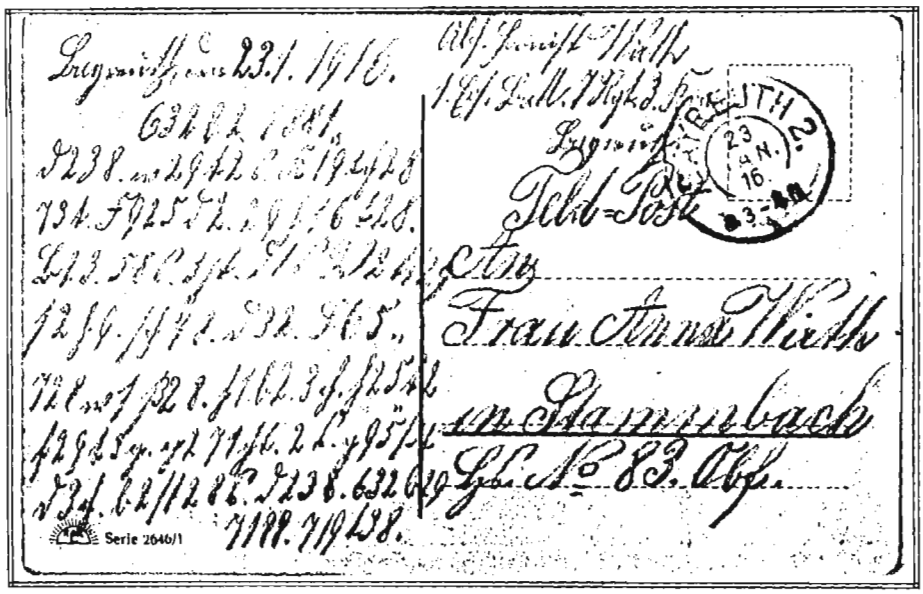
S2H9.SCH4̈8.D32.BG5

72W1SS28.H1B2.3CH.H25T2

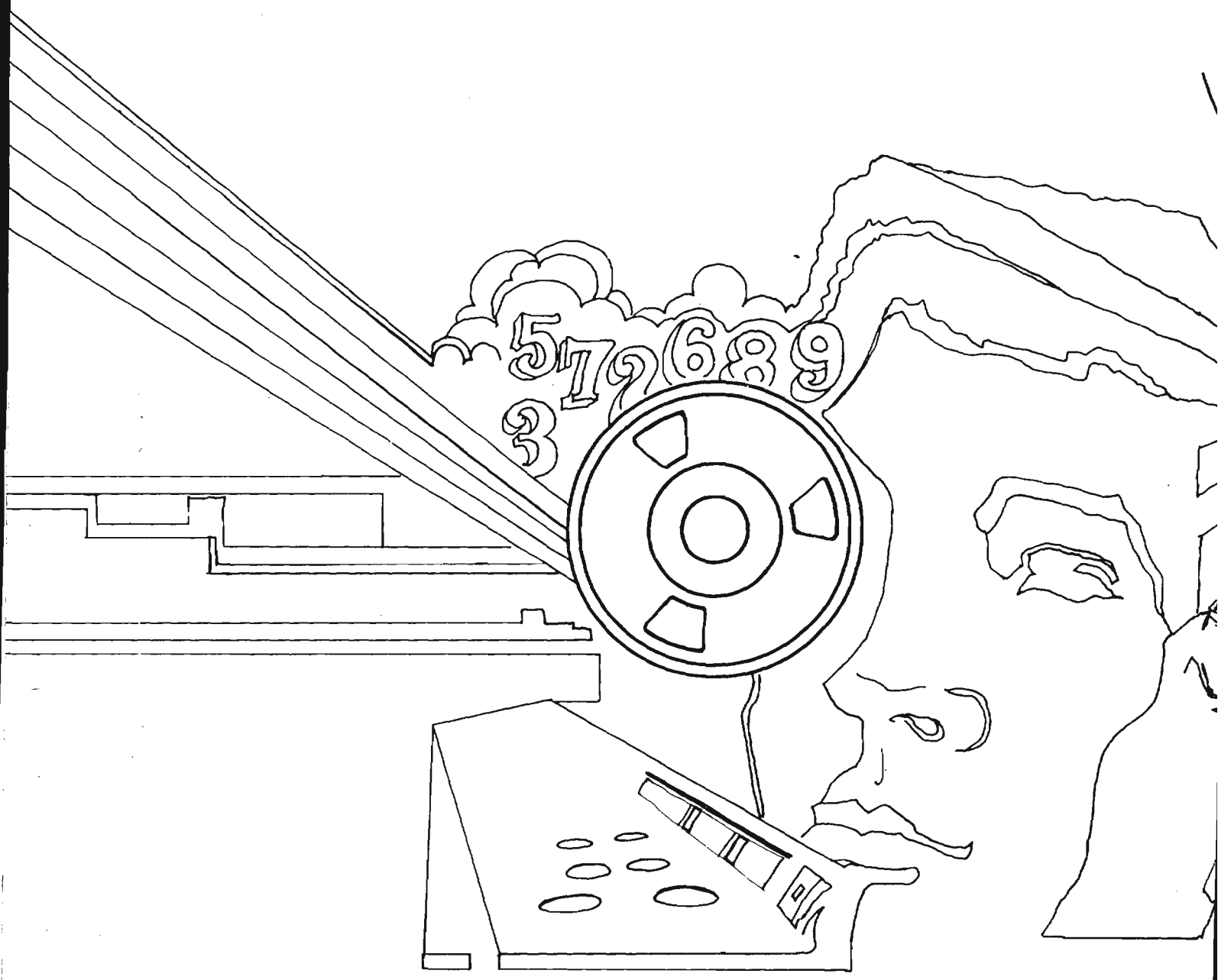
F29T3G.G271CHT.2S.G9̈5SST

D3CH.B2ST28S.D238.G32B29

7188.719T38



~~FOR OFFICIAL USE ONLY~~



~~NOCONTRACT~~

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

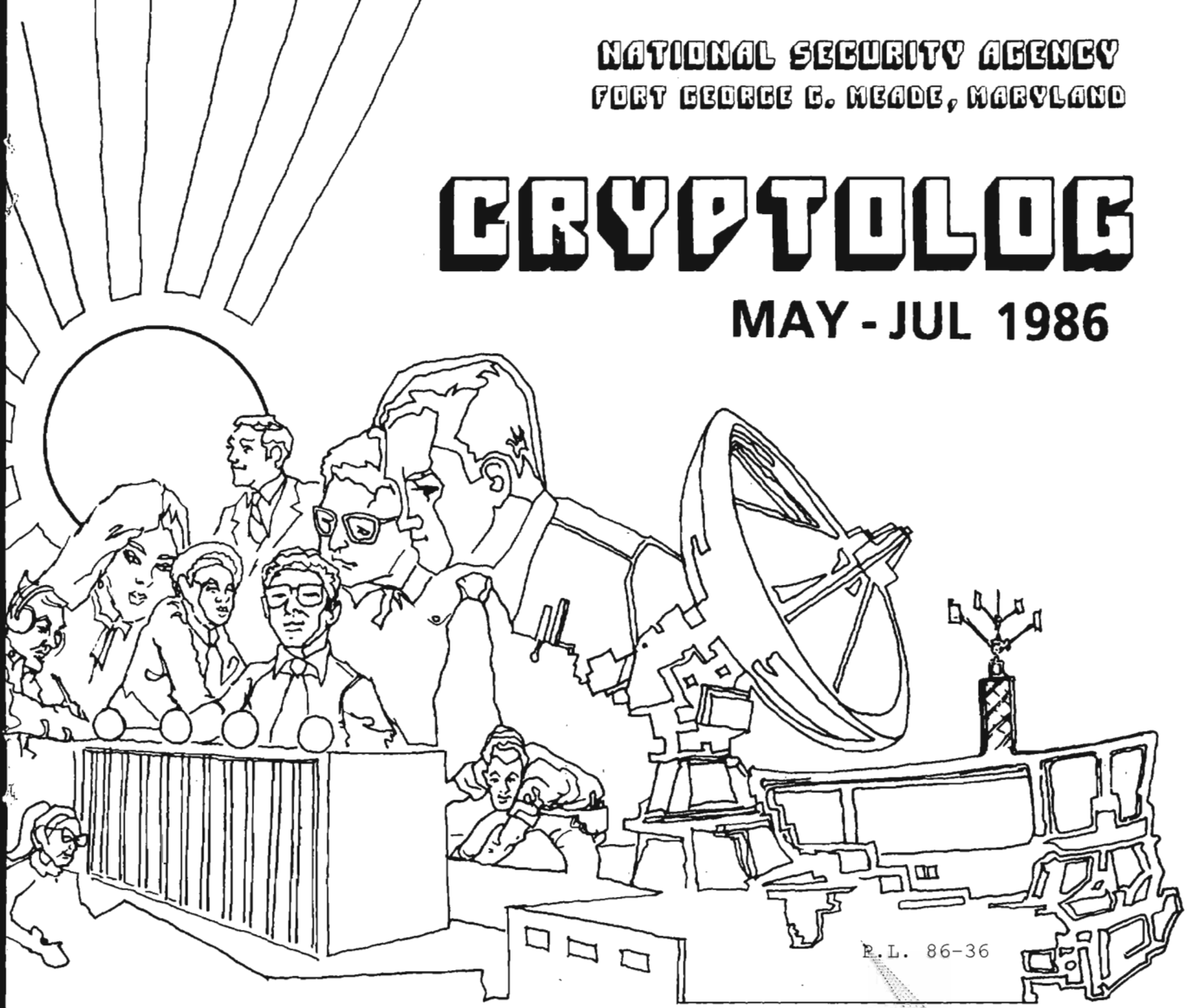
DOCID: 4019705

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MAY - JUL 1986



ODYSSEY (U) . . . . . [redacted] 1
BULLETIN BOARD (U) 6
ORGANIZING FOR EFFECTIVE C3 ANALYSIS (U) . . . [redacted] . . 7
A LINGUIST MEETS THE ASTW (U). . . . . [redacted] . . .10
AI AT NSA (U). . . . . [redacted] . . .12
PRESERVING VALUABLE NSA/CSS PAPER RECORDS (U). [redacted] . . .14
TEAM BUILDING (U). . . . . [redacted] . . .18
USER-FRIENDLY PASSWORDS (U). . . . . [redacted] .22
ERRATUM (U). 25
LETTERS (U). 26
OUT OF MY DEPTH #4 (U) . . . . . WES 28
READERS' SURVEY.(U). 29

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~NOT RELEASABLE TO CONTRACTORS~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

DOCID: 4019705

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XIII, Nos. 5-7 ..... May-July 1986

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Collection ..... (963-5877)
Computer Security ..... (968-8141)
Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-6424)
Cryptolinguistics ..... (963-1596)
Index ..... (963-5292)
Information Science ..... (963-1145)
Intelligence Research ..... (963-3095)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (963-4191)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-5734)

Illustrators ..... (963-3057)
..... (963-6211)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptolg at bar1c05
(bar-one-c-zero-five)
(note: no 'o' in 'log')

Always include your full name, organization, and secure phone number.

For Change of Address
send name and old and new organizations to:
Editor, CRYPTOLOG, P1

Contents of CRYPTOLOG should not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

P.L. 86-36

ΚΥΔΟΣ

Accolades to the anonymous author at the National Cryptologic School who composed that most absorbing and inspiring tome On Watch. We were privileged to see an advance copy of this classified history.

The purpose, as stated in the Preface, was to "make new employees aware of the unique history of NSA ..." It's doing more than that. It's also informing some of us who played a part in the events described. All too often the participants behind the scenes do not get to see the big picture.

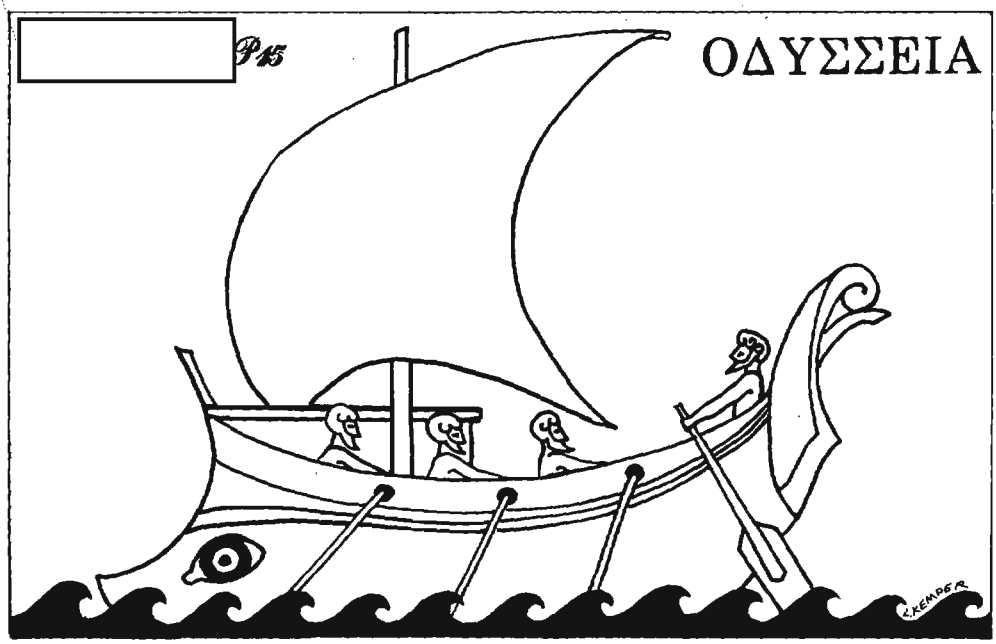
We want more! Don't stop now!

Author! Author!

DOCID: 4019705

P.L. 86-36

~~SECRET~~

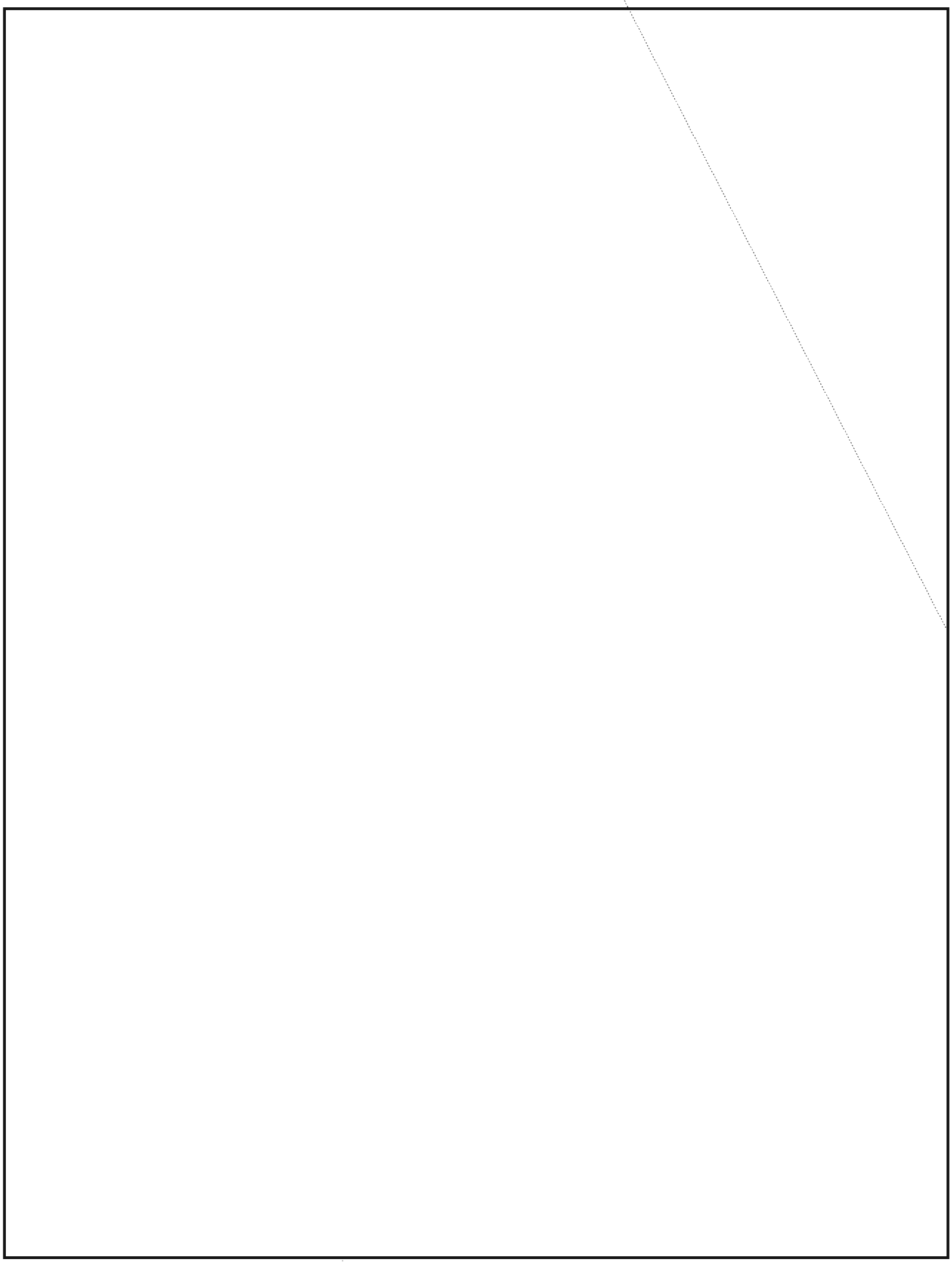


P.L. 86-36
EO 1.4.(c)

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4019705

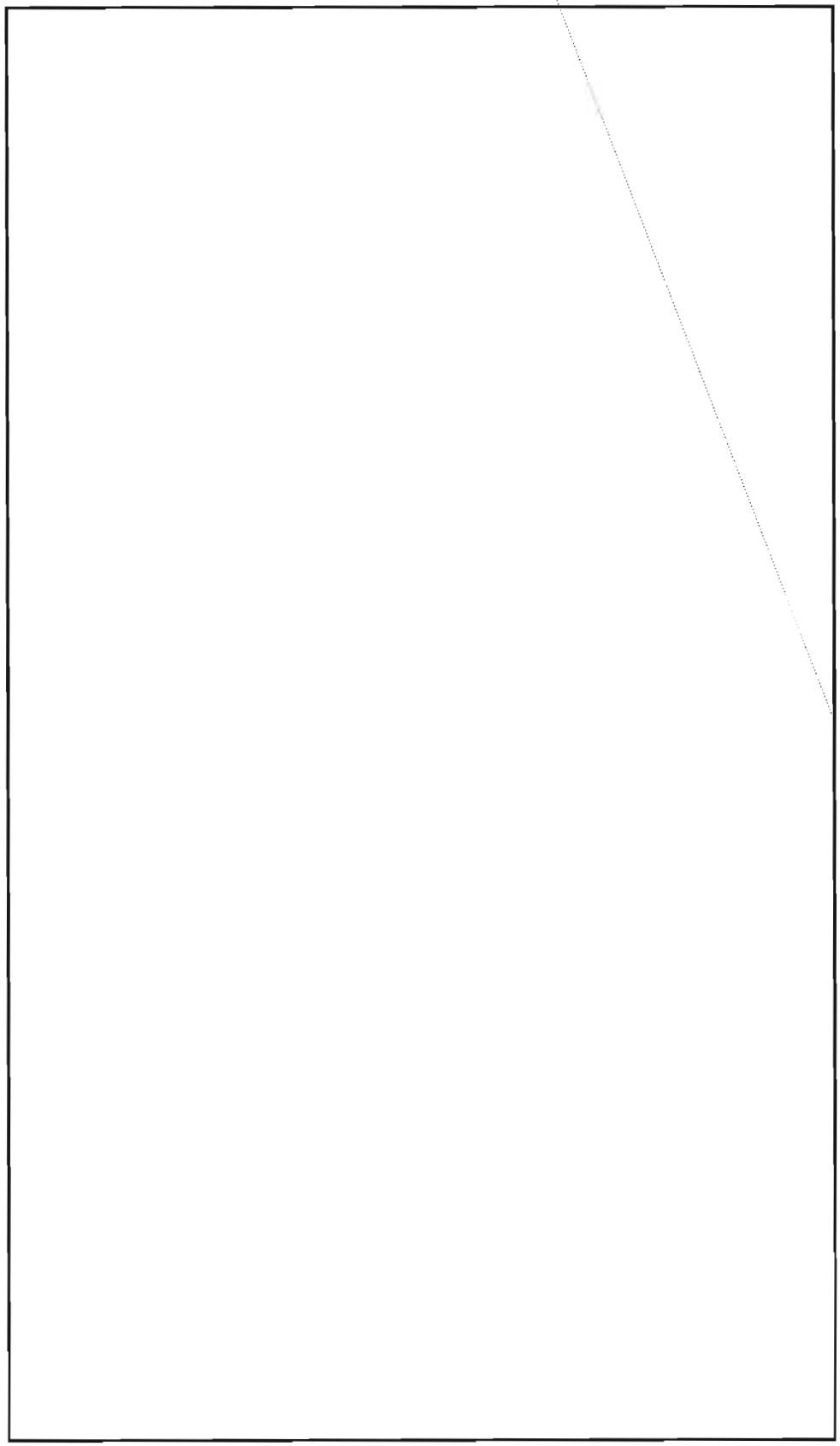
P.L. 86-36
EO 1.4.(c)



OCID: 4019705

P.L. 86-36
EO 1.4.(c)

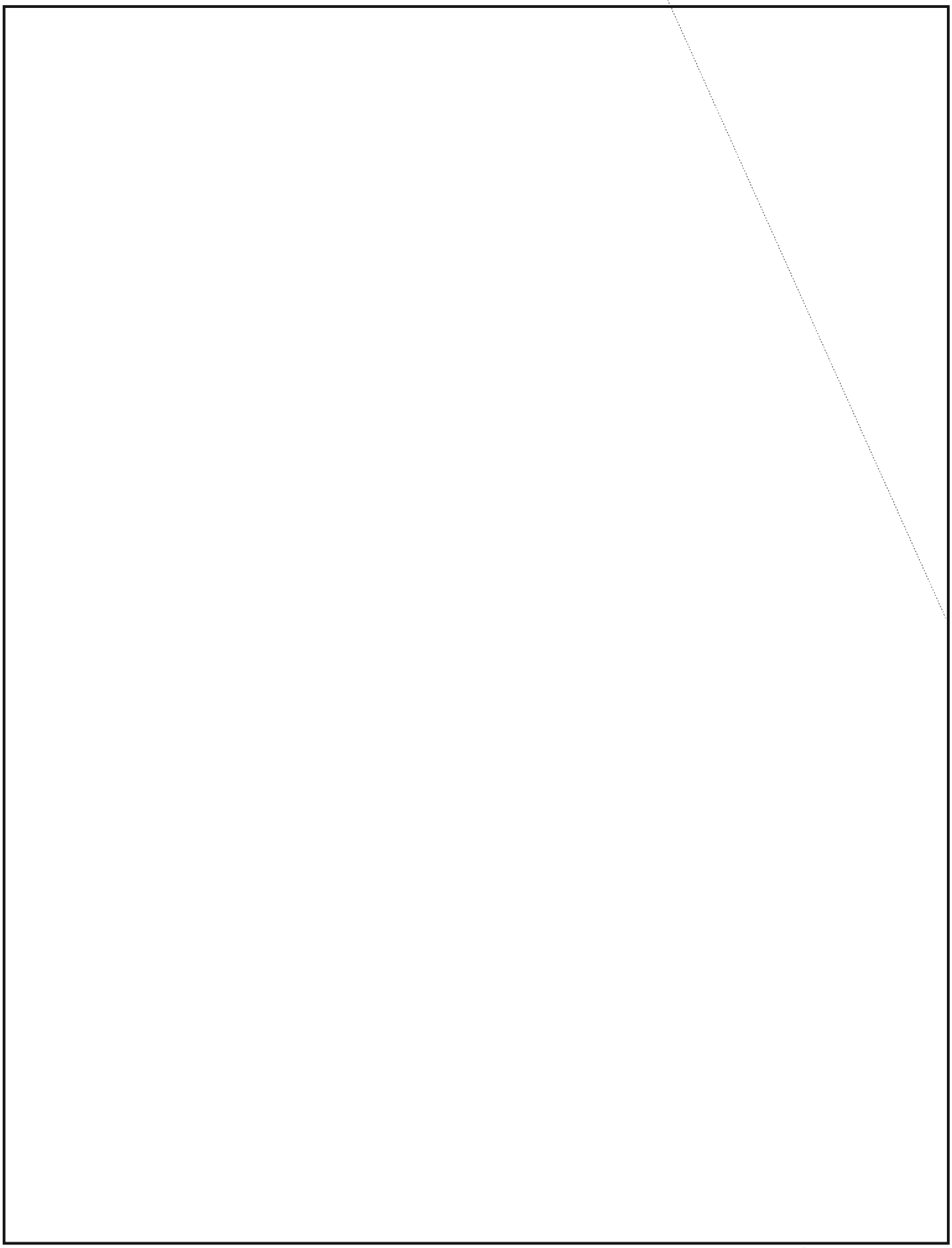
~~SECRET~~



~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4019705

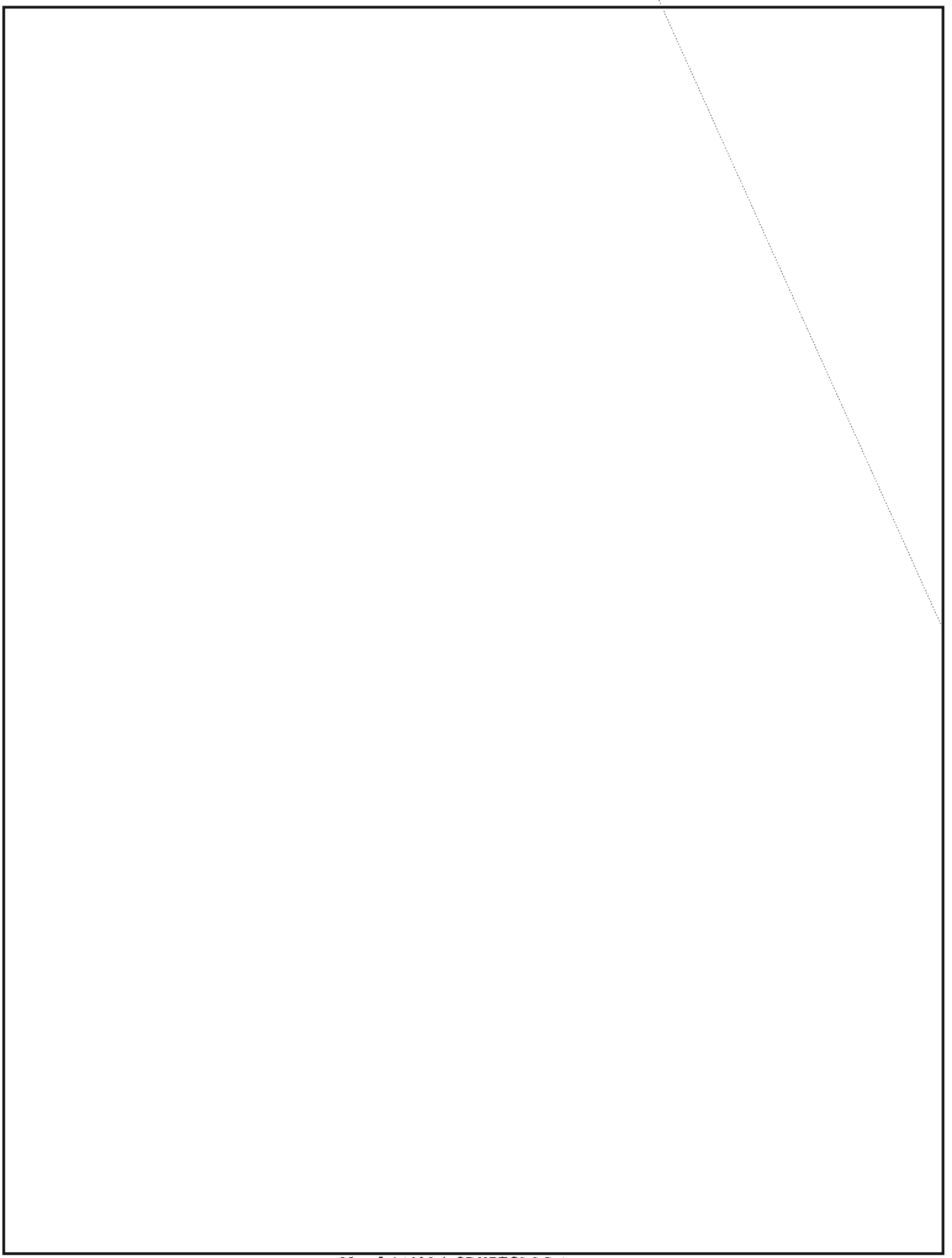
P.L. 86-36
EO 1.4.(c)



DOCID: 4019705

E.O. 1.4.(c)

~~SECRET~~



~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4019705

P.L. 86-36
EO 1.4.(c)

~~SECRET~~

The FOX *and the* CROW.

Answers to:

MORAL DISQUISITION

(Mar-Apr 1986)

Find the five-letter anagram to fill all blanks

"**Spera** in Deo," so the saying goes

(One cannot **parse** it, though the sense one knows.)

However, after "mon **repas**" one day,

When **pears** and port had both been cleared away,

I fell to musing, would God **spare** a Cain

Who **reaps** the heads of men, instead of grain?

At jousts the knight with **spear** to win a prize

Pares his opponents down to half their size

With him is damned the conqueror

To murder, also he who **rapes** and burns.

Answers provided by [redacted] *P16*

BULLETIN BOARD

SPECIAL FOR LINGUISTS (U)

~~(FOUO)~~ Copies of *Collected Articles on Translation, 1973*, are available again. The book, which is classified TSC, contains reprints of articles pertaining to COMINT translation that first appeared in *QRL, Keyword*, the *Cryptologic SPECTRUM*, and *The NSA Technical Journal.*

~~(FOUO)~~ To obtain a copy send your name, organizational designator, building, and room number to [redacted] P16, HQ, 8A187. Telephone orders are not accepted. □

P.L. 86-36

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4019705

ORGANIZING FOR EFFECTIVE C3 ANALYSIS (U)

[redacted]

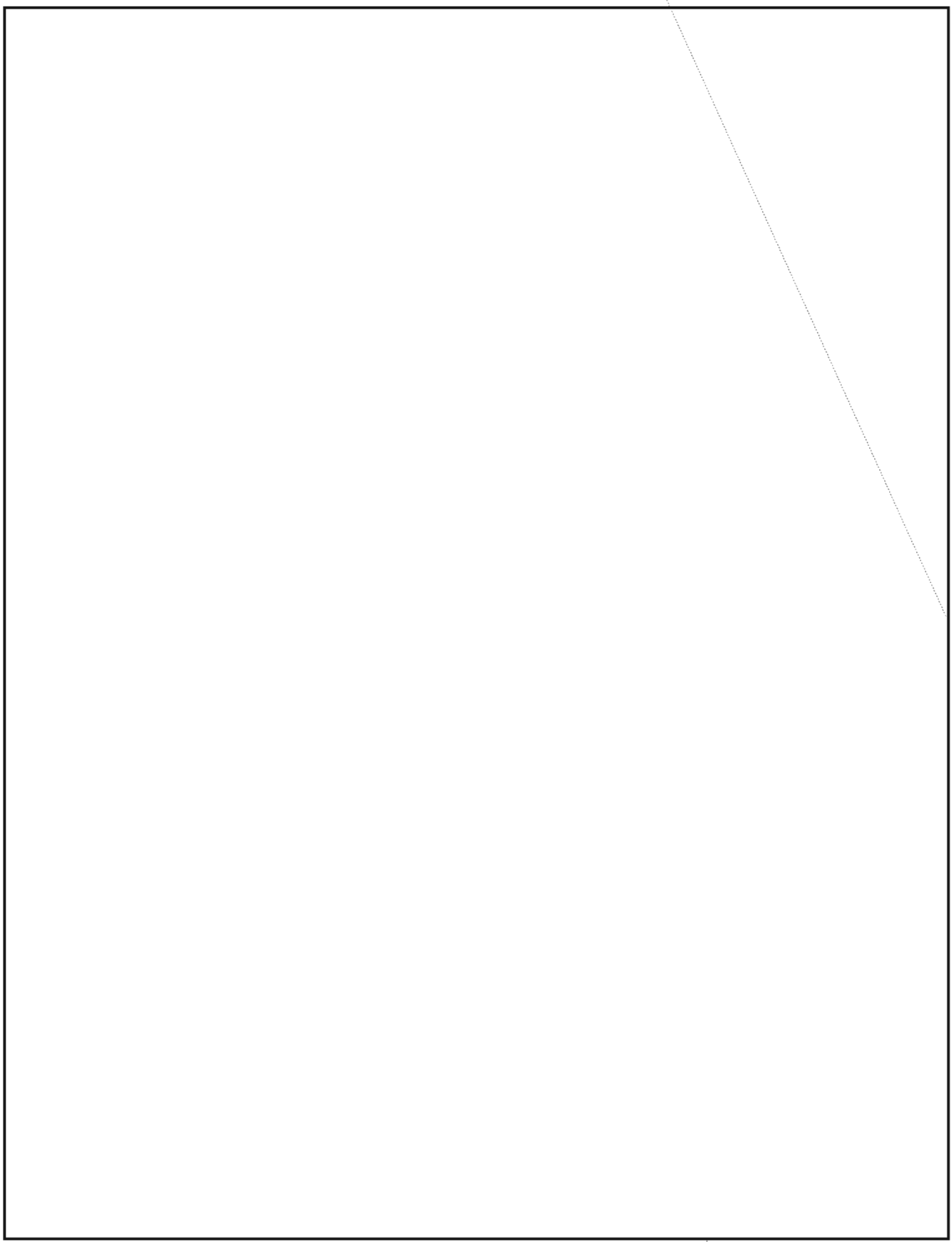
P.L. 86-36

[redacted]

P.L. 86-36
EO 1.4.(c)

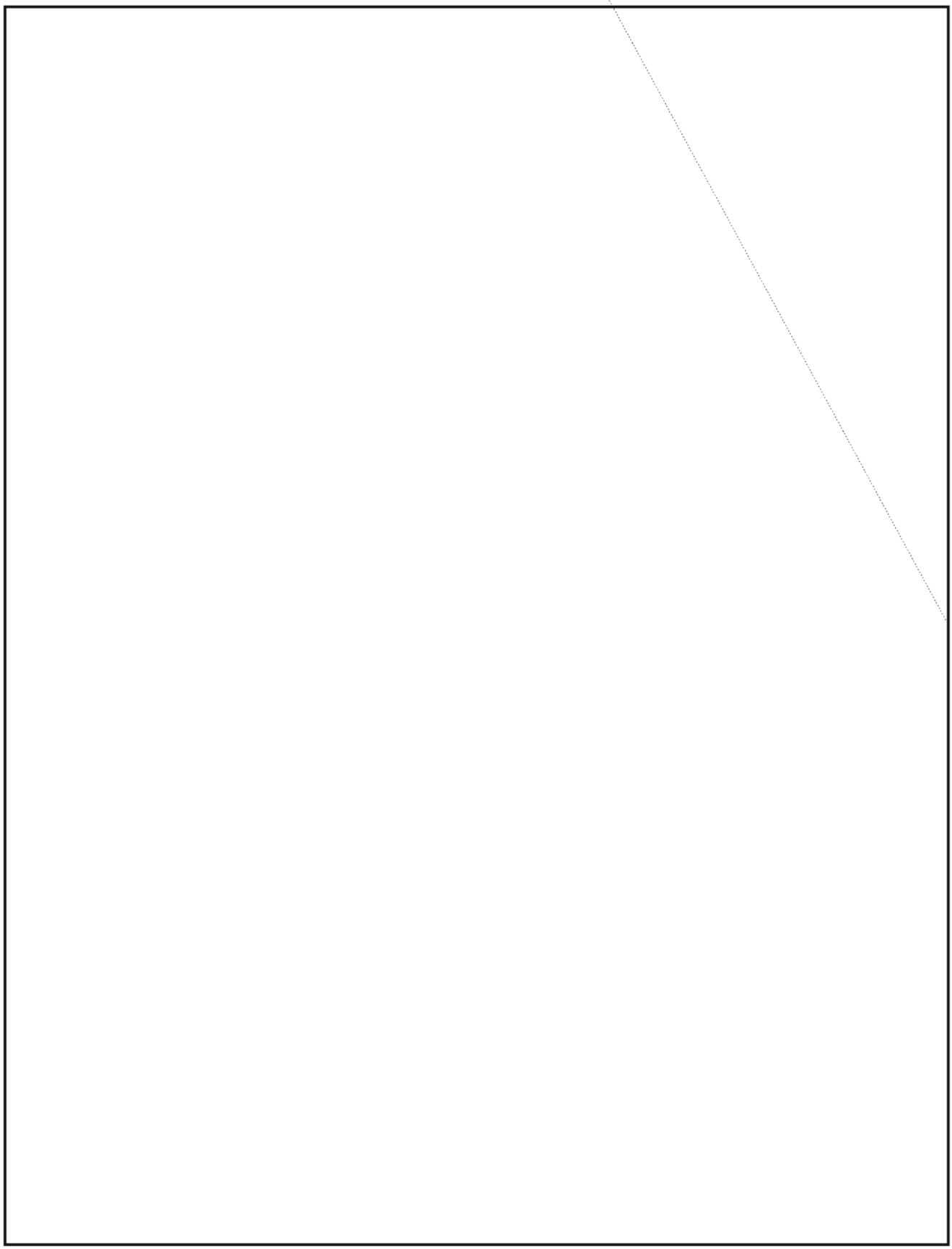
P.L. 86-36
EO 1.4.(c)

DOCID: 4019705



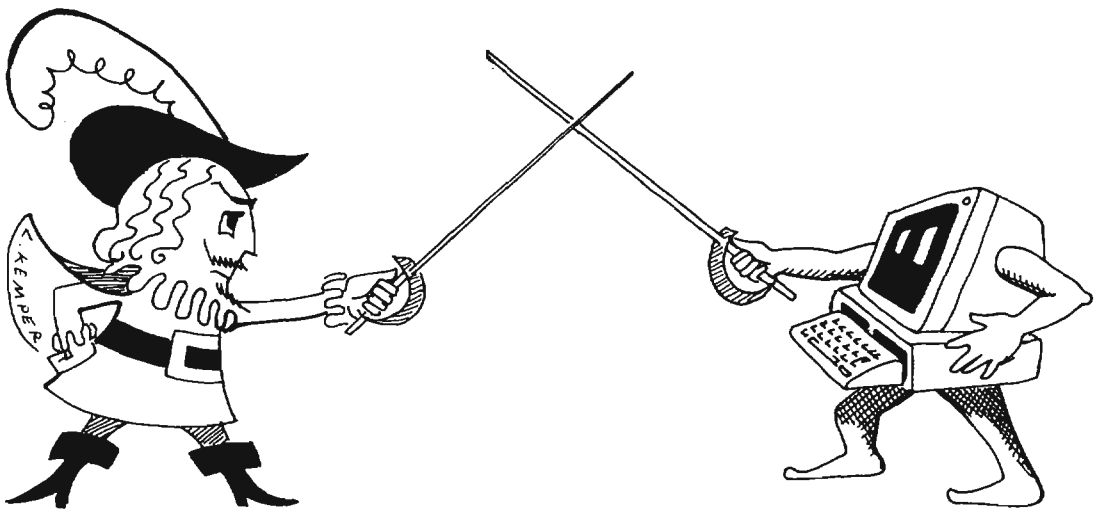
P.L. 86-36
EO 1.4.(c)

DOCID: 4019705



DOCID: 4019705

A LINGUIST MEETS THE ASTW (u)



A/SLAG

P.L. 86-36

This article is classified ~~FOUO~~ in its entirety

Author's Note: The comments below are based on using the UNIX operating system on the ASTW (an IBM XT) and the IBM Graphics printer.

Editor's Note: Readers might be amused to follow the transmogrification of four segments of text as the article flowed from the ASTW monitor to the Star printout, via an IBM floppy converted to an 860 floppy then to an 8010 floppy, and finally output on the Star laser printer. In the text below the segments are shown as converted to the Star. Mel's efforts appear in the footnotes; the first line is the text as output single-spaced on his IBM Graphics printer, and the second line as output on the same printer but double-spaced.

My computer was delivered in a huge box. Surely was glad that my offer to carry it up to my office myself was not accepted. I would never have made it. I unpacked the huge box and discovered a big carton of intimidatingly thick manuals to go along with the computer. Of course, no guidance could I see on how to get started or even on what manual to look in first. Fortunately, in glancing through some of the manuals, I looked in one labled Tu'taProcussi gaGuidu ® and saw that a tutorial was provided. Reasoning that no matter what sort of files I wanted to construct, I would need some word processing functions afforded by the PC/IX operating system, I set about putting myself through the tutorial.

I had been working with the computer 15-20 minutes when I wanted to cancel a command, which is done by pressing the <Alt> and <Lang> keys simultaneously (nothing about "cancel" there - but, really, that's the way it's supposed to be done). Well - clumsy me - my thumb missed the <Alt> key - meaning that I had pressed the unaltered <Lang> key. To my horror, the whole screen was immediately flooded with Cyrillic, the alphabet used for Russian. It wasn't the Russian language, mind you: just the Russian alphabet. I spent about an hour trying unsuccessfully to get out of that - trying to get back the English that I had typed in. Finally, a colleague said that I should press <Ctrl> and <Lang> simultaneously. I tried that - and sure enough I was out of the Cyrillic mode! But when I

tried to type the letter "e" to edit or to create a file, all I got was an "a" with an umlaut (two dots) over it. I struggled with that one about 15 minutes before I somehow got back to "normal" operations.

It turns out that there is a little system file that allows one to set the computer for color (which I don't have) or graphics (which, it turns out, I do have) instead of the monochrome monitor that the computer comes set for. Setting that file correctly takes care of those Cyrillic letters all over the screen when you don't want them there. Anyway, now that I've made the adjustment to the file, I am able to type in Russian when I want to and in English when I prefer to do that.

The only trouble in using Cyrillic is that I cannot sort in Cyrillic alphabetic order and cannot print Cyrillic on my printer. And I have destroyed huge parts of files when I have tried to use some of the normal word processing functions. When I tried to replace a Russian word with another Russian word (quite a normal function for English), all hell broke loose: all but a few words at the left-hand side of my screen were wiped out. That was true throughout the number of lines I had specified for the Cyrillic characters.

Though I can't print Cyrillic, some weird things happen when I try: my printer dances all around, whistles, spews out blank pages, and in general acts like a wild person. Some of the Cyrillic letters have the same ASCII coding as some of the printer control functions. I have harnessed this knowledge to help me in a few instances - e. g., to get a larger print, I just type in the Cyrillic "o", and the rest of that line will print out in double width. Very handy for a major title.

The peculiarities of printing do not end with the Cyrillic story. They extend to English iua ouatr atoau durli u. ③ After hitting <Alt> "f" (for font), the text will appear underlined and in reverse video on the screen. Then, using the print command ($print filename), the nice underlined portion in English shows up on the printed page as European letters with diacritics and graphics characters!

Within a few days after getting into operations, I really did it to myself again - or maybe the system did it to me. Curious about what the "Menu" under Function Key 1 (F1) was, I pressed that key. Three options appeared on my screen. The third one was "Edit your editor profile." Naturally, I wondered what my editor profile was, so I chose that option. But only a blank screen for creating a file came up. The only way to get out of that was to press <Alt> "d", which "copies" a file. But then when I tried to create new files or view old ones, I could not invoke the editor - that is, I could not do a blasted thing. It turned out that the editor profile (.eprofile) file overrides the normal system commands for the editor and that a blank file (which I had just created) means to do nothing. And the computer was doing exactly what I unknowingly had told it to do - otui g. ④ The solution to the problem was to delete the .eprofile file.

At first, I spent a great deal of time trying to figure out what all the keys on the keyboard meant when I pressed the <Alt> and a given key. But finally I found a little picture of the keyboard in the manual cited above, the Tu'taProcussi gaGuidu ⑤ (p. 2 of the "INed" section). I cut the picture out and pasted it on my keyboard, and that made life a lot easier for me. I had to be sure to change the position of the CAPS LOCK, CTL, and ALT keys in the picture to fit the reality of my keyboard.

The ASTW using the PC/IX is, indeed a powerful and flexible device - one that is sometimes quite a pleasure to use. But frustrations that anyone might well suffer are compounded for the linguist when he tries to make his machine truly bilingual.

① ∟σ° ⌠á⊥≥∩πσ≤≤θ∈τá⌡ θΣσ
Text Processing Guide

② θμá·∩⌡á⌠≥·á⌠∩á⌡∈Σσ≥ωθ∈σ.
if you try to underline.

③ ∈∩⌠δθ∈τ.
nothing.

④ ∟σ° ⌠á⊥≥∩πσ≤≤θ∈τá⌡ θΣσ
Text Processing Guide

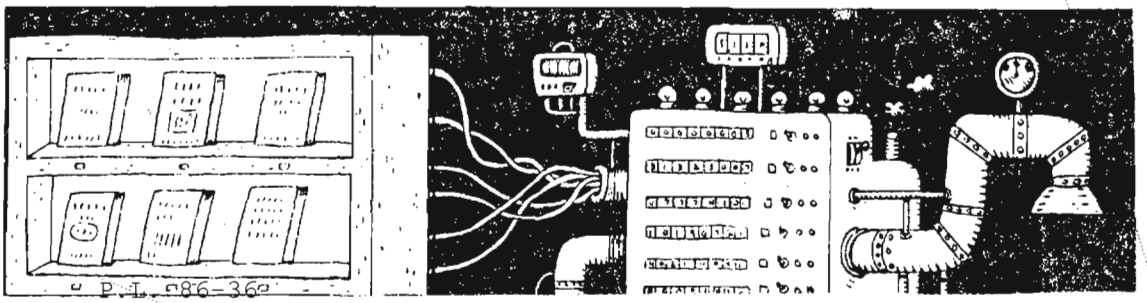
←——————————→

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

P.L. 86-36

AI AT NSA (U)



P.L. 86-36
EO 1.4.(c)

(U) Approximately two years ago the NSA Artificial Intelligence Working Group was formed to introduce AI to Agency tasks, with emphasis upon identifying suitable projects, and to establish a forum for the orderly exchange of information among Agency personnel and with outside sources. The Group, chaired by Norman Glick of Z, comprises representatives from many Agency elements in which AI techniques are being studied and applied, thereby avoiding duplication of effort.

(U) Development of AI at NSA began with the procurement of hardware and with the training of personnel. The Pentagon agency DARPA (Defense Advanced Research Projects Agency) provided NSA with several Symbolics 3600s, computers designed specifically for AI applications. The 3600s are now placed in offices throughout the Agency. Training is available both outside and in-house. Johns Hopkins Applied Physics Lab has a Master's degree program in AI and George Washington University a program in knowledge engineering, a skill essential to the construction of an expert system. NSA offers a self-paced video course in the Learning Centers and a platform course on LISP, the AI programming language most popular in the United States. A three-day Technical Development Program Seminar entitled "Overview of Artificial Intelligence Research and Applications" was held in January, 1986. Agency personnel have participated in conferences and seminars on AI, some of which have been hosted by NSA. The NSA libraries contain many books on AI, ranging from introductory surveys to highly technical material.

AI PROJECTS AT NSA

~~(C-CCO)~~ Information about AI projects at NSA was obtained through interviews with individuals who are applying AI techniques to Agency problems. Following is a small sampling of applications in progress at NSA.

W1

(U) (American industry is currently using a similar process, in which "seeing" robots compare product parts against a model to search for anomalies that could indicate a faulty product.)

(U) The development of W1's expert system was shared between NSA personnel and a contractor. W1 supplied two experts for the initial stages; when the contractor eventually took over, he was able to provide analysts with related expertise. The interaction between the experts and the knowledge engineers (those responsible for collecting the expert's knowledge and organizing it into machine-comprehensible form) took no fewer than five rounds. This project was concluded just in time before the two W1 experts, upon whose knowledge this system was based, left the project.

~~(S)~~ W1 already has one Symbolics 3600 computer and is expecting two more, along with additional hardware such as an experimental workstation. The new equipment will be compatible with other hardware used by W1, including VAX, IBM, and CDC computers. As each stage of the AI system is completed, it is implemented in that operational element, thereby allowing the analysts to give feedback during the development stage. Implementation of the expert system could reduce the time spent in analyzing one event from several months to less than a week.

G424

P.L. 86-36
EO 1.4.(c)

~~(FOUO)~~ [redacted] a graduate of the CA intern program, is trying to develop an expert system to avoid such a situation. Along with [redacted] of G431, she was awarded a grant for this project from the NSA Director's Skunkworks Fund, an account designed to support innovative approaches to aspects of the Agency's mission.

~~(TSC)~~ Development began with selecting a commercially available expert system shell. Using an existing shell saves development time; moreover, eliminating the need to create a shell allows the development team to be composed entirely of cryptanalysts, without external computer programming support. The selected hardware, a Symbolics 3670, has already been installed. Upon receipt of the software, formulation, testing, and modification of the expert system can take place.

AI AS A POSSIBLE CA INTERN TOUR

~~(C-CCO)~~ [redacted] found that, even as a permanently assigned cryptanalyst, it took him nearly three months to acquire sufficient background to be useful to the A54 expert system development team. [redacted] on the other hand, believes that an intern can play a useful role in certain stages of the development of the G424 expert system.

~~(C-CCO)~~ It may be of interest to note that neither of the intern graduates (Susan and Steve) had courses in programming or mathematics before coming to the Agency; since then Susan has taken courses in programming and math, and Steve in programming Susan suggests the following as minimum requirements for an intern who might be interested in her AI project: basic knowledge of NSA data systems, familiarity with the rudiments of CA, and successful completion of the probability/statistics course(s).

ACKNOWDGEMENTS

(U) I am grateful to [redacted] for their considerable assistance and to [redacted] for classification review. □

CID: 4019705

PRESERVING VALUABLE NSA/CSS PAPER RECORDS

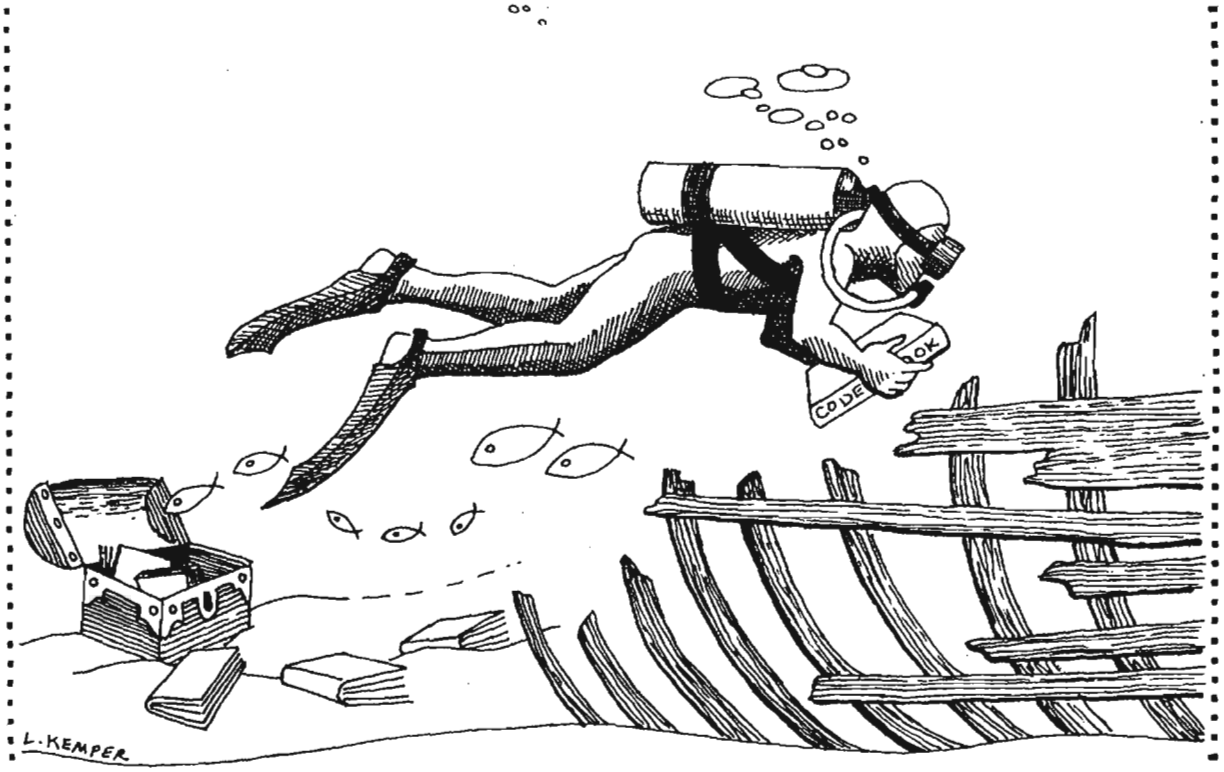
[redacted] T54

P.L. 86-36

Most paper records are valuable only for the information they contain and, therefore, the medium in which the information is held is normally irrelevant. In such cases, it suffices that the information be portrayed as a true copy and be easily accessible and readable. Beyond this, there are some paper records that have intrinsic value. In such cases, ways must be found to preserve the original paper medium from the deleterious effects of rough use and poor storage conditions, or to conserve it by appropriate restoration techniques when damaged.

In recent years, NSA/CSS has become a leader among Federal Government agencies other than the National Archives and Records Administration (NARA) in the effort to preserve valuable paper records. "Normal" Federal agencies usually transfer their inactive permanent records to NARA control long before they are so old that a critical stage is reached in their physical existence. However, almost all of our records still require restricted access and special security handling, even after they become fully inactive

For this reason, they are not stored with the records of other agencies at a Federal regional



~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

records center, or at the National Archives building itself. Because of this, NARA has given NSA/CSS special permission to retain its classified permanent inactive records in a special Cryptologic Archival Holding Area (CAHA) until they are fully declassified and can be released. [As an aside, there are perhaps only two or three archival holding areas permitted in the entire Government.]

Recognizing that declassification may be many years away for our permanent records, NARA has also required, and NSA/CSS has agreed, that we undertake special measures to preserve them. What follows is a description of the system that the CAHA staff has devised to carry out this task.

But first, some background information on preservation techniques is necessary. Preservation includes passive measures taken to insulate or protect records from external forces or influences that attack, make unreadable, or eventually destroy them. This includes inhibiting the transference of acid between the pages of paper articles, and the boxes, folders, or containers housing them; isolating paper from exposure to ultraviolet rays emitted by the sun or fluorescent lighting; removing rustible bindings; and, protecting paper from adverse environmental factors such as excessive heat, humidity, flooding, and pollution -- all of which embrittle, fade, debilitate or otherwise destroy the cellulosic fibers of which paper is composed. Preservation also includes taking appropriate active conservation methods, to include those that directly affect or change the inherent structure, properties, or composition of paper. Included in this are deacidification-encapsulation, mending, and restoration.

Active records in NSA/CSS "mature" and reach a final disposition stage at varying periods, as described in our four Records Disposition Schedules (RDS). The RDS's are titled: Signals Intelligence, Communications Security, Research and Evaluation, and Administration-Management. At some point, the records in these schedules become candidates for either destruction or permanent preservation. The RDS's are approved by the Archivist of the United States, who is the final authority on whether a given record is permanent or temporary.

In NSA/CSS, when a permanent record reaches its 20th - 30th year, it is ready for processing into the CAHA. It is at this juncture that CAHA archivists begin to apply preventive maintenance preservation measures. Staples, clips, rubber bands, metal fasteners, and all similar binding materials that rust and adversely interact with paper are removed; folders and containers laden with acid are replaced by acid-free ones. Other minor repairs to damaged paper records are made at this time.

While gathering and inputting information designed to give us good intellectual controls over records in a storage area, as well as the usual bibliographic controls needed, agency archivists also identify records that require advanced preservation treatment. This includes cleaning, flattening, deacidification, encapsulation, etc. The Archival Information and Retrieval System, an automated finding aid system in use in the CAHA, is then annotated as to what further preservation measures are needed. When the required controls have been established, review for continuance of classification has been made, and all finding-aid data have been entered into the system, records requiring advanced treatment are queued until an archivist-conservator has the time to process them further.

In NSA/CSS, active preservation for valuable permanent records includes state-of-the-art as well as centuries-old archival conservation techniques. CAHA archivists dry-clean dirty documents with opaline and other compounds and repair ripped or torn pages with long-fibered Japanese papers appropriately matched for color and texture, and home-brewed wheat starch or methyl cellulose pastes. Paper can be deacidified with non-aqueous chemicals that also leave a protective coating of alkaline on the paper's surface. To further protect documents that have become so embrittled, spotted, or worn that more handling might jeopardize them, archivists encapsulate. Encapsulation is the enclosing of a document (preferably first deacidified) between two sheets of an acid-free, ultraviolet ray inhibiting polyester material. The two outer polyester sheets create a field of static electricity (after vigorous rubbing with a clean cotton pad) that effectively grips the sandwiched sheet of paper and permits its safe (even *rough)* handling. The polyester keeps out dirt and other airborne pollutants and its U/V shield repels the fluorescent light/sunlight rays that attack exposed paper.

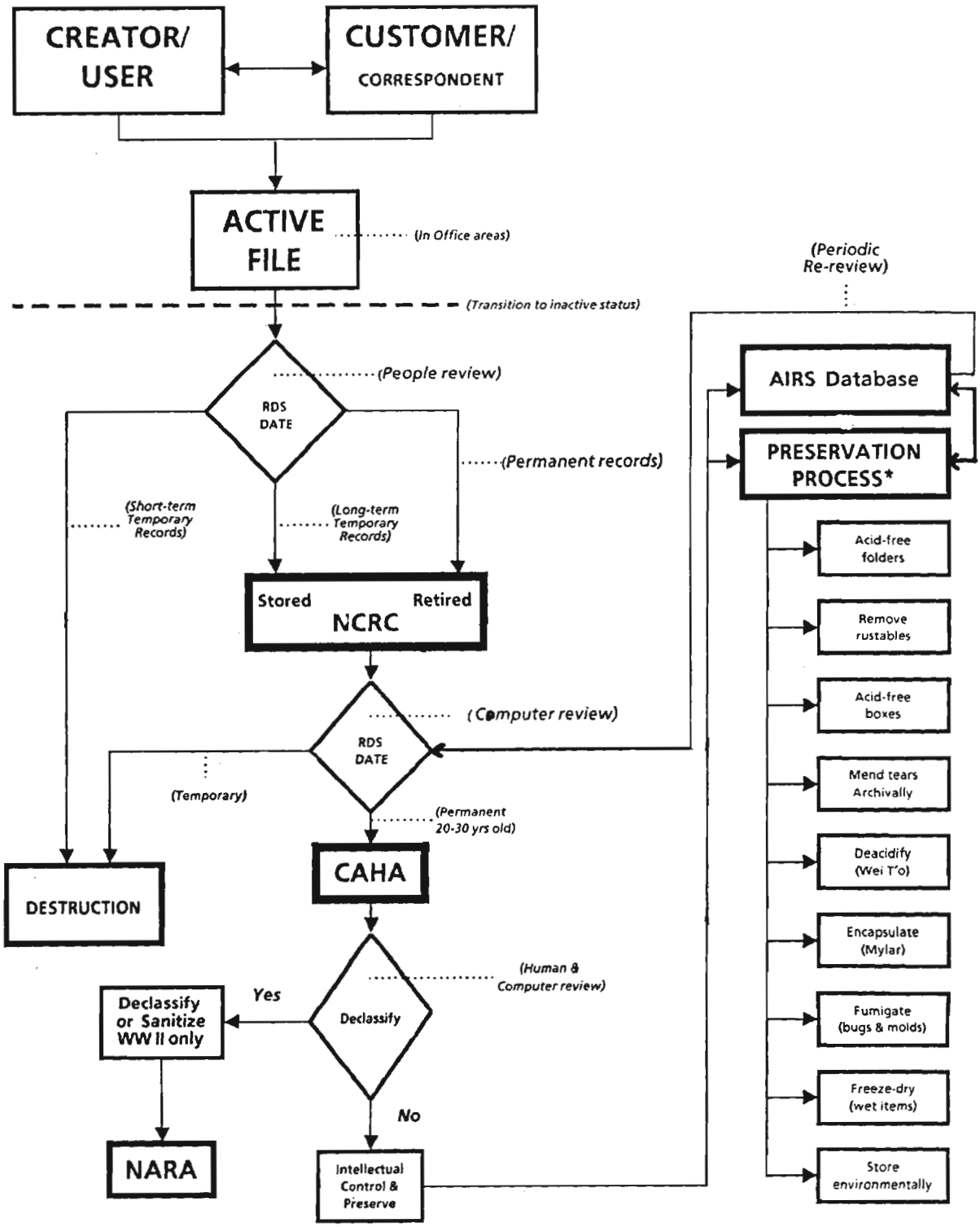
Best of all, encapsulation is fully reversible and one need only rip open the electrostatically sealed (special machine-generated) seams, none of which have touched the paper, to get back to the document in its original state.

The CAHA's latest preservation acquisition is a freeze drying chamber capable of holding and treating up to 16 cubic feet of records. It provides our most exotic preservation capability. Imagine having a very valuable operations-related document fished out of a cesspool after

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

THE NSA/CSS PERMANENT DOCUMENT PRESERVATION CYCLE



* As needed and authorized by the NSA/CSS Archivist

Abbreviations Key

RDS	=	NSA/CSS Records Disposition Schedules (4)
NCRC	=	NSA/CSS Records Center
CAHA	=	Cryptologic Archival Holding Area
NARA	=	National Archives and Records Administration
AIRS	=	Archival Information and Retrieval System

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

abandonment by a target, or recovered from a safe in a sunken vessel. What is the normal state of such a document after it has been subjected to the usual methods of drying? Shriveled, bulged, warped, cockled, or drawn pages, permanently stuck together; totally smeared or obliterated ink or pencil entries; key words and phrases in the text covered by impenetrable stains or accretions. Not a very good document to work with.

With the lyophilization (freeze-dry) process of recovery, a 99% readable and usable document can emerge. First, however, the document must either be kept in its wet state, or be frozen. (If such a document were delivered to the CAHA in a bucket of water, it would first be frozen.) After the freeze drying chamber has been sealed and all the air evacuated to create a vacuum, the process would begin. It essentially involves removal of the ice from the fibers of the paper by conversion to vapor and then reconversion to ice in an accumulator chamber. The amount of ice removed is weighed periodically to determine just how much water has been removed from the paper. When "just enough" water is left, the process is stopped. At this point, a highly readable and usable document emerges.

This process works equally well for recovering electronic equipment that has been inundated. [The CAHA recently offered its facilities to NASA if it needed help to restore electronic parts recovered from the exploded shuttle; our help was declined with thanks because all recovered equipment was impounded by the investigating board.]

There is also a bit of serendipity attached to our acquisition of this device. We have since discovered that it can function very efficiently as a paper fumigator. When paper lice, mites, and other live things are found in old boxes, we can quickly freeze the entire box, killing all the live things, and then create a vacuum, which effectively explodes and destroys any eggs about to hatch.

The agency now has other tools available to make operational tasks easier. If you have an intrinsically valuable document that has been soaked (remember the recent flood in the computer operations area of the Operations building basement?), or if it is infected with lice or is otherwise too fragile for continued use, call the author or the CAHA staff (972-2268s) for assistance. □

Solution to Essex Cipher, War of 1812 (Jan-Mar 1985)

```
.QD66.94DK.C7.G4C66C.
.SELL THEM IN CHILLI.

.AP8QPD2.
.PURSUED.

.A8DAF8D2.
.PREPARED.

.AX6C9CGF6.
.POLITICAL.

.7X9.7F0CBF9D.94D.AFGC3CG.C7.QF3D9O.
.NOT.NAVIGATE.THE PACIFIC.IN.SAFETY.



 Plain:  A B C D E F G H I J K L M
Cipher:  F . G 2 D 3 B 4 C . . 6 K

 Plain:  N O P Q R S T U V W X Y Z
Cipher:  7 X A . 8 Q 9 P 0 . . O .
```

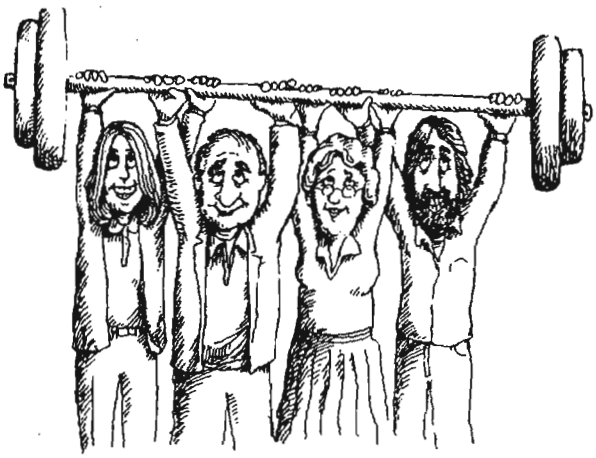
Readers are invited to submit a complete solution of the substitution system.

~~FOR OFFICIAL USE ONLY~~

CID: 4019705

TEAM BUILDING

A TOOL FOR IMPROVING ORGANIZATIONAL EFFECTIVENESS (U)



E622

P.L. 86-36

Imagine the people in your organization--even the most indifferent--suddenly finding new excitement and challenge in the job they now take for granted. What would it be like to have a management team that plays the "What Might We Do" game and not the "Ain't It Awful" game?

All this and more can happen when an organization makes a decision and commitment to work as a team. A formal team building workshop may be all that you need to start improving your organization. Following is an explanation of what team building is and is not, and how it might help your organization become more effective.

Only a very small part of a manager's or executive's work is spent in isolation; most of the time is spent working as part of a team in project meet-ings, committee meetings, executive teams, staff meetings, and task forces, as well as in other "teams" -- family, fraternal, political, recreational, and religious. Yet many managers do not know how to function either as a team member or a team leader. They can learn, however, by participating in team-building workshops.

Team-building workshops are designed to:

(1) enhance the effectiveness of persons who share goals and are dependent on each other for achieving them;

(2) increase collaborative efforts to achieve both individual and team objectives.

During the past 15 years, team building, a facet of organizational development, has emerged as a major technique to improve the way in which work is accomplished by individuals who have common work relationships and goals.

WHAT IS TEAM BUILDING?

Team building is a planned and managed event involving a group of people who have common organizational relationships and/or goals. In the Agency, team-building workshops are conducted primarily to help the organization achieve optimum organizational effectiveness, and are problem-solving oriented, that is, they center around accomplishing tasks. Team building should not be confused with "T-Group" or "sensitivity training" which was popular in the 60's. Sensitivity training focuses primarily on the individual in interpersonal relationships and

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

on the emotions, such as hostility and anger, surrounding the relationships.

The team-building process requires a trained internal (E62) or external (contract) consultant who assists the group members to work through semi-structured or structured activities and work-related problems. The object is to develop and sustain positive, integrated work relationships so that the members function more effectively together. While a workshop may center on the tasks and activities performed by a particular group, it must also focus on the team-action production process. Thus, it tends to be more **process** than **content** oriented.

Occasionally, teams meet to work on specific issues or problems without the aid of a facilitator or consultant. These sessions are generally called management retreats, project meetings, or planning meetings, and tend to be mostly content-oriented.

Quite often a question arises about the need for an external facilitator. We have learned that teams who use a member of their own organization -- a division chief, staff chief, or executive -- as a facilitator for their initial attempt at a team building workshop are less successful than those which are led by a trained facilitator. That may because the team-member facilitator may be a part of the team's problem, or perhaps because a team-member facilitator becomes so involved with the content and with solving content problems that the process goes unattended; thus the purpose of the workshop is defeated. But once team members learn to work together and manage the team process, there is usually no further need for an outside consultant.

TYPES OF TEAM-BUILDING WORKSHOPS

There are several varieties of team-building workshops:

- family team building workshop--a division chief and the branch chiefs;

- start-up team building workshop--members from various organizations can be used as a means of getting a project or organization off to a spirited start;

- transition team building workshop--designed to integrate a new manager such as a field station chief, office chief, division chief, etc., into an existing team. The objective is to minimize disruption of work and to reduce the time it takes a manager to become acquainted with the management team;

- follow-up team building workshops --designed to review progress on action items from a previous team building workshop, identify new issues and concerns, and develop action plans to create the desired change. Follow-up workshops are routinely conducted four to six months after the initial workshop.

All team building efforts are an approach to improving working relationships so as to result in more effective functioning as a group and in accomplishing a task. The key point is that team building is centered around mission accomplishment.

THE PROCESS

To have the greatest impact, team building needs to start at the top of the organization. Starting at the bottom is an exercise in futility since some of the top-level managers might not understand exactly what is taking place. At a minimum, the leader or team must brief upper management on the team's intentions and provide adequate follow-up data on actions the team has taken or expects to take. Also, it must give periodic briefings to inform management of the results accomplished through its efforts.

Individual consultants have their own style of conducting a workshop. After an internal or external consultant is selected by E62 to conduct a workshop, the consultant meets with the manager to discuss the goals of the workshop. Some consultants conduct interviews with every participant, while others conduct interviews with only a few; still others conduct no interviews at all. Some consultants make extensive use of questionnaires before starting, and others collect data during the initial segment of the workshop. Some consultants set an agenda prior to the workshop; others prefer to be flexible and develop it as the workshop progresses . No one method seems to be more effective than the other. The key to success seems to require two things: a consultant who is sufficiently skilled in consulting procedures and team work techniques, and a team which understands the objectives of the team-building session prior to going to the workshop.

At a minimum, the workshop must focus on developing action plans to create some kind of positive change. When teams fail to develop action plans or develop only superficial plans, the workshop has minimum impact on the organization, and in some cases, a negative one.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

This may happen because though there is awareness of a problem, nothing is done about it.

Following is an example of a team building process commonly used by external and internal consultants conducting Agency workshops:

The team warm-up phase:

◆ identifying factors influencing functioning as a team

◆ creating a team climate for optimum functioning

The team-diagnostic phase:

◆ identifying concerns influencing individual and team performance and satisfaction

◆ collecting data, acquiring data feedback, and planning action

The team-prescriptive phase:

◆ enhancing creative team problem-solving

◆ developing skills for improving individual and team performance

◆ developing mutual coaching skills

◆ learning to analyze team effectiveness

The team action plan phase:

◆ converting options to action items--making it happen

◆ committing resources to optimize team effectiveness

The team implementation phase:

◆ identifying and managing hindering factors

◆ identifying and managing facilitating factors

The team assessment phase:

◆ establishing criteria for team evaluation

◆ identifying means for continuing team improvement

RESULTS

The product of every team-building workshop, in addition to a general feeling of cooperation and trust, is a set of action plans that address areas for improvement. These areas frequently include: how to solve problems, make decisions, formulate policy, set goals, communicate, relate on an interpersonal and organizational level, set stan-dards, and so on. A useful format for action plans is "who, does what, with whom, by what date for what purpose?". A typical action plan might be:

> By 1 January develop a plan for reorg-anizing. George will develop and coordinate the plan with XX and have a proposal for discussion at the next corporate review on 1 November.

The benefit of reorganizing will be less duplication of effort and more equitable distribution of the work load.

While managers have reported a wide span of results, almost all of the feedback indicates that team-building workshop benefited the organization by:

1. Making the team a more effective problem-solving unit.

2. Providing the team a more effective climate in which to work.

3. Developing more openness in communication about issues that are central to the team and the individual effectiveness of team members.

4. Increasing an awareness of and competence in dealing with conflict and change.

5. Developing a new understanding of how the group operates and the benefits of the participative management process.

6. Expanding insights into the members' and the team's roles and purposes in a larger setting.

7. Increasing the team's ability to work with other teams.

8. Developing a stronger feeling of support and interdependence among members with more emphasis on collaboration and less on competition.

In order for a team-building workshop to be successful, several conditions should exist which include:

1. A desire to change;

2. A minimum of severe interpersonal problems.

~~FOR OFFICIAL USE ONLY~~

OCID: 4019705

3. A firm commitment to follow up and evaluate activities and action plans.

4. An adequate amount of time for the session--normally three days -- and subsequent project meetings.

5. A competent consultant/facilitator.

6. A manager or executive who is prepared to deal with a more open and candid system.

7. A manager or executive who is willing to genuinely support the team's desired, legitimate outcome.

LIMITATIONS

What are the limitations of team building? Change cannot be expected to occur overnight. The leader and the team must frequently evaluate the effects of the team-building workshop, readjust strategies, and reinforce positive change resulting from the team's efforts.

To insure the maximum long range results, several Agency organizations have conducted two or three formal follow-up team-building workshops and 20 or more project meetings or informal sessions. One must remember that organizational change is a very slow process and requires time to work through the action plans developed at the workshop.

SUMMARY

Team-building workshops simply attempt to eliminate barriers to collaborative behavior within the team by developing skills that foster greater team attention and direction to the achievement of tasks. Team building is based on problem-solving rather than fault-finding to promote individual and team growth. The bottom line is improved organizational effectiveness and employee satisfaction.

Team building cannot be viewed as a panacea for problems or ineffective behavior in an organization. Other factors such as the total organizational environment or culture, leadership styles of the managers, organizational structure, a willingness to change, etc., all play an important role and impact on the team's operation. Other management improvement techniques may be more appropriate in some cases.

For assistance or information on setting up team building workshops, please contact [redacted] or Charles Hall in the National Cryptologic School, E622, 968-8971s.

This article contains material prepared by Dr. George F.J. Lehner, a private consultant, for handouts in his workshops.

The following sources are recommended for additional information on organizational development and team building:

Baker, H.J.,
"The Hows and Whys of Team Building" *Personnel Journal*. 1979.

Blake, R.R., Mouton, J.S.
The Managerial Grid III-The Key to Leaders-hip Excellence. Houston: Gulf, 1985;
Corporate Excellence Through Grid Organizational Development.
Houston: Gulf, 1968.
Productivity--The Human Side.
New York: AMACOM, 1980.

Davis, S.A.
"An Organic Problem-Solving Method of Organizational Change." *Journal of Applied Behavioral Science*. 1967.

Francis, D. Young, D.
Improving Work Groups-A Practical Manual for Improving Work,
San Diego: University Associates, 1979.

French, W.L. & Bell, C.H., Jr.,
Organizational Development.
Englewood Cliffs, NJ: Prentice-Hall, 1973.

Rubin, I.M., Plovnick, M.S., and Fry, R.E.
Task-Oriented Team Development.
New York: McGraw-Hill, 1977.

Weisbord, M.R.,
Organizational Diagnosis: A Workshop of Theory and Practice.
Reading, MA: Addison-Wesley, 1983.

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

P.L. 86-36

USER-FRIENDLY PASSWORDS (u)

CRYPTOLOG has been the forum for several discussions on passwords, most of them in the vein of "what not to do." Here are some ideas of "what to do" that have proven useful to my co-workers and me.

At one time I had accounts on a Multics system, a large IBM system, and three Unix systems, all of which required passwords. I was really tempted to use one password for all of them. But I had been trained in the military to be sensitive to avoiding the use of crypto material from one system on another lest there be compromise. So I felt compelled to find some way of keeping the passwords for so many systems separate and yet easy to remember. Fortunately for me, I shared a group account on one of the systems. The group consisted of unusual people who got involved in a "more-security- conscious-than-thou" contest which taught me something about secure passwords.

From these two factors (the need to generate and remember several passwords and my group's security contest) came two easy rules to use to make your passwords more secure and a third to make them more easy to remember.

FOR THE SAKE OF SECURITY,
use passswords that:

* ARE LONG ENOUGH (6 to 8 characters long will do); and

* CONTAIN UPPERCASE LETTERS, NUMBERS, AND SPECIAL CHARACTERS.

Using these two rules will go a long way toward frustrating an exhaustive search for your password by someone else on the system. The mathematics behind these concepts can be simplified to comparing the possible number of four-letter, lower-case words (26^4 or 456,976 -- about half a million) on the weak side against the possible number of six-letter words using upper-case and lower-case letters plus numbers and special characters (92^6 or 606,355,001,344 --

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

about half a trillion, or about a million times as many). You can see that the longer the password and the bigger the character set from which it is drawn, the longer it would take, on average, for an exhaustive search to recover passwords.

There are smarter ways to recover passwords than through an exhaustive search. An interesting experiment was conducted in the early 1980's by a system guru who got permission to check on password usage in an agency system with users scattered all over the R Organization. He wrote a routine to compare the words in the UNIX spelling checker's dictionary with the list of passwords. He found that roughly half of the passwords were dictionary words and involved only lower case letters! Worse yet, some of them were only four or five letters long. Let us hope that after reading this article you will be having too much fun to use such puerile passwords.

TRULY MEMORABLE PASSWORDS
CAN BE FUN!

FOR THE SAKE OF HAVING FUN AND OF REMEMBERING YOUR PASSWORD EASILY, DRAW YOUR WORDS FROM SOME FAVORITE CATEGORY SUCH AS BASEBALL TERMS OR FLOWER NAMES

For example, if you enjoy baseball, your password for one month might be

ball&Bat

(note the use of a special character and a capital letter). The next month you might choose

61Maris

to celebrate Roger Maris' 1961 record of 61 home runs. Next you might use

O_fever *or* **>goCUBS<** *or* **LAisBad!**

(notice the use of upper case and special characters). I have found that anything humorous or emotional is easier to remember than something bland. For example,

3Stooges

would be easier for many people to remember than

3Donuts.

Moreover, passwords that call up vivid mental images are better than abstractions. For example,

Sinatra

would be easier for most people to remember than

Vocalist.

Another way of adding fun to your passwords is to replace letters with similar-looking special characters or numbers. For example the last two passwords could be written

$!na + ra** *and* **v0{al!$ +

If you do not already know, you will have to ask someone or experiment to find out which characters --such as # and @ in UNIX--cannot be used because they have special functions. Passwords like these are harder to type but lots more fun. This element of fun helps people set aside their old passwords for cute new ones. Sometimes I can hardly wait for the month to end because I want to start using a new password I have dreamed up!

Another fine idea for secure, memorable passwords is to think of a sentence with six to eight words in it and use the first letters as the password. Using the example of my security advisor:

I have five kids too many!

would become

Ih5k2m!

When I was involved with many computer systems at the same time, I drew the passwords for each one from a different category That was the only way I could think of to keep them all straight without writing them down Once a month I would have a psychic trauma when I had to change all of the passwords, but the categories helped me keep them straight

I have found a few problems with the mechanisms built into our machines to keep them secure. On the UNIX systems I learned the hard way that I could change to a nine-character (or larger) password and the "passwd" routine would not complain. However, when I tried to log in with it the system would not accept it. I

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

wish that both the passwd routine and the login routine would ignore anything beyond the eighth character. That way I could use my easy-to-remember passwords that exceed eight characters; the six-to-eight character range is too limited for my taste, but this is only a minor nuisance. A friend gets around this limitation by remembering to stop after 8 characters when his easy-to-remember password is too long. He would, for example, type in

BigBadWo

instead of BigBadWolf. As I said it is a minor nuisance.

Ludlow, however, goes beyond the nuisance of UNIX. For those of you who have never had to cope with Ludlow, a brief explanation is in order. In Ludlow-protected systems, the computer selects a password for the user; that is one way to keep people from using common dictionary words as passwords. The Ludlow passwords consist of nonsense syllables randomly chosen by the computer, such as:

SEN-SLES-GAR-BYJ

The combination of syllables is often hard to pronounce, let alone remember. The problem was so bad that Ludlow was "upgraded" to tell the user how to pronounce the password ("senseless garbage" in the case of the example)! Many users have developed their own technique for remembering their passwords: THEY WRITE THEM DOWN! This practice creates a different kind of security problem in place of the ones Ludlow supposedly overcomes. Worse yet, Ludlow strikes without warning. When Ludlow decides that it is time for a new password, it will cram one down your throat before it will let you log in the next time. My term for this kind of approach is "user-hostile!" Where were the Human Engineering advocates when Ludlow was developed? Ludlow is enough to make a dedicated time-sharer welcome a personal computer, even the ASTW!

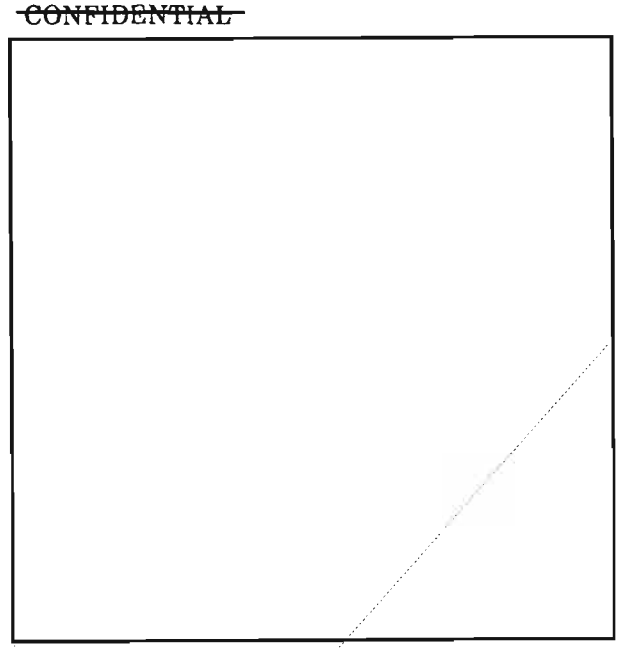
Actually, a combination of the UNIX and Ludlow approaches to renewing passwords would be more effective, secure, and user friendly. The UNIX approach is to nag the user into changing the password once the old one has gone stale, after 30 days. Unfortunately I have seen employees hardened to nagging who will put up with the UNIX reminders for extended periods rather than give up their comfortable old passwords. For such people I would like to see the reminder get some Ludlow teeth so that after a grace period the user would be forced to change before logging in. Ludlow also prevents people from engaging in the cute but unsecure practice of circumventing the UNIX renewal provisions by changing their password to something temporary and then immediately changing back to their comfortable old password.

This raises the point that no system is more secure than the way humans use it. Humans cannot design machines that other humans cannot circumvent. The people who use computers must of their own volition adhere to security procedures in order to minimize security risk. That is the main reason I have suggested these three easy rules for secure, user-friendly passwords. By making secure passwords more easy and fun, I hope to help people want to be more supportive of the security of the computers they use. □

SOLUTION TO CRYPTO-PUZZLE No. 29

(May 1985)

~~CONFIDENTIAL~~



~~(C-CCO)~~

EO 1.4.(c)
P.L. 86-36

DOCID: 4019705

ERRATUM

To the Editor:

I wanted to thank you for your help with my most recent article ["A Morality Play in One Act," Jan-Feb 1986], but I also must point out that the Xerox Star seems to have misplaced the various deadlines on Rosa Really's "Anatomy of a Project" chart by about 60 days each. I am enclosing a corrected version of the chart with hopes that you could publish this corrected version in the next issue.

Also, Rosa has pointed out to me that, while common usage frequently expands "PR" as "Purchase Request," the correct expansion is "Procurement Request." I have made this correction on the chart as well.

The Editor replies:

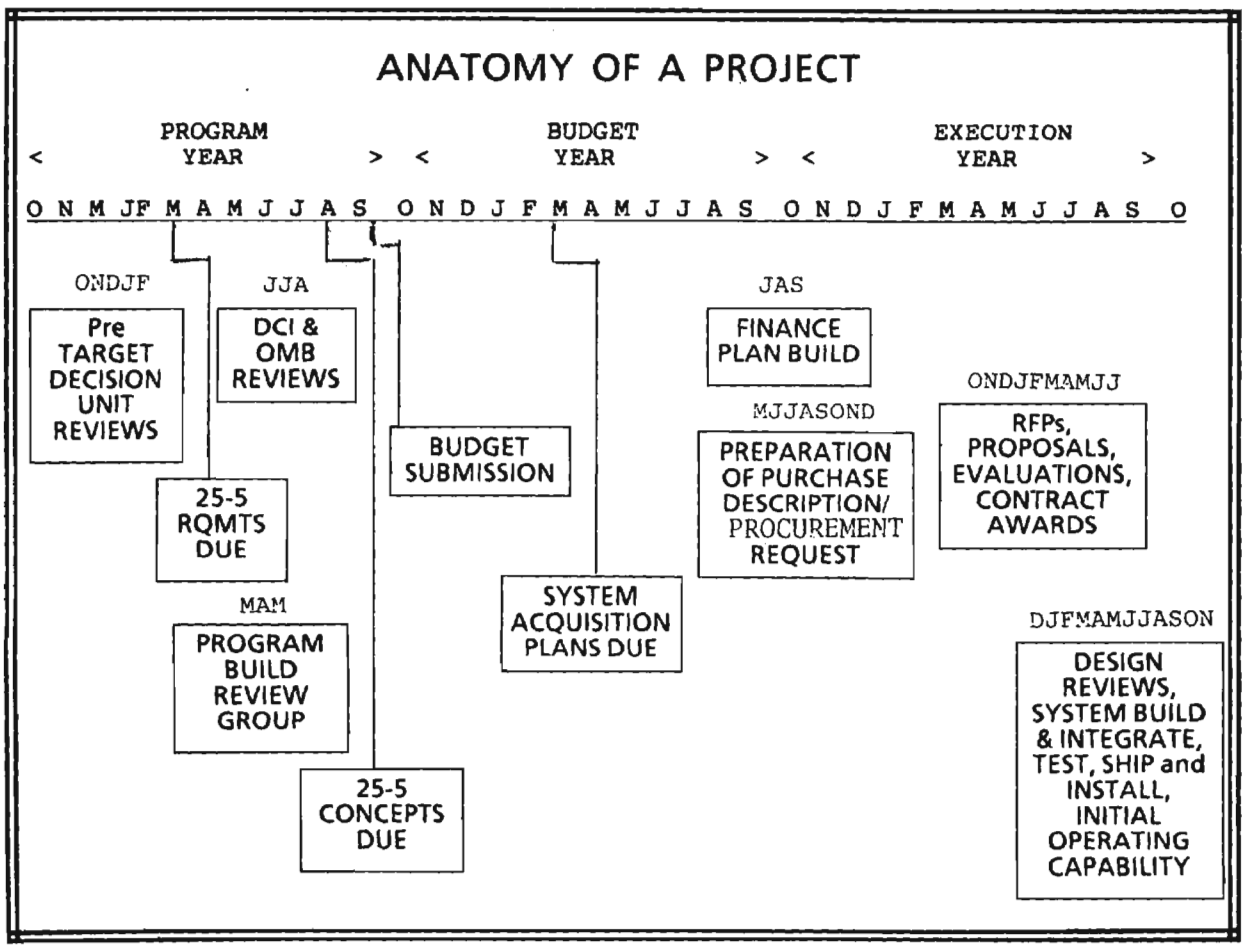
The Star apologizes for its error. These fancy word processors do take a lot on themselves !

The corrected chart appears below.

You're lucky to have Rosa and her eagle eye on your staff. CRYPTOLOG can use someone of her talents.

Any chance of borrowing her at press time?

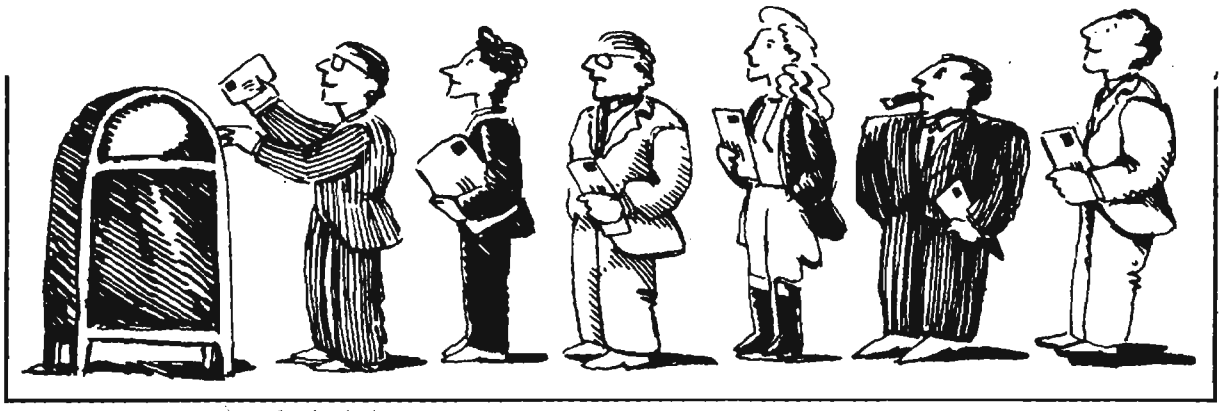
[redacted] P.L. 86-36



~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

Letters



EO 1.4.(c)
P.L. 86-36

To the Editor:

[redacted]

P.L. 86-36

To the Editor:

(U) Regarding the article "Why Do We Need Those Funny Alphabets?" in the November-December issue of CRYPTOLOG: the ASTW, under PC/IX, does support the 8-bit ASCII character set that was mentioned at the top of page 9. ASTW-PC/IX also supports the Cyrillic alphabet as an alternate character set. This alternate character set is accessed via the <LANG>key.

[redacted] T322

The author snarls: P.L. 86-36

(U) The ASTW can display 256 characters only by switching to the color mode (ASTW User,'s Manual, p. 17). This does not give the ASTW a full 8-bit capability, as is illustrated in Mel Deatherage's article on pp. 10-11 in this issue.

[redacted] *P16*

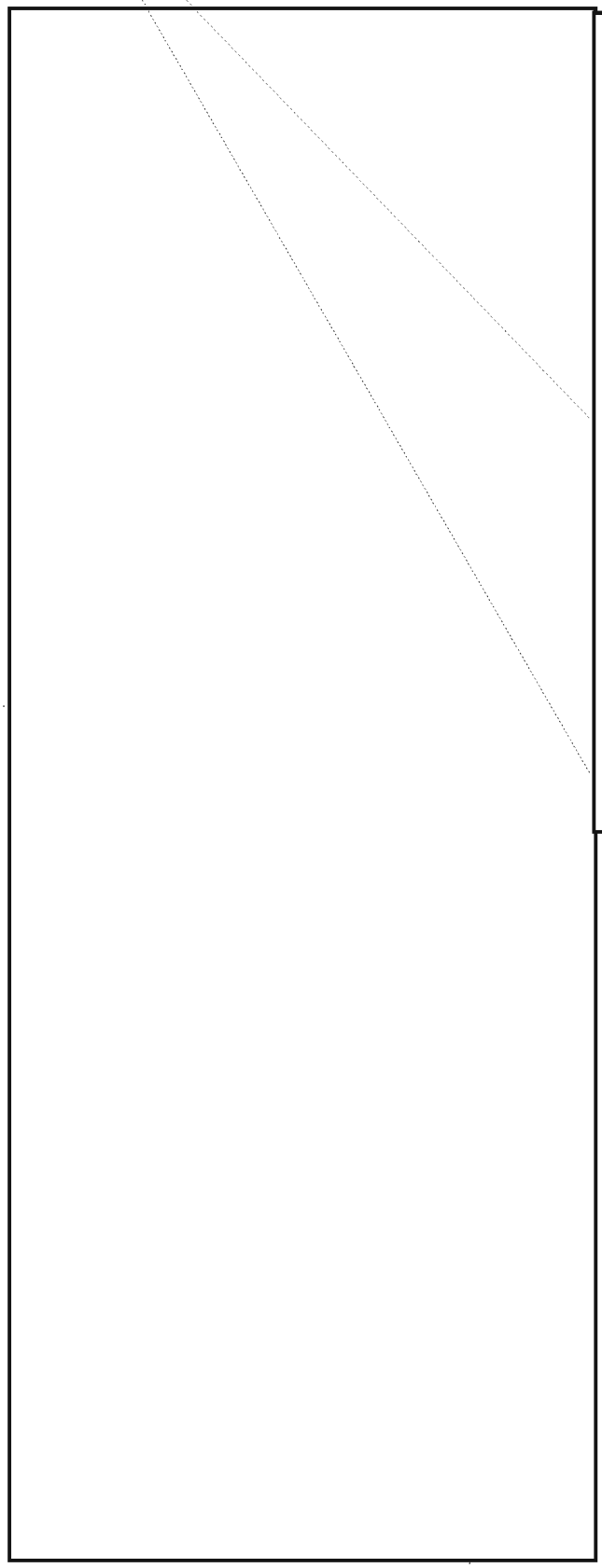
[redacted]

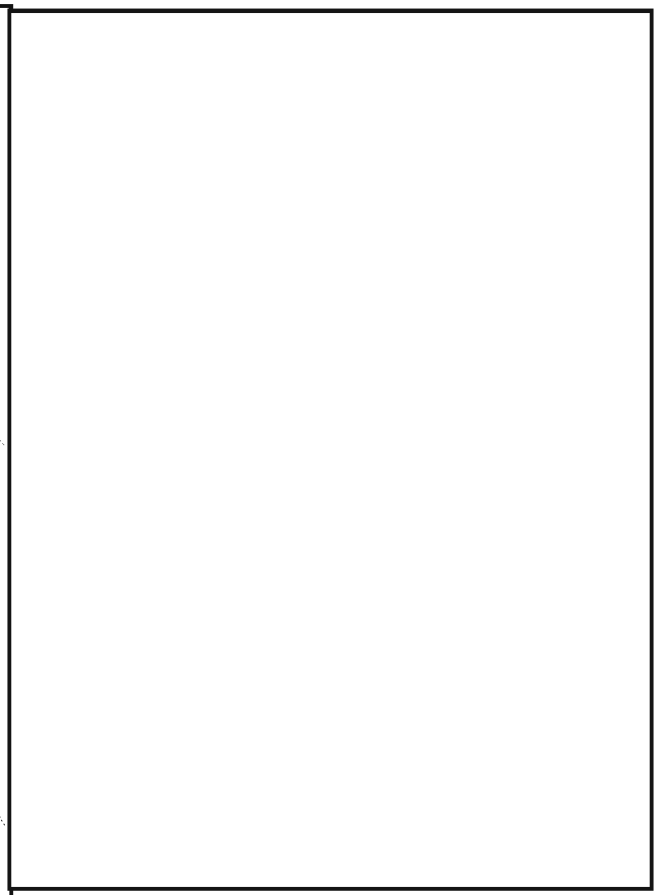
EO 1.4.(c)
P.L. 86-36

DOCID: 4019705

P.L. 86-36

~~SECRET~~





P.L. 86-36

To the Editor:

(U) Thank you for writing and publishing the help wanted ad for the SEASCAPE project. It provided an effective means of reaching the unique talent needed for the job, and opened it to a larger pool of people.

(U) The job is filled!

(U) Thanks again.

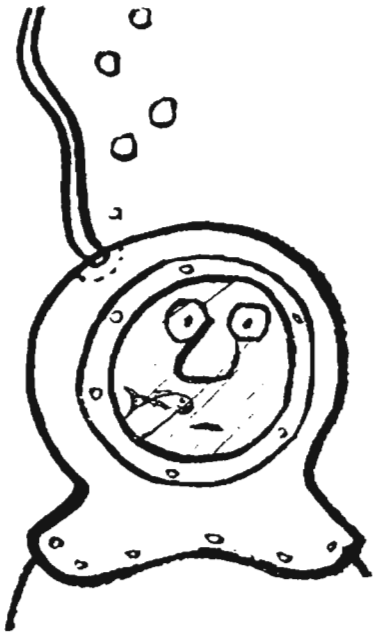
D/C. G434

P.L. 86-36

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4019705

OUT OF MY DEPTH #4 (u) wes



(U) Strictly speaking, this is a puzzle only in lay terms, in that a cryptogram can be viewed as a kind of puzzle. Cryptanalysts will recognize it as a standard school exercise and may give it a miss.

~~(FOUO)~~ You are given three clues besides the line-up of the messages. One is free key (that's the digit **5** sitting up there by its lonesome). The second is the meaning **period (.)** for the intermediate plain dinome **56**. The third is the stereotypic message ending **56 = period**.

(U) If you need more to go on, write for instruction, **do not call**, to The Puzzle Editor, CRYPTOLOG, P1.

EO 1.4.(c)
P.L. 86-36

DOCID: 4019705

READERS' SURVEY

As an experiment we used a variety of fonts and spacings in this issue.

Which do you find easiest to read?

Please number your preferences 1-15, best to worst, and send this sheet (or a copy thereof) to:

Editor, CRYPTOLOG, P1, HQ 8A187.

___ ODYSSEY

___ EFFECTIVE C3 ANALYSIS

___ A LINGUIST MEETS THE ASTW

___ AI AT NSA

___ PRESERVING DOCUMENTS

___ TEAM BUILDING

___ PASSWORDS

ERRATUM

___ [ ]

___ Editor

LETTERS

___ [ ]

___

___

___

___

___

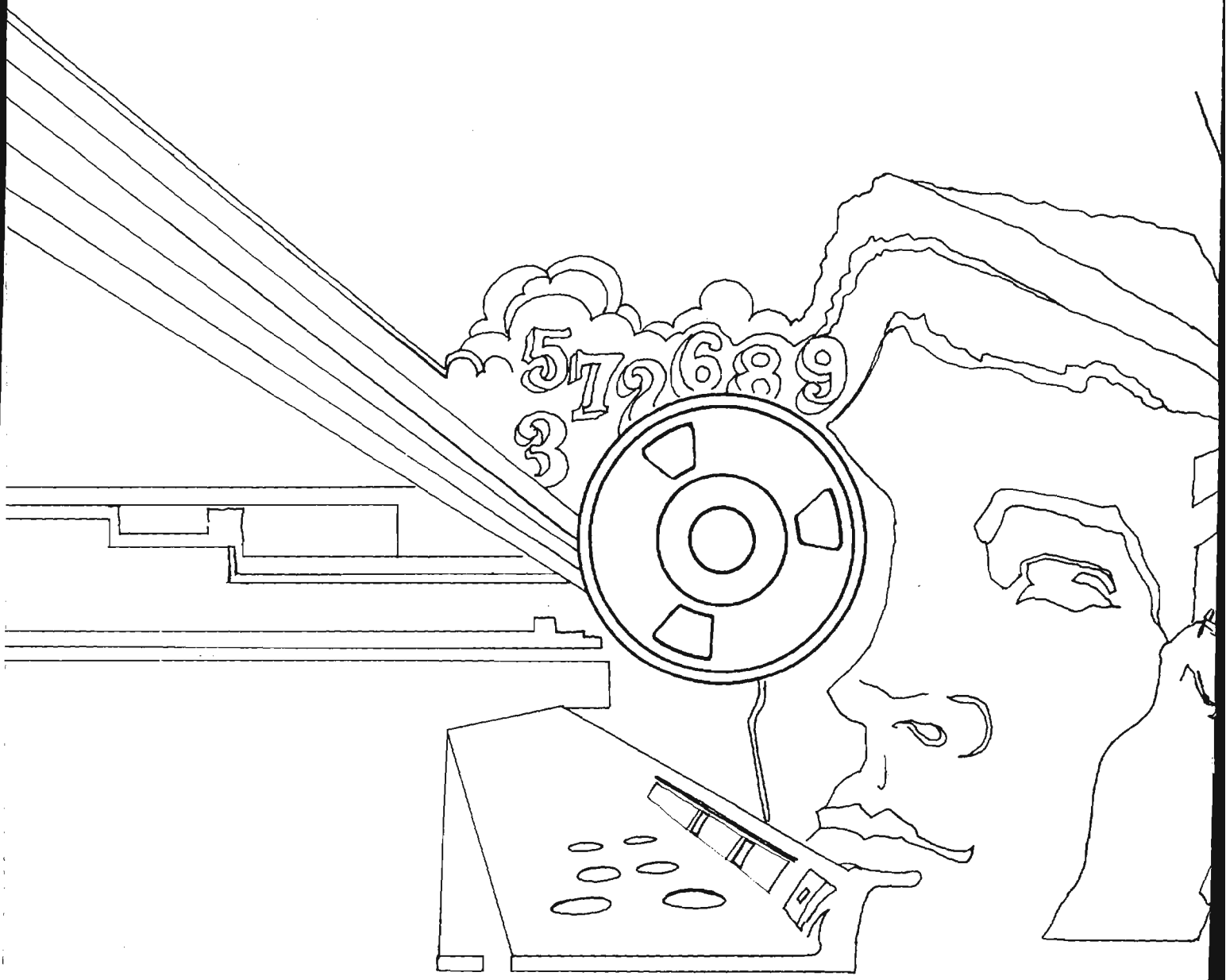
P.L. 86-36

COMMENTS

Optional: Name, Organization, Secure Phone

~~FOR OFFICIAL USE ONLY~~

P1-JUL 86-Y1-111512


5726893

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009980

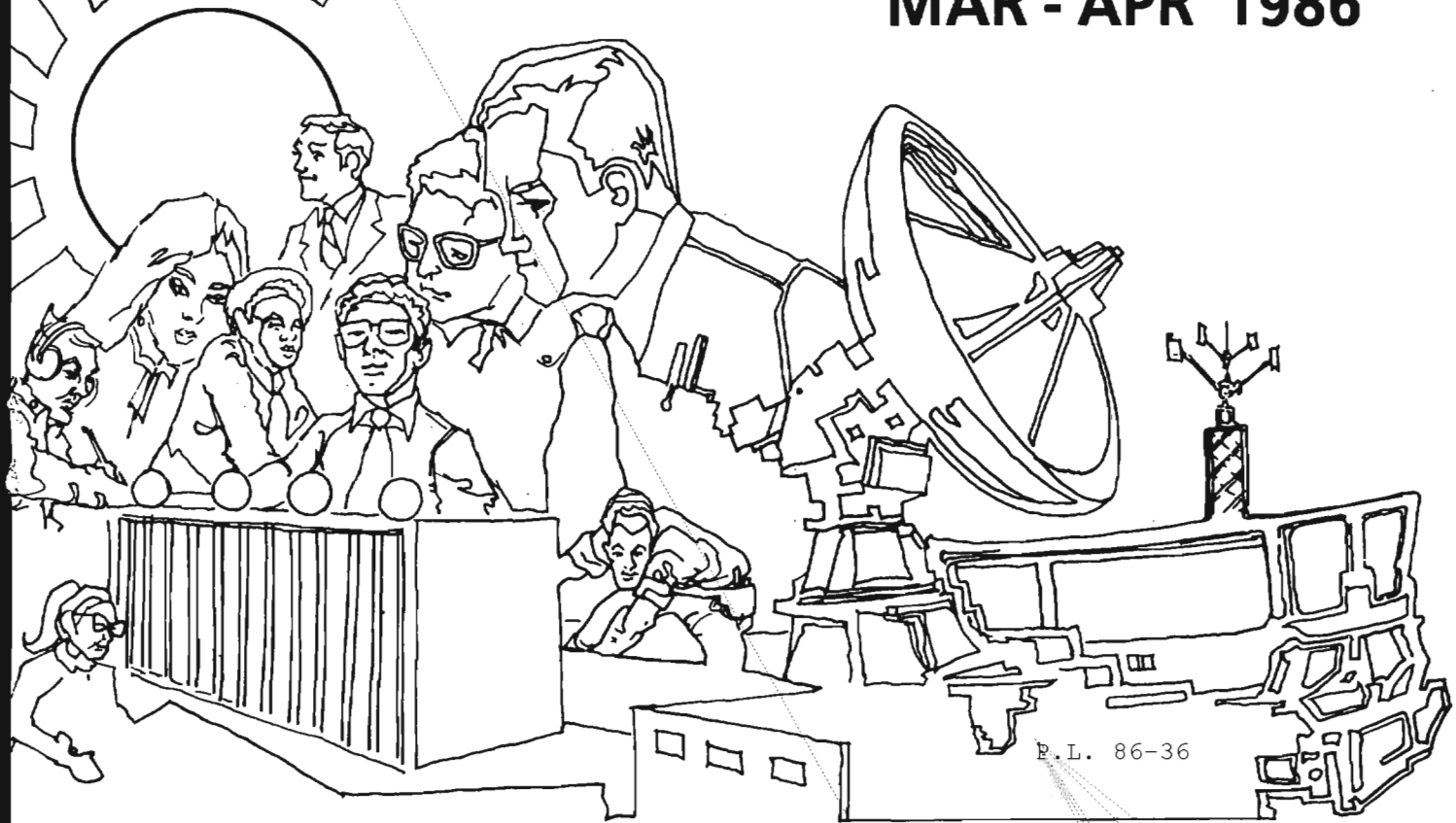
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

EO 1.4.(c)
P.L. 86-36

MAR - APR 1986



P.L. 86-36

[redacted] . . . 1
EXPERT SYSTEMS--FOR NSA? (U) . . . . . [redacted] . . . 4
BULLETIN BOARD (U) 6
AN INTRODUCTION TO AI (U). . . . . [redacted] . . . 7
LEVELS OF CLASSIFICATION (U) . . . . . [redacted] 10
THE 39 STEPS (U) . . . . . [redacted] 11
PUZZLE (U) 13

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

~~NOT RELEASABLE TO CONTRACTORS~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

DOCID: 4009980

CRYPTOLOG

P.L. 86-36

Published by P1, Techniques and Standards

VOL. XIII, Nos. 3-4 ..... March-April 1986

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Collection ..... (963-5877)
Computer Security ..... (968-8141)
Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5230)
Cryptolinguistics ..... (963-1596)
Index ..... (963-5330)
Information Science ..... (963-1145)
Intelligence Research ..... (963-3095)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-3648)
Science and Technology ..... (963-4191)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-5734)

Illustrator ..... (963-3057)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptolg at bar1c05
(bar-one-c-zero-five)
(note: no 'o' in 'log')

Always include your full name, organization, and secure phone number.

For Change of Address
send name and old and new organizations to:
Editor, CRYPTOLOG, P1

Contents of CRYPTOLOG should not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

TIGHTENING OUR BELT (U)

Like everything else in the federal government, CRYPTOLOG has been affected by budget cuts, but to an even greater extent. As a Class 1 publication in the Defense Department we have been ordered to cut by 55%.

That's a lot for a spartan periodical with nary a frill, ruffle or furbelow to do without. We don't use color, the paper is minimum quality usable on a press, and the format is the most cost-effective. Even so, in the past year we've done what we could to bring costs down:

- For word processing we've moved to the Xerox Star from the Unix Editor on the BARDOLPH TSS, resulting in impressive savings in labor costs, especially in making printouts and in doing layouts;
- To avoid retyping we're using the Data Conversion Center for converting floppies made on other word processors;
- We've gone over to the high-speed Solna press which is more economical but prints only multiples of 16 pages;
- We're publishing half as many issues;
- We are down to a one-person staff (the editor) who has other duties as well;
- We are trimming the distribution list.

We can use your help on this last item:

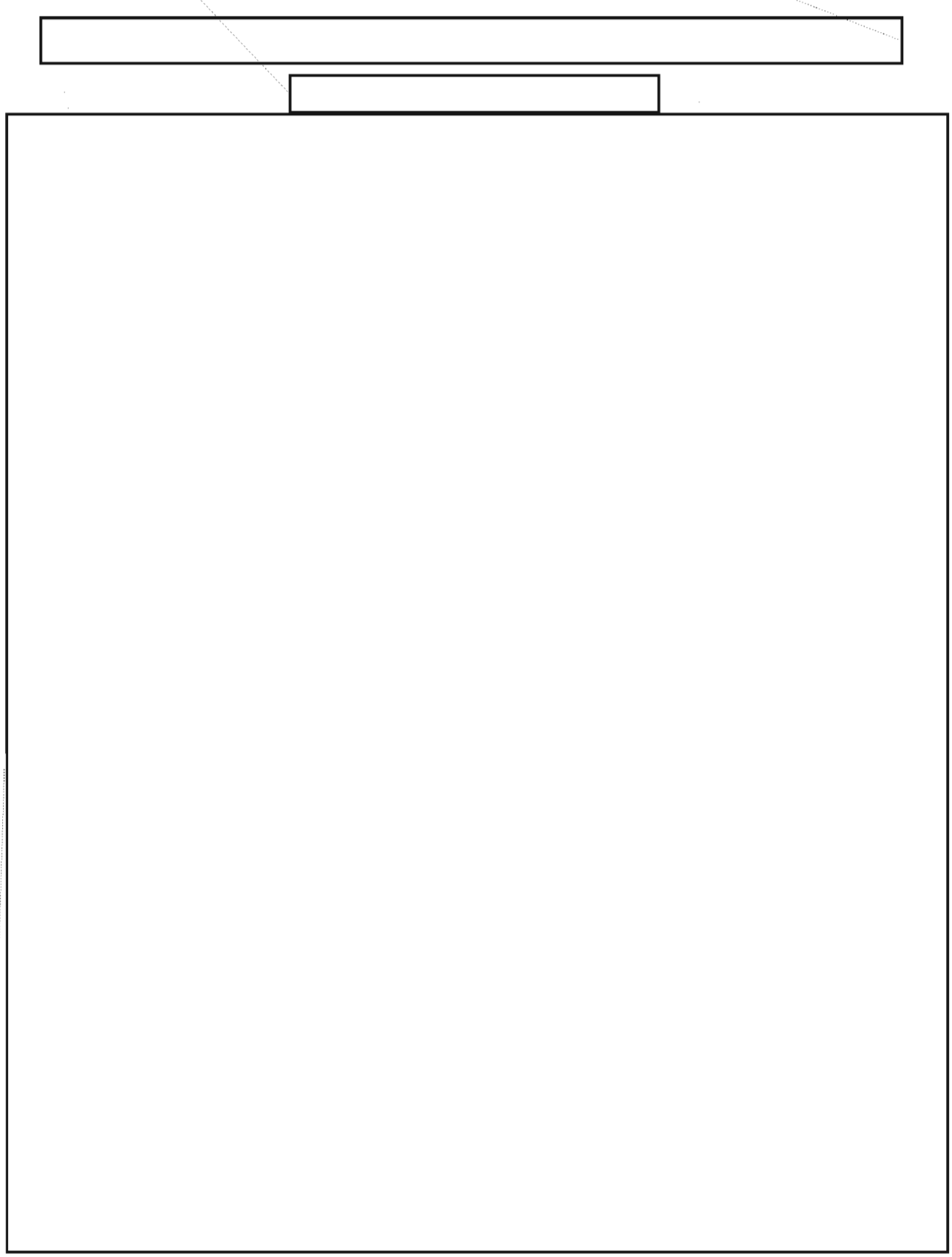
- If you are going to the field or into retirement, let us know so that we can remove your name from distribution. (Organizational, not personal copies, are sent to the field. You can have a personal copy again when you return.)
- If your organization is now smaller than it was, request fewer copies.
- As the number of personal copies in your element increases, eliminate an appropriate number of organizational copies.

Thanks.

~~FOR OFFICIAL USE ONLY~~

OCID: 4009980
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

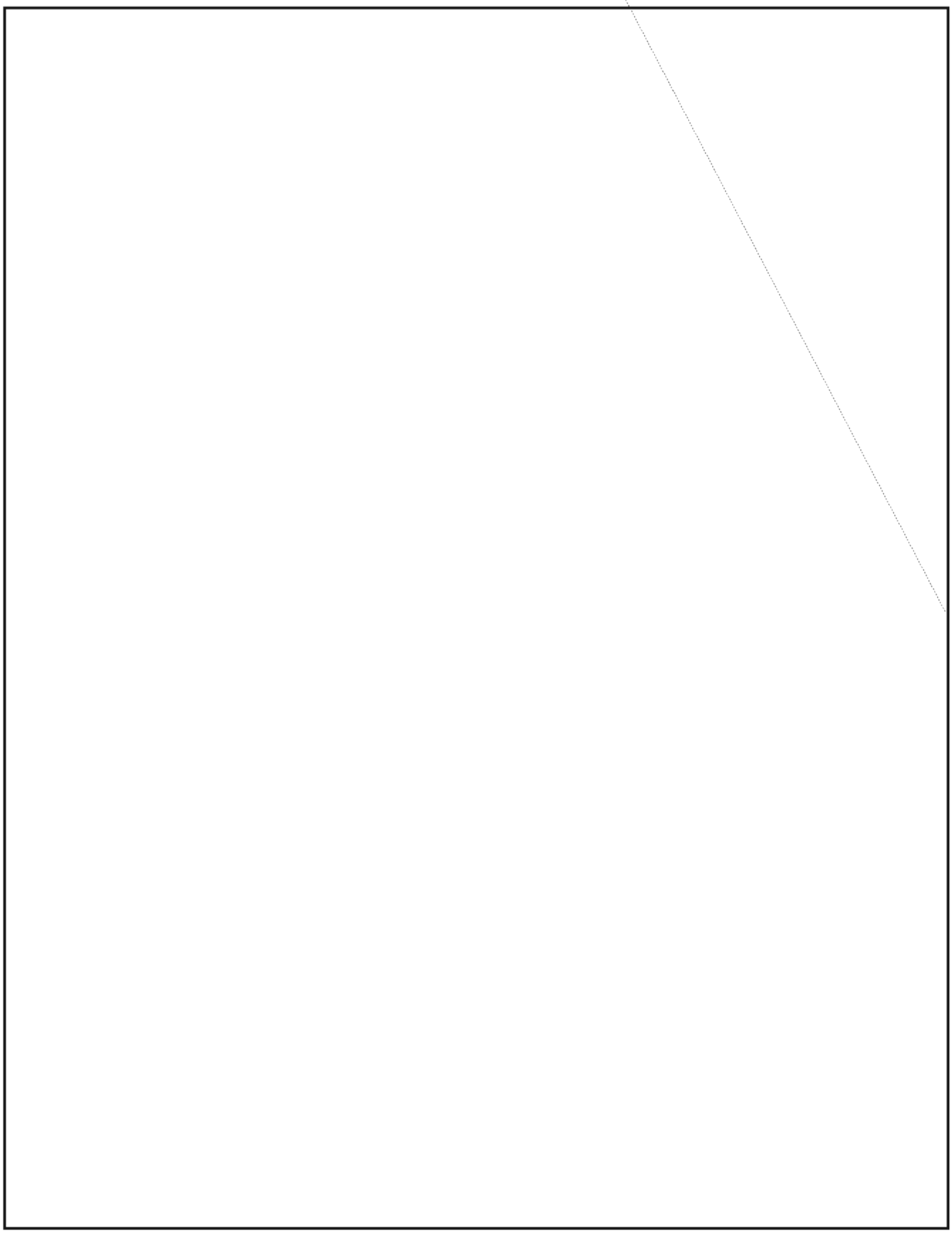


P.L. 86-36
EO 1.4.(c)

DOCID: 4009980

P.L. 86-36
EO 1.4.(c)

~~SECRET~~

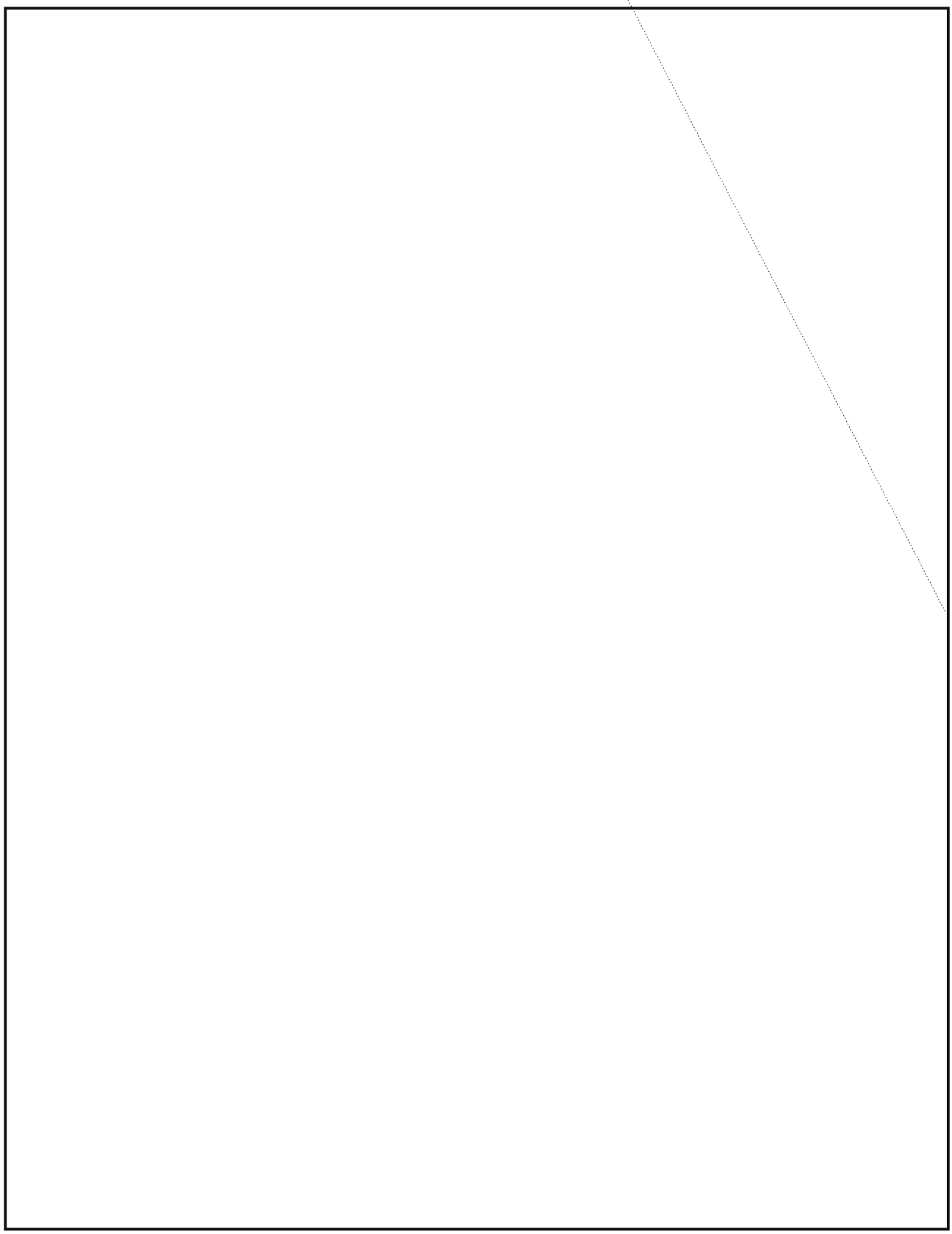


~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

DOCID: 4009980

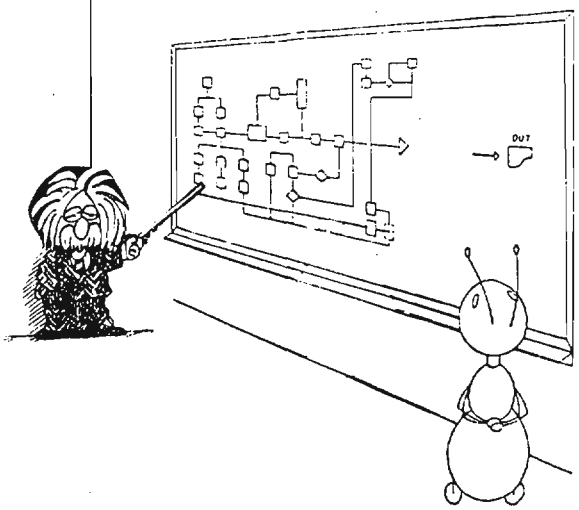
P.L. 86-36
EO 1.4.(c)

~~SECRET~~



DOCID: 4009980

P.L. 86-36



EXPERT SYSTEMS--FOR NSA?
(u)

One of the more profitable advertising gimmicks in computer software today is the use of the word "expert." Numbers of products claim to be "expert systems" or to have "expert" capabilities. After we cut through the hype, do we find that expert systems actually have any value? When are they useful? Can we use them at NSA?

WHAT CAN AN EXPERT SYSTEM DO?

In general, an expert system starts with a set of facts, obtains more facts from the user through interaction, and,using a database of knowledge about the application, produces a reasoned conclusion. The system can, in most cases, explain its conclusion by displaying the logic chain.

An expert system is very good at applying heuristic rules (rules of thumb) to a set of loosely related data, and deriving a conclusion -- much like an expert does. It has been said that an expert is one who jumps to the right conclusions, because the expert picks just the few facts that are important to a conclusion, often bypassing complex computations, and arrives at a conclusion while other people are still sifting facts.

An expert system on a computer can be used to record the heuristic rules that a particular expert uses -- to "clone" the expert. This can be used to spread the expertise around or to substitute for an expert who is leaving. It can also be used to train new experts -- to organize the expertise so that it can be taught. The expert system leads the student through a correct logic chain with sample data, an improvement over traditional computer-aided instruction systems that merely quiz a student repeatedly.

Putting rules into a knowledge base can help to organize knowledge that was not well understood or not centrally located. Books and papers can also be used for these purposes, but the user interaction with the expert system gives it an advantage. Also, the expert system actually tries to apply the knowledge; it does not just serve as a repository for that knowledge.

An expert system could be used to explain rules and regulations, particularly those that have accumulated over time and are not logically consistent. Expert systems have been used most successfully to diagnose problems in expensive, complex mechanisms.

WHAT IS AN EXPERT SYSTEM?

I use the term "expert system" narrowly, to refer to software that separates the application domain knowledge from the program's control structure and that can explain its reasoning to a user. The repository of domain knowledge is commonly called the "knowledge base" (as in "data base") and the program control structure an "inference engine." This is a specialized program to read the knowledge base and process it logically to derive some conclusion or conclusions.

The most common class of expert system building tools, or shells, on the market today (there are dozens of them) use a knowledge base of rules in the form of "IF some condition or conditions THEN some condition or conditions." The conditions usually are expressed as a parameter/value combination, and may refer to other rules, which are determined to be true or false in a chain of logic going back to data entered by the user or sensed by the system externally. This chaining usually goes backward from a "goal

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009980

rule" to the original data, but may go forward from a set of data to one or more conclusions (see box). Key to the usefulness of the expert system is the fact that the sequence of rule use is data-driven and may vary drastically in different runs. The inference engine selects rules, as needed, and chains through the knowledge base in the most efficient manner.

Most expert systems have some ability to handle uncertain data. A piece of data can be true, not true, or somewhere in between: probably, possibly, not likely, almost certainly, almost certainly not, etc. Data that is "probably true" pushes the system in the direction of a positive conclusion, and data that is "probably false" pushes the system in the opposite direction.

In addition to dealing with uncertain data, most expert systems have some mechanism for handling unknown data, by assigning a medium value, or extrapolating from known data, or by ignoring the rules involving unknown data.

Some expert systems have mechanisms for representing knowledge in some form other than simple rules; e.g., complex data objects that can have different kinds of values, or attributes, and can inherit attributes from certain other objects.

PROBLEMS WITH EXPERT SYSTEMS

Some knowledge simply doesn't need to be organized in a randomly arranged data base. The steps follow each other in a purely sequential fashion, and the solution can be programmed more simply and efficiently in a traditional programming language.

The structure of knowledge representation is very important. Considerable thought needs to be given to this, just as you would give considerable thought to the design of an important and complex computer data base.

Inexact reasoning is a black hole. Although it is possible to combine values that are inexact, no one has proven that one way of doing this is better in a general sense than any other way. It appears that some methods are better for some applications, some for others, but the selection of a method is not well understood.

Conflict resolution can be tricky. The inference engine matches patterns of rules to find the best rule to apply in any particular instance. If two or more rules match the pattern, some conflict resolution technique must be used. There is not a good understanding of how to resolve these conflicts.

Expert systems tend to use up large amounts of computer resources -- both time and memory. Most of the smaller systems are severely limited in the number of rules they can process (one of the most successful expert systems, DEC's XCON, uses 8000 rules; a system which runs on an IBM PC might be limited to as few as 100 rules).

SAMPLE RULES: KNOWLEDGE BASE

1. if SCREEN is BLANK
   then POWER is OFF (0.5)

2. if KEYBOARD is not WORKING
   then PROGRAM is HUNG (0.4)

3. if DISPLAY is ERROR
   then PROGRAM is HUNG (1.0)

4. if PROGRAM is HUNG
   then FIX is CTL-ALT-DEL (0.5)

5. if POWER is OFF
   then FIX is SWITCH POWER ON (1.0).

6. if FIX is KNOWN
   then DIAGNOSIS is COMPLETE.

Forward Chaining: The system tries rule 1; if the screen is blank, then rule 1 concludes that the power is probably off (confidence factor of 0.5). The system then looks for (chains forward to) a rule which is true if the power is off (rule 5). Rule 5 then says that the fix is to switch the power on. Once the fix is known, rule 6 concludes the diagnosis. If the screen is not blank (rule 1), the system tries rule 2, and then rule 3, until it either exhausts the knowledge base or finds a rule that works (whose premise is true). Any chain of rules which reaches the goal rule (rule 6) ends the program.

Backward Chaining: The system starts with the goal rule (rule 6). If the fix were known, it could stop. It therefore looks for a rule which, if true, would make the fix known (rule 4 or rule 5). The system picks rule 5 and checks its premise (is the power off?). Rule 5 chains backwards to rule 1; if the screen is blank, the power is probably off, and the fix is to switch the power on. If rule 1 is false, the chain fails, and the system must try another chain; it tries rule 4, which chains to either rule 2 or rule 3. The system continues backtracking through the knowledge base until it either completes a valid chain or exhausts the rules.

EXAMPLES OF EXPERT SYSTEMS

Until recently, all expert systems were built to run on mainframe or mini computers. Only in the last couple of years have PC-based tools entered the market.

One of the oldest expert systems is MYCIN, developed at Stanford University to diagnose infectious diseases and to prescribe antibiotics.

~~FOR OFFICIAL USE ONLY~~

Although MYCIN has never been used operationally, its techniques have been copied by many commercial expert system packages.

One of the most successful expert systems is DEC's XCON, which configures DEC computer systems. Using 8000 heuristic rules, XCON takes a customer's order and identifies all the parts that are needed to fill the order, making sure that they all fit together. DEC estimates that XCON saves the company at least $18 million a year. Before XCON was built, the human experts found the task boring most of the time and therefore made numbers of mistakes. Traditional programs had been tried but didn't work; the rules kept changing, the knowledge was scattered, and the totality of the logic was not well understood.

More recently, and on a smaller scale, the Campbell Soup company built a small expert system on a PC to diagnose breakdowns in their giant soup cooking machines. A few hundred rules enabled a non-expert to diagnose most problems effectively.

The General Electric company built an expert system to diagnose GE locomotive problems. The improvement in repair time was so dramatic that GE's market share increased by a large margin.

Autometric, an NSA software contractor, is developing an expert system to diagnose software problem reports. They estimate that the prototype system, with about 200 rules, correctly identifies a problem module about fifty percent of the time, saving about four hours of diagnostic time each week. Eventually, the system should enable a relatively inexperienced programmer to solve most software problems. One of the chief reasons for developing this system was that the experts who had designed and built the software didn't want to maintain it, and staffing became a problem.

Burroughs has a prototype expert system to diagnose personal computer problems for users calling a Burroughs hot line. This hot line has been staffed by experts, who are bored to tears by the mundane problems posed by most callers. The expert system will enable an unskilled person to answer the hot line and effectively diagnose most user problems. The experts will then work only on the more challenging problems.

[redacted] in R8, has developed a PC-based expert system to identify the classification of cryptanalytic information, according to a set of rules published by P1.

R53 researchers are working on a number of expert systems, including one to support DEFSMAC. Other expert system experiments are underway in G4, P1, W1, A2, and T3.

BUILDING YOUR FIRST EXPERT SYSTEM

Pick a problem. Use the criteria described in "Selecting Your First Application," and add other criteria if they are important to you. Pick a problem you know well, one that looks too small to bother with (because it probably will take more work than you thought), but pick a problem that matters to someone -- preferably your boss.

Pick an expert. You want someone who really is THE expert, and who wants to help. If you are the expert, so much the better.

Develop a prototype. Set some relatively short period of time, and see what you can do in that period. The schedule depends on your problem, of course, but three to six months should be enough to accomplish something that can be evaluated.

Evaluate the performance of your prototype system. Does it make a good decision or provide satisfactory advice? Evaluate the reasoning process: do those right answers come from a valid line of reasoning? Is the user interface acceptable for operational use? Does the system run efficiently enough to be usable? Will it still be usable when you get the full system (more rules) built? Will the system be cost-effective when compared to the current (manual) way of doing it?

Proceed with incremental development of an operational system, if your evaluation produces acceptable answers to your questions. If the answers don't look good, you need to fix whatever is wrong, or go back and try a different application (or, possibly, you need a different expert system building tool).

Prepare the users for using the system. This is the most important item, if you are building an operational system. DEC's XCON almost failed, after three years of research, because the people doing the work manually thought (erroneously) that the system would replace them and they would lose their jobs.

~~FOR OFFICIAL USE ONLY~~
P.L. 86-36

OCID: 4009980

P.L. 86-36
EO 1.4.(c)

SELECTING YOUR FIRST APPLICATION

Your application doesn't have to match all of these criteria, but the more items it matches, the better your chances of success.

- **Traditional technology doesn't work.** Before DEC hired CMU to build R1, they tried three times to write the program in FORTRAN.
- **The knowledge domain is narrowly defined and primarily involves logical deduction.** One way of looking at it is to ask if a human expert could solve the problem over the telephone.
- **Recognized experts know how to solve the problem.** You will have trouble teaching a machine how to solve it if you don't know how yourself.
- **The task involves a few minutes to a few days of an expert's time.**
- **A traditional approach to solving the problem requires combining a large number of steps in a large number of complex sequences.**
- **Wrong answers will not result in loss of life, or other unacceptable consequences.** Because of the heuristic rule approach, optimal results are not guaranteed.

P.L. 86-36

- **The resulting system will have a high payoff.** You don't want to put a lot of effort into a system that doesn't really do anything.

[redacted] In hardware or software support, an expert system might help diagnose problems in large, complex computer systems, or analyze network performance problems. An expert system might assist with computer language translation when the two languages involved have different structures (for example, from FORTRAN to Ada).

GETTING STARTED

If you are interested in developing an expert system, look around; there is probably someone not too far away who is experimenting with the technology and can help you. If you don't find someone close at hand, call [redacted] He is chairman of the NSA Artificial Intelligence Working Group, and he can put you in touch with a number of people to talk to. □

BULLETIN BOARD

[redacted]

Dave Fitzpatrick E42 968-8418

[redacted]

Bill Patterson B5093 963-3490

[redacted]

SOLUTION TO NSA-CROSTIC No. 62

[Arthur J.] Salemme, "Joys of Plural Dropping," *CRYPTOLOG*, January 1978.

"When our daughter and a friend of hers were both five and were eating lunch at our house, my wife gave them each a sandwich and a slice of American cheese cut in strips. The little friend particularly [enjoyed] the latter and asked what they were. `Cheese,' she was told. `Well, then,' she asked, `can I please have another chee?' "

P.L. 86-36

P.L. 86-36

CID: 4009980

AN INTRODUCTION TO AI (U)

P.L. 86-36 [redacted] H111/G924

This is an abridgement of an article that appeared in the February 1986 issue of the Cryptanalysis Intern Bulletin.

Artificial intelligence (AI) comprises elements of many disciplines. It was once explored only by academics; now it has become a topic of vital interest to both government and private industry. It is worthwhile for the cryptanalytic community to familiarize itself with developments in AI because of potential applications to cryptanalytic tasks.

The history, characteristics, and applications of artificial intelligence provide a fascinating exploration into the essence of the interaction between man and machine that characterizes contemporary human existence.

DEFINITION AND HISTORY

Although the discipline known as AI has been in existence for over thirty years, no single definition is accepted by all the experts. A survey of definitions given by leaders in the field, however, has yielded these concepts in common:

1) AI seeks to enable a machine to perform

- tasks traditionally thought to require human intelligence,

- in a manner approaching the working of the human mind.

This pursuit includes research in the cognitive sciences, in an effort to understand more fully the human capabilities upon which intelligent machines are to be modeled.

2) AI is distinguished from conventional computer science by its focus on symbolic rather than numeric (qualitative rather than quantitative) processes.

New capabilities for enabling machines to imitate man have been created as a result of fundamental developments in diverse fields, including computer science, the psychology of learning, physiology, and information science. The work of cryptanalyst Alan Turing (hypothesizing a machine that could perform mathematical operations in a binary format and developing a test to evaluate whether a disguised correspondent was machine or human), Claude Shannon (applying Boolean algebra to electronic circuitry), and Norbert Wiener (cybernetics) are only a few examples of contributions that made AI possible.

The term "artificial intelligence" appeared concurrently with the first major event to bring together from a variety of academic backgrounds those who shared a common interest in enabling machines to perform intelligent tasks. The event was the 1956 Dartmouth Conference, organized by John McCarthy and attended by others who were to become prime movers in the field in subsequent years. Although the Dartmouth Conference did not yield the results predicted, it did set the atmosphere for interdisciplinary cooperation and challenge. In addition, two conference participants, Allen Newell and Herbert Simon, both connected with Carnegie Tech (now Carnegie Mellon) and the RAND Corporation, came to the conference with a working program demonstrating the intelligent processing of information that conference participants had discussed and sought.

During the 1950s and 1960s, expectations were high that machines could be programmed to imitate human thinking in the realm of common sense, that is, everyday acts of reasoning that are performed by most people without conscious recognition of the processes involved. As the passing years revealed the unexpected complexity of this task, AI in the 1970s was marked by a philosophical and methodological shift toward specialization. Programs were written that would enable a particular machine to perform intelligently within a very limited domain. In addition, whereas once the goal was to equip a computer with a general set of theories that would enable it to make a wide variety of decisions, the

~~FOR OFFICIAL USE ONLY~~

OCID: 4009980

focus shifted to providing an impressive array of facts about a given topic.

Since the late 1970s, a major trend in AI has been commercialization. What was once a topic that concerned academics and a limited number of research corporations has now become an industrial and a governmental fad of sorts, especially within the US Department of Defense. Moreover, AI is an integral part of an emerging technical war between Japan and nations of the West. In 1982, Japan announced a massive computer research initiative to take place during the next ten years. Entitled the "Fifth Generation of Computer Systems," the project aims to put Japan in the forefront of world computer technology by the 1990s. Many of the project's goals fall into the area defined as AI. Response to the challenge was not slow in coming: Britain, Europe and the United States initiated efforts related to those of the Japanese. AI is included in DARPA's (Defense Advanced Research Projects Agency) ten-year development program and in the plans of MCC (Microelectronics and Computer Technology Corporation), a corporation of 21 companies under the leadership of former NSA Director Bobby Inman.

AI PROCESSES AND APPLICATIONS

AI software has developed in channels largely unknown to conventional programming languages. Instead of using essentially linear reasoning, AI programs endeavor to imitate the flexibility of the human mind. LISP, developed in 1958, is the most popular programming language used by AI experts in the United States. Short for List Processing, LISP allows the organization of data in network-like structures. "Items" of data may be descriptive statements, lists, or many other data groupings. "Frames" and "scripts" are two popular ways of storing information. Frames contain slots into which data is inserted; scripts have a similar structure, including a series of scenarios into which the data might be expected to enter.

The hardware associated with AI falls into two categories: computers designed especially for AI usage, and AI adaptations of other computer systems. Advertisements describing AI systems reveal AI-related innovations: use of "windows" and a "mouse" pointer to allow greater flexibility in examining the relationships between data sets, the adaptation of computer graphics to capture the essence of symbolic processing, and a variety of developmental tools to assist the programmer in formulating programs that exploit all of the networking potential of AI languages. Many of these features are being used in areas other than those associated specifically with AI.

One AI application that is now receiving much attention is the development of expert systems. This is described in another article in this issue.

Other areas of artificial intelligence are also the objects of intensive research efforts. Natural language processing is the ability to program and receive feedback in a conversation-like context. Computer vision and speech recognition are receiving attention from DARPA for their defense potential. In addition, robotics, educational computer interactions, and a variety of office workstation uses for AI are currently under investigation, and in some cases, implementation.

PROSPECTS FOR AI

It soon becomes apparent that scientific opinion is divided regarding the ability of AI to substantiate its claims. The early AI pioneers were premature in declaring their ability to convert the mysteries of human intelligence to machine form. Although the people currently at the forefront of AI development communicate a more cautious and realistic outlook, the recent transformation of AI into a prime business venture has subjected the discipline to the exaggerations of commercial advertising.

While AI is still in development, significant contributions have already come from AI research and technology. AI professionals are quick to recognize that the potential of machine capabilities has barely been tapped. The next decade should prove critical to the question of whether AI is able to prove itself to the rest of the scientific community, as the concerted efforts of government, universities and industry seek to overcome the current limits of computer technology.

ACKNOWLEDGMENTS

A major source of information was Agency personnel who are currently active in AI research. [redacted] were all generous in sharing their time and personal resources in helping to explain AI.

P.L. 86-36

Books and Articles Used

[redacted] "Artificial Intelligence Expert Systems," NSA briefing,1985.

McCorduck, Pamela. *Machines Who Think: A Personal Inquiry into theHistory and Prospects of Artificial Intelligence.* San Francisco: W.H. Freeman, 1979.

Mishkoff, Henry C. *Understanding Artificial Intelligence.* Dallas, Texas: Texas Instruments, 1985.

Waldrop, M. Mitchell. "Artificial Intelligence." *Science* reprint (from 24 February 1984, 23 March 1984, 27 April 1984, 15 June 1984, 10 August 1984 and 14 September 1984). □

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009980

P.L. 86-36

★ LEVELS OF ★ CLASSIFICATION (U)

★ [redacted] P05/SAO

(U) Recognized classification levels and the factors involved in establishing them are as follows:

~~(TS-CCO)~~ **TOP SECRET** shall be applied only to information or material when its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.

~~(S-CCO)~~ **SECRET** is used for information or material the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security.

(U) **CONFIDENTIAL** is the appropriate classification when the unauthorized disclosure of the information or material in question could reasonably be expected to cause identifiable damage to the national security.

(U) **UNCLASSIFIED** material will not normally be marked or stamped **UNCLASSIFIED** unless it is essential to advise the recipient of the material that it was examined in order to assign a classification, and was then determined not to require one.

"FOR OFFICIAL USE ONLY"

(U) The caveat **FOR OFFICIAL USE ONLY (FOUO)** is a unique marking in that, although it can be used to preclude public dissemination of certain information, it is not in itself a level of security classification. The rules governing the use of this handling instruction can be quite confusing, so we often decide, or are told by others, to mark an item **FOUO** without understanding its meaning, the impact of its use, or whether it may be legally used in a given context.

(U) Certain information that has not been given a security classification under the criteria for assignment of **CONFIDENTIAL, SECRET**, or **TOP SECRET**, may be marked **FOUO** and withheld from the public domain under Freedom of Information (FOI) Exemptions. Additionally, at NSA, such unclassified information is generally covered by Public Law 86-36, the National Security Act of 1959. Section 6 of this act states, " ... nothing in this act or any other law ... shall be construed to require the disclosure of the organization or any function of the National Security Agency, of any information with respect to the activities thereof, or of names, titles, salaries, or number of the persons employed by such Agency." Thus, this Act provides **FOR OFFICIAL USE ONLY** protection of our organizational designators, unclassified missions and functions, budgetary information, and personnel strength. Only information that has not been previously available to the public may be marked **FOUO**.

(U) Included among the FOI exemptions permitting **FOUO** protection are:

(1) Regulations, orders, manuals, directives and instructions relating to the internal personnel rules or practices of a DoD component, if such publication or inspection would not affect the general public, or if release to the public would hinder effective performance of DoD functions;

(2) Internal advice, recommendations, and subjective evaluations, as contrasted with factual matters, that are reflected in records pertaining to the decision-making process of an agency or DoD component;

(3) Information in personnel and medical files, and personal information in other files that, if disclosed, to the public, would result in clearly unwarranted invasion of personal privacy;

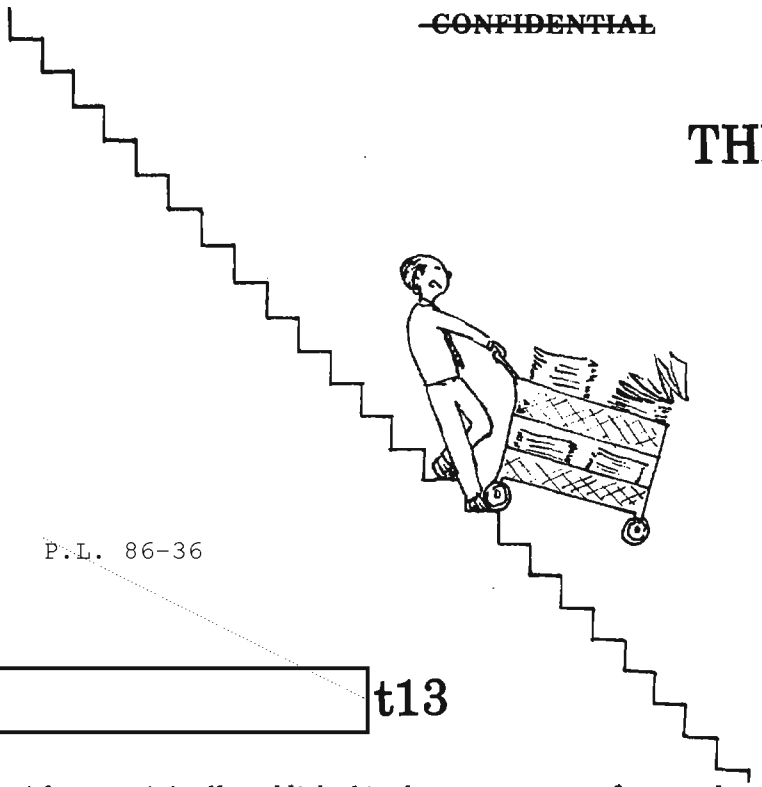
(4) Investigative records compiled for the purpose of enforcing civil, criminal, or military law.

(U) Please remember that, properly used, the **FOR OFFICIAL USE ONLY** caveat can afford us a great deal of protection against the public disclosure of unclassified information that is not in the public interest. □

EO 1.4.(c)
P.L. 86-36

DOCID: 4009980

THE 39 STEPS (U)



P.L. 86-36

t13

This article was originally published in the December 1980 issue of the T15 Technical Bulletin.

(U) In 1957 NSA was scattered around the Washington Area: at Arlington Hall, Virginia, at Nebraska Avenue in D.C., and in barracks at Ft. Meade, Maryland. The Agency had acquired a new building (today OPS 1) but it was not quite ready for occupancy. The Agency had also acquired a new computer - a second IBM 704. The decision was made to install the new machine at Ft. Meade rather than at Arlington Hall because that complex was scheduled to move. Having installed the machine it seemed a prudent thing to run it.

One Friday in October, 1957, at 11:30 p.m.

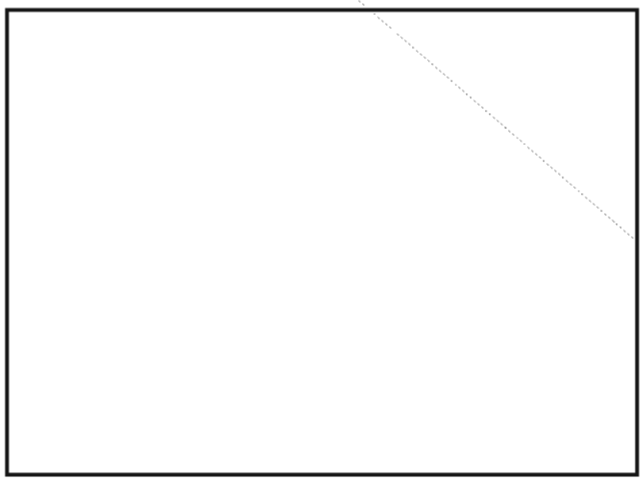
(U) The Baltimore-Washington Parkway was unusually dark that night. The fog masked the lights of the few southbound cars and even the warm glow from BINDERS (which at this time had yet to succumb to the arsonist) was not to be seen. The old Studebaker seemed especially reluctant to pursue its course to Route 32. The scene was something out of Rod Serling's THE TWILIGHT ZONE, though in this case more aptly it was the MIDNIGHT ZONE. Eventually the Studebaker groaned to a stop in front of Gatehouse 3. Carrying his brown bag and thermos, the operator passed by the nodding Marine guard and descended into the basement. The eve shift delayed its departure only long enough to tell its replacement that his partner on the shift had called in sick. The promise of a long lonely night was about to be fulfilled.

(U) The 704 occupied some portion of space which today belongs to the CAP area. The area was a restricted area and in fact at the time was one of a very few populated areas in the new building. A limited amount of production was running on the system since all customers, programmers, etc., were located at Arlington Hall and Nebraska Avenue. The 704 was one of the most powerful computers on the market. From an operational view it was a simple machine. It ran one program at a time. The operator's function was to load the program (it was on cards) into the card reader, set any necessary sense switches (there were 6), mount and ready any required tapes, check the printer, and press the program load button.

(U) The computer room was a sterile place. In addition to the computer, its furnishings consisted of two government issue gray desks, (one of which was placed in front of the machine console), a gray table, a gray coat rack, and a few gray chairs, all of which sat on a gray raised floor. This exotic color combination was offset by a pile of brown burn bags and a brown Frieden Calculator (circa 1812) which sat on the gray table. The atmosphere always convinced the operator that it was raining. He was constantly amazed when at the end of the shift he would emerge into sunshine.

(U) It was 1 a.m. The only sound in the room was the aching drone of the air handler punctuated by a periodic clacking of the printer. Sitting in front of the console, it was hard for the operator not to be mesmerized by the lights. He had heard of an operator who got some erotic pleasure from the console lights; but hard has he tried, he could receive only soporific sensations. He was running KNOLL IXC. Actually, the machine was running KNOLL IXC. It was a production job and it had been running for weeks. It was the only production job or any other kind of job available.

DOCID: 4009980 E.O. 1.4.(c) P.L. 86-36



(U) It was too early for 'lunch' yet the emptiness of the room induced a similar sensation in his stomach. The bologna sandwich, potato chips, and the coffee consumption took 30 minutes. It was now 2 a.m., only 6 hours to go. There were three projects available. One, track down the cat that everyone agreed was somewhere under the false floor. Previous efforts at this hunt had proven fruitless. The operator decided against the project. The cat, he was sure, had its own secret entrance to this secure area.

(U) The second project was the repair of the Frieden Calculator. This electro-mechanical marvel had not worked since the day it came over from Arlington Hall. The fall from the truck probably had something to do with its condition. The operator and his partner had decided to repair it and in so doing had ended with 15 parts left over. Its present condition, however, was no worse, i.e., it still didn't work. The operator vetoed this task since the hammer had been missing the last two nights and such a tool was needed for the delicate repair procedure.

(U) The third project was do-it-yourself programming.

(U) In retrospect, the 50's were an extraordinary time for learning about computers. The Agency was in the forefront in the acquisition of hardware. ABNER, ATLAS, and the IBM 700, 705 and 704 were on board. But where were the people, the mechanics, who knew how to use them? They did not exist. As a result, the Agency embarked on a course of do-it-yourself. It provided its populace with a million-dollar machine, a manufacturer's manual, and said, "Learn It!" and they did.

(U) The operator's partner had spent some time looking at a dump of the KNOLL IXC program. He had determined where the program read the cards. He produced changes which read the pattern cards from tape rather than the card reader. The effect was, that after doing a "load card to tape," the operator never had to service the program for the entire shift, except for the printer. Not to be outdone, this operator, too, had been looking at the dump and had produced changes to put the printer output on tape, also. At 4 a.m. he was ready to implement his change. He loaded the program. It began. It read the pattern cards from tape. It cycled. It produced output ... ON THE CARD PUNCH !!!

(U) The operator recovered. The original version of KNOLL IXC was back in production. His version was in the burn bag. Tomorrow would be better. It was time to shut down.

(U) While there was a great deal of compute time available, the number of applications programmed were not enough to justify weekend work on overtime. The Agency was thus in the ideal posture for processing on demand, a posture never to be seen again.

(U) Since it was the weekend, Saturday morning, the operator began the shut down procedure. He powered down the tape drives, the printer, the main frame. He placed all tapes, all cards, all listings in the oversize shopping cart. He secured the area and pushed the cart down the deserted roadway to the elevator.

(U) At the time, when the building had yet to be approved for "beneficial occupancy," there were very few secure areas. In the North end (first floor) there was established a vault room for the computer operations activity. It had a 3-way combination lock.

(U) The elevator refused the operator's call. Try as he would, it would not come. What to do? The operator was glad he had been lifting weights. Pulling the loaded cart up the 39 steps to the first floor was not in his job description but he was not enough of a PMM lawyer to know it. It was a thing that had to be done.

(U) It was now 8 o'clock. The darn combination didn't work. Here he was, the fate of the free world in his shopping cart. He couldn't open the vault. Once again, "my age, my father's age, the playboy centerfold's age." Would it work? It worked.

(U) He left. It was not raining, Depositing his empty brown bag and his empty thermos beside him, he urged the Studebaker to start. It did. As the car staggered down the B.W. Parkway, the operator wondered if he had done any good.

(U) KNOLL IXC made a major contribution to what the Agency is all about. It is a fact of life, then, as now, that our operators are prime movers in successes which they know not of. □

CRYPTOLOG invites readers to submit vignettes of historical interest

DOCID: 4009980

PUZZLE PAGE

MORAL DISQUISITION

Find the five-letter anagram to fill all blanks

" ----- in Deo," so the saying goes

(One cannot ----- it, though the sense one knows.)

However, after "mon ----- " one day,

When ----- and port had both been cleared away,

I fell to musing, would God ----- a Cain

Who ----- the heads of men, instead of grain?

At jousts the knight with ----- to win a prize

----- his opponents down to half their sizes

With him is damned the conqueror

To murder, also he who ----- and burns.

●●●●●●●

Reprinted from the
ASA *Review*, Vol. 1. No. 4, July-August 1950

Solution to NSA-CROSTIC No.61

[A. J.] Salemme, "[Guide to Russian] Technical Translation," NSA, 1974.

> "The translator must ... determine the precise type of [rotary-wing] aircraft ... being referred to in Russian as ВЕРТОЛЕТ so that his rendition will conform to precise English usage. He must not ... avoid the issue by translating it in formal context as "chopper" or "eggbeater."

Solution to

CRYPTARITHM

(Jan-Feb 1986)

```
1 2 3 4 5 6 7   1 1 0 0 1 0
K R Y P T O S   3 2 4 0 6 7 5
+S O C I E T Y +5 7 9 8 1 6 4
C P K I I K C   9 0 3 8 8 3 9
```

Number the columns left to right, 1-7. Note that no two letters refer to the same digit.

Column 1 shows that **C** is greater than **S**. Hence column 7 shows that **Y = C-S**. Now column 1 shows that there must have been a carry from column 2, so that **1 + K + S = C**, so **Y = K + 1**.

Since column 2 produces a carry, **P** in that column cannot be **9**. Therefore column 4 shows that **P** equals **0**.

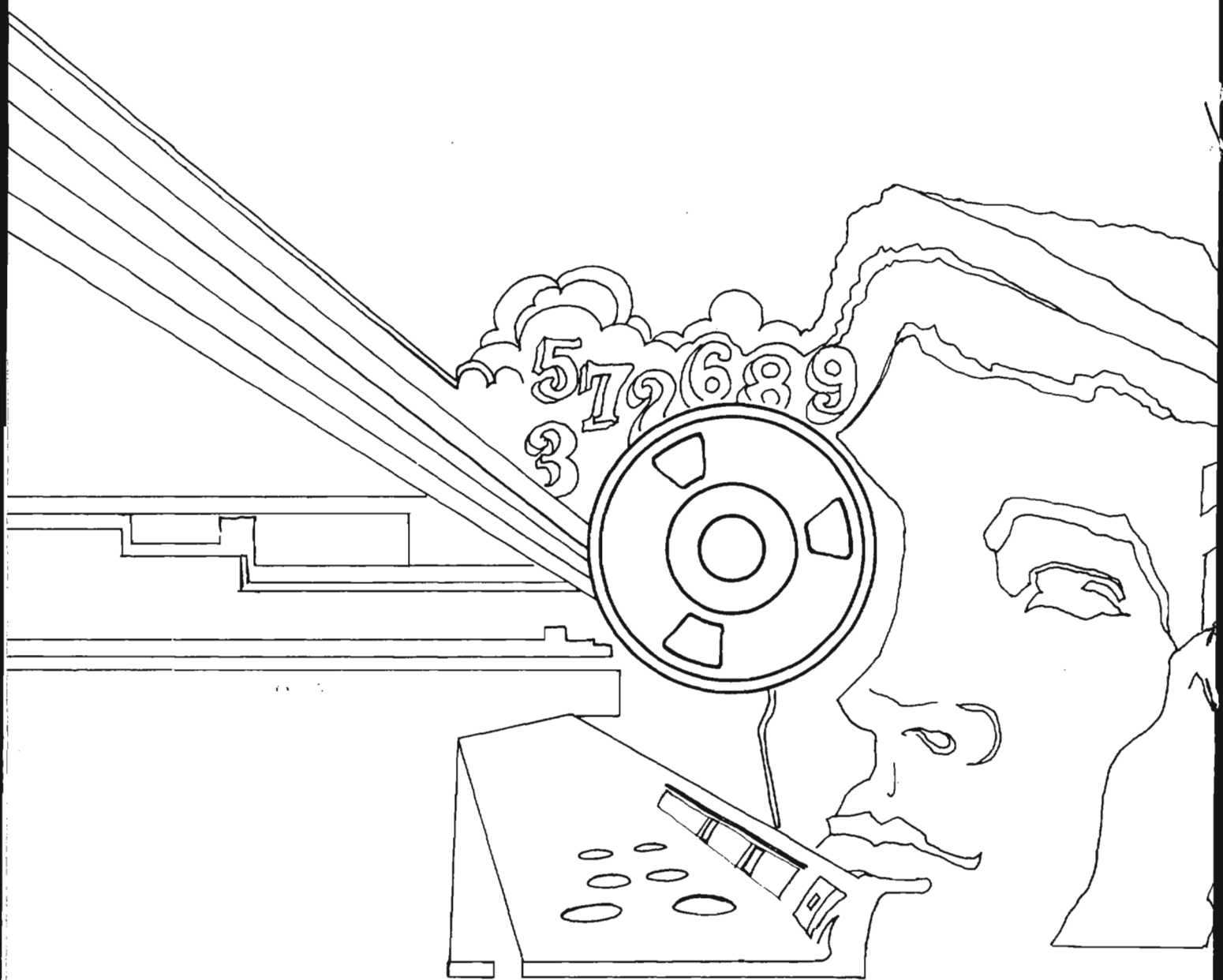
Column 4 introduces no carry into column 3; since **Y = K + 1**, **C** must equal **9**. There must be a carry into column 2, so **R + O = 9**. And column 1 informs that **S + 8-K**.

Hence **K** cannot equal **0, 4, 8** or **9**. An assumption of any of the remaining six values for **K** gives tentative assumptions **Y** and **S**.

Letter **O** cannot equal **0, 9, K, Y, S**, or **9-S**, so there remain four possible values after a **K** assumption. Then **R = O-9**; column 6 gives **T = K-O**; column 5 produces no carry so **E** is less than **I** and must be the smaller of the two digits still unaccounted for.

The six **K** assumptions and the four **O** assumptions make for just 24 things to try, far fewer than the 10! possible permutations of ten letters. Continued analysis or a computer program leads to the unique solution **PERKY STOIC**. Alternatively, knowledge that the correct arrangement constitutes a phrase would quickly eliminate wrong assumptions; e.g., if **K** equaled **1**, the phrase sould have the unpromising beginning **PK**.

~~FOR OFFICIAL USE ONLY~~
P16-MAY86-Y12-105312


5726893

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

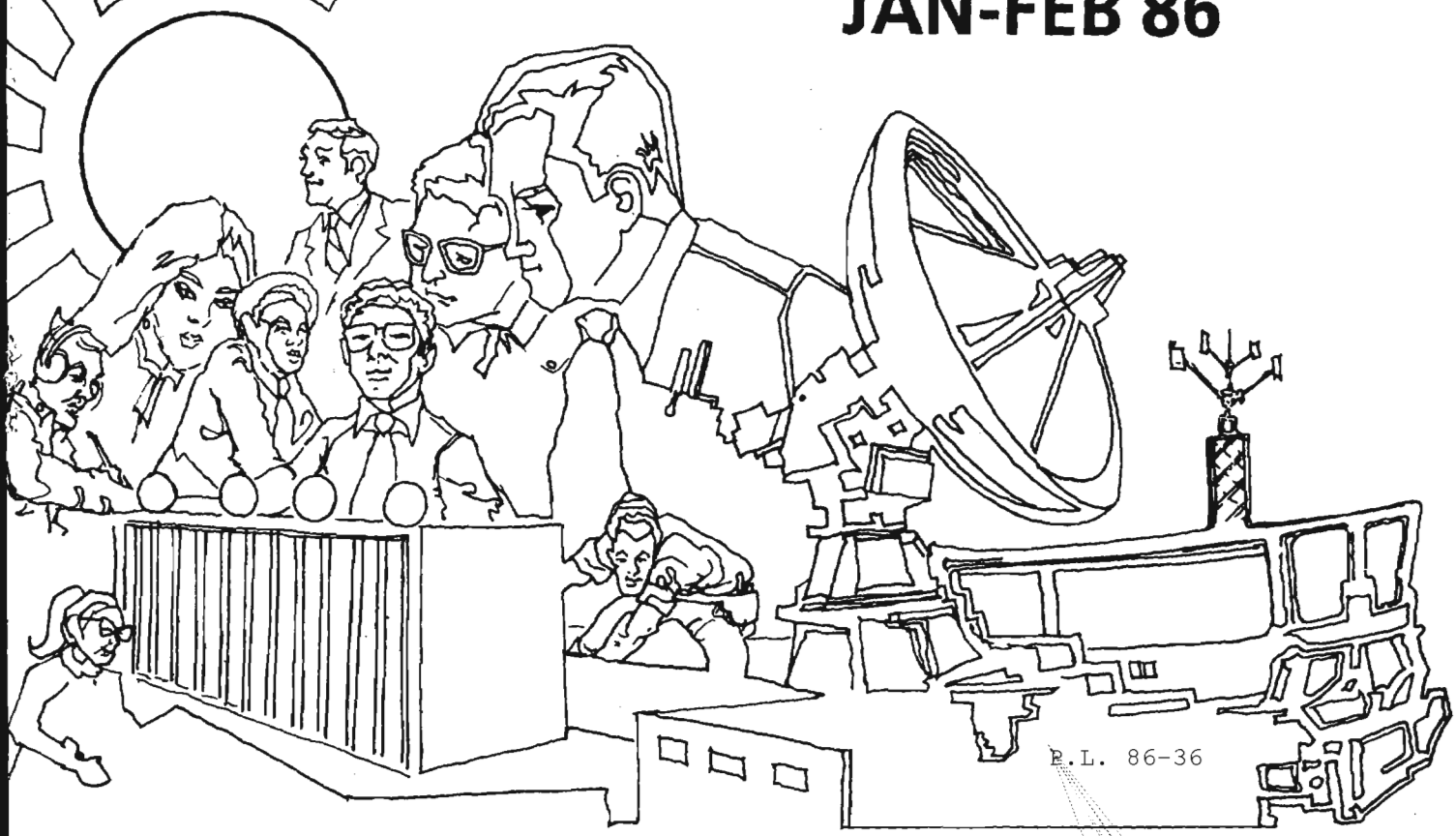
DOCID: 4012017

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JAN-FEB 86



P.L. 86-36

WHAT I PERCEIVE TO BE HAPPENING IN THE PACIFIC (U) 1
DIARY OF A GEISHA (U) 6
CAREER OPPORTUNITY (U) 11
A CASE OF FORENSIC SIGINT (U) 12
CRYSCOM-86 (U) 16
A MORALITY PLAY IN ONE ACT (U) 17
A PROBLEM IN RETRIEVAL (U) 22
IMPROVING TRAINING IN TECHNICAL ELINT (U) 24
BULLETIN BOARD (U) 26
LETTERS (U) 27
PUZZLE (U) 28

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~
~~NOT RELEASABLE TO CONTRACTORS~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

DOCID: 4012017

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XIII, Nos. 1-2 ..... January-February 1986

P.L. 86-36

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Collection ..... (963-5877)
Computer Security ..... (968-8141)
Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5230)
Cryptolinguistics ..... (963-1596)
Index ..... (963-5330)
Information Science ..... (963-1145)
Intelligence Research ..... (963-3095)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-4740)
Science and Technology ..... (963-4191)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-5734)

Illustrator ..... (963-3057)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptolg at bar1c05
(bar-one-c-zero-five)
(note: no 'o' in 'log')

Always include your full name, organization, and secure phone number.

For Change of Address
send name and old and new organizations to:
Editor, CRYPTOLOG, P1

Contents of CRYPTOLOG should not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

HYDE PARK CORNER (u)

Readers sometimes hesitate when they mention an idea for an article because the subject might be "controversial" and therefore not suitable for CRYPTOLOG.

On the contrary!

*From its inception CRYPTOLOG was intended to be "informal, newsy, **controversial**, lively, and timely ... " If you read carefully some of the articles in this issue you will certainly find examples of controversy {DIFFERENCE OF OPINION}. If you leaf through back issues of CRYPTOLOG and of its predecessors you will sure find controversy {DISCUSSION, DISPUTE, DEBATE}. Especially in the Letters to the Editor you will find a notable instance or two of somewhat heated controversy {QUARREL, STRIFE}.*

For CRYPTOLOG is the analysts' own Hyde Park Corner. We actively solicit articles and letters on the hot topics of the day. We especially welcome comments -- the free and easy kind that analysts make around the coffee pot -- on articles that have been published. Open discussion, dispute and debate are absolutely vital for keeping things in perspective, as we function in an environment that is necessarily closed to the outside world.

Among the "controversial" subjects that are frequently suggested is the relationship between NSA and contractors and vendors: how it affects what we do and the way we do it.

Another frequently mentioned subject is whether technical experts or generalist managers should make certain kinds of management decisions.

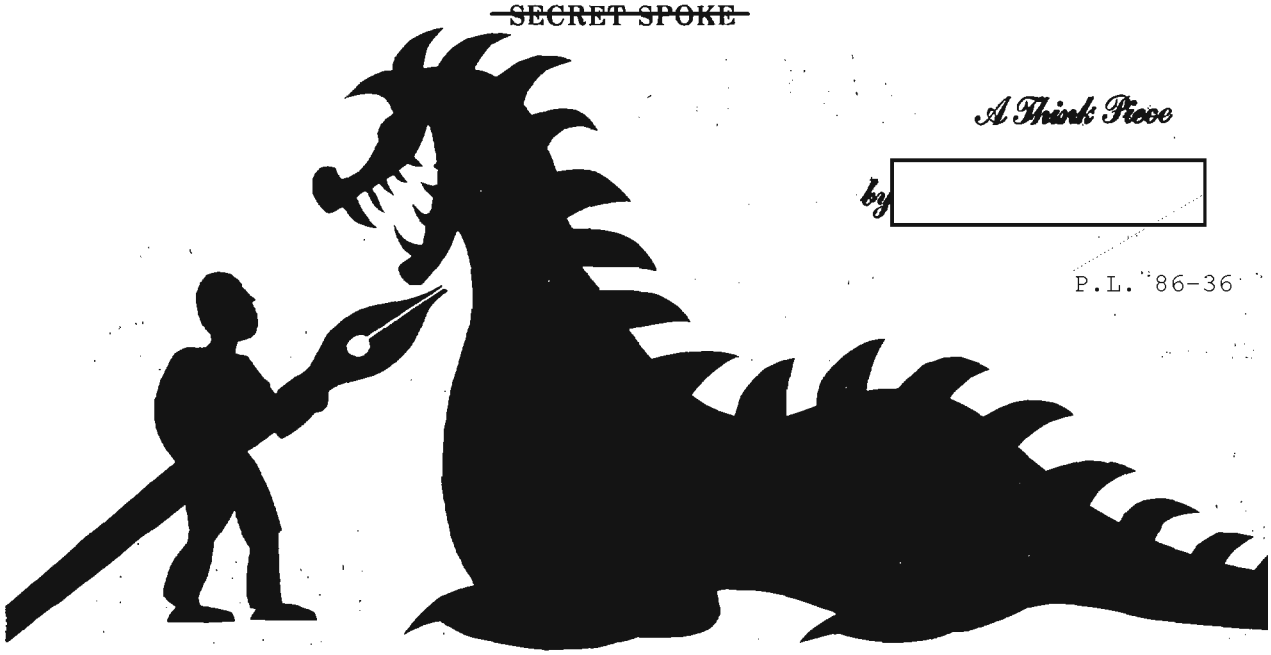
Now, when can we have that article ...

Ug

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012017

~~SECRET SPOKE~~



A Think Piece

by [redacted]

P.L. 86-36

What I Perceive to be Happening in the Pacific (u)

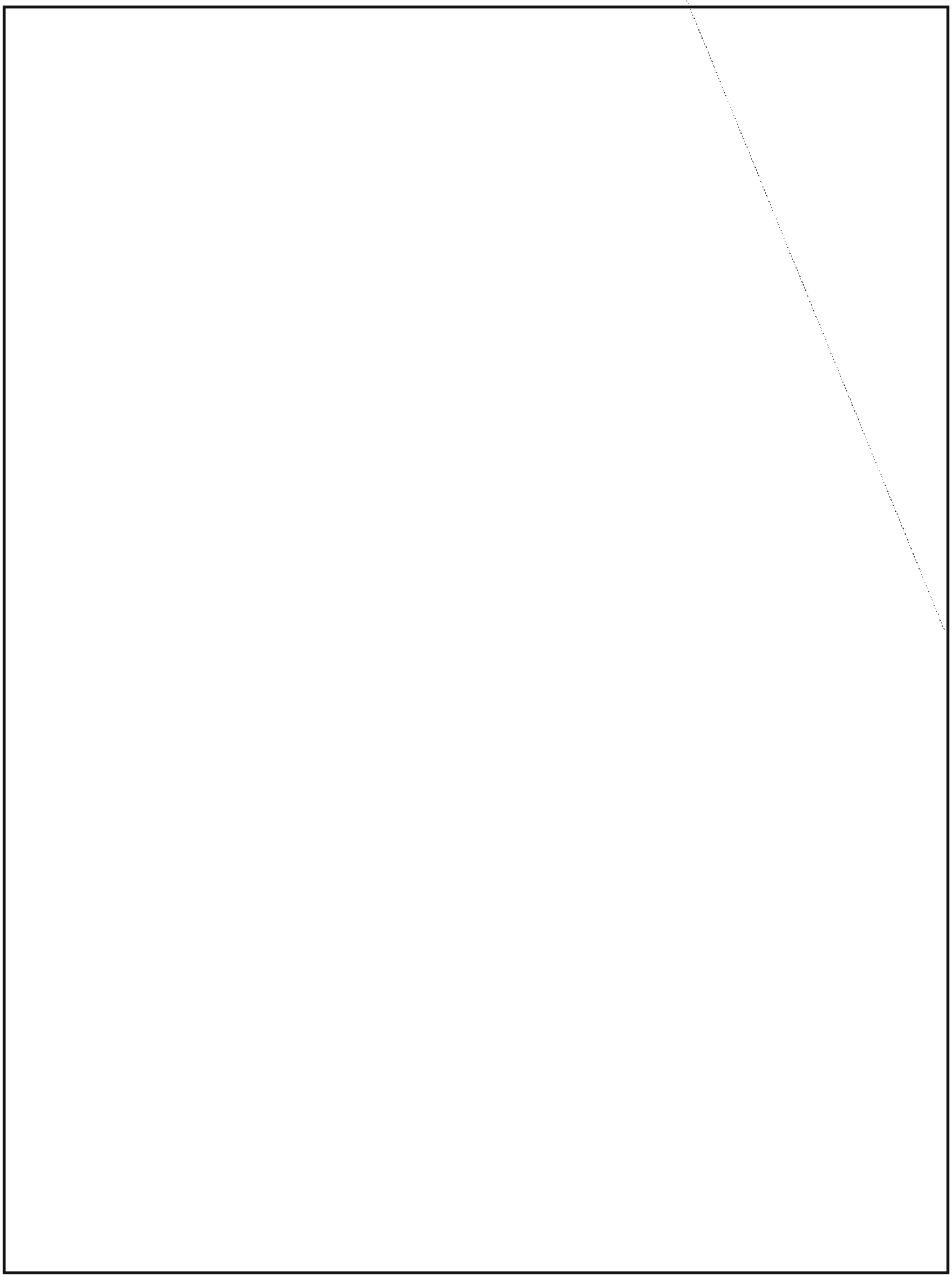
EO 1.4.(c)
P.L. 86-36

[redacted]

~~SECRET SPOKE~~

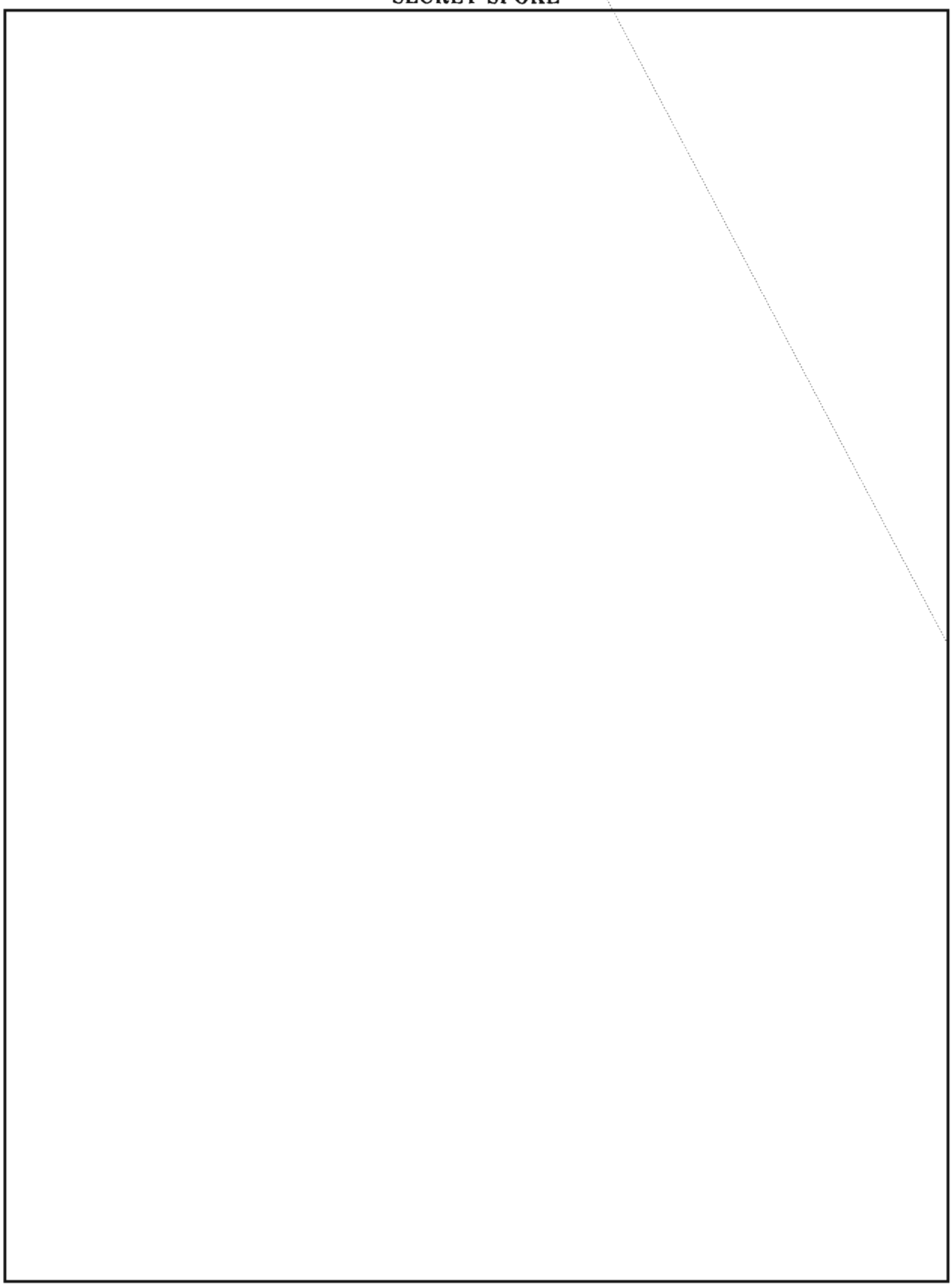
DOCID: 4012017

EO 1.4.(c)
P.L. 86-36



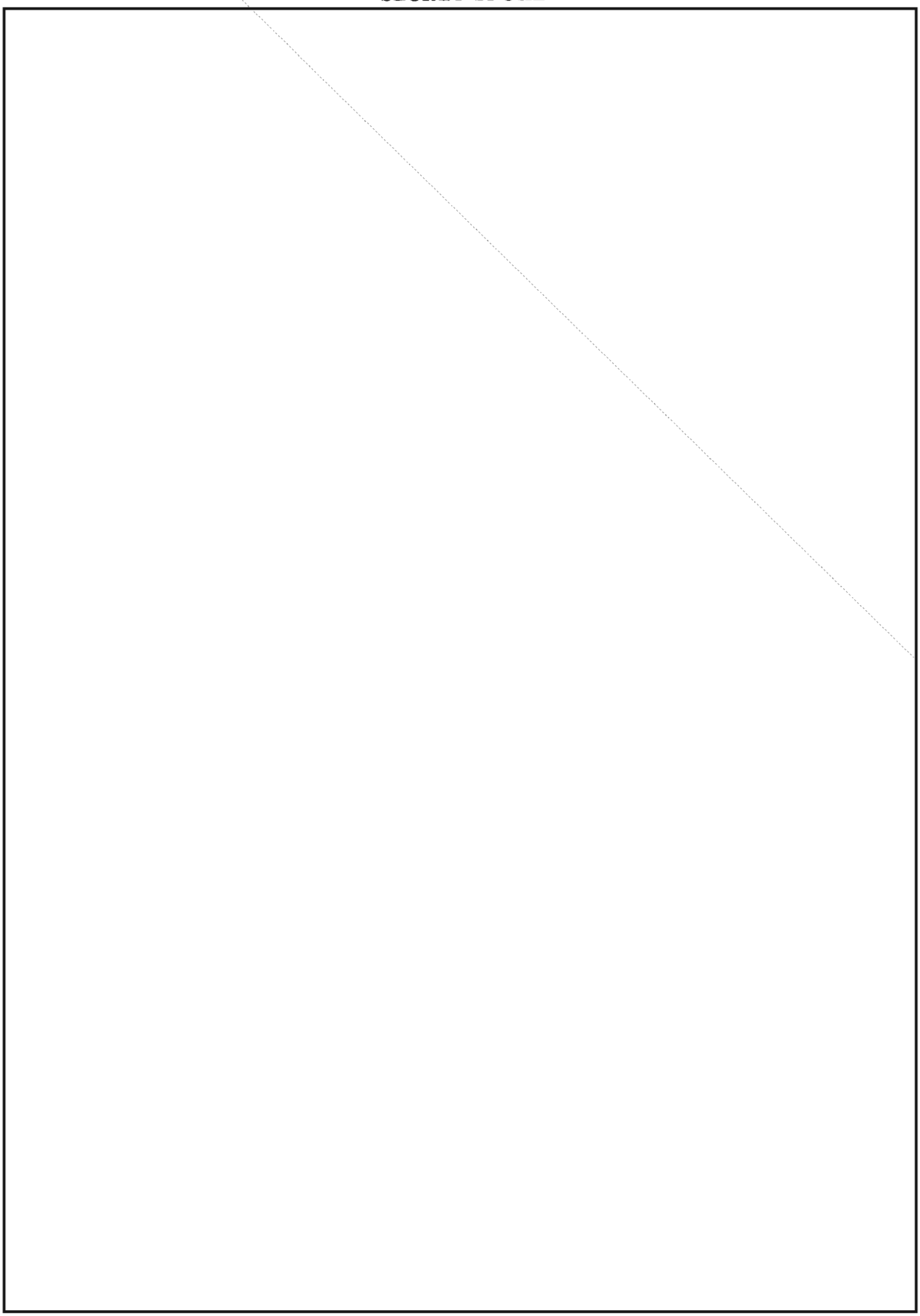
DOCID: 4012017

EO 1.4.(c)
P.L. 86-36



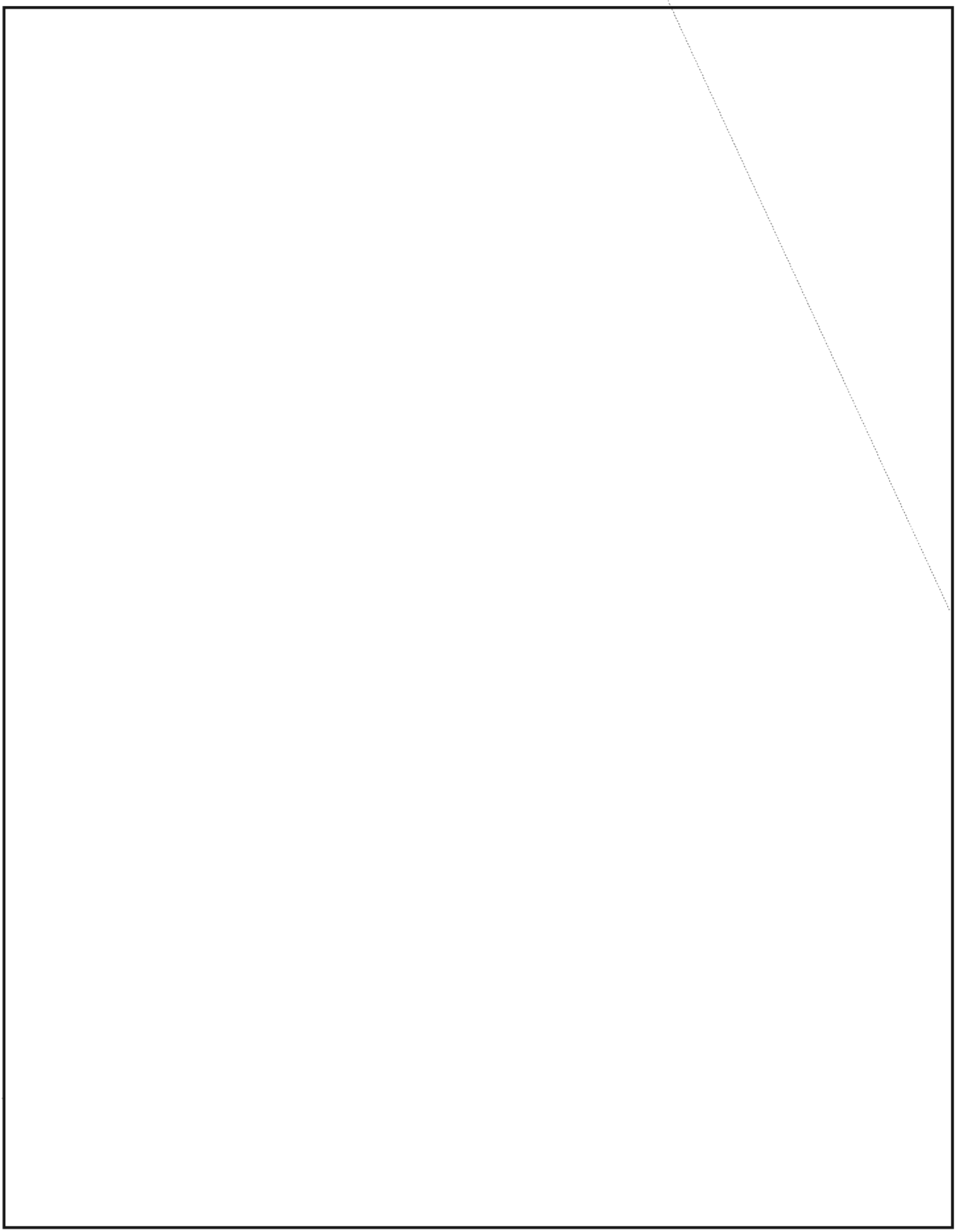
EO 1.4.(c)
P.L. 86-36

CID: 4012017



DOCID: 4012017

P.L. 86-36
EO 1.4.(c)



DOCID: 4012017

Diary of a Geisha (u)

E.O. 1.4.(c)
P.L. 86-36

P.L. 86-36

[redacted] *P56*

[redacted]

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

DOCID: 4012017

EO 1.4.(c)
P.L. 86-36

(U) The result was many, many meetings between reporters, programmers, and a patient group of interpreters on the G95 computer support staff who attempted to make sure each group knew what the other was talking about. Eventually a series of truths became self-evident:

P.L. 86-36
EO 1.4.(c)

▪ Preparation of product would take longer. Although it at first appeared incompatible with the goal of speed through computer automation, in fact using computers meant more work for the reporters. Speed and accuracy were gained by alleviating retyping of the item, and by easing the work of editors. But the time required to translate and prepare a product would be significantly longer, especially during the initial training period.

▪ Changes in the translating/report writing/editing sequence (i.e., the way we did our work) would be necessary. We would no longer be able to have two people working on one message at the same time and we could no longer casually pass a translation to someone for checking. We would be required to formalize our product preparation and release chain.

▪ People resist change. Back in the early days of PPREP, personal computers were rare and even the few existing enthusiasts were leery of a change that was going to slow down their work.

▪ We were going to do it anyway.

(U) Early on, it became clear that the software being used in G5 was not going to work for G9 and probably not for the rest of G Group. Being the first G office to go operational in a big way, G9 worked over a number of proposals and tried out a number of test programs. The general requirements as expressed to the programmers were:

▪ The system had to be non-technical, requiring only that users know how to operate the terminal. A knowledge of programming and sophisticated user techniques would not be necessary. In addition, instructions on using the system were to be integrated into the screen display so that the computer itself would move the user along, give him choices as to what to do next, point out errors, etc., and hopefully make it impossible for him to create a really serious problem. In programmer jargon, the system had to be user-friendly.

▪ The system had to be 95% error free before we would use it operationally. In addition, we had to have the ability to know where a given report was at all times until it left the building. We could not press the send button and just assume that the report had gone to the correct destination. As we were to learn, this didn't always happen. We

DOCID: 4012017

EO 1.4.(c)
P.L. 86-36

needed a system of receipt and the possibility of a complete audit trail for each product.

▪ Technical backup in the form of programming and hardware support had to be available at all times.

(U) We had many more requirements, some technical and some intended to limit the computer burden being placed on the analysts. But the point we kept hammering home was that the product had to get out and that timeliness and accountability were essential.

~~(FOUO)~~ As we looked to the future we identified two major tasks. The first was to come up with a good, reliable system. The second was to figure out how we were going to get hundreds of diehard pencil pushers and blue pencil editors to sit at a computer terminal and use the system that was developed. Hard though it is to remember now, as late as 1983 linguists and reporters still functioned in a totally paper world. We had access to SOLIS and a few other computer-age aids, but the tools of our trade were the yellow legal pad, carbon translation forms, and the much hated G-Group Expert sheet for technical accountability. In many ways this was a comfortable method of operation, reminiscent of our days in academia when we were tucked away with dictionaries and reference volumes, busily filling reams of paper.

BEFORE PPREP

~~(C-CCO)~~ In those Days of Olde, translators selected an item to report and wrote out a translation. If they made a mistake they crossed out or erased and, when they needed help, they took the translation to another linguist for consultation. When the translation was completed, both the text and the translation were placed into a checker's bin for review. When the checker had finished, the translation and text were placed back on the preparer's desk for correction and revision. Sometimes the whole translation/checking process had to be repeated several times.

~~(C-CCO)~~ When the translation was approved, the decision was then made as to whether the item would be published in full-text translation format or as a gist. Finally, the preparer was responsible for completing the EXPERT sheet, filling in the report title, TAG line, requirements, collectors, times of intercept, links, lanes, mat numbers, case notations, worksheet numbers, serial numbers, languages, etc. etc. etc. for the traffic used in preparing the report. Then, the finished product package, usually made up of at least three copies of the report and five copies of the Expert sheet, was placed in a supervisor's bin for review.

~~(C-CCO)~~ The supervisor edited the product and usually passed it on to the branch level for further review. The branch chief then passed the package to the people responsible for assigning the correct product distributions, DDIs, etc. The product was

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

CID: 4012017

EO 1.4.(c)
P.L. 86-36

FORM M3015A REV APR 79 (Supersede) ~~HANDLE VIA COMINT CHANNELS ONLY~~ FICATION

~~SECRET~~

CID: 4012017

(U) All of this may sound cumbersome, but it was the system we knew and loved and we were loath to give it up. At least it worked.

CHANGES

~~(FOUO)~~ Obviously, many things had to be changed as we moved to computers. We had nowhere near the number of terminals required for the number of reporters/linguists who needed to use the system. In addition, you could not casually pass a computer screen back and forth to a checker, nor could you allow everyone to release product to NSOC without control. Following a lot of talk and a lot of compromises, a number of procedures were developed:

- Reporters were not to take the place of the FLEX pool. By that was meant that we would not carry on as before, preparing translations and reports on paper and then once they were approved, retyping them into the computer as FLEX had been doing. Rather, analysts would work directly on the computer from step one. As more terminals became available, more reporters would use them. Any given report, however, would either be prepared and processed using the computer route or the paper route, no mixing of the two.

- A chain of logins with limited sending authority would be developed. Linguists would be able to send a report for checking to anyone in their login, and could then get it back again. The finished report could be sent only to an authorized login. This restriction extended up the editing chain as the product package was prepared for release; it was intended to minimize the risk of losing product through careless typing. Although there developed individual variations within offices, usually a product went from preparer, to checker, to branch, to distribution, and finally to NSOC, where it became that element's problem to dispatch product to the recipients.

- Distribution personnel within each division were made responsible for ensuring that product was not lost enroute to NSOC. This was done through use of a system of PPREP report numbers and a system of receipts generated by the various computer systems sending and receiving the reports.

- Training of personnel and operational use of the system would be very carefully controlled and instituted very slowly. Training was obviously one of our biggest headaches. Once we had a fairly workable system we had to ensure that people knew how to use it properly. Yet we also knew that the system would change frequently, particularly in the early months, and we had to have some mechanism for quickly disseminating information about changes in procedures or system usage.

TRAINING

(U) What evolved was a training strategy based on the pyramid. Initially a small team of fewer than ten people was formed, consisting of two people from each of the G9 reporting divisions. This group formed a steering committee and was fully indoctrinated into the system both technically and emotionally. That is, not only were they to learn the system inside and out, but hopefully they would like using the computer and drum up a little enthusiasm among their more reluctant co-workers. Once this initial group was trained, these people became responsible for training other people in their division, who were made responsible for training others, etc.

(U) Information on changes in the use of the system was passed downward the same way. The main advantage of this system was that we had to train formally only a small group of people, thus lessening the burden on the steering committee whose members, after all, were linguists and reporters with other responsibilities.

~~(FOUO)~~ The actual training involved the preparation of a number of G9 working aids among them:

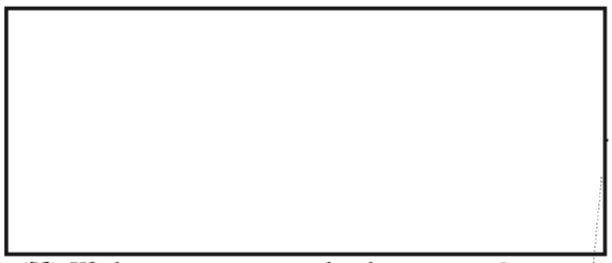
- "PPREP Users' Guide," which tried to include everything known about PPREP operations;

- "PPREP Users' Instructions Quick Reference," which gave step by step instructions for logging in and making the appropriate screens appear;

P.L. 86-36

(U) The prospective user was first presented with the fifty-some pages of instructions as a security blanket, told to skim through this documentation, and then then swiftly brought over to the terminal itself for the all-important hands-on training. After several magic shows in which the razzle dazzle of the computer was displayed, the students quickly settled down to discover that they had to use the system in order to learn it.

STARTING OUT



(U) We began very, very slowly--two products a day to start. If we had trouble one day we tried only one product the next day. We tracked each product through the system and checked the DDP feedbacks very carefully. To say that we had problems would be an understatement: we had trouble getting receipts, product was lost "somewhere," extraneous letters appeared in TAG lines, lines of text disappeared, we had product that the computer simply would not forward although we couldn't find any errors. One day we issued what turned out to be utter gibberish--the computer had taken a tabular report and forced it into paragraphs resulting in unreadable nonsense.

(~~FOUO~~) We made progress. With constant support from the programmers in T3 we gradually increased the number of products prepared and released via PPREP each day. By December, we had achieved such success that we decided it was safe to expand the training and operational use of the computer to the three other G9 reporting divisions. We gained an additional terminal subsystem (TSS) which, of course, caused a whole set of new problems. But within six weeks all four reporting divisions were using the computer. In January 1984, G9 was producing 5.3% of its product on [redacted]; in March it was producing 15%, in April 30 percent, and by June, G9 was producing 52% of its product on [redacted]. Product review items can now be prepared and released via PPREP.

(U) PPREP has become a way of life for G9ers. Most junior linguists continue to do paper and pencil translations which they have had checked and then bring to the computer to prepare a gist. Words like NROFF and ARG BREAK and PICKING and PUTTING are bandied about as product is prepared and preformatted expert sheets with prefilled standard fields are completed. Word is passed to editors when they have product in their "mailbox" and distribution personnel check technical details before pushing the button that sends the product to NSOC. The number of available terminals has gradually increased as has our dependence upon them. Many people find that they actually write better on the terminal than on paper because of the ease of self-editing.

(U) During system outages, which occur, alas, all too frequently, albeit (usually) for not too lengthy a period, most analysts find something else to do, leaving report preparation for when the system comes back up. During a recent extended outage when we had to get product out, my section first had to resurrect some typewriters from atop file cabinets. Major problems occurred when we tried to remember how paper Expert sheets were supposed to be filled out and how many copies of everything were required.

(U) Is PPREP a success? Most analysts will say yes. Are there still problems? Yes. There are major headaches and minor inconveniences but in the main, the lot of the linguist/reporter has improved and continues to do so because of the computer system and the programmers who patiently support us.

(U) Recently G9 began to receive the Agency Standard Terminal Workstations, a/k/a ASTWs. The terminal works as a stand-alone computer but can also connect to the GEISHA system to be used for product preparation. One set of key functions is written on a plastic overlay that surrounds the keyboard; we use those key functions when the terminal is being used in the GEISHA mode. Another set of key functions is posted on a keyboard diagram attached to the side of the terminal; this applies (mostly) when the terminal is being used as a stand-alone. (A third set of functions keys we ignore; the standard keyboard issued from the manufacturer contains keys which have not been enabled.) There is also a "forbidden key" in the stand-alone mode which turns everything into what resembles irreversible hieroglyphics

P.L. 86-36

POSTSCRIPT

(U) My technical mentor tells me that the Forbidden Key problem has been solved with new software. However, just the other day my office got a new ASTW, and as I struggled to load it I accidentally pressed that key! I shouldn't have... □

CAREER OPPORTUNITY

FOR A COMPUTER SPECIALIST WITH WRITING SKILLS WHO WANTS TO MAKE A DIFFERENCE IN THE COMPUTER SECURITY ARENA.

Experience in one or more of the following is desirable:

networks

distributed systems

operating systems

data base management systems

Location: beautiful new office overlooking the gazebo at Airport Square.

For information cal[redacted]Chief, C11 859-4452 (black).

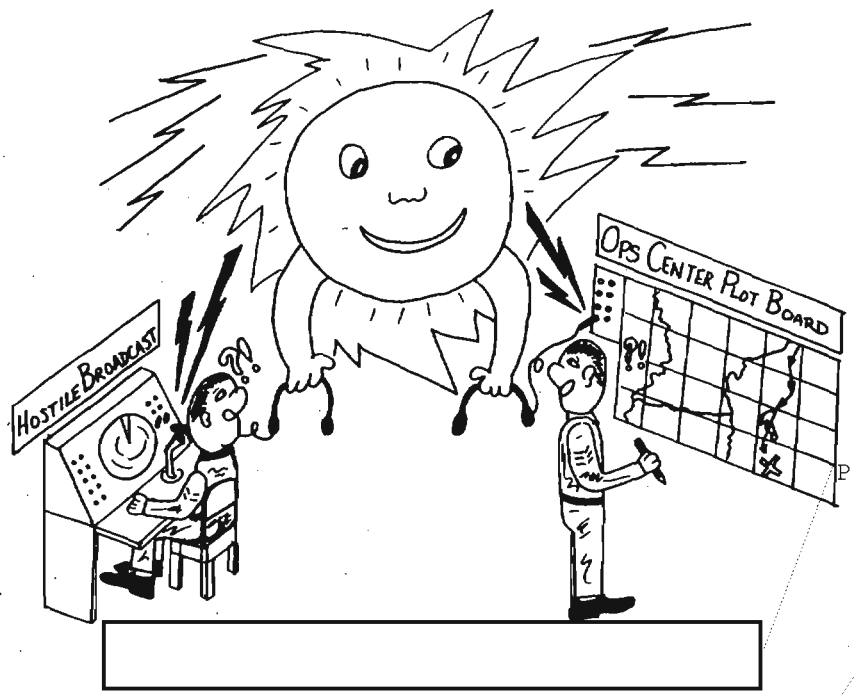
P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)

P.L. 86-36

DOCID: 4012017

A CASE OF FORENSIC SIGINT (u)



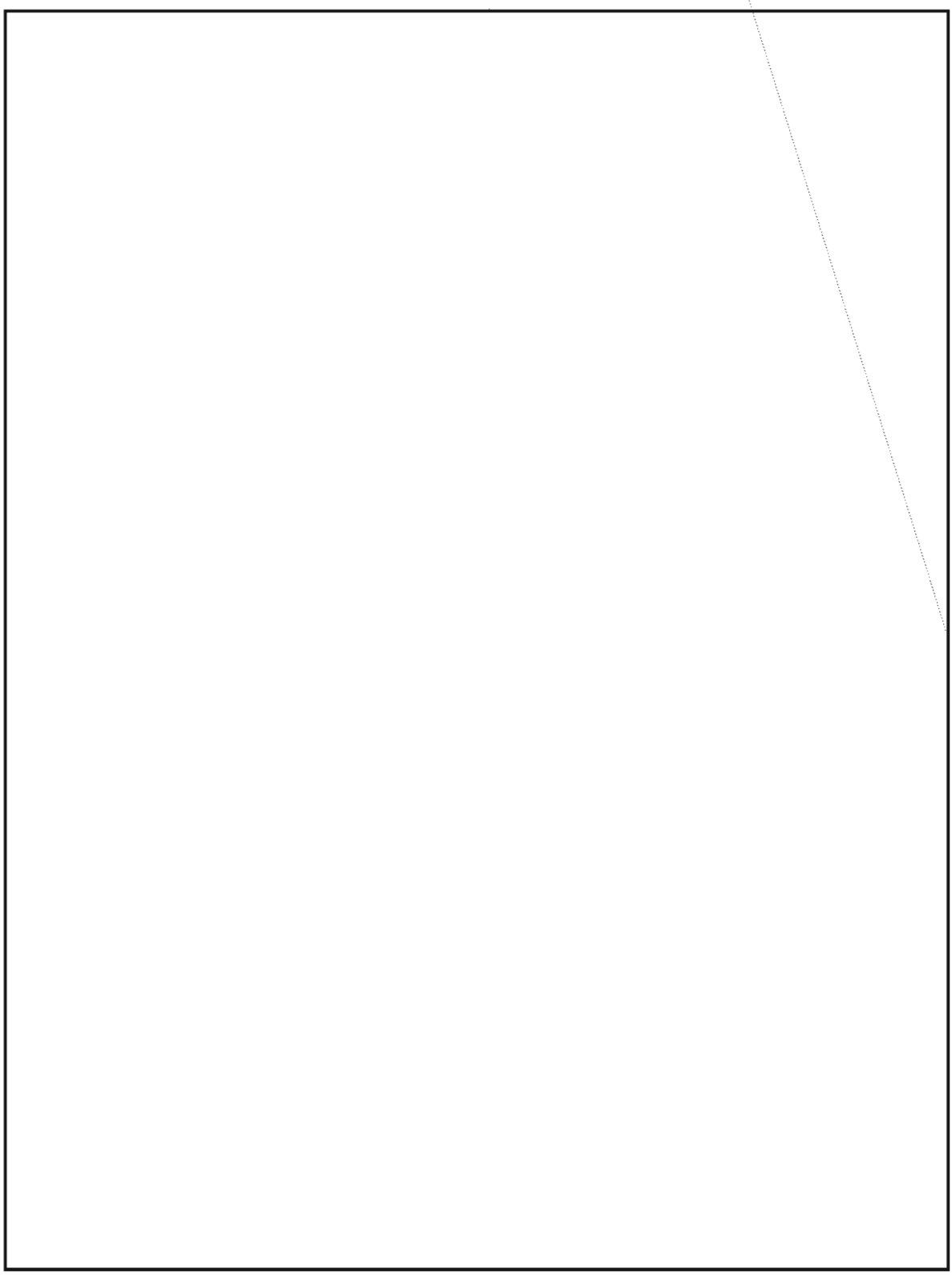
EO 1.4.(c)
P.L. 86-36 P.L. 86-36

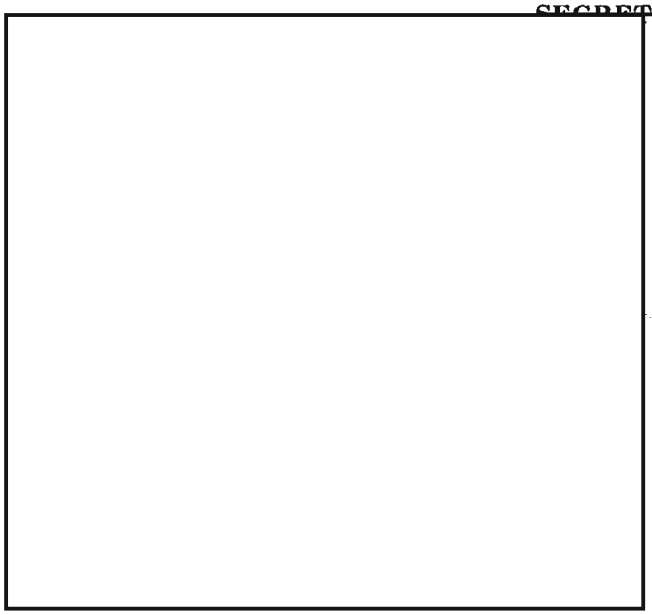
(U) SUNSPOTS???

~~(FOUO)~~ While I knew that our colleagues would find our explanation of what had just happened hard to believe, the reaction was even stronger than I had anticipated. But the first explanation of the event had been just too simple to be correct. On top of that, it didn't square with the target's mode of operation. There had to be another answer, and it had to be atmospheric in origin.

DOCID: 4012017

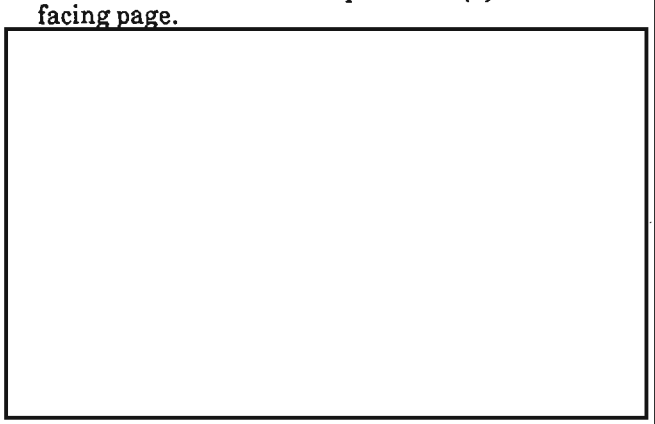
EO 1.4.(c)
P.L. 86-36

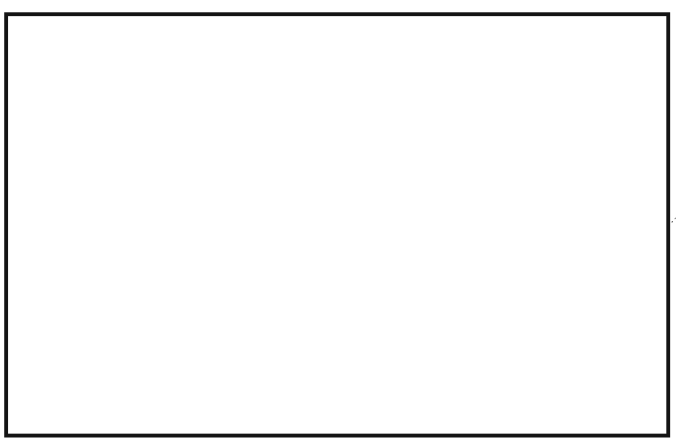




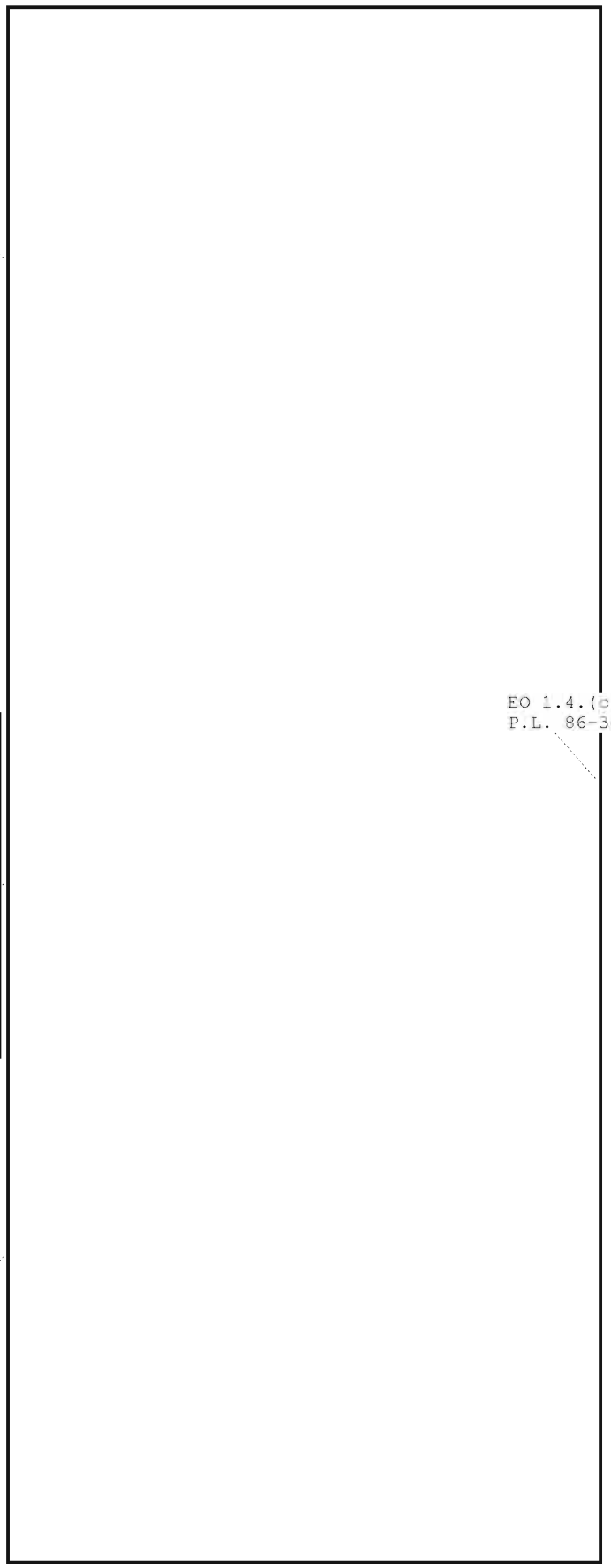
(U) As luck would have it, Murphy's Law was operative on that day. A US field station in the vicinity issued the SPOT report marked {1} on the facing page.

(U) Approximately one hour later, the same station issued the follow-up marked {2} on the facing page.





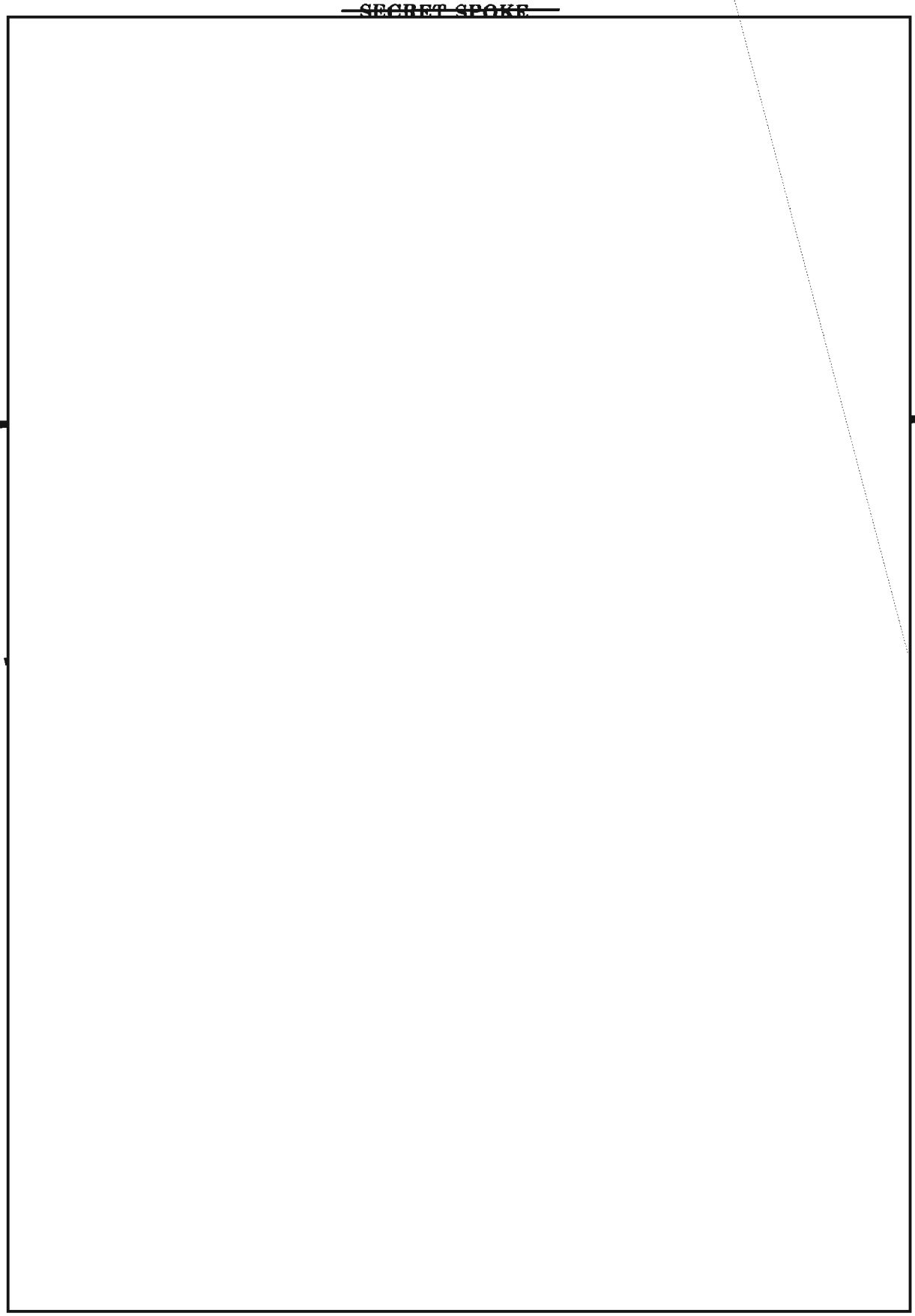
~~(S)~~ This indicated to our analysts that the answer lay not in willful suppression of tracking, but inability to communicate. What was the cause, then? Jamming? That was not considered a



EO 1.4.(c)
P.L. 86-36

DOCID: 4012017

EO 1.4.(c)
P.L. 86-36



CID: 401201?
EO 1.4.(c)
P.L. 86-36

[redacted]

Ed,

Your question prompted me to do some more homework on solar flares. In the NSA library I found a book titled Solar Flares *by Smith and Smith (McMillan, 1963).*

Pages 242-250 describe the sudden ionospheric disturbances (SID) accompanying some solar flares and consequent short wave fadeout (SWF) alluded to in our report.

According to Smith and Smith, SID is noted "only in the illuminated hemisphere" and occurs simultaneously with the event. "This class of terrestrial response must therefore be due to short-wave electromagnetic radiation of the flare." (p. 242.)

"SWF are the most familiar and certainly the most economically significant ionospheric flare effects ... Fadeout may become complete in as short a time as one minute, and can endure from a few minutes to several hours." (p. 243.)

"An ionospheric disturbance characteristically begins about 7 minutes after the flare commences, but this time is always during the flare's rise to maximum." (p. 244.)

"We mentioned earlier the observed time delay between maxium phases of flare and SID [7 minutes]. Some authors have pointed out that the delay can be interpreted simply in terms of the normal response of ionsopheric layers to an impulsive rise in the flux of ionizing radiation. Thus there is no need to assume that in the rising stage of a flare, there is time sparation between its visible and its ionizing radiations." (p. 249.)

[redacted]

CRYSCO - 86

THIRD ANNUAL CONFERENCE

2 - 6 June at NSA

Sessions held in the Friedman Auditorium
and in Conference Room 2W087

AUDITORIUM SESSIONS ARE OPEN
to persons with green or orange badges

OTHER SESSIONS REQUIRE TICKETS
(distributed through your office)
a green or orange badge
and LACONIC access.

Topics for the conference room sessions include:

- HYPERCAN hardware, present and future;
- CRYSCOs in review;
- Components of distributed processing;
- Cryptanalysis on personal computers;
- Life after IMP;
- Software exchange -- can it work?
- Major applications packages;
- Parallel computers and their applications;
- Automatic processing packages;
- Diarization packages;
- Computer graphics for cryptanalysis;
- CRYSCO-86 wrap-up.

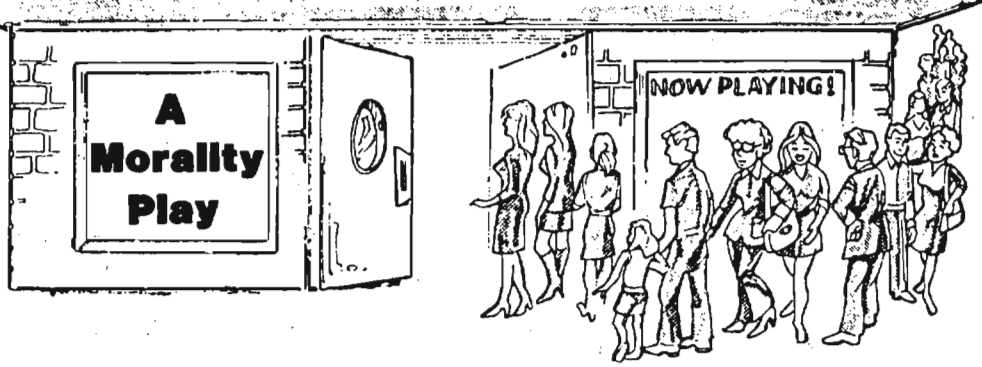
Additional information can be obtained from the CRYSCOM Executive [redacted] *A531/P13, 963-3197s.*
(FOUO)

P.L. 86-36

P.L. 86-36
EO 1.4.(c)

DOCID: 4012017

HOW 25-5 REALLY WORKS



HOW 25-5 REALLY WORKS

A MORALITY PLAY IN ONE ACT

BOOK

by [redacted] N34

Adapted for the Stage

by [redacted] *T091*

and [redacted] *T091*

Sets and Costumes

by [redacted] *B54*

★ *A Va Production* ★

★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★

DRAMATIS PERSONÆ

in order of appearance

Fred Finder, a DDO analyst

Heinous Merger, his boss

Tom Talker, an N34 budgeteer

Rosa Really, his boss

★

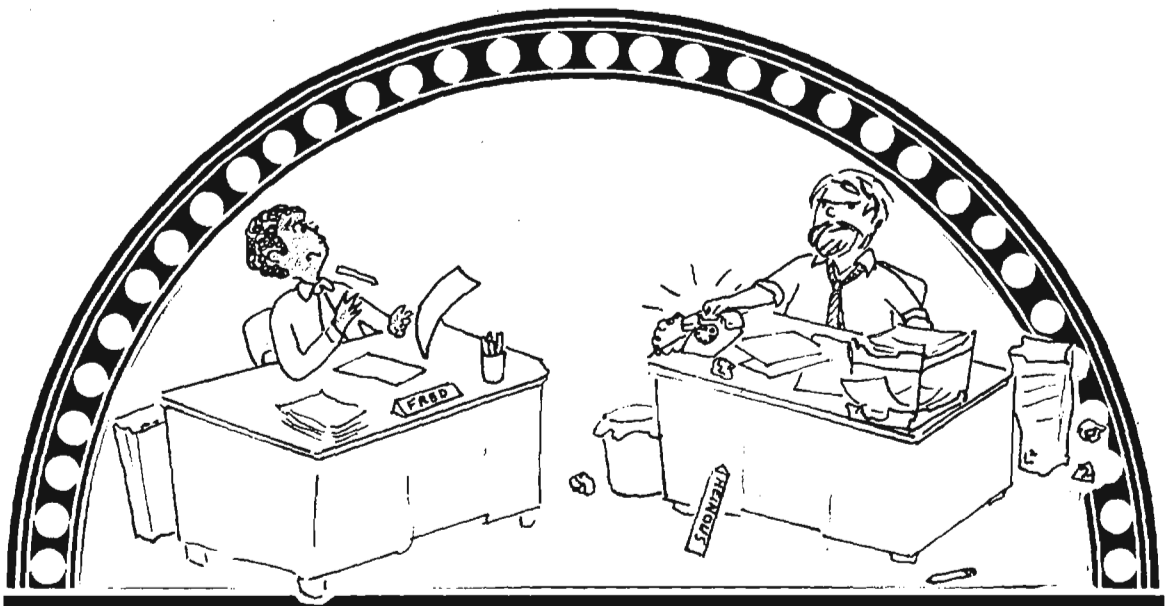
The action takes place at NSA

★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

OCID: 4012017



Scene 1

Heinous Merger's office in a DDO element.

Don Dillman runs a free wheeling R&D Shop and had been building "black boxes" for Heinous. Everything had worked well until he and Heinous dreamed up RATTLECAN. Heinous did not have any problem getting the funding into the outyear program, but the cost and the wide deployment of the RATTLECAN asymmetric permutated muxes (APMs) attracted attention in N34.

As Heinous crashes the phone into its cradle, Fred jumps.

Fred: Take it easy on the phone, Heinous ... it's not MILSPEC.

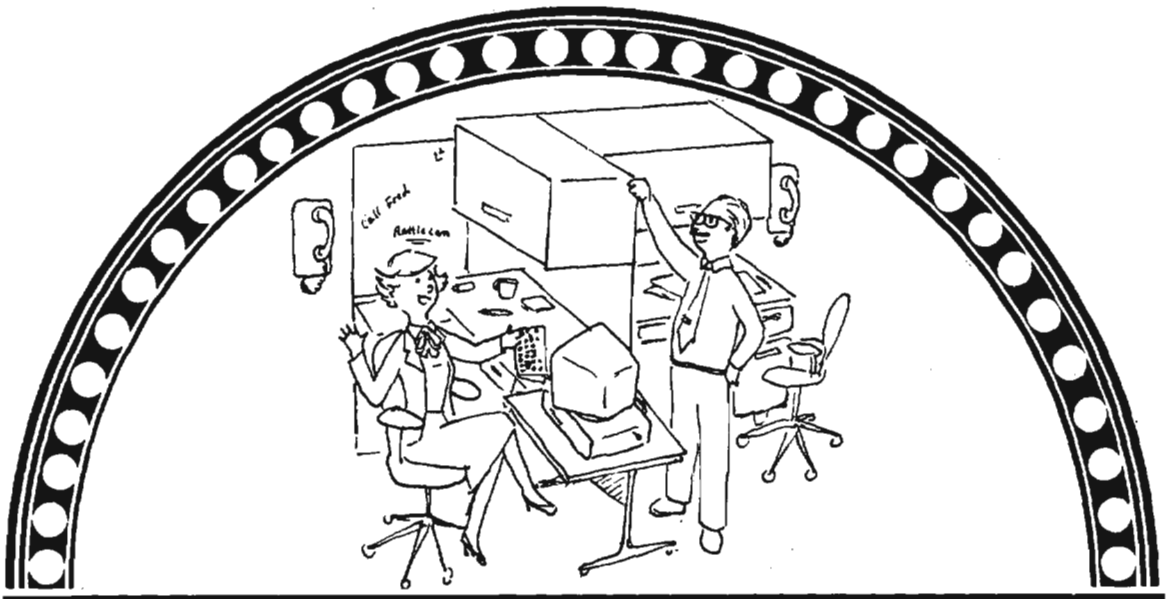
Heinous: #$%&*@! That nerd Tom Talker in N34 took the RATTLECAN money out of the program build.

Fred: I've tried to tell you, Heinous, you can't duck the regs forever. Sooner or later you've got to document RATTLECAN.

Heinous: I don't see why, Fred. I got my money in the budget and I know what I want to do. Don Dillman's shop has been working with those APMs and they'll be just the thing to get this signal.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012017



Scene 2: Rosa Really`s office in N34

Tom: Rosa, I think that we ought to bring RATTLECAN under NSA/CSS Circular 25-5.

Rosa: Why?

Tom: First, the project clearly falls under 25-5 because of the cost, $11M.

Rosa: I know that, but do we really need 25-5 monitoring for an off-the-shelf buy like this? Isn't Dillman's shop just going to use a bunch of APMs?

Tom: Yes. They have worked well in stand-alone applications, but a network of them could be a considerable risk. There may be a better way.

Rosa: Well, what should we do?

Tom: I think that, considering the cost, the potential risk, and the widespread use, a few other organizations need to look at RATTLECAN, and corporate management needs a say also.

Rosa: I certainly can't argue with that rationale, Tom. That's what 25-5 is all about. Send a memo to DDO reminding them that they need to get their RATTLECAN documentation in by 1 March if they want to get into the FY88 program build.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012017

Scene 3: Same as Scene 1.

H [screaming]: I haven't written a 25-5 requirements paper yet and I don't intend to start now!

F: Oh yeah, How are we going to get the money for RATTLECAN without one?

H: Oh @#$*! What do we do now, Fred? I've spent my whole career ducking 25-5.

F: It can't be as bad as all that. Lots of people have done it. A classmate of mine from the War College is in N342 now; maybe she can help us.

A few minutes later.

Rosa enters stage right with Tom.

F: Hi, Rosa it's good to see you again. Thanks for coming over. Meet, Heinous Merger, my boss.

H: Hello Rosa, my friends call me Heinous the Hutt but you can call me Heinous. How can you stand all that paper shuffling Rosa? When are you going to start producing some SIGINT like we're paid to?

R. Let me explain a few things. The 25-5 process has some good and proper goals. It gives the project sponsor high-level visibility and corporate support; it gives the Agency seniors a mechanism to review acquisition initiatives; it gives the acquisition organization a bounded task; and, it provides an established procedure for project coordination. Everyone should understand what it's all about and know how to use it.

H: Sounds like baloney to me!

R: Tell me Heinous, do you think that you and Don Dillman should have free rein with the $11M for RATTLECAN? Don't you think that there is an off chance that someone else might have some useful information to add? Don't you think that the corporate management is entitled to some say in how money is spent? And what about the SCE's that will have to train people to operate and maintain the RATTLECAN gear, shouldn't they get a warning of what's coming?

H: Well, sure, in fact, I ran into the Director on the elevator yesterday and I told him all about RATTLECAN. He said to keep charging.

R: Is that the way we inform our corporate management, Heinous, on the elevator? Do you remember exactly what you told him?

H: Well, not exactly.

R: That's my point, Heinous. If we are going to run an Agency this big, many people have to know what others are doing. 25-5 is the way we make that happen.

H: I never thought about it that way. I guess the seniors do need a cut in here somewhere but I don't have to worry about communicating with DDR. My buddy in R, Don Dillman is a wiz. If it's SIGINT, he can make it.

R: Well, Don Dillman isn't the only engineer in R. There is another R office that's doing almost the same thing that you want to do with AMPs, only using massed digital modulators.

H: I don't care. I know Dillman and he can deliver.

R: Maybe so, but the MDM is the new agency standard for this type of collection. Integrating RATTLECAN into the MDM architecture will improve interoperability, lower costs, and improve maintenance.

H: Well, maybe so, but why do we have to get this stuff in so early? It seems like I just thought up RATTLECAN and the next thing I know I get a memo asking for a ton of paper.

R: There are many people involved in the 25-5 process. If things get dragged out at any one point it holds up everything else. You need to get started as soon as possible.

Rosa stands up and draws the chart shown on facing page

R: If we're going to have smooth acquisition planning, people have to do their parts on time or they'll mess up the people on the next link of the chain.

H: Boy this is bureaucratic, Rosa. Do we have to go through all this to get a system fielded?

R: Not always. The chart shows a situation in which all the steps of the 25-5 process are applied. In many situations, we modify the process considerably. We use only those steps that are appropriate to the action at hand. For minor systems you can use the PBS -- the Project Baseline Summary -- instead of the SCP route.

H: Gee, you mean we might not always have to do a SCP-III?

R: That's right. There are some times that it may be more appropriate to move straight from the requirement to the SAP. It all depends on the circumstances.

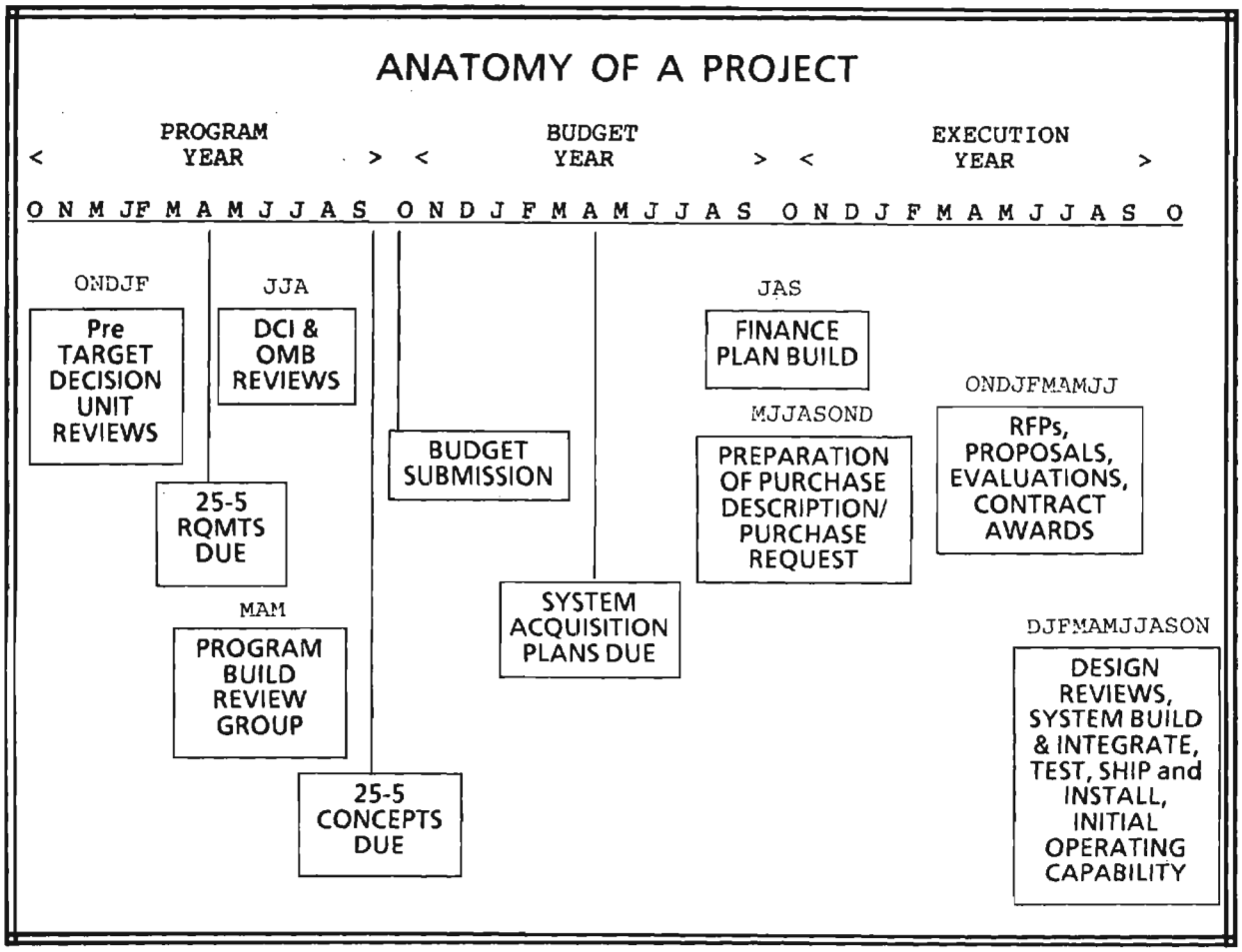
H: OK, but why all the big sweat about getting all this planning done so fast? After all we have three years to spend procurement money.

R: That's true, on a project basis, but things don't work that easily for the Director.

H: What do you mean?

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012017



R: Every year the Director and other Agency seniors go to Congress and defend our budget. They look pretty foolish asking for a big pile of money for the new fiscal year when they haven't even spent the money that was available in an earlier year. Also, if we don't spend the money on time, we lose millions of dollars a year just to inflation.

H: So the aim is to spend the money on what we asked for when we said we would need it.

R: Yes, plan your work and work your plan!

H: I'm convinced, Fred. Start up the boilerplate factory so we can get Ms. Really her requirement.

R: Thank you, but I hate to read boilerplate even more than you hate to write it. You don't have to rejustify your projects in the 25-5 documentation. All you have to do is describe them. We prefer clarity to volume. Six pages is the PBS goal, and two or three should suffice for a PBS Section I.

H: Six pages! Are you kidding?

R: No. SCPs of necessity will be longer but we don't pay for them by the pound, either.

H: Gee, Rosa, how do you know all of this anyway?

R: In N34 we review all the 25-5 documentation and it enables us to act as an "honest broker" for actions like the RATTLECAN. We're in business to make the 25-5 process go as smoothly as possible. Our system management officers all have considerable DDO, DDT or DDR experience. They can help you with all facets of 25-5 from writing PBS-Is to coordinationg SAPs. If we don't know the answers we'll find them for you. There are a lot of people who contact us before they even start a project. That way we can start greasing the skids for the project before it's even in the starting blocks. If you like we can set up a briefing for your people on the whole process.

H: That would be great! How can we get in touch with you?

R: We are located in 8A134 and our phone number is 963-1171.

Thanks for giving me this chance to explain what we do, and remember, we're N34 and we're here to help.

[*Exeunt tutti for ice cream.*]

~~FOR OFFICIAL USE ONLY~~

EO 1.4.(c)
P.L. 86-36

A PROBLEM IN RETRIEVAL (U)

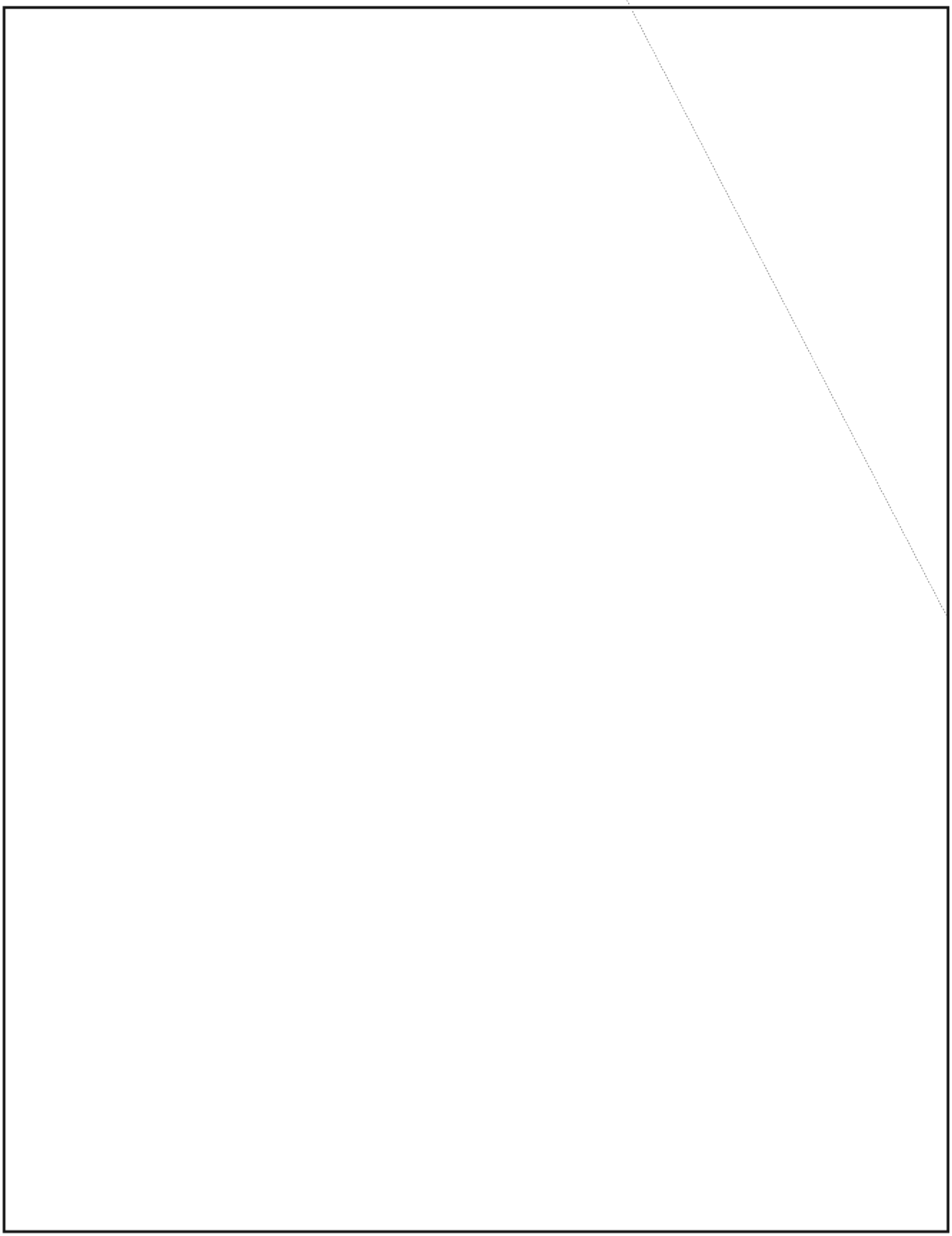
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

OCID: 4012017

EO 1.4.(c)
P.L. 86-36

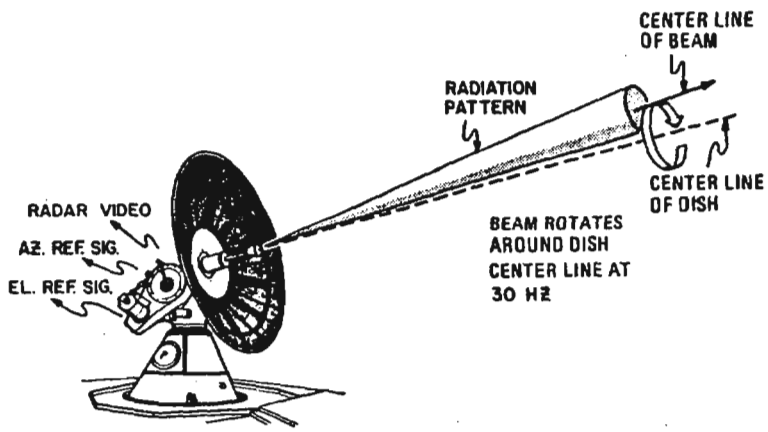


DOCID: 4012017

~~CONFIDENTIAL~~

IMPROVING TRAINING IN TECHNICAL ELINT

E54 P.L. 86-36



~~(C)~~ The National ELINT Plan dated 25 March 1985 identifies nine training and retention issues in Section VII, 3. Of the nine issues, four are considered to be actual training issues and they cover such things as:

(1) standardizing ELINT training throughout the community;

(2) designing a series of mandatory continuing self-study courses to expand the knowledge of ELINT people in the field;

(3) modernizing courses to reflect advancing technology;

(4) familiarizing non-ELINT people with ELINT operations.

As a result of this plan, the National Cryptologic School (NCS) has scheduled SIGINT Training and Advisory Committee (STAC) meetings for the 2nd QTR FY86. The STAC meetings will be convened to gather all interested parties together to obtain a corporate review of ELINT training. They will:

(1) Assess the impact of HQ, NSA/CSS and Service operational requirements on training;

(2) Review the impact on training of projected changes in operational targets and technological advancements;

(3) Identify the job performance requirements and training necessary to improve operational effectiveness;

(4) Assess the adequacy of existing training;

(5) Recommend to the Assistant Director for Training changes to training that will improve operational effectiveness and keep pace with projected needs.

A solution to the familiarization problem has already been accomplished by the new exportable IS-070 course which is available, worldwide, as a prerequisite to IS-250 (SIGINT Reporting). It is also teaches non-ELINTers about OPELINT and the differences between OPELINT and TECHELINT.

~~(C)~~ Basic technical ELINT training has traditionally been given at three service schools: Naval Technical Training Center (NTTC), Corry Station, Florida; Keesler AFB, Biloxi, Mississippi, and Ft. Devens, Massachusetts. On November 6, 1985, the United States Air Force transferred its basic ELINT training course to Goodfellow AFB, Texas. All intermediate and advanced level training has been conducted at NCS. These are the technical ELINT courses now being offered:

ARMY	233-98J	Electronic Warfare/Signal Intelligence Non-Communications Collector 402 Hours (Basic Course)
	233-98J30	Electronic Warfare/SIGINT Non-Communications Interceptor 290 Hours (For assumption of duty at E6 level)
NAVY	A-231-0028	Cryptologic Technician--T Field Operations Type FOUR (ELINT Operations) 480 Hours (Basic Course)

~~CONFIDENTIAL~~

OCID: 4012017

TECHNICAL and OPERATIONAL ELINT

Technical ELINT has the signal as its primary focus.

Operational ELINT takes the radar activity and relates it to a radar site, a weapon, a platform or an event.

Examples of the differences are shown below:

TECHNICAL	OPERATIONAL
Signal Descriptions	Emitter Deployment
Emission Characteristics	System Employment
Modes of Operation	Activity Levels/Schedules
Emitter Functions	Weapons System Tactics
Weapon and System Associations, Capabilities, Vulnerabilities	Platform Recognition
	Force Composition
Foreign Technology Indications	Indications and Warning

USAF	E3ABR20530	Electronic Intelligence Operations Specialist 628 Hours (Basic Course)
NCS	EA-202	ELINT Measurement and Analysis Techniques 140 Hours (Intermediate Level Civilian, Self-Paced)
	EA-280	Intermediate ELINT Collection and Analysis 280 Hours (Intermediate Level Military)
	EA-380	Advanced ELINT Collection/Analysis 320 Hours (Mixed military/civilian)
	EA-210*	Digital Analysis of ELINT Signals 160 Hours (Mixed military/civilian)
	EA-281*	ELINT Digital Analysis Training 80 Hours (Mixed military/civilan)

EO 1.4.(c)
P.L. 86-36

* *Developed by a contractor.*

REMINDER

CRYPTOLOG is a classified publication. It may not be read in the cafeteria or in other insecure areas.

DOCID: 4012017

BULLETIN BOARD

~~(FOUO)~~ Have you written a program applicable to manual cryptosystems? If so, MADCAPS invites you to submit a summary of information about it for inclusion in a compendium it is compiling. Just reproduce the form below, fill it out, and send it to [redacted]Z. (It is necessarily reduced in CRYPTOLOG; if you can't squeeze everything in, ask for a full-size form.) Don't forget to classify! If you have a question, you may call her on 963-1211.

P.L. 86-36

~~(FOUO)~~ At present a draft compendium is available that contains programs submitted up to 15 January. You can obtain a copy from Alice.

****

Manual Systems Survey

Name of process:_____ Category:_____

Function:_____

Type of Data:_____

Type of System:_____

Programming language:_____Computer:_____Operating System:_____

Point of Contact: Name_____Organization_____Phone_____

Brief Description:( )_____

_____

_____

Availability:_____

Comment: ( )_____

_____

_____

****

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

DOCID: 4012017

Letters

To the Editor:

NSA is approaching a milestone of sad significance. As of 1 January 1987, for the first time in its history, NSA will not have a current centralized collection of [redacted] It is an event that should not go unnoticed, for it dramatically reflects the shifting priorities in a bureaucracy that has lost sight of the requirements of intelligence analysis.

NSA will stand alone in the US intelligence community as the only agency with no centralized collection [redacted] This will not be seen as evidence of cost-effective, intelligent management, nor will it inspire confidence that NSA reporting [redacted] is informed and accurate.

If and when this giant step backwards comes to pass, the consequences will be real, and they will be serious in terms of squandered dollars and lost access to invaluable information.

[redacted]
P.L. 86-36

Editor's note: As we go to press we learn that the subscription will be renewed for 1987.

To the Editor:

Re Vera Filby's entertaining limericks in the Sep-Oct 1985 CRYPTOLOG: The limerick about the linguist named Rease reminded me of his cousin, a gent I wrote about in 1969. Here is a copy:

A gloomy defeatist named Reese
Decided to study Chinese,
When asked to select
A fit dialect,
His choice, was of course, Can'tonese.

The editorial staff of the old CLA Bulletin ran a monthly contest from mid-1968 through mid-1969 for language-related lickericks. The prize each month was mighty check for $1.00, and I cleared a cool $4.00 in that year with these ditties. Here are the other three:

There was a pig farmer named Patten,
Who became an M.D. in Manhattan.
Though his patients adored him,
The druggists abhored him,
For he wrote his Rx in Pig-latin.

A great polyglot, Heinrick I. Berman,
Claims his best tongue is hard to determine.
He speaks Polish with polish,
While his French is quite Gaulish;
And, when drunk, he speaks perfect High German.

There was a fine lass, Polynesian,
Whose feature were Classical Grecian
But her giggling betrayed her,
Foolish sounding it made her.
Alas, she spoke mainly Teeheesian.

You might also get a chuckle from this prophetic poem of mine which was published in the Agency's *Quarterly Review for Linguists* in 1970 during the height of Mao's power:

In China everyone will take a vow
That the key to every trouble is,
A panacea double is,
The little red Works of Mao.

This volume is a real wow,
It makes the weak strong again,
The short becomes long again,
The little red Works of Mao.

In Peiching they all know how
The sick will feel fine from
Just reading one line from
The little red Works of Mao.

They tell you with a curt kowtow
That his great work is liable
To outsell the Bible,
The little red Works of Mao.

The farmer behind his plow
Swears the meanest loaf of rye
Is changed to pheasant by
The little red Works of Mao.

Since the volume first took its bow,
China's youth has been bolting from,
They've become quite revolting from,
The little red Works of Mao.

I"ll make a prediction now
Today we're at the peak of it,
Posterity will speak of it
As the little-read Works of Mao.

[redacted]
P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012017

P.L. 86-36

CRYPTARITHM

by [redacted] P12/G42

Given:

```
  K R Y P T O S
+S O C I E T Y
  C P K I I K C
```

Solve for:

0 1 2 3 4 5 6 7 8 9

_ _ _ _ _ _ _ _ _ _

Every letter represents a distinct digit. When the letters are associated with digits so that the arithmetic is correct, they will spell out a phrase describing the successful cryptanalyst.

SOLUTION TO NSA-CROSTIC No. 60

From "Q.E.D. - 2 Hours, 41 Minutes," by Lambros D. Callimahos. *NSA Technical Journal*, Fall 1973.

"Spencer Akin: Letter to Birkhan.

"Your letter indicates that the purpose of your entering into communication with this office on the subject of the Kryha cipher machine is to make known its merits for consideration for use in the military service. This device has already been well studied and, I regret to advise, was found unsuitable for adoption in the military service."

ANSWERS TO

ETYMOLOGIST'S DELIGHT

(Sep-Oct 1985)

SOURCE LANGUAGES	BORROWED WORDS
Bantu [Sotho]	milo (a sorghum)
Hindi	shampoo, bund (a quay)
Arabic	massage, saffron, soda, mortise, lemon
Tamil [Telugu]	go down
Sanskrit	yoke, Juggernaut, jute, sugar
Malay	catty (a unit of weight)
Algonquin	terrapin, skunk, moose, squash, raccoon
Japanese	tycoon
Turkic	khan
Tibetan	yak, zebu
Turkish	drub, casaba
Breton	menhir
Basque	jai-a-lai
Russian	sable, pogrom
Czech	pistol, howitzer
Narragansett	quahog (a clam)
Spanish	machete, ranch
Norwegian	vole, skull, tangle (seaweed)
Greek	cactus, licorice, skink
Polish	doodle
Celt	barnacle
Gypsy (Romany)	pal
Swedish	addle, mink
French	faucet
Persian	azure, scimitar, caravan
German	snorkel, dowel
Dutch	snook, selvage
Maori	kiwi
Finnish	sauna

SOLUTION TO

PUZZLE IN PURPLE ⇒⇒⇒

(Nov-Dec 1985)

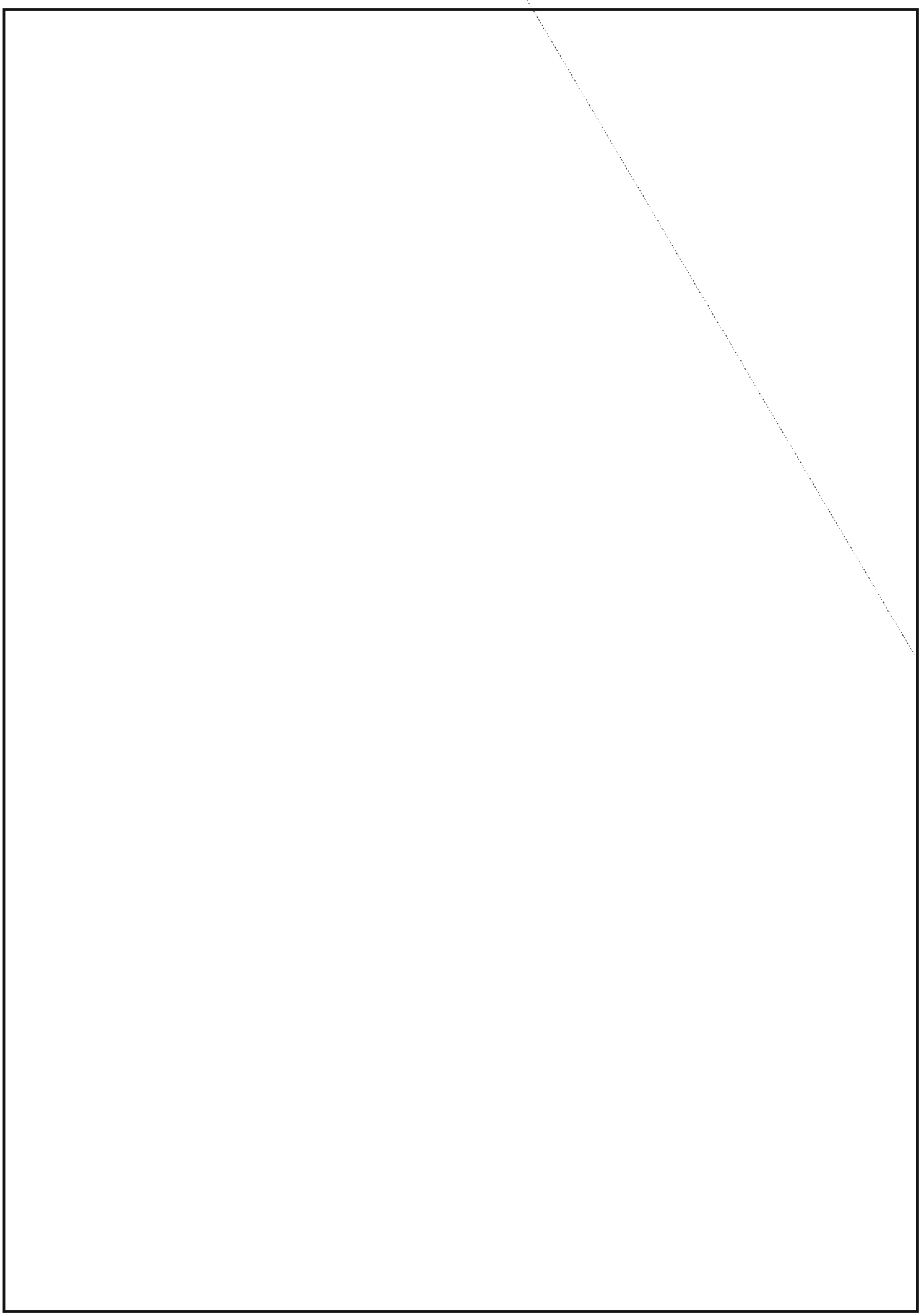
Provided by [redacted] *P12/G42*

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

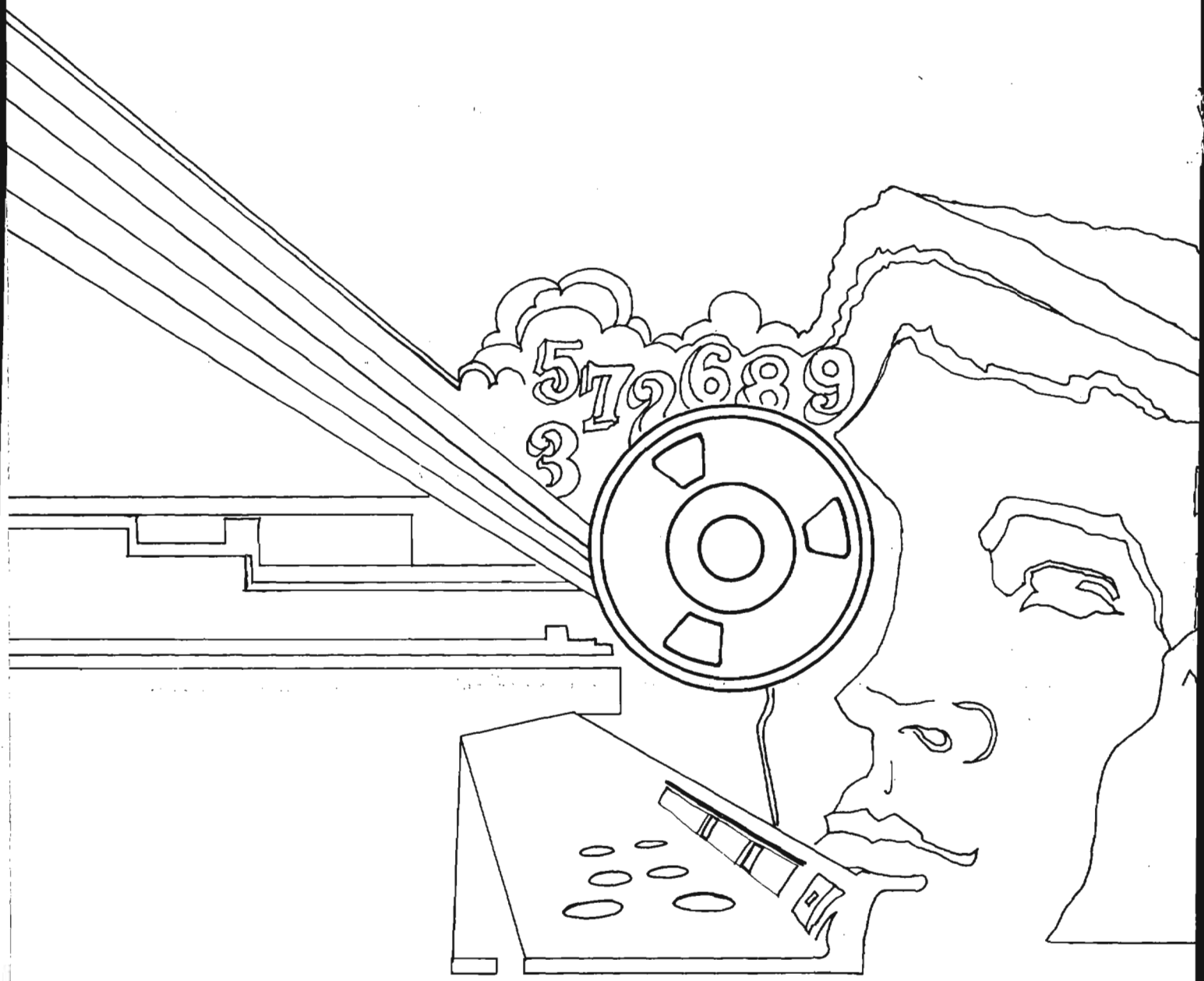
P.L. 86-36

DOCID: 4012017



~~FOR OFFICIAL USE ONLY~~

P1-APR 86-Y1-104801


5 7 2 6 8 9
3

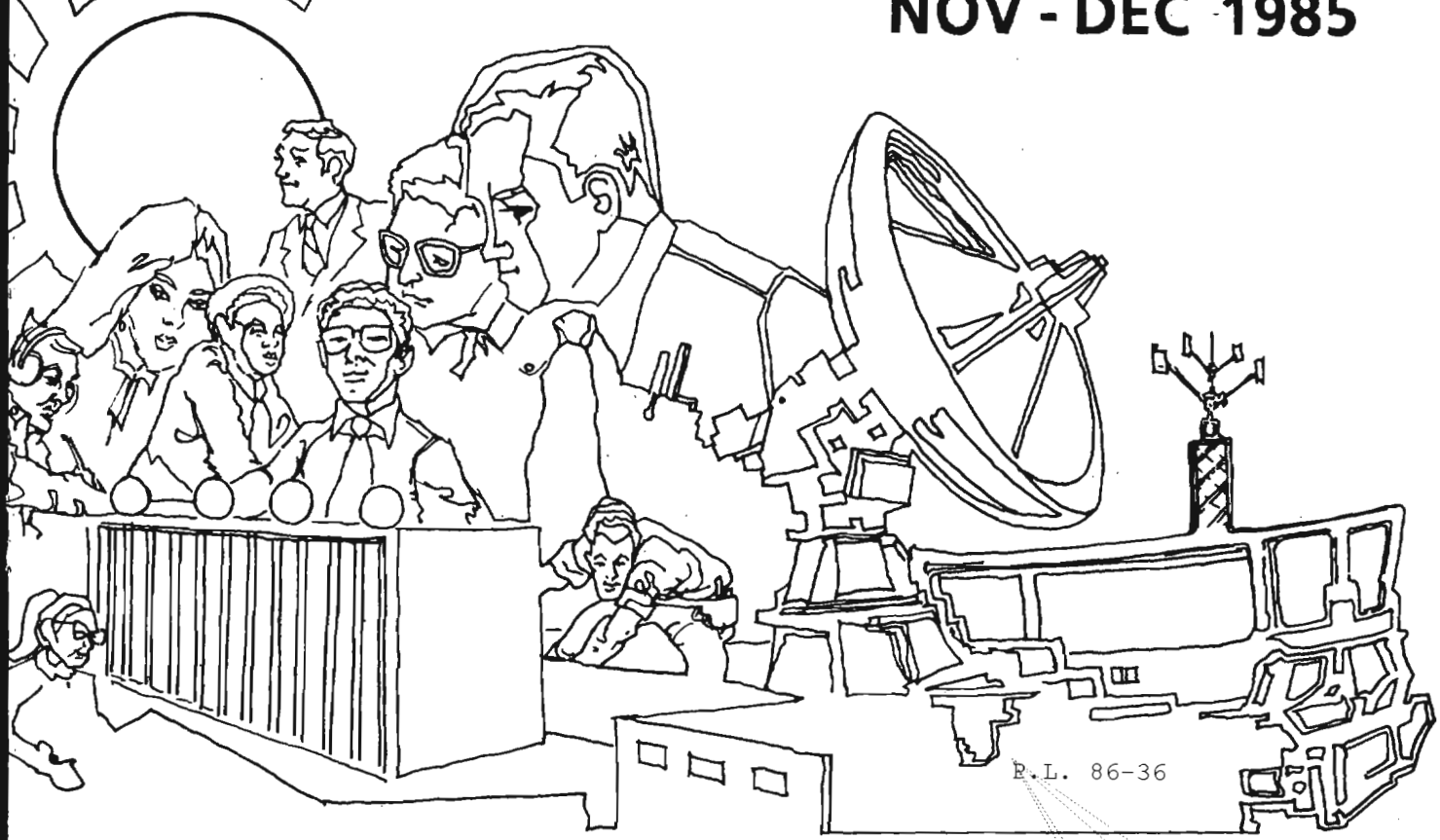
DOCID: 4012016

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

NOV - DEC 1985



P.L. 86-36

SEMESTER: A QUANTUM LEAP FORWARD (U). . . . [redacted] . 1
BULLETIN BOARD (U) 6
WHY DO WE NEED THOSE FUNNY ALPHABETS? (U) . [redacted] . 7
SHELL GAME: HYPHENATION (U). . . . . WES 10
BOOK REVIEW: KRYPTOLOGIE (U). . . . . [redacted] . . .11
LETTER TO THE EDITOR (U) . . . . . [redacted] . . .12
OPPORTUNITY (U). 12
PUZZLE (U) 13

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

~~NOT RELEASABLE TO CONTRACTORS~~

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

DOCID: 4012016

~~CONFIDENTIAL~~

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XII, Nos. 11-12 . . . . . November-December 1985

PUBLISHER . . . . . [redacted]

BOARD OF EDITORS

Editor . . . . . [redacted] (963-1103)

Collection . . . . . [redacted] (963-5877)
Computer Security . . . . . [redacted] (968-8141)
Computer Systems . . . . . [redacted] (963-1103)
Cryptanalysis . . . . . [redacted] (963-4740)
Cryptolinguistics . . . . . [redacted] (963-1596)
Index . . . . . [redacted] (963-5330)
Information Science . . . . . [redacted] (963-1145)
Intelligence Research . . . . . [redacted] (963-3095)
Language . . . . . [redacted] (963-3057)
Mathematics . . . . . [redacted] (963-5566)
Science and Technology . . . [redacted] (963-4191)
Special Research . . . . . Vera R. Filby (968-8014)
Traffic Analysis . . . . . Robert J. Hanyok (963-5734)

Illustrator . . . . . [redacted] (963-3057)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptolg at bar1c05
(bar-one-c-zero-five)
(note: no 'o' in 'log')

Always include your full name, organization, and secure phone number.

For Change of Address
send name and old and new organizations to:
Editor, CRYPTOLOG, P1

Contents of CRYPTOLOG should not be reproduced or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

P.L. 86-36

PUZZLE MAKERS, PUZZLE SOLVERS (u)

(U) David H. Williams, Puzzle Editor and former Editor-in-Chief of CRYPTOLOG, retired in November. He is better known as DHW, the compiler of those fiendish NSA-Crostics that challenge even the most successful of NSA's renowned puzzle solvers. Those puzzles have been a popular feature of this magazine, and will be missed by the many subscribers who always turn to the back pages first.

(U) DHW, in his persona as Dave, linguist, telemetrist, punster, and walking encyclopedia, will also be missed by his colleagues, and especially by the present editor. He was a favorite source of information, for he presented facts with witty explanations and humorous illustrations, even on sober and arcane subjects.

(C) In a small circle David H. Williams will always be remembered [redacted]

(U) Now a word of comfort for the busman's holiday puzzle solvers who abound in this Agency: Take heart. We'll see to it that there's a puzzle of some kind or another in the back pages. And we invite puzzle makers among the readers to contribute their concoctions.

(U) About solutions to the puzzles: "all the news that fits we print," to quote the motto of this editor's high school newspaper. We expect to catch up in the next issue. But we do solicit comments from readers on whether the solution should appear in the same issue as the puzzle or in the next issue.

P.L. 86-36
EO 1.4.(c)

P.S. for DHW fans: find the pun.

~~CONFIDENTIAL~~

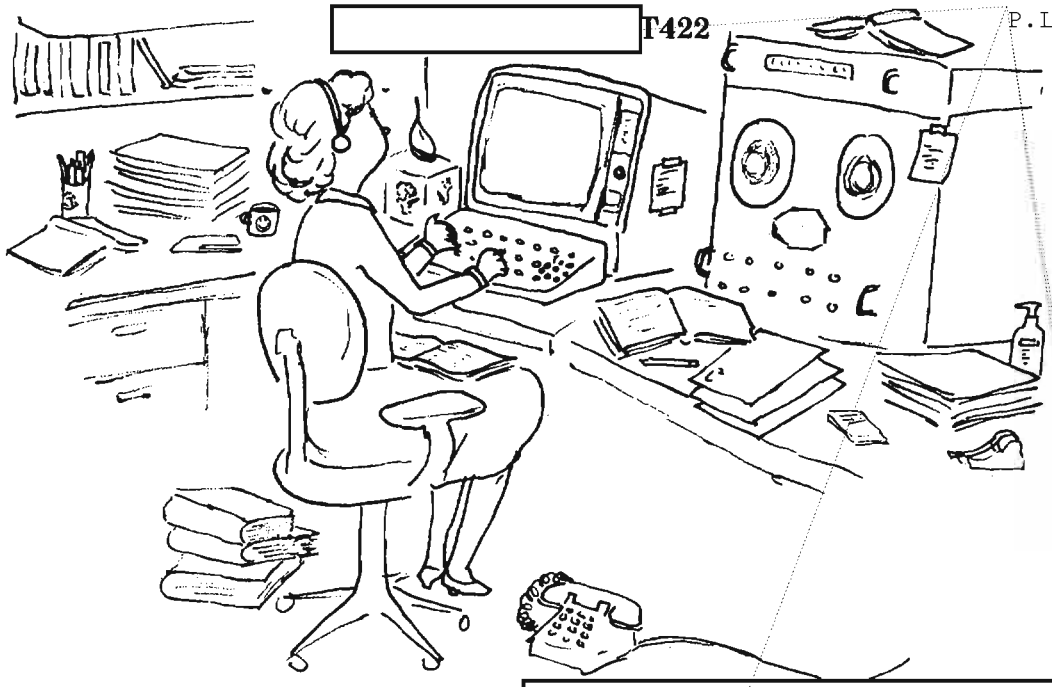
DOCID: 4012016

~~CONFIDENTIAL~~

SEMESTER: A QUANTUM LEAP FORWARD (U)

T422

P.L. 86-36



P.L. 86-36
EO 1.4.(c)

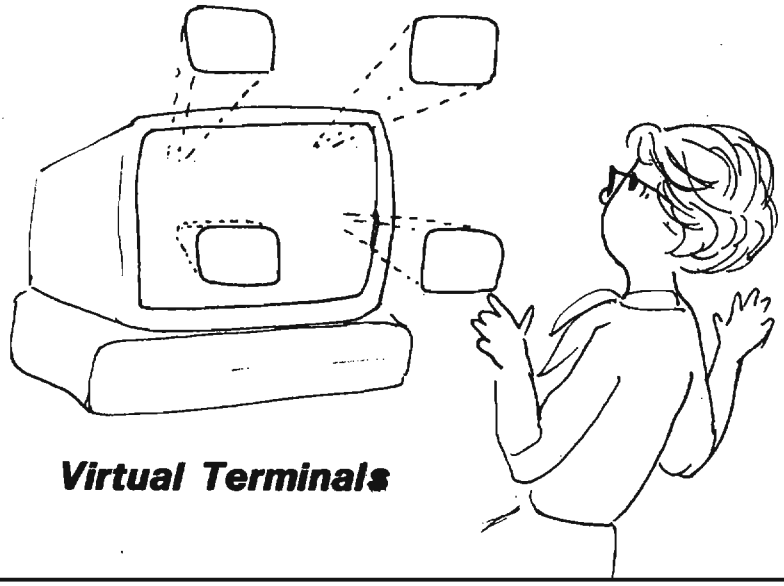
~~This article is classified C CCO in its entirety~~

Computer-supported transcription has taken a quantum leap forward. Now under the project name SEMESTER

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~CONFIDENTIAL~~

DOCID: 4012016

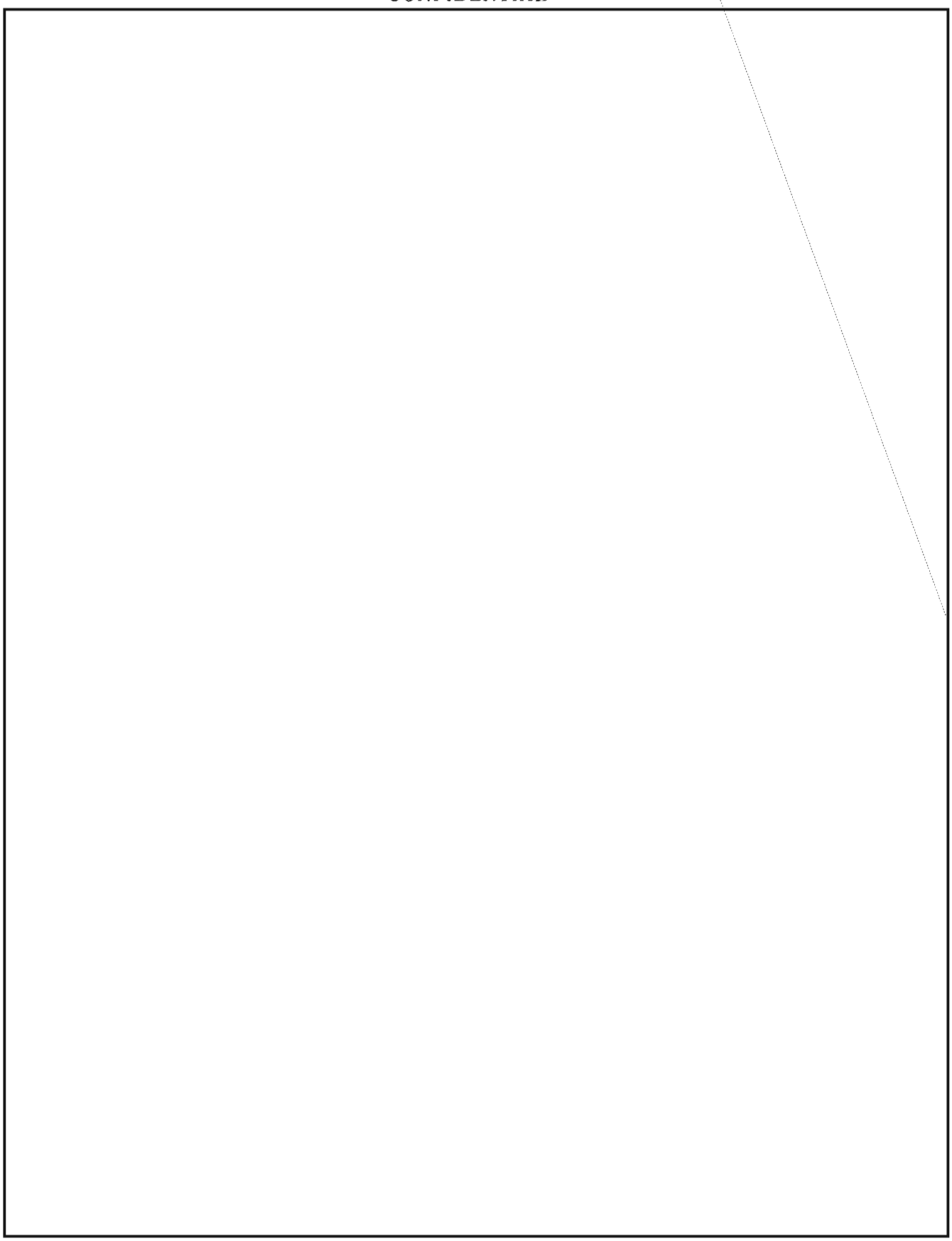


Virtual Terminals

P.L. 86-36

DOCID: 4012016

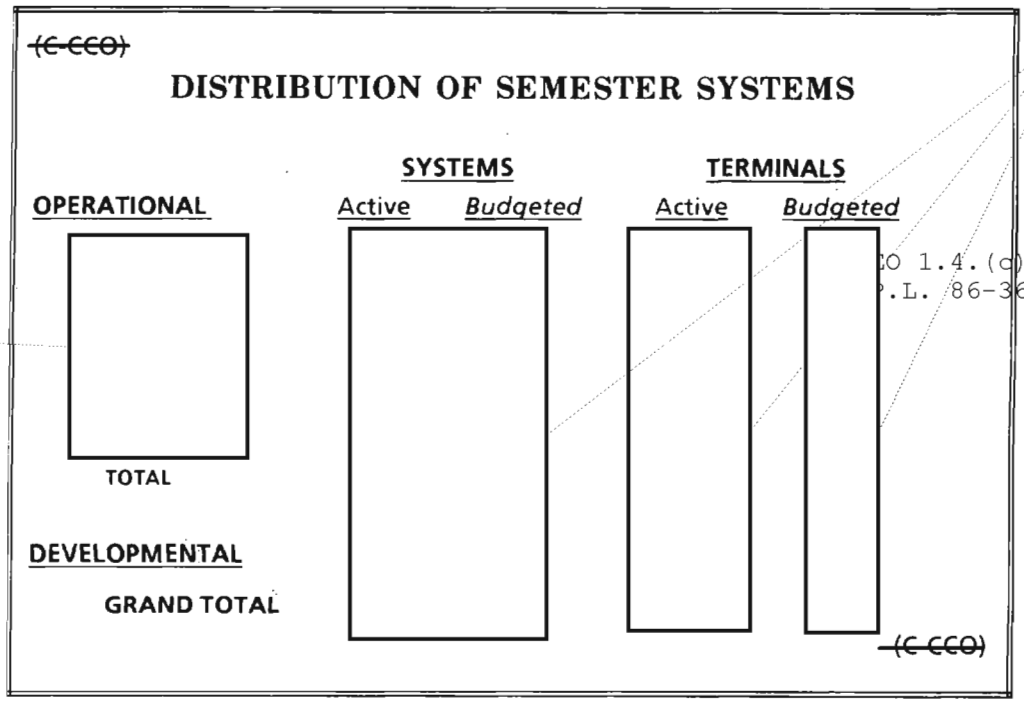
P.L. 86-36



DOCID: 4012016

~~(C CCO)~~

DISTRIBUTION OF SEMESTER SYSTEMS



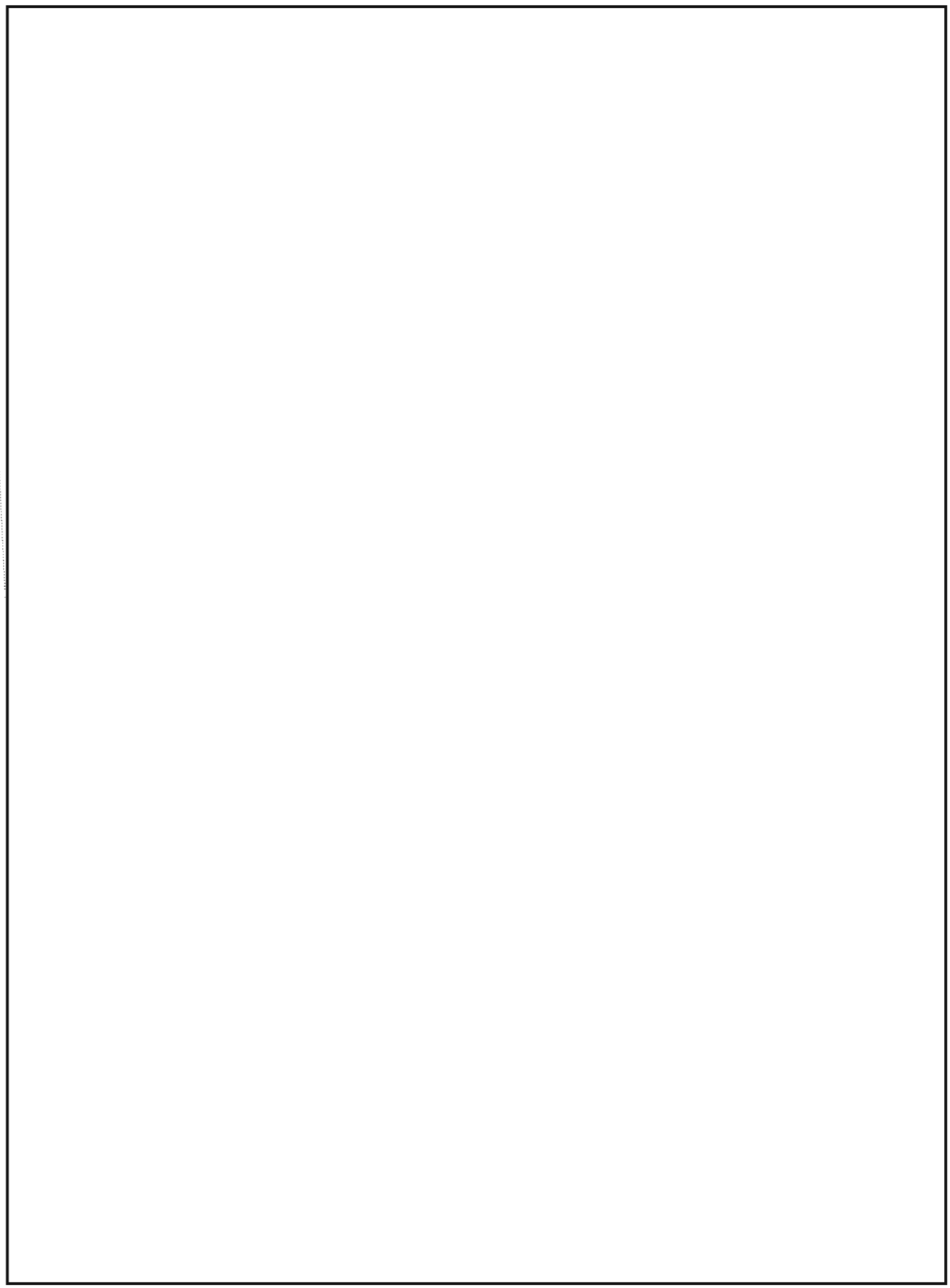
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

EO 1.4.(d)
EO 1.4.(c)
P.L. 86-36

P.L. 86-36

DOCID: 4012016 P.L. 86-36



P.L. 86-36

P.L. 86-36

DOCID: 4012016

~~CONFIDENTIAL~~

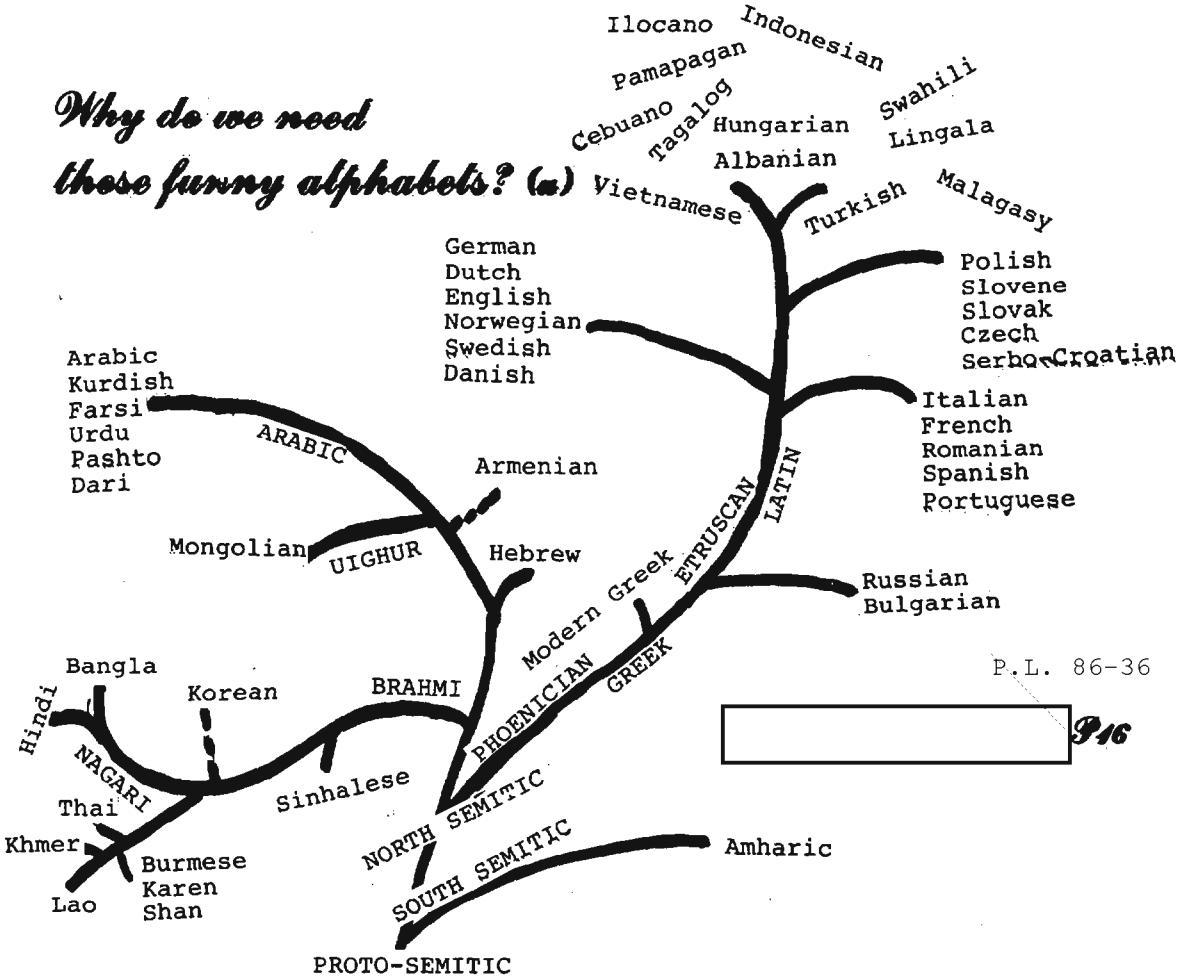
Editor's Note:
Readers may be interested in the article "Computer-Aided Transcription" by the same author that appeared in the April 1976 issue of CRYPTOLOG.

BULLETIN BOARD

~~HANDLE VIA COMINT CHANNELS ONLY~~ EO 1.4.(c)
~~CONFIDENTIAL~~ P.L. 86-36

DOCID: 4012016

Why do we need those funny alphabets? (a)



P.L. 86-36

[redacted] P16

We have reached the level of technology in which we plan supercomputing research centers, fill the basement with Crays, and strain our electrical circuits to the breaking point with ASTW's, ASH's, HPW's, and every kind of advanced electronic equipment we can find. With such great advances in the state of the art do we still have to use that good old 26-letter English alphabet to represent all of our foreign language material on computers?

What Can We Do With Foreign Scripts?

Foreign scripts and diacritical marks on Roman letters convey useful information to the translator which is sometimes missed in transliterations into Roman letters lacking those marks. Because of the variety of transliteration schemes, transliterations are often ambiguous and sometimes confusing, and lack the subtle distinctions of a language written in its own script. In addition, our linguists usually come to NSA trained in reading the native script, and having to learn a new representation for the language delays their effectiveness.

The same problem arises in creating on-line working aids for linguists, and here the correct representation of the language is even more important. The transliteration is often a cruder version of the language, and therefore transliteration systems vary from target to target and even from analyst to analyst, so that transliterations are less useful for dictionaries, glossaries, bookbreaker's tools, etc. Without the proper tools to build a glossary, some linguists at NSA are building on-line working aids with idiosyncratic transliterations which make them difficult to use by anyone but the authors. When the authors transfer to new assignments their experience and insight are lost because other people cannot find the terms they have recorded.

Where Did All Those Foreign Alphabets Come From?

Oddly enough, they all came from the same place. Considering how useful an alphabet is for representing a language, it is surprising that the alphabet was invented only once, about 3500 years ago in the Fertile Crescent. All of the many other alphabets in the world either borrowed an alphabet descended from this early

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012016

Semitic alphabet, or borrowed the idea of an alphabet and invented their own script, as apparently the Koreans did.

The Greeks received the Semitic alphabet from the Phoenicians when trade brought them into contact. The Greeks recognized the potential of an alphabet, although the Phoenician alphabet was not suitable for Greek because it did not contain signs for Greek vowels. In the Semitic languages vowels are not very important for distinguishing words (as they are in Indo-European languages) because they usually denote inflections and different parts of speech which can be understood from context.

The Greeks added vowels, a very important innovation to the alphabet. Greek words stripped of their vowels, as is the case with many languages, are indistinguishable from other words with different meanings. In English, the consonants "ct" could stand for "act" "cat" "cut" "cute" "acute", etc.

The Greeks took letters of the Phoenician alphabet which they didn't need (because their language didn't have the same sounds as Phoenician) and used them for the Greek vowels. This adaptation by the Greeks made their alphabet a reasonable representation for European languages, and the two alphabets now found in use in Europe, Roman and Cyrillic, can both be traced to the Greek alphabet.

The other alphabets in the world can be traced to other Semitic variations of the alphabet. The only surviving descendent of South Semitic is the Amharic script. Aramaic, a North Semitic alphabet, was as productive as the Phoenician alphabet, giving rise to Arabic and the Arabic-related scripts used for Urdu, Farsi, Dari and Pashto. The Indian and Southeast Asian scripts probably also came Aramaic. The Nagari, Devanagari, and Gurmukhi scripts (among others in India) are descended from the Indian branch of the Aramaic-based scripts, while another very productive branch, the South Indian, has given rise to the Southeast Asian scripts: Burmese, Karen, Shan, Lao, Thai, Khmer, etc.

How is an Alphabet Adapted to a New Language?

The sound pattern of each language is unique, as distinct as a fingerprint. Some type of adjustment must always be made to fit an existing alphabet to a new language. A variety of techniques can be used for this task, including dropping unneeded letters or using them for other sounds which are needed in the new language, combining two or more letters to represent a new sound, inventing new symbols or borrowing symbols from another alphabet to represent a new sound using diacritical marks (small marks above or below the letter, such as accents), or using one symbol for two or more sounds.

The Roman alphabet was adopted by many languages from different linguistic groups, so it is not surprising that many changes had to be made. In adapting the Roman alphabet to their languages, most people combined letters or added diacritical marks. The result of all these adaptations is that the extended Roman alphabet bristles with diacritics, predominately on the vowels. The 5 vowels of the Roman alphabet are its most glaring weakness in representing a language. English has approximately 12 vowels (depending on the dialect) so we have to overcome this shortage by combining vowel sounds under a single vowel representation. Any one who has worked with a child learning to spell English is aware of the confusion which this can cause.

The Roman Alphabet: A Gift from the Gods or Just Another Script?

We received the upper case letters of the Roman alphabet literally, carved in stone. The Romans had a penchant for building monuments and chiselling inscriptions on them. They therefore modified their alphabet to forms which could be carved easily into stone, and would at the same time provide a grand and elegant display.

Centuries later, after the invention of the computer by English-speaking people, these same letters proved to be easy to display with a small matrix of dots by a printer, or later on a CRT. The lower case Roman letters evolved differently. In addition to writing on stone, the Romans wrote on wax tablets, papyrus, and later, parchment. These media, with stylus or ink, demanded a different style of letters which could be written more quickly than the capital letters. This need gave rise to the cursive style and lower case letters.

The lower case letters are not as easy to print and display on a computer because some of them extend below the base line, and the enclosed spaces are smaller, requiring higher resolution, that is, more dots, to represent them clearly.

Nevertheless, lower case letters have been added to computer character codes, and ASCII, the American Standard Code for Information Interchange, now has both upper and lower case Roman letters to represent English. Lower case letters are therefore available on a growing number of computers.

In terms of the development of the computer, the English version of the Roman alphabet has been a gift from the Gods, providing the simplest writing system in the modern world for displaying text on a computer, and thereby facilitating the development of the computer.

In terms of representing text, or understanding natural languages, however, it is important to

~~FOR OFFICIAL USE ONLY~~

OCID: 4012016

ALPHABETS ON THE XEROX STAR

Afrikaans	Dutch	Japanese	Romanian
Albanian	English	Khmer	Russian
Amharic	Farsi	Korean	Serbo-Croatian
Arabic	French	Kurdish	Slovak
Armenian	German	Lao	Slovene
Bangla	Greek	Lingala	Spanish
Bulgarian	Haitian Creole	Maghrebi Arabic	Swahili
Burmese	Hebrew	Malagasy	Swedish
Cebuano	Hindi	Norwegian	Tagalog
Chinese	Hungarian	Pampangan	Thai
Czech	Ilocano	Pashto	Turkish
Danish	Indonesian	Polish	Urdu
Dari	Italian	Portuguese	Vietnamese

(U)

P.L. 86-36

remember that the English version of the Roman alphabet is just another script.

How Can We Represent the Other Scripts on the Computer?

The standard ASCII character code of 7 bits gives us 2^7 or 128 characters to work with. This is only enough for English, and is the character code size of the ASTW and other UNIX-based systems. The extended ASCII code of 8 bits gives us 2^8 or 256 characters, and is displayable under DOS and other operating systems. The extended ASCII code gives us some vowels with diacritical marks and two consonants with diacritics so that we can represent the Scandinavian and West European languages. The extended ASCII code is not sufficient for representing the East European or Asian languages which are written in the Roman alphabet. It contains a few Greek letters used in mathematical or scientific notation, but does not contain the entire Greek alphabet.

In order to complete the Roman alphabet and to add all of the other alphabets and the Chinese and Japanese syllabaries, we obviously need a far larger character code than we can get using a single computer word of 8 bits.

Xerox has solved this problem by building a double word for the Xerox STAR character code. The 16-bit character code gives us 2^{16} or 65,536 characters to use in representing our alphabets and syllabaries, which is ample space to specify the various characters for all [redacted] languages. The code expands to 16 bits only where needed for the language fonts, so space is not wasted in processing text in the standard ASCII code. In addition to developing an operating system and character code which is capable of displaying all of these foreign languages, Xerox has already built many foreign-langauge character fonts. With the 1986 software release, a total of 52 languages will be available on the new, faster, fully-programmable Xerox STAR.

Should NSA Abandon the 7-bit ASCII Standard for Language Processing?

Yes. The 16-bit extended ASCII code is compatible with the 7-bit or 8-bit ASCII codes, so our data bases in English will be fully compatible with the 16-bit character code as has been demonstrated by connecting the Xerox terminals to CARILLON and other computer systems.

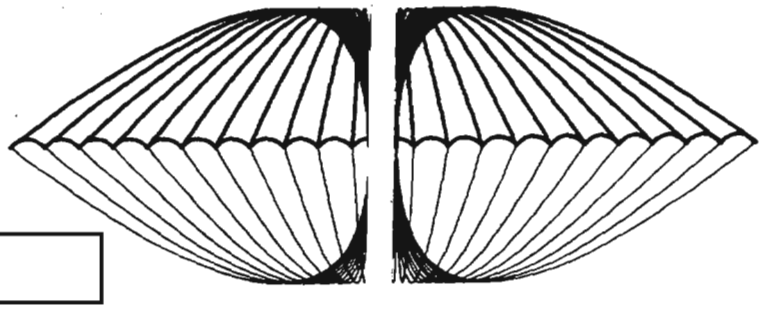
Now that computer processing has developed to the point where we are talking about massively parallel processing and millions of operations per second, do our linguists still need to be shackled by a writing system devised by Roman stonecutters 2000 years ago? □

~~FOR OFFICIAL USE ONLY~~

OCID: 4012016

SHELL GAME

hyphen-ation



wes

P.L. 86-36

The other day I wanted to check the hyphenating done by **nroff** on a document I'm getting ready to produce. If you've worked with **nroff** (or almost any other hyphenating system), you know that it tries hard but has a few flaws, some of them genuine howlers. **Nroff** allows you to force the hyphens wherever you want, for any given word, but you have to know which words it botches. And every now and then one finds a new one ...

So I decided to build a little shell that would pull out those lines ending with a hyphen, along with the line following, and print them onto a separate file for examination. I decided to use the stream editor **sed**, mostly because it is rather fast. It zips through long files with great ease. I don't know if I want to check the hyphens in a REALLY long file, but I'll worry about that if I ever get one.

The shell file is called **hyck** and looks like this:

```
if x"$1" = x goto usage
= l $s/lib
echo hyck of file: $1 > hyck.out
sed -f $l/hyck.lib $1 >> hyck.out
wc hyck.out
e hyck.out <--
exit
: usage
echo Usage: hyck filename
```

Line 1 checks for a filename in the command line and bails out with an error message if it doesn't find any.

Line 2 assigns the variable **l** (letter L) a string which equates to my directory **lib** at top level. I have top level directories named **bin**, for my executable files, including shells, and **lib**, for my library files. It is my habit in my.profile to assign my **bin** directory the shell variable **b** and to assign my **lib** directory the variable **l**.

This shell **hyck** is kept in my **bin**, and a companion file called **hyck.lib** is kept in my **lib**. The variable **s** on line 2 is a standard shell variable which always expands to my home login directory.

Line 3 puts the first line into file **hyck.out**, a reminder of the content of the file -- I get forgetful sometimes.

Line 4 does the work, running the **sed** according to the commands listed in the companion file **hyck.lib** located in my **lib** directory. The output is added to file **hyck.out**; if the >> were a >, the file would first be erased.

Line 5 gives me a count of words and lines.

Line 6 puts the output file into the screen editor for me.

The companion file **hyck.lib** looks like this:

```
#n Pr hyphen lines and fol lines
/[¢ -]-$/{
     =
     : loop
     p
     n
     /[¢ -]-$/b loop
     p
}
```

Line 1 says "don't print any line unless asked to."

Line 2 looks for a line ending with a '-' but not preceded by a space or another '-'. (Note: on some UNIX systems, the ¢ will be a 'hat' or circumflex.)

Line 3 prints the line number

Line 5 prints the line

Line 6 moves to the following line

Line 7 branches back to Line 4 ('b loop') if this is another line ending with a hyphen.

Line 8 prints this line, presumably one that doesn't end with a hyphen.

Your own private bells and whistles can be added. □

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012016

BOOK REVIEW

P.L. 86-36

by [redacted] P12.

KRYPTOLOGIE

by PATRICK HORSTER,
Rheinisch-Westfälische Technische Hochschule Aachen

published by Bibliographisches Institut
Wissenschaftsverlag, February, 1985

Editor's note: In order to make it easier for readers to distinguish between the unclassified published material and the classified reviewer's remarks, the latter are shown in **boldface.**

~~(FOUO)~~ **This is a textbook on cryptography which is elementary by our standards and breaks no new ground. But a few of the examples are novel; they will be emphasized in the paragraphs which follow.** The text follows notes which the author has apparently used for a course.

(U) The first five chapters are introductory. The next three concern "classical" cryptology, including DES in Chapter 8. There follow three chapters on public-key cryptosystems. Then two chapters summarize needed results in number theory and elementary algebra. The last chapter contains a brief sketch of rotor machines and the McEliece public-key system (based on "old" Goppa codes). We shall treat only the six central chapters (6-11) which deal with "classical" and "public-key" systems.

(U) Chapter 6 starts with substitution methods. Some of the examples are harbingers: one finds a keyed "P-Box" which permutes inputs; a matrix which later will implement a Hill system appears too. The familiar Vigenère and Caesar systems are also discussed, as are one-time pads and periodic additive systems. Linear feedback shift registers make an appearance, as do Playfair systems and an old system which I didn't recall (it had appeared in a 1902 book in French by Dellastelle).

(U) Moving quickly through transposition methods, he closes the chapter with a section on composite codes. He defines an SP-system, of which DES is an example, as a product of substitutions and permutations. Huffman coding also appears here. He says that composite ciphers can be very hard to break, giving an example in which three operations are performed:

(1) addition mod 36 (the standard alphabet followed by the ten digits 0-9) using a periodic key. In his example, the key is TEXT and the plaintext SCHUTZ is enciphered: SCHUTZ + TEXTTE = BG4DC3;

(2) conversion to digraphs from the alphabet {A, B, C, D, E, F} by use of a 6x6 matrix with the 36 alphanumeric elements in scrambled order in the matrix;

(3) finally, application of a fixed 6-long permutation to the resulting stream in blocks of six.

(U) Horster gives a second composite scheme which he associates with the Russian spy Reino Hayhanen:

(1) encipherment with a monome-dinome matrix, with the resulting stream entered into a 9-wide matrix;

(2) application of a permutation key followed by extraction by columns from the 9-wide matrix; the resulting text is then entered into a 6-wide matrix not horizontally but following a "staircase" design.

(3) application of still another permutation key; and extraction of the columns of the 6-wide matrix to be read off as cipher.

(U) Chapter 7 details standard cryptanalytic techniques, with an emphasis on monoalphabetic frequency distributions. Shannon's information-theoretical approach is mentioned. The "method of Kasiski and Friedman" shows how the length of the key in a periodic polyalphabetic substitution system can be determined by counting the distance between long repeats. The index of coincidence is cited as a useful tool. He shows that book ciphers can be attacked by cribbing, using high frequency letters. His text came from Ray Smullyan's "This book needs no title"! He shows that knowledge of the first 2n values of a key stream generated by a

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~CONFIDENTIAL~~

OCID: 4012016

EO 1.4.(d)
P.L. 86-36

P.L. 86-36

linear n-stage shift register will allow solution. He uses Gaussian elimination to solve the system of n equations. Finally, he explains a chosen plaintext attack on the Hill system.

~~(FOUO)~~ Chapter 8 is devoted to DES. It contains the usual description, a section on modes of operation, **and an inconclusive section on security. I could find nothing new in this chapter.**

~~(C-CCO)~~ Chapter 9 deals with the public key distribution system, attributed in the outside literature to Pohlig and Hellman [redacted] the encipherment of a message x is x^e mod p; decipherment is performed by an operation of the same form (exponent d, with ed = 1 mod p-1). Horster discusses known methods for taking logarithms mod p, but does not get into the exciting recent work of Odlyzko and Coppersmith.

~~(C-CCO)~~ In Chapter 10 we find a description of the RSA (Rivest-Shamir-Adleman) algorithm, [redacted] Horster shows how to recover the plaintext when two identical messages are enciphered with different exponents but the same (compound) modulus. He discusses the attack on RSA which arises from the iteration of the encipherment operator. One section is allotted for a discussion of the modification attributed to Hugh Williams (recall that one of the two primes whose product yields the modulus n is congruent to 3 mod 8, the other to 7 mod 8) and the proof that this modification makes solving the RSA scheme as difficult as factoring.

~~(FOUO)~~ The longest chapter in the book is Chapter 11, presenting systems based on knapsacks. Although all of the knapsacks had appeared in the literature, I confess to an unfamiliarity with a few of them. He defines the usual superincreasing knapsack ("simpel," or "extra simpel" if the knapsack elements are not permuted) and shows how a modular transformation provides a trapdoor in the system. The Graham-Shamir system is introduced. A knapsack attributed to C. Leung (1978) and another designed by Willett (1983) are described. Both of these had escaped my attention. **Others who may have seen them have, quite reasonably, ignored them.** The attack of Shamir which destroyed the Merkle-Hellman knapsack is sketched, but the recent developments (due to Brickell and Lagarias) which showed the weakness of the iterated Merkle-Hellman scheme are not mentioned. Signatures via knapsacks receive cursory consideration.

~~(FOUO)~~ **In summary, this book is an elementary summary of known results. I find that it is well written, but it is neither as complete nor as advanced as, for example, the recent book of Konheim.** □

LETTER TO THE EDITOR

Thank you for publishing the help-wanted ad for A331. This was a quick way to put the word out to the cryptanalytic community; it was faster than going through normal personnel channels. As a result we found a cryptanalyst to fill the position [redacted] ~~(FOUO)~~.

Chief, A331

~~SECRET~~

OPPORTUNITY

ONE-OF-A-KIND JOB FOR:

- *a technically-oriented SR, IR, or linguist*
- *a literate cryppie or computer scientist*
- as a team member on a high-visibility project involving G4's enciphered speech mission to document software engineering development
- must be able to communicate with highly creative managers, programmers, and analysts
- will be expected to develop a coherent document from the writings of several authors
- will have a chance to publish independent papers
- must be able to meet deadlines.

For further information contact:

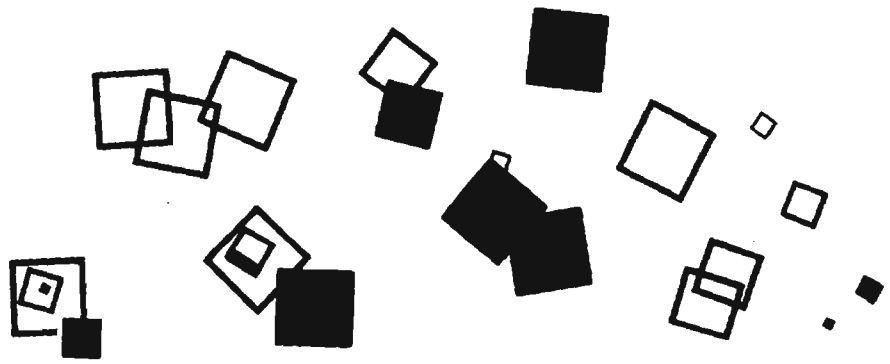
[redacted] 5434, 963-1499

~~(S-CCO)~~

P.L. 86-36

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

DOCID: 4012016

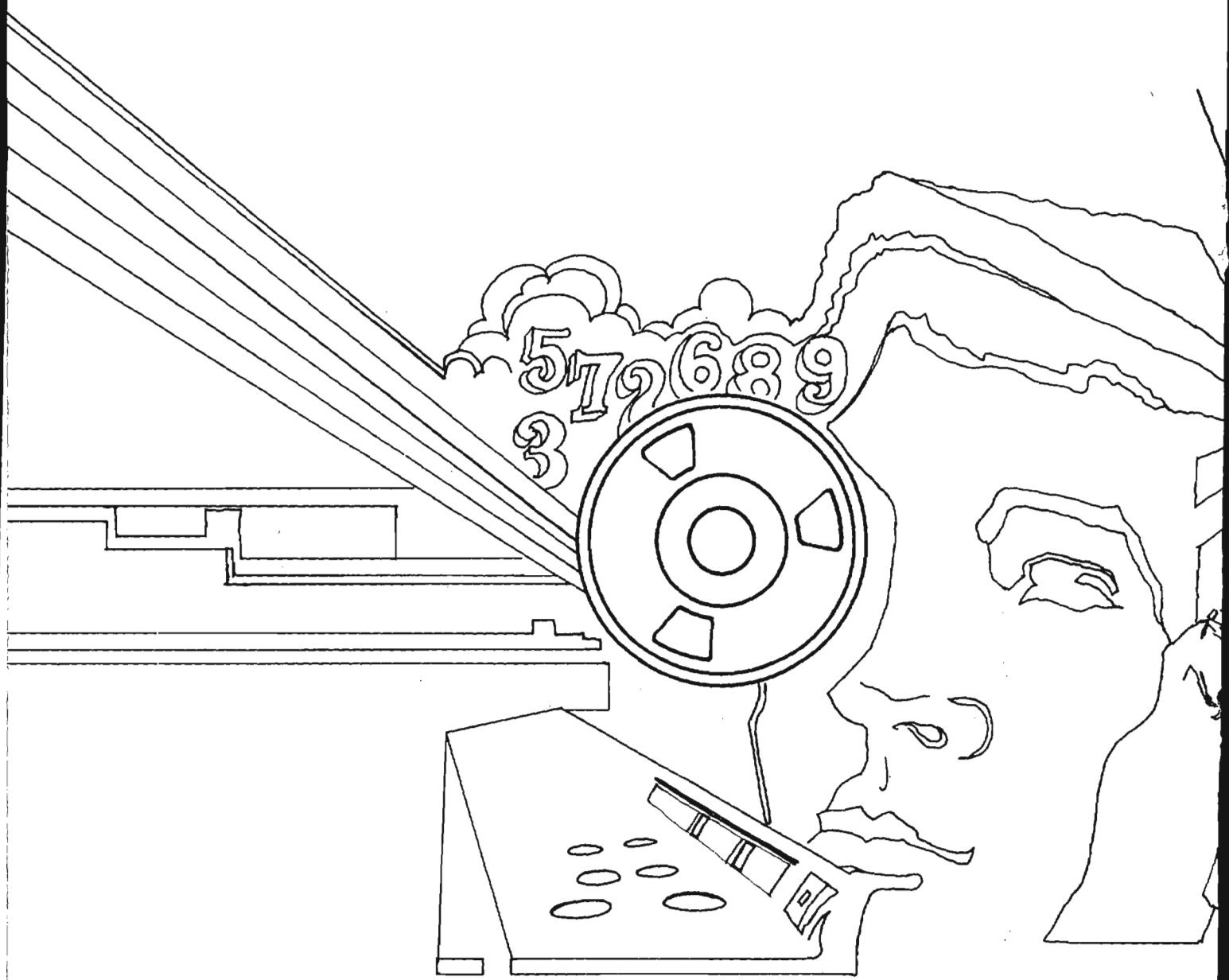


P.L. 86-36

PUZZLE IN PURPLE

CONTRIBUTED BY M.W. ("DANNY") WALTZ

~~FOR OFFICIAL USE ONLY~~


5726893

DOCID: 4009965

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

SEP-OCT 1985

P.L. 86-36

UNDERSTANDING THE FREEDOM OF INFORMATION ACT (U).. [redacted] 1
QUOTE WITHOUT COMMENT (U).....4
LETTER TO THE EDITOR (U).....Albert I. Murphy.....5
THE WORLD-WIDE SOFTWARE SUPPORT SYSTEM (U)..... [redacted] ...6
BOOK REVIEW: THE NEW KGB (U)..... [redacted] 9
BULLETIN BOARD (U).....10
ON THE LIGHTER SIDE (U).....Vera R. Filby.....11
FROM THE PAST (U).....12
ETYMOLOGIST'S DELIGHT II (U)..... [redacted] ...13

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

DOCID: 4009965

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XII, Nos. 9-10. . . . . September-October 1985

PUBLISHER . . . . . [redacted]

BOARD OF EDITORS

Editor . . . . . [redacted] (963-1103)

Collection . . . . . [redacted] (963-3683)
Computer Security . . . . . [redacted] (968-8141)
Computer Systems . . . . . [redacted] (963-1103)
Cryptanalysis . . . . . [redacted] (963-4740)
Cryptolinguistics . . . . . [redacted] (963-1596)
Index . . . . . [redacted] (963-5330)
Information Science . . . . . [redacted] (963-1145)
Intelligence Research . . . . . [redacted] (963-5275)
Language . . . . . [redacted] (963-5151)
Linguistics . . . . . [redacted] (963-3896)
Mathematics . . . . . [redacted] (963-5566)
Puzzles . . . . . David H. Williams (963-1103)
Science and Technology . . . . [redacted] (963-4191)
Special Research . . . . . Vera R. Filby (968-8014)
Traffic Analysis . . . . . Robert J. Hanyok (963-3888)

Illustrator . . . . . [redacted] (963-3057)
Distribution . . . . . [redacted] (963-3369)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptolg at bar1c05
(bar-one-c-zero-five)
(note: no 'o' in 'log')

Always include your full name, organization, and secure phone number.

For Subscriptions or Change of Address
send name and organization to:
Editor, CRYPTOLOG, P1

Contents of CRYPTOLOG should not be reproduced or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

EDITORIAL

P.L. 86-36

"Ah, for the good old days ..." NSA writers often sigh when faced with the final chore of their task: marking each paragraph with the appropriate classification. It is a tedious job, and somehow there's always a paragraph or so that takes an unbelievably long time to classify properly.

Well, we've got to do it. One reason can be found in the article on the Freedom of Information Act, beginning on the next page. Everything we write is subject to review. Yes, *everything*. So it does make things easier for the overworked reviewers to scan paragraph classifications than to read carefully an extensive paper that might have but a single classified reference.

And it's no fair trying to play dodgem by overclassifying -- it's also no go; someone will catch it (there are eagle-eyed people everywhere) and make more work for you. Besides, it's hard as it is to get people on the outside to respect our classification system; this will come only when we respect it ourselves. When classification is assigned properly in accordance with the rules, it can successfully withstand challenge.

Occasionally you'll see a notation to the effect that the entire report or article has been classified thus-and-so. That is usually because the classification is the same throughout. If in doubt, do consult your classification officer.

Meanwhile, a true confession: even with all the review CRYPTOLOG undergoes, there's slippage every once in a while, as you will see below.

Ed.

CORRECTION

Please make the following classification changes in the May 1985 issue: Change the classification of page 4 to S-CCO, and change the classification of the fourth paragraph of the article "The Summer Language Program" on page 4 to S-CCO.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009965

UNDERSTANDING THE FREEDOM OF INFORMATION ACT (U)

[redacted] U P.L. 86-36

The Freedom of Information Act (FOIA) affects everyone at NSA. All of us, whether we know it or not, do work which is subject to review - and possible release - under the FOIA. Some of us, sooner or later, may be called upon to review information in response to an FOIA request. Most of us, however, are unaware of the FOIA, have questions about the Act, or would like to understand it better.

The FOIA was enacted by Congress for the principal purpose of broadening access to information about the governmental process. Strengthened by a series of amendments in 1974 and 1976, the FOIA is the primary disclosure statute opening the records of the U.S. Government to public scrutiny. NSA records are subject to requests made under the FOIA and, since virtually all written work product reflecting the official business of the Agency is considered an "agency record," this has the practical effect of subjecting nearly all the written documentation prepared by Agency employees to review and possible disclosure under the FOIA.

BASIC STATUTORY CONTENT

The basic concept of the FOIA requires that an agency, upon receipt of any request reasonably describing the records sought, provide those records to the requester unless the information contained within the records is protected against disclosure by the coverage of nine narrowly drawn statutory exemptions. The exemptions are designed to protect information of particular sensitivity. Thus, there is an attempt to strike a balance between the public's need for information concerning the governmental process and the government's need to preserve the secrecy of certain information compiled in performing its governmental functions.

Exemption 1 to the FOIA protects information currently and properly classified pursuant to executive order in the interest of national defense or foreign policy. Used by NSA to protect classified information from public disclosure, it protects all information properly classified under Executive Order 12356, or originally classified under previous executive orders where the information remains properly classified under Executive Order 12356.

Exemption 2 applies to matters relating solely to the internal rules and practices of an agency. Under this exemption, NSA withholds matters meeting one of two criteria:

- routine, trivial administrative matters in which there is no genuine significant public interest; or
- matters which are "predominantly internal" where, despite the existence of genuine public interest in the subject matter, disclosure would risk circumvention of the

~~FOR OFFICIAL USE ONLY~~

statutes or regulations governing Agency activities.

Exemption 3 authorizes the withholding of information which is protected against disclosure by statute. Federal agencies currently utilize over 130 different statutes to withhold information under the auspices of the third exemption, but NSA principally relies on four different statutory mandates:

- Public Law 86-36 (50 U.S.C. §402 note) - This is the National Security Agency Act of 1959, section 6 of which protects against the disclosure of any information regarding the organization, functions, and activities of NSA; or of the names, titles, salaries, or numbers of employees at the Agency. In asserting the third exemption, NSA cites Public Law 86-36 more frequently than any other statute in protecting both classified and unclassified information concerning the Agency's functions and activities.

- Section 102(d)(3) of the National Security Act of 1947 (50 U.S.C. §403(d)(3)) - This statutory provision authorizes the Director of Central Intelligence (DCI) to protect intelligence sources and methods. As a member of the Intelligence Community, NSA uses this statute in protecting its own sources and methods pursuant to authority conferred by the DCI.

- 18 U.S.C. §798 - A criminal statute, section 798 makes it unlawful to disclose classified information concerning: (a) cryptographic systems, equipments, devices, or designs; or (b) the communications intelligence activities of the United States or any foreign government to any unauthorized person. In requiring that information be classified as a prerequisite to its application, this statute is always used in conjunction with the first exemption.

- 10 U.S.C. §140C - Recently enacted, this statute authorizes the withholding of technical data with military or space application in the possession of, or under the control of, the Department of Defense, if such data may not be lawfully exported outside of the United States without an approval, authorization, or license under the Export Administration Act of 1979 or the Arms Export Control Act.

Exemption 4 protects trade secrets and confidential commercial information. Used primarily in handling requests for information relating to NSA contracts, it allows the Agency to withhold commercial or financial information provided by contractors and other outside entities where disclosure would either impair the Agency's ability to obtain similar information in the future or would cause substantial competitive harm to the company providing the information.

Exemption 5 permits the Agency to withhold information contained within intra-agency or inter-agency memoranda where the information is otherwise protected against disclosure by legal privilege. The privileges most commonly applied are the attorney-client, attorney work-product, and the executive privilege with the latter being used extensively to protect information reflecting predecisional opinions or advice rendered by employees in the Agency decision-making process.

Exemption 6 allows the Agency to withhold information where disclosure would constitute a clearly unwarranted invasion of personal privacy.

Exemptions 7, 8, and 9 are inapplicable to NSA's mission so they are seldom, if ever, invoked. They cover information in investigatory records compiled for law enforcement purposes, information regarding the regulation or supervision of financial institutions, and geological or geophysical information.

MECHANICS OF ADMINISTERING THE FOIA

While the FOIA establishes basic principles of disclosure, administering the act is accomplished through procedures developed and implemented by the individual agencies. NSA procedures provide that a requester may seek access to Agency records by a written request reasonably describing the records sought. The Directorate of Policy is charged with administering Agency FOIA activities and the Director of Policy serves as the Agency's Initial Denial Authority; i.e., the Agency official responsible for all initial determinations regarding the releasability of Agency records.

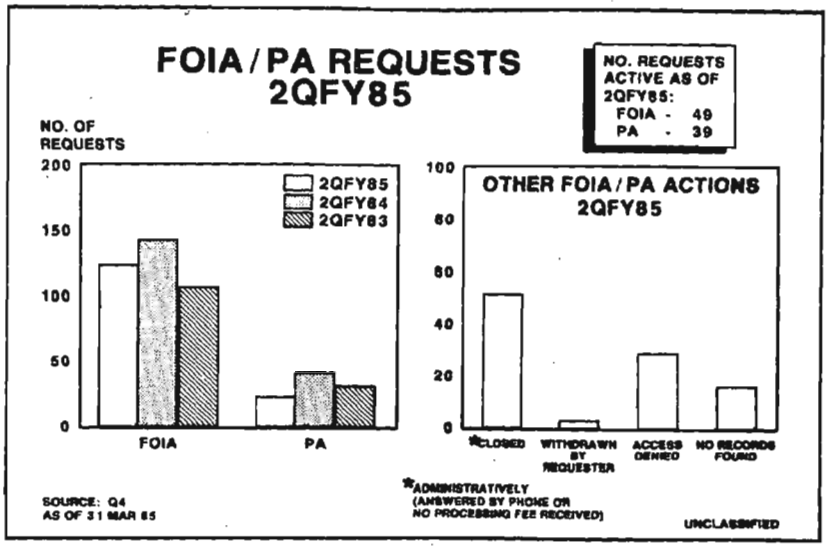
Upon receipt of an FOIA request, the Information Policy Division coordinates both the search for and the review of NSA records responsive to the request. In reviewing records, Agency components must be mindful of the FOIA's requirement to release all "reasonably segregable" information contained within otherwise exempt material. The concept of "reasonable segregability" means that even classified documents must be reviewed to determine whether information responsive to a request can be separated from otherwise classified material and released to the requester. (It is for this reason that marking classified documents by paragraph is now the rule. It greatly faciliates the review process.)

The FOIA provides 10 working days to process a request (i.e., search for, recover, and review responsive documents) and reach a determination regarding the releasability of responsive records. An additional 10 working days is permitted under "unusual circumstances," e.g., the need to obtain records from outlying field facilities, the processing of voluminous records, or the need to consult with other agencies having an interest in the disposition of the records.

CID: 4009965

STATISTICS ON FOIA AND PA REQUESTS TO NSA, 2QFY85

(U) The following reflects the actions processed under the provisions of the FOIA and PA for 2QFY85 and also compares actions processed for 2QFY83 through 2QFY85. In addition to the actions highlighted below, 108 requests were processed in which the requester received records from which certain sensitive information had been removed. A total of 277 FOIA and PA requests have been received by the Agency through 2QFY85 (versus 330 for the same period last year). To date, 71 of the requests were referred to NSA/CSS by other agencies. The figures do not reflect PA requests by Agency employees which were handled internally by the record holders.



Upon reaching a determination regarding the disposition of responsive records, NSA releases those non-exempt records (or portions thereof), informs the requester, in writing, of the specific exemptions supporting the withholding of those records not released, and advises the requester of the right to appeal any withholdings. Replies to FOIA requests must explain any denials of information, citing the exemptions and statutes invoked.

Under NSA FOIA regulations, a requester has 45 days in which to appeal the withholding of any information. Upon receipt of an appeal, the information at issue in the appeal is reviewed *de novo* by the Office of General Counsel which submits its recommendation regarding the appeal to the NSA FOIA Appeals Authority (the Deputy Director) for a final decision which must be made within 20 days of receipt of the appeal. The FOIA provides that any requester denied information on appeal may sue for release of the information in U.S. District Court.

THE FOIA AND NSA

NSA receives hundreds of FOIA requests annually from requesters seeking information about the Agency, about themselves, and about virtually every topic of interest or concern to any segment of the public.

The most common FOIA requests received by the Agency pertain to commercial information and to current or historical events. Requests concerning particular events have included such subjects as the Cuban Missile Crisis, the attack on the U.S.S. *Liberty*, and the assassination of JFK.

Also common are requests for information about the Agency and for personal records. Many people request information about the Agency as a whole, including the history of NSA and/or pictures of the Agency, or about prominent Agency figures such as the Director or Deputy Director, or about particular Agency projects or developments such as the new building or the Computer Security Center. Copies of the *NSA Newsletter* are also frequently requested.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009965

Some individuals want copies of information the Agency may have on file on them. These personal requests usually are also processed under a sister law regarding personal information, the Privacy Act.

Numerous FOIA requests, however, fall in still other categories. Interesting requests received in the past have included:

- queries about UFO's;

- queries from crypt buffs about purchasing classified crypto-equipment.

While requests may often seem arcane, self-serving, and even frivolous, the FOIA remains the principal means by which individuals can obtain information about the government and its activities directly from the government itself.

COSTS AND CONCERNS

Federal agencies spend millions of dollars administering the FOIA each year. (NSA spent over a third of a million dollars on FOIA last year.) While not designed to recoup all the expenses of FOIA administration, the FOIA does provide for the assessment of fees in conjunction with processing FOIA requests. Fees may be assessed for search and duplication costs, but not for the effort expended by professionals in reviewing documents to evaluate the disposition of responsive information. The FOIA provides further that fees should be waived or appropriately reduced where a fee waiver is sought by the requester and when furnishing the information responsive to the request can be considered as primarily benefiting the general public. The Department of Justice has provided considerable guidance to assist agencies in evaluating requests for fee waivers and ensuring compliance with the statutory policy on fees.

Agencies are concerned about the cumulative amount of information released under the FOIA and the degree of effort and number of employees involved. Companies are worried that their competitive ability may be impaired over time by commercial FOIA releases.

Meanwhile, NSA, like all government agencies, must carry out its obligations under the FOIA as long as the Act is in effect. With regard to commercial information, we must provide releasable information to requesters, while also considering the legitimate concerns of the contractors and vendors. In the case of government records, we must respect the public right to be informed, while simultaneously protecting the national security.

Two things are certain: the FOIA will not go away, and like it or not, the FOIA is the law. □

QUOTE WITHOUT COMMENT

Remarks by Dr. Solomon Kullback, guest speaker, at the Phoenix Society Annual Meeting and Dinner Dance, 27 May 1983, at the Fort Meade Officers Club. Reprinted, with permission, from the PHOENICIAN, Summer 1983.

Sometime in January 1981, I received a telephone call in Florida, from an individual who identified himself as "BAMFORD" of "Houghton Mifflin," writing a book about NSA. My mistake was even to talk to him. Although I cannot now remember the details of the telephone conversation, it was limited to some anecdotes about the period of the thirties.

I did not disclose to Mr. Bamford classified or otherwise sensitive information concerning the activities, organization, and personnel of the NSA. Since I have not been privy to any NSA activities since May 1962, I could not make any disclosure, even inadvertently.

Bamford's reference to me in the Preface is completely unwarranted by the facts and of course was without my permission or knowledge. In his unscrupulous fashion he obviously used me to lend an aura of authenticity to his book. I am particularly distressed by the fact that an AMERICAN CITIZEN and an AMERICAN PUBLISHING HOUSE, apparently motivated by the possible monetary returns, and displaying an obvious bias against NSA, would and could publish a book like *The Puzzle Palace*.

Dear Dr. Kullback,

I recently received a summary of a talk you gave to members of the Phoenix Society. I thoroughly enjoyed the stories of your early days in the cryptologic field; you can be very proud of the legacy left by you and your compatriots.

I appreciate your expressions of support for the National Security Agency and your obvious continuing security consciousness. I can imagine your distress over the misrepresentations made by

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009965

Mr. Bamford in his preface, which you referred to in your speech and in your November letter to me. As you noted, he used your reputation to attempt to bring credibility to his book. He did this with other previous -- and some present -- employees to whom he spoke.

Again, thank you for your support.

Sincerely,
Lincoln D. Faurer
Lieutenant General, USAF
Director NSA/Chief, CSS

10 June 1983

LETTER TO THE EDITOR

This is to let people know about a contact I had with James Bamford, author of The Puzzle Palace.

He called me at home one Sunday afternoon to interview me about my lawsuit against NSA for his new book on security practices in government agencies, including those in the intelligence community.

I declined, said that I was still working at NSA, and told him that I had also declined to be interviewed by Mike Wallace on "60 Minutes." He replied that it did not matter, that he had "the entire court record," and that it would be in his book, including my work record which he found "very impressive."

How could he know that? I wondered then, and still do. A summary of my work experience at NSA exists only in a sealed portion of the record, classified TOP SECRET Codeword. It was not to be part of the open record. Nevertheless, on the basis of Mr. Bamford's words and the general tenor of his conversation with me, I am concerned that somehow he did acquire knowledge of the sealed classified record which was a part of my case. An alarming development if so. Or perhaps he was trying to make me believe that, and so entice me into revealing classified information.

These events were duly reported to the proper authorities. But I am assuming that Mr. Bamford is going to describe the case as he said he would and that no effort will be made to prevent him from doing so; a senior Agency official once remarked that such action would be counterproductive.

What must have interested Mr. Bamford is that I won a precedent-setting suit against the Agency under the Privacy Act; I suppose he assumed that I'd be willing to talk to him about it simply for that reason.

The case put on notice those people who, through deliberate intent or just plain ignorance, violate the law. We don't want to see any abuse whatsoever of the constitutional rights of individuals. Nor do we want to see any weakening of our ability to maintain the security practices that are so vital to our National Security. We want to be able to carry out the responsibilities entrusted to us by the American public while at the same time avoiding any actions that have a built-in potential of leading us in the direction of a police state. The task of maintaining the critically important balance between the two is ever-present and difficult. But we can do it without the harmful revelations of Mr. Bamford and others of his ilk.

Albert I. Murphy, E403

LONESOME

Attractive illustrations on Africa (3) seek interesting articles on same. May be scholarly or homespun or straight-from-the-shoulder. Shorties preferred.

Address inquiries to
Editor, CRYPTOLOG, P1

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009965 P.L. 86-36

THE WORLD-WIDE SOFTWARE SUPPORT SYSTEM (U)

~~(FOUO)~~ This is an account of the evolution of software support for NSA computer systems deployed to the field. In the 1970's, fielded ADP encompassed over 300 computer systems consisting of over 30 unique computer mainframes and 60 unique software systems. Contractors were used to deploy these systems to the field, while T311 provided software life-cycle support. Documentation standards were being developed and applied to these systems, but it was not unusual to relax documentation requirements to avoid cost overrun.

DEVELOPMENT

~~(FOUO)~~ The PDP-11/70 was chosen because:
- There were many DEC systems in the field, and even more were to be installed;
- It was compatible with the PLATFORM network and the UNIX/PWB operating system.

~~(FOUO)~~ The UNIX/PWB operating system was to provide:
- Network file transfer capability
- Electronic mail capability
- Word processing and editing features
- File security
- A source code control system

(U) The TSSFs were to be headed by an NSA person and staffed with NSA, SCE, and contractor data system analysts. P.L. 86-36

SOFTWARE SUPPORT FACILITIES

(U) With these implementations, Phase I of W2S3 was completed.

REMOTING TERMINALS TO FIELD SITES

~~(C)~~ Direct communication with major fields sites for software support from the TSSFs was the next step. Terminals at these sites were to be interfaced with the theater facility PDP-11/70 software support system via a 600-9600 baud communication circuit. These remote terminals consisted of a Delta Data 7000 terminal and an Anderson Jacobson letter-quality printer.

~~(FOUO)~~ The Delta Data 7000 was chosen because it was:
- the T standard terminal for UNIX systems;
- TEMPESTed;

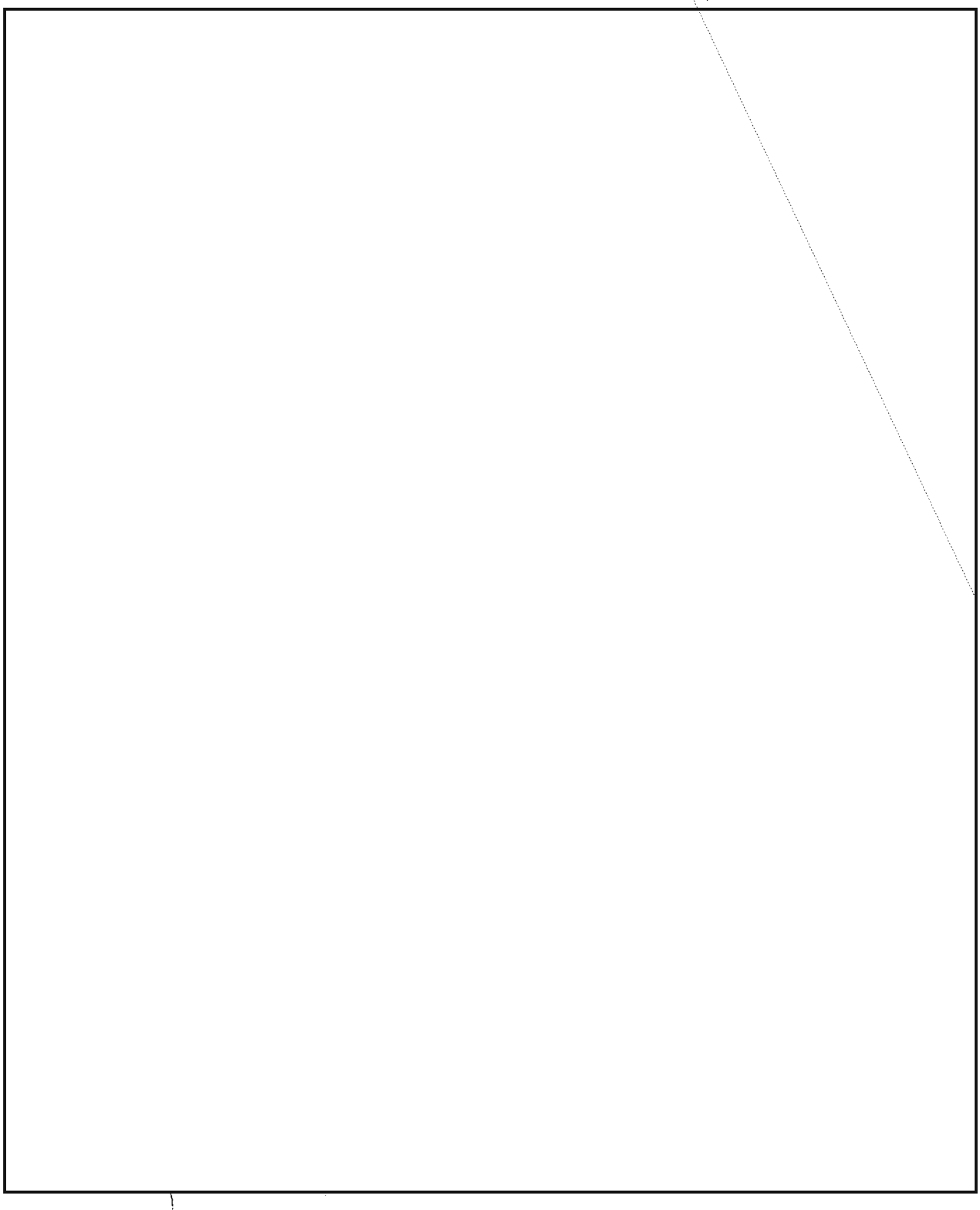
P.L. 86-36
EO 1.4.(c)

 P.L. 86-36

DOCID: 4009965

EO 1.4.(c)
P.L. 86-36

THE WORLD-WIDE SOFTWARE SUPPORT SYSTEM (U)



- a "smart" terminal with a TMS 9900 microprocessor and 24K of memory.

(U) Software packages were being developed to take advantage of the Data Delta's capabilities, including:

- a text editor capable of editing a block of 20,000 characters within the terminal;
- a forms package;
- virtual terminal software which allows the screen to be partitioned into four parts, each capable of performing a different function simultaneously;
- TBASIC, for developing software packages to run on the terminal.

SITE SUPPORT FACILITIES

INCLUSION OF THE SCEs

THE FUTURE

(U) Because of the increasing use of floppy disks for input, storage, and software documentation, they have been purchased for the CSSF, ESSF and PSSF.

~~(FOUO)~~ Microprocessors and their firmware are being proliferated around the world. To meet the demands for programmable read-only memory (PROM) firmware support, a portable universal PROM programmer capable of working with over 200 different PROMs is being purchased for each TSSF and SSF. A hexadecimal keyboard is used to make changes and patches to the PROMs. This suitcase device uses 40 to 60 Hz a/c power. It is capable of interfacing with an RS232 port, such as that on a host CPU, a microprocessor development laboratory, or any remote Delta Data 7000 terminal.

~~(FOUO)~~ The need for and use of a microprocessor development laboratory, cross assemblers/compilers on the network, and the configuration management of microprocessors via the PLATFORM network are now being investigated. Much more remains to be done in the continuing development of this new concept in the support of SIGINT systems in the field. But it has already proven to be a cost-effective asset. □

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4009965

book review

THE NEW KGB

by W.R. Corson & R. T. Crowley

Morrow, NY, 1985

P.L. 86-36

Reviewed by [redacted] P13

Editor's note: In order to make it easier for readers to distinguish between the unclassified published material and the classified reviewer's remarks, the latter are shown in **boldface.**

~~(FOUO)~~ The book traces the history of the KGB from its Cheka origins through the OGPU and NKVD periods, with a great deal of fascinating detail, much of it based on FOIA documents. One of the authors was a senior CIA official. **Although cryptology is only a minor theme in the book, it is worth careful reading for it gives a fairly comprehensive picture of the multi-faceted KGB activities. The brutal and clumsy thugs of the past have been replaced by an elite of competent and loyal Russians who are well prepared to control Russia and to penetrate foreign targets.**

(U) Yuri Andropov was a skilled morse code operator and "knew a great deal about the technical aspects of comunications intelligence, including communications security, cryptography techniques, and related technology. In essence, his own familiarity with all aspects of communications intelligence protected him from being overwhelmed by experts in the field ..." (p.434.)

~~(S ——)~~ As soon as Andropov became chief of the KGB in 1968 he put his knowledge of communications intelligence to work in a sustained exploitation of KL-7 traffic from US military forces in Vietnam, using the rotors, keylists and other information obtained in 1963 and later from the US cipher operator Helmich. (p. 342.) **It is well known that in the black markets of Vietnam, current crypto keys were being sold for about $100.**

(U) Andropov also improved the technical competence of the KGB staffs so that they were able to quickly exploit the "Falcon and Snowman" source that provided satellite technical data and crypto keys. (p 376). In the past, the GRU had provided the technical skills, but KGB technical staffing have improved, so that the authors estimate that there are now between 4000 and 8000 KGB and GRU agents in the US concerned with just scientific and technical espionage, concentrated around technical targets such as Silicon Valley and Ft. Meade. (p. 376.)

(U) The exploitation of the Pueblo capture by the KGB in 1968 also seems to reflect Andropov's interest in ciphers and US communications intelligence. (p. 345). The movements of the Pueblo were observed with the help of bar girls and tailors in Yokosuka, and KGB personnel from the Eighth Directorate were moved to the Far East in anticipation of a trap set for the US ship. When the ship was towed in, the KGB team was waiting in the harbor to remove all the equipment and documents for shipment to Moscow, The information taken from the Pueblo gave the Russians a five-year jump forward in their race against the US in cryptography and communications intelligence. (p.346.)

~~(C)~~ **This illustrated the great benefits that can result when the political leadership and the people at the top of the intelligence system can foresee the rich bounty that can come from well-planned "black activities" to augment SIGINT.**

(U) Soviet interest in the cryptography and communications intelligence of other nations has been of long interest. In 1928 the OGPU seized an opportunity to blackmail a disgruntled British Foreign Office cipher clerk who had offered to sell cipher information to their embassy in Paris. They swindled him, but then decided that he could be of further use. In order to locate the clerk in London, an agent deceived the British police into calling the Foreign Office and getting the man's name. (p. 149.) Once he was contacted, they used him to supply cipher information and also to recruit a co-worker in the Foreign Office cipher room. The British Foreign Office was told by an OGPU defector that there was a leak in their cipher room, but the Foreign Office pooh-poohed the notion. When the clerk became uncooperative in 1933 he died an apparent suicide. The co-worker continued to serve the OGPU (KGB) until 1940 when he was identified by an OGPU defector and subsequently imprisoned. The defector was killed in Washington a year later. Through this leak the KGB had advance knowledge of British action and intentions in India, Afghanistan, Persia, and Turkey.

DOCID: 4009965
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

~~(TSC)~~ KGB reaction to the penetration of their ciphers was much more vigorous than that of the Foreign Office. [redacted] After the British police forced their way into the building of the All Russian Cooperative Society in London in 1927 to get proof of Soviet espionage, Prime Minister Stanley Baldwin, a Socialist, stated in Parliament that the British Government had been reading Soviet diplomatic cipher traffic for years, and even read aloud a decrypted message, noting that a group was undecipherable. All this information was published in the parliamentary record, the Hansard. The Soviets immediately changed their diplomatic ciphers worldwide. In a talk at the US State Department in 1975 R.V. Jones said that from that time until 1946 when he left MI6, Soviet diplomatic ciphers were unreadable. (p. 440.) [redacted]

(U) In spite of improvements in Soviet ciphers, an NKVD cipher was read in the postwar era, one that exposed the Rosenberg spy ring. (p. 221.)

(U) The KGB was energetic at compromising and exploiting cipher room personnel of other countries, and took stern measures to keep their own clerks and cryptographers from being exposed to corresponding efforts by foreign intelligence services. Despite this, Igor Gouzenko was able to defect in Canada, taking messages and other materials. Subsequently the controls were tightened even further. (p. 225.)

(U) The KGB recruited low-level military people such as the American NCO Johnson and the British RAF NCO Prime, and maneuvered them into situations where they could supply cryptographic and COMINT information. (pp. 343 and 357.) Sgt. Dunlap at Ft. Meade photographed documents he was supposed to deliver as a messenger and passed them on to the Soviets. (p. 460.) Prime was infiltrated into GCHQ, whence he was able to pass on a variety of information.

[redacted]

(U) One of the outstanding attributes of the KGB is its persistence. It is tireless in going after its targets. The case officers are also good at handling the human element in running agents, combining pressure and rewards. Several appendices give copious details of incidents from the 1920-1950 period that show this combination of ruthlessness, ingenuity and tenacity. And to its own members the KGB is merciless. But in spite of its long sinister history, it is still considered a highly prestigious part of Soviet society, as its "sword and shield."

~~(S-CCO)~~ The authors' closing thesis is that the power in the USSR has shifted away from the Party and the Army, and the KGB will now operate Russia more efficiently than did the ageing and corrupt survivors of the Stalin era. The [redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

BULLETIN BOARD

DEMONSTRATIONS OF [redacted]

~~(C-CCO)~~ The Bookbreakers' Forum on Machine Aids is sponsoring demonstrations of NUTHATCH, a set of bookbreaking programs on the ASTW designed for plain or decrypted codes. The demonstrations are scheduled for the week of 13 January 1986, every day at 0930, in room 2C030. As only six persons can be accommodated at each session, reservations are required. Call [redacted] 963-3045.

PC NEWSLETTER

~~(FOUO)~~ A PC Newletter for G Group personnel is now being published by G331. It lists software for analysis and processing developed in G and elsewhere, and contains helpful hints for both novice and experienced users. For a subscription call [redacted] 963-4524.

FOREIGN-LANGUAGE VIDEOTAPES

~~(FOUO)~~ Videotapes of selected foreign TV programs can be obtained upon request. To inquire about the availability of tapes in your language, call [redacted] 16, 963-1103.

P.L. 86-36

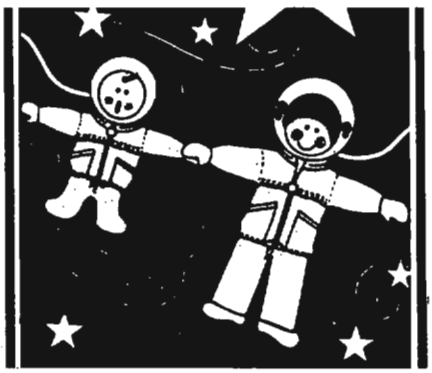
DOCID: 4009965

~~SECRET~~

ON THE LIGHTER SIDE

Vera R Filby, E42

There was a new hire named Larking
Who on his first course was embarking.
But he missed his car pool,
(U) So he drove to the School
And was last seen in Overflow Parking.



An NSA linguist named Rease
Could never quite manage with ease
Verb forms in Slovenian
(U) Or Czech or Ruthenian
And therefore he switched to Chinese.

A clever young cryppie named Sue
Had a message that [redacted]
She recovered the keys
~~(S-CCO)~~ With the greatest of ease
But she didn't know [redacted] Do you?

EO 1.4.(c)
P.L. 86-36

There was a reporter named Grotius
Whose grammar and style were atrocious.
But he learned how to spell
(U) And to punctuate as well,
And now he's considered precocious.

When I foolishly tried cryptanalysis
I was suddenly seized with paralysis,
Faced with grids, grills, and matrices,
(U) Vigeneres, generatrices ...
I fear I need psychoanalysis.

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

DOCID: 4009965

★★★THE ★ NEW ★ SECURITY ★ LAW★★★

★ *Evert Conder*

★ On 13 May 1950 President Truman signed a new bill designed to safeguard the security of cryptographic and communication intelligence information. Previously, there was only the Espionage Act of 1917: "An Act to punish acts of interference with the foreign relations, the neutrality, and the foreign commerce of the United States, to punish espionage, and better enforce the criminal laws of the United States, and for other purposes."

★ The new measure, Public Law No. 513, is entitled: "To enhance further the security of the United States by preventing disclosures of information concerning the cryptographic systems and the communication intelligence activities of the United States."

★ The safeguarding of this information has always presented a difficult problem. Even though years may pass, publication of techiques or past successes may be dangerous. There is no time limit when security limitations may be safely lifted.

★ The ideal, of course, is to develop your own techniques as far as possible, while trying to keep the other person as uninformed as possible. What he doen't know will not hurt you, while what he learns from you may do great harm. The more secure his lines of communication become, the more difficult your own work becomes.

★ It has always been difficult, even in time of war, for a court to secure a conviction against a civilian accused of disclosing vital military information. Adequate protection, of course, is available for the prosecution of military personnel and other persons subject to military control and the Articles of War. Civilians, however, until now could only be tried under the rather broad Espionage Act mentioned above. The weakness of the Act lies in the fact that (1) pre-meditated knowledge that a foreign government will receive the information, and (2) "intent or reason to believe that it would be used to the injury of the United States or to the advantage of a foreign nation" must be proved. Thus as long as "intent" could not be proved there was no way in which the Espionage Act could be invoked to punish civilians who disclosed military information to unauthorized persons.

★ This fact has been clearly demonstrated several times. In 1931 Herbert O. Yardley published a book entitled: "The Black Chamber" which disclosed certain information about the cryptographic activities of several foreign governments. Although great harm was done, Yardley apparently could not be held to account legally because of the inability of the government to prove "intent to injure." In defense of his actions Yardley maintained he had acted for the good of the country since he was attempting to show how insecure and inadequate our cryptosystems were at that time. A few years later, when Yardley attempted to publish a similar book, it was necessary for Congress to pass "A Bill for the protection of Government records" directed specifically towards gagging Yardley and preventing the publication of his manuscript.

★ Since the end of World War II there has been only one other case where the courts were successful in obtaining a conviction under the Espionage Law. This was the recent case of Judith Coplon. Even here the judge had to charge the jury to consider only two counts: (1) unlawful possession of government records, and (2) conspiracy to commit espionage. The other cases have been tried for perjury. One reason apparently for this is the government's reluctance to chance further disclosures of information which might occur in the court proceeding.★

Reprinted from the
ASA *Review*, Vol. 1. No. 4, July-August 1950

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009965

ETYMOLOGIST'S DELIGHT II

Match the borrowed word with the source language.

Edward D. Rockstein, P16, p16edr@bar1c05

"Un draille?"

The etymology of the word "draille" should perhaps be recorded before it has time to fall into obscurity. Before becoming "un draille" it was "un dry." And before that, it was "un dry Martini."

From *Madame Aubrey and the Police* by Hugh Travers

SOURCE LANGUAGES

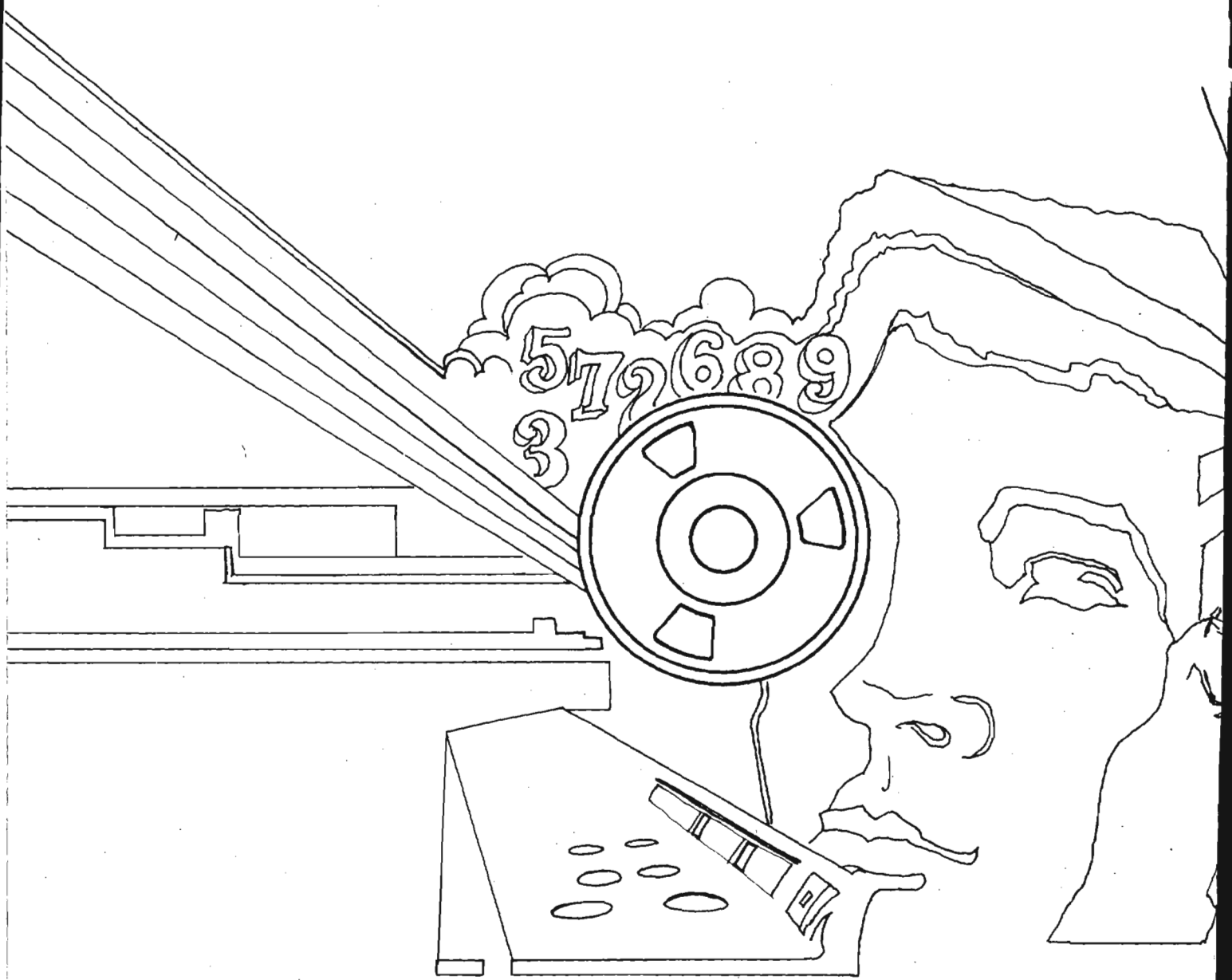
1. Algonquin
2. Arabic
3. Bantu [Sotho]
4. Basque
5. Breton
6. Celt
7. Czech
8. Dutch
9. Finnish
10. French
11. German
12. Greek
13. Gypsy (Romany)
14. Hindi
15. Japanese
16. Malay
17. Maori
18. Narragansett
19. Norwegian
20. Persian
21. Polish
22. Russian
23. Sanskrit
24. Spanish
25. Swedish
26. Tamil [Telugu]
27. Tibetan
28. Turkic
29. Turkish

WORDS

A. milo (a sorghum)
B. shampoo, bund (a quay)
C. massage, saffron, soda, mortise, lemon
D. go down
E. yoke, Juggernaut, jute, sugar
F. catty (a unit of weight)
G. terrapin, skunk, moose, squash, raccoon
H. tycoon
I. khan
J. yak, zebu
K. drub, casaba
L. menhir
M. jai-a-lai
N. sable, pogrom
O. pistol, howitzer
P. quahog (a clam)
Q. machete, ranch
R. vole, skull, tangle (seaweed)
S. cactus, licorice, skink
T. doodle
U. barnacle
V. pal
W. addle, mink
X. faucet
Y. azure, scimitar, caravan
Z. snorkel, dowel
AA. snook, selvage
BB. kiwi
CC. sauna

~~FOR OFFICIAL USE ONLY~~

P1-Jan 86-Y1-93609


5 7 9 6 8 9
3

DOCID: 4019704

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JUN-AUG 1985

P.L. 86-36

NSA'S INITIATIVE ON SECURE VOICE (U)..... [redacted] 1
TELEPHONE SECURITY, 1918 (U).....4
BULLETIN BOARD (U).....4
SHOPWORK (IV) (U)..... [redacted] 5
AN APPLICATION OF PINSETTER (U)..... [redacted] 7
VALEDICTORY OF A TRAFFIC ANALYST (U).....Joseph Starr.....9
BACK UP YOUR DATA FILES (U).....Norman P. Smith.....10
ESCHEW OBFUSCATORY SCRIVENERY, PLEASE (U)..... [redacted] 11
NSA-CROSTIC NO. 62 (U).....D.H.W.....12

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating~~ ~~quired~~

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019704

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XII, Nos. 6-8 ..... June-August 1985

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Collection ..... (963-5877)
Computer Security ..... (968-8141)
Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-4740)
Cryptolinguistics ..... (963-4704)
Index ..... (963-5330)
Information Science ..... (963-1145)
Intelligence Research ..... (963-3095)
Language ..... (963-5151)
Linguistics ..... (963-3896)
Mathematics ..... (963-5655)
Puzzles ..... David H. Williams (963-1103)
Science and Technology ..... (963-4423)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-3888)

Illustrator ..... (963-3057)
Distribution ..... (963-3369)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptolg at bar1c05
(bar-one-c-zero-five)
(note: no 'o' in 'log')

Always include your full name, organization, and secure phone number.

For Subscriptions or Change of Address
send name and organization to:
P14

P.L. 86-36

Contents of CRYPTOLOG should not be reproduced or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

P.L. 86-36

EDITORIAL

Analysts in NSA have an opportunity to share their views and experiences with others by writing for one of the several periodicals published in the Agency.

One of them is CRYPTOLOG. It is specifically intended for informal exchanges among analysts on subjects of interest to them. The editorial blue pencil is lightly applied, and only in the interest of clarity ... it's up to you to sustain the readers' interest and to put your ideas across persuasively.

For assistance, advice, or just plain aid and comfort, you may call on any of the editors; it need not be the one on your subject.

As for anonymity, we follow the standard etiquette of most publications: We will honor the author's request to remain anonymous, (we will even provide a nom de guerre for those who might want one) but the identity of the author must be made known to the Editor. Anonymous contributions (that is, lacking identification of the author) may as well be written in invisible ink ... we throw them out unread.

Another point of etiquette that authors must observe is about multiple submissions. If you send your article to more than one publication, you must so state.

Now for a few tips to ensure early consideration:

** The subject should be related in some way to our business. Unclassified term papers seldom fill the bill.*

** The article should be shorter rather than longer. A readers' survey showed that long articles are not read.*

** The text and illustrations should be of reproducible quality.*

** Every paragraph and illustration should be appropriately classified.*

** Hard copies of articles prepared on word processors should be accompanied by the mag card or floppy. (We send it to the Data Conversion Center where it is transformed to an 860 floppy, and then we convert that to an 8010 floppy.) Be sure to state what equipment and what software you used, and the operating system in the case of a pc.*

** If you submit a contribution via electronic mail, notify us by some other medium that you are doing so. (There's slippage every now and then.)*

** If you're going off on a field assignment or extended training or if you are retiring, designate someone who can act as your literary executor.*

** Label every submission with your full name, organization, and secure phone.*

~~FOR OFFICIAL USE ONLY~~

SECRET

NSA'S INITIATIVE ON SECURE VOICE (U)

P.L. 86-36

[redacted]

(U) The Soviet Union and other hostile governments can intercept and exploit, with ease and impunity, many U.S. telecommunications in the continental United States and around the world. Classified and sensitive communications over unsecured telephone systems alone represent such a lucrative and easy source of intelligence that NSA has undertaken a bold new approach to counter this threat.

(U) Each of NSA's past efforts to develop and distribute COMSEC equipments to the field has taken many years to complete. To reduce this time significantly NSA decided to tap the knowledge and resources of major commercial manufacturers of telecommunications equipment in a program called The Future Secure Voice System (FSVS) whereby NSA provides the cryptologic expertise and contractors provide technical, manufacturing, and marketing know-how. The goal is to design and produce a secure telephone the size of a conventional office deskset which will plug into a modular jack, cost less than $2,000, and be simple to operate.

EO 1.4.(c)
P.L. 86-36

EXTENT OF THE THREAT

(S-CCO) Unsecured telephone conversations can be easily exploited by hostile intelligence-gathering activities to reveal governmental, military, and industrial secrets and technology. That is because communications over commercial telephone systems, especially long distance, are likely to be transmitted via microwave or satellite which are particularly easy to intercept; all it takes is equipment costing about $25,000, small enough to fill the back of a station wagon.

[redacted]

(S) Moreover, mission-essential, classified information is sometimes discussed over unsecure telephones simply because secure communications are unavailable. Unclassified but sensitive technological data also pass over the telephone system daily. As a recent National COMSEC Committee Biennial Report points out, "the industrial base which produces the nation's most advanced military hardware and develops its most sensitive technology is almost completely without a secure communications capability. Critical secrets are lost before the sensitive systems and technologies they represent can be fielded by military or other government users."

(U) The unsecured telephone has been determined to be the most lucrative source of classified and sensitive information available to unauthorized recipients. To counter this vulnerability, President Reagan recently signed National Security Decision Directive (NSDD) 145, which directs that all U.S. Government systems carrying classified information be secured, including telephone.

(U) NSDD-145 requires that NSA, as the new National Manager for Telecommunications Systems Security, provide a secure communications capability for as many as 500,000 users beginning in 1987. The FSVS program has been conceived to help implement this directive.

PRESENT SECURE TELEPHONE SERVICE

(C) The only DoD-wide, secure telephone system available today is AUTOSEVOCOM, which serves about 2,500 locations around the world. This system, however, secures only a small fraction of the total telephone conversations of the DoD, and much of the equipment is outdated and provides poor voice quality. Under the recently implemented AUTOSEVOCOM Life Cycle Extension Program (ALCEP), older HY-2/KG-13 equipment is being replaced by newer VINSON devices, which will update the system and improve voice quality. The total AUTOSEVOCOM community will, however, remain small.

(C) NSA's Secure Telephone Units (STU-II and STU-IIM) are also being procured by military departments and the civil sector. Over the next five years the total number of STU-II and STU-IIM units should reach approximately 14,000 units, which is only a small portion of the half-million or so of the secure telephones needed. Because of their relatively high cost ($12-25,000) and their dependence on the Bellfield Key Distribution Centers (KDCs) each of which can service only a limited number of subscribers, these units cannot be distributed to the field in large

HANDLE VIA COMINT CHANNELS ONLY
SECRET

quantities. KDCs act as centralized points for electronically distributing key, a function necessary in communications security.

STU-III FAMILY OF TERMINALS

(U) With a half million or more potential customers to satisfy, NSA realized there will be a variety of user requirements. A family of telephone terminals rather than a single type will therefore be developed to satisfy the diversity. This family of equipments has been designated STU-III or Low Cost Terminal (LCT).

(U) Military planners have stated a requirement for the STU-III to interoperate directly with existing STU-II units. This is being satisfied with the STU-III Command & Control (C^2) version, designated KY-77. The C^2 terminal will meet environmental requirements for mobile radio telephones and is planned for limited military and civilian government applications. It will be slightly more expensive than the other members of the STU-III family, and is being developed by RCA on a separate contract. The KY-77 should be available early in 1987.

(U) Of the non-military users of STU-III, some handle classified information and others handle unclassified but national security-related information. Classified user requirements will be satisfied by a Type I LCT, while unclassified users will be limited to Type II terminals. An example of a Type I application is the securing of conversations between NSA and contractors working on classified NSA projects. Typical Type II applications include the protection of proprietary information such as financial, organizational, marketing, and technical data.

(U) Another version of the LCT being conceived is a cellular radio telephone model. This unit, compatible with other LCTs and regular, unsecured telephones will satisfy secure mobile requirements.

(U) Members of the STU-III family will look and act much like conventional telephone desksets. In fact, an LCT will interoperate easily with a regular telephone for unsecured communications. Secure operations between STU-IIIs will require only a few extra steps by the users. The terminals themselves will include modern telephone features like repertory dialing, and will offer a light-emitting diode (LED) or liquid crystal display (LCD). The display will indicate the identity and security clearance level of the distant end terminal, and will help guide users through STU-III operating procedures.

PROGRAM STRATEGY

(U) In the Spring of 1984 NSA asked five major telecommunications contractors (AT&T, ITT, GTE, RCA, and Motorola) to define a concept for the STU-III/LCT and the attendant system necessary to key and support it. This concept definition phase lasted six months.

(U) NSA's program strategy was to select three of the vendors to produce telephones, and one contractor to develpp a system responsible for such things as key management. The selection process is now complete, and the system contract has been awarded to GTE, while AT&T, RCA, and Motorola have been contracted to produce the phones. This parallel acquisition strategy is necessary to achieve NSA's goal of initial delivery in early 1987.

COMSEC DOCTRINE

(U) Physical handling requirements for such a large quantity of COMSEC devices are a major concern. COMSEC doctrine is being rethought in order to lessen constraints and make COMSEC more desirable to the user community. Older security doctrine dictated the handling of cryptographic equipment according to equipment type. STU-III equipment, however, will be governed by new doctrine, which bases the amount of required protection on the specific application of the device. For instance, a STU-III located within the NSA compound will require less stringent control than a unit housed overseas, where foreign nationals may have easy access to it.

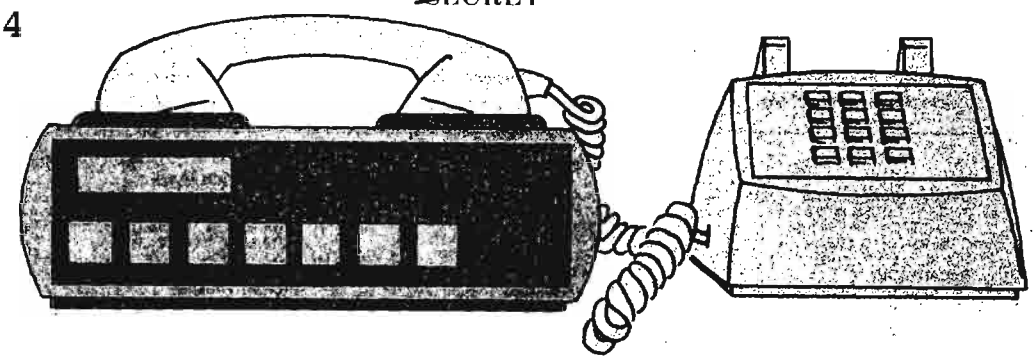
(U) In December, 1984, NSA commissioned A.D. Little Company to complete a market survey to determine the size of the potential market for STU-IIIs and to establish a priority list of user preferences and demands. According to the company's preliminary report, the number one requirement expressed by potential users in both Government and industry is that the units be unclassified when unattended. This condition presents a problem, however, since these terminals are to be high-grade cryptographic devices which normally require special handling. A device called a crypto-ignition key (CIK) will therefore be implemented to help solve that problem.

(U) The security of U.S. COMSEC equipment depends on protecting the key which is instrumental in determining the pattern of ones and zeros, called the key stream, produced by a key generator or cryptologic. The CIK is a removable device, small enough to fit in a shirt pocket, that contains a portion of the key; the other portion resides in the STU-III. A keyed STU-III is therefore sanitized by unplugging and removing the CIK, and the sanitized phone becomes unclassified and can be left unattended. Controls on the CIK will depend on specific applications, but in some cases simply locking the device in a desk drawer or taking it home will be sufficient.

(S) Because STU-IIIs will be widely distributed, it must be assumed that U.S. adversaries will obtain some of the units and attempt reverse engineering in order to recover the cryptologic. To counter this potential threat, NSA has decided on a special chip coating as a way of preventing the reverse engineering of cryptographic chips within the terminals. NSA engineers are confident that this protection will effectively thwart the recovery of information from the circuitry or memory of the chip sets.

KEYING SCHEME

(U) A major effort is required to provide keying material to COMSEC equipment in the field. In most cases, NSA produces the key in some hard copy form like key tape, key card, or key list, and then distributes the key among many users. Some newer equipments, like the STU-II, employ remote keying which reduces NSA's burden significantly. These remote keying schemes, however, generally depend on a KDC or other central point to distribute key electronically to remote users. There are, however, physical limitations on the number of users the KDCs



can support. Therefore, if a half million or more LCTs must be supported, a new keying method is necessary.

~~(C)~~ The new method is called FIREFLY II. This is a breakthrough in key distribution technology in that it will eliminate the need for a KDC by allowing each STU-III to generate and securely exchange key with other STU-IIIs. The calling and receiving terminals themselves generate random components which are then securely exchanged, combined, and used by both terminals on a session or per-call basis. Session keys enhance the security of the system by eliminating back-traffic vulnerability, and the entire process of generating and exchanging random components takes less than 12 seconds.

~~(C)~~ Added benefits of FIREFLY II include positive authentication of distant end terminals, and very long cryptoperiods. (A cryptoperiod is the length of time a particular key may be used before it is replaced.) Although each STU-III generates and exchanges key each time it is used securely, there are also keys which reside within each terminal which must be replaced periodically, every one to three years. This replacement will be as simple as placing a call to a key management center, and receiving new key securely over the telephone line.

APPLICATIONS OF THE STU-IIIs

~~(C)~~ NSA's Deputy Director for Telecommunications has expressed support for the eventual replacement of some NSA black telephones with STU-IIIs. The FSVS initiative, in fact, seeks to install 500,000 secure phones in the Department of Defense, Civil Government sectors, and defense contractors. That number grows considerably when other potential LCT customers are included. Financial institutions, academics doing Government research, and any company performing high-tech research and development that could be transferred to an enemy's military or security systems must be considered prime LCT candidates.

(U) Only a preliminary report of A.D. Little's market survey has been completed to date, but NSA believes that private sector interest in an inexpensive, secure telephone could eventually increase the market to 1.1 million. Independent market surveys performed by some of the bidding contractors indicate an even larger potential market. An RCA-financed study established the market size as over 1.6 million, while other contractor studies indicate a potential private sector market demand by 1990 as high as 2.6 million. The higher numbers reflect the private sector's interest in acquiring secure telephones to protect against loss of proprietary information.

(U) NSA will permit direct, controlled sales of LCTs by the contractors to authorized purchasers. This will allow the vendors to have a direct effect on the size of their market. Clearly, LCT vendors could benefit dramatically from the production, marketing and sale of secure phones. Even if NSA's initial estimate of 500,000 units is inaccurate by 50%, it still means a market of 250,000 phones priced at around $2,000 each, for an estimated total market of $500 million over the next five years. If the private sector market pans out and over a million units are sold, LCT vendors stand to profit handsomely.

(U) Parallel production by three vendors should increase the number of units produced, which will in turn bring down unit cost. The benefits of low cost and high quantity to NSA's COMSEC effort is that many telephone conversations containing classified or sensitive data will be secured, and unaccessible to Soviet and other hostile intelligence activities.

SUMMARY

(U) The huge amount of classified and sensitive information the U.S. is giving away through unsecured telephone communications must be stopped and stopped soon. Older methods of developing and implementing COMSEC are too time-consuming to be effective quickly enough. NSA's FSVS program has therefore been established as a new approach to meeting this COMSEC challenge.

(U) The STU-III family of secure telephone equipment is now in contract, with initial distribution to the field planned for April, 1987. It will provide advantages in size, acquisition and life cycle cost, security and performance over current secure voice equipment, and meet a broad variety of needs.

(U) Various STU-III models will provide compatibility with conventional office telephone systems, military strategic command and control requirements, and conventional and cellular mobile radio telephone systems. Most significant is the very scale of the program, with quantities ultimately expected to exceed half a million units.

(U) All aspects of NSA's Future Secure Voice initiative add up to an strong program to protect the voice communications of the U.S. If this effort is successful, and the contractors and NSA believe it will be, we can truly button up U.S. voice communications by the end of this decade, and, at the same time, deal the Soviets a severe blow. □

P.L. 86-36

TELEPHONE SECURITY, 1918

Extract from Confidential orders to 1st Lt. (Chaplain) John McDowell Alexander Lacy, October 12, 1918.

1. Having reported at this office, this date, for transportation in compliance with order Headquarters, Port of Embarkation, Hoboken N.J. or from Navy Department, you will report at Officer's Gangway, Vessel No ..*56*.. Pier No ..*59*.. North River, Foot of West ..*18th*.. Street, New York City, at ..*4*.. ~~A.M.~~ P.M. ..*Oct 16*..1918.

3. You are directed not to visit pier to which you have been assigned before date of embarkation except for the purpose of delivering your baggage. You will then go only to the Baggage Room, and under no circumstances wander about piers or go near vessel.

8. No information will be given by telephone.

9. THIS INFORMATION IS STRICTLY CONFIDENTIAL.

Courtesy of [redacted] *S052, grandson of Chaplain Lacy*

BULLETIN BOARD

FOR DATA BASE ADMINISTRATORS

~~(FOUO)~~ The Computer Record Format (CRF). form H3173C, has been revised. It is now on the new standard paper size, 8½x11, to be consistent with the Computer Services Work Request form, H3173, which it accompanies. The CRF is a vehicle for documenting files; it is the official repository for information about the individual file(s) and record formats, subordinated to a particular file or data base, which are going to reside on T-controlled resources, such as CARILLON, CARONA, HOLDER, METEOR, PLATFORM, WINDMILL.

~~(FOUO)~~ The National Data Standards Center, P13D, recommends that data base administrators use this form to document all files created under their cognizance, including those entered experimentally or provisionally on micros or terminal subsystems. Then, when the programmer is sud-denly transferred, you'll have some idea about what those strange files are. The failure to document small, private files which go on to become big, shared files is becoming a serious problem in the Agency.

(U) The new forms should be available in Supply by the time you read this.

DO YOU WRITE AND EDIT IN YOUR JOB?

(U) If you do a significant amount of writing and/or editing in your job and do not hold a COSC as an editor/writer, please make yourself known to [redacted] T54, SAB 2, Door 3, 972-2355s

CALL FOR CA TERMS

~~(C)~~ The SIGINT Terminology Group is compiling an on-line database of cryptanalysis terms and definitions. Initial input has been drawn from the following sources: *Military Cryptanalytics II*, Lambros D. Callimahos, October 1959; *Basic Cryptologic Glossary*, P1, 1971; *NSA Technical Journal*; *CRYPTOLOG*; [redacted] Suggestions for additional sources are solicited. Please forward your submissions to [redacted] P13D, 968-8162s.

~~(FOUO)~~ The database now contains about 1600 terms and definitions. When the total reaches 2,000-2,500, it will be reviewed by a panel of experts appointed by the chiefs of key components.

SUGGEST-A-BOOK

(U) The NSA Library is soliciting suggestions for books and periodicals to be purchased for the Library. For each book, provide the following information and send it to T51: Author, Title, ISBN, Price, Publisher, Source of Information, and your name, organization and telephone number. It would be helpful if you also include a review of the book or an ad for it.

GLOSSARY OF MACHINE TERMS

~~(FOUO)~~ Contributions are solicited for the Supplementary Working Aid for Machine Terminology (SWAMT) for the updated edition planned to be published early in 1986, the first since 1981. SWAPT is an informal glossary rather than a standard one, so the less formal style allows for the frequent updates which such a rapidly changing technology demands. The next edition will be printed in both upper and lower case, as it is now being processed on an IBM PC to be printed on a laser printer.

~~(FOUO)~~ Contributions, suggestions and comments may be sent to [redacted] P13D, FANX III, or you may call her on 968-8162s.

FOR PINSETTER USERS ON THE XT OR ASTW

~~(FOUO)~~ A new PINSETTER applications manual, *How to get Started with the IBM PC/XT or ASTW* is now available at the PCIC and P14. It provides helpful hints to new users of the PC/XT or ASTW, whether experienced or not in using the TSS/UNIX version of PINSETTER.

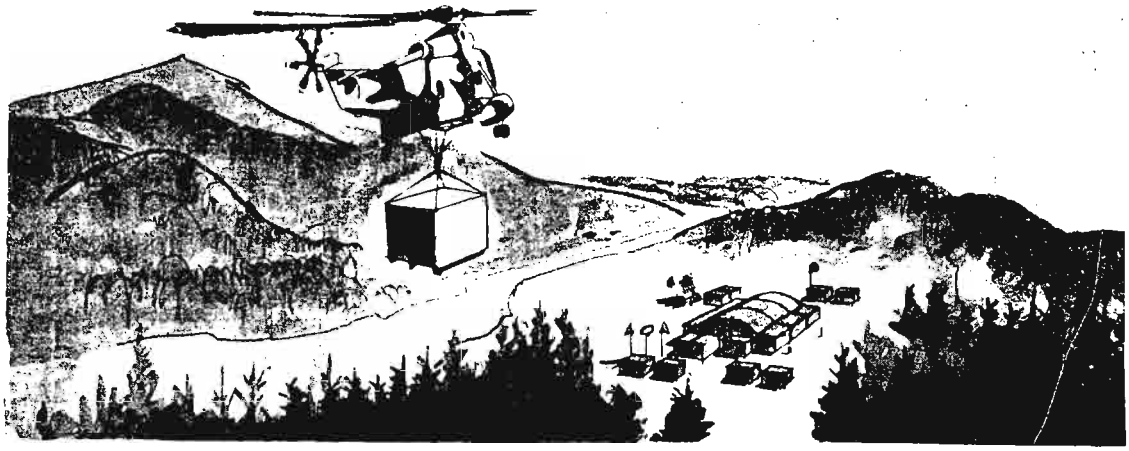
~~(FOUO)~~ For further information or assistance, call [redacted].□

DOCID: 4019704

SHOPWORK IV (U)

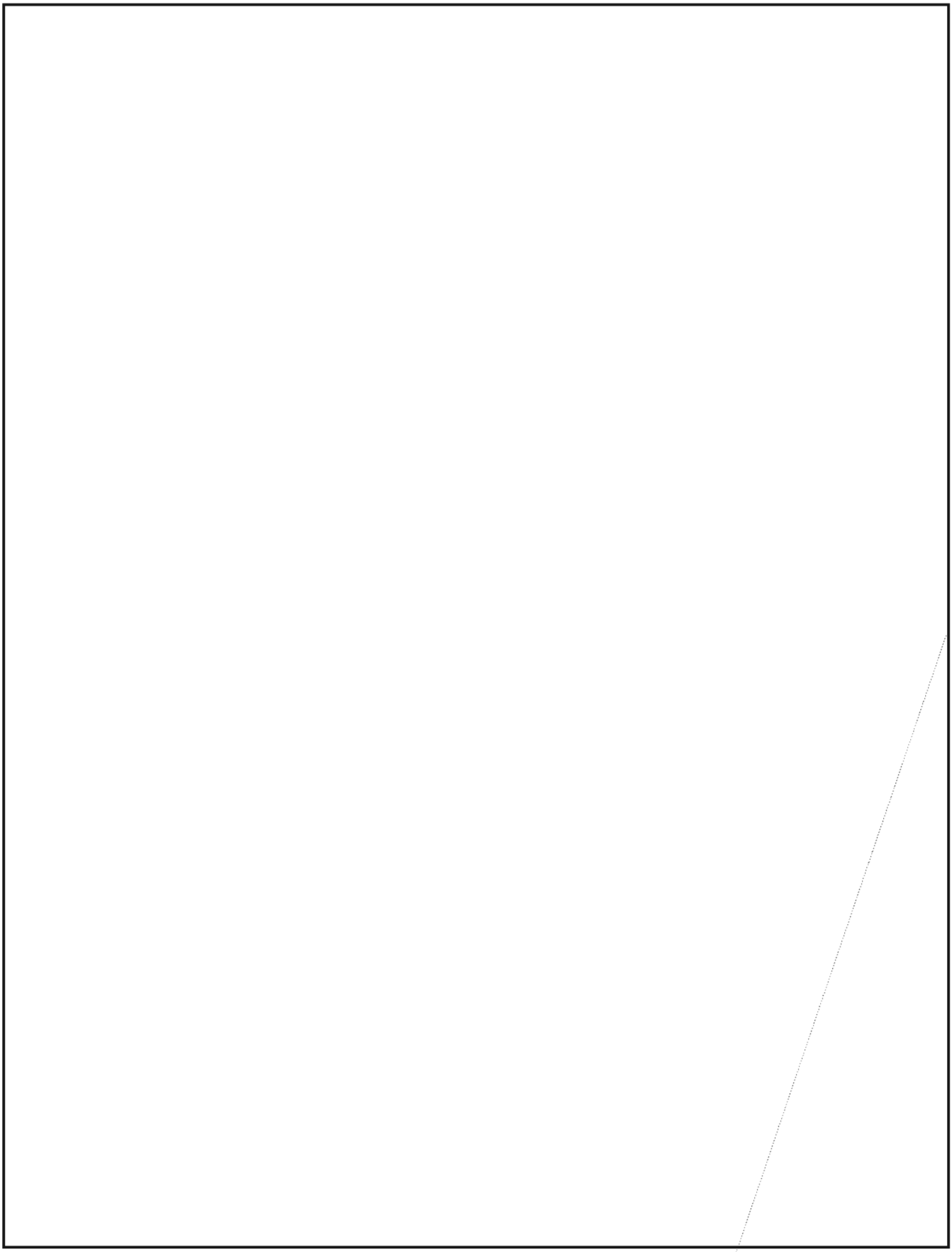
[redacted] *USA, JOCCP*

P.L. 86-36



[redacted]

P.L. 86-36
EO 1.4.(c)



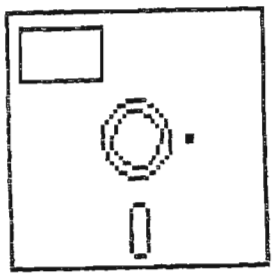
P.L. 86-36
EO 1.4.(c)

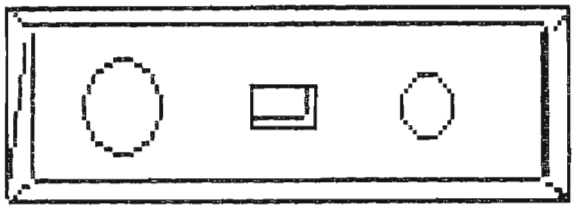
DOCID: 4019704

AN APPLICATION OF PINSETTER (U)

[redacted]

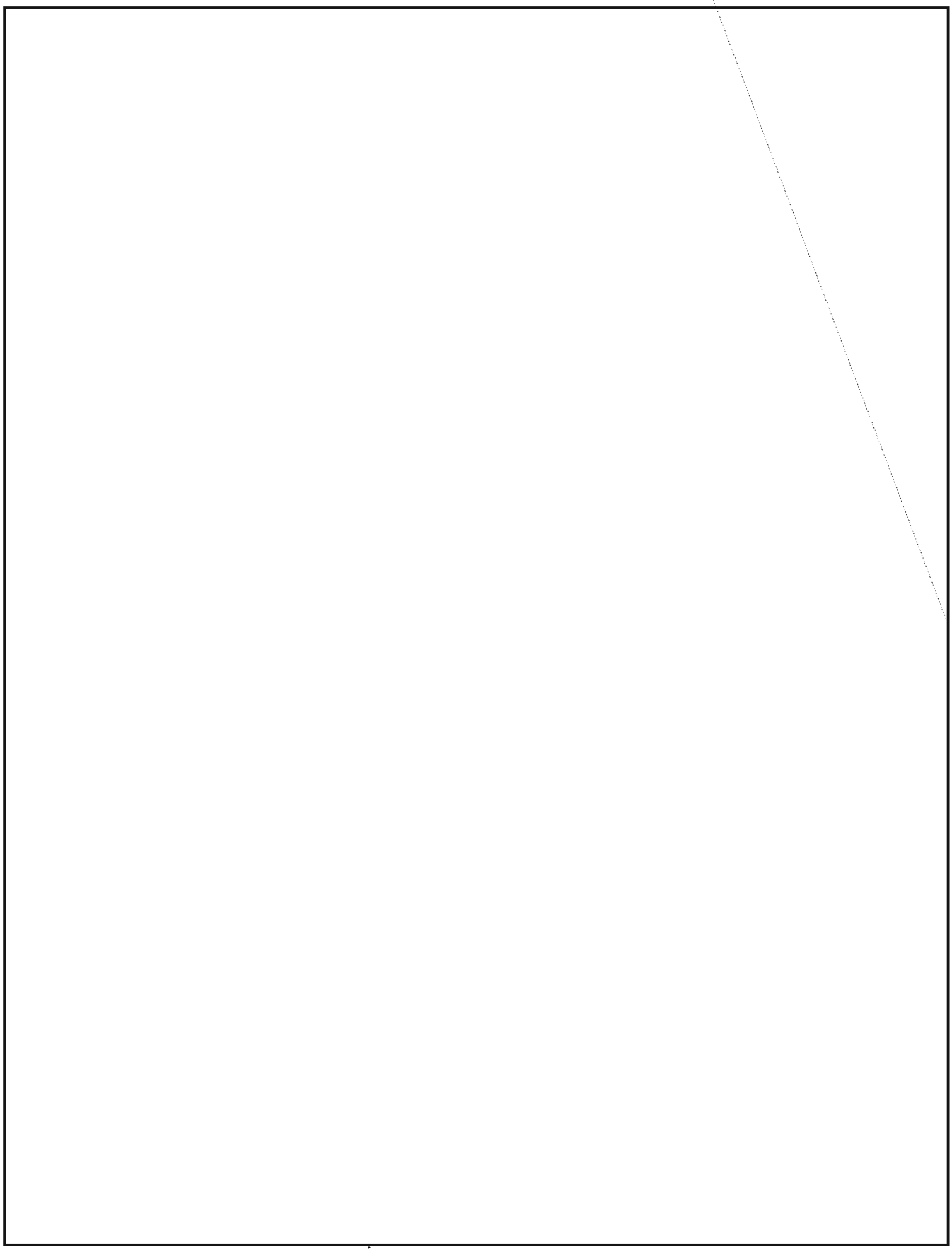
P.L. 86-36





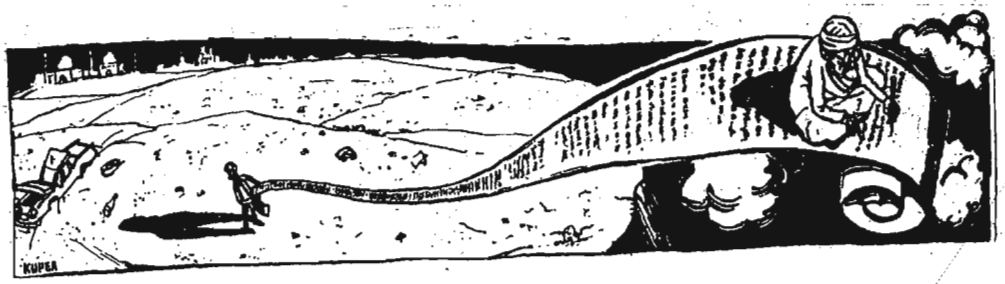
[redacted]

P.L. 86-36
EO 1.4.(c)



DOCID: 4019704

VALEDICTORY OF A TRAFFIC ANALYST (U)



[redacted] Ret.

(U) On August 1, 1985 I retired from the National Security Agency after almost 40 years of cryptologic work which included at one time or another most of the things NSA does in the fields of collection, analysis, and SIGINT reporting. I enjoyed every minute of it. I honestly don't believe I could have chosen a more enjoyable or rewarding career. If I had been born rich, Iwould have done traffic analysis for nothing; if I had been independently wealthy, I would have paid the Agency to let me do it. Hang with me for a few minutes of serious discussion about machine processing problems, and I'll share with you a few observations, comments, and recommendations that may contribute to your enjoyment of the profession and perhaps help you to avoid some of the pitfalls that beset the paths I wandered in.

(U) The most important question confronting the profession today is why, from a traffic analyst's viewpoint, data processing systems have not yet produced the Utopia we were led (or stampeded) to expect back in the early 1960's.

(U) In the January-March 1980 CRYPTOLOG, [redacted] correctly sorts working analysts into three categories: loggers, case analysts, and research analysts. He then predicts that automated processing techniques will permit us to eliminate the loggers, and assesses that the research analyst is the one with the bright future because he is concerned with the "why of analysis ... driven by his desire to explain." But every analyst should be saying why, and George's prediction that the logger will become obsolete just hasn't happened, although it should have. Indeed, we now have a new generation of loggers who have even less understanding of traffic analysis than those who preceded them.

(U) After George discusses how analysts are going to have to adapt in order to be productive in a modern (machine oriented) world, he puts his finger squarely on the major problems area, "manageable machine systems that will function as designed." And he goes on to point out,"... our track record for the development of such systems is not impressive."

(U) In the December 1981 CRYPTOLOG [redacted] published an article on machine processing that everyone who claims to be a traffic analyst should have read. Part of what Dale addressed was the problem with keeping competent programmers on the job, and how the traffic analyst could be freed from total dependence on the programmer.

(U) Traffic analysis is basically a very simple art if you are able to keep your mind loose so that you can recognize and exploit whatever the target gives you to work with. This is a fairly easy exercise intellectually, but it is much more difficult to structure your thought processes in order to design a machine processing system that will give you essentially the same versatility. Unfortunately, we have some managers and analysts who have produced processing systems and tried to make the target fit the processing scheme, and I include in this category most of those procedures which were designed to replace a hand log kept by the analysts with a similar log prepared by the machine. The results were predictable. What we have now are logs prepared by machine that in many instances are inferior to those the analyst prepared by hand. And, without the benefit that accrued from working the traffic by hand, today's analyst has even less understanding of the data and may in fact be at a total loss to explain observed anomalies.

~~(C)~~ We can reverse this trend. We need to build on the good decisions we have made with regard to automating data processing for traffic analysis, and we must be willing to discard the bad decisions. What we really need to do now is to get on with developing an expert system that will process automatically all incoming traffic, compare what is observed to a dictionary of stated norms, and send appropriate alert messages to analysts and reporters on trouble spots.

[redacted]

(U) None of this should be difficult. Building and testing dictionaries will be tedious but in the process of doing this, the analyst will be compelled to learn a great deal more about his cases than he now knows, and supervisors will be compelled to work with analysts to a much greater extent than is taking place now. When an expert type system is in place and functional, one of the benefits will be that time will become available for a different and much more meaningful kind of on-the-job training.

~~(S-CCO)~~ We began exploring how to develop an expert system for processing [redacted] just before I retired. I expect initial development to be slow, painful, and frustrating but I do expect the system to "function as designed." What we must have to make it work is a sufficiently confident estimate of our analytic judgments and capabilities to tell the machine

 EO 1.4.(c)
P.L. 86-36
~~HANDLE VIA COMINT CHANNELS ONLY~~ P.L. 86-36
~~SECRET~~

DOCID: 4019704

how to do all the dog work for us and then let it do the job. There can be no doubt as to our ability to make the right technical and reporting decisions based on the alert messages because each analyst must understand his responsibilities well enough to have described his case, net, and network norms to his analytic dictionaries.

(U) We will see vastly improved data bases as a side benefit of this kind of processing. If the input data aren't good, the expert system is going to make noise; it will not permit any analyst to do a poor job on editing input data without sounding off.

(U) I am not persuaded that an expert system can be developed and implemented by evolution; probably the best (and certainly the quickest) way to effect such radical changes in the way traffic analysis is accomplished would be to select the right analysts and programmers, charge them with developing an expert system to do traffic analysis on a specific target, and set a deadline of perhaps a year hence for the initial job to be finished. There should be no restrictions as to how the task is to be accomplished, and there should be no arbitrary limitations as to the techniques to be used (e.g. storage of norms for ordinary comparisons should not be made excessively difficult by the intricacies of an existing data base).

(U) There is no question that the agency will deve-lop an expert system at some point in the future; if not for normal traffic analytic functions, then to provide rapid data evaluations for tactical support of military forces. I regret that I will not be here to see it.

(U) Here is the advice I promised earlier.

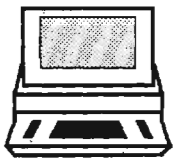
(U) Learn to be persuasive as well as informative in any presentation you make. The best ideas you have aren't worth much if you can't sell them. You cannot depend on decision makers to steer the right course because it is (or appears to you to be) the logical thing to do.

~~(FOUO)~~ Reporting the results of your analysis is part of your job. Learn what the intelligence requirements are for the target you are assigned and relate them directly and specifically to how you work your traffic. If you don't understand what it is that you are supposed to be getting out of the traffic and don't try to find out, you are still a logger and that's all you're ever going to be.

(U) Avoid meetings. I am convinced that many people at the Agency really and truly believe that they are making progress as long as they are talking with each other regardless of whether or not anything is actually being done. I have attended some meetings where the only concrete thing accomplished was an agreement to meet again at some specified date in the future to discuss the same subject. And so help me, they all left happy.

(U) Don't take sinful pride in your own words. If the staff officer who reviews your message or report wants to change your words for his, don't be offended. Staff officers do serve a useful function. If you have treated them with respect in the past, they will often help you get out of trouble.

(U) I finished this article just as my NSA career came to an end. Reading it over, I find a line or two that may be mildly objectionable to one person or another. It was not my intention to offend anyone by my choice of words or by my comments, and if I have given offense, I apologize. This doesn't sound like me but it does sound nice and I think I'll leave it right there. Goodbye, good luck, God bless you all. □



BACK UP YOUR DATA FILES (U)

Norman P. Smith, H215

Enough cannot be said about the importance of local backup of data files, especially data being stored in micros. The first thing new users should learn when they receive their own ASTW, PC, or other micro, is how to backup all files and the operating system. The command below will allow all ASTW-PC/IX users to backup their own directories:

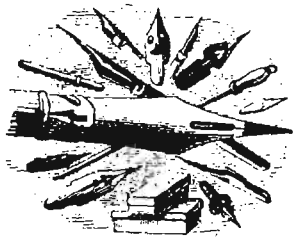
find <pathname> -print _ /priv/dump -i -v

where pathname is the complete pathway to the directory being backed up (i.e., /usr/npsmith). Users of TSS and other systems depend upon their systems administrator and the operating systems themselves. Backup copies should probably be made at least every 12 hours, if not every 6 hours, and held for 24 to 48 hours. The rule of thumb for backing up data is to back up your data for the span of time you find acceptable to spend re-creating your work.

Another method to accomplish this on the ASTW is to work directly from floppy disks, where each floppy contains an entire working directory. You then use the MOUNT and UNMOUNT commands to bring up and take down access to the floppy These commands are covered in the ASTW Users' Guide. □

DOCID: 4019704

ESCHEW OBFUSCATORY SCRIVENERY, PLEASE (u)



P.L. 86-36

This article is classified ~~SECRET SPOKE~~ in its entirety.

Many operators frequently use the TR NOTE during transcription to elaborate on the traffic, yet few stop to realize just why and for whom they are making the additional entries. When properly employed, the comments contained in the TR NOTE can be of great assistance to those who ultimately read the transcripts, giving them useful information and insights. When abused or misapplied, the TR NOTE adds little of any worth, wastes the transcriber's (and the reader's) time and can be potentially embarrassing for the unit as well as for the U.S. intelligence effort as a whole.

Such notes are brief, informative, professionally executed, and to the point. They add insight, correct mistakes, present information not reflected in the words themselves, and save leg-work for the reader. Contrast them with the following:

Notes such as the latter are most often rendered on mids on the last page of lengthy transcripts of poor readability. They are personal expressions of frustration and exasperation, and do little more than trivialize your work and detract from its overall impact. Please avoid the temptation to indulge. □

P.L. 86-36
EO 1.4.(c)

Reprinted, with permission, from the Summer 1985 issue of VOX TOPICS.

DOCID: 4019704

NSA-Crostic No. 62

A. Put away the swords, Heather said

209 219 86 62 189 191 215

B. Ornithogalum thyrsoides (2 wds)

92 76 113 146 155 79 163 88 119 132 24 60 199

143 250 54 4 106 12 176 239

C. Surrey town located above U.S. Marine

142 33 158 130 240 228 145 248 29 9 180

D. Twins age fast at new museum (2 wds)

84 178 202 169 95 127 100 56

E. "And so he mediates, twice near
The tides that wash on old Algier"
(2 wds)

111 14 94 105 247 123 152 131 173 148 201 52 245

226 23 237

F. Head of Metro and DDE visit Douglas

230 154 227 253

G. Get Helen Kennedy.

184 135 89 112 235

H. "Does it hurt?" "___ I laugh." (2 wds)

164 6 91 63 186 223 107 128

I. Hilaire Belloc hero usually has
yellowish hue

26 97 2 224 21 68 65 182

J. Twenty-four hours ago he was a
steady rye drinker

232 77 238 210 137 7 25 241 73

K. Wrapped in the wads of bandage

222 214 225 190 136 171 149

L. Not on hand

37 109 144 67 87 117 213

M. It's the wonderful lather we feel
leads to such a state of perfection
(comp)

20 151 66 121 140 98 203 236 194 254 217 138

N. "Bonnie ———" (2 wds)

133 30 22 17 118 167 251 61 208 177 160 75 81

O. Wearily I left to see my solicitor

104 19 47 166 3 34

P. Disregard

69 179 170 200 206 168

Q. Double checker of a tergiversation

159 147 114 45 42 162 70 141 96 78 244 53 211

15

R. Restive; not asleep (var.)

188 1 231 183 50 27 10 57

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019704

S. Worse than a vile sea monster

T. Indian town for two idiots

U. Large ice sheet in Antarctica (var.) (2 wds)

V. To make the stout weed tender, he boiled it longer than anyone else

W. I betrayed him when I saw him swipe a cheddar cheese

X. Smelly seat in church?

Y. Remark directed at Dr. I.Q. (8 wds)

Z. The salamander went home

Z_1. Develop a large state in the mind

212 71 80 41 116 153 83 110 55

229 156 72 46 125 85

49 5 129 122 103 31 187 243 216 40

64 58 174 204 218 197 32 48 101

234 192 99 124 205 195 18

150 39 35 207

233 28 102 242 43 181 172 90 185 161 139 59 82

252 220 36 16 157 198 246 93 193 8 108 115

126 165 196

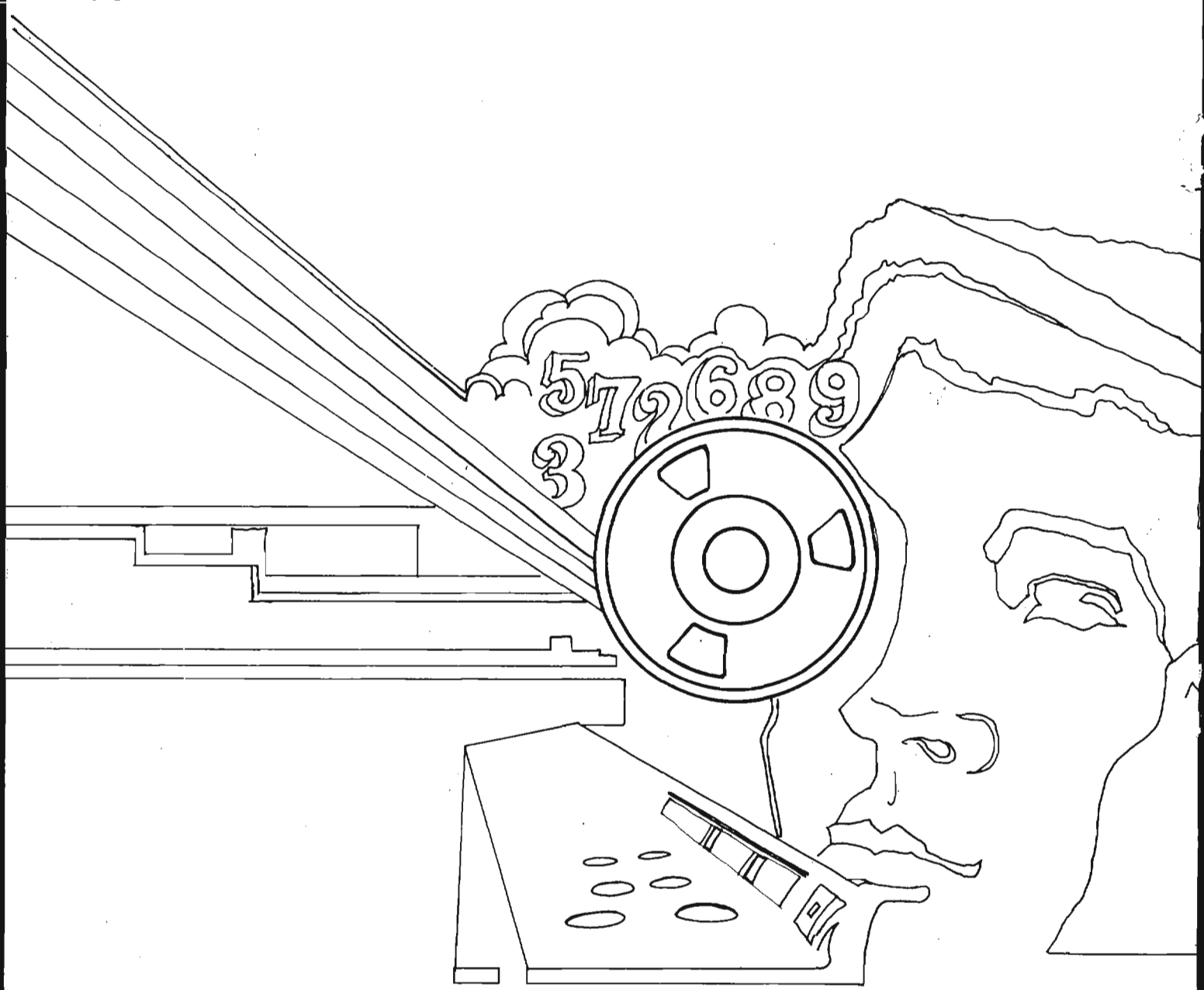
221 120 74 38

11 51 134 13 44 175 249

1 R	2 I	3 O	4 B	■	5 U	6 H	7 J	■	8 Y	9 C	10 R	11 Z_1	12 B	13 Z_1	14 E
15 Q	■	16 Y	17 N	18 W	■	19 O	■	20 M	21 I	22 N	23 E	24 B	25 J	■	26 I
27 R	■	28 Y	29 C	30 N	31 U	■	32 V	33 C	34 O	35 X	■	36 Y	37 L	38 T	39 X
■	40 U	41 S	42 Q	43 Y	■	44 Z_1	45 Q	46 T	■	47 O	48 V	49 U	50 R	■	51 Z_1
52 E	53 Q	54 B	55 S	56 D	■	57 R	58 V	59 Y	60 B	61 N	■	62 A	63 H	■	64 V
65 I	66 M	■	67 L	68 I	69 P	70 Q	71 S	■	72 T	73 J	■	74 Z	75 N	76 B	77 J
■	78 Q	79 B	80 S	81 N	■	82 Y	83 S	84 D	85 T	■	86 A	87 L	88 B	89 G	■
90 Y	■	91 H	92 B	93 Y	94 E	95 D	96 Q	97 I	98 M	■	99 W	100 D	101 V	■	102 Y
■	103 U	104 O	105 E	106 B	107 H	■	108 Y	109 L	■	110 S	111 E	112 G	113 B	114 Q	115 Y
116 S	117 L	■	118 N	119 B	120 Z	121 M	122 U	123 E	■	124 W	125 T	126 Y	■	127 D	128 H
■	129 U	130 C	131 E	132 B	133 N	134 Z_1	■	135 G	136 K	137 J	■	138 M	139 Y	140 M	141 Q
142 C	143 B	■	144 L	145 C	146 B	147 Q	148 E	149 K	■	150 X	151 M	152 E	153 S	154 F	155 B
156 T	157 Y	158 C	159 Q	160 N	161 Y	■	162 Q	163 B	164 H	165 Y	166 O	167 N	168 P	■	169 T
170 P	171 K	■	172 Y	173 E	174 V	175 Z_1	176 B	177 N	■	178 D	179 P	180 C	■	181 Y	182 I
183 R	184 G	185 Y	■	186 H	187 U	188 R	189 A	■	190 K	191 A	192 W	193 Y	■	194 M	195 W
196 Y	197 V	■	198 Y	199 B	200 P	201 E	202 D	203 M	■	204 V	205 W	206 P	■	207 X	208 N
209 A	■	210 J	211 Q	212 S	213 L	■	214 K	215 A	216 U	217 M	■	218 V	219 A	220 Y	221 Z_1
■	222 K	223 H	224 I	■	225 F	226 E	227 F	228 C	229 T	■	230 F	231 R	232 J	■	233 Y
■	234 W	235 G	236 M	237 E	238 J	239 B	■	240 C	241 J	242 Y	243 U	■	244 Q	245 E	246 Y
247 E	248 C	249 Z_1	250 B	■	251 N	252 Y	253 F	254 M	■						D.H.W

P1-Nov 85-Y1-87742

~~FOR OFFICIAL USE ONLY~~


5 7 9 6 8 9
3

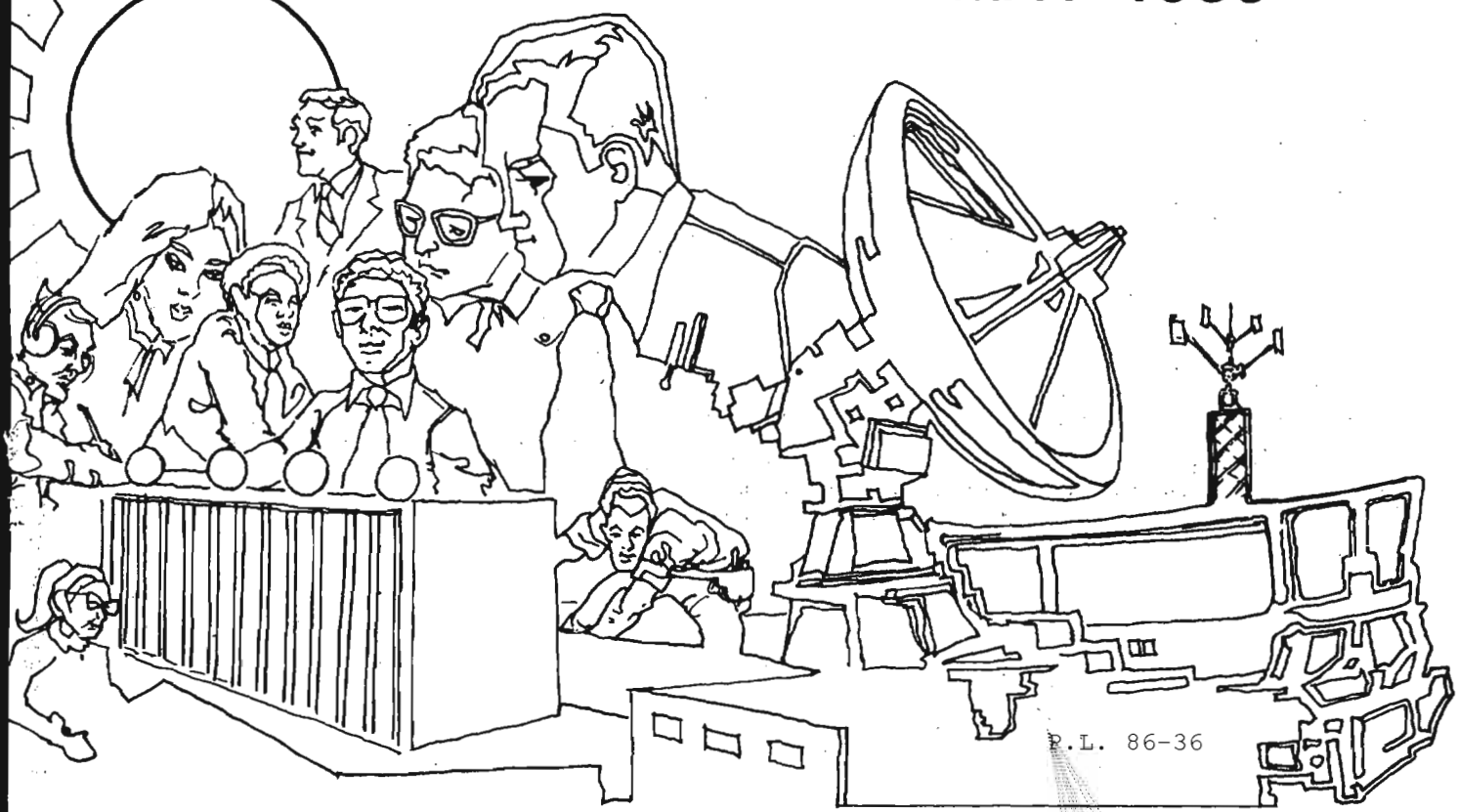
DOCID: 4009943

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MAY 1985



P.L. 86-36

THE G4 PLAN FOR CAREER DEVELOPMENT (U)..... [redacted] 1
THE CRYPTOLOGIC LINGUIST PROGRAM (U)..... [redacted] 4
THE SUMMER LANGUAGE PROGRAM (U)..... [redacted] 4
COPING WITH CAREER CHANGE (U)..... [redacted] 5
CA SKILLS ENHANCEMENT PROGRAM (U)..... [redacted] 6
GALAXY (U)..... [redacted] 7
THE FUTURE OF TRAFFIC ANALYSIS (U)..... [redacted] 9
LETTER TO THE EDITOR (U).....Robert J. Hanyok.....10
FROM THE PAST (U).....11
CRYPTO-PUZZLE NO. 29 (U).....William Lutwiniak.....12
NSA INTERN TRAINING PROGRAM [1955] (U).....13

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating~~
Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54775

DOCID: 4009943

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XII, No. 5 ..... May 1985

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Collection ..... (963-5877)
Computer Security ..... (968-8141)
Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-4740)
Cryptolinguistics ..... (963-4704)
Index ..... (963-5330)
Information Science ..... (963-5711)
Intelligence Research ..... (963-3095)
Language ..... (963-5151)
Linguistics ..... (963-3896)
Mathematics ..... (963-5655)
Puzzles ..... David H. Williams (963-1103)
Science and Technology ..... (963-4423)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-3888)

Illustrator ..... (963-3057)
Distribution ..... 963-3369)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment and what software you used.

via PLATFORM mail, send to:
cryptolg at bar1c05
(bar-one-c-zero-five)
(note: no 'o' in 'log')

Always include your full name, organization, and secure phone number.

For Subscriptions or Change of Address
send name and organization to:
P14

P.L. 86-36

Contents of CRYPTOLOG should not be reproduced or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

P.L. 86-36

In this issue we commemorate the 20th anniversary of the Career Development Program. It was celebrated in the Agency by a week-long series of presentations, discussions, and seminars. Two of these are reported in these pages; others will appear in subsequent issues.

The professionalization program certainly has taken hold. Now there is a certification procedure for just about every calling in NSA: for executive secretary as well as for cryptanalyst; in logistics as well as in language. Over the years there have been modifications, too, reflecting changes in philosophical outlook, changes in our targets, and advances in technology. (It would be fun to check out the "pqe" of 14th century Venice.) New fields have been recognized and added, and two -- cryptologic staff officer and editor-writer -- have been dropped And one field -- intelligence research is its latest appelation -- has always been in the throes of change.

What is significant is that most operational elements are seeing to it that their direct-hire pre-professionals are given the training and work assignments necessary for certification, though perhaps at a slower pace than that set for interns in the same fields. One element has even developed for its own people a very successful formal program patterned after the CA program.

Some people wonder not at the longevity of the program, but that it is only 20 years old. Why did it take so long, to get going, they ask. Actually, there were earlier attempts at a development program: the intern training program of 1955, the PATA program and CY-100 (even CA-400 in its infancy) come to mind. But they were very different in concept; the participants consisted of a small segment of the population who were to be the future leaders, having first undergone a rigorous course of formal instruction or OJT with a focus on cryptanalysis. It would be interesting to hear from participants in those or other similar programs and from people who had a hand in designing them.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009943

The G4 Plan for Career Development

(U)

[redacted]542

P.L. 86-36

~~(FOUO)~~ For many years, vacant billets in G4 for professional or pre-professional jobs at the middle level were usually filled with graduates of intern programs, notably the P1 Math Program and the Cryptanalysis Panel, and from other panels as well. By 1981, however, G4 was beginning to increase the number of new billets and soon exceeded the capacities of existing training programs. A few college graduates were hired directly into G4 where they received on-the-job training (OJT) and were enrolled in certain relevant courses offered by the training school. To fulfill its ever-expanding mission, G4 made further plans to increase sharply the number of direct college hires for the next several years.

~~(FOUO)~~ In order to attract the best candidates, the chief of G4 [redacted] thought it wise to afford them the same opportunity to attain professional certification, usually in cryptanalysis (CA), in three years' time as those entering a formal intern program. As Chairman of the Cryptanalysis Career Panel he was well versed in the requirements and the ways to satisfy them. He devised a plan that would lead to professional certification and at the same time prepare new hires for their careers in G4 -- the specialties of their home branch where they are assigned, on the one hand, and a view and appreciation of the varied and complex mission of all three divisions within G4 on the other -- in production as well as in analysis, research, and developing new techniques.

IMPLEMENTATION

~~(FOUO)~~ By August 1982, Jim had formulated his ideas and asked the author of this article to be coordinator of the plan. He outlined to me, as well as to the three division chiefs, the diversification tours he had in mind to satisfy the two goals of CA certification and preparation for careers in G4. He quickly and easily convinced me of the worth of this career development project; I not only believed in it, I knew it was good. As coordinator I saw my role to be a combination of "travel agent" -- arranging diversification tours -- and "faculty adviser" -- informing the new college hires of the requirements, recommending relevant courses, and encouraging them in these worthy endeavors for their own future and upward mobility.

~~(FOUO)~~ To this end, I devised various ways to keep track of their progress toward the goals, such as charts and worksheets for planning tours. As the number of new college hires has grown, we have turned to the IBM PC, recently made available, for help in this regard.

~~(FOUO)~~ The Plan has its own floppy disk. [redacted] of G424 designed a comprehensive, yet easy-to-use package to retain pertinent and useful information that can be easily updated. This will be a boon when an avalanche of new college hires engulfs us later this year.

~~(FOUO)~~ [redacted] G409, is invaluable in the preliminary billet preparation, initial counseling of the new hires before assignment, and seeing to the formal personnel actions. [redacted] G409, carries the ball on training requests for specific courses. Most of all, the help, advice, and cooperation we received the first year from the then CA Panel executive, [redacted] and his assistant, [redacted] enabled us to get off the ground quickly and attain the momentum for our fast track.

~~(FOUO)~~ Fortunately, for all of us -- me, the new college hires, and their branch chiefs -- the selection process provided us with a group of winners. Most of them were able to get on the fast track and, with a push from me, traveled to other realms for diversification and experience, digested relevant courses, and thrived on OJT. Those who had had algebra, statistics, and/or computer science in college satisfied most of the prerequisites for relevant or advanced courses, which they could sign up for without delay. They plunged immediately into learning to program in IMP; some floundered a bit longer than others, but all have survived and have become able and talented programmers.

~~(FOUO)~~ As for the tours, in less than a month (by early September 1982) we were off and running. Among the group of newcomers who had joined the Agency and G4 the year before, 1981, there were five who had had at least six months' experience. They were our first pioneers for the new set of diversification tours.

P.L. 86-36

DOCID: 4009943

STATISTICS ON THE G4 DEVELOPMENT PLAN (U)

P.L. 86-36
EO 1.4.(c)

EOD G4	
1981	5
1982	15
1983	14
1984	7
1985	11
Total	52

	SAT FOR EXAM	PASSED
Part I.....CA	19	19
Part II....Related Fields	19	19
Part III...Essay	19	18

TOURS

~~(C-CCO)~~ Happily, the two goals of the G4 Plan can be met with a set of designated tours of six months or more each:

1. G41 - for production experience
2. G42 - for diagnosis and techniques
3. G434 - [redacted] and production
4. Manual Systems - for CA diversification
5. An optional tour at the discretion of each division

When new college hires have finished the indoctrination course (CY-157) at Airport Square and received their clearances, their initial assignment to a branch in G4 (hereafter referred to as their "home" branch) constitutes one of the first three tours specified above. After six months or longer, they are considered ready for a tour in another area. Upon completion of some or all of CA-107 they are eligible for a tour in manual systems.

~~(C)~~ We soon found that training slots were in great demand. The CA Panel had hired that same year, 1982, a bumper crop of interns that filled the usual spaces in G6 and G9. In desperation we hunted elsewhere and found tours eventually in A3, B1, B5, G2, and P16 for manual systems. When all the available training slots for manual systems were filled, we scheduled other tours in G4 for our group. We were only too happy to cooperate with the CA Panel and made a point of yielding to them on these matters.

~~(FOUO)~~ We also explored other parts of the Agency for the optional tour. At first, G42 specified another tour in a different type of branch within G42; but we have by now extended the range to include S6, and will soon include A5 as well. As for G43, a tour in G431 is appropriate, and tours in W3, R5, and R8 have also been scheduled. In this way a branch can acquire expertise from different areas as the new college hires complete the optional tours and return "home" to stay.

~~(FOUO)~~ Another way to arrange tours is to agree to an exchange, i.e., providing a tour in G4 to someone assigned elsewhere who needs a diversification tour also. We have had to make these double arrangements four or five times in order to keep to the fast track schedule. One or two branch chiefs want their new people to do all their tours back-to-back before returning "home;" their projects are usually long-term and not easily interrupted.

~~(FOUO)~~ We also have a more moderate-paced track for any who might need more than three years to achieve CA certification and complete the G4 Plan. Several branch chiefs are not in favor of back-to-back tours; they need their people between each tour for a full six months or more because they are short-handed and under pressure to keep backlog to a minimum. There are instances, too, where relevant courses cannot be completed in time because of scheduling delays or prerequisites that take time to satisfy.

COURSES

~~(C-CCO)~~ Three formal courses constitute the bare minimum of what is required to prepare for the CA PQE:

CA-107 Manual Systems
CA-110 Cryptostatistics
CA-123 Shift Registers

P.L. 86-36

The math majors take MA-145 and MA-146 (probability and statistics) in place of CA-110; these longer math courses are a prerequisite to other advanced and relevant math courses. To supplement the over-subscribed CA-123 course at the training school, we have given our own in-house course a number of times to the new arrivals. They all need this particular course, some sooner than others. We have found among the experts in G4 two who have been willing to conduct such a class -- William Mixer of G433, and more recently [redacted] of G415. Our instructors coordinate with the training school people and use their course materials and their tests and exams, which are graded by the school; consequently, we can offer the course for credit.

~~(C-CCO)~~ We have also found a willing instructor [redacted] of G425, to teach a course in IMP programming. This has proved to be very useful and popular: it was SRO in a conference room the first time he gave it. He has had to repeat it a number of times by popular demand. It is not given for credit, but the lectures and handouts help prepare for any equivalency exam. Most everybody takes either CA-223 or CA-235 [redacted] and the math majors all take MA-213 [redacted] and other specialized math

P.L. 86-36
EO 1.4.(c)

EO 1.4.(d)
P.L. 86-36
DOCID: 4009943

courses. We also recommend CA-261 (diagnosis) and CA-247 (vocoders) to help prepare for the PQE, as well as EA-010 (at the Learning Center) for the Related Fields, in addition to CA-110 and CY-157, and advise MP-160 to those who had no computer science courses in college.

INTERNATIONAL ASPECTS

~~(FOUO)~~ Once we were organized and running, G4 was asked to provide cryptanalytic training to an analyst from CSE, Ottawa, who would be sent here for a three-year tour. We were delighted at the prospect of a Canadian connection and charted a special set of tours that would provide both diversification and areas of special interest to his organization. [redacted] joined us in July 1983 and is into his fourth tour at present writing. He is taking many courses that we recommended in cryptanalysis and mathematics. He gave a talk recently in the CA-305 series about CSE and his PCS here, and also a G4 SIGSEM talk on a technical project.

RESULTS

~~(FOUO)~~ This mixture of courses, tours, and OJT provides a potent brew. As members reach their second anniversary they are eligible to sign up for the PQE. Most everyone does so, having accumulated the necessary 700 points. The results, as of present writing, broken down by exam parts, are given above; parts I and II are the biggest milestones. These results reflect the unusually fine performance of our people.

~~(FOUO)~~ Three members have already received the formal CA certificate, having reached their third anniversary and having completed all the other requirements: 1000 points, PQE, computer program, technical paper, and diversification.

~~(FOUO)~~ The G4 trainees are often in demand for a tour now that their fame has spread. Some of them have had a chance to contribute substantially and in an innovative way to projects while on tour. These efforts have been recognized and appreciated. Our people get their fair share of awards - SSWPs, QSIs, and SPCAs in varying amounts. We are proud of them, and they reflect great credit on G4.

~~(FOUO)~~ Five of our people have been sidetracked onto special projects within G4 for one or two years. This will delay their ultimate completion of the G4 Plan, but their association with these important projects and the experience they gain can only enhance their record. They can always rejoin the Plan; it is conveniently flexible.

~~(C)~~ These newcomers even have a chance to go on TDY for consultation and to attend conferences. Last year, one of our members attended the ACE conference in Princeton; more are expecting to go this spring. Another one of our people, a member of a team of five was included in a TDY trip to IDA to assist in a briefing about their project. Still another had a trip to Bell Laboratories.

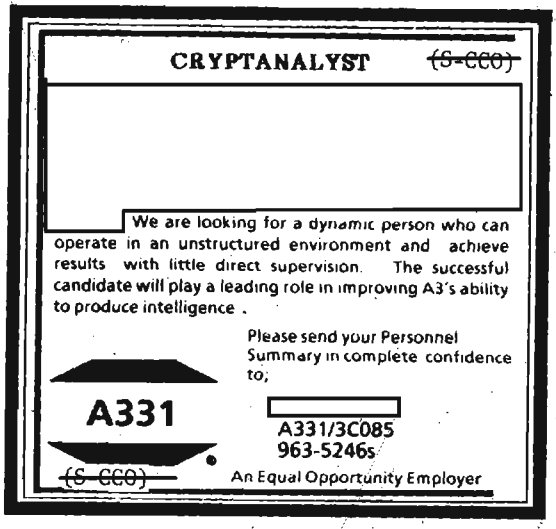
OTHER CONSIDERATIONS

~~(FOUO)~~ There is no doubt that we have a viable career development program in G4. Implemented some two and one-half years ago, it has grown and developed to fill the needs of our new pre-professionals and to respond to demands of G4's mission. But there have been a few drawbacks that, on the one hand, cause delay and frustations for me in arranging tours, and that, on the other, risk a disappointing, unchallenging tour for the individual. For example, interns usually get first chance at training slots (often in short supply) and the better projects to work on -- all for the simple reason that their permanent assignment is made after their first three years, whereas the G4 permanent assignment is made at the beginning upon entering on duty in G4. Furthermore, interns more often than not have a voice in choosing their permanent assignment. All managers, including those in G4, want to attract interns to join them eventually. It is only natural, therefore, for interns to be placed first in tour areas and be assigned the better projects from which to learn new things, whereas the G4 trainees are often expected to contribute their talents, developed elsewhere, and may not have as rewarding a tour. We now know from experience where the better tours for our G4 people are likely to be.

CONCLUSIONS

~~(FOUO)~~ The G4 career development program described in this article works very well indeed. Our people are able to compete professionally with graduates of intern programs in the same length of time. They like the idea of a "home" branch and belonging to G4 from the start. They look forward to coming "home" between tours and after completion of the Plan. Through the tours they have experienced a variety of technical problems, and production and management styles, and have made many contacts that could prove useful professionally. Best of all, their "home" branch chiefs want them back ASAP. □

EO 1.4.(c)
P.L. 86-36



P.L. 86-36

DOCID: 4009943

~~Secret~~

☐ THE
☐ CRYPTOLOGIC
☐ LINGUIST
☐ PROGRAM
☐ (u)

[redacted] *P16*, p16edr@bar1c05

☐ THE
☐ SUMMER
☐ LANGUAGE
☐ PROGRAM
☐ (u)

P.L. 86-36

[redacted] *P16*, p16lap@bar1c05

~~(FOUO)~~ The Cryptologic Linguistic Program (CLP) was promulgated in 1974 by the director of NSA, General Allen, on the recommendation of the DDO, General Wolff. It is administered by P16, the Language and Linguistics Division of P1, Office of Techniques and Standards.

~~(FOUO)~~ Essentially, the CLP is designed to develop a small but dynamic nucleus of linguists, each with several languages and/or cryptologic skills, in order better to be able to meet changing requirements of production elements, especially during crises. The program strives primarily to develop multilinguists. Participants in the program normally are trained in at least one additional language. The new language is determined by operational necessity and by the language background of the participant.

~~(FOUO)~~ The program runs approximately three years, depending upon the background and experience of the individual participant. In those three years participants rotate through work and training assignments. There are two overseas training opportunities, one in Europe and the other in Asia. Selection for overseas tours depends upon the needs of the overseas organization, the participant's language mix, and timing.

(U) Most participants in the CLP are direct hires with graduate degrees in language or linguistics. On-board candiates who are certified in a language may apply when positions are advertised in the announcement of Competitive Selection Vacancies. Previous selectees have had a wide range of language backgrounds and experiences. Typically, they have had advanced degrees in language, linguistics, or closely related subjects, and usually, they have also demonstrated considerable ability in two or more languages.

~~(FOUO)~~ Since 1974 fifteen participants have completed the program and have been assigned to production elements. Currently there are thirteen participants in the program. ☐

(U) NSA sponsors a summer employment program for undergraduate and graduate students of foreign languages. It provides them an opportunity to use and improve their skills while sampling language work at the Agency. The experience also offers a "foot in the door" towards a career with NSA upon completion of academic work.

(U) Undergraduate students are eligible to participate during the summer before their senior year, while graduate students may participate any summer prior to completion of their studies. Applicants must have a minimum of 25 semester hours of course work in applied language and pass the Agency`s language proficiency test. A major in a language, while desirable, is not required.

(U) Students are given clearances through TSC. Because the processing of applications is necessarily lengthy, eligible students are urged to apply early in the fall prior to the summer for which they seek employment. Interested students should send an SF-171 to the Employment Division, Office of Civilian Personnel. The application and envelope both should be clearly marked, "SUMMER EMPLOYMENT."

~~Secret~~

~~(FOUO)~~ For the summer of 1985 five students have been hired, three undergraduate and two graduate. Two students have Russian, one has Chinese and Japanese, one French, and one French and German. These students are to be assigned to offices in A, B, G, and W.

~~(FOUO)~~ The operational areas profit as well as the students from having linguists without encumbering billets, particularly during the summer when vacations thin the ranks of linguists. It also allows management to identify prospective hirees on the basis of demonstrated performance. Supervisors interested in having a language student for the summer of 1986 should contact the author at 963-1103. ☐

~~Secret~~

OCID: 4009943

COPING WITH CAREER CHANGE (u)

P.L. 86-36 [redacted] Y845

As part of Career Development Week activities, a panel moderated by John Monroe, now D/Chief, P04, discussed the topic, "Coping with Career Change." The emphasis was on self-help and initiative, and the dialogue centered on both career change and changing jobs. After general discussion by the panel members, the audience was invited to address questions to the panel.

Sue prepared the following highlights for dissemination to the field because the topic is particularly relevant to employees in field assignments.

During field assignments, individuals are often called upon to develop new skills and to enter new career fields in support of the mission. Such persons sometimes decide to change career fields or to seek certification in still another field. But whether at home or in the field, many people will find the discussion helpful and interesting.

P.L. 86-36

The panel members were:

*John Monroe, DDO Special Assistant; Moderator
*Dr. R. L. James, Chief, Psychological Services, M72
[redacted] Deputy, D8, Equal Opportunity Office
[redacted] Technical Advisor to Chief, B
[redacted] M315

Mr. Monroe introduced the panel and indicated that any point in a career can be a time for reflection. The panel members then elaborated on factors to be considered when an individual is contemplating career changes.

Dr. James: Consideration should be given to the medical aspects of career change during the middle years. It should be considered as part of the crisis triad: life change, family change, and career change. The individual undergoes a great deal of stress during this period and it is necessary for the person to refocus and redefine what is meaningful activity to him. The person may be suffering from a loss of self-esteem and may not feel as competitive, career-wise, as he did formerly. In addition, the individual may have reached that point in a career, perhaps grade level 12 or 13, where there is a heightened selectivity in awarding promotions.

[redacted] Job satisfaction is important. Self-perceptions and attitudes are important. There are batteries of aptitude tests administered to new employees at NSA which the individual is free to consult at any point during his career and reflect upon if he is considering a career change. On the other hand, it may be time to take advantage of educational opportunities, which are numerous in our agency to prepare for a career change. The key to a career change is: know yourself, know the system, know who can help you, and work on self-improvement.

[redacted] Do a self-diagnosis. List your strengths and weaknesses. What does it take to get into another job or career field? Networking can be useful. If you have worked for or with another employee who knows your capabilities, you may be able to seek advice or recommendations regarding a new job from that individual. Visibility, familiarity, and the image you project can be important factors in a career change.

[redacted] Remember, you can't always control career changes. A reorganization, a new mission, or technological change can result in a career change for you. Some of these changes can be a shock to the individual. A new job may not be as good as an old one, but it is still necessary to do the best job you can in the new position, to develop new skills, and to enhance your professional profile so that you will be competitive with contemporaries and promotable.

[redacted] Remember that a positive attitude and performance are important and can make opportunities available.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009943

P.L. 86-36

Dr. James: A PCS or field assignment may be sought when a lack of job opportunity occurs at HQ. The important thing is to find a job that interests you. Try to assess what your career problem is and solve it. Then pursue a field assignment or any reassignment you desire.

[redacted] Remember that performance is just one of the keys to getting ahead. Visibility is another key. Visibility can be gained by working on various panels, projects, or task forces where your contribution and ability will be noticed.

Mr. Monroe: Perhaps we can discuss visibility and the value of seeking it out.

[redacted] Before you seek visibility, you should try to assess whether or not you are a highly competitive person. You should have a strong sense of adequacy to support you as you pursue new career goals or seek visibility.

[redacted] Some employees try to move to jobs with greater visibility. Moving, in general, is encouraged at this agency, but moving from job to job is not the same as a career change.

Dr. James: Be prepared to deal with stress if you seek visibility. Similarly, stress and frustration can accompany any job change, such as a change from a technical track type of job to a management job. The individual can seek help in such cases. At times, individuals have returned to technical jobs and have successfully gotten rid of stress.

[redacted] Some agencies automatically rotate personnel to new jobs every two or three years. Some employees are suspicious of change and feel threatened by it. Many times our management initiates change by reorganization, field assignment, technical track career development, Galaxy, and the vacancy announcement system, just to name a few vehicles of change. Management is working to improve the methods used to effect change in the system. There is a real need for change to meet both management needs and the needs of the individual.

QUESTIONS FROM THE AUDIENCE

Q: Don't we have diversification, job change, and rotation here at NSA?

Panel: Few of the newly hired employees at NSA have TA or CA skills. These skill, in general, are not available in the market place. NSA hires people with related skills and trains them in specific cryptologic disciplines. With this need, NSA has been developing career paths as a kind of road map for career development which ias available for all employees. If you are interested in a specific career field or have an aptitude for it, it is up to you to pursue a job in that career specialty. The means are available here. Decide what you want to do and pursue it.

Q: Are ticket punching and regular moves needed for career advancement? How do these activities relate to the personal crisis?

Panel: In the past, some people have chosen to ignore professionalization. They've said to heck with it. In some cases, at a later date, an individual may have personally decided to reevaluate this decision, changed his mind, and decided to work for certification, while others continued to resist the career development movement. It is never too late to reconsider, especially once an individual reaches career levels that require professionalization for additional progression. It is always possible to reconsider, especially when performance and skills are top-notch and the employee is highly promotable.

Promotion boards need a weed-out factor. They must consider all qualifications and accomplishments. Factors of concern include: college degree, field assignments, certification, additional education, and staff or operational experience, just to name a few.

The age factor has been raised in career opportunity and promotion cases. Employees who are 40 years of age or older are covered under the EEO umbrella. Hopefully, managers are striving to prevent age discrimination.

If you are not longer being selected or sought for jobs, perhaps you should reflect and consider what you can do to improve your prospects. If you are experiencing stress on the job, confidential counselling is available throught psychological services, M72.

The career development office hopes that this panel discussion will help you if you are contemplating a career change. Certainly the experience you gain in a field assignment will be of value to you as you pursue your career. Likewise, self-evaluation, taking advantage of educational opportunities, and application to the Career Development Office for assistance are steps that can help each employee prepare today for a better career at NSA tomorrow. □

CA SKILLS ENHANCEMENT PROGRAM (U)

[redacted] P15 P.L. 86-36

This article is classified FOUO it its entirety.

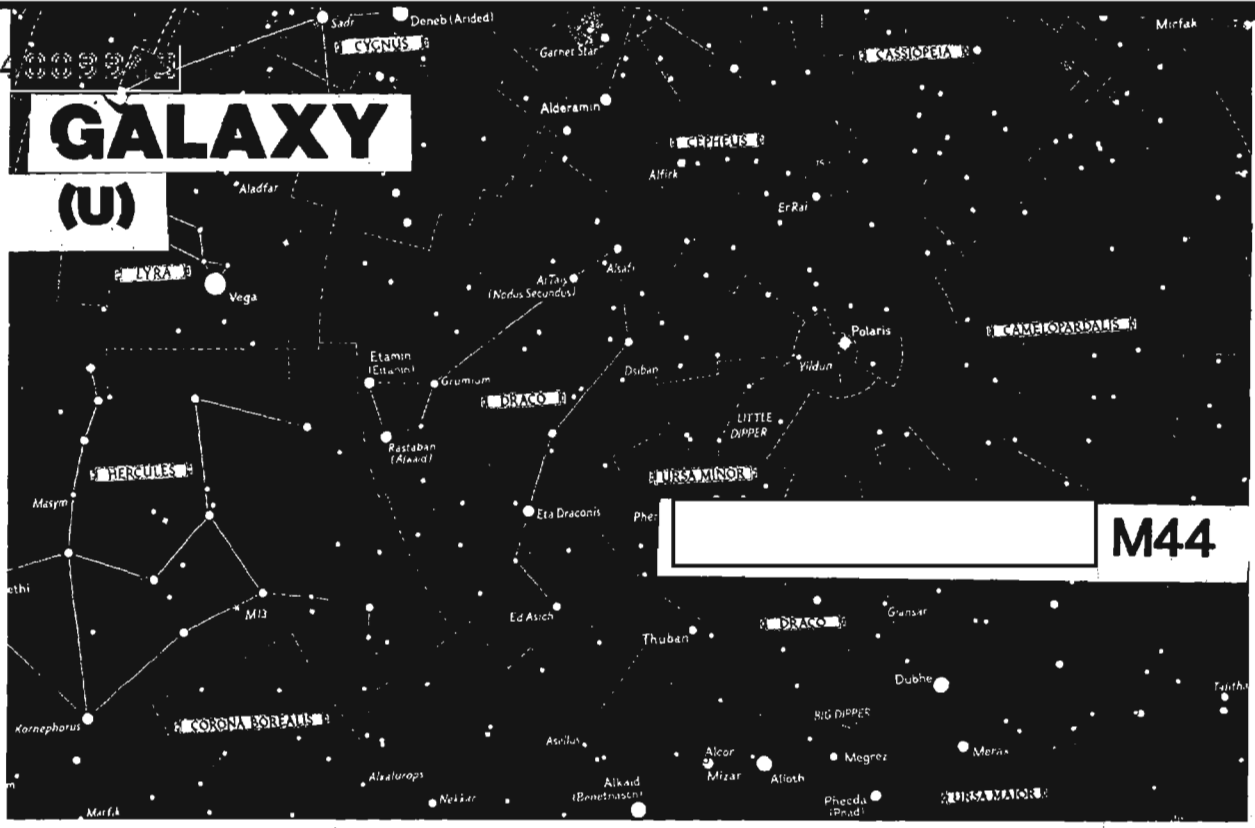
In 1981 P1 initiated a two-to-three-year development program for cryptanalysts and former cryptanalysts who wish to work in the field of manual systems cryptanalysis. The purpose is to identify and cross-train or retrain selected applicants at the GG12-14 level . This program affords participants an opportunity to broaden their experience and sharpen their skills through a series of varied operational assignments and training that are tailored for each individual.

Openings in the program are announced through GALAXY. All candidates must be certified cryptanalysts. For information call [redacted] at 963-3957. □

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

OCID: 4



For many years Agency personnel have struggled to find direction for their careers once they became professional-ized in their field(s) and reached the GS-12/13 grade level. This situation might be labeled the post-professionalization syndrome. When faced with this problem, people take one of several routes. They latch onto a sponsor or mentor who can guide them through the organizational thickets, or they press ahead on their own initiative using the proverbial trial and error method of career management, or they simply do nothing and rely on the "system" to take care of their careers for them. All these career management methods have drawbacks, particularly because they rely heavily on chance rather than on specific procedures.

Agency management has long recognized that there is a void in career development for the post-professionalization population. Finally in 1983 the then Director, Lieutenant General Faurer, formed a task force to establish a mid-level career management program. This task force conceived a program, now known as GALAXY, which would manage assignment and reassimilation actions and implement a career development system for all mid-level (GS-13/15) personnel. The task force perceived GALAXY as a bridge between theProfessionalization and the Executive/Technical Development programs. One of GALAXY's main objectives is to provide people with developmental assignments and training to prepare them to fill future Agency senior managerial and technical positions.

The GALAXY staff has been working on the assignment aspect of the program for more than a year. In addition, the program is in the midst of its first reassimilation cycle and is handling assignments for field returnees in the GG-13/15 category. It has also begun to process assignment of mid-level Agency personnel to field sites for the FY-86 cycle.

It is important to note, however, that the GALAXY assignment procedures are still in a developmental stage and are not yet firmly established. GALAXY and the GALAXY Steering Group, whose members are senior Agency managers, are currently reevaluating the program to determine the best method of handling the assignment of mid-level personnel. P.L. 86-36

At the same time, GALAXY is moving ahead with planning the second phase of the program, a career development system. As currently envisioned, this phase will include the implementation of career pathing procedures, rotational work assignments, career counseling, advance planning for key positions, and career-related training. The chart depicts how the proposed system will mesh organizational needs and individual aspirations with a variety of career development activities to produce positive results for the Agency and its mid-level workforce.

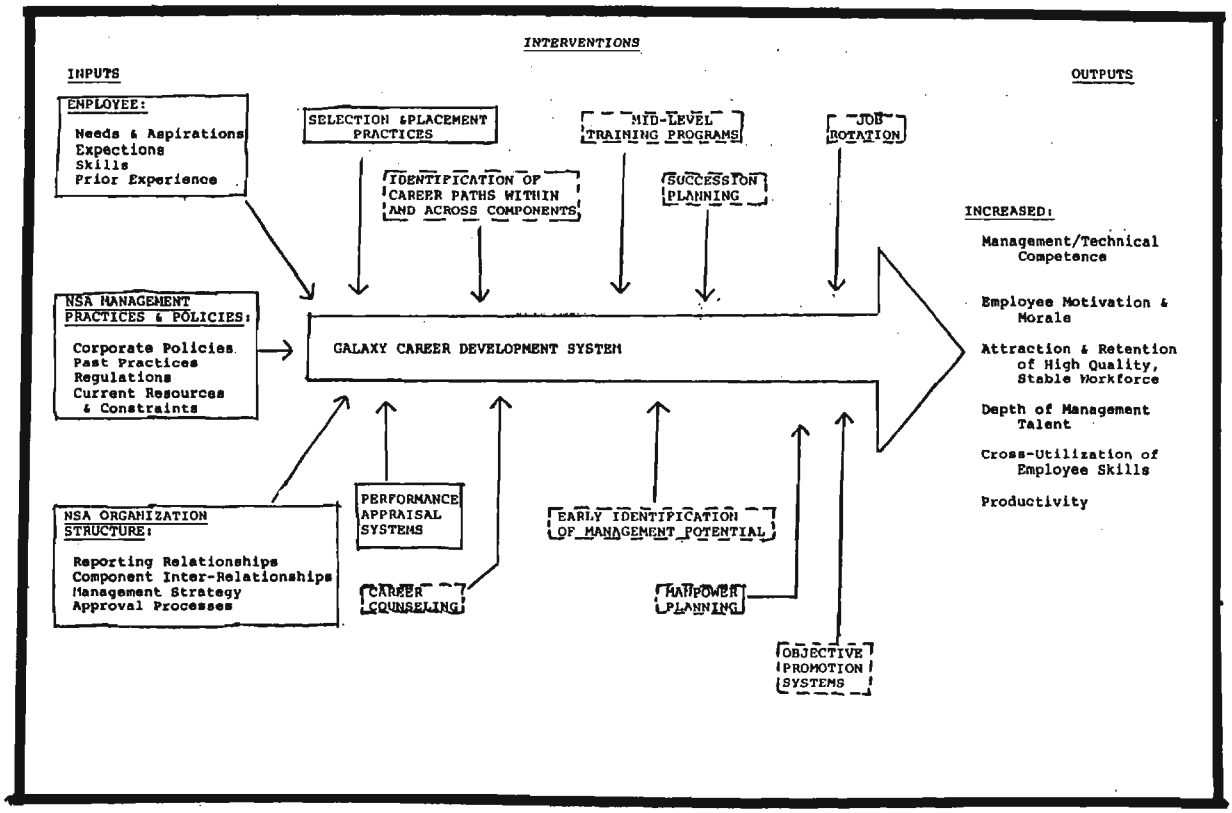
Basically, we envision a five-part program which will be phased in over a two- to-three year period. To accomplish this, we expect to employ the services of outside professionals throughout the design and implementation process. Once all segments of the program have been installed at NSA, we anticipate that mid-level career development services will be maintained for the most part by the GALAXY staff.

The initial task is to construct a "competency inventory," a database which describes, catalogs , and cross-references basic competency requirements within occupational specialties as well as across specialties, fields, and families of fields. The inventory will maintain the distinction between technical and supervisory skills and knowledges so that career guidance can be provided for both the management and technical tracks. Generation of this competency inventory will depend upon guidance from Agency senior managers, career panels, etc. This presents an excellent opportunity for Agency management to establish guidelines for the future direction of the NSA mid-level population.

The second task is to develop self-assessment surveys which will allow mid-level employees to determine their current competency levels, individual preferences, and motivations. This data can then be used to compare the invidividual's competencies with the requirements of the position(s) to which they aspire. We will also design a complementary

~~FOR OFFICIAL USE ONLY~~

OCID: 4009943



assessment survey for use by supervisors as a counseling tool in private session with their subordinates. These surveys will assist both the organizations and the individuals to reach their respective objectives in the career planning process.

The next task, to be undertaken simultaneously with the previous one, is to initiate a form of long-range planning to fill key positions. To accomplish this we first need to determine relative growth trends within Agency career fields. Once high growth areas have been identified, competency profiles can be delineated and then appropriate career paths can be outlined for mid-level employees who desire to advance into the high growth areas. These procedures will help to insure that the Agency has sufficient qualified personnel prepared to fill future staffing requirements.

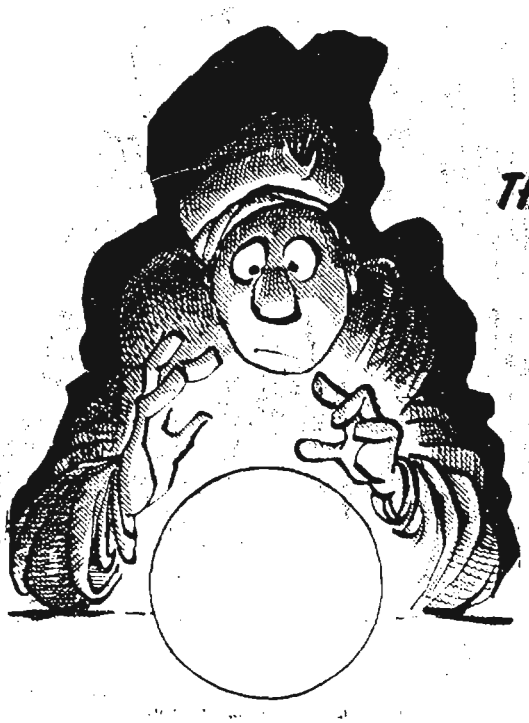
The fourth task is to establish several career management mechanisms to support career planning. One such mechanism is an automated data base which will permit individual career pathing by matching employee competencies with the requirements of position openings and identifying areas for individual development. Another mechanism is a mid-level training package being devised by M4 and the NCS to help the GALAXY population reach their career objectives. A third mechanism is a career counseling center which will contain, among other things, listings of all current position vacancies, jobs identified as rotational assignments, educational and training opportunities, and self- assessment materials. This center will be staffed by GALAXY personnel who will provide counseling, guidance, and feedback.

The fifth and final task is to integrate all mid-level career management and placement support systems in a competency framework. This includes developing competency-based criteria for entry into higher level Agency positions, as well as criteria to assist employees in choosing between the management and technical tracks. Also at this stage, the competency inventory may require refinement. This will be accomplished by acquiring feedback from managers and non-managers alike as to the comprehensiveness and utility of the program.

All segments of the career development system will be available for use by the GALAXY population as soon as they are completed. The competency inventory will provide employees with guidance on technical and supervisory skills and knowledge requirements for jobs through-out the Agency. The assessment surveys will aid supervisors and non-supervisors alike in determining individual abilities. Planning well ahead to fill key jobs will help to point out trends in future requirements for Agency positions. The automated data base will allow employees to develop individual career planning information. The mid-level training program will help prepare the GALAXY population for higher level positions. And the career counseling center will be the focus for interaction between the GALAXY staff and general population.

In summary, the implementation of a mid-level career development system will help meet future Agency requirements for highly skilled managerial and technical personnel, and will prepare the GALAXY population to fill these requirements. The design of this phase of the GALAXY program is still in its early stages. Therefore, if anyone has any questions or recommendations about this proposed system, we invite you to write, stop by, or call the GALAXY office, M44, Room B6E36, FANX III, 968-7160s or 859-4678b. □

OCID: 4009943



THE FUTURE OF TRAFFIC ANALYSIS (U)

P.L. 86-36

[redacted]

It is a pleasure to be here and to be asked to think about the future of TA. That's a subject I've been thinking about, in one way or another, for most of my adult life.

I would like to begin by making some predictions about TA twenty years from today. I found a crystal ball and was going to set it up here on the podium for these predictions. However, the guy that owned it couldn't figure out why I wanted it, so I decided it wasn't worth the trouble.

Here are the predictions.

** Twenty years from today, people outside the field will be telling us that TA has no future.*

Back in 1946 when I first started, people were quick to tell me that TA was a wartime skill, that it did a fair job during the war, but that it wouldn't be around very long in peacetime. In fact, I can remember not really wanting to be in the field of TA. I was convinced that CA was more interesting, and for a while I did my best to get out of TA so I could work in CA.(Later on, when I got my hands on some actual raw traffic and began to work with collectors, I found that TA was a lot more interesting than I thought.) And people have been predicting the demise of TA ever since. By now it's an old song, but I even hear it today. So it doesn't take much nerve to predict that we will still be hearing that song twenty years down the road.

** The highest graded individual in the TA field will be a supergrade, or whatever they are calling them twenty years from now.*

This is another easy prediction. [redacted] got to be a super-grade as a Traffic Analyst, and so did I. I see no reason why other Traffic Analysts can't do the same. If anything, it ought to be a little easier for you, because the Agency is now more attentive to the technical track than it has been in times past.

** Most of the daily front page news in the intelligence community will be provided by TA.*

This is another easy one. We do it now. We have been doing it. It seems an easy projection to say that we will continue. We will still be relying on TA for much of our Information & Warning. There may be some new high-tech wrinkles in the I &W world twenty years from now, but TA has a good track record for reliability and consistency in this area. It is so simple for TA to "reach out and touch" targets to see if they are normal. Even if some good gadgetry comes along, the result will be some sort of partnership between the new techniques and the old reliable methods of TA.

** We will still rely on TA for collection steerage.*

It is funny how often this is overlooked in day-to-day operations. And yet, some TA shops could almost pay their own salaries in the savings from more efficient use of collection resources. Signals are getting more complex. Some of today's targets have a lot of money to spend and are modernizing faster than our collection system. All of this will require even <u>more</u> efficiency for collection steerage, and that's where TA has to come in.

[redacted]

This hasn't changed for years, and probably won't over the next twenty. TA people are still "batching" traffic into

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

DOCID: 4009943

homogeneous groups to prepare it for cryptanalytic attack. Ask your favorite cryppies if they would like this to continue. Once cryptanalysts experience good TA support, they become believers; they will ask for it again and again, because they know it helps them to do their own job well.

** On Tuesday, the 24th of May, in the year 2005, someone will be heard to say, "My problem isn't a standard TA problem--we don't use callsigns."*

I think I first heard this about 35 years ago when I started working on a radioprinter problem. I really don't think there is a standard TA problem. What we have is one or two problems that are so large, we tend to think of them as standard. But they aren't. Traffic analysts have a large bag of tools, built up over the years. We keep adding to that bag of tools, but we don't throw old tools away. Lately, we've been added some computer tricks to our toolkit, and over the next twenty years, I suspect that other new tools will be developed. We need every tool we can get.

Art Levinson used to say that we were a bit like a man that has lost his wallet on a very dark street. We don't look for it where we think we lost it--in the dark. We look for it over under the street light where we can see. We have to work with what the target gives us. And we use whatever tools are appropriate for the features the target gives us.

This leads me to my last prediction, one I hope does not come true.

** Sometime during the next twenty years, your target, or the target you are most interested in, will have a major communications change.*

Maybe the target will find out what we use to exploit his communications, how we do our little magic tricks to produce TA results. Maybe they will have a spy, or maybe some public figure will slip and say too much, or maybe someone will go out and write another dumb book. Whatever the reason, the target will change its system, perhaps at great cost and inconvenience.

First there will be panic and a lot of running around. Then, after things settle down a bit, the traffic analysts will begin to take a look at what the target is giving us to work with. Then they will dip into that big old bag of TA tools, and start building another processing system, a system that will feed the collectors, and the cryptanalysts, and the intelligence community. As they recover the new signal plan, what the traffic analysts find will be new, and maybe some of the tools they use will be new. But it will still be TA. □

LETTER TO THE EDITOR

~~(FOUO)~~ *One of the advantages of being associated with a program such as the Traffic Analysis Intern program is the opportunity to watch the big picture develop. For three years I watched the traffic analysis career field being continually rescued from threats to its survival that came from whatever managerial wonders happened to be exerting influence at the time.*

~~(FOUO)~~ *While specific to the TA experience, these remarks point out the crucial aspects of organizational life: organizations, agencies, corporations, or whatever, are really people. Hiding behind the various bureaucratic identities cannot diguise this reality. The "health" of the people affects the organization's. When people stop caring, growing, and producing, the organization ossifies and eventually fails.*

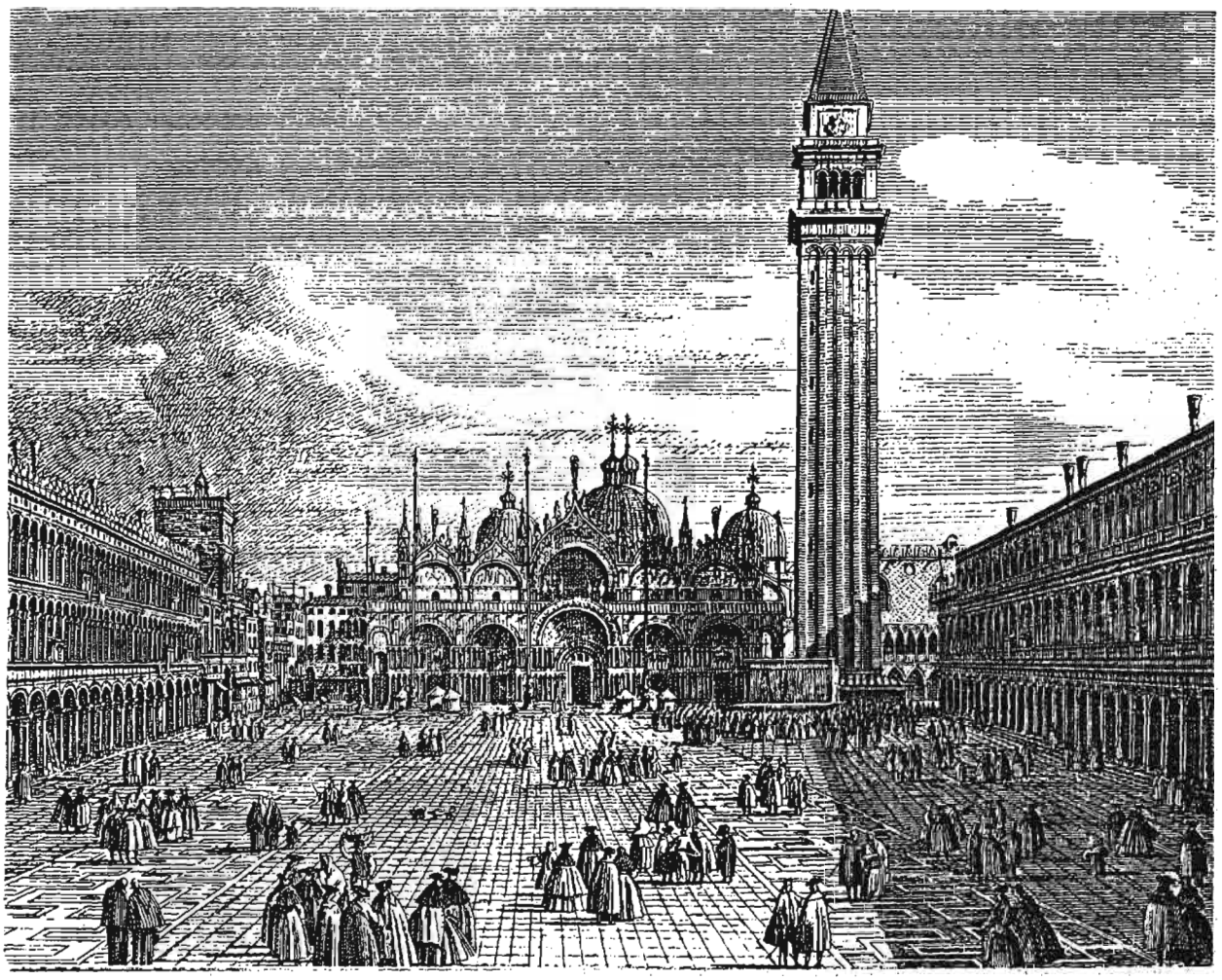
~~(FOUO)~~ *Personal career and organizational development are intimately linked. This Agency has taken vital steps to facilitate career development, thereby assuring its future. This month's Career Development activities are a celetration of this process -- in the past, present and future -- and its meaning for us and the Agency.*

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009943

FROM THE PAST



extract from

"The Contribution of the Cryptographic Bureaus in the World War" by Yves Gyldén, published in *The Signal Corps Bulletin*, Nos. 75-81, Nov-Dec 1933 - Nov-Dec 1934.

Mr. Gyldén was a well-known Swedish code and cipher expert. The article first appeared in a pamphlet entitled, "Chifferbyråernas Insatser I Världskriget Till Lands," published in 1931 in Stockholm.

The oldest known cryptographic bureaus were located at Venice under the Doges and at the papal curia in Rome. From 1300 to 1400 these centers were so very well organized that they may in some respects be considered as models even today. Their work included both cryptography and cryptanalysis to an equal degree, and with a logic which even today has no equal in many places, cryptanalysis was placed first for the very logical reason that the person who is best able to solve a cryptogram is able to grasp the weaknesses of his own systems and work out means for eliminating them.

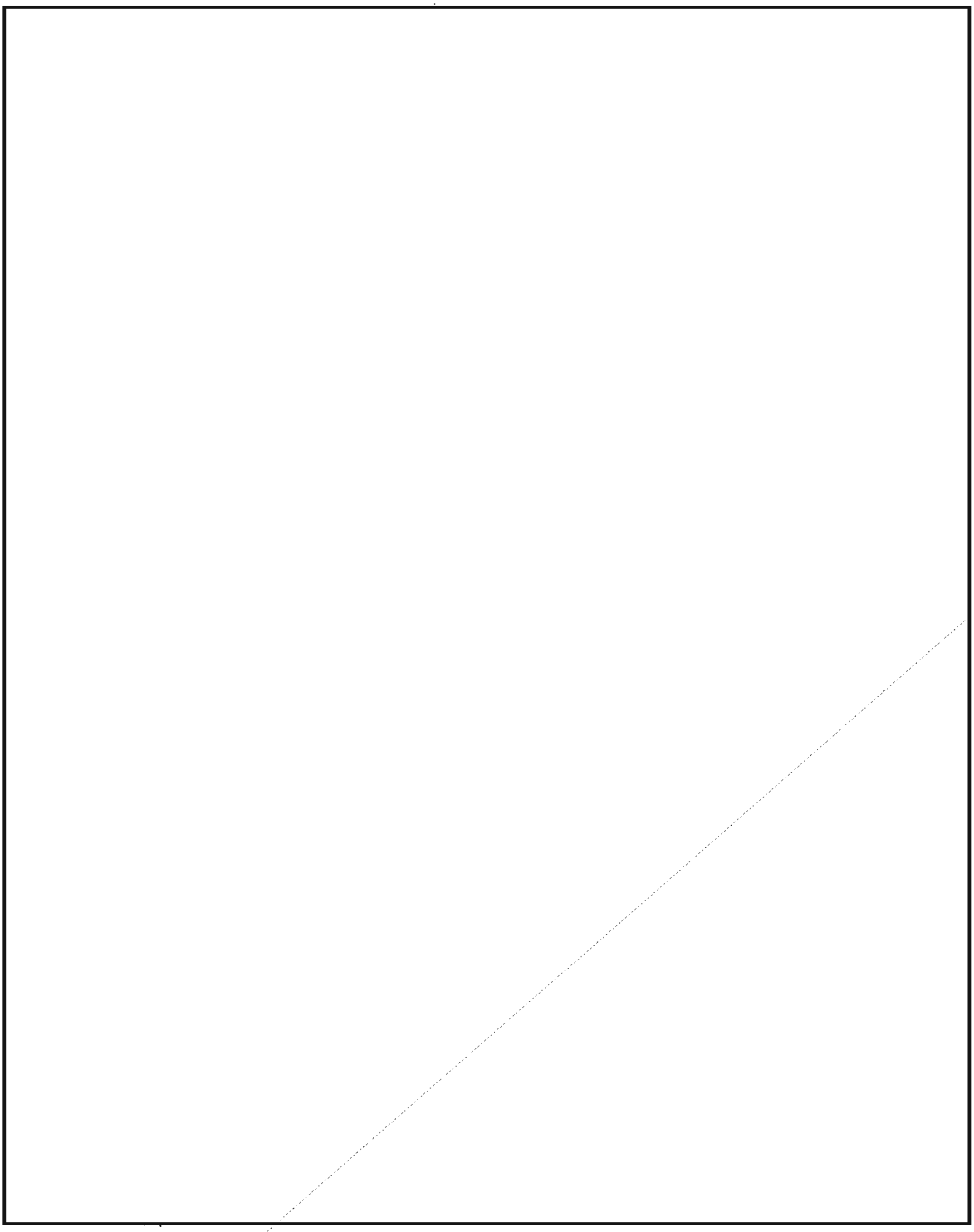
The requirement for admission to the said Italian bureaus, especially that in Venice, for this reason consisted of the passing of a very difficult examination in the science of cryptanalysis, which was given once a year for applicants satisfactory in other respects.

The technical literature on cryptography of that period also shows a most surprising insight into the problems of cryptography, and we must call attention to the fact that the dissertation [1] on cryptanalysis written in 1474 at Milan by Sicco Simonetta, a cipher clerk, is even today considered greatly superior to all reports prepared by the German school [immediately preceding and during the World War] on the solution of the same cipher system.

[1] *Regulae ad extrahendum litteras zifferatas sine exemplo.*

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009943



EO 1.4.(c)
P.L. 86-36

Reprinted, with permission, from the Spring 1979 issue of the Cryptologic SPECTRUM

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009943

EO 1.4.(c)
P.L. 86-36

NSA BEGINS INTERN TRAINING PROGRAM

Nine employees have been selected from 100 applicants to participate in the first Agency Intern Training Program.

Designed to provide a reserve of management-trained personnel from among outstanding civilian career employees, the program began January 31 and ends July 8.

The nine selected received two weeks of orientation and are now beginning rotating work assignments which will take each into from four to seven Agency areas. They meet as a group twice weekly for specialized training in the principles of management and administration.

The selectees are

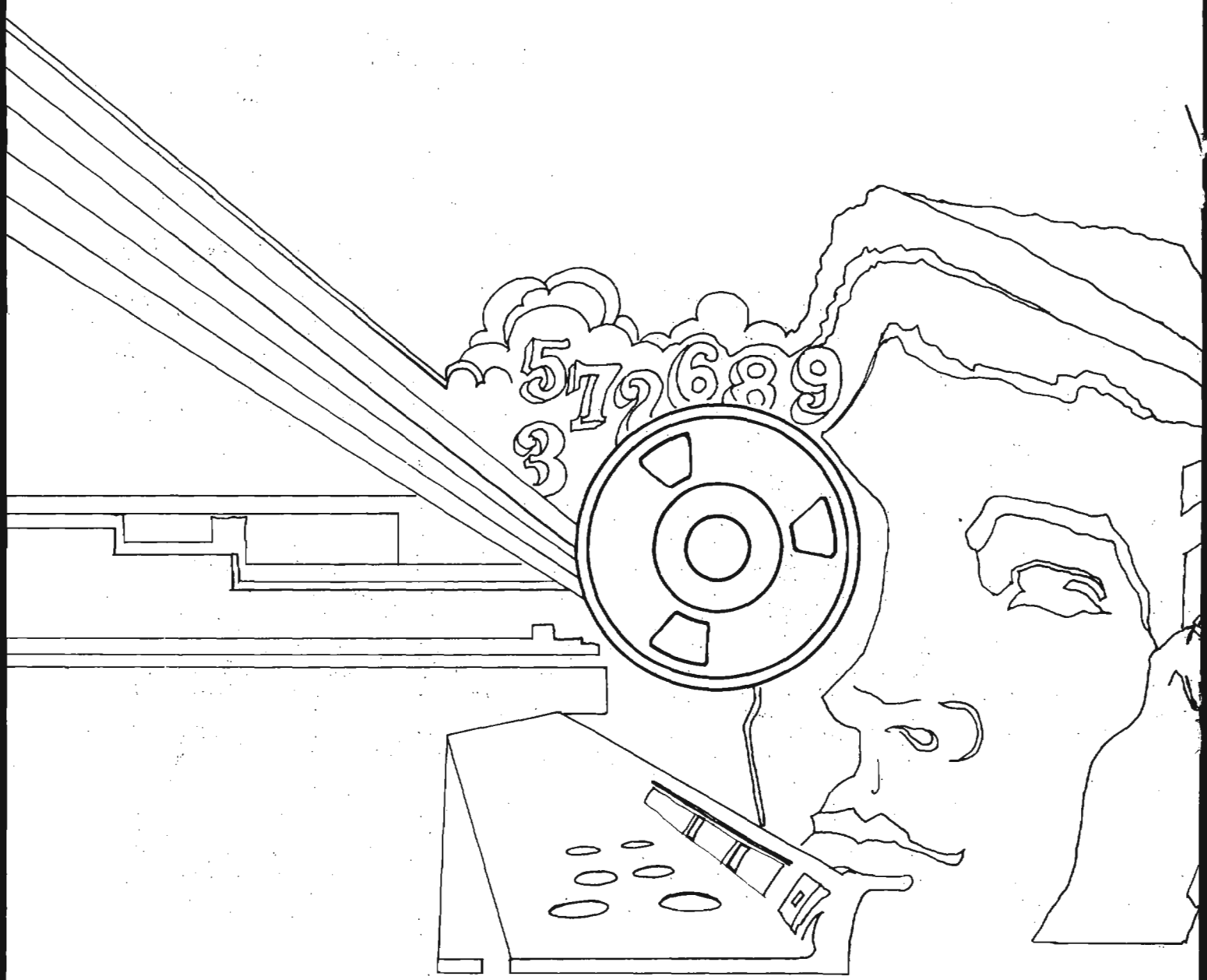
Selection of the participants was handled by Personnel Division, and was based on a written examination, group oral interview, work history, and evaluation by supervisors.

The actual program is conducted by Training Division.

NSA NEWSLETTER, FEBRUARY 1955 ~~(FOUO)~~

P.L. 86-36

Pl-Oct 85-Y1-85225


5726893

DOCID: 4019702

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

APRIL 1985

P.L. 86-36

FINDING A HOME FOR AFSA 1949-1952 (U)..... [redacted] 1
SUPPORT TO LANGUAGE ON THE ASTW (U)..... [redacted] 3
BULLETIN BOARD (U).....4
A UNIQUE HUMINT ORGANIZATION (U)..... [redacted] 5
IMPROVING LIFE WITH AN ASTW (U)..... [redacted] 7
... AND THERE WE WERE! (U)..... [redacted] 9
GOLDEN OLDIE (U).....10
NSA-CROSTIC NO. 61 (U).....D.H.W.....12

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating~~ ~~ion Required~~

Declassified and Approved for Release by NSA and DIA on 10-16-2012 pursuant to E.O. 13526, MDR Case #54778

DOCID: 4019702

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XII, No. 4 ..... April 1985

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Collection ..... (963-5877)
Computer Security ..... (968-8141)
Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-4740)
Cryptolinguistics ..... (963-4704)
Index ..... (963-5330)
Information Science ..... (963-1145)
Intelligence Research ..... (963-3095)
Language ..... (963-5151)
Linguistics ..... (963-3896)
Mathematics ..... (963-5655)
Puzzles ..... David H. Williams (963-1103)
Science and Technology .... (963-4423)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-3888)

Illustrator ..... (963-3057)
Distribution ..... (963-3369)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment and what software you used.

via PLATFORM mail, send to:
cryptolg at bar1c05
(bar-one-c-zero-five)
(note: no 'o' in 'log')

Always include your full name, organization, and secure phone number.

For Subscriptions or Change of Address
send name and organization to:
P14
P.L. 86-36

Contents of CRYPTOLOG should not be reproduced or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

P.L. 86-36

P.L. 86-36

Many years ago P16 was issued an experimental model of a manual typewriter to try out. But before it could go into production, it was overtaken by another technical advance -- the electric typewriter with changeable "golf ball" fonts and a correcting ribbon.

We still have that manual typewriter. It has come in handy during our many moves, for we usually arrive at our new place before the electricians can do their thing. And it's more than a simple back-up to an impressive array of word processors. Among the many useful features is the provision for adjusting spacing, which makes it ideal for filling out forms. It's better for that chore than any other machine around. Best of all, it's just the thing for writing first drafts. It's as good as a sharp #1 pencil on a yellow pad, and faster. Moreover, there's something about the configuration of the machine and its neat design that compels clarity of thought and precision in the use of words.

A similar kind of technical advance has affected CRYPTOLOG. The Xerox Star has come along with some desirable features that make it especially appropriate for a periodical. The principal ones are the large variety of font styles and sizes, automatic paper feed, and graphics. No longer will we have to cut and paste because only one font (of the two available) can be printed at a time. And no longer will we have to feed in single sheets by hand, ever so carefully, one at a time.

The "we" in this case has been [redacted] *to whom warmest thanks are due for continuing support to CRYPTOLOG in many important ways not apparent to readers.*

As you might guess, in leaving BARDOLPH and the UNIX editor we will be doing without a nice feature or two. Alas, we'll be without automatic hyphenation and a spell check.. And so, back to ragged rights, just like the earlier issues of CRYPTOLOG which were typed.

Ug.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019702

~~CONFIDENTIAL~~

FINDING A HOME FOR AFSA 1949-1952

or,

Why We Don't Have Bluegrass in Front of the Building and Mint Juleps in the Dining Parlour

[redacted] Q42

P.L. 86-36

~~*This article is classified CONFIDENTIAL in its entirety*~~

Although the "who" and "when" questions about the decision to locate NSA's predecessor, the Armed Forces Security Agency (AFSA), at Fort Meade are generally known, the "why" and "how" are somewhat vague. This account of the decision is based entirely on minutes of the meetings of the AFSA Council (AFSAC) from 1949 through 1952.

The question of location was a priority agenda item for AFSAC as early as the Council's initial meeting in July 1949. At that time, AFSA was operating in run-down buildings at Arlington Hall Station (AHS). There were really two questions -- where to locate AFSA's permanent headquarters, and what to do about AHS in the meantime. In the fall of 1949 the Army was prepared to release $12 million for a new building at AHS, but some AFSAC members, dissatisfied with the existing location, feared that taking money for new construction or rehabilitation there would jeopardize funding for future new construction elsewhere.

At the January 1950 meeting, Army Assistant Chief of Staff for Intelligence, Major General Irwin, reported that rehabilitating AHS to reasonable standards of fire and structural safety would cost $2.5 million, including air conditioning, considered necessary in order not to disrupt vitally important work during the summer months. The estimate for a new building there was $9.5 million, and General Irwin expressed the hope that the $7 million difference could be allocated for building a new headquarters away from Washington. The January session produced the following consensus: "No new construction should be requested for COMINT activities in the Washington area at this time. This should not operate to prevent the rehabilitation and maintenance of existing structures recognized to be necessary. An operational cryptologic nucleus should be established at a site outside the Washington area as soon as possible."

In discussing whether or not to leave any functions in the Washington area, Army Security Agency Director Brigadier General Clarke stated his belief that there would be no need for any activity in the Washington area except for liaison and dissemination. The meeting ended with the Council agreeing to leave the determination of the character of the cryptologic unit remaining in Washington to the future, while concentrating on establishing the new headquarters away from Washington.

At the April 1950 AFSAC meeting, each service was asked to nominate one representative to an ad hoc Site Selection Board which was to recommend a location for the new headquarters. The main motive for moving away from Washington was, of course, the fear that Washington would be a primary target in a nuclear war.. Although little was known at the time about Soviet delivery capability, the shock from the first Soviet nuclear test in September 1949 was still reverberating through the corridors of the Pentagon. The Site Board's task was to find a location far enough away from Washington for safety, but not so far away as to make coordination difficult.

The Board's rather voluminous report, AFSAC 59/6, was delivered to the members at the November 1950 meeting. As recommended locations close to Washington the Board had listed Fort Belvoir, Fort Holabird, Fort

~~CONFIDENTIAL~~

DOCID: 4019702

Meade, and Andrews Air Force Base (AFB). Thirty-two other sites, primarily military bases and arsenals, were listed, in Colorado, Georgia, Indiana, Kentucky, Missouri, North Carolina, Ohio, Oklahoma, and Texas. The top three, in priority order, were the Kansas City Records Center, Air Force Plant Number 3 in Tulsa, and the St. Louis Administration Center. The report conceded that the distance of all of these from the seat of government is such that it would probably more or less adversely affect the efficiency of AFSA operations. The only two sites on the list within a 350-mile distance from Washington as well as a safe distance inland were Fort Belvoir and Fort Meade. It was the opinion of the Board that the Fort Meade site was the more suitable of these two, being at a greater distance (25 miles) from the Washington metropolitan area, and 15 miles from Baltimore. The report pointed out that the AFSA headquarters would probably constitute a priority target by itself wherever it was located, and asked rhetorically, "Who can say that Baltimore is more likely to be bombed than Kansas City?"

Admiral Stone, as AFSAC Chairman and AFSA Director, then threw the issue out for discussion. Major General Bolling, who by that time had replaced General Irwin as Army Assistant Chief of Staff for Intelligence, wondered whether Bainbridge, Maryland, had been considered. Air Force Director of Intelligence Major General Cabell viewed it unwise to locate so close to prime targets such as Baltimore or Kansas City. He suggested locating near a "cultural or non-industrial" city -- perhaps "on the prairie." General Bolling suggested Fort Francis Warren in Cheyenne, Wyoming (now, ironically, a Minuteman missile base). Admiral Stone pointed out that locating at a remote site without facilities, like Cheyenne, would greatly increase construction costs. General Cabell characterized the threat to such a site as three-fold: air attack, sabotage, and submarine-launched missiles; very prescient for 1950! He described Fort Meade as vulnerable to all three, while Kansas City would be especially susceptible to sabotage. The discussion rambled on in an inconclusive fashion, as one member after another mentioned Birmingham, Alabama, Chambersburg Pennsylvania, Hagerstown and Frederick in Maryland, and Fort McClellan, Arkansas. When pressed to characterize the ideal site, Admiral Stone described it as within a 350-mile radius from Washington, roughly a day's travel. Not only did the meeting end without a decision about the site, but the Council decided to go back and re-examine the criteria and methodology used by the Board.

At the February 1951 meeting Air Force Security Service Director Brigadier General Lynn presented a paper with two lists. The first listed sites where adequate facilities already existed: the Kansas City Records Center, the Air Force Plant in Tulsa, and a Quartermaster depot in Charlotte, North Carolina. The "no facilities" list included Fort Knox, Lockbourne AFB in Ohio, Fort Benjamin Harrison in Indianapolis, Brooks (now Goodfellow) AFB in Texas, and the Rocky Mountain Arsenal in Denver. The first three on the second list were quickly eliminated: Kansas City as "too fat" a target, and Tulsa and Charlotte because those facilities had been committed to military production for the Korean War. General Lynn described Fort Knox as the best of the "no facilities" installations. General Bolling wondered why Cheyenne had been omitted, and was told that the population base was too small to supply a civilian workforce. General Lynn suggested a vote, and, according to the minutes of that meeting, AFSAC approved Fort Knox as a suitable site for locating the major cryptologic establishment (AFSA) outside the Washington area, and authorized the Director of AFSA to draw up a paper for the Joint Chiefs of Staff (JCS) containing recommendations in accordance with the Council's decision. The target date for the move.was established as 1955

The decision seemed to have been made, but the members were called back for a meeting on 26 February to receive some unpleasant news: that decision was not acceptable; the JCS had rejected their choice of Fort Knox and instructed them to come up with a new list of three sites in priority order. Admiral Stone suggested Brooks AFB, Lockbourne AFB, and again, Fort Knox, and also asked for additional suggestions. This time the discussion centered on the availability of a suitable civilian workforce. The AFSAC's own paper recommending Fort Knox had listed its distance from Louisville (20 miles) as its biggest disadvantage. (Given the distances that most NSAers commute to and from work , it is interesting to note AFSAC's fear that employees wouldn't be willing to travel 20 miles from the closest major city.) Navy Captain Dyer, the Site Board Chairman, reported having been informed by personnel officers in Hagerstown that Fairchild Industries was able to draw its workforce from a 50-mile radius. Admiral Redman said that if AFSA moved to Brooks AFB, the headquarters of the Air Force Security Service, it would be "like the mountain going to Mohammed." After more discussion, it was decided that AFSAC would recommend that the JCS choose from among Brooks AFB, Lockbourne AFB, and Fort Knox. The papers also contained a subtle element of an ultimatum: should none of these three be acceptable to the JCS, there would be no alternative but to purchase non-government land in a suitable location, at considerable expense and delay. This was forwarded to the JCS in the form of AFSAC 59/23.

At the March meeting Admiral Stone informed the body that since the Air Force had decided upon other plans for Lockbourne AFB, it would be necessary to come up with a new third choice for the JCS to choose from. He suggested the following new priority list: Fort Knox, Brooks AFB, and Fort Meade. He mentioned that "someone" had suggested that locating in Florida would solve the problem of attracting a civilian workforce, but didn't believe that Florida would meet the other criteria. General Cabell criticized Fort Meade as "too vulnerable," and General Lynn induced Admiral Stone to state that the primary reason for leaving the Washington area was to

DOCID: 4019702

reduce vulnerability. The Army went on record as opposing Fort Meade and favoring Fort Benjamin Harrison as the new third choice, but the Army representatives were outvoted. Even though the JCS had asked for three locations in priority order, the paper recommended Fort Knox as first choice and listed four second choices in no particular order of preference: Brooks AFB, Fort Benjamin Harrison, Fort Meade, and Rocky Mountain Arsenal. This time it stuck, and, on 10 April 1951, Secretary of Defense Robert Lovett approved Fort Knox as the permanent site for AFSA.

How that decision came to be cancelled eight months later cannot be completely explained from the AFSAC meeting minutes. On 7 December 1951 General Canine, the new AFSA director and AFSAC chairman, was asked for his views on the move by Deputy Secretary of Defense Foster. General Canine told Secretary Foster that he was concerned about AFSA's ability to operate "so far removed" from its recipient agencies. He also expressed fears about serious personnel losses. He conveyed the same views to JCS Chairman General Omar Bradley, who suggested that General Canine accompany him to a special JCS meeting. General Canine asked for time to convene AFSAC first.

General Canine called for a meeting on 11 December, at which he announced his preference for rescinding the AFSAC/JCS decision to relocate to Fort Knox. He argued that AFSA should stay within commuting distance of Washington from the standpoint of service to the recipient agencies and the Services. He also stressed the personnel factor. He stated, "There can be no substitute for experience, and one good man is worth 100 mediocre people, and one exceptional person is equivalent to five good people."

There still remained the issue of vulnerability, however. Admiral Johnson, the navy representative to AFSAC, recalled that the original JCS tasking suggested the establishment of a backup facility away from the Washington area, rather than moving the entire headquarters. Several suggestions were put forth for a backup location: Brooks AFB, the United Kingdom, and even a ship in the Atlantic Ocean. Eventually AFSAC agreed to recommend to the JCS that the Fort Knox decision be rescinded and that AFSA be relocated "within the dispersal area of Washington D.C.," defined as that area within a 20-mile radius of Washington. No recommendation was made regarding a backup location.

General Canine gave basically the same story to a special JCS session on 12 December, and the Secretary of Defense directed him to select a new site. This time, the Site Board selected Fort Meade, and AFSAC concurred with this recommendation at its 36th meeting on 23 January 1952. General Canine told the Council that, based on his informal discussions with "various civilians", he didn't anticipate any serious personnel losses in moving from AHS to Fort Meade.

What turned the JCS around between April and December 1951? A recent (unclassified) book attributed the switch to a "near-mutiny among the agency's civilian work force," but that would seem to be an oversimplification; opposition by Washington-area COMINT customers was probably the most important factor. Deputy Secretary of Defense Foster told General Canine in their 7 December conversation that "some alumni" of AFSA, after reading the recently announced plans to move AFSA to Fort Knox, had prompted some rather important and influential people in Washington (i.e., the newspaper editors) to express their concern to the Secretary of Defense over the advisability of such a move.

The JCS may also have seen a logical flaw in the planned move that should have been apparent to AFSAC. As we have seen, the only real reason for moving away from the Washington area was to reduce AFSA's vulnerability to attack. While further inland than Washington, Fort Knox is not much further south, and was therefore would be only a little further away from a Soviet bomber attack over the Pole. In short, Fort Knox is almost as likely to be nuked as Washington.

Certainly, the fact that General Canine replaced Admiral Stone as director of AFSA and as chairman of AFSAC was a factor in the reversal. Not only was General Canine more concerned than Admiral Stone about the question of personnel loss, but he came to AFSAC comparatively late in the process and did not have the personal involvement in the site search and in the decision process that Admiral Stone did.

Another interesting aspect of the selection process is the apparent lack of political pressure. Competition among congressmen for military bases in their states and districts was common at that time, but it does not seem to have played any role in this case. There are two possible reasons for this: the almost total anonymity of AFSA at the time, and the relatively small number of people involved.

In November 1952 AFSA became NSA, and the contract for the building at Fort Meade was signed in July of 1954. And the rest, as they say, is history...

This will hardly be the definitive article on the subject. There are many people still working here who were at AHS while all this was going on, and anyone who can shed more light on the subject is more than welcome to comment;.it would be particularly interesting to hear what employees were thinking and saying during the eight months when the move to Fort Knox appeared to be a sure thing. □

SUPPORT TO LANGUAGE ON THE ASTW

P.L. 86-36

[redacted] A432

This article is classified ~~FOUO~~ in its entirely.

The PC-DOS operating system installed on the ASTW has the inherent capability of supporting foreign languages. The original foreign language that is installed is the Cyrillic alphabet. However, the installed sorting sequence is incorrect. [redacted] of A432 have provided to the PCIC a modification to the operating system that corrects the sorting sequence and provides a better character display than that provided by IBM.

We have also created a character set that can be downloaded to an EPSON-FX series printer that allows the ASTWs to print Cyrillic. This printer character set will not, however, work with the printer that is supplied by IBM as part of the ASTW contract.

As a results of our attempts to use the Cyrillic character set on the IBM family of personal computers, we have identified several software packages that work quite well with foreign language data. If you need a data base manager, both CONDOR 3 and dBASE II work quite well. dBASE III probably does also. The PERSONAL EDITOR, WORD PERFECT 4.0, and BONNIE BLUE word processing programs also work quite well. All of these packages allow the full definition of characters above 127 in the ASCII table to be used as data only. Field names, commands, and other characters that must interact with the software package must be accomplished using the standard 127 ASCII characters.

Many software packages, such as WORDSTAR, the most popular word processing program, do not work with the foreign language capabilities at all.

All of the above software, including the modifications that A432 have created, are available from the PCIC in the Main Library. Answers to questions concerning the modifications to the IBM-supplied software can be obtained by calling us at 963-4788.

Note that none of the modifications created by A432 affect the performance of the ASTW under the PC/IX operating system. As a UNIX system the ASTW is a bilingual disaster. □

EO 1.4.(c)
P.L. 86-36

BULLETIN BOARD

BOOKBREAKING ON THE IBM XT

~~(FOUO)~~ [redacted] is a new bookbreaking package for the IBM XT, suitable for small codes. A copy of the program and a user's guide can be obtained from the PCIC in the Main Library. For further information call [redacted] P13, 963-5868.

PROGRAM FOR LANGUAGE ANALYSIS

P.L. 86-36

~~(C-CCO)~~ A package of programs that provide language counts, statistics and patterns similar to those contained in MILCRYPT I has been written for the CDC JEEP. The package, titled [redacted] has four options: [redacted] for text without punctuation or spacers; [redacted] for text with spacers but no punctuation; [redacted] for text with both spacers and punctuation. A fourth option, [redacted] provides all of the above. As part of this package there are routines to excise spacers and punctuation from the original text. The programs can accept user-determined alphabets of up to 60 characters. For information call [redacted] G42, 963-4845.

PROBE FOR DIAGNOSIS

P.L. 86-36

~~(C-CCO)~~ A new diagnostics program is now on JEEP. It is similar to [redacted] but treats text in group-length rather than in character-length. Possible group size is 1 through 6, fixed-length only. For information call [redacted] or [redacted] G952, 963-585.

[redacted]

REVISED PINSETTER MANUAL

~~(FOUO)~~ A revised edition of the PINSETTER manual for traffic analysis is now ready for distribution. If you are not already on the PINSETTER distribution list, you can obtain a copy from [redacted] P14, 963-3369.

P.L. 86-36

MANUAL ON SECURITY MARKINGS

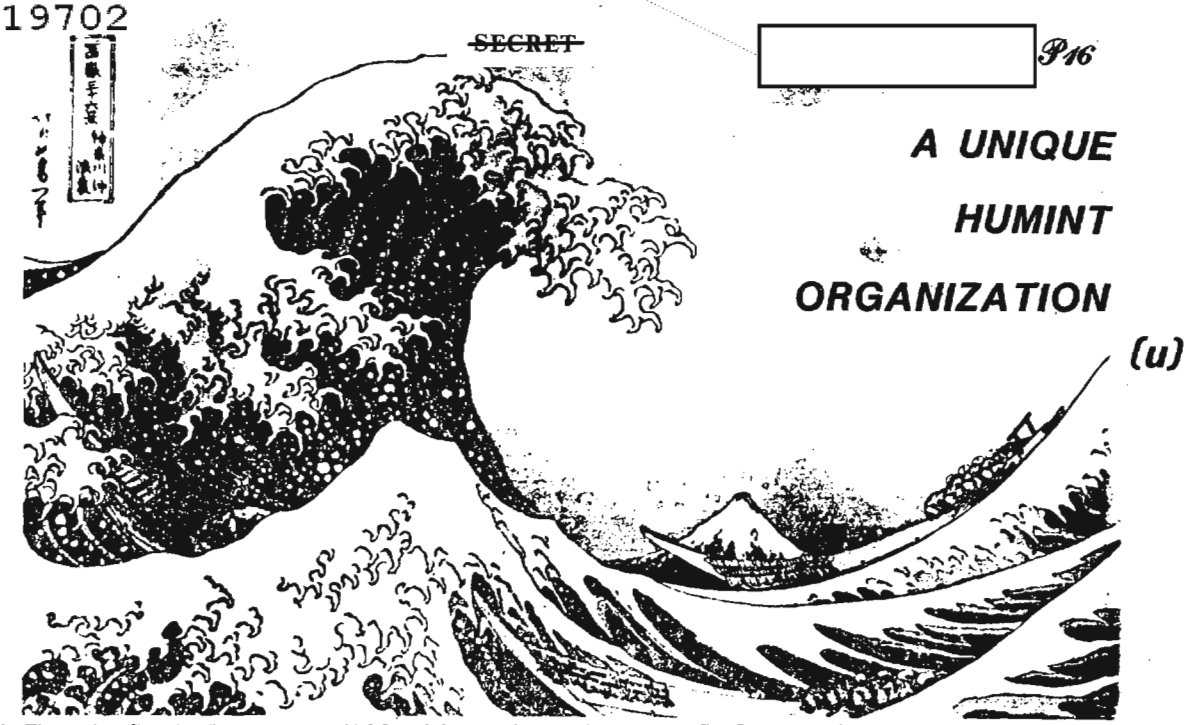
~~(FOUO)~~ The DIA manual titled Standard Security Markings (DIAM 65-19) is available in the National Data Standards Center, P13D, 968-8161. It is applicable to all members of the DoD Intelligence Information Systems Community, including NSA.

DOCID: 4019702

P.L. 86-36

~~SECRET~~

[redacted] P16



A UNIQUE HUMINT ORGANIZATION (u)

[U] The Asian Studies Detachment (ASD) of the 500th Military Intelligence Group, currently located at Camp Zama, Japan, is a unique human intelligence (HUMINT) organization. It is composed of approximately nine Department of the Army civilians, nine military members, and 75 Japanese employees. The Japanese work under the provisions of the Master Labor Contract between the Government of Japan and the US Government.

EO 1.4.(c)
P.L. 86-36

(U) The reporting/production arm of ASD is the United States Army Document Center (UDC), which exploits open source foreign documents such as newspapers, magazines, and technical journals. The UDC has eight analytic teams, each team named for its primary intelligence focus:

* China [redacted]
* North Korea
* USSR [redacted]
* Middle East.

(U) All of the analyst teams are manned by Japanese nationals, the majority of whom are retired from the Imperial Japanese Army, (or, more recently, from the Japan Self-Defense Forces) who had extensive experience in intelligence as Foreign Area Officers. [redacted]

(U) This unusual composition began to evolve shortly after the end of WW II. Predecessor organizations engaged in the translation of captured documents and archives were among the building blocks of UDC. One of the most important was the employment of Imperial Army flag officers who had been unemployable up until then because of regulations enforced by Supreme Commander Allied Forces Pacific. Once permission was granted to employ these officers, a large pool of expertise became available, particularly in endeavors requiring knowledge of Chinese characters.

(C) For the documents that UDC exploits, the term "open source" may be somewhat misleading. In restrictive societies such as the Soviet Union, North Korea, and the Peoples Republic of China documents which are circulated domestically are sometimes restricted for use by certain groups, for example, the military, and may not be taken out of the country overtly. Consequently, some of the open source documents are obtained covertly. In 1984 UDC analysts processed over 43,000 documents in their intelligence production effort.

OGA

[redacted]

(U) Some members of the intelligence community have called the type of intelligence work performed at UDC LITINT (literature intelligence) but those at UDC prefer to call it DOCINT, or document exploitation. The DOCINT process practiced at UDC has evolved over the years in much the same way as the organization and its structure has.

(U) The UDC is considered a collector but it also issues product, mainly in the form of Intelligence Information Reports [redacted] which are standard reporting vehicles [redacted] UDC reports are unique, however, in that they always carry a comment called the UDC Comment. These reports in many cases resemble finished intelligence while technically they are not. They are sent [redacted] on the basis of specific subject matter and general distribution

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

OCID: 4019702

OGA

OGA

guidelines. [redacted] distribution of these reports when they deem it appropriate.

(U) HITS has an evaluation program whereby reports are evaluated by the organizations which originated the requirements; actually 20-25% of the reports are evaluated. [redacted] Valuation of reporting is very useful for the collector, for it enables him to fine tune his reporting and to focus on the most productive avenues of investigation.

(C) Now for a brief description of the UDC's *modus operandi*. The [redacted] analyst daily reviews documents passed to him. [redacted] In his UDC comment the analyst points out items in the report he considers to be of significance, [redacted] in exploiting the material, etc.

(C) Next, the analyst submits this draft report, written in [redacted] to his supervisor for review, who might return it for more polishing before it goes to the translation section. At this time, also, any special graphic, cartographic, or photographic materials to be submitted with the report are ordered from the appropriate support facilities within the organization. [redacted] The report next is reviewed by the Chief of the Reports Review Branch, the Chief of the UDC, and the Chief of the Asian Studies Detachment. The report then goes back to the [redacted] analyst who reviews the translation and returns it through his supervisor to the editor for final decision.

(U) The report then goes to typing and from there back to the editor for proofing. It is then typed in final form for distribution. [redacted] issued either in electrically forwarded copy or hardcopy if the report is less time sensitive and contains maps, graphs, charts, photographs or other enclosures. The distribution copy is reviewed by the UDC and ASD Chiefs and released for distribution.

(C) The amount and types of information available through the exploitation of open source documents that are responsive to validated intelligence requirements is truly amazing. [redacted] One of the really useful and important features of UDC reporting, in my estimation, is the fact that it is entirely independent of other US intelligence holdings. Consequently, UDC reporting provides either independent verification of, or challenges to, other intelligence holdings, while avoiding the in-bred nature of some reporting which echoes others' reports and later echoes its own echoes. [redacted] Furthermore, each section reports weekly to the others in a general meeting of all analysts on the hot topics of the week. They also keep each other apprised of new requirements received. [redacted]

(C) Most UDC reporting is issued at the CONFIDENTIAL level unless the documents involved were obtained through more sensitive sources. [redacted] These reports represent a very valuable currency [redacted]

(S-CCO) To sum it all up, the UDC is a singular HUMINT organization which provides an invaluable service to the US intelligence community in an extremely cost-effective manner. My detail to the UDC for two years from May 1982 through June 1984 provided me with a marvelous opportunity to learn every facet of document exploitation as practiced at UDC. Owing to unusual circumstances I became Acting Chief of the Reports Review Branch in UDC in October 1982, then in 1983 I became Acting Chief of the UDC, and remained in that position until I returned to NSA in June 1984.□

EO 1.4.(c)
P.L. 86-36

DOCID: 4019702

P.L. 86-36

Improving Life with an ASTW

[redacted] G613

These hints may benefit users of the IBM PC-XT running PC/IX (the version of UNIX developed by Interactive Systems Corp. and licensed for sale by IBM for the PC-XT and ASTW) as well as new operators of the ASTW.

As currently received from the vendor, the PC/IX operating system contains several potential threats to computer security and system integrity, some of which are listed below in the form of problems encountered. The changes indicated will improve overall computer security, system integrity, and general ease of operability of the new workstation. These changes will also help users maintain their systems with fewer system errors, and save considerable time for the systems managers. All of these changes must be made by a "super user."

Clobbering Your Own File System?

Problem: If the power is turned off before the system has completed all the necessary disk writes, the file system may be left in such a state that it will be difficult or impossible to recover some files. That is because some basic file operations require multiple disk writes.

Solution: A special program */priv/shutdown* should be run before the power is turned off to assure that all necessary disk writes have been completed.

Method: Create a user login account called *shutdown* that will automatically run the program */priv/shutdown* and nothing else. This is accomplished as follows (what you type is printed in boldface):

```
$ adduser <R>
> add user shutdown <R>
Login           shutdown
Fullname
Uid             204
Group           100 (staff)
Directory       /usr/shutdown
Program
Filesize
Siteinfo
Password
 Maxage
 Minage
 Agenow

OK? (y)         no <R>
Field?          program <R>
Program         /priv/shutdown <R>
Field?          <R>
OK? (y)         <R>
Creating new directory
Standard new user initialization? (y) <R>
[ADDED]
> q <R>
```

Before the terminal is turned off, the user merely types in the login *shutdown*, hits the return key for the password, and waits for a new login prompt before turning off the power. This normally takes only about five to ten seconds. Since the only program allowed to run under this account is */priv/shutdown*, no password protection is needed and all users may use it.

Is Your File System Healthy?

Problem: A system crash, accidental power outage, or inadvertant power down can leave the file system with errors if *shutdown* is not run. If undetected, minor errors can continue to grow until they become disastrous.

Solution: The System Manager's Guide recommends that the file system check program (*fsck*) be run every time the system is initialized. This program will locate and often be able to correct any minor discrepancies in the file system before they become unmanageable. A minor change to the system initialization procedure will force the automatic execution of *fsck* during system initialization.

Method: Replace the letter *d* in line six of the file */etc/rc* with the letter *m*:

```
originally:     case $1 in
                "d")

change to:      case $1 in
                "m")
```

Classified Displays Left on Your Screen?

Problem: When a user logs off, the login prompt is displayed on the line immediately following the last bit of text, leaving a possibly classified data still displayed on the screen.

Solution: The licensing logo that is displayed with the login prompt can be readily modified to clear the screen before it is displayed.

Method: First make sure that the right hand margin in the INed editor is turned off before making the

~~FOR OFFICIAL USE ONLY~~

OCID: 4019702

modification, or else the text will wrap and cause a problem during system initialization. To turn off the margins, consult page 22 , Beginner's Tutorial to PC/IX, in the Text Processing Guide.

In the */etc/ports* file insert a backslash "f" (\f = *form feed* which clears the screen) before the licensing logo:

originally: herald = "\r\nPC/IX - 6428163 (c) Copyright IBM ...

change to: herald = "\f\r\nPC/IX - 6428163 (c) Copyright IBM ...

put \f here ↑

Disks Overflowing with Garbage?

Problem: Default values are set up so that the *skulker* program that cleans out outdated backup files and ...filename INed temporary files runs at 3 AM. In areas where the computer is turned off at night, the *skulker* will never run and the disk will eventually get overloaded with "garbage" files.

Solution: Force the automatic running of the *skulker* programs during system initialization. This increases initialization time by about five minutes.

Method: In the file */etc/rc* add the lines:

```
echo Running SKULKER
/priv/skulker
```

immediately before:

```
echo Normal startup completed.
```

Somebody Else Messing With Your Files?

Problem: A user who fails to logout makes the terminal available to other persons who may not be authorized to gain access to the terminal and to all the files. .

Solution: Set up the terminal so that it will automatically log out any user who fails to strike a key on the terminal keyboard for a specified number of minutes.

Method: Include a timeout command in the */etc/environment* file such as:

```
TIMEOUT = 10
```

This is the number of minutes the keyboard may be inactive before automatic logoff will occur. Any number may be specified.

Funny Faces In Your File?

Problem: Files transferred between DOS and PC/IX end up with a "smiley face" character at the end of each line. This happens because of the different ways of specifying carriage return and line feed. DOS uses two characters at the end of each line of an ascii file to represent a carriage return and a line feed (015 and 012 respectively) whereas PC/IX uses only one (012). When a DOS file is transferred to PC/IX, the superfluous function key on each line is displayed as a "smiley face" character.

Solution: Execute the following shell to remove them.

Method: Put the following shell in your */usr/bin* directory with a mode of 555:

```
# fixdos by Ron Hecox, G613, 6005s November 1984
# Repairs DOS files so that they are PC/IX compatible.
rpl "" "" ¦ tr "\015" "\012" < $1 > $1.t
sed -e "/^\$/d" < $1.t > $1.nu
rm $1.t
echo "The DOS file $1 is repaired and is called $1.nu"
exit
```

Printing Wide Text?

Problem: When you print a file that is wider than 80 characters on a standard printer, only the first 80 characters of each line will be printed.

Solution: Set the line printer default line width to 132 instead of 80. (Proper commands must still be inserted in the file to control the IBM Graphics printer when printout of 132 characters is desired.)

Method: Change the file */etc/rc* to read as follows:

```
# Set defaults on /dev/lp if the system has a parallel line
printer.
splp indent = 0 width = 132
```

Editor Losing Your Files?

Problem: On very large files, (2,000 to 3,000 lines), the INed editor has been known to exit and automatically re-invoke itself without any file saves. This happens when using the "insert key" (F4) or the "put down key" (F6).

Solution: Keep your files small.

Method: Split large files into smaller parts for editing and then concatenate them back together for processing.

Time Getting In Your Way?

Problem: The current time is automatically displayed every hour. Many users find it annoying to have the time suddenly displayed in the middle of their work.

Solution: Turn off the automatic display of the current time. Use the *date* command if you need to display the time.

Method: In the file */usr/lib/crontab* insert a # and a space before the date display command so it will be treated as a comment as follows:

```
# 0 * * * * exec echo "The hour is" 'date'. > /dev/console &
```

Cyrillic Display Problems?

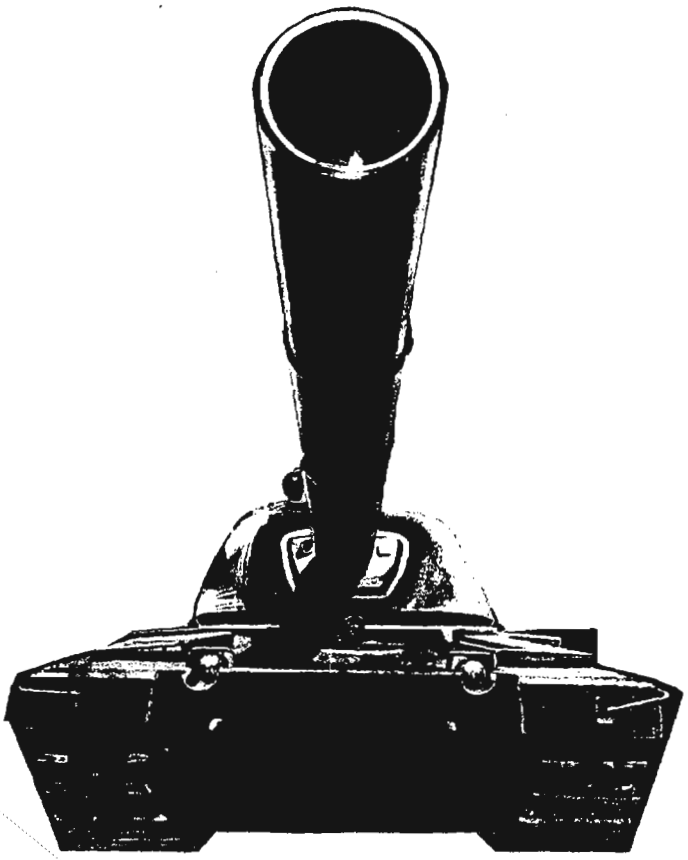
Problem: You have a USI graphics monitor on your ASTW and try to display Cyrillic text, but the characters display only halfway. In addition, when you try hitting the *language* key to turn it off nothing happens. This is because the character maps for the monochrome display and the color displays are different. The PC/IX system comes configured for a monochrome monitor while the USI monitor is, in reality, a color monitor with sixteen shades of green.

Solution: Your system files must be reset to identify it as a color monitor and require downloading of the correct character map for your display.

Method: In the file */etc/rc* comment out the 'mono.map' statement and uncomment the 'color.map' statement so it reads as follows:

```
# Uncomment only ONE of the following:
/priv/charam -a /etc/color.map
# /priv/charam /etc/mono.map
```


~~FOR OFFICIAL USE ONLY~~



EO 1.4.(c)
P.L. 86-36

P.L. 86-36

...AND THERE WE WERE! (u)

[redacted] G111

EO 1.4.(c)
P.L. 86-36

~~(C)~~ It's 1963. I have about four weeks to go on an 18-month tour [redacted] As usual, when our bunch finishes a six-day stint on duty in the boondocks, we hop on the bus [redacted] for a break of two or three days. As we approach [redacted] on the main road, we notice tanks on both sides of the highway.

(U) Well, that even happens at home on Armed Forces day; maybe it's just a parade.

(U) Wait a minute -- the turrets are turning, keeping pace with the bus. Holy Smoke! (Or words to that effect.) There's a roadblock ahead with armed troops! It must be the (then) annual attempted takeover of the national government by a disgruntled officer corps.

~~(C)~~ All of us are in civilian clothes, except for "Monte," who had arrived only three days ago and whose civvies hadn't. We're at the roadblock now and I see a [redacted] Second Lieutenant step out from behind the barricade and motion for the bus door to be opened. His six troops train their weapons on the driver.

~~(C)~~ Where the thought came from I don't know to this day. If necessity is the mother of invention, desperation is its father. I tell Monte to take out a stick of gum, fold the solver-colored wrapper into a small rectangle, and place it in his fatigue cap. Rising to his full six feet seven inches, he confronts the [redacted] Second Lieutenant with all the bluster he can summon up.

~~(C)~~ Having all his life been accustomed to social classes and ranks, the [redacted] officer backs down from the American "first lieutenant's" silver bar and allows said "lieutenant" to pass the roadblock [redacted]

~~(C)~~ Before our break is over, the disaffected troops have been arrested, the tanks have been removed, and we notice, as we ride back out [redacted] for another six-day stint, that you can't even tell that there was a roadblock right over there, just the other day. □

EO 1.4.(c)
P.L. 86-36

OCID: 4019702

P.L. 86-36
~~SECRET~~ 1.4.(c)

Saga of [redacted] Stretch (u)

This article is classified ~~S-CCO~~ in its entirety

golden oldie

It started in September
of seventy four.

Perhaps a few days sooner,
or a few days more.

The minds of these men
were in an awful state

Over the absence
of certain vital real estate

[redacted]

And certain information
for their leaders could fetch.

And ideas flowed
as if poured from a flask.

Their critics were numerous
and soon did emege,

And chanted a chorus of doom
to the tune of a dirge.

But our players pressed onward
not knowing when to quit.

Their minds were tormented
as if by a fit.

If our saga were written
from the Wayside Inn

To historic events
these words would seem akin,

"One if by land,
and two if by sea."

Three if by air
is the alternative key.

Our players did travel
from coast to coast

Seeking solutions to problems
that bothered them most.

Certain of these men
put their careers on the line

And a possible approach
they did finally define.

Then the champions emerged
to cry it out

To overcome resistance, opposition,
apathy and doubt.

A Jerry named Kozlowski
a Light Colonel called Reed

P.L. 86-36
EO 1.4.(c)

Gave answers to questions
and nourished the seed.

They called for support
from their Can Do team

The responses were varied
or so it did seem.

But the players did gather
from the ends of the earth,

And the mother of invention
to a baby gave birth.

They would steal all the assets
from the Compass called Bright

And gather in funds
from any program in sight.

There was talk of assassination
below the third floor

Of the Pentagon palace,
the Joint was now sore.

But strength nourished by faith
over what had already been done

Helped overcome doubt
and the first battle was won.

Then a schedule was established
by the heads of state

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

DOCID: 4019702

And a tempo was set
that most players would hate.

A meeting was called
In Virginia's Falls Church

For a forty-five day miracle
our players did search.

Colonel Reed started the proceedings
and spelled out the plan,

Sweet Old Bill rose to the occasion
with the answer "We can,"

Followed by Lloyd
who said what he'd do

To make the dream of this project
if at all possible come true.

The "Skunk Works" was called on
to reconfigure a deuce

And Bob Farley
would give the program the juice

Then we returned to our locations
and started to go

Though the dollars were short
for funding was slow.

Finally in November
we got our full start

From the ninth day and onward
we'd from sanity depart

There was hardware to build
and parts to procure

Inventions to make
and GFE to appear

On a cold night in December
for the Coast we did head,

The airborne equipment
was finally put to bed.

Then the search for the tower
did not seem to bear fruit.

We built them another
with a job-crane to boot.

The airlift was kept busy
on the way to both coasts,

The men worked with their heads down
without any boasts.

The days stretched into nights
and then into days,

They worked on without failing
their minds in a haze.

Then on to flight test
at Andrews and Meade.

The work pressed on forward,
this crew would succeed.

After some disappointments
and a time to stand down,

The crew assembled again,
this time they'd never give ground.

Finally a successful conclusion
all objectives were met.

The vict'ry celebrations
were more than a sure bet.

Then stand down again
until time to deploy.

The legal maneuvering
brought few people joy.

They painted the airplane,
and painted again

To please all the Generals
was a task Herculean.

Then the word went on forward,
we're ready to go.

There were few who weren't anxious
to start the big show.

The effort seemed worth it
the Team made a score.

There's work still to be done,
there's no denying that

But we're all very anxious
for our next turn at bat.

It's great to be part
of the Can Do team

There's nothing we can't handle
or so it would seem.

P.L. 86-36

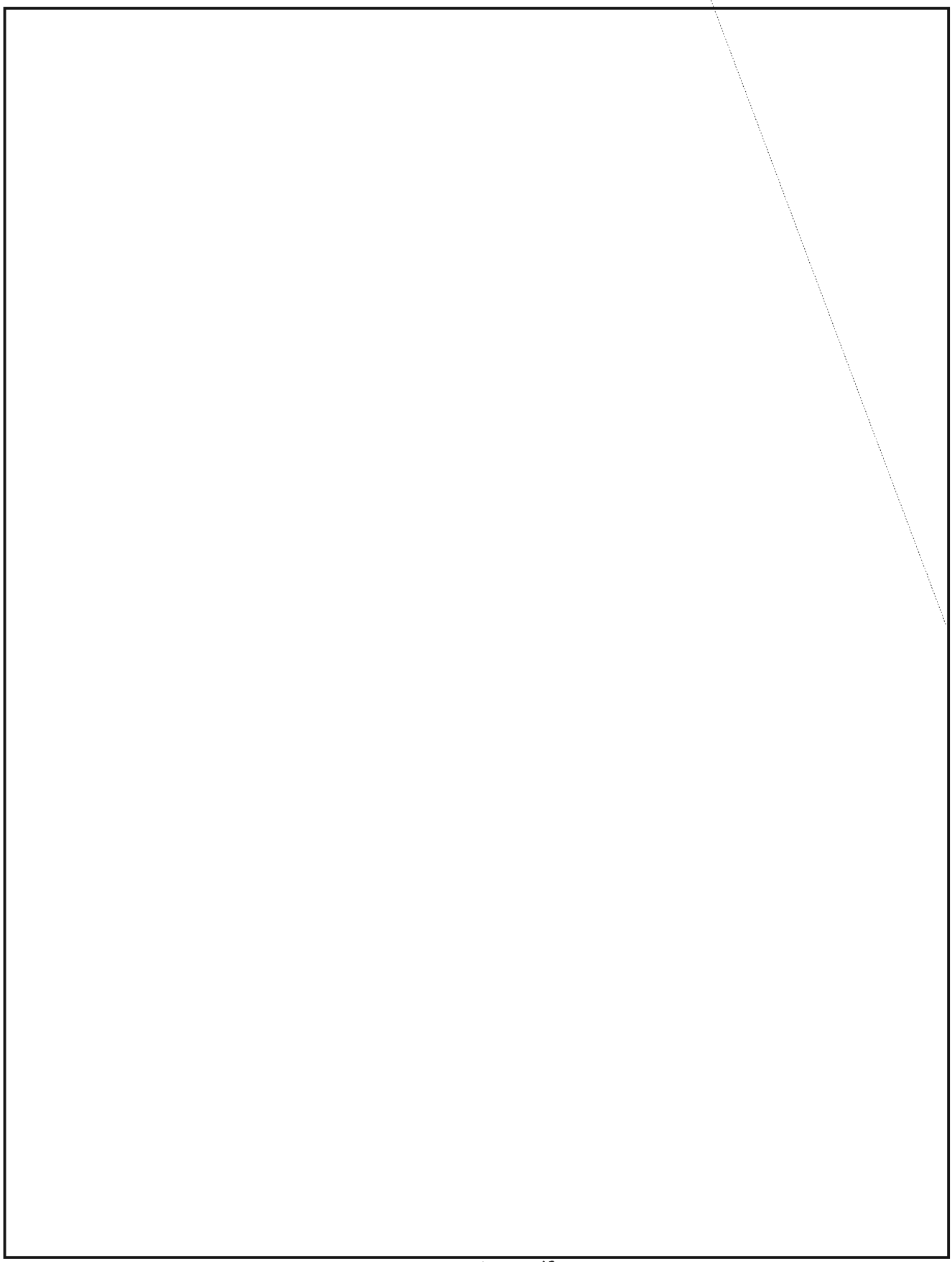
P.L. 86-36
EO 1.4.(c)

[redacted]

A conventional account of [redacted] appeared in the Spring 1976 issue of The Cryptologic SPECTRUM

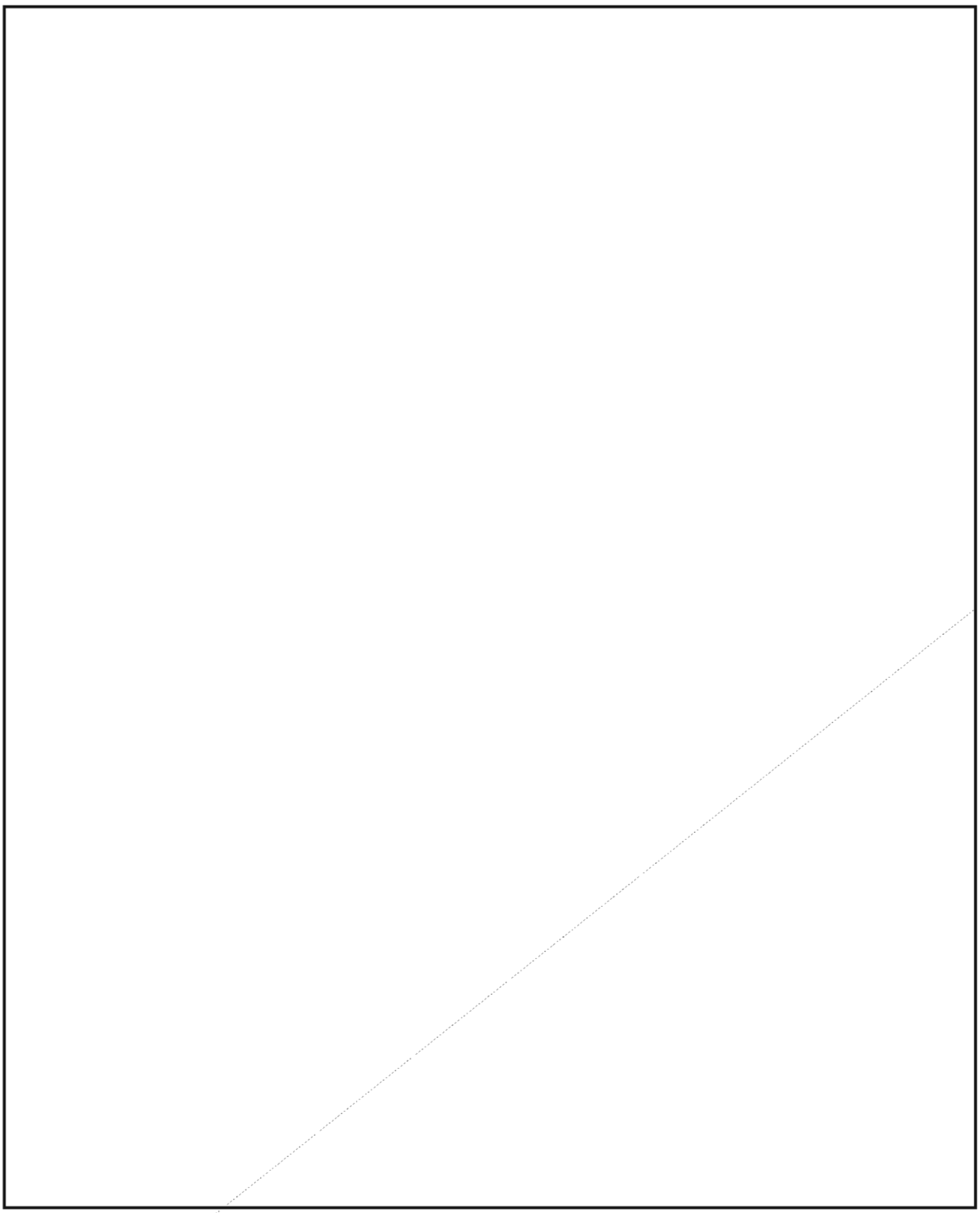
DOCID: 4019702

P.L. 86-36



~~FOR OFFICIAL USE ONLY~~

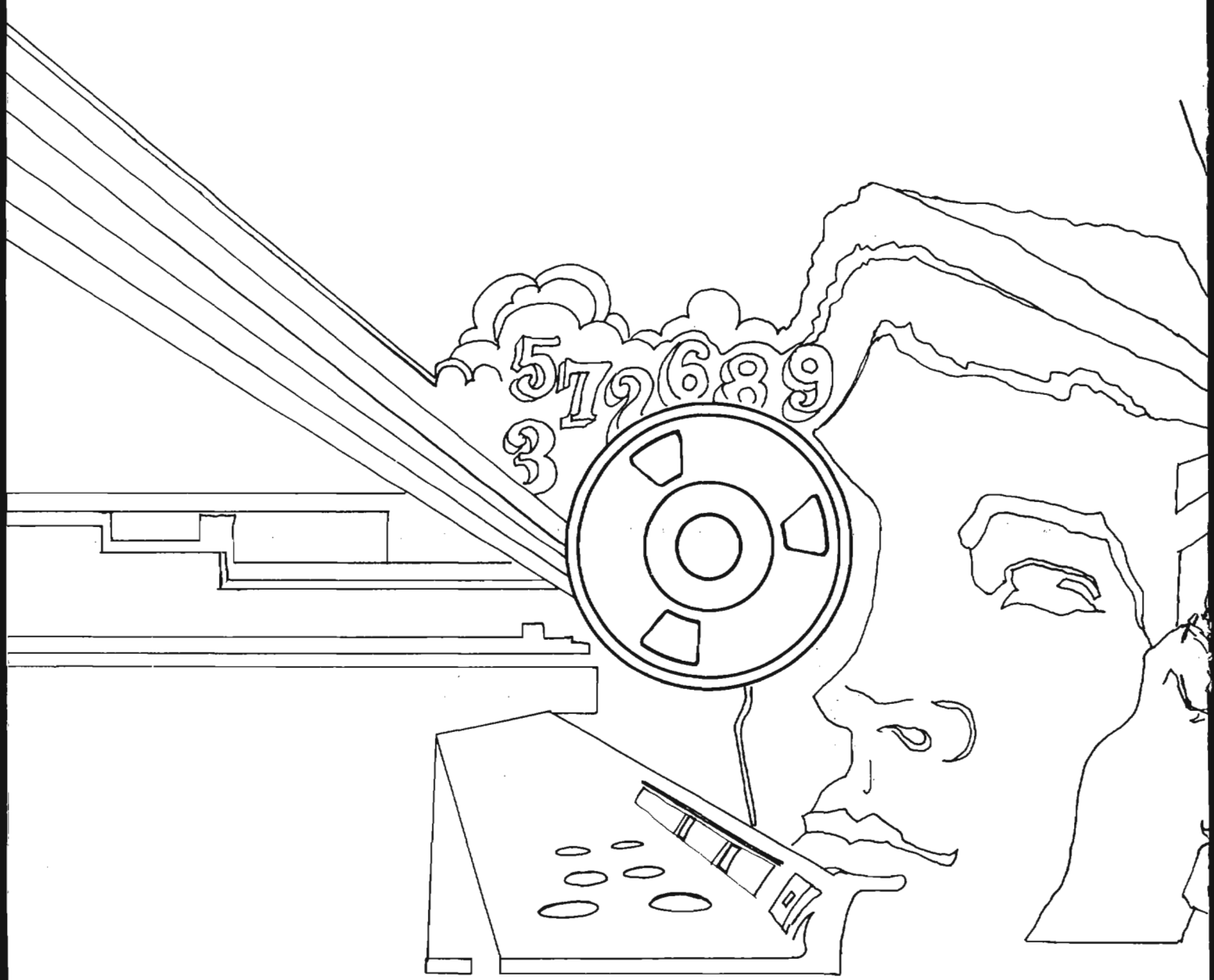
DOCID: 4019702



P.L. 86-36

Pl-Sep 85-Yl-84397

~~FOR OFFICIAL USE ONLY~~


5 7 2 6 8 9
3

DOCID: 4009937 P.L. 86-36

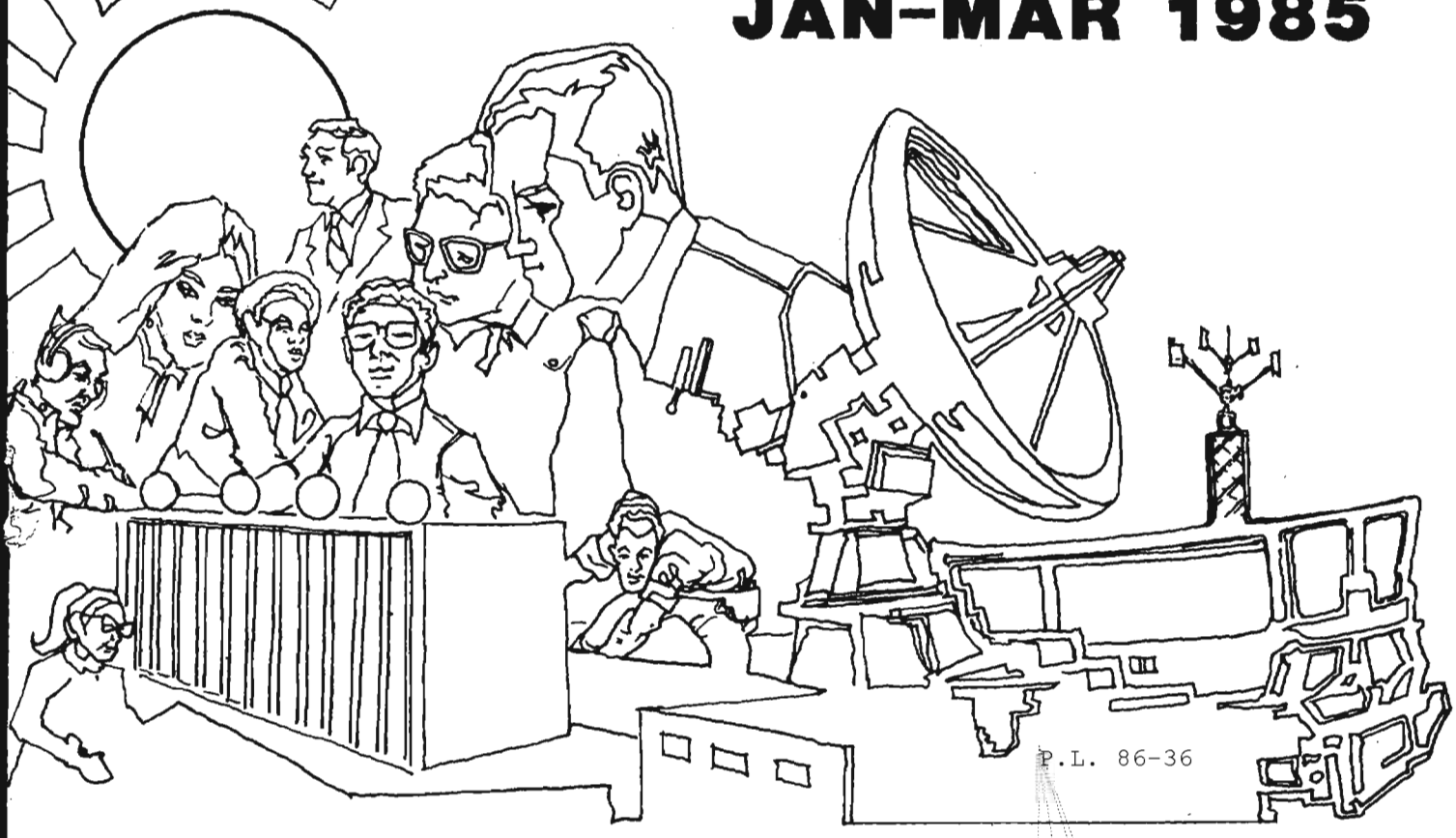
~~TOP SECRET~~

G51 [redacted]

TIONAL SECURITY AGENCY
T GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JAN-MAR 1985



P.L. 86-36

VIDEO TELECONFERENCING (U)..... [redacted] 1
LETTER TO THE EDITOR (U).....4
A MESSAGE TO CRYPTANALYSTS EVERYWHERE (U).....'THE MAD HATTER'.....5
I WOULDN'T HAVE MISSED IT FOR THE WORLD! (U)....Mary Ann Harrison.....6
SHELL GAME (U).....W.E.S.....8
BOOK REVIEW:
EASE MY SORROWS (U)..... [redacted] 9
BULLETIN BOARD (U).....13
A NOTE ON IMPROVING CRYPTOLOGIC RESEARCH (U)....Nathaniel C. Gerson.....14
FOOD FOR THOUGHT (U).....15
A TRAVELER'S TALE (U)..... [redacted] 16
TYME SHELL (U)..... [redacted] 17
ON EXCELLENCE (U).....18
FROM THE PAST (U).....19
NSA-CROSTIC NO. 60 (U).....D.H.W.....20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009937

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XII, No. 1-3 JANUARY-MARCH 1985

PUBLISHER [redacted]

BOARD OF EDITORS

Editor..... [redacted] (963-1103s)
Production..... [redacted] (963-3369s)

Collection..... [redacted] (963-3961s)
Computer Security
..... [redacted] (968-8242s)
Computer Systems.... [redacted] (963-1103s)
Cryptanalysis..... [redacted] (963-4740s)
Cryptolinguistics... [redacted] (963-1911s)
Information Science
..... [redacted] (963-5711s)
Intelligence Research
..... [redacted] (963-3095s)
Language... [redacted] (963-5151s)
Linguistics. [redacted] (963-3896s)
Mathematics... [redacted] (963-5655s)
Puzzles.....David H. Williams (963-1103s)
Science and Technology
..... [redacted] (963-4423s)
Special Research.....Vera R. Filby (968-8014s)
Traffic Analysis..Robert J. Hanyok (963-3888s)

For subscriptions
send name and organization
to: [redacted] P14

P.L. 86-36

To submit articles or letters
by mail, send to: P1, Cryptolog

via PLATFORM mail, send to:
cryptolg at barlc05
(bar-one-c-zero-five)
(note: no '0' in 'log')

Contents of Cryptolog should not be reproduced or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

[redacted] retired on 31 December. During his stewardship as Editor he brought CRYPTOLOG into the contemporary world of word processors and electronic mail. He started with the UNIX system, then wrote innumerable shells specifically designed to do CRYPTOLOG layout. There are commands for the columnar format, for paragraphing with appropriate classification, for indented inserts, for "bullets," and for many other editing chores. There's a clever routine that allows the editor to make comments to the author via footnotes that do not disrupt the text. And there are even commands which automatically go in effect at specified off hours to execute the nroff-type shells for printing CRYPTOLOG.

As a dyed-in-the-wool problem solver, Wayne also tackled the minor annoyances endemic to any computer system. He did this by writing many useful shells to smooth the way for the general UNIX user, and published them in CRYPTOLOG. An example of this type appears elsewhere in these pages.

Access to electronic mail has been a special boon to one set of people, that is, contributors in the field. By courier mail, whether air or surface, turn-around time for the usual sequence of submission, comment, review, etc., is too long to be practicable. Now, field contributors can get their articles to CRYPTOLOG via electronic mail faster than HQ people do using internal Agency mail!

Thanks, Wayne, and the very best to you from all of us.

Vg

~~FOR OFFICIAL USE ONLY~~

VIDEO TELECONFERENCING:

can it increase

SIGINT productivity? (u)

P.L. 86-36

[redacted] **P11**

(U) Point-to-point video communication is clearly the next step on the road to teleportation ("Beam me down, Scotty"). Once face-to-face visual exchanges become routine, only the olfactory and tactile senses will remain to be remoted. Neither of these has wide usage in legally approved business transactions.

~~(C)~~ The increasing use of point-to-point video in the commercial world makes it important that the SIGINT community get some experience with this type of communications facility in order to make an informed assessment of its applicability to SIGINT operations. The question then becomes: can facilities of this type in fact increase productivity and the effectiveness of operations between NSA HQ and field units? To answer this question, P1 and T4 are jointly conducting a series of tests [redacted] the aim of which is to give a broad spectrum of working-level personnel, both at NSA and overseas, a chance to use video communications in actual operational exchanges.

~~(FOUO)~~ The following is a discussion of current technology and commercial applications of video telecommunications, and the results to date of the P1/T4 tests.

BACKGROUND

(U) Because of the pervasiveness of mass-media television, system designers and potential video telecommunications users in the business world have tended to focus on full-motion commercial television technology. But bandwidth requirements and dollar costs severely limit its use. Even with state-of-the-art image compression techniques, normal TV bandwidth of 45 megabits (Mbits) can be reduced to only 1.5 Mbits, or, reportedly, to 750 kilobits (kbits). Equipment costs per node with a fairly modest studio will run from $500k to $750k, that is, $1M-$1.5M for each two-station link. Space requirements, servicing, and management overhead add further direct and indirect costs. Annual communications costs for leasing fully dedicated channels bring total costs to an even larger figure.

(U) To avoid making this heavy capital investment, businesses are using AT&T video conference studio facilities. Cost for a half-hour video connection between New York and London is now $2000; between New York and Los Angeles $700. Only in a very small percentage of business transactions can such costs be justified. Further, even if the benefits of video conferencing are substantial, they are, for the most part, intangible. A using organization, therefore, must not only be large enough to pay the high costs, it must also be able to avoid close cost-benefit scrutiny. These facts effectively limit the user population for full-motion video facility to business officials at or near the chief executive officer level, to high-ranking government officials, and to defense-related applications of critical importance.

(U) Savings in travel costs are invariably cited by both video equipment manufacturers and by users of video conference facilities as the pay-off for video investment, but at a recent symposium on video teleconferencing it was generally agreed by participants who have actually used a video system that a great proportion of the trips "saved" would never have

been made in the first place. It was also noted that many of the high-level executives for whom full-motion video telecommunications facilities had been acquired found them inconvenient and an unsatisfactory substitute for person-to-person contact. Phantom travel savings are nevertheless put forward regularly by operational users of video systems to demonstrate, in terms acceptable to in-house cost control authorities, that value is being received for money spent.

(U) Another type of video technology with much lower investment and operating costs is freeze-frame video. It is being used increasingly by business organizations to link working-level technical specialists at widely separated sites. IBM, for example, has a 60-site worldwide network set up primarily to serve programmer personnel.

(U) In a freeze-frame system, instead of sending 30 image-frames per second, as is the case in full-motion video, single images are sent at intervals which are a function of the bandwidth used. For example, when a 9.6-kbit voice-grade circuit is used, successive uncompressed color images (512 x 240 pixels, 6-bit resolution) can be sent every 78 seconds; with 64 kbits, a new image can be transmitted approximately every 10 seconds; and with 200 kbits, a new image can be sent every 4.5 seconds. With image compression software, these times can be shortened substantially, or, from another point of view, the bandwidth needed for a given refresh rate can be, at minimum, cut in half.

(U) Commercial applications have geared freeze-frame sales and applications to the telephone channel bandwidth, 9.6 kbits or analog equivalent. The resulting 78-second refresh rate is not suited to the easy interactive exchange of visual information, so use of the freeze-frame video image transmissions facility has been mainly as a graphics adjunct to an audio conference.

~~(FOUO)~~ Relatively unexplored up to this time, but now under study in the P1/T4 tests, is the question of whether a system with a video refresh rate in the 4- to 12-second range can be used to advantage in a general-purpose audio-visual communications link between working-level personnel.

THE TEST PROGRAM: [redacted]

(U) The impetus for undertaking the test program was the well-recognized phenomenon that temporary duty (TDY) assignments at overseas locations by working-level personnel are typically followed by an increase in the effectiveness of cooperation between the home and overseas elements and also by an increase in the information content of post-TDY messages and phone conversations. This appears to be the case even where, prior to the TDY, personnel in the respective organizations have spoken together regularly on the secure phone. It has also long been a fact of operational life that TDY budgets often fail to stretch much beyond the requirements of the "Chiefs" and very high priority projects, with little left for working level "Indians." Further, for a variety of reasons, it is often impractical to take productive personnel off ongoing tasks for a one- or two-week TDY trip.

(U) A second motivation for the tests was a two-sided one: a desire (1) to avoid getting caught up in the high-tech hype which usually accompanies the appearance of a new technique and too often generates imaginary and expensive requirements for "gold-plated" systems; and (2) to ensure that operational and intellectual inertia does not prevent timely acquisition by the SIGINT community of video communications if, in fact, such support would be operationally useful and cost-effective.

(U) The initial aim of the test, therefore, is to find out whether some of the benefits of TDY visits can be obtained by a video conference facility. Obviously, the closest analog to TDY would be a full-motion video facility; and just as obviously, the economic and communications costs point to freeze-frame technology.

TEST DESIGN

~~(C)~~ Test equipment, test configuration, and test sites were chosen with the following in mind:

- [] low cost
- [] adaptability to normal office environment
- [] manageability of equipment by users
- [] ability to test several refresh rates
- [] availability of communications bandwidth (on a temporary loan) between NSA and the site
- [] limited space requirements
- [] mobility of equipment
- [] reliability of equipment
- [] distance between paired locations. [redacted] agreed to be the first test site.

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

DOCID: 4009937
E.O. 1.4. (b)
P.L. 86-36

(U) A simple (not compressed) freeze-frame video system in fairly wide use commercially was selected, with special options to allow operation at various refresh rates. Video bandwidth for the test was set at 192 kbits, and the audio bandwidths at 32 and 64 kbits. A special refresh-rate timing mechanism was incorporated in the equipment to allow examination of the usefulness/awkwardness of 40-second, 10-second, 6-second, and 4.5-second refresh rates. Test communications used bandwidths which had been installed and tested for operational projects but which had not yet come into full operational use.

~~(c)~~ The NSA mode shares a 11' x 20' area in P1 spaces, while the [redacted] mode occupied shared space in the mission conference room. The equipment, which is in wheeled cabinets, operates in a normal office environment, that is, without studio lighting or soundproofing, and needs no special technical services, so the conferees can manage the cameras and sound equipment themselves.

(U) The operational utility of the video system is likely to vary considerably from one application to another according to the type of conference, the numbers of people involved, and the conference skills and motivations of the participants. Each of following three types of video exchange requires separate consideration, so test participants are asked to conduct operational exchanges in each of them: 1) the stereotypic conference where two sides meet to iron out a problem; 2) a briefing or seminar format where one or more participants at one location make a presentation, with active questioning from the personnel at the other location; 3) a periodic assembly, similar to a staff meeting, of co-workers at the two locations to review matters of mutual interest.

PRELIMINARY FINDINGS

(U) a. In each of the above-mentioned types of video exchange, group-to-group communication is the key element; most one-on-one exchanges are adequately accommodated by secure telephone.

(U) b. In a normal office environment, discussing everyday work matters, and using video equipment of which they have hands-on control, conference participants to date have exhibited little of the stage-fright stiffness which vendors and commercial users of video systems have repeatedly mentioned as a major problem. It seems likely that the reported stiffness among commercial users is a side-effect of a studio atmosphere, which this test has carefully avoided, and/or of a slow refresh rate which might freeze for over a minute the picture of some person with tongue halfway out, or with eyeballs rolled; the faster refresh rate avoids extended displays of awkward postures.

(U) c. A pivotal question of interest in each type of conference has to do with a suitable image refresh rate. Looking to the possibility of standard operational deployment at major overseas sites, 32- or 64-kbit channels would be much more practical than 128- or 200-kbit channels. Preliminary results suggest that 4-second (192-kbit) and 6-second (128-kbit) refresh rates are not very different from a user's point of view; that a user can, with some difficulty, adapt to a 10-second (64-kbit) refresh rate, and that a 40-second (16-kbit) refresh rate is functionally more a facsimile system than a video system and is very awkward to use. A compression system, as noted above, could cut these rates in half.

(U) d. Audio quality sufficient to make the output of a speaker system easily intelligible to a group of conferees cannot be achieved at much less than 32 kbits.

(U) e. Allowing for a modest seating capacity, the minimum space requirement per node is 12' x 16'; group sessions of 8-12 people increase this requirement to 12' x 20'.

(U) f. The TDY savings to be realized from the use of video telecommunications are not likely to be large. The availability of a video link with a given station, can, however be viewed as a means of cushioning the adverse effects of a sharp cut in TDY funds for trips to that station.

(U) g. Loss of information attributable to the use of freeze-frame technology as opposed to full-motion technology has been minimal. When the refresh rate is either 4 or 6 seconds, there has been no apparent decrease of any significance in the usable (i.e. absorbable by the recipient) information-rate with respect to graphics. Also, with those refresh rates there has been no difficulty in establishing a well-defined personal "presence" for each participant in something very close to real time. Individual facial reactions and body language as well as local interactions between participants come across with only a mildly inconvenient delay. The nuances of facial expressions are of course lost.

(U) h. For the purposes of working-level exchanges, therefore, there appears to be little difference between the usable information carried by a full-motion video system and that carried by a quick-refresh freeze-frame system. If that perception is correct, there

are very few circumstances in which cost-benefit factors could justify paying the high costs of a full-motion video on long-distance links.

PROBLEMS IN MAKING ASSESSMENTS

(U) Reaching an objective conclusion about video cost-effectiveness is particularly difficult because the main advantages of video telecommunications are neither directly or discretely measurable. One typical test participant said, "This is great. I can't cite specific savings, but I can now show my workers who have never had a chance to visit this station exactly how the material they work with is acquired and processed in the field. They, and, in fact I myself, now have a much better idea of how this whole system operates." Based on that type of reaction, one observer might conclude that the video link is nice-to-have but not demonstrably cost-effective; another might claim that the pace of production and coordination tasks between the NSA and the field will increase enough to justify the costs of video communications.

(U) The basic problem is identifying what might or might not have happened if the video conference facility had not been used. It is likely that the best measure of cost-effectiveness will be an informed estimate by individual conferees of the length of time required to achieve an equivalent coordination of ideas between the conferring parties. User guesstimates, so far, have ranged from zero to two months. One to two weeks seems to be a figure of merit.

(U) Another problem which will make it hard for the community to reach an agreed-upon assessment of cost-effectiveness is the fact that a great many people (no correlation with grade-level discernible) have made up their minds either for or against the desirability or feasibility of video telecommunications before actually seeing it in operation. Some are convinced that video telecommunication is the overdue solution to a host of problems which have long plagued efforts to coordinate operations between NSA HQ and field units. Others are equally certain that video communications are a nice-to-have gimmick which can never justify the use of the communications bandwidth required ("Do you know how many 'grey lines' that is equal to?"). Still others take the position that as a means of sending graphics in support of an audio conference, a video system would be a great help, but that sending pictures of people would serve no real purpose. Since there is a full range of a priori opinions, someone must have it right, and, just as surely, the rest are in some degree wrong. The test series will, at minimum, narrow the area of disagreement.

PRESENT STATUS

~~(C)~~ At the time of this writing, tests with [redacted] are in progress. Present plans are to begin a 60-day test [redacted] in late February, and thereafter to shift the equipment to a site of a Service Cryptologic Element for the final test phase. A report summarizing test results will be published shortly thereafter. The report, together with the experience gained, should furnish a sound basis for decisions by the operating elements about whether to program or not to program for video telecommunications support.

EO 1.4.(c)
P.L. 86-36

Letter to the Editor

What a delight to read [redacted] *editorial!!!! To read that THE computer wizard was "thinking of ordering another file cabinet" gave me a good chuckle.*

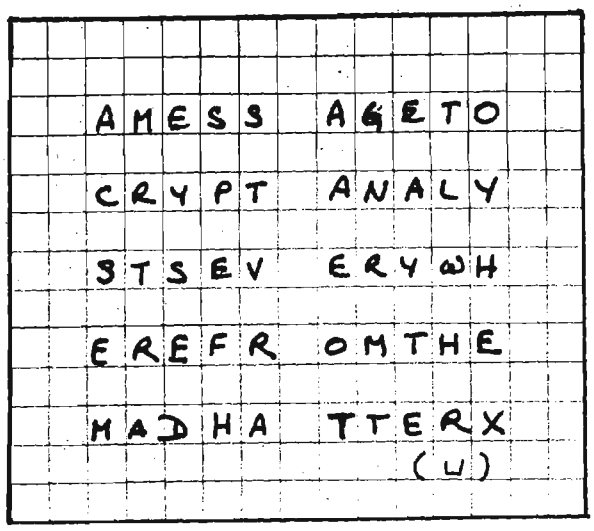
Thanks, [redacted] *for making those of us who are definitely less-than-computer-wizards feel a little better about the abuse we receive from those inanimate objects, be they hardware, software, connectors, or whatever.*

Mr. Sawyer's and [redacted] *articles were also excellent and too true.*

Thanks for a fine issue of CRYPTOLOG.

[redacted] *B12*

P.L. 86-36



~~(FOUO)~~ MADCAPS is here at last! It's a continuing project to assist cryptanalysts working on manual systems. The purpose is to collect, document, organize, and invent diagnostic programs, and to make them available on supercomputers and on Agency Standard Terminal Workstations. The project, though informal, is blessed by upper management, and is staffed by a steering committee, a working group, and cryptanalysts at large:

[] steering committee = TOPCAPS = will provide continuity;

[] members of the working group = MADCAPS = will be assigned for short tours from various offices throughout DDO.

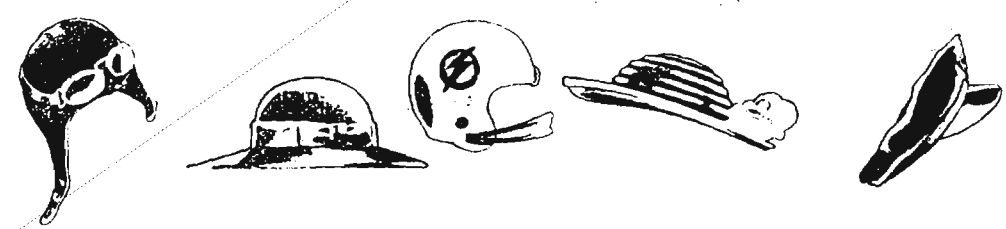
[] cryptanalysts at large = THINKING CAPS = That's you!

(U) Among the services that MADCAPS will be providing are: supporting the DPP in the TCAP main tube room; assisting users personally; developing a training course in conjunction with the NCS; and holding tea parties (seminars) for programmers.

(U) So, THINKING CAPS, let the MAD HATTER hear from you after you have tried these programs. As the MAD HATTER refuses to be identified, send your comments to the CRYPTOLOG editor; she has agreed to give space for this exchange and to act as intermediary pro tem.

(U) Is there a cryptanalyst around who likes to write and is willing to take on the CRYPTOLOG exchange?

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

I Wouldn't Have Missed It for the World!

(u)

Thoughts on the Senior Executive Fellows Program, John F. Kennedy School of Government, Harvard University, September-December 1984

Mary Ann Harrison, A67

(U) The Senior Executive Fellows (SEF) Program is designed to provide training for high-level managers in public sector organizations, to assist them in improving their management skills and techniques, and to add to their understanding of the issues and institutions which shape the governmental working environment. The program's major goals, to quote from a Kennedy School brochure, are:

* To challenge participants to step out of their prior professional identities and to think concretely and analytically about themselves as executives;

* To expose them to historical, institutional, and thematic perspectives that will deepen their knowledge and understanding of the public manager's larger operating environment;

* To train them in essential cognitive and behavioral skills that will enable them to operate more efficiently and effectively;

* To encourage them to reexamine old assumptions and to assess their attitudes, values, and beliefs in light of new and increased public responsibilities;

* To inspire them with a sense of pride and confidence in the practice of their profession, through an awareness that public management demands the best efforts of talented people, that it is socially important and personally rewarding.

(U) The thirteen weeks I spent in the program this past fall convinced me that, in all respects, the Kennedy School has overfulfilled its plan.

(U) Our SEF class comprised forty students; we represented two state governments and more than 25 federal departments. The Kennedy School provided apartments for us (save for two Army men who were there as part of another program and were required to find accommodations on their own) and meals were furnished on most days. Many of the books used in class are ours to keep; other books could be purchased, usually at discount, at one of the many excellent bookstores in the Cambridge area. (It is said that, outside of buildings belonging to Harvard, all buildings in Cambridge are either clothing stores, book stores, or restaurants; some seem to be all three at once!)

(U) Our class spent two hour-and-a-half sessions with an internationally known authority on the art of negotiation, a man who helped hammer out the Camp David accord between Begin and Sadat. We had ten hour-and-a-half sessions on leadership with a man who is a psychiatrist, musician, philosopher, and a highly creative teacher. We examined the attack on the Marine barracks in Lebanon with the only civilian to serve on the Long Commission, which investigated that tragedy. We also studied:

* micro- and macro-economics;

* the uses and misuses of statistics;

* the whys and wherefores of computers and management information systems;

* how to deal with the press;

* how to deal with lawyers;

* what makes McDonald's more successful than

Burger King;

* the Richard Helms perjury trial;

* how to organize a public service organization so that it truly does serve the public;

* the features of the "Japanese management style" that perhaps could/should be adopted by U.S. business;

* the relationship between the Executive and Legislative branches;

* the growth of Presidential staffs and their influence;

* the effect on world politics and economics of multinational corporations;

* crisis management, using the Cuban Missile Crisis as an example;

* competition and regulation in U.S. business;

* decision analysis: what it is and how to do it.

We also discussed our own strengths and weaknesses as managers and what it means to manage in the public sector. This list includes only the highlights of our studies; I hope it gives some idea of the diversity of the program.

(U) The predominant method of instruction was the case method, "a teaching technique which requires a high level of involvement by participants." The brochure goes on to say:

> The success of case teaching depends upon the full participation of each class member and demands thoughtful analysis and active contribution to class discussion...the entire class explores the case under the guidance of the instructor. Typically there is no "right" answer; participants must be ready to defend their analyses and conclusions against the total experience of the class. The instructor serves as catalyst, devil's advocate, and moderator in leading the class through the analysis to a workable solution. Analysis of real problems and learning by vicarious experience are the essence of the case method. It puts the burden of learning on the participant, who gains a new level of understanding of the complexity of public decisions.

(U) Although the size of the class precluded as much dialogue as many of us would have liked, the intellectual exchanges were usually lively and interesting.

(U) For the first hour of each day we met in groups of eight, to discuss the day's cases and to experiment with the dynamics of small-group decision making. Each of us gave his or her own case study during the semester, typically a description of a management problem each of us was facing in our own jobs, with the hope of eliciting suggestions and solutions from our seven "groupmates."

(U) Shortly before Thanksgiving the SEFers were assigned in pairs to work with small groups of first-year graduate students in an exercise on cutting the food stamp program. The groups were responsible for creating a briefing book proposing alternative ways to reduce the food stamps budget, with recommendations for action. They then briefed a present or former Health and Human Services official involved with food stamps. This exercise was, for me, one of the highlights of the semester.

(U) After the conclusion of the food stamps project, several graduate students asked some of the SEFers to participate with them in a seminar on the ethics of the workplace. "To Resign or Work Within" was the topic, what to do when you are instructed to do something that runs counter to your personal sense of right and wrong. The discussion was interesting and exciting; I hope the graduate students got as much out of it as the SEFers did.

(U) The official SEF program ran from 8:00 to 12:00, five days a week and most Saturdays. Afternoons were open for the SEFers to audit any course they chose, graduate or undergraduate, at Harvard (Kennedy School, Business School, Law School, etc., anywhere the professor allowed auditors), Radcliffe, Massachusetts Institute of Technology. I audited two courses: Communications and Information in Foreign Policy; and Current Issues in American Foreign Policy: Managing the Superpower Relationship. Some of my classmates audited courses in psychology, Japanese history, poetry, computer science, even one very unusual class entitled The Beast in Literature!

(U) Fellows of the Institute of Politics held weekly seminars on such disparate subjects as the future of liberalism, the Arab-Israeli conflict, the contemporary right, social welfare policy in the 80's, and criminal justice. They were informal meetings; one could simply drop in on whatever session sounded interesting that particular week. The caliber of guest speakers is indicated by the fact that the liberalism seminar heard from the former Prime Minister of Canada, Pierre Elliott Trudeau, and from David Steel, Leader of the British Liberal Party.

(U) The SEFers also had occasional dinner guests, people who were scheduled by the SEF program coordinators, or who were suggested by us, the students, as interesting folks who had something to share with our classmates. Included in this group were an expert on the Far East who had some fascinating information about the origin and development of the Chinese civil service; a witty refugee from the Harvard Business School who talked about management information systems; and one of the leaders of the foreign policy seminar who gave his thoughts on what's ahead for the second Reagan administration.

(U) Speakers at the Kennedy School Forum included Zbigniew Brzezinski, Daniel Yankelovich oi Yankelovich, Skelly and Wright, and J. Peter Grace of the Grace Commission. These seminars were open to all, and if you didn't claim a seat by 7 o'clock (for an 8 o'clock speaker) there was standing room only!

(U) As members of the SEF program, we received Harvard Student Cards which entitled us to use all Harvard facilities - libraries, gymnasiums, swimming pool, theaters, museums, etc. Some of my classmates learned how to row (crew? scull?) and renewed their swimming skills as they retrieved themselves from the Charles River after their boats capsized!

(U) Much of what I learned in the SEF program can be applied at once: how to be a better manager, how to be a better subordinate. Some of my newly acquired knowledge probably won't come into service until later: how to design organizational strategy, how to marshall resources and support. But all of the SEF experience is an important and valuable part of my professional "tools of the trade."

(U) I envy the next NSAer who becomes an SEFer. I'd like to do it all over again!

SOLUTION TO NSA-CROSTIC No. 58

[redacted] "The Islamic Time Bomb," CRYPTOLOG, December 1983

"What are the objectives of the new Islamic revolution?

"The elimination of undesirable or immoral behavior such as gambling, [drunkenness,] prostitution, pornography, and corruption;

"The conformity of secular law with Islamic law; and

"The establishment of Islamic governments."

Shell Game (w)

WES

(U) The other day, I got a note from a reader over the network titled "Asleep At The Switch," apologizing for not having answered a message I had sent him. I had sent the message to his personal account, but he was in the habit of logging in to the group account on his host computer and so hadn't seen my message for several days. That's a common problem when people have group accounts as well as personal accounts.

(U) This magazine is done on a group account, and it is easy to forget to check for mail in one's other account. For that reason, we have set up the file that runs automatically whenever you log in called ".profile" so that it checks for mail in the companion accounts. For example, the ".profile" for CRYPTOLOG's group account looks something like this:

```
if -s /u6/wes/.mail then
        = b 'There is '
else
        = b 'No '
endif
if -s /u2/hes/.mail then
        = c 'There is '
else
        = c 'No '
endif
pump
        $b mail for wes
        $c mail for hes
!
```

(U) Over on my personal account, the .profile contains similar instructions to check the mail file in CRYPTOLOG's group account.

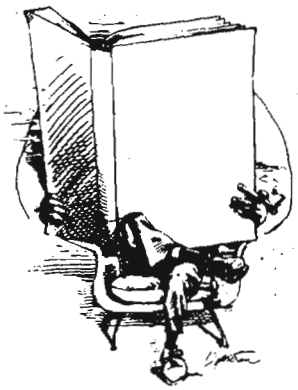
(U) We have learned to put this command at the end of the .profile, so that it is one of the last things to come up onto the screen after logging in. That way, a long "message of the day" doesn't push this mail notice off the screen.

(U) By the way, if you ever need another look at that "message of the day" it is always available with:

```
cat /etc/motd
```


P.L. 86-36

DOCID: 4009937



BOOK REVIEW

(u)

P.L. 86-36

[redacted] **P13**

P.L. 86-36
EO 1.4.(c)

Review:
Ease My Sorrows
by Lev Kopelev
Random House, NY, 1983

~~(TSC)~~ In early 1950 Alexander Solzhenitsyn was abruptly transferred out of a job of evaluating the intelligibility and security of Soviet analog telephone scramblers, to a dull mathematical job in cryptographic design, because he had proved that a voice scrambler designed by the KGB head of the research lab was the worst of the candidate cipher machines. After that the evaluation work fell apart, with profound results for the USSR [redacted]

(U) Lev Kopelev was the linguist in a small three man team, including Solzhenitsyn and the engineer Dmitri Panin, who had pioneered in Soviet work in speech analysis, building their own sonogram, and developing new equipment, concepts and techniques for the analysis of Russian speech. With the other two, he was imprisoned in a "sharashka," a high class prison for technical workers, in the Marfino suburbs of Moscow.

(U) In his book The First Circle, Solzhenitsyn first described the Soviet speech research and cryptography at "Mavrino." Kopelev was the character Rubin in that book. This new account illuminates many new aspects of the Marfino work and the prison life. Ironically, Solzhenitsyn has revised part of The First Circle (the voice recognition spy hunt) to conform more closely to Kopelev's account.

(U) The Marfino sharashka was housed in a former church with the name Ease My Sorrows, and run by the KGB (called MGB in 1950). All three men, and most of the other prisoners, had been convicted of violations of Article 58 which covered terrorism, espionage, sabotage, and other acts against the State [p.46]. Solzhenitsyn had been captured by the Germans. Kopelev had tried to restrain rape and pillage by troops under his command in Germany in 1945. Panin was arrested in 1940 for "conversations," and then sentenced while in a Russian prison in 1943 for "defeatist agitation." In these trials the accused was usually not present and had no right to defend himself. Kopelev, a Jew, had served with front line troops, and was an ardent Stalinist, even in prison.

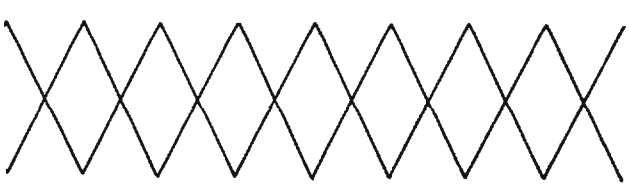
(U) There were numerous sharashkas, and they represented an idea that only Stalin could have thought up, where the political prisoners with special skills such as engineers, mathematicians, etc. could serve the state by conducting useful research. Airplanes, radars, and many other high technology products were designed and developed in the various sharashkas, where the conditions, though severe, were far better than the forced labor camps in Siberia, or the uranium mines. The prisoners, called "zeks" in prison slang (from a contraction z/k of zakliuchennyi), knew when they were well off, and worked with the greatest intensity to avoid being sent to a labor camp, where they would die. In the prison environment there was not much to take their minds off work and so Stalin got a maximum effort from these scarce scientific

resources. Tupolev, the aircraft designer, was arrested in 1938, worked in a sharashka, and was released in 1943.

(U) The sharashka at Marfino was engaged in speech engineering and encryption. In addition to the Russian zeks, there were German POW's, many of whom were very gifted and industrious, KGB administrators, such as Anton Mikhailovitch V. [Vasleyef], a KGB colonel, some Russian "free" workers, and various Germans, Czechs and Austrians who had been arrested and charged with espionage because the Soviet research programs apparently needed their skills.

~~(C)~~ Technology transfer was an important foundation for the lab's activity. The Philips lab in Berlin was dismantled and moved to Marfino. The technical library, a key element, was made up of Soviet technical books and of war spoils: German, British, French and American scientific journals [p.16]. This was augumented with linguistic books, and books of literature and poetry, which Kopelev said he needed for linguistic research, but actually valued for their culture and intellectual inspiration. An uncommon prison library.

~~(C)~~ Colonel Mikhailovitch supplied them with stacks of British and American journals on acoustics. Fletcher's Speech and Hearing was the foundation of their work. The published American work in spectrum analyzers was adapted by Kopelev, Panin, and Solzhenitsyn to create a visible speech recorder of their own [pp.50-51]. This single instrument played a crucial role in both speech recognition and cryptographic evaluation, but its potential was inevitably thwarted by the realities of prison existence.



(U) The basic idea of the speech scrambler was based on German and Allied wartime speech coding which split the voice channel into several subbands by filters, wrote these sub bands on a magnetic recording disc, and then picked them up in short segments of 150 milliseconds, with mixing of the time-frequency segments by a "coder." This signal was sent down a telephone line, and then decoded and reassembled at the receiving point. The KGB lab chief Anton Mikhailovitch V. (the prototype of Yakonov in The First Circle) originally spoke of absolute security for this system, in 1948 [p.35]. The zeks were promised rewards and early release if they succeeded, and some actually did get reprieves and big cash awards [p.140].

~~(C)~~ To provide a foundation for the work, Kopelev, Solzhenitsyn and Panin undertook new linguistic research, identifying Russian spoken syllables and their frequencies. From these data, they developed various methods of evaluating how well scramblers preserved the information bearing elements of speech. This linguistic work was a novelty compared with the "engineering" method of treating speech merely as a waveform. Kopelev tried to get his discoveries published in someone else's thesis, but various reorganizations of the sharashka led to the destruction of all his data, the breakup of the team, the discrediting of sonograph analysis, and a general frustration of all this important cryptologic work.

~~(C)~~ The top secret sonograph (phonoscopy) work was disbanded, and Kopelev and a few others were put under a major Federovitch K., who was a serious mathematician and engineer. The speech coders could be solved by intensive human effort, ranging from 120 to 600 minutes per minute of speech. Kopelev used sonograph pictures to decode the mosaic coded speech, and came to the conclusion that they could be quickly read by the Americans, with their better equipment [p.137]. A fellow zek warned them they were sawing off the branch they were sitting on, and would be sent to the mines if they showed that the sharashkas's work was worthless. KGB Major Federovitch decided that the mosaic coders were needed by the state, they were better than nothing, and prevented simple wiretapping, and the sonograph decoding could be done "only under laboratory conditions." He then sent Kopelev back to the acoustic lab, away from scrambler evaluation [p.138].

~~(C)~~ In addition to the analog "mosaic" coders, Kopelev also mentions a "superdependable 'impulse' coding" [p.155]. Since "coder"

DOCID: 4009937

means enciphering device, this implies that digitized speech encipherment was also being worked on at Marfino, but he does not elaborate. The impulse coding thwarted his attempts to recreate the characteristics of a voice.

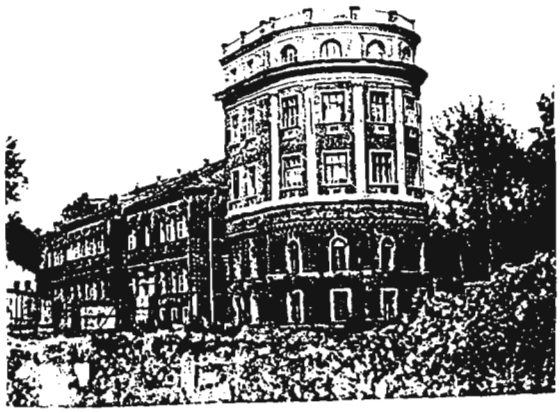
(U) Kopelev noted, in leaving the mathematics group, that all the desks were open--all surfaces in view--and every task precisely defined; you couldn't get sidetracked [p.138]. This strict environment apparently suited the KGB managers, who had arrived at their positions in charge of the cryptologic work by torture and assassination, but the zeks (who were the Soviet cryptologic technical track) were intellectuals and scientists who not only found this stultifying, but frustrating to their abilities and to the mission of the sharashka [pp.154,161].

(U) The sonogram that Panin, Kopelev and Solzhenitsyn developed was also applied to a spy hunt, in one of the illuminating episodes in the book. In the fall of 1949 a wiretap on the US embassy recorded a Soviet speaker trying to tell the Americans that a US scientist would shortly pass atomic secrets to a Soviet agent in New York [p.73]. The problem was to identify who made the telephone call. Several suspects had their conversations recorded, and Kopelev, who was best at reading the sound pictures, tried to identify the right suspect.

(U) A new secret sonogram laboratory was instantly established in the sharashka. The zeks had to take a secrecy oath, which authorized them to be shot without a trial [p.76]. Kopelev told Solzhenitsyn about the project, but Solzhenitsyn warned him not to tell anyone else. The zeks described the taped informer as a "bastard." Solzhenitsyn shared Kopelev's disgust with the man who called the Americans, and called him "bitch," "viper," "whore" and so on. When questioned, the informer, a Soviet foreign service official, denied calling the Embassy, but Kopelev and the other zeks had the satisfaction of helping the state convict him. They denounced him for giving away information about the atomic spy contact. The suspect had had all the advantages of Soviet life, and had been in Komsomol as well, with family Party connection. They despised him.

(U) It is hard to imagine Americans imprisoned for political crimes, (such as being POW'S) being such patriots in reinforcing the power of the police. [1]

(U) This counter-espionage success made the sonograph work important to the KGB, and the



The sharashka in Martino on the outskirts of Moscow, formerly the church, "Ease My Sorrows"

zeks were praised. Soon after new tapes arrived. Some Soviet Army tank repairmen had called the US embassy as a prank, pretending to have information to pass. A sergeant's notebook was found with some data about tanks and their state of repair and other military facts. The sergeant confessed, and said he was just trying to bluff the Americans. However, Kopelev discerned that three buddies were in the scheme, and that the man who confessed was not the one who had called the embassy. Realizing that the accused sergeant had behaved selflessly, taking all the blame to protect his buddies, Kopelev fudged his results. He could have exposed the truth, and gotten long sentences for three soldiers rather than one, and this would have confirmed the value of sonogram speaker identification, but he knew that evidence of a "collective" crime would be much harder on the men. The KGB supervisor Mikhailovitch was furious, because he had ballyhooed the sonograph discoveries, and then had no new success. This discredited the sonograph.

(U) In this second incident, Kopelev sympathized with the "spies," and protected them as well as he could, at the cost of discrediting his work, because he didn't think they were truly enemies of the Soviet state.

(U) When the sharashka was taken over by a new KGB officer in 1950, it was also transferred administratively from the MGB to the Directorate of the Central Committee of the Party [p.154]. To tidy up for the transfer, anything not included in the inventory that covered the transfer was ordered destroyed. This was a catastrophe for the project. Hundreds of thousands of irreplaceable foreign documents, and priceless equipment including a 70,000 Mark Zeiss microscope, were burned and smashed and thrown in a pit by the enthusiastic KGB staff. All Kopelev's sonographic data and research materials went. Zeks could no longer be authors or sign anything. Controls were tightened. [pp.151-4]

(U) In spite of his prison sentence and treatment, Kopelev remained a dedicated Stalinist, rationalizing even his own fate as historically inevitable. "We are on a train, bound for socialism, and only the stupid guards have put us in the prison car." His fellow zeks replied, "We are going nowhere, mired in shit, and you call it honey".

(U) Kopelev tried to defend Stalin's brutal policies and actions even after his death, but got heated arguments from other prisoners [p.224]. Gradually he concluded that the punitive actions of the NKVD, MGB, and OSO in the prison camps were senseless and useless, rather than part of a historical pattern. He began to think about God. He came to realize that Stalin had not been a major historical figure, because the system rejected his methods and henchmen and discredited his memory, almost before the corpse was cold.

(U) One of the most interesting points about the book is made in the foreword by Robert Kaiser, former Washington Post correspondent in Moscow, who knew Kopelev during his assignment. The Russian intellectuals began with the assumption that a reporter from as important an newspaper as the Post would not only speak Russian fluently (Kaiser's Russian was not bad), but would be familiar with all of Russian literature, and would know who all the key people in Russian intellectual life and publishing were. They were disappointed in this assumption, but still clung to the belief that at the least, the reporters and their wives would be completely familiar with all the important works in German literature, or at the very least, American literature. Alas! The Russian intellectuals knew not only all their own literature, but were taken aback when the Kaisers could not answer their searching questions about the meaning of this and that element of American literature. Kaiser remarked that Russian intellectuals "are serious about their work." [p.viii].

~~(C)~~ Therein may lay the key to Marfino and its gifted zeks. Kopelev, Solzhenitsyn, and many others were intensely educated people, who carried their passion for knowledge and intellectual endeavor into every situation. Kopelev, the loyal Stalinist, tried to rationalize the whole prison system and his own treatment as historically inevitable. Solzhenitsyn attacked the gulag system, and the whole Soviet state, as an outrage against democracy and the Russian people. Inside Marfino, they and the other zeks worked intensely to serve the state, as loyal Russians. They struggled to create a work environment in which they could carry on discussions of literature, art and politics, while they worked--and resisted the efforts of the sharashka managers to narrow them to routine prescribed tasks. Being an intellectual was a full time task, even in a prison.

~~(TS)~~ [redacted] the MVD managers of Marfino were as stupid and shortsighted as they were, so that they largely wasted the scientific and intellectual talents of the people they arrested and put to work on speech encryption. The zeks knew their efforts were being frustrated, but in the end were unable to keep the important research going, or stop the production of deficient cipher machines. This waste of ability by a despotic government seems to have persisted for a long time in Russia, with anguish and hardship for the people who understood the situation best. No wonder that a church was named "Ease My Sorrows."

SOLUTION TO NSA-Crostic No. 59

"Naming Soviet Cities," VOX TOPICS, Vol 11, Spring 1984

"A noticeable trend in Soviet city naming began with the death of Lenin: important cities were renamed for deceased Bolshevik heroes. It was [extremely] fitting that after Lenin's death, his birthplace and the place where the revolution erupted should be named for him.

BULLETIN BOARD (u)

FIELD STATION MAIL

* Sending mail to co-workers who are now in the field is not hard when you know when and how. What you must not do is forward mail, because some items cannot be sent to certain field sites. The thing to do is to return the mail to the sender, with a note to the effect that J. Schmoe is now at Fxxx. Then it's up to the sender to check it out. If you're the sender, and it's permitted, consult these NSA Regs: R10-04, Armed Forces Courier Service; R10-12, Personal and Personally Addressed Mail; R10-27, Official Mail. Your Staff Security Officer can help you interpret these Regs. What not to do? Pop it in a shotgun envelope. Never, Never, Never!

SPEAKERS OF FOREIGN LANGUAGES

* Can you speak a foreign language with native or near-native fluency? If so, please make yourself known. On a piece of paper write your name, language(s), organization and secure phone number, and send it to [redacted] P16.

P.L. 86-36

FILBERT FOR CRYPTANALYSIS

* Attention, hand systems cryptanalysts! Do you have an IBM PC, XT, or ASTW? Are you tired of having to go to the tube room to do a short run? Consider FILBERT. It's a set of routines for the pc designed to help with the diagnosis, recovery, and exploitation of low-level manual systems, and is intended as an adjunct to the mainframe rather than a replacement for it. The CA techniques implemented on FILBERT are the established, tried-and-true routines familiar to cryppies. FILBERT is available through the PCIC (Personal Computing and Information Center) in the main library, or call P13 (963-5868) for more information and/or a demonstration.

FILBERT USERS

* Notice to current FILBERT users: FILBERT version 2.0 is now available. It incorporates changes, upgrades, and additional programs, all as a result of your input. Thanks! If you have not been contacted about receiving the new version, call P13 on 963-5868.

CODE WANTED

* Wanted: a small operational code of 1000 groups or under to be used for training purposes, as is or disguised. The code may be one-part or two-part, preferably, in a language other than English, and need not be well recovered. It should be unenciphered, or if enciphered, the keys provided as well. Either hard copy or machine-readable traffic can be used, 25 messages or more. A bennie is that bookbreaking programs for that code will be developed for a PC. For further particulars call [redacted] E42, 968-8418.

P.L. 86-36

LINGUIST PC USERS

* Special for linguists who use computers: As personal computers and workstations become more widespread throughout the Agency, some of you are modifying or developing your own programs to aid you in your daily work. In order to establish a clearinghouse for existing software and to share ideas for software tools, P16 is establishing a users' group for linguists and reporters interested in software packages for foreign languages. A description and demonstration of [redacted] a multilingual terminology retrieval and maintenance system available for the IBM PC will be presented at the first meeting, scheduled for the last week of May, specific time and location to be announced. All Green and Orange badgers are invited. Point of contact is [redacted] P16, 963-1103.

TELECOMMUNICATIONS TERMINOLOGY

* Just out! Hot off the press is the Glossary of Telecommunications Terminology. It was prepared by the Policy and Liaison Staff of the Telecommunications and Computer Service Organization, with the assistance of the National Data Standards Center, and carries an overall classification of CONFIDENTIAL. For copies call or write [redacted] P13D, FANX III, 968-8162s.

P.L. 86-36

A NOTE ON IMPROVING CRYPTOLOGIC RESEARCH (u)

Nathaniel C. Gerson,

W36

(U) Following is a suggestion for improving cryptologic research in the fields of physics, engineering, and computer technology. It involves:

(a) defining a strong relevant program, and
(b) insuring that it will be carried out.

DEFINING RESEARCH GOALS

~~(FOUO)~~ The first step requires the formulation of an overall, cryptologically-related research plan. Such a plan may evolve either by inclusion in "SIGINT 2000--TECH FOCUS" or as the result of an internal seminar specifically held for this purpose. In the latter case, the seminar could be of five days' duration to an audience consisting of middle managers responsible to DDR, DDC and DDO. Presentations would be made as follows: during the first two days, operationalists would outline their immediate and projected technical problems and indicate the relative importance of each problem. On the second two days, researchers would describe their current ongoing investigations and provide their views on how these studies impact on operational problems. On the final day the audience would attempt to draft mutually agreeable research objectives. If the final day produced even a single draft plan, the seminar would all be worthwhile. In any case, it would be illuminating to the management.

(U) An intangible objective of the seminar would be to initiate a frank dialogue, long overdue, between the Operational and the Research elements of NSA. (I sometimes wonder whether contractors attending the annual Defense Intelligence Technical Forum do not, in fact, gain a better understanding and appreciation of cryptologically oriented research than do personnel in R!)

(U) In any event, if an internal seminar on research were held, it would be desirable to allow ideas to gestate for four to six months. Thereupon a very small number of knowledgeable individuals of those attending the seminar would be tasked with defining a cryptologic research program. About every three years thereafter critical reviews of the total program would be necessary to examine pertinence, quality, and progress. It is imperative to note that applied researchers have a dual obligation: to originate investigations directed to the parent agency, and to put an end to unpromising lines after an honest trial period. It should be understood that only short- or intermediate-term research would be undertaken; long term investigations (of second, third, etc., order effects) are properly the province of other institutions, such as the National Science Foundation.

ORGANIZATIONAL RESTRUCTURING OF RESEARCH

~~(C)~~ A serious question should be raised as to whether the present arrangement of placing research in R is conducive to progress. In R, research is somewhat concentrated in R1, mainly for COMSEC, and R5, mainly for COMINT. (Minor research projects are underway in other elements of R as well as in S, T, W, etc. These efforts need not be considered here.)

~~(FOUO)~~ The primary thrust of R as it exists today is that of a technical contracts group. It easily could be called TECON or some other name and its function would be unchanged. To place matters in perspective, we might note that the current activities of R comprise about 90% technical contracting and 10% research.

~~(FOUO)~~ The principal difficulty facing NSA is the relationship between the problems identified in Operations and the manner in which they are investigated in Research. Moreover, referral of problems from Operations to Research is hindered by organizational barriers, among other things. Also, the formal flow of updated information from DDC and DDO to DDR is apt to be slow and ponderous. These factors mean that the relevance of on-going research in NSA gradually fades as R continues to work on problems which are of interest only to itself. Thus money is spent to no advantage, but spending gives an illusion of progress.

~~(FOUO)~~ Restructuring the research effort organizationally might be a method of removing some of the present built-in obstacles. One way would be to put R1 to under the jurisdiction of DDC and R5 under DDO, both as staff elements reporting directly to the appropriate deputy director. Another might be to combine R1 and R5 and form a new element at the directorate level.

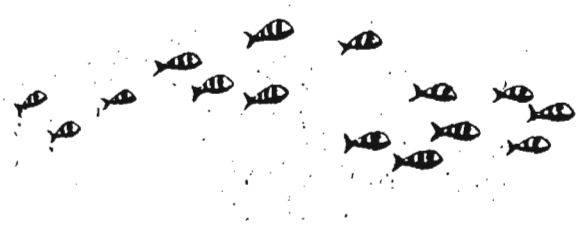
(U) Either of these arrangements would permit the detachment from day-to-day operations that is necessary for research, yet allow the control needed to insure that the research is relevant and cryptologically oriented. Also, it could better shield the research from some of the wild disruptive fluctuations in funding. Research would become more meaningful, and NSA would be less likely to be taken by technical surprise.

EDITOR'S NOTE

~~(FOUO)~~ As we go to press, we learn that R1 has just been transferred to DDC.

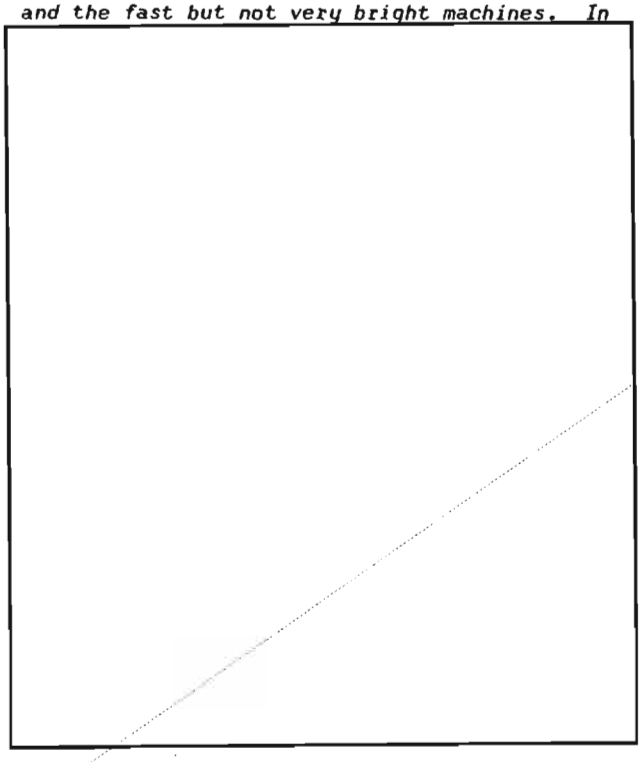
FOOD FOR THOUGHT

(u)



Extract from "General Utility Programs for Cryptanalysis" by Carolyn Palmer, published in Collected Papers on Cryptanalytic Diagnosis, NSA, April 1969 (S-194,074)

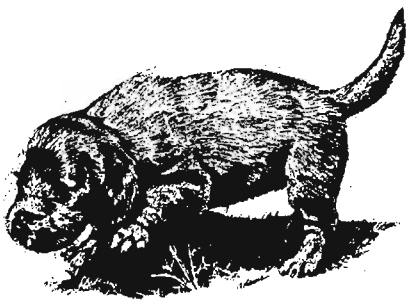
~~(S-CCO)~~ There is another factor which, in my experience, has always been necessary for reaching a successful conclusion to any problem complex enough to require a series of machine processing steps. This is continuous interaction between intelligent human beings and the fast but not very bright machines. In

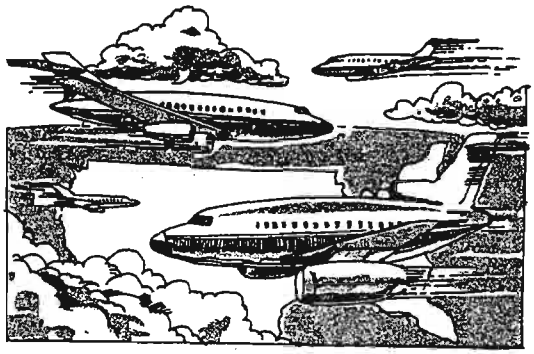


EO 1.4.(c)
P.L. 86-36

OCID: 4009937

A Traveler's Tale (u)





P.L. 86-36

The trip was planned as a nice spring TDY to Oak Ridge, Tennessee. Of course, spring in Oak Ridge is not necessarily spring in Baltimore, and I watched in horror as the fog rolled in the day I was to leave. The ticket agent at BWI postulated that if any airport open for outgoing flights, it would be National. O.K. Take a limo to National, have a nice lunch except for a funny twinge of pain whenever chewing anything hard. Oh well!

Wait several hours at National. Finally the announcement comes that the plane is on the ground at Dulles. They load us on a bus and take us to Dulles. We're only running 6 hours behind!

We take off at last, but not before the stewardess intently examines the "What To Do In An Emergency" card. (Is this her first flight??) The pilot announces "Please keep your seat belts on, we're headed for a little turbulence." KA-BOOM! The cabin lights up from the outside and the stewardness shakily tells us to stay in our seats! The pilot comes on the intercom and calmly announces a minor case of "St. Elmo's Fire" (Did I mention that I flew on the 13th and sat in aisle 13? Not that I'm superstitious, mind you.) Eventually we do arrive in Knoxville, and take a limo to the hotel in the pouring rain. We arrive, of course, after the restaurant has closed and there are no restaurants within walking distance. Oh well, peanut butter crackers and soda for dinner weren't too bad except for the funny twinge when chewing.

Next day dawns bright and balmy and the day goes well. Back to the room in preparation for dinner hosted by the organization we're visiting. I had been worrying about that funny spot in my mouth and suddenly discovered a broken tooth! Great, a stranger in town, what should I do? Try the hospital emergency room, I'm told. O.K....that was a mistake, they're no help!

I got the name of a dentist and make an appointment for the next morning. The taxi drops me off at the dentist and I spy a brown dog nestled in the shrubs. "Nice Doggie!" I walk up to the door, turn the handle and the dog attacks! She nipped my leg, tore a small hole in my slacks and scared the life out of me. Finally after what seemed like hours, the dentist appears, calls off the dog, and states, "She hardly ever bites people!" Lucky Me! At least I got a temporary crown for the tooth for next to nothing and a new pair of slacks free.

The rest of the TDY passed fairly uneventfully, but I did have a moment's hesitation when it was time to leave and we were told to board at Gate 13!

OCID: 4009937

TYME SHELL (u)

This is a time shell to compute Greenwich Mean Time (Z) and Local Time based on the System Time. It is written for the IBM PC/XT and ASTW with a color monitor. Shading will be different on USi monitors Pi2 and Pi3. It will not run on terminals with a monochrome monitor.

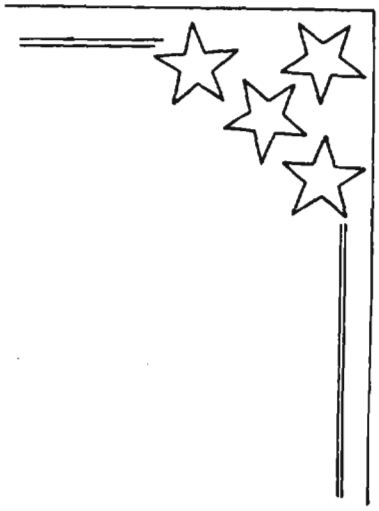
P.L. 86-36

P14

```
echo "\f"                # Clears screen. "\f" is a form feed.                  #
# Set variables $month, $date and $hour.                                       #
month='date "+%m"'          # "+%m" is month portion of system date/time.      #
date='date "+%d"'           # "+%d" is date portion of system date/time.       #
hour='date "+%H"'           # "+%H" is hour portion of system time.            #
   case $month in
          11)     e=S f=05              # Sets EST; $e=S and $f=05.             #
                  ;;
          12)     e=S f=05
                  ;;
          01)     e=S f=05
                  ;;
          02)     e=S f=05
                  ;;
          03)     e=S f=05
                  ;;
          04)     if test $date -ge 28     # Test for last Sunday in April #
                  then e=D f=04        # Sets variables for month of April #
                  else e=S f=05
                  fi
                  ;;
          05)     e=D f=04                    # Sets Daylight Savings Time #
                  ;;
          06)     e=D f=04
                  ;;
          07)     e=D f=04
                  ;;
          08)     e=D f=04
                  ;;
          09)     e=D f=04
                  ;;
          10)     if test $date -ge 27     # Test for last Sun in October #
                  then e=S f=05      # Sets variables for month of October #
                  else e=D f=04
                  fi
                  ;;
   esac                                          # escape case/in test #
   zulu='expr $hour + $f'
echo "\n\t 32m\0311\0715\0715\0715\0715\0715\0715\0715\0715\0715\0715\0715\0715\
0715\0715\0715\0715\0715\0715\0715\0715\0715\0715\
echo "\t 32m\0272\c";date "+     31mTIME:  35m$zulu:%M:%S Zulu     36m(%H:%M E.$
e.T.)"
echo "\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b32m\0272"
echo "\t 32m\0272                                                    \0272"
echo "\t 32m\0310\0715\0715\0715\0715\0715\0715\0715\0715\0715\0715\0715\0715\07
15\0715\0715\0715\0715\0715\0715\0715\0715\0715\07
```

```
#  The echo statements above set the colors and draw a box around the      #
#  output when the results are printed on the screen.  Color change        #
#  functions such as 32m are preceeded by ESCI (Escape Key/open bracket).  #
#  Special ASCII characters \0310\0715\0715, etc. are part of the graphics #
#  chara set used to draw a box around the output.  Character constants    #
#  \n, \t, \b and \f are newline, tab, backspaces and formfeed. "\c" kills #
#  the <CR> function.  In /usr/lib/crontab you can replace the statement   #
#  "0 * * * * exec echo "The hour is" 'date'. > /dev/console &" with       #
#  "0 * * * * exec /usr/rej/bin/tyme > /dev/console &" to use your "tyme"  #
#  SHELL rather than the system default time.  Specify the pathname, e.g., #
#  "/usr/rej/bin" to where your executable "tyme" SHELL is located.        #
```

DOCID: 4009937



ON EXCELLENCE (u)

From the keynote address at the Quest for Quality Conference in Seattle in November 1962 by Henry M. Jackson, Senator from Washington.

Published in Achieving Excellence in Public Service, The American Academy of Political and Social Science, Philadelphia, August, 1963.

As never before, we have to provide a government environment that encourages excellence.

Standards of performance adequate for quieter times will not do. State, Defense, the military services, the economic agencies, and the rest of our government must meet new tests of excellence. Yes, and Congress, too.

For two years, our Senate Subcommittee on National Policy Machinery conducted a nonpartisan study of our machinery for making and executing national-security policy. This study had something of a surprise ending: We concluded that the heart of the problem of government is not machinery but men.

Good national policies require both good organization and good people. But people are the critical factor. Wise, experienced, hard-working, incisive government officials may win out over poor organization. But poor people will defeat the best organization.

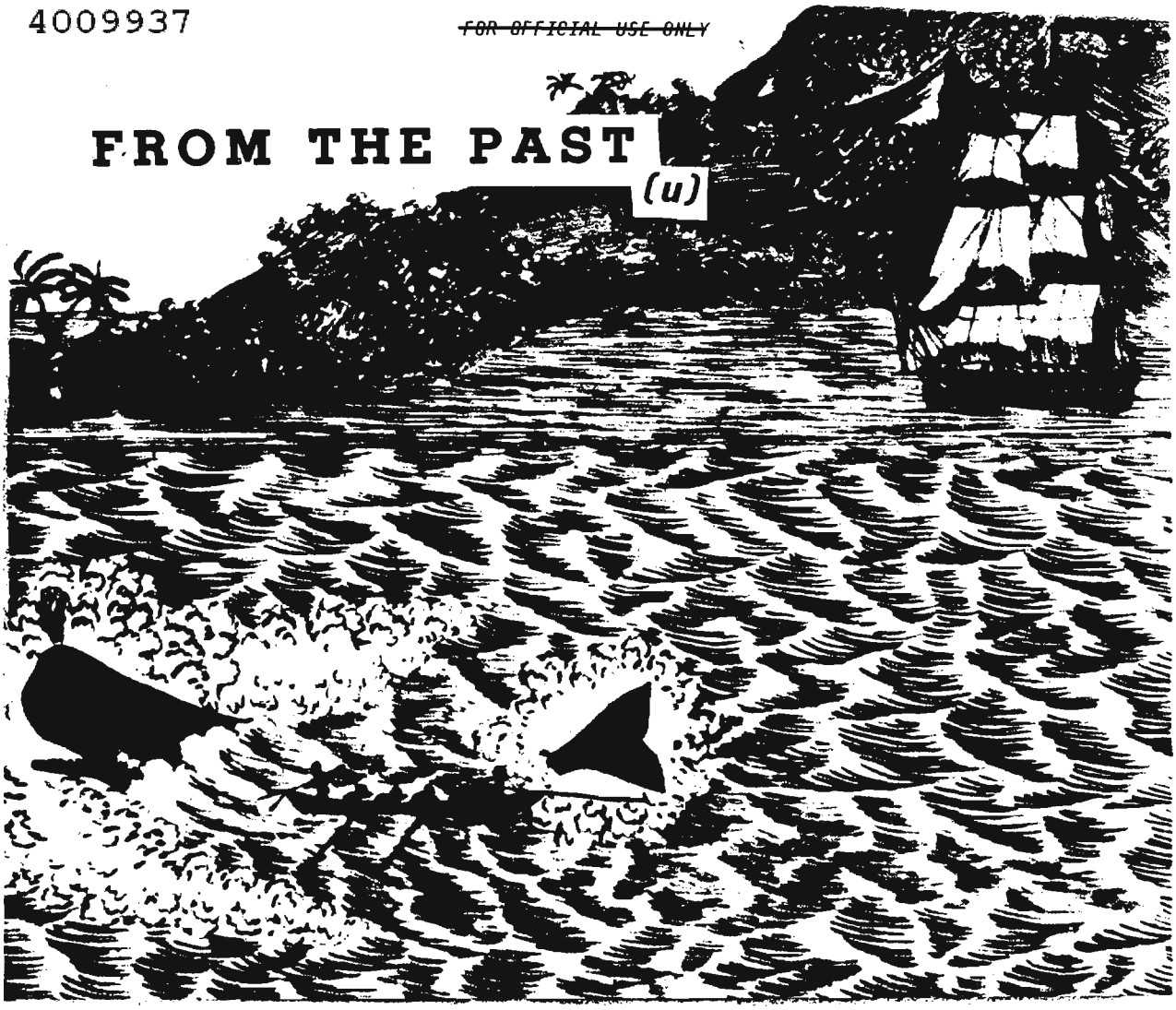
Moreover, reforms in machinery cannot cure troubles which are really not due to defects of machinery. Organizational gimmickry is no substitute for practical measures to improve the competence and the performance of government officials.

Earlier this year, the Senate of the United States established the Subcommittee on National Security Staffing and Operations and asked it to make a study of how well our government is staffed to conduct national security operations.

The Subcommittee's inquiry is based on the simple proposition that the number one task is to get the right men into the right jobs at the right time and to make it possible for them to do a job. Men rise to responsibility, if they are given half a chance. The Subcommittee's modest goal is to help them get half a chance.

OCID: 4009937

FROM THE PAST (u)



The following letter was written by Commodore David D. Porter during the famous cruise of the ESSEX in the War of 1812. The first part is of little interest. Near the end of the letter, however, the Commodore intersperses a bit of cipher.

"U.S. FRIGATE ESSEX AT SEA"

Lat. 2° 26' S, Long. 82° 20' W

July 2, 1813

Excuse me sir for not making known my present intentions as this letter may not reach you, it may however be satisfactory to you to know how I intend to dispose of my prises, let it suffice to say that I shall endeavor to .QD66.94DK.C7.G4C66C.

British letters of Marque are numerous in these seas and were it not for my arrival our whale fishers would have been much harrassed, but they now find it necessary to keep together for mutual protection. I expect to be .AP8QPD2. but shall be .A8DAF8D2.

The State Department will no doubt inform you of the effect our presence has produced; in a .AX6C9CGF6. view on that head I shall be silent.

A British ship shall
.7X9.7FØCBF9D.94D.AFGC3CG.C7.QF3D9Q.

To decypher part of this letter I must refer you to the cypher sent me at N Orleans dated 13 June 1809.

I have the honor to be
with great respect
Your Obt Servt,
D.D. Porter

Hon Paul Hamilton
Secy of the Navy
Washington.

OCID: 4009937

~~FOR OFFICIAL USE ONLY~~

NSA-Crostic No. 60

This puzzle, which originally appeared in 1980, has been re-edited to incorporate cryptic definitions. If you need an explanation of these clues, call the Puzzle Editor on 1103s, and you'll be sent one.

Word D, as seen in Word Z

A. "_____ and speak each other in passing." *Tales of w Wayside Inn*, Longfellow (6 wds)
84 68 166 255 206 23 179 270 222 103 195 19
273 76 57 148 110 177 123 133 47 263 7

B. If ever I see pond in capital, I'll know
30 39 63 174 143 238 279 159 59 9

C. He, she, you, I, etc., etc., have a low melting point
230 3 244 18 101 207 257 139

D. Former Hollywood leading lady (1924—), in such films as *Crash Landing*, *Donovan's Brain*, etc. (Full name)
240 147 12 186 272 226 252 276 210 32 10 40
168 219 108 64

E. New England city trainer warned chimp on chores left undone (3 wds)
176 124 201 278 53 271 13 259 145 202 104 100
107 27 241 161 185 169 88

F. Little junction merges with ease to get rid of undesirables
211 87 105 109 167

G. Rolls follower
138 34 197 77 203

H. Mau Mau stereos are severe and unadorned
60 85 233 116 131 220 162

I. Romantic-sounding town in Florida
122 180 190 72 243 163 130 113 221

J. Richard III sounds quite treacherous
175 80 115 62 196 149 117 208 181

K. My female relative is not Polish civil engineer
141 158 199 89 194

L. Fate, at the turn of the card (4 wds)
5 28 52 120 73 234 128 25 43 144 173 213 231

M. The wheel and tire are to be sent to northern Ethiopia
157 275 260 256 251 78 232

N. Women as mates, says Thurber, should be those "who have great constitutional strength and are not _____."
24 65 127 223 160 183 29 36

O. Fearful Moro is wearing mixed-up suit
8 277 54 51 97 91 242 135

P. Only the true die well-educated
95 106 155 212 266 69 264

~~FOR OFFICIAL USE ONLY~~

Q. Knockout punch used for storing locomotives

132 235 56 214 182 82 140 38 229 248

R. With time, this is not a waiter

178 164 215 218

S. Toast _____ (3 wds)

258 249 90 21 200 269 137 125 151

T. In pointing out why a fifth of Scotch on the bar was preferable to major brain surgery, he explained, "I'd rather have a _____." (9 wds)

86 254 67 93 205 6 102 126 75 4 250 261 50

224 152 265 83 262 70 225 112 119 136 44 79

237 17 191 247 165 31 198 150 134 37 55 98

U. I know why TV blinds five-eyed man of inseparability

268 41 253 58 184 71 142 14 246 216 204 48 20 1

V. Ask Omar Sharif if I can see 1955 robbery movie

193 228 35 111 92 114

W. Totes certain blue terriers?

96 121 154 146 45 26 129

X. Are this lady's jacket and skirt hairy?

94 11 217 156 239 81 187

Y. Headless maid needs help

16 66 209

Z. The only film in which Word D and her husband were co-stars (1959)(4 wds)

188 33 192 267 15 22 61 171 2 74 42 99

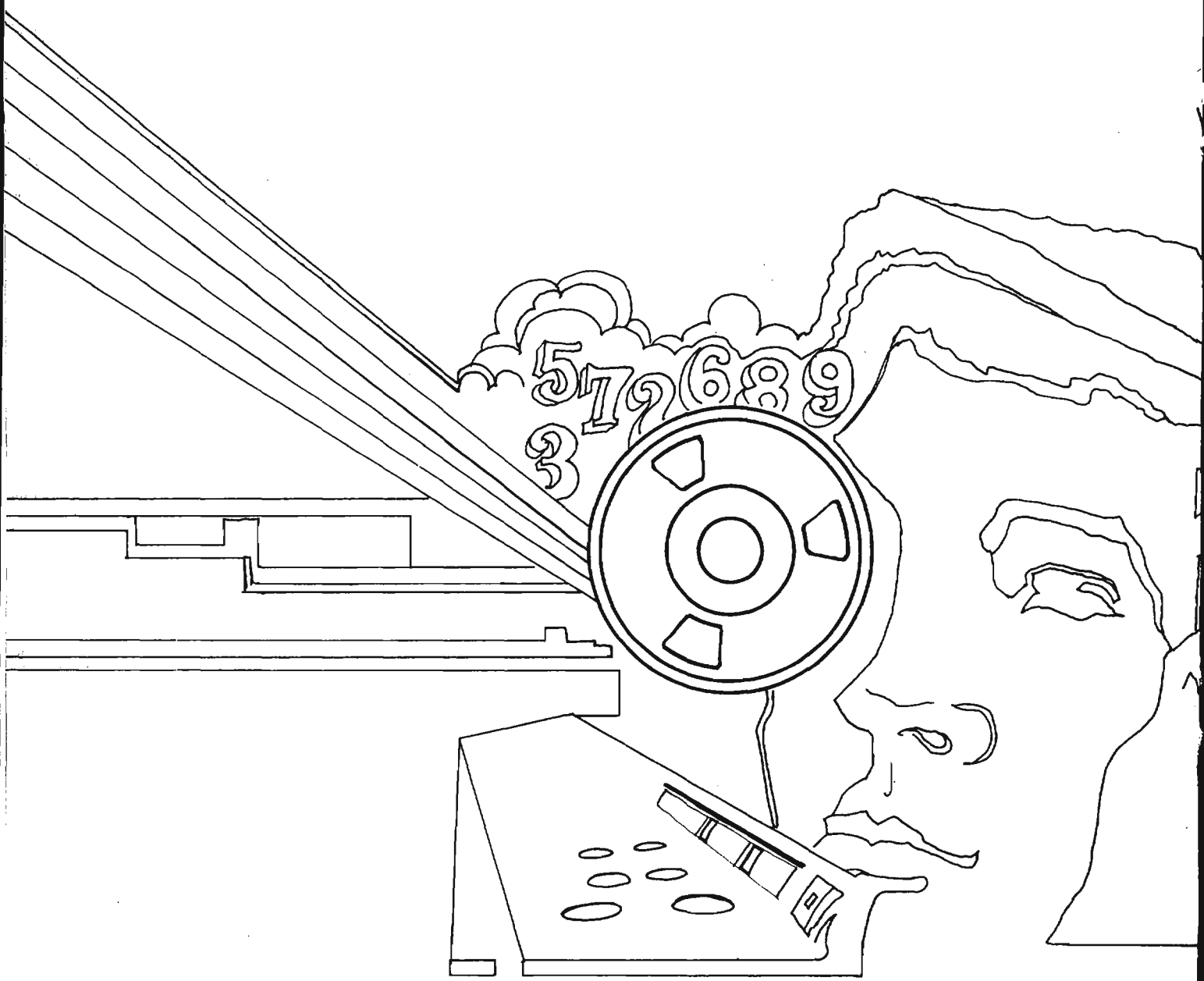
274 49 245 227 170

a. Did you see a emu on going back to New Guinea?

46 153 236 118 172 189

		1 U	2 Z	3 C	4 T		5 L	6 T	7 A	8 O	9 B	10 D		11 X	12 D	13 E	14 U	15 Z	16 Y
17 T	18 C	19 A		20 U	21 S	22 Z	23 A		24 N	25 L	26 W		27 E	28 L	29 N	30 B	31 T	32 D	33 Z
	34 G	35 V		36 N	37 T	38 Q	39 B		40 D	41 U	42 Z	43 L	44 T	45 W	46 a	47 A		48 U	49 Z
50 T	51 O		52 L	53 E	54 O	55 T	56 Q	57 A	58 U	59 B	60 H	61 Z	62 J	63 B	64 D		65 N	66 Y	67 T
68 A		69 P	70 T	71 U	72 I		73 L	74 Z	75 T	76 A	77 G	78 M		79 T	80 J		81 X	82 Q	83 T
	84 A	85 H	86 T	87 F	88 E	89 K	90 S		91 O	92 V		93 T	94 X	95 P		96 W	97 O	98 T	99 Z
100 E		101 C	102 T	103 A	104 E	105 F	106 P		107 E	108 D	109 F	110 A	111 V	112 T	113 I		114 V	115 J	
116 H	117 J		118 a	119 T	120 L	121 W		122 I	123 A	124 E	125 S	126 T		127 N	128 L	129 W		130 I	131 H
132 Q	133 A	134 T	135 O		136 T	137 S	138 G		139 C	140 Q	141 K	142 U	143 B	144 L	145 E	146 W	147 D	148 A	149 J
150 T	151 S		152 T	153 a	154 W		155 P	156 X	157 M		158 K	159 B		160 N	161 E	162 H		163 I	164 R
165 T	166 A	167 F	168 D	169 E	170 Z		171 Z	172 a	173 L	174 B	175 J	176 E	177 A		178 R	179 A	180 I	181 J	
182 Q	183 N	184 U	185 E	186 D	187 X		188 Z	189 a	190 I		191 T	192 Z	193 V	194 K	195 A	196 J	197 G		198 T
199 K	200 S	201 E		202 E	203 G	204 U	205 T		206 A	207 C	208 J	209 Y	210 D	211 F	212 P		213 L	214 Q	215 R
	216 U		217 X	218 R	219 D	220 H	221 I	222 A		223 N	224 T		225 T	226 D	227 Z	228 V	229 Q	230 C	
231 L	232 M	233 H		234 L	235 Q	236 a	237 T	238 B		239 X	240 D	241 E	242 O	243 I	244 C	245 Z	246 U	247 T	248 Q
	249 S	250 T	251 M		252 D	253 U	254 T	255 A	256 M	257 C	258 S	259 E		260 M	261 T		262 T	263 A	264 P
	265 T	266 P	267 Z	268 U	269 S	270 A	271 E	272 D		273 A	274 Z	275 M	276 D	277 O	278 E	279 B			

P1-May 85-S3-75972


5 7 9 6 8 9
3

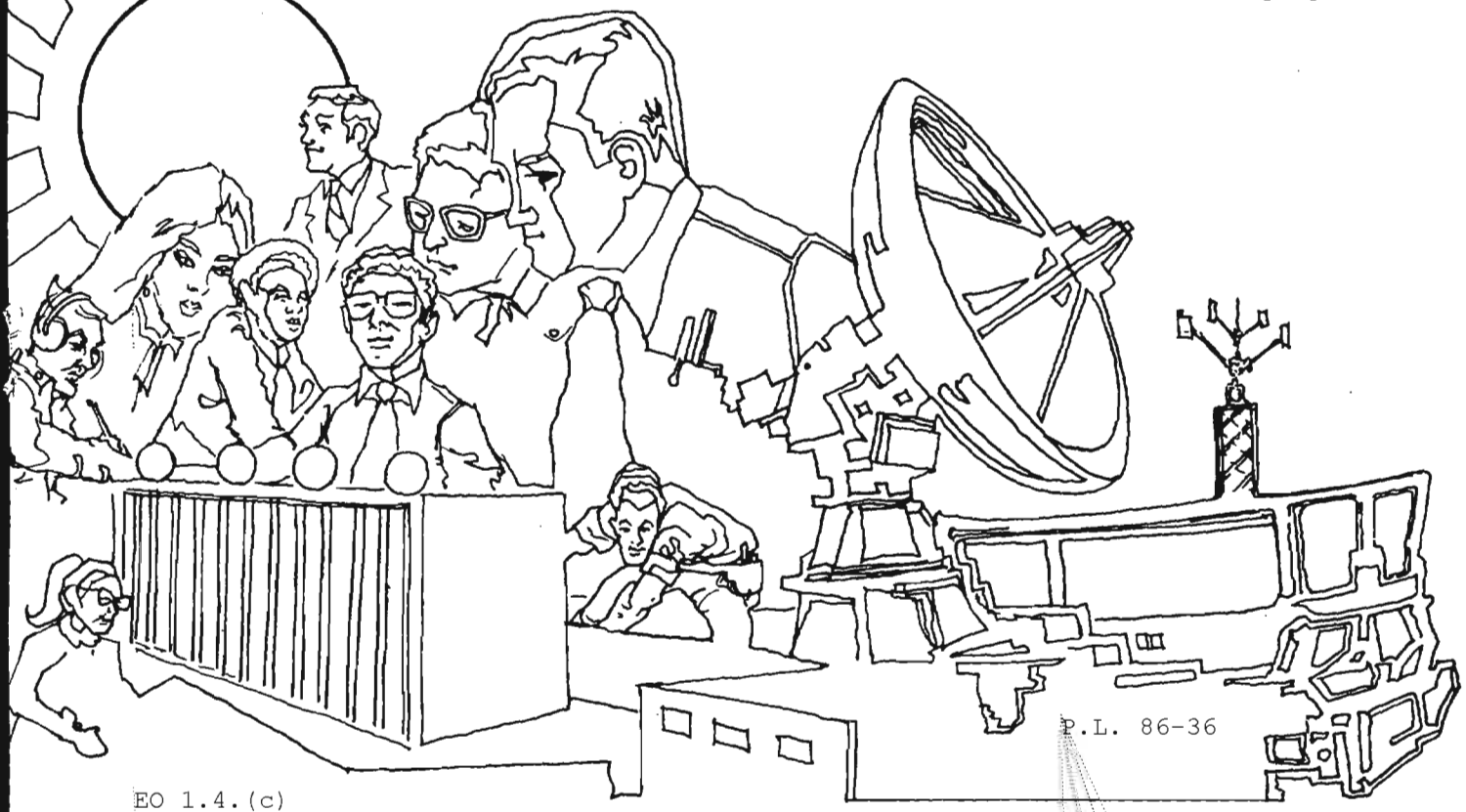
OCID: 4009933

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

NOV-DEC 1984



P.L. 86-36

EO 1.4.(c)
P.L. 86-36

TRENDS IN HF COMMUNICATIONS (U)..... [redacted] 1
SWITCHBOARD:
PAST, PRESENT AND FUTURE (U)..... [redacted] 5
OUT OF MY DEPTH (U).....7
[redacted] ..... [redacted] 8
EXPLORING A DOS DISKETTE (U)..... [redacted] 12
HUMAN FACTORS (U)..... [redacted] 22
CAN YOU TOP THIS? (U).....E. Leigh Sawyer.....24
PERSONAL COMPUTING IN A GROUP (U)..... [redacted] 25
FACTION LINE (U).....Cal Q. Lator.....35
NSA-CROSTIC NO. 59 (U).....D.H.W.....36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2
DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009933

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XI, No. 11-12 NOVEMBER-DECEMBER 1984

EO 1.4.(c)
P.L. 86-36

Editorial

PUBLISHER [redacted]

BOARD OF EDITORS

Editor..... [redacted] (963-3045s)
Production..... [redacted] (963-3369s)

Collection..... [redacted] (963-3961s)
Computer Security
..... [redacted] (859-6044)
Cryptolinguistics. [redacted] (963-1103s)
Data Systems..... [redacted] (963-4953s)
Information Science
..... [redacted] (963-5711s)
Puzzles.....David H. Williams (963-1103s)
Special Research.....Vera R. Filby (968-7119s)
Traffic Analysis..Robert J. Hanyok (968-3888s)

For subscriptions
send name and organization
to: [redacted] P14

P.L. 86-36

To submit articles or letters
by mail, to: P1, Cryptolog

via PLATFORM mail, send to:
cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no '0' in 'log')

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

~~FOR OFFICIAL USE ONLY~~

~~SECRET SPOKE~~

TRENDS IN HF COMMUNICATIONS [U]

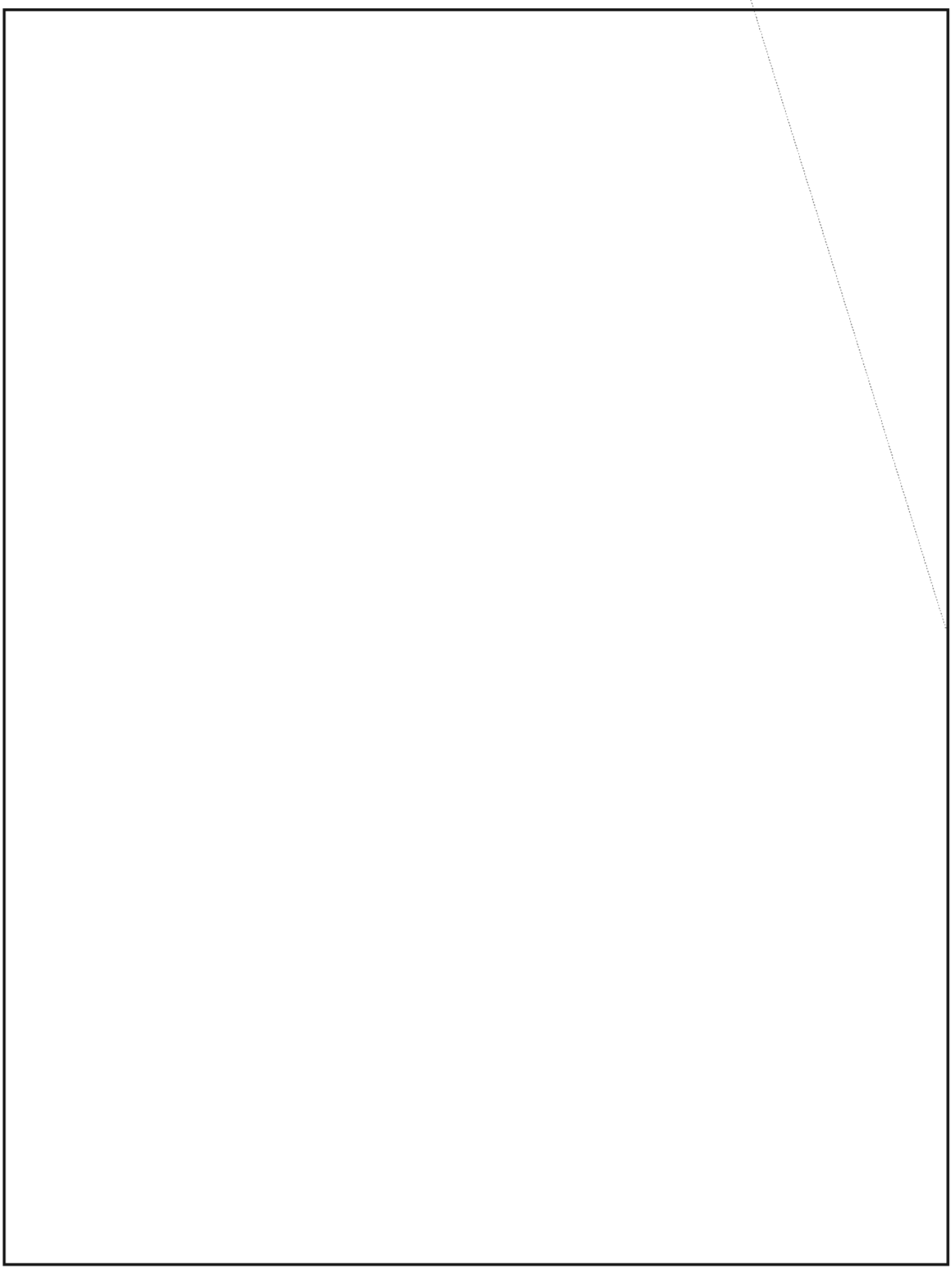
P.L. 86-36

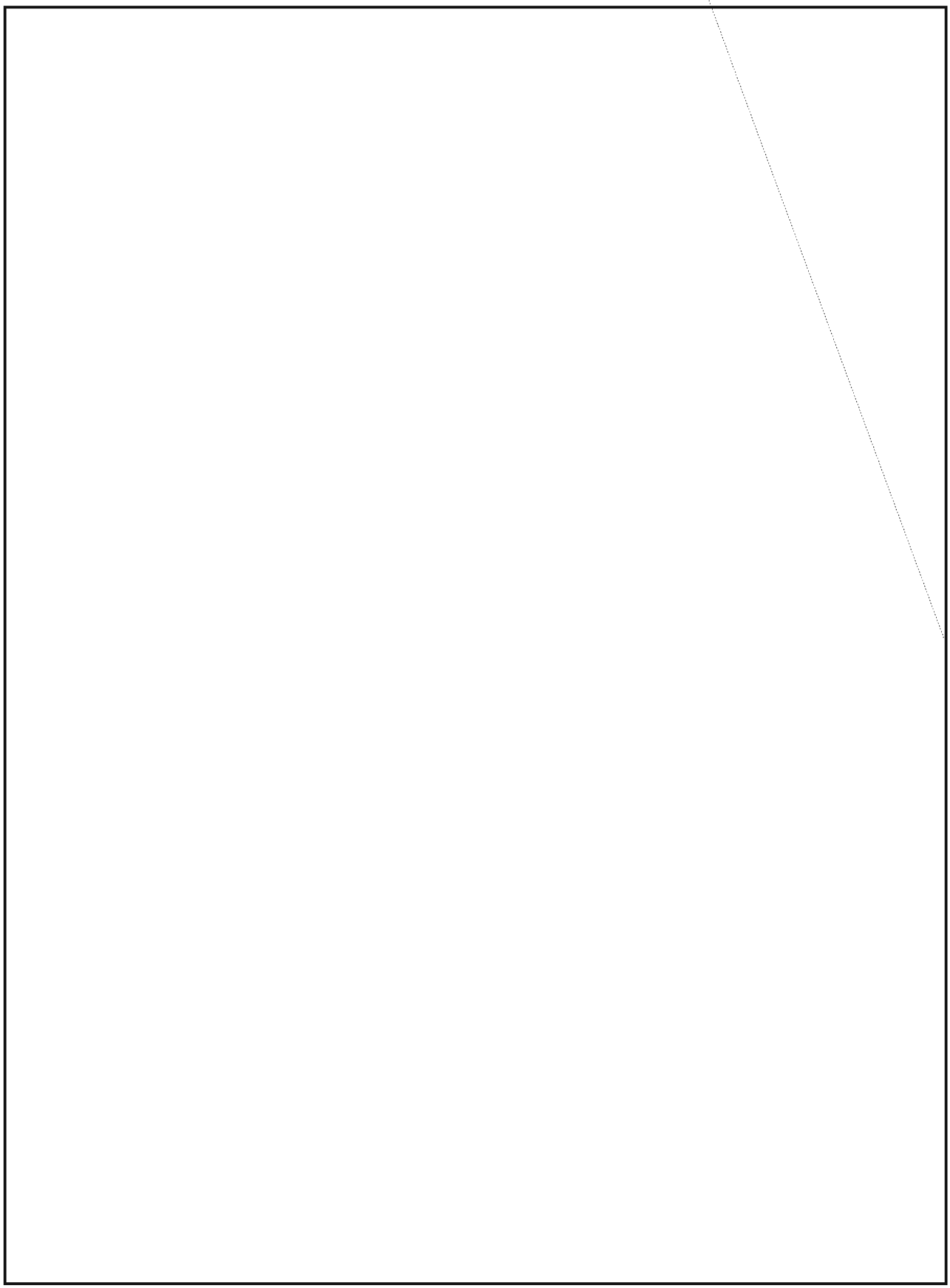
by [redacted]

[redacted]

EO 1.4.(c)
P.L. 86-36

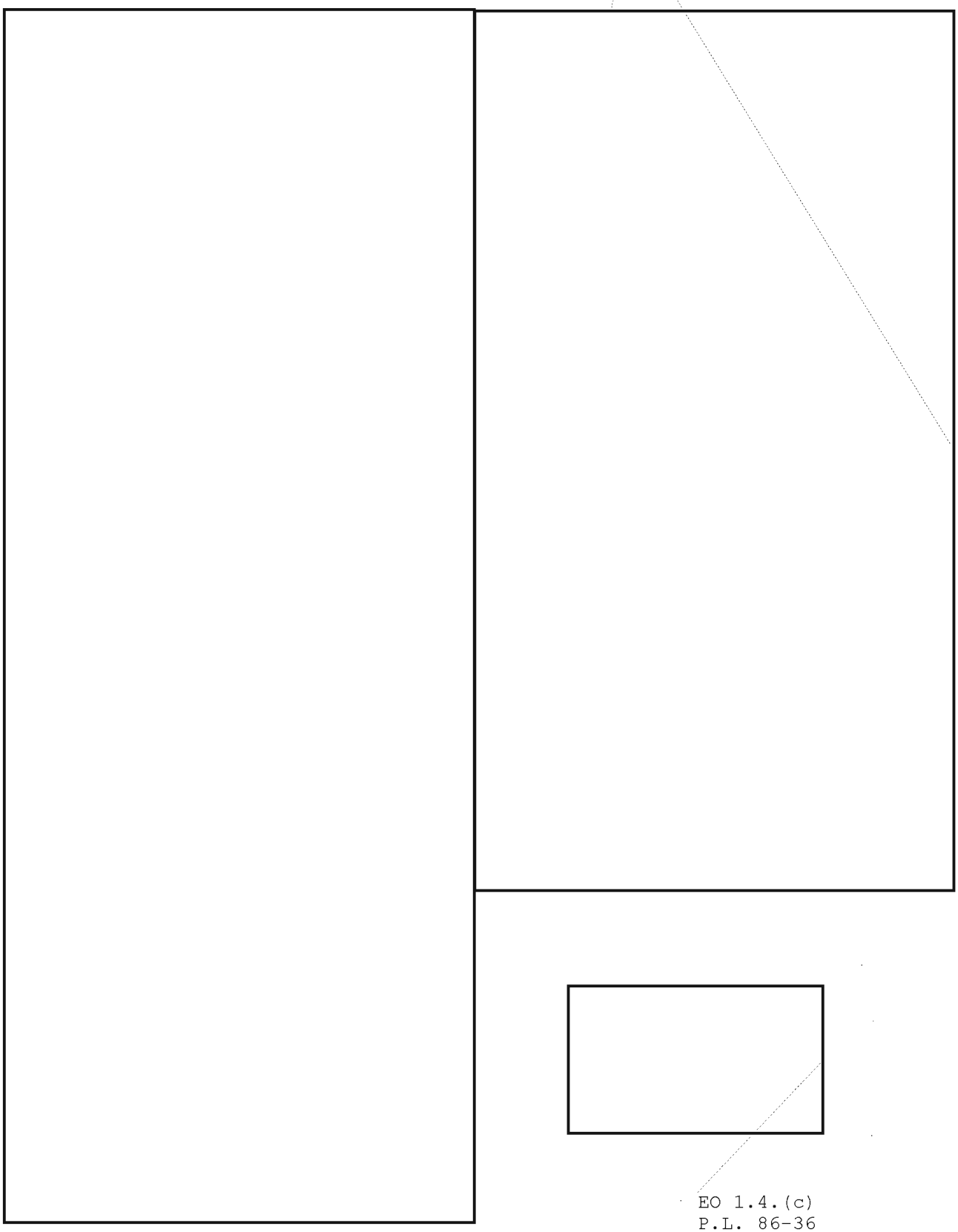
~~SECRET SPOKE~~





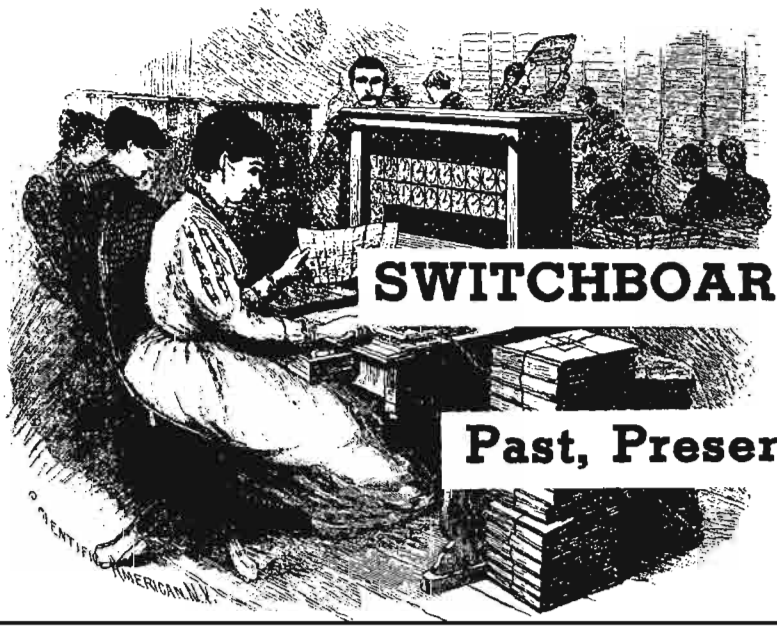
~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

OCID: 4009933



by [redacted]

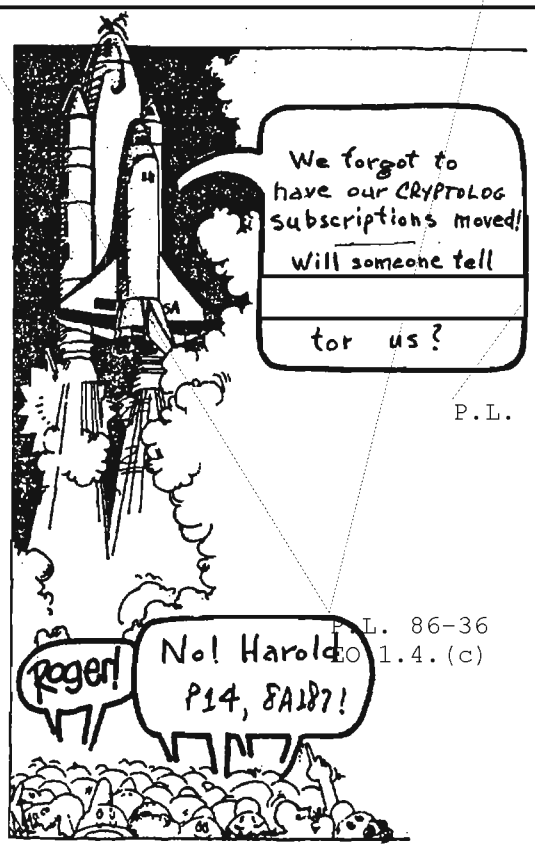
P.L. 86-36

SWITCHBOARD:

Past, Present, and Future [U]

[redacted]

P.L. 86-36
EO 1.4.(c)

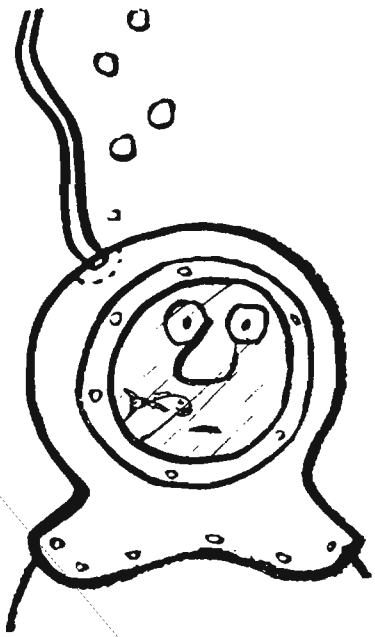


P.L. 86-36

P.L. 86-36
EO 1.4.(c)

EO 1.4.(c)
P.L. 86-36

OUT OF MY DEPTH [U]

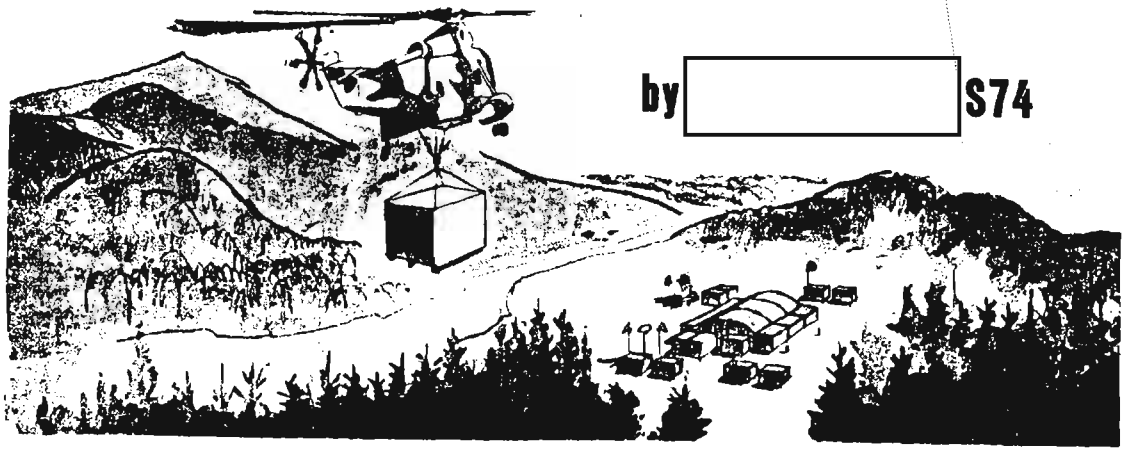


DOCID: 4009933

EO 1.4.(c)
P.L. 86-36

[redacted]

P.L. 86-36



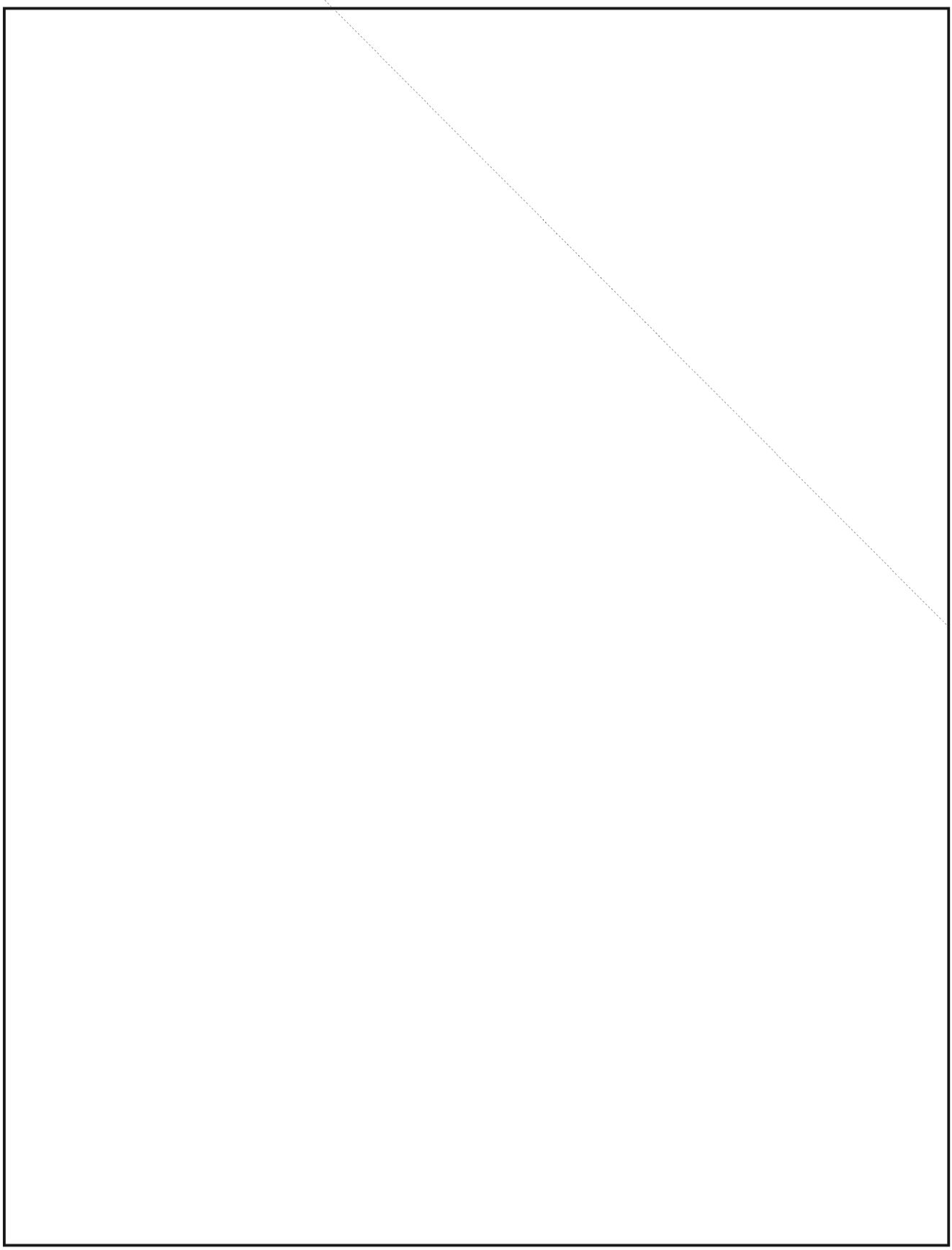
by [redacted] S74

[redacted]

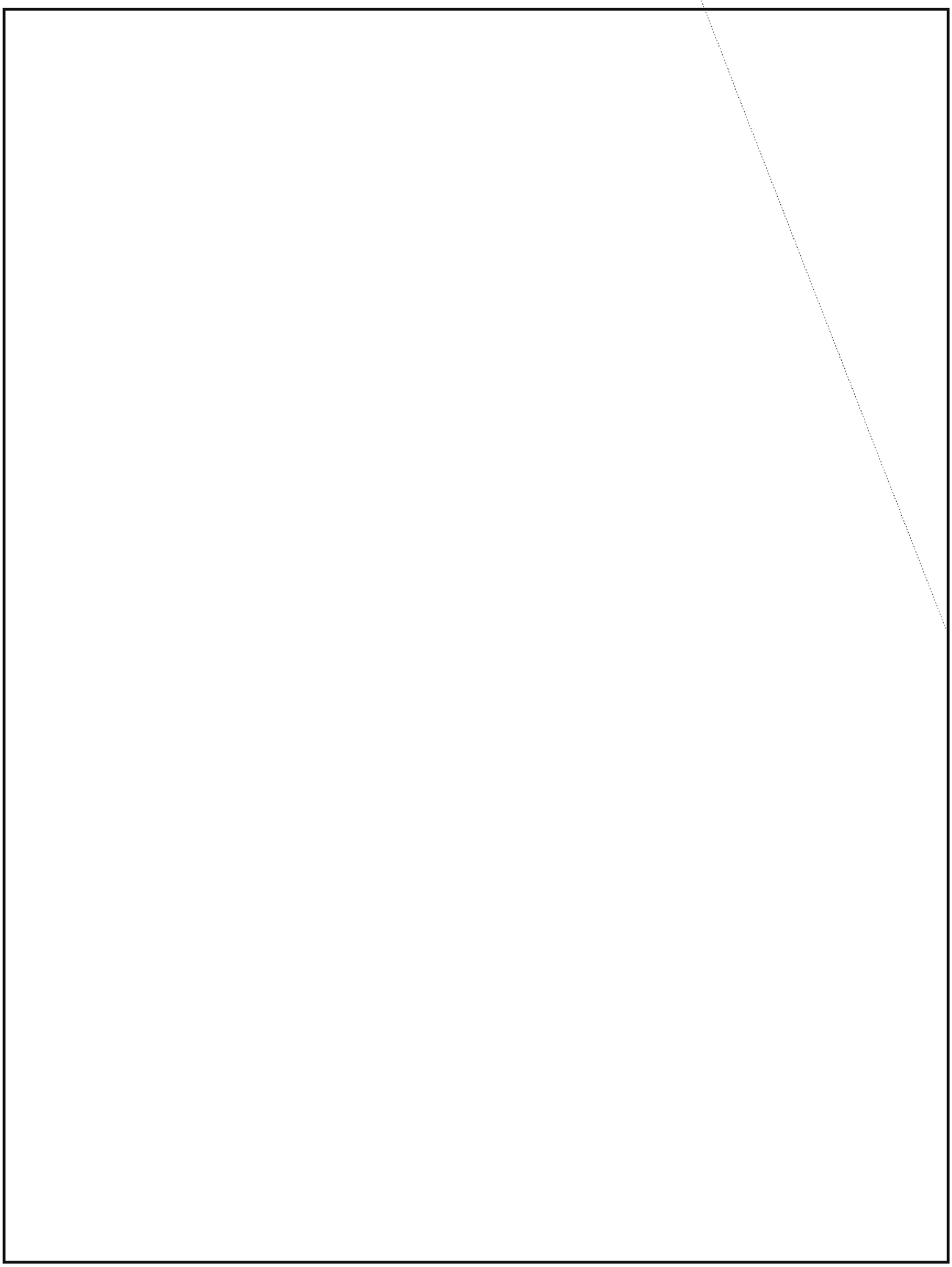
EO 1.4.(c)
P.L. 86-36

DOCID: 4009933

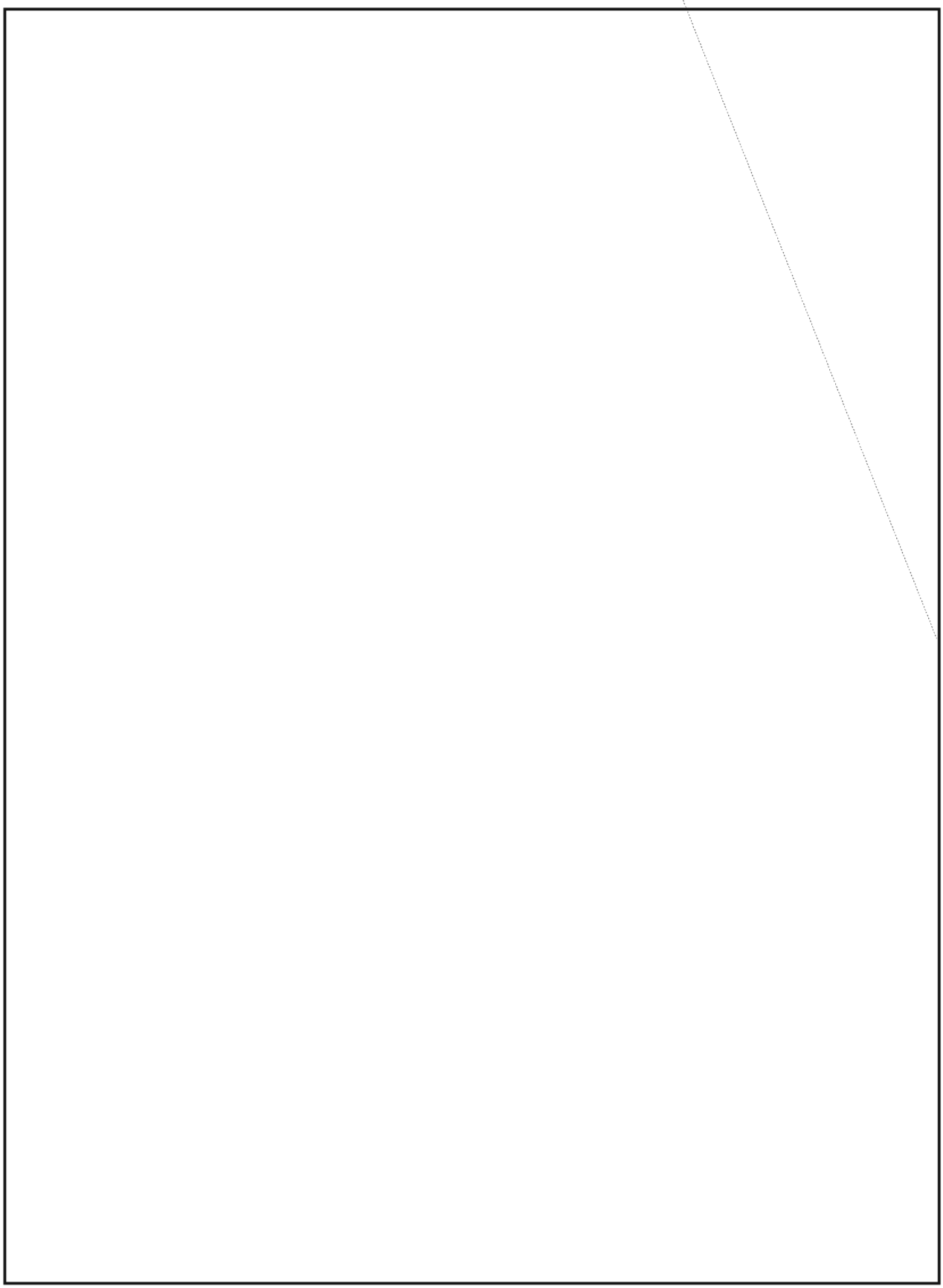
EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36



DOCID: 4009933

EXPLORING A DOS DISKETTE (U)

by [redacted] P13

P.L. 86-36

INTRODUCTION

Many data systems professionals will go through an entire career using a personal computer and handling small diskettes without really having an idea of how data is organized on them. There is nothing magic about it and, in fact, it isn't really difficult to understand where and how information is being stored and what it looks like on the disk.

This paper will attempt to explain how a 5 1/4 inch floppy disk is organized under PC-DOS 1.1, written by Microsoft for the IBM-PC. We will be using an IBM-PC and two double-sided double-density disk drives.

Most information was obtained from the Peter Norton book, Inside the IBM-PC, one of the most useful books on small computers I have found, and the IBM DOS 1.1 manual--very useful both as to information and as a cure for insomnia.

The diskette data displays were obtained through the use of the Peter Norton utility DISKLOOK.

Microsoft went to great lengths to have the software overhead take up as little room on the diskette as possible. This, obviously, makes good sense. A small computer isn't much good to you if the operating system takes up the entire disk. As a consequence, the directory and allocation table look rather cryptic, but once explained they are easily understood.

LOOKING AT THE DISKETTE

Formatting

When a user removes a blank diskette from the box for the first time he has two choices. He can use it as a frizbee or he can turn it into a reliable storage medium for use in his personal computer. We will address the second possibility with the full knowledge that we do not exclude the first possibility at any step of the process.

When you run the FORMAT program, as you already know, the diskette under DOS 1.1 is divided into 40 tracks per side, 8 sectors per track, with a boot record, directory, file allocation table, and, optionally, an entire operating system. Ok, let's format it.

Exploration

We'll now take our formatted diskette and place it in drive "B"--the one on the right. In the left drive we'll place the Norton Utilities and type in DL for DISKLOOK. This assembly language program will allow the user to look at the floppy diskette in the right drive sector by sector.

After DL is typed a self explanatory list of options comes up on the screen. We choose one that allows us to select a particular sector, side, and track. We'll start by looking at the 'Boot Record', which is on the first sector of the disk.

```
Side 0, Track 0, Sector 1
 1st sector of Boot record
EB279003 01140000 00000000 00000000 00000000 00000000 ..'.....................
00000000 00000000 00000000 000000CD 19FA8CC8 8ED833D2 ......................3..
8ED2BC00 7CFBB860 008ED88E C033D28B C2CD1372 69E88500 .....|..`.....3.....ri....
72DD2E83 3E037C08 74062EC6 06647D02 BB00002E 8B0E037C .r...>.|.t....d}........|.
51B0092A C1B4008B F05633D2 33C08AC5 2EF63664 7D8AE88A .Q..*.....V3.3.....6d}....
F48BC6B4 02CD1372 2D5E592E 2936057C 741F8BC6 2EF72665 ........r-^Y.)6.|t.....&e.
7D03D8FE C5B10151 BE08002E 3B36057C 7C052E8B 36057CEB .}......Q....;6.||...6.|..
C0EA0000 6000BE67 7DE80200 EBFE32FF 2EAC247F 740B56B4 .....`..g}.....2...$.t.V..
0EBB0700 CD105EEB EFC3E933 FFBB0000 B90400B8 0102CD13 .......^....3.............
1E72338C C88ED8BF 0000B90B 0026800D 2026804D 202047E2 ..r3.........&.. &.M  G..
F4BF0000 BE8B7DB9 0B00FCF3 A6750FBF 2000BE97 7DB90B00 .......}......u.. ...}....
F3A67502 1FC3BE1B 7DE8A2FF B400CD16 1FF9C30D 0A4E6F6E ...u.....}.............Non.
2D537973 74656D20 6469736B 206F7220 6469736B 20657272 .-System disk or disk err.
6F720D0A 5265706C 61636520 616E6420 73747269 6B652061 .or..Replace and strike a.
6E79206B 65792077 68656E20 72656164 790D0A00 0100020D .ny key when ready........
0A446973 6B20426F 6F742066 61696C75 72650D0A 004D6963 ..Disk Boot failure...Mic.
726F736F 66742C49 6E632069 626D6269 6F202063 6F6D3069 .rosoft,Inc ibmbio  com0i.
626D646F 73202063 6F6D3005 C606772F FF837EFC 00750B80 .bmdos  com0...w/..~..u...
7EF73B75 05C60676 2FFF89EC 5DCA0400 00000000 00000000 .~.;u...v/...]...........
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 00000000 . . . . . ..........
```

Figure 1 - The Boot Record

This record serves one purpose. It instructs the operating system in read only memory (ROM, as it is known to its friends) to go to the location on the diskette containing the rest of the operating system and read it into memory. If the system is there, it is read in; if not, control returns to the boot record and an error message is printed out.

So as the prompt comes up, we type in 0 for the side, 0 for the track, and 1 for the sector. Zero for the side? Real people start counting at 1, computer people start at zero. OK, why didn't we start at track zero? There is no track zero! Tracks on the PC were numbered by a computer person who skipped class the day they learned how to count. Tracks start at 1, everything else at 0.

As soon as this information is entered, the screen display comes up with 6 columns of hexadecimal numbers on the left, and a few readable words and other symbols on the right. This is the sector we requested, and is a display of the Boot Record.

Looking at the boot record (Figure 1), you can see rows of hexadecimal numbers broken into six columns with an ASCII translation next to each row. Since the boot record is in machine language we would not expect to see many ASCII characters and, in fact, we don't. Look down, now, at the 13th row and below. There we do see a translation and we probably recognize it. We are, of course, looking at the error messages that we get when we have put a non-system diskette in drive A and attempted to boot up. To keep the boot record as small as possible, Microsoft wrote the program in machine language but the messages to the user had to be in ASCII characters.

The Directory

The next two sectors contain what is known as the File Allocation Table (FAT). We will skip the FAT for a moment and proceed to sector 4, still on side 0.

Sectors 4 through 11 have the directory. This area contains all the information necessary for the operating system to retrieve files requested by the user, to sort them by time and date, if required, and to perform other operations as needed.

Looking at the directory (Figure 2), we do see some sort of information in the first couple of lines, and we'll get to that shortly, but for the most part we see rows of F6's and, every so often, an E5. When we formatted the

disk, the program took all 40 tracks (0 - 39) and put a pattern of 11110110 (F6 in hex) on them. It then went to the directory area and, each 32 bytes put an E5. The E5 signifies the beginning of a file record. Now, a sector will hold 512 bytes of data and there are 8 sectors allotted for the directory. Eight sectors will have space available for 4096 bytes (8 x 512). Since there are 32 bytes per record, a DOS 1.1 diskette can hold 128 files (4096 divided by 32).

The first few lines of the directory do appear to be telling us something. Microsoft organized the entries in the following manner: With this information, we'll try to understand the directory.

Starting at the first line of Figure 2, we can see some readable characters. The first ten bytes contain the hex equivalent of the ASCII characters for PROJECT.BAK. We can see this translation on the right. So, bytes 0 through 10 show that the first entry in our directory is PROJECT.BAK.

Byte 11 has a 00 as it is supposed to because it is not a hidden file or a system file. The user has the opportunity to make a

BYTE	
0 - 7	File name (an E5, at offset 0, indicates that the the file has been erased).
8-10	Filename extension
11	File attribute 02 = hidden file, 04 = system file, 00 for all other files.
12-21	Reserved; this implies that in a future version of this operating system some or all of these bytes will be used to further describe the file.
22-23	Time the file was created or last updated. Time is mapped according to the following rules:

```
|            23          |          22            |
|     hour      |     minutes     |   seconds     |
 15 14 13 12 11 10 09 08 07 06 05 04 03 02 01 00
```

hours = binary number of hours (0-24)
minutes = binary number of minutes (0-59)
seconds = binary number of two-second increments

24-25	Date the file was created or last updated. Mapping is done as follows:

```
|           25           |          24            |
|      year          |   month   |     day       |
 15 14 13 12 11 10 09 08 07 06 05 04 03 02 01 00
```

year = 0 - 119 (1980 - 2099)
month= 1 - 12
day = 1 - 31

26-27	Cluster number of the first cluster in the file.
28-31	File size in bytes. The first word contains the low order part of the size. Both words are stored with the least significant byte first.

OCID: 4009933


```
Side 0, Track 0, Sector 4
 1st sector of Directory
50524F4A 45435420 42414B00 00000000 00000000 0000914D .PROJECT BAK.............M.
E4080200 00360000 324A554C 59202020 42414B00 00000000 .....6..2JULY   BAK......
00000000 0000ABA4 E3081000 80100000 E5F6F6F6 F6F6F6F6 ................................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................................
E5F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................................
F6F6F6F6 F6F6F6F6 E5F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 E5F6F6F6 F6F6F6F6 ................................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................................
E5F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................................
F6F6F6F6 F6F6F6F6 E5F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 E5F6F6F6 F6F6F6F6 ................................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................................
E5F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................................
F6F6F6F6 F6F6F6F6 E5F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 E5F6F6F6 F6F6F6F6 ................................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................................
E5F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................................
F6F6F6F6 F6F6F6F6 E5F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 E5F6F6F6 F6F6F6F6 ................................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................................
E5F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................................
F6F6F6F6 F6F6F6F6                                     ........
```

Figure 2 - The Directory

file hidden so that in a directory search the particular file in question will not appear. Bytes 12 through 21 have 00's as they are supposed to.

Bytes 22 and 23 have the time as you can plainly see. You say you don't plainly see that? It really is a little confusing, so lets take a look:

For the file PROJECT the time is written as 914D. This can be represented as 1001 0001 0100 1101. Referring to our file description on page 14, the first thing we do to translate this is to reverse bytes 22 and 23. So we would get 0100 1101 1001 0001. Now, the leftmost five bits represent the time. This means we have:

$$(0 \times 2^4) + (1 \times 2^3) + (0 \times 2^2) + (0 \times 2^1) + 1$$

which equals 9 AM; if it were 9 PM, we would get 21 (2100 hours).

The next 6 bits represent the minutes. Using the same logic as before, we get 44. The last bits give the number of 2 second increments, 10001 would give us 17 indicating 34 seconds.

Well, that's how the time is represented--somewhat confusing but it does minimize the space needed and that is important to an operating system.

Bytes 24 and 25, which contain an E408, represent the date, and again, we'll examine this closely:

We first switch them.

08E4 = 0000 1000 1110 0100

Now the first seven bytes represent years past 1980. In our case 0000100 represents 4, indicating that the file was made in 1984. The next four digits, 0111, represent the month: 7 (July). The last digits 00100 represent the day, 4 in our case.

So, now we know that PROJECT.BAK was placed on the disk on July 4, 1980 at 9:44 in the morning.

Bytes 26 and 27 give the starting cluster. We will look at that further when we examine the FAT but suffice it to say right now that this file starts at cluster 2.

Bytes 28 - 31 contain the file size with the first word containing the lower order part of the size and both words stored with the least significant byte first. This is

```
Side 0, Track 0, Sector 2
 1st sector of File Allocation Table
FFFFFF03 40000560 00078000 09A0000B C0000DE0 000FF0FF .....@..`.................
11200113 4001FF0F 00000000 00000000 00000000 00000000 .. ..@.....................
00000000 00000000 00000000 00000000 00000000 00000000 ............................
00000000 00000000 00000000 00000000 00000000 00000000 ............................
00000000 00000000 00000000 00000000 00000000 00000000 ............................
00000000 00000000 00000000 00000000 00000000 00000000 ............................
00000000 00000000 00000000 00000000 00000000 00000000 ............................
00000000 00000000 00000000 00000000 00000000 00000000 ............................
00000000 00000000 00000000 00000000 00000000 00000000 ............................
00000000 00000000 00000000 00000000 00000000 00000000 ............................
00000000 00000000 00000000 00000000 00000000 00000000 ............................
00000000 00000000 00000000 00000000 00000000 00000000 ............................
00000000 00000000 00000000 00000000 00000000 00000000 ............................
00000000 00000000 00000000 00000000 00000000 00000000 ............................
00000000 00000000 00000000 00000000 00000000 00000000 ............................
00000000 00000000 00000000 00000000 00000000 00000000 ............................
00000000 00000000 00000000 00000000 00000000 00000000 ............................
00000000 00000000 00000000 00000000 00000000 00000000 ............................
00000000 00000000 00000000 00000000 00000000 F6F6F6F6 ............................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ............................
F6F6F6F6 F6F6F6F6                                     ..........
```

Figure 3 - The File Allocation Table

basically the same idea that Microsoft used when storing the time and date so we won't go through it again, but the file size is 13,024.

There, without much stress we have been able to understand how file information is stored in the directory by DOS 1.1.

The File Allocation Table

In addition to sides, tracks, and sectors, the diskette is also divided into clusters with two sectors per cluster. Since a sector can hold 512 bytes of data, a cluster can hold 1024. The function of the File Allocation Table is to keep track of which clusters are holding which files' data. If data is to be put onto a diskette it is allotted room in 1024 byte chunks at a time. If a file only consists of 1 byte it is still allotted 1024. This may seem wasteful, but every cluster requires a corresponding entry in the FAT. If we decrease the size of the clusters, we increase the size of the FAT and, therefore, increase the amount of time that must be spent looking in the FAT for the next cluster. The designers of this operating system evidently felt that 2 sectors per cluster was just about right.

Since there are a total of 640 sectors per diskette, there are 320 clusters. How many bytes do we need to represent a cluster? Clearly 1 is not enough, it could only represent numbers from 0 to 255. Two would be fine (up to 64k could be represented) but this takes up too much room. Microsoft settled on 1.5 - 12 bits. So, when we talk about offsets in the file allocation table we are talking about groups of three hex characters (a byte and a half!). Since a nibble is half a byte, how about a 'chomp' for a byte and a half?

Let's first look at offsets 0 and 1 in the FAT in Figure 3. Remember, when we talk about an offset in the FAT, we are talking about 1 chomp--a byte and a half. We see FFF for offset 0 and then another FFF for offset 1. The first FFF tells the operating system that we have a double sided diskette. If it were single sided there would be an FFE. The FFF at offset 1 is a filler reserved for future use by IBM or Microsoft.

As mentioned above, the first cluster of our first file is #2, which corresponds to track 0, sectors 3 and 4, of side 1. These relative correspondences can be found in the IBM DOS 1.1 manual, Appendix C. After the operating system has read that cluster, where does it go next? Does our file continue at

DOCID: 4009933

~~FOR OFFICIAL USE ONLY~~

```
Side 0, Track 0, Sector 4
  1st sector of Directory
E5524F4A 45435420 42414B00 00000000 00000000 0000914D ..ROJECT BAK.....M.
E4080200 00360000 324A554C 59202020 42414B00 00000000 .....6..2JULY   BAK.....
00000000 0000ABA4 E3081000 80100000 E5F6F6F6 F6F6F6F6 ................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................
E5F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................
F6F6F6F6 F6F6F6F6 E5F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 E5F6F6F6 F6F6F6F6 ................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................
E5F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................
F6F6F6F6 F6F6F6F6 E5F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 E5F6F6F6 F6F6F6F6 ................
```

Figure 4 - Directory With First File Erased

the next cluster or is it located at some entirely different location on the disk. Or, for that matter, is there a next cluster? This is where the FAT comes in. We read the first cluster which happened to be cluster #2. We are now interested in the next cluster of our data. You take the cluster that you have just read, and if it is an odd number you subtract 1 (in this case you don't do anything because 2 is not odd). You then go into the FAT 2 positions and write down the next two chomps that you find. You should be writing down 034 000.

In general, if we have 6 hex digits:

h1 h2 h3 h4 h5 h6,

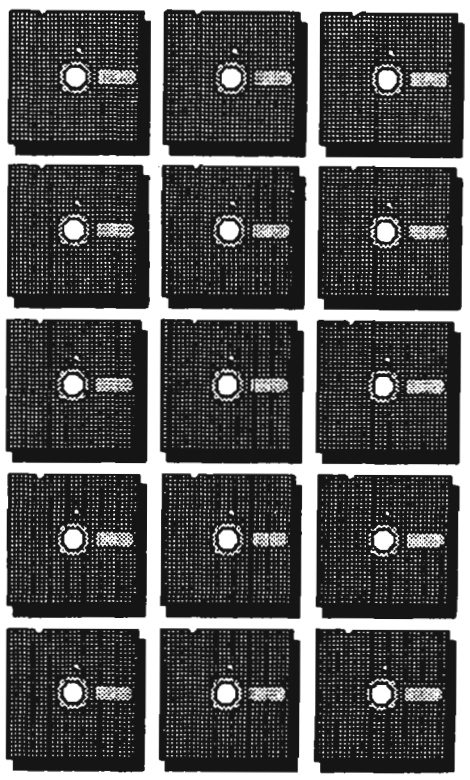
we unscramble them to form two words:

0 h4 h1 h2 0 h5 h6 h3.

OK, let's try that with the 034 000. In this case, the h1 = 0, h2 = 3, h3 = 4, and h4, h5, and h6 equal 0's. Rearranging our numbers we get: 0003 0004. Now, we were interested in cluster #2. Since it is even, we use the first byte (0003), if it were odd we would have used the second byte (0004).

Looking at the FAT again, it does appear that the clusters were assigned in order. Suppose we were interested in the 15th cluster. We count in 14 (remember, with an odd number--15--we subtract 1) groups of 3 hex digits at a time. We come to 0FF0FF. The digits are unscrambled according to the above formula, and we come up with 000F 0FFF. Since 15 is odd, we are interested in the second of the two words. 0FFF is clearly too large a number to represent a cluster and, yes, as you have probably deduced, it indicates an end of file. The 15th cluster of PROJECT.BAK is the last cluster of our file. There is no 16th cluster.

As you can see the FAT is quite important. It is so important that there are two copies of it on the diskette, one in sector 3 and one in 4. If one cannot be read, for whatever reason, hopefully the other one can be. Both the FAT and the directory are read into memory when the system is brought up and are kept there.



~~FOR OFFICIAL USE ONLY~~

DOCID: 4009933


```
Side 0, Track 0, Sector 2
  1st sector of File Allocation Table
FFFFFF00 00000000 00000000 00000000 00000000 00000000 ....................
11200113 4001FF0F 00000000 00000000 00000000 00000000 .. ..@.................
00000000 00000000 00000000 00000000 00000000 00000000 ....................
00000000 00000000 00000000 00000000 00000000 00000000 ....................
00000000 00000000 00000000 00000000 00000000 00000000 ....................
00000000 00000000 00000000 00000000 00000000 00000000 ....................
00000000 00000000 00000000 00000000 00000000 00000000 ....................
00000000 00000000 00000000 00000000 00000000 00000000 ....................
00000000 00000000 00000000 00000000 00000000 00000000 ....................
00000000 00000000 00000000 00000000 00000000 00000000 ....................
00000000 00000000 00000000 00000000 00000000 00000000 ....................
00000000 00000000 00000000 00000000 00000000 00000000 ....................
```

Figure 5 - FAT With First File Erased

Removing Files

Suppose that for reasons of privacy we decide that we don't want anyone to see the file PROJECT.BAK so we erase it. Looking at the revised directory (Figure 4), there is an E5 in place of the first character of the file name but it doesn't appear that anything else has changed.

If we look at the FAT (Figure 5) it appears that the sectors that were being used for PROJECT.BAK are now available. They, of course, are the ones starting at offset 2 (chomps), and continuing for the entire line.

Looking through the diskette (which we will do shortly) you would find that PROJECT.BAK is still there and, in fact, has not been touched.

So, as you can seen, when a file is erased the FAT is changed to indicate that the area taken up by that file is now available. The first character of the file name is changed to an E5. But that's it. The file is still there! If you create a new file, chances are that you will write over the old one but if you erase the file, and then remove the diskette from your computer, you have not done much of anything to assure privacy. If someone decides to go searching through the disk, the FAT could not be used but the name in the directory could probably be recreated and the file could be found. There are, in fact, programs that could make very educated guesses as to what the FAT probably looked like and recreate it for you.

Editing Files

Suppose we decide to edit the first of the two files on our diskette and, in fact, make it longer. What happens? I'll take a file known to be longer, give it the same name as the first file now on the diskette and we will see what happens.

Looking at the new directory (Figure 6), it would appear that the date and time have changed and the file size is bigger. The starting cluster did not change.

Now lets look at the FAT (Figure 7). The starting cluster is the same as before but look at offset #15. Remember we used to have 0FF0FF, which translated to an end of file. If we look at the entry there now, by using our calculations we see that this new longer file takes up the same spaces that the older shorter one did, and then routes itself around the second file, 2JULY.BAK. This is an interesting and important feature of DOS 1.1. A less sophisticated operating system, such as the UCSD p-System would always look for a contiguous area large enough to hold the entire file. If such an area were not found, the user would get an 'out of space' error when, in fact, there may very well be more than enough room. DOS, however, would not do this.

```
 Side 0, Track 0, Sector 4
  1st sector of Directory
50524F4A 45435420 42414B00 00000000 00000000 00002791 .PROJECT BAK.....'..
84080200 808E0000 324A554C 59202020 42414B00 00000000 .....2JULY   BAK.....
00000000 0000ABA4 E3081000 80100000 E5F6F6F6 F6F6F6F6 ........................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ........................
E5F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ........................
F6F6F6F6 F6F6F6F6 E5F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ........................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 E5F6F6F6 F6F6F6F6 ........................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ........................
E5F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ........................
F6F6F6F6 F6F6F6F6 E5F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 ........................
F6F6F6F6 F6F6F6F6 F6F6F6F6 F6F6F6F6 E5F6F6F6 F6F6F6F6 ........................
```

Figure 6 - The New Directory

```
 Side 0, Track 0, Sector 2
  1st sector of File Allocation Table
FFFFFF03 40000560 00078000 09A0000B C0000DE0 000F5001 ....`@..`.............P..
11200113 4001FF6F 01178001 19A0011B C0011DE0 011F0002 .. ..@..o.............
21200223 40022560 02278002 29A002FF 0F000000 00000000 .! .#@.%`.'..).........
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 00000000 00000000 00000000 00000000 00000000 ........................
```

Figure 7, The New FAT

It simply places the file, a cluster at a time, onto the disk. The clusters do not have to be contiguous. Of course, there must be enough clusters available.

An ASCII File

We've looked at an assembly language program (the Boot record), the FAT, and the directory. It would be instructive to look at a couple of ASCII files. The first one that we will look at will be exactly that--a pure ASCII file, and the second one will be an 'almost' ASCII file--a file make by a wordprocessing program.

Figure 8, has a few phrases from "The Midnight Ride of Paul Revere".

This is quite readable without anyone's help. Notice that in the middle of the second line, there is a 0D and then a 0A. This is an ASCII 13, which is a carriage return, and then an ASCII 10 which is a line feed.

The file in Figure 9 was created by one of the more popular word processing programs, Wordstar. So that we may better understand what we are looking for, we will first take a look at the file as it would appear in print:

discussion of the necessities of comparing
the architecture of micro-processors rather than simply relying on a
benchmark or two when attempting to determine the merits of two or
more different devices.
In discussing the 8086, it should also be understood that we are
discussing the 8088. Any reference in this report to the 8086 also
implies the 8088. Where there are differences

Looking at the translation on the right side of Figure 9, it seems almost readable. The first thing that appears to be slightly wrong, however, is that the last ASCII character of each word is not quite right. What's wrong with it? Lets look at the first line. Looking at the string 69 73 63 75 73 73 69 6F EE, we know that the word should be 'discussion', but where is the 'n'? Lets look at the EE:

EE = 1110 1110

If we removed the most significant bit we would have:

110 1110

which is a decimal 110 or an ASCII 'n'. Since only seven bits are required to represent the standard ASCII characters, it appears, then, that what Wordstar did is use the most significant bit of the last character in a word to indicate end of word.

In Wordstar and most other wordprocessors, the typist does not push the carriage return except at the end of a paragraph. As we can see from the above quote, after the word 'comparing' (Figure 9, line 2) there should be a carriage return and line feed. At the beginning of the 5th column in the second row we see an E7. As before, we strip away the left most 1, giving us a hex 67 which is an ASCII 103, the 'g' that we expected. Next to that is a hex 20, a space, and then an 8D.

Pulling our usual operation with the leftmost 1, we would get 0D = 13, a carriage return. Next to that is a 0A = 10, a line feed, then another line feed and carriage return. So it appears that carriage return, line feed combinations which are inserted by the wordprocessor have a 1 in the leftmost position of the carriage return byte.

We can verify this by looking at the end of line 10. There we have a carriage return inserted by the user--end of paragraph. Notice that this time we have 0D 0A 0D 0A whereas before we had 8D 0A 8D 0A. This is how Wordstar knows when it has gotten to the end of a paragraph.

If you have ever wondered why you couldn't use a standard wordprocessor to write Pascal programs, you are probably beginning to see the problem. Since each byte is eight bits and ASCII character representation only requires the least significant seven bits, the wordprocessor has the remaining 128 characters that it can put to very good use. The compiler cannot always recognize these characters.

In the case of Wordstar there actually is a mode which will allow you to write programs but, to allow this, Wordstar has to sacrifice some of its versatility.

DOCID: 4009933


```
Side 1, Track 5, Sector 5
  1st sector of TESTREC
4C697374 656E206D 79206368 696C6472 656E2061 6E642079 .Listen my children and y.
6F752073 68616C6C 20686561 720D0A6F 66207468 65206D69 .ou shall hear..of the mi.
646E6967 68742072 69646520 6F662050 61756C20 52657665 .dnight ride of Paul Reve.
72652E0D 0A4F6E20 74686520 31387468 206F6620 41707269 .re...On the 18th of Apri.
6C20696E 2037352C 0D0A6861 72646C79 2061206D 616E2069 .l in 75,..hardly a man i.
73206E6F 7720616C 6976650D 0A77686F 2072656D 656D6265 .s now alive..who remembe.
72732074 68617420 66616D65 6F757320 64617920 616E6420 .rs that fameous day and .
79656172 2E0D0A0D 0A486520 73616964 20746F20 68697320 .year.....He said to his .
66726965 6E642C20 69662074 68652042 72697469 7368206D .friend, if the British m.
61726368 0D0A6279 206C616E 64206F72 20736561 2066726F .arch..by land or sea fro.
6D207468 6520746F 776E2074 6F6E6967 68740D0A 68616E67 .m the town tonight..hang.
2061206C 616E7465 726E2061 6C6F6674 20696E20 74686520 . a lantern aloft in the .
62656C66 72792061 7263680D 0A6F6620 74686520 4E6F7274 .belfry arch..of the Nort.
68204368 75726368 20546F77 65722061 73206120 7369676E .h Church Tower as a sign.
```

Figure 8 - An ASCII File

```
Side 1, Track 0, Sector 5
  3rd sector of PROJECT.BAK
69736375 7373696F EE206FE6 207468E5 206E6563 65737369 .iscussio. o. th. necessi.
746965F3 206FE620 636F6D70 6172696E E7208D0A 8D0A7468 .tie. o. comparin. ....th.
E5206172 63686974 65637475 72E5206F E6206D69 63726F2D .. architectur. o. micro-.
70726F63 6573736F 72F32072 61746865 F2207468 61EE2073 .processor. rathe. tha. s.
696D706C F9207265 6C79696E E7206FEE 20E1208D 0A8D0A62 .impl. relyin. o. . ....b.
656E6368 6D6172EB 206FF220 7477EF20 776865EE 20617474 .enchmar. o. tw. whe. att.
656D7074 696EE720 74EF2064 65746572 6D696EE5 207468E5 .emptin. t. determin. th..
206D6572 6974F320 6FE62074 77EF206F F2208D0A 8D0A6D6F . merit. o. tw. o. ....mo.
72E52064 69666665 72656EF4 20646576 69636573 2E0D0A0D .r. differen. devices.....
0A202020 202049EE 20646973 63757373 696EE720 7468E520 ..      I. discussin. th. .
38303836 AC2069F4 2073686F 756CE420 616C73EF 2062E520 .8086. i. shoul. als. b. .
756E6465 7273746F 6FE42074 6861F420 77E52061 72E5208D .understoo. tha. w. ar. ..
0A8D0A64 69736375 7373696E E7207468 E5203830 3838AE20 ....discussin. th. 8088. .
20416EF9 20726566 6572656E 63E52069 EE207468 69F32072 . An. referenc. i. thi. r.
```

Figure 9 - A Typical Sector from a Wordprocessor

CONCLUSION

There you have it--a walk through a DOS 1.1 diskette. There was nothing very hard or complicated about what was seen or done and, hopefully the reader has gained some information about an object that is very important in their professional life--a 5 1/4 inch diskette.

BIBLIOGRAPHY

Microsoft, Disk Operating System, IBM Corp. Boca Raton, FL 33432, 1982.

Norton, Peter, Inside the IBM-PC, Robert J. Brady, Co., Bowie, MD 20715, 1983.

-----. The Norton Utilities, Peter Norton, Santa Monica, CA 90403, 1983.

~~FOR OFFICIAL USE ONLY~~

HUMAN FACTORS (U)

P.L. 86-36

by [redacted] P13

Many people tend to think that human factors specialists produce nothing but reports, papers, and advice (usually too late and largely unheeded!). A recent article in the Human Factors Society monthly Bulletin vividly counteracts this limited impression.

"...Buried within human factors R&D work are lots of products that have value, that will solve real problems, and that can and will command the respect of the 'hard' disciplines....For too long we have too often been known as the discipline that produces nothing more than long, boring, cumbersome technical reports. And you know about technical reports--they usually end up on the shelf, never to be read."

A survey made by the author, William B. Askren (Air Force Human Resources Laboratory, Wright-Patterson Air Force Base) revealed a wide range of practical "products" within various projects carried out by his organization and others. He lists them as follows, in order from concrete to less tangible:

- prototypes, mockups, drawings
- handbooks, training curricula, training manuals, users' guides
- algorithms, models, task analyses
- classification schemes, software, methodology, questionnaires, analysis formats
- requirements, regulations, standards, specifications
- costing data, human capacity information, evaluation criteria
- proposals, recommendations, plans, alternatives
- definitions, descriptions, examples, illustrations
- hypotheses, concepts, relationships

Askren continues, "I would propose that it is incumbent upon those of us engaged in human factors R&D projects or application efforts to help our customers define their research requirements in such a way that specific products are identified. Secondly, each product should be made a separate deliverable to the customer. If a technical report is to be prepared as part of the effort, it should be thought of as an adjunct to the products."

I heartily agree, and I believe a large part of the problem arises in the total ignorance on the part of most people about the meaning of "human factors" and what its practitioners can do. At our Agency in particular, most people (if they have heard of human factors at all) seem to think of it as concerned with the "subjective" aspects of terminals, furniture, etc. Human factors is everything that is left over when you take away "hardware", "software", and "cost"! Human factors, these people think, is restricted to "vague", "emotional" things like whether a chair is "comfortable", a screen is "readable", or a console is "attractively styled". We really need to do a strenuous job of education to demonstrate to people that human factors can provide concrete, useful products that make a difference to the success of a project. In fact, at our Agency, a great many things that should be done with the advice and aid of human factors specialists are being done by engineers and technicians without the faintest regard for any but technical considerations. Many things that are defined as "hardware" and "software" are really basic human factors issues and problems. For example, what about control of the cursor on a VDT? Our managers define this as "software" or "hardware", because it is implemented in a board or program. But isn't the behavior of the cursor a central issue for the USER of a system? I think cursor behavior is a HUMAN FACTORS issue, not just "software" or "hardware. What do you think?

~~FOR OFFICIAL USE ONLY~~

OCID: 4009933

SOME RECENT ARTICLES AND PUBLICATIONS

Readability of Text Scrolled on Visual Display Terminals as a Function of Window Size
R.L. Duchnicky and P.A. Kolers
Human Factors Journal, Vol. 25, No. 6, December 1983, pp. 683-692.

ABSTRACT: "Readability of text scrolled on visual display terminals was studied as a function of three different line lengths, two different character densities, and five different window heights (either 1, 2, 3, 4, or 20 lines). All three variables significantly affected reading rate, but to markedly different extents. Lines of full and two-thirds screen width were read, on average, 25% faster than lines of one-third screen width. Text appearing at a density of 80 characters per line was read 30% faster than text in a format of 40 characters per line. Text appearing in windows four lines high was read as efficiently as text in 20-line windows, and text in one- or two-line windows was read only 9% more slowly than text in 20-line windows. Comprehension of the passages did not vary as a function of window size, indicating that subjects maintained a constant level of comprehension by varying their reading rate. Implications of the results for mixing text and graphics and for limited-capacity electronic displays are discussed."

Ergonomics in Technical Communication
Peter Martin
IEEE Transactions on Professional Communication, Vol. PC 27, No. 2, June 1984, pp. 62-64.

ABSTRACT: "The technical communicator must be a 'human engineer' because a communication, like a computer system, can be a technical success but a practical failure if its design discourages its use. Four parallels between technical communication and user-friendly systems are discussed: (1) Its overall structure should be apparent to the user; (2) it should be congenial without being chatty or too personal; (3) its nomenclature and syntax must be consistent throughout all functions; and (4) its logic must not trap users in loops but should lead them straight to their goals."

Not Seeing is Relieving:
Invisible Writing With Computers
Stephen Marcus and Sheridan Blau
IEEE Transactions on Professional Communication, Vol. PC 27, No. 2, June 1984, pp. 69-72.

ABSTRACT: "Word processors with adjustable video screens are used to test students' writing facility with and without visual feedback. Lack of visual feedback seems to have a salutary effect in forcing concentration onto emerging thoughts rather than words and sentences. It also prevents interrupting the train of thought to edit and correct every few sentences. 'Local editing' is regarded as counter-productive because it deals with individual words and lines instead of reconceptualization and reorganization. For some students, however, the lack of feedback per se was disturbing and thought disrupting."

(NOTE: This is a really intriguing paper, with some provocative concepts. Especially interesting are the subjects' quoted comments on the inability to see what they had written, and the effects on their thinking. MED)

A Study of Revising and Editing at the Terminal,
Jean A. Lutz
IEEE Transactions on Professional Communication, Vol. PC 27, No. 2, June 1984, pp. 73-77.

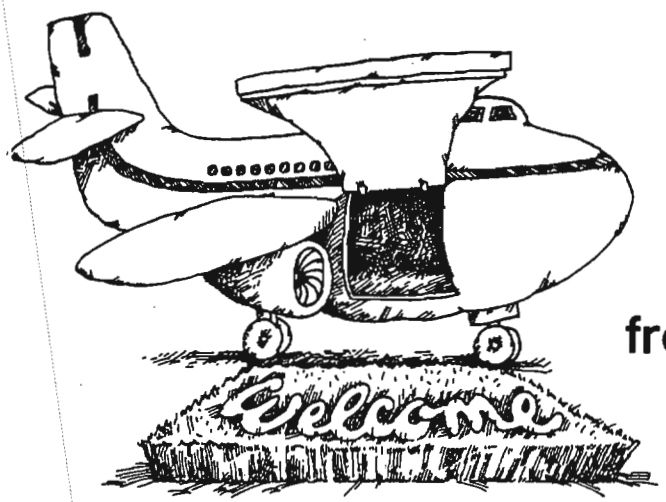
ABSTRACT: "This paper presents the results of a comparative study of experienced writers editing and revising at a word processor and with pen and paper. Seven writers performed four writing tasks, each of which provided several kinds of data. Among these are statistical analyses and graphs of a chronological record of changes made in both modes and summaries of interviews with the subjects after each writing task. Results suggest that the word processor directly alters a writer's composing style."

(NOTE: this is another highly interesting paper. It brings up a point that I have never seen expressed before, but which seems to agree with my own subjective experience over many years of composing, revising my own writing, and editing others' writing both on paper and at a terminal. It appears likely that the terminal provides a somewhat smaller, more linear, and more restricted psychological "window" into a document than a book or sheets of paper. It functions more like a tape and less like a random access memory. This is no problem for most writers with their own compositions, since they have a relatively clear concept of the structure at a high level. When editing others' papers, however, or using reference materials, the smaller mental "window" can be a hindrance. Even in my own writing, I often prefer to print out a draft and make final revisions on paper to get a feel for the document as a whole. If the terminal does, indeed provide a smaller, more linear psychological "window" for the user in contrast to printed books or pages, there are important implications for automation of some of our analytic tasks. I recommend this article. MED)

DOCID: 4009933

EO 1.4.(c)
P.L. 86-36

CAN YOU TOP THIS (U)



?

from E. Leigh Sawyer, B

1961. End of a lengthy TDY to sites in Europe [redacted] Ready to go home. Pan-Am flight out of Orly. All on board. Capacity load of passengers, freight, mail, and fuel. 707 trundles out to end of runway. Swings around for takeoff. Final checks. Can see all sorts of funny control devices in wing sliding back and forth, going up and down, and so on. Observe that wing is remarkable hunk of engineering. All set now. Jets on full power. Brakes released. See man near runway with hands over ears. Must be dickens of a noise out there. Pretty close to rotation now. Plane lifts off. Strange thing. No familiar clunk noise as soon as wheels leave runway. Stranger thing. Angle of climb barely perceptible. Terrifying thing. Plane airborne 10 to 15 seconds and still only 20 feet off the ground. More terrifying thing. Plane is yawing badly left and right. First reaction is rapid calculation of ongoing insurance and special flight insurance to know how much wife will get. Total acceptance. This is where I buy the farm. For the next half hour, pilot earns pay for next five years. Wins fight to claw plane up to 2,000 feet. Intercom comes on. Pilot's voice. Cool, confident. The father image ("Daddy's taking us for a ride today"). "Lost engine on takeoff beyond rotation. Airplane didn't want to fly. Sorry for inconvenience. Will circle Orly for next hour dumping fuel." Landed safely. Passengers wined and dined during engine change. Duty free liquor store open. Most of passengers were floated on board three hours later. Seemed very carefree. I passed out before takeoff. Woke up over middle of Atlantic. Pilot comes to mind. Pushing 60. Gray hair. Probably logged over 1,000,000 miles. Thank you, pilot, God bless you.

Wayne,

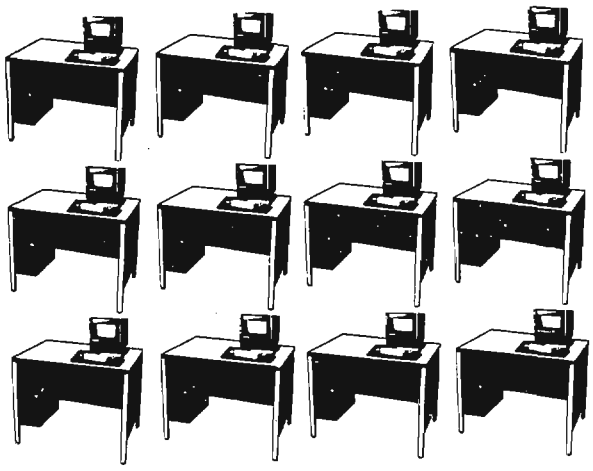
Have you ever considered the endless number of unusual experiences, both humorous and serious, that have befallen TDYers all over the world? They would make for a very entertaining book. How about a Cryptolog feature called something like "Can You Top This?" If people responded to it, it could ultimately make for a very intriguing collection of anecdotal tidbits. Attached is a case in point.

E. Leigh Sawyer

DOCID: 4009933

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36



PERSONAL COMPUTING IN A GROUP (U)

by [redacted] A63

(U) This paper is a slightly expanded version of a paper given at the CISI Spring Conference in May 1984.

Introduction

Relevancy of the topic. The subject matter of this paper is particularly relevant for at least three related reasons. First, personal computers are relatively new at NSA. In fact, they arrived on a large scale less than a year ago beginning around November 1983. Second, they are numerous. It is estimated that there are over 2,000 personal computers at NSA at present. Third, because they are new and because there are a lot of them, questions are being raised regarding their usefulness and their capability of being applied to every day agency problems as well as their effect on the organizations that have acquired them.

Currency of the data. Since they are so new at NSA, it is not illogical to assume that any study concerning personal computers that is undertaken at this time will find the data in a state of flux. It is, therefore, worthwhile to note that all the data that was gathered for this study is current as of April 1984 and is subject to change.

Definition by features of 'personal computer'. In order to properly discuss any subject, it is useful to define it in sufficient terms so that any misunderstanding resulting from its mention will be minimized. Accordingly, for the purposes of this paper, we define 'personal computer' to be a single user micro computer programmable by the user, and with a price under $10,000. The three essential features in this definition, as discussed below, effectively define the set of 'personal computers' to include systems such as IBM PC, IBM PC/XT, TRS 80, and Apple II, to mention just a few.

On the other hand, examples of systems not members of the set include the Hewlett Packard 9845, Wicat Systems 150WS, and the Xerox 860. The first does not meet the set criteria since its cost is in the $30,000-and-above range. The second is a multiuser microcomputer system with a base price in excess of $10,000 and thus it fails to satisfy two out of the three set criteria. The last system does not qualify as a member of the set since it is a dedicated word processor and not programmable by the user.

Single user. The 'single user' feature means that the resources of the computer are not shared and are for the exclusive use of a single user under normal circumstances. Although there is at least one operating system for microcomputers out on the market that is advertised as a multiuser system (Venix, a UNIX look-alike), the vast majority of personal computers are not equipped with the required hardware or software to handle more than one user at a time.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009933

Average cost under $10,000. Although the 'price under $10,000' feature seems arbitrary at first glance, there is some supporting evidence for such a choice. In the April 1984 issue of PC WORLD, 46 personal computers were compared in terms of cost and hardware features. They ranged in price from a low of $1995 to a high of $14,995. It is notable, however, that only one system out of the 46 reviewed cost more that $7300--the GRiD Tempest, a briefcase portable with 256K of RAM, 384K of bubble memory, and a 300/1200 bps modem to list just a few features. The average cost for all 46 personal computers reviewed was $3723--well under $10,000.

Programmable by user. The 'programmable by the user' feature was included as part of the definition to exclude turnkey systems dedicated to a specific function--such as standalone word processors. Normally, these kinds of microcomputers do not have the software necessary to allow the average user to write and execute programs on them.

Collection of the data. An informal phone survey was used to determine the organizations within A Group that have personal computers. A questionnaire was then prepared that covered the following topics:

(1) type and quantity of personal computers;

(2) off-the-shelf personal computer software used;

(3) applications on personal computers;

(4) operational policies regarding personal computers;

(5) problems and concerns relating to personal computers; and

(6) personal computer hardware and software support.

The questionnaire was then applied in personal interviews arranged with each organization in A Group that was determined to have personal computers. A total of 34 organizations were interviewed.

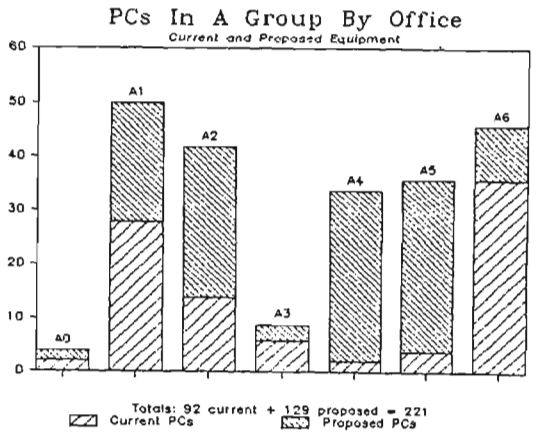
Although the results of the interviews revealed a fairly large proportion of interesting and innovative applications using personal computers, a detailed description of these applications is beyond the scope of this paper.

Topic arrangement. The topics covered in this paper are roughly the same as those covered in the questionnaire. Section 2 covers the distribution of personal computers in A Group. Sections 3 and 4 deal with off-the-shelf and custom software and the way in which they are applied. On the other hand, the final sections deal more with the human aspect: section 5 examines operational policies for personal computers, section 6 takes a look at users' problems and concerns, while in section 7 user support for personal computers is investigated.

2. Distribution of personal computers in A group

This section looks at several aspects relating to the distribution of personal computers throughout A Group: the distribution of current hardware in relation to the distribution of proposed hardware, the ratio of users to personal computers, the types of personal computers and the quantity of each, the functional break-down of personal computers, and the distribution of personal computer usage.

Figure 1

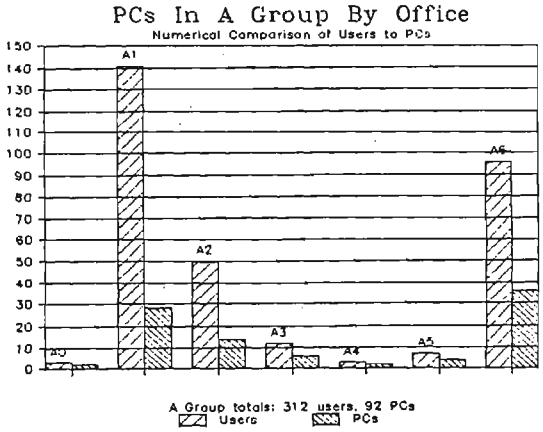


Current and proposed quantity of personal computers. In Figure 1, the data show that A Group currently has a total of 92 personal computers with another 129 systems proposed for the next six-month to one-year period. It should be pointed out that some organizations indicated that they would like to acquire a quantity of agency standard terminals (AST) in the coming year. Since, however, the AST has not yet been officially selected, it remains an unknown and for this reason data of this type were not included with the data for proposed acquisitions.

The distribution by Office is as follows. A0 currently has two personal computers and would like an increase of two in the next year for a total of four. A1 has at present 28 and desires 22 additional units for a total of 50. There are currently 14 personal computers in A2 and 28 new units are desired for the coming year for a total of 42. A3 would like to increase its current six units by three for a total of nine. A4 presently has two personal computers and would like 14 units in the coming year. A5, with four personal computers at present, would like to add 32 new units in the coming year. Finally, A6 currently has 36 personal computers and would like 10 additional units in the coming year.

Numerical comparison of users to personal computers. The data indicate that throughout A Group there is an overall user-to-personal computer ratio of 3.39 to 1 with 312 users for 92 personal computers. As shown in Figure 2, these data are broken down by Office with the greatest concentration of users and personal computers appearing in A1, A2 and A6. The totals are as follows:

Figure 2

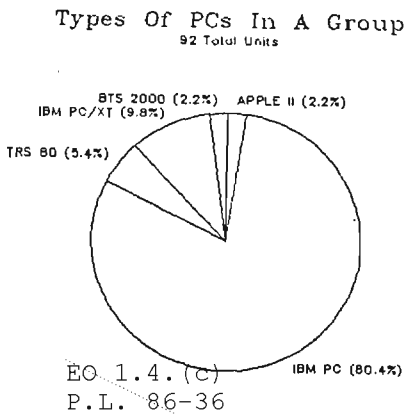


A0: 3 users, 2 personal computers (1.5 : 1)
A1: 141 users, 28 personal computers (5 : 1)
A2: 50 users, 14 personal computers (3.6 : 1)
A3: 12 users, 6 personal computers (2 : 1)
A4: 3 users, 2 personal computers (1.5 : 1)
A5: 7 users, 4 personal computers (1.8 : 1)
A6: 96 users, 36 personal computers (2.7 : 1)

Types of systems and their distribution. The data in Figure 3 show that there are only five types of personal computers in A Group that satisfy the criteria outlined in Section 1.3 above. These are: IBM PC (74 units), IBM PC/XT (9 units), Radio Shack TRS 80 (5 units), Apple II (2 units) and Tri-information Systems BTS 2000 (2 units).

Typical equipment configurations. In investigating the equipment configurations for each of the five types of personal computer, it will be noticed that color monitors are conspicuously absent. One of the main reasons for this absence seems to be that color monitors currently are TEMPEST approved only for zones 4 through 5. Another general trend due to the TEMPEST character of the equipment is the almost total lack of hard disk drives. There are only seven personal computers in A Group with hard disk drives at present.

Figure 3



EO 1.4.(c)
P.L. 86-36

configurations include 2 floppy disk drives and a printer--usually a dot matrix graphics printer. Typical equipment configurations for each of the five types of personal computer are listed below.

IBM PC. Most of the IBM PCs have 2 floppy drives, 1 printer, a monochrome monitor and 128K, 256K, 384K or 512K of RAM--depending in part on how they were acquired. Those units acquired through the PCIC come with 512K of RAM, while personal computers acquired by sole source or competitive bid vary in the amount of memory and type of peripherals according to the organization's requirements at the time. IBM PCs used only as dumb terminals do not, in general, have printers.

IBM PC/XT. As a general rule, the standard configuration for IBM PC/XTs is 512K of RAM, 1 floppy drive, 1-10M hard disk drive, 1 printer and a color monitor. As indicated elsewhere, seven of the nine IBM PC/XTs have color monitors.

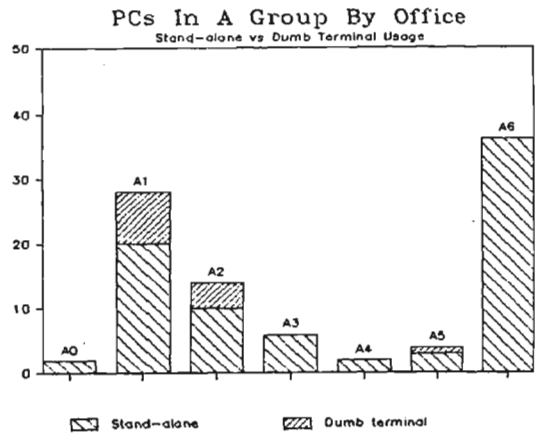
Radio Shack TRS80. Aside from the usual personal configuration of 2 floppy drives (one has 3 floppy drives), 1 printer and a monochrome monitor, the TRS 80s have either 48K or 128K of RAM.

Apple II. While both Apple IIs have 2 floppy drives and a printer, one has 48K of RAM and a monochrome monitor and the other has 184K of RAM and both a color and a monochrome monitor.

BTS 2000. Both BTS 2000s have 64K of RAM, 2 floppy drives, 1 printer, a monochrome monitor, and 3 communications ports.

Functional break-down. The question posed here was how many personal computers are being used solely as dumb terminals as opposed to stand-alone computers. As indicated in Figure 4, there are personal computers in A1, A2, and A5 that are used only as dumb terminals. 86% (or 79) of the current personal computers in A Group are being used only in stand-alone mode, while 14% (or 13--8 in A1, 4 in A2 and 1 in A5) are being used as dumb terminals.

Figure 4



Present and future acquisition methods. Three principle means of acquiring personal computers have been used in A Group:

(1) PCIC;

(2) sole source procurement; and

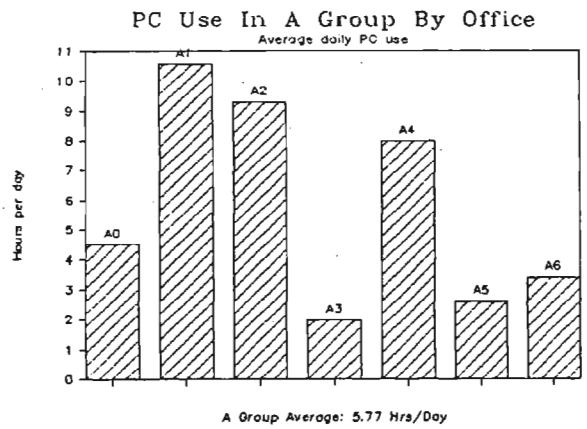
(3) loan from another organization.

64% of the organizations interviewed indicated they would not change their method of acquiring personal computers in the coming year.

Use of personal computers on a daily basis. The data in Figure 5 indicate that the average time per day that personal computers are used in A Group is 5.77 hours. Personal computer usage broken down by Office is most in A1, A2 and A4. It should be noted that a contributing factor to the high daily average in A1 is the fact that six personal computers are being used as dumb terminals 24 hours per day. The Office averages are as follows:

DOCID: 4009933

Figure 5



A0: 4.5 hours per day
A1: 10.6 hours per day
A2: 9.3 hours per day
A3: 2 hours per day
A4: 8 hours per day
A5: 2.6 hours per day
A6: 3.4 hours per day

3. Off-the-shelf software

Figure 6 shows the off-the-shelf software that is currently being used in A Group. Organizations were also asked to subjectively rate the software they use on a 1 to 10 scale of poor to excellent. The results are shown in column three. Note that the software with the greatest number of users (seven or more) is available through the PCIC. Looking at the packages (exclusive of the operating system MS DOS) which have the greatest amount of users, it is interesting to note that 56% of the dBaseII users had specific complaints--which may account for its 6.8 overall rating. On the other hand, only 33% of Word Star users and 37.5% of Lotus123 users had complaints about these packages. The complaints referred to were in response to question number 10 of the questionnaire: "what needs of your organization are not being met by current off-the-shelf software?"

4. Applications

Three general categories of applications are examined in this section: applications with off-the-shelf software, applications with custom designed and written software and applications which interface off-the-shelf software with custom written software. It should be noted, however, that there are currently only two examples of the third category in A Group. For this reason as well as the fact that one of these applications uses only off-the-shelf software, Figure 7 treats them as commercial software applications.

The purpose of the data arrangement in Figure 7 is to show how organizations use their personal computers. Notice that 50% of the 34 organizations interviewed have applications using off-the-shelf software only while 35% of these organizations have applications using both off-the-shelf software and custom-written software. Only 6% have only custom-written applications, while 9% have no applications. Organizations with no applications are, in general, using their terminals as dumb terminals only.

Applications with off-the-shelf software. Off-the-shelf software is being used in A Group in three principle ways: for text processing, for management or project tracking systems, or for data base applications.

Text processing. The software being used for this type of application is Word Star, Volkswriter, Easy Writer, Edix + Wordix, and Professional Editor. At least four organizations indicated that they use Word Star as a program editor, while one organization uses it to produce graphics-like charts.

Tracking systems for management and projects. The software used in this type of application is Lotus123, Multiplan, and Supercalc--the spreadsheet packages. In general, these applications are relatively small.

Data base applications. For the purposes of this survey, a data base on a personal computer is classified as small (less than 50,000 bytes), medium (50,000 to 175,000 bytes), and

~~FOR OFFICIAL USE ONLY~~

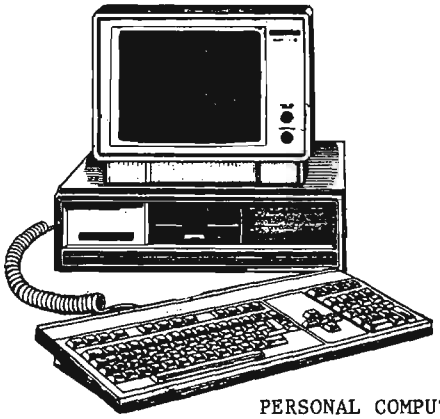


Figure 6

PERSONAL COMPUTER OFF-THE-SHELF SOFTWARE IN A GROUP
Average Rating by Users on a 1-10 Scale

	software name	hardware	rating	number of responses
	APPLE DOS	APPLE	8	1
	APPLE PASCAL	APPLE	8.5	2
	CONDOR	IBM	7.8	2
	CP/M	APPLE	7	1
o	DBASE II	IBM	6.8	16
	DDIT	IBM	9	1
	EASY WRITER	IBM	4.5	2
	EDIX + WORDIX	IBM	8	1
	LATTICE C	IBM	7.3	5
o	LOTUS 123	IBM	8.8	8
	MAXIMANAGER	TRS 80	8	1
o	MS DOS	IBM	7.7	22
o	MS DOS BASIC	IBM	8	7
o	MULTIPLAN	IBM	6.6	7
	NORTON UTILITIES	IBM	9	1
	OPEN ACCESS	IBM	8	1
	PC CRAYON	IBM	6	1
	PC FILE 3	IBM	8	1
	PC/IX	IBM	8.5	2
	PFS FILE	IBM	7	1
	PFS REPORT	IBM	7	1
	PL/I-86	IBM	8	3
	PROFESSIONAL EDITOR	IBM	6	2
	PROFILE 3 PLUS	TRS 80	10	1
	QUICKCODE	IBM	9	1
	QUNIX	IBM	8.3	2
	QUNIX C	IBM	7	2
	R:BASE 4000	IBM	9	2
	SCRIPSIT	TRS 80	8.3	3
	SUPERCALC	IBM	6	2
	SUPERSCRIPSIT	TRS 80	7	1
	VOLKSWRITER	IBM	9	1
o	WORD STAR	IBM	7.8	21

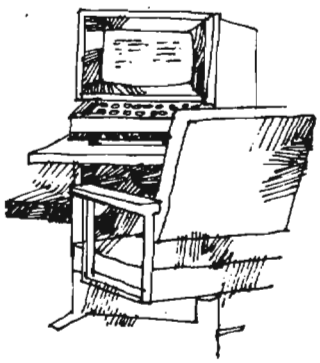
~~FOR OFFICIAL USE ONLY~~

DOCID: 4009933

Figure 7

APPLICATIONS WITH PERSONAL COMPUTERS IN A GROUP

(34 divisions or branches interviewed)



IN-HOUSE
CUSTOM-WRITTEN
APPLICATIONS

COMMERCIAL SOFTWARE APPLICATIONS	none	one	multi
none	3	2	0
one	8	2	0
multi	9	7	3

TOTAL ORGANIZATIONS: 20 + 11 + 3 = 34

large (over 175,000 bytes). For the data base software currently being used, it is a given that a data base is limited to the size of the disk--with the exception of those systems with hard disks this means an upper limit of about 300,000 bytes (exclusive of any indexes).

The software used is mostly dBaseII with a very small number of applications using Condor and R:Base 4000. dBaseII applications range from small data bases to large data bases with typical applications being inventory control, personnel tracking, job profile tracking, and clearance tracking. For organizations using dBaseII, ten have small data base applications, two have medium data base applications, and four have large data base applications.

Applications with custom designed and written software. The most varied applications are those that are custom designed and written using a programming language such as BASIC, C, or Pascal. Although, as Figure 7 shows, only 41% of the organizations interviewed have written any custom designed software, they are broken down into seven functionally different applications. These applications are categorized by Office as follows:

A1: a text editor written in C and two separate device control software projects written in C and BASIC, respectively

A2: collection processing and reporting in the field

A3: signals analysis software using Pascal on an Apple II

A5: graphics written in C

A6: text format translation from personal computer format to a format compatible with PWB, written in BASIC and collection management software written in C

Applications interfacing different software packages. A1 has a budget planning system that interfaces Lotus123, Word Star and dBaseII. A6 has an educational software application that interfaces dBaseII with custom software written in BASIC.

5. Operational policies and procedures

In general, it seems that there is an absence of formal operational policies regarding personal computers due to the lack of large enough concentrations of personal computers in any one organization. The two exceptions in A Group, A4 and A6, are discussed below. The remainder of A Group organizations have in general some informal procedures they follow that deal with security and training, for the most part. Informal security procedures include periodic back up of files, locking up data diskettes at night, ensuring that the personal computer is turned off at night, while training involves either getting a manual and learning by trial and error, using an automated tutorial, if available, or having an experienced user tutor the new user.

On the other hand, both A4 and A6 have formal written operational policies (A4's is still in draft form). The topics covered in the draft version operational policy of A4 are: security, standardized files, procurement of software, supplies, management of hardware, and assistance.

A63, with the largest single concentration of personal computers in A Group, has two operational policies: one dealing with installation and the other with operation. The IBM PC Hardware/Software Installation Plan covers:

[] installation phases;
[] installation personnel;
[] installation schedule;
[] equipment control;
[] identification of standard software package;
[] software distribution plan;
[] identification of IBM PC supplies to be stocked; and
[] training schedule, material, and categories.

The IBM PC Hardware/Software Policy deals with the following topics:

[] hardware management;
[] acquisition and distribution of supplies;
[] maintenance;
[] software evaluation;
[] software management;
[] training; and
[] security.

6. Problems and Concerns

The final question on the questionnaire asks the interviewee to list any problems or concerns the organization has, in general, regarding personal computers. Out of a total of 34 organizations interviewed, 25 indicated that they had such problems and concerns. A total of 66 problems/concerns were listed for an average of 2.6 per organization. The responses fall roughly into six categories:

[] acquisition and installation of hardware and software;
[] training and support;
[] general operation and maintenance of hardware;
[] human interface with the hardware and software;
[] intermachine communications; and
[] security.

Acquisition and installation of hardware and software. Sample responses were:

[] no dust covers are provided or are generally available;

[] not enough personal computers are available: waiting for the AST impedes acquisition of personal computers which it may render obsolete;

[] there are too many bureaucratic levels to go through in the procurement process;

[] supplies are hard to get and there are many delays;

[] there is a need for color graphics, but the standard configuration does not have a color monitor; and

[] there is no mechanism for upgrading the personal computer hardware.

Training and support. Among the problems listed were

[] software manuals are difficult to understand and use;

[] personal computer training and support is not centralized, thus causing the user to waste time and effort learning by trial and error;

[] there is an overall lack of planning for training and support and not enough to go around;

[] training at the branch and division level needs to be conducted regarding the usefulness of personal computers; and

[] software evaluations need to be centralized, published and distributed on a regular basis to the users.

General operation and maintenance of personal computer hardware. Typical problems listed in this category were:

[] the graphics printer is too slow;

[] personal computer response time is too slow; and

[] there is not enough memory or peripheral storage for some applications.

Human interface with personal computer hardware and software. Some sample responses in this category were:

[] the keyboard is poorly designed and therefore difficult to use accurately;

[] images on the monochrome monitors are fuzzy and difficult to read, which causes eye strain;

[] the available software and documentation are too complex for user requirements and difficult to understand;

[] there is not enough space to put the personal computers;

[] the graphics printer is too loud and disturbs co-workers; and

[] several personal computers in the same area give off enough heat to make the room uncomfortably warm.

Intermachine communication. This category includes problems expressed concerning networking as well as communications to a host computer. Sample problems listed were:

[] networking is not being addressed despite a requirement for it;

[] the reliability of file transfer between a host and personal computer is doubtful;

[] there is a need to have communications hook up to main frames;

[] there needs to be an efficient, quick method for inputting large quantities of information from a host computer; and

[] there is a need for Xerox 860 compatibility.

Security. Problems listed under this category included:

[] there is a need for a removable hard disk capability;

[] organizations fear the proliferation of compartmentalized data;

[] there is no password security; and

[] TEMPEST should be done before acquisition of hardware.

7. Support

The questions addressed in this section deal with where A Group personal computer users currently get hardware and software support, if any, and the existence of a local, centralized support within A Group.

Sources currently cited by A Group users. Figure 8 shows that seven sources for personal computer support were cited. These include: 'individuals in A Group', A109, A63, B6, the PCIC, T2, and T3. Interestingly enough, eleven organizations (32%) indicated that they receive no support at all. A slightly larger number indicated that A63 provides support--although it should be borne in mind that fourteen of the organizations interviewed are in A6. In other words, it would seem that the role of A63 to provide computer applications support for all of A Group is not yet widely understood--at least in the context of personal computers.

Figure 8

According to official A63 memoranda dated 22 February and 1 May, A63 is equipped to provide the following support to A Group personal computer users:

[] hardware/software consultation,

[] software demonstrations and training;

[] hardware demonstrations and training;

[] off-the-shelf software evaluations; and

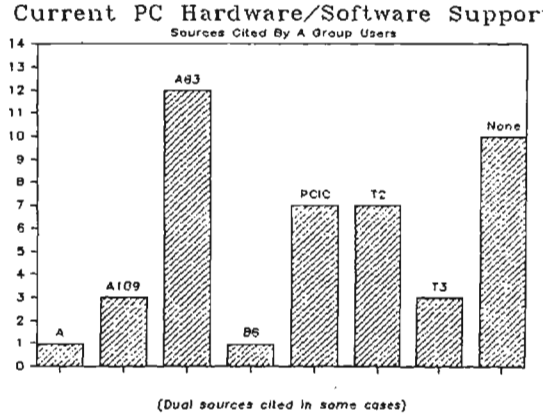
[] a personal computer users group.

The PC users group meets once a month for an hour and is an excellent opportunity for A Group users to exchange ideas and discuss mutual problems. In addition to these services, A63 currently provides personal computer applications development support to A606 and A2.

8. Conclusions

PCs have been in A Group only a relatively short length of time and thus it should be stressed that the situation regarding PCs in A Group is transitory and will likely change in many ways. There is naturally some reticence on the part of prospective users who are used to the power of a main frame to recognize the utility of the PCs. At the same time, in-house training and software evaluation were not initially available to user's on an official basis and are only now starting to develop. As a result, inexperienced users are experiencing some frustration and hence many PCs are not being fully utilized. Other reasons include the fact that most organizations do not have communications to main frames yet although they have a requirement to work with data stored on the main frame.

Current PC Hardware/Software Support



DOCID: 4009933

FACTION LINE (U)

Dear Faction Line:

Something must be done before it is too late! We are approaching a situation akin to the "critical mass" in the cafeteria. I refer to the "to and fro gang." You can see them any day wandering about looking for a table, knuckles growing white holding their trays as desperation assails them, their eyes flickering endlessly in 360° sweeps, and their food, so near yet so far, growing cold. What is needed are bold and innovative measures. A few of these are addressed as follows.

Make people eat faster. This may be subdivided into two categories: (1) chewing and (2) gulping. It is suggested that M7 monitor chewing and gulping norms as they currently exist on the part of those eating in the cafeteria. Based upon physiological stress standards as they affect the alimentary tract, it is believed that more rapid chew and gulp rates may be achieved. Special courses or seminars to this end could be established in order to enable personnel to meet newly prescribed standards for chewing and gulping. In order to raise motivations, a new skill field in this area should be established which could lead to certification and even bonuses, e.g., FLAP (Food Loading Acceleration Pay). Further, for those achieving chew/gulp rates (CG/r) faster than prescribed, compensatory leave should be allowed. This could be achieved by a time card check in/check out system at the entrance to the cafeteria or even possibly tied into the new badge system by assigning everyone a "GIN" (Gastronomic Intake Number).

Use larger forks: doubling the size of forks would double intake. In this regard, forks should be provided in two configurations: one twice the length and one twice the width in order to conform to varied oral specifications. The large fork factor (LFF) when combined with CG/R would materially accelerate consumption time (CT). In short, LFF + CG/R = CT. The same approach should be used for spoons, and, when peas are on the menu, knives. Thus we can also add both large spoon factor (LSF) and a large knife factor (LKF). Therefore, even when a person has soup, and a hot plate with peas, it still obtains that

$$CG/R + LFF + LKF + LSF = CT.$$

Use higher tables or lower chairs. This lessens the distance the arm must travel between plate and mouth. The optimum distance is suggested as two inches, as opposed to the more normal distance of 18 inches. This would increase by a factor of 9 the rate of food intake (9 x RFI). When combining RFI with increased CG/R and the realization of LFF/LSF/LKF, CT should be reduced to approximately three minutes, a savings of 27 minutes based upon current standards. When calculated against a loss of $300,000,000 per annum for the nonproductive cafeteria time of 15 extra minutes a day beyond the prescribed half hour, the savings of 27 minutes a day would add $540,000,000 of production rate per annum beyond the normal work year of the federal establishment. With perhaps $40,000,000 of this employed to subsidize free antacids, the new cost-out of increased production rates would still be substantial. Lets move out smartly! It is time to clip the wings of this octopus!

Cal D. Lator

DOCID: 4009933

~~FOR OFFICIAL USE ONLY~~

NSA-Crostic No. 59

by David H. Williams

Here's another puzzle in the cryptic vein. If you're not familiar with this type of definition, and would like to give it a try, call the author on 1103s, and you'll be sent an explanation of how these clues are put together.

*	*	1 V	*	2 S	3 C	4 P	5 G	6 D	7 E	8 I	9 B	10 A	11 T	*	12 G	13 U	14 S	15 J
16 E	*	17 R	18 M	*	19 Y	20 P	21 B	22 G	23 M	24 S	*	25 V	26 P	27 E	28 A	*	29 K	30 A
31 P	32 B	33 C	34 G	*	35 S	36 B	37 A	38 K	39 G	*	40 N	41 H	42 L	43 G	*	44 N	45 V	46 L
*	47 Y	48 L	49 T	50 B	51 D	*	52 Q	53 P	*	54 Q	55 I	56 S	57 Y	58 N	*	59 I	60 S	61 F
62 A	63 V	64 P	65 H	66 G	67 D	*	68 Y	69 M	70 I	71 P	72 S	73 G	*	74 U	75 E	76 I	77 D	*
78 E	79 J	80 Y	81 D	82 O	83 I	84 G	*	85 A	86 C	87 F	*	88 V	89 D	90 H	91 Y	92 O	93 I	94 G
95 J	*	96 G	97 P	98 S	99 Q	100 E	101 X	102 A	103 T	104 K	*	105 E	106 V	107 R	108 B	109 C	110 G	*
111 W	112 U	*	113 Z	114 E	115 a	*	116 J	117 C	118 P	119 B	120 N	121 O	122 U	123 G	124 I	*	125 X	126 G
127 I	128 D	129 P	130 E	131 O	*	132 M	133 U	134 S	135 E	*	136 G	137 X	138 P	139 B	140 Y	*	141 I	142 a
143 E	144 Y	145 B	146 P	*	147 J	148 A	149 P	150 W	151 E	*	152 a	153 R	154 N	*	155 I	156 S	157 A	158 X
159 C	160 F	161 T	162 P	163 Y	164 F	*	165 O	166 H	167 I	*	168 T	169 D	170 Z	*	171 F	172 P	173 a	174 T
175 Y	*	176 B	177 D	178 Z	179 M	180 P	*	181 D	182 K	183 W	*	184 S	185 Y	186 R	187 B	188 R	189 I	190 P
191 G	192 E	193 C	*	194 R	195 B	196 P	197 C	198 I	199 A	200 H	*	201 P	202 B	203 I	204 G	205 A	206 H	*
207 a	208 F	*	209 P	210 B	211 V	212 J	213 Q	*	214 I	215 E	216 W	*	217 T	218 S	219 L	dhw	*	*

A. Did Dale counterfeit tickets to battleground (2 wds)

B. When visiting with a boor, never sing Dorothy's great song (3 wds)

C. Call this Greek by phone on Roman 10

D. Ax me not where to bury this (2 wds)

E. Where the much bejeweled lady wore her sixth ring (4 wds)

102 30 205 10 199 28 85 62 157 37 148

108 21 139 195 50 202 36 119 210 32

145 9 187 176

117 109 33 3 197 159 86 193

67 169 77 177 81 128 6 51 89 181

192 143 135 105 7 215 27 100 75 78

151 114 130 16

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009933

F. Ease peas are for the doctor

61 208 160 171 164 87

G. Try to use Indian blight in indiscernible circumstances

191 39 84 22 110 12 126 66 34 204

5 73 43 136 96 123 94

H. Frank camera

90 65 166 200 41 206

I. "The New Colossus": The *other* structure with which Alexander Eiffel was associated (3 wds)

93 127 8 70 189 55 203 214 141 59

155 83 76 198 124

J. He wanted Ned, Dee and Sam

15 79 212 95 116 147

K. Cross off King Tut's middle name

38 29 104 182

L. Ran into little Edward and gave him his share

219 48 42 46 167

M. Bury between

69 18 132 23 179

N. These reptiles enjoy tea amid the cardinal points

58 120 40 44 154

O. Literally, Greek magma

131 165 121 82 92

P. In a state of stimulation, it has a fixed period of expiration (3 wds)

201 118 149 4 196 64 180 20 53 172

129 31 26 138 162 190 71 97 209 146

Q. Auto pioneer after whom *two* cars were named — the other one being the Reo

52 54 213 99

R. That liver I ate made me feel very macho

186 153 107 17 188 194

S. That mineral I bent seemed to go on and on and on

156 2 24 72 184 60 218 56 134 35 98 14

T. This Latin is amid late back type of drug

11 168 217 103 174 49 161

U. Tossed with rewarding results

112 133 13 122 74

V. Enchanted, he marched off

25 45 1 63 211 106 88

W. Caesar's white road

111 150 183 216

X. This African grain is not efficient

158 101 125 137

Y. When I saw rainbow effect on iced screen, I cried

144 140 57 47 175 19 68 185 80 163 91

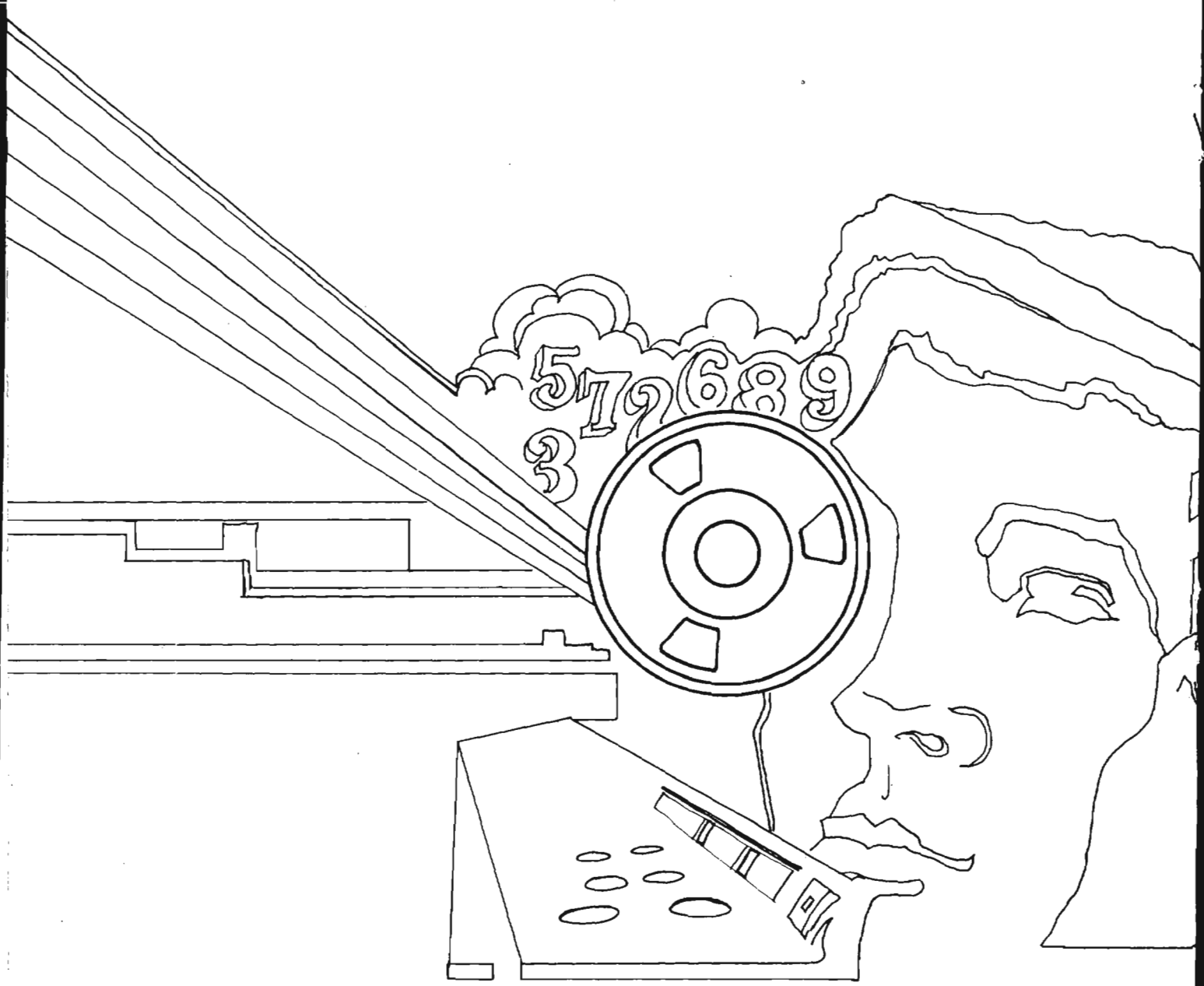
Z. Los Angeles Ram's embraceable one

178 113 170

a. He laughed as he bantered with the African queen

115 152 142 207 173

P1-Feb 85-S3-66829



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

DOCID: 4009931

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG
OCTOBER 1984

P.L. 86-36

THOUGHTS OLD AND NEW,
RANDOM AND CAUSAL (U)..... [redacted] 1
DEVELOPMENT OF ON-LINE PROCESSING SYSTEMS (U).. [redacted] 5
A PARTING SHOT (U).....E. Leigh Sawyer.....9
I REMEMBER... (U).....W.P. Meyer.....11
ON SPELLING "PLAIN?TEXT" (U)..... [redacted] 12
NATIONAL INTERESTS:
CORNERSTONE OF OUR FOREIGN POLICY (U)..... [redacted] 14
PROGRAMMING, CREATIVITY, AND HUMOR (U)..... [redacted] 18
NSA-CROSTIC NO. 58 (U).....D.H.W.....20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009931

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XI, No. 10 OCTOBER 1984

PUBLISHER [redacted]

BOARD OF EDITORS

Editor.....[redacted](963-3045s)
Production.....[redacted](963-3369s)

Collection.....[redacted](963-3961s)
Computer Security
.....[redacted](859-6044)
Cryptolinguistics.[redacted](963-1103s)
Data Systems.....[redacted](963-4953s)
Information Science
....[redacted](963-5711s)
Puzzles.....David H. Williams (963-1103s)
Special Research.....Vera R. Filby (968-7119s)
Traffic Analysis..Robert J. Hanyok (968-8418s)

For subscriptions
send name and organization
to: [redacted] P14

P.L. 86-36

To submit articles or letters
by mail, to: P1, Cryptolog

via PLATFORM mail, send to:
cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no 'O' in 'log')

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

Well, we moved again. Just about the time we got the magazine caught up, too. Once again we were reminded about how far we have come since the old pencil and graph paper days. It was a shock to realize that without this big brown Volkswagen Bus of a terminal, we were lost.

It was once true that after a move we could just sit down and begin to work. All our raw data was on paper, in folders or bundles, safely tucked away in our file cabinets. So long as those file cabinets stayed with us, so did our ability to do our assigned job.

But that is no longer true. All our data is now buried in a computer somewhere among the viscera of this mini-city. To touch it, to look at it, to work with it, you need an electrical connection to wherever it resides. Given that connection, any one of us can do things it took many people to do in those "good old" days, and often in much less time. However, once we come to rely upon this new high-tech approach, we are at the mercy (literally) of the system that keeps those connections working.

I put quotes around the "good old" days because I'm not so sure they were. Frankly, I like the new approach. I think that moving the computer out of the machine room and onto the analyst's desk is the right thing to do. However, I have just spent seven weeks without my terminal connection; on a previous move, I waited almost six months to be permitted to do my job. I still advocate this new high-tech approach, but at just this moment it is not easy to plead the case with a straight face.

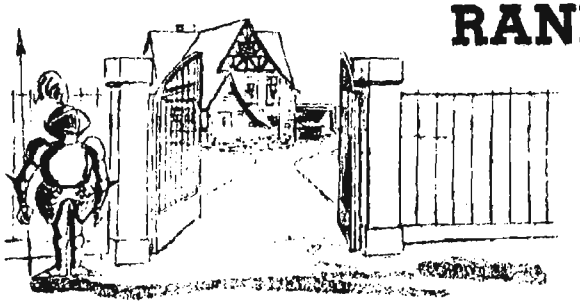
In fact, I'm thinking of ordering another file cabinet.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009931

THOUGHTS OLD & NEW,

RANDOM & CAUSAL [U]



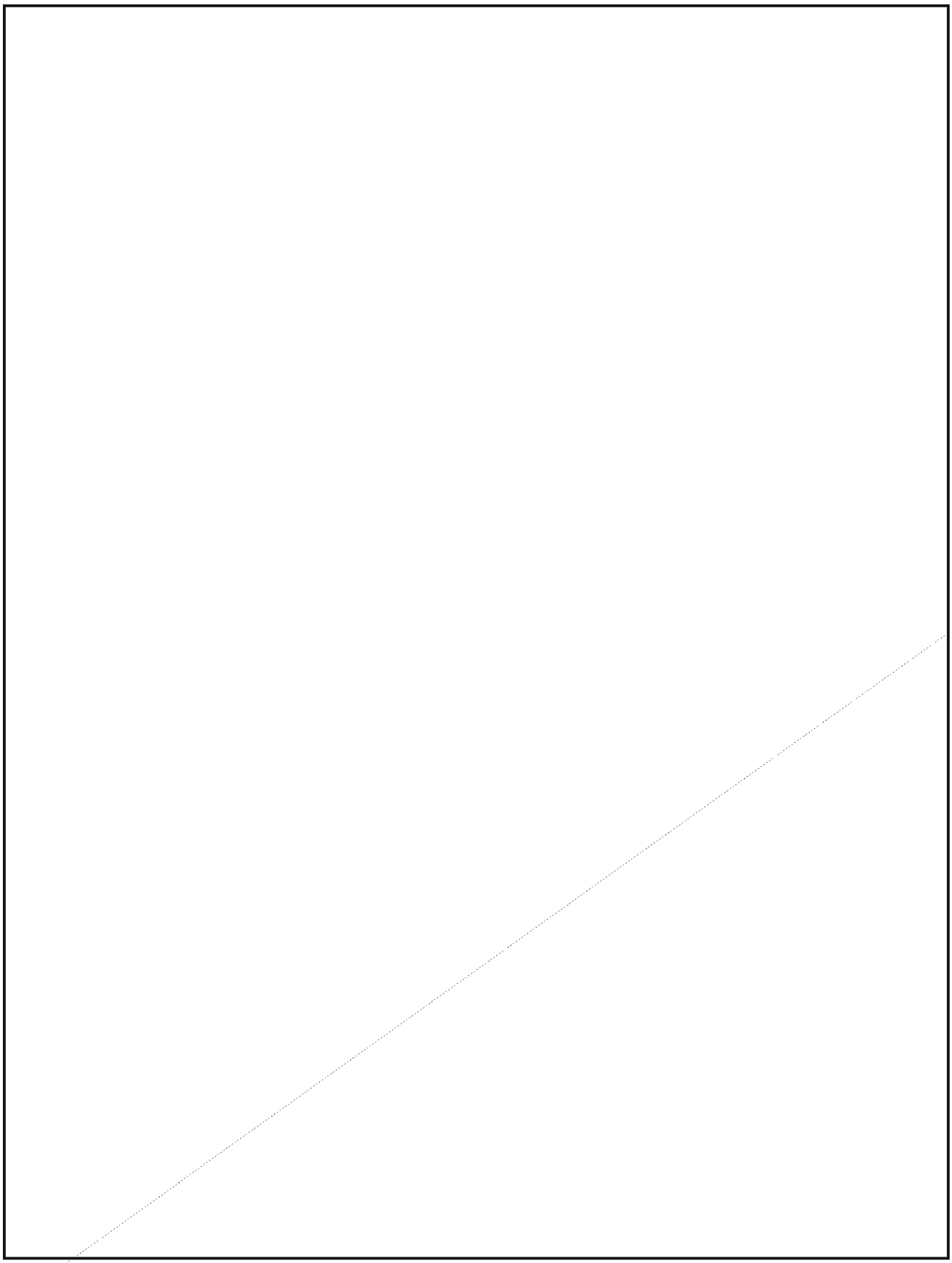
EO 1.4.(d)
P.L. 86-36

by [redacted]

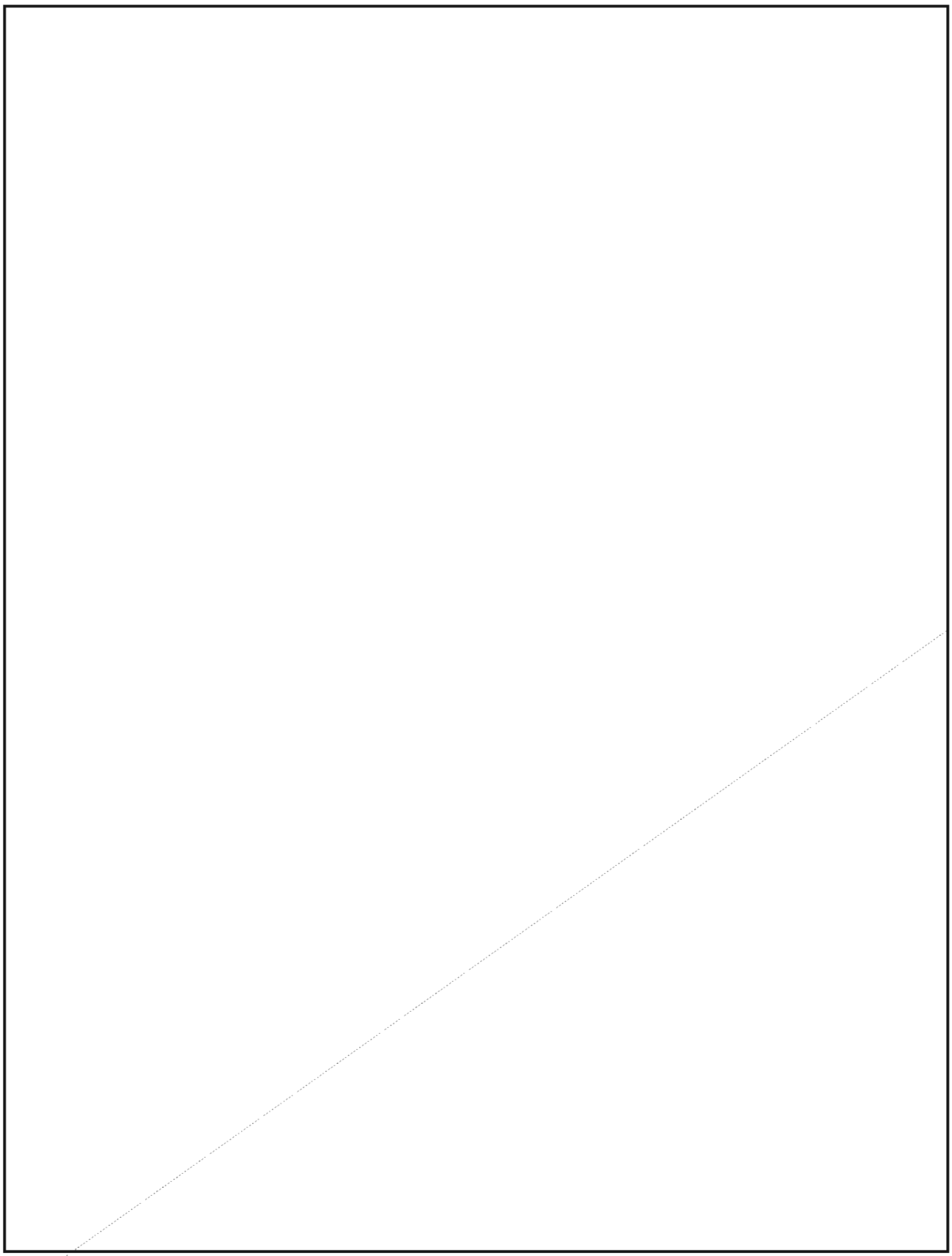
[redacted]

EO 1.4.(d)
EO 1.4.(c)
P.L. 86-36

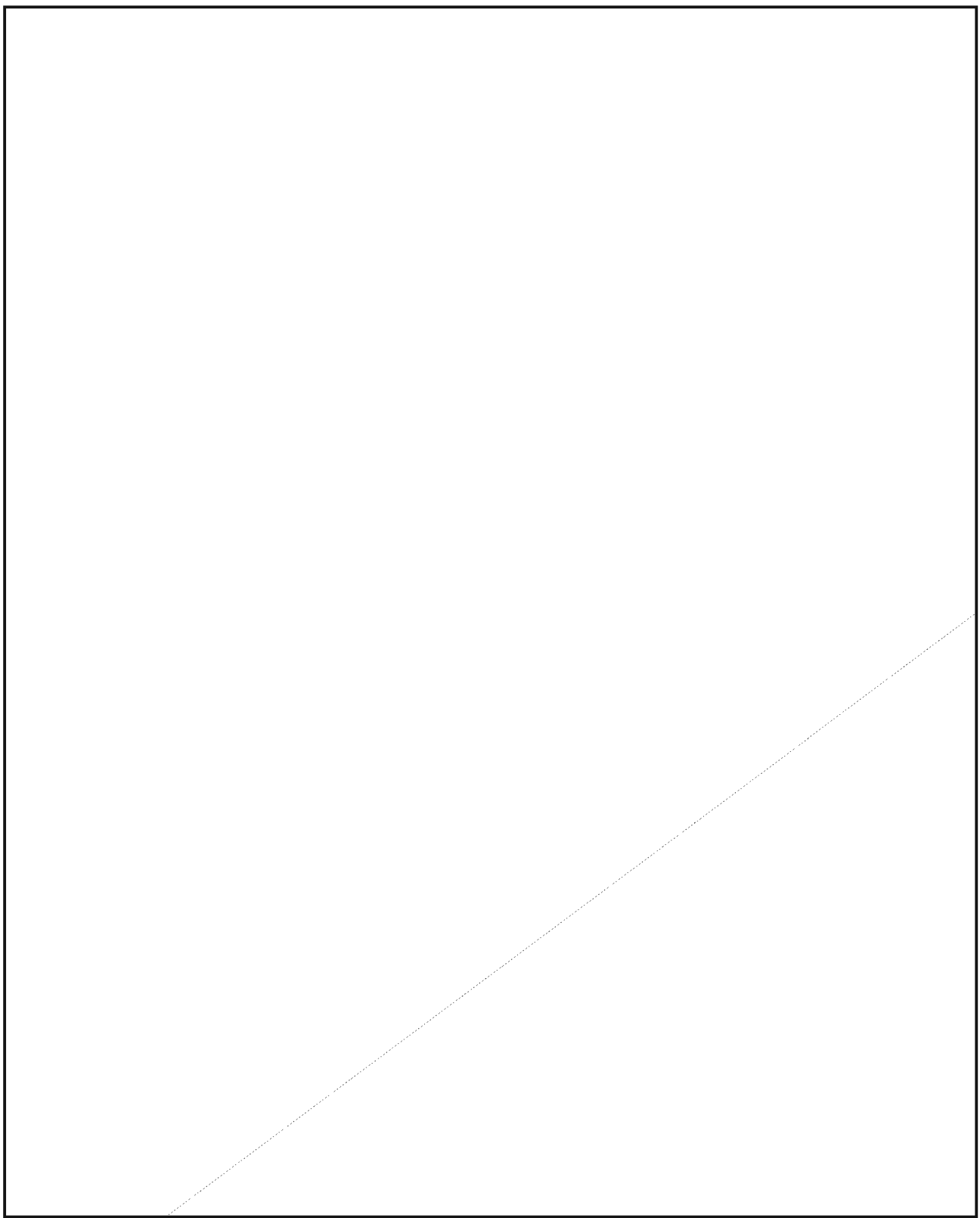
DOCID: 4009931



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



[redacted]
Chairman
Bookbreakers' Forum on Machine Aids

P.L. 86-36

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

DOCID: 4009931

EO 1.4.(c)
P.L. 86-36

DEVELOPMENT OF ON-LINE PROCESSING SYSTEMS

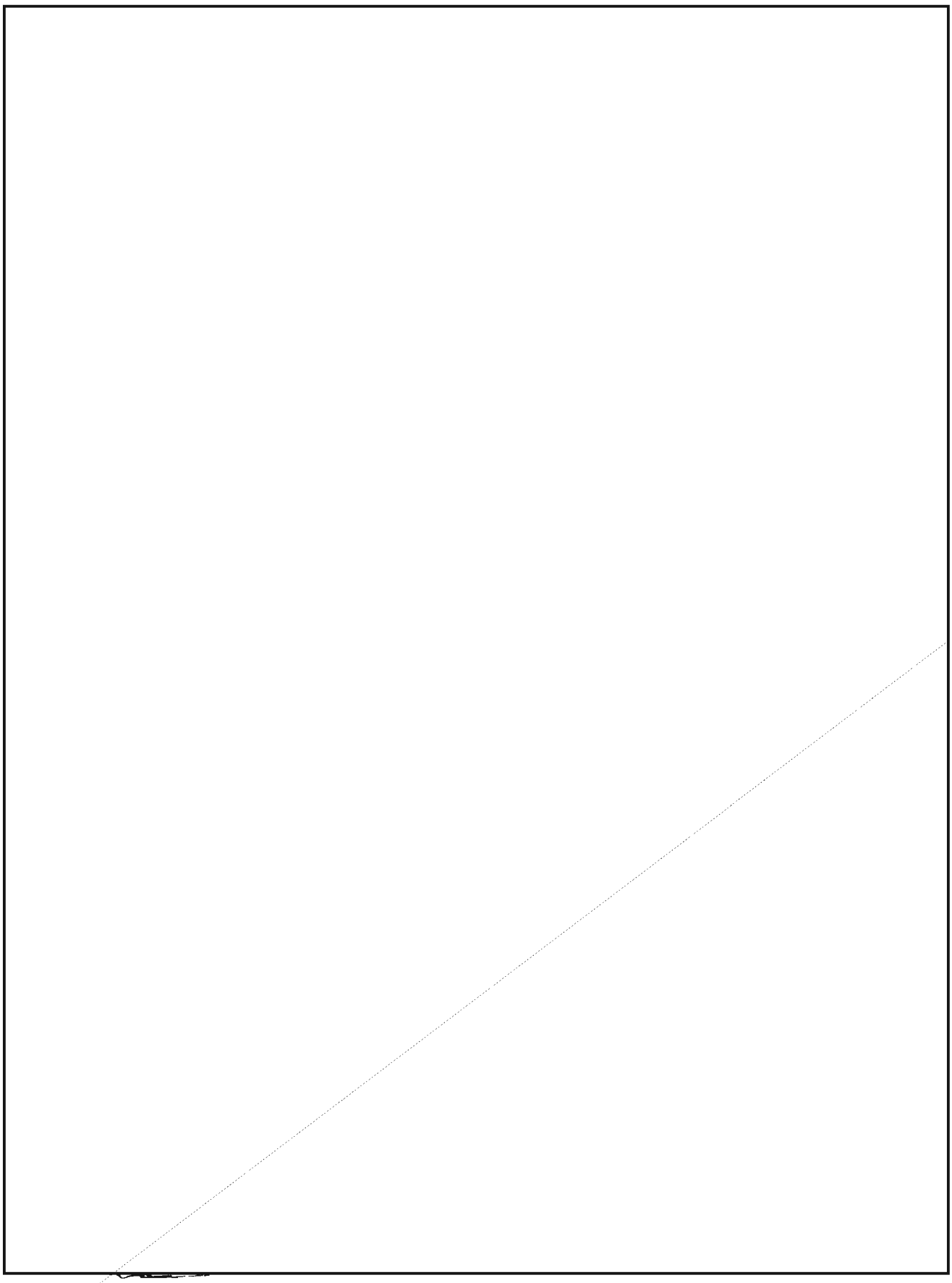
[redacted]

P.L. 86-36

by [redacted] G85

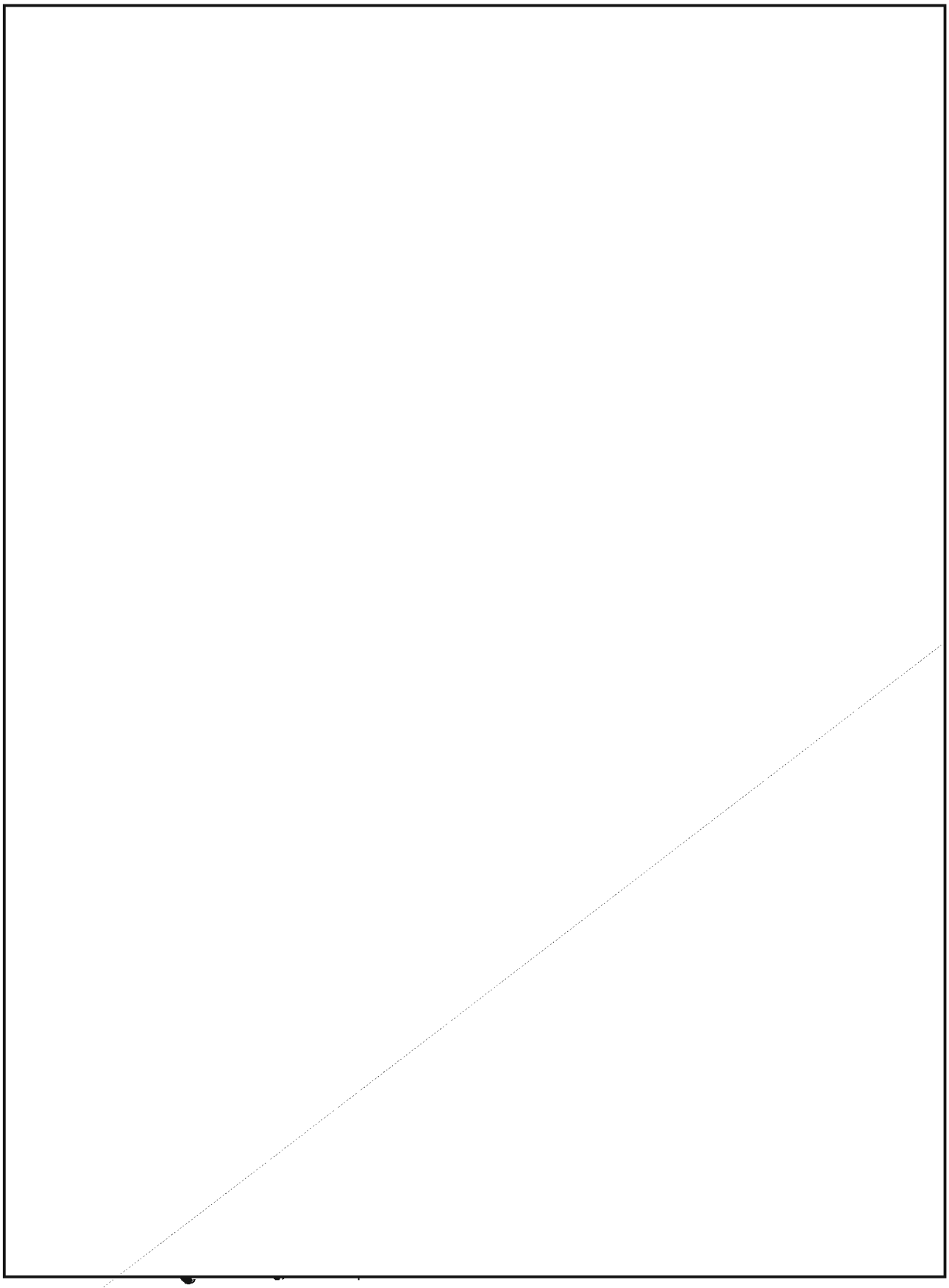
[redacted]

EO 1.4.(c)
P.L. 86-36

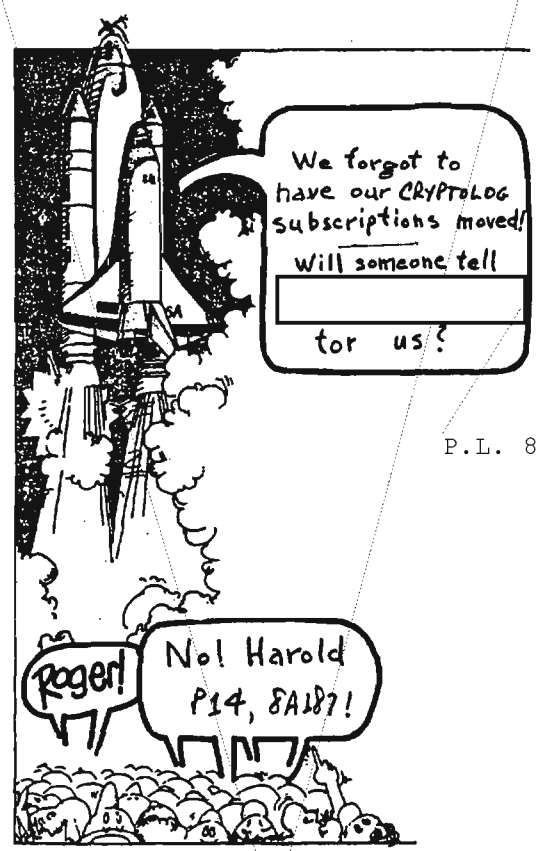


EO 1.4.(c)
P.L. 86-36

DOCID: 4009931



EO 1.4.(c)
P.L. 86-36



P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4009931

PARTING SHOT (U)

by E. Leigh Sawyer, B

PREFACE

When I was recalled to military service in 1951, I was living in Connecticut and had never heard of some sort of government instrumentality with the acronym AFSA. I soon found out when I found myself working in Building 19 at 3801 Nebraska Avenue. I was soon aware as well of AFSA operations going on at Arlington Hall Station in A and B Buildings. Since that time, I have watched NSA, the successor of AFSA, grow at Fort Meade, FANX and, for that matter, world-wide. Some NSA folks still on board will remember the two locomotives in the mid-50's, adjacent to the barracks just to the east of the eastern segment of Canine Road. Belching steam and smoke all day, they supplied the heat to the barracks we were occupying temporarily until the new operations building was completed. Since that time, the proliferation of NSA plant facilities, and of the people to work in them, has been dramatic. In fact, the looming of Building 2A in its final stages of completion and Building 2B not too far behind in its construction is almost mind-boggling when considering the NSA of 25 years ago. On the other hand, from this growth arises the specter of the penalty of bigness. One symptom of this specter is what led me to write what is to follow. In this connection, there occurs to me at times what might be termed the parable of the dinosaur and the cockroach. The dinosaur, in essence, specialized himself into extinction. From what I understand, the cockroach today is pretty much unchanged from when it co-existed with the dinosaurs and is still sufficiently efficient to be fattening the pockets of extermination companies. A lesson of sorts here?

CRYPTOLOG has published a number of articles by Leigh Sawyer. This will be his last, for he is retiring at the end of this year. His "Parting Shot" draws upon his perceptions from the era of Ralph J. Canine to the present. His concern expressed in this article reflects a deep-seated devotion to NSA and sensitivity to the critical importance of its mission to the nation.

In the September 1984 UPDATE on the Campaign for Excellence (PQS), the results of a survey were included which reflected the views of a slice of the civilian work force on PQS issues. The issues concerned covered a fairly broad spectrum involving a variety of individual perceptions of being a part of NSA. As I read the results of the survey, I was particularly interested in the findings appearing under "EMPLOYEE KNOWLEDGE OF THE NSA MISSION." These were:

[] 53%: A good understanding

[] 40%: Some idea but would like more

[] 5%: Very little but would like to know more

[] 2%: Not important

The survey results noted above immediately triggered my mind on a subject that I have preached on many times in the past--ranging from lunch table conversation to addresses I

have made to various management classes. My text has been centered on some confusion between ends and means. It is my very strong conviction that far too many NSA personnel believe that their work may be characterized as ends in themselves when, if the truth were to be known, they are involved only in the means. The distinction is of the greatest importance and relates directly to those survey results noted above.

The mission of P, with which I am most familiar, is to report SIGINT. This is one of the two prime reasons for the existence of this Agency. The other, of course, is the mission of S. On the one hand, we exploit the communications of target countries; on the other, we protect our own. This is it in a nutshell. It follows naturally that every drop of energy exerted by the entire NSA work force somehow relates to the successful accomplishment of either one of these two mission objectives. The survey results confirm my long time conviction that too many NSA employees are far from sensitive to this fact of life.

Delving into the P organization, let's consider for a moment which people are involved in ends and which ones in means. If you wish to be a complete purist, you might judge that only those who write SIGINT reports are involved with ends. This is probably far too narrow for definition purposes. Certainly the transcriber, the traffic analyst, the cryptanalyst, and others directly involved in hands-on processes must also be counted in as "ends" people. You needn't ask them if they are aware of the NSA mission in any survey. Insofar as P is concerned, they are what the success of the mission directly depends upon, beyond any question. If you don't believe this, consider the consequences if suddenly, with a wave of the magic wand, they all disappeared. Consider further the remaining P organization. On the basis of the bottom line mission objective of P, as noted above, the remaining P organization would have literally nothing to do. This is somewhat akin to what would happen to the multi-faceted fishing industry--from processing plants to the man in the white apron at the local super market who will fillet your flounder; from the wholesale outlets to the guy who writes TV commercials for cat food; and on and on--if all fishermen worldwide decided that they would rather raise chickens? Whether it be fresh fish or fresh SIGINT, one can easily bring to mind in either case the dust rising from a vast expanse of rubble after a previously elaborate structure has collapsed on itself.

One may ask how far we must go to reach that magic dividing line with the "ends" types on one side and the "means" types on the other. Not very far, really. In the P world, I would draw the line basically at the division level. To put it in the vernacular, from the division down is "Where it's all at." The further you go up the line from the division level, the less frequently will you encounter people in "ends" jobs--if you find any at all. This is not to stigmatize unfairly the "means" people in any way. As a matter of fact, I would judge throughout the P organization that the entire work force has a good perspective of the ends being sought and how their work relates in some fashion to it. There might be a few backwashes where this assumption does not hold up, but not many in my opinion.

So let's depart from P and consider the rest of the Agency (except for some chunks of S and R). If I could find a blanket large enough, I would throw it over them emblazoned with the letters, "MEANS". Now, supposing I were to lift a corner of this blanket and grab out the first soul I saw. Supposing I were to say to him, "Sir, step outside here for a moment. See those big words on the blanket? You and all those other people under the blanket are 'means' types. What basic ends do you serve?" If he were one of the 2% respondents in the survey, he would say, "I don't know, I don't care. Get off my back." If he were one of the 5% respondents, he might say, "I'm not sure. It's got something to do with national security, doesn't it?" And as for a respondent in the 40% bracket, he might say, "It's something or other about something called SIGNIT, or something like that."

I'm not certain what the latest buzz figure is for the total Agency civilian population, but I do know that 47% of it (assuming the 825 people polled are representative) constitutes a lot of people who are far from clear in varying degrees about basic work motivations. Pride on the part of a person doing a job in some sort of a supporting role is to be expected. But this same pride can be far deeper, far more meaningful, if that same person understands that, somehow, what he has done, and done well, is traceable for ultimate effect to the "ends" people on the firing line. If he does not know this, he can only experience what I would term pride in a vacuum. How much greater and meaningful is his pride if he knows his accomplishment, no matter how remote from the firing line, was done as a part of "the team." Every blessed person in the Agency is part of that team. The depressing thing is that they all don't know it. It follows that the challenge of this is to ensure that everyone knows what the

DOCID: 4009931

fundamental ends are that justify the existence of NSA. Putting it in horological terms, that little itty bitty cog on that little itty bitty gear in the innards of the clock is contributing somehow to the movement of the hands. If you were to ask that cog what it does, it would be much better to hear "I help people tell time" rather than "I hang on and spin around."

Without belaboring further the main thread of the foregoing, the prime question arising is how to cope with this problem. One might be inclined to suggest that the initiation of some kind of program to make all personnel far more sensitive to the fundamental ends that the Agency attempts to accomplish might trespass on the principle of "need to know." This would be a ridiculous reservation since there is a sharp difference between what the ends are and the methods used to achieve them. Along these lines, a flier was recently distributed about a program labelled "HINT." In essence, the program invites all cleared and indoctrinated personnel, especially those outside the Operations Directorate, to hear briefings on current intelligence and related subjects. This is a step in the right direction but will never overcome the basic problem of mission awareness. The main reasons for this are very simple--lethargy, apathy, and physical remoteness for many from either of the two auditoriums specified for the purpose.

(U) We are continually bombarded by the need for innovativeness and imaginativeness in our work. In this particular situation, such is badly needed. How can you expect a person to be a cognizant member of "the team" until he knows what "the game" is? For example, if we trundle a VCR from work space to work space so that the cast of "Cheers" can tell us why we should buy bonds, why can't we use the same device to broaden awareness of the fundamental Agency mission? This is one way to do it. There are others. The point is, who is smart enough to know that something of this sort should be done and has the authority to say "do it"?

(U) Back in the 6th century B.C., the Chinese philosopher Lao Zi proposed the planting of trees around the imperial palace both for beautification and for screening from the winter winds. He was told that the trees would need at least 100 years to reach full growth. Lao Zi replied, "Then we'd better get started now."

SOLUTION TO NSA-CROSTIC No. 57

Department of Golden Oldies: Management Survey of the Philharmonic." Reprinted in CRYPTOLOG, Vol. I, No. 1, August 1974, from HOSPITALS, March 1954. The author is unknown.

"Excerpt from a 'management survey' of the ----- Philharmonic Orchestra.

"...For considerable periods the four oboe players have nothing to do. Their number should be reduced and the work spread more evenly over the whole of the concert thus eliminating peaks of activity."

I Remember ... (U)

~~(C)~~ During the 1960's, Security asked Library Acquisitions to obtain a publication called, I believe, "Directory of Far Right Organizations." It was published by an obscure post office box firm somewhere in the West. Price unknown.

(U) Library Acquisitions normally verified price and availability of all publications before placing an order. This time I asked a small book store in Washington, D.C. if they would order it for us. After a few weeks, the publication was received by them and forwarded on to us.

~~(C)~~ A year later the same firm issued their new publication, "Individuals and Organizations interested in the Far Right." The Washington Post picked up on this and published a little squib about the only book store in the Washington area that was listed as being an outlet (sic) of far right publications. The book store listing was a direct result of our request to them to order the publication.

(U) Many organizations rent their membership list out to other publishers; obviously this firm had taken their mailing list and capitalized on it. What if I had written a cost-and-availability letter to them? Certainly it would have been very embarrassing to have NSA appear on their list.

W.P. Meyer
FANX Librarian

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009931

ON SPELLING "PLAIN?TEXT" (U)

by [redacted] G61

P.L. 86-36

First of all, if "plain text" were the suitable spelling for the noun, then "plain-text" would be the appropriate spelling when the noun is used to modify another noun. However, as I intend to demonstrate that "plain text" is not at all desirable, this observation will be rendered moot.

Secondly, to avoid begging the question, I resort to spellings like "plain?text". Fortunately, this essay is written rather than spoken, since "plain text" and "plaintext" have quite different pronunciations, and I don't know how to pronounce "plain?text".

Now the spelling of compounds in English is not at all straightforward. It fluctuates a good bit, almost always in the direction of the solid spelling (sometimes bypassing a hyphenated spelling entirely). In this article I will concentrate on adjective-noun compounds, hoping that everyone can agree that the "plain" of "plain?text" is an adjective even though the "cipher" of "cipher?text" is a noun.

Consider the following sentences:

Blue?birds are blue?birds.
The blue?bird is a blue?bird.
That blue?bird is a cerulean warbler.

Without visual or aural clues, it may be difficult at first to discern even what is being said, but nearly everyone will agree that the correct spellings are:

Bluebirds are blue birds.
The bluebird is a blue bird.
That blue bird is a cerulean warbler.

Wayne:
I think that I told you about the brief discussion I had with [redacted] when we changed his title from "On Saving Plain-text" to "On Saving Plain Text" because Creepylog had been making a distinction between the adj (one wd) & the noun (2 wds). He doesn't exactly agree, as you can see.

HGR

(Other spellings give other meanings, some of which even make sense in certain contexts.) Note how the accentual pattern of "bluebirds" differs from that of "blue birds": in the compound, the first syllable has the stronger accent.

Now "plain?text" has the accentual pattern of "bluebird". The spelling "plain text" suggests the accentual pattern of "blue bird", and can momentarily throw the reader off the track. (Note that "plain?text" when contrasted with "cipher?text" has a third accentual pattern, the same as in "That's not a green bird, it's a blue bird"; this pattern is sometimes represented in writing with italics, but the reader usually needs no clue beyond the context. In any case, this paper does not deal with the contrastive pattern.) Derailing readers, as the preceding long parenthesis may have done, is not nice.

So we have at least a prima facie case for the spelling "plaintext". The burden of proof shifts to those who favor the broken spelling. And perhaps I should simply let them speak for

~~FOR OFFICIAL USE ONLY~~

OCID: 4009931

themselves. But (to prepare the way for weightier matters) I will suggest two arguments they could put forth.

First, not all English compounds with the accentual pattern of "plain?text" are written solid. We have "yellow jacket" (not a flavid garment, but a wasp); some noun-noun examples include "ice cream" (originally "iced cream") and "light ray" (no, not a slender manta). Sometimes a compound remains open because closing it would lead to a word odd in appearance or seemingly hard to pronounce, as in "lightray" or "seaurchin". These observations hardly seem to provide adequate reason to flout common sense in the case of a compound like "plain?text". Tradition gives "plain text" some support, whether it be CRYPTOLOG's Consistency Guidelines, or Random House's Dictionary (rumored to have assigned the wrong number of humps to a dromedary), or Funk & Wagnalls (once a national joke, now out of print). Although Merriam-Webster used to have "plain text", it now gives "plaintext"; Merriam wisely refuses to give space to alternate spellings of compounds, listing the version it observes most or a version formed by analogy to similar compounds. The other two leading college dictionaries are silent on "plain?text", but the New World does suggest the solid spelling when "the referent having a compound name becomes so familiar that it is thought of for itself rather than mainly within a generic classification, as ha[s] 'redbird'" (page xxi). No cryptanalyst thinks of "plain?text" as merely some kind of "text"! Tradition is certainly a good thing, but to insist that standards never be changed is logically equivalent to insisting on the spelling "clarus textus", or whatever the Proto-Indo-European for "plain?text" may have been.

A second argument is that consistency has merit, whether to enhance a publication's esthetic appeal or to facilitate data retrieval. But as standards change, and some inevitably do, there comes a time when a new consistency should be inaugurated. Possibly "plain?text" did in fact have the accentual pattern of "blue bird" years ago when the standards were first promulgated, and only years of frequent contrast with "cipher?text" have given it a pattern like "bluebird". A new standard seems to be in order. Certainly most examples of "plain?text" that I have seen in print have the spelling "plaintext", especially if I may discount examples in publications like CRYPTOLOG that consciously adhere to other standards. For editors to insist on consistency in the spelling of compounds may result in the slowing down of the natural process by which careful writers enable a language's written form to more closely approximate its spoken cadencies.

It's certainly desirable to encourage good writing standards, but I think it is important to advocate sympathetic reading habits as well. Let me give two examples that I think reflect an excessive zeal for standards that inhibits a reader's comprehension. Please don't misunderstand: I do not ascribe to all who wield a red pencil the infelicities I am about to relate. For one thing, I sometimes wield a red pencil myself; moreover, I realize that many who do so are trying to protect people like me from what nearly befell me in the second incident below. (Incidentally, it was refreshing to see the spelling 'Bluepencils' in the December issue; CRYPTOLOG is way ahead of the lexicographers on this one.)

A recent CRYPTOLOG writer chided a reporter who "either didn't do his homework or decided to go modern when, in describing a recent hurricane, he said: 'Damage will be in the millions, but only one person lost their life.'" Apparently the reporter is male, but the sex of the victim is irrelevant to the story and perhaps unknown to the reporter. "His or her" and "his/her" seem especially inappropriate. "Their" is the only pronoun suitable to the occasion. This use of "their" is not "modern"; the Oxford English Dictionary has examples as long ago as Middle English. Now I suppose the reporter could have said "... only one person died." These grammatical reflections distract us from the observation that perhaps the reporter should have said: "Damage will be in the millions. One person has died."

A few years ago I submitted a paper towards certification in Computer Science. The first reader rejected it, citing for the most part alleged grammatical errors. A second reader accepted it, as did the tiebreaking third reader; in fact, they both accepted the paper "with honors", entitling me to the sweetest after-taxes $37.50 in a long time. The first reader's zeal obscured the paper's merit from him. And his zeal was all but unbounded. One "error" was my use of "commoner" and "commonest" (Fowler insists on the morphological comparison, and I have noted dozens of fine writers using these forms). The other "error" was the absence of "with" after "begin" (as if the answer to the question "How does the National Anthem begin?" has to be "It begins with 'O say can you see ...'").

So now you know why I originally entitled my CRYPTOLOG article from last January "On Saving Plaintext" (and why I am glad the CRYPTOLOG people didn't reject it out of hand for alleged spelling errors). Anyways, I at least snuck a split infinitive past the editors' watchful eyes ("... to automatically generate ...")!

DOCID: 4009931

NATIONAL INTERESTS:

CORNERSTONE OF OUR FOREIGN POLICY (U)

by [redacted] G64 P.L. 86-36

A noted historian recently wrote "Foreign policy is the face a nation wears to the world. The minimal motive is the same for all states--(U) the protection of national integrity and interest." The allusion to the protection of national interest will be a familiar phrase to those who follow recent discussions of foreign policy. Within the last year the protection of national interests has been evoked as the basis for our country's military action in Grenada and the stationing of American marines in Lebanon. The terms "national interest", "vital interests", and "strategic interests" pervade media discussions of our nation's relations with the rest of the world. The almost constant references to these concepts naturally lead to the question "What are these national interests that seem so quickly threatened and require such decisive action?"

(U) The purpose of this essay is to look at the concept of American interests in its most basic form. The essay seeks to trace very briefly the historical background and trends that have made our perception of American national interests what it is. Along with defining broadly national interests, this essay will also seek to point out the implications resulting from how we define our national interests.

(U) At this juncture, a disclaimer is necessary. This essay will not attempt to judge the various perceptions of national interests adopted by past administrations. This discussion is not large enough in scope to judge between such nuances, and the taking of particular sides is not a function of this undertakeing. Still, although limited in scope, the importance of analyzing the concepts at hand must again be emphasized. A direct and concise discussion of American national interests in the foreign policy sphere should provide a valuable perspective concerning the place our country has assumed in the world community.

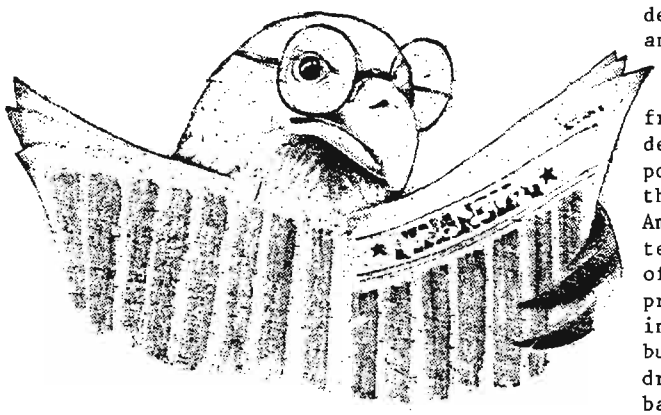
(U) Our nation's early leaders recognized the role of national interests in the sphere of international relations. Of their views, it has been written

> "They believed that states responded to specific national interests--and were morally obliged to do so, if there were to be regularity and predictability in international affairs."

George Washington said "No nation is to be trusted farther than it is bound by interest."

(U) Our founding fathers viewed the birth of our nation as the beginning of a unique experiment in democracy. The precarious nature of the undertaking became all too apparent when the newly established colonies were threatened by the great powers of Europe early in the nineteenth century. It was at this point in our history that an abiding aspect of our national interest took form. The continuation of our experiment in democracy depended upon the maintenance of a balance of power in Europe. In other words, it became in our national interest to have those countries who were in a position to threaten us held in check by one another. In those years the threats came from France and Great Britain.

DOCID: 4009931



(U) The possibility that one country should come to dominate the others in the Old World greatly concerned our first policymakers. Such a series of events was perceived to be a grave threat. John Adams noted, concerning the two great powers of his time:

> "It never could be in our interest to unite with France in the destruction of England. ... On the other hand, it could never be our duty to unite with Britain in too great a humiliation of France."

(U) In 1814, when Britain was at war against France and America, Thomas Jefferson nevertheless expressed concern for Napoleon's victories in the rest of Europe. He wrote:

> "It cannot be to our interest that all Europe should be reduced to a single monarchy. Were he [Napoleon] advanced to Moscow, I should again wish him disaster as would prevent his reaching Petersburg. And were the consequences even to be the longer continuance of our war, I would rather meet them than see the whole force of Europe wielded by a single hand."

(U) The view of our early policy makers was that the United States was marking the beginning of an experiment in democracy that could affect the whole world. If left on its own course, the early leaders expected that the development of democracy in America would, in time, prove to be an example for other nations. Therefore, the overriding national interest became the encouragement of international events to proceed in a direction that would keep power from becoming concentrated in a single place. A dangerous level was perceived to be the point at which the American democratic experiment could be threatened by an outside party.

(U) Following the resolution of the threats from England and France during the first few decades of America's existence, the European powers were held in balance by each other throughout most of the nineteenth century. American intervention to protect national interests was not needed. However, as evidence of the concern, the Monroe Doctrine evoked a prohibition for the Old World against meddling in the New World. Through this action a buffer was provided against possible hindrances to American development. Because a balance of power was maintained in Europe, there was no threat to America and thus the new nation was able to distance itself from European entanglements.

(U) With the coming of the twentieth century, a new threat arose. Twice in the first half of the century the domination of Europe by a single nation seemed a possibility. As Jefferson had earlier remarked, our interest dictated that war was a more attractive option than seeing Europe succumb to foreign domination.

(U) Following World War II, the threat to the international balance of power shifted eastward to the Soviet Union, where it remains today. In fact, the need to contain the USSR's expansionist policies has been the primary concern of American national interests since 1945.

(U) Although the way our nation defined its national interest remained basically the same following World War II, the American position on the international scene permanently changed. After the war, the United States emerged as a superpower and began to assume a position as leader of the Free World. Also, the potential for threats to our experiment became much greater with the advent of nuclear weapons. These factors contributed to the reluctant end of the American tradition of isolationism, once and for all.

(U) Because of America's new-found responsibility as leader of the Free World, our national interests naturally have been affected. While not being significantly altered, the concept of protecting democratic experiments has expanded. In time the assumption developed that our interests were not merely confined to ensuring the prosperity of our own unique experiment in democracy. As the leader of the Free World, our responsibility now involved guaranteeing the potential of other nations to pursue their own experiments as well.

(U) It is precisely at this point that we find ourselves today. After a decade in which the view of national interests seemed muddled or slightly out of focus, the outline is emerging clearly once again. The threat to our national interest is again perceived to be the concentration of international power in the hands of a force that could threaten the democratic institutions of the Free World, including our own.

(U) Foreign policy makers within the current administration have articulated this traditional view of American interests succinctly. In 1982, when testifying before a subcommittee of the House of Representatives Foreign Affairs Committee, the Deputy Assistant Secretary for East Asian and Pacific Affairs stated:

> "In its broadest terms, our principal strategic interest is deterring the increasingly assertive Soviet presence in East Asia and the Indian Ocean. This can best be achieved by supporting growth and stability in the region through the variety of security, political, economic, and commercial programs we pursue."

(U) In Latin America, this country's interests are defined in similar terms. The President's speech before the National Association of Managers in March 1983 provided the following excerpts:

> "Central America is simply too close, and the strategic stakes too high, for us to ignore the danger of governments seizing power there with ideological and military ties to the Soviet Union."
>
> "The Communist agenda, on the other hand, is to exploit human suffering in Central America to strike at the heart of the Western Hemisphere. By preventing reform and instilling their own brand of totalitarianism, they can threaten freedom and peace and weaken our national security."
>
> "We've been too slow to understand that the defense of the Caribbean and Central America against Marxist-Leninist takeover is vital to our national security in ways we're not accustomed to thinking about."

(U) Hopefully, at this point in our discussion a definition of American national interests is becoming clear. Although the definition is admittedly broad, these interests can be summarized as the desire to contain the consolidation of power and influence in the world by a single state. This containment is desirable so that democratic institutions may prosper. While American concern initially centered primarily on the protection of our own institutions, our responsibilities have in this century expanded to include protecting similar institutions in other nations.

(U) The natural progression of our discussion leads now to an analysis of the implications that our definition of American national interests has for our country's foreign policy. Commenting on America's aptitude for engaging in foreign affairs, Alexis de Tocqueville wrote:

> "Foreign politics demand scarcely any of those qualities which are peculiar to democracy. They require, on the contrary, the perfect use of almost all those [qualities] in which it is deficient. Democracy is favorable to the increase of the internal resources of the state; it diffuses wealth and comfort, promotes public spirit, and fortifies the respect of law in all classes of society. All these advantages have only an indirect influence over the relations one people bears to another. A democracy can only with great difficulty regulate the details of an important undertaking, persevere in a fixed design, and work out its execution in spite of serious obstacles."

(U) Tocqueville suggests that inherent qualities of a democratic nation make it difficult for that nation to operate in the foreign policy sphere. One aspect of the difficulty is that a democratic nation is quite capable of operating in an international political vacuum. Even in the absence of political support from abroad, a democratic state can still perfect its own national institutions. In fact, it is during this absence of outside political interference that democratic institutions often find their most fertile environment for growth.

(U) But the question is raised "How does this relate to a discussion of the national interest?" Basically, the implication is that our national interests will have a tendency to combine with these inherent qualities of democracy to cause our foreign policy to be reactionary. In other words, a foreign policy will be fostered that is better suited to respond or react to threats or crises than to dictate the course of world events. Left to their own devices, American policymakers would be content to concentrate on our nation's internal development. The reluctance of many policymakers to endorse our recent deployment

DOCID: 4009931

of American forces in the Caribbean and Middle East evidences this tendency. Also, this internal development of our nation can be accomplished with no political help or influence from abroad. However, when threats are perceived to the safety of our institutions, then we undertake the most active involvement in foreign affairs.

(U) The vision (mentioned earlier) that the United States is destined to provide a democratic example to the world is not precluded because of our tendency to be reactive to international events. While this vision has been a part of our national psyche from the beginning, it has never been a precondition for our national development. The contrast can be drawn with the Soviet Union. A fundamental principle of the Soviet raison d'etre is that fostering revolution in other countries. The fulfillment of its purposes means significant involvement in the affairs of other nations. In much the same way, our vision for influence by example is far removed from the insatiable appetite for domination evidenced by some ultra-rightwing regimes, most notably Nazi Germany.

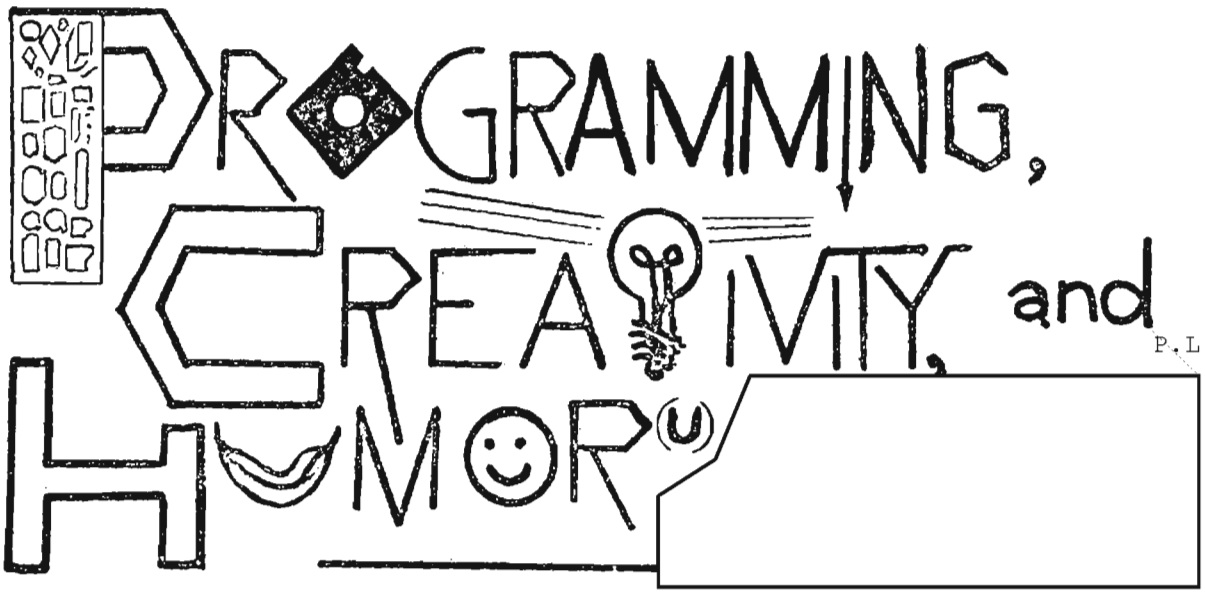
(U) The tendency to participate most actively in the international arena when responding to threats leads to some difficulties. An emphasis is placed on solving the pressing international problems. Less importance is given to the preventive possibilities of foreign policy, in other words on catching the problems before they become pressing. America has at times remained on the sidelines in great disputes until catastrophes have occurred. Our positions with regard to the aggression of Japan and Nazi Germany, prior to our involvement in World War II, comes to mind.

(U) Another implication of our definition of national interests is that our foreign policy might tend to globalize regional disputes. The tendency could be to focus on the threats to the global balance of power resulting from a local dispute. An obvious example of this is the Middle East. This area, where enhancement of the Soviet position is rightly perceived as a threat to the stability of the democratic institutions of the West, is also experiencing much of the turmoil simply because of local conflicting cultural and religious factors. The conflicts between the various Muslim and Christian ethnic groups, which are responsible for most of the fighting, are factors that have at times been lost in concerns about a threat to vital national interests. The danger, in this situation and in similar ones, is that the United States may delay its active involvement to resolve local difficulties until a crisis is reached where the global implications are very real and threatening.

(U) Another foreign policy issue resulting from our basic definition of national interests is how to clarify the degree to which our interests are being threatened. Although general agreement may be reached concerning the basic definition of American national interests, the very nature of a democracy dictates that there will be diversity of opinion when the threat potential of a particular situation is questioned. Once consensus is reached that a real threat to our national interests exists, a new consensus must be reached regarding the adequate response. Again, Tocqueville's observation that those qualities considered great about a democracy tend to be the least useful in international affairs seems to be quite relevant.

(U) In summary, the implications of our nation's foreign policy are not as bleak as might be concluded from several of the previous paragraphs. Our objectives, as defined by our national interests, have generally been met when those interests have been clearly articulated to the world. The Cuban Missile Crisis, when a Soviet action was clearly declared to be opposed to our national interest, shows the effectiveness of such a forthright reaction. When other nations, whether allies or potential adversaries, have been fully aware of the high priority the United States places on protecting developing democratic institutions, our ability to exert a positive influence on other nations in the world has been enhanced. When America has accepted the role as leader and, at times, protector of the Free World, our ability to mediate and assist in disputes at various points around the world has been increased. In short, it is evident that certain uniquely democratic qualities might make it difficult for the United States to undertake and execute many great foreign policy initiatives; however, it is just as clear that these same democratic qualities have allowed us to rise to a pinnacle of influence where we are looked to for such initiatives and leadership. Our national interests dictate that we continue to protect the development of these democratic institutions in our nation and the world.

CID: 4009931



P.L. 86-36

If I were asked to give one word to describe government writing, that word would probably be "humorless." Not only are there no jokes in (U) government documents (actually, I agree there should not be), but there are no figures of speech, no similes or metaphors, and rarely is there anything in a government document which appeals to anything but your sense of duty to read it.

(U) This problem also exists in government computer program documentation. It seems the more bland and serious the commentary of a computer program is, the more likely it will be accepted by one's boss and the cryptologic community. I contend that such an emphasis on seriousness may sometimes hamper the computer programming effort here at NSA.

(U) Let me fully explain such a drastic statement. During my tours as a Computer Systems Intern, I met a programmer who had a novel (for me) concept of programming: A program and, indeed, a computer itself are nothing more than tools. As such, they should be easy to use, and techniques for designing better tools really must meet a single criterion: Do they get the job done? I believe this has been misconstrued as a concept, and now the question that supervisors are asking is, "Does a program get the job done in the most direct, lackluster, standard, structured way possible?"

(U) The wrong that is inherent here is the neglect of creativity and motivational aids. Too much emphasis on structure (stricture?) not only blinds some people to sense, but it can also hamper the creativity of many brilliant minds. The freedom to program in the fashion you find readable and easy for you, and the freedom to document your program in a way that might even make it enjoyable to use, should not be denied. If I am going to warn the prospective user of my program that a certain procedure is dangerous, I should not be censured for displaying

WHOA!!!!! HOLD ON A MINUTE!

on the terminal. It is much more likely to get someone's attention than a message such as:

POSSIBLE DATASET HAZARD -- <CR> to continue, <CTRL>Y to halt

Unfortunately, it is also more likely to get me a reprimand for the "unprofessional" appearance of my programs. When supervisors vehemently discourage a lighthearted approach to documentation of a program, they make the documentation harder to read (because of its dryness, who would WANT to read it?), and thus impede the ease of use and the ability to pass the programs on to future generations of programmers.

(U) But something worse happens. (Hang on. I'm about to wax philosophical now.) The rejection of humor leads to a danger rarely admitted at NSA: It is possible to take our work, and the cause for which we work, too

DOCID: 4009931

seriously. We can take it seriously enough to do our jobs properly, using whatever techniques work well for us, or we can impose a seriousness that stifles, produces stress, and makes an uneasy, totalitarian uniformity settle glumly over all of us. The serious struggle for peace, which NSA fights bravely, makes humor necessary. Certainly, we do not go through the traumatic experiences of a MASH unit or a combat battalion on the front lines, but our work is hard, stressful, and often monotonous. If a programmer responds to the pressure by writing a program that produces a chuckle while it does its job, this is certainly no sin.

(U) Maybe a humorous line in a program or a programmer's affinity for exploring a computer's collection of games should enlighten a supervisor rather than anger him or her. It could well be that the occasional joke--or the occasional fight against Space Invaders--is a programmer's way of saying, "My work sometimes seems fruitless, and once in a while I need to fool myself into thinking I'M WINNING!" The mental rewards that such humor can create may lead to a happier programmer and a more successful effort on his or her part.

(U) There's one more argument I haven't tackled:

> "When I was programming, there wasn't any time to joke around. We came in, we did our job, we went home. I don't see any reason for all the nonsense some people get away with nowadays."

My only answer to this argument is to remind the reader that this is merely the expression of the urge we all have to keep things the way they are. Certainly the people of the 16th century might envy us because of all of our modern conveniences. Still, just because previous generations of programmers wrote their programs stodgily doesn't mean that future generations shouldn't try to improve their product by adding a little levity.

(U) Certainly, let's not overdo humor. But let's not overdo seriousness, either.

TO: Cryptolog

P.L. 86-36

SUBJ: "User Friendly Writing"

(U) I endorse [redacted] *"Human Factors" in "User Friendly Writing" (CRYPTOLOG, Feb 84). Most culprits will not recognize themselves as guilty. Most who do will not make the effort to change, because they either don't care or are lazy. Mary's efforts are worthwhile for the couple of people who try to improve their writing style. (Personnel Summaries are as fraught with being not "user-friendly" as Mary's Research Summaries. I wonder if people realize that managerss read the former as examples of a person's writing abilities, as well as for the content?)*

(U) Mary's article reminded me of two "classic" memos. The text of one, in two numbered paragraphs, said: "1. Agency correspondence should be brief. 2. This is an example." It was signed by the Director, VADM Noel Gaylor. The text of the other, on the subject of "Utilization," was "Please stop utilizing "utilize" and utilize "use." That one was from MG John Morrison, Assistant Director for Production (the forerunner of DDO). I mislaid my copy of the first memo, but still have a copy of the second as an example of clear writing.

[redacted]

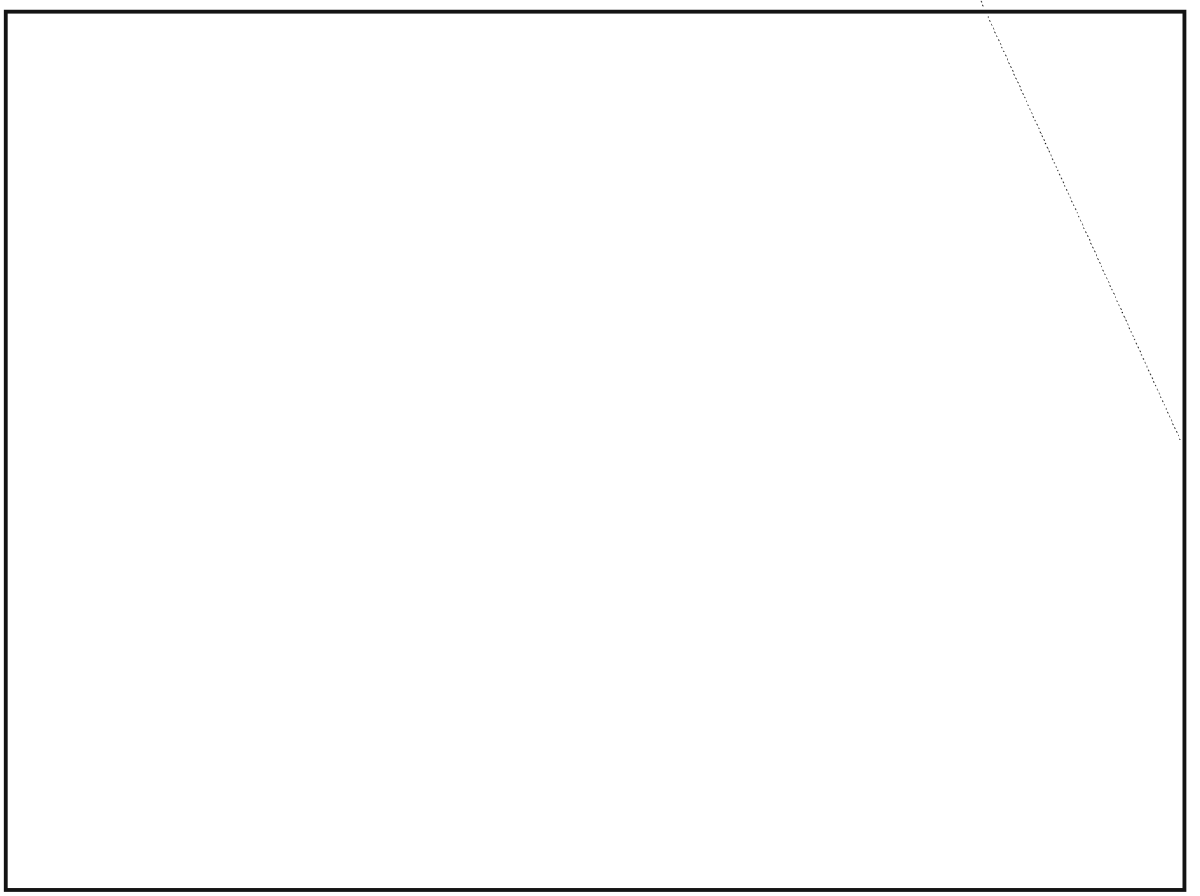
P.L. 86-36

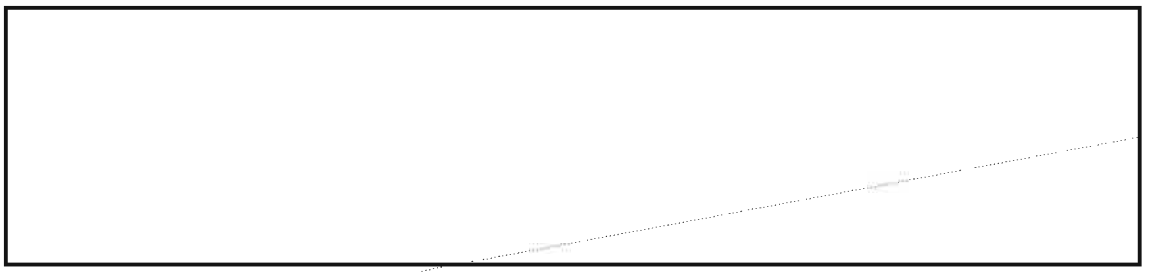
DOCID: 4009931

NSA Crostic No. 58

Several of the definitions in this puzzle consist of the ticketing code trigraphs for various American airports. The answer to each of these is a major league sports team which might use this airport. (For the purposes of this puzzle, the USFL is considered to be a major league.)

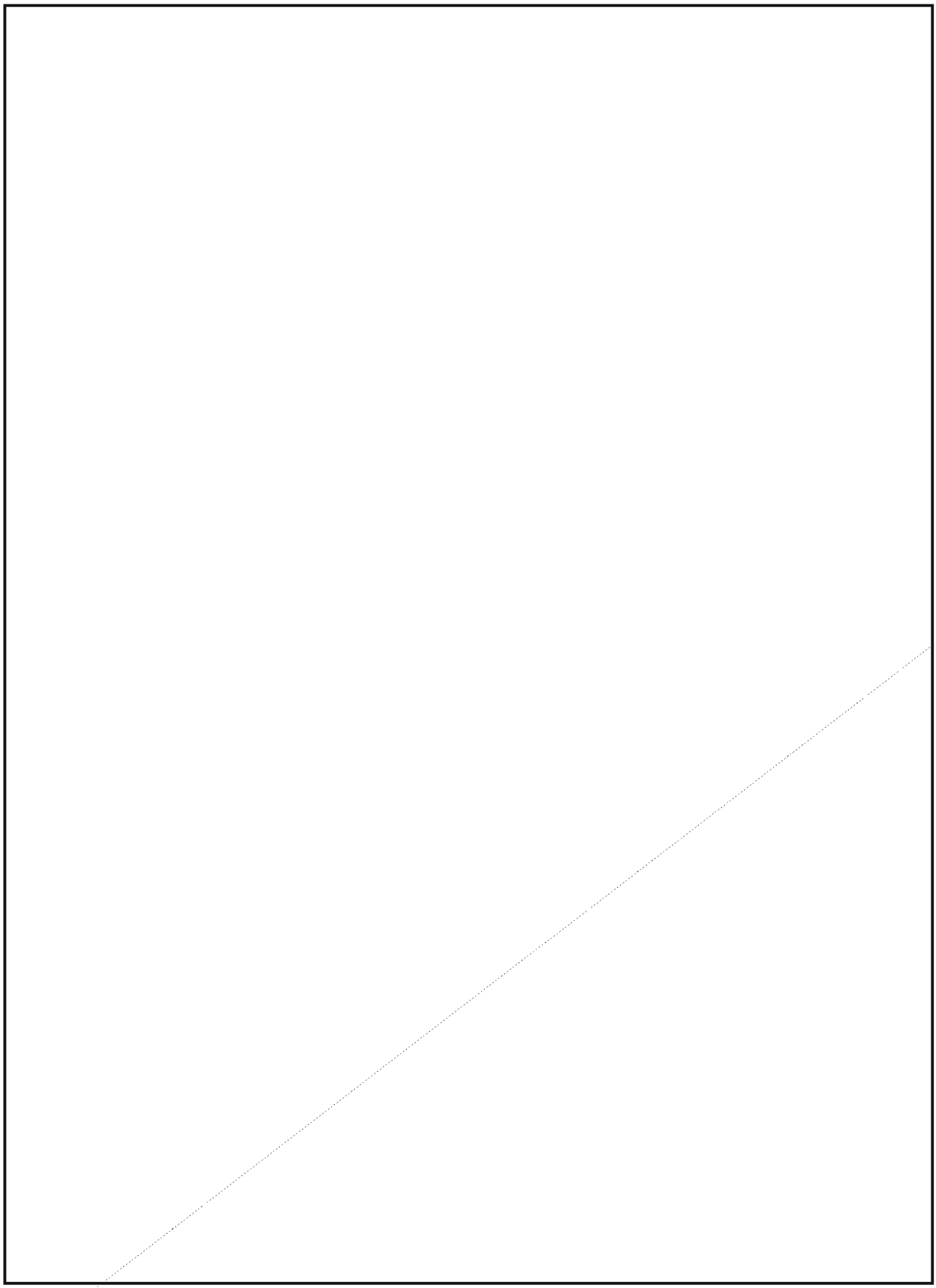
P.L. 86-36



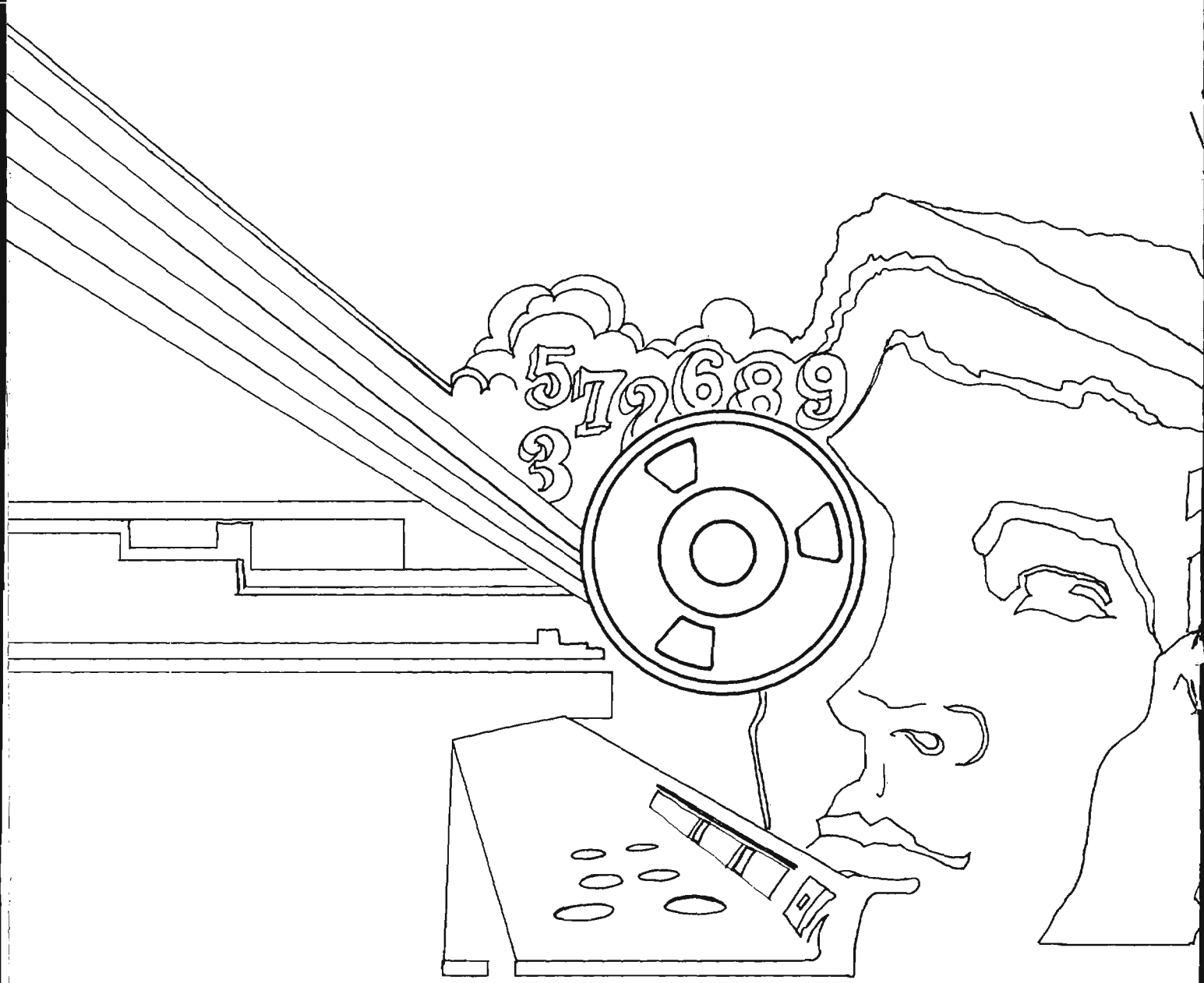


P.L. 86-36

DOCID: 4009931



P.L. 86-36


5 7 9 6 8 9
3

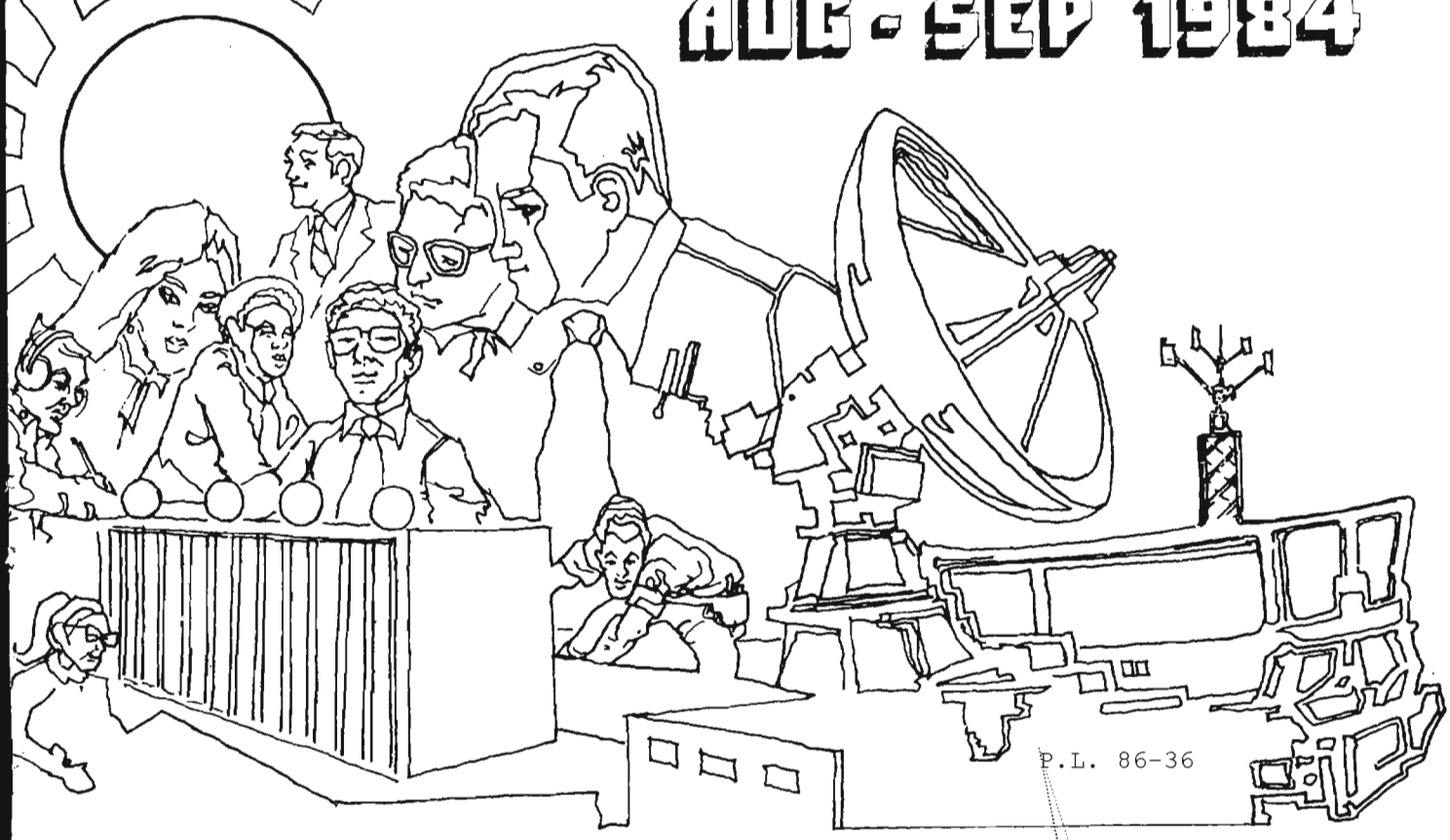
DOCID: 4009929

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

AUG - SEP 1984



P.L. 86-36

DIRECTOR'S REMARKS:
1984 CISI SPRING CONFERENCE (U).....Lincoln D. Faurer.....1
THE SOVIET CENSORSHIP DILEMMA:
MOTIVATION VS. SECRECY (U)..... [redacted] 3
LONG-RANGE PLANNING AND NSA (U)..... [redacted] 6
THE AT&T DIVESTITURE
AND NATIONAL SECURITY (U)..... [redacted] 10
QUALIFICATIONS OF A CRYPTANALYST (U)..... [redacted] 13
LINGUISTS AND OTHER MINORITIES (U)..... [redacted] 14
STUMBLING INTO SPACE (U).....Nathaniel C. Gerson.....18
NSA-CROSTIC NO. 57 (U).....D.H.W.....28

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009929

~~FOR OFFICIAL USE ONLY~~

CRYPTOLOG

P.L. 86-36

Published by P1, Techniques and Standards

VOL. XI, No. 8-9 AUGUST-SEPTEMBER 1984

PUBLISHER [redacted]

BOARD OF EDITORS

Editor..... [redacted] (963-3045s)
Production..... [redacted] (963-3369s)

Collection..... [redacted] (963-3961s)
Computer Security
..... [redacted] (859-6044)
Cryptolinguistics. [redacted] (963-1103s)
Data Systems..... [redacted] (963-4953s)
Information Science
..... [redacted] (963-5711s)
Puzzles.....David H. Williams (963-1103s)
Special Research.....Vera R. Filby (968-7119s)
Traffic Analysis..Robert J. Hanyok (968-8418s)

For subscriptions
send name and organization
to: [redacted] P14

To submit articles or letters
by mail, to: P1, Cryptolog

via PLATFORM mail, send to:
cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no 'O' in 'log')

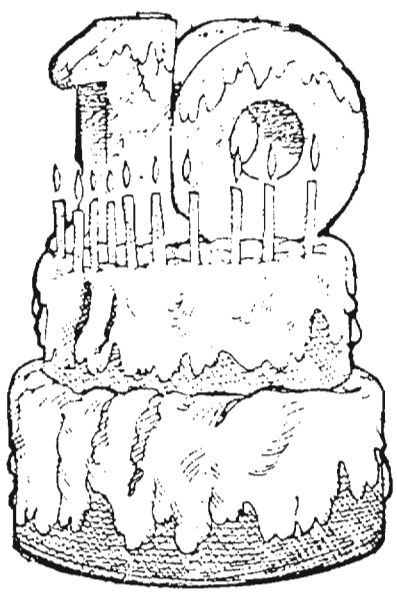
Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

Just ten years ago this month, the first issue of CRYPTOLOG appeared. That issue was introduced to its readers by MGen Wolfe, DDO, as

"...a new vehicle for the interchange of ideas on technical subjects in Operations. Operations is a large organization; the skills and talents on which we depend are many, our workings widely scattered and often sequestered in compartments. These conditions argue for special efforts to keep us in touch with each other and with new problems as they arise and new solutions as they are developed...To be successful, CRYPTOLOG must reflect current operational topics in a way that interests you and others. I hope that you will want to read it and will help write it."

Looking back over the decade, it is clear that a lot of people have wanted to read it, and quite a few have helped write it, and many more have helped to get the magazine out, working behind the scenes in a variety of ways. Whatever its success, it has been the result of many willing people.



~~FOR OFFICIAL USE ONLY~~

DOCID: 4009929

~~FOR OFFICIAL USE ONLY~~

OPENING REMARKS: 1984 SPRING CONFERENCE (U)

LT. GEN. LINCOLN D. FAURER,

Director, NSA/CSS

Good morning. I'm happy to be able to open the 1984 CISI Spring Conference and I can't think of a more appropriate and timely topic than "Personal Computing." In the course of the next four and a half days, nearly every facit of personal computing at NSA will be covered in the various sessions and demonstrations which are listed in your programs. I urge you to attend as many of these as your time permits. Whether you are a newcomer to NSA, or an NSA veteran new to personal computers, or a seasoned NSA computer professional, I think you will find this a worthwhile conference.

In the next few minutes, I will give you some of my ideas about personal computing and the role I believe it should have in our future.

This Agency has had a long history of leadership in the application of the very latest technology to our missions. From our earliest days at Arlington Hall during World War II to the present, computers have been an indespensible tool to both the SIGINT and COMSEC professional. By the early 1960's, vacuum tube computers had been replaced by second generation transistor machines and the first software operating systems made their appearance. Users could now submit their jobs in the form of punched card decks and magnetic tapes "over-the-counter" for operators to run. Computers were extremely expensive and these jobs were batched up for efficiency and run sequentially on the machines. The emphasis was on machine efficiency--not "people efficiency".

As hardware increased in speed and capability and decreased in price, new software techniques made operating systems possible which could run a number of programs seemingly at once. Communications hardware and timesharing software made it possible to put computer terminals remote from the main computer and for the first time, analysts and users of all kinds were able to access programs and data from their work areas and not make the trip to the basement. Terminals were still often shared, however. They simply cost too much to put on every desktop.

By the mid-1970's, the teletype type of terminal was giving way to the CRT terminal and by the end of the 1970's, many of these terminals (now considered "intelligent" with their own microcomputers inside) were being connected to smaller mini-computers which were able to communicate with the large mainframe computers over the PLATFORM network. Although computing capacity and service continued to improve, in many cases the user was still totally dependent for even the simplest processing tasks upon computers and professional programmers over which he had little control.

In 1978, K. Speierman, then the Assistant Deputy Director for Telecommunications and Computer Services, began the first systematic introduction of commercial personal computers into NSA. Encouraged by a few experimenters in various parts of the Agency who were using these inexpensive machines to solve problems in telemetry, signals, and cryptanalysis, he arranged to buy a half-dozen Radio Shack TRS-80's and he gave them to analysts in various parts of the Agency to evaluate in their work. The result was a real but not unqualified success, as you might expect. It often took the analysts longer to poke in their traffic than it did to run the programs against it. Many did this willingly, however, because for the first time, it gave the analyst direct control over some part of his processing using his personal computer. Nonetheless, it became clear that to be really useful, we needed to connect these personal computers to the larger computers that already processed our signals and traffic.

~~FOR OFFICIAL USE ONLY~~

As the demand for personal computers increased throughout the Agency, the need for TEMPEST-qualified personal computers, and for standards in hardware and software were necessary. Since DDT already had a program underway to replace computer terminals with full-fledged personal computers through a competitive procurement, some interim standards were established for both hardware and software.

The same situation existed in the office automation arena. Again, interim standards were established and DDT initiated the Agency's Office Automation Program (which includes an Executive Support System) to help those of us at every level who manage this large, complex organization.

Last year, DDT also established a personal computer "store"--the PCIC or Personal Computing Information Center--where Agency "customers" can obtain computers and software, get information and demonstrations, and be assured of continued maintenance and support and help for whatever problems they might have.

Many organizations in this Agency are making significant contributions to personal computing. DDC pioneered in using personal computers for executives and managers who needed to communicate with each other, to access project information, and to perform a variety of other office functions.

DDR has had a program to develop and promote powerful personal workstations for several years now. Many of you have seen the very impressive graphics capabilities which have been developed and which are finding their way into important SIGINT and COMSEC applications throughout the Agency. More recently, powerful symbolic processors are being evaluated as part of our Artificial Intelligence program.

Local area networks are being introduced to connect a large number of personal computers or office workstations together with PLATFORM and the major processing systems in the basement and at various other locations. The Defense Computer Security Center here at NSA is developing ways to safeguard the very sensitive data we handle in these computers and networks. Security becomes even more important as computing is decentralized and computers move out of the computer rooms.

Throughout DDO, people are continually finding new and imaginative ways to apply personal computing to their work. The SIGINT and COMSEC analysts, and people everywhere with difficult problems to solve, continue to be the pathfinders and you will have a chance to hear about their experiences during this conference.

Three years ago, an NSAAB Panel published a report on Network Architecture. In that report, they estimated that if automation could result in a modest gain in individual productivity of only 8 to 10 percent, it would pay to invest up to one-third of the average annual salary (then about $27,000). That's $9,000 per employee. I believe that such gains are possible for a large part of our workforce and I would like to see us aggressively planning to make that level of investment in our people. I am pleased with the progress made thus far. But, I want us to do a good deal more.

I want to see a personal computer or office workstation on the desk of every individual in this Agency who believes he or she can put it to use. I want to see these workstations interconnected on networks where sending notes, messages, files, correspondence, and reports is a routine practice--the way we do business--and as commonplace as picking up the telephone. I want to see all of our information adequately safeguarded--yet easily accessible to anyone who needs it. I want to see intelligent workstations which can do routine tasks and free people for more challenging tasks, which can help our top professionals accomplish even harder tasks than they can today, and which can capture some of the expertise of our very best analysts, managers, and planners to assist those less experienced to do a better job. I want us to continue to try to apply the very best and the very latest in hardware and software technology to our work and our problems.

While NSA has always been in the forefront of technology and its application to the very difficult and complex job we have, our people are our greatest resource. Technology is an important tool to help people work better--work smarter. This new generation of personal computing technology, when coupled with supercomputers, networks, and information storage systems, has the potential to do just that.

Just as the personal, family automobile changed the face of America, so will personal computing. Just as the automobile brought with it problems such as congestion and pollution, so personal computing will not be without its problems such a security and information management. Nonetheless, just as the private automobile brought with it the opportunity for people to expand their personal and professional horizons, so too will personal computing in ways which we are only beginning to imagine. I would urge you--whatever your job might be--to continue to look for those opportunities. We at NSA are indeed fortunate to be a part of the beginning as well as the future of personal computing.

DOCID: 4009929

P.L. 86-36

THE SOVIET CENSORSHIP DILEMMA:

MOTIVATION VS. SECRECY (U)

by [redacted]

Soviet elections are usually the subject of ridicule in the west because of the lack of choice at the ballot box. However, they play a crucial (U) role in legitimizing the Soviet leadership and the political system as a whole, and are the focus of exaggerated media attention whenever they are held. For about two months prior to each election, the newspapers are full of accounts of the nomination of Ivan Ivanovich to be a deputy to this or that Soviet, and subsequent accounts of his meeting with prospective constituents. Considering that Soviet newspapers as a rule are only four pages long with the last two pages devoted to international news, sports, and weather, this makes the elections the single biggest news item of the entire "campaign" period.

(U) There is a dilemma in this orgy of media hype. Probably most people know that the USSR has an entrenched and disciplined bureaucracy devoted to press censorship. The censors' job is to assure that none of a voluminous list of "State Secrets" are exposed. High on that list apparently is any information on the Soviet defense industries. This is carried to such extremes that under normal circumstances many defense industry facilities will not be identified by name, even in the most innocuous context: key managers and experts are virtual non-persons. The censors must go crazy at election time.

(U) The process of elections is intricate: first a date must be set; electoral districts must be defined geographically; electoral commissions must be appointed to validate the nomination of candidates; the candidates (designated by the party) must be formally nominated and registered with the electoral commission; the candidates must meet with their prospective constituents; and only then are the elections held. Finally, a few days after the election, the list of deputies is published.

~~(TSC)~~ Each of these stages is fraught with danger for the censors. A classic example of vigilant (but too obvious) censorship backfiring occurred in 1971. The published list of electoral districts for the Tadzhik Republic elections skipped over four districts in the Leninabadskaya Oblast'. This was fairly obvious, because the districts are numbered consecutively, and the list skipped from district number 255 to 260. Theodore Shabad, a renowned expert on the USSR writing for the New York Times, noted this discrepancy and, using census data and other public information, extrapolated the existence of a "secret city" with a population of 24,000 engaged in the mining and processing of uranium. Probably as the result of severe embarrassment, the 1974 USSR Administrative-Territorial Handbook acknowledged the existence (since 1958) of the city of Chkalovsk with a population of 26,000. SIGINT and collateral information confirmed Shabad's other speculations.

(U) That episode apparently convinced the censors of the futility of totally omitting electoral districts: the practice has not been repeated. The censors have a more difficult problem with the candidates themselves. Public recognition and praise are especially important in the Soviet Union where financial incentives are not very strong for ideological as well as economic reasons. For those in the defense industries, the system is torn between the need to reward deserving personnel publicly and safeguarding "state secrets."

~~(C)~~ This problem is particularly acute in the local city elections as opposed to the Republic or National elections where a much more diffuse population is involved; Moscow elects 1,000 deputies to its city soviet every other year, but sends only a score of deputies to the USSR Supreme Soviet every four or five years. Until 1982 the censors used three devices to limit the exposure of defense industry personnel elected to the Moscow City Soviet:

1. News reports of meetings with prospective constituents generally were limited to the non-defense sectors. There were exceptions, notable by the fact that usually distinguished by the fact that the facilities were not directly identified. Even these reports were revealing though, because almost invariably the director of the enterprise introduced the candidate (usually to warm or stormy applause), and sometimes the mere identification of a director can have intelligence value.

2. Reports on the registration of candidates were spread out over several weeks and between two different newspapers with no biographic information. All that was published was the full name and electoral district of the candidate (e.g., "District 651"), so no determination of defense industry affiliation could be made.

3. The final list of deputies was published in alphabetic order by name, again giving only the electoral district of the deputy.

Because of these censorship practices, the best you could do was collect all the reporting to garner whatever identifications there were, rearrange the list of deputies in electoral district order, supply the identifications from the collected reports, and notice the remaining gaps. Since electoral districts are apportioned by section (RAJON) of the city, and deputies are chosen by their area of employment rather than residence, the result is an economic-geographic profile of Moscow, with the blanks suggesting, however tenuously, the location of defense industries and related personnel.

~~(C)~~ 1982 was different. Prior to the election of 20 June, the names and job titles (of a sort) of all (all!) the nominees were published in the two city newspapers over a two-week period from 20 May to 2 June. Thus by simply cutting and pasting (for want of a word processor), it was possible to create a list of all deputies to the Moscow City Soviet arranged by electoral district, and consequently by rajon, with the organizational affiliation of each deputy.

(U) The personality identifications provided by the press ranged from numbingly complete for the least significant individuals to super perfunctory for defense industry employees: of the 122 defense industry employees elected to the Moscow City Soviet in 1982, over 70% were identified enigmatically with "a machine building plant" (39%) or "a scientific research institute" (26%) or "a mechanical plant" (9%). These "incomplete identifications" are dead giveaways to defense industries: they're better than asterisks. Perhaps these facilities have no proper titles (not likely), or their titles may be too provocative--identifying too clearly the function of the organization; but then again the editors of the newspaper may simply want to play it safe and not get a security violation. Soviet censorship practices may generally be very predictable, but in these minor details they seem inconsistent.

(U) It seems that the Soviets themselves are often not too sure what to call these organizations. When you compare the 1980 and 1982 elections, you find the same persons identified differently. In many cases a person was identified as head of "a scientific research institute" one year and head of "a machine building plant" the next. One possible explanation is that the individuals oversee a research and production complex incorporating both an institute and a plant. So technically they could be identified with either. It's a good bet however that changing the job titles was done deliberately to be confusing.

~~(S)~~ Other examples of changing job titles are more interesting. In one instance the correct organization title was given in 1982 where it had been sanitized in 1980; in another instance two organizations that were properly identified in 1980 were sanitized in 1982. Apparently the censors or the editors or both can't make up their minds. One example is the Scientific Production Association "Kvant" (Quantum) headed by Nikolaj Stepanovich Lidorenko. In 1980 Lidorenko was properly identified, but in 1982 he was identified as "general director of a machine building plant." The Association is subordinate to the Ministry of the Electrotechnical Industry, which is not considered a defense industry. The censors' ambivalence regarding Kvant is prima facie evidence that its primary function is defense industry-related regardless of its ostensible subordination.

~~(C)~~ Even the enigmatic can be revealing. Yurij Ivanovich Krashnoshchekov was identified simply as "director of a scientific research institute" in the Krasnovardejskij Rajon. A search of open literature revealed that he is a chemical laser expert. Previously he had been just another name on technical manuscripts. Now his writings may take on added significance for analysts of the Soviet laser weapons program.

(U) For the Moscow City Soviet as a whole, 12.2% of the deputies came from defense industries. The following list shows the administrative areas ranked by the number of defense industry representatives on the city soviet.

P.L. 86-36
EO 1.4.(c)

Since some areas are much larger than others, the number is also shown as a percentage of the delegation from that area; e.g., Zelenograd had only 8 deputies from the defense industries, but that represents almost half of the deputies from Zelenograd.

Administrative Area	Defense Industry Deputies	Percentage of Deputies from that area
Tushinskij Rajon	13	46%
Frunzenskij Rajon	9	32%
Kuntsevskij Rajon	9	26%
Zelenograd City	8	47%
Kievskij Rajon	7	25%
Kujbyshevskij Rajon	6	15%
Cheremushkinskij Rajon	6	14%
Perovskij Rajon	6	13%
Krasnogvardejskij Rajon	6	12%
Leningradskij Rajon	5	14%
Timiryazevskij Rajon	5	13%
Pervomajskij Rajon	5	12%
Kirovskij Rajon	5	10%
Dzerzhinskij Rajon	4	15%
Sovetskij Rajon	4	9%
Baumanskij Rajon	3	18%
Leninskij Rajon	2	10%
Sverdlovskij Rajon	2	10%
Sokol'nicheskij Rajon	2	10%
Lyublinskij Rajon	2	7%
Vorshilovskij Rajon	2	6%
Proletarskij Rajon	2	6%
Volgogradskij Rajon	2	5%
Kalininskij Rajon	1	6%
Zheleznodorozhnyj Rajon	1	5%
Moskvoretskij Rajon	1	5%
Krasnopresnenskij Rajon	1	4%
Babushkinskij Rajon	1	3%
Sevastopol'skij Rajon	1	3%

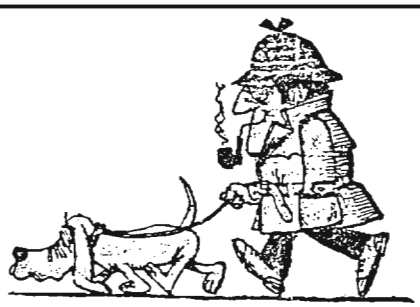
Gagarninskij, Zhdanovskij, and Oktyabr'skij Rajons had no defense industry deputies.

cause the chances are that by now they already have realized the jeopardy in repeating the 1982 procedures.

[redacted]

P.L. 86-36
EO 1.4.(c)

[redacted]



WE ARE ALWAYS LOOKING FOR

ARTICLES, COMMENTS, NOTES, LETTERS,

THAT WOULD BE OF INTEREST TO OUR READERS

DOCID: 4009929 EO 1.4.(c) P.L. 86-36

by [redacted] Q11

LONG-RANGE PLANNING & NSA (u)

(U) Long-range planning. The words glide smoothly off the tongue. Like motherhood, long-range planning has few detractors, but most give it only lip service. In actual practice we often fail to plan, even in the most important areas of our work--and, indeed, in our everyday lives. Too often we become victims to events, tossed in one direction or the other, unable in the midst of a crisis to plot an effective course. The wisdom of planning for the future is virtually self-evident: it gives our actions a reasonableness, a sense of purpose, that would otherwise be missing.

(U) What are the benefits of long-range planning? In studies that compared organizations that do such planning with those that do not, the results are conclusive: planners consistently outperform nonplanners. [1] Why? An important reason is that organizations without long-range planning tend to concentrate on what they are already doing. They try to improve their present operations by doing more, being more efficient, and working harder. And this often works. But sometimes the "try harder" approach fails, not because the people don't work harder but because the external conditions have changed. The current strategies of the organization, those that may have served so well in the past, no longer apply. Perhaps technological change has caused the dilemma, and the change may be so extensive that the organization no longer serves a useful purpose. Alvin Toffler refers to this problem in Future Shock when he describes "Rising rates of change [that] compel us not merely to cope with a faster flow, but with more and more situations to which previous personal experience does not apply." [2]

> *"If we could first know where we are and whither we are tending, we could better judge what to do and how to do it."*
>
> *--Abraham Lincoln*

(U) Effective long-range planning concentrates on what we should be doing now to prepare for, say, 15 years from now. This perspective encourages the consideration of creative, nontraditional approaches. It prompts us to think about where we want to be and how to get there from where we are, as opposed to concentrating only on today's problems. It is truly an opportunity to try to "invent" our future.

(U) With the above as background, let's take a look at the Agency's long-range planning efforts.

~~(C)~~ Long-range planning at NSA has a rather brief but rocky history. Although the Agency was created by Presidential Order in 1952, it was not until 1974 that the Director, General Allen, recognized the need to develop an effective long-range planning system, particularly for SIGINT. Some long-range planning may have been going on during this 22-year interval, but the Agency had no overall long-range planning system. Our planning was often fragmented and uncoordinated by the various organizational elements. All too often it was focused on and driven by the near-term concerns of the programming and budgetary processes and by what was of current interest to intelligence users.

~~(C-CCO)~~ There is no simple explanation for why it took so long for the Agency to recognize the need for a long-range planning system. One reason might be that the discipline of long-range planning was still in its infancy and was neither well known nor widely practiced during this period. Then too, the SIGINT business was somewhat simpler in the 1950's and 60's. We didn't need to justify our actions to the Congress in such painstaking detail--and the communications signals we were collecting were relatively unsophisticated and easier to deal with. The equipment to collect and process such signals was not so complex or so terribly expensive. It could be built in our own research laboratory or purchased outside without much difficulty. But with the virtual explosion of sophisticated, high-speed signals worldwide in the 70's and the long lead times needed to develop and field the expensive equipment capable of collecting and processing such signals, long-range planning became essential.

~~(U)~~ In 1974, in response to pressures from the Intelligence Community, the Agency produced the National SIGINT Plan (NSP), our first effort "to provide a single, coherent statement of the direction in which the SIGINT effort ought to go during the next several years." [3] Because the writer of the NSP was in desperate need of help, and at the Director's urging, an Architectural Planning System was developed in 1975 and continued to function until 1979 "to establish a framework that will permit optimizing of the SIGINT system" and to help those charged with writing the NSP. [4] It was not long before an Architectural Board was created. The Board was supported by Target Architects, who were selected from appropriate target mission organizations (e.g., A Group, B Group), and by Area Architects, who focused on such topics as Collection Systems, Central Processing Systems, Exploitation Systems, and Support Systems. Unfortunately, those involved in the venture received little guidance. Their "marching orders" seemed to amount to "I'm not exactly sure what it is I want, but I'll know it when I see it." And the various Architects often did not operate through the regular line management structure of the Agency. In effect, they represented a structure apart from the regular organization, sometimes even competitive with it. Then there was the lingering problem of getting agreement on a pictorial model that represented NSA's SIGINT architecture. Any number of models were offered, but none presented a comprehensive depiction of the SIGINT System.

(U) Some of the important lessons learned from the exercise were:

[] Before writing any plan, know who will use it, the form they want it in, and how they intend to use it;

[] Everyone involved understood the need to plan first, but all too often there was a tendency for the plan to be controlled by the budget;

[] If planning can be divided, divide it in a way that can be readily understood and is consistent with the organizational structure;

[] A good plan is a good map that clearly shows what should be done, when it should be done, who should do it, and (at least roughly) how much it will cost; and

[] There has to be a review or control mechanism to ensure proper execution of a plan.

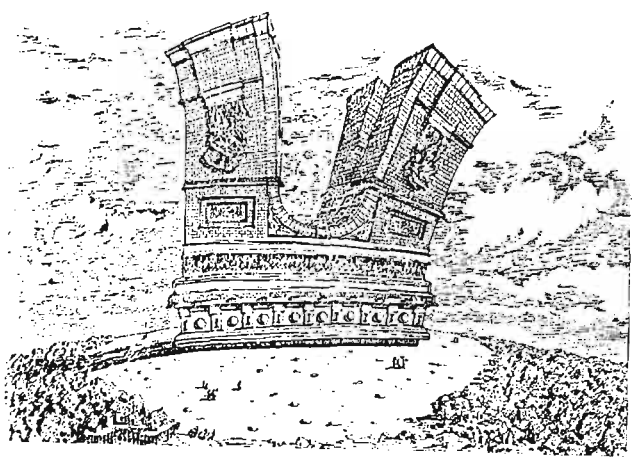
~~(FOUO)~~ After 1978 the NSP became the United States SIGINT Plan (USSP), but this was merely a change in title. The problems associated with developing a comprehensive long-range planning system persisted. Various studies were performed during this period, including one by A. D. Little, a Systems Acquisitions Study, and a study on Resources Management. All pointed out that planning was not adequately performed within the Agency and all recommended substantial changes.

~~(FOUO)~~ Recognizing the need for a formal long-range planning system, the Director in 1980 established a new Key Component, the

Deputy Directorate for Plans and Policy (DDPP). The long-range planning function, which was formerly the responsibility of the Assistant Director for Programs and Resources (ADPR, now called DDPR), now resided in the new organization, in the Directorate of Plans, Q1. It was hoped that by separating long-range planning from the short-term concerns of the budgeting and programming processes, more effective and innovative planning would result, planning that would be based on clearly defined goals and objectives.

~~(FOUO)~~ The Baseline Planning System was implemented in 1980. Two cycles of SIGINT Baseline Plans were completed, one in 1980 and the other in 1981. Only one cycle of COMSEC Baseline Plans was completed, in 1980. After affected elements received planning and procedural guidance from DDPP, they developed plans which were modified and adopted on their way up the organizational chain to the Deputy Directorate for Operations (DDO) or the Deputy Director for Communications Security (DDC), as appropriate. Various other Key Components, like the Deputy Directorate for Telecommunications (DDT) and the Deputy Directorate for Research and Engineering (DDR), were then expected to write "Response Plans" in reaction to the DDO and DDC Baseline Plans.

~~(FOUO)~~ Although an improvement over the Architectural Planning System, the Baseline System was plagued by a number of problems. Procedural guidance was provided by DDPP, but it was often inadequate to assist planners in developing effective plans. In addition, the process generated enormous amounts of paperwork, far too much for upper-level managers to have time to read and absorb. And, contrary to the intent, the system tended to produce "bottom-up" plans: lower-level managers presented executives with long-range plans, with little or no insight as to what the executives intended as the long-range goals and objectives of the Agency. And finally, although it was intended that the Baseline Plans "drive" the program build (the process whereby plans are implemented), they actually had little or no effect on it.



~~(FOUO)~~ To create a more effective long-range planning system, one that would have the full support of senior executives, a Task Force on Planning was convened in 1982 under the direction of DDPP. It developed a "Revised Planning System." [5] The Senior Review Board (SRB), which had been formed in 1981, was reorganized in late 1982 and met, as recommended by the Task Force, to corporately guide and implement the long-range planning concepts and objectives that were proposed. The SRB is composed of the NSA/CSS Deputy Directors (DDA, DDC, DDO, DDPP, DDPR DDR, and DDT), the Assistant Directors (ADC, ADIL, and ADT), the Chief Scientist, and the Chief of Staff. Other senior managers, including SCE chiefs and chiefs of field activities, may also be invited to attend meetings, depending on topics under discussion. Initially chaired by the Deputy Director, NSA, since September 1983 the SRB has been chaired by the DDPP.

~~(FOUO)~~ The new planning system differs from the previous long-range planning systems in some important ways:

[] there is top-down direction and control; senior managers are fully involved and support the system; corporate review and approval of plans is an essential feature of the system;

[] planning has been institutionalized in a number of Key Components; specific organizational elements have been established primarily to do long-range planning;

[] the long-range planning process is continuous throughout the year, rather than being a once-a-year exercise;

[] line managers are responsible and directly accountable for plans and their implementation; and

[] plans are based on established long-range goals and objectives, as documented in NSA/CSS Directive 25-2.

~~(C-CCO)~~ As one surveys the landscape of NSA's long-range planning efforts, it becomes increasingly clear that the task of developing and implementing a long-range planning system is extremely difficult. The rewards of an

DOCID: 4009929

effective system, however, are great. As the Director wrote in his guidance for the development of the FY86-90 Consolidated Cryptologic Program (CCP), "The accelerating growth and sophistication of worldwide electronic communications and weapons-related data, and a commensurate foreign effort to protect and deny information, presents an unparalleled challenge to the mission of the National Security Agency/Central Security Service.... Given the breadth and complexity of the challenges, the expanded requirements, and the rising costs we will face in the next several years, it is clear that some difficult choices will have to be made." [6]

(U) It is important that we support the Agency's long-range planning system. The new system is not perfect--it will need time to evolve and mature--but it offers the best hope for a vital, effective cryptologic effort as we face the decade of the 90's and beyond.

FOOTNOTES

1. George R. Terry and Stephen G. Franklin, Principles of Management, Richard D. Irwin, Inc., 1982, pp. 153-4.

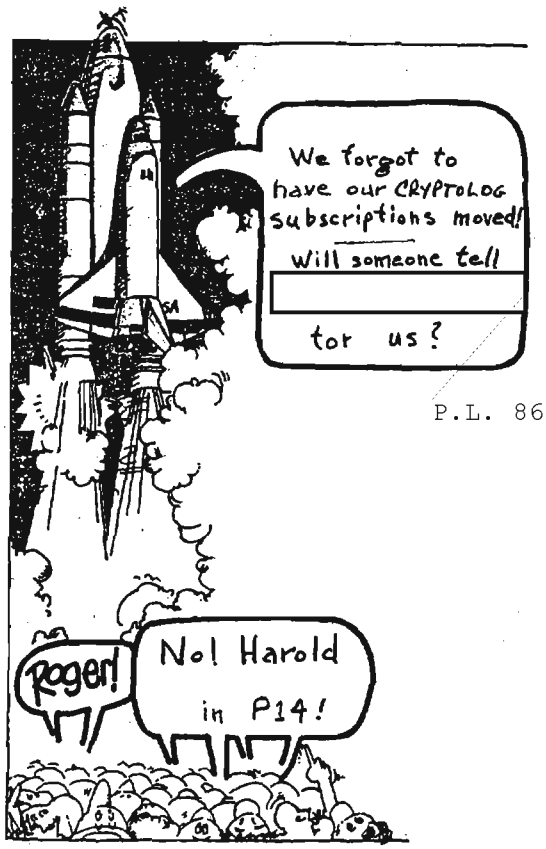
2. Alvin Toffler, Future Shock, Random House, Inc., 1970, p. 34

3. National SIGINT Plan, 14 November 1984, p. 1.

4. Information on the Architectural Planning System is derived from a briefing given in the Friedman Auditorium on 16 December 1982 by [redacted] Jr., Chief of T2, and is used with his permission.

5. "The Revised Planning System" was retitled "NSA/CSS Planning System." The latter is formally documented in NSA/CSS Circular 25-11, dated 28 February 1984.

6. Memorandum from the Director, subject: FY86-90 Consolidated Cryptologic Program Planning Guidance, 16 March 1984.



P.L. 86-36

P.L. 86-36

SOLUTION TO NSA-CROSTIC no. 54

"Identification of [Antennas and Other] Items [on the Roof of the Operations Building 1]," L5 Memorandum by T. L. [redacted] dated 31 January 1984. P.L. 86-36

"The Exterior Retrofit...Project is entering into the final design stage. In order to install the TEMPEST shielding on the roof, all items attached to the roof...must be identified... Items not identified...will be removed and disposed of during the construction."

Solvers who had difficulty with this puzzle are advised that Word 0 is boustrophedonic, *an adjective describing writing systems in which the lines read alternately left-to-right and right-to-left, which is the way this puzzle was set up.*

P.L. 86-36

(U) On 1 January 1984 the American Telephone and Telegraph (AT&T) Company completed the terms of the divestiture agreement which spun off all local operations and the Yellow Pages into seven regional holding companies. The consent decree modified final judgment was carefully scrutinized by the courts, the Congress, the Federal Communications Commission (FCC), and the Department of Justice (DoJ) for its "public interest" considerations. However, the national security impact is only now starting to be realized. The new competitive structure of the telecommunications industry will of necessity alter the fundamental relationship between DoD and AT&T. Partly in response to concerns expressed by DoD, a Central Service Organization (CSO) has been formed. It will be jointly owned by the seven regional companies and will furnish the companies with technical assistance, such as network planning, engineering, and software development. It will also provide various consulting services and other assistance that can be more effectively provided on a centralized basis. Even though the CSO will help coordinate central planning requirements, the days when DoD could call a single point of contact (e.g., AT&T) who would provide end-to-end service for all requirements is over.

(U) Recent national security policies have recognized the dependence of our national defense on the privately owned common carriers for providing the majority of the national telecommunications for Continuity of Government (COG), National Command, Control, Communications, and Intelligence (C^3I), and other critical functions. According to LTG William Hilsmann (USA, Ret.), former manager of the National Communications System (NCS), 95 to 98 percent of the DoD's communications in the US are controlled by the private sector, whereas in Europe between 65 and 70 percent of the communications network is actually operated by the military or the host government under the Post Office department. The existence of AT&T as a dominating monopoly which could provide end-to-end service and set technical standards for the industry made coordination a relatively straightforward process. The AT&T divestiture will complicate requirements for end-to-end service. More complicated and time-consuming competitive arrangements will have to be made with the Bell operating companies, equipment manufacturers, AT&T, and other long-haul carriers for communications services and equipment. The cost of communications services to DoD may rise because of the increased requirements to coordinate the various suppliers of service and the increased complexity of the contracting process.

(U) During the divestiture process, there was preoccupation by the FCC and the courts with the issue of how to move from a monopoly to a competitive environment, often to the detriment of national security and emergency preparedness concerns. DoD worked with the courts and DoJ to address the concerns. DoD worked with the courts and DoJ to address the potential conflicts between defense requirements and the new marketplace approach. Unfortunately, all the problems were not reconcilable with the divestiture and a less than ideal result has emerged. In the past DoD could count on AT&T to set standards for interoperability and, in the event of natural or man-made disaster, AT&T had the authority and power to direct personnel, equipment, and material in the execution of emergency relief operations. To fill the power vacuum created

DOCID: 4009929

by divestiture, the National Security Telecommunications Advisory Committee (NSTAC) was created to bring together senior executives, leaders of the major elements of the telecommunications industry, and the NCS for long-range communications planning in the new competitive environment. New technical initiatives to improve the emergency responsiveness of the nation's telecommunications systems depend heavily on the commercial common carriers. NSTAC was intended to be a source of expertise, knowledge, and insight for the President that would not otherwise be available within the Government. For the nation's emergency and defense requirements to be satisfied in the long run, members of the NSTAC will have to lay aside their competitive interests and agree on standards of operation, interoperability, and emergency procedures. It is still unclear how NSTAC members will respond to national security/emergency preparedness proposals that might adversely affect service or result in the loss of competitive edge and revenues.

~~(S)~~ The divestiture of AT&T will directly impact on NSA's telecommunications protection efforts underway in the S Organization, which has been working with the National Communications System, AT&T, and other major common carriers to protect some of their most vulnerable circuits from intercept. The divestiture adds new complexity to the telecommunications protection program, which will now require involvement of the regional and local Bell operating companies and the CSO.

~~(C)~~ National telecommunications policy planners are especially concerned at this time with the growing participation in the design, manufacture, and engineering of the telephone system infrastructure. Foreign technological capabilities and manufacturing abilities, which have resulted from cooperative foreign governmental and industrial arrangements, have strategically coincided with the divestiture of AT&T and the large-scale introduction of the new services and equipments to the telecommunications system. The US telecommunications network and industrial structure is in the process of considering and implementing some major changes. The telecommunications system is changing, becoming primarily digital, and the old equipment is being replaced by sophisticated "smart systems." These new digital equipments are being energetically marketed by foreign equipment suppliers. The situation presents an opportunity for unprecedented penetration of the US national telecommunications system.

(U) DoD communications planners have traditionally not had to concern themselves with the problems and consequences of unrestrained foreign competition. Until recently, AT&T and its manufacturing subsidiary Western Electric handled the nation's telephone network equipment and planning requirements. Western Electric worked closely with the national security planners to ensure that certain minimum technical standards were maintained for the responsiveness of the system in the event of disaster or to satisfy mobilization requirements. The advent of the AT&T divestiture complicates this situation considerably by reducing AT&T (including Western Electric) to just another member in the field of telecommunications competitors. This field also includes, for the first time, a large number of economically aggressive and technically competent foreign competitors. Now policy planners must consider a number of new factors when evaluating the national security impact of foreign suppliers:

1. Will the foreign-manufactured equipments meet previously established standards for technical capability and quality? This raises another question: Should all equipment standards be published for the benefit of all competitors, even though in so doing we might be giving away information of value to military adversaries?

2. Will foreign suppliers have the capacity to resupply US emergency requirements? (Some national defense planners question their ability to do so.) Along this same line, would any foreign equipment supplier have the military capability or political will to support resupply efforts?

3. What about the national security concerns over the requirement for a foreign firm to maintain a mobilization base in the US to develop, manufacture, and maintain equipment in wartime?

(U) A recent case illustrates the defense concerns as they relate to the telecommunications equipment industry in the new, unregulated era. This case involved the installation of the first long-haul lightwave (fiber optic) cable. The first leg of this system

DOCID: 4009929

runs between New York and Washington, DC, with additional links planned to run north to Cambridge, Massachusetts and south to Richmond, Virginia.

(U) FCC approval was given to Bell to proceed with the initial New York-Washington line with the proviso that the system be procured through competitive bidding rather than by traditional implementation and procurement through Bell Labs/Western Electric. The FCC further ruled that performance requirements could not be specified in the bidding, only system design specifications. The FCC staff was concerned that performance requirements might give Western Electric an advantage over other competitors. However, the result was that requirements for the protection of the system against the effects of nuclear weapons and other defense considerations could not be included.

(U) In response to AT&T's call for bids, there were responses from two US firms (including Western Electric) and six foreign companies (including Fujitsu of Japan). The lowest bid was submitted by Fujitsu, which was in the process of being awarded the contract when the questions of national security were interjected. The national security concern led to the awarding of the contract to Western Electric.

(U) If this contract had been awarded to a foreign firm, it would have been the start of foreign encroachment into an area of critical importance to the US communications network. This is another instance of confusion and lack of coordination between Government elements. The FCC failed to consider the national security implications of carrying out its regulatory goals.

(U) The divestiture of AT&T and the deregulation of the telecommunications industry will create new problems and new opportunities for the national security telecommunications planners. Ironically, the result of this new competitive environment will call for increased Government collaboration with the telecommunications industry to ensure that national security and emergency preparedness interests are considered. The planning methodologies and relationships relied on in the past by the DoD are no longer possible in the new, competitive, post-divestiture era of telecommunications policy.

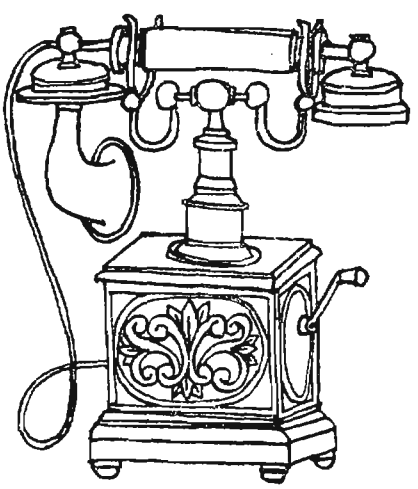
Correction

The article called "Suicide Shell" in CRYPTOLOG, May 1984, pp. 6-7 contains an error. Near the end of the second column on page 6, there was a line that read

```
5>1,$s/^.*$/mv & ../part2/
```

and should have read

```
5>1,$s/^.*$/mv & ..\/part2/
```



OCID: 4009929

Golden Oldie

QUALIFICATIONS OF A CRYPTANALYST (U)
from Elements de Cryptographie
by Capt. Roger Baudouin, 1939

translated from the French
by Capt Albert E. Highley, A.U.S. [c 1945]

The history of cryptographic science teaches us that the "decipherer" (today we would say decrypter) has long been considered a kind of magician, a likely candidate for the stake.

Thus in 1595 when the mathematician Francois Viete, in the service of King Henry IV, imprudently boasted to the Venetian ambassador Giovanni Mocenigo that he had decrypted several despatches from the Spanish King, Phillip II, the latter complained vehemently to the Pope about it and accused France of "having the Devil and sorcerers in her pay."

Voltaire wrote in the article "Postes" in his philosophic dictionary, "those who would boast about decrypting a letter without knowledge of the contents thereof and without preliminary assistance are greater charlatans than those who would boast about understanding a language they have not learned."

This extraordinary idea of the "decrypter" seems to have persisted for a very long time. During the war of 1914-1918 Major Givierge, Chief of the Cipher Section at GHQ, will always be listed among the greatest masters of cryptographic science, was often called the "Sorcerer" by his comrades on the General Staff.

The reality about "decrypters" is very different. Cryptanalytic research, because it requires intellectual training and broad cultural background, is the achievement of an elite, but it does not to any degree depend upon magic or the art of divination. Although it is true that it requires special gifts of logic and intuition, it is also true to say that any cultivated mind can attempt it with a chance of success. Experience shows that many individuals who were unfamiliar with this discipline at first, have eventually become able cryptanalysts with brilliant successes as the result of work and private study, and with the assistance of only their own enlightened intelligence.

Above all the cryptanalyst--and this is an essential condition--must have an inclination for research. The main attraction of cryptanalytic research--and those already familiar with this subject know how fascinating it can become--lies in the employment of sure logic and a disciplined imagination, based solidly upon well-founded technique, all employed in unveiling the secret of the cryptogram and conquering even the most ingenious artifices employed by the "enemy" for hiding his thoughts. In this silent battle between two intellects, the joy of discovery and the intellectual satisfaction that follows are an ample recompense for the trials and tribulations of the cryptanalyst.

A cryptanalyst needs many qualities. He must:

1. First, understand and grasp perfectly the mechanics of most classic systems of cryptography. This is the very root of his technique.

2. Show evidence of several mental qualities: clear judgment, logic, imagination, memory, ingenuity, perspicacity, intuition. Actually, experience shows that intuition, which some authors consider the prime attribute of the cryptanalyst, is considerably developed by practice.

3. Have some basic idea about the language to be studied. Although a fluent speaking knowledge is not indispensable, it is necessary to know well its characteristics, essential vocabulary, and fundamental rules of grammar and syntax.

4. Have patience capable of enduring any test. Cryptanalytic study involves long, fastidious research, a sometimes thankless and always wearisome task. Tenacity and obstinacy are indispensable to success.

5. Finally, know how to remain modest, to keep silent about achievements and to restrain boastfulness. In such matters it is easy to see that all considerations of self-esteem must be eliminated.

As one sees, the task of the cryptanalyst presupposes a broad cultural background and at the same time requires a combination of diverse intellectual abilities often hard to find. One might add that mathematical training, though not strictly indispensable, will nonetheless be a valuable help to the beginner.

By contrast to the many qualities needed to be a cryptanalyst, the materials necessary for cryptanalytics can be reduced to very few, essentially, cross-section paper, pencils and an eraser.

DOCID: 4009929

LINGUISTS

AND OTHER MINORITIES (U)

P.L. 86-36

by [redacted]

(U) In 1919 the United States Army sent Joseph Stilwell to the University of California at Berkeley for his first year of Chinese studies. He was slated to go to China as an attaché and later would lead Chinese and American forces against the Japanese in World War II. Stilwell had already mastered several languages and had served with distinction in liaison with our allies in World War I. At Berkeley he quickly realized he was wasting his time because "... there was no one to talk Chinese to after school."[1] He knew he would be better off transferring to China right away because there he could hear and practice the spoken language. He was a proven professional whose ideas should have received careful consideration. In fact, no one refuted his logic. Everyone agreed but no one took action on his recommendation.[2]

~~(C)~~ We tell ourselves that we've come a long way since then, but if we look closely at our governmental approach to foreign language training and application, this anecdote is uncomfortably familiar. Some SIGINT linguists have noted that they are expected to maintain current colloquial and technical proficiency in a language without having any contact with foreign nationals. Linguists and other professionals (such as security managers) really shouldn't be working at cross purposes. There are examples of how to do it right. The Government subscribes to large numbers of foreign newspapers and magazines so that linguists can have access to current materials without direct subscription. There are also recorded materials available, such as broadcast tapes. They are of great supplemental value, but hardly a substitute for two-way conversation. More importantly, they represent a compromise in which two groups of professionals came to understand each others' concerns.

The author, who is now attached to CINCPACFLT CSG in Hawaii, wrote this article before leaving NSA in June 1984.

(U) Before we talk very much more about who those linguists are what concerns them professionally, we had better take note of the fact that most Americans are not linguists. Most Americans, in government and out, are monolingual. Although this monolingualism is a relatively recent phenomenon in human history (the product of large nation states and means of mass communication, such as printing), it is the rule in modern America. By the sheer weight of their numbers, monolingual people will make most of the decisions effecting that specialized group--the linguists

~~(C-CCO)~~ A [presumably] monolingual American once wrote a letter to the editor of a news magazine complaining about the salaries paid to translators at the United Nations "... who only have to look up one word after another in a dictionary." An NSA manager once engaged in the following exchange with one of his senior linguists:

Senior Linguist: Sir, those new intercept positions are very complex. When we deploy the platform for an unexpected contingency, we can't expect linguists for the new target area to be able to cope with all this gear.

Manager: Then we'll use your linguists from the home base area.

[redacted]

Mgr: They don't need to tell us everything, just what's important.

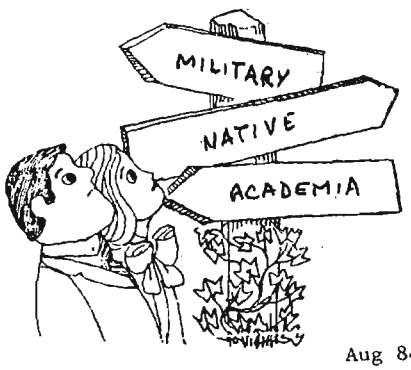
(U) These two anecdotes are not intended to imply that most non-linguists are totally insensitive to the problems of translation. The ability to make an intelligent decision effecting subordinate specialists depends upon finding some way to appreciate the specialist's concerns and involving that specialist in the decision process. Many people automatically assume that because of his celibacy, a Catholic priest can never be a marriage counselor, and yet many of them are. They succeed by drawing from the experiences of married couples whom they have helped and they also consider their own experiences with interpersonal relations in the seminary and rectory. In the final analysis, the priest really doesn't make a "decision" anyway. What he does is help those married people involved to make their decision, guiding them as best he can toward a resolution that is healthy for the larger family and community. Empathy is never automatic, but it is also never out of reach.

(U) There is probably no such thing as a "typical" linguist in or outside the SIGINT community, but there are three main paths to becoming a SIGINT linguist:

[] in the military;

[] being a "native speaker" (i.e., a member of an immigrant family or growing up in a foreign country); and

[] through academia.



~~(C)~~ Many linguists started out as youngsters from monolingual America who joined the Armed Forces and took a bunch of tests. They scored high on the language aptitude test which required them to discern patterns in an unfamiliar language. The easier versions are based on Esperanto, an artificial language in which the inventor wrote all the grammar rules first and then made up the words to fit the rules. Tests based on computer-generated artificial languages with realistically complex grammatical structures are more challenging.

[redacted]

(U) Having done well on the aptitude test, our young linguist-designate goes to language school and learns rote recognition of a limited and highly specialized vocabulary. This training is done very effectively. The academic community has always had the highest respect for the Defense Language Institute at Monterey, California--even in the 1960s and 70s when the defense establishment was none too popular on the campuses.

(U) The young SIGINT linguist is off to a good start, providing that the people he is working for understand that it is only a start. After several months on the job, with proper supervision and supplemental training, he will be an effective SIGINT linguist. Only if he broadens his own linguistic horizons on his own initiative will he ever be able to accompany the President as the interpreter on a state visit.

(U) A second path to becoming a SIGINT linguist is to be a "native speaker," either from an immigrant family or by growing up in a foreign country (e.g, the children of businessmen or missionaries). The immigrant family is one of the many benefits of our melting pot society because it literally takes a lifetime to acquire this type of language proficiency. Of course, the native speaker may find the specialized vocabulary of radiotelephone chatter to be totally obscure at first. A native speaker's vocabulary may also be archaic. One member of the large Hungarian community of Cleveland, Ohio, upon hearing the speech of the Hungarian "man in the street" for the first time, was surprised to hear an indigenous phrase for "rush hour." In Cleveland they had simply inserted the English words in a Magyar sentence. When her parents left Budapest in 1946, the phenomenon of "rush hour" did not exist there.

~~(C)~~ The third path is through academia. Persons trained at a college or university will often have a very solid background, although they will almost certainly have to strengthen their technical background to work as a SIGINT linguist. Those who majored in

the common western languages (German, French, Spanish) may be asked to cross-train in another language. Not only are the college-trained linguists already proven in their ability to learn, but certain combinations of languages are particularly useful

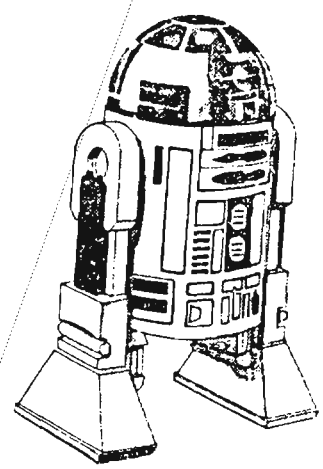
~~(C)~~ When SIGINT linguists work as a team, the skills acquired on the various paths combine to strengthen the total effort.

[] The native speaker may have initially felt he knew only "household" words but he can contribute to an understanding of the colloquial turn of phrase as no one else can.

[] The academic linguist, having helped his professor grade papers for elementary language courses, may be thrown off by the kinds of usage common to soldiers talking on the radio. However, he will bring to the team an appreciation for the structure of the language and an ability to apply certain research skills.

[] The experienced military linguist understands the operational context and peculiar jargon he has heard.

~~(C)~~ Most of the managers in the chain of command above this team will probably not be linguists. However, most of them will be (1) smart, (2) well-intentioned, and (3) generally aware of the sorts of things we have been talking about. They were good at Traffic Analysis, or ELINT, or whatever or they wouldn't be managers now. They will know that their linguists are pros. Hopefully, they will involve the linguists in the kinds of collection management, processing, and analytic decisions that affect them. The managers should encourage the linguists to work interactively with each other. They should encourage them to continue linguistic training and provide them with the necessary tools. They should also help them get the intelligence background they need, to include foreknowledge of friendly operations, so that linguists may see us through the eyes of others and recognize this for what it is.



(U) There are three common misconceptions that monolingual managers should avoid if they have linguists working for them.

(U) First, they should purge the word "fluent" from their vocabularies altogether. This is a very dangerous little word. Webster defines it as "ready or facile in speech." Most people seem to think fluency means that someone who is fluent in a stated language can understand anything that is said in that language and can render it into standard American English in the same length of time it took to utter the original phrase. It takes too long to acquire a working knowledge of a language to reduce the results to being either fluent or not. Much useful work can be done by people at various stages of proficiency.

(U) A second misconception is that linguists can soon be replaced by machines. Many popular science fiction works in print and on the screen have depicted automated translation systems. This has been a useful dramatic device. There is no need to explain the presence of an interpreter in the story. However, a fully automated voice-to-voice translation machine is about as far from reality as WARP drive and protocol droids. The two existing print-to-print systems are of very limited value. The machine translation projects currently under way are valuable for what they are teaching us. Researchers who abandoned the notion of fully automatic translation started to make real progress of immediate practical benefit in the distinct field of machine-assisted translation.[3] This gives a linguist the sorts of tools which have increased the efficiency of so many other white collar workers. There are now multilingual word processors, specialized magnetic dictionaries, and programs which will translate relatively unambiguous phrases and present them to the linguist for review.

(U) Finally, a monolingual manager should avoid the cliché that "it's easier to teach a professional _____ [fill in the blank] to speak a foreign language than it is to teach a linguist to be a professional _____ [ditto]." In some cases this may be true, but in other cases it may be

precisely the opposite that is true. A businessman, scientist, or military officer may study a language for a few months and then go to exchange ideas with his counterparts in another country. His fellow professionals will receive him warmly. They'll put up with mistakes and iron out misunderstandings. But extensive knowledge of a foreign language in a specified period of time, as the following story should illustrate.

(U) A US company once chose a promising young executive to run its operation in France. At great expense, the company contracted with a language school to tutor the executive and his wife. At the first session the teacher put a book on the table and said "le livre." The wife mimicked "le livre" beautifully. The husband croaked out something like "... leu leueueu ..." Two weeks later the wife was learning at a rapid pace and the husband was still stuck on "... leu leueueu ..." The husband and wife got a divorce and the company gave him a new assignment within their domestic division.

(U) The story of the US executive who couldn't learn French brings us back full circle to General Stilwell and his early Chinese training. Anyone can learn another language, albeit slowly and retaining a strong accent. However, many do not learn because the way we go about is so artificial. Our country is so big and our language so pervasive that we can easily get by without learning other languages. In most of North America, learning languages is left to a few specialists. In Europe, on the other hand, it is common for the majority of citizens in a country (especially in the smaller countries) to be multilingual. They become multilingual by daily contact with speakers of foreign languages. Given this context, being multilingual in North America is the normal state. For an individual, or for the nation as a whole, monolingualism is probably a disadvantage for commerce and diplomacy. It does not have to be a debilitating problem if we take it into account.

(U) In a professional context, Americans who are linguists and Americans who are not must all consider language as a factor as much as automated data processing, logistics, and everything else. Linguists must realize how alien foreign-language considerations are to a largely monolingual clientele. Non-linguists must realize that they need qualified specialists and they must go through a selection and appraisal process, just as they would in getting medical or legal help. There are many examples from everyday life in government to show that some people on both sides of the issue do not understand these problems of human communication across language barriers (including linguists speaking to non-linguists in the same language). Hopefully, these realizations will grow along with the parallel realization that the world in all its diversity is getting smaller.

FOOTNOTES

1. Barbara Tuchman, Stilwell and the American Experience in China, pp. 62-4.
2. Ibid.
3. Professor Alan Melby of Brigham University at CLA presentation, January 1984.

DOCID: 4009929

1. INTRODUCTION

(U) This paper attempts to trace the events that thrust the space age first upon the United States and then upon SIGINT. It is very gratifying to have participated in--and perhaps influenced in some small way--both efforts. I believe that my closeness to the former led to my pressing for the latter.

(U) Before describing the actions themselves, I would like to give some background information on conditions that existed during the gestational years. Two or possibly three threads became interwoven to produce a nationally integrated space program. The first was rocket exploration of the upper atmosphere; the second, the International Geophysical Year; and the third, the rather bitter interservice rivalry that then prevailed in this field.

2. US ROCKETRY 1948-1952

(U) My involvement with rocketry began in 1948, when Army Air Corps abolished its Watson Laboratories at Fort Monmouth, NJ. Most sections moved to Griffiss AFB, NY, and established the Rome Air Development Center. A smaller contingent was transferred to the Cambridge Field Station and, together with the Upper Air Laboratory already there, formed the Geophysics Research Directorate of the AF Cambridge Research Center (AFCRC).

(U) I was Chief of the Ionospheric Physics Laboratory, which was engaged in an intensive study of the upper atmosphere and its effects upon radio wave propagation. Our experimental investigations used ground-based or aircraft-borne instruments. The Upper Air Laboratory had overlapping interests and was involved with rocket-borne, in situ probings of the lower ionosphere. Thus, even though the experimentation was quite different, the objectives of the two laboratories overlapped and had much in common.

(U) Serious United States concern with rocketry had been sparked by the availability of captured German V2 rockets. In essence, after three decades of neglect, the US once again began to restudy the works of Goddard (US), reexamine the results of Tsiliokowsky (USSR), and learn the practical techniques of Von Braun (Germany). To obtain hands-on experience, the V2s were to be fired from the US Army rocket range at White Sands, New Mexico. Also, rather than fire them with ballast, the warheads were to contain instruments which could measure properties of the upper atmosphere.

(U) In 1948 the principal DoD groups concerned with rocket-borne exploration of the upper atmosphere were the Ballistic Missile Laboratory (BRL), the Naval Research Laboratory (NRL), and the Air Force Cambridge Research Center. Each service prepared and defended its own program and budget. Although they acted independently, they exchanged information through a V2 Rocket Research

Committee whose membership was limited and confined to the active groups and their respective contractors. Initially the launch vehicles were the V2s. Later rockets manufactured in the US (Wac Corporal, Honest John, Viking, Aerobee) were introduced.

(U) It was unfortunate, but true, that a considerable amount of tension existed between NRL and AFCRC. Marcus O'Day, Chief of the Upper Air Laboratory at AFCRC, and Homer Newell, head of the Rocket Sonde Section of NRL just were not simpatico. Both were knowledgeable, but they had completely distinct characters. O'Day was easy-going and casual and Newell more formal and rigid. Whether the friction arose from personality differences or organizational loyalties may never be known, but there was no doubt about the internecine warfare that existed between AFCRC and NRL. While I never knew how it originated, there was no doubt about its existence [1].

(U) The first few years witnessed both successes and failures. Many of the latter could be attributed to problems in the propulsion system (leading to unpredictable rocket behavior), unreliable telemetry, or experimental deficiencies. Some of these problems persisted into the 1960s.

3. THE INTERNATIONAL GEOPHYSICAL YEAR

(U) The International Geophysical Year (IGY) was an 18-month period (July 1957 to December 1958) during which most nations joined together for a detailed investigation of the planet as a whole. They recognized that national boundaries had no influence upon weather, ionospheric storminess, earthquake formation, tidal changes, etc., and that to better understand and predict these phenomena, a more thorough understanding of planetary physics was necessary [2].

(U) The International Council of Scientific Unions (an arm of the United Nations) endorsed Berkner's suggestion and invited all nations to participate. In response to this call, the US National Academy of Sciences established the US National Committee (USNC) for the IGY in 1953. I was appointed to the Committee and later was designated as Secretary and Secretary of its Executive Committee. I was also active on the scientific panels and lesser committees; e.g., the Ionospheric, Geomagnetic, and Rocketry Panels; chairman of the first two Antarctic Committees; and vice chairman of the Arctic Committee. These activities, of course, were in addition to my responsibilities at AFCRC.

(U) The USNC first sought to develop an internal US program in geophysics, and then to coordinate the program internationally to ensure that (a) international duplications were eliminated, and (b) gaps in coverage at national boundaries did not occur. All major nations joined the endeavor. The final program was truly global in nature. It incorporated studies on the continents and on the seas, in the Arctic and Antarctic, and it included rocket- and satellite-borne probings of the upper atmosphere.

4. INTERNATIONAL COOPERATION

(U) Although the USNC considered all aspects of geophysics, only those concerned with the upper atmosphere will be recounted here. The USNC Rocketry Panel contained many individuals on the old V2 Rocket Research Committee, now named the Upper Atmosphere Rocket Research Panel (UARRP). It also included active researchers not on UARRP, and thus was more broadly based. During early meetings the Panel confined itself primarily to experiments which essentially continued or improved already ongoing efforts. S. Fred Singer of the University of Maryland and James A. Van Allen of the University of Iowa expanded their "rockoon" (balloon-launched rockets) program for studying incoming extraterrestrial particles. Singer in 1962 published his MOUSE (Minimum Orbiting Unmanned Satellite, Earth). He brought this proposal to the attention of the Panel on Rocketry, but it was not endorsed [3].

(U) The first convocation of the Special Committee for the IGY, known as CSAGI from the initials of its French name, met in Rome, Italy, in 1954. It presented an opportunity to begin integrating the various national programs. The Secretary General of CSAGI, Marcel Nicolet of Belgium [4], asked me during the sessions, "When will MOUSE be ready?" I had

no suitable answer; the Technical Panel on Rocketry had not accepted it.

5. FALTERING FOOTSTEPS INTO SPACE

(U) Berkner forced a decision on US plans for launching satellites. He had brought his wife and daughter to the meetings and had a suite in the Hotel Majestic. One day he asked a number of us (including Joseph Kaplan, Hugh Odishaw, Harry Wexler, Wallace Joyce, Allan Shapley, Homer Newell, S. Fred Singer, John Adkins, Athelstan Spilhaus, and myself) to visit him that evening. After pleasantries he broached his concern: rumors were circulating that the Soviet Union was about to propose that CSAGI endorse the launching of earth satellites as an integral portion of the IGY program. Satellite-borne instrumentation would allow direct investigations of the upper atmosphere. Berkner wanted us to propose a US position. It was obvious that he was in favor.

(U) The discussions lasted well into the evening. It was quickly apparent that practically everyone present felt that the US should either independently propose, or join in proposing, the launch of earth satellites during the IGY. We all understood that such a stand committed the US to implementing scientific satellite experiments before the end of 1958 or shortly thereafter. However, it was the considered judgment of most that such a schedule was not unrealistic. Several of us had a working knowledge of the difficulties and problems affecting launches: thrust availability, costs, experimental possibilities, etc. Berkner himself was very familiar with the total US effort, including the progress in propulsion systems, and from a much higher level in Government than any of us.

(U) The lone serious holdout was Newell: there were no readily available boosters; solar cell outputs were too low; energy requirements could not be met; experiments could not be prepared in time; proven experiments were not at hand; the batteries would boil; etc. He stated that the US could not fabricate and launch an acceptable experiment in time, that the difficulties were too great, and that there were also doubts about Soviet capabilities. The rest of us felt comfortable about a positive stand for the US. The problem was not one of developing new technology or introducing untested theory; it was that of a modest expansion of existing technology.

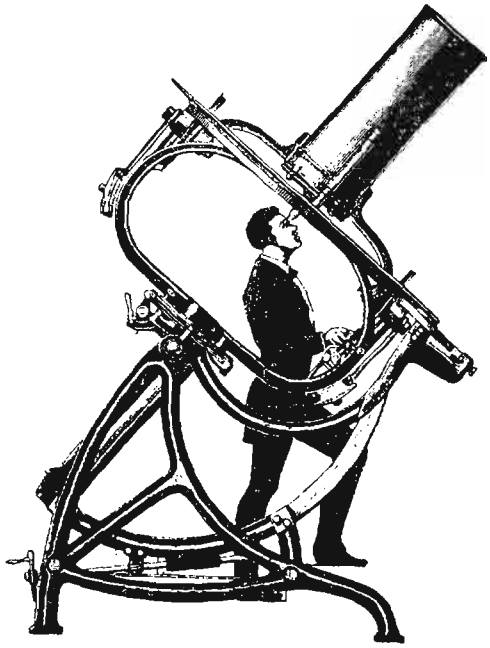
(U) Finally Berkner asked for a vote. It was unanimous in favor: the US would propose incorporation of a satellite program within the IGY framework. With this decision in hand, Berkner, on behalf of the US, and Pushkov, on behalf of the USSR, jointly proposed that an earth satellite program be included in the IGY. The plenary session of CSAGI adopted this recommendation.

(U) Knowingly or unknowingly, man was about to leave the confines of his planet. Wittingly or unwittingly, consciously or unconsciously, a race had started. Most of us were too closely involved with details to anticipate the ramifications of our decision.

6. THE LURCHINGS OF GOVERNMENT

(U) After we returned to the US, the machinery of Government slowly began to clank. Berkner, who was on a first-name basis with the President, briefed Eisenhower. On July 29, 1955 the president publicly announced US participation. One day later, in a TV broadcast from the White House, Presidential Press Secretary James Haggerty, Spilhaus, and Shapley appeared on national TV to inform the public, explain the scientific implications, and clarify details. The Government now had formally committed itself to support the decision of our rump meeting.

(U) Deliberations within the Executive Committee of the USNC took an unexpected turn. Kaplan, the Chairman, termed the proposed satellite "the LPR" (long-playing rocket), and stated that the US effort would be wholly civilian in concept and fulfillment. Let the USSR use its military capabilities to launch a satellite for the civilian-scientific IGY; the US would not [5].



(U) I did not agree and privately pointed out contrary examples, most notably the US Antarctic program, supported solely by the US Navy, which provided all logistic and housekeeping support, transported the scientists and their equipment to the experimental site, and provided all facilities. Analogously, in the satellite case, DoD would logistically place the instrumentation in orbit, but the experiments themselves were to be scientific-civilian. If the USNC had not requested its own ships in support of the Antarctic endeavors or its own planes for the Arctic investigations, why should it request its own boosters for the space studies?

(U) Kaplan prevailed. The USNC found a surplus unused Vanguard rocket; it was refurbished to serve as a booster for the IGY satellite. The Technical Panel on Rocketry and Satellites considered its experimental possibilities. About this time rumors reached several of us on the USNC to the effect that the Army planned to launch a rocket which would "accidentally" attain earth orbit. I was later told, without substantiation, that Kaplan had objected and that, as a result, the Army was told to cease efforts toward this end.

7. REALITY AND ILLUSION

(U) As refurbishment of the Vanguard progressed, a meeting was held at the US National Academy of Sciences to discuss the satellite programs planned for the IGY. My invitation, in a telegram dated September 30, 1957, noted that the gathering constituted the international working party on rockets and satellites. Attendees consisted of delegates from the US and USSR. The press was represented. The Soviet delegation, led by Gen. Anatoly A. Blagonravov, invited us to a party at their Embassy on October 4, 1957. The meeting included papers on scientific and technical topics, which then were followed by discussion periods. Both nations outlined their scientific programs.

(U) In typical national fashion, the US provided much more information than it received. All Panel members were already familiar with many aspects of the US program, and we listened avidly to the Soviet presentations. In my view, two strong areas of disagreement crystallized during the deliberations. First, the US desired one common downlink telemetry frequency from the satellite at about 120 MHz. The US had chosen this frequency by happenstance; surplus military equipment suitable for downlink had been found and it operated at this frequency. The Soviets would not agree. Pushkov, who spoke English better than most of his colleagues, answered many of the questions. He was not convinced that 120 MHz was the best or only frequency to be utilized. Also high frequencies (HF) could be used and could provide some indication of refraction produced by the ionosphere. He patiently maintained his position. Discussions on this point were abandoned when it became apparent that the Soviets would not budge.

(U) A second point of discord occurred during the morning of October 4. It stemmed from US pressure for the Soviets to provide an official launch date for their IGY satellite. The Soviets were pushed rather relentlessly and intently--almost to the point of embarrassment. The replies were polite and courteous. Finally Pushkov, answering forcefully, stated that, "at the present state of the art, to predict the launch of a rocket is difficult and it becomes even more difficult to predict the launch of a satellite." There were too many uncertainties, too many things that could go wrong. Why state a date in advance when such doubt exists? He would prefer to provide a date after a successful launch.

(U) Richard Porter was the Chief US delegate at the meeting. I had wanted to discuss a number of topics with him and had decided to do so during the lunch break. However, the press reached him first and reporters crowded around him. I then sat behind and to his right and waited while the reporters held sway. It was interesting to hear his comments. While most questions were about the Soviets' prowess, progress, and competence, many also touched upon the reports presented during the Conference.

(U) Porter relished the attention, expressing himself freely and at some length while the pencils scribbled. The Soviets, he claimed, were "'way behind the US"; there was no other possible explanation for their reticence in providing a launch date for their satellite. Their program must have run into extreme difficulties. They did not have the competence-- "Just listen to their answers!" (I shook my head in wonderment. How could two

knowledgeable individuals listen to the same technical discussions and arrive at such divergent views? If I had been engaged in research at MIT and a researcher in the same field from Harvard approached me, I would become vague if not mute. Furthermore, most of my colleagues would behave similarly: "The stalking cat does not purr.") On one occasion I was tempted to interrupt but thought otherwise and remained silent. Porter orated on.

(U) The sessions resumed that afternoon. Although I had an invitation for the party at the Soviet Embassy that evening, I had planned to miss it; it was a religious holiday and I would proceed home to Boston instead. Practically every other delegate attended. At the height of the festivities, Berkner received a telephone call: the "beep beep" of the 40-MHz signal radiated by the earth's first satellite, Sputnik 1, had been picked up. Berkner, I have been told, returned to the room, stood on a chair, clapped his hands, and publicly commended the USSR on its accomplishment. (The long-term US response, unfortunately, was weak: a burst of effort in the physical sciences that persisted for about one decade.)

(U) The USNC pursued its "open" space effort. The Vanguard was publicized and readied. The experiment was encapsulated and emplaced in the "bird." Complete television coverage took place during the day of launch to show the world that the US utilized only civilian-scientific talent in its space program. Unfortunately, Vanguard did not cooperate. Immediately after ignition it fell over and burned--with complete TV coverage. The US had learned a lesson. The Army was called in and asked to make the next launch attempt. Van Allen prepared new instrumentation for observing cosmic radiation (essentially a particle counter to measure the intensity of particles bombarding the earth). The satellite, named the Explorer, discovered the radiation belts that now bear Van Allen's name. The US had not been first in space, but its scientific efforts to date had been best--we had discovered a hitherto unknown major feature of the planet.

8. ONE NATIONAL EFFORT

(U) In 1956 I left AFCRC and joined the National Security Agency (NSA). However, I still participated in USNC activities. During this period NRL submitted a proposal to the Rocketry and Satellite Panel requesting post-IGY funding of specific experiments. The letter contained a "save us" plea--the Navy might not fund the program. I was rather dissatisfied with the contents for several reasons and finally wrote to the Chairman of the Panel. My letter, on USNC stationery, was typed in the old REMP-43 offices at the Naval Security Station. It treated three points. The first two aspects included (a) specific comments relative to the proposed experimentation and (b) questions as to whether the USNC should be the vehicle for post-IGY funding. It seemed to me that funding of this type was outside the intent and charter of the USNC and that the precedent that would be established would be unwise. The third topic opened the entire subject of one national space program for the US.

(U) The third aspect was probably the most important. What was the future role of US rocket and satellite explorations? I noted the long history of vicious backbiting in this area among the Services and suggested that this field be removed from DoD and placed in an independent Agency that pursued national objectives. Only an approach of this type would benefit the US as a whole. The present assignments within DoD did not and could not provide the healthy environment needed for progress. For the US to become competitive in the Space Age, a national focus was required.

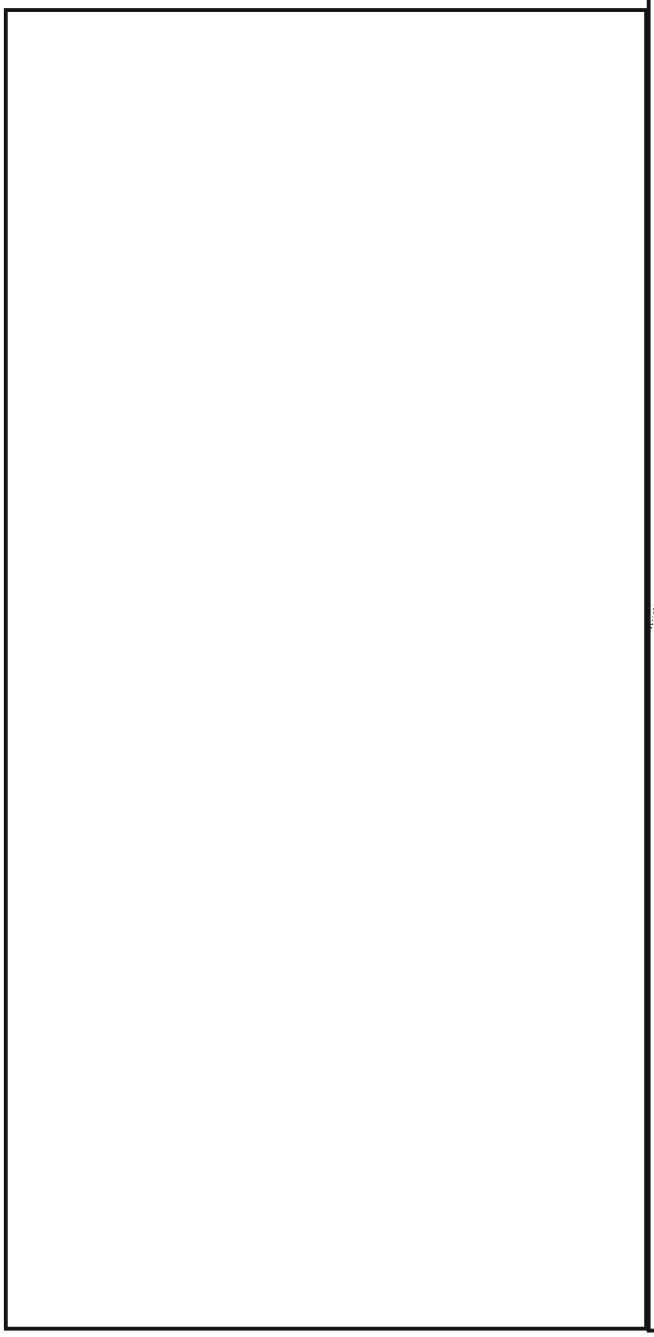
(U) I recommended that the future national program (to be defined) be housed within the National Administration for Civil Aeronautics (NACA). I had had many dealings with NACA previously and had worked with their personnel in the old NACA offices at DuPont Circle, Washington. (At that time I had been engaged in atmospheric thermodynamics.) I had been very impressed with the competence of the personnel and with their appreciation of research.

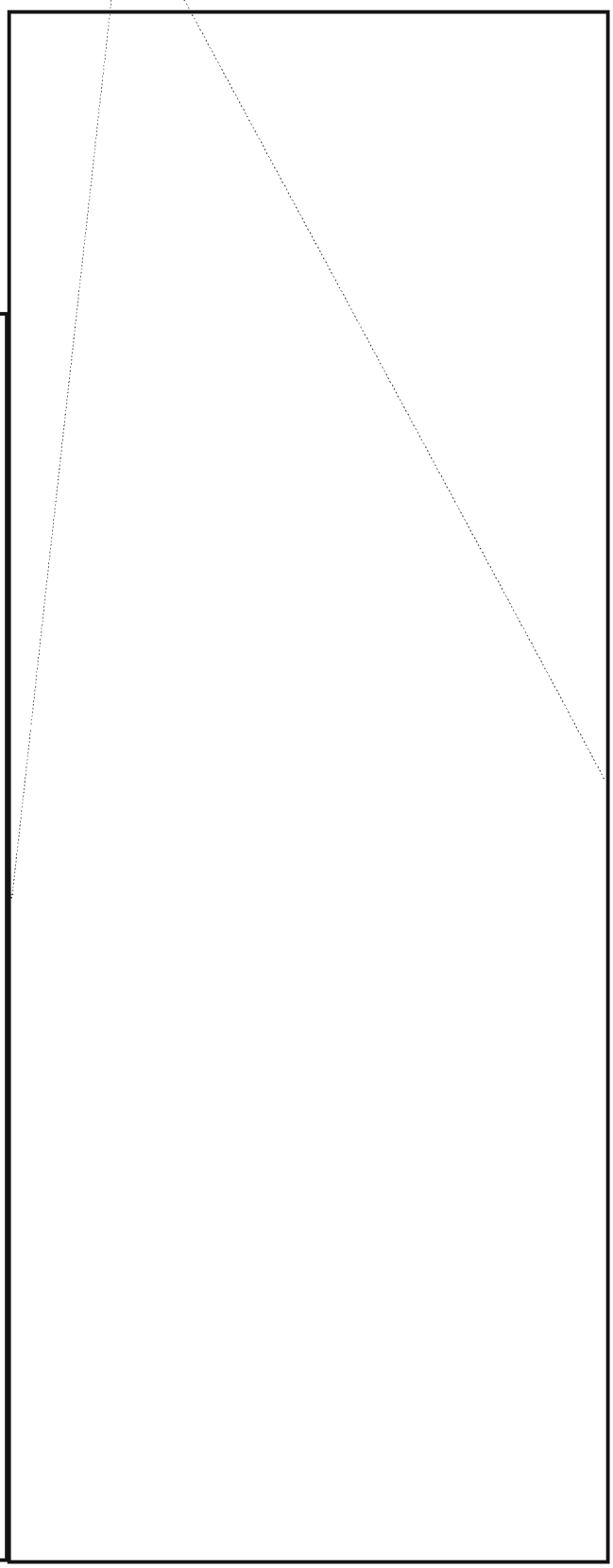
(U) Slowly my attention turned elsewhere--towards NSA. However, the results stemming from my letter were dramatic. A series of meetings occurred at various levels of government. Within two years the National Aeronautics and Space Administration (NASA) was formed. It absorbed the old NACA. NASA embraced a strong program that brought credit to the US.

HCCUA

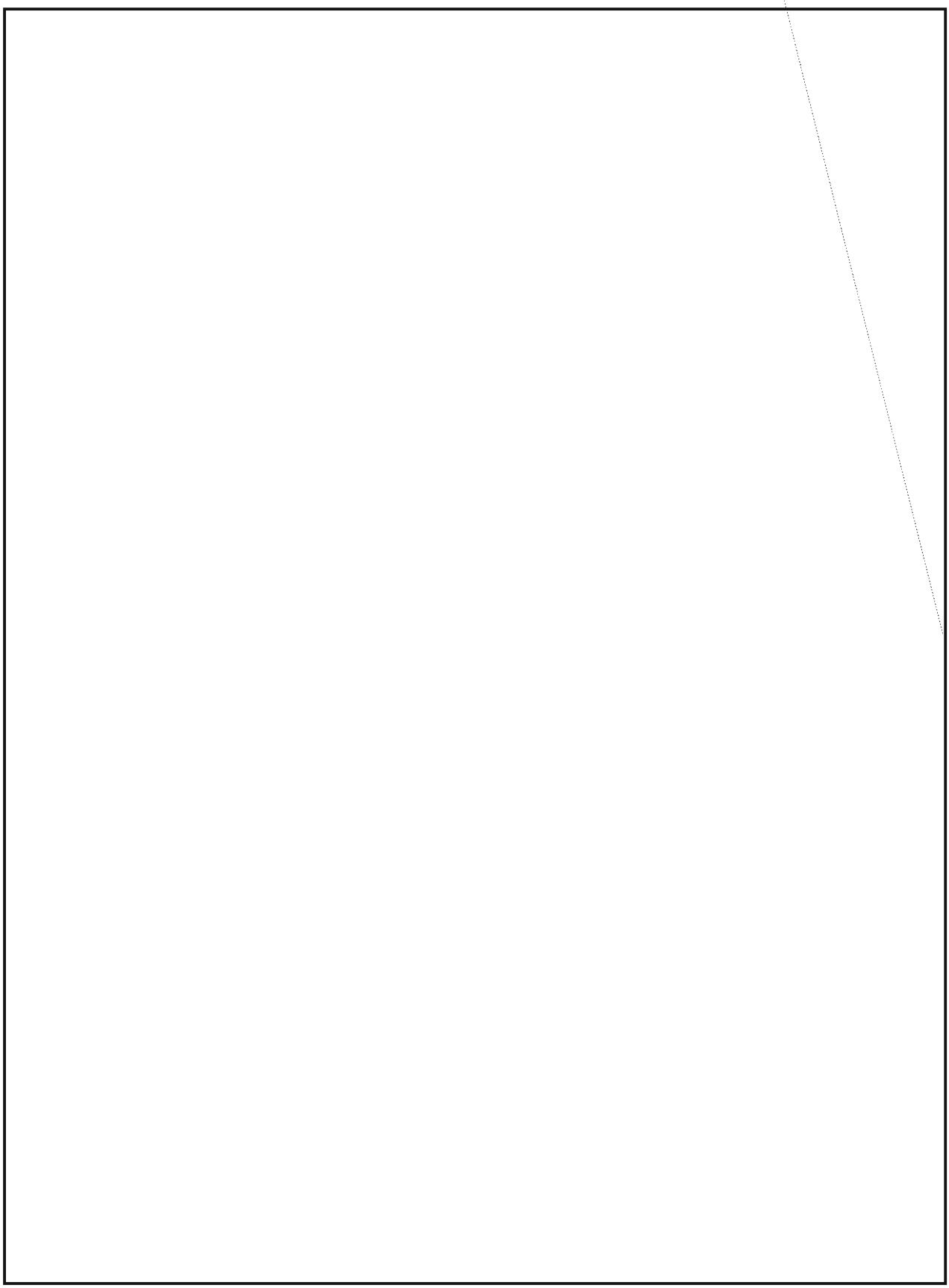
9. SIGINT ENTERS SPACE

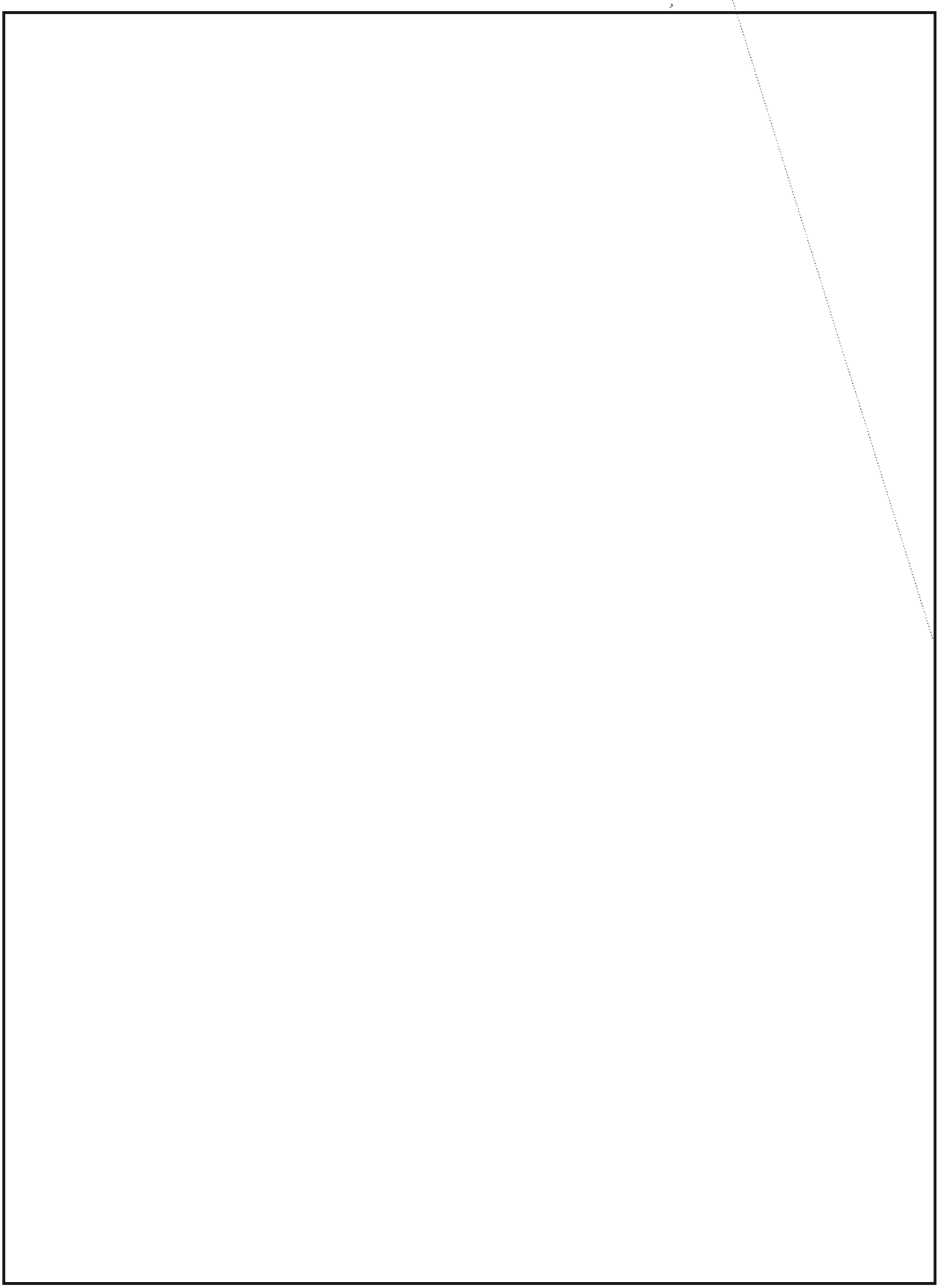
(U) For my part, I became more and more involved with problems affecting NSA and less and less with those involving the IGY. I had joined NSA in 1956 and Kaplan, after learning of this association, felt that I should leave the Committee. I subsequently resigned from both the full USNC and its Executive Committee in the summer of 1957. My attention turned towards applied research in SIGINT [6].





EO 1.4.(c)
P.L. 86-36





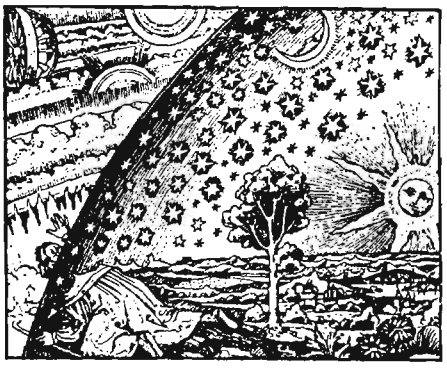
(U) The greatest problem was the small lunar gravity (one-sixth that of the earth) which would not allow retention of an earth-like atmosphere for any length of time. There were other problems: distilling the needed gases from lunar rocks, the thermodynamic properties of the atmosphere, and the warming of the dark side of the moon once an atmosphere was established.

(U) I cheerfully went ahead and assumed an atmosphere of 20% oxygen and 80% argon with a surface pressure about equal to that of Denver. (On the earth the composition at the surface it 21% oxygen, 78% nitrogen, and 1% argon. Argon was chosen as a potential filler gas for the moon because its molecular weight is much greater than that of nitrogen.) The thermodynamic properties of this atmosphere were curious, but the crucial unsurmountable obstacle was the loss of gas; the low gravity allowed the oxygen to "boil off" at an almost irreplaceable rate. Obviously, the answer is to utilize domed cities.

13. POSTLOGUE

(U) This paper has recounted many of the events that led NSA to its present course of action. It illustrates the thinking and problems at the time and the chain of events that led inexorably to our present concepts.

(U) From the vantage point of today, it seems clear that the research problems in physics facing the Agency lie in analysis and not in collection. Nevertheless, I fear that an adequate and viable program is lacking and that the Agency may be selling its future birthright for a mess of present pottage. We need new, stimulating ideas from competent researchers who know our problems. Where are the vibrant leaders? Spending money is not tantamount to ensuring progress.



FOOTNOTES

1. O'Day was particularly upset over an incident involving funding for a new Aerobee vehicle. His proposal was at first approved by the Pentagon. NRL, however, greatly deprecated the effort (in favor of the NRL Viking rocket) and it was canceled. O'Day was correct: the Viking was an expensive white elephant that delayed the total DoD program for at least three years. He firmly believed that the NRL objective was to "seize control of the entire US space and rocketry program and shut out USAF." His numerous stories in this vein indicated that an unhealthy rivalry sapped the total US effort.

   NASA's text Beyond the Atmosphere: The Early History of Space Science (1980) contains a number of allusions to this bitter friction but does not discuss them in detail. It omits many relevant contributions by other groups engaged in the early US space effort; in one instance it comments pejoratively on AFCRC.

2. The IGY was conceived by Lloyd V. Berkner, president of Associated Universities, Inc., Brookhaven, NY. Because of his accomplishments in fostering the IGY, I later suggested to Detlev Bronk, president of the National Academy of Sciences, that Berkner be nominated for a Nobel Peace Prize.

   The IGY was a continuation of a series of Polar Years. The first Polar Year, held in 1872, was conceived by Karl Weyprecht, a lieutenant in the Austro-Hungarian Navy. It was followed 50 years later by the Second Polar Year. The objectives of both were extensive examinations of weather, auroras, geomagnetism, ice conditions, etc., in the Arctic and Antarctic. Berkner's proposed IGY shortened the period between Polar Years to 25 years and expanded their scope to include middle and low latitudes. In a survey of the Polar Years and the IGY, I questioned (in 1956) the need for future geophysical years since there currently existed a global network of active geophysical stations in constant operation.

3. Singer privately thought that NRL opposition caused the demise of MOUSE. NASA's publication Beyond the Atmosphere states that security classification muzzled discussion of this topic. If so, we at AFCRC had not been informed.

4. I had first met Nicolet when I invited him to a Conference on Ionospheric Physics that I sponsored at the Pennsylvania

State College. Arthur Waynick of the Electrical Engineering Department and I then induced him to accept a research and teaching position at the College and conduct research on the physics and photochemistry of the ionosphere.

5. In Beyond the Atmosphere NASA contrasted the activities of the two nations by considering the space effort of the US as primarily open and scientific, and that of the USSR as primarily military. However, it is not possible to characterize them so neatly. Both nations designed realistic programs to accommodate their respective national interests in both defense and science. Furthermore, the long-term goals of one country were not materially different from those of the other. Thus, their objectives a priori included a mixture of military applications, national prestige items (lunar and planetary probes), and space research. Both nation realized that research represents vital national insurance for the future.

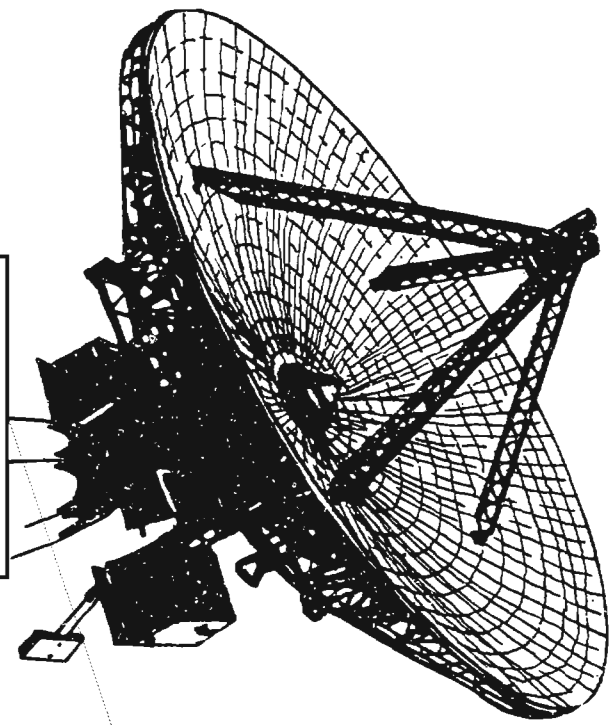
6. Within NSA I worked for Howard Campaigne, Chief of REMP, and John Crone, Chief of REMP-43. Initially I was involved with planning the program for the REMP College Park facility. One goal was laboratory studies which simulated ionospheric (low-pressure) conditions. Additionally, I worked very closely with Arthur Hausmann, Chief of RADE, and Robert O. Alde, RADE-3. I was extremely lucky on all counts. Better and more instructive teachers could not have been found.

7. [redacted]

8. About this time or slightly earlier, NRL had proposed construction of a massive steerable dish for moonbounce purposes. It would be capable of being steered to practically any area in the heavens and [redacted] I was wary of the project and recommended that NSA neither endorse it nor participate in it. It was subsequently plagued by cost overruns aggravated by further cost overruns, followed by discoveries of faulty design. Costs rose from a modest amount to over $600 million. Secretary of Defense Robert MacNamara finally canceled it. At a very early briefing, NSA was told that the dish was designed for scientific radioastronomical studies and that intercept was a by-product. [redacted]

9. The dish at AIO has been updated considerably [redacted] Its surface now is spherical over its 300-meter radius to within 2 cm. It still remains one of the best radio telescopes the US ever constructed and, by any reasonable measure, probably the cheapest in relation to the research potential that it provides.

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

DOCID: 4009929

~~FOR OFFICIAL USE ONLY~~

FROM *CRYPTOLOG*, VOL I, No.1

NSA-Crostic No. 57

Solvers are reminded that when the answer to a definition contains more than one word, a remark to this effect is included in the definition.

		1 E	2 X	3 J	4 G	5 M	6 C	7 F		8 X	9 H	10 F	11 J		12 X		13 M	14 J	15 A
16 D	17 X	18 C	19 G	20 E	21 R	22 F		23 J	24 X	25 F	26 E	27 C	28 G		29 J	30 L		31 J	32 F
33 B		34 K	35 V	36 X	37 O	38 C	39 J	40 H	41 M	42 G	43 E	44 X	45 V		46 H	47 B	48 X	49 V	50 L
51 J	52 D	53 E	54 M		55 P	56 J	57 M		58 J	59 A	60 I	61 M	62 X	63 D	64 L	65 H	66 G	67 O	68 X
69 U		70 X	71 D	72 V	73 K	74 M	75 P	76 J		77 V	78 M	79 J		80 P	81 J	82 X	83 G		84 J
85 O	86 P	87 G		88 J	89 X	90 F	91 O	92 T	93 S	94 V		95 S	96 X	97 N	98 Q		99 G	100 K	101 B
102 I	103 X	104 J	105 M		106 J	107 X		108 X	109 O		110 J	111 B	112 S	113 X	114 J		115 U	116 V	117 L
118 J	119 A	120 E		121 X	122 K	123 S	124 M	125 J	126 U		127 C	128 N		129 H	130 E	131 S	132 W	133 X	134 J
135 M		136 X	137 D	138 A		139 X	140 F	141 W		142 J	143 N	144 K	145 G		146 X	147 W	148 N	149 R	150 J
151 F		152 L	153 C	154 X	155 W		156 E	157 D	158 R	159 T	160 J	161 F		162 W	163 R	164 B	165 X		166 J
167 Q	168 X		169 J	170 J	171 F	172 X	173 H		174 X	175 H		176 T	177 F	178 X		179 X	180 U	181 M	182 J
183 F	184 W	185 S		186 G	187 S	188 F	189 X		190 H	191 T	192 X	193 G	194 V	195 S	196 J	197 Q	198 M	199 U	200 F
	201 X	202 H	203 V	204 J	205 M		206 V	207 F		208 S	209 E	210 M	211 X	212 A	213 J	214 F	215 V	dhw	

A. English county

$\overline{138}\ \overline{119}\ \overline{212}\ \overline{59}\ \overline{15}$

B. Anesthetic; upper regions of space

$\overline{164}\ \overline{101}\ \overline{111}\ \overline{33}\ \overline{47}$

C. Singer Snow; flycatcher

$\overline{6}\ \overline{38}\ \overline{153}\ \overline{18}\ \overline{127}\ \overline{27}$

D. Season in the Christian religious calendar; arrival

$\overline{16}\ \overline{63}\ \overline{157}\ \overline{71}\ \overline{137}\ \overline{52}$

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009929

E. Awe, profound respect

53 1 26 20 120 156 43 209 130

F. Idea of the *moment* (4 wds)

214 140 10 188 200 32 22 207 171 25 7 177 183

151 90 161

G. Type of high-interest investment fund (2 wds)

193 42 99 4 28 19 66 83 145 87 186

H. Without mistakes (comp.)

190 9 129 46 65 175 40 202 173

I. Ultimate, as of a degree

60 110 102

J. "When ____": 1940 popular song commemorating an event which occurs annually on March 19th (6 wds)

31 170 134 23 142 14 160 125 56 169 51 182 84

11 79 118 39 3 204 106 81 58 196 88 213

76 166 114 150 104 29

K. "Quinquiremes of Nineveh from distant ___" (*Cargoes*, Masefield)

100 34 122 73 144

L. "Cherchez la _____."

30 64 117 152 50

M. Movie (1947), TV series (1969—70) about a widow whose house is haunted by the ghost of its former owner (4 wds foll. *The*)

105 78 74 61 210 54 181 135 41 57 205 13 124 198 5

N. On top of, above; finished

143 97 128 148

O. Waiting room; pressure group

37 109 85 67 91

P. Remove, as one's hat

75 86 80 55

Q. Icelandic letter

98 197 167

R. Granular snow

21 158 163 149

S. By contrast, to the contrary (2 wds foll. "on the")

123 185 187 112 93 95 208 195 131

T. Season in the Christian religious calendar; afforded

191 92 159 176

U. English poet, 1572—1631

126 180 199 115 69

V. Extinct marine reptile with a fish-like body, having fins and limbs

194 45 49 77 35 215 206 94 203 116 72

W. Continent

141 132 184 162 147 155

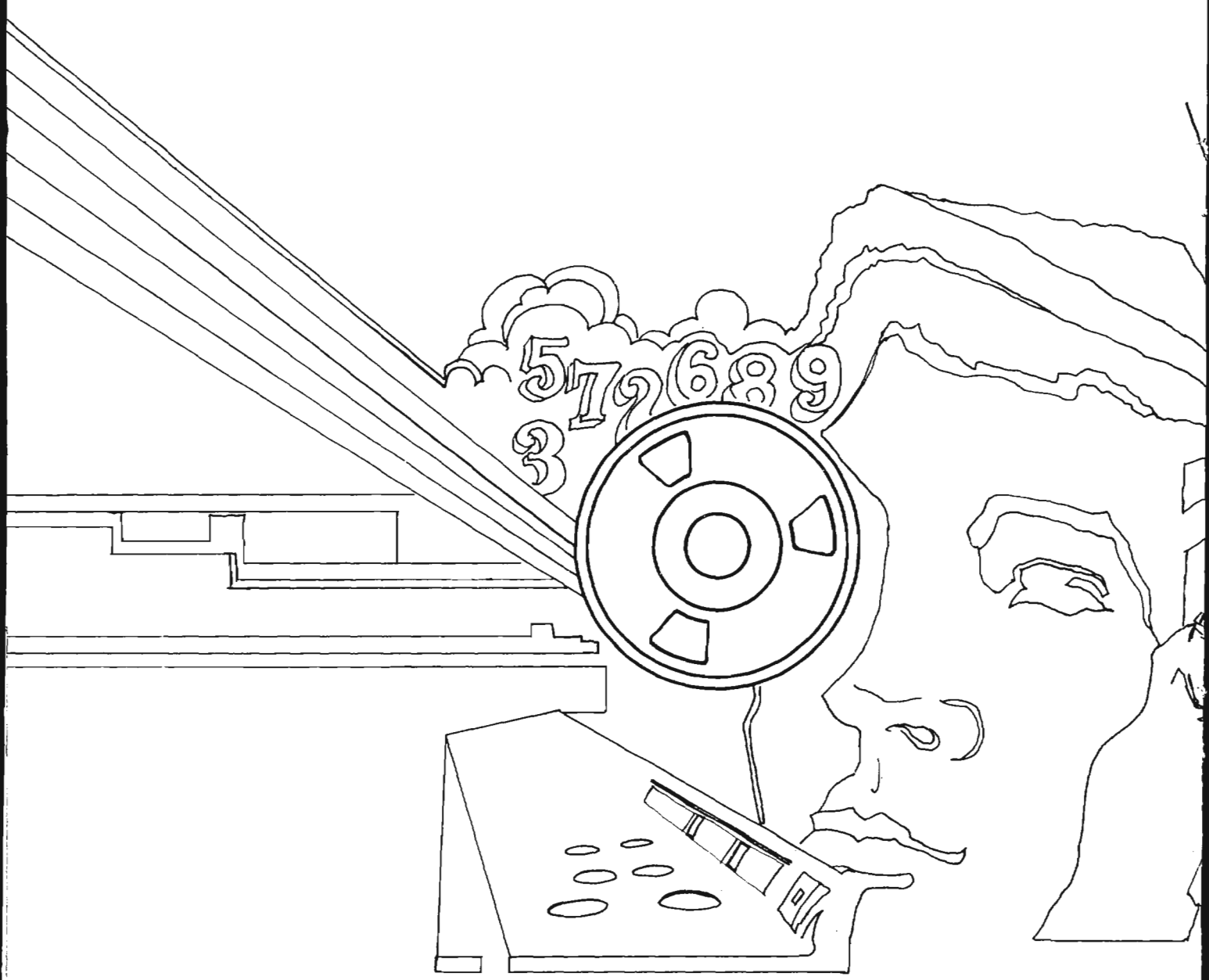
X. 1964 popular song

189 24 70 168 154 179 12 68 192 8 165 96 17

211 89 62 146 139 44 48 178 2 201 103 136

172 113 108 174 133 36 107 82 121

P1-Sep 84-58150


5 7 2 6 8 9
3

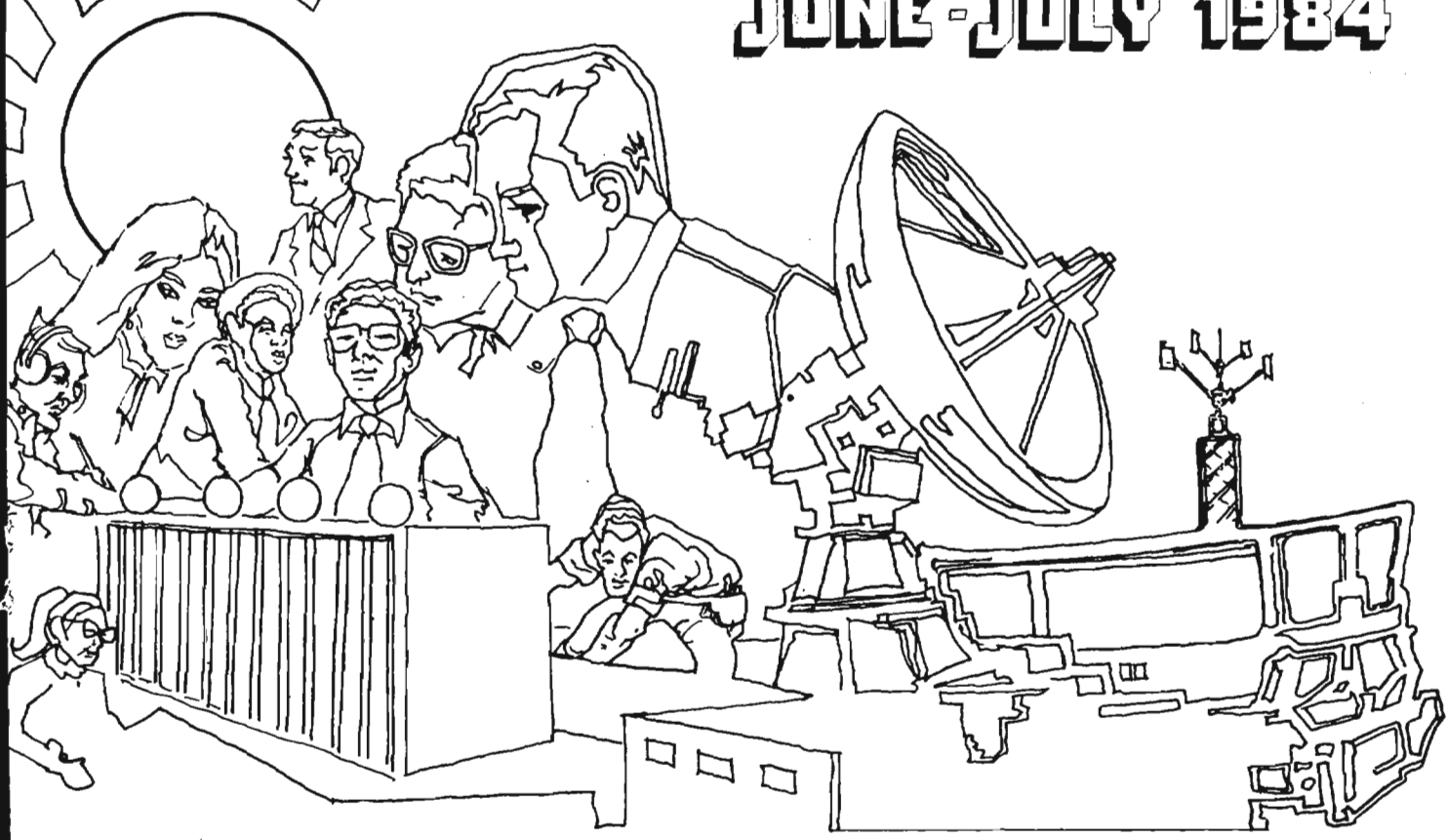
DOCID: 4033691

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JUNE-JULY 1984



TRAFFIC ANALYSIS: A CURRENT PERSPECTIVE (U).....[redacted].....1
ESPIONAGE AS A TOOL
OF TECHNOLOGY TRANSFER (U).....[redacted].....8
INTELLIGENCE ANALYSIS
IN THE COMPUTER AGE (U).....Jack Gurin.....12
NAMING SOVIET CITIES (U).....16
THE BOOKBREAKER (U).....Stuart Buck.....17
WORD PROCESSING PLAIN AND SIMPLE (U).....[redacted].....18
UNLESS TEXTS HANG TOGETHER, LINGUISTS
WILL ALL HANG SEPARATELY (U).....[redacted].....25
NSA-CROSTIC NO. 56 (U).....[redacted].....28

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating~~ ~~ration Required~~

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54776

DOCID: 4033691

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XI, No. 6-7 JUNE-JULY 1984

PUBLISHER [redacted]

BOARD OF EDITORS

Editor..... [redacted] (963-3045s)
Asst. Editor... [redacted] (963-1103s)
Production..... [redacted] (963-3369s)

Collection..... [redacted] (963-3961s)
Computer Security
..... [redacted] (859-6044)
Cryptolinguistics [redacted] (963-1103s)
Data Systems..... [redacted] (963-4953s)
Information Science
..... [redacted] (963-5711s)
Mathematics..... [redacted] (968-8518s)
Puzzles.....David H. Williams (963-1103s)
Special Research.....Vera R. Filby (968-7119s)
Traffic Analysis..Robert J. Hanyok (968-8418s)

For subscriptions
send name and organization
to: [redacted] P14

P.L. 86-36

To submit articles or letters
by mail, to: P1, Cryptolog

via PLATFORM mail, send to:
cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no 'O' in 'log')

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

This month we bid farewell to our assistant editor, [redacted] who is retiring (the verb, not the adjective).

If you have ever known him, you will find it hard to imagine him as a retiree. Harry doesn't seem to have a "second gear" or any way to go at half speed. There is a rumor that when Harry talks REALLY fast, only dolphins can understand him.

We will miss him. He has been a stalwart force in keeping this magazine going.

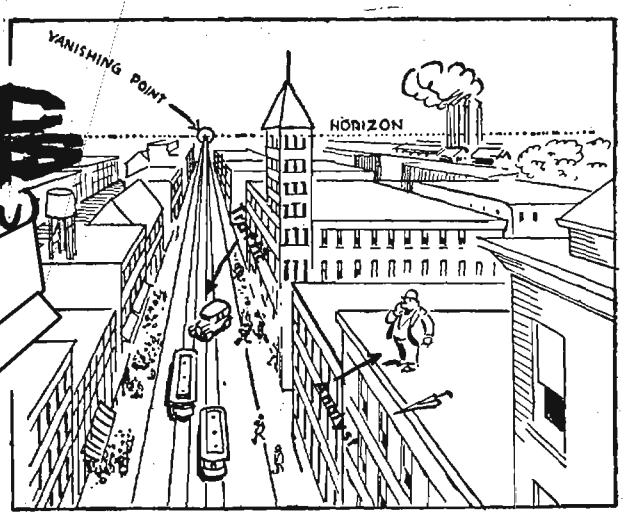
Thanks, Harry, for your inexhaustible supply of energy, enthusiasm, and encyclopedic knowledge. Shalom.

DOCID: 4033691

P.L. 86-36

TRAFFIC ANALYSIS: A CURRENT PERSPECTIVE (U)

by CW2 USAFS



(c) Traffic analysis today is beset by a variety of problems affecting the analyst, not the least of which is a lack of understanding concerning the separate functions which comprise traffic analysis. Contrary to popular definition, the traffic analysis (TA) field of today encompasses much more than the mere analysis of communications externals. Traffic analysis consists of six separate functions:

[] Collection Management;

[] Collection Support;

[] Processing;

[] Analysis;

[] Reporting; and

[] Evaluation.

EO 1.4.(c)
P.L. 86-36

which are intended to be mutually supportive of each other. However, because both managers and analysts lack understanding of the interrelationship that exists between and among these functions, they all too often are performed at cross purposes, with one function inadvertently affecting the success (or failure) in a follow-on activity. In these days of meager collection and analytic resources, it is imperative that an understanding of the relationship bonding the six functions of traffic analysis be fostered at all levels to ensure the complete and proper use of these resources.

~~(C)~~ To function effectively in the traffic analysis world of today, the traffic analyst must have a rudimentary knowledge of several areas in addition to communications externals. Among these areas are

Collection Management: including the Collection Objective Performance Evaluation Systems (COPES) and its follow-on Collection Evaluation System (CES) statistical reporting;

Collection Support: including knowledge of working aids available to assist in collection and identification duties, as well as of target characteristics that can support both current and future collection operations;

Processing: including Automated Data Processing (ADP) routines available to assist in manipulating the intercepted data for subsequent analysis;

Analysis: including sufficient knowledge of the various traffic analysis techniques and target characteristics that develop information to satisfy consumer requirements;

Reporting: including the criteria and appropriate reporting vehicles for providing information to satisfy consumer requirements;

Evaluation: including the techniques available to constantly monitor and compare tasked and acquired collection so as to redirect these resources to areas of the target's communications that are susceptible to exploitation; and

Perspective: including a thorough knowledge of the target's order-of-battle (OB) structure that underlies the target's communications, as well as a thorough understanding of the targets past history from which to view changes in the target's communication habits.

A lack of knowledge in any one of these areas can ensure failure in attaining the ultimate goal of consumer satisfaction. Additionally, an incorrect managerial emphasis on any one function over another will also ensure failure in attaining this ultimate goal.

Collection Management

(U) The first function to be encountered by the traffic analyst is the Collection Management function. It is at this point that the consumer's requirement is translated into specific collection tasking to acquire the needed information.

Collection Support

(U) Once the tasking is accurately developed and transmitted to the field site, the next function, Collection Support, determines the success or failure of a field element in satisfying its tasked requirements.

(U) At the local level, field site managers usually are faced with a decision of where to use their most talented personnel: an effective Collection Support element or an effective Analysis & Reporting effort. Unfortunately, all too often the choice is for the A&R effort because of the high visibility of analytic breakthroughs and consistent product reporting.

(U) This decision on the part of the field manager leaves the Collection Support effort

with poorly trained analysts, generally those with the least experience in TA duties. These individuals are then placed in the fast-paced environment of the collection floor, an environment that breeds confusion and is the least likely place to learn the functions of traffic analysis.

(U) In addition to the assignment of poorly trained personnel at the local level, at the national headquarters level technical support material is seldom provided in a manner that facilitates its use in the field. Most often this material is seldom provided in a bulk manner, which dictates tedious manipulation in the field to extract desired information. Yet this same manipulation is often performed within the national headquarters on a daily basis through various computer routines but is not made available to field sites. Thus, while a steady and voluminous stream of technical support material is provided to the field element, it is seldom provided in a manner that facilitates its use in the field, and it is often too unwieldy to be used on the collection floor, with all its hectic activity.

Of these, the misidentification rate should be of the greatest concern since it dramatically impacts on the Processing, Analysis, Reporting, and Evaluation functions that follow the Collection Support function. A poor case (notation) identification rate in the Collection Support function means that all case identifications received for processing must be verified to ensure that the correct notation is applied, a time-consuming process for an individual already strapped for time in performing his or her other processing duties. Failure to verify the correct identification on all cases can have disastrous effects:

[] on processing, necessitating complete revisions of case history records;

[] on analysis, which attributes incorrect technical operating characteristics to the wrong case;

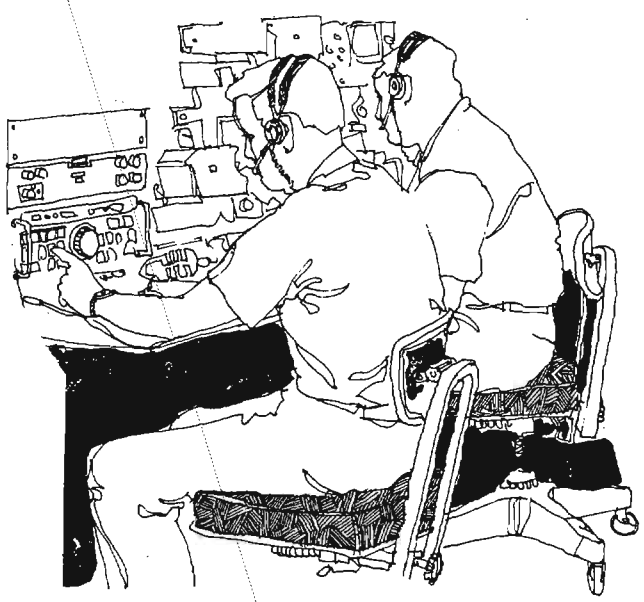
[] on reporting, which provides false information to the consumer; and

[] on evaluation, which attributes tasking satisfaction to the wrong target.

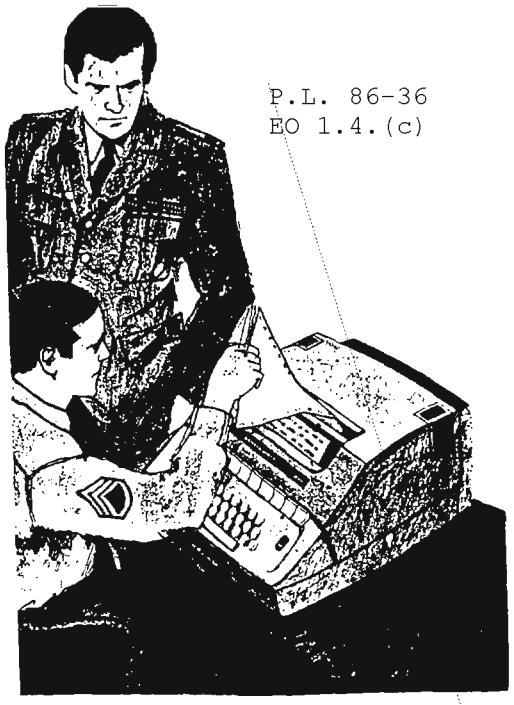
To ensure the most effective Collection Support effort possible, field managers must develop an operational system that exposes all elements of the assigned analytical work force to both collection support duties and desk analysis duties. Ideally, such a system, which rotates the individuals between these two worlds, will ultimately increase the expertise levels available in both areas. Likewise, at the national level all methods of developing collection support material for field elements must be closely scrutinized to ensure that a minimum of manipulation is required onsite to use the data.

Processing

~~(C)~~ The next function of traffic analysis, Processing, often assumes a life of its own. From the analyst's standpoint, processing (or, to use a more common term, "logging") quickly becomes associated with drudgery. The fact that processing is accomplished merely in order to organize intercepted data for subsequent analysis is quickly forgotten. Processing then becomes a mindless transfer of data from one medium, the raw intercept, to another medium, the casebook or data base. Further, this attitude quickly leads to overlooked items of significance that otherwise would require immediate analytic or reporting attention.



P.L. 86-36
EO 1.4.(c)



P.L. 86-36
EO 1.4.(c)

(U) From the managers' standpoint, however, processing quickly becomes the key productivity measurement because of the statistical data available from data base maintenance inputs. Since the underlying desire is for an accurate data base from which to extract material for subsequent analysis, and from which to drive any automatic collection support vehicles which emanate from the data base, the managers' concern becomes one of concern over data base maintenance accuracy and volume. Unfortunately, this concern for accuracy normally translates into a concern over the correct formatting of the input rather than over the validity of the information itself. Likewise, the volume concern translates into a meaningless "body count" that is used to spur further productivity.

[redacted]

poses should be deleted from existing requirements. For example, the processing of voluminous message serialization data should not be imposed on the affected analyst if no one intends to perform a study of this aspect of the target's communications. The processing requirements should be continually geared to the voids of the target's communications that need to be exploited, and not to those characteristics that are commonplace and seldom change, as these voids are reduced through exploitation.

P.L. 86-36
EO 1.4.(c)

Analysis

[redacted]

DOCID: 4033691

underlying military force must be the first priority of the traffic analyst. Only through such mastery can an analyst understand the communications facing him or detect changes in those communications which can be attributed to something reportable. In addition to ensuring that the analysts are knowledgeable of the structure of the military force, managers at all levels must ensure that the analytic studies to be undertaken first have the potential of satisfying either established reporting criteria or of developing material that will aid Collection Support activities. All other studies, no matter how well-intentioned, are merely a waste of an analyst's valuable time.

Reporting

(U) The reporting function is the sum total of how well the earlier functions were conducted. If these earlier functions were conducted in a shoddy manner, they normally will culminate in an inaccurate report that bears little relationship to the consumer's initial state requirement. Conversely, if these earlier functions were conducted in an orderly manner so that each function supported the following one, the report will probably satisfy the consumer's request. In addition to satisfying the consumer's request, the analyst must also concern himself or herself about using the proper format for the information to be used in the report. Poorly formatted reports, while factually correct, convey a sense of disorganization that can color the credibility placed on the information by the recipient.

[redacted]

[redacted]

(U) Both of these rationalizations have effectively downgraded the opportunities available to the traffic analyst to participate in the reporting function, the only function which at present is directly keyed to reporting criteria that match the consumers' requirements. By reducing the analysts' participation in this function, we also reduce their ability to ensure that the previous functions remain directed towards the ultimate goal of consumer satisfaction. Managers at all levels must emphasize the development and maintenance of effective and imaginative reporting programs that challenge the analysts' skill to ensure that that reporting function does not become divorced from all that has preceded it.

P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)

Evaluation

[redacted]

P.L. 86-36
EO 1.4.(c)

(U) Through their involvement in the evaluation process, the traffic analysts are well placed to redirect the collection resources to exploitable areas--or at least to areas that have not been satisfied through past intercept--of the target's communications. Unfortunately, the evaluation process is normally either not performed at all or it keys on indicators which, when viewed alone, fail to provide an accurate reflection of the productivity of the resource.

[redacted]

(U) As should be apparent, the traffic analyst of today is faced with a variety of functions. However, all of these functions are tied together by a thread of continuity relating to the final goal of consumer satisfaction. If these functions are not kept in their proper relationship to each other, either through analyst neglect or improper managerial emphasis, it will be difficult--if not impossible--to achieve a cohesive operational mission that satisfies consumer requirements. Only through mutually supporting functions, as originally envisioned, can our scarce collection and analytic resources be used to their fullest extent. In other words, perhaps a return to the basics may be in order for the traffic analyst of today!

P.L. 86-36
EO 1.4.(c)

To: Editor, Cryptolog

Dear Ed:

(U) "To err is human, to forgive--divine." We should feel that way, but it's not easy. When the Data Standards Center was alerted to look for that verbum horribile "JULIAN DATE" in the latest Shell Game article entitled "Time Shells" (February-March 1984, pp. 9-11) our dismay was great. Here again was that atrocious misnomer staring at us from the pages of an otherwise excellent publication. Only arch conservatives who don't believe in progress would dare use the term "Julian Date" when what they meant was really Ordinal Date (which is a Federal standard as well as DoD/NSA.) After all, when Pope Gregory XIII gave us the modern calendar (circa 1580), he likely never dreamed that 20th century man would still be using the JULIAN calendar after all these years. It's now 13 days behind our Gregorian one, which is hard enough to keep up to date, what with leap years and all that.

(U) So, please, repent and be forgiven--and henceforth use only ORDINAL DATE when you want to record a date such as 21 June 1985 in the form "85172." (The Standards Center expounded on this theme in the September '83 issue of CRYPTOLOG, in a piece called "Do You Really Mean Julian?") Verb. sap.

[redacted]
P13D

P.L. 86-36

Dear Editor:

Improved communications, processing centralization, and widespread computer use have all contributed to the apparent demise of the ITC (Informal Technical Circular) vehicle used by the traffic analyst. No one seems to remember when the last ITC was issued or who is the keeper of ITC serialization (or even if they are serialized for that matter). This is all very regretable because after many long years of searching I have finally found a TA item that meets ITC criteria and merits widespread circulation among the agency's analytic work force. As a last resort this ITC is being sent to you in the hope that it can be published via CRYPTOLOG.

[redacted]

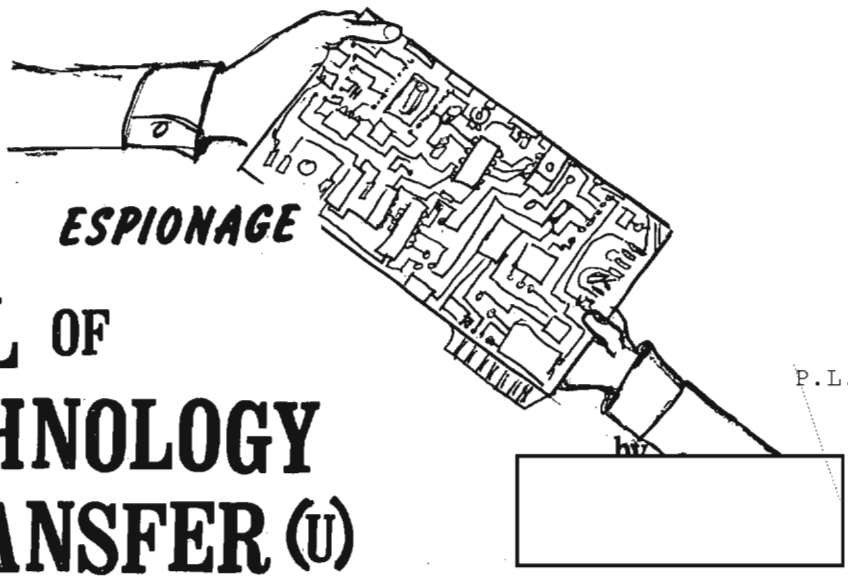
[redacted]

jim@barlc05

P.L. 86-36
EO 1.4.(c)

DOCID: 4033691

ESPIONAGE AS A TOOL OF TECHNOLOGY TRANSFER (U)



P.L. 86-36

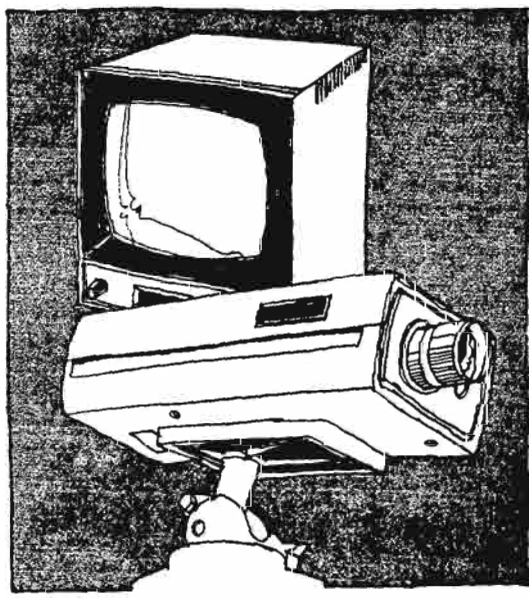
Technology has become one of the major variables that influences and determines United States national security policy. What can or cannot be done as a part of this policy is largely determined by the technological capabilities of the United States and of its adversaries. Technology thus has a major impact on strategy with tactical and strategic doctrine constantly changing in response to rapid advances in technology. These changes necessitate an almost continual alteration of strategy and policy to incorporate improvements in technology and to counter those of our potential adversaries. Our enemies are faced with the same dilemma.

The result of technology becoming a vital component of a nation's security is that any power that lags significantly in military technology, no matter how large its military budget or how efficiently it allocates resources, is likely to be at the mercy of its more progressive enemies. Thus the importance of military science and technology to national security is increasing in almost direct proportion to the importance of science and technology to society. Although the United States has enjoyed military superiority since World War II because of the advanced scientific and technical base that was built up over a number of years, today this dominance is being threatened by the Soviet Union.

The Soviet Union views scientific and technological achievements as the keystone of political and economic power; however, they traditionally have done well only in processes not noted for technological complexity in which central coordination of large amounts of capital and resources confer some kind of comparative advantage. This has caused them problems since there is more to technological innovation than the mere discovery of the concept. The concept has to be translated into something useful. Nonetheless, the gap between US and Soviet military technology is closing and we are rapidly approaching an era of equality. Although the Soviet Union is currently the second most technologically advanced nation in the world, we continue to provide them with the products and processes that they require to develop new and increasingly more sophisticated weapons systems.

Modern weapons become obsolete in a comparatively few years since the lead time to develop weapons is often considered long when compared to the rate of change in science and technology. The cost and complexity also increases with each new generation of weapons and this has resulted in a premium being added to careful and accurate research and development planning. Sudden technological achievements that impact on doctrine and set nations off on a new course are rare and occur only after decades of research and development. The development of these weapons systems is time-consuming, expensive, and important. Since the success of a country's foreign policy rests increasingly on technological superiority, technology has become one of the most decisive influences in international affairs. The necessity for obtaining technological information has become paramount to existence as a world power; therefore, espionage to determine where on the scale of technological possibilities the enemy lies has become important, commonplace, and necessary for the survival of many governmental systems.

The necessity for obtaining military and political information by espionage has always been accepted, although it has been the convention never to acknowledge that it was being done. As early as World War II the Soviets began to use espionage to improve their technology. The friendly relationships between the Allies during the war years made espionage easy and lucrative. As a result, the Soviets gained important knowledge of the US atomic energy program, data on jet engine propulsion, and access to many US production techniques. In addition, because of the Lend-Lease program, they had actual US equipment to use as models. Even so, despite a theoretical heritage and German scientists captured at the close of World War II, the Soviets began from a rather meager technical base. Until the early 1950s they continued to rely heavily on outside assistance. With the development of thermonuclear weapons and the systems to deliver them during the mid-1950s, scientific and technological advances became more rapid and more important. As a result, the Soviets increased and intensified their intelligence collection, using espionage to gain information regarding advances in science and technology. Acquiring or stealing technology was assigned the highest priority for Soviet intelligence operations. Both the KGB and GRU, the two major Soviet intelligence organizations, were tasked with using whatever means were available to ensure that a continuing flow of Western technology found its way to Soviet agriculture, Soviet industry, and, most important, to Soviet military users. Thus, the collection of scientific and technical information became a normal function of the Soviet intelligence services.



In the United States, more than three-fourths of all military-related research and development is done by private industry with the Department of Defense contributing over $200 million a year to their basic research activities. In addition, there are many other research activities that often result in new processes or techniques that could have military application. The difficulty is that a piece of research can serve both the purposes of peace and war. This causes considerable problems in controlling this kind of information since the openness of our society has caused a dilemma. In the name of national security, our government often feels compelled to constrain the flow of technology to the Soviet Union or other countries who might pass on the critical information to the Soviets or their counterparts. For economic health, however, the US government must promote the export competitiveness of our high-tech products. These controls have always been at the heart of controversy and have made the denial of information to the Soviets difficult. This has made the acquisition of information by their intelligence apparatus highly successful and therefore very damaging to the interests of the United States.

The research and development programming system of the United States and its annual military posture statement give many details of our future military plans. These documents are widely distributed and available to the Soviet agent. As stated in a 1970s study on the arms race, "The United States, for reasons of policy, tradition, and ineptness in keeping secrets, has been so open that Soviet military planners perhaps know as much about these matters in the US as the US military planners." Using this type of data, Soviet agents can be directed towards available open source documents. They find them in great numbers. It is estimated that there are at least 50,000 technical journals, most of them monthly, published throughout the world and that, in some technical areas, notably electronics, plastics, and chemicals, literature output doubles every 10 to 15 years. About 30 percent of the agents' requirements could be met by legal, open means such as subscribing to Aviation Week, attending international conferences, using contacts with Soviet citizens attending American universities, and through the adroit use of the Freedom of Information Act. Often by asking the right questions they are able to acquire from the federal government files and other technical data materials not generally available to the public. Much of this data is often recently declassified.

The Soviets are also able to buy technologically sophisticated equipments on the open

market. Legal acquisitions generally have their greatest impact on the industrial base and affect military technology on a relatively long-term basis. These legal acquisitions almost always find their way into military industries and subsequently into the civilian sectors of industry that support military production. Although the Soviets will state that these acquisitions will be used solely for civilian applications, legal purchases are part of a well-organized and well-coordinated plan to acquire Western technology that is militarily significant and of benefit to Soviet industries engaged in research, development, and production of weapons systems.

Although massive amounts of information are gained by using open source publications and through the legal acquisition of American equipment, about 70 percent of the Soviets' technology requirements are met by their illegal purchases and through information gained by their intelligence services. According to Edward J. O'Malley, an FBI official in Washington, "They buy what they can, they steal what they can't buy." [1] Clandestine acquisition of the West's most advanced military-related equipment and know-how by the Soviet intelligence apparatus is a major and growing problem. These organizations have been so successful that the manpower allocated to this effort has increased significantly and there are now several thousand technology collection officers operating in the United States under various covers ranging from diplomat to journalist to student. FBI Director William Webster, in an appearance on CBS's "Face the Nation" on 24 April 1983, stated that "there are about 3,000 Soviet bloc diplomats in the United States and 30 to 40 percent pursue US secrets--especially military information and laser and computer technology." A favorite technique of these agents is to set up a dummy corporation chartered to provide an authentic-looking letterhead. At the present time, the Soviets are bankrolling about 400 of these companies in the free world. These companies place orders for the high-tech equipment required by the Soviets. The equipment is then sent to some non-Communist country in Europe and eventually diverted to Russia. [2] Another method used by the Soviet agents is to persuade legitimate foreign companies to import US equipment and then sell it to the Russians for a profit. The acquisitions gained through these illegal trade channels often have important military applications.

If the Soviet agent fails to acquire the necessary equipment or information using the methods described above, he may resort to larceny. One method used successfully is to persuade a disaffected employee of a high-tech company, usually through monetary inducements, to sell the company secrets. If necessary, the agent may even hire thieves to steal the information. This practice has been particularly lucrative for thieves in the Silicon Valley, where many have found that stealing microchips is more profitable and less risky than stealing cars. Among some of the secrets recently lost to the Soviets through the illicit transfer of technology have been the details of the quite radar system for the B-1 and Stealth bombers, the F-15 look-down, shoot-down radar system, and the Phoenix air-to-air missile--clearly some of our most modern and most important military technology. So confident are the Soviets that they can obtain whatever US technology they need that they now start building the new weapons system before the necessary high-tech components have emerged from US laboratories--and promptly steal them when we do.

When the Soviets receive Western technology, whether it was obtained through legal or illegal means, it is coordinated with information and equipment obtained through a complex network of international governmental, scientific, and technical exchange agreements the Soviets maintain with industrial nations worldwide. These include know-how, equipment, and computer data base collection activities of Soviet scientists and engineers who participate in academic, commercial, and official science and technology exchanges. Richard D. DeLauer, Under Secretary of Defense for Research and Engineering says that one problem with these exchanges is that US scientists and engineers "go off in the corner and shoot the bull with the Russians and anyone else who's there for the wrong reasons." [3] These visiting Soviet technical and student delegations generally consist of expert scientists, many of whom are connected with classified work. The mastery they gain in assimilating one technology enables them to use subsequent transfers of related technologies. The increased mastery that results can be used to undertake independent technological efforts that may include replication and adaptation of foreign technologies and eventually the creation of new technology.

Soviet candidates in various academic and scientific exchange programs nearly always propose research activities that involve technologies that have a military application. This is especially true in areas where the Soviets have a deficiency. In the past two years, more than 30 percent of the proposals offered under the graduate student exchange programs have been unacceptable because of the prospective technology loss. [4] Many other proposals had to be modified before they could be allowed. These Soviet students are often intelligence agents with the necessary scientific and technological backgrounds to make them extremely efficient in gathering information on technological interest.

Soviets also regularly attend high-technology trade shows and attempt to visit commercial firms, particularly small and medium size firms that are active in developing new technologies. These activities are used as a subterfuge to gain access to emerging Western technologies before they have been identified by the US government as having military applications and to make contacts with the personnel of these companies for future exploitation.

The information-gathering efforts that have been described above save the Soviets billions in research and development costs. Stephen Bryen, Deputy Assistant Secretary of Defense for International Economic Trade and Security Policy says, "We keep getting numbers that are so big, and so frightening, that we have given up trying to calculate the amount. But it is in the billions." [5]

In a cost-benefit analysis, espionage may be the most economically productive element of the Soviet economy. The benefits, however, do not stop there and are not totally economic. Using US technology, the Soviets can develop countermeasures to negate our weapons superiority before the weapons are ever deployed. Since the US must rely on technological superiority to offset the Soviets' advantages in quantitative military power, the illegal transfer of advanced technology is providing the Soviets with the rope to hang us--exactly as Lenin prophesied over a half century ago. In addition, the Soviets learn from our mistakes. They can then focus their research and development capital to areas where we are the weakest and select from the best of both technological worlds. The Soviet use of industrial espionage imposes increasing costs on our economy and results in a continual struggle to overcome technology we have invented. As someone once said, "We have met the enemy and it is us."

Footnotes

1. "US Mounts a Belated Effort to Halt the Theft of Electronic Secrets," Life, April, 1983, pp. 29-36.

2. "FBI Claims 30 Percent of Soviets Here to Spy," Washington Times, April 15, 1972, p. 4.

3. "Padlocking the Laboratory," Business Week, April 2, 1983, p. 100.

4. Ibid.

5. "Stemming Flow of High Tech to East," Christian Science Monitor, 11 April, 1971, p. 4.

SOLUTION TO NSA-Crostic No. 55

"The Things They Say," by Doris Miller, KEYWORD, August 1968, reprinted in CRYPTOLOG, November 1976.

"'I know it doesn't make sense, but that's what it says!' This is the granddaddy of them all, the great classic disclaimer, ...the most spontaneous, universal, and irrepressible outcry in the translating world; surely there is no one in the business who hasn't given tongue to it at some time."

INTELLIGENCE ANALYSIS IN THE COMPUTER AGE (U)

by Jack Gurin, SRL

In intelligence work, the day of the 3 x 5 card file is over, or nearly so. Those files, on which so much depends, have moved into something more distant from the user--somehow more difficult to reach--an entity that sometimes seems to thumb its nose at those who would seek its help, the data base. But no matter what your opinion may be of the data base, whether you describe it with kind words or harsh ones, that is where you must go for the information you need. And what is it but a collection of all sorts of data used by many people for many different purposes. It should never be an end in itself, since its only reason for existing is to serve the needs of those who feed it and ask it questions. But, like some of the ancient gods, it sometimes assumes a role in which ritual supplants substance, and the needs of those who support it are subordinated to the requirements of the system created to serve them.

(U) The data base is a creature of the computer. Until recently, it has been possible to obtain information from this repository only by means of special languages and, even then, in a highly restricted number of approaches. As the computer becomes more versatile and responsive, it is not asking too much to expect the data base to move under the direct control of the user of the information, without requiring the acquisition of yet another strange language. With the rapid changes in computer technology and with the increasing accessibility of personal computers, it is time for us to take another look at data bases and how we may make them serve our purposes more effectively than in the past.

FILE SYSTEMS AND DATA BASE SYSTEMS

(U) Files have always been with us and probably always will be. There certainly will be a role for them in a highly localized arena. When the same type of data is needed in many different places by many different people, however, it becomes difficult to ensure that all copies of the information are accurate and up to date. Especially in a rapidly changing intelligence environment, the importance of a maintaining the accuracy, timeliness, and completeness of a commonly held fund of information is obvious.

(U) Another shortcoming of file systems is their inflexibility. If you need the data items grouped in different ways, there may be difficulties, delays, or denials. How often we have been disappointed because the organization of the data did not permit a particular question to be answered? And restructuring the data may be out of the question, since a seemingly trivial change in a file environment sets off a chain reaction of other changes that must be made. This is the kind of thing that gives data systems a bad name, since they seem not to be able to fulfill their purpose without requiring expensive alterations every time a slightly different question is asked.

(U) A file is a thing unto itself. It just isn't tied to anything else, any more than a book is tied into another book. Of course you may have cross references to other files, just as you may find a find a bibliography in a book you are reading. If the cross references or the bibliographies are extensive, they discourage the user from any attempt at com-

DOCID: 4033691

pleteness. Unless you have lots of time, it is not practical to follow all the suggested additional references.

THE HIGH COST OF COMPUTER PROGRAMMING

(U) It is all to obvious that programming costs have consumed a larger and larger part of the data processing budget and, as far as the user is concerned, most (or all) of that has been spent on keeping the old systems going, not improving them but keeping them alive. Often it is the user who triggers many of these costs by asking for information that is just a bit different than what can be derived from the system as it stands. This kind of proliferation of maintenance requirements, if not carefully controlled, tends to increase as the number of programs grows, until it threatens the entire programming budget by its size.

(U) One of the main objects of a data base system is to allow changes in the information to be made just once, and to have that update available immediately to all users. Another is to permit a programmer to make a change in one of the elements of a data base without having to change the other structures. In other words, the data should be independent of the programs as far as the user is concerned. To achieve these goals we have to move into data base management systems that have been created for just these purposes. It is not necessary for the user to know how a data base management system works; it is enough to know that it exists only to provide, easily and quickly, the needed information (if it is stored within the system).

DATA BASE DIALOGUES

(U) The user should be able to deal with the data base without relying on intermediates. Data should be organized in such a manner that, by employing a simple, easy-to-use query language, the user will be able to express needs directly and extract satisfactory responses. The job of combining those elements in the data base that must be brought together to provide a complete and accurate answer to the query is a task for the data base system, not for a special program that needs to be written for the purpose.

(U) No doubt when this kind of flexibility is provided, much more use will be made of the data bases, especially as the users learn more about the potential of such a system in the exploitation of accumulated information.

SIZE OF THE DATA BASE

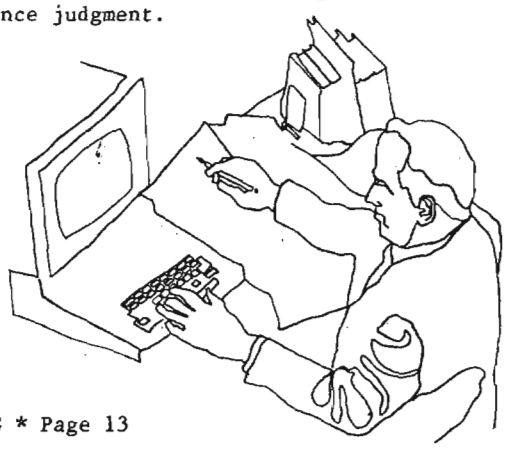
(U) When we talk of THE data base, it should not be assumed that there should be one humongous collection of information, with all users dipping into the reservoir when looking for answers. What appears more likely is that there will be many data bases, all on the same system, but physically and logically separate. They should be linked by common query languages and design policies so that, when necessary, linkages between them may be forged. It is entirely possible that the system will be called upon to provide information that transcends the province of any one collection of data, no matter how comprehensive it may be.

P.L. 86-36

DATA SHARING

(U) Ignoring for the moment the obvious considerations of security, which will vary from one application to the next, one of the great advantages of effective use of a data base system is sharing the data. This means that everyone who is in the system and needs it has access virtually immediately to the information in its most recent and accurate form. It will be necessary to develop clear lines of responsibility (where they do not already exist) as to which is the office of primary interest for each type of data item and to ensure that all participants understand the distribution of responsibilities for entering and maintaining the data items.

(U) The difficulties involved in linking together or integrating the data base and of standardizing the data items may turn out to be considerable, since so many organizations have developed their own ways of keeping files of information. But that is a cost that must be borne if we wish to take full advantage of the capabilities of the computer to assist in the task of bringing to our attention ALL the relevant data that should go into an intelligence judgment.



THE DATA MODEL

(U) Data items do not exist in isolation but are associated with one another. Maps need to be drawn showing which data items are associated with which others, and what types of association these are. Such maps give an overall representation of the data that is needed to service the inquiries of users. A map showing different data items and how they are associated with one another is called a data model. The development of such a data model, or map, is the first step in organizing a data base that will be most responsive to the user's requirements.

(U) Development of a model calls for the direct participation of users, since they are the ones to define the various elements that are to go into the data base, and they must also describe the nature of the relationships between those elements. Some kind of consensus must be reached if the model is to be suitable for a group of users, but in all cases the opinions of the user rather than the data system professional must prevail.

(U) The user's view of the data may be much simpler than the actual data and should be tailored to his own application. This structure may be referred to as the "logical" structure. The actual data structure, stored on tape or disks, may be referred to as the "physical" structure. To illustrate this difference, think of the map of the Metro system in Washington as it is displayed in the subway cars. It merely displays the relationships of the stations to each other and to the line they are on. There is little representation on that schematic of actual distances between stations and actual paths followed by the train. The map is a logical rather than a physical map of the system. The user of the system, whether subway or data base, need not be concerned about anything but the logical structure. When using the data base, nothing about the system should remind him that the physical structure is different. It will be up to the system to convert the user's queries, whether naive or informed, into whatever is required to provide the desired response.

CREATING THE DATA MODEL

(U) The question of what would be the best logical structure for the data is vitally important for the success of the data base system. We expect the system not only to provide complete, rapid, and accurate responses to today's queries from the user, but also to allow itself to be updated easily and, as intelligence needs vary in the future, to be responsive to changes in the nature of queries. If the logical structures are designed badly, operational personnel will not rely on them but will turn once again to local files which, for all their shortcomings, can be created and manipulated with some feeling of security.

(U) Another key factor in determining the success of the data base is the extent to which the user can be protected from the impact of changes that have to be made in the structure. These changes can be minimized by careful system design, but they are unlikely to be eliminated. When such changes are to be made, they should be accomplished in a manner that does not alter the external appearance of the system. The data may be expected to change constantly--especially in an intelligence environment--but the structure of the data base itself should be as stable as possible. If in the future our data base system itself will require the services of programming personnel to make repeated changes in order to cope with changing demands, we will return to the same old problem of expending an unconscionable proportion of resources in patching up the system to keep it going. Chances are that only the minimal investment will be made, and the system will creak badly.

(U) When talking about data modeling, we refer to items about which we store information as entities. Examples of entities are personalities, weapons systems, organizations, abbreviations, job titles, and abstract concepts.

(U) Each entity has various attributes that contribute to the definition of that particular entity. It may be a rank, a location, a title, or other type of data. Of course what is an attribute in one case could well be an entity in another. If one is pursuing a personal name, then organization becomes an important attribute. If, on the other hand, an organization is the focus of interest, then a membership list could be an important attribute. The same case could be made for the relationships between, say, pilot, aircraft, and flight number. The challenge to developers of a data base system is to make the most effective use of the entity-attribute relationship.

FOURTH GENERATION LANGUAGES

(U) As was said earlier, the data base should be so configured that the user will be able to deal with it directly, seldom having to rely on a programmer to adjust the system to his changing requirements. One of the obstacles facing many users or would-be users of computer-based information systems has been the mysterious language that must be mastered before one is allowed to talk to the computer.

Over the years, the number and levels of sophistication of such languages have increased, and we are at the point where the machine can be addressed in words that almost resemble (but really aren't) normal English. Some of these languages are procedural and some non-procedural; some have both capabilities. A procedural language specifies how something is accomplished; a non-procedural language specifies what is to be done but not in detail how it is to be done. For example, should you wish to go by taxi to BWI Airport, you would expect to enter the cab and simply announce your destination to the driver, confident that he would know how to get there. You made a non-procedural request. If, however, he did not know the route, you might have to describe not only which roads to take, but when to turn, etc. In the latter case, you would specify the how as well as the what and would issue procedural instructions. To illustrate this point with a query directed to the computer, suppose your question was "Give me the names of all pilots stationed at Andrews AFB who are qualified to fly F-16s." With a procedural language you would have to specify the path to follow:

```
get personnel list for officers at Andrews AFB
find rated officer
     select if qualified to pilot F-16
     do until no more rated officers
print names of selected officers
end
```

When all the conditions for our ideal data base are fulfilled, the user will merely say what is to be done and will not be concerned with how. For the latter he will rely on the application generator, a part of the system that is designed to perform that task.

(U) Users should not only be allowed to create their own applications without having to resort to programmers, but they should also be able to direct the system to extract wanted data and to format it into reports. Some of these report generators are independent of the data base or query facilities; others are extensions of the data base query languages. Ideally the user should be able to start by learning to make simple data base queries and should steadily extend that skill to data manipulation and report formatting.

(U) Another facility available to some data base users permits them to specify WHETHER they want the data displayed in graphic form. Then they specify HOW. The system may be asked to search files or data bases and to chart the resulting information according to different criteria.

(U) All of the preceding marvels are not only possible. They are reality in some lucky circles. Before they can be made available locally, however, the system must be redesigned and equipped with data base management facilities suited for creating applications. A better logical design is required for the data bases now in use. Only then can effective use be made of data base query languages, report generators, and application generators. Remember that we are talking not about what may be possible in the future, but about the present state of the art. And it is likely that the coming months will bring additional advances that will permit the user to manipulate data even more effectively and speedily.

A NEW ERA FOR INTELLIGENCE ANALYSIS

(U) What is the significance of these advances in data base manipulation to translators, transcribers, analysts--anyone engaged in intelligence analysis? Why go through the trouble--and it will require quite a bit of effort--to reorganize all information files according to a demanding discipline that will appear foreign to previous practice and experience? What kind of payoff is to be expected from this investment of time, labor, and sophisticated new equipment?

(U) The justification lies in the potential of the computer to serve the intelligence community as it has the scientific and technological communities. The computer will be able to assist the user of information files with greatly increased speed, accuracy, and completeness, and this alone could raise productivity sufficiently to justify the investment. In addition, the computer will be able to assist the user by exploring the relationships of data items in a way that the analyst could only do if time and effort expenditure limitations did not exist. Data base searches of possible relationships, performed at enormous speed, could provide to the user information that would otherwise simply not be available. The combination of a powerful personal computer and a relational data base that may be reached via a non-procedural language and a data base management system will provide a tool for intelligence analysis such as we have never had before.

DOCID: 4033691

NAMING SOVIET CITIES (U)

Since the October Revolution, the Russians have seen an inordinate number of their larger and more important cities undergo name changes at least once, and, in some cases, as many as three times. A study of this twentieth-century phenomenon reveals certain trends which have developed in Soviet city name-changing through the years. In addition to isolating such trends, a study of this type gives us a quick course in Soviet history over the past fifty years or so. In the material which follows only the larger Soviet cities have been included.

(U) Not long after the Bolsheviks assumed power a crusade was started to change the names of Russian cities which were named after tsars or tsarinas, or were otherwise associated with tsardom. Accordingly, Novonikolaevsk became Novosibirsk, Aleksandrovsk was changed to Zaporozh'e, Ekaterinoslav was renamed Dnepropetrovsk, Tsarkoe Selo became Pushkin, etc. Today none of the major Soviet cities have Tsarist-associated names although there is still a fair smattering of Ekaterinovkas, Nikolaevkas, Elizavetovkas, etc., throughout the country.

(U) Another noticeable trend in city naming began with the death of Lenin: important Soviet cities were renamed for deceased Bolshevik heroes. It was perfectly fitting that after Lenin's death, his birthplace and the place where the Bolshevik Revolution erupted should be named for him. Other leading Bolsheviks like Sverdlov, Kirov, Kujbyshev, and Frunze were also posthumously honored by having cities named after them.

(U) Reprinted from the Spring 1984 issue of Vox Topics, where it appeared with no author's name given. City names were written with Cyrillic characters in the original and the only change made in the text was to transliterate those names for readers of Cryptolog.

(U) During 1924, the very year of Lenin's death, another less durable city-naming practice, that of naming large cities after living Soviet heroes, came into vogue. Cities all over the Soviet Union began taking Stalin's name. Zinoviev also had this dubious honor bestowed on him when Elizavetgrad became Zinovievsk. Later Molotov and Voroshilov were similarly honored when the cities of Perm' and Lugansk respectively were named after them. The trouble with the practice was that most of these men fell into disfavor while still alive or, in the case of Stalin, after death. This necessitated changing the names of the cities once again. Rather than dreaming up new names, the Soviets tended to resolve these dilemmas by giving the cities back their harmless former names. Thus, Perm' and Lugansk where reinstated while Dyushambe, which had become Stalinabad, returned as Dushanbe. The only two major cities to escape this fate were Kalinin, formerly Tver', and Gorkij, formerly Nizhni Novgorod [1].

(U) New names, however, had to be found for Zinovievsk and Stalingrad which could not go back to their tsarist-tainted named of

DOCID: 4033691

Elizavetgrad and Tsaritsyn. The same was also true for Stalino which could not return to Yuzovka, which had been named after an Englishman. In searching for new names for these last two cities, the Soviets decided to name them after fairly noncontroversial things--rivers. Thus, Volgograd and Donetsk came into being. Zinovievsk had its name changed twice more, first to Kirovo and finally to Kirovgrad.

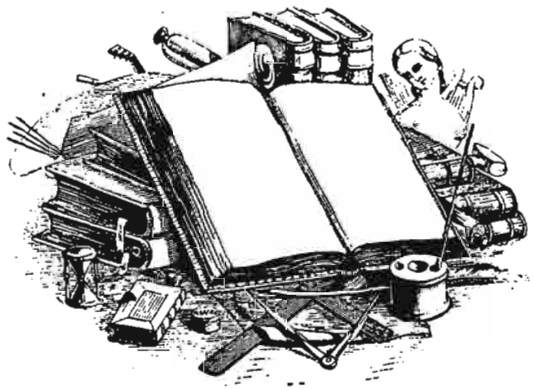
(U) The Soviets in their naming and renaming of cities over the years seem to have become more conservative and sophisticated. No major cities have been named after living persons in recent times. It seems apparent that they have finally realized the problems related to bestowing names of living Soviet giants on their major cities. They have carried this even further by not naming any larger cities after dead stalwarts in recent times. When the cosmonauts Gagarin and Komarov died there was no rush to name Kiev, Rostov, or other large cities after them. An interesting sidelight is that in the last few years the very few non-major Soviet cities to be named after dead people were named in honor of recently deceased foreign Communist leaders. Thus, Stavropol in Kujbyshevskaya Oblast' was named after the Italian Communist Togliatti, Chistyakovo took the name of the Frenchman Thorez, and Liski became Georgiu-Dej after the Romanian leader.

(U) The trend today, however, seems to be to hold on to the city names they have and to honor their heroes by naming schools, ships, parks, and the like after them.

---

1. Kalinin was a noncontroversial symbol of the Russian peasantry who got along with everyone, while Gorkij's literary fame evidently overshadowed any political troubles in which he became involved.

BOOKBREAKER (U)



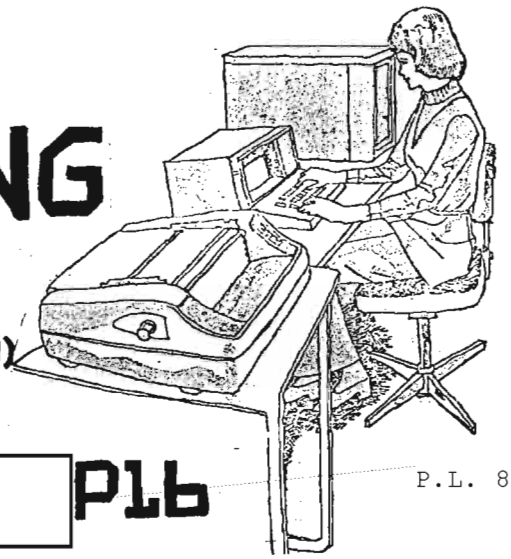
excerpt from
Bookbreaking Improvisations, Part II,
by Stuart Buck
(P1 Informal, June 1966, p. 98)

EO 1.4.(c)
P.L. 86-36

DOCID: 4033691

WORD PROCESSING PLAIN & SIMPLE

(For the User, That Is) (U)



by [redacted] P1b

P.L. 86-36

(U) By now, most people have heard of word processors, and a fairly large segment of the Agency population has used one. We would here like to examine their characteristics and describe our "ideal" word processor. If in some small way our words help influence the features available to us, we shall be most grateful.

(U) The term "word processing" is a gift from the IBM Corporation coined, according to the Encyclopedia of Computer Science and Engineering,[1] in 1964, and like many products of that ubiquitous company it has--as they say--"caught on." Caught on so well, in fact, that it hardly seems necessary today to define it. Define it we shall, however, being ever solicitous of our readers and wanting to have some way to start. As we see it, a word processor is a program, system, or machine

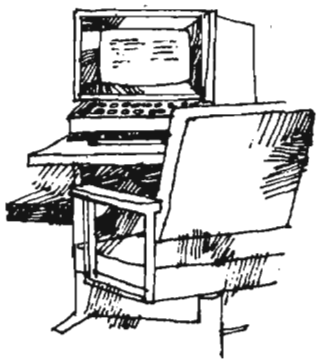
- [] which offers the capability to place a text onto an electronic medium, usually using a keyboard;
- [] which displays the text selectively to the user; and
- [] which offers a variety of features which facilitate modifications of the text.

Word processing is the process of doing all that.

(U) What, then, is the difference between word processing and text editing? One might well wonder. We have attempted mightily to find a consistent distinction, to no avail. "Text editing" is an older term, dating from a time when "terminal" referred to a printing device that might have a keyboard, as opposed to today's view that it is a scope. Therein lies much of the difference between the two usages, but there are pockets of vendors and users who make other, less consistent, distinctions between the two.

(U) The reason for the great popularity of word processors is that they take a lot of the pain out of writing--make it almost effortless, in fact. They are helpful in getting words recorded in the first place, and they come into their own when it comes to modifying the text or performing certain simple checks on it. They also have their little aggravations, not least of which, in our view, is the fact that none of them seems to have all the features we would like to have available to us.

(U) Popular as word processors have become, however, the novice user may have to overcome certain apprehensions before approaching an electronic device for the purpose of writing a few words. That tiny screen, for example, can't possibly hold the entire text (in fact, sometimes no more than half a typed page, and usually no more than two typed pages). It is helpful to think of the screen as a window onto the text. The user is given some method for navigating the text--that is, moving the window about so it offers views of other parts of the text. Once mastered, the process is no harder than flipping the pages of a book. A somewhat new concept is that of coming to terms with the computer about the location for some action to occur. If we wish to write on paper, we have only to position our pen appropriately for the writing to occur where we wish. For most word processors, we are not writing directly on the screen, so the computer must know where we want to write, and we must have confirmation that the computer knows that is where we want to write. This little problem is usually solved by the identification of a special symbol (underline, reverse blank, arrow, etc.) which marks our spot. This symbol is called a cursor.



Standard Features

(U) There are certain features that are common to most word processors, and we shall begin by reciting them as a means of getting them out of the way. We are pleased to see that the number of features a word processor is expected to support is growing, truly reflecting our desires.

(U) Most word processors can be directed to insert automatically sequenced page numbers, prepare headers and footers automatically (either may include the page number), justify either margin or both, and center text on a line. The cursor's movement about the screen is typically controlled by depressing a key (e.g., carriage return, tab, right-arrow) or moving a little device called a "mouse" (it's about the size of the animal and a long "tail" connects it to the computer). The user may intersperse the text with typed formatting commands, or by typing a function key, or by selecting a task from a "menu" of possible tasks, perhaps accompanied by manipulation of the mouse. Some word processors perform the command immediately, giving the user a "what-you-see-is-what-you-get" view of the text. Others embed the commands and require that the user perform a subsequent processing step in order to achieve the proper format. Moving the viewing window about in the text may be performed by means of function keys that cause the portion of text shown to go forward or back a designated amount; to the very beginning or very end, or to a specified line; or shift the window to the right or left. Alternatively, the user may move a graphical representation of a thumbnail to a location judged to be near the desired text, perhaps moving a cursor (the cursor causing text to be "scrolled", or moved line-at-a-time, up or down on the screen when it reaches the top or bottom, respectively, of the window) to reach the precise text segment. A desired location may also be reached by searching for a specific string of letters.

(U) More than one portion of the same or different texts may be placed on the screen simultaneously by means of multiple windows, also called "ports," that may be placed on the screen as desired. The overall capacity of the screen never changes, of course, so there is a logical limit to the number of windows that can be used realistically.

(U) Now we get to the part of the word processor that makes it all worth while. Once some text has been placed in the computer, all sorts of modifications can be made. A text sequence can be copied from one document to another, thus making it possible to create boilerplate files which may be copied selectively and repeatedly for the creation of a new document tailored to the needs at hand--a feature particularly useful for legal documents and the like. Instead of copying the text, the user may delete it from one part of the document and move it to another--a cut-and-paste type of procedure particularly useful for draft revisions. Or a string of text may be deleted completely. Word processors with a "spell" feature may be used to check each word of text against the system's dictionary, a very useful feature.

(U) Most word processors have a string search feature, which allows the user to command the computer to locate a selected string of characters. We might, for example, ask the computer to find the next occurrence of the string "thu" in this text. It would examine each of these characters in turn, until it reaches the end of the text or finds a match. If no match is found, the system so informs the user: if one is found, it moves the cursor to mark the string, thus.

Other Features

(U) Competition and success have produced the desirable effect that new and handy features are introduced regularly. The undesirable consequence is that the present-day user usually has to wait for another implementation of the system at hand before being able to enjoy the benefits. Some of the more recent features are designed to make data entry, as distinct from text modification, faster and easier.

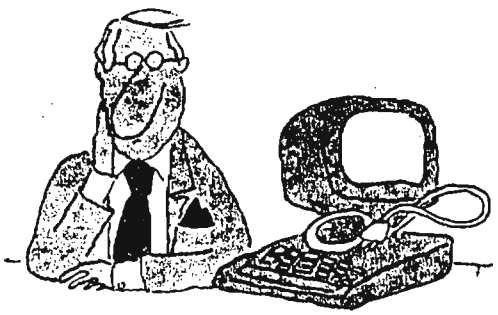
(U) "Word wrap" is a feature that has by now become almost universal. Word wrap occurs when the cursor reaches the right end of the screen. Instead of requiring the user to hit a carriage return at the appropriate place, the word processor positions the cursor at the beginning of the next line, pulling the unfinished beginning of the word along with it. For example, suppose the user has just typed "unfi" when the end of line is reached. When an "n" is typed, the word processor deletes "unfi" from the current line, places "unfin" on the next line, and positions the cursor immediately following the "n".

(U) Because margin justification is so commonly available, a good syllabification scheme is sorely needed. We have seen manuscripts that might have looked very professional because of the justified right margin but instead looked amateurish because there were too many spaces between words. This happens when there are a lot of long words in the text and the word processor has no capability to divide a word between two lines. If the final product is to look professional, syllabification, properly done, is de rigueur.

(U) The ability to change location of the margins, such as for a block indent is certainly a wanted feature.

(U) Some word processors give the user the option of marking certain words to be selected for the automatic preparation of an index. Some provide for special-purpose formats, such as an outline format, so that the user need only keep track of the level of indentation, and the system keeps the numbering scheme in sync. Others, such as those intended for use by computer programmers, identify structural errors in the text. Facility with manipulating columnar text is another feature of interest. Selection of special fonts, such as bold face and italics, or even foreign character sets, is another option. A few word processors offer a graphics capability.

(U) Selection of the font (e.g., bold face, italic, Times Gothic, Greek) and size of print are very desirable features for professional-looking copy. An appropriately adaptable printer is, of course, required to take advantage of such features.



(U) Many desirable features are needed frequently by some users but never by others. Among these are

[] superscripts or subscripts;

[] a decimal tab, which aligns a column of figures at the decimal point; and

[] an overstrike capability, which allows an accent mark to be placed above a letter or a sequence of text to be marked for deletion (useful especially for legal texts where it is important to display proposed textual deletions).

Some users will need a mail merge capability for sending out personalized form letters.

(U) We have not exhausted the list of useful features, but we have grown weary of the task and fear that an exhaustive list may, in any event, be virtually impossible to construct.

Some Cautions

(U) An apparent deficiency of a spelling checker cannot be attributed to the word processor but to its user. Until word processors with ESP are developed, there is no way for them to assure that what the user intended to say is represented accurately and completely. A spelling checker helps the user find words that are misspelled. Some spelling checkers perform better than others, but it is still the responsibility of the user to proofread the copy. At the very least, a sentence parser would be required to identify an "and" where you wanted an "an" or to spot that familiar problem of duplicated words, as in

Paris
in the
the Spring

or ungrammatical but properly spelled constructs. The phrase "Man bite dog" is not grammatical, but all the words are spelled correctly. The proper procedure, then, is to obtain a list of misspelled words, use the search feature to find the offenders, make the necessary corrections, and then review the entire corrected text. A powerful way of correcting the same mistake every time it occurs is to use the global-search-and-replace feature. Note once again, however, that it is not foolproof: the user who habitually transposes the same letters, rendering, for example, "the" as "hte", may want to change all misspellings throughout the text--without also creating a misspell in words like "heighten."

Problems

(U) There are obvious faults with a two-pass process, which requires the user to look at a file containing formatting instructions, then checking the formatted file to be sure everything is as it should be. Perhaps it is less obvious that the "what-you-see-is-what-you-get" approach may, unless very skillfully designed, introduce its own variety of difficulties. Suppose, for instance, we have a long text with many indented paragraphs interspersed with text at a standard line length. When entering this for the first time we want a quick and easy way to move back and forth between the various formats. Having to reset left margin, then reset right margin, and maybe also reset tab stops is not quick and easy enough for us. A "ruler line" that operates quickly and easily, and that the program knows not to print out on our copy, may do the job if easily accessed. Suppose that when we start to print this text, we discover that the line lengths are not suitable after all, and we must change them. We would like to be able to issue a global command that changes all the line lengths appropriately throughout the document (no protests, please: we are confident that with sufficient ingenuity, someone can satisfy our demands).

(U) Established typing and printing conventions are difficult for word processors, partly because their designers are unacquainted with the rules, and partly because completely correct implementation is difficult. Consider, for instance, the standard convention that two spaces separate sentences. When the word processor "fills" a line (brings text from the next line up to fill empty space in the current line), it typically separates the two pieces of text with a single space. If the last character is a period, however, it presumably must insert an extra space. Not all periods signal the end of a sentence, however. In the by-line of this article the reader will find a period that does not mark the end of a sentence. It is usually the case that a period preceded by a capital letter does not finish a sentence. An exception is when the author begins discussing, for example, a PhD. A question mark also identifies the end of a sentence and must be followed by two spaces. Complicating the issue are conventions regarding parentheses and quotation marks. A printing convention is to place a period within the final quotation mark, even when it is a "sentence-ender." Therefore, the word processor would need to check on the character preceding a quotation mark to determine whether or not it is a period and take appropriate action. (Parentheses, too, may enclose a sentence-ending period.)

(U) Other conventions which are frequently ignored by word processors are prohibitions against widows and orphans. A widow is a short line ending a paragraph which is carried over to the top of the next page or column. An orphan is the opening line of a paragraph dangling by itself at the bottom of a page or column. The general rule taught in typing classes is to have no fewer than two lines of a paragraph on a page. Similarly, no word should be divided between lines if the division leaves only two characters on either line. Hyphenation of the last word on the page is also considered bad form.

(U) Justification of both margins calls into focus certain subtleties of the printer's art. The importance of syllabification for an aesthetic appearance was mentioned earlier. Syllabification rules in English are quite complex, however, so designing a system which correctly chooses "prof-it" but "pro-fane," "la-tent" but "lat-i-tude," and "na-tion" but "nat-u-ral" is a nontrivial task. Scanning for "rivers" is another task of the printer that your usual word processor has not yet addressed to our satisfaction. As the reader surveys a page of text, there should be no sequences of white space (caused by inserting extra blank space between words) running across several lines and causing the reader to be distracted. Like housework, attention to small details like this is never noticed until neglected. It should be noted that until word processors made it easy to justify both margins, typeset materials had a corner on the market, and they are usually set with variable-width fonts. The advent of large amounts of monospaced text may accustom us to

its face, but we are not at all certain that we will ever like it as much as "properly" printed text.

(U) Some systems approach the notion of word wrap without giving the full-blown feature. Some versions of the Rand Editor, for example, position the cursor on the next line without dragging the unfinished word down with it. This defeats the intention of word wrap, since it saves neither the key stroke to reposition the cursor (carriage return) nor the effort of having to look at the screen to assure that the word is not split between lines.

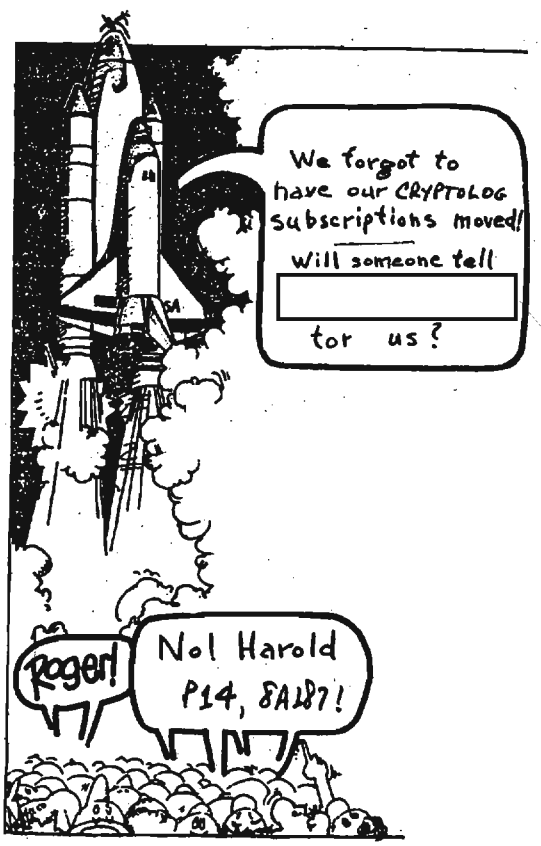
(U) Capital letters pose a lot of problems for word processor designers. For example, the search function is usually designed to find only an exact match, not allowing for a change in case. But the spell program may ignore capitalization and return to the user a list of not-found words in lower case only. Suppose it failed to find "capital" in its dictionary and we wanted to find it in our text. If we give that string to the search routine of most word processors, we will not find the first word of this paragraph.

(U) We have encountered other problems with the search function as well. Suppose the spelling checker produces in its list of unfound words the sequence "ns". Gazing at this sequence, we fail to remember anything we wrote that might have been represented thus, and we haven't a clue where in our 50,000-byte text this string may appear. We wish to find it and a long list of such strings as expeditiously as possible so we can print the text within the next hour. Since "ns" is a common sequence we prefer not to have to look at every instance of it in our text. So we try looking for " ns "; we have reasoned that if the word processor identified it as a word it will be bounded by spaces. Unfortunately, this is not necessarily the case. For most word processors once in each line the space between words is replaced by a carriage return. Therefore, if our "ns" falls at the beginning or end of a line, the match will not occur and the search fails. We may then try " Ns ", " ns", " Ns", "ns ", "Ns ", and "NS", perhaps not in that order. (If the spelling checker distinguishes between upper and lower case, we are spared some of these trials.) By now we have probably become quite dispirited and may no longer care whether we find the error or not. If we subsequently remember that we referred to "n's", which the spelling checker contracted to "ns" (now we remember), our humor is not restored.

The Ideal Word Processor

(U) We view our specification of the ideal word processor as an ongoing project. As soon as a word processor meets all our specifications, we are quite prepared to think up new ones. The system designer should not be discouraged by this prospect but rather should look upon it as job security if not as a challenge. In any event, let the record show that our Ideal Word Processor is not intended as a be-all-and-end-all, forever after, Amen. It merely reflects our thinking on the matter at this moment. We anticipate, that once you readers have been stimulated by these few notions, you will contribute many additional features which we will instantly laud and add to our list. Consider this, then, the beginning of our specification statement.

(U) As you might expect, we want all the desirable features now available to us. Put them all in the same package please. We tire of being teased by having word wrap but not font selection in one word processor while another one has font selection but not word wrap.



P.L. 86-36

(U) We of course want corrections to all the problems noted above. For the print conventions, we feel these have been stated adequately already, so we won't repeat the requirements. The search feature should be enhanced in several ways. We would like the option of finding a string exactly as given or with upper/lower case equivalents of letters (e.g., if the string is "next", having it find "Next" as well). When doing a search-and-replace in such instances, the usual need would be to have the replacement character be in the same case as the one replaced (e.g., replace "naxt" with "next" would replace "Naxt" with "Next"). We also wish to include a space in our search and retrieve any character which may serve as a word divider. This includes the carriage return character. Speaking of which, we may as well request the option to search for a function character.

(U) Cursor movement is another good candidate for enhancement. If a word processor is supposed to process words, why not let the user move the cursor through the text in word increments? We would like to move the cursor to the beginning of the next word, sentence, or paragraph--and, of course, also to the previous word, sentence, and paragraph. Another feature that would help the user who hits the wrong key or simply has a change of mind would be to send the cursor back to its location before the previous cursor change command. We cannot tell you how many times we have hit the "home" key by accident when we were busy placing the cursor just where we wanted it.

(U) There now, that wasn't so bad, was it? We would be ever so grateful if you could just see to it that we find this package all wrapped up in our next word processor.

NOTE

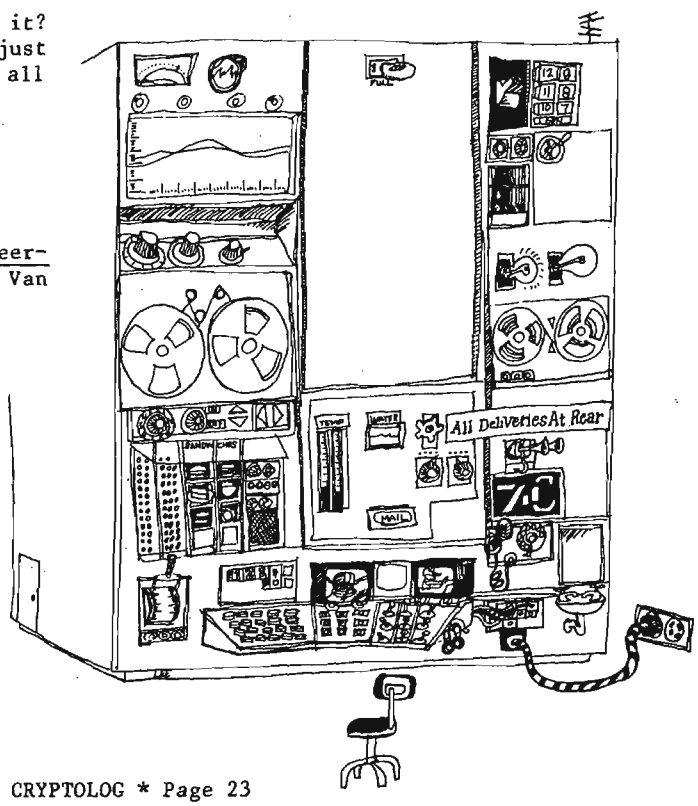
Encyclopedia of Computer Science and Engineering, 2d edition; Anthony Ralston, editor; Van Nostrand Reinhold Co., 1983.

Date: 6 Jul 1984 at 0943-EDT
From: vag at punix [redacted]
Subject: Editorial Reply P.L. 86-36
To: cryptolg at barlc05

Ekcej moernb asodfc dfk cmdf youdf wls c df basdfasdf?!?!?!?! Edf ckd sdfk tdsfyr df glcdoe? Thsas mrwo sdfkwe, cme pcm th wjch riddmre.

In other words, yes we do read the Editorial!!

[redacted]
T3511 P.L. 86-36



OCID: 4033691

ANSWERS TO "WHAT'S THE CAPTION?"

From [redacted] P14: P.L. 86-36

"Operations Building 2A gargoyles near completion."

or

"Identify the seven staff officers in this picture."

or

"The tech track."

From [redacted] G31: P.L. 86-36

"I should have known there was a catch to his 'end-of-the-month special' on nose jobs."

From [redacted] B413: P.L. 86-36

Friar Nip: What the devil is Brother Chip up to?
Friar Tuck: His doctor told him to take two aspirins and gargoyle!

Friar Nip: That certainly is a marble-ous piece of work!
Friar Tuck: Yes, but future generations probably will take it for granite.

Friar Nip: What a farce! The sculptor has little talent, the stone is cheap, and the model is ugly as sin.
Friar Tuck: Maybe that's why Brother Chip has named his work "The Statue of Limitations."

From Clint Brooks, S4:

"SRB Program Review"

From "Jess Possible"

"I can see where the badge goes, but where do we punch in the numbers?"

Here's an extract from a collection of papers that ought to be distinguished in some way from the usual Golden Oldies. It's a prediction that came true, though it seemed far-fetched until just a few years ago. V.V.

Perhaps the principal element in the ignorance of the public in cryptography has been the attitude of the military and diplomatic governmental authorities of the world. It has not been deemed wise to admit the public to a knowledge of a science which might at some time or other endanger the safety of a state. Governments have gone so far as to restrict the use of secret means of communication to its diplomatic or military agents. A ban of this kind was placed by several of the European states in the 18th and 19th centuries. With the advent of more democratic forms of government, the public has taken to inquiring more closely into the affairs which concern it. Peoples everywhere have begun to insist that they be admitted into the confidence of the governments which rule them. It is to be expected, therefore, that the science of cryptography which has hitherto been so jealously guarded by a chosen few of the elect will in a few more years become a matter of more general knowledge.

extract from "General Principles of Cipher"
by James Rives Childs,
1st Lt. Inf, U.S.R.
April 1919.

Unless Texts Hang Together, Linguists Will All Hang Separately or Coherence, Cohesion, & LG-140 (U)

by [redacted]

P.L. 86-36

In his article in the December 1983 Cryptolog entitled "Non Posse vs. Posse Non (U)," [redacted] (C) brings up a point that is fundamental to Agency translators and, in many cases, transcribers as well. Communications, be they in our personal lives or those of our target countries, have one very important fact in common: there is always a message. It so happens that in order for the message to be understood, there are certain conventions that must be followed by both sender and receiver. Our knowledge of these conventions or characteristics of messages allows us to process the many messages we receive every day.

(U) The problem is that with regard to our native language, we are not aware of our use of these message traits for our understanding because they were acquired along with the language that we learned as children. Moreover, the large majority of language teaching separates the language from its main purpose, that of sending messages. Put another way, the method of teaching isolated vocabulary items, word endings, sentence, patterns, etc., puts the emphasis on the medium rather than the message.

[redacted]

[redacted]

(U) Granted, an experienced trainer can shorten the process somewhat, but what is often the case is that the experienced linguist has internalized those tools he uses to deal with a message. As a result, it is as hard for him to pass these tools on to the new linguists as it is for us to explain a certain quirk in English grammar to a non-native speaker. In light of this situation, how does the new linguist learn the point that Mr. [redacted] has "been trying to push over the years: all parts of a text are related!" without a long period of trial and error?

(C) The National Cryptologic School has one answer in the form of a new course, LG-140, Applied Cryptologic Linguistics. This class is focused directly on the problem of how we process language at the Agency. While it does cover some linguistic theory and some descriptions of various types of language applications at NSA, the majority of the course consists of lectures, exercises, and class discussions about the characteristics of messages or texts and how this nature can be exploited.

(U) The course covers such characteristics of texts as COHERENCE and COHESION, to name just two. Cohesion, the property of a text to hang together syntactically, is illustrated by various kinds of chaining exercises where one follows a certain element of a text from the beginning to the end, despite the fact that it takes various forms throughout. One chaining example focused on the different ways of

P.L. 86-36

be certified by their parent U.S ...ment organization to NSA Visitor Clearance (M5611) at lea...king days prior to the date of the visit.

(2) The NSA/CSS sponso... ...at M5611 is on distribution for all incoming clearance, ...tion messages to include SOCOMM Mess... ...at are recei... ...the sponsor. When M5611 ...is not indi... must provide a copy c... ...M5611 fo...

(3) The NSA... Request (Form G2450) for ea... submitted to Vi... ...Clearance (M... cation at lea... ...days prior ... M5611 maintai... ...on in... cleared and SI...

(4) Vis... concerning foreign nation... Directorate of Foreign Relations ...

(5) ... concerning congr... the Legislative ...

(6) Addi... controls, and sponsor's responsibilities is set ... Chapter 803, NSA/CSS PMM 30-2.

b. ~~(FOUO)~~ Visits to Field Activities and to Non... Facilities

(1) The certification of appropr... access information is required when NSA/CSS organizations or facilities on classified certifications will be limited to require ...ivities of the U.S. Government. The clearance/ac... ...ation is accomplished as follows:

(a) CONUS - NSA/CSS Form G2901, "Official Visit Notification", is prepared in the sponsoring NSA/CSS element and forwarded to Visitor Clearance (M5611). M5611 provides the necessary certification to the organization or activity being visited. Guidance for the preparation of Form G2901 is contained in Annex A to this Letter.

(b) Overseas - Planning messages, which are prepared within the sponsoring element for release by Travel Management and Support, M62, must contain appropriate security clearance/access authorization information.

referring to a Metrobus in an article about a bus accident. Although this may seem a trivial example, it nonetheless illustrates something that can be very problematic, especially in voice texts.

(U) Coherence, often lumped together with Cohesion, is really a measure of how well those concepts which are elicited by the text match our understanding of the world. Put another way, Coherence is a measure of the degree to which a text makes sense. Something can be cohesive (or syntactically correct) but still not make sense. One place this often occurs is in newspaper headlines, such as

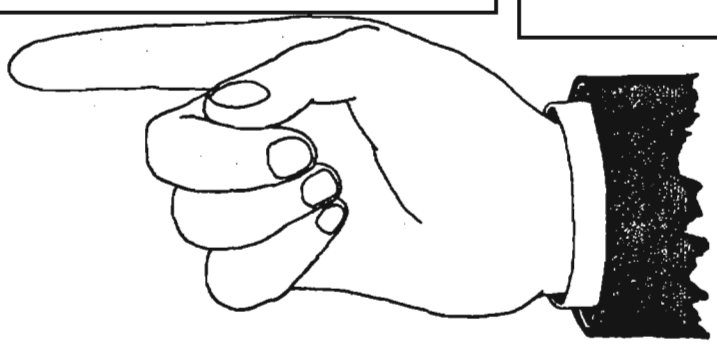
HERSHEY BARS PROTEST

EO 1.4.(c)
P.L. 86-36

or

ESCAPEE RECAPTURED IN SANDWICH

Both of these examples (which were taken from LG-140 material) are grammatically correct, but it is not until we apply our world knowledge that they really make sense. You have to know that General Lewis Hershey, the head of Selective Service, refused to let some draft protestors carry out their activities near his headquarters and that Sandwich is a town in Massachusetts.



~~FOR OFFICIAL USE ONLY~~

NSA-Crostic No. 56

by [redacted]

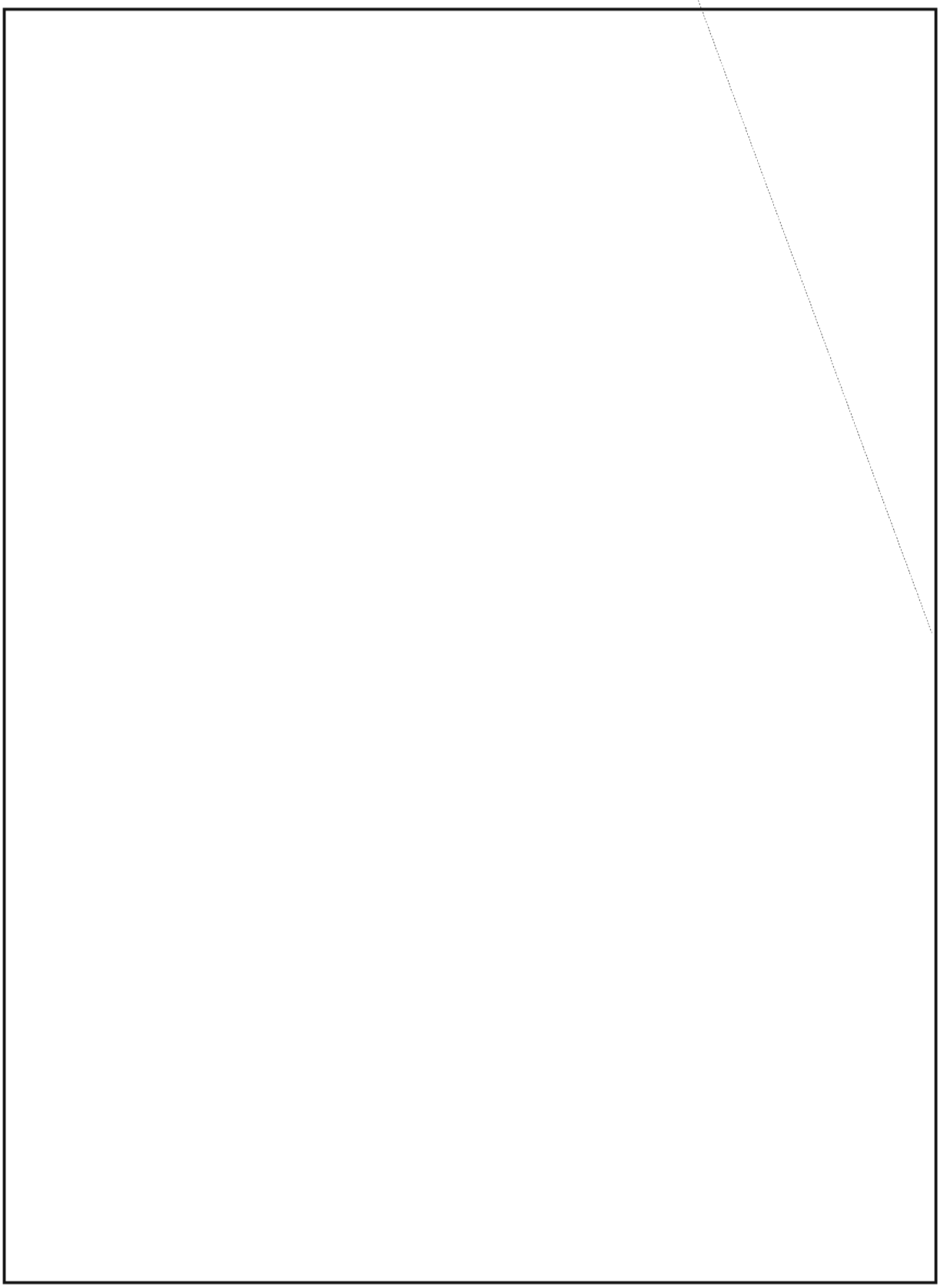
THE FEMALE LEADS OF WORDS H, J AND S

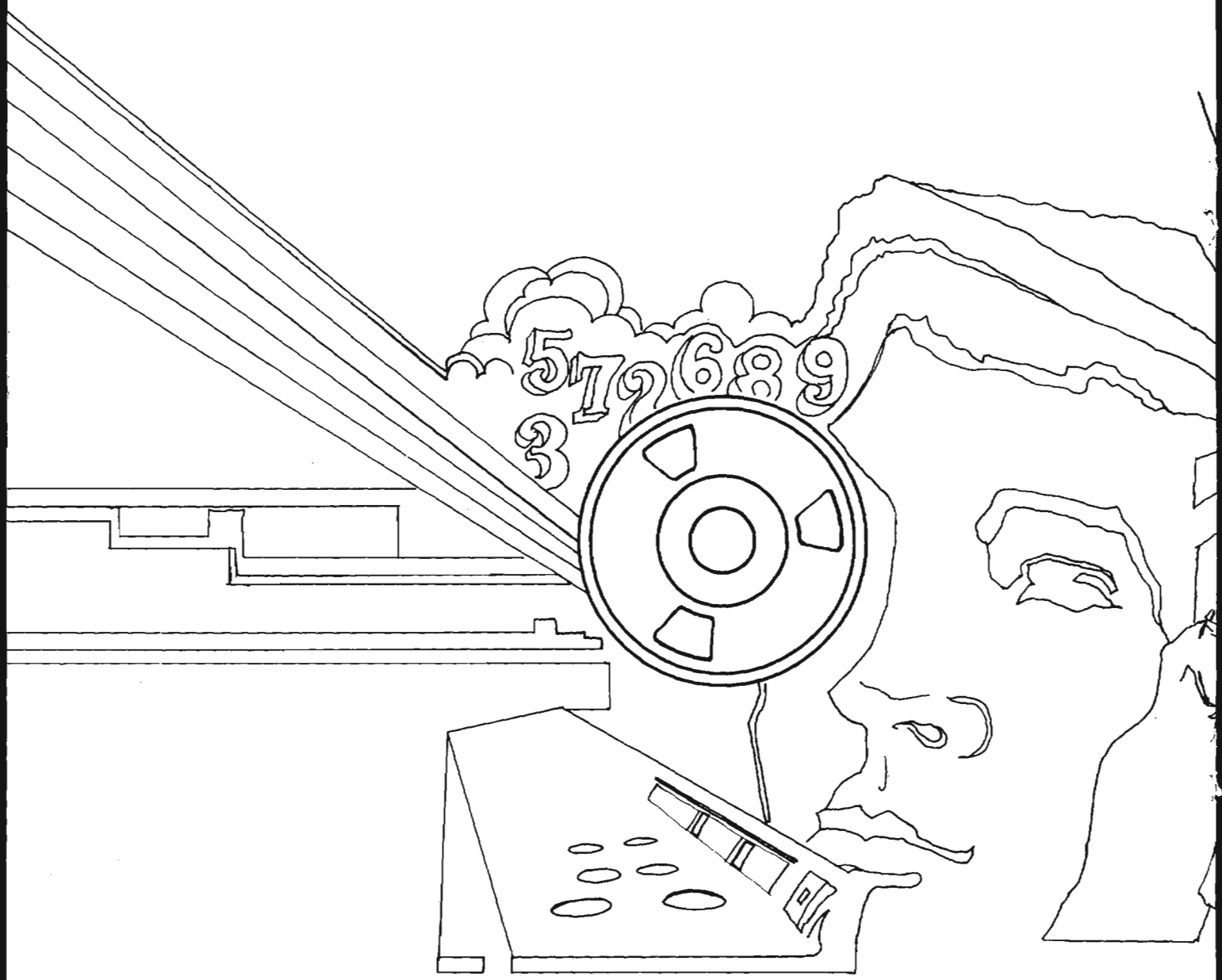
P.L. 86-36

[redacted]

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~




5726893

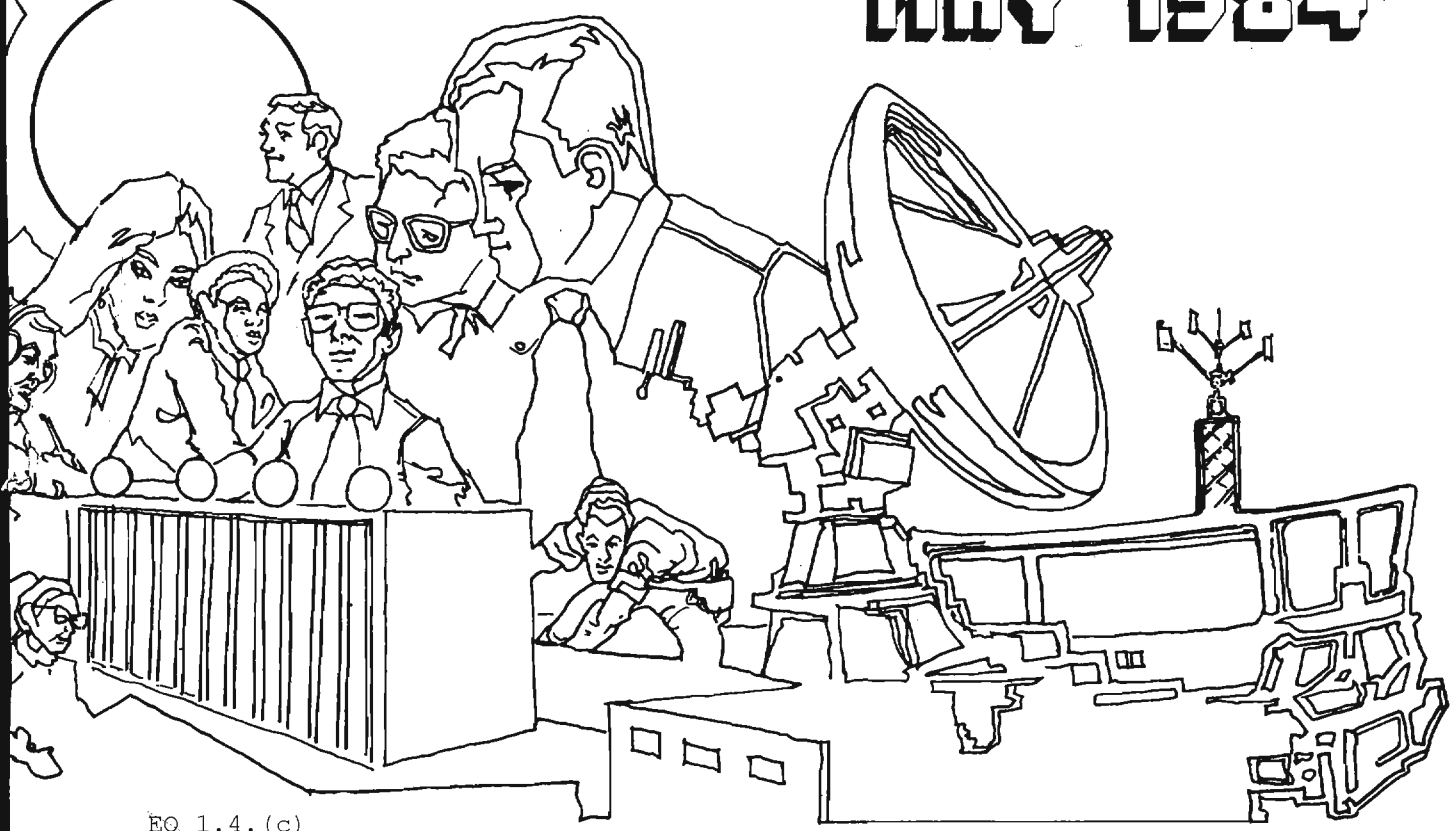
DOCID: 4019700

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MAY 1984



EO 1.4.(c)
P.L. 86-36

P.L. 86-36

MEXICAN OIL & US ENERGY SECURITY (U)..... [redacted] 1
GOLDEN OLDIE (U).....5
SHELL GAME: SUICIDE SHELL (U)..... [redacted] 6
[redacted] ..... [redacted] 8
[redacted] ..... [redacted] 11
'I SPY' A LA MOSCOW (U)..... [redacted] 13
NSA-CROSTIC NO. 55 (U).....David H. Williams.....20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019700

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XI, No. 5 MAY 1984

PUBLISHER [redacted]

BOARD OF EDITORS

Editor..... [redacted] (963-3045s)
Asst. Editor... [redacted] (963-1103s)
Production..... [redacted] (963-3369s)

Collection..... [redacted] (963-3961s)
Computer Security
..... [redacted] (859-6044)
Cryptolinguistics. [redacted] (963-1103s)
Data Systems..... [redacted] (963-4953s)
Information Science
..... [redacted] (963-5711s)
Mathematics..... [redacted] (968-8518s)
Puzzles.....David H. Williams (963-1103s)
Special Research....Vera R. Filby (968-7119s)
Traffic Analysis..Robert J. Hanyok (968-8418s)

For subscriptions
send name and organization
to: [redacted] P14

P.L. 86-36

To submit articles or letters
by mail, to: P1, Cryptolog

via PLATFORM mail, send to:
cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no 'O' in 'log')

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

(U) Attitudes change. It has been some years now since a senior government official said, "Gentlemen don't read other people's mail." It is not resting on our laurels to say that most senior people in our government now recognize the usefulness of what we do. However, there is a new attitude around about secrecy--that it is somehow immoral. And anyone who keeps secrets is evidently immoral too, at least until proven otherwise.

[redacted]

EO 1.4.(c)
P.L. 86-36

DOCID: 4019700

MEXICAN OIL & US ENERGY SECURITY (U)

A Convergence of National Goals

by

[redacted] S041

P.L. 86-36

(U) This paper was awarded Second Prize in the 1983 Essay Contest of the International Affairs Institute, when the author's name was [redacted]

Energy--a basic concept in the industrial world--has taken on an importance to our generation well beyond the confines of its dictionary definition. (U) Energy truly is power--not only in the mechanical sense of force, but also in the global sense of military strength and political control. Energy is not only ability to perform work; it is the basic component of the West's industrial and defense structures. Energy is the foundation of the industrialized world.

(U) Over the last several decades the United States has shifted its military and industrial base so as to now equate energy supply with the supply of crude oil and petroleum products. The seeming world abundance of oil occasioned a transition from traditional reliance on coal to dependence on petroleum. The nation's entire economic structure is built on a foundation of cheap, readily available oil supplies, and its continued functioning is critically dependent on maintenance of those supplies. This transition of energy supply sources could be viewed as a domestic policy issue if it were not for the fact that US oil production is insufficient to meet US oil demand.

(U) The United States, though one of the world's largest producers of petroleum, must import significant quantities of oil to meet its strategic defense and industrial needs. Successful oil exploitation in the US is failing to keep pace with domestic consumption, and the need to import oil to satisfy demand will continue to exist for the foreseeable future. Thus, the security of energy supplies is now a key element in US strategic planning.

(U) There are only two ways to improve a nation's energy security. They are "to reduce dependence on imports of energy--particularly from insecure sources--and, to the extent that such imports are unavoidable, to diversify the sources from which they are obtained."[1] The first requires both a commitment to the development of alternative sources of energy and long lead times. Since the US Government has decreased its emphasis on the development of alternate energy sources for various political, economic, and environmental reasons, and since even a renewed, full-force commitment could not alleviate short- and medium-term energy supply problems, immediate US policy initiatives need to be focused on the diversification of sources of petroleum supply.

(U) Because of the fact that 56 percent of the world's proven oil reserves are located in the Middle East, acquisition of foreign supplies has been heavily weighted toward the nations of that area, but recent history has shown the Middle East to be a region with "significant risk of political disruption."[2] The United States also imports petroleum from other geographic area and has made some effort to diversify suppliers by focusing its oil trade negotiations on the countries judged to be most stable. It is this aspect of US energy policy which must be expanded. Although the long-term stability of a system

of government can never be guaranteed, certain factors point to the advisability of a shift toward Mexico as a more prominent supplier of critically needed US petroleum. The historical roots of oil relations between the United States and Mexico, the overall long-term stability of bilateral relations between the two nations, and the potential for their continued stability create the basis for US consideration of a policy of greatly expanded and strengthened oil ties with Mexico.

(U) Mexico is not in a position to replace Middle East Oil suppliers but, on the basis of politics, geography, and overall mutual economic and strategic benefits, it is a supply source which merits closer examination. Mexico is currently the world's fourth largest producer of crude oil and possesses proven reserves in quantity second only to Saudi Arabia. As a traditional supplier of oil to the US and a nation which enjoys relative political stability--particularly in its relations with the United States--Mexico could become a significant factor in US strategic energy planning. And, in the case of Mexico, the risks of dependence and concomitant vulnerability would be lessened by the mutuality of the benefits based on such a relationship. Mexico's current financial crisis, although partially caused by the downturn in the world oil market, is also dependent on oil for its resolution. Thus the dependence implied in increased US reliance on Mexican oil supplies would be offset by the dependence of Mexican economic recovery on increased oil revenues. Such interdependence would lessen the risks for both sides.

(U) Mexico as a source of imported oil stands apart from the Middle East suppliers for many reasons. Its stability, its geographic proximity to the US and the volume and quality of its oil reserves all add up to an attractive alternate to near-total dependence on Middle East oil suppliers. Mexico's current financial crisis offers the United States an opportunity to develop a strong interdependent relationship with Mexico which could serve the national interests of both countries. Furthermore, the economic strengthening of Mexico could do more than ensure continued political stability in that country; it could concurrently strengthen the US position within the hemisphere, particularly in the now volatile Caribbean region.

(U) Although the ultimate size of the petroleum resources which Mexico possesses will be important to that nation's long-term economic planning, it is already sufficiently large and sufficiently well-documented to support an increase in oil production. Mexico's current reserves-to-production ratio remains conservative by international standards and could be considerably increased, based on current proven reserves alone. Such an increase requires only the firm decision to proceed, but that decision hinges on both internal and external economic factors. Although Mexico's domestic petroleum needs have been projected at only about 2 million barrels per day by the late 1980s [3], making any significant production increase contingent on petroleum export policy decisions, those decisions will have a noticeable impact on internal Mexican socio-economic conditions and will have to be considered in light of their potential to improve--rather than exacerbate--current economic difficulties.

(U) Despite the risk that the accelerated development of Mexico's oil resources could exacerbate current economic problems and the criticism that such a pace will serve only to deplete the nation's main natural resource, there do not appear to be other viable alternatives. Most Mexican officials recognize that the risk must be taken. Oil--with all its potential for creating further ills--is the answer for Mexico. Despite understandable reluctance to becoming a single-export economy, the exploitation of Mexico's petroleum resources will be necessary--at least over the short run--to provide funding for diversification of the economy through industrial development, export promotion, and revived agricultural output. What does all of this mean to the United States? Can--and should--Mexico's oil potential have an effect on US oil supplies in particular and on US energy security in general? There are several reasons why Mexican crude oil discoveries are of interest to US policymakers, not the least of which is their potential for alleviating several pressures on the security of US supplies.

P.L. 86-36

SOLUTION TO NSA-CROSTIC No. 52

"Education in Diagnosis," by [redacted] *NSA Technical Journal, Vol. XIV, No. 1, Winter 1969, and quoted in Ars Conjectandi: The Fundamentals of Cryptodiagnosis, by Lambros D. Callimahos, 1970.*

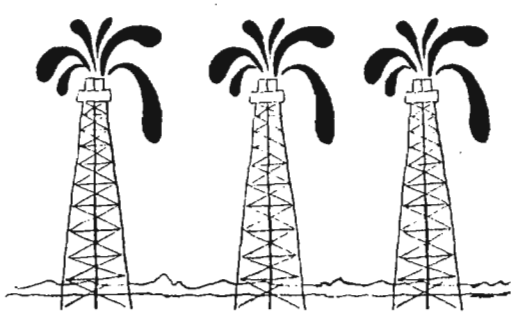
"In brief, the task of the diagnostician consists of collecting and organizing available material, searching for and recognizing phenomena, building up hypotheses and making every effort to knock them down again."

DOCID: 4019700

(U) One of the most fortuitous aspects of Mexican petroleum is its quality. Mexico is one of the few sources of light to intermediate grades of crude oil at a time when world supplies of these grades are subject to production restrictions, especially by OPEC member nations. US refineries need and can use Mexican oil, and Mexico is willing to sell it at world market prices. Mexican crudes also contain a low percentage of sulfur, another technical characteristic which makes them attractive to US refiners. In addition, the geographic proximity of Mexican oilfields makes international transport of Mexican crude less expensive and more secure than oil from other sources.

(U) Thus, in view of the US need to acquire more secure sources of crude oil and Mexico's desire to achieve economic stability and growth, the development of a strong, interdependent "special relationship" between the two countries could go a long way toward helping each to achieve its national goals. With a focus on the energy security and economic development issues in an atmosphere of cooperative interdependence, many of the problems between the two nations--trade, finance, undocumented workers, and the like--could enjoy a higher probability of resolution.

(U) By shifting oil supply emphasis away from the Middle East and toward a more stable, dependable supplier in the Western Hemisphere, the United states could greatly enhance the security of its petroleum supplies. A further US decision to speed up the fill rate of the US Strategic Petroleum Reserve (SPR)--relying on long-term Mexican oil supply contracts rather than spot market purchases--would buy additional insurance against energy supply disruption during the upcoming decades of transition to alternative fuels. Active encouragement of Mexico's oil development program--by means of a long-term increased quantity purchase agreement--or passive assistance--using advance payments for oil or bridge financing to ease Mexico's current liquidity crisis--could be sufficient incentive for Mexico to accelerate the exploitation of its petroleum resources.



(U) For Mexico's part, a conscious decision to hasten its exploration for and exploitation of its most valuable natural resource. within a calculated blueprint for socio-economic development, will help to ensure the attainment of modernization.

(U) An analysis of past disruptions of threats to cutbacks of US oil supplies leads to the conclusion that

> "only diplomatic/economic efforts which are in the national interests of oil producers will accomplish the [US] goal of oil security."[4]

The United states must be willing to admit that this gives oil producers the ability to create alliances that further their own national goals, but not that this inherently gives producing nations the upper hand in supply relationships. US policymakers can, and should, exploit the self-interests of oil-exporting nations by creating an interdependent environment in which both producer and consumer interests are served. One way in which this can be accomplished is through the establishment of a special relationship with Mexico.

(U) Some political theorists will argue that in today's complex, interrelated world system, the concept of special relationships is outmoded. They contend that the United States must take a global approach to foreign policy issues. Although this argument is not without merit as it pertains to such issues as defense, its applicability to energy security it not as fitting. Surely the global implications of energy supply are, and should be, of paramount concern to the US Government, but the encouragement of special oil supply relationships can enhance, rather than detract from, the overall security of world supply not only by diminishing US vulnerability, but also by easing the growing worldwide competition for Middle East oil.

(U) For the United States, increased oil purchases from Mexico would

- [] reduce dependence on OPEC;
- [] lessen the probability of precipitous price increases because of the already strong interdependence of the two nations' economies; and
- [] facilitate the transition to alternate energy sources by providing "insurance" during the period of passage.

But perhaps the most important reason increased Mexican production and export would

enhance the security of supply worldwide lies in its psychological value. "The OPEC countries are well aware that Mexico has huge petroleum reserves which are growing rapidly as exploration continues. The mere knowledge that there is a growing new petroleum source seems likely to reduce the power of the other oil exporters to influence the West with implicit threat of an oil embargo."[5]

(U) The principal result of increased US dependence on Mexico as a source of imported oil would be reduction of its reliance on Middle East oil. In addition to serving US national energy security interests, such a shift could also enhance worldwide availability of oil by decreasing the impact of US involvement in the anticipated intense competition in the 1980s among West European nations and Japan--and possibly even the USSR [6]--for access to Middle East oil.

(U) Furthermore, diminished US presence in and dependence on Middle East oil-producing nations need not imply a diminished concern for security of the region. Not only would the US continue to work toward achieving peace in the Middle East out of basic concern for the overall goal of worldwide peace and stability, but also because the supply security of its West European and Japanese allies hinges on the security of the region. In fact, decreased US reliance on Middle East oil supplies could enhance the credibility of US peace initiatives in the region by deflecting the charges of "self-interest" and "ulterior motives" often leveled by Arab spokesmen.

(U) It becomes increasingly clear that Mexico could--and probably should--become an important source of oil imported by the US in the coming years. But it must be remembered that even the immensity of recent Mexican oil discoveries will only postpone by a decade or so the inevitable era of oil scarcity. Nonetheless, those discoveries can "buy consuming nations the time needed to curb their growing appetites for oil and to make less disruptive the conversion to more abundant energy sources."[7]

(U) Energy security, particularly during the upcoming period of transition to renewable sources, will require a balance of power between the oil-exporting nations and the US. The pursuit of a special oil supply relationship with Mexico is a step toward creating that balance of power, both by reducing Middle East influence over US policy through decreased imports (and, hence, decreased vulnerability) and by enhancing hemispheric stability through the creation of a mutually beneficial interdependent relationship.

NOTES

1. Energy Requirements and Security, Report by the Combined Energy Staff, International Energy Agency, Organization for Economic Cooperation and Development; Paris: n.n., May 1983, p. 29.

2. Ibid., p. 2.

3. Richard B. Mancke, Mexican Oil and Natural Gas: Political, Strategic and Economic Implications; New York: Praeger, 1979, p. 61.

4. Edward J. Laurance, "An Assessment of the Arms-for-Oil Strategy," in Energy and National Security, ed. Donald J. Goldstein; Washington: National Defense University Press, 1981, p. 89.

P.L. 86-36

5. Mancke, op. cit., p. 128.

6. Some analysts, [redacted] predict that because of the diminishing production capability and lack of advanced recovery technology, the USSR will become a net importer of oil in the 1980s.

7. Senator Frank Church, Foreword to Congressional Research Service's Mexico's Oil and Gas Policy: An Analysis; Washington: Government Printing Office, 1979, p. v.

OCID: 4019700

GOLDEN OLDIE [U]

During his debriefing after World War II, Wilhelm Fenner, Ministerialrat of the Signals Intelligence Agency of the High Command, German Armed Forces (OKW/Chi), was asked whether publication of decrypts between the wars had any effect on German cryptology. This was his answer. Extracted from TICOM/I-206, dated 7 August, 1947. This is classified ~~TOP SECRET HVCCO~~ in its entirety.

Publication of VNs [decrypts] was strictly forbidden. Each VN was classified as Secret (Geheime Kommandosache) and enjoyed the highest security protection. It was forbidden to mention VNs and decipherment outside of the office and inside only with those personally known, not with unknown officers and officials, so called visitors who came in on one pretext or another. Every serious cryptologist knows the consequences of publication of a VN. When Ambassador Page published the Zimmerman despatches after World War I, Chi used these to prove how important exact decipherment is and how important it is that every cryptographic system be tested before being put into use. And Page's publication was worth more than a whole series of lectures! [1]

Once when an English correspondent obtained knowledge in AA [Foreign Office] of an Italian VN deciphered by Chi and published it in a Manchester paper, including an error in decipherment, this Italian system was replaced and Ambassador Amadori (who, as Fenner recalls, was then in Riga) was likewise replaced.

In general the rule was that publication of all sources 25 years after an important event is as soon as it will serve the truth. Earlier may be very intriguing but there will be so many decent people involved, people who have erred not from bad motives but solely from human inadequacy, that it is better to maintain silence and wait. (For this reason there was still no exact story of certain events of World War I).

When the French Intelligence Service learned that Chi was working successfully on French diplomatic ciphers, this information alone was enough to induce the Quay d'Orsay to replace certain ciphers sooner than was its wont. Thus not only every publication but de facto every rumor, represents a danger for one's cryptologic work, the purpose of which is not lust for sensation but promotion of the security of the country one serves, with means which one prefers to employ when dynamite and acetylene torch would draw too much public attention, and would endanger it without bringing the slightest gain.

---

1. The publication of the Room 40 crypt solution of the Zimmerman telegram in 1924 was followed by German comsec changes.

P.L. 86-36

SUICIDE SHELL(u)

P.L. 86-36

by [redacted]

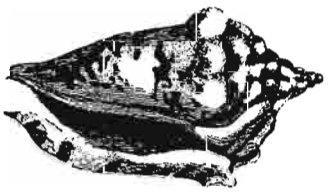
Some years ago, somebody came up with a little box that would shut itself off. The box had an ON/OFF switch on the front; when you turned it on, the lid slowly raised up and an arm came out, turned the switch off, and silently withdrew back into the box.

You can make a shell file do more or less the same thing: turn itself off. I call such a file a suicide file, and you can make one by putting in as the last line:

```
rm shellfile
```

The file will dutifully take all the actions you have listed and, like the little box, as the last action, remove itself from the current directory.

I find a lot of uses for this feature. Suppose I have a directory full of pieces of my work and I want to divide the files into two groups and put one of those groups into another directory. In the example below, the directory 'part1' contains files from sect1.* and sect2.* and I want to set up all the sect2.* files in another directory called part2. Using the UNIX line editor 'ed' and a "suicide" shell file called 'junk', the following dialogue illustrates how the shell is created that moves the files and then disappears.



```
% pwd
/u6/wes/demo/part1
% ls -l
-rw-r-----  1 wes     2462 Apr 17 16:11 sect1.1
-rw-------  1 wes     2842 Apr 17 16:11 sect1.2
-rw-rw----  1 wes     2336 Apr 17 16:11 sect1.3
-rw-r-----  1 wes     4510 Apr 17 16:11 sect1.4
-rw-------  1 wes     1024 Apr 17 16:11 sect1.5
-rw-r-----  1 wes     2026 Apr 17 16:11 sect1.6
-rw-r-----  1 wes     3762 Apr 17 16:08 sect2.1
-rw-------  1 wes     4274 Apr 17 16:08 sect2.2
-rw-rw----  1 wes     3455 Apr 17 16:08 sect2.3
-rw-r-----  1 wes     7011 Apr 17 16:08 sect2.4
-rw-------  1 wes     1168 Apr 17 16:08 sect2.5
total 77
% cd ..
% ls -l
drwxr-xr-x  2 wes      256 Apr 17 16:11 part1
total 1
% mkdir part2
% ls -l
drwxr-xr-x  2 wes      256 Apr 17 16:11 part1
drwxr-xr-x  2 wes      112 Apr 17 16:14 part2
total 2
% cd part1
% ls sect2* > junk
% ed junk
40
5>1:
  1 sect2.1
  2 sect2.2
  3 sect2.3
  4 sect2.4
  5 sect2.5
5>1,$s/^.*$/mv & ../part2/
5>1:
  1 mv sect2.1 ../part2
  2 mv sect2.2 ../part2
  3 mv sect2.3 ../part2
  4 mv sect2.4 ../part2
  5 mv sect2.5 ../part2
```

DOCID: 4019700


```
5>a
rm junk
.
6>1:
  1 mv sect2.1 ../part2
  2 mv sect2.2 ../part2
  3 mv sect2.3 ../part2
  4 mv sect2.4 ../part2
  5 mv sect2.5 ../part2
  6 rm junk
6>f
junk
6>w
108
6>q
% sh junk
% ls -l
-rw-r-----  1 wes    2462 Apr 17 16:11 sect1.1
-rw-------  1 wes    2842 Apr 17 16:11 sect1.2
-rw-rw----  1 wes    2336 Apr 17 16:11 sect1.3
-rw-r-----  1 wes    4510 Apr 17 16:11 sect1.4
-rw-------  1 wes    1024 Apr 17 16:11 sect1.5
-rw-r-----  1 wes    2026 Apr 17 16:11 sect1.6
total 35
% cd ..
% ls -lx
drwxr-xr-x  2 wes     256 Apr 17 16:15 part1
-rw-r-----  1 wes    2462 Apr 17 16:11   sect1.1
-rw-------  1 wes    2842 Apr 17 16:11   sect1.2
-rw-rw----  1 wes    2336 Apr 17 16:11   sect1.3
-rw-r-----  1 wes    4510 Apr 17 16:11   sect1.4
-rw-------  1 wes    1024 Apr 17 16:11   sect1.5
-rw-r-----  1 wes    2026 Apr 17 16:11   sect1.6
drwxr-xr-x  2 wes     112 Apr 17 16:15 part2
-rw-r-----  1 wes    3762 Apr 17 16:15   sect2.1
-rw-------  1 wes    4274 Apr 17 16:15   sect2.2
-rw-rw----  1 wes    3455 Apr 17 16:15   sect2.3
-rw-r-----  1 wes    7011 Apr 17 16:15   sect2.4
-rw-------  1 wes    1168 Apr 17 16:15   sect2.5
total 82
%
```

To get us oriented, we begin with 'pwd' to print the working directory. The answer tells us we are in my account 'wes' (a part of filesystem u6) and that within my directory 'demo' we are in a subdirectory called part1. The long form listing of the directory (ls -l) gives us a lot of information, but here we are mostly interested in seeing that we have two groups of files, one called sect1.x and the other called sect2.x .

The command cd .. changes the directory to '..' which is the one above the current one; in other words, move "up" to 'demo'. There is only one subdirectory in demo: part1. We then make a new directory called 'part2' and then change directory back down to part1 where we will begin to build the shell to move the sect2.x files.

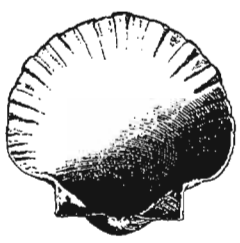
We begin by using 'ls' (the short form this time since we only want the file names) to give us every filename that begins with 'sect2' followed by anything (or nothing), and this list of file names is put into a new file called junk. The line editor 'ed' is then called with the new file and after first looking at the contents (1:), the following line creates the file we want using the ed substitute (s) command. A loose translation of that line would be:

1. From the first (1) to the last ($) line;
2. Substitute on each line...
   a. From the beginning of the line (^);
   b. Including every character (.*);
   c. To the end of the line ($);
3. The following replacement:
   a. The UNIX command for file move (mv);
   b. The entire original line (&);
   c. The string '../part2'

The new directory is called '../part2' because to get to it from where we are (in part1), we must first go up one level (to '..') and then back down to 'part2'. We now review what the file looks like (1:) and it consists of five separate move commands. To keep things tidy, we add the suicide line using the append command and once again review the file.

At this point, the shell file is ready to run, but I try to remember to verify what the file name is before leaving, partly to insure that the suicide line will throw away the correct file. All the work we have done in the editor is still in a temporary file; the original version of junk still resides as it was before we entered the editor. The write command sends the current version of junk off to replace the old, and we can then leave the editor with the quit command.

The only thing left to do now is to execute the suicide shell (no pun intended) and then look at the results to be sure we did what we wanted to do.



DOCID: 4019700

EO 1.4.(c)
P.L. 86-36

[redacted]

by [redacted]

B DSO, Kunia, Hawaii

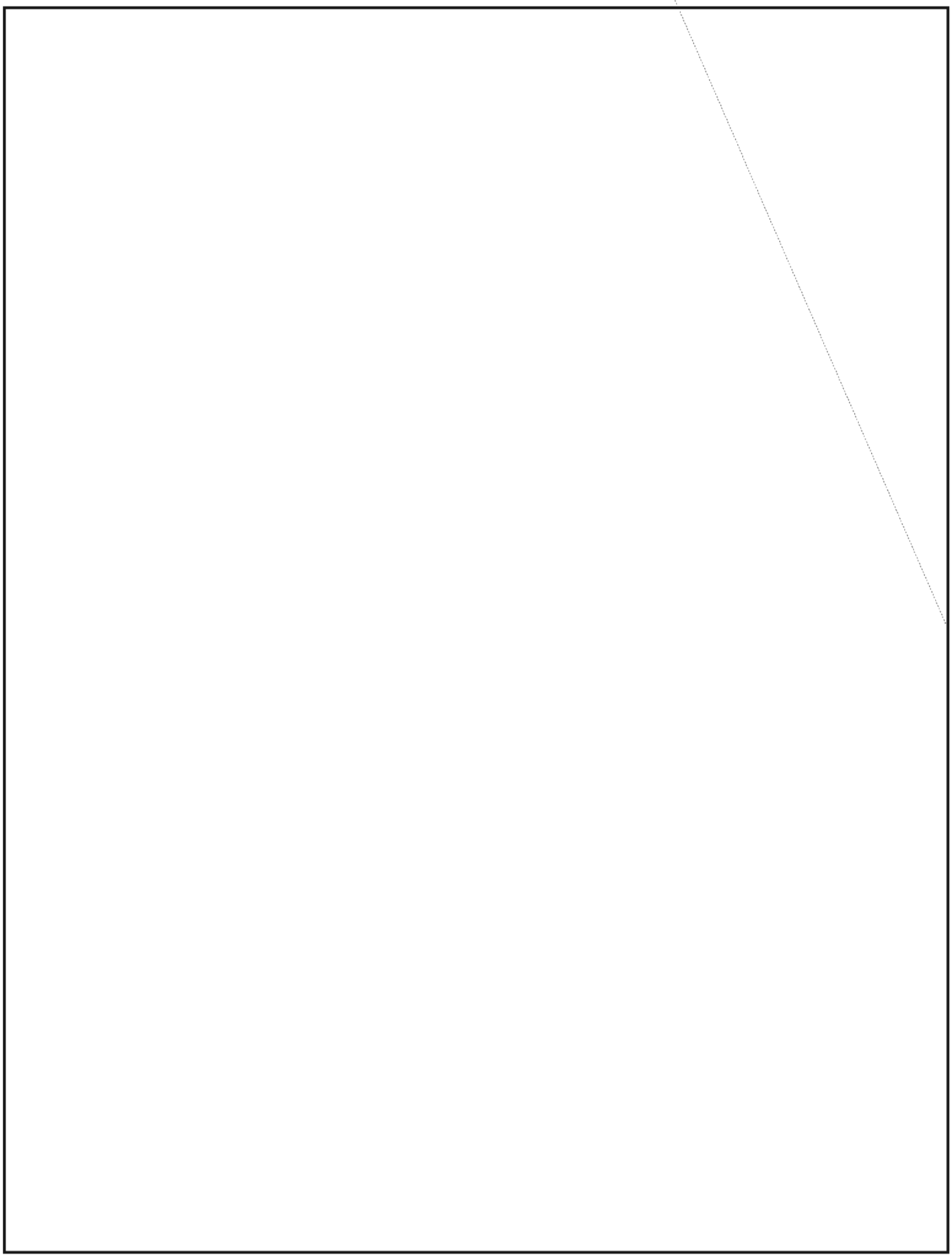
[redacted]

P.L. 86-36

[redacted]

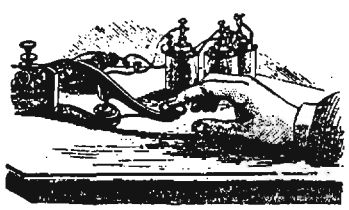
EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

Answers to
N-U-M-E-R-O-L-O-G-Y Quiz ~~(C-CCO)~~
(previous issue)



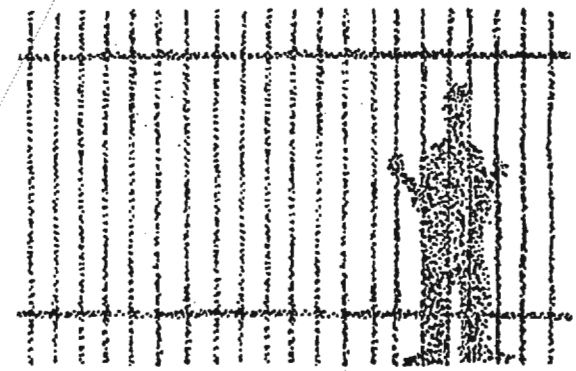
EO 1.4.(c)
P.L. 86-36

by jre

EO 1.4.(c)
P.L. 86-36

DOCID: 4019700

EO 1.4.(c)
P.L. 86-36



On 22 March 1984, the Director declassified the following documents:

[] Military Cryptanalytics, Part I (Monoalphabetic Substitution Systems), by William F. Friedman and Lambros D. Callimahos, published by NSA in 1956.

[] Military Cryptanalytics, Part II (Periodic Polyalphabetic Substitutuion Systems), by Lambros D. Callimahos and William F. Friedman, published by NSA in 1959.

[] The Friedman Lectures on Cryptology, published by the National Cryptologic School in 1965.

Also declassified are Military Cryptanalysis, Part I (Monoalphabetic Substitution Systems) and Part II (Periodic Polyalphabetic Substitutuion Systems), by William F. Friedman, published by the Government Printing Office in 1938.

Anyone holding copies of these books should send them or bring them to T541 (Cryptologic Archives), SAB 2, Door 3, at Fort Meade. They will be given a declassification marking and will be returned to the holder. In case of large holdings of the books, arrangements may be made for us to come to you. Please call the Archives on 972-2268.

SOLUTION TO NSA-CROSTIC No. 54

"The Things They Say." by Doris Miller, KEYWORD, August 1968, and reprinted in CRYPTOLOG, November 1976.

"'I know it doesn't make sense, but that's what it says!' This is the granddaddy of them all, the [great] classic disclaimer...the most spontaneous, universal, and irrepressible outcry in the translating world. [Surely,] there is no one in the business who hasn't given tongue to it at some time."

WE ARE ALWAYS LOOKING FOR

ARTICLES, COMMENTS, NOTES, LETTERS,

THAT WOULD BE OF INTEREST TO OUR READERS

DOCID: 4019700

I SPY à la Moscow:

A Soviet View of US Intelligence Activities (U)

by [redacted]

P.L. 86-36

(U) In the wake of the attempted assassination of Pope John Paul II, the Soviet Union became the target in the Western press of allegations that it was the ultimate source of international terrorism. To counter these allegations, the Soviet Union has resorted not only to its periodical press, but also to popular fiction to reach those segments of its population that do not follow Pravda or Izvestia as closely as the Communist Party of the Soviet Union (CPSU) might like. In May 1983 Molodaia Gvardiia, the official publishing house of the Young Communists' League (Komsomol), brought out what they termed "a political detective novel" entitled Project Valhalla[1]. By using the style and format of a detective novel, the Soviets undoubtedly hope to gain wider acceptance of the views presented in the novel. For the average Soviet citizen, the novel, which is based on "actual recent events" [128], should have a very high degree of credibility, especially since the view of the Central Intelligence Agency (CIA) presented in the novel is well supported by an American film, "Three Days of the Condor,"[2] which is currently being shown in the Soviet Union[3].

"There is no need for propaganda to be rich in intellectual content."
--Joseph Goebbels

(U) The novel depicts the machinations of an international, ultra-rightist, anti-Communist, neo-Nazi group, the "Brown Front," which is attempting to "return" to power in Germany, Italy, Japan, and Spain. The theme of resurgent Nazi power strikes an especially responsive chord in the Soviet Union, where World War II is written about as if it ended only yesterday. Every year scores of new books about the War are published in the USSR. Articles about the War are commonplace in the periodical press. Russian schoolchildren to this day stand guard at the tombs of the war dead, the number of which (20,000,000) the Soviets continually cite as proof that they suffered more than anyone else at the hands of the Germans during WWII. Even Soviet page-a-day calendars carry a warning against resurgent Nazi power. The page for 23 November 1983 cautions that:

> The assertions of the West German authorities that the scope of the criminal activities of neo-Nazi forces has expanded dangerously and that it is time to put a stop to them remain just so much noise[4].

(U) In the scenario laid out by the author, the Soviet Union is merely the innocent victim of the ruthless anti-Soviet campaign. The Brown Front, which is made up of Nazi war criminals and their now grown offspring, is gaining support among the masses who believe that "without a strong hand (at the helm) the rule of order will disintegrate" [103]. Since "the masses only respect and acknowledge strength and decisiveness" [103], these are the qualities that the Brown Front demonstrates in its campaign of political terror. The Brown Front is "successfully organizing terrorist acts in Italy and West Germany pretending to be leftists" [88]. "There are more than 20 fascist terrorist groups operating in Italy" [90], where "the Marxists have become far too numerous" [103].

DOCID: 4019700

(U) The Brown Front has, with the complicity of the CIA and the assistance of the Republic of South Africa, established a research institute in an unnamed South American country to develop its own atomic weapon. The code name for this project is Valhalla. They plan to use the weapon as "a sort of atomic terror" [103] to blackmail the government of the Federal Republic of Germany into political concessions or, should that prove impractical, to send the weapon into the Soviet bloc aboard an American aircraft and detonate it. "After all, siccing Moscow on Washington wouldn't be bad (for us) either" [104].

(U) As the book closes, the President's National Security Adviser states at a press conference: "A report prepared by the Central Intelligence Agency contains substantial evidence of the involvement of one of the great powers in terrorist acts in Europe" [123]. In spite of the fact that the "leftist press, armed with the facts, had begun reporting on the political terrorism being spread by the neo-Nazis" [122], the Western press reported the Security Adviser's statement in banner headlines such as

SOVIET UNION ENCOURAGES TERRORISM

and

RUSSIANS BEHIND KILLINGS
IN GERMANY AND ITALY [124].

(U) Riding on the wave of excitement surrounding this announcement, the President of the United States "asked Congress to allocate supplementary funds to combat international terrorism and to strengthen the Rapid Deployment Force" [124]. The author thus implies that it is the United States, not the Soviet Union, that is responsible for international terrorism and that the US is conducting a disinformation campaign in the press against the Soviet Union in order to cover up the covert (i.e., terrorism) and gain support for the overt (i.e., the RDF) arms of its foreign policy.

(U) In the course of developing his story, the author paints an interesting picture of how the Soviets perceive--or would like their citizens to perceive--the motives behind and the methods used in American covert intelligence operations. The Director of Central Intelligence is depicted as a political appointee:

> not a professional intelligence officer, (who) sharply felt his lack of expertise. He tried to compensate for his lack of experience through diligence, attention to detail, and hard work. [9]

> (He) was a newcomer to the administration and, unlike the other appointees, always took the President's comments too much to heart. His friends had tried to talk him out of the post, predicting some serious unpleasantries, but he hadn't listened to them. He understood, however, that any failure on the part of the Agency would mean the end of his career. [10, 11]

The Director was resentful of not being able to deal with the President directly, but having to go through the President's Security Adviser, Professor White who, prior to his appointment:

> had been one of the youngest professors at Princeton and the author of a dozen books on key international issues. The Director was almost as old as White but, in speaking with him, he clearly felt White's superiority. [10]

(U) In spite of his academic degree, Prof. White was "completely unacademic in his approach to politics" [86]. He made his decisions

> based not on the analyses presented to him by specialists but was guided by his intuition. ... His political Weltanschauung (was) defined by three things: a hatred of ideology; the dream of forming an international intellectual elite which would rule the world of the future; and hostility toward the Soviet Union. [86]

(U) In the eyes of the author, the real power at CIA was not the Director but his deputy, Edward Malcolm, a professional intelligence officer who

> ... had served in the Directorate of Plans for 25 years and covert operations were his forte. ... Therefore his appointment to the post of Deputy Director was seen as an attempt by Washington to emphasize not the passive collection of intelligence information, but rather the active interference in the course of world events. [39]

In a statement to the Senate Select Committee on Intelligence at a closed-door session, Malcolm "swore to make the maximum effort to 'stabilize' the world, beginning with Western Europe." [39]

(U) Malcolm made it clear that he felt that "political measures alone would not correct the situation" [92] in Western Europe.

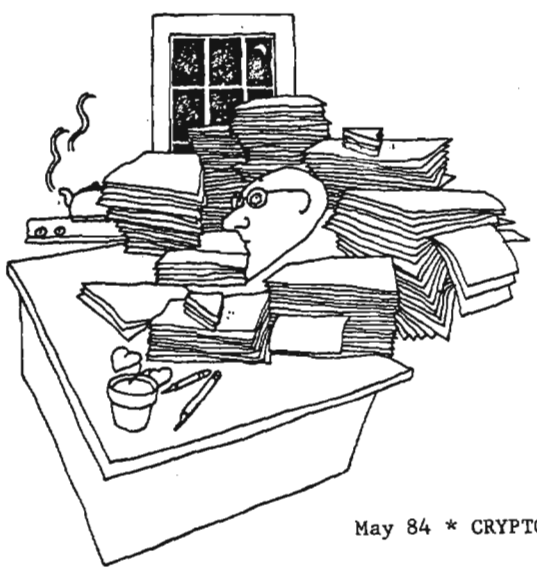
DOCID: 4019700

> In the late forties and early fifties American secret services, using every possible method from bribes to blackmail, managed to remove the Communists from the governments of France and Italy and to push these countries into the "cold war." As a consequence, the CIA was able to achieve some successes.
>
> However, in the last few years CIA operations for "stabilizing" Western Europe had been unsuccessful. Besides that, Washington has more and more often demanded the active support of the Western European capitals in its anti-Soviet strategy. [93]

Malcolm, therefore, believed that "well worked-out, coordinated covert operations in Western Europe" [93] were necessary and ordered a standard operating plan drawn up to outline the "principles and methods of action for correcting the political course of this or that country" [93]. Since the plan was to be presented for White House approval, he also instructed that counterarguments for any possible criticism of the plan be prepared:

> Interference in the internal affairs of a sovereign power is illegal and immoral, but almost everybody does it. Besides that, every country has the right to use force in its own defense. Our actions against Communist intrigues are justified as the defense of our forward positions. Therefore, our actions are moral and necessary. [93]

(U) Malcolm was the personification of the rift between the collection and analysis of intelligence information and active covert operations. He "hated analyzing intelligence data and compiling memoranda and reports" [39]. The Directorate of Plans, of which Malcolm had so long been a part, was the part of the CIA that



> ... conducted subversive operations. The overseas residencies, which were subordinate to the Deputy Director of Intelligence, looked askance at the people who did the dirty work. The poorly concealed dislike that the two services had for one another made their members keep track of the actions of the other with suspicion. Since the orders of Edward Malcolm, the Deputy Director of CIA for Plans, were carried out by the overseas residencies with some reluctance, in the countries that interested it the Directorate of Plans had created small groups of its own which were only formally subordinate to the resident. [25-26]

(U) The theme of the need to give preference to active measures over the passive collection of intelligence is echoed in the book by James Jackson, Malcolm's assistant, who says:

> "We get in a stack of paper everyday that you couldn't read in a month. It's those who were failures as college professors and were seduced into our line of work by the adventure who think that intelligence is the compilation of fat reports that present a dozen different possibilities with an equal number of proofs for all of them. Just take your pick! It's this defective approach that's paralyzing the political decision-making process. Intelligence is supposed to provide clear-cut answers to the questions. The world is becoming unsettled, and on various parts of the globe events are taking place that we have no control over. You already know the results: the United States is retreating under the pressure of world Communism and is losing influence in areas of the world vital to our national interests.
>
> "We don't want to waste our forces ... on crisis management. Our goal should be the formation of a future which is built on our value system. The process of selecting policies capable of influencing events on a global scale should be an ongoing one, based on thorough analysis, timely planning, and carefully considered decisions. I'm talking about the difference between active and passive policies, between the ability to influence the course of events and just attempts to react to the events. We have to overcome the problems before they overcome us. If you like, it's the difference between the academic approach of the people in the Directorate of Intelligence, trying to make sense out of what's happening, and the activities of our department, trying to make events work for us." [26-27]

(U) This is exactly the reasoning advanced in "Three Days of the Condor" by Cliff Robertson, portraying Deputy Director Higgins of the CIA's New York Center when he defends the renegade operation to invade the Middle East that was being planned by the Deputy Director for Mideast Operations:

> The fact is there was nothing wrong with the plan. Oh, the plan would have worked. ... It's simple economics. Today it's oil, right? In 10 or 15 years--food, plutonium. Maybe even sooner. Now what do you think the people are going to want us to do then? ... Not now! Then! Ask 'em when they're running out. Ask 'em when there's no heat in their homes and they're cold. Ask 'em when their engines stop. Ask 'em when people who've never known hunger start going hungry. You want to know something? They won't want us to ask 'em. They'll just want us to get it for 'em.

The fact that this is an American movie lends a great deal of credence to the perceptions of American motives and methods described in the book. For those readers who did not manage to see the movie, the recent invasion of Grenada will certainly make the book's emphasis on active measures to achieve political goals more credible.

(U) In addition to providing verbal portraits of the elite of the US intelligence community, the author of Project Valhalla also sketches US intelligence operations overseas.

(U) In Spain the CIA considered its main goal to be:

> "1) to hinder the Communists in the country from improving their position;
>
> "2) to bring Spain into NATO; and
>
> "3) to help the rightists to power." [43]

(U) In Madrid the local CIA residency was housed on the seventh floor of the US embassy. There the 30 people assigned to the residency were carefully analyzing everything that was taking place in the country and evaluating the chances of success for the military coup that had begun with the seizure of the Spanish Parliament[5].

(U) The attempted coup in Spain appears to be the "actual recent events" [128] upon which the novel in partially based. This event received such wide coverage that it would be nearly impossible for the average Soviet reader not to have at least heard about it or about the subsequent entry of Spain into NATO[6]. The author plays on the Soviet citizen's tendency to discount the amount of truth in the press by showing a similar reaction on the part of Deputy Director Malcolm to the summary of press reports on the unsuccessful coup in his morning briefing. The press had reported that:

> Agents of the CIA had established strong ties with the young ultra-rightist officers who had created the Spanish Military Union, modeled after General Franco's underground organization which started the mutiny of 18 July 1936. ...
>
> The conspirators had met with an American Presidential Adviser ... (who) did not promise any concrete help to the conspirators but, at the same time, did not exclude the possibility of cooperation with them if the coup succeeded. ...
>
> Several Spanish journalists cooperating with the CIA, on instructions from Langley, had prepared special materials sharply criticizing the cabinet for its inability to rule the country, calling for the creation of a strong government, and praising the military. At the present time there are more than 40 journalists cooperating with the CIA. The CIA has at least one of its people at every influential newspaper, magazine, and radio station in the country. ...
>
> In order to ensure that the ultra-rightist Fascists would come to power, the CIA promised to place American troops stationed at Torrej'o''n de Ardos, 15 kilometers from Madrid, at the disposal of the conspirators. ...
>
> On the evening before the attempted overthrow, two American military transport ships with cargoes of arms and ammunitions for the conspirators, docked at a port not far from Valencia. [63, 64]

Malcolm was upset because an actual CIA operation had been uncovered by the press. He did not mind "the fabrications" about the ties with the Spanish Military Union or the journalists; after all, "everybody blames everything on the CIA these days" [64]. He was upset because American interest in the success of the coup and the arrival time and mission of the two transport ships had been leaked to the press.

(U) This approach shows the Soviet reader that, while perhaps not everything that appears in the press about the CIA is true, some of it is. This will in turn reinforce the reader's natural assumption that while not

everything in this book about the CIA is true, some of it must be.

(U) The CIA's final analysis of the events in Spain was not that the coup had been a total failure but rather that, even though it was unsuccessful, it would hasten the process of bringing Spain into NATO.

> Madrid would protect itself from another attempted coup on the part of the ultra-rightist military officers and at the same time curtsy to us. So the leak of information about our possibly being interested in the military's coming to power will only push Madrid toward rapprochement with us. [64]

(U) Rome is pictured as the center of the American telephone intercept system in Italy. Located at 153 Via Cristoforo Colombo under the guise of a NATO communications facility, the center provided the results of its 24-hour monitoring of the city's telephone network to several customers, including the CIA residency in Rome. [54] As a result of the intercept of a telephone call from a provincial police commissioner to one of his friends in Rome about the case he was investigating involving the terrorist organization called the "Militant Order of Mussolini" (the Italian branch of the Brown Front), the commissioner was removed not only from the case, but from the police force as well. [90]

(U) In Tokyo the CIA residency is pictured as having a close working relationship with the foreigners' department of the Tokyo police, the members of which the CIA pays well for "interesting information." [20] Besides the residency, Tokyo also has a special group from the Directorate of Plans, which is housed separately from the residency on the 15th floor of the Hotel Asahi [25]. The CIA further has the ability to monitor the telephone calls of selected individuals in at least Kyoto and Nagoya [76]. In spite of the considerable emphasis the author places on active measures, the only task accomplished by these CIA activities is the collection of information on the "Movement for a Greater Japan," the Japanese branch of the Brown Front.

(U) In the book, the CIA also controls an airline called Central Aviation Transport Agency, the abbreviation for which, CA, sounds "almost like CIA" [28]. Pilots for CA were all ex-air force officers who had been kicked out of the service for one reason or another. They trained together "on the farm" [29] with regular air force pilots from the "weather service squadron" [29], who were in fact spy plane pilots. CA planes flew from USAF bases all over the world delivering arms to insurgents in Laos or intervening wherever necessary. Of course, the facet of CA's activities given the most coverage in the book was its covert shipments to the Brown Front laboratory in Latin America [28, 29].

(U) One of the key subplots in the story is the detection by the US intelligence satellite Orion of a the Brown Front's first nuclear bomb.

> Intelligence satellites had long ago become part of the routine of the Agency. Every year two or three behemoths filled with expensive equipment would be launched from an air force base in California. Traveling at 18,000 miles per hour, the satellites circled the globe once every hour and a half taking pictures of objects that interested the agency during every orbit. Urgent photographs were transmitted to the ground immediately in much the same way that television signals are relayed; the remainder of the pictures were ejected and returned to earth in a special canister. When it entered the earth's atmosphere, a parachute would open, slowing its fall. The canister would be caught in midair by a special air force unit stationed in Hawaii or would be fished out of the water. [7]

(U) The author points out that the most interesting thing about Orion's detection of the detonation was that Orion was not where it was supposed to be. "It had been launched more than ten years ago and over the years its navigational equipment had become defective so that it follows an unpredictable orbit" [7] Because the area in which the detonation took place was not one that the Agency normally took imagery of, it was only "by accident" [7] that the detonation was detected.

(U) As the story progresses, it becomes clear that a passenger liner "which had strayed from its course" [116] was destroyed by the test of the Brown Front's nuclear weapon.

> The detonation could have been delayed, giving the ship a chance to leave the area, but the residents of the (Brown Front) Institute were in a hurry to find out if Project Valhalla was successful. The fate of 150 people did not disturb them. [116]

(U) Nor was the fate of those people of much consequence to the CIA agent whose job it was to exploit the Brown Front. Rather than exposing the Front to the world when he found out that they were the ones responsible for the loss of the ship, he decided to sidetrack the investigation of the nuclear detonation detected by the wayward Orion satellite to the Directorate of Plans to ensure that knowledge of the real reason for the ship's loss would remain a secret. His knowledge of the Brown Front's culpability would provide him with extra leverage to extract "additional services" [102] from the Brown Front for the CIA.

(U) When it eventually became necessary for Prof. White to suppress his investigation of the nuclear detonation, he gave Deputy Director Malcolm a severe reprimand. In dressing down Malcolm, White noted that this whole affair with the bomb had been just plain madness, and much too adventurous. "But, in principle, the ideas that (Malcolm) was developing appealed (to White). The ideas, but not their execution." [124] James Jackson, on the other hand, who had been directly responsible for operations with the Brown Front, was forced to leave the Agency. But that was really only a slap on the wrist, as he was simply moved to a position with Boeing.

(U) While Western society was aghast at the Soviet Union's allegations that the United States had sent Korean Airlines flight 007 over Soviet airspace on a spying mission "with the knowledge that there might be, and perhaps the hope that there would be, a loss of human life,"[7] the scenario presented in Project Valhalla, which was written well over a year before the KAL 007 incident,[8] clearly shows that the Soviets believed the United States capable of at least condoning the loss of 150 innocent lives as the price to be paid for a covert operation that went wrong.

(U) Since an action of this kind on the part of the United States cannot be supported by any prior similar action, it is reasonable to look for the basis of Soviet belief in another area. The most logical alternative source is mirror imaging. That is, attributing to your opponent motives and actions which you yourself would take in a similar situation. In other words, the Soviets believe that we would risk the lives of innocent civilians in a covert intelligence operation because they would do so themselves. Indeed, mirror imaging should be considered as a possible source for all the methods and motives attributed to US intelligence activities in this book. The perceived need for the US to undertake covert action in Western Europe may be easily viewed as a Soviet interpretation of the US response to its problems in Western Europe based on the Soviet experience in Eastern Europe. The view of the US's desire to support rightist terror in order to bring about a favorable change of government or policy may be seen as the mirror image of the USSR's desire to support leftist terror in Western Europe. That the CIA would be assigned the task of bringing a non-member state into NATO to strengthen it is the mirror image of the KGB's being asked to break a member state (Greece)[9] away from NATO to weaken the alliance.

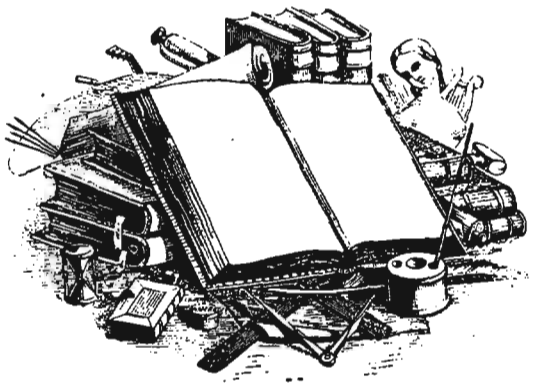
(U) As a propaganda piece, Project Valhalla is a success. It shows the United States as a declining world power that is forced to take active measures to shore up its faltering position of power. The US's slide from power is pictured indirectly in the description of its ten-year-old satellite that only discovered a nuclear blast "by accident" [7] and directly in the "quotes" from members of the US intelligence elite: "In the forties and fifties ... the CIA was able to achieve some successes" [93] but now "the United States is retreating under the pressure of world Communism and losing influence in the areas of the world vital to our national interests" [27].

(U) The targets of the US's active measures are, of course, the Communists. This is explicitly stated in a number of places in the book. One of the CIA's goals in Spain is "to hinder the Communists in the country from improving their position" [43]. The ultimate US goal, however, is "the formation of a future which is built on our value system" [27]. If the President's National Security Adviser has his way, it would be a future ruled by "an international intellectual elite" [86]. In isolation, the Security Adviser's desire is similar to the Marxist-Leninist vision of the future, but the Security Adviser's "unacademic" approach to politics and "hatred of ideology" [86] are antithetical to the "scientifically" founded Marxist theory which has, in the Soviet Union, produced a completely ideological state. Then, as if this were insufficient, the author adds that one of the cornerstones of the Security Adviser's Weltanschauung is "hostility towards the Soviet Union" [86].

(U) The United States is pronounced guilty by association of using Fascist methods in the active measures it takes. By associating the US with the Brown Front, the book hopes to

achieve transference of the fear and hate that the Russian people feel for Nazi Germany into a much more real threat to the Soviet Union: the United States. The Soviet leadership fondly remembers the days when the populace was united behind the government in the defense of the homeland during World War II (which they call "The Great Patriotic War") and would like to have that kind of support that kind of support again. Silencing domestic opposition by uniting the "people against an external enemy" would allow the Soviets to present a unified front to the world without the embarrassment of domestic opposition. Such a united front would make Soviet propaganda directed at the rest of the world (especially the Communist and potentially Communist portions of it) more credible and would make it easier for the Soviets to fend off Western allegations of impropriety.

(U) This book alone will not achieve Soviet goals, but as an old proverb says, "A journey of a thousand miles begins with but a single step." Project Valhalla is therefore of interest as an indication of the direction[10] in which the CPSU wants popular perceptions of US covert intelligence activities to develop.



P.L. 86-36

SOLUTION TO NSA-CROSTIC No. 53

"Topical Reporting," by [redacted] *CRYPTOLOG, October 1983.*

"Identify the areas of primary concern among military thinkers and planners at the present time. This practice has its hazards, though. The tendency in any field of endeavor, but especially in military circles, is to grab a "hot topic" and run with it."

NOTES

1. Mlechin, L. I., Proekt "Val'khalla": Povest' (Project "Valhalla": a novel), Molodaia Gvardiia, Moscow, 1983. Quotes from this novel will appear in this article, followed by the page number in square brackets, [ ].

2. "Three Days of the Condor," Paramount Pictures, 1975, starring Robert Redford, Faye Dunaway, and Cliff Robertson.

3. Dobs, Michael, "Fascination, Hostility Color Soviet View of US," The Washington Post, 23 October 1983, pp. A1, A25.

4. 1983 Otryvnoj kalendar' (1983 page-a-day calendar), Politizdat, Moscow.

5. On 23 February 1981 Lieutenant Colonel Antonio Tejero Molina led a group of Spanish Civil Guards in the seizure of the lower house of the Spanish Parliament just as it was completing a vote to approve Spain's new government.

6. Spain entered NATO officially on 30 May 1982.

7. Marshal of the Soviet Union Nikolaj V. Ogarkov, Izvestia, 10 October 1983.

8. The novel was released to the typesetter on 25 November 1982 [128].

9. During the time period covered by the "actual recent events" [128] described in the book, the question of whether or not Greece would remain a member of NATO was a major issue in the Greek elections. Also of note during this time frame were Soviet accusations that the West was trying to break Poland away from the Warsaw Pact.

10. Another recent Soviet spy novel Letnaia pogoda (Flying Weather) by Sergei Abramov, Moskovskii Rabochii, Moscow, 1983, describes CIA operations inside the Soviet Union. It also associates the CIA with the Nazis and Nazi methods.

~~FOR OFFICIAL USE ONLY~~

NSA-Crostic #55

Here's the puzzle that answers the question: What would be the world's dullest ball game if cricket hadn't been invented?

A. AL team whose ballpark used to be called Briggs Stadium (2 wds)

B. This AL team used to be based in Philadelphia (2 wds)

C. English meadow where King John granted the Magna Carta (1215)

D. Prosperous, well-off (colloq.; 3 wds)

E. Brother or sister; blood relation

F. After one year as the Seattle Pilots, this team moved in 1970 to its present location (2 wds)

G. Either, other (Brit. dial.)

H. Team formerly located in the only US city having three major leagues baseball teams at the same time (3 wds)

I. Restrict; confine; circumscribe

J. Ancient city of Ionia

K. Inflammation or pain in muscles or joints

L. Gratuities

M. NL team, formerly the Colt '45s (2 wds)

N. Wields the blue pencil

O. 1951 movie in which James Arness played the title role (2 wds)

P. Greeting for a tan bovine (2 wds)

Q. ____ of Court; small hotels

R. Pecan; bolt partner

84 19 29 166 209 225 13 62 190 50

116 125 81

103 199 2 120 38 12 55 33 139 27

135 167 170 90 83 152

126 112 144 157 142 91 10 54 174

6 122 25 146 108 14 178 151 130 59

200 182 187

97 82 153 159 52 188 16 92 206 23

117 213 31 127 141 111

124 7 185 49 93

168 4 220 75 207 158 22 78 227 11

58 215 163 211 17 173 194

67 143 222 133 184

181 102 95 172 118 24 30

129 32 192 110 65 119 155 85 80 226

217 156 128 99

198 179 212 86 105 137 113 150 189 41

51 9 131

96 123 175 224 44

26 196 64 34 42 1 20 203

63 109 5 201 98 195

216 183 177 176

180 165 208

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

S. See Word T

$\overline{72}\ \overline{35}\ \overline{66}\ \overline{3}\ \overline{219}\ \overline{40}$

T. Crosswordist's favorite Mel Ott played with this team before it moved to the west (2 wds foll. by Word S)

$\overline{21}\ \overline{79}\ \overline{53}\ \overline{61}\ \overline{161}\ \overline{28}\ \overline{104}\ \overline{87}\ \overline{43}\ \overline{164}\ \overline{140}\ \overline{221}$

U. Palindromic Vietnamese holiday

$\overline{214}\ \overline{186}\ \overline{76}$

V. Member of an African tribe

$\overline{171}\ \overline{60}\ \overline{47}\ \overline{145}\ \overline{136}\ \overline{107}\ \overline{69}\ \overline{197}\ \overline{148}$

W. The Icelandic letter ð

$\overline{74}\ \overline{57}\ \overline{70}$

X. Jewish rabbinical seminary

$\overline{169}\ \overline{71}\ \overline{37}\ \overline{48}\ \overline{45}\ \overline{205}\ \overline{121}$

Y. They play in Busch Memorial Stadium (3 wds)

$\overline{18}\ \overline{100}\ \overline{68}\ \overline{160}\ \overline{138}\ \overline{204}\ \overline{132}\ \overline{77}\ \overline{15}\ \overline{149}$

$\overline{8}\ \overline{114}\ \overline{191}\ \overline{218}\ \overline{88}\ \overline{101}$

Z. Formerly, the Boston Bees (2 wds)

$\overline{89}\ \overline{202}\ \overline{162}\ \overline{56}\ \overline{210}\ \overline{94}\ \overline{154}\ \overline{134}\ \overline{73}\ \overline{106}$

$\overline{115}\ \overline{223}\ \overline{193}$

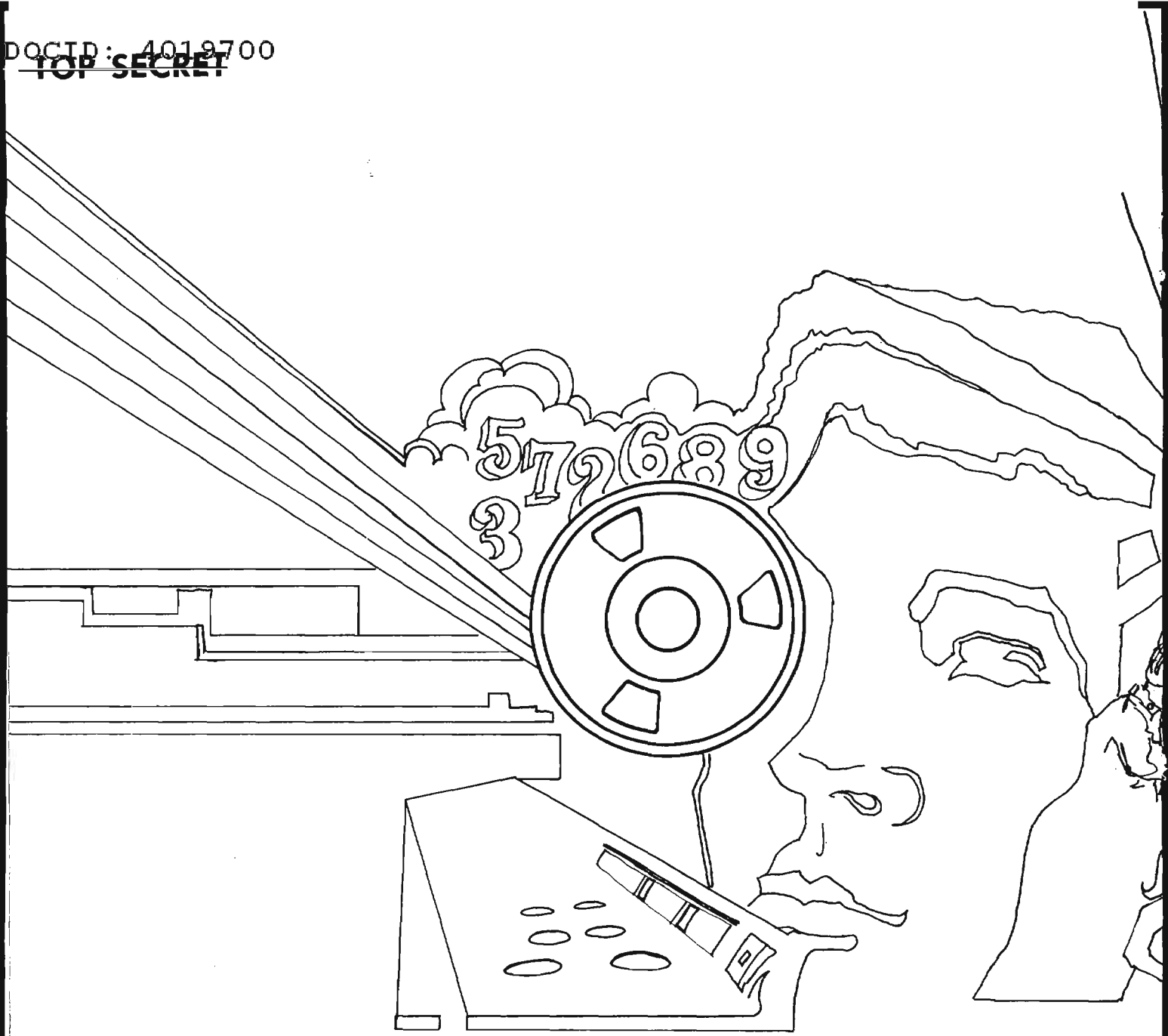
a. Yeast (arch., var.)

$\overline{39}\ \overline{147}\ \overline{46}\ \overline{36}$

■	■	■	■	1 O	■	2 B	3 S	4 H	5 P	■	6 D	7 G	■	8 Y	9 M	10 C	11 H	12 B
13 A	■	14 D	15 Y	16 F	17 H	■	18 Y	19 A	20 O	21 T	22 H	■	23 F	24 J	25 D	■	26 O	27 B
28 T	29 A	30 J	■	31 F	32 K	33 B	34 O	■	35 S	36 a	■	37 X	38 B	39 a	40 S	■	41 M	42 O
43 T	44 N	■	45 X	46 a	■	47 V	48 X	49 G	■	50 A	51 M	52 F	53 T	54 C	55 B	56 Z	57 W	58 H
59 D	■	60 V	61 T	■	62 A	63 P	64 O	65 K	■	66 S	67 I	68 Y	■	69 V	70 W	71 X	■	72 S
73 Z	74 W	75 H	76 U	■	77 Y	78 H	79 T	80 K	81 A	82 F	83 B	■	84 A	85 K	86 M	87 T	88 Y	89 Z
90 B	91 C	92 F	93 G	■	94 Z	95 J	96 N	■	97 F	98 P	99 L	100 Y	■	101 Y	102 J	103 B	104 T	105 M
106 Z	107 V	108 D	109 P	110 K	111 F	■	112 C	113 M	114 Y	115 Z	116 A	117 F	118 J	119 K	120 B	■	121 X	122 D
123 N	■	124 G	125 A	126 C	127 F	128 L	129 K	130 D	131 M	132 Y	133 I	134 Z	135 B	136 V	■	137 M	138 Y	139 B
140 T	141 F	142 C	■	143 I	144 C	■	145 V	146 D	147 a	■	148 V	149 Y	150 M	151 D	152 B	153 F	154 Z	155 K
156 L	157 C	158 H	■	159 F	160 Y	161 T	162 Z	163 H	■	164 T	165 R	166 A	167 B	168 H	169 X	■	170 B	171 V
172 J	173 H	174 C	■	175 N	176 Q	■	177 Q	178 D	■	179 M	180 R	181 J	■	182 E	183 Q	■	184 I	185 G
186 U	■	187 E	188 F	189 M	190 A	191 Y	192 K	193 Z	194 H	■	195 P	196 O	197 V	■	198 M	199 B	200 E	201 P
202 Z	■	203 O	204 Y	205 X	206 F	207 H	■	208 R	209 A	210 Z	211 H	212 M	213 F	■	214 U	215 H	■	216 Q
217 L	■	218 Y	219 S	■	220 H	221 T	222 I	223 Z	■	224 N	225 A	226 K	227 H	d_{hw}	■	■	■	■

P1-July 84-S3-53931

~~FOR OFFICIAL USE ONLY~~


5726893

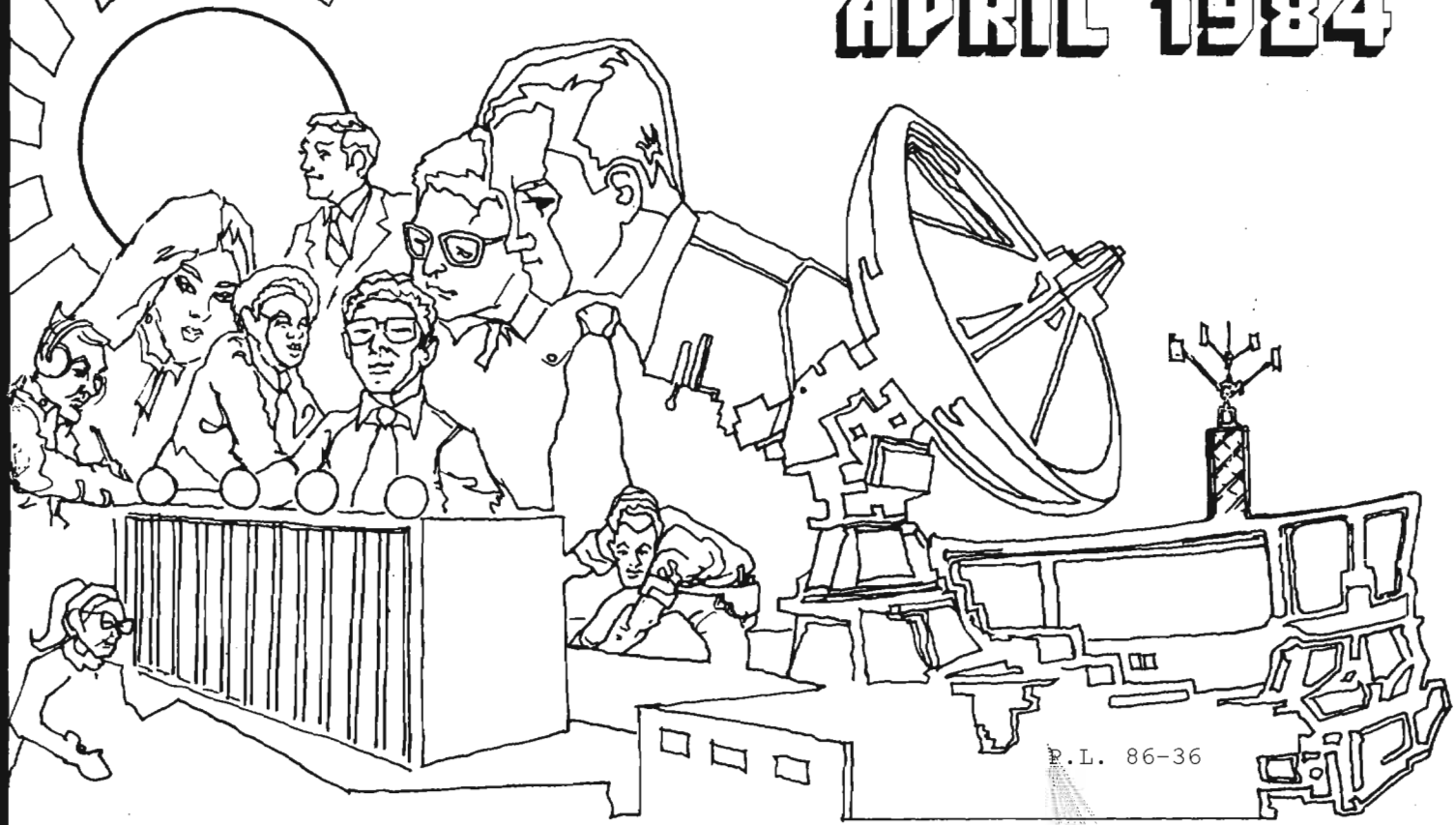
OCID: 4009898

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

APRIL 1984



P.L. 86-36

OIL AND DEVELOPMENT:
EFFECTS ON NIGERIAN ECONOMY (U)..... [redacted] 1
ARMS CONTROL IN THE WAKE OF KAL 007 (U)..... [redacted] 7
GOLDEN OLDIE (U).....10
RESERVATIONS ABOUT THE MBTI (U)..... [redacted] 11
NUMEROLOGY (U)..... [redacted] 12
THE STAFF IN TODAY'S BUREAUCRACIES (U)..... [redacted] 13
THE MAGDEBURG INCIDENT (U)..... [redacted] 18
THE POSITION OF NSA/CSS
IN THE US GOVERNMENT (U)..... [redacted] 22
DO YOU KNOW THE DIFFERENCE? (U)..... [redacted] 26
NSA-CROSTIC NO. 54 (U).....David H. Williams.....28

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009898

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XI, No. 4 APRIL 1984

Editorial

P.L. 86-36

PUBLISHER [redacted]

BOARD OF EDITORS

Editor..... [redacted] (963-3045s)
Asst. Editor... [redacted] (963-1103s)
Production..... [redacted] (963-3369s)

Collection..... [redacted] (963-3961s)
Computer Security
..... [redacted] (859-6044)
Cryptolinguistics. [redacted] (963-1103s)
Data Systems..... [redacted] (963-4953s)
Information Science
..... [redacted] (963-5711s)
Mathematics..... [redacted] (968-8518s)
Puzzles.....David H. Williams (963-1103s)
Special Research.....Vera R. Filby (968-7119s)
Traffic Analysis..Robert J. Hanyok (968-8418s)

For subscriptions
send name and organization
to: [redacted] P14

To submit articles or letters
by mail, to: P1, Cryptolog

via PLATFORM mail, send to:
cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no 'O' in 'log')

P.L. 86-36

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

DOCID: 4009898

OIL and DEVELOPMENT: Effects on Nigerian Economy (U)

by [redacted] S041

P.L. 86-36

I. INTRODUCTION

(U) Since 1974 the significance of petroleum has become increasingly more apparent to developed and developing nations alike. The phenomenal rise in the international market price of crude oil, which began to grow in geometric proportion following the 1973 Arab oil embargo against the United States, has heightened the awareness on the part of individuals and nations of the power of oil as a political and economic weapon. Industrialized and non-oil-producing developing nations suffered the shock waves of OPEC[1] price hikes beginning in 1974--and many have yet to recover. Some oil-producing nations, on the other hand, have until recently experienced the economic "boom" of increased national revenues and expanding international prestige.

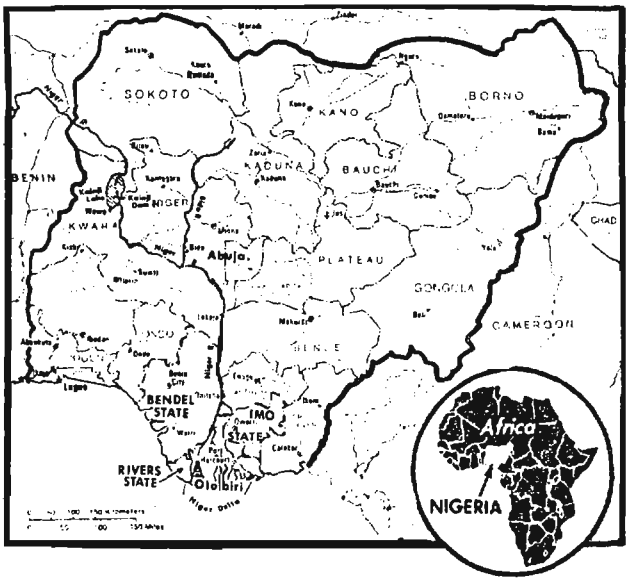
(U) The current oil glut and resultant "soft" market for crude, however, is beginning to reverse that trend. Though economic recovery is not on the horizon for many non-oil-producers as a result of the increased availability and lower prices of petroleum, the opposite is true for some of the oil-producing nations. The sudden decrease in oil is causing slowdowns--and, in some cases, stoppages--of ambitious national development plans predicated on constant or increasing oil revenues.

(U) A case in point is Nigeria. Oil--Nigeria's most significant revenue-producing resource--has in recent years become the backbone of that nation's economy. As of mid-1982, exports of Nigerian crude oil accounted for 90 percent of the country's foreign exchange earnings and approximately 80 percent of government revenues.

(U) This paper was awarded First Prize in the 1983 Essay Contest of the International Affairs Institute.

(U) Oil had transformed Nigeria from a developing country whose economy was constantly "in the red" (pre-1966) into a nation enjoying large surpluses--until lately. Oil revenues have become the most significant factor in Nigeria's economy--both in the positive and in the negative sense. For the trend toward ever-increasing reliance on oil revenues to finance national development plans, which seemed to be a logical course of action in the mid-1970s, is now confronting the vagaries of the international crude oil market, making future oil revenues unpredictable at best.

(U) This paper will attempt to sketch the history of petroleum as a facet of the Nigerian economy, its effects on national development plans, and the impact of the fluctuating international crude oil market on the implementation of Nigeria's projected development program.



II. GENERAL HISTORY

(U) Although Nigeria has been producing oil in sufficient quantity for export since 1948 and has only been a member of OPEC since 1971--interest in oil and earnest exploration efforts date back to 1937, when geological and geophysical investigations were first conducted by Shell-British Petroleum (Shell-BP). The search for oil in Nigeria actually began in 1908 but was abandoned shortly afterwards. Efforts were revived by Shell-BP in 1937 and drilling operations commenced in 1951. Nigeria's first commercially productive oilfield was discovered in 1956 at Oloibiri in the Niger delta. Production levels grew gradually, and Nigeria's first export of crude oil took place in 1958 from the newly constructed port and terminal facilities at Port Harcourt.

(U) Petroleum rapidly became Nigeria's principal and most lucrative export, and by 1965 foreign exchange earnings eclipsed those from cocoa, formerly its leading export commodity. During the period from 1957 to the start of the Nigerian civil war (1967), 176 oil deposits were identified and over 600 wells were drilled--with a success rate of nearly 70%. Shell-BP's exploitation efforts focused primarily on what was formerly known as the Eastern region of Nigeria, and onshore oil production grew rapidly until the civil war brought it to a virtual standstill. By 1966 production had reached 20.7 million tons and petroleum exports constituted 33 percent of Nigeria's total exports. Foreign exchange earnings from these exports continued to rise from that point on (after a brief hiatus during the civil war), and since 1973 oil export earnings have accounted for 90 percent of Nigeria's total export revenues.[2] Much of this can be traced to the rising price of petroleum on the world market since 1974, rather than to significant increases in export volumes.

(U) As of 1981, there were approximately 140 producing oilfields both onshore and offshore. Mot are located in the Niger delta region, primarily in Bendel, Rivers, and Imo states. Estimates of Nigeria's total proven reserves range from 17.5 billion to 20 billion barrels. Exploration is being promoted in other parts of the country and promising new areas include the Anambra, Benue, Bida, Lake Chad, and Sokoto basins.

III. FOREIGN OWNERSHIP

(U) The issue of foreign ownership, and hence--from the perspective of a Third World developing nation--foreign control, played a part in the evolution of the oil industry in Nigeria. As noted earlier, Shell-BP was the dominant actor in the Nigerian oil sector both pre- and post-independence. As the colonial ruling power, Great Britain naturally bore the brunt of foreign investments in Nigeria, and the oil industry--the showcase of the Nigerian economy--was the most prominent example of "foreign domination." During the 1950s Shell-BP invested over $300 million in exploration, wells, pipelines, and a refinery--"a sum that represented 85 percent of all new foreign investment during the period and exceeded the total investment in [the] Nigerian manufacturing industry."[3] Such heavy foreign investment in the burgeoning oil sector can be viewed both positively and negatively.

(U) Surely the input of financial and technological resources in the early developmental stages helped to create an oil industry which is today a major factor in Nigeria's rapid development. The combination of Nigeria's precious natural resource and Britain's infusion of capital and technology formed a viable, productive industry which has helped to pave the way toward modernization of the Nigerian state.

(U) On the other hand, the growth of nationalism in Nigeria--and its emergence as a political factor after 1960--led to a sense of "foreign domination" of the nation's economy. The oil boom of the 1950s and 1960s left the Nigerian economy even more dependent on outside control than it had been before this

period. John Hatch goes so far as to state that

> "Oil revenues played an important part in the conflict leading to the civil war; it seemed probable that [the] Nigerian government would become increasingly dependent on the revenues gained from the oil companies, with all the consequences to national economic policy."[4]

(U) By 1971 Nigeria was the world's seventh largest producer of petroleum. In that year the nation joined OPEC. At the risk of oversimplification, these factors--growing nationalism, rising production and revenues, and association with other oil-producing nations in a commodity cartel--converged after a divisive civil war and resulted in the beginning of a Nigerian takeover of the oil industry.

IV. INDIGENIZATION

(U) After its bloody civil war, the Nigerian government, as part of its consolidation and rebuilding efforts, announced its desire to take over a controlling interest in the operations of the petroleum-producing companies in Nigeria.[5] The manner in which this was accomplished in no way resembled the abrupt "nationalizations" which occurred in some of the other Third World nations endowed with marketable natural resources, but rather was an expression of Nigeria's recognition of its own mineral wealth and its intention to exercise more control over its own natural resources.

(U) After the establishment of the Nigerian National Oil Company (NNOC) in 1971, and in a relatively orderly process of "indigenization," the Nigerian government began in 1973-74 to negotiate the gradual purchase of majority interest in the foreign oil companies. In 1977 the NNOC was replaced by the Nigerian National Petroleum Corporation (NNPC), which was granted broader powers regarding commercial activities in the petroleum sector. By mid-1979 NNPC had increased its holdings to 60 percent of all foreign oil operations.

(U) The only actual instance of "nationalization" of a foreign oil company took place in 1979. As a result of Nigeria's belief that Shell-BP was "supplying crude oil, by subterfuge, to South Africa in total contravention of Nigeria's stand against all dealings by international firms with that country,"[6] NNPC nationalized BP's 20 percent share of the producing organization and its 40 percent equity in the joint NNPC-BP marketing organization. Arrangements were later made to compensate BP, however, and other oil companies were assured that this action did not presage a wave of nationalizations "as long as the companies respected Nigerian policies and sensitivities."[7]

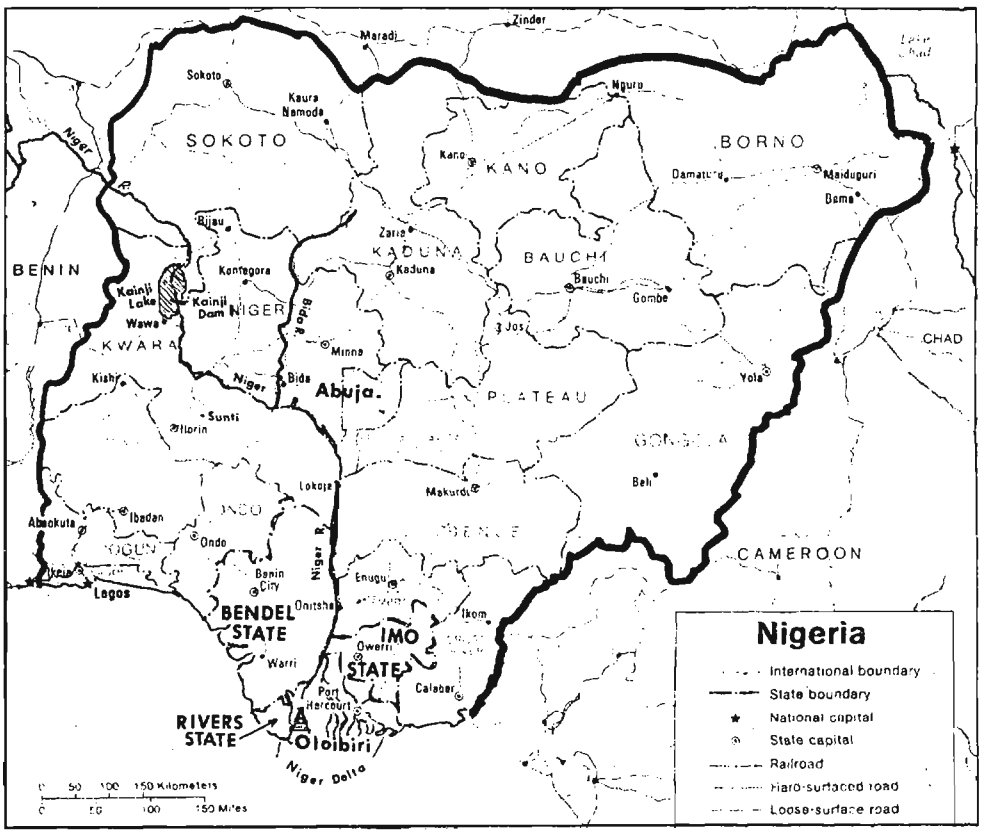
(U) Thus, despite one case of nationalization (which, from the Nigerian perspective, was politically justified), Nigeria peacefully regained control of its oil resources, avoiding the trauma and potential loss of technological and marketing expertise which could have occurred if more dramatic measures had been taken.

V. ROLE OF OIL IN DEVELOPMENT PLANNING

(U) Economic planning is not a recent phenomenon in Nigeria, though the effects of oil revenues on national plans are relatively new. Structured economic planning has a long history in Nigeria. The first 10-year development plan was adopted in 1946 and was supplanted in 1955 by a British-devised program which addressed each of Nigeria's (then) three regions separately. In 1960 the new independent Nigerian government inherited the colonial plan, deemed it fragmented and inappropriate, and replaced it in 1962 with the First National Development Plan (1962-68). Some large government-sponsored projects were completed under this program, including the country's first oil refinery, paper and sugar mills, and the Kainji Dam and hydroelectric station, but government revenues were at this point largely unaffected by the still-nascent oil industry.

(U) The Second National Development Plan (1970-74) was geared to the reconstruction of war-torn Nigeria. Despite some government investment, major setbacks in agricultural production during the first half of this planning period decreased output and caused the beginning of what are now chronic food deficits. The Second Plan was extended to cover FY 1974-75, during which time the monumental rise in world oil prices filled the Nigerian coffers.

(U) The nation's sudden increased wealth translated in the Third National Development Plan (1975-80) into a grandiose blueprint for accelerated national growth. The Third Plan set public investment levels at ₦26.5 billion (c. $40.3 billion), eleven times greater than the government's actual capital expenditures on the Second Plan. The focus of development spending was on transportation, heavy industry, and education. Agricultural expenditures were increased, but they were still inadequate to reinvigorate the sector. Among the successes of the Third Plan were an increase in cement-producing capacity, two new oil



refineries, port construction and expansion, new airports, power-generating facilities, and new industrial facilities.

VI. FOURTH (CURRENT) DEVELOPMENT PLAN (1981-84)

(U) Despite the fact that oil revenues had begun to decline before the conclusion of the Third Plan and that resource restraints postponed some programmed expenditures and curtailed others, Nigerian government officials expected to move deferred projects into the Fourth Development Plan. As recently as April 1982, the American Embassy in Lagos[8] outlined the major components of the Fourth Plan, which includes:

[] Expanded agricultural development;

[] Agribusiness, manufacturing, and infrastructure projects;

[] A multibillion-dollar new federal capital project at Abuja;

[] Construction of 2,000 housing units annually in each state of the federation;

[] Electricity generation, transmission, and distribution facilities; and

[] Federal medical centers in six states

(U) This expansive program is already running into difficulty as a result of the reduction in worldwide demand for oil which had caused Nigerian foreign exchange reserves to fall to an estimated $4 billion by early 1982. Clearly the continued slide of crude oil prices & decreased production production levels will demand at least deferral of many of Nigeria's economic and infrastructure development projects.

(U) Indications that the Fourth Plan will not be met began to appear in late 1982, when budget proposals for 1983 first became known.

VII. EFFECTS OF SLOWDOWN IN THE INTERNATIONAL OIL MARKET

(U) The glut of oil on the international market in the early 1980s was countered to a degree by OPEC's decision to impose production

DOCID: 4009898

ceilings on member nations in an attempt to tighten availability and thereby prop up slacking oil prices. Nations such as Nigeria reluctantly agreed, reasoning that this move would result in smaller revenue losses than would occur if production levels were maintained and prices plummeted. OPEC's efforts were undercut somewhat, however, by the non-OPEC oil-producing nations (e.g., Mexico, Great Britain, Norway), and world oil prices continued their gradual decline.

(U) The effects on Nigeria's economy in general, and on its infrastructure and industrial plans in particular, can be seen most clearly in the nation's budget statistics for 1982 and 1983.[9] The 1983 budget presented to the Nigerian National Assembly will be ₦9.3 billion (c. $13.5 billion), 20 percent lower than the figure presented in the previous year's budget projections. Of this figure, projected oil income will represent only about 59 percent of the nation's total revenues. In the years 1973-80, oil revenues accounted for 80 percent of government revenues.[10]

(U) At the same time President Shagari presented the 1983 budget proposal, he submitted to the National Assembly revised figures for 1982 which reflected a 37 percent drop in oil income by 1982.

(U) More than a third of Nigeria's budget covers recurrent expenditures which would be difficult to trim. Significant shifts will occur in order to accommodate reduced revenues and, in the more flexible capital portion of the national budget, heavy reliance will be placed on foreign borrowing (c. $5.5 billion). In view of Nigeria's current international current international debt of $15 billion[11], the nation's borrowing plans are optimistic.

(U) Nigeria's proposed 1983 capital expenditures represent only a 5 percent decrease from 1982 levels, despite an estimated oil revenue shortfall of 21 percent since 1981. The effects of reduced oil revenues on infrastructure and economic development plans are compounded by a projected threefold increase in defense spending for 1983. Although capital expenditures for agricultural projects in general will increase slightly, funding for the Nigerian Industrial Development Bank was cut by almost 80 percent, the allocations for the Sunti sugar project has been reduced 70 percent from the 1982 level, and the government's scheme to finance small-scale industries will be cut to less than 20 percent of its 1982 budget allocation.

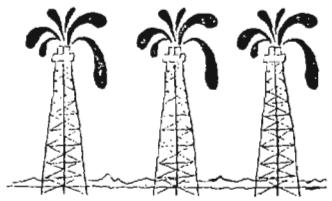
(U) Not all infrastructure expansion plans will suffer budget reductions. The transportation sector will investments for land, water, and air transport systems, but the 22 percent increase in this sector will be at the expense of other sectors of the economy (health, education, housing). Capital investments in the energy sector will also increase, but will focus on the development of the petrochemical industry and expansion of the Port Harcourt refinery, as opposed to investments in exploration and transport. In conjunction with this emphasis, the Nigerian government expects to achieve a significant increase (80 percent) in income from NNPC direct sales to oil lifted by the producing companies, indicating a planned move to cut supplies available to the producing companies and to increase NNPC's international marketing efforts.

VIII. OUTLOOK

(U) In view of the trend toward almost total reliance on foreign exchange earnings from oil to finance its national development plans--and a simultaneous neglect of its agricultural sector--Nigeria must now hope for a quick turnaround of the international oil market in order to fulfill its dreams of modernization. Government and industry analysts do not predict a firming up of the market in the immediate future, however, and according to the US State Department's assessment:

> Even assuming a pick-up in oil production ... the country still faces an estimated US $6 billion in short-term trade arrears to pay off, long-term debt servicing on the order of US $2 billion per year, and an annual food import bill of perhaps US $1.5 billion. In short, unless Nigeria's oil revenues increase to the US $8-10 billion range, there will be little discretionary income available for major new development projects and the purchase of raw materials and spare parts for industry will be constrained.[12]

(U) Based on both the negative prospects for a rapid recovery of the international oil market and the improbability of Nigerian success in the world's capital markets, the likelihood that the Fourth National Development Plan's goals will be met is minimal. For it is estimated that, even if oil revenues increase, they will not again reach the peak levels registered in 1979-80, making deferment of major portions of the Fourth Plan necessary. Many of the projects listed in the Plan have already been slowed down or suspended so that the scarce financial resources can be applied to the servicing of existing debts.



(U) For the short term, the pace of economic development in Nigeria will depend on the rate of recovery (from the nation's standpoint) of the international oil market and the willingness of banks and international lending institutions to extend their risks through further investment in the Nigerian economy. As the US Embassy, Lagos, states:

> The Nigerian economy is presently severely depressed and may experience significant changes. Nigeria's almost total dependence on oil as a source of income makes the country extremely vulnerable to shifts in world crude markets. The currently unsettled situation in those markets, coupled with Nigeria's precarious foreign reserves position and the tightness of world financial markets make the market prospect for Nigeria bleak in the short term.[13]

IX. CONCLUSIONS

(U) The main conclusion which must be drawn from the foregoing is that, despite thwarted attempts at industrial diversification, Nigeria is still overly reliant on oil--an unstable and uncontrollable revenue source--for development financing. It is likely that Lagos will weather the current storm, albeit through austerity measures and deferment of development goals, but longer-term economic planning for Nigeria must take a decided shift away from dependence on a single source of government revenues.

(U) At the same time, a more concerted effort must be launched to revitalize the country's agricultural sector. Heavy imports of foodstuffs continue to drain the nation's reserves, while a once agriculturally rich country expends billions of dollars to feed its populace. Nigeria must redouble its efforts, even during this current period of reduced revenues, to improve agricultural productivity. Achievement of self-sufficiency in this sector could ease the strain on financial resources and improve the overall balance-of-payments ledger for Nigeria.

(U) In all, it appears that austerity measures will alleviate the short-term financial crisis in Nigeria, but an overhaul of the nation's economic planning apparatus will be needed to ensure attainment of future national development goals.

NOTES

1. Organization of Petroleum Exporting Countries, a 13-member cartel of oil-producing nations established in 1960.
2. Provisional value figures for Nigerian exports for 1979 totaled some ₦10.7 billion. Of that total, petroleum export values accounted of ₦10.2 billion. Harold D. Nelson, ed., Nigeria: A Country Study (4th ed., Washington, DC: American University, Foreign Area Studies Division, 1982), p. 294. Exact currency conversion rates for the naira (₦) for 1979 are not available. As of 1983, however, ₦1 = US $1.45. At that rate, 1979 oil export values were over US $14.7 billion. State Department cable, Lagos, 11731-82 (171446Z Nov 82).
3. John, Hatch, Nigeria: The Seeds of Disaster (Chicago: Henry Regnery Company, 1970), p. 269.
4. Ibid., pp. 269-270.
5. Although Shell-BP dominated the field, other international firms were active in oil exploration and exploitation efforts in Nigeria from 1965 onward. For example, offshore exploration in the Okan field was undertaken by the Nigerian Gulf Oil Company in 1965. French, Italian, and other US firms were also active in commercial exploitation. See Nelson, op. cit.
6. Nigeria: A Country Study, p. 166.
7. Ibid., p. 167.
8. For a more detailed description of all the elements of the Fourth National Development Plan, see the State Department cables Lagos 02990-82 (070740Z Apr 82) and Lagos 02596-83 (011739Z Mar 83).
9. A detailed account of the Federal Government of Nigeria's 1983 budget proposal is contained in State Department cable Lagos 11731-82 (171446Z Nov 82).
10. (U) As of February 1984 Nigeria was producing 1.6 million barrels per day (b/d) of oil, which is 300,000 b/d over its OPEC quota. This excess production was being "permitted" informally by OPEC in order to help Nigeria with its massive debt problem and its severe foreign exchange deficit. It appears that the new government will again fall into the trap of reliance on oil production revenues to repay debts.
11. The Washington Post, May 15, 1983, p. F1, col. 1.
12. State Department cable Lagos 02596-83 (011739Z Mar 83).
13. ibid.

THE BEST HOPE STILL

Arms Control in the Wake of KAL 007(U)

by [redacted]

P.L. 86-36

(U) As I walked into my office one morning shortly after the shootdown of Korean Airlines flight 007, one of my coworkers, an army sergeant first class, looked at me with a devilish grin.

(U) "What do you think of the Soviets now?" he asked, gleam in his eyes.

(U) I sighed heavily but said nothing. I knew what he meant. The shootdown was a defenseless act and in his eyes I am a staunch defender of the Soviet Union. After all, hadn't I been the one who suggested that perhaps the Soviet Union is not responsible for all the acts of terrorism in the world? That maybe the United States is not altogether blameless in the ever-escalating arms race? Hadn't I also intimated that the Soviet Union may not be an "evil empire," but rather simply a cultural and political system alien to our own? That peace between our nations through negotiations, though a long and arduous task, might be possible? Yes, I had suggested each of these. And now, by one act, the Soviets had proven that I was wrong. Their crime against humanity was the final piece of evidence that would convict them of being, in the final analysis, a malevolent aggressor whose only interest is to amass power and territory regardless of the human cost. My helpless silence seemed to satisfy the sergeant, and the subject was dropped.

(U) Since then I have often considered this widely-held interpretation. Was the shootdown a calculated act by the Soviet government? Was it so reprehensible that all attempts at negotiating an end to the arms race and erstwhile "cold war" should be stopped? We may never know the answer to the first question, but the answer to the second is an emphatic "No!"

(U) Arms control is like a living, breathing organism. It is the result of a long, painful birth during the late 1960s and early 1970s. It has lived a very precarious life since then, almost constantly "on the brink," as the Soviets have attempted to strangle it to death at various times, while the US has simply hoped that it will die of neglect.

(U) It was, of course, the United States which initiated arms control over two decades ago. The "Hotline" agreement and the Limited Test Ban Treaty of 1963 were the first formal accords between the two superpowers. The US initiated them not for idealistic purposes but for pragmatic purposes: international security was becoming increasingly unstable due to the proliferation of nuclear weapons and own survival was at stake. The Soviet Union was equally pragmatic, accepting the accords as favorable to their own national interests. It would hardly be fair of us, after all, to expect them not to be predominantly concerned about themselves. This does not threaten our interests but is merely "business as usual" in political exchange. In 1967 President Johnson proposed a ban on ABM systems and the idea was summarily dismissed by Alexei Kosygin. Five years later, however, a treaty limiting ABMs was incorporated into the SALT I agreements. Thus had Soviet interests changed. And so does the arms control process continue on both sides. So negotiations have continued as negotiations will continue: at a snail's pace, changing only as perceived interests change. But the payoff began with the ratification of SALT I.

DOCID: 4009898

(U) In 1972 an arms control "contract" was signed by our two nations, the importance of which far exceeds the word of the agreements. Richard Nixon and Leonid Brezhnev did not only commit their nations to certain "counting rules" concerning nuclear missiles when the signed the SALT I Treaty, but they agreed to enter into a cooperative relationship to reduce the threat of world destruction. The relationship exists to this day. For even as the Soviets propagandize their opposition to the United States and President Reagan rails against the "evil empire," each side is careful to protect that relationship for fear of what might result if the contract is broken. Robert Kaiser of The Washington Post wrote in June 1983 that that contract is "the real measure of the danger of Soviet-American relations" and "despite the temperature of public rhetoric ... As long as it holds, we are not reverting to the bad old days, no matter what the atmospherics are like." That is why, despite the absence of a legal treaty, the conditions of the SALT II agreements are observed by both sides.

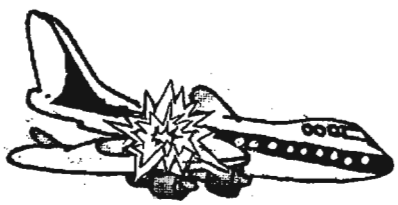
(U) So who benefits from this contractual relationship? Many people express concern that the contract favors the Soviet Union. In negotiations, the US seems to make concessions while the Soviets give up little. The Soviets continue to reject our proposals, make few "realistic" proposals of their own, and yet keep us on the defensive at the negotiating table. Why is this so? It is so because the Soviet nature, by its very nature, is a manipulative one. And, as maddening as that is for us to deal with, therein lies the road to agreement. We are people from antithetical systems. Friendship may be impossible. So be it! Distrust is a two-way street and just as we find their system incomprehensible, so do they find ours. Patt Derian, Assistant Secretary of State for Human Rights in the Carter Administration, wrote in The Washington Post on June 9, 1983:

> The longer both sides believe they are dealing with madmen, the likelier one will choose to go down fighting.

(U) By making an attempt to understand Russian history and culture, however, we can see that there is ample reason for their xenophobic paranoia. Our own political history and ideology, on the other hand, demonstrate that we can afford magnanimity. We can afford to be more flexible than the Soviets. Indeed, we can't afford not to be, since they will not be. If we are serious about arms control, we must accept this role. In the process, we will hope not to "change their ways"--which is a naive goal--but rather to draw them our of their paranoiac shell and into the world community. When we have accomplished this, we will have reached a milestone toward world peace. In the meantime, we all benefit from the fruits of arms control.

(U) But still we are confronted with the stark reality of Soviet foreign policy, which even to a discerning eye is the world's most aggressive. The invasions of Hungary and Czechoslovakia were defensible from a Soviet viewpoint, if hard to swallow for Americans whose ideals include the right of a people to choose their government. The Afghanistan invasion was more tenuous, harder to justify even from the Kremlin, but so far clearly a less "successful" one for them than previous incursions.

(U) There is no reasonable defense, however, nor is one forthcoming from Moscow, for the shootdown last summer of a commercial airliner. The "plane full of spies" story is hardly reasonable. Even the facts are sketchy.

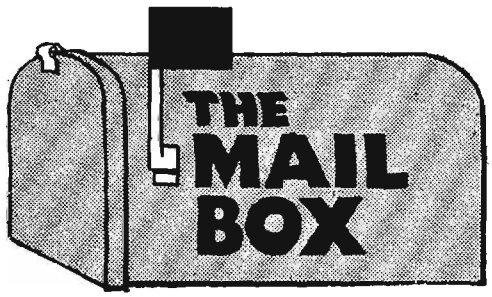


(U) At about 3:00 a.m. local time on 31 August 1983 Korean Airlines flight 007 had, for some still unknown reason, flown off course over the North Pacific Ocean near the USSR while flying from Anchorage, Alaska, to Seoul, South Korea. It flew into Soviet airspace, passing over the Kamchatka Peninsula. When it did that, it was in violation of international rules of law and aviation. Soviet fighter aircraft in the area did not intercept the 747, again for unknown reasons. The airliner proceeded on a southwesterly course over the sea of Okhotsk until it reached Sakhalin Island, where Soviet fighters reacted to it, intercepted it, and shot it down. The 747 fell into the Sea of Japan and 269 people were

dead. The world still wonders how such a tragedy could have happened.

[redacted]

(U) That night 269 people died. It was a tragedy, but equally tragic is the fact that many people believe that all hopes for arms control and world peace died also died that night. Many Americans are now prepared to abandon our attempts to deal peacefully with the Soviets, but deal with them we must. Although our initial reaction to the shootdown was rightly one of horror and outrage, we cannot allow the deaths of the 269 to be in vain by abandoning all prospects for arms control. If nothing else, let this tragedy awake us to what is really at stake. Although our nations as they exist today may never be able to live together completely free from discord, the opportunity to reduce the mutual feeling of threat between us and to bring security to the world through negotiation of our crucial common interest in arms control is still the best hope for world peace.



Subject: Article request P.L. 86-36
To: cryptolg at bar1c05

EO 1.4.(c)
P.L. 86-36

[redacted]

~~(C)~~ My name is [redacted] *and I'm the editor of F88's PROFESSIONAL ASSOCIATION NEWSLETTER. Our Professional Association is basically a chapter of the Agency's Collection Association and made up of the collectors and other personnel* [redacted] *I just read your December 1983 issue of the CRYPTOLOG and would like your permission to include* [redacted] *in our June issue.*

~~(C)~~ Our PROFESSIONAL ASSOCIATION NEWSLETTER is relatively new and, since F88 has a rather small field (pardon the expression) to draw on, articles can be hard to come by. We've published one issue (March) this year and plan one for June.

(U) Thank you for any assistance you can provide.

P.L. 86-36
EO 1.4.(c)

Regards,

[redacted]

P.L. 86-36

DOCID: 4009898

GOLDEN GLOBE (U)

This is an extract from "Problems of Code" by Colonel Marcel Givierge, French Army, which first appeared in the Signal Corps Bulletin No. 34, May 1926.

Now, it is very much to the interest of the cryptanalysts to learn the personal habits of the encoders. A division in the Chemin des Dames sector, in 1918, made it a practice to require of the regiments in the line a brief report every morning. Frequently the report was drawn up in this form: "Night calm, nothing to report." When the code book was changed, the routine practices did not change and the same text was the subject of numerous messages, which could be classified, thanks to their being encoded in exactly the same way. The capture of even an obsolete code book enabled the enemy to read cryptograms belonging to this daily series which were repeated and, even if these were dated some time back, this helped the specialists to make a hypothesis as to the meaning of groups in messages of a similar style, transmitted under similar conditions, and encoded with the new code book. Now almost always the great difficulty in studying code is the identification of a few first groups. This is what is called finding an entrance or getting a start. With an entrance effected, and a thousand groups, a number quickly acquired on the front during the last war, the cryptanalysts are full of hope in the success of their task. We have not found any statistics as to the number of telegrams in code collected in one day, but the days at the beginning of the war, or during the attacks of 1918, when the posts of the major units furnished us 60 messages are not rare, and many of these telegrams have more than 20 groups. What is to be said then of the transmissions of the small units?

The repetitions of formulas composed of the same words, placed in the texts at places known to cryptanalysts is therefore especially favorable for the latter in case the code book is changed. These are the formulas which have been called "stereotyped." We must include therein the forms: "I have the honor to ..."; short telegrams acknowledging receipt of communications or requesting repetition of untranslatable [undecipherable] telegrams; references such as "in continuation of telegram," "in reply to," "to follow"; too numerous indications of punctuation such as "Paragraph 2," "Paragraph 3," "end of message"; grammatical indications such as "three large (plural) man (plural)," etc. We have taken here as the subject of the article only field cryptograms, but it is known that the code section has always had good success in decoding diplomatic matter, in which, among others, distinction was achieved by Captain Bassières...and the reserve interpreter Déjardin....The studies in this branch were especially aided at the beginning by long service designations at the head of telegrams and by final formulas indicating the office of origin. The numbering was the basis of hypothesis which made possible the long-sought "entrance" into the first German code reconstructed--that for communications with submarines; and alternations of numbers in clear and numbers in code, assumed to be such because the text had no number in clear at that time, served as a point of departure of another code. ...

We have shown the danger of stereotyped formulas. Without using any formula of this kind, however, the text of telegrams contains numerous repetitions. We are not speaking only of frequent words, prepositions, or auxiliary verbs, for which various equivalents may be assigned in the code book, enabling us to employ now one group and now another, but of names of places, of units, etc., which in the course of an action will recur frequently in the dispatches. Encoded ordinarily by words or by syllables, these terms give rise to repetitions of groups which attract the attention of the cryptanalyst. The latter compares these series of groups of names on which it is possible to build hypotheses. In may cases, he secures in this way means of cross reference--for example, syllables common to several names appear in each series of groups. He then possesses an entering wedge.

DOCID: 4009898

RESERVATIONS about the MBTI (I)

by [redacted] P13

P.L. 86-36

[redacted] sent me the following brief admonitory comment on the Myers-Briggs Type Indicator, the personality inventory described in the November 1983 issue of CRYPTOLOG:

"I must admit that I have reservations about [the broad application of the MBTI to management]. I believe it reveals more about a person's private side than an employer needs to know. It also could be dangerous in the wrong hands.

"While I agree with Mary that working with highly compatible people is pleasant, it leads to a very narrow mindset called 'group think.' This can result in waste when the same old ideas/solutions are used repeatedly without questioning or searching for other possible alternatives because 'the group thinks it's a great idea.' I think everyone and every group needs a devil's advocate to spark creativity."

P.L. 86-36

I appreciate the interesting and provocative questions [redacted] has raised and the opportunity for further discussion of some points that were probably misleading in my article. I certainly agree wholeheartedly that every tool can be misused; in fact, every tool inevitably WILL be misused by a number of shortsighted businessmen and administrators trying to take ruthless shortcuts to profits, or trying to pare down their budgets. I feel, however, that the MBTI is considerably LESS likely to be abused in truly destructive ways than most other psychological instruments already current in both the private and public sectors. It is possible that a company might decide that it wanted only "ENTJs" at the upper management levels, "ESFJs" at middle and lower levels, and "INTJs" in the Accounting Department, for example. Instead of using the test as an INDICATOR, to give them data to be factored in with other data from interviews, resumes, their own experience, etc., the hiring decisionmakers in this hypothetical company might set up cutoff scores on the four type dimensions and refuse to hire anyone lacking the requisite patterns at or above those scoring levels. That would be an abuse of the MBTI, and a highly stupid one. Many companies have done just this with other tests, using them as rigid filters to rule out applicants scoring below a cutoff point on some supposedly desirable attribute, or above a cutoff on some supposedly undesirable one. Unfortunately, that kind of approach is an enduring temptation to human nature, since it looks like a shortcut to "efficiency." It will be with us throughout our stay on this planet. No tool or instrument that provides a score can be protected from that kind of unimaginative, brutal misuse. The MBTI is, I suspect, a bit less likely to be used this way, because it does not score substantive attributes such as specific job-related knowledge or skills.

P.L. 86-36

The point [redacted] raises about "group think" is a very interesting one. I believe that I may have misled some readers by my emphasis on the exercise we had at our seminar, where we were split into groups with similar types to perform a small task. This made a tremendous impression on me and I enjoyed it immensely, so I may have made it sound more

important than it was. I certainly didn't mean to imply that our instructor at the seminar was recommending that people of similar type must always work together in segregated groups! In fact, that's just the opposite of the thrust behind all the work of the MBTI's developers. The idea of the MBTI, as I understand it, is to learn about your own type, with its strengths and weaknesses, and to relate that insight to knowledge of other people's types, so that you can work well with all kinds and make the most of any mix you are in. A good manager should be able to use his understanding of all the types in his team in creative and constructive ways. Among those ways might very well be the seeding of task groups with carefully chosen "devil's advocates," just as [redacted] suggests. The MBTI can provide some valuable insights to help the manager choose the right person to stir up a particular group and spark their creativity. Our homogeneous groups at the seminar were just a device to demonstrate the nature of the types to us. Even at that, they were chosen to equate only two of the four type letters (my group were "SJs"), leaving two other dimensions free for wide variation. I think it is quite possible, as I write this, that I enjoyed working in such a homogeneous group because of my own type, which tends to like sameness, safety, structure, and predictability. Others at the seminar in other groups (for instance, "SPs") might have found the experience frustrating and stultifying because they are more likely to enjoy variety, social challenge, and surprises. The MBTI allows us to define and study these differences so that we can appreciate them and use them constructively.

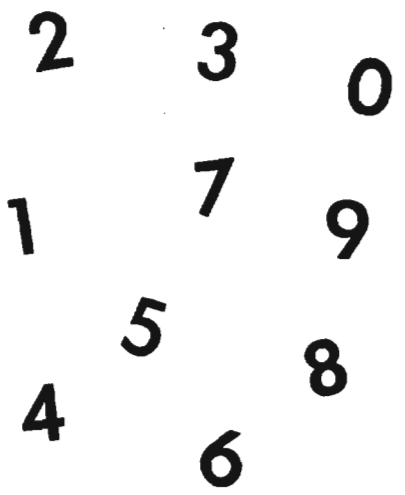
To: cryptolg at bar1c05

(U) In connection with that poem about the six serving men which you printed in connection with [redacted] article in the January 1984 issue of Cryptolog, I thought you might be interested in this sequel which I wrote to that verse:

I have a seventh serving man
Who taught me quite a lot.
The buddy of those other six
Is simply named "Why Not?"

(signed) Mudguard Stripling

P.L. 86-36



P.L. 86-36

N-U-M-E-R-O-L-O-G-Y (U)
A Quiz

by [redacted] P16

~~(FOUO)~~ Here are some numbers graven in the memory bank of every good cryppie. How many can you recognize?

a. 17,576

b. 101,405,850

c. 288,000

d. 5,008

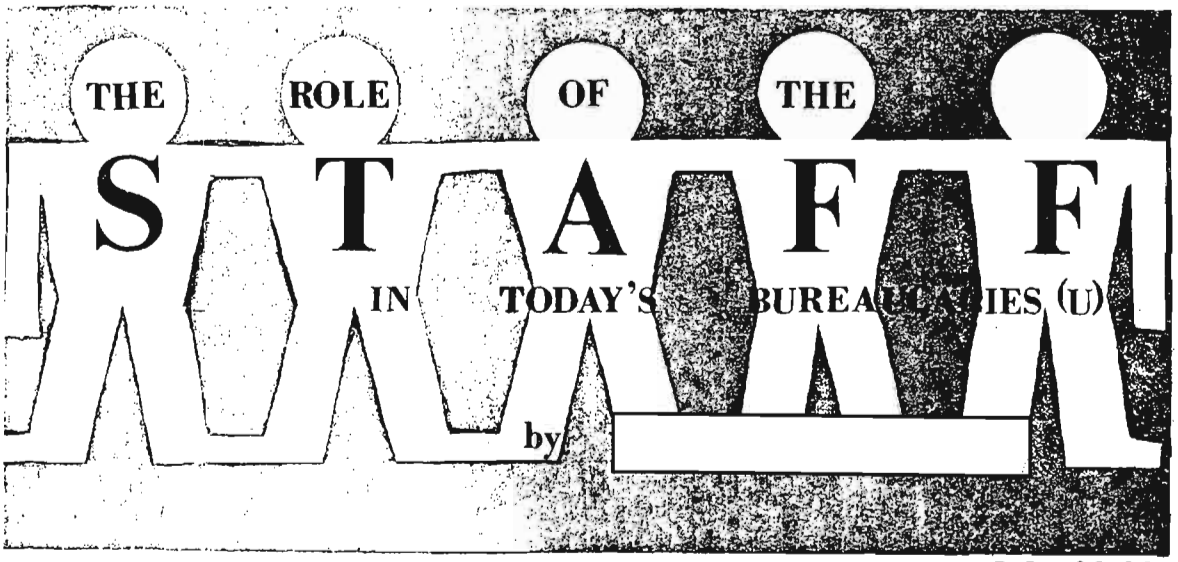
e. 15,600

f. 676

g. 11,881,376

h. 32,768

OCID: 4009898



P.L. 86-36

I. INTRODUCTION

(U) The bureaucratic institutions of government are growing larger and more influential with each passing year. This growth is seemingly independent of the political affiliation of the incumbent administration. It has shown resiliency to attacks directed at reducing government size and regulation. In our discussion of the role of the staff in today's bureaucracies, we will not attempt to debate whether growth and influence are desirable. Suffice it to say that if these factors continue to increase, it becomes all the more important to understand how and why bureaucracies function. This paper will deal with one important aspect of the bureaucratic structure, the staff.

II. STAFF FUNCTIONS

(U) The functions of the staff are both essential and diverse. In many instances, the staff is the glue that holds large organizations together. Staffs get involved in a wide range of activities including

[] coordination and liaison;

[] information dissemination and filtering; and

[] decision recommendations.

They will sometimes also serve as a repository for expertise which it might otherwise be impractical to allocate separately to line organizations.

A. Coordination and Liaison: These activities are critical to the smooth operation and interaction of the various departments within the bureaucracy and also to successful interface with outside organizations. The staff will coordinate policy and standards and ensure that the separate activities of two or more departments are directed toward achievement of the overall corporate goals. Disagreements or misunderstandings between departments are often not resolvable in head-to-head confrontations. A staff organization, however, can often act as a sounding board or as an honest broker to resolve differences and get operations back on track.

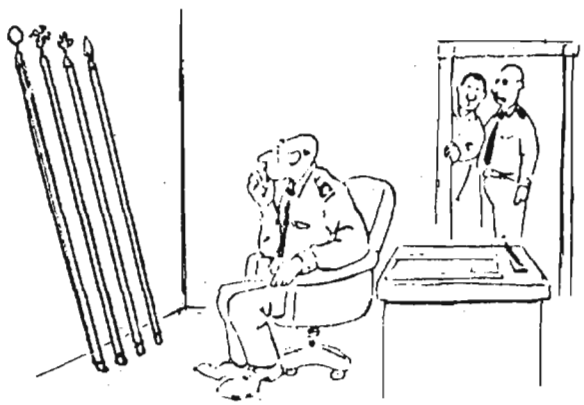
A Staff is many times the ideal focal point for liaison with other organizations outside the bureaucracy. In the Defense Department, for example, the various intelligence agencies must coordinate their activities to achieve the best results with optimum use of resources. In accomplishing this, it is usually the staff organizations serving as focal points in the various agencies that will carry out the liaison functions first. It is there that decisions are made to which agency elements are most likely to contribute. Appropriate internal directives are issued and the tasks are undertaken.

B. Information Dissemination and Filtering: Staffs serve as a point of dissemination for information flowing from the chief executive to the line organizations. When there are policy changes or specific tasks to be assigned, it is often left to the staff to choose the correct distribution or identify specific department that will carry out the tasks.

(U) This information flow also works in the other direction. The executive's staff also filters information passing across his desk. The information generated today in the form of memoranda, reports, special studies, etc., is tremendous. For a chief executive to read all such data would be both time-consuming and impractical. It is the function of the staff then to assimilate the information and pass to the executive only those items deemed to have some impact on or interest to the organization.

C. Decision Recommendations: One of the prime functions of the staff is to make decision recommendations to the executive. In this role the staff gathers the appropriate facts, establishes possible courses of action, and recommends the route or routes deemed most desirable.

D. Repository of Expertise: To more effectively use scarce resources, the staff offers a very good centralized location for personnel with special skills. Where it may be impractical to assign a separate person to each department requiring such skills, assignment to the staff makes the skilled individual available to all departments. An example is in the area of special mathematical or engineering support. Selected departments may not be able to justify the full-time employment of a person with these skills; however, the skills of one such person assigned to a staff could be accessed by all departments as required.



"He's doing a staff study."

(U) All of the above staff activities are important to any organization, be it a one-man enterprise or a large bureaucracy. Often in a small business these functions are not assigned to a separate staff but are accomplished by the owner or manager. In a bureaucracy with wide-ranging interests and responsibilities, it is often more efficient to pool these functions together into an organization (the staff) which can develop high proficiency in these tasks. This practice also releases line organizations to do the essential business with which the particular bureaucracy is charged. As a final note on the functions of staff organizations, the following paragraphs condensed from a University of Utah article provide valuable insight into the ultimate goal of the staff: to present the executive with completed staff recommendations.

"Completed staff work is the study of a problem and the presentation of a solution by a staff employee in such form that all that remains to be done on the part of the executive is to indicate his approval or disapproval of the completed action. The words completed action are emphasized because the more difficult the problem is, the more the tendency is to present the problem to the executive in piecemeal fashion. It is a staff member's duty to work out details, no matter how perplexing they may be. The product, whether it involves new policy or affects an established one, should, when presented to the executive for approval or disapproval, be worked out in the finished form.

"The impulse which often comes to the inexperienced staff member to ask the executive what to do recurs more often when the problem is difficult. It is accompanied by a feeling of mental frustration. It is so easy to ask the executive what to do and it appears so easy for him to answer. The staff member must resist that impulse, but will succumb to it if he does not know his job. The staff must advise the executive what he ought to do, not ask him for guidance. HE NEEDS ANSWERS, NOT QUESTIONS. The staffer must study, write, restudy and rewrite until what has evolved is a single proposed action--the best one of all he has considered. The executive merely approves or disapproves. Alternate courses of action are desirable in many cases and should be so presented. But, the staff should state its recommendation as to which course of action is thought best.

"Writing a memorandum to the executive does not constitute completed staff work,

but writing memoranda for the executive to send to someone else does. Staff views should be placed before him in finished form so that he can make them his views simply by signing his name. The statement should be submitted with supporting documents, as appropriate. If the proper result is reached, the executive will usually recognize it at once. If he wants comment or explanation, he will ask for it.

"The completed staff work theory may result in more work for the staff employee, but it results in more freedom for the executive. This is as it should be. Further, it accomplished two things:

[] The executive is protected from half-baked ideas, voluminous memoranda and immature oral presentations and

[] The staff employee who has an idea to sell is enabled more readily to find a market." [1]

III. EVOLUTION OF STAFF STRUCTURES

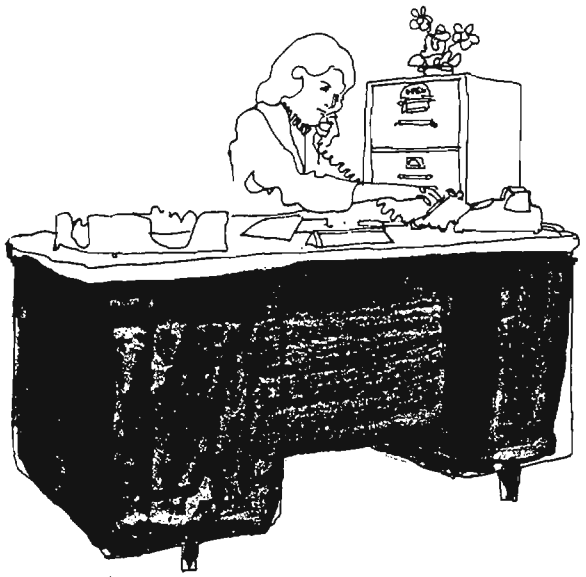
(U) Staff organizations have been with us practically since the dawn of history. Ever since the first leader attracted a group of followers, staff men were counted on to provide advice, act as messengers, and serve as a buffer between the leader and his flock.

(U) Today's concept of the staff organization in both business and government has evolved out of the complexities of modern, large-scale, cooperative effort. Those businesses without staff functions are adequate only as long as an organization is small enough so that its leaders can give it effective direction and control. For example, in a small organization the chief executive may also serve as the production manager, financial manager, procurement agent, personnel director, etc. With growth, however, the organization faces problems and pressures of increasing difficulty. The need for specialists becomes increasingly important.

(U) One method of building specialists into the organization is by applying the concepts of staff structure and authority. For example, an executive staff may be created which will allow the executive to divide major responsibilities so that his control over the activities of the organization is direct, yet will permit him to turn over to his subordinates those functions in which he has little interest or lesser abilities. It makes possible the introduction of specialists who extract from the line functions certain difficult tasks and responsibilities requiring highly developed skills and knowledge.

(U) Staffs in business and government are often formed with one or both of two types of individuals: the staff assistant and the staff specialist. The staff assistant's relationship with other organizational elements is often a difficult one. It presents possibilities of ambiguity as to the decision-making authority between the executive and his assistant. This kind of assistant is usually not a specialist in the strict sense, although the appointing executive usually seeks a person with the interests, abilities, special training or experience needed for the performance of functions to be delegated. Such a staff member performs the work subject to the approval and support of his chief, without formal authority to command the actions of others. He does not act independently of his superior, and his work is done "in the name of" that superior. Often this leads to the implication of authority on the part of the assistant that he does not actually have or to the acquisition of authority that the executive never intended to delegate.

(U) The staff specialist is perhaps the more common role of the two. Such specialists work very closely with line organizations and are specifically tasked to support them. Specialists may provide assistance in the areas of finance, personnel, engineering, procurement, etc. Since their supporting roles directly relate to line organizations, there is usually no great area of authority or control to contend with.



IV. LINE AND STAFF RELATIONSHIPS

(U) According to the Dimocks' text on Public Administration, generally speaking "line" connotes action and "staff" advice; "line" is hierarchical, "staff" collateral; "line" is authority, "staff" influence. A bureau chief is a line official, his research assistant is a staff officer. What the correct relationships should be between the two types of activity has long been a matter of debate, to the point where students of the subject have come to believe that the right adjustment between line and staff constitutes one of the difficult areas of management. [2]

(U) Theorists are agreed on the fact that as an organization grows in size and complexity, problems of planning and coordination also grow, not only vertically but horizontally. Operating executives need the help of staff officials to assist in planning objectives, developing programs, and effecting coordination. The main problem is how to organize this relationship.

(U) In studies of the US Department of Agriculture conducted by Gaus and Wolcott, and also by Paul Appleby, it was revealed that this particular department placed substantial power in the hands of staff officials. By necessity, most, if not all, line matters directed to the Secretary of Agriculture had to be cleared through his general staff. There were insufficient hours in the day to permit the Secretary to give adequate attention to all, or even the most important, questions.

(U) Within the general staff, probably the most important positions were those of the four assistants to the Secretary. They occupied his outer office and were closer to him in daily contacts than most line or other staff personnel. The functions of the assistants were

[] to reduce the pressure on the Secretary;

[] to evaluate each matter in the light of all its relationships, departmental functions, and overall policy; and

[] to determine the merits of each case and pass it on to the Secretary with a recommendation for action.

The four assistants could themselves virtually determine courses of action. Ordinarily they decided who should see the Secretary and what matters did not warrant his attention.

(U) The four assistants had to be generalists in order to be able to translate the narrow, specialized thinking and action into broader terms that helped the Secretary discharge his leadership function within the Department and as a member of the President's Cabinet. In his study of the staff functions, Appleby agreed that the first requirement of a good staff man is breadth of knowledge and ability; he must be a generalist. Also, he must be self-effacing, must like people, and, as a new man in an agency, must be able to assimilate himself into it so as to avoid the jealousy usually accorded an outsider. He must also possess a certain intangible quality that partakes of both integrity and wisdom. A sense of humor also helps. [3]

(U) It all too often occurs that conflict rather than cooperation is the product of line and staff relationships. Line officials resent what they consider interference by the staff in matters of policy and internal administration. A technique that effectively reduces the barrier between line and staff officials is the use of interchangeable tours of duty. Line officials are rotated to staff positions for two or thee years and then returned to their line jobs. This exchange, which could occur several times int he career of a key individual, tends to foster understanding of the other fellow's point of view and the problems he faces.

V. STAFF PROS AND CONS

(U) In their contributions to the smooth conduct of organizational management, staff organizations have their supporters and detractors--depending mostly on whom you ask. Executives tend to favor the staff element as an extension of themselves. Line

organizations, on the other hand, tend to treat staffs with some detachment, a necessary but bothersome part of the bureaucratic system. Some of the pros and cons of staff organization are:

A. Pros:

1. The staff provides more freedom for the executive. By using the staff to smooth out and communicate his decisions, he saves time and is able to concentrate on the more critical aspects of management. The staff will also ensure that he is not bothered by mundane aspects and issues which might otherwise cross his desk. They serve to filter out the unnecessary and provide him with the essential items requiring his attention. They are an extension of himself and serve as his finger on the pulse of the organization.

2. The staff eases the coordination process amongst the various departments and ensures that cooperation is being achieved. It also serves as a central point for liaison with outside organizations.

3. The staff serves as the central location for personnel with special skills that can address events companywide or can be allocated to different departments when needed.

B. Cons:

1. Too many layers of coordination frustrate and inhibit the production managers who require full resources and adequate freedom to perform their duties. The additional coordination channel imposed means additional delays in reaching decisions.

2. Some believe that staffers have too much power. Although the staffer may pay lip service to the idea that he has no authority and merely coordinates and gives advice to the line element, in practice it is rare to find a career staffer who does not seek to enhance his power at the e expense of other personnel in the line of command. The real power of the staffer can many times be attributed to his proximity to the chief executive. Being close to the executive's ear means a potential for significant influence on decisions and policy.

VI. SUMMARY

(U) In today's bureaucracies and in private enterprise as well, the staff is viewed as a body of individuals who have advisory responsibilities but no command authority. They report directly to top executives and are experts in functional areas. This contrasts with line personnel, who have operational responsibilities and line authority. They report to top executives through a chain of command and managers supervising many different operations.

(U) Livingston wrote that the creation of a staff does not mean the creation of new functions but rather the collection of services or other special functions under one head so they can be more effectively performed. The staff represents no special interest, but rather the overall interest of the organization.

(U) The growth and appearance of staffs varies widely with the kind of association involved. The staff, as the name implies, is something to lean upon. It gives service of advice or counsel as distinguished from authority to perform. However, the staff has certain rights, especially that of performing its service. Staffs are not only for the top echelons. For its full utilization, the concept of staffing should permeate the whole organization. For staff services to be effective, two things are essential: coordination and infiltration.

(U) As the size and complexity of an organization grow, the importance of staff services increases. The presence and use of staffs does not deny the line officers' competence or authority. It is merely a form of specialization. The staff gives advice, makes recommendations, and may even be able to order its recommendations into effect. But it is not charged with putting them into effect. Generally, the line and staff officers work very closely together, the staff having to do with how, when, or where to do something, the line officers with the actual accomplishment. [4]

Notes

1. "Completed Staff Work," University of Utah (1973).
2. Dimock, Marshall E. and Gladys O., Public Administration (New York: Holt, Rinehart and Winston, 1964), pp. 273-294.
3. Gaus, John M., and Leon O. Wolcott, Public Adminstration and the United States Department of Agriculture (Chicago: Public Administration Service, 1940), pp. 289-377. Appleby, Paul, "Organizing Around the Head of a Large Federal Department," Public Administration Review, VI, Summer 1946, pp. 205-212.
4. Livingston, Robert T., The Engineering of Organization and Management (New York: McGraw-Hill Book Co., 1949), pp. 67-86.

DOCID: 4009898

~~FOR OFFICIAL USE ONLY~~

THE Magdeburg INCIDENT:

Russian Intercept and Cryptanalytic Efforts in World War I (U)

P.L. 86-36

by [redacted]

(U) Originally prepared as an Appendix to the author's article on "Communications Intelligence and Tsarist Russia," which appeared in the Jan 84 issue of Cryptolog.

During World War I, much of the early success at sea enjoyed by the Allied Powers stemmed directly from the Russian recovery of German radiotelegraphic codebooks from the (U) cruiser MAGDEBURG, which had run aground near Oldensholm (now Osmussar) Island in the Baltic on 26 August 1914. The full story of this incident and the resultant actions taken based on it has never been completely told, especially from the Russian point of view. The following account is far from complete, but it should serve at least to put a portion of the Russian view on the record in English for the first time.

The running aground of the MAGDEBURG immediately came to the attention of Captain 1st Rank Adrian Ivanovich Nepenin,[2] chief of the Baltic Fleet's Communications (and Intelligence) Service. Nepenin quickly dispatched Lieutenant Mikhail Vasil'evich Hamilton of the torpedo boat LT. BURAKOV to the MAGDEBURG. Aboard the German cruiser, in the captain's cabin under a pile of shirts, Hamilton discovered a radiotelegraphic "Three-Flag" codebook.[3] Hamilton shielded his find from everyone in the cabin and took it back to Nepenin. The MAGDEBURG's crew, including the captain, were interned in POW camps in faraway Siberia for the duration of the war so that no word of the captured codebook would be revealed.

Later, while Russian divers were examining the submerged portion of the MAGDEBURG, they found the body of a German code clerk in whose hands was clasped a second copy of the codebook. Two photographic copies were made of the original book and provided to the Baltic and Black Sea Fleet Commands by the Russian Naval General Staff.[4] Shortly thereafter Captain 1st Rank Mikhail Aleksandrovich Kedrov and Captain 2nd Rank Mikhail Ivanovich Smirnov were sent to England with the original copy of the German codebook, which they handed over personally to the First Lord of the Admiralty, Winston Churchill.[5]

Before going into the Russian cryptanalytic efforts involving the German codebook, let's look at the special intercept station set up by the Russians prior to the MAGDEBURG incident.

From the first days of the war Captain Nepenin was concerned about German espionage activity on the territory of Finland (then a part of the Russian Empire) and in the Baltic area where enemy agents could monitor the movements of Russian ships. Although there was strict censorship in the area, discovering enemy agent radio stations operating independently would be a difficult task. Even though counterespionage was not a direct function of the Communications Service operation, Nepenin received permission from the Commander-in-Chief, Baltic Fleet, and the Chief of the Naval General Staff to set up special radio stations to monitor the airwaves for unusual

~~FOR OFFICIAL USE ONLY~~

emissions in order to locate enemy transmitters. Thus, the first special intercept stations were planned with both counterintelligence and positive intelligence-gathering roles in mind.

The location of the first "special-purpose radio intercept station" (RADISTANTsIYa OSOBOGO NAZNAChENIYa, or simply OSNAZ) was at Cape Shpitkhami (now Cape Poosapea/Pyaspea in Estonia) on the far western tip of the southern coast of the Gulf of Finland, some distance inland from the coast.[6] In the middle of a pine forest, land was cleared away for the site. High pine trees hid the construction from both sea and shore. An operations building and another one for living quarters of the assigned personnel were constructed. In the words of one of the Communications Service Officers who worked there:

> As always it was comfortable and practical, just like everything that came from Captain Nepenin."[7]

The intercept station personnel were allowed no direct contact with the outside world and a reinforced guard was set up around the station for added protection. The necessary supplies were delivered to the station at specified times by car from Revel. Captain 2nd Rank Przhilenskij was placed in charge of this OSNAZ station, which was given the cover story of a Gendarme station to conceal its real purpose. The information acquired later by the station as a result of the cryptanalysis was given the covername "Agent Network X" (AGENTURA IKS) material to also conceal its real source, and all information was then sent by underground cable to the Southern Region administration of the Communications Service in Revel.[8]

However, before "Agent Network X" material could become a reality, the Russians had to make some sense out of the German codebook. According to the former Baltic Fleet Headquarters historian, Captain 2nd Rank Fedor Yul'evich Dovkont, finding the German codebook on the MAGDEBURG did not mean that the encrypted German communications could be immediately read by the Russians. The German communicators changed their enciphering keys every 24 hours at midnight with a special cipher designated "ALFA-GAMMA" or "GAMMA-ALFA." In addition to the codebook on the MAGDEBURG, there was also found a set of official instructions, maps with quadrants of the Baltic Sea marked off, and other documents, the most essential parts of which were reproduced by the Naval General Staff in classified books and sent to interested Headquarters of Russian Fleet units.

Before the MAGDEBURG incident, Captain Nepenin had instructed radio stations at Communications Service posts to write down precisely all enemy radio transmissions and to send these notes to Communications Service Headquarters, where they were protected until the day when they could be decrypted. With the enemy cryptographic materials now in hand, the difficult task of sorting out these notes and trying to find the keys was begun. A special section was established under Captain 1st Rank Mikhail Platonovich Davydov. Parallel to Davydov's group, Captain 2nd Rank Ivan Ivanovich Rengarten from Baltic Fleet Headquarters also worked at trying to find the keys.

Rengarten made the first breakthrough after one month's intensive effort in partially decrypting a message from the German cruise AUGSBURG.[9] At the same time that the Davydov group (Communications Service) and Rengarten group (Baltic Fleet HQ) were trying to decrypt the German messages, select groups from several headquarters of Baltic Fleet operational units were also independently involved with this effort. For example, the navigation office at the Headquarters of the Baltic Fleet Cruiser Brigade, Captain 2nd Rank Nikolaj Nikolaevich Kryzhanovskij stated:

> "Up until the organization of the 'Black Cabinet' [the Shpitkhami cryptanalytic group; see below], a copy of the codebook was sent to us at the Cruiser Brigade Headquarters and we ourselves worked at decrypting the 'FEK' [cover term used in the Baltic Fleet for the German reencipherment tables]. This was highly secret work, even from other officers, and the cause of much talk. On board the cruiser RURIK we had a very small staff at the wish of the ship's captain. Besides myself, there were an senior flag officer and two others, one of whom had an excellent command of the English, French, and German languages."[11]

Following on these early efforts, it was decided that a more systematic effort at cryptanalysis was needed. Therefore it was decided to concentrate the cryptanalytic effort in the Baltic at the Shpitkhami radio intercept station. For this purpose, six officers who know the German language well and had experience in cipher work were selected. At the head of this operation the Naval General Staff placed a

man named E. Fetterlein from the Ministry of Foreign Affairs cryptanalytic establishment. Since Fetterlein's last name was of German derivation and could bring unwanted publicity from Russian right-wing nationalist newspapers, such as Novoe Vremya (New Times), then conducting hysterical "anti-German" campaigns in Russia, it was decided to give him the last name of "Popov" to use until the war ended.[12]

As a further security measure, those persons assigned to the "Black Cabinet," as the Shpitkhami cryptanalytic group was known, were instructed to write their relatives not to send them any letters directly until the end of the war because of their secret work location. All mail was to be sent to them via the Communications Service Headquarters, which would then forward the correspondence to the individuals. The naval officers of the group still hoped that they might bring their wives to live at the site. However, according to one member of the cryptanalytic group, Nepenin's reaction to this suggestion was:

"What? Wives? I don't want any women combing their hair among the pine trees!"[13]

Captain Nepenin, though, not only made an exception to the "No Wife" rule for chief cryptanalyst Fetterlein-Popov but also went so far as to have a special house built at the Shpitkhami site for the couple.[14]

The initial breakthrough in cryptanalysis by Captain Rengarten made the task of the Shpitkhami group a little easier. The main task was was still discovering the daily key which served to reencrypt the German code. British Navy Headquarters also worked closely with the Russian Naval Headquarters in this effort. In addition to a copy of the codebook, all material published by the Russians was sent to the British. This effort reached such a degree of success that within an hour of introduction of the new "FEK" into operation by the Germans, the Russian or British side first discovering it would report it immediately to their counterparts in as simple a manner as possible in order not to attract attention to itself from possible German agents.

The German attribute of being systematic played a major role in the successful cryptanalytic effort. The German Navy separated its ships into different groups, each of which had only its own group's codebook. Therefore, the radio messages of two or more groups were always repeated in each of the recipients' respective codes. Finding the primary and most complete codebook on the MAGDEBURG was especially helpful. There was a sufficient number of already decrypted radio messages in this codebook to assist in decrypting corresponding passages in all the remaining ones.

The German Navy frequently abused it use of radio communications, which provided more material for the Shpitkhami cryptanalytic to use. In addition, with the aid of radio direction finding (RDF) bearings, the quadrant numbers of the Baltic Sea in which German ships were using radiotelegraphic communications were determined. Since the enemy ships frequently sent their position or rendezvous site (quadrant of the Baltic Sea), this allowed the Russians to use the quadrant maps found on the MAGDEBURG to decrypt the corresponding encrypted locations.

Another significant mistake of the Germans was to be excessively systematic in sending daily routine official reports to naval units and even to individual ships by radio. For example, a detailed radio message sent by the Germans in the first hour of each day with the new reencryption key contained about 10% of the information needed to decrypt it. Often within 30 minutes--almost always within 90 minutes--either the Russians or the British had the new key worked out and then passed it on to the other. Even in 1916, when the German Navy introduced a new codebook with new words and phrases, the later edition kept the same alphabetical order as the replaced version, which allowed the Russians to interpolate unknown locations with those already known. The ultimate success of this cryptanalytic operation can be attributed, on the Russian side, to the efforts of Captain Rengarten, Fetterlein-Popov, and the cryptanalysts of Shpitkhami.[15]

FOOTNOTES

1. Except where otherwise noted, information in this article is based on articles by Rear Admiral Boris Petrovich Dudorov in the emigré journal Morskie Zapiski (The Naval Records), New York, March and August 1960, passim.

2. See "Communications Intelligence and Tsarist Russia" and "Admiral Adrian I. Nepenin: Father of Modern Russian Naval Intelligence" by [redacted] in previous issues of Cryptolog.

P.L. 86-36

DOCID: 4009898

3. Dudorov, op. cit., March 1960, pp. 51-53, and Pavlovich, N. B. (editor), Flot v Pervoj Mirovoj Vojne (The Navy in World War I), 2 vols, Moscow: Voenizdat, 1964, Vo 1, p. 95. Prior to the war Russian naval intelligence agents has acquired a copy of the German codebook in Berlin, but this particular codebook's use ended with the outbreak of the war. See Dudorov, op. cit., March 1960, p. 49, and Woodward, David, The Russians at Sea, London: William Kimber, 1965, p. 166.

4. According to Yankovich, V., "On the Origins of Radio Intelligence in the Russian Navy," Voenno-Istoricheskij Zhurnal (Journal of Military History), Moscow, February 1961, p. 116, the French also received a photocopy of the German naval codebook from the Russians. This may have been the result of the Franco-Russian Naval Convention Agreement of 16 July 1912, which was updated in May 1913 to include the exchange of intelligence information between the naval commands of the two countries. See The Military Attache by Alfred Vagts, Princeton: Princeton University Press, 1967, p. 369; Grunwald, Constantin de, Franko-Russkie Soyuzy (Franco-Russian Alliances) [translated from the French], Moscow: International Relations Publishing House, 1968, p. 246; and Rodionov, A., "The Navy and Coalition Warfare," Morskoj Sbornik (Naval Collection), July 1976, p. 22. No such formal agreements existed between the Russian and British Naval Commands.

5. Steblin-Kamenskij, Senior Lieutenant I. I., "Mine Warfare in the Black Sea," La Revue Maritime (Naval Revue), Paris, Nov 1932, p. 620. According to another version, the British probably received the second codebook, as Churchill himself (in The World Crisis, Toronto: Macmillan, 1931, p. 254) described receiving a water-damaged copy found on the body of a drowned German sailor. However, in a more recent revelation, three copies of a codebook, designated SKM 145, 151, and 974. were apparently found on the MAGDEBURG and copy SKM 151 was turned over to the British. See Room 40 by Patrick Beesly, London: Hamish Hamilton, 1982, p. 6n.

6. Dudorov, op. cit., March 1960, pp. 64-66; Rengarten, I I., "On Radio Communications in the Navy," Morskoj Sbornik (Naval Collection), Moscow, Jan-Mar 1920, p. 42; Yankovich, op. cit., p. 116; and Timirev, Rear Admiral Sergej Nikolaevich, Vospominaniya Morskogo Ofitsera (Recollections of a Naval Officer), New York: American Society for Russian Naval History, 1961, pp. 46-47. Timirev says the site was located between Revel (now Tallin) and Baltijskij Port (now Paldiski), but his information was not first-hand, as was Dudorov's and Yankovich's.

7. Warrant Officer Markov, cited in Dudorov, op. cit., March 1960, p. 65.

8. Dudorov, op. cit., March 1960, pp. 54-66 and June 1961, p. 115; Timirev, op. cit., pp. 46-47; Yankovich, op. cit., p. 116; and Beesly, op. cit., p. 181. According to Beesly, "Commander Przyleneki [sic, Przhilenskij?] in December 1916 visited Room 40 in London and left a memo describing all the advantages which cryptanalysis had given the Russian Naval COMINT effort.

9. Dudorov, op. cit., August 1960, pp. 19-20; Chernomor, Volnyj Baltiki: 1914-1915 (Waves of the Baltic: 1914-1915), Riga: Dlya Vas, 1939, p. 142; and Yankovich, op. cit., pp. 115-116.

10. Kryzhanovskij, cited in Dudorov, op. cit., August 1960, pp. 19-20.

11. After the Revolution in 1917 Fetterlein was apparently employed by the British Government Code and Cipher School as a cryptanalyst, a position he was still occupying in World War II. See Seale, Patrick, and Maureen McConville, Philby: The Long Road to Moscow, New York: Simon & Schuster, 1972, pp. 152, 158; and Beesly, op. cit., p. 182. One former employee of the Tsarist Ministry of Foreign Affairs has characterized Fetterlein as a most gifted cryptanalyst. See Korostovetz, Vladimir, Lenin im Hause der Vaeter (Lenin in the House of the Fathers), Berlin: Verlag fuer Kulturpolitik, 1928, pp. 50-51. Also see Timirev, op. cit., pp. 46-7; and Dudorov, op cit, August 1960, p. 22.

12. Warrant Officer Markov, cited in Dudorov, op. cit., August 1960, p. 22.

13. Dudorov, op. cit., June 1961, p. 118. This is indeed indicative of the way a professional member of the COMINT service was held in high esteem by those Russians "in the know" under the Tsars.

14. Dudorov, op. cit., March and August 1960; Yankovich, op. cit., passim

OCID: 4009898

THE POSITION OF NSA/CSS IN THE US GOVERNMENT (U)

by [redacted] Q4

P.L. 86-36

(U) This article outlines the relationship of the National Security Agency/Central Security Service and Director/Chief with the rest of the US Government. Many of the source policy documents referenced herein are extremely sensitive and not available to the total cryptologic populace. They have been disseminated as required and appropriate decisions have been implemented by the NSA/CSS system of directives.

Relationship with CONGRESS

(U) Congressional interaction with NSA takes several forms:

[] legislation;

[] oversight;

[] program and budget authority; and

[] appropriation of funds.

(U) There have been comparatively few legislative acts passed which relate directly to NSA's functions. The major interaction is with the House and Senate committees on intelligence: the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, established in 1975 and 1977 respectively. Under the provisions of the 1981 Amendment to the National Security Act of 1947, NSA keeps these two committees fully and currently informed, provides advance notice of significant activities, and submits timely reports in problems. The basic oversight techniques employed by the committees are hearings and investigations.

(U) There are four committees--the House and Senate Armed Services Committees, as well as the two intelligence committees--responsible for authorizing programs and for establishing funding ceilings. The actual appropriation of funds is done by the House and Senate Appropriations Committees. They define the precise purpose for which the money is to be spent, adjust funding, and prohibit expenditures for certain purposes.

(U) Other means of oversight include

[] program evaluations;

[] studies by congressional support agencies such as the Office of Technology Assessment and the General Accounting Office; and

[] investigations by individual members.

(U) The DIRNSA and other senior officials occasionally testify in open and closed sessions of congressional committees.

Relationship with the PRESIDENT

(U) Executive Order (EO) 12333 of 4 December 1981, an unclassified document, provides for the intelligence activities of the US. It established the Director of Central

Intelligence (DCI) as the head of the Intelligence Community and authorized him to establish such advisory groups as required. The Intelligence Community is defined in paragraph 3.4.(f) to include NSA. The EO prescribes general duties and responsibilities of "Heads of Executive Departments and Agencies" (including NSA) and "Senior Officials of the Intelligence Community (also including DIRNSA).

(U) Specific responsibilities assigned to the Secretary of Defense by the EO include

[] "conduct, as the executive agent of the United States Government, signals intelligence and communications security activities";

[] "provide for the timely transmission of critical intelligence" (a prime function of NSA/CSS but including all sources); and

[] "direct, operate, control, and provide fiscal management for the National Security Agency."

(U) The EO assigns specific responsibilities to the National Security Agency, including collection, processing, and dissemination of SIGINT in accordance with guidance from the DCI, "executing the responsibilities of the Secretary of Defense as executive agent for the communications security of the United States Government"; and SIGINT security and security of COMSEC material.

~~(C)~~ The COMSEC mission, NSA's (not CSS's) second national mission, is most recently provided for in a presidential directive (PD/-NSC-24) of 9 February 1977, Telecommunications Policy. (This PD is currently under updating review. One draft we have seen also includes "automated information systems security" or COMPUSEC.) The Secretary of Defense is designated "the Executive Agent for COMSEC to protect government-derived information which relates to national security." In this capacity the Secretary of Defense has issued a National Communications Security Directive dated 20 June 1979 which, among other things, established the National COMSEC Committee. The Deputy Under Secretary of Defense for Communications, Command, Control, and Intelligence (DUSD(C3I))chairs the committee. Membership includes representatives of

[] the Director, National Security Agency (DDC);

[] the Secretaries of Army, Navy, and Air Force;

[] the Secretaries of State, Transportation, and Energy;

[] the Attorney General; and

[] the DCI.

The Secretariat is provided by and quartered at NSA. The National COMSEC Directive assigns to DIRNSA the responsibility "for executing the COMSEC responsibilities of the Secretary of Defense" and lists specific details for carrying out this basic responsibility.

Relationship with the NATIONAL SECURITY COUNCIL

(U) The NSC members are the President, Vice President, and Secretaries of State and Defense. Statutory advisors to the NCS are the DCI, Chairman of the JCS, and Assistant to the President.

~~(FOUO)~~ National Security Decision Directive Number 2, "National Security Council Structure," was promulgated by President Reagan of 12 January 1982. Included in the structure is the Senior Interagency Group-Intelligence (SIG-I) to advise and assist the NSC on intelligence matters and policy. Membership includes the DCI (chairman), Assistant to the President for National Security Affairs, Deputy Secretary of Defense, and the Chairman of the Joint Chiefs of Staff (JCS). By SIG-I Directive No. 1 dated 5 August 1982, two Interagency Groups were established, one for Counterintelligence (IG/CI) and the other for Countermeasures (IG/CM). The DDO represents NSA on the IG/CI, with the Chief of G1 as his alternate. ADDC and Chief G1 are the member and alternate, respectively, of the IG/CM.

~~(C)~~ The present NSC Intelligence Directive for SIGINT (NSCID No. 6) was published 17 February 1972, is consistent with EO 12333, and is still in effect. This directive has undergone little change in its several versions since 1952. It reiterates the basic responsibilities from EO 12333 (and its predecessors) of the DCI, Secretary of Defense, and DIRNSA, but specifically for SIGINT. The NSCID says that DIRNSA "shall report to the Secretary of Defense and shall be the principal SIGINT advisor to the Secretary of Defense," the DCI, and the JCS. It also establishes "under the Secretary of Defense and subject to his authority and control a National Security Agency." The Director and Deputy Director shall be designated by the Secretary of Defense, subject to approval by the President. The duration of their appointments shall be at the pleasure of the President. "The Director shall be a commissioned officer of the armed services, on active or reactivated status, and shall enjoy not less than three-star rank during the period of his incumbency. The Director

shall have a Deputy who shall be a career civilian with SIGINT experience."

(C) The NSCID-assigned duty of DIRNSA is "to provide for the SIGINT mission of the United States, to establish an effective unified organization and control of all SIGINT collection and processing activities of the United States and to produce SIGINT in accordance with objectives, requirements and priorities established by" the DCI. The Central Security Service (CSS) was established in 1972 under the DIRNSA. All military elements that perform SIGINT activities are in the US SIGINT System and, in turn, are in the CSS.

Relationship with the DIRECTOR OF CENTRAL INTELLIGENCE

(FOUO) Under the authority of EO 12333 and NSCIDs, including the SIGINT NSCID, the DCI established a National Foreign Intelligence Board (NFIB) and National Foreign Intelligence Council (NFIC) by DCI Directives (DCIDs) of 28 January 1982, replacing the US Intelligence Board (USIB). These bodies deal with all-source intelligence. The NFIB is the senior Intelligence Community advisory instrumentality on substantive aspects of national intelligence. The NFIC deals with "national intelligence issues, other than substantive"; it advises on priorities and objectives for the National Foreign Intelligence Program (NFIP) budget. The DCI and his deputy are Chairman and Vice Chairman, respectively, of both bodies. Membership on the NFIB and NFIC includes:

[] DIRNSA;

[] Executive Director, CIA;

[] Director, DIA; and

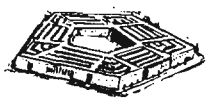
[] senior representatives of the State, Treasury, and Energy Departments and of the FBI.

(FOUO) Senior representatives of the military intelligence services and of the DoD special reconnaissance programs are members of the NFIC; they are observers on the NFIB except that the latter are "members when programs under their purview are considered." Additional members of the NFIC (but not of the NFIB) are senior representatives of the Secretaries of Defense and Commerce, of the Attorney General, and of the Assistant to the president for National Security Affairs.

(S) The DCI SIGINT Committee, which functions under a DCID of 12 May 1982, advises and assists the DCI and the DIRNSA. The Chairman comes from NSA but is a full-time member of the DCI Intelligence Community Staff. The Director of Policy (Q4), NSA, is the NSA member. Other members are representatives of the Intelligence Community principals (see EO 12333 for definition). The Committee meets frequently, at least weekly on the average, and advises on all facets of SIGINT: requirements, priorities, objectives, security, etc. The Chairman also establishes subcommittees or task forces as required.

(S-CCO) A DCID of 17 May 1983 sets forth the rules and regulations for SIGINT liaison with and release of SIGINT to foreign governments. The DCI establishes policy and approves procedures, with the advice of DIRNSA. The Director of NSA is executive for conduct of arrangements with the United Kingdom, Canada, Australia, and New Zealand. Except as specifically exempted by the DCI (in favor of DIRNSA), [redacted] SIGINT Security Regulations make up another DCID: Volume I, dated June 1982, covers COMINT; Volume II, dated January 1982, covers sensitive-source ELINT. All of these SIGINT DCIDs are products of SIGINT Committee recommendations.

EO 1.4.(c)
P.L. 86-36



Relationship with the DEPARTMENT OF DEFENSE

(C) Computer security is at present only a DoD mission, the most recent, assigned to NSA by DoD Directive 5215.1 of October 1982, though it is expected to develop into a national mission. The DoD Directive established the DoD Computer Security Center. The directive is unclassified and releasable to the public.

(C) Under the provisions of the law (the National Security Act of 1947), EO 12333 (and its predecessors) and the SIGINT NSCID, the Secretary of Defense issued a DoD Directive charter for NSA (DoD Directive S-5100.20, dated 23 December 1971). The DoD charter directive references only the SIGINT NSCID but is consistent with the EO, as is the NSCID. This charter is primarily based on higher

DOCID: 4009898

level intelligence documents and is primarily intelligence-oriented (i.e., toward SIGINT) but it does, as does the EO, provide for the COMSEC mission. The charter accurately reflects the provisions of the NSCID. It requires

[] the DIRNSA/Chief, CSS to "report to the Secretary of Defense";

[] the Deputy Chief, CSS to be not less than two-star military rank, normally of a different Service than the DIRNSA/Chief, CSS; and

[] the Service cryptologic organizations and "their subordinate activities which conduct SIGINT to be subordinate to the Chief, CSS" (DIRNSA).

(U) The DoD charter Directive for the Under Secretary of Defense for Research and Engineering (R&E), DoD Directive 5129.1, most recently dated 25 January 1984, requires that he exercise staff supervision on resource management matters over the NSA/CSS. This is handled primarily by courtesy copy of budget correspondence between NSA and the DCI, who develops the National Foreign Intelligence Program (NFIP). The DIRNSA is the program manager of the Combined Cryptologic Program (CCP), which makes up part of the NFIP.

(U) A separate DoD charter Directive for the Deputy Under Secretary of Defense for Policy (DUSD(P)), DoD Directive 5130.2 dated 16 June 1977, requires that he exercise staff supervision on policy matters over the NSA. (DoD Directive 5130.2 is titled and refers to the Director of Policy Review, but that position, by separate action, is currently designated Deputy Under Secretary of Defense for Policy.)

~~(C)~~ Two separate DoD functional Directives have been issued for SIGINT and COMSEC, S-3115.7 in 1973 and C-5200.5 in 1981. The SIGINT Directive references the NSA/CSS charter directive, repeats the responsibility for DIRNSA/Chief, CSS to exercise SIGINT operational control over the SIGINT resources of the US, and sets forth responsibilities for other DoD components: support, budget, requirements, etc.

~~(C)~~ The COMSEC directive promulgates basic DoD COMSEC policy and responsibilities of of DoD components. It designates DIRNSA as COMSEC program manager; DUSD(P) as the principal staff assistant to the Secretary of Defense for COMSEC policy; and DUSD(C3I) as Chairman of the National COMSEC Committee, the Secretary of Defense's representative for governmentwide COMSEC activities, and the principal staff assistant to the Secretary of Defense for COMSEC resources.

INFORMATION SECURITY

(U) A discussion of NSA's relationship with the rest of the US Government requires separate treatment of information security.

(U) The NSA/CSS Information Security Program for safeguarding the security of cryptologic information is directed by several issuances of the Executive Branch.

(U) Executive Order 12356, National Security Information, dated 2 April 1982, prescribes the uniform system for classifying, declassifying, and safeguarding national security information within and among the executive departments and organizations of the US Government. Policy direction of EO 12356 is the responsibility of the National Security Council. Implementation and oversight of the program is the responsibility of the Administrator of General Services, who delegates this responsibility to the Director of the Information Security Oversight Office (ISOO). ISOO Implementing Directive No. 1 carries out the provisions of EO 12356, effective 1 August 1982, and

[] prescribes a uniform information information security system;

[] establishes a monitoring system to enhance its effectiveness; and

[] sets forth guidance to governmental agencies on original and derivative classification, downgrading, declassification, and safeguarding of national security information.

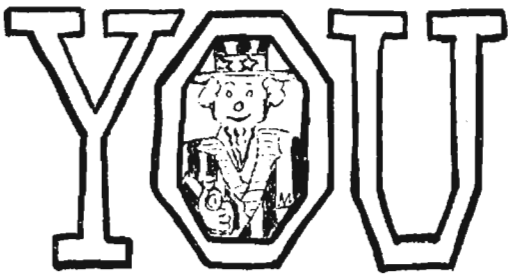
(U) The Department of Defense issued DoD Directive 5200.1, The DoD Information Security Program, dated 17 June 1982, and DoD Regulation 5200.1-R, Information Security Program Regulation, dated 1 August 1982.

~~(FOUO)~~ NSA/CSS has issued regulations for internal security and, to the US SIGINT System, USSID 3, "SIGINT Security." In addition, National COMSEC Instructions; security guides for specific projects, activities, and related directives; regulations; and instructions are issued.

~~(C)~~ NSA/CSS issuances take into account the UKUSA COMINT Agreement of 1946 which includes security policies for the protection and exchange of SIGINT. DCI issues the Signals Intelligence Security Regulations (SISR). A DoD Directive implements the SISR for the SIGINT user community.

DOCID: 4009898

DO YOU KNOW



THE DIFFERENCE BETWEEN A DATA ELEMENT AND A DATA ITEM?(U)

P.L. 86-36

In case somebody comes up to you out of the blue and wants to know the difference between "Data Element" and "Data Item," you may need some (U) handy definitions to quote. Accordingly, we thought we'd devote a little space to those two basic terms. As you know, a major goal of data standards is to CONCRETIZE the recording of data so that when you see a standard Data Element you will have an idea of what it will look like in a file.

(U) This involves laying a sharp eye on what you see in a data field. The NAME of a particular field confronting you may not by any means be the same as that of the DATA ELEMENT it contains. It may not even give you a good clue. Here is where data representatives are supposed to earn their pay--namely by

1. digging beneath the surface deep enough to see what the DATA ELEMENT itself is. Having done that, the data rep must then
2. consider what the DATA ITEMS are that constitute that DATA ELEMENT.

Remember, the DATA ITEMS are the things--or the representations of things--that actually appear in a given field of a data file. And each of these units of information MUST by definition belong to some DATA ELEMENT. That is, the DATA ELEMENT names and denotes what these DATA ITEMS pertain to. To pursue this train of thought further, take a look at the following more-or-less official descriptions/explanations of these two basic terms.

DATA ELEMENT: "A unique grouping of related informational units."

Reprinted with slight changes from NDSC Standards Bulletin, #3-84, 22 March 1984.

(U) This is the "official" USSID definition as given in USSID 414, section 2.1, and in NSA Regulation 80-9.

(U) The Department of Defense Dictionary of Military and Associated Terms, put out by the Joint Chiefs of Staff as JCS Pub. 1, is somewhat more specific than the "official" NSA definition. It says:

DATA ELEMENT: "A basic unit of information having a unique meaning and which has subcategories (data items) of distinct units of values. Examples ... are military personnel grade, sex, race, geographical location, and military unit.

(U) The Defense Department definition is "standardized and approved for use by all DoD components," according to JCS Pub. 1. Let me add a footnote to the effect that that the NSA Data Standard Center (NDSC) heartily endorses the spirit of this definition. Several years ago, however, Bob Register and I from the NDSC did join a working group at the National Bureau of Standards' Institute of Computer Sciences and Technology. The aim of the group was to improve the current definitions for the entire range of data standards terms. The members finally arrived at a slightly different version, which has not however officially superseded the USSID definition:

DATA ELEMENT: "A uniquely named and defined category of data having values expressed by the member data items of its data item set."

(U) This definition brought in the concept of "data item set"--that is, the collection of "legal" values which a Data Element could take on. (More on this below.)

(U) As you can see from the above definitions, some key phrases jump out at you:

[] Category or CLASS of data

[] Unit of Information

[] UNIQUE name/definition

[] Unique DATA ITEM SET (set of values)

(U) The above key phrases are important to understanding what a Data Element is. These ideas tend to be somewhat abstract however. Remember that the other side of the coin, the DATA ITEMs, represent the concrete units of information recorded in a data field. Following are the corresponding (and strikingly similarly worded) definitions of this other key term in data standards terminology.

DATA ITEM: "A subunit of descriptive information or value classified under a Data Element. (Data Items for "Month" are January, February, etc.) [from USSID 414]

DATA ITEM: "A subunit of descriptive information or value classified under a data element. For example, the data element "military personnel grade" contains data items such as sergeant, captain, and colonel." [from JCS Pub. 1.]

(U) The definition that the NBS working group arrived at again emphasized the idea of a UNIQUE data item set:

DATA ITEM: "A unique, defined entity which serves as a member of a data item set and as a particular value of a data element. It may be expressed in a field of a record or a block on a form by a discrete representation configured as an abbreviation, code, name, quantity, or statement."

(U) As we just noted, the latter definition stresses the concept of DATA ITEM SET--which in some cases is finite and in others open-ended. For example, Callsign, Frequency, and Year are all open-ended, whereas Day of the Week and Month both have finite sets of data items. This view of the DATA ELEMENT/DATA ITEM relationship allows us to posit what we might call "Data Standards Law #1." It states emphatically that Each and every Data Element by definition has its own set of UNIQUE values.

(U) The corollary of this Law is:

No other "data element" can claim the SAME set of data items and still consider itself a separate data element.

By DS Law #1 it really would have to be viewed as the same data element--masquerading under a different name. For example, Transmitter Frequency, Frequency First Observed, and Frequency of Receiver are all the SAME DATA ELEMENT because they theoretically share the same units of information (Data Items), recorded the same way.

(U) To summarize, Data Items are like the various family members of the MacKenzie Clan. Each one is unique, and there is no way you can match them up exactly with the Stewarts or the Buchanans--which are blessed with their own unique members. (In this imperfect analogy we are not considering the possibility of intermarriage.)

(U) We plan to expand further in a later issue on the theme of basic terms associated with Data Standards. In the meantime, don't let anyone tell you that "DATA ELEMENT" and "DATA ITEM" are just alternate names for the same thing. If anyone does so, we will accuse of him of being a follower of Humpty Dumpty in Through the Looking Glass, who proclaimed ex cathedra and ex muro--from his wall--that any word he used would "mean just I choose it to mean--neither more nor less."

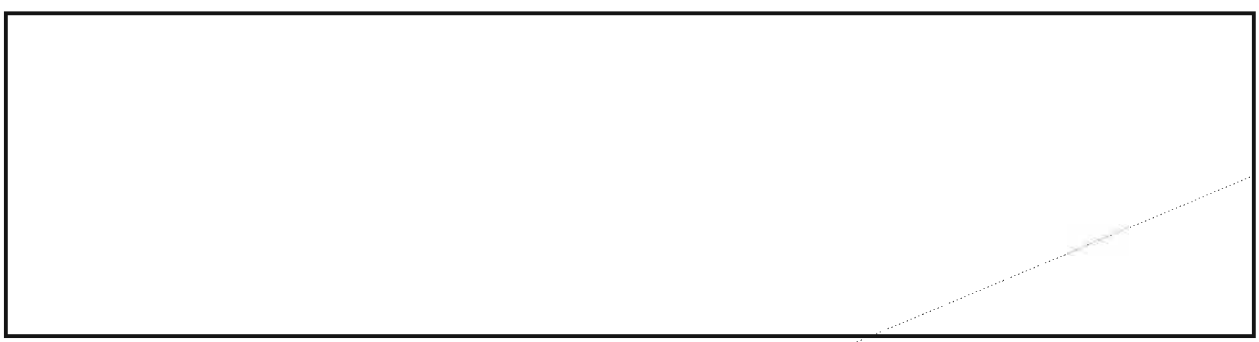
~~FOR OFFICIAL USE ONLY~~

NSA-Crostic No. 54

APRIL FOOLS' DAY
VOCABULARY BUILDER

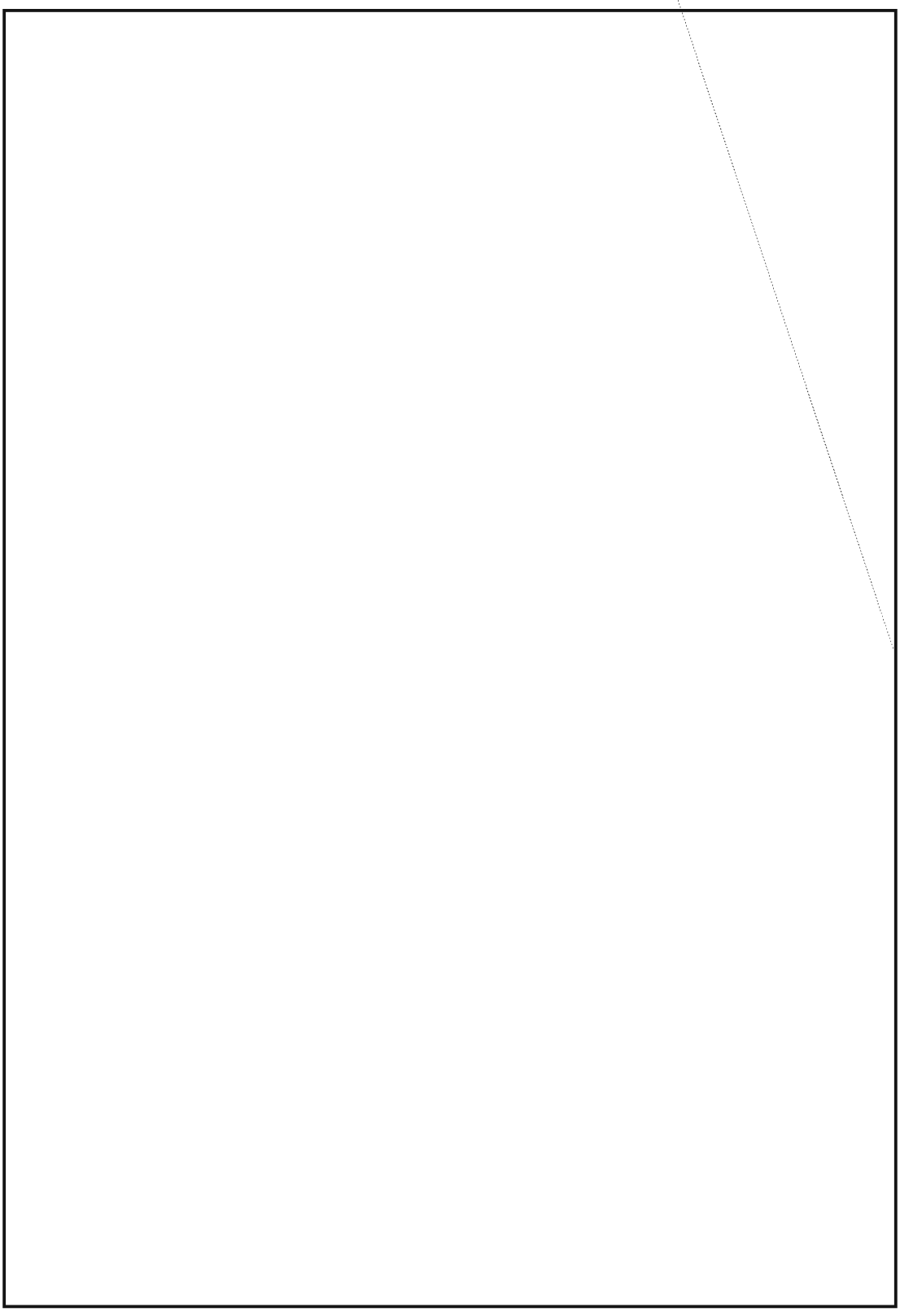
If you don't know Word D when you begin this puzzle, you certainly will by the time you've finished it.

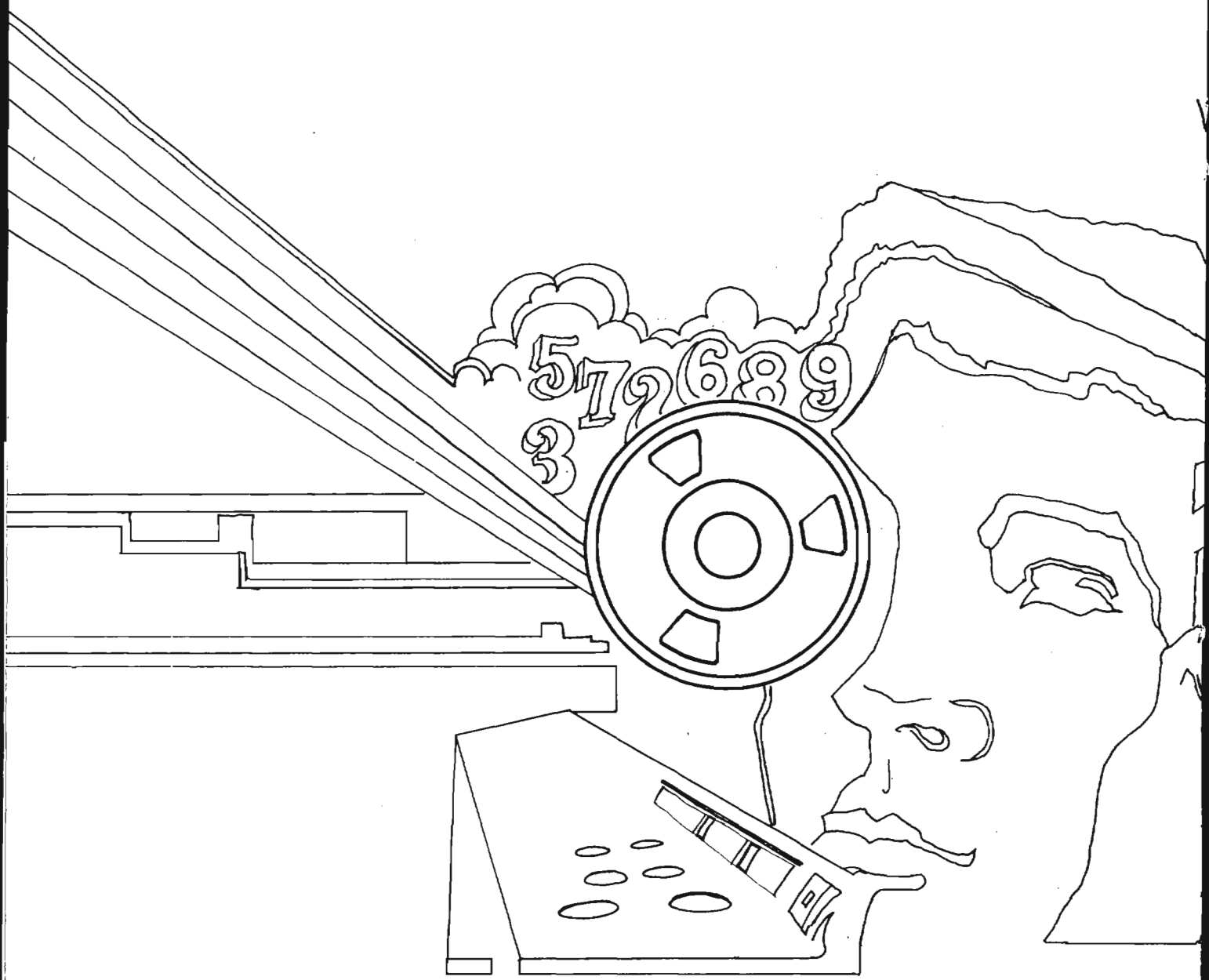
P.L. 86-36



 P.L. 86-36

~~FOR OFFICIAL USE ONLY~~




5726893

DOCID: 4009895

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

FEB-MAR 1984

ADMIRAL A.I. NEPENIN: FATHER OF MODERN
RUSSIAN NAVAL INTELLIGENCE (U)..... [redacted] 1
THE CRYPT BUG (U)..... [redacted] 2
USER-FRIENDLY WRITING (U)..... [redacted] 3
NATIONAL SUPERCOMPUTING RESEARCH CENTER..... [redacted] 6
SHELL GAME: TIME SHELLS (U).....W.E.S.....9
NSA-CROSTIC NO. 53.....David H. Williams.....12
AUTOMATED INFORMATION SECURITY (U)..... [redacted] 15
CRYPTOLOG 1983 INDEX (U).....21

~~HANDLE VIA COMINT CHANNELS ONLY~~

P.L. 86-36

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2
DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009895

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XI, No. 2-3 FEBRUARY-MARCH 1984

PUBLISHER [redacted]

BOARD OF EDITORS

Editor..... [redacted] (963-3045s)
Asst. Editor... [redacted] (963-1103s)
Production..... [redacted] (963-3369s)

Collection..... [redacted] (963-3961s)
Computer Security
..... [redacted] (859-6044)
Cryptolinguistics. [redacted] (963-1103s)
Data Systems..... [redacted] (963-4953s)
Information Science
..... [redacted] (963-5711s)
Mathematics..... [redacted] (968-8518s)
Puzzles.....David H. Williams (963-1103s)
Special Research.....Vera R. Filby (968-7119s)
Traffic Analysis..Robert J. Hanyok (968-8418s)

For subscriptions
send name and organization
to: [redacted] P14

P.L. 86-36

To submit articles or letters
by mail, to: P1, Cryptolog

via PLATFORM mail, send to:
cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no 'O' in 'log')

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

As an agency, we live today on yesterday's discoveries. Today's output, which pays the bills around here, is based largely upon technical breakthroughs made sometime in the past. Most of our people are working to produce today's results, but here and there, mostly in back rooms, there are a few scattered people doing the "discovery" work. We used to call them "break-in artists." They are busy making tomorrow's production possible and, in a very real sense, making it possible for tomorrow's bills to be paid.

Once in a while, one runs across a whole cluster of this discovery work. It is as if a renaissance had broken out in one particular shop. A whole group of people seem to be bubbling over with invention, intuition, and discovery. It is an exciting place to be, when it happens.

There used to be one or two managers who seemed to have such a renaissance around them wherever they went. They seemed to have the knack of creating an atmosphere that fostered discovery, that encouraged breakthroughs.

I can remember studying those managers, to see if I could emulate their evident ability to stimulate the discovery process. I can remember going to management courses and reading various books on the latest fads in management styles, looking for clues about how to generate the atmosphere that discovery and creativity seem to need. I can't remember finding much that was useful; it seemed to be easier to talk about things that were easier to count or measure.

For an outfit that depends so much on break-in artists, we ought to worry about finding, growing, and managing tomorrow's crop. Perhaps we already are.

[redacted]

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009895

ADMIRAL A.I. NEPENIN: FATHER OF MODERN RUSSIAN NAVAL INTELLIGENCE (U)

P.L. 86-36

by

[redacted]

Originally prepared as an Appendix to the author's article on "Communications Intelligence and Tsarist Russia," which appeared in the Jan 84 issue of Cryptolog.

The history of Russian military affairs has been one of incompetence mixed with flashes of brilliance. The brilliance has usually been in the form of individual military "shakers and movers" who have risen to the occasion with determination and forcefulness to carry through their goals, come what may, to the end. One might include Marshals Suvorov and Zhukov or Admirals Senyavin and Gorshkov in this category. However, there is one individual, although he is little known in the West, who as a "shaker and mover" might be said to be the father of modern Russian naval intelligence: Admiral Adrian Ivanovich Nepenin.

Nepenin, in his capacity as Chief of the Baltic Fleet's Communications (and Intelligence) Service both prior to and during World War I, built the naval intelligence organization into a formidable arm of the Russian Navy and ultimately established roots which have carried over into the Soviet era.

Adrian Ivanovich Nepenin was born 21 October 1871 in Pskov Province, Russia. He entered the Russian Naval Academy in 1885 and graduated in 1889. In 1898 he was assigned to the Far East Fleet. In December 1904 Captain 2nd Rank Nepenin was assigned to command the destroyer STOROZHEVOJ at Port Arthur. During the war with Japan, Nepenin was captured and spent the last part of that war as a POW in Japan. Between 1905 and 1910 Nepenin held various ship commands in the Baltic Fleet.

In 1910, after much thought, Nepenin sent a plan for reorganization of the Communications and Observation Service of the Baltic Fleet to Admiral Nikolaj Ottovich von Ehssen, Commander-in-Chief, Baltic Fleet. Admiral von Ehssen liked Nepenin's energetic idea for the Communications Service and in 1911 appointed Nepenin as Chief of the Communications Service. Nepenin probably made Captain 1st Rank at this time.

Over the next few years, under Nepenin's guidance and direction, the Communications Service--almost alone within the Russian Navy --achieved a high esprit de corps among all its personnel. By October 1915 Nepenin had achieved the rank of Rear Admiral for his efforts. His admirers included not only his own men but even foreign allies assigned to Russia during the war. During a visit to a Communications Service airbase in the Baltic in 1916, Admiral Sir Richard Phillimore (British Naval Representative to Russian General Staff Headquarters, "STAVKA," 1915-16) was quoted as telling the Communications Service officers and men:

DOCID: 4009895

"Everything is excellent in our British Navy ... except that we do not have such an Admiral as your Nepenin who knows everything."[1]

On 6 September 1916, largely on the basis of his Communications Service record, Nepenin was offered and accepted the command of the Baltic Fleet along with the rank of Vice Admiral. Nepenin's time as CINC, however, was brief with little opportunity to carry out his ideas on reorganizing and revitalizing the spirit of the Fleet. On 15 March 1917, while on his way to meet with a group of disgruntles sailors near the Helsingfors Railway Station, Nepenin was killed by a shot from behind by either a mutinous sailor (according to the Soviet version) or a German agent dressed in the uniform of a Baltic Fleet sailor (Russian emigré version).[2]

Although Nepenin's period on the stage of History was brief, he left an indelible imprint on the development of Russian naval intelligence in the 20th century.

FOOTNOTES

1. Apparently Sir Richard forgot (?) in his remarks about Admiral Reginald "Blinker" Hall of "Room 40 OB" fame.

2. Dudorov, Rear Admiral Boris Petrovich Dudorov in the emigré journal Morskie Zapiski (The Naval Records), New York. See also The Russian Navy in War and Revolution by G. K. Graf, Munich: R. Oldenburg, 1923, pp. 119-121, and The Russians at Sea by David Woodward, London: William Kimber, 1965, pp. 181-182. For the traditional Soviet negative view of Nepenin from 1916 as "suppressor of the Revolutionary in the Baltic Fleet," see Pavlovich, N. B. (editor), Flot v Pervoj Mirovoj Vojne (The Navy in World War I), 2 vols, Moscow: Voenizdat, 1964, Vol 1, p. 241.

THE CRYPT BUG (U)

by [redacted]

P.L. 86-36

When all good folks are sound asleep,
And all the rest are counting sheep,
He concentrates on cipher text,
And contemplates ways most complex
To render an approved solution
Of some obscure substitution.

While all the world is sleeping, snoring
Loud enough to rip the flooring,
He derives much satisfaction
From the spatial interaction
Of poly-graphic frequencies
And isomorphic sequences,
Of characters on paper slips
Better know as sliding strips.

Slides them West and tries the "Chi" test,
Slides them East and tries the "Phi" test,
Clamps his pipe tight in his mouth,
And grimly slides them North and South,
And if success eludes him then,
Tears them up and starts again.
Meanwhile the clock ticks on and on,
Until at long last comes the dawn.

As the milkman rattles by,
He is heard to heave a sigh,
Slowly piles the work sheets higher,
Calmly throws them on the fire,
Having proved one simple fact;
There can be do doubt of that--
As suspected all along,
Everything he did was wrong.

from Signal Corps Bulletin No. 109,
July-December 1940

DOCID: 4009895

~~FOR OFFICIAL USE ONLY~~

Human Factors

USER-FRIENDLY WRITING (U)

[redacted] P13 P.L. 86-36

We have seen and heard a lot lately about our writing. Our Director has made a special point of urging us to write more clearly and directly. A hard-hitting article on the same topic may be found in the November 1983 issue of CRYPTOLOG, pp. 13-18. A number of services are available to help us improve our communication skills, including courses at the School and the new "Write-Line." The quality and effectiveness of our writing and speaking is far more important than many of us seem to realize, in spite of these management initiatives. Unfortunately, our writing will only get better if we care about it and feel that it matters. I am not going to launch into a long article about good writing, or how to improve our writing. That has been done already by many others; I will mention two sources that I have found particularly useful. But I feel that good clear writing is an important human factors issue, and I'd like to say a few things about it in these Tech Notes.

I read a lot of technical papers and research reports, and I edit my office's Monthly Research Summaries. I am sorry to say that I have seen a great deal of very bad writing. It is bad because it is not "user-friendly." I am going to direct my comments to anyone out there who writes the kinds of prose I have to fight my way through each month in our Research Summary.

As a reader, I am a user of your paper or report, just like a user of any other tool. The paper probably says something I need to know or I wouldn't have picked it up. If you create long, intricate sentences choked with jargon, you are putting major obstacles in my way. You are making me spend far too much of my time and energy to get your meaning. Sometimes your sentences are so complicated that you lose your own way through them, so how can you expect me, the reader, to understand them? I know that you don't set out to mystify the reader on purpose. I believe that scientific and technical writers have certain basic misconceptions about writing; some or all of these they probably learn from their teachers at colleges and technical schools, many of whom are also apallingly bad writers. Let's take a look at some of the faulty assumptions that may give rise to the bad writing technical people so often produce.

"If I say it simply, people will think I'm uneducated."

People in technical fields have gotten so used to a certain very heavy, convoluted style of writing that simpler writing just sounds inappropriate and anticlimactic to them. Even if they are just telling us that they debugged a program or checked out some minor electronic gadget, they feel they must sound like a candidate for the Nobel prize.

~~FOR OFFICIAL USE ONLY~~

"If I say it simply, people won't know it's important."

Many people seem to think that the length of their words and the complexity of their sentences are a direct measure of the importance of the topic. I "use" a Kleenex to blow my nose, but I "utilize" the computer, because the computer is a lot more expensive and important than a Kleenex or my nose! I might "make it easier" for the cat to use the litter box, but I feel I must "facilitate user accessibility" to project X.

"If I say it simply, I won't be able to hedge and fudge."

Technical and scientific people are masters of the art of hedging their bets. To some extent, this is necessary and justified; we have a professional obligation to specify the degree of significance of a result, the reliability of a statement, or the statistical context of an event. We have to convey these matters to our readers at those times and places where they are important and appropriate. Unfortunately, the hedging gets to be a habit, so that it infects all our writing, and shows up in lots of places where it serves no purpose. I suspect that the long sentences starting out with endless strings of subordinate clauses arise in this hedging habit. Each subordinate clause is like a safe little fence to push the bald, direct subject and verb further away from the reader, until the meaning disappears in a comfortable mist. I have seen some cases where the subject and main verb never arrive at all. In many cases, the writer has forgotten whether the subject was singular or plural, or even what the subject started out to be, by the time he gets to the main verb. It's a real help to the reader when you put the main subject and verb at or near the beginning of the sentence. Don't get into the habit of writing English as if it were German!

A frequent error I see in technical writing is the "dangling participle." The long string of subordinate clauses at the beginning of the sentence often starts with a participial phrase that does not refer to the real subject of the sentence. Strunk and White (reference 2 below) say, "A participial phrase at the beginning of a sentence must refer to the grammatical subject." [p. 8] As the reference states, sentences violating this rule are often ludicrous, for example, "Being in a dilapidated condition, I was able to buy the house very cheap." Even when they aren't ridiculous, dangling participles are confusing and sloppy. This kind of writing doesn't impress a careful reader with the quality of the writer's thinking.

"My readers are all experts in my field and know the jargon."

Perhaps this is true; if so, I think the writer is making a mistake. What about managers in other organizations that might make use of his ideas? They may be familiar with the field at a global level without knowing all the buzzwords and abbreviations he tosses off in his report. What about technical people in related fields? They may have a similar problem with some of the jargon. Finally, I maintain that jargon and alphabet soup are far too often a lazy substitute for thinking. If we understand what we are doing, we should be able to express it clearly with a minimum of jargon. When I am talking to someone who throws a lot of alphabet soup and jargon at me, I make a point of asking politely for one or two definitions or expansions. Very often, I get a blank look, a silence, then "Well, gosh, now that you ask, I don't know!"

OCID: 4009895

"Oh, EVERYBODY knows what that means!"

The remarks in paragraph 4 apply to this one too. I came across the phrase "repartitioning the functionality" in a recent research summary. I very much doubt that "everybody" knows what that might mean, and I'm sure that some simpler, clearer way could have been found to express the idea, whatever it was.

"If I simply say 'somebody did thus and so,' I am leaving somebody's posterior alarmingly uncovered."

We seem to think it is much safer for all concerned to use the passive voice. Nobody DID it. It just happened. It was done. That also sounds much more impressive, like an act of God: it rained, there was light. We've also had it hammered into us throughout a technical or scientific education that we must always be "objective." The worst sin in the world is to be "personal" or "subjective"! That's another reason why we avoid the active voice like the plague and prefer passives or impersonal constructions like "there were indications that" and "it is apparent that." These constructions make our sentences needlessly complicated right at the start: harder for us to write, and harder for the reader to read. At their worst, they can totally obscure the meaning.

Here's a sample of user-unfriendly prose to illustrate the needless syntactic tangles and sloppy semantics of bad writing: "In addition to examining the use of, and designing a gadget for a frammus for project GLITCH, the use of a widget for project FOO was also studied." Exercise: find the subject of this sentence. Here's a better way of saying it: "We designed a gadget for a frammus for project GLITCH, and examined its use. We also studied the use of a widget for project FOO." I am still unhappy about the vagueness of "studying the use" of gadgets and widgets. Does the writer mean "try out the gadget to see how useful it is"? Or does he mean "observe operators using the gadget and study how they use it"? Maybe he means "perform various experiments to see if there is any point in trying to use the gadget." When we look closely at this sentence, we see that it doesn't convey much meaning to the reader unless he already knows all the intimate details of the projects and equipment.

In closing, I'd like to stress one final point: writing matters. It matters HOW something is expressed. Engineers and mathematicians know that the formal systems they use (mathematical and scientific notation, models, and methods) are powerful tools. Computer systems people hold up certain standards for writing good code and for the efficient, economical use of programming languages. Technical people respect those tools and appreciate the value of elegance and economy in their use. Natural language is another tool, just as powerful and deserving of respect. Unfortunately, too many technical and scientific workers tend to ignore or look down on natural language. They don't think of English as a tool that can and should be used with elegance and skill. Their mathematics may be beautiful, and their programs may be clear and economical, but if their writing is messy their minds are likely to be a bit messy too. The exercise of stating something clearly and directly in good plain English can often clear up the mess for the writer as well as his readers.

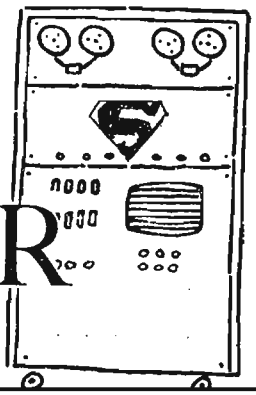
References

"Just Plain English," Department of English, US Air Force Academy, Colorado 80840 (no date).

Strunk, W., Jr., and E. B. White, The Elements of Style, New York, Macmillan, 1972

DOCID: 4009895

NATIONAL SUPERCOMPUTER RESEARCH CENTER(U)



b

P.L. 86-36

Introduction

(U) A National Supercomputing Research Center is important to NSA because it will help us to solve many future supercomputing problems. The word "supercomputing" simply means the intelligent use of the most powerful computational tools currently available. Such a center will probably solve these problems better than we have done before and in a way to help other national defense efforts as well. It will do this with outside people and outside money. But we need to fight for it.

Background

(U) The Chief Scientist of NSA, Mr. Kermith Speierman, was asked by DIRNSA to formulate NSA recommendations for DoD regarding supercomputer initiatives. The Speierman Committee was formed to develop those recommendations and reported to the Director in the autumn of 1983, urging four functions for a federal supercomputing initiative to help supercomputing:

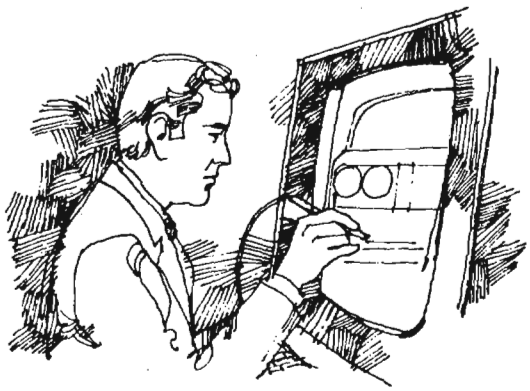
a. In-house, NSA: Highly classified special projects;

b. Defense Parallel Processing Laboratory (DPPL): Medium-level classified work on massively parallel processing for national security in the next decade;

c. NSRC: A largely unclassified lab for supercomputing hardware and software research, with special emphasis on support of:

d. Regional Computational Facilities (RCFs): An unclassified program to provide supercomputer access to academic researchers.

(U) The in-house function is already being performed and will continue. If no other initiatives are acted on, RCFs will be partially done by the National Science Foundation (NSF) and the Department of Energy (DoE) laboratories under existing plans. The really new features are the DPPL and NSRC. But the DPPL seems to be on its way to receiving acceptance. Therefore, this article is dedicated solely to justifying the NSRC.



Possible Objections to the NSRC

(U) The major objections to a new, independent NSRC are four:

1. No need because of current open research;
2. The DoE labs could do this (and they want to);
3. An intense, open research program would transfer information and technology to the outer world; and
4. Suggestions for an NSRC would arouse opposition from DoE or the President's Office of Science and Technology Policy (OSTP) and thus possibly imperil the whole initiative.

(U) I believe that objections 1 and 2 are essentially false (as stated) and that 3 and 4 are true but can still be handled.

Objection 1

(U) This objection is that no radically new efforts in unclassified supercomputing research are necessary because of existing work in government, industry, and academia. However, a look at specific examples (e.g., operating systems and software) shows how inadequate the current efforts really are. The vendors typically supply poor operating systems and FORTRAN. After all, operational software is not their main interest and something really sophisticated is quite beyond their current capability. The result is that the users either get substandard performance from their machines or have to develop new operating systems and languages, usually different from anybody else's.

(U) The DoE labs have developed their own operating systems with a line editor and complicated user commands that would be unsuitable for NSA. The NSA supercomputing environment--i.e., the [redacted] system and IMP language--is powerful and easy to use. Yet it cannot be the general supercomputing standard for various technical reasons. In addition, it is difficult to transfer to different machines. If we soon have a wide variety of supercomputers, it will be impossible for us to maintain [redacted] IMP on all without a great increase in the number of systems programmers. UNIX/C may become the de facto standard since it will soon be available on almost all supercomputers. However, we see it as having inherent inefficiencies that make it difficult to use the full power of the computer when we wish to.

P.L. 86-36

(U) One possible response is to put this problem in the DPPL or keep it in NSA (by using more people). But the systems programming problem is essentially unclassified. How much better to free up NSAers and DPPLers for classified work and put systems software in the NSRC, where it will be serving an independent need anyway (support of the regional centers). Driven by a variety of applications from academia, with a few clever interns from the labs and NSA bringing the best of their methods, the NSRC could have a resounding success. Specifically, they might well develop once and for all a portable, easy, powerful environment that could be used by all and enhance the vendors' products at the same time. And the really great thing is the leverage we get by having this work done by other people with others' money. Similar statements could surely be made in the other areas of NSRC emphasis besides languages and operating systems; i.e., algorithms, hardware technology, architecture, numerical analysis, artificial intelligence, and graphics.

Objection 2

(U) Los Alamos National Labs would dearly love to have the functions of the NSRC. However, even a casual glance at their record must produce skepticism inasmuch as:

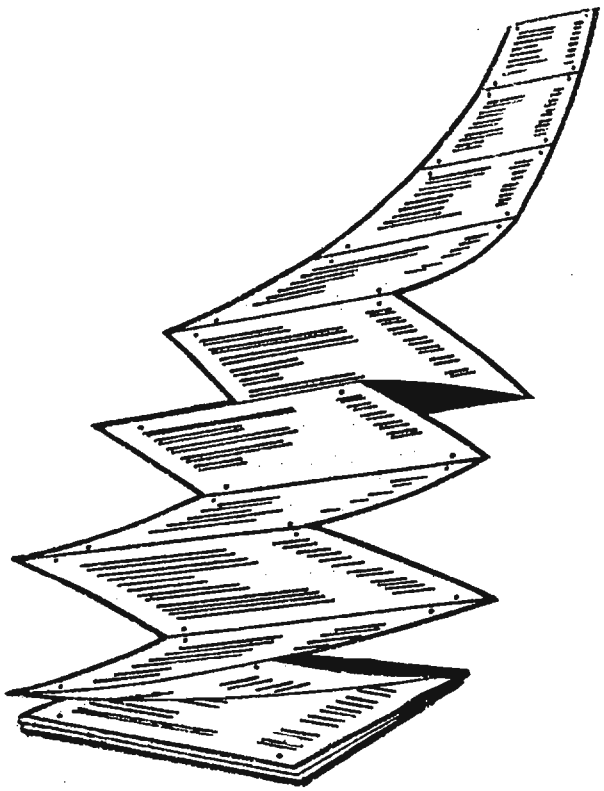
[] they get relatively poor performance from their Crays (the current standard supercomputers);

[] they have a clumsy operating system;

[] they discourage assembly language and modern high-level languages; and

[] they have relatively few experts, partly because they have not encouraged (as NSA has) scientific personnel to become relatively sophisticated.

(U) Maybe they will change if the labels on their doors are changed, but I doubt it. And I doubt that even "safeguards" written into new terms of reference, or even a change of location, would really change their modus operandi. If Los Alamos gets the NSRC, then I predict that the whole effort will be irrelevant to NSA and we will be back to having to use many NSAers and DPPLers to do unclassified work.

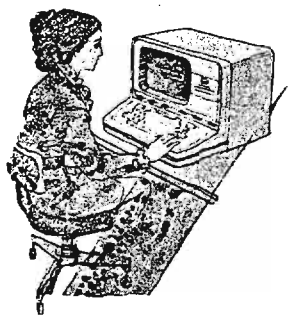


Objection 3

(U) The Speierman federal initiative would result in some information transfer to the outside. However, since the outside world is no longer very far behind us, the real question is what will be the marginal increase in harm (as opposed to what would happen anyway), weighed against the potential benefits to us. Since the in-house programming and the DPPL are classified, the only threat comes from the regional centers and the NSRC. The regional centers should provide only computational access at the end of a telephone line, and that only by grant. Thus the foreign graduate student in astrophysics could get time to study galactic structure, but he could not dump critical software, and he would have to break the terms of his grant to study cryptography on the sly. The NSRC itself should be physically restricted to US nationals since it will have at least company proprietary, and possibly classified, information. The problem with the NSRC is that useful hardware and software work will eventually become public. After all, the people there will be developing very powerful unclassified operating systems. My contention is that the outside world is catching up anyway. It is far better to have them trying to get up to the level of our unclassified base a few years after us than for us to have an unclassified base behind that of other countries and to try to build our classified technology from it.

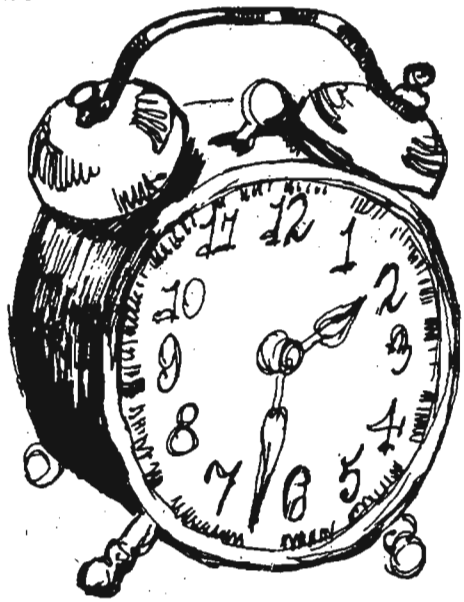
Objection 4

(U) If the NSRC is worth having, it's worth fighting for. We should not regard it as a political chip to be bargained away for DoE support for the whole initiative. The best approach is to keep trying to persuade the interested parties, especially DoE, that the NSRC is in their best interest too. They also will get leverage from having the NSRC solve their problems.



OCID: 4009895

SHELL GAME



TIME SHELLS [U]

by WES

You may not have noticed, but the time function on our UNIX systems has been converted to GMT, or ZULU time. The other day, the phone rang and the voice at the other end said, "The boss would like to see you at 2:45 today." Since I was on the system and probably would be for most of the day, I typed in

```
remind 2:30
See boss at 2:45
```

and finished with a control-D. Then, being a cautious sort (remind has sometimes had a mind of its own), I typed in 'delrem' and looked at what the system thought it was going to do. By now you have guessed that the system, operating in the time zone of the mythical kingdom of ZULU, had stored away my "wake up call" as 1430Z. So much for modern efficiency.

Now I don't really mind using ZULU time, but it's just three more things to remember: the summer difference, the winter difference, and which are we in right now. Frankly, I'm still trying to remember all my PIN numbers (how many bank cards do you have?), and all the passwords to the various systems, and a couple of door combinations, and...well you get the idea. Every time I get another one of these important things to remember, I forget something trivial like a birthday or an anniversary.

So I went looking for some way to get the system to keep track for me. What I found were two shells, one short and sweet, and the other much more involved. Here is the first one, called "tyme":

```
date "+%H" | = t
expr $t - 05 | = t
date "+TIME: %H:%M:%S ZULU ($t:%M EST)"
```

What I hadn't realized was how much the 'date' program had changed since UNIX Version 6. Since Daylight Saving Time runs from the last Sunday of April to the last Sunday of October, I added some commands and the shell now looks like this:

```
date "+%m" | = a
date "+%d" | = b
date "+%w" | = c
expr $b - $c | = d
switch "$a"
:       'standard time'
: 11
: 12
: 01
: 02
: 03
        = e S
        = f 05
        breaksw
:       'last Sunday in April change'
: 04
        if $d -ge 24 then
                = e D
                = f 04
                breaksw
        else
                = e S
                = f 05
                breaksw
        endif
:       'daylight saving time'
: 05
: 06
: 07
: 08
```

```
: 09
        = e D
        = f 04
        breaksw
:       'last Sunday in October change'
: 10
        if $d -ge 25 then
                = e S
                = f 05
                breaksw
        else
                = e D
                = f 04
                breaksw
        endif
endsw
date "+%H" | = t
expr $t - $f | = t
date "+TIME: %H:%M:%S ZULU ($t:%M E$eT)"
```

At the other end of the scale, I found the shell 'time1', written by [redacted] in P14. It begins in the following column.

P.L. 86-36

The original version of Bob's shell uses reverse video to set up a rather startling display on the screen. It will also clobber your terminal if you try to use it across the network. If you get the original version, you could insert a test to see whether the terminal of the user was a network terminal, something like:

```
switch "$t"
: [X-Z]
        (change to net-friendly version ...)
        ...
endsw
```

depending upon how the network terminals are labelled on your host. Then all you need is a second version of those lines that have reverse video, replacing them with whatever your artistic heart desires.

After some discussion, we decided to print the shell without the inverse video, in the interests of minimizing the chaos around the TSS community.

```
goto start
: Bob Jones, P14, 3369-s
: (5741-s)-- 04 Mar 83
: See list of variables at end of file
: start
date "+%H" | = t
date "+%d" | = d
date "+%j" | = c
expr $t - 5 | = l
expr $t + 3 | = m
expr $t + 09 | = k
expr $t + 11 | = f
if $k -gt 23 then
expr $k - 24 | = k
expr $d + 01 | = a
expr $c + 1 | = b
else
expr $d + 0 | = a
expr $c + 0 | = b
endif
if $f -gt 23 then
expr $f - 24 | = f
expr $d + 01 | = g
expr $c + 1 | = h
goto skip
else
expr $c + 0 | = h
= g "$d"
expr $g + 0 | = g
endif
: skip
if "$g" -lt "10" then
= g "0$g"
else
endif
if "$d" -lt "10" then
= d "0$d"
else
endif
if "$h" -lt "100" then
= h "0$h"
else
endif
if "$b" -lt "100" then
= b "0$b"
else
endif
if "$f" -lt "10" then
= f "0$f"
else
endif
if "$k" -lt "10" then
= k "0$k"
else
endif
if "$a" -lt "10" then
= a "0$a"
else
endif
if "$l" -lt "10" then
= l "0$l"
else
endif
if "$m" -lt "10" then
= m "0$m"
```

DOCID: 4009895


```
else goto rundate
endif
: rundate
pump
^G
```

```
**************************************************************************
**************************************************************************
**                                                                      **
**                                                                      **
!
date "+** LOCAL---  DATE: %d %h %y  TIME: $l:%M (EST) JULIAN DATE:  %y%j **"
echo "**                                                                 **"
date "+** ZULU----  DATE: %d %h %y  TIME: $t:%M (Z)   JULIAN DATE:  %y%j **"
echo "**                                                                 **"
date "+** MOSCOW--  DATE: %d %h %y  TIME: $m:%M (C)   JULIAN DATE:  %y%j **"
echo "**                                                                 **"
date "+** KOREA---  DATE: $a %h %y  TIME: $k:%M (I)   JULIAN DATE:  %y$b **"
echo "**                                                                 **"
date "+** FIJI----  DATE: $g %h %y  TIME: $f:%M (L)   JULIAN DATE:  %y$h **"
echo "**                                                                 **"
pump
**                                                                      **
**************************************************************************
**************************************************************************
```

```
^G
!
exit
: 'VARIABLES-(refered to as $t, $m, etc)--t or $t=system hour; d or $d=system '
: 'date; c=system Julian Day; l=local time; m=Moscow time; k=Korean time; '
: 'f=Fiji Time; The following are computed if the time is after 2400 -- '
: 'a=Korean Date; b=Korean J=Day; g=Fiji Day; and h=Fiji J=day. '
: 'Other computations such as 'if $m -lt "10" then' place a zero in front of '
: ' '$m'.  This, and the statements such as 'if "$h" -lt "100" then' are '
: 'required because the math functions will drop leading zeros. '
: ' ^G    -- Rings Terminal Bell'
```

Bob also has a version of this that runs on the IBM PC in living color. I'm sure he would be happy to let you have a copy of either version.

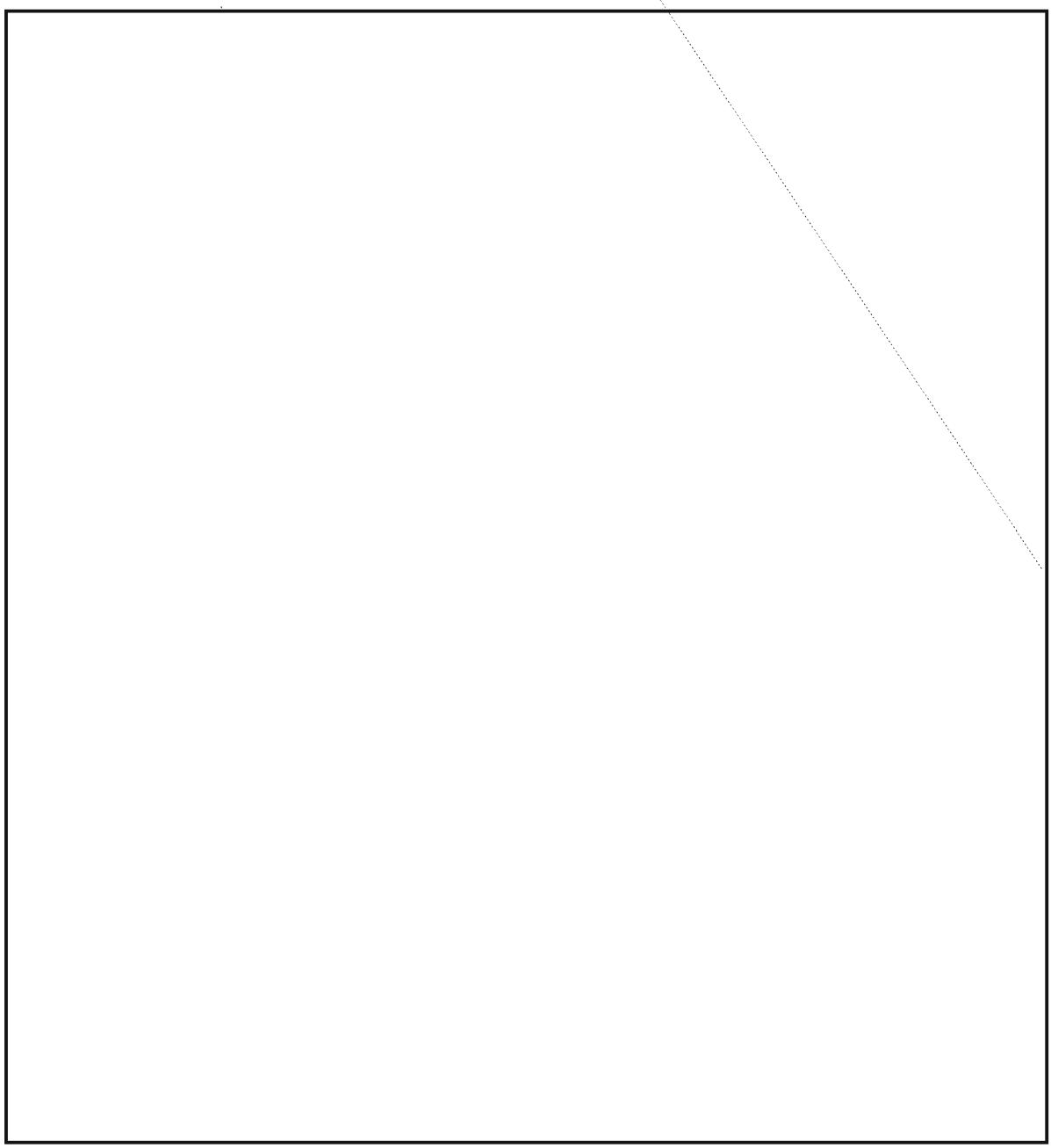
These shells are more for demonstration than anything else, and that is the spirit in which they are presented here. For example, the first shell does not add a leading zero when the local hour is less than ten, and will probably do something weird if the local hour is less than 5. The third shell doesn't quite understand what to do at the end of the month and the 31st day in the land of ZULU may become the 32nd in some other time zone. If some reader comes up with a good fix, we will be happy to print it.

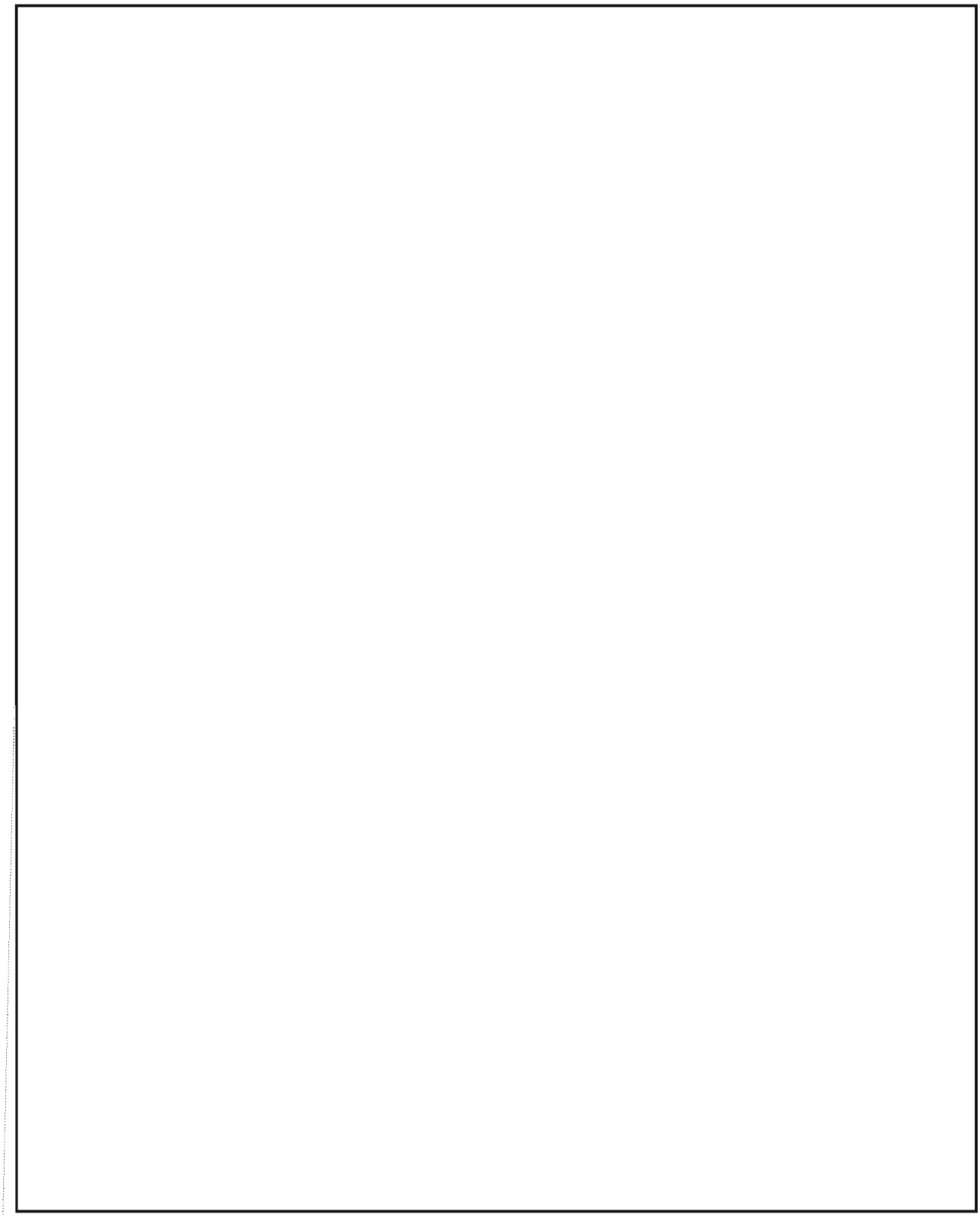
DOCID: 4009895

P.L. 86-36

NSA-Crostic #53

In case you were born on February 29th — Leap Year Day — well then, Happy Birthday to you, too!





P.L. 86-36

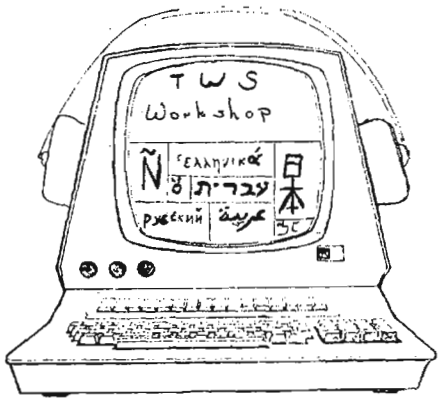
~~FOR OFFICIAL USE ONLY~~

BE PART OF THE PROCESSing

CRYPTO-LINGUISTIC ASSOCIATION

LANGUAGE AUTOMATION COMMITTEE

presents



Translator/Transcriber Work Station

Are you now using computer power in your language activities?

Will you be using it soon?

Feeling frustrated, intimidated, or uninformed about language automation in your office?

At the TWS Work Shop you can
* learn about current and future computer systems
* express your ideas
* share your concerns

4 - 7 June 1984
2W087

Monday, Tuesday, Wednesday	0830-1100
repeated at	1300-1530
Thursday Wrap-up	1300-1500

All interested Green-Badge personnel invited

See you there!

~~FOR OFFICIAL USE ONLY~~

OCID: 4009895

AUTOMATED INFORMATION SECURITY[U]

EDITED BY EDWIN F. STEEBLE, C22

P.L. 86-36

This article is extracted from the Department of Defense Computer Security Center's (DoD CSC) response to the USMC. The Marines had requested computer security guidance and evaluations of several architectural plans. That paper was authored by [redacted] Chief of the Applications Evaluations Systems Office, with aid from [redacted] Chief Scientist, DoD Computer Security Center and [redacted] Col, USAF, Deputy Director, DoD Computer Security Center. The COMSEC policy, procedures, and guidance were supplied by [redacted] COMSEC Doctrine and Threat Assessment Office; [redacted] COMSEC Standards and Evaluations Office; and [redacted] Jr., COMSEC Applications Office.

For this publication minor editing and revisions, mostly to delete USMC specifics, were done by [redacted] Chief, Operational Systems Evaluation Division, DoD Computer Security Center.

I. Computer Security Guidance

A. Policy Requirements

Computer security requirements derive from the need for the information processing system to control access to classified information. These requirements are described more fully in the DoD CSC Trusted Computer System Evaluation Criteria, 15 August 1983 [1]. Briefly, such systems are required to implement the following:

[] MARKING - An ADP system which is used to process or handle classified or other definitely categorized sensitive information shall clearly store and maintain the integrity of classification or other sensitivity marking labels for all information. The system shall assure that the classified or other sensitive information is accurately marked when included in output from the ADP system.

[] MANDATORY SECURITY - The computer system must enforce the formal system of information control reflected in the security classification designation and special handling restriction set associated with the sensitive information handled or processed by the ADP system together with the clearance set associated with the individuals who may request access to the information.

[] DISCRETIONARY SECURITY - The computer system must enforce access limitations placed on classified or other sensitive information based on identified individuals or groups of individuals who have been determined to have a Need-to-Know for the information.

[] ACCOUNTABILITY - An ADP system which is used to process or handle classified information must account for usage on a named-individual basis whenever classified information is generated or accessed.

[] CONTINUOUS PROTECTION - Security-relevant portions of a trusted computer system must be maintained under configuration control to assure that unauthorized changes have not been made which could possibly subvert the system's ability to control classified information.

OCID: 4009895

These policy requirements form the basis for defining security requirements at the system level, as well as for the hardware and software components of the system. They also determine procedural requirements to support the continuous protection policy and assure the operational effectiveness of technical safeguards.

The degree to which a system must comply with these requirements, either in the use of specific security features or in the degree of assurance that the features are effective, is a function of risk of exploitation. This risk depends upon motivation, capability, and opportunity of an opponent to exploit the system's protection controls and mechanisms. These factors, in turn, are influenced by such things as the most sensitive information in the system, the least restrictive clearance of system users or those associated with its development and operation, the hostility of the environment, and time.

B. System Requirements

A primary system requirement is to have a clearly defined security perimeter that includes a suitable combination of manual and automatic trusted processes to control access to classified or sensitive data in the system. Each such process is designed and operated to implement a well-defined interpretation of DoD security policy (e.g., minimally, information that is labeled SECRET will not be accessible by personnel holding less than a SECRET clearance). The perimeter may be entirely defined by environmental (i.e., physical, personnel, and operational security) controls, as is the case in a dedicated mode of operation. It may require hardware, software, and COMSEC controls in addition to the environmental controls. For example, electrically connecting two different computer systems requires hardware and software controls over the interfaces between systems operating at different system-high levels. These controls must ensure, for example, that the integrity of classification labels on internal files is protected and that information flowing from one system to another is classified no higher than the maximum authorized for the receiving system. This, in turn, requires assurance that the integrity of classification labels on internal files is protected in the computers. In the multilevel mode one relies very heavily on controls internal to the computer to enforce applicable security policy, and thus the computer hardware and software controls become an even more critical element of the security perimeter.

The specific security requirements, both technical and environmental, to be enforced by a computer systems application are prescribed by the Designated Approving Authority (DAA), in accordance with DoD Directive 5200.28 or DCI Computer Security Directive "Security of Intelligence Information in Automated Systems and Networks" (formerly DCID 1/16), while the requirements for determining the technical efficacy of the system's security controls and mechanisms are stated in the Center's Trusted Computer Systems Evaluation Criteria. The DAA is then required to make an explicit decision to use the system operationally when convinced that these security requirements are satisfactorily met. We elaborate below on the computer hardware/software certification and accreditation process to support this.

C. Hardware Requirements

Computer systems that are trusted to enforce a security policy employ a combination of hardware and software mechanisms. The hardware mechanisms of concern are those that simplify and optimize the implementation of access control over the subjects and objects as defined in the formal security policy model abstraction. Below we list desirable features worth considering in the selection of a hardware architecture. Note that these features, while helpful, do not supplant the need for a security kernel. However, they may improve performance throughput significantly over the pure use of software controls.

[] Virtual Memory - This hardware feature is essential. It can be realized in either a page- or a segmented-based organization and would provide an effective environment for multiple processes. Both require address mapping circuitry that automatically provides access checking during address translation.

[] Execution Domain - It is minimally essential that the hardware support two execution domains (preferably three), where one domain is privileged and protected from the less privileged domain. Security kernel software runs within the most privileged domain, and untrusted user software executes within the less privileged domain(s).

[] Controlled Access to I/O Devices - It is essential that computer architecture provide some mechanism that enables a security kernel to maintain control over accesses to input/output (I/O) devices. A sufficient solution is the notion of

privileged I/O operations. Here, I/O is performed only by a process executing in the appropriate privileged domain. The kernel must control access to this privileged state.

[] Multiple Processes - Many users normally share concurrently the available resources of a general-purpose computer system, therefore the base computer architecture must provide support for an efficient multiple-process structure. The minimal hardware support necessary is the capability to save and restore process definition information.

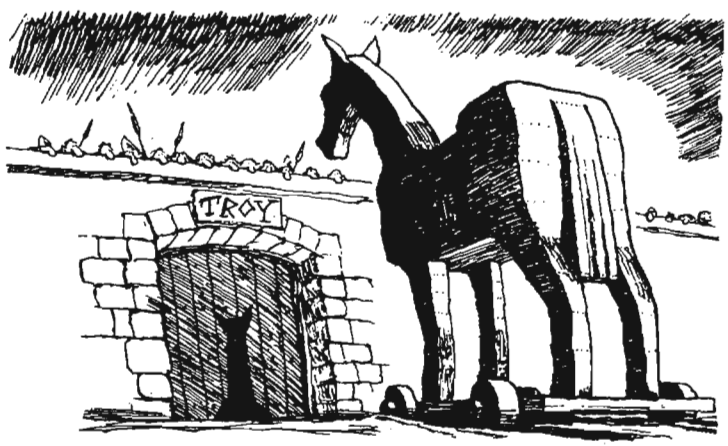
Additional information may be found in MITRE Technical Report No. ESD-TR-78-170 "Minicomputer Architectures For Effective Security Kernel Implementations" by John D. Tangney, dated October 1978.

Because of the reliance one has on these controls, there are several security concerns to be addressed in the acquisition and use of this hardware. One concern is correctness. Assurances must be given to show that the hardware mechanisms have been designed and built to function correctly. A second concern is reliability. Failures in the hardware must not weaken or eliminate the security controls that are implemented in the hardware itself or in the software which, in turn, requires correctly functioning hardware. A third concern is integrity. Configuration control measures during hardware design, implementation, operation, and maintenance must deter accidental or deliberate modifications of the hardware that can cause security controls to be bypassed or weakened. The degree of concern in each area and the corresponding steps taken to reduce the risk is application-dependent. Although exploiting such avenues of vulnerability is possible, one must consider them in the context of other areas which could be more susceptible to attack (e.g., software).

In those cases where the hardware will be used in a periods processing mode, it should permit rapid and reliable erasure of all internal memory (e.g., primary storage, non-removable secondary storage and buffers). It must also support the capability for a physical disconnect from those other devices in areas with a lesser degree of protection. There is ongoing research as part of the consolidated DoD Computer Security R&D program to develop a "job stream separator" which automatically and reliably performs all necessary color change procedures.

In those cases where the computer will simultaneously process or store information of different classifications, the hardware should support internal labeling of files with the appropriate security classification, and these internal labels should be used as the primary basis for access control decisions. This is particularly the case if the system users are not all authorized access to all of these files (e.g., as in the controlled or multilevel mode of operation). A similar requirement may exist for systems which process personnel proprietary or other sensitive unclassified information.

Individual hardware components must meet TEMPEST requirements commensurate with their operational environment, current policy, and the perceived threat of exploitation.



DOCID: 4009895

D. Software Requirements

Software that must enforce DoD security policy must be designed, implemented, and documented to permit credible evaluation and verification that it, in fact, correctly enforces that policy. This requirement would have to be applied to all system software including the operating system, system utilities, data base management systems (DBMS), compilers, or application software. Such evaluation would be difficult and lack credibility if the security-relevant mechanisms are complex and scattered throughout the software. One simply cannot determine that an unstructured collection of these mechanisms correctly implements the policy and cannot be circumvented. Thus, the Center requires that in trusted computer systems all security-related functions be implemented in well-defined portions of software, firmware, and hardware, the totality of which is called the trusted computing base (TCB). The TCB must be designed and implemented so that its security controls are always invoked and are tamperproof, that is, the controls cannot be modified or bypassed by the remaining (untrusted) portions of the system and that they be of sufficiently simple design as to be subjected to thorough test and analysis. During its design and development, the TCB is subjected to specification and design analysis verification and testing to assure that these properties are indeed satisfied. The DoD CSC Trusted Computer System Evaluation Criteria amplify these requirements further.

Determining the specific requirements for software controls and level of assurance, i.e., the evaluation class, for a particular application must reflect the level of risk and degree of trust required of the hardware and software. One indicator of this is security range that is, the difference between the classification of the most sensitive information and the least restrictive user clearance. Thus, for example, a Class C2 system may provide adequate trust for a system-high application. A multilevel mode application would, on the other hand, normally be expected to meet the criteria of a Class B2 or higher system, depending on its security range.

E. Procedures

The continuous protection requirement is primarily satisfied with procedures to control and monitor access to hardware and software security components during their design and implementation, and then during their operational life cycle. Such procedures are a critical part of gaining assurance that the security mechanisms are designed and built to meet stated requirements and then maintained and used to remain effective. Specific requirements include:

[] clearing system support personnel to the highest level of data in the system;

[] clearing maintenance personnel commensurate with the sensitivity of information to which they could get access; and

[] developing and maintaining software which protects sensitive information in an environment consistent with the sensitivity of the data being protected and with a level of risk that is acceptable to owners of sensitive information.

In systems which involve periods processing, accreditable procedures are needed to change processing classification levels. Procedures include removing sensitive data from the system, disconnecting or reconnecting peripheral devices and remote terminals, and rebooting the appropriate operating system at the new processing level.

F. Classified Software

The security mechanisms and their implementation in trusted system hardware and software are generally unclassified. However, as noted earlier, this software may be treated as if it were classified to meet the continuous protection requirement. There may be instances in which security-related software is classified (e.g., if it implements a classified cryptographic algorithm) or security-related software contains classified data (e.g., the routing tables in a message system). Such software must be protected like any other classified information while it is stored in the computer. There may be multiple copies of it in primary and secondary storage, all of which must be labeled and protected, as must all hardcopy printouts of it.

G. General

It is DoD policy that all ADP systems which process classified information will be accredited; that is, there will be an explicit decision that the system adequately protects information and can be used operationally. This accreditation is frequently based upon a technical evaluation of the system to determine how well it meets predefined requirements. However, unless the system is designed and built to be evaluated, as is NOT the case with most existing computer systems, the technical evaluation consists almost entirely of looking for flaws in the system or conducting tests of the system's ability to withstand penetration. Neither case gives assurance that the system is secure because such exhaustive testing never finishes. Thus, it is vitally important that security requirements be identified early in the system's development. It is equally important that the system security architecture identify trustworthy mechanisms to control the flow of information into, out of, and within the system. One can then determine explicitly the policy model which each trusted hardware and software component of this architecture must enforce and the appropriate Trust Class as described in the Criteria. One can then specify, implement, verify, and certify that those enforcement mechanisms that are implemented correctly enforce the policy. To assist with this, there is a growing collection of formal design and verification methodologies which can be used. These include SRI's Hierarchical Development Methodology, University of Texas' GYPSY system, and SDC's Formal Development Methodology. The C organization is undertaking an effort to make these tools more easily available to and usable by system developers as well as by NSA and DoD system test and evaluation organizations.

Computer vendors, (i.e., DEC, UNIVAC, Honeywell, etc.) have developed or are developing trusted systems which might meet long-range requirements. Additionally, software houses are developing add-on packages to provide a little increase in software security (i.e., SKK's ACF2, IBM's RACF, CGA's Top Secret, etc.). In Section III below we note other possible uses of trusted systems as part of the security architecture. Thus, a first step in developing the architectural strategy and planning for using trusted systems would be to determine what the long-term security requirements are (i.e. will multilevel security become an operational necessity, and if so, over what range of classification and user clearance?).

ADP Security Certification/Accreditation Planning Guide (reference #2) provides additional information on the critical steps in the certification/accreditation process. Further direct interaction with the user, designer, and C2 could follow the reading of this literature and enable C2 to work on recommending or finalizing a recommended secure system.

II. Telecommunications

A well-defined, layered network security architecture is needed that

[] addresses all the threats of concern to the user; and

[] is consistent with, or is at least not incompatible with, the security architectures of networks to which various users are connecting.

It is desirable to have a single, layered, inter-network security architecture that can be deployed across all DoD certified nets. An ambitious DoD effort is under way to achieve this initiative.

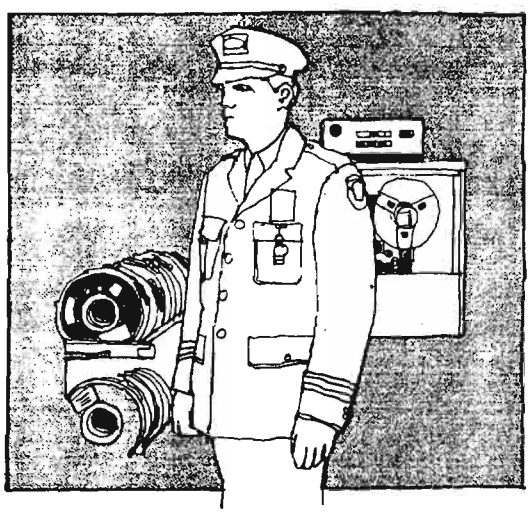
III. Policy

Electrical Interfaces - Electrical interfaces between systems operating at different classification levels must ensure that only appropriately classified information flows from the more sensitive to the less sensitive system. It must also prevent users of the less sensitive system from making unauthorized changes, accidentally or deliberately, to data in the other system or from disrupting its use. A manual interface has, until recently, been the accepted method. However, trustworthy devices for controlling such interfaces have been proposed for several systems. One such device currently in development will use the Honeywell SCOMP as a basis for implementing a GUARD to allow SECRET users to access SECRET data bases on the US Army Forces Command's Top Secret system-high WWMCCS computer. There is another approach which uses a cryptographically derived cryptographic check to verify the releasability of information when it is being electronically transferred between security perimeters (reference #3).

*-Property[2] - DoD security policy for ADP systems was discussed in Section I above. The *-property is one part of the Bell & La Padula[3] policy model for mandatory security. It is more conservative than DoD policy as it relates to paper documents but it precludes the success of Trojan Horse attacks.

Data Aggregation - DoD policy for correct classification and handling labels for data elements (alone or in aggregate) should be implemented in data processing systems. This requires reliable labels on internal files and on output giving the classifications or other special handling instructions, as determined by the owner of the information at the field, record, file, or data base level, as appropriate.

Data Encryption Standard (DES) - Present policy requires that NSA approve, on a case-by-case basis, any proposed use of DES to protect classified communications. With respect to the use of DES to protect unclassified, national security-related communications, recently issued national policy requires that Services, Departments, and Agencies determine the risk of exploitation of their unclassified communications, either in consultation with or based upon prior guidance from NSA in accordance with Federal Standard (FS) 1027. Where there is high risk of exploitation, NSA will prescribe or approve the cryptographic system used, on a case-by-case basis. For all other applications, commercial cryptographic systems (to include DES) may be used if they have been endorsed for general application by NSA.



IV. General

There will be additional costs associated with implementing, using, and maintaining physical, emanations, personnel, and procedural security safeguards. Some of this additional cost (e.g., for physical and emanations safeguards) is part of the capital investment. On the other hand, the costs for personnel and procedural safeguards are part of the operational costs. The actual costs for a facility depend upon the level of protection required for the information being processed in a given threat environment. There will also be additional costs associated with acquiring and using trusted computer systems. Designing security into the system can lower these costs and have a beneficial payoff through improved reliability and maintainability which results from a well-structured software design and implementation. We note that there are two key aspects to be considered in estimating the cost of safeguards in these security areas. They are (1) what level of protection is required, and (2) how must these safeguards be used and maintained to ensure their continued effectiveness?

[Doesn't protection of sources, methods, and products require this? EFS]

Footnotes

1. This and the other referenced papers can be obtained from the DoD CSC Technical Library (C422).
2. Pronounced "star property"
3. [redacted] was recently hired as Deputy Chief of C3.

P.L. 86-36

Bibliography

1. Trusted Computer System Evaluation Criteria, CDC-STD-001-83, 15 Aug 83 (S-225,711).
2. ADP Security Certification/Accreditation Planning Guide, undated.
3. On the Feasibility of Connecting RECON to an External Network, [redacted] dated 16 Mar 81.

P.L. 86-36

DOCID: 4009895

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

EO 1.4.(c)
P.L. 86-36

CRYPTOLOG 1983 INDEX (U)

The following is a cumulative index of CRYPTOLOG (Vol X, 1983) and is in three parts, by title, by author, and by keyword. Items in multiple issues (January-February 1983, for example) are indicated by the first month (i.e., by Jan 83).

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

TITLES (U)

Acronymania; Nov 83; [redacted]
Ada News; Jan 83; [redacted]
Ada: Conquering the Tower of Babel; Jan 83; [redacted] Apr 83; [redacted]
Announcement: Contributions Solicited for CRYPTOLOG Articles; Sep 83;
Announcement: KRYPTOS Society Spring Meeting; Mar 83;
Announcement: Request for Copies of Jan-Feb 83 Issue (CISI Essay Contest); Aug 83;
Announcement: Students! (NCEUR Independent Study Programs); Mar 83;
Announcement: Two New Language Aids [redacted] and Chinese-English); Jun 83;
Banners, Cowboy Hats, and ELINT Notations; Oct 83; [redacted]
The Case of the 'Fowled-Up' CRITIC; Aug 83; [redacted] Nov 83; [redacted]
Computer Graphics to Enhance Collection Management; Jan 83; [redacted]
Computerizing Traffic Analysis; May 83; [redacted]
Confessions of a Briefer; May 83; [redacted]
Correction: Do You Know the Differences?, Jun-Jul 83 Issue; Aug 83;
Correction: October 1983 CRYPTOLOG Issue Add to Classification: 'REL UK CAN AUS NZ'; Dec 83;
Crisis Management: Remarks; Oct 83; [redacted] L.D.
Cryptic Crossword #3; Mar 83; [redacted]
Cryptography At GLOBECOM 82; May 83; [redacted] J.A.
Cumulative Index (1974-1982), Part 1: Authors; Mar 83;
Cumulative Index (1974-1982), Part 2: Titles; Apr 83;
Cumulative Index (1974-1982), Part 3: Keywords; May 83;
DCL; The Direct Communications Link; Dec 83; [redacted]
Do You Know the Differences?; Jun 83; [redacted] D.S.
Do You Really Mean Julian?; Sep 83; [redacted] C.
Does Your Office Make You Sick?; Aug 83; [redacted]
E.T. At NSA; Mar 83;
FBIS Latin American Reference Aid; Apr 83; [redacted] 1975-77; Sep 83; [redacted] 1982; Sep 83; [redacted] Apr 83; [redacted]
5-4-3 Puzzle; Nov 83; 'Watt Zizname'
Foreign Microwave Radio; Sep 83; [redacted]
Frontier Dentist; Apr 83; 'Marian D. Librarian'
The Future Brightens for Flat-Panel Displays; Jan 83; [redacted]
Getting Personal; Jan 83; [redacted]
Government of the People, By The Party, For The Leadership; Apr 83; [redacted] Jun 83; [redacted]
I Remember JFK; Nov 83; H.G.R
I Remember Mabel Babel; Aug 83 [redacted]
Improving Raster Graphics Images by Anti-Aliasing; Jan 83; [redacted]
The Intelligence Watch Officer; May 83; [redacted] L.S.
Is The Glass Half Empty Or Half Full?; Mar 83; [redacted]
The Islamic Time Bomb; Dec 83; [redacted] F.W.
Letter to the Editor: Computerizing of TA, May 83 Issue; Nov 83; [redacted]
Letter to the Editor: Government of the People... reply to [redacted] letter; Aug 83; [redacted]
Letter to the Editor: Government of the People..., Apr 83 Issue; Aug 83; [redacted]
Letter to the Editor: Management of Coordination, Sep 83 Issue; Oct 83; 'Juan Tuthri'
Letter to the Editor: My Staff--It Comforts Me, Apr 83 Issue; Aug 83; [redacted]
Letter to the Editor: Out of My Depth, May 83 Issue; Aug 83; [redacted]

P.L. 86-36

P.L. 86-36

EO 1.4.(d)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

P.L. 86-36

Letter to the Editor: Redbaron, Roadrunner..., Jun-Jul 83 Issue; Sep 83; [redacted]
Letter to the Editor: Security of Classified Information; Jun 83; [redacted]
Letter to the Editor: The Tower of Babel; May 83; Mollick J.J.
Letter to the Editor: Tips on Topical Reporting, Oct 83 Issue; Dec 83; [redacted]
Letter to the Editor: Tips on Topical Reporting, reply to [redacted] letter; Dec 83; [redacted]
Letter to the Editor: UNIX ED (I) Manual Page Comment; Oct 83; [redacted]
Letter to the Editor: Video Teleconferencing, Mar 83 Issue; Jun 83; [redacted]
The Literary Bends; Nov 83; Murphy A.I.
Logic Design Exceeding Boolean Capabilities; Jan 83; [redacted]
MBTI: The Management Tool of the Future; Nov 83; [redacted]
Man Does Not Live By Matzos Alone; Apr 83; 'Marian D. Librarian'
Management of Coordination; Sep 83; [redacted]
Managing Our Systems for Performance; Jan 83; [redacted]
Menu Selection As A Tool for Human/Machine Interaction; Jan 83; [redacted]
[redacted]
Mar 83; [redacted]
[redacted]
Dec 83; [redacted]
More on Passwords; Mar 83; [redacted]
My Staff--It Comforts Me; Apr 83; 'Zebulon Zilch'
NSA in The Space Age; Apr 83; [redacted]
The NSA High-level Display File; Jan 83; [redacted]
[redacted] Jun 83;
[redacted]
NSA-Crostic No. 46; Apr 83; Williams D.H.
NSA-Crostic No. 47; May 83; Williams D.H.
NSA-Crostic No. 48; Jun 83; Filby V.R.
NSA-Crostic No. 49; Aug 83; Williams D.H.
NSA-Crostic No. 50; Sep 83; Williams D.H.
NSA-Crostic No. 51; Dec 83; Williams D.H.
1982 Local Area Network Status; Jan 83; [redacted] E.M.
Non Posse vs. Posse Non; Dec 83; [redacted] H.G.
On How The 'Game' of the Agency Should Be Played; Sep 83; Santiago-Ortiz R.
Out of My Depth; May 83; P.L. 86-36
Out of My Depth; Dec 83;
PARPRO: Reconnaissance Programs; Sep 83; [redacted]
Picture: What Is The Caption?; Nov 83;
Punching The Biological Timeclock; Jun 83; [redacted]
Puzzle; Jan 83; Williams D.H.
Redbaron, Roadrunner, Bronzstar: What's In A Name?; Jun 83; [redacted]
Review: The Battle For The Falklands; Aug 83; [redacted]
Review: Digital Telephony; May 83; [redacted] J.A.

P.L. 86-36

SIGINT Challenge: A Scenario; Mar 83; [redacted] J.L.
Shell Game: System Shells; Dec 83; [redacted] W.E.
Shell Using If; Mar 83; [redacted]
Some Tips on Getting Promoted; Jun 83; [redacted] V.
Soviet Military Goals And Their Effect on Negotiations for Arms Limitations; Oct 83; [redacted]
Soviet Psi Experiments; Dec 83; [redacted]
Specifying Colors for Computer Graphics; Apr 83; [redacted]
Static Magic: The Wonderful World of Tempest; Nov 83; Donahue T.M.
Still More About Passwords; May 83; [redacted] M.E.
A Survey of Parallel Sorting; Jan 83; [redacted] S.B.
TDY Travail; Mar 83; Filby V.R.
TELECOM 83:; Oct 83; [redacted]
Tempest for Every Office; Nov 83; [redacted]
Thousands Miss Demonstration; Oct 83; [redacted] R.L.
Tips on Topical Reporting; Oct 83; [redacted]
A Tutorial on Color Theory and Human Color Perception for the Color Graphics Programmer; Jan 83; [redacted]
UIS: User Interface System Part One: Concept; Apr 83; [redacted]
UIS: User Interface System Part Two: Architecture; Apr 83; [redacted]
Video Teleconferencing: NSA Applications; Mar 83; [redacted]
Weather: A Key Intelligence Indicator; Mar 83; [redacted]
The White House Is Singing Our Song; Nov 83; Murphy A.I.
Why Pascal? (Why Not?); Jun 83; [redacted]
Word People at NSA; Apr 83; 'Dickson Airy'
Wrangler...One Tough Customer; Sep 83; [redacted]

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

AUTHORS (U)

Mar 83 Announcement: KRYPTOS Society Spring Meeting
Mar 83 Announcement: Students! (NCEUR Independent Study Programs)
Mar 83 Cumulative Index (1974-1982), Part 1: Authors
Mar 83 E.T. At NSA
Apr 83 Cumulative Index (1974-1982), Part 2: Titles
Apr 83 FBIS Latin American Reference Aid
May 83 Cumulative Index (1974-1982), Part 3: Keywords
May 83 Out of My Depth
Jun 83 Announcement: Two New Language Aids [redacted] and Chinese-English)
Aug 83 Announcement: Request for Copies of Jan-Feb 83 Issue (CISI Essay Contest)
Aug 83 Correction: Do You Know the Differences?, Jun-Jul 83 Issue
Sep 83 Announcement: Contributions Solicited for CRYPTOLOG Articles
Nov 83 Picture: What Is The Caption?
Dec 83 Correction: October 1983 CRYPTOLOG Issue Add to Classification: 'REL UK CAN AUS NZ'
Dec 83 Out of My Depth

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

'Dickson Airy'
Apr 83 Word People at NSA

'Juan Tuthri'
Oct 83 Letter to the Editor: Management of Coordination, Sep 83 Issue

'Marian D. Librarian'
Apr 83 Frontier Dentist
Apr 83 Man Does Not Live By Matzos Alone

"H.G.R"
Nov 83 I Remember JFK

'Watt Zizname'
Nov 83 5-4-3 Puzzle

'Zebulon Zilch'
Apr 83 My Staff--It Comforts Me

[redacted]
Mar 83 [redacted]

[redacted]
Dec 83 DCL; The Direct Communications Link

[redacted]
Jun 83 Letter to the Editor: Video Teleconferencing, Mar 83 Issue

[redacted]
Aug 83 The Case of the 'Fowled-Up' CRITIC

[redacted]
Oct 83 Tips on Topical Reporting
Dec 83 Letter to the Editor: Tips on Topical Reporting, reply to Day's letter

[redacted]
Jan 83 Ada: Conquering the Tower of Babel

[redacted]
Mar 83 Cryptic Crossword #3

[redacted]
Jun 83 Punching The Biological Timeclock

[redacted]
Mar 83 More on Passwords
Apr 83 Specifying Colors for Computer Graphics
May 83 Still More About Passwords
Aug 83 Does Your Office Make You Sick?
Nov 83 MBTI: The Management Tool of the Future

[redacted]
Jun 83 Punching The Biological Timeclock

[redacted]
Mar 83 [redacted]

[redacted]
Dec 83 Letter to the Editor: Tips on Topical Reporting, Oct 83 Issue

[redacted]
Sep 83 PARPRO: Reconnaissance Programs

[redacted]
Nov 83 Static Magic: The Wonderful World of Tempest

[redacted]
Mar 83 Weather: A Key Intelligence Indicator

[redacted]
Nov 83 [redacted]

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

[redacted]
Oct 83 Thousands Miss Demonstration

Faurer L.D.
Oct 83 Crisis Management: Remarks

[redacted]
Jan 83 Ada News

Filby V.R.
Mar 83 TDY Travail
Jun 83 NSA-Crostic No. 48

[redacted]
Mar 83 SIGINT Challenge: A Scenario

[redacted]
Jan 83 Improving Raster Graphics Images by Anti-Aliasing

[redacted] EO 1.4.(c)
Jan 83 Getting Personal P.L. 86-36

[redacted]
Aug 83 Letter to the Editor: Government of the People..., Apr 83 Issue

[redacted]
Sep 83 Management of Coordination
Nov 83 Acronymania

[redacted] P.L. 86-36
May 83 Confessions of a Briefer

[redacted]
Apr 83 UIS: User Interface System Part One: Concept

[redacted]
Jun 83 [redacted]

[redacted]
Apr 83 [redacted]

P.L. 86-36

[redacted]
Jun 83 Some Tips on Getting Promoted

EO 1.4.(d)

[redacted]
Nov 83 Letter to the Editor: Computerizing of TA, May 83 Issue

[redacted]
Mar 83 Shell Using If

[redacted]
Aug 83 Letter to the Editor: Out of My Depth, May 83 Issue

[redacted]
Jun 83 Why Pascal? (Why Not?)

[redacted]
Oct 83 Soviet Military Goals And Their Effect on Negotiations for Arms Limitations

P.L. 86-36

P.L. 86-36

[redacted]
Dec 83 The Islamic Time Bomb

[redacted]
Oct 83 Letter to the Editor: UNIX ED (I) Manual Page Comment

[redacted]
Apr 83 NSA in The Space Age

[redacted]
Nov 83 Tempest for Every Office

[redacted]
Jun 83 Redbaron, Roadrunner, Bronzstar: What's In A Name?

[redacted]
Apr 83 Government of the People, By The Party, For The Leadership
Aug 83 Letter to the Editor: Government of the People... reply to [redacted] letter

[redacted]
Apr 83 [redacted]
May 83 Cryptography At GLOBECOM 82
May 83 Review: Digital Telephony
Aug 83 Review: The Battle For The Falklands
Sep 83 Foreign Microwave Radio EO 1.4.(c)
Oct 83 TELECOM 83: P.L. 86-36
Dec 83 Soviet Psi Experiments

[redacted]
May 83 Letter to the Editor: The Tower of Babel

[redacted]
Jan 83 A Survey of Parallel Sorting

[redacted]
Sep 83 Do You Really Mean Julian?

Murphy A.I.
Nov 83 The Literary Bends
Nov 83 The White House Is Singing Our Song

[redacted]
Jan 83 Computer Graphics to Enhance Collection Management

[redacted]
Jan 83 The Future Brightens for Flat-Panel Displays

[redacted]
Jan 83 1982 Local Area Network Status

[redacted]
Jun 83 Do You Know the Differences?

[redacted]
Mar 83 Is The Glass Half Empty Or Half Full?

P.L. 86-36

P.L. 86-36

[redacted]

Jun 83 [redacted]

Aug 83 I Remember Mabel Babel
Aug 83 Letter to the Editor: My Staff--It Comforts Me, Apr 83 Issue
Dec 83 Non Posse vs. Posse Non

[redacted]

Jan 83 Menu Selection As A Tool for Human/Machine Interaction

[redacted]

Sep 83 Letter to the Editor: Redbaron, Roadrunner..., Jun-Jul 83 Issue

[redacted]

Sep 83 On How The 'Game' of the Agency Should Be Played

[redacted]

Jan 83 The NSA High-level Display File

[redacted]

Apr 83 UIS: User Interface System Part Two: Architecture

[redacted]

Jan 83 Logic Design Exceeding Boolean Capabilities

[redacted]

Dec 83 [redacted]

[redacted]

Mar 83 Video Teleconferencing: NSA Applications

[redacted]

May 83 The Intelligence Watch Officer

[redacted]

Jun 83 [redacted]

[redacted]

Oct 83 Banners, Cowboy Hats, and ELINT Notations

[redacted]

May 83 Computerizing Traffic Analysis
Dec 83 Shell Game: System Shells

[redacted]

Sep 83 [redacted]
Sep 83

[redacted]

Jan 83 Managing Our Systems for Performance

[redacted]

Jan 83 A Tutorial on Color Theory and Human Color Perception for the Color Graphics Programmer

P.L. 86-36

P.L. 86-36

[redacted]

Sep 83 Wrangler...One Tough Customer

[redacted]

Jun 83 Letter to the Editor: Security of Classified Information

Williams D.H.
Jan 83 Puzzle
Apr 83 NSA-Crostic No. 46
May 83 NSA-Crostic No. 47
Aug 83 NSA-Crostic No. 49
Sep 83 NSA-Crostic No. 50
Dec 83 NSA-Crostic No. 51

[redacted]

Jan 83 Computer Graphics to Enhance Collection Management

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

KEYWORDS (U)

Acronyms
Nov 83 Acronymania;

Ada
Jan 83 Ada News;
Jan 83 Ada: Conquering the Tower of Babel;

EO 1.4.(c)
P.L. 86-36
Apr 83

Aircraft
Sep 83 PARPRO: Reconnaissance Programs;

P.L. 86-36

Book Review
Apr 83 Frontier Dentist;
'Marian D. Librarian'
Apr 83 Man Does Not Live By Matzos Alone;
'Marian D. Librarian'
Aug 83 Review: The Battle For The Falklands;

P.L. 86-36

Briefing
May 83 Confessions of a Briefer; Hankey J.

CAA News
Oct 83 Crisis Management: Remarks; Faurer L.D.

Caption
Nov 83 Picture: What Is The Caption?;

Chinese
Jun 83 Announcement: Two New Language Aids and Chinese-English);

Classification
Jun 83 Do You Know the Differences?; Rankin D.S.
Aug 83 Correction: Do You Know the Differences?, Jun-Jul 83 Issue;
Dec 83 Correction: October 1983 CRYPTOLOG Issue Add to Classification: 'REL UK CAN AUS NZ';

P.L. 86-36

Collection
Jan 83 Computer Graphics to Enhance Collection Management;
Mar 83 Is The Glass Half Empty Or Half Full?;
Nov 83
Dec 83 Modernization of G Group's High-Frequency Intelligence Collections; W.G.

Color
Apr 83 Specifying Colors for Computer Graphics;

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

COMINT
Mar 83

P.L. 86-36

Communications
Sep 83 Foreign Microwave Radio;
Dec 83 DCL; The Direct Communications Link;

Computer Applications
Jan 83 A Survey of Parallel Sorting; S.B.
Jan 83 Computer Graphics to Enhance Collection Management;
Jan 83 The NSA High-level Display File;
Mar 83
May 83 Computerizing Traffic Analysis;

EO 1.4.(c)
P.L. 86-36

Computer Graphics
Jan 83 A Tutorial on Color Theory and Human Color Perception for the Color Graphics Programmer;
Jan 83 Computer Graphics to Enhance Collection Management;
Jan 83 Improving Raster Graphics Images by Anti-Aliasing;
Jan 83 The NSA High-level Display File;
Apr 83 Specifying Colors for Computer Graphics;

P.L. 86-36

Computer Networks
Jan 83 1982 Local Area Network Status; E.M.
Apr 83

Computer Programming
Jan 83 Ada News;
Jan 83 Ada: Conquering the Tower of Babel;
Jan 83 Menu Selection As A Tool for Human/Machine Interaction;
Mar 83 Shell Using If;
Jun 83 Why Pascal? (Why Not?);
Dec 83 Shell Game: System Shells; W.E.

Computer Security
Mar 83 More on Passwords;
May 83 Cryptography At GLOBECOM 82; J.A.
May 83 Review: Digital Telephony; J.A.
May 83 Still More About Passwords; D'Imperio M.E.

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

Computer Systems
Jan 83 Getting Personal; [redacted]
Apr 83 UIS: User Interface System Part One: Concept [redacted]
Apr 83 UIS: User Interface System Part Two: Architecture; [redacted]
Sep 83 Wrangler...One Tough Customer; [redacted]

Computer Systems Management
Jan 83 Managing Our Systems for Performance; [redacted]

Computer TA
Nov 83 Letter to the Editor: Computerizing of TA, May 83 Issue; [redacted]

Coordination
Sep 83 Management of Coordination; [redacted]
Oct 83 Letter to the Editor: Management of Coordination, Sep 83 Issue; 'Juan Tuthri'

Covername
Jun 83 Redbaron, Roadrunner, Bronzstar: What's In A Name?; [redacted]
Sep 83 Letter to the Editor: Redbaron, Roadrunner..., Jun-Jul 83 Issue; [redacted]

CRITIC
Aug 83 The Case of the 'Fowled-Up' CRITIC; [redacted]

P.L. 86-36

CRT
Jan 83 The Future Brightens for Flat-Panel Displays; [redacted] J.

Crypto-TA
May 83 Out of My Depth;
Aug 83 Letter to the Editor: Out of My Depth, May 83 Issue; [redacted]
Dec 83 Out of My Depth;

Cryptography
May 83 Cryptography At GLOBECOM 82; [redacted] J.A.
May 83 Review: Digital Telephony; [redacted] J.A.
Oct 83 TELECOM 83:; [redacted]

P.L. 86-36

CRYPTOLOG
Mar 83 Cumulative Index (1974-1982), Part 1: Authors;
Apr 83 Cumulative Index (1974-1982), Part 2: Titles;
May 83 Cumulative Index (1974-1982), Part 3: Keywords;
Aug 83 Announcement: Request for Copies of Jan-Feb 83 Issue (CISI Essay Contest);
Sep 83 Announcement: Contributions Solicited for CRYPTOLOG Articles;
Dec 83 Correction: October 1983 CRYPTOLOG Issue Add to Classification: 'REL UK CAN AUS NZ';

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

Data Security
Jun 83 Letter to the Editor: Security of Classified Information [redacted]

Data Standards
Sep 83 Do You Really Mean Julian?; [redacted] C.

ELINT
Sep 83 Wrangler...One Tough Customer; [redacted]
Oct 83 Banners, Cowboy Hats, and ELINT Notations; [redacted]

English
Aug 83 I Remember Mabel Babel; [redacted]

ESP
Dec 83 Soviet Psi Experiments; [redacted]

[redacted]
Jun 83 [redacted]
Sep 83 [redacted]
Sep 83 [redacted]

P.L. 86-36

Field Station
Mar 83 Is The Glass Half Empty Or Half Full?; [redacted]
Apr 83 Field Station Network Applications; [redacted]
Oct 83 Thousands Miss Demonstration; [redacted] R.L.

P.L. 86-36

Greek
Jun 83 Announcement: Two New Language Aids [redacted]

HF
Dec 83 [redacted] W.G.

P.L. 86-36

History
Nov 83 [redacted]

Hotline
Dec 83 DCL; The Direct Communications Link; [redacted]

Human Factors
Jan 83 Menu Selection As A Tool for Human/Machine Interaction; [redacted]
Apr 83 Specifying Colors for Computer Graphics; [redacted]
Jun 83 Punching The Biological Timeclock; Creswell D.T. [redacted]
Aug 83 Does Your Office Make You Sick?; [redacted]

P.L. 86-36

DOCID: 4009895 EO 1.4.(c) P.L. 86-36

HUMINT
Jun 83 [redacted]

Humor
Apr 83 Frontier Dentist; 'Marian D. Librarian'
Apr 83 Man Does Not Live By Matzos Alone; 'Marian D. Librarian'
Apr 83 My Staff--It Comforts Me; 'Zebulon Zilch'
Apr 83 NSA in The Space Age; [redacted]
Apr 83 Word People at NSA; 'Dickson Airy'
May 83 Letter to the Editor: The Tower of Babel; [redacted]
Aug 83 Letter to the Editor: My Staff--It Comforts Me, Apr 83 Issue; [redacted]

Index
Mar 83 Cumulative Index (1974-1982), Part 1: Authors;
Apr 83 Cumulative Index (1974-1982), Part 2: Titles;
May 83 Cumulative Index (1974-1982), Part 3: Keywords;

Indicators
Mar 83 Weather: A Key Intelligence Indicator; [redacted]

Iran
Dec 83 The Islamic Time Bomb; [redacted] F.W.

P.L. 86-36

Islam
Dec 83 The Islamic Time Bomb; [redacted] F.W.

[redacted]
Aug 83 The Case of the 'Fowled-Up' CRITIC; [redacted]

P.L. 86-36

KRYPTOS News
Mar 83 Announcement: KRYPTOS Society Spring Meeting;

Language
Jun 83 Announcement: Two New Language Aids [redacted] and Chinese-English);
Jun 83 [redacted]
Aug 83 I Remember Mabel Babel [redacted]

Latin American
Apr 83 FBIS Latin American Reference Aid;

Linguists
Dec 83 Non Posse vs. Posse Non; [redacted] H.G.

Logic
Jan 83 Logic Design Exceeding Boolean Capabilities; [redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

Management
Sep 83 On How The 'Game' of the Agency Should Be Played; Santiago-Ortiz R.
Oct 83 Crisis Management: Remarks; Faurer L.D.
Nov 83 MBTI: The Management Tool of the Future; [redacted]

Mathematics
Jan 83 Logic Design Exceeding Boolean Capabilities; [redacted]

Microcomputers
Jan 83 Getting Personal; [redacted]

Microwave
Sep 83 Foreign Microwave Radio; [redacted]

Mx
Jan 83 Logic Design Exceeding Boolean Capabilities; [redacted]

EO 1.4.(c)
P.L. 86-36

NCS
Mar 83 Announcement: Students! (NCEUR Independent Study Programs);
Nov 83 The Literary Bends; Murphy A.I.
Nov 83 The White House Is Singing Our Song; Murphy A.I.

NSOC
May 83 The Intelligence Watch Officer; [redacted] L.S.

[redacted]
Mar 83 [redacted]

Pascal
Jun 83 Why Pascal? (Why Not?); [redacted]

Password
Mar 83 More on Passwords; [redacted]
May 83 Still More About Passwords; [redacted] M.E.

Performance
Jun 83 Punching The Biological Timeclock; [redacted]
Aug 83 Does Your Office Make You Sick?; [redacted]

Personality
Mar 83 E.T. At NSA;
Apr 83 Word People at NSA; 'Dickson Airy'
Aug 83 I Remember Mabel Babel; [redacted]
Nov 83 I Remember JFK; H.G.R

Promotions
Jun 83 Some Tips on Getting Promoted; [redacted] V.

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

P.L. 86-36

Puzzle
Jan 83 Puzzle; Williams D.H.
Mar 83 Cryptic Crossword #3; [redacted]
Apr 83 NSA-Crostic No. 46; Williams D.H.
May 83 NSA-Crostic No. 47; Williams D.H.
May 83 Out of My Depth;
Jun 83 NSA-Crostic No. 48; Filby V.R.
Aug 83 Letter to the Editor: Out of My Depth, May 83 Issue; [redacted]
Aug 83 NSA-Crostic No. 49; Williams D.H.
Sep 83 NSA-Crostic No. 50; Williams D.H.
Nov 83 5-4-3 Puzzle; 'Watt Zizname'
Dec 83 NSA-Crostic No. 51; Williams D.H.
Dec 83 Out of My Depth;

Reconnaissance
Sep 83 PARPRO: Reconnaissance Programs; [redacted]

Reporting
Aug 83 The Case of the 'Fowled-Up' CRITIC; [redacted]
Oct 83 Tips on Topical Reporting; [redacted]
Dec 83 Letter to the Editor: Tips on Topical Reporting, Oct 83 Issue; [redacted]
Dec 83 Letter to the Editor: Tips on Topical Reporting, reply to Day's letter; [redacted] D.G.

EO 1.4.(c)
P.L. 86-36

Satellites
Apr 83 [redacted]

Security
Jun 83 Do You Know the Differences?; [redacted] D.S.
Jun 83 Letter to the Editor: Security of Classified Information; [redacted]
Aug 83 Correction: Do You Know the Differences?, Jun-Jul 83 Issue;

SIGINT
Mar 83 SIGINT Challenge: A Scenario; [redacted] J.L.

Sorting
Jan 83 A Survey of Parallel Sorting; [redacted] S.B.

P.L. 86-36

Soviet
Apr 83 Government of the People, By The Party, For The Leadership; [redacted]
Aug 83 Letter to the Editor: Government of the People... reply to [redacted] letter; [redacted]
Aug 83 Letter to the Editor: Government of the People..., Apr 83 Issue; [redacted]
Oct 83 Soviet Military Goals And Their Effect on Negotiations for Arms Limitations; [redacted] G.L.
Dec 83 Soviet Psi Experiments; [redacted]

Spanish
Jun 83 [redacted]

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Dec 83 Non Posse vs. Posse Non; [redacted] H.G.

Staff
Apr 83 My Staff--It Comforts Me; 'Zebulon Zilch'

TDY
Mar 83 TDY Travail; Filby V.R.

TELECOM
Oct 83 TELECOM 83:; [redacted]

Tempest
Nov 83 Static Magic: The Wonderful World of Tempest; Donahue T.M.
Nov 83 Tempest for Every Office; [redacted]

Terminology
Sep 83 Do You Really Mean Julian?; [redacted] C.

Time
Sep 83 Do You Really Mean Julian?; [redacted] C.

Traffic Analysis
May 83 Computerizing Traffic Analysis; [redacted]
Nov 83 Letter to the Editor: Computerizing of TA, May 83 Issue; [redacted]

Training
Mar 83 Announcement: Students! (NCEUR Independent Study Programs);

UIS
Apr 83 UIS: User Interface System Part One: Concept; [redacted]
Apr 83 UIS: User Interface System Part Two: Architecture; [redacted]

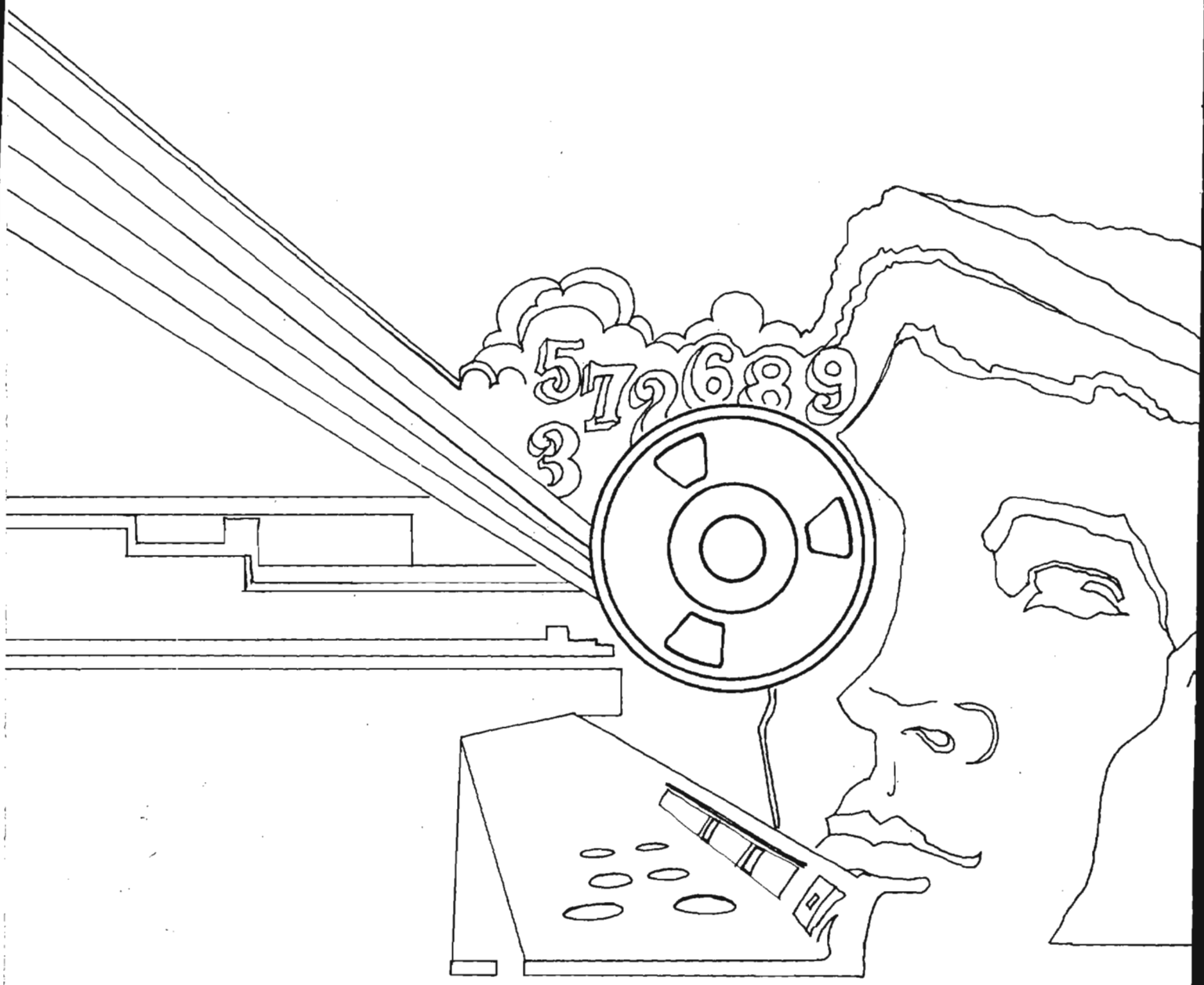
UNIX
Mar 83 Shell Using If; [redacted]
Oct 83 Letter to the Editor: UNIX ED (I) Manual Page Comment; [redacted]
Dec 83 Shell Game: System Shells; [redacted] W.E.

Video Teleconferencing
Mar 83 Video Teleconferencing: NSA Applications; Snodgrass C.L.
Jun 83 Letter to the Editor: Video Teleconferencing, Mar 83 Issue; [redacted] J.R.

Weather
Mar 83 Weather: A Key Intelligence Indicator; [redacted]

P.L. 86-36

Writing
Nov 83 The Literary Bends; Murphy A.I.
Nov 83 The White House Is Singing Our Song; Murphy A.I.



~~HANDLE VIA COMINT CHANNELS ONLY~~

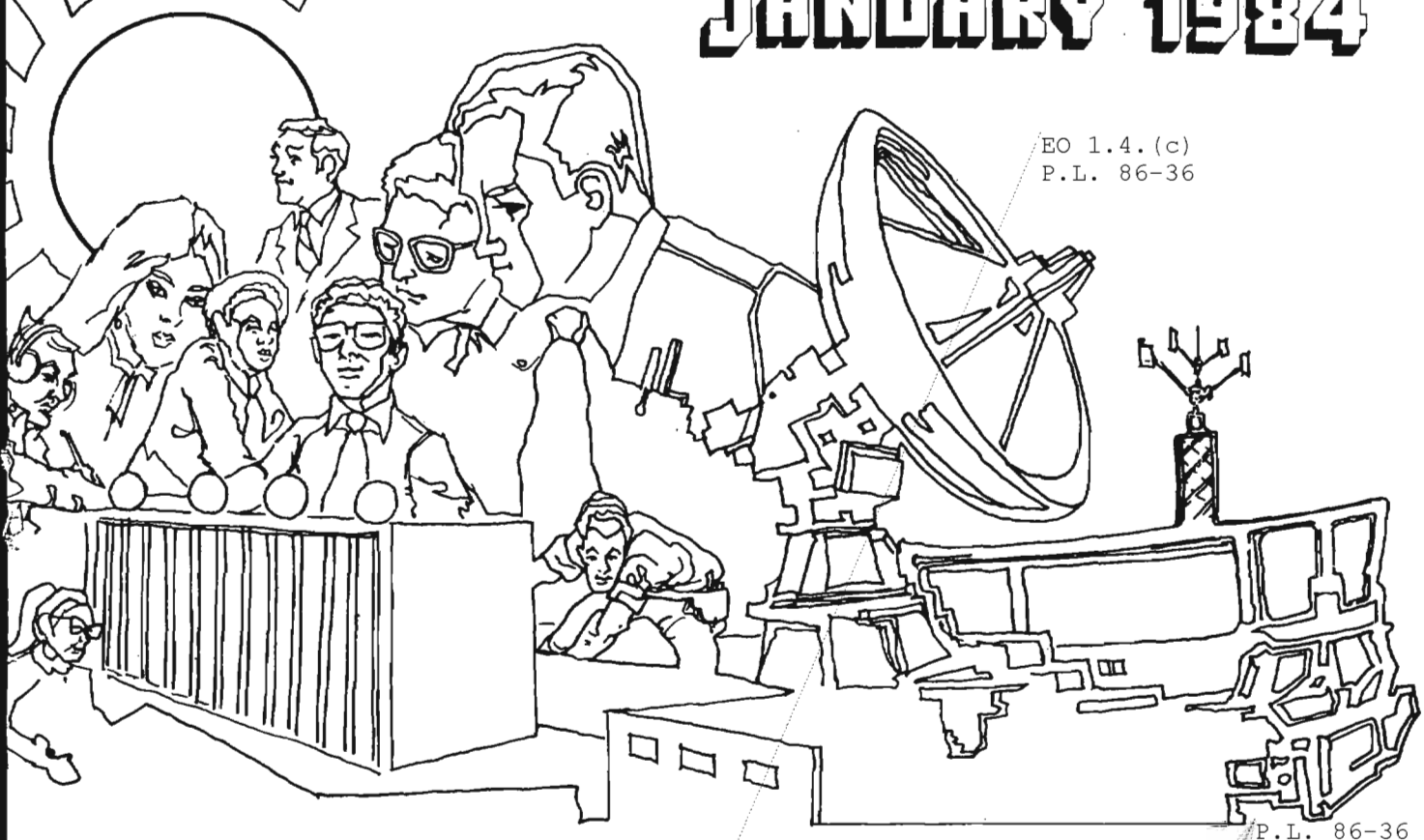
DOCID: 4009891

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JANUARY 1984



EO 1.4.(c)
P.L. 86-36

P.L. 86-36

COMMUNICATIONS INTELLIGENCE AND TSARIST RUSSIA (U) ..... [redacted] 1
PRESENT STATUS AND FUTURE DEVELOPMENT OF CHINA'S TELECOMMUNICATIONS (U) ..... Zhu Gaofeng 13
1983 CISI ESSAY AWARDS (U) ..... [redacted] 17
1983 CISI ESSAY ABSTRACTS (U) 19
THE LANGUAGE PROBLEM AT NSA (U) ..... [redacted] 24
[redacted] ..... [redacted] 25
NSA-CROSTIC NO. 52 ..... [redacted] 28

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009891

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XI, No. 1 JANUARY 1984

PUBLISHER [redacted]

BOARD OF EDITORS

Editor.....[redacted] (963-3045s)
Asst. Editor...[redacted] (963-1103s)
Production.....[redacted] (963-3369s)

Collection.....[redacted] (963-3961s)
Computer Security
.....[redacted] (859-6044)
Cryptolinguistics.[redacted] (963-1103s)
Data Systems.....[redacted] (963-4953s)
Information Science
.....[redacted] (963-5711s)
Mathematics.....[redacted] (968-8518s)
Puzzles.....David H. Williams (963-1103s)
Special Research.....Vera R. Filby (968-7119s)
Traffic Analysis..Robert J. Hanyok (968-8418s)

For subscriptions
send name and organization
to: [redacted], P14

P.L. 86-36

To submit articles or letters
by mail, to: P1, Cryptolog

via PLATFORM mail, send to:
cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no '0' in 'log')

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

~~(SC)~~ Some years ago, during the early stages of the Vietnam War, one of the things we had on our wishlist was a way to get good, precise direction-finding fixes on the many VC targets we kept continuity on. Somebody theorized that what we really needed was an airborne direction finder, one we could put into an aircraft. However, we were assured that, for a variety of technical reasons, it couldn't be done.

(U) Of course, it could be done, because some time later, it was done. However, the thing that interested me most was that once someone had done it, there suddenly appeared a half dozen schemes for doing it. At least two principal methods came into general use at almost the same time, and they both delivered consistent and accurate results. It is a tribute to how well they worked that control of these new "assets" became a major political issue within the community at that time.

(U) The key to all this development and the sudden emergence of a new technique was, quite simply, knowing it could be done.

(U) Some time later, after our own systems were operational, we happened to learn that the French had managed to do it first, and also in Vietnam. Suppose we had known that from the first! I have always wondered what we could have done--and how much earlier--if we had known that it could be done, because someone had already done it.

DOCID: 4009891

COMMUNICATIONS INTELLIGENCE & TSARIST RUSSIA (U)

by

[redacted]

P.L. 86-36

INTRODUCTION

This article explores the early development and use of communications intelligence by the Tsarist Russian regime through World War I and the importance attached to it, especially by the Russian Navy. The article is UNCLASSIFIED in its entirety.

Western publications in recent years have been providing frequent revelations about the use of communications intelligence (COMINT) by major nations of the world.[2] The one notable exception, at least in English-language publications, has been Russia. At the logical source, the natural secrecy attached to COMINT information in general, combined with the traditional obsession with secrecy throughout its society, has held discussion of the subject to a minimum. Outside the USSR, such imperial Russian failures in communications security as Tannenberg in World War I have contributed to the impression that the Russians must have known little about COMINT. Despite these constraints, however, since the early 1960s several rather specific articles concerning COMINT organizations and operations under the Tsars[3] and even on the early development on radio intelligence service in the Soviet Army[4] have appeared in Soviet journals. When supplemented with information available from non-Soviet sources, a general picture emerges of an early Tsarist COMINT effort approaching similar efforts in the West. This article is an initial attempt to shed some historical light on this little-known area of Tsarist intelligence.

It should be noted that the absence of any discussion in the present article concerning Russian Army COMINT activities before World War I or Ministry of Internal Affairs COMINT operations during WWI itself does not necessarily mean such activities did not exist, but merely that insufficient documentation was available from which to draw any conclusions. It should also be noted that the early Russian COMINT efforts apply to communications in their broadest sense, including secret or coded written messages.

Ministry of Foreign Affairs (MID)

Traditionally, communications intelligence involving foreign governments and their representatives fell within the purview of the Ministry of Foreign Affairs (MID). This tradition has been traced back at least to the reign of Peter the Great.[5] The methods used, of course, involved gaining access to the diplomatic correspondence, opening it (perlustration), and (if found to be encrypted) either purchasing the necessary cryptographic materials from a willing employee or actually engaging in operational cryptanalysis to exploit the document. Even so wily a statesman as the "Iron Chancellor," Otto von Bismarck, while serving as Prussian Ambassador to St. Petersburg (1859-1863), fell victim to MID's reading of Prussian ciphers.[6] MID was aided in its COMINT efforts by the so-called "Black Cabinets" of the Imperial Russian Postal Service.

DOCID: 4009891

Black Cabinets were set up at the post offices in major cities of the Russian Empire. One of their important functions appears to have been opening suspect correspondence, photographing the contents, and disseminating the information to the appropriate ministry:

[] information of "general State interest," usually comments about the Imperial Family made by segments of Tsarist nobility, to the Minster of Internal Affairs;

[] "political" correspondence to the Department of Police;

[] "diplomatic" correspondence to the Minister of Foreign Affairs; and

[] "espionage" correspondence (presumably during wartime) to the Army and Navy General Staffs.

According to one former Black Cabinet official, there was never much of a problem gaining access to or photographing the contents of foreign diplomatic pouches. When the diplomatic correspondence was found to be encrypted, it was not worked on at the Black Cabinet itself but sent to a "similar establishment attached to the Ministry of Foreign Affairs." Copies of all encrypted telegrams sent and received by embassies in St. Petersburg were delivered to this MID organization. In important cases, even copies of reports carried in locked leather briefcases by special diplomatic couriers were forwarded to this same unit.[7] As most couriers and embassy employees were underpaid by their governments, they could be prevailed upon for a small bribe to allow the contents of their briefcases to be photographed by Black Cabinet specialists.

The fact that diplomatic documents were encrypted only served to intensify MID's efforts to discover their contents. One Black Cabinet official described the ease with which foreign cryptographic materials could be obtained, even on the open market, in the following manner:

> "Codebooks were acquired not only with the assistance of embassy employees but also in the cities of Brussels and Paris, where well-known persons engaged directly in the open trade of foreign codebooks for a fixed price.[8] The situation was completely identical in both cities. Codebooks which were of less interest to us, e.g., Greek, Bulgarian and Spanish, and could be obtained rather easily, cost 1,500 to 2,000 [rubles]. Such codebooks as those of the Germans, Japanese or U.S.A. cost several tens of thousands. The prices for the remaining countries fluctuated between 5,000 to 15,000. It was possible with this trading in codebooks to place an order for this or that new codebook, and these orders were filled within a short period of time."[9]

The "similar establishment" of the Ministry of Foreign Affairs to which the encrypted diplomatic correspondence was sent by the Black Cabinets was, of course, the main COMINT organization within MID responsible for diplomatic cryptanalysis. Little information is available on the specific structure and operations of this organization. Before World War I, purportedly, it could read the encrypted correspondence of at least France, Great Britain, Turkey, Austria-Hungary, and Sweden. According to one source the following additional countries' diplomatic correspondence was being read by MID cryptanalysts during WWI itself: Italy, Japan, Bulgaria, Romania, and Greece. Shortly before World War I this cryptanalytic organization was reorganized by Aleksandr A. Savinskij, Chief of the MID Cabinet (1901-10), and brought directly under control of the foreign affairs minister himself.[10]

Ministry of Internal Affairs (MVD)

Like the Ministry of Foreign Affairs, the Ministry of Internal Affairs (MVD), through the cryptanalytic organization of its Department of of Police, was an important component of the Tsarist Russian COMINT community. The internal security and surveillance functions of the MVD, including the monitoring of communications of both anti-Tsarist revolutionary groups and the general populace of the Empire as a whole, have been rather well documented elsewhere.[11] What is not generally well-known is that, at least for a short period of time, the MVD expanded its jurisdiction to include monitoring the communications (as well as the movements) of foreign ambassadors, ministers, and military attaches based in Russia. This extension of the MVD into an area normally under sole control of the Ministry of Foreign Affairs occurred between 1904 and 1906. Included among those whose communications were being monitored by the MVD was the US Ambassador.

DOCID: 4009891

The monitoring of US diplomatic communications, according to the former chief of this self-described "Top Secret" MVD bureau, Colonel Mikhail Stepanovich Komissarov, had "enormous significance for Tsarist diplomatic initiatives." On 4 May 1917, in testimony before the Extraordinary Investigating Commission of the Provisional Government,[12] Komissarov stated:

> "During the Portsmouth Treaty (Conference), we knew all the American conditions (positions) earlier than the American Ambassador[13] in Petrograd."[14]

This statement may have been only post-Revolutionary bluster on the part of Komissarov, but it might be added that the principal Russian delegate to the Portsmouth Conference, Sergei Witte, received the title of "Count" from the Tsar upon his return to Russia specifically for his work at Portsmouth. Thus, the Portsmouth Treaty Conference may not have been the major Russian loss or Teddy Roosevelt's personal victory, as it has so often been portrayed by historians.

Army Radio Intelligence

The integration of radio communications into the military forces of the major world powers at the beginning of the 20th century greatly expanded the horizons of COMINT in obtaining information on one's adversaries. It is unknown precisely when a radio intelligence service was first established in the Russian Army, but it undoubtedly was influenced by the successful radio intelligence set up in the Baltic and Black Sea Fleets during the 1911-14 period.[15] Although there was no centralized control of intelligence, COMINT or otherwise, within the military command structure overseeing both Army and Navy operations, according to a former Soviet Communications Service chief close cooperation did in fact exist between the Army radio intelligence services of Russia, Great Britain, and France. This cooperation included frequent exchanges of information on the operating characteristic of enemy radio stations, callsign constructions, and signal codes.[16]

In the Russian Army, at each Army Headquarters, radio intelligence operations were controlled by the chief of Army Communications through his Assistant for Technical Matters. Each Army's radio battalion had a radio intelligence squad or section, which operated two radio stations: one station monitored the radio waves for enemy communications and, when it detected some, the other station then recorded them. Presumably, the radio direction-finding (RDF) stations also located at each Army Headquarters were controlled by the Assistant for Technical Matters too. (See Chart I.)

Although information on Russian Army radio intelligence operations is almost nil, one example can be cited. Between February and April 1915, on the eve of the German breakthrough in Galicia, Russian Army COMINT-provided information revealed the appearance of several new German Corps at the front, including a Guards Corps which had just been transferred from another area in Galicia. The radio intelligence service had discerned this information on the basis of certain peculiar operating characteristics of these corps' radio stations and by the distinctive "fists" of their radio operators. Russian RDF stations were also being used extensively at this time.[17]

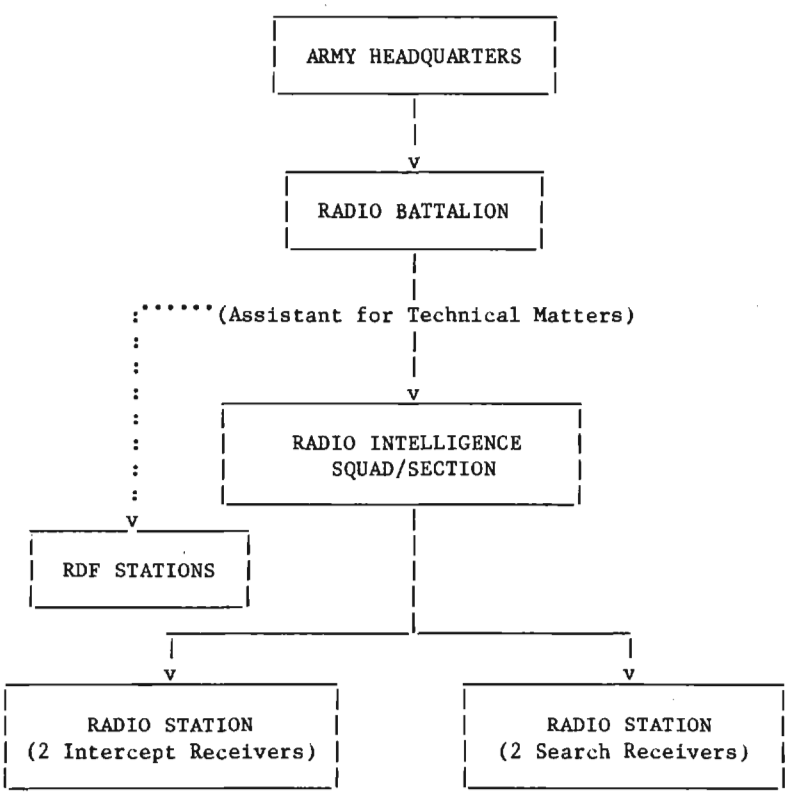
By the end of 1915 the encrypted German Army radio messages were being intercepted on at least the Northern Front and sent to a "special bureau of the Main (Operations) Directorate of the General Staff" (SPETsIAL'NOE BYuRO GLAVNOGO UPRAVLENTYa GENShTABA) in St. Petersburg for cryptanalysis. According to one former high-ranking Tsarist intelligence officer, however, tangible results of this bureau's work were not passed on and the radio work itself was poorly organized in the Army, when compared to similar work in the Russian Navy.[18]

Navy Radio Intelligence

If communications intelligence was organized and operated poorly in the Army, the exact opposite was the case in the Russian Navy. In fact, the organizational structure of the radio intelligence service was so thoroughly developed during World War I in the Baltic Sea Fleet that operations undertaken by the fleet were almost always successful. Like the Baltic Sea Fleet, the Black Sea Fleet also had an effective, if somewhat less well-developed, radio intelligence effort. From available evidence, it appears that each fleet's radio intelligence service was independent and responsible ultimately only to its respective fleet headquarters.

OCID: 4009891

BASIC COMINT STRUCTURE IN A RUSSIAN ARMY (circa 1915)



..... Postulated Control

——— Actual Control

(from Peresypkin, op. cit., p. 56)

CHART I

The decision to set up radio intelligence services in the Navy can be traced to the debacle suffered by the Russian Navy during the Russo-Japanese War of 1904-05 and the decision of young Russian naval officers never to allow such an occurrence to happen again. Restructuring of the Navy became the order of the day. In 1911 the Commander-in-Chief of the Baltic Fleet, Admiral Nikolaj Ottovich von Ehssen, appointed Captain 1st Rank (later Vice Admiral) Adrian Ivanovich Nepenin[19] to be Chief of Communications Service, Baltic Fleet. This appointment was to have enormous consequences on the development of COMINT in the Russian Navy.[20]

Nepenin immediately set about reorganizing the Communications Service to support the Baltic Fleet Command, not only with better communications but also with effective and accurate intelligence information. To this end Nepenin placed his closest assistant[21] in key Communications Service positions and the staffed the Service with only well-trained personnel. To further enhance the skills of enlisted personnel, Nepenin set up several Communications Service schools with special attention given to training "radiotelegraphic intercept operators" (RADIOTELGRAFISTI-SLUKhAChI).[22] Although it is unknown precisely when land-based radio intercept operations began in the Communications Service, according to the official Soviet history, radio intercept operations were carried out by Russian Baltic Fleet ships during training exercises held prior to the outbreak of World War I.[23] By the beginning of the war the communications service was well-organized and ready for action. However, it was only with recovery of the German radiotelegraphic codebooks from the cruiser MAGDEBURG, which had run aground near Oldensholm (now Osmussar) Island in the Baltic Sea on 26 August 1914, and the subsequent use to which they were put that the radio intelligence service really came into its own and became quite effective.[24]

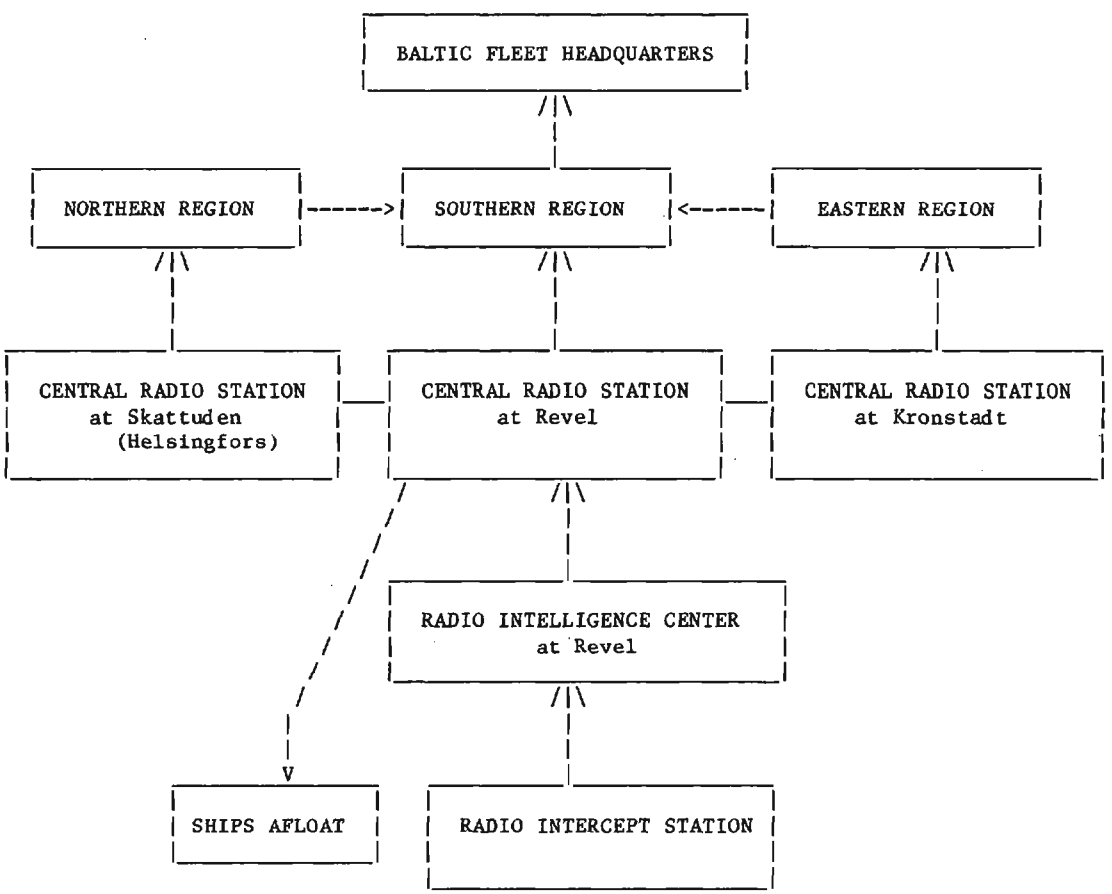
Before going into specific examples of the use of COMINT information by the Russian Navy, let's look at the overall radio intelligence structure as it was set up in the Baltic and Black Sea Fleets.

At the beginning of the war the Baltic Fleet Communications Service was divided into three regions:

1. Northern, stretching from Helsingfors (now Helsinki, Finland) to the Abo-Aland Islands;
2. Southern, from the Kunda Inlet in the west to the German border; and
3. Eastern, covering the Gulf of Finland east of Helgoland Island.

Each of these regions had a Central Radio Station (CRS) attached to it which provided communications support to the fleet and received intelligence information from aerial reconnaissance and shore-based observation posts in addition to radio intelligence from intercept and RDF[25] stations. Except for the Southern Region, which served as the headquarters for the Chief of the Communications Service, it is unknown when the other regions first set up their COMINT stations. By the autumn of 1916, however, the Northern Region had five RDF and five radio intercept stations in operation, while the Southern Region had expanded its operations to five RDF and four radio intercept stations. It is possible that the Eastern Region did not have a COMINT effort at all or that the effort was only of limited duration. In March 1915 a so-called "Radio Intelligence Center" was set up at Revel (now Tallin), subordinate to the CRS of the Southern Region. This "Center" was probably connected with all radio intercept and RDF stations within the Souther Region by underground cable. It is possible similar "Centers" were established within the other regions to deal strictly with COMINT-related data before forwarding the information on to their respective CRSs. Once the COMINT information reached the CRS, if it was time-sensitive and extremely urgent, it would be transmitted immediately to commanders of Russian ships operating in the Baltic. (See Chart II.)

EARLY DEVELOPMENT OF THE COMINT SERVICE IN THE BALTIC FLEET
(circa 1915)



——— Probable reporting flow

----- Postulated reporting flow

(From Zernov & Trukhin, op. cit., p. 107;
Yankovich, op. cit., p. 116;
Timirev, op. cit., p. 46;
Steblin-Kameskij, op. cit., p. 620; &
Dudorov, op. cit., May 1959, pp. 35-36)

CHART II

DOCID: 4009891

Although the Black Sea Fleet's radio intelligence organization was somewhat similar to the Baltic Sea Fleet's, there are fewer details available.[26] The Communications Service was divided into a northern region, stretching from the mouth of the Danube to Feodosiya, and an eastern region extending from Feodosiya to Batumi. Except for one known radio intercept station set up at Sevastopol' early in the war,[27] it is unknown if or when other similar stations were established. (See Chart III.)

It might be added that while some of the equipment for the radio intelligence services was provided to the Russians by foreign firms,[28] some of it was constructed by specialists of the Russian Navy Department itself,[29] possibly associated with the Naval Ministry's own radiotelegraphic equipment factory (now called the "COMINTERN" factory).[30]

The use of COMINT information by the Russian Navy during the war, especially in the Baltic Sea Fleet, proved to be very effective. Part of the reason for this effectiveness, according to a former high-ranking Tsarist Baltic Fleet officer, lay in the analytical judgments of Captain Nepenin as chief of the Baltic Fleet Communications Service:

> "Nepenin had developed to the highest degree the gift of establishing a complete picture of the movements of enemy ships and from this determining the plans and intentions of the enemy. Nepenin was able to accomplish this task by logically comparing facts and conjectures, which had been provided to him by Communications Service posts, both on the basis of decrypted German radio messages and bearings obtained by radio direction-finding stations. His predictions of enemy movements, sometimes very bold and apparently with little basis, almost always were vindicated. ... Not one operation was undertaken [by the fleet] without first receiving a detailed and almost always correct interpretation (of information) on the requested area from Nepenin."[31]

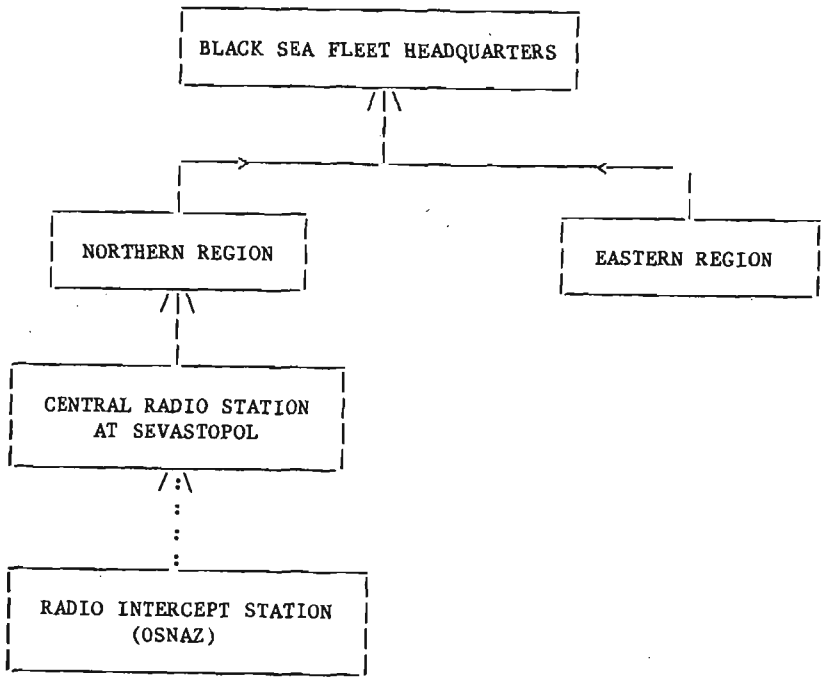
The importance of COMINT to the Russian Navy was not limited to officers of the Baltic Fleet. The chief of a special British military intelligence liaison mission in Russia, Sir Samuel Hoare, was also most impressed with the Russian Naval COMINT effort:

> "I was on intimate terms with certain officers of the Russian Naval General Staff and I learned many interesting details about secret codes and ciphers. In this branch of intelligence the Russians excelled. Their experts could unravel almost any cipher in an incredibly short period of time. One of them implored me as a friend and ally to ask the British Foreign Office to change a cipher that he could read almost as easily as his daily paper."[32]

The information provided by the radio intelligence service under Nepenin's direction was looked upon with such favor by the Russian Naval Command that it was one of the reasons why Nepenin was designated as Commander-in-Chief of the Baltic Fleet in September 1916. Nepenin was succeeded as Chief of the Communications Service by Captain 1st Rank Davydov,[33] the head of the Communications Service's analysis and reporting section. Davydov may himself have been succeeded by Captain 1st Rank Novopashennyj,[34] who was noted as Chief of the Baltic Fleet Communications Service in 1917,[35] and Novopashennyj by Captain 1st Rank Rengarten.[36]

In the Baltic Fleet, the first operation known to have been taken on the basis of COMINT information[37] took place on 14 February 1915, when the Russians learned in advance the scheduled times for the arrival and departure of a German cruiser at the port of Libau (now

EARLY DEVELOPMENT OF COMINT SERVICE IN THE BLACK SEA FLEET (circa 1915)



——— Probable reporting flow
..... Postulated reporting flow

From Zernov & Trukhnin, op. cit., p. 107; and Steblin-Kamenskij, op. cit., p. 620.

CHART III

Liepaya). A Russian submarine was immediately dispatched and sank the cruiser as it left Libau. COMINT information also played a major role in mine-laying operations involving German ships in the Baltic. On 14 May 1915 the radio intelligence service decrypted a message from the German mine-layer DEUTSCHLAND revealing the location of a German minefield in the area of the Bogsher-Dagerort islands, thus allowing the Baltic Fleet Command to take corrective measures.[38]

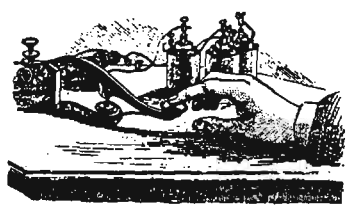
Another example of the utilization of time-sensitive information derived from COMINT by Russian ships afloat occurred on 1 July 1915. A detachment of Russian cruisers, while in transit to bombard German targets in Memel (now Klaipeda), received a report on the location of a scheduled rendezvous between the cruiser AUGSBURG and a group of other German ships. The Russian detachment then broke up the rendezvous by forcing the German ships to retreat.[39]

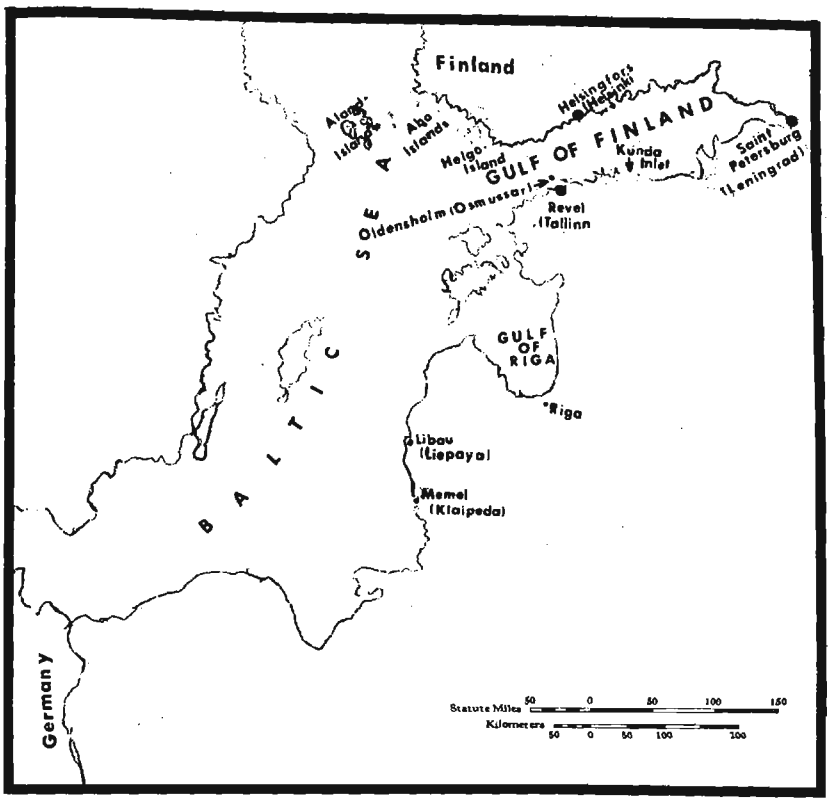
The high point in the operations of the Baltic Fleet's radio intelligence service was reached on 31 July 1915, when the Russians gained foreknowledge of the German Navy's proposed forcing of the Gulf of Riga in conjunction with the German Army's seizure of the city of Riga. Information obtained by cryptanalysis, as well as from aerial reconnaissance and shore-based observation posts, provided the proposed time and date of the offensive, including the deployment of enemy forces. When the German Navy attempted to carry out the operation on 8 August, ships of the Baltic Fleet were already in place and broke up the attack.[40] By May 1916, however, the Germans began to restrict their use of radio communications in the Baltic and the Baltic Fleet Communications Service had to rely more on aerial reconnaissance for advanced warning of German activities.

As a result of its operations, the official Soviet history of the Russian Navy in WWI rated the Baltic Fleet intelligence effort very highly:

> "The organization of operational intelligence in the Baltic Fleet reached a very high level of development during the First World War. Fleet Headquarters received timely, precise, reliable information on the activities and intentions of the enemy. Thanks to this, the Fleet Command right up to the end of the war had the opportunity to be both forewarned about enemy operations and to organize in a timely manner countermeasure.
>
> "In carrying out reconnaissance activities in the Baltic Theater of Military Operations (TMO), Baltic Fleet Headquarters used agents, submarines, naval air reconnaissance, radio-technical [SIGINT] facilities, a widely developed network of NIS (Observation and Communications) posts, and on certain rare occasions, surface ships. For purposes of reconnaissance, an especially high value was placed on the use of radio-technical facilities.
>
> "Radio-technical intelligence in the Baltic Fleet during the period of 1914-1915, in essence was the primary type of intelligence in that TMO." [41] [Emphasis added. TRH]

The earliest known example of an operation undertaken by the Black Sea Fleet based on COMINT occurred in September 1916, although undoubtedly there must have been earlier operations.[42] The Russians were aided in the Black Sea Fleet radio intelligence effort by the Turkish Navy's reliance on the Germans for cryptographic material, which the Russians already had in their possession. On 15 September 1916 Black Sea radio intelligence elements (subunits) intercepted information from a shore-based Turkish radio station regarding the sweeping-up of Russian mines obstructing the approaches to the Bosporus. A large Turkish transport ship was to pass through the swept area with a cargo of coal from Zonguldak. Russian ships were quickly sent to relay mines and the Turkish ship was sunk. In December 1916 the Russians decrypted an order for a German submarine to return to Constantinople along with the coordinates of the mine-swept channel through which the submarine was to pass. Torpedo boats were immediately dispatched from Sevastopol' to remine the area. It was learned by the Russians within 48 hours through another decrypted message that the submarine had been sunk by the mines. This was the last German submarine to embark for the Black Sea during the war. Up until the last days of WWI Black Sea Fleet radio intelligence facilities played a key role, in conjunction with aerial reconnaissance, in informing the Black Sea Fleet Command of the German battleship BRESLAU's departure to sea.[43]





Conclusion

It is clear from the above that communications intelligence was an important and integral part of information-gathering under the Tsars. The invention of radio and its integration into the military forces of the major world powers at the turn of the century also opened up a new horizon for Tsarist COMINT activities, although the Russian Military Command appears to have been somewhat slow in recognizing the possibilities inherent in using the radio for intelligence purposes. Nevertheless, Tsarist Russia, whatever faults it may have had, was not totally inept in intelligence-gathering, as implied by some historians; and, despite its slowness, it did achieve some success, at least in the Navy, with its use of COMINT.

FOOTNOTES

1. [redacted]

2. Kahn, David, The Codebreakers, New York: Macmillan, 1967; Winterbotham, F. W., The Ultra Secret, New York: Harper & Row, 1974; Beesly, Patrick, Very Special Intelligence, London: Hamish Hamilton, 1977; and Montagu, Ewen, Beyond Top Secret Ultra, New York: Coward, McCann & Geoghegan, 1978, to list just a few.

3. Yankovich, V., "On the Origins of Radio Intelligence in the Russian Navy," Voenno-Istoricheskij Zhurnal (Journal of Military History), Moscow, February 1961; Peresypkin, Marshal I. T., Voennaya Radiosvyaz' (Military Radio Communications), Moscow: Voenizdat, 1962; Zernov, M., & N. Trukhnin, "The Communications Service in the Russian Navy during World War I," Voenno-Istoricheskij Zhurnal, March 1966; and Pavlovich, N. B. (editor), Flot v Pervoj Mirovoj Vojne (The Navy in World War I), 2 vols, Moscow: Voenizdat, 1964.

   It is interesting to note that the Soviet articles began appearing approximately at the same time as similar articles in the Russian naval emigré press. See, for example, Rear Admiral Boris Petrovich Dudorov's articles on Admiral Nepenin in the emigré journal Morskie Zapiski (The Naval Records), New York, April 1956-April 1962.

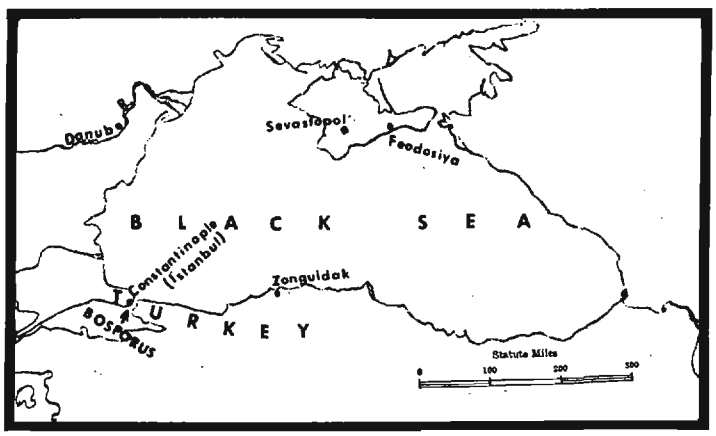
4. Ural'skij, Yu., "The Organization and Combat Use of Radio Intelligence during the Civil War," Voenno-Istoricheskij Zhurnal, November 1972. (A translation of this article appeared in Cryptolog,

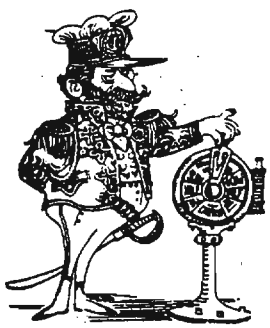
P.L. 86-36

September 1978, under the title "Soviet COMINT and the Civil War: 1918-1921.")

5. For instance, see Kahn, op. cit., p. 614.
6. Cited in Richard W. Rowan's Secret Service, New York: Literary Guild, 1937, p. 699.
7. Majskij, S., "Black Cabinet: Recollections of a Former Tsarist Censor" in Byloe (The Past), Paris: July 1918, p. 191.
8. Probably a reference to the so-called "International Secret Service Bureau" with pre-WWI headquarters in Brussels and described by some as a semi-private business available to the highest bidder. Russian intelligence was know to have had extensive dealings with this bureau during the pre-WWI era. See Graves, Armgaard Karl, The Secrets of the German War Office (New York: McBride, Nast & Co., 1914), p. 28 and Ludecke, Winfried, The Secrets of Espionage, Philadelphia: J. B. Lippincott, 1929), p. 227.
9. Majskij, op. cit., p. 192.
10. Swedish cryptanalyst Yves Gylden, quoted in Kahn, op. cit., p. 621, and Gottlieb, W. W., Studies in Secret Diplomacy during the First World War, London: George Allen & Unwin, Ltd., 1957, passim.
11. For example, Kahn, op. cit., pp. 618-621. Anti-Tsarist revolutionary groups even used COMINT activities against the MVD itself by, on at least one occasion, obtaining a copy of the Department of Police's own cipher with which it communicated with subordinate elements throughout the Empire. See "The Department of Police Cipher" in Byloe, November-December 1909, pp. 189-190.
12. The Extraordinary Investigating Commission was set up by the Provisional Russian Government after March 1917 to take testimony from former Tsarist Russian officials on the functioning of the old regime. Its operations were ended with the Bolshevik Revolution.
13. George von Lengerke Meyer served as US Ambassador to Russia from 8 March 1905 to 26 January 1907. He later served as US Postmaster General (1907-09) and Secretary of the Navy (1909-13). According to the US State Department, US diplomatic communications were encrypted by 1905.
14. Cited in "The Revolution of 905-06 in the Reports of Foreign Diplomats" by M. G. Fleer in Krasnyj Arkhiv (Red Archive), Moscow, Vol 3 (16), 1926, p. 220. The Portsmouth Peace Conference (August-September 1905) which took place at Portsmouth, NH, ended the Russo-Japanese War of 1904-05. President Theodore Roosevelt won the Nobel Peace Prize for his mediation efforts at the conference. It is also interesting to note that Colonel George Fabyan, later William F. Friedman's boss at Riverbank Laboratories, was a member of the US delegation at Portsmouth.
15. See "Navy Radio Intelligence," the next section of this article.
16. Peresypkin, op. cit., p. 57. The existence of Russian Army COMINT liaison with the COMINT services of Great Britain and France has not heretofore been acknowledged in any western publication concerning Allied COMINT activities in WWI.
17. Peresypkin, op. cit., p. 57, and Ocherki Vneshej Politiki Rossii: 1914-1917 (Studies of Russian Foreign Policy: 1914-1917) by V. A. Emets, Moscow: Nauka Izdar., 1977, p. 165, footnote 441.
18. Batyushin, General-Major Tajnaya Voennaya Razvedka i Bor'ba s Nej (Secret Military Intelligence and Combat with It), Sofia: Nov'Zhivot Press, 1939, p. 73. See also General Batyushin's articles "Cryptography in World War I," Ratnik (Soldier), Belgrade, June-July 1928, and "Radiotelegraphic Intelligence," Vestnik Voennykh Znanij (Herald of Military Knowledge), Bosnia (Yugoslavia), January-March 1931.
19. Captain Nepenin will be the subject of another article by [redacted] in a future issue of Cryptolog. P.L. 86-36
20. Dudorov, op. cit., July 1958, p. 39.
21. According to Dudorov, op. cit., December 1958, pp. 17-22, Nepenin's chief assistants included Mikhail Platonovich Davydov, who was in charge of all critical analysis and intelligence reporting based on all-source data received by the Communications Service resources; V. P. Orlov, who as Chief Engineering Officer was in charge of all engineering and mechanical support to the Communications Service; Anatolij Koval'skij, who was in charge of the Central Radio Station (CRS) at Revel and later chief of the Southern Region of the Communications Service; and B. P. Dudorov, who set up and operated the first aerial reconnaissance wing of the Communications Service.
22. Dudorov, op. cit., December 1958, p. 38.
23. Pavlovich, op. cit., Vol 1, p. 79.
24. An article by [redacted] about the MAGDEBURG incident will appear in a future issue of Cryptolog. P.L. 86-36
25. Ivan Ivanovich Rengarten, a leader in Russian radiotelegraphy and RDF, had set up two RDF stations by September 1914: one on Osel (now Saarema) Island and one at Libau. See Dudorov, op. cit., March 1960, pp. 50-51, and "On Radio Communications in the Navy" by I. I. Rengarten, Morskoj Sbornik (Naval Collection), Moscow, Jan-Mar 1920, pp. 32-33.
26. Even the official Soviet history of the Navy in World War I (Pavlovich) does not credit the Black Sea Fleet with any substantial intelligence activity.

27. Steblin-Kamenskij, Senior Lieutenant Ivan Ivanovich, "Mine Warfare in the Black Sea," La Revue Maritime (Naval Revue), Paris, Nov 1932, p. 620.
28. There was some cooperation between the British firm of Marconi and the Russian firm of R.O.b.T.i.T. (Russian Company of Wireless Telephone and Telegraphy) in building accurate RDF stations, according to Rengarten, op. cit., p. 33, and Peresypkin, op. cit., p. 31.
29. Ural'skij, op. cit., p. 84.
30. Zernov & Trukhnin, op. cit., p. 107, and "Obituary of I. I. Rengarten," Morskoj Sbornik, Jan-Mar 1920, pp. 1-5.
31. Timirev, Rear Admiral Sergej Nikolaevich, Vospominaniya Morskogo Ofitsera (Recollections of a Naval Officer), New York: American Society for Russian Naval History, 1961, pp. 14-15. On the non-emigré side, the official Soviet history of the Russian Navy in World War I, while condemning Nepenin's brief tenure as Commander-in-Chief of the Baltic Fleet (1916-17), complimented him on his intelligence foresight and ability:
    "The Communications and Observation Service in the Baltic Fleet was excellently organized by Rear Admiral A. I. Nepenin for operational intelligence. ... A. I. Nepenin was also one of the first admirals of the Russian Navy to appreciate the significance of naval aviation as a most important means of reconnaissance."
    See Pavlovich, op. cit., pp. 75-76.
32. Hoare, Rt. Hon. Sir Samuel, The Fourth Seal, London: William Heinemann, Ltd., 1930, p. 57.
33. Dudorov, op. cit., p. 100.
34. According to one source, Captain 1st Rank P. A. Novopashennyj was later chief, intelligence/counterintelligence department, White Russian Naval Directorate in support of White Armies fighting in northwest Russia during the summer of 1919. See A Short Survey of White Forces under the St. Andrew Flag by Lieutenant N. Z. Kadesnikov, New York: private printing, 1965, p. 41. This is probably the same Novopashennyj who "had rendered good service during World War I in the imperial Russian Navy" and from 1922 on served as a senior assistant to the chief of a German cryptanalytic organization. See War Secrets in the Ether by Wilhelm F. Flicke, Laguna Hills: Aegean Park Press, 1977, Vol. II, pp. 292-293.
35. Timirev, op. cit., p. 165.
36. "Obituary of I. I. Rengarten."
37. Although this is the first known operation, the Baltic Fleet radio intelligence service was active before this time. For example, daily consolidated radio intelligence summaries (based on Communications Services assets information, foreign broadcast transmissions, and weather forecasts) were regularly being compiled in Oct-Nov 1914 when the Baltic Fleet first began active operations in the southern part of the Baltic Sea. See Pavlovich, op. cit., pp. 104 & 109-110, and Zernov & Trukhnin, op. cit., p. 107.
38. Chernomor, Volnyj Baltiki: 1914-1915 (Waves of the Baltic: 1914-1915), Riga: Dlya Vas, 1939, pp. 275-276.
39. Zernov & Trukhnin, op. cit., p. 107; Yankovich, op. cit., p. 117; and Pavlovich, op. cit., pp. 169-171.
40. Korostovetz, Vladimir, Seed and Harvest, London: Faber and Faber, Ltd., 1931, pp. 220-221; Monasterov, Nestor, & Sergej Tereschenko, Histoire de la marine russe (History of the Russian Navy), Paris: Payot, 1932, pp. 289-297; Dudorov, op. cit., Aug 1960, pp. 34-35; Yankovich, op. cit., p. 117; Zernov & Trukhnin, op. cit., p. 108; and Pavlovich, op. cit., pp. 175-6 & 225.
41. Pavlovich, op. cit., p. 311.
42. On 25 January 1915, for example, Black Sea Fleet ships were intercepting communications of enemy cruisers. See Pavlovich, op. cit., p. 470.
43. Steblin-Kamenskij, op. cit., pp. 621-622; Zernov & Trukhnin, op. cit., p. 110; & Pavlovich, op. cit., p. 470.





DOCID: 4009891

电信业务

PRESENT STATUS AND FUTURE DEVELOPMENT OF CHINA'S TELECOMMUNICATIONS (U)

by ZHU GAOFENG,
Vice Minister of Posts and Telecommunications,
People's Republic of China

The following paper was presented at TELECOM 83 (see CRYPTOLOG, October 1983, pp. 12-15).

INTRODUCTION

Scope

The subject matter will be covered as follows:

1. China's telecommunication services;
2. China's telecommunication industries and scientific research;
3. Main development targets for the next 20 years;
4. Some factors affecting the development of telecommunications infrastructures; and
5. Measures to be taken for developing communications.

CHINA'S TELECOMMUNICATION SERVICES

China's earliest telecommunications facilities were set up in the 1870s in the latter part of the feudal Qing dynasty (1644-1911). But up to 1949, when the People's Republic of China was founded, there were only 736 urban telephone exchanges; of these only 59, or 8 percent of the total, were equipped with automatic telephone connection. The total capacity of these was 712,000 lines, among which 208,000, or less than one third, were automatic. Thirteen provinces and municipalities had no automatic telephone exchanges at all. The limited telecommunications equipment was concentrated in the coastal regions and the handful of larger inland cities. There were no telecommunications services whatsoever in the vast rural areas. Before 1949 shortwave circuits were the main transmission medium for long-distance telecommunications. Open wires were miserably scarce. There were only about 2,000 transmission lines for long-distance telephone and they were mainly single-channel and three-channel carriers. Throughout the nation, the postal and telecommunications offices numbered only some 25,000.

Over the past 34 years since the founding of the People's Republic, post and telecommunications systems have developed rapidly. Equipped with open wires, cables, microwave and shortwave circuits, a network of telecommunications, with Beijing as the hub, has been built. This network links up cities and towns with the vast rural areas. The first 1,800-channel coaxial cable carrier system from Beijing to Shanghai went into operation in 1967. The experience gained in building this project provided the basis for developing more big-capacity trunk networks of telecommunications. Construction of another trunk cable system for telecommunications, the Beijing-Wuhan-Guangzhou 1,800-channel coaxial cable carrier system is in full swing. When completed in 1985, this will form another big north-south telecommunications artery. More than 10,000 kilometers of trunk cables have been built and a series of new ones are under construction. Over 14,500 kilometers of

microwave links with 600- or 960-channel capacity have been completed. These form a nationwide network linking 26 provinces, autonomous regions, and municipalities so that telephone calls, telegrams, facsimile transmission, radio, and television programmes can be exchanged between them.

In 1982, the number of urban telephone offices were four times as many as in the early days of liberation. Of these, the number of those with automatic equipment rose by 20 times, with a total capacity of 8.3 times as much as that in early 1949. Before 1949 telephones were unknown in the rural areas. Now there are over 2.4 million lines there. There are 26,000 long-distance telephone circuits, 9 times the figures in the early days of liberation. The national number of post and telecommunications offices has reached nearly 50,000, a 90 percent increase over 1949. Through the use of cables and microwaves, automatic or semi-automatic long-distance telephone service is available in 24 of the provincial capitals. The growth of post and telecommunications services in the countryside and border regions of the national minorities is even more remarkable. Now 95.8 percent of the people's communes (townships) and 53.9 percent of the brigades (villages) have access to a telephone. In Qinghai province, an area of 700,000 square kilometers, there were only five post offices and one telecommunications office before liberation. Today there are more than 200.

All these achievements made in the past three decades were unthinkable in the old China.

CHINA'S TELECOMMUNICATION INDUSTRIES AND SCIENTIFIC RESEARCH

In the past 34 years following the policy of taking the initiative into our own hands and self-reliance, we have built through our own efforts a comprehensive post and telecommunications industry and made big progress in scientific research in this field. Twenty-eight affiliated factories, two institutes, and a dozen research units have been established under the Ministry of Posts and Telecommunications.

We have now basically mastered the switching technique of analogue telecommunications and large-capacity transmission. A fairly big production capacity for these has been reached. We have also formed the basis for developing the digital communications technique. We are able to produce cross-bar local telephone exchanges with a capacity of more than 10,000 lines, coded cross-bar toll telephone exchanges with medium or large capacity, 1,800-channel coaxial cable carrier systems, and 960-channel microwave systems. 30-channel and 120-channel PCM systems have already gone into operation. Apart from these, scientific research and the trial manufacture of modern telecommunications equipment is also underway. Trial operation of an 1,860-channel microwave system and a 4,300-channel Cazler system will soon be completed.

We can now manufacture earth stations for satellite communications and are testing under actual operating conditions a short wavelength optical fibre system. A stored program controlled automatic message transmitting system of medium capacity, electronic teleprinters, and group 2 subscriber-to-subscriber facsimile machines are being publicized.

MAIN DEVELOPMENT TARGETS FOR THE NEXT 20 YEARS

The experience gained from our own endeavours over the past 34 years and from advanced countries shows that telecommunications are an important infrastructure of modern society and should develop in harmony with, or quicker than, the growth of the national economy. Yet in present day China, posts and telecommunications is one of the weak links in our national economy. As is known to many, China has set herself the goal of quadrupling her gross annual value of industrial and agricultural production by the year 2000. In our struggle to attain this goal, we have recognized the necessity for telecommunications to

develop at a slightly higher rate than national economy as a whole. The Central People's Government and People's Governments at all levels are giving higher priority to telecommunications in investment and other forms of support. All these mean that telecommunications are entering a new phase of development. Based on progress in science and technology, by 2000 China will have gradually built a modernized posts and telecommunications network which will be able to provide high-quality, highly efficient services to the customers. This is the starting point in drawing up our strategy for development.

Concrete targets are as follows:

Telephone network

A telephone network is the main emphasis for development. We shall employ, step-by-step, SPC digital telephone exchanges and digital transmission equipment in the big cities and use cross-bar toll telephone exchanges for the medium-sized and small cities and other areas. By 2000 the national figure for telephones will increase several times. The urban and county telephone exchanges will be largely automated.

For long-distance telephones, a complete network with multiple tandem centres and multiple functions suitable for normal direct connections, will be gradually built and many alternative routes will be formed. Long-distance telephone circuits and automatic exchanges will increase considerably. Inter-city long-distance calls will have automatic or semi-automatic dialing.

Transmission media

Before 2000 new-type local telephone cables, long and short wavelength optical fibre systems will be introduced in a big way. Apart from bigger capacity carrier cables and microwave system, optical fibre cables, satellite communications and digital transmission technique will be employed in long-distance services.

Data communications

Data communications will be developed on a large scale. Medium-speed data communications are now available in telex networks and public automatic telephone networks. Later, a better data transmission network will be established which will be suited to packet switches and will enable the use of computers and other terminals with different bit rates, codes, and protocols to interwork. A state public data communications network will also be built.

Satellite communications

As China has a vast territory, complicated topography, and varied climates, we will space-lift our own communications satellites and thereby step-by-step build a satellite communications network for domestic use. In the near future we shall lease transponders from Intelsat so as to meet the communications needs of our border areas and other regions where earth networks cannot easily reach. The transponders will also serve the special duty communications of different sectors of the national economy.

SOME FACTORS AFFECTING THE DEVELOPMENT OF TELECOMMUNICATIONS

Infrastructures

Though China's telecommunications has developed greatly in the past 34 years, they still fall short of meeting the growing needs of the national economy and the social life of our people. The main problems here are as follows: Switching equipment and transmission lines are seriously inadequate, thus service capacity is far from sufficient. This is particularly evident in the state of urban telephone systems. The national percentage of telephone availability for per hundred inhabitants is very low. Even in Beijing, the capital, the percentage is only 4.2. In many big cities there are long lists of people and units waiting to have telephones installed. Quality and efficiency of service is not satisfactory. Communications equipment is little and technology low. For instance, one third of the urban telephone exchanges (mainly in counties) are manually operated. Manual operation also prevails in long-distance telephone service. As a result, efficiency is low. This situation has hindered domestic and international telecommunications service. In the recent years, as China has adopted an open-door foreign policy and aimed at bringing her national economy into full swing, the gap between the rising demands for telecommunications services and their low capacity becomes wider. Responsible for such a situation are the following: weak foundation, low investment, backward technology, and faulty management.

MEASURES TO BE TAKEN
FOR DEVELOPING COMMUNICATIONS

In order to change the backwardness of our communications service as soon as possible so as to meet the needs of modernization, the Government has made telecommunications one of its major strategic emphases in its general development plan. To speed up the process, we have adopted several measures:

[] Beginning from 1982, the State has increased the proportion in its total investment for post and telecommunications construction and increased the percentage of services profits and foreign exchange revenues to be retained by the post and telecommunications administration so that it can have greater financial resources for equipment and upgrading technology.

[] The national banks are to grant low-interest loans to the post and telecommunications administration so that it can import stored program-controlled telephone switching equipment and other advanced devices for use in the transformation of existing networks or building new ones.

[] The Government has approved a proposal to lease Intelsat transponders and establish new earth stations to provide domestic satellite communications.

[] The Government is giving full support to the initiatives of various governmental departments, enterprises, and local authorities to coordinate the development of special service telecommunications networks.

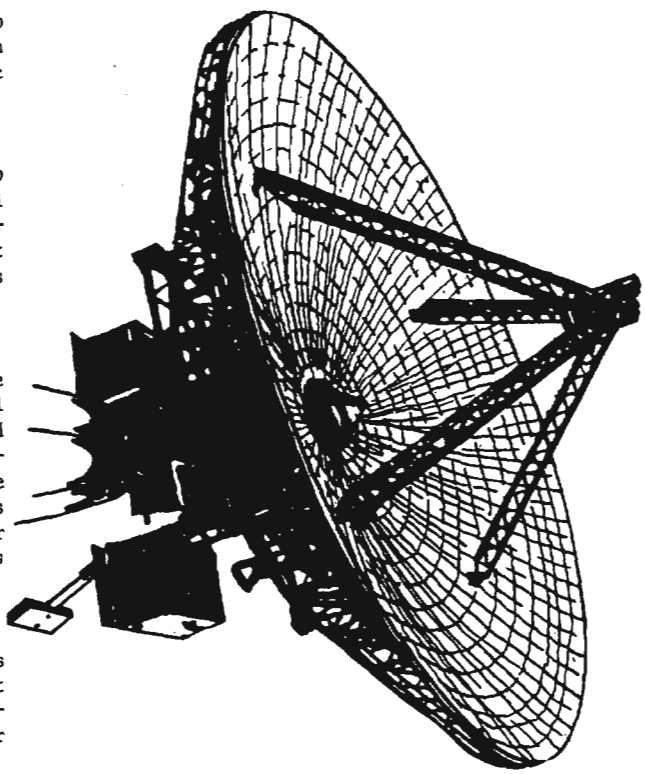
[] Greater attention is being paid by the Government to the development of rural communications facilities. Under unified planning and technical standards, localities and departments are expected to take the initiative in building rural networks with investment from local authorities or collective donation by the subscribers and peasants.

[] Profits from urban telephone services need not be turned over to the State, but are kept by the post and telecommunications administration as special funds for expanding telephone services.

[] Construction of urban telephone facilities is framed into the overall development plans of cities so that the investment required can be drawn from both the Central People's Government and the local authorities.

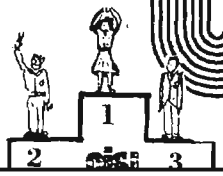
[] New subscribers will be charged for the installation of telephones and the revenue from this set aside as supplementary funds for construction of urban telephone systems.

We have now realized that in a country with a vast territory and huge population such as ours, to carry out the task of modernizing telecommunications, we should rely mainly on our own efforts. At the same time, following our foreign policy, we will import advanced technology and equipment from abroad. We will also strengthen economic ties and technical cooperation with friendly foreign countries and undertake joint ventures with them. Friends and our colleagues in telecommunications, industrial and commercial circles abroad are welcome to cooperate in our efforts to accelerate China's telecommunications development.



DOCID: 4009891

1983 CISI ESSAY AWARDS (U)



by [redacted] R53

P.L. 86-36

(U) In 1982 I was newly elected as a Member-at-Large of the CISI Board. During discussions for the 1982 CISI Spring Conference, there was some sentiment for not having a paper competition coupled with the conference, as it had been for the past several years. I suggested that CISI should run a totally separate essay awards competition in the fall, as other NSA professional organizations did. The CISI Council agreed wholeheartedly with my idea and promptly appointed, elected, or maybe railroaded me into the job of organizing and running such a competition for 1982. As you may remember, we had a very successful 1982 competition with 15 papers submitted in three categories and five cash prizes were awarded. Most of these papers were published in a very nice (but somewhat late, due to size and color printing) special issue of Cryptolog. This was billed by me as the "First Annual CISI Essay Awards Competition."

(U) When 1983 rolled around, I once again was asked to organize and run the essay awards competition for 1983. (However, this time I had volunteered to do so.) As you will see below, we had another good year in this, the "Second Annual CISI Essay Awards Competition." After the 1983 version was completed, when I was cleaning up my documentation for both 1982 and 1983 to file it for CISI posterity, I asked the CISI secretary where I should file all this material. She handed me the CISI Essay Contest file folder (as yet not seen by me). Inside, I discovered memoranda and notes dating from 1969 to 1972, which showed that the truly FIRST annual CISI essay contest was held in 1969, not 1982. My apologies to anyone offended by my renumbering efforts. One interesting discovery on my part was that most of my judges for 1982 and 1983 had been entrants in these much earlier contests. Some of them had even won awards.

(U) The main purpose of the CISI Essay Awards competition is to encourage NSA employees to share their expertise and experience in computer and information sciences with the NSA community. CISI feels that publishing papers from the competition in Cryptolog and elsewhere helps further this purpose, especially for papers that might not receive wide distribution otherwise. The secondary purpose of the competition is to reward NSA employees for excellent technical writing with cash prizes. We hope that these prizes stimulate papers to be written which might not otherwise make it to hard copy.

(U) Papers submitted for a CISI Essay Awards competition need not be written specifically for the Awards. Any paper on an appropriate topic written during the previous year may be entered. Papers written for work-related purposes, for classes, or for professional certification (especially those designated Honors Papers) may be acceptable entries. Papers may be classified up to Top Secret Codeword. All authors of papers submitted to this competition must be NSA employees. Papers published or accepted for publication in outside technical journals are not automatically excluded from this competition.

DOCID: 4009891

However, only the author's final draft as originally submitted for outside publication will be accepted for this competition.

(U) For the 1983 competition, papers were solicited in the following three general categories:

[] Systems Software

[] Applications Software

[] Systems Design and Hardware

(U) Nineteen papers were received in all. Each category had its own panel of judges who refereed (i.e., decided which papers should be published) and judged (decidin which ones derserved prizes) each paper in that category. Judging criteria included relevance to the field, quality of writing, completeness, and significance to NSA.

~~(C)~~ After hard work on the part of our three panels of judges, the following prizes were given as the 1983 CISI Essay Awards:

Category I: Systems Software

[] First Prize: [redacted] of W196 for "Logical and Structural Conflicts"

[] Second Prize: [redacted] of B613 for "A Computer Graphics Data Base Design Aid Package"

Category II: Applications Software

[] First Prize: [redacted] of G622 for "Computer Scripting of Arabic: Not the Impossible Dream"

[] Second Prize: [redacted] of R531 for "INTERROGRAPH: An Information Tool for Counter-Terrorism Intelligence Centers"

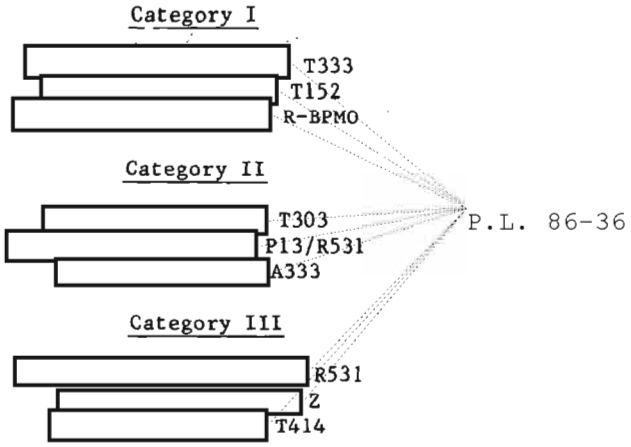
P.L. 86-36

Category III: Systems Design and Hardware

[] First Prize: [redacted] of A215 and [redacted] of T443 for "Designers vs Users: Bridging the Communication Gap"

[] Second Prize: [redacted] of G331 for "The Apollo DOMAIN Network: An Integrated Approach to the Networking of Powerful Personal Computers"

(U) I would especially like to thank our nine judges, several of whom also served as judges last year:



(U) Our publication procedures will be different this year. Rather than wait a very long time for an extremely big, special issue of Cryptolog, the abstracts of all successfully refereed papers will be published in THIS issue of Cryptolog. A number of these papers are already scheduled to be published in a special issue of the NSA Cryptologic Quarterly (due out in February or March) and those abstracts will be so noted. The editors of Cryptolog will work with the remaining authors and will publish their papers in various issues of Cryptolog during the coming year. This procedure will allow you to very quickly see all of the abstracts and to fairly quickly read those papers which require little or no editing.

(U) I hope you enjoy reading the results of the 1983 CISI Essay Awards competition. It's not too early to begin thinking about a paper for the next competition. Many of this year's entries AND winners began as a class term paper or as a paper for professional certification.

SOLUTION TO NSA-CROSTIC No. 51

[NSA] Safety Hazard Notice, dated 12 Jan 84.

"Failure to use a three-prong plug with this equipment [may] cause operator shock. Every user should contact the Occupational Health and Safety Office to obtain labels which should be affixed to the equipment."

DOCID: 4009891

ABSTRACTS (U)

Category I: Systems Software

P.L. 86-36

Conflicts Between Logical and Supporting Structures: Concern for Computer Software Professionals

by [redacted]

(U) Visual constructs and documentation used by human analyzers of computer source language documents often conflict with the logical structures that they support. Basic types of conflicts are identifiable as well as their causes. Techniques are given for detecting discrepancies. The function and form of coding constructs can be controlled to ensure correctness of the ancillary structures. Changes to existing programming tools are suggested which could reduce the probability of conflicts being generated.

A Computer Graphics Data Base Design Aid Package (Cryptologic Quarterly)

by [redacted]

(U) The most important phase of data base development is the design phase. A poorly designed data base may not be able to handle important applications in a timely and efficient manner. In fact, a costly and possibly prohibitive redesign may become necessary if new applications not originally envisioned are suddenly needed. Because data base design is the most difficult and time-consuming phase when done properly, the temptation is to avoid expending the necessary amount of time in this phase. One solution to ease this temptation is to automate the design process using computer graphics. The designer can input his design at a terminal and allow the computer to analyze it, enabling him to quickly spot weaknesses and flaws. This paper presents the man-machine interface for such an interactive graphics data base design tool running on a powerful personal computer.

NOS/BE To NOS 2 Conversion: Significant Differences from a User's Perspective

by [redacted]

(U) The purpose of this paper will be to evaluate if the change from the Network Operating System / Batch Environment (NOS/BE) to the Network Operating System, version 2 (NOS 2) on the METEOR complex will have a major impact on its users. Conversion is tentatively scheduled for November 1984. Significant differences in the two systems from a user's perspective will be outlined. Where these are reductions in current capability, proposed or available compromises will be presented. This paper should serve as a useful guide in assisting users converting to NOS 2.

P.L. 86-36

C Programming Using UNIX System Calls

by [redacted]

(U) UNIX system calls are a way of interfacing between C programs and the operating system. These system calls can be subdivided into several categories which include: I/O calls, Process Management calls, and File System calls. The purpose of this paper is to provide additional explanations and examples of the system calls found in Chapter II of the PWB/UNIX documentation manuals in order to aid C programmers. This paper is a supplement to the manuals, which present a brief description of the calls but do not explain how to implement them or why they may be needed in C programs.

Category II: Applications Software

P.L. 86-36

Computer Scripting of Arabic: Not The Impossible Dream (Cryptologic Quarterly)

by [redacted]

~~(C)~~ Agency nonvoice linguists are tasked with extracting intelligence by translation, working under a variety of conditions ranging from mildly inconvenient to near crippling. This paper will concentrate on those difficulties that result from conflicting transliteration systems imposed on an already foreign language, while examining the question of computer scripting of Arabic with output in soft and hard copy. It will then address solutions to these problems, using as examples descriptions of the work done in private industry on Arabic scripting. A complete

scenario of how such a system should look to the working linguist at NSA is also presented.

(U) Although current technology is available to generate computer scripting of Arabic, other factors, including limitations on personnel and monetary resources, would probably preclude implementation of such scripting at the Agency in the immediate future. However, given the rapid strides made in computer technology in recent years, together with declining relative costs, computer scripting of Arabic might well be a reality at NSA in the not too distant future.

INTERROGRAPH: An Information Tool for Counter-Terrorism Intelligence Centers (Cryptologic Quarterly)

by [redacted]

(U) A user interface design for a Spatial Data Management System for the retrieval of information on international terrorism is outlined. After a discussion of the benefits of using graphics to interact with a data base, the concept of SDMS is briefly described. The qualities that make SDMS an appropriate system to use in conjunction with a terrorism data base are mentioned. Several examples of possible incidents involving terrorists and how questions arising from these incidents could be answered by INTERROGRAPH show the efficacy of the system for a watch center.

M(A)T: Method from Madness

by [redacted]

(U) This paper discusses the field of machine translation in general and my own theory in particular. Chapter I introduces the terminological distinction between machine translation (MT) and machine-assisted translation (MAT) and considers the most important US groups currently doing MT. Chapter II explores the three-way nature of the problem: language, theoretical linguistics, and computer science and traces the history and development of linguistic science, especially those recent treatments rigorous enough to be simulated by computer. Chapter III deals with the nitty-gritty of translation at the syntactic level and the kinds of abstract structures that need to be created and manipulated by any serious MT system. Chapter IV considers the specific strategies of syntactic description required by MT. Chapter V describes and flowcharts my computational implementation in SNOBOL4. Chapter VI cites recent literature in support of the methods adopted and proposes a schedule for an NSA feasibility study.

P.L. 86-36

Top-Down COBOL Management

by [redacted]

(U) Having a set of standards guarantees neither efficient coding practices nor the staff's willingness to apply them to module development. Design considerations and management decisions can affect the rate at which code is produced and the correctness of the executable code. These factors also affect the amount of time spent during any one phase of the program development to correct for design errors.

(U) This paper details an approach to software design and development which defines elemental activities in the design and production of COBOL code at the module level. The definitions are then used as tools in the technical and managerial aspects of module production.

(U) An outline of adjunct COBOL coding standards will be presented which stresses naming conventions. Most importantly, all development documentation is an integral part of the delivered product, thereby eliminating redundancy and the conflict that can occur between internal and external documentation.

(U) Suggestions on how the phases in this methodology can be PERTed or used in other resource management techniques will be offered.

Ada and Cryptanalysis

by [redacted]

(U) Ada is the new computer language developed by the Department of Defense. After a brief introduction to Ada and the concept of staged testing in cryptanalysis, this paper takes a look at the advantages and disadvantages of using Ada in the cryptanalytic environment. The paper tries to decide how best to use Ada in cryptanalytic applications, if at all.

A Graphic User Interface for the Transcriber-Analyst (Cryptologic Quarterly)

by [redacted]

(U) Designers of new computer systems are placing increasing emphasis on user friendliness, specifically on the ability of non-ADP professionals to gain quick and easy access to their data and data base systems. Two of the newest and most intriguing systems, from the intelligence analyst's point of view, are the

Xerox Star and the Computer Corporation of America's Spatial Data Management System (SDMS). Both systems use visual/graphic approaches to data storage and retrieval and are based on the principle of having the user select files and data from graphical menus/directories, rather than rely on often complicated query languages. This paper will detail how these state-of-the-art systems could be used by transcriber-analysts here at NSA.

CRITICOMM Management
A User Interface
(Cryptologic Quarterly)

by [redacted]

~~(C)~~ As NSA moves into the 80s and the age of increasing automation of data-collection facilities, the human beings who are called on to interpret that data become more and more inundated by the sheer volume. T13, for example, receives large volumes of data daily, only part of which is used because of a lack of resources to organize it into information. Some means must be found to convert more of the data into information which can be used by a person sitting at a desk or a terminal. One concrete example of this data explosion is circuit management of the CRITICOMM network. This is accomplished through monthly statistical reports (NSA-760s) which are sent to T133 from the stations of the network and are incorporated into the monthly CRITICOMM Operational Summary (COS) prepared by T133. Circuit management is also accomplished on a near real-time basis through the CRITICOMM Systems Management system (CSM). As a result of Project TREEHOPPER, a manual data entry system for the NSA-760 monthly statistical report was converted to an automated system using GENED and SPECOL to manage the data base, but even this advance left the analyst with hard-to-understand reams of alphanumeric data.

(U) This paper illustrates how interactive graphics techniques can be used to convert the present follow-on reports to the NSA-760 report into a pictorial format in order to clarify the information. It suggests report formats to make use of data in the NSA-760 report not now used--as well as formats which tie together data from the NSA-760 reports and other data bases. Applications of interactive graphics to the time-sensitive work of the CSM are also presented.

Category III: Systems Design and Hardware

Designers vs. Users:
Bridging The Communication Gap
(Cryptologic Quarterly)

by [redacted]

(U) The communication gap that has existed between users and designers of computer systems has widened with the introduction of new terminology and new methods of user interaction. A design technique known as "mock-ups" was eventually devised to improve communication with users during the requirements specifications and design phases of new graphics projects. This paper presents a detailed example of the mock-up strategy. For those individuals interested in composing a design using this technique, some instruction has been provided, including a section on an automated mock-up maker.

The Apollo DOMAIN Network:
An Integrated Approach to the Networking
of Powerful Personal Computers

by [redacted]

(U) One of the most exciting new data processing technologies to emerge in the past couple of years is the local area network (LAN). The continued maturation of this technology has opened the door to a host of innovative and economical approaches to distributed processing, resource sharing, and high-speed local communications. Still in its formative years, the LAN industry currently consists of a large number of vendors offering a wide variety of LAN devices and systems designed for an equally wide variety of applications.

(U) One of these applications involves the use of the local network to build a system of linked microprocessor-based workstations which share a pool of common resources, such as disk files and printers, via the local net. Such local network resource sharing is a very cost-effective mechanism for greatly enhancing the processing environment available to the user of a microprocessor. Examples of such systems are the Corvus Omninet and the Xerox 8000 Network System.

(U) Another company to incorporate this concept into a system design is Apollo Computer. In addition to utilizing current LAN technology, Apollo has taken advantage of other state-of-the-art hardware and software technologies (high-density RAM, 32-bit VLSI processors, interactive high-resolution graphics with bit-mapped interfaces, Winchester

DOCID: 4009891

disks, and high-level object-oriented operating systems) to develop a very sophisticated system of powerful personal computer workstations integrated into a high-speed resource sharing local network. This network, called DOMAIN (Distributed Operating Multi-Access Interactive Network), presents the scientific and engineering professional with a promising processing alternative to current timesharing and dedicated systems.

(U) This paper outlines the concepts behind the Apollo DOMAIN network, describes the integrated design approach and the primary architectural features of the DOMAIN and its associated nodes, discusses some of the advantages and disadvantages of this type of system, and briefly looks at potential applications for the Apollo and Apollo-like systems at NSA.

Cartography in The Electronic Age
Paper vs. Display Screen

by [redacted]

(U) Maps have been an invaluable tool of communication since earliest time. Although the basic nature of maps is relatively uniform, the characteristics of individual maps are dictated by the use for which the map is created. Static paper maps have been common for centuries. Today, however, the availability of computer technology has caused the advent of dynamic electronic maps. This paper discusses the characteristics of maps and compares and contrasts paper maps to electronically generated ones. It then examines the various factors involved in designing flexible, detailed, and portable map display systems and compares the current technologies available for creating such systems. Finally, an evaluation of the potential for future use of these interactive map display systems, together with NSA implications, is presented.

Management of TDY Funds:
A Graphical Approach
(Cryptologic Quarterly)

by [redacted]

(U) A manager's primary resource is time. He has only so much time in a day to absorb information relevant to his immediate decision-making responsibilities. Managers therefore prefer graphic displays which reduce large amounts of complex information into readily understood pictorial form.

(U) This paper addresses the area of computer graphics for management applications. An example of this application is presented, displaying the management of TDY funds. A systems design is provided on a computer graphics system for the Travel Program at NSA. The present system and its shortcomings are described, and requirements for a new graphics system and examples of the desired outputs are presented. Fortunately for NSA, this requirement can, by and large, be satisfied with an off-the-shelf "turnkey" system recently announced by the Xerox Corporation. The graphics system, Xerox Star workstations linked by the Ethernet communications facility, is then described, and the TDY application is demonstrated. An additional NSA application for this computer graphics system, the Stock Fund program, is also described. Computer graphics systems, like the one referred to in this paper, will provide managers with a means to quickly analyze and respond to complex information. Satisfying such Agency requirements with off-the-shelf equipment will also reduce the burden on NSA's data system personnel.

Optical Disk Technology:
The Future of Mass Data Storage

by [redacted]

(C) Optical disk technology is still a relatively new field. Consumer products have been on the market for approximately five years and have been fairly slow to catch on, mainly because they lack the record/play flexibility of video tape recorders. This disadvantage on the consumer front becomes a real advantage on the data processing front as government agencies and private industry explore their needs for long-term archival storage of large amounts of data. Optical disk storage capacities are in the terabyte region, and their relative low cost and indestructability make them the logical choice for this use. This paper covers the types and capacities of various optical disks, discusses NSA's research and development effort in that field, and the objectives of the contract NSA has let for the acquisition of a prototype system. In addition, commercial applications and NSA applications for optical disks will be explored.

Replace RACE

by [redacted]

(U) RACE is the name given to a computer system operated by T154, the goal of which is to provide signals data base and management support to Management and Signals Conversion Technicians. It is no secret that over the past few years this system, with respect to its task effectiveness, has been declining. Also the workload being placed upon it has

P.L. 86-36

increased to such a degree that the time has arrived for management to take an objective look at the prospect of replacement. RACE is, after all, an essential tool in the fulfillment of the mission of the Agency.

(U) This paper addresses RACE in its past and present operating environments, while examining its functions, capabilities and requirements. It attempts to show that there is a limited future for RACE in its present working environment mainly due to its single job processing and low-level assembly language characteristics. The author will demonstrate that RACE is slow, outdated, and inadequate based on todays demands and has outlived its usefulness within the T organization. Also, it will be shown that the operational elements supported by RACE critically need a replacement computer.

(U) This paper will also discuss and summarize the results of research into the UNIVAC 90/30 computer system, a prime candidate for replacement of the present RACE equipment.

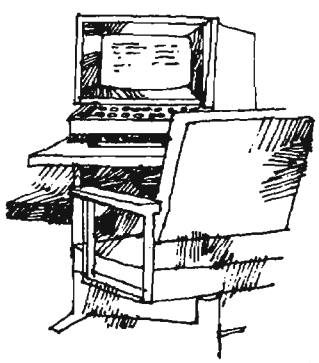
P.L. 86-36

Excellence Must Be Cultivated Corporately:
Some Ideas For Improving Productivity

by [redacted]

P.L. 86-36

(U) This paper focuses on the issue of excellence, excellence in terms of products, people and the management of both. We will consider several perspectives on what excellence is and means, why it is especially important now and how it might apply to NSA in general, and to computer and information science in particular. Next we will address the theme of this paper, that excellence must be cultivated corporately and what that implies. Then we will learn about what others are doing to cultivate excellence. We will also consider the need to generate more feedback in order to effectively apply what others have learned to NSA. Finally, a number of specific suggestions will be proposed which could significantly improve the productivity of our products, our people and our management process, if we corporately commit ourselves to the cultivation of excellence.



WE ARE ALWAYS LOOKING FOR

ARTICLES, COMMENTS, NOTES, LETTERS,

THAT WOULD BE OF INTEREST TO OUR READERS

DOCID: 4009891

~~FOR OFFICIAL USE ONLY~~

The Language Problem at NSA

by [redacted]

P.L. 86-36

(U) In February 1976 the US Air Force's Foreign Technology Division invited NSA and other agencies to send a representative to a Conference on Translation. The purpose of the conference was to share mutual translating problems and interests. Representatives were asked to present a brief introductory (and unclassified) statement about the language problems at their respective agencies. Ms. [redacted] were NSA representatives, and [redacted] was tasked with presenting the introductory statement, which is reproduced here.

P.L. 86-36

(U) There is no language problem to speak of at NSA. Let me phrase that another way: there is a language problem at NSA, but we don't speak of it in mixed company. If I were to speak of it, I would state that the language manager at NSA is looking for a language specialist

* who at the time of hiring has a native understanding of the subject language (or better yet, of several languages);
* who is a rapid reader and a prolific writer;
* who is well-versed in the subject language culture;
* who understands various specialized jargons equally well in English and the subject languages;
* who is a top-notch intelligence analyst;
* who is a native-born, loyal American citizen who has never traveled abroad;
* whose command of English is superb;
* who enjoys the opportunity to learn exotic or low-density languages in spite of the poverty of tools available about that language;
* who spends his or her spare time maintaining these skills without making contact with any foreign nationals;
* who enjoys taking--or teaching--courses to improve proficiency (with no decrease in production chargeable to class time);
* whose private life is above reproach (and especially blackmail);
* whose needs are simple and whose wants are few;
* who enjoys the challenge of maddeningly incomplete or imprecise text from which an accurate translation is to emerge; and
* who is imaginative and creative in tackling hard problems as well as a stickler for accuracy in translation.

(U) Those language managers also expect this person's name to be Legion--but Nemo is more apt.

~~FOR OFFICIAL USE ONLY~~

EO 1.4.(c)
P.L. 86-36

G61

P.L. 86-36

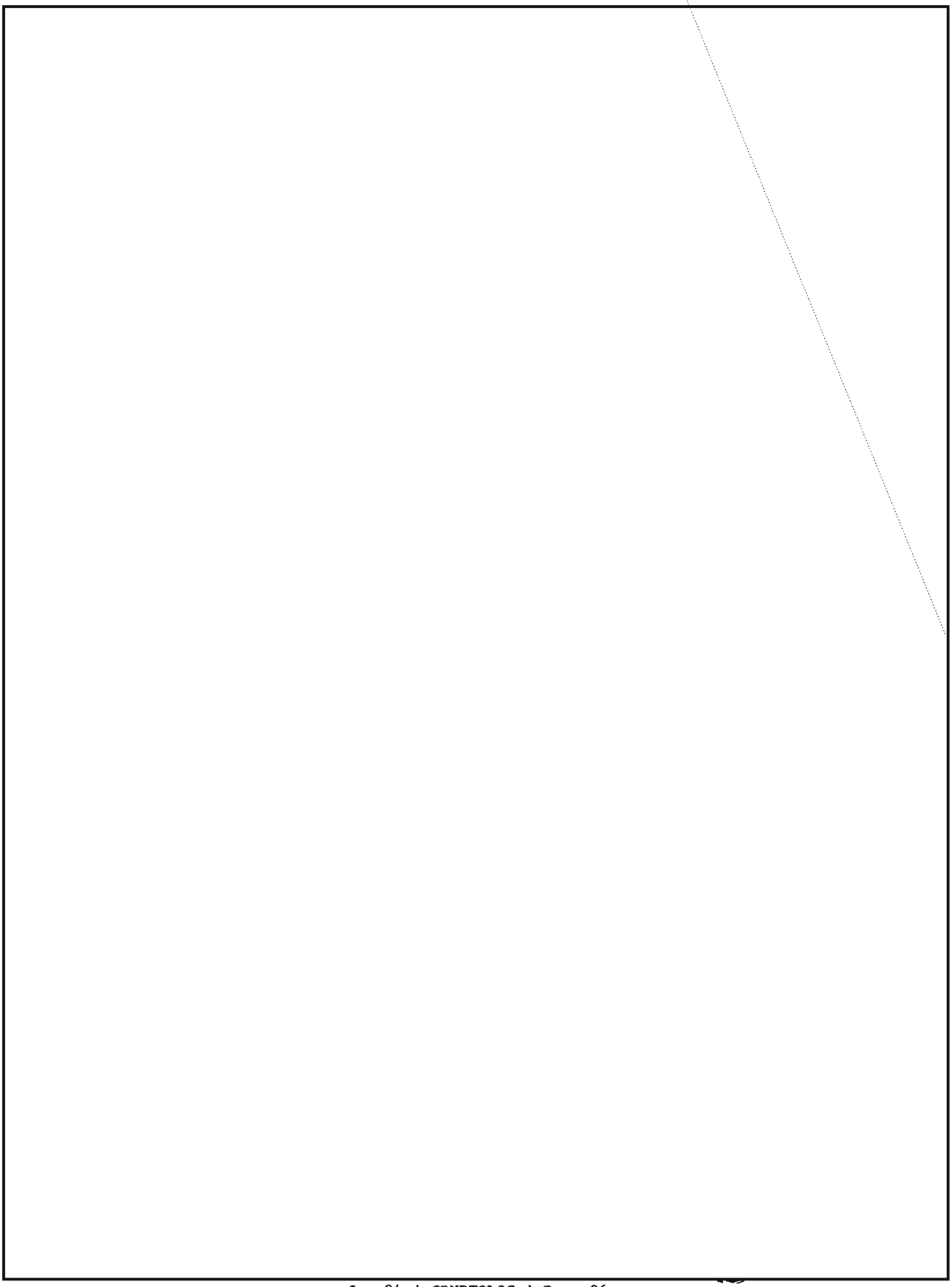
****

I keep six honest serving-men
(They taught me all I knew):
Their names are What and Why
and When
And How and Where and Who.

--Rudyard Kipling

****

EO 1.4.(c)
P.L. 86-36



P.L. 86-36

To: [redacted] P14
From: [redacted] A3111

Re: *Subscribing to the CRYPTOLOG*

(U) Please add me to the subscribers' list for CRYPTOLOG. I have discovered that some of the articles (like the one on ELINT notations in the October 1983 issue) are so useful that I clip them and save them, or else I stash the thing in my desk and the rest of the branch is deprived of the chance to read it. Clearly I need my own copy!

---

1. ~~(FOUO)~~ Per our phone conversation ..., this is to inform you that the following two articles from the October 1983 CRYPTOLOG were reproduced and disseminated to selected [redacted] employees:

a. "Tips on Topical Reporting"

b. "Banners, Cowboy Hats, & ELINT Notations"

2. ~~(FOUO)~~ [redacted] recipients were advised of the requirement to keep the articles within the cryptologic community. ...

[redacted]

To: [redacted] *Editor*
Fm: [redacted]

~~(C)~~ I found the article in the Sept 83 issue of Cryptolog entitled PARPRO (beginning on page 15) most informative and interesting.

[redacted]

To [redacted]

~~(FOUO)~~ In regards to your "I Remember JFK" in the Nov 83 issue of Cryptolog, I was here at the Agency on the day President was shot. I was working in A2 at the time ... [in] Room 3E039.

~~(FOUO)~~ For your information, there were 2 announcements made over the loudspeaker system. The first one said "Ladies and gentlemen: The President of the United States has been shot and is in critical condition." The second one in a very solemn voice (male) simply said "Ladies and gentlemen, the President of the US is dead."

~~(FOUO)~~ You may or may not have been informed by the people who were here at the time. If so, sorry for the inconvenience.

[redacted]

[redacted] *replies:*

~~(FOUO)~~ *If* [redacted] *says he heard two announcements, I won't argue with him. But I stand by my original statement that the folks in the office where I was working on that day (Room 2C-something-or-other) didn't hear even one. I'm fairly sure that I wouldn't forget any announcement that started off with "Ladies and gentlemen" instead of the standard "May I have your attention please!" (especially if it happened twice).*

HGR

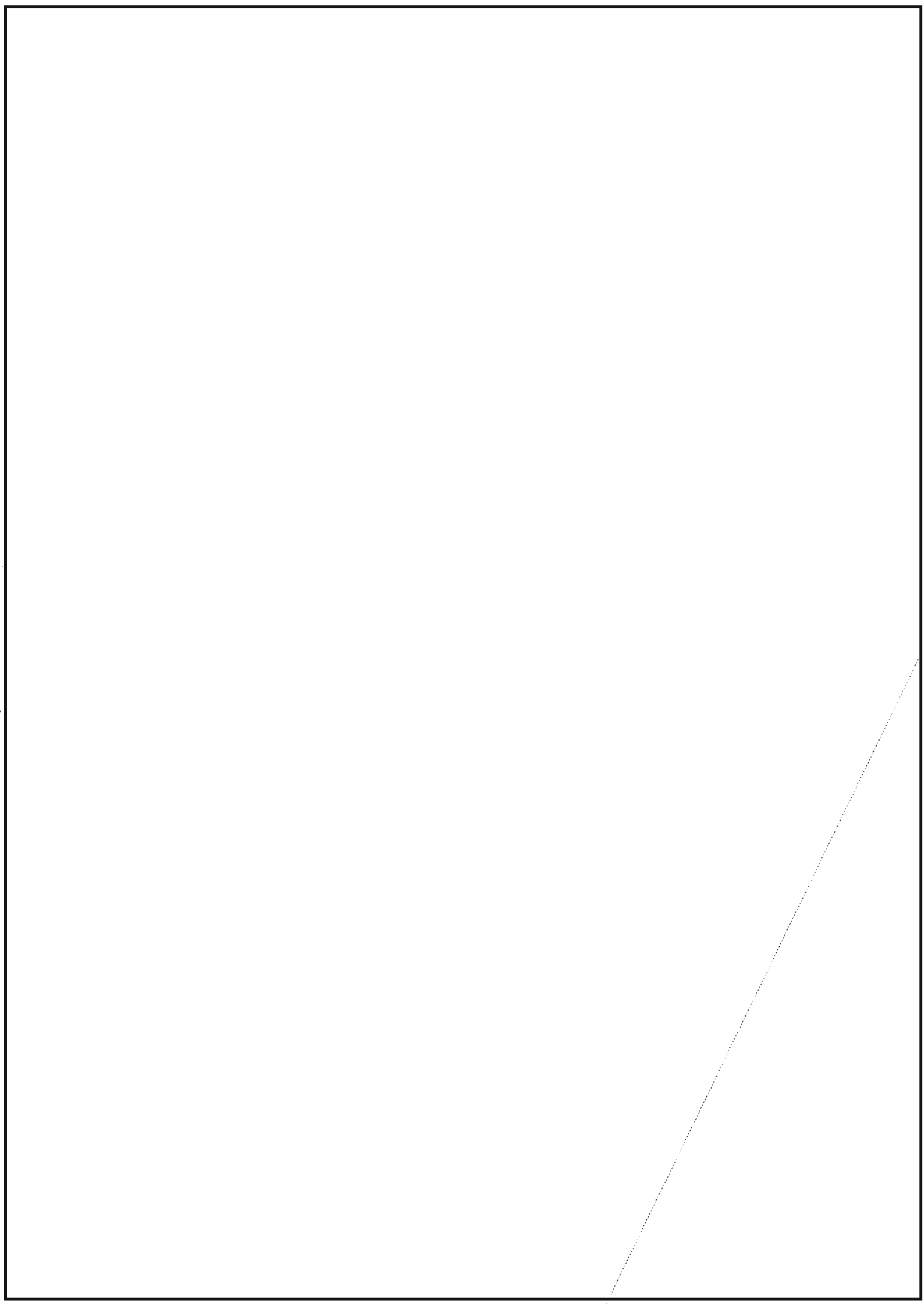
DOCID: 4009891

P.L. 86-36

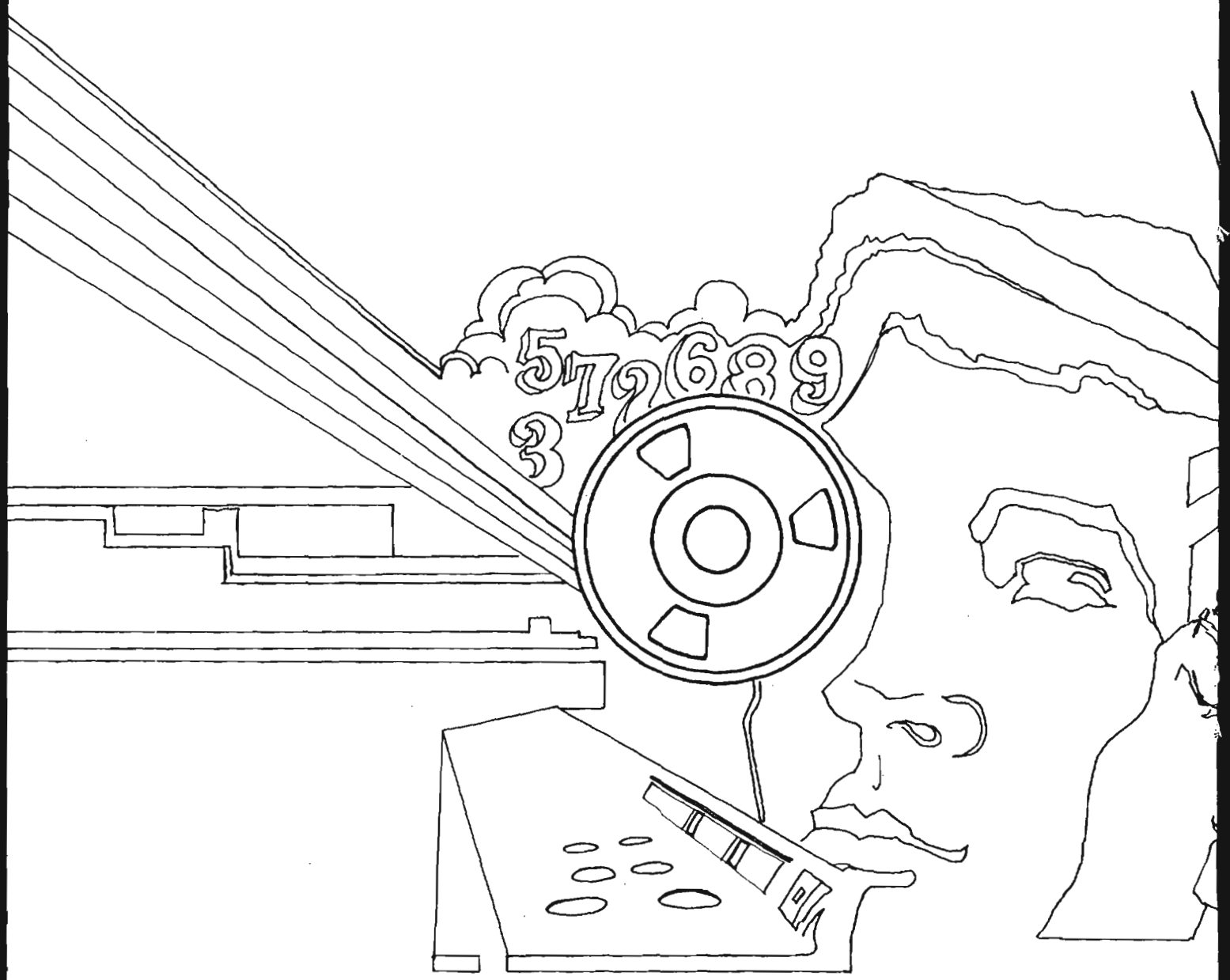
NSA Crostic No. 52

[redacted] this month's Guest Acrostician, crafted this fine first effort over a weekend, because "I just wanted to see if I could do one."

P.L. 86-36



P.L. 86-36


5726893

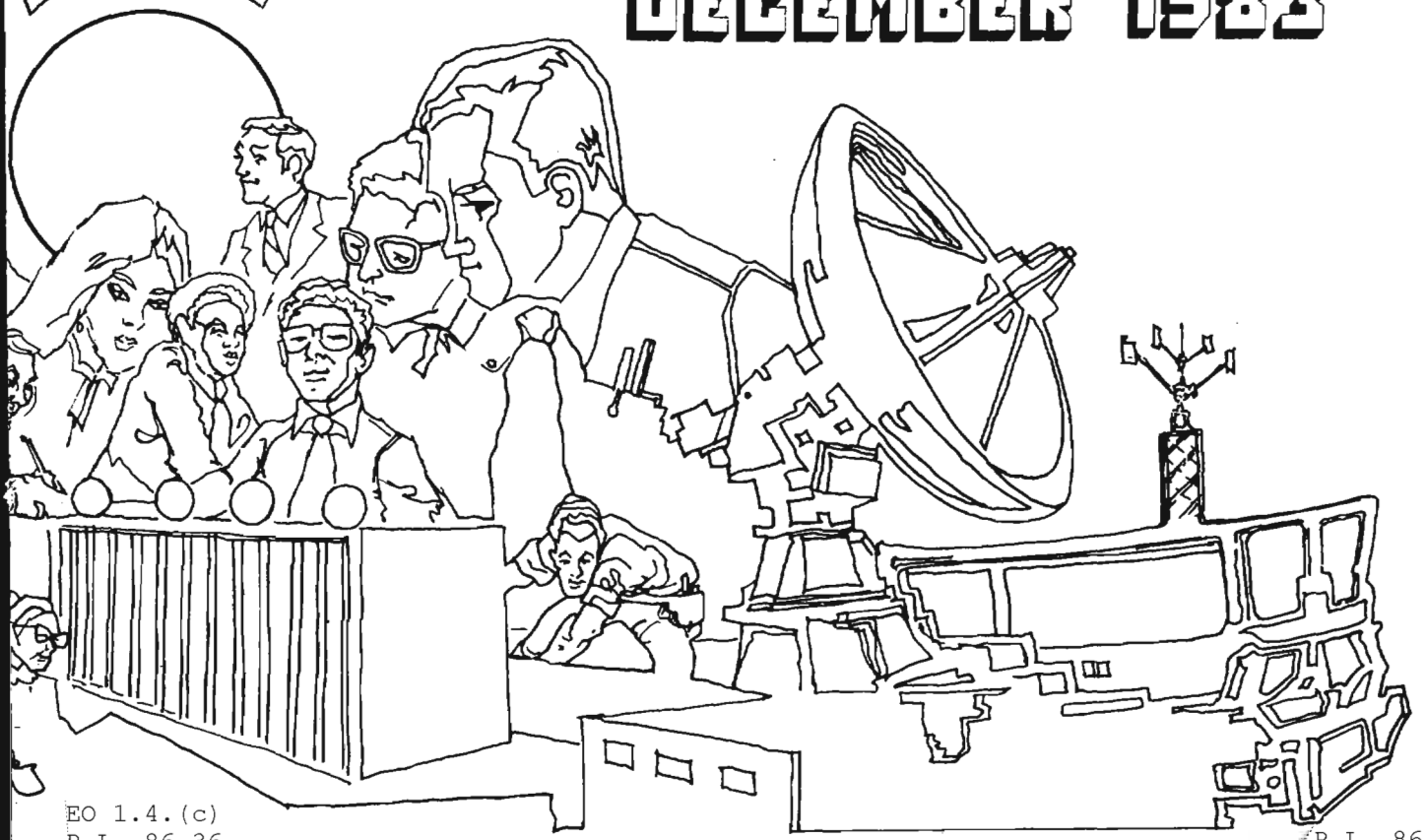
DOCID: 4009888

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

DECEMBER 1983



EO 1.4.(c)
P.L. 86-36

P.L. 86-36

THE ISLAMIC TIME BOMB (U)..... [redacted] 1
OUT OF MY DEPTH (U).....5
NON POSSE VS. POSSE NON (U).....H.G.R.....7
SOVIET PSI EXPERIMENTS (U)..... [redacted] 9
[redacted] ..... [redacted] 14
SHELL GAME: SYSTEM SHELLS (U)..... [redacted] 20
DCL: THE DIRECT COMMUNICATIONS LINK (U)..... [redacted] 21
NSA-CROSTIC NO. 51.....David H. Williams.....28

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating~~

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009888

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. X, No. 12 DECEMBER 1983

PUBLISHER [redacted]

BOARD OF EDITORS

Editor..... [redacted] (963-3045s)
Asst. Editor... [redacted] (963-1103s)
Production..... [redacted] (963-3369s)

Collection..... [redacted] (963-3961s)
Computer Security
..... [redacted] (968-7313s)
Cryptolinguistics. [redacted] (963-1103s)
Data Systems..... [redacted] (963-4953s)
Information Science
..... [redacted] (963-5711s)
Mathematics..... [redacted] (968-8518s)
Puzzles.....David H. Williams (963-1103s)
Special Research.....Vera R. Filby (968-7119s)

For subscriptions
send name and organization

to: [redacted] P14

P.L. 86-36

To submit articles or letters
by mail, to: P1, Cryptolog

via PLATFORM mail, send to:
cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no '0' in 'log')

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

One of the first articles we published after I took over as editor of this magazine was Ken Williams' piece documenting the decline in technical reporting (October 1982). One of my original reasons for getting into this magazine business was to explore whether technical reports could be produced by an analyst with access to a TSS. The challenge was to see if the "office automation" tools that were already on the TSS/UNIX systems could produce something like this magazine. Looking back over the last two years, my personal verdict is that those tools are sturdy enough to do almost any technical reporting that I have ever had to do.

Consider this magazine: all the layout and formatting is done using the UNIX package 'nroff' along with several related tools. Until recently, each article began on one system (at FANX-III) and finished on a second (at Fort Meade). Except for the titles and graphics, which are added in at the end of the process, all of the layout, including the provision of white space for graphics, is done "on line" at a Delta Data 7000 terminal; the final form of the page is called up onto the screen for a visual check before any printing is done. When the image on the screen looks right, the page is printed out on an Anderson-Jacobson 832 printer, the graphics and titles are added, and the result goes to the printshop for the final production.

Many articles come in over PLATFORM, some from outside the continental US. Thus the words you see are often the author's original keystrokes.

There are presently three of us who keep the magazine rolling. All three do it on a part-time basis, and none of the three of us is a programmer. You don't have to convince us that UNIX/TSS can be used for technical reporting...we are doing it!

* * * CORRECTION * * *

The cover of the October 1983 issue of CRYPTOLOG and the article by [redacted] titled "Banners, Cowboy Hats, and ELINT Notations" should be marked "REL UK CAN AUS NZ"

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009888

The Islamic Time Bomb (U)

P.L. 86-36

by [redacted] W. E41

Any understanding of the current unstable situation in the Middle East necessarily requires a basic knowledge of the past. Let me give you some historical background as a prologue to the present--a historical perspective.

In the great medieval French epic of the wars between Christians and Saracens in Spain, the Chanson de Roland, the Christian poet endeavors to give his readers, or rather listeners, some idea of the Saracen religion. According to this vision, the Saracens worshipped a trinity consisting of three persons: Muhammad, the founder of that religion, and two others, both of them devils, Apollin and Tervagant. To us this seems comic, and we are amused by medieval man unable to conceive of religion or indeed of anything else except in his own image. Since Christendom worshipped its founder in association with two other entities, the Saracens also had to worship their founder, and he too had to be one of a trinity, with two demons co-opted to make up the number. In the same spirit one finds special correspondents of the New York Times and of other lesser newspaper describing the conflicts in Lebanon in terms of right-wing and left-wing factions. As medieval Christian man could only conceive of religion in terms of a trinity, so his modern descendant can only conceive of politics in terms of a theology or, as we now say, ideology, of left-wing and right-wing forces and factions. [1]

Seven centuries after the birth of Jesus Christ, a new monotheistic force sprang forth from the deserts of Arabia called Islam (which means submission in peace to the will of God). Islam was destined to become the third great monotheistic religion of the world to be founded in the Middle East, along with Judaism and Christianity. To Muslims, Muhammad was the last true prophet of God on earth. Muslims refer to Muhammad as Al-Khatim, "The Seal of the Prophets." His message was simple: "There is no other deity but Allah (God) and Muhammad is His Prophet."

The year 622 AD is the starting point for the Muslim calendar because it is the date of Muhammad's pilgrimage from Mecca to Medina. By the year 632 AD the Muslim conquest of Arabia was complete and the Prophet died. The Period of the Rashidun, or Rightly Guided, Caliphs lasted from 632 AD to 661 AD and saw a remarkable expansion of Islam from Persia to Spain. This was due to the phenomenon of Jihad, or Holy War. Fighting Holy Wars to expand Islam was not only considered ethical but was seen by all Muslims as a sacred duty as the following quotes from The Glorious Qur'an will amply attest:

> 190. Fight in the way of Allah against those who fight against you, but begin not hostilities. Lo! Allah loveth not aggressors.
>
> 191. And slay them wherever ye find them, and drive them out of the places whence they drove you out, for persecution is worse than slaughter. And fight not with them at the Inviolable Place of Worship until they first attack you there, but if they attack you (there) then slay them. Such is the reward of disbelievers.
>
> 192. But if they desist, then lo! Allah is Forgiving, Merciful.
>
> 193. And fight them until persecution is no more, and religion is for Allah. But if they desist, then let there be no hostility except against wrongdoers. [2]

As early as 632 AD the seeds of a great schism with the Umma, or Community of Believers, occurred. The vast majority of Muslims felt that the successor to Muhammad, the Khalif (usually spelled "Caliph" in English), who would become the new spiritual and political leader of Islam, should be elected by a consensus, ijma', of the believers. Also, to these believers, contact between God and man was to be direct and personal. These became known as the Sunnis, or Orthodox Muslims. A minority of Muslims felt that the successor should be a blood relative of Muhammad through the Prophet's son-in-law 'Ali and his wife Fatima, the Prophet's daughter. These became known as Shi'ites, or Partisans of 'Ali. Later progeny of 'Ali came to be known as Imams who provided a spiritual bridge between man and God. Today, most of the Islamic world, which numbers between 700 and 800 million adherents, are Sunni. Only in Iran is the majority Shi'ite, 93%, compared to 5% Sunni. [3] 'Ali and his son Husayn were assassinated by their political opponents. Their martyrdoms have caused the Shi'ites to remember such massacres during the holy period of when they mutilate their heads with knives and beat their backs with chains.

From 661 to 750 AD the Umayyad Empire was centered in Damascus and the Arabian conquerors intermarried and converted Persians, Syrians, Copts, and Berbers. At the same time, the philosophy, mathematics, and science of the time were assimilated. Most of the Shi'ites were located in what is now Iraq and Iran. "Many of the heterodoxies which arose in the first century of Islam and were themselves a veiled protest against the victorious religion of the Arabians" gradually gravitated to Shi'itism. Hence, the Ismailis, the Qarmatians, the Druze, the Nusayris were all Shi'ite offshoots. [4] The Umayyads reached the greatest peak of their civilization during the reigns of the Caliph, 'Abd al-Malik (685-705 AD) and his son Al-Walid I (705-715 AD), and are perhaps best personified by the beautiful Dome of the Rock Mosque in Jerusalem and the Ummayyad Mosque in Damascus. [5]

From 750 to 1258 AD the capital of the Muslim world shifted from Damascus to Baghdad under the 'Abbasid Empire. The first 'Abbasid Caliph Abul 'Abbas (750-754 AD) referred to himself as as-saffah, the bloodshedder, and the executioner's carpet became a necessary adjunct to the throne. The 'Abbasid Empire was more international than the Umayyad Empire and was a Shi'ite-dominated institution, unlike that of the Umayyads who were Sunni. [6] The 'Abbasids were characterized by magnificent achievements in literature, art, architecture, science, medicine, mathematics, and philosophy. This empire reached its zenith in the period of Harun ar-Rashid (786-809 AD) and his son Al-Ma'mun (809-833 AD). The 'Abbasids did not fall from power until Baghdad was sacked and burned by the Mongol hordes in 1258 AD. [7] The fall of the 'Abbasids did not mean the disappearance of Islam. The Mongols and the Ottoman Turks were also converted to Islam. In fact, by the middle of the 15th century the Islamic world stretched from Spain in the west across North Africa and the Middle East, northward to Vienna, Austria, and Russia, and eastward to China, Indonesia, Malaysia, and the Phillipines.

It is against this historical background that the Shah of Iran fell in 1979 and a new Islamic revival and state under the leadership of the Ayatollah Ruholla Khomeini came into existence. The Ayatollah Khomeini, whose thinking is more appropriate to the 7th century, has become the popular 20th-century spokesman for the Shi'ite world of Islam today. Although he is proclaimed as the Imam in Iran, not all Shi'ites follow his lead; but his rejection of the West and his virulent anti-Americanism, anti-Zionism, and anti-Communism have struck a responsive chord in millions of Muslims, Sunni and Shi'ite.

What are the objectives of the new Islamic revolution?

[] The elimination of undesirable or immoral behavior such as gambling, alcohol, sexual promiscuity, prostitution, pornography, and corruption;

[] The conformity of secular law with Islamic law; and

[] The establishment of Islamic governments. [8]

One reason Islamic society did not accept Western values is that there has never been a clear separation of the powers of church and state in Islam comparable to that in the West. Muhammad and his successors were spiritual as well as political leaders. This, in part, explains why the Shah's push for secularization and modernization was rejected by the Iranian

DOCID: 4009888

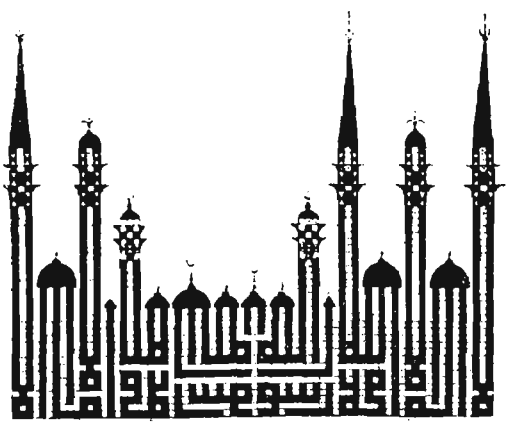
people. It is also one reason, in addition to atheism, why Soviet-style Communism has not taken hold in the Muslim Middle East.

Another reason for rejecting modernization is that although Islamic societies admire technology, political and military power, and scientific achievement, many Muslims feel humiliated and inadequate in the face of an economically superior West. [9] This attitude has persisted to some degree in the Islamic world ever since the Napoleonic invasion of Egypt in 1798. The military superiority of Israel and the humiliating defeats of the Arabs in 1948, 1956, and 1967 added further aggravation. Additionally, Jewish nationalism and Arab nationalism have been at loggerheads with each other, especially since 1948. Some two million Palestinian refugees continue to evoke great sympathy for the Palestinian national cause. The Muslims see the Israelis in Palestine, as "intruders" (like the Crusaders several centuries earlier) who must be removed, especially from the control of Jerusalem, which is also a Holy City for Islam.

The 1973 Arab-Israeli War did something for the Arab psyche that eventually led to the Camp David accords between Egypt and Israel. The Arab Oil Embargo and the battlefield performance of the Arab forces finally restored a portion of the pride that had been lost in previous conflicts. The war demonstrated that the Arabs were capable of planning, coordinating, and executing an effective military action. [10]

Muslims conveniently divide the world into two halves: Dar ul-Islam, the sphere of Islam, and Dar ul-harb, the sphere of war. The extremist Muslim seeks to convert the entire world to the Dar ul-Islam. The means to achieve this objective can be peaceful persuasion or violent Holy War (Jihad). It is significant that Iran, a state which has declared Jihad against Israel and the United States, has only one political party, the Party of God (Hizbollah). Incidentally, this is the name of the so-called "terrorist group" thought responsible for killing 241 American and numerous French soldiers on 23 October 1983 when suicide missions used vehicle bombs to attack the American and French Headquarters in Beirut. This attack repeated the pattern of the 18 April 1983 attack on the US Embassy in Beirut. In my opinion, the appeal of the name Hizbollah is more universal than the press has yet realized and in reality is an appeal to all Muslims anywhere in the world. Later, the Israeli Headquarters in Southern Lebanon was attacked. The Palestine Liberation Organization claimed credit for that attack. Also, on 12 December 1983, another so-called "terrorist group" called al-jihad al-Islami, The Islamic Holy War, attacked the American Embassy and other targets in Kuwait. The ten attackers were later identified as three Lebanese and seven Iraqi Shi'ite Muslims. Again, in my opinion, the appeal of the name of the group is international and pan-Islamic in intent, and its aim is to widen the conflict. These events followed other recent violence against the West or pro-Western governments in the Middle East since the Ayatollah Khomeini has come to power in Iran. For example, we can all recall that 52 Americans were held hostage for almost a year from 1979-1980. Iran and Iraq have been at war for over four years now, with no end in sight. In 1979 the Great Mosque at Mecca was attacked by Islamic extremists, and in 1981 an extremist coup was attempted in Egypt and Bahrain, and President Anwar Sadat of Egypt was assassinated.

Terrorism is not new to the Middle East, and it is certainly not new to Islam. The very term assassin is a corruption of the Arabic plural Hashishiyeen, users of hashish, as an Ismaili Shi'ite sect of Alamut, Persia, was known. These assassins struck terror in the hearts of the world's leaders during the 11th century. The French learned about Islamic terror in Algeria and were finally forced to leave after the endless cycles of violence, bombings, and retaliatory actions made Algerian independence a reality in 1962. Foreign military forces were not welcome in the Islamic world at that time, and they are not welcome now.



Drawing of the cupolas and minarets of Mecca with the Moslem creed in Cufic alphabet

DOCID: 4009888

Recent press reports disclosed that on 10 December 1983, 1,000 suicide bombers were being trained in Lebanon, apparently by Iranians, to launch new terrorist attacks, possibly worldwide. [11] Fortunately for us, Khomeini is a Shi'ite Muslim so his appeal is somewhat limited by the centuries of conflict between Shi'ites and Sunnis, but his appeals are not confined to Shi'ites alone, as is clearly reflected in the following quotation:

> "In many respects Khomeini's ideas are extremely progressive. In his book Islamic Government he discusses subjects such as imperialism, exploitation, and the influence of America in very modern terms, while he introduces the book with an appropriate verse from the Koran: 'If kings enter a village, they will despoil it, loot it, and turn its honourable inhabitants into slaves.' In this book, as elsewhere, he emphasizes his main themes--hostility to the United States, which he regards as Iran's arch-enemy, and hatred for Zionism and Israel. One of his fetwas (legal opinions) was that it was right that some of the money due to the Imam should go to the Palestinians; this of course pleased the Arabs.
>
> "It was characteristic of Khomeini, and one of the reasons for the growth of his reputation, that his interests extended far beyond the confines of Iran; he was never parochial. He tried to address people not just as a Shi'a ayatollah, not just as a Persian, but as a Moslem leader who could speak with authority to all Moslems. Islam, he said, made a man free in all that he does--in his person, in his reputation, in his work; in where he lives and what he eats, provided that he does nothing that is contrary to Islamic law, to the Sharia." [12]

Prior to 1979 Khomeini's forces would welcome being killed. During his fight against the Shah, Khomeini offered the following philosophical advice to his adherents:

> "'Do not attack the army in its breast, but in its heart' was his message. 'You must appeal to the soldiers' hearts even if they fire on you and kill you. Let them kill five thousand, ten thousand, twenty thousand--they are our brothers and we will welcome them. We will prove that blood is more powerful than the sword.'" [13]

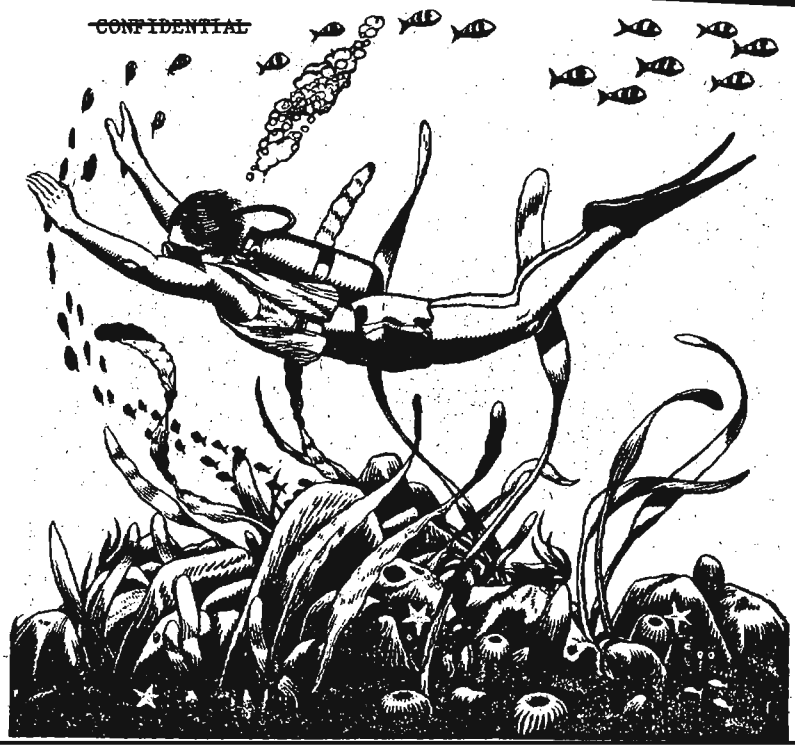
When dealing with such religious fanatics, we should remember that they will welcome death as an instant path to eternal paradise and martyrdom. Khomeini's own son, Mustapha, was killed by an act of terror by the Shah's secret police, SAVAK, so why should Khomeini avoid such means against his perceived enemies? It's clear that, with such a philosophy, terrorist acts could widen significantly. After all, why should the number of suicide terrorists be limited to only 1,000? Why not 10,000, or 100,000, or even a million? It would appear that a new approach to the complex problems of the Middle East is in order. The injustice of the Palestinian issue must be faced. Israel and Syria must play key roles in the peace process. Israelis have learned that violence for violence has not stopped more violence. Most Muslims are not terrorists or extremists, but I think the forces of extremism worldwide could become an "Islamic time bomb" caused by actions that unnecessarily provoke undecided Muslims to actions that they would otherwise abhor. In such a situation, Islamic states that are currently pro-West or neutral may be overthrown or forced into the extremist camp. Recent comments by Iran's Ambassador to the United Nations indicated that Iran does not feel responsible for whatever happens. If terrorism expands, even to the territory of the United States, it is Allah's will. Iran is not to blame. People are simply reacting to the "Imperialistic" policies of the United States. Need I say more?

Footnotes

1. Lewis, Bernard, "The Return of Islam," Religion and Politics in the Middle East; Boulder, Colorado, 1982. p.9.
2. Pickthall, Muhammad Marmaduke, The Glorious Qur'an; New York, New York: Muslim World League, 1977. p. 29.
3. The World Factbook, CIA Document No. CR83-11300, 1983; p. 104.
4. Hitti, Philip K., History of the Arabs; New York, New York: Macmillan, 1967. pp. 240-249.
5. Ibid. pp. 263-265
6. Ibid. pp. 288-289
7. Ibid. pp. 288-298
8. Curtis, Michael, Religion and Politics in the Middle East; Boulder, Colorado, 1982. p. 3.
9. Ibid. p. 3.
10. Stookey, Robert W, America and the Arab States; New York, New York: John Wiley & Son, 1975. p. 246.
11. "Reagan Says 1,000 Readied as Mideast Suicide Bombers," The Washington Post, December 10, 1983, pp. A1, A14 Col 1.
12. Heikal, Mohammed, Iran, the Untold Story; New York, New York: Pantheon Books, 1982. p. 139.
13. Ibid. pp. 145-146

DOCID: 4009888

OUT OF MY DEPTH (U)



EO 1.4.(c)
P.L. 86-36

DOCID: 4009888

Correspondence

To: Cryptolog

~~(S-CCO)~~ In his article, "Tips on Topical Reporting (U)" in the October 1983 edition of Cryptolog, [redacted] states that "the National SIGINT Requirements Lists (NSRL) are only general guides to themes of continuing interest" to analysts. He also states that, while analysts should become familiar with requirements, they should not regard the requirements as "crucial" in deciding what topics are reportable. He goes on to say that anything in a "military context" is covered by a requirement.

(U) I submit that the words "guides" or "guidance" and "requirement" have quite different meanings. "Guidance," according to Webster, is "the act or process of guiding" and a requirement is "something wanted or needed--a necessity."

~~(S-CCO)~~ The requirements in the NSRL are intended to be expressions of the needs of our customers. Guidance went out with the demise of the IGCP. NSA has agreed to use the requirements to direct its collection, processing, analysis and reporting efforts. Also, the requirements are statements of specific needs and not just "themes."

~~(S-CCO)~~ The priorities associated with line items in requirements are assigned after careful deliberation by the SIGINT Requirements and Validation Subcommittee (SIRVES) of the SIGINT committee. NSA uses them as a basis for assigning the Agency's limited resources. SIRVES ensures that NSA abides by the priorities by conducting evaluations of NSA reporting.

[redacted]

~~(S-CCO)~~ I recommend that [redacted] read the Handbook for the National SIGINT Requirements System.

[redacted] replies:

~~(S-CCO)~~ [redacted] criticism of my points about the National SIGINT Requirements Lists (NSRLs) reflects his more detailed knowledge of the process than mine. At his invitation, I have read the Handbook for the National SIGINT Requirements System, a publication not widely distributed--and rightly so, I believe--to working-level analysts at NSA. (Its technical details need to be known intimately on a day-to-day basis by specialists in NSRL development and implementation.) I also appreciate the time and care that goes into formulating the NSRLs and assigning priorities to the line items in them. In the spirit of fostering better understanding of our SIGINT world, I suggest that [redacted] expand on his letter and develop a full Cryptolog article on the National SIGINT Requirements System.

~~(S-CCO)~~ A few comments from [redacted] invite specific rebuttal. Having been in this business for a long time now (in collection, processing, and analysis), I know what a SIGINT user needs--or requires--is not necessarily what NSA can provide in great detail. In this intelligence business, we target our resources, then take what we can get, sometimes in huge quantities but often in quite meager amounts. So, what a user requires serves toguide us in our search for good information. But we are not held responsible for producing required data if it is just plain unobtainable or acquired in an unusable form ..., nor are we exempted from using good judgment in interpreting the urgency of the requirements we are tasked to fulfill.

~~(S-CCO)~~ I disagree that the word "specific" is applicable to most of the National SIGINT Requirements. Some items are quite to the point, but the large majority are couched in such terms as "systems studies," "data base," or threat analysis information." That gives a lot of leeway for subtopics that are not spelled out.

~~(S-CCO)~~ [redacted] missed an important point in my article said "almost anything ... in a military context is covered by at least one requirement." Also implied--but I thought it unimportant to spell out--was that this statement applied to a military force regularly targeted by SIGINT resources. I seriously doubt that most readers of the Article would get excited about the order of battle of a [redacted] unless the area, [redacted] became the focus of a crisis. If that were the case, the other advice in my article would be pertinent.

[redacted]

P051 3803s

DOCID: 4009888

P.L. 86-36

NON POSSE vs. POSSE NON

BY

[redacted] PIG

When Saint Augustine back in the fifth century wrote in his City of God about the differences between angels and human beings, he never realized that he was laying the groundwork for a QRL article in the 20th century. But a distinction that he pointed out was related to a grammatical point that gave a lot of NSA linguists trouble on a Spanish Professionalization Qualification Examination, so this article is being written. The purpose is not to point the finger of scorn at those who made the error, but rather to point out the distinction in the hope that linguists who have not yet made the mistake will have the information to avoid making it.

Augustine said that angels NON POSSUNT PECCARE while humans POSSUNT NON PECCARE. A novice translator might translate both expressions as "cannot sin" and thereby miss the point entirely. Even writing "angels cannot sin" and "humans can not sin" would escape the average reader. It is necessary to use circuitous phrases such as "angels are incapable of sinning" or "it is impossible for angels to sin" and "men have the ability to avoid sinning" or "can refrain from sinning." The idea is that while an angel couldn't sin if he wanted (and probably wouldn't want to anyway), homo sapiens is a sin-inclined creature who has it in his power to "not sin" if he tries. The linguistic distinction depends on whether the negative NON refers to being able (POSSUNT) or to sinning (PECCARE).

Reprinted from QRL, The Quarterly Review for Linguists, November 1972.

The same distinction can be made in a number of other languages, including Spanish. It was the crux of a sentence in PQE #2, given in February 1969. In a selection entitled AGRESIÓN, there were two paragraphs about "the starting of armed struggle," "offensive action of a country which attacks the territorial integrity of another," and "a declaration of war," and then this sentence:

> La agresión internacional puede no revestir la forma de operaciones bélicas, sino traducirse en presión de otra indole (bloqueo, amenazas, campana difamatoria y provocativa, etc.) que obligue por seguridad o dignidad a reaccionar armadamente al agraviado en sus intereses o en sus derechos.

This states that, in contrast to the "offensive action" and other hostilities described in the preceding paragraphs, "Aggression between nations does not have to take the form of (PUEDE NO REVESTIR) warlike acts, but can be expressed by other types of pressure (a blockade, threats, a campaign of smears and threats, etc.), obligating the aggrieved party to react with arms in its own interests or for its own rights."

Many people translated PUEDE NO REVESTIR as if it had been NO PUEDE REVESTIR. There were test papers that said "international aggression cannot be in the form of ..." or "cannot assume the appearance of ...", etc. Maybe in their own minds, the translators were making the distinction outlined above, but it didn't show through to the readers (i.e., the graders). The simple translation of PODER NO as "cannot" or "can not" did not suffice. As I recall, one person did say, "... can take the form not of ... but can be ...." This was acceptable and, incidentally, took advantage of a linguistic clue: the infinitive TRADUCIRSE later in the sentence, which needs some reason for being there in the infinitive form. It is a complement to PUEDE ("can") and might cause a careful translator to take another close look at PUEDE and its immediate complement (REVESTIR, actually NO REVESTIR) and possibly reevaluate the meaning of the whole clause.

This reenforces a point I've been trying to make to translators over the years: ALL PARTS OF A TEXT ARE RELATED! Words don't stand by themselves; they're usually in sentences with other words. Sentences don't stand alone; they're usually in paragraphs with other sentences. Even paragraphs don't stand alone; they're quite often just a part of a longer text, and it is this whole text that should be thought of as the thing to be translated, not just the individual words in it. [1] A good translator tries to make sure that all the pieces hang together in a finished translation. If two or three paragraphs say one thing, the next paragraph shouldn't say just the opposite.

Machines may have to translate word for word, but humans are capable of thinking and reasoning. If you consider word-for-word translation to be a sin, we might say that human translators POSSUNT NON PECCARE.

NOTE

1. Another error in the same selection of the same PQE is related in meaning to the PODER NO mistake, but is also attributable to "word-for-word" translation. Switching from the international to the personal sphere, the text points out that aggression

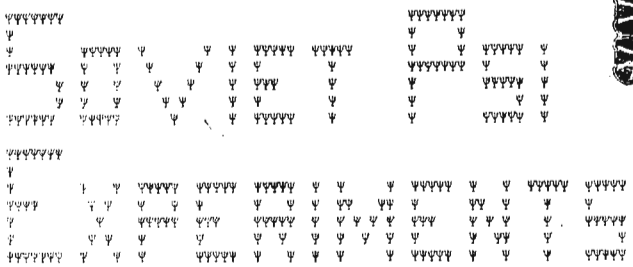
> ... existe en el acometimiento o acto de fuerza y también en el propósito evidente de realizar aquél o de recurrir a ésta; por ejemplo hay agresión tanto en el disparo como en el hecho de buscar y sacar una arma de la funda o del bolsillo.
>
> (There is aggression in an assault or an act of force, as well as in the clear intent to carry out an assault or have recourse to an act of force; for example, there is aggression both in firing a gun and in looking for a weapon and taking it out of a holster or pocket.)

While this sentence should have cast some light on the PUEDE NO REVESTIR passage (or vice versa), it didn't help very many of those taking the test. Of course, besides failing to recognize the similarity of the underlying thought, several testees forgot about TANTO ... COMO meaning "both (this) ... and (that)" so they translated individual words. Since TANTO means "so much, as much" and COMO is often "as," they rendered the part after the semicolon as "for example, there is as much aggression in a shot as in the act of looking for and taking a weapon out of its sheath or pocket."

In addition to the fact that this translation disregards Spanish grammar—it doesn't say "hay tanta agresión ..." --it just doesn't make sense and should have made the translator sit up and take notice just because it was so patently illogical. As [redacted] (the Chairman of the PQE Committee) pointed out, "There is not as much aggression in shooting someone as there is in waving a gun at him There's a whole lot more!"

P.L. 86-36

LOOKING AROUND with



P.L. 86-36

(U) Recent Soviet experiments in remote viewing and animal telepathy have produced some significant, well-controlled results. This work was described at the Seminar on Applied Anomalous Phenomena, in the Xerox center at Leesburg, on 1 December 1983 by Doctor Russell Targ, who had just returned from Russia where he visited several Soviet Psi facilities.

(U) The Soviet scientific community is rather hesitant about Psi research, (telepathy, clairvoyance, poltergeists, etc.), but a theory of low-frequency radio propagation has been devised to justify some telepathy phenomena, and the Soviet Academy of Sciences (SAS) has established a separate department to deal with this work. The "Department for Research on Theoretical Problems" is headed by Professor Andrianka, who is an Academician and who is the only member of this unusual department.

(U) Much of the unclassified Soviet work takes place in hospitals around Moscow and is concerned with measurement of subtle physiological changes, particularly in GSR (galvanic skin response), that would correlate with response to some stimulus, including the onset of hypnosis.

(U) There are apparently problems of image and semantics, for the research center in the hospital is called the "Center for the Non-Drug Treatment of Mental Problems," while the Academy of Sciences calls it the "Department for Special Problems." There are also doctrinal problems, for a Soviet scientist named Kagan published a definitive book on information theory in which he explained Psi phenomena in terms of low-frequency radio propagation. Psi experiments in Russia, the US, and elsewhere which appear to show precognition do not fit this radio model and produce curious reactions by the Soviet scientific community, as noted below.

(U) The concentration of the Psi research in hospitals is also based on this radio model, for the Soviet medical researchers have been doing a lot of work in treating cancer patients and others with low-frequency radio waves (in the 10-Hz to 100-Hz range) and have discovered that during this treatment the patients have mystical experiences, relax, and some appear to experience cures. The experiments are conducted without any specific theory. Targ found that this resulted in a lot of hospital visits in the Moscow area, to see the ELF (extremely low frequency) equipment and hear about the experiments.

(U) Dr. Targ, the visiting scientist, had worked in various areas of hard science, including lasers and wave physics, for GTE before moving to SRI in the early 1960s to pursue a NASA-funded project for an ESP teaching machine. Since then he has worked on a number of Psi projects at SRI and recently formed a company to do applied Psi work. His emphasis has been on controlled experiments in remote viewing and precognition.

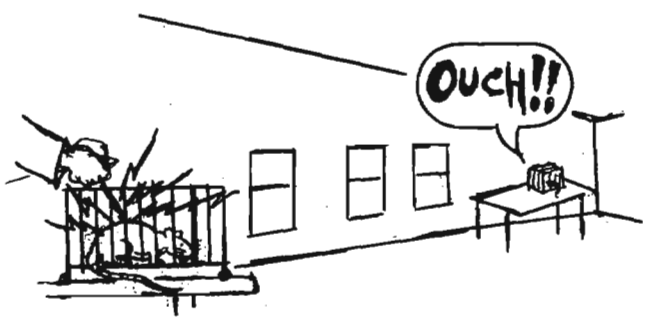
(U) At the August 1983 meeting of the International Society on Psychic Research, a Soviet theoretical physicist, Guberev, suggested he come to Moscow as a tourist to see the Soviet work. Targ, who had worked on Defense contracts, refused to go to Russia as a tourist, fearing that the Soviet authorities might detain him, but said that he would be happy to go as an officially invited guest of

the Soviet Academy of Sciences (so that the Soviet authorities could not misconstrue the purpose of his visit). The official invitation arrived two days after the KAL 007 shootdown. Targ decided to accept the invitation, he said, because he felt the KAL incident was a result of a refusal to communicate (viz., neither the Japanese nor Soviet air controllers would notify each other of the divergence from the flight path), and he thought his visit would help to counteract the deterioration of US-USSR scientific communications. He took his daughter, who is fluent in Russian, as a translator. At the end of September Targ, his daughter, and a colleague arrived in Russia via Interflug. (The other airlines had suspended service to Russia.)

(U) Targ was careful to preface his exposition with the caveat that he could report only what the Russians had told him of their work. He did not see any experiments conducted and, although he had known Guberev for about ten years, he could not prove that all the results reported to him were not intentional disinformation.

(U) His impressions were that the Russians had a number of smart people, such as Guberev, doing good controlled experiments on remote viewing. A 1976 IEEE paper by Targ on remote viewing had been translated into Russian, as had the 1982 paper on Psi phenomena by Dr. Robert Jahn, Dean of Engineering at Princeton, which was published in the prestigious IEEE Proceedings and soon translated. In general, Targ found, the Russians were up-to-date with US work in this field.

(U) Psi work is regarded seriously at high levels in the Soviet scientific (and defense circles, Targ found, because the scientists had to clear their work with the Soviet military authorities before disclosing it or letting him into their labs. Targ found that there were closed facilities, unambigously presented to Targ as not permitted for him to visit.



(U) Most of the experiments are done in or near major hospitals in Moscow. One large experiment in "rat telepathy" was disclosed to Targ. Rats raised together were separated into two groups. They were shock-conditioned separately, in standard Pavlovian fashion, by being shown a light, followed soon afterwards by an electric shock. The rats learned that the light was associated with the shock and would manifest fear at the light. Then two cages were connected by a modem, at various distances. Some experiments used cages more than a kilometer apart. A computer would call up one of the cages and shock one of a pair of rats. Apparatus measured the galvanic fear reaction of the unshocked rat when the warning light was turned on in the other one's cage.

(U) A large computer in the hospital was used to process the galvanic response data. Fast Fourier Transforms (FFTs and autocorrelation were used to detect changes in the GSR (galvanic skin response) in response to some stimulus. Targ said that the computer looked like a PDP.

(U) The signal-to-noise ratio of the GSR data in the rat experiment was clear and the analysis was considered (by the Russians apparently) as a trivial application of a mathematical algorithm. The experimenter was apparently Guberev, whom Targ has known for a decade. Targ could not vouch for the experimental data. The experimenter wanted to use computer analysis of GSR data to find the exact instant that a subject drops into a hypnotic trance. This is somewhat controversial, because it is apparently widely believed in the US that there are no known physiological correlates to the hypnotized state, i.e. no measurable difference. Guberev claims that there are unambiguous GSR changes at the crossover point.

(U) GSR changes are also monitored in medical experiments which use 10-Hz to 100-Hz radiation to treat various illnesses. Because of translation problems, the Russian descriptions of the experiments were incoherent to Targ (his daughter translated), however cancer treatment was one of the ELF applications. Targ said that different stochastic modulations, including high-frequency noise, were impressed on the ELF carriers.

(U) Their Soviet host, Barazin, took them on a tour of "the Department for Research on Special Problems." Targ thought this was the Soviet analog of the US phrase "anomalous problems" that masks Psi experiments with an ambiguous, scientific-sounding name.

(U) Targ and his party presented the SRI work in remote viewing to two kinds of audiences:

[] medical people and psychologists, and

[] physical scientists.

The standard format was for Targ to give his talk in English, after which his daughter would give the same material in Russian. The medical people had good questions on experimental technique; e.g., the signal-to-noise ratio of the data, the mental processing, how the remote viewers felt during the viewing experiments, etc. Targ felt that they had all read the relevant US papers. But the physicists were another matter.

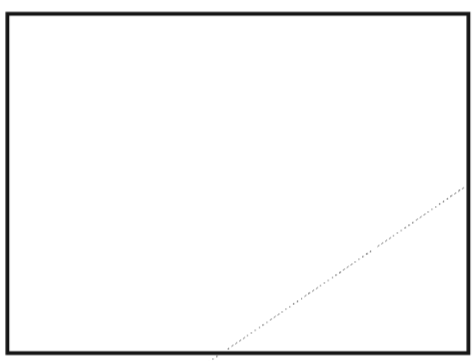
(U) When Targ's daughter began to present the Russian-language version of the SRI work to the audience of physicists, all went smoothly until she reached the part about precognition, at which point there was an uproar. She could scarcely finish a sentence. For two hours the physicists interrogated her mercilessly, demanding an explanation of how the Psi subjects did the precognition; i.e., a physical theory that would account for the phenomena. Because Kagan's book on information theory explained Psi phenomena as ELF radio, the SRI precognition results conflicted with this (approved) theory. The Soviet physicists refused to hear any data until Targ could provide them with a theory which they could accept, one that provided a model for precognition.

(U) The Targ party visited Yuri Guliyayev, an Electrical Engineer who is the director of "the Soviet version of the IEEE" (probably the Popov Society). There was noticeable antagonism between the Academy of Science people and the electrical engineering society. His SAS host drove him to the door of Guliyayev's institute but would not enter. Yuri Guliyayev wanted to know who Andrianka was, looked him up in a directory, and announced to Targ that he was an Academician and that his Department in the Academy had only one member.

(U) Guliyayev knew all about US Psi work, including Psi experiments on US submarines. Targ found that the Russians seemed to know everything that was going on in the US, (apparently even unpublished work) but wanted to talk about what the Russians were doing. Yuri Guliyayev is doing tests in bioradiation, repeating what Vasiliev did, to see all the RF, IR, and other electromagnetic energy coming out of people's bodies, and to correlate this with different physical states. Yuri kept saying that he was doing physics, not ESP. But Targ noted that Guliyayev's work is almost the same as what "aura readers" are doing in spectraphotometry. The Targ party was given a paper that rather sketchily described the Soviet work in bioradiation.

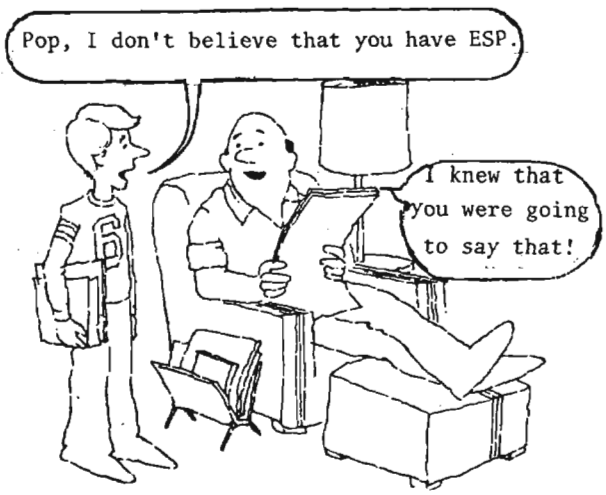
(U) There was also an experiment with a noted psychic, Nina Kalada. The Russians report that she can read a page in a book in another room, with results well above random. For example, she might be asked to read the first line of page N of a book with a certain title in a library in the next room. Her results were well above random, according to the Russians, as long as she had feedback of results, i.e., could see immediately how close she came. When she was sent out of the room during the verification and not allowed to know how well or poorly she had done, her results were no better than random. Dr. Targ felt that this meant that documents in locked in safes in the US Embassy in Moscow were safe from Ms. Kalada, since she would not get the feedback necessary to produce successful results. He said he assumed that espionage was the point of the research.

(U) One of the asides in the journey was a trip to a "free market" in Leningrad, where fresh fruit and vegetables can be purchased by approved people at black market prices in large armory-sized covered markets. Because of the shortage of fresh fruit and vegetables in Russia, only certain foreigners and Russians are allowed into these markets. Russians approached the Targ party before they went, in an effort to get them to change some money or make some purchases on their behalf. Targ, fearing he was being set up for a police trap, refused. His scientific friends then confirmed that this was a standard ploy, to implicate visiting foreigners in some illegal activity. At the food market, the police refused to allow Targ to take any photographs at all and interfered with his efforts to do so. Apparently fresh fruit is so hard to obtain that they did not want any photographic evidence that it was available at all.



EO 1.4.(c)
P.L. 86-36

DOCID: 4009888



(U) From Leningrad their Russian hosts took them on an unscheduled side trip to Yerevan, capital of Soviet Armenia. Targ, apprehensive about what might happen, resisted, saying it was not on his itinerary and he would not go to Armenia. The Russians replied that there had been a large-scale experiment in remote viewing and the Armenian scientists wanted to see Targ and his party—in Armenia. Professor Rubiky Gasumsan, of the Department of Psychology, had done experiments with graduate students. Apparently they were given no choice, and had to go to Armenia. In the remote viewing experiments, an architect picked a number of sites in the city that had distinctive features. These locations were sealed in envelopes and picked at random. Students, called "guards," were used to escort the "agent" to the site, which they only learned about by opening the envelope while on the way. The other member of the RV (remote viewing) pair sat in a lab and waited until the "agent" reached the site. Then he described what he thought the agent was looking at. (This is similar to the SRI experiments.) The Armenian scientists described work which had strikingly successful results.

(U) Targ and his party were then taken on a brief holiday, still protesting, to a remote place in the mountains of Armenia to see "the church at the end of the world." It was only when they were in the back of the Intourist bus, far away from all witnesses, that the Armenian scientists revealed what they really wanted to talk about. They had encountered precognition of targets before the "agent" reached the site to be viewed. The student in the lab, even when he was told that the agent was not yet in place, would go ahead and describe the remote site anyway.

(U) The problem for the Armenians was what to do with the data. They have trouble dealing with the data at the labs in Yerevan and in the Academy of Sciences. Targ and the Armenians had a long discussion on protocol, i.e., the form for such experiments, similar to US protocol analyses.

(U) (Obviously, they were using Targ to "publish" results that they could not publish in Russia, because they conflicted with accepted theory, and staged his visit so they could talk to him and still deny things afterwards, if there were any repercussions. Add in the potential for disinformation, and the situation has various possibilities--a commentary on being a scientist in Russia.)

(U) Summarizing, Targ said there were a lot of hospital visits to show ELF signals and apparatus which caused the subjects to have mystical experiences, and so on.

(U) In reply to a question, Targ said he had made informal agreements to do long-distance remote viewing experiments between the USSR and the US, providing the "communications" between the US and Soviet scientific parties were good enough. He has not started this work because of communication problems.

(U) What the secret Soviet work in Psi applications might be was neither known nor hinted at in Targ's exposition.

(U) Apparently there were no live demonstrations of anything for the Targ party and no detailed papers that they could take out.

(U) Other papers at the SAAP meeting covered a lot of US work in sensing objects underground, or at some distance, and also covered criminological applications to get clues to serious crimes. The Chinese had also reported experiments in seeing printed materials through sealed envelopes, in which a successful "read" set off a number of field sensors and also gave a "blurred photographic impression" of the string of five Chinese characters when a success occurred. There was audience interest in using these remote sensing and underground and undersea detection techniques to find submarines and missile silos. Possibly the Russians, who seem to be abreast of US work, have similar interests.

(U) A recent Congressional Research Service (CRS) study by Christopher Dodge (83-511 SP) cited other Soviet Psi work, noting considerable Soviet interest in remote hypnotic manipulation and dowsing for water, oil, and minerals. This is referred to in Soviet literature as the "biophysical or biolocational effect." Psychokinesis (PK or Polterism, in which the mind affects physical objects) and psychic healing have also attracted Soviet interest. The Soviets claim that

scientific studies of dowsing have yielded significant results. (US researchers make the same claim.) Therefore, dowsing is taught to professional mineralogists and geologists at Tomsk Polytechnical Institute. The CRS report says there are various speculations that the USSR is spending tens of millions of dollars on Psi experiments and applications directed to military research, but this is unconfirmed. A paper, "Psi in the USSR: Applied Aspects" by L. Vilenskaya, Applied Psi Newsletter, Vol. I, no 1, 1982, pp. 4-5. Bulgaria and Czechoslovakia also conduct Psi research and applications, according to the CRS report.

P.L. 86-36

Analysis

~~(FOUO)~~ The ability to read a page of a book in another room (the Kalada experiment) would have security implications for COMSEC if it worked reliably. The Russians could, for example, use such a technique to determine whether a pinched keylist was in use [redacted]

~~(FOUO)~~ The GSR research, using FFT and autocorrelation to detect the instants at which subjects are responding to stimuli or becoming hypnotized, could be applied to electronic interrogation and debriefing techniques. One of the key factors in Psi experiments is determining when the Psi subject is reliably reporting Psi experiences, and US experimenters have been using voice tremor analysis and pupil dilation photographs to bracket valid episodes. The Russians are undoubtedly aware of this work, and if they are able to develop very good methods for determining when people are responding correctly to an interrogation, they would be able to apply it to non-Psi interviews. The rat telepathy experiments, if applied to humans, might give them ways of determining when agents are under stress, e.g., after they have been arrested. The dowsing (i.e., biolocation of specific distant objects such as ships, computers, nuclear weapons, etc.) would have obvious intelligence applications if it worked as well as conventional intelligence techniques.

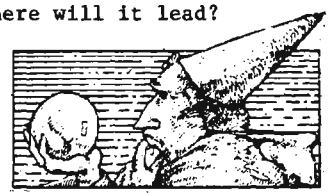
~~(C)~~ Recent US experiments, presented at Leesburg, showed that PK subjects could affect the performance of random noise generators in subtle but persistent ways. However, the observed effects would not appear to jeopardize well-designed cryptographic devices. In another reported experiment, a subject was able to guess 2,000 random dibits correctly out of a stream of 6,000 dibits, which is fairly significant statistically but not of much use in cryptanalysis. Generally, there is a problem in getting the Psi subjects to repeat their work because of emotional factors--at least in the US.

~~(C)~~ Summing up, Psi work is still very nebulous and unpredictable. There is a lot of doubt about it. In spite of this, the Russians are openly experimenting in certain areas where they apparently feel there is an acceptable theoretical base (e.g., ELF radio and biolocation), while they reject other unacceptable Psi effects. They are obviously keeping up with the work in the US and other countries. The establishment of a one-man department in the Academy of Sciences implies that the established disciplines don't want to be closely associated with Psi work, but possibly the Russians feel the experimental results are too strong to be ignored. The difficulty Russian scientists are having with precognition, for which there is no approved theory, is somewhat comical, but probably no different from the general attitude in Western science.

~~(C)~~ One of the subtle undercurrents of Targ's visit was his concern about being arrested, the arbitrary way in which the Russians made him go to Armenia (as if he had no more rights than a Soviet citizen), and his inability to get sufficiently detailed expositions of the Russian work--in a field in which he has been a leading researcher for over 20 years--to determine whether anything he was told was true or false. If he actually does some joint experiments with the Russians, the nature of the results and their interpretation should be interesting.

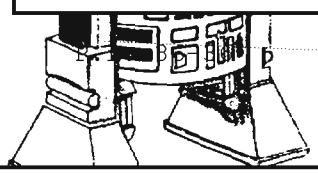
~~(C)~~ Another subtle point, noticeable because it was never mentioned, was the "human element" of Soviet Psi work. In the US, much of the current work is in trying to improve the rapport between the experimenter and his subjects, trying to find more people with Psi abilities, and then getting them to cooperate in Psi experiments. The key to success in US experiments has apparently been the emotional factors of getting the Psi subject to feel the work is important, and also for the experimenter himself to be equally committed to the importance of the work. This of course makes it difficult to repeat experiments, because the emotional charge cannot be sustained. On the basis of Targ's exposition, this matter of subject cooperation and the emotional component of the work did not come up at any point in the Soviet work.

(U) There is probably food for thought, on several levels, in this unconventional Soviet development. What are they up to? What does it mean? Where will it lead?



~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36

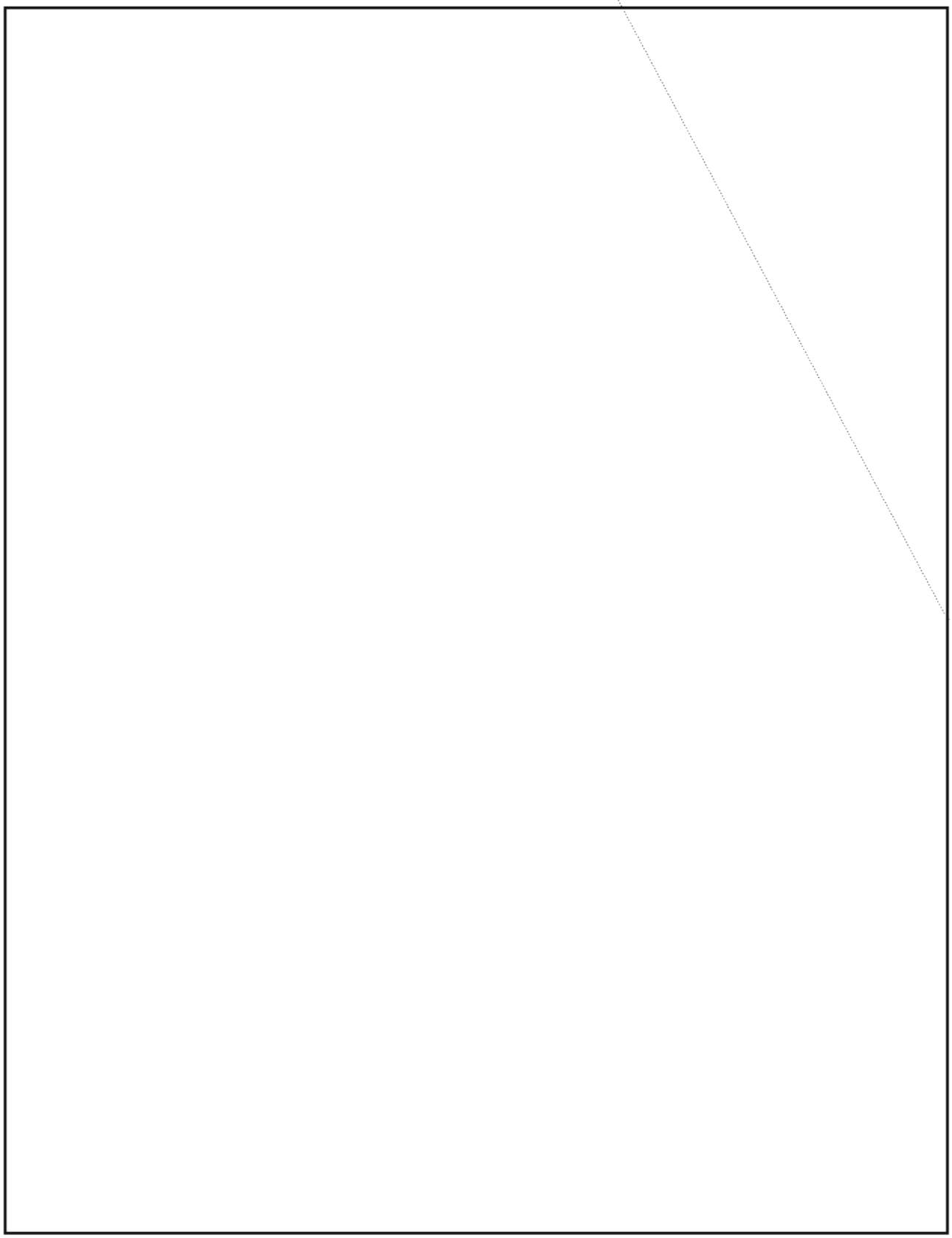


by

EO 1.4.(c)
P.L. 86-36

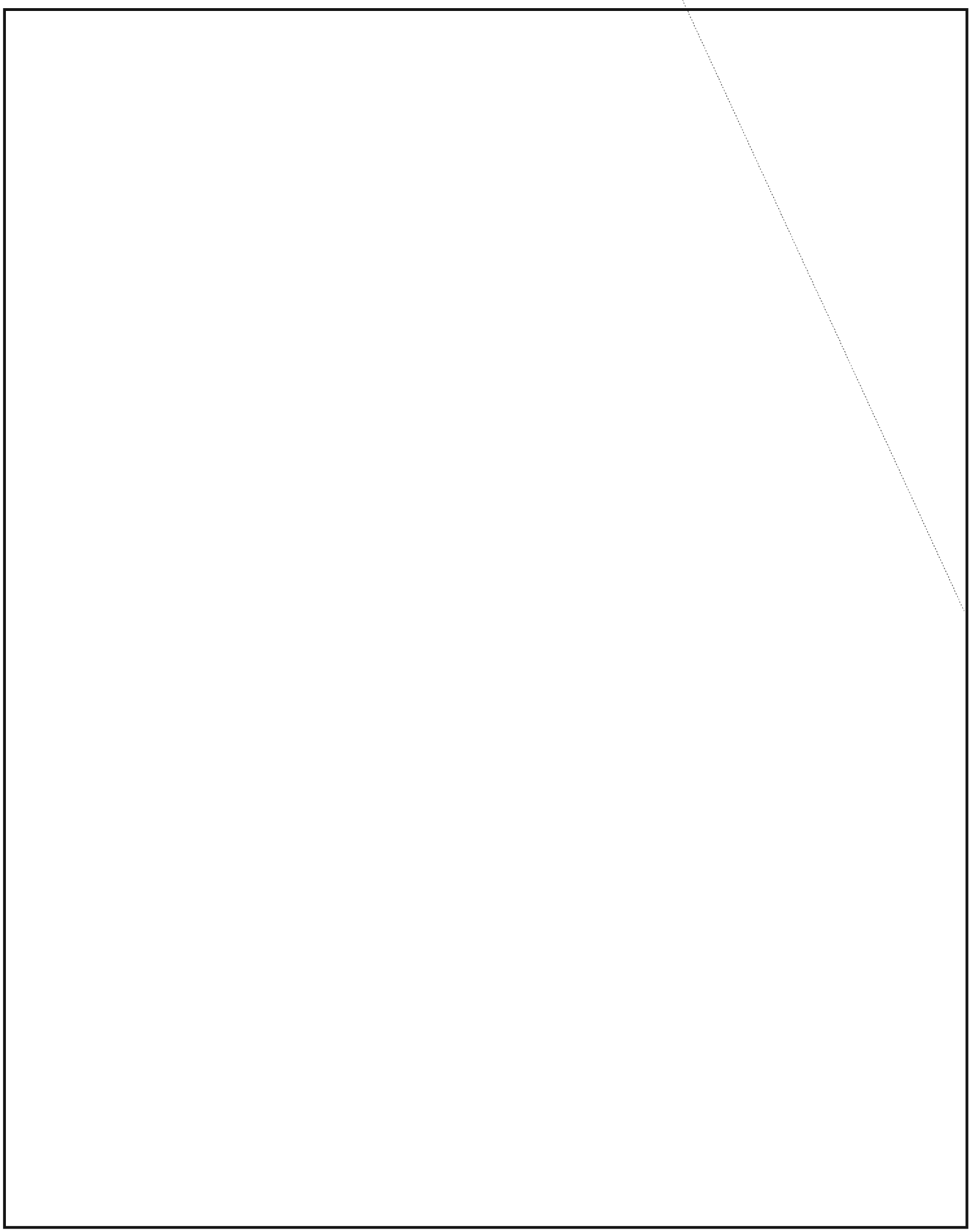
~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36



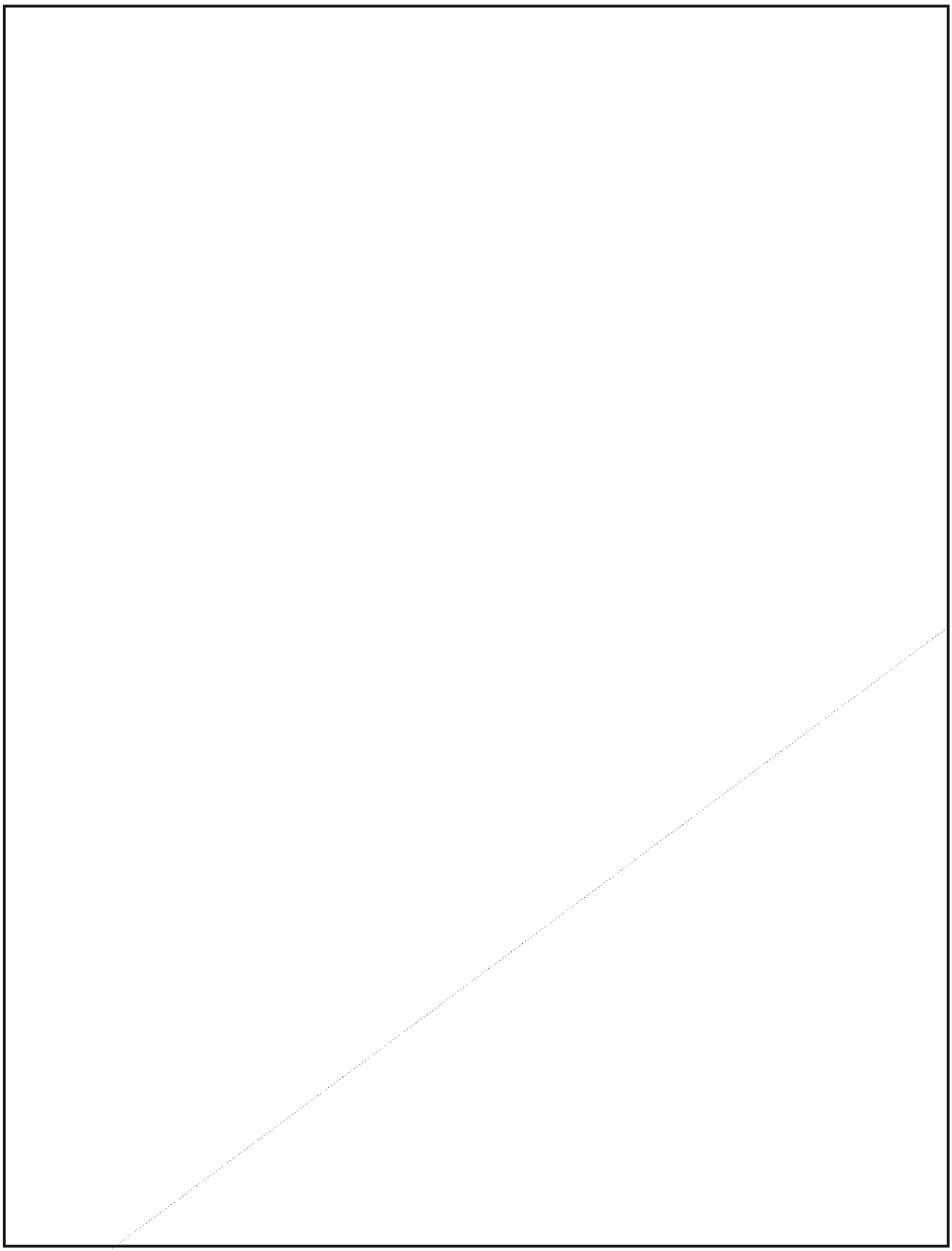
~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36

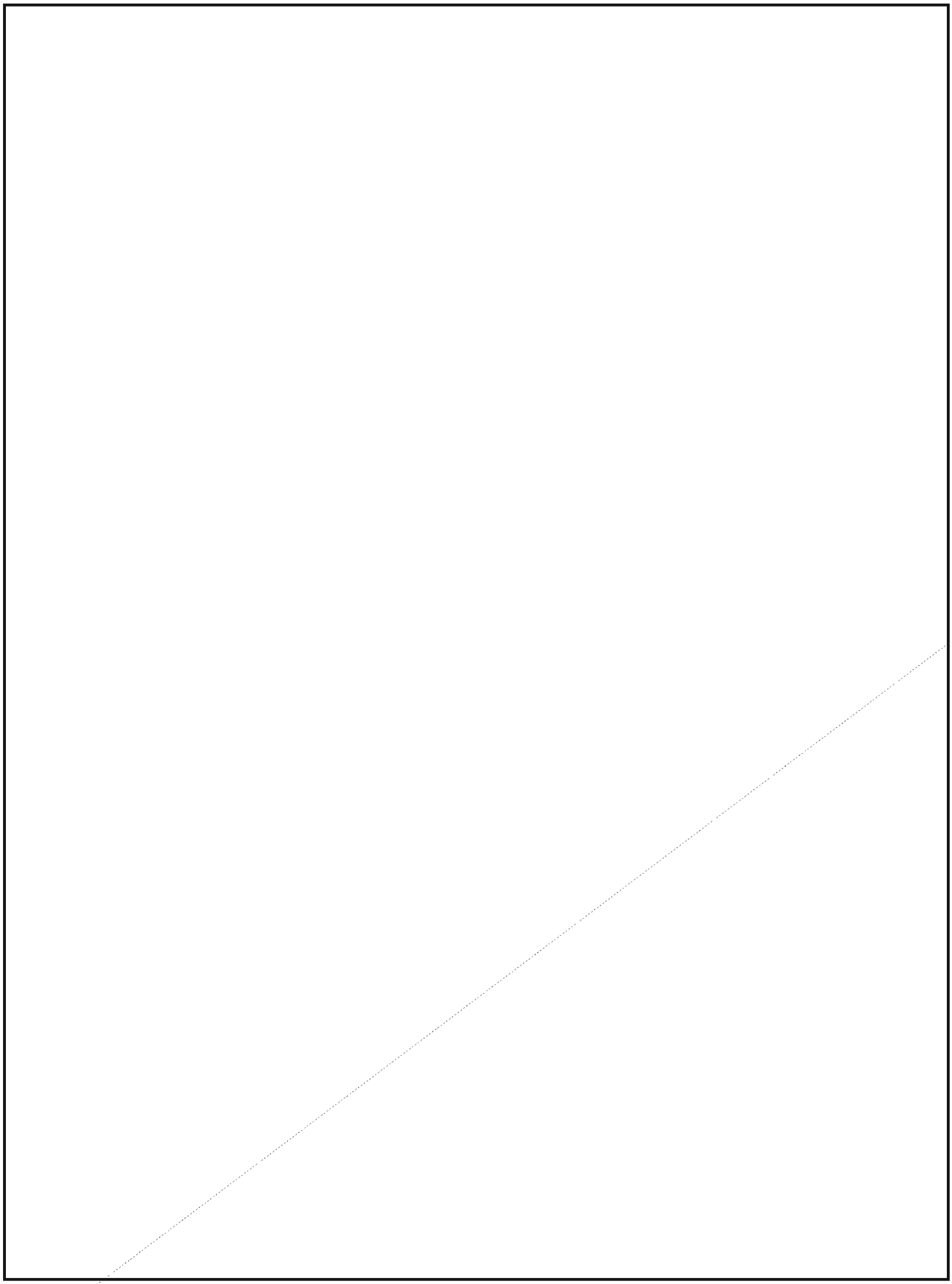


~~SECRET SPOKE~~

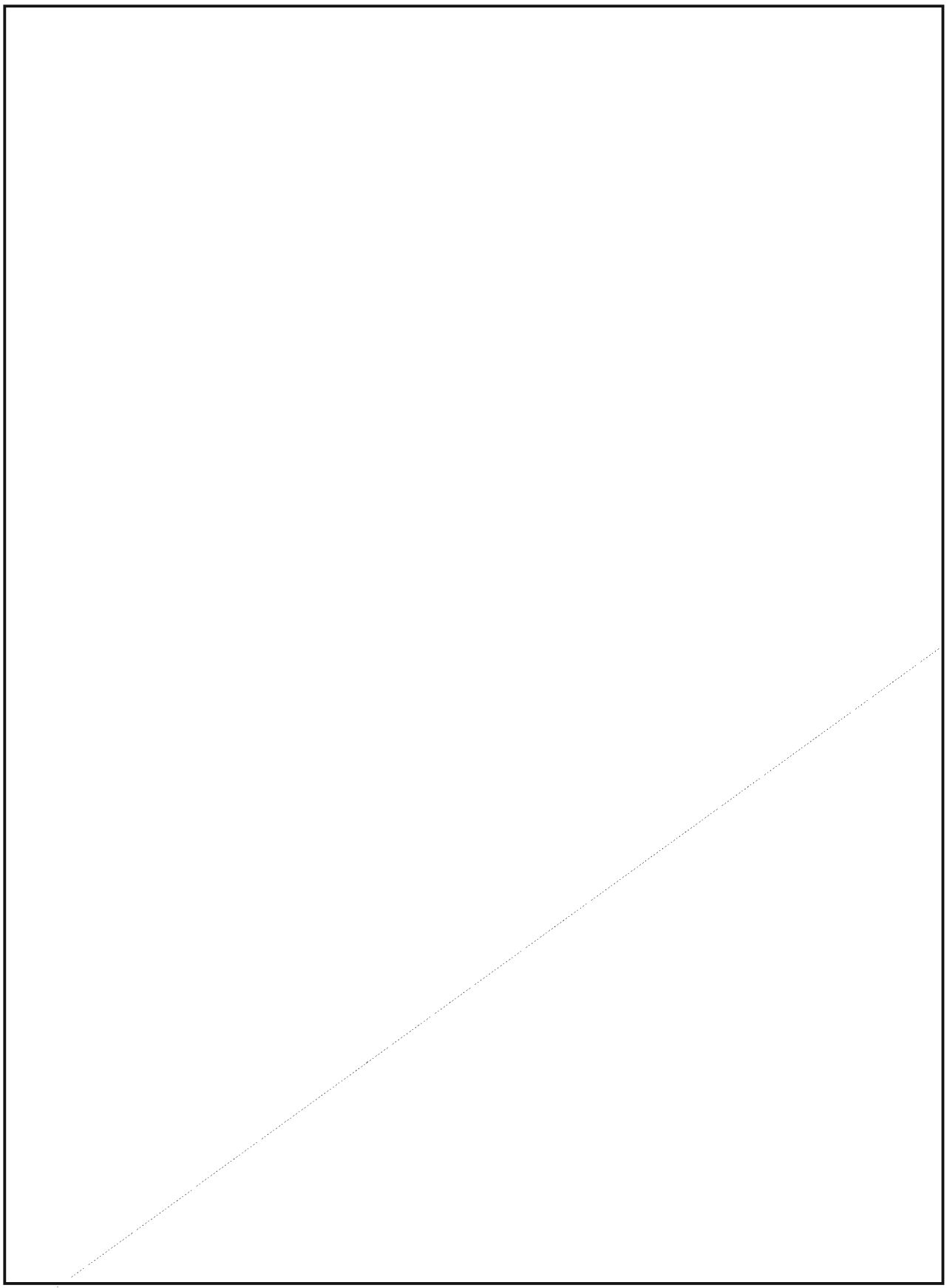
DOCID: 4009888



EO 1.4.(c)
P.L. 86-36



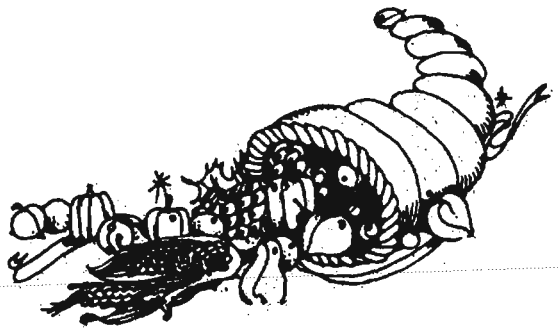
EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

SHELL GAME:

SYSTEM SHELLS (U)



by [ ]

P.L. 86-

One of the best ways to learn about shells is to look at shell files that other people are using. Some of the commands on the UNIX system (U) you are using may well be shell files. Shell files execute more slowly than compiled files, so most of the executable commands will be in binary form, the kind that does strange things to your terminal screen when you try to look at them.

(U) The UNIX command

file filename

can be used to determine (or make a pretty good guess at) whether 'filename' is a "commands" (shell) file. Prowling around the places where the system commands are stored, one can turn up a number of shell files. Some of these files are complex and require some extra effort to understand, but others are short and relatively easy to read.

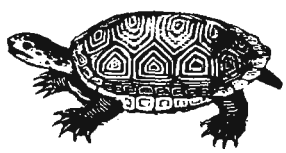
(U) We found the following files on our system, all of which are shell files. They are grouped (roughly) according to complexity. You ought to be able to find most of them (and possibly others) on your system. Have fun!

Easy

/bin/lsm
/usr/bin/mrsinputcvt
/etc/sched

Intermediate

/usr/bin/commands
/usr/bin/doc
/usr/bin/news
/usr/bin/suggest
/etc/labelof



Complex

/bin/csplit
/bin/diff3
/usr/bin/diction
/usr/bin/fixpib
/usr/bin/guidemaker
/usr/bin/help
/usr/bin/lorder
/usr/bin/man
/usr/bin/mm
/usr/bin/notate
/usr/bin/sccsdiff
/usr/bin/spell
/usr/bin/style
/usr/bin/xfer

DOCID: 4009888

P.L. 86-36

(U) The Direct Communications Link (DCL) earth station at Fort Detrick, Maryland, is the tracking and communications station of the United States for the intercontinental link which in 1978 replaced the terrestrial "Hotline" linking Washington and Moscow. (See Figure 1.) The DCL is a direct private communications link between the President of the United States and the President of the of the Soviet Union. [1]

(U) This paper covers the DCL earth station at Fort Detrick, including its link with Moscow and Washington. The Intelsat system of the United States, whose earth station is located at Etam, West Virginia, is covered only as necessary to understand the entire concept.

I. WHAT WAS AVAILABLE BEFORE THE DCL?

(U) Prior to 1963 the United States and Soviet Union had no real-time communications with one another. The original Hotline was first proposed in 1960 by Jess Gorkin, the editor of Parade magazine. Because of the lack of direct communications, the need for a direct-communication Hotline between Washington and and Moscow first became obvious during the October 1962 Cuban Missile Crisis. Misunderstandings caused by the lack of direct communications could have led to a nuclear confrontation. [2] A direct communications link was finally approved by President Kennedy and Premier Khrushchev shortly after the Missile Crisis.

(U) The United States and the Soviet Union signed the "Hotline" agreement in 1963. This agreement established a direct communications link between Washington and Moscow for use in emergency situations. [3] The terrestrial US-USSR Hotline system was designed and put into operation in the fall of 1963. In addition, a back-up radio link was established. Both the direct-communications link and its back-up were duplex teleprinter circuits which made use of cable and high-frequency radio links. The circuits used a speed of 50 baud/66 words per minute. The original US "Hotline" printer now sits in the Smithsonian Institution.

DOCID: 4009888

II. HISTORICAL EVENTS

(U) During its years of existence, the "Hotline" was used many times. The first well-known use was by President Johnson during the Arab-Israeli Six-Day War in 1967. He advised the Soviets of US ship and aircraft movements in the Mediterranean following an Israeli attack on the USS Liberty. President Johnson also sent several Hotline bulletins to notify the Kremlin of crucial Vietnam developments later on.

(U) In April 1969, when North Korea shot down an American reconnaissance plane, President Nixon used the Hotline to ask the Soviets to help search for survivors. Apparently President Ford did not have occasion to use the system during his administration, but the White House disclosed that President Carter and President Brezhnev used the Hotline several times to exchange messages. [4]

(U) The original "Hotline" consisted of undersea cables, radio links, and landlines, all susceptible to mishap. During the years which followed its beginning, several accidents occurred: a fire in a Baltimore manhole caused the line to be out of service temporarily; a farmer in Finland dug up the cable with his tractor; and both a deep-sea fishing trawler and a bulldozer in Copenhagen cut the line. [5]

III. WHY THE DCL CAME INTO BEING

(U) In each of the above cases the back-up radio system took over, but concern over the mishaps led to a US-Soviet agreement to create a pair of independent, but parallel, satellite communications circuits, each using a separate communications satellite in each country.[2]

(U) Advantages of the new system are:

[] it is less vulnerable than the older system;

[] it depends less on extensive terrestrial microwave or cable relays;

[] it eliminates dependence on third country facilities

[] it is not subject to interruptions caused by atmospheric interference.

(U) As a result of the 1971 Strategic Arms Limitation Talks (SALT), a supplemental 1971 accord (signed in Washington, September 1972, and in Moscow, December 1973) resulted in a new agreement which provided for two separate satellite circuits to replace the existing circuits, permit multiple teleprinter terminals and reduce the vulnerability of the terrestrial direct communication facilities. [6] An annex to the 1971 SALT agreement stated that the Hotline would be deactivated upon mutual agreement that it was no longer required.

IV. HOW THE DCL CAME INTO BEING

(U) Technical negotiations between the US and USSR involved US Departments of State and Defense officials and representatives of the Soviet Ministries of Foreign Affairs and Communications. Through a series of technical discussions, the new satellite system was jointly engineered, resulting in a Molniya earth station being constructed in the US at Fort Detrick, Maryland, and Intelsat earth stations being constructed in the USSR Moscow and L'vov. [7] Teams from each country were exchanged to familiarize the operators with some equipment differences, procedural rules, and other factors that were needed to ensure complete understanding of the system.

(U) The US portion of the link between the US and the USSR (which uses the Soviet Molniya II satellites) was awarded by the US Army Satellite Communications Agency to be built by the Harris Corporation on a 15-acre site at Fort Detrick, Maryland, at a cost of $7.5 million. Construction of the Fort Detrick DCL station began in October 1972 and was completed in April 1974.

(U) All the equipment is housed in a prefabricated steel building located between the two antenna subsystems on grounds enclosed by a security fence. The building provides a floor area of 7,000 square feet. The control room, which seems small considering the importance of its duties, measures approximately 20 by 60 feet and contains the computer, transmitters, receivers, and other equipment necessary to maintain the system

(U) After an extended period of testing between Fort Detrick and its sister station in the Moscow area, the line became fully operational in January 1978. During the testing years the older Hotline and new DCL operated in tandem. The original baud/wpm rate was retained; [7] also the older Hotline link was retained for emergency back-up.

(U) The Russians employed their Molniya and the Americans the commercial Intelsat satellites (both of which operate simultaneously) so that if one system fails, the other can be used. [8]

(U) The Fort Detrick DCL station consists of two identical and independent communications systems, providing simultaneous transmission and reception of C-band, FM-modulated

signals through its tracking communications antennas. Both communications systems interface via baseband processing equipment with government telephone cables that complete the Washington-Moscow connection. [8] The final telephone cable link from Fort Detrick to Washington goes first to the National Military Command Center in the Pentagon and from there directly to the White House. The telephone company has the responsibility for this final telephone cable link. If the US President wanted to converse with the Soviet Premier, a link would be established between Fort Detrick and the Pentagon, where communications experts can patch the President in to anywhere. [9]

V. THE PHYSICAL LOCATION OF THE DCL AND ITS ALTERNATE SITE

(U) The satellite portion of the United States is a leased duplex voice bandwidth circuit from a Comsat earth station at Etam, West Virginia, over an Intelsat IV satellite to a USSR-provided earth station at Moscow. The USSR satellite portion is a duplex voice bandwidth circuit from a Molniya II earth station at Vladimir, USSR (about 100 miles east of Moscow), through the Molniya II satellite to a US-furnished earth station at Fort Detrick. [8] Sending the traffic over those two routes minimizes chances that the messages will be distorted or lost. (See Figure 2.)

(U) Messages from Washington to Moscow are transmitted in English, using Latin characters. Communications from Moscow are in Russian, using Cyrillic letters. All the messages, including hourly tests, are automatically encoded upon transmission and decoded upon receipt. [1]

(U) Despite what Hollywood showed in the movie "Failsafe" starring Henry Fonda, the Hotline is not a red telephone. The fact is that President Reagan and the Russian premier are linked by a teleprinter. When the leaders of the two countries "speak" to each other, their messages are in their own native language, primarily to ensure accuracy. Printed messages have the advantage of overcoming language barriers, avoiding possible misunderstanding by simultaneous interpreters, and providing a written record of the traffic exchanged. [9] The traffic between the two countries is transmitted simultaneously over three independent systems. The United States circuit uses the Molniya II system and a cable system which passes across northern Europe. All three systems use the Pentagon as a central communications point.

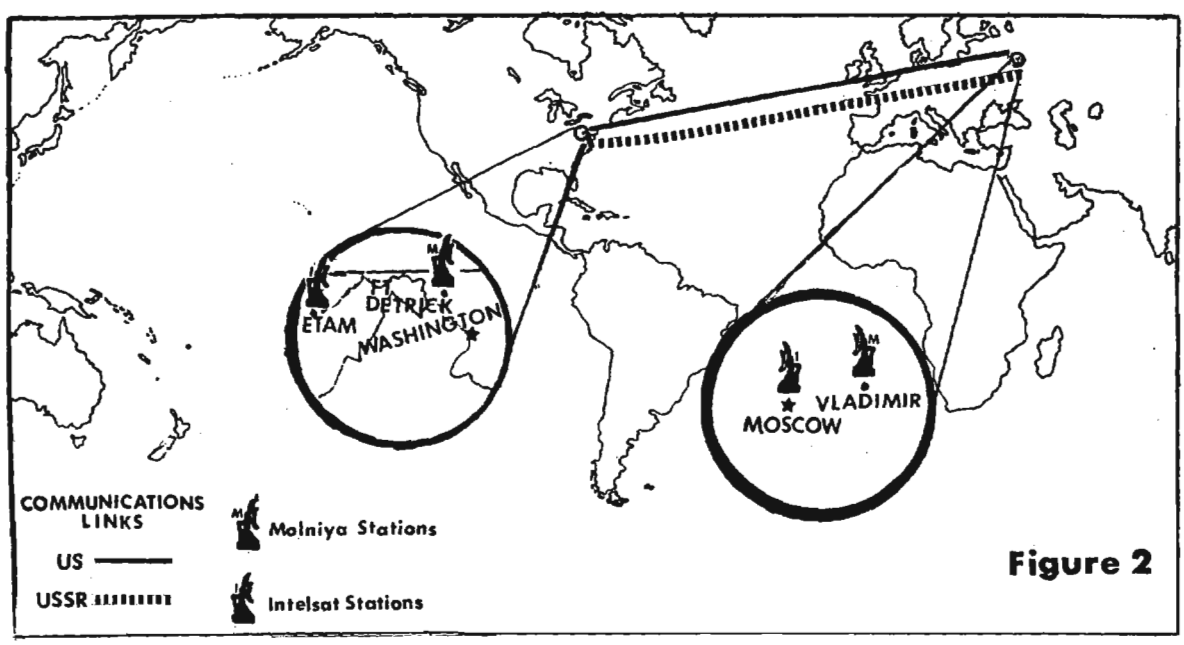


Figure 2

DOCID: 4009888

VI. ON-SITE OPERATIONS

(U) At the present time the operation and maintenance of the Fort Detrick earth station is under contract from the Army to the Bendix Field Engineering Corporation at an annual rate of one million dollars. Approximately 20 workers maintain the DCL at Fort Detrick 24 hours a day, seven days a week. [10] The workforce includes Russian linguists, technicians, and maintenance personnel. The staff monitors the signals going to and coming from Moscow, enhancing the power, if needed, and making sure that the antennas remain on target. There is not much chance that automation will reduce the number of people involved because of the terms of the supplemental 1971 SALT accord.

(U) The Fort Detrick DCL Station sends and receives traffic in the Russian language with an interpreter providing the necessary translations. Transmissions concerning technical data are translated into English by the linguists and filed. The setup is reversed for technicians operating the US Intelsat circuits.

(U) The technicians at Fort Detrick talk to their counterparts in the USSR over a service channel to check the operation of the system. Conversations are always very polite but almost never personal. Nevertheless, a lively exchange between American and Soviet technicians has been going on since December 1975, when testing first began. "Good morning, esteemed colleagues," the Soviets often open their remarks. [1]

(U) On occasion the dialogue has been very emotional. For example, the Russians send the US congratulations on such holidays as the Fourth of July and the American technicians congratulate their counterparts on the anniversary of such dates as the launching of the first Sputnik. [2] Following each communications exchange, the linguist types the appropriate translation so that this translation becomes part of the official station records. The communications from Moscow are typed in red and the outgoing US texts use black ink.

(U) The technicians at the DCL station cannot read the messages that are sent between Moscow and Washington. All they see are the readings on monitors as the signals are scrambled, with the only decrypting devices located at the terminals used by the two heads of state.

(U) Although the technicians are not military personnel, security is tight. Armed military guards are located directly across the street and the only entrance to the building is electronically operated. The DCL compound, if the need arises, can be sealed off from the rest of the base.

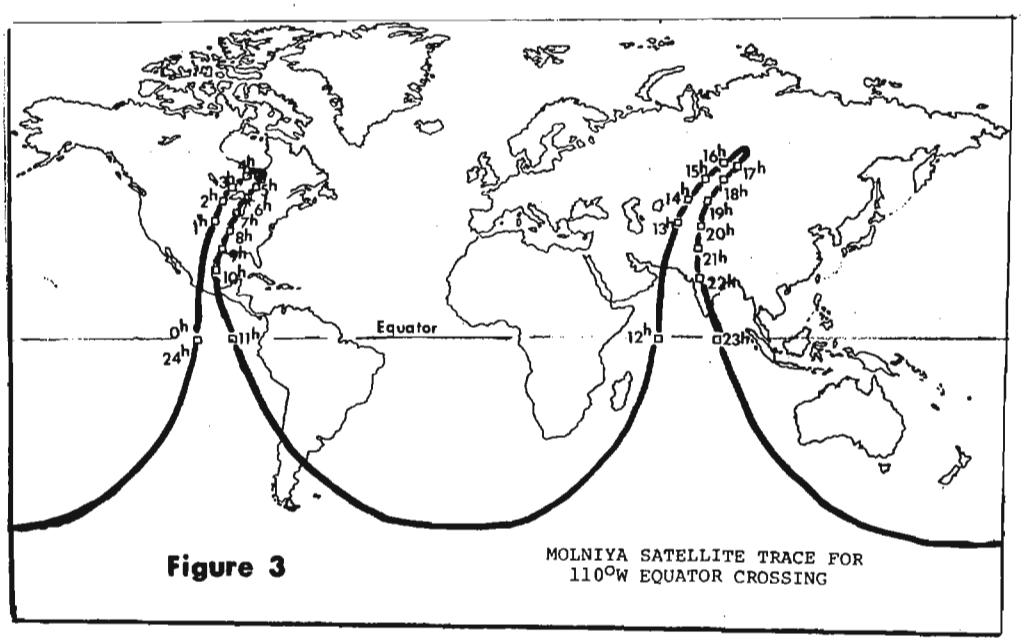


Figure 3 MOLNIYA SATELLITE TRACE FOR 110°W EQUATOR CROSSING

VII. THE USE AND OPERATION OF MOLNIYA II SATELLITES

(U) Unlike the US Intelsat satellites, the Russian Molniya satellites move in a highly eccentric orbit. This orbit brings each of the eight (four active and four standby) satellites forming the Molniya II operational system over the United States DCL earth station in a high looping arc once a day. Both of the Fort Detrick antennas track the satellite as it moves across the sky, which provides the system a minimum communications interruption, even in the unlikely outage of one antenna. [5]

(U) The reason for the deviation and eccentricity of the Molniya II satellites is essentially geographical. The northern portions of the Soviet Union are not visible to a satellite located over the equator. For this reason, the Molniya II satellites are placed in a highly elliptical orbit with an apogee (high point) of nearly 25,000 miles and a perigee (low point) of only 300 miles. The 65-degree direction provides an apogee over the northern hemisphere and the satellite's 12-hour orbital periods mean that they make two complete revolutions around the earth each day. [11]

(U) When the North American apogee occurs, each satellite remains visible to both Russian and American ground stations for approximately eight hours before the spacecraft moves down to its perigee in the southern hemisphere. By placing four Molniya satellites (plus four spares) in orbit and spacing them suitably, at least one will always be in view and available for communication between the two countries. [8] If the satellites' paths were traced on a map, they would look like two crested waves, one reaching into the center of North America and the other into Asia. [12] (See Figure 3.) These orbits are essential because the Russian satellites carry signals other than those of the Hotline. Therefore, a more conventional orbit around the Equator would make it impossible to reach the most populated areas in the northern part of Russia.

OPERATION OF THE DCL OPEN GRID ANTENNAS

(U) Twin 60-foot open grid antennas located at Fort Detrick are used to follow the Soviet Union's Molniya communications satellites in their highly eccentric orbited around the earth. Both antennas track the same satellite to provide complete redundancy except during period of handover from one satellite to another. [13]

(U) Shortly before the time when the active satellite moves out of the region of mutual visibility between Washington and Moscow, one of the two DCL antennas will swing away from it and obtain the next vehicle in preparation for the communications handover. Once a communications circuit has been established through the next satellite, the original DCL circuit will be transferred; the other antenna will move over to provide backup. [12] In this way 24-hour coverage is achieved. Handovers from one satellite to another are accomplished approximately every six hours to ensure minimum interruption of communications capability; usually the interruption lasts only 14 to 20 seconds. In addition, if difficulties prevent maintenance communications via the Molniya system, then the DCL at Fort Detrick has the capability to operate via the USSR Stationstar synchronous satellite, a satellite which orbits around the equator. This procedure is implemented only during emergency conditions and requires the approval of the Federal Communications Commission.

(U) Both DCL antennas at Fort Detrick have the full hemispherical angular coverage and precision tracking capability needed to direct their narrow beams toward the satellites. [8] During the daily period in which each earth satellite is jointly visible by Washington and Moscow, its pilot signal is autotracked by the two DCL antennas. The earth station includes two complete radio frequencies so that autonomous tracking of the Molniya satellite can be achieved.

AN EXPLANATION OF THE EQUIPMENT NECESSARY TO MAINTAIN THE DCL

(U) In addition to the two communications systems (including the transmitting, receiving, and antenna subsystems), there are ancillary subsystems that serve the earth station. These ancillary subsystems include:

- [] a dual programmer subsystem;
- [] a control, monitor, and alarm subsystem; and
- [] the prime power subsystem. [13]

(U) The dual programmer subsystem is built around twin Datacraft Model 6024/5 central processors operating through multiple parallel channel control buffers. [5] These twin computers provide automatic tracking of the satellites. Orbital variables furnished by the Soviet Union are programmed into these computers. Each processor accepts as input the orbital geometry elements of a satellite, and then the computers automatically generate the attendant look angles for the specified satellite. In addition, one of the technicians manually selects the program track which activates the computer to move the antenna to a preselected position for acquisition. The computers also provide corrections for antenna

error, as well as a real-time servoloop closure for the antennas. [8]

(U) The control, monitor, and alarm subsystem functions as the operator interface for station control status display and provides the logic circuitry to control automatic switchover to standby items of critical equipment in the event of an on-line failure. The occurrence of faults within the equipment of any subsystem activates distinctive audible alarms which sound throughout the DCL station until a maintenance action is started. [8]

X. RELIABILITY OF THE DCL SATELLITE SYSTEM

(U) The DCL station also had two prime power generators, each capable of accepting the power load of the entire DCL station. Two uninterrupted power sources (UPSs) give the station the ability to operate without communication channel outage despite any temporary loss of power.

(U) Special redundancy is provided within each of the two antenna subsystems of the Fort Detrick DCL site. For example, standby transmitting and receiving equipments are held in constant readiness so that a failure in any on-line unit can be quickly countered. [7] Monitoring circuits keep a steady watch on the status of all critical equipment within the DCL station. These circuits can switch in a standby unit automatically to prevent all but a momentary loss of communications. By these means extremely high communications link reliability is assured. [5] The DCL system has an efficiency of over 99.99% with a total down time of only 35 minutes for 1983. It would seems that the original concept of creating a more dependable, more reliable system of communication between the two superpowers has been realized. [13]

(U) The longest period of time that the Fort Detrick station has been off the air occurred July 27, 1982, when a bolt of lightning hit inside the compound fence, causing considerable damage. The DCL station was back on the air within seven minutes, with the technicians tracking and working all systems manually.

(U) Even with strict US-USSR requirements that any interruption which exceeds five milliseconds be considered a failure, the DCL system Mean Time Between Failures (MTBF) is greater than 835 hours (almost 35 days). [13] In addition, operational requirements include:

[] the need to restore one signal route to operation within 15 minutes of a failure and

[] for 90 percent of all failures, the restriction of corrective maintenance to a maximum of 45 minutes.

XI. BACKUP CAPABILITIES

(U) Each of the two identical earth station communication systems forms a fully redundant communications path from an interface with baseband processing equipment through its transmitting and receiving subsystems. Dual uplink and downlink communications chains are formed in on-line/standby pairs such that single failures within the equipment of either system cannot cause more than an instant loss of signal continuity. Circuit status is monitored at all times and switchover to a standby chain upon detection of an on-line failure is automatic. [14]

(U) Each of the two channels of baseband information frequency modulates a carrier and is up-converted and amplified within redundant transmitting chains. The output of one of the two power amplifiers is then selected for radiation via the antenna subsystem. [13]

(U) Received signals are routed from the antenna subsystem to one of the two low-noise amplifier channels within the receiving subsystem where four down-converted channels carry the band signals to a signal processor. Two of the four channels normally provide a redundant path for the Moscow link communications traffic. The other two channels (pilot/monitor and pilot) are not directly in the communications path but give the signal processor auxiliary inputs for the earth station frequency and power control and automatic tracking.

(U) The system's success could be attributed to a comprehensive preventive program which includes regular maintenance and evaluation of operating equipment. Several monitoring and control modifications have kept equipment up to the changing levels of technological advancement. [14]

(U) Normally the station operates on commercial power. In the event of a commercial power outage, emergency generators capable of accepting the load of the DCL station are located nearby at Headquarters, East Coast Telecommunications Center. In addition, within the DCL station, two uninterruptible power sources provide the station with the capability to operate on batteries for short periods of time without a communications channels outage despite any temporary loss of prime power. [7]

(U) The technique for automatic frequency and Effective Isotropic Radiated Power (EIRP) are controlled by comparing the received level and frequency of two carriers passing through the satellite. The first of these is a pilot carrier generated within the Soviet Union, while the second is the earth station's own transmitted signal. The frequency and EIRP of the locally transmitted signal are automatically controlled by the signal processor to maintain the frequency and power level at which the two carriers are received in a fixed relationship. [14] Failure of either pilot demodulator chain diverts the standby demodulator from its normal communications function so that frequency, power control, and tracking can be continued.

(U) Each antenna subsystem employs a pseudo-monopulse automatic tracking feed in a Cassegrain configuration within the 60-foot reflector. The feed system, which combines transmit, receive, and tracking functions in a single horn, is a modified version of that used in communications satellites in the Intelsat series. [12] The control system for each DCL antenna operates in both automatic and tracking or computer-directed modes to direct its beamwidth accurately toward a satellite. Antenna position is directed by precision resolvers which supply programmer subsystem inputs, drive illuminated position displays, and furnish (through the computers) a paper-tape record of time-tagged tracking angles.

(U) The antenna pedestals of the DCL earth station are rigged X-Y positioners capable of supporting 85-foot-diameter reflectors. The X-Y axis configuration can track satellites directly through zenith and the near-hemispherical angular excursion capability includes all altitudes at which the satellites are visible in both Washington and Moscow. Neither reflector nor pedestal requires a radome protection to survive winds as high as 150 mph. A deicing system prevents the accumulation of ice or snow on either the reflectors or subreflectors. [14]

XII. HOW THE DCL WILL BE UTILIZED IN THE FUTURE

(U) President Reagan proposed several times during 1982 and 1983 that considerations be given to upgrading the Hotline to permit a higher rate of data or, in fact, even voice communications. [16] This change will not take place for several years because, in order to change from the current 66 words per minute to a higher rate, the change must be established with the Russians in a treaty, which takes time.

(U) The establishment of other DCLs with other countries has not been formally proposed to date and does not seem likely for quite some time.

FOOTNOTES

1. News, Public Affairs Office, Fort Detrick, Maryland, September 14, 1972.
2. L. H. Whittemore, "U.S.-Soviet Hotline begins operating by satellite," The Baltimore Sun, January 1978.
3. "20 Years of Arm Agreement," U.S. News and World Report, May 1979.
4. George Gedda, Associated Press dispatch, January 16, 1978.
5. John Whitman, "Hotline terminal links U.S.-U.S.S.R.," Radiation Ink, Melbourne, FL, April 1973.
6. Ministry of Communications, USSR, "Organization of the U.S.S.R.-U.S.A. Direct Communications Link Through the Molniya-3 Satellites," 1976.
7. US Army Communications System Agency, "Logistics Support for U.S.A.-U.S.S.R. Direct Communications Link," August 1973, chapter 3.
8. "Molniya Earth Station Becomes Operational for Washington-Moscow Direct Communication Link," Communication News, February 1975, p. 3.
9. "Hotline," The Morning Herald, Hagerstown, MD, September 4, 1979.
10. "Local Bendix Subsidiary Runs Political Hotline," The Baltimore Sun, September 23, 1981.
11. Hugh Hartman, in Bendix Corporation newsletter, Columbia, MD, October 1981.
12. Douglas Tallman, "Fort Detrick 'dishes' link White House to Kremlin," The Post,, Frederick, MD, April 21, 1982.
13. Conversation with Hugh Hartman, Bendix Corporation DCL Site Manager, Columbia, MD, December 1982.
14. William Pitman, Harris Corporation Information System, Melbourne, FL, November 1982.
15. Dinny Quinn, "Fort Detrick--Hotline to U.S.S.R.," The Post, Frederick, MD, August 25, 1980.
16. Henry Jackson, "Nuclear War and the Hotline," The Wall Street Journal, September 3, 1982.

DOCID: 4009888

~~FOR OFFICIAL USE ONLY~~

NSA-Crostic No. 51

Leonard, Adolph, Julius, Milton and Herbert - otherwise known as Word R.

A. Almond or pecan, for example
143 71 84

B. Lefty
61 59 26 124 76 95 146 28

C. Probably Word R's best movie (1935) (5 wds(
129 100 167 23 157 116 49 184 30 152 18 63
24 7 140 135

D. She played Word R's mother in the play *Minnie's Boys* (2 wds)
51 62 169 102 4 68 47 138 179 110 87 36 60 72

E. 1946 film with Word R (4 wds)
164 43 130 27 174 14 98 83 122 2 35 57
147 160 133 183 154 139

F. Given to the use of obscene talk
166 126 94 149 181 125 159 173 117 123 137

G. Reverberate: repeat
148 93 132 77

H. Integer
88 151 99

I. Young; fresh, vigorous
70 53 50 44 33 120 5 25

J. _____ mad
112 172 54 40 153 131 144

K. 1930 movie with Word R (2 wds)
13 22 3 45 104 79 81 20 96 48 65 42 56 11

L. The unfunny member of Word R
134 90 19 180 9

M. 1937 film starring Word R (5 wds)
46 170 101 108 114 8 32 31 182 16 109 86 52 75

N. French engineer (1604—1680), built the Canal du Midi, linking the Mediterranean and the Bay of Biscay
69 34 177 38 163 128

O. French historian (1805—1859), who wrote extensively about the United States (*Democracy in America*, etc.)
161 106 58 118 64 37 178 73 67 29 145 115 175

P. Knob, lump; gist, point
141 78 162

Q. Not on
82 119 105

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009888

R. American comedy team (3 wds) — 171 15 12 41 85 136 168 127 74 91 107 89 / 176 6 156

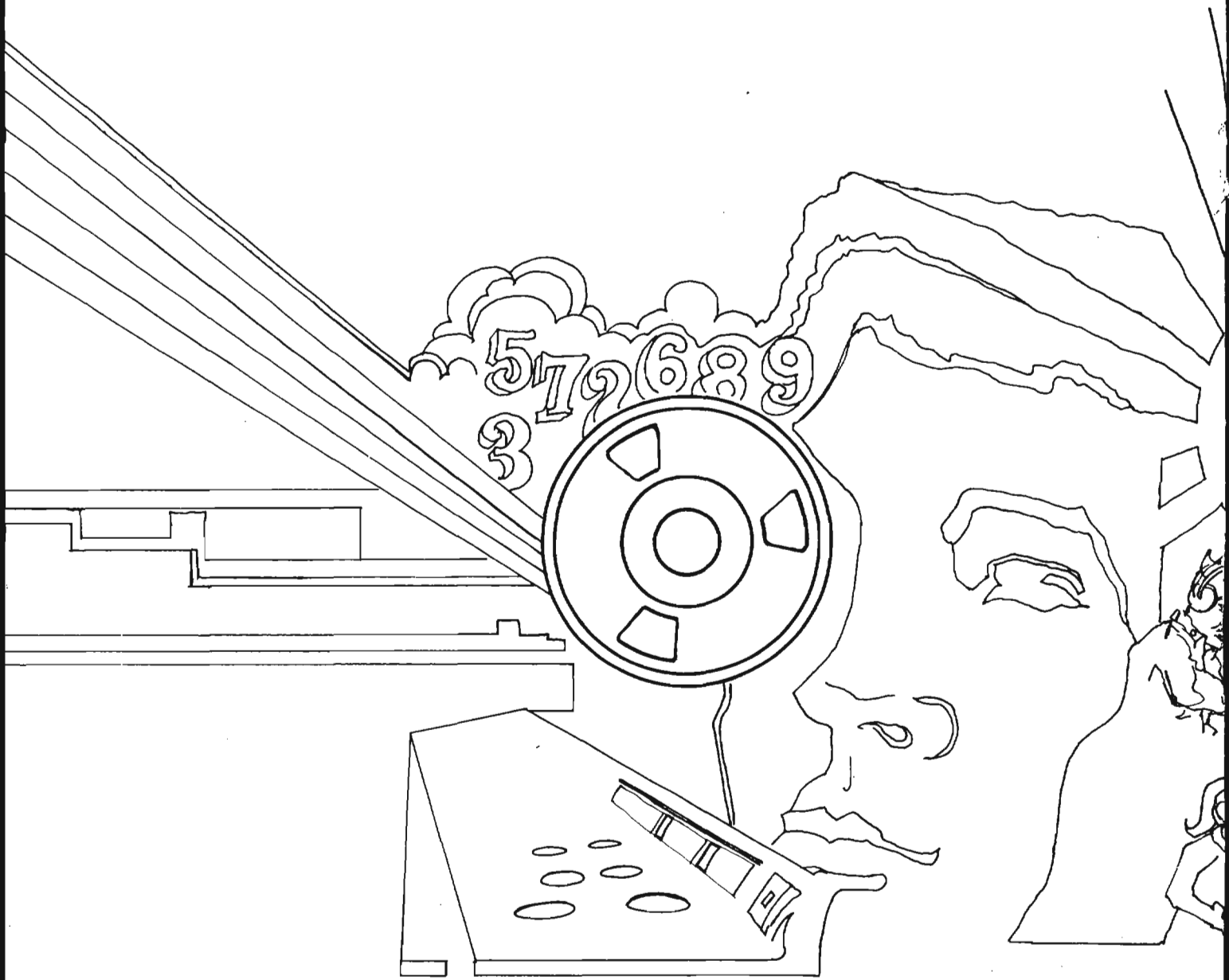
S. ____ Amin — 39 111 121

T. Place where certain refreshments are sold — 92 158 1 165 66 17 155 21 10 150 55

U. Bluepencils — 113 80 142 97 103

			1 T	2 E	3 K	4 D	5 I	6 R	7 C		8 M	9 L		10 T
11 K	12 R		13 K		14 E	15 R	16 M	17 T	18 C		19 L	20 K	21 T	22 K
23 C		24 C	25 I	26 B	27 E		28 B	29 O	30 C	31 M		32 M	33 I	34 N
35 E		36 D	37 O	38 N	39 S	40 J	41 R	42 K	43 E	44 I		45 K	46 M	47 D
	48 K	49 C	50 I	51 D	52 M		53 I	54 J	55 T	56 K	57 E	58 O	59 B	60 D
	61 B	62 D	63 C	64 O	65 K		66 T	67 O	68 D	69 N	70 I		71 A	72 D
73 O	74 R		75 M	76 B	77 G	78 P	79 K	80 U		81 K	82 Q	83 E	84 A	85 R
86 M	87 D		88 H	89 R	90 L		91 R	92 T	93 G	94 F	95 B	96 K	97 U	98 E
99 H	100 O	101 M	102 D		103 U	104 K	105 Q	106 O	107 R	108 M		109 M	110 D	111 S
	112 J	113 U	114 M	115 O	116 C	117 F		118 O	119 Q	120 I	121 S	122 E	123 F	
124 B	125 F		126 F	127 R	128 N	129 C	130 E	131 J		132 G	133 E	134 L	135 C	136 R
137 F		138 D	139 E	140 C	141 P	142 U	143 A	144 J		145 O	146 B	147 E	148 G	149 F
150 T		151 H	152 C	153 J	154 E	155 T		156 R	157 C	158 T	159 F	160 E	161 O	
162 P	163 N		164 E	165 T	166 F	167 C	168 R	169 D	170 M		171 R	172 J		173 F
174 E	175 O		176 R	177 N	178 O	179 D	180 L	181 F	182 M	183 E	184 C	dhw		

Pl-Apr 84-S3-47296


5 7 2 6 8 9
3

DOCID: 4009885

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG
NOVEMBER 1983

P.L. 86-36

STATIC MAGIC:
THE WONDERFUL WORLD OF TEMPEST (U)..... Thomas M. Donahue..... 1
TEMPEST FOR EVERY OFFICE (U)..... [redacted]..... 3
I REMEMBER JFK (U)..... H.G.R..... 5
MBTI: THE MANAGEMEMNT TOOL OF THE FUTURE (U).... [redacted]..... 8
ACRONYMANIA (U)..... [redacted]..... 11
THE WHITE HOUSE IS SINGING OUR SONG (U)..... Albert I. Murphy..... 13
THE LITERARY BENDS (U)..... Albert I. Murphy..... 14
CIRCA 1949 (U)..... [redacted]..... 19
5-4-3 PUZZLE..... Watt Zizname..... 20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2
DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009885

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. X, No. 11 NOVEMBER 1983

PUBLISHER [redacted]

BOARD OF EDITORS

Editor.....[redacted] (963-3045s)
Asst. Editor...[redacted] (963-1103s)
Production.....[redacted] (963-3369s)

Collection.....[redacted] (963-3961s)
Computer Security
....[redacted] (968-7313s)
Cryptolinguistics.[redacted] (963-1103s)
Data Systems.....[redacted] (963-4953s)
Information Science
.....Carolyn Cornelius (963-5711s)
Mathematics.....[redacted] (968-8518s)
Puzzles.....David H. Williams (963-1103s)
Special Research.....Vera R. Filby (968-7119s)

For subscriptions
send name and organization

to: [redacted] P14
(963-3369s)

P.L. 86-36

To submit articles or letters
by mail, to: P1, Cryptolog

via PLATFORM mail, send to:
cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no 'O' in 'log')

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

"Wayne:

"While I was perusing the Black Books for quotable oldies I realized that CRYPTOLOG comes from a long tradition. In the 1920s the Signal Corps Bulletin published articles on cryptanalysis along with other subjects related to communications. Before that, as I recall, around 1911 I think it was, Maubourgne published the solution to the PLAYFAIR cipher in a periodical of the War College (I think...don't remember exactly).

"You might want to write an editorial on the (disrupted) continuity of documentation, exchange of ideas, etc. Before CRYPTOLOG was KEYWORD, and I dimly recall something before that, including the underground press.

"I think that there's something deep inside every professional that urges towards the passing on of the torch, to chat in writing with others of similar ilk, to want to find out what everyone else is doing, and how others are solving the same problems.

[redacted]

Well said, Virginia.

****
*
* CORRECTION
*
* The notation "This Document Contains *
* Codeword Material" on the covers of the *
* October 1983 CRYPTOLOG are in error. The *
* proper caveat is HANDLE VIA COMINT CHAN- *
* NELS ONLY. Please change your copy accord- *
* ingly.
*
****

DOCID: 4009885

STATIC MAGIC

OR The Wonderful World of TEMPEST (U)

OR One Man's Static Is Another Man's Treasure!

by Thomas M. Donahue, T44

(U) "DID YOU SEE WHAT I SAW?"

(U) The COMSEC engineer almost had his nose pressed against the screen of the oscilloscope.

(U) How the devil did I know if I saw what he saw if I didn't know what he saw? Besides, it was hot and I had a headache.

(U) Staring at RF noise being displayed on an oscilloscope is like looking into a blizzard on New Year's Eve. You start to imagine things. It had been a long day. Suddenly two words appeared on the screen: TERMINAL READY. I blinked; they were gone.

(U) The engineer twisted the dials on the electronic intercept receiver. A couple of blurred words appeared. A few more twists and they became clear. "TOP SECRET" danced at the top of the screen.

(U) We smiled at each other. I gave the engineer a pat on the the back. My headache was gone. We had done our thing. There was tension in the air--like being caught with your hand in the cookie jar. But it was our cookie jar.

(U) The oscilloscope we were looking at was displaying classified information radiating from distant terminals in NSA Operations Building Number 1. We were sitting in a Winnebago camper van in the visitors' parking lot near Gate 2.

~~(C)~~ During the following two days we were able to intercept classified text from 84 terminals in A Group and 4 in B Group. The terminals were immediately removed from service.

(U) Another time, another place, and more stolen cookies.

~~(C)~~ A secretary in the R Organization at FANX II was typing a classified memo that dealt with TEMPEST radiation. Her curiosity was aroused. The engineers in the lab were complaining about her new typewriter causing static in their equipment. Could this static be a form of the "compromising radiation" she was reading about, and could it be picked up by the cars and vans parked less than 50 feet away in the NSA parking lot?

(U) Later she asked her boss, "Am I radiating?" Always the gentleman, he replied, "You certainly are, Nancy. Is that a new dress?"

(U) Fortunately for the Agency, she explained that it wasn't her dress she was worried about but her typewriter. The typewriter she was using was being placed throughout the Agency because tests had shown it had very good TEMPEST characteristics. What had not been foreseen was that an enterprising salesman, to show his company's appreciation for the new contract, was upgrading the typewriters at no cost to, and without the knowledge of, NSA management. He was installing a device that let the typist see each line as it was being typed on an electronic display. Unfortunately, it also let someone 200 yards away with TEMPEST intercept equipment see each line as it was being typed.

(U) These are just two examples of TEMPEST problems at NSA. There have been others.

(U) There is no special meaning in the word "TEMPEST." It was simply picked from a covername list by an NSA engineer in the early 1950s. However, TEMPEST has now become a generic word used throughout the US Government and industry to describe the unintentional emanation of classified information from an equipment. It is used as a noun, verb, or adjective; sometimes in the same sentence. For

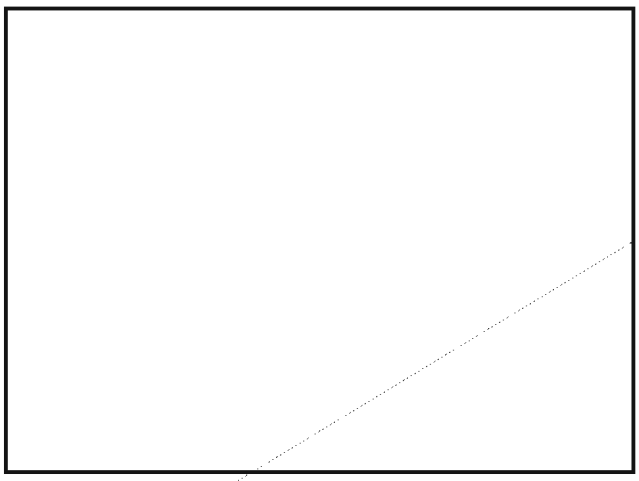
example, "TEMPEST requires that we TEMPEST equipment to suppress TEMPEST radiation."

(U) NSA, because of the variety of equipment and sensitivity of its work, has always worried about possible TEMPEST leaks. However, it wasn't until the late 1970s that a workable plan was initiated to categorize equipment into groups by their TEMPEST characteristics. Until then there was only one standard for describing TEMPEST characteristics: NACSEM 5100.

(U) This specification, NACSEM (NAtional ComSec/Emsec Memorandum) 5100, stated the laboratory tests and radiation limits an equipment must meet to be TEMPEST approved. It either did or did not meet it. The intent of the specification was to prevent someone in one room from "reading" the emanations in an adjacent room.

(U) Designing and building equipment to meet the strict requirements of NACSEM 5100 is expensive. It has been estimated that the cost of modifying all the typewriters, computers, etc., used by NSA to process classified information to meet NACSEM 5100 would probably exceed the entire defense budget. Yet Milton Zaslow, a former Deputy Director for Telecommunications, was fond of saying, "TEMPEST is a price we must pay to stay in business." To overcome the cost versus security problem, COMSEC developed the "zone" concept.

(U) The compromising radiation levels of off-the-shelf equipment are measured and the equipment is assigned a TEMPEST zone rating. A "Zone 1" rating means it has a low radiation profile, while a "Zone 5" rating is given to those with high levels of compromising radiation.



(U) There are two ways of providing TEMPEST protection. The equipment can be designed so that it doesn't radiate in the first place, or measures can be taken to insure that any radiation can't be intercepted. The latter can be accomplished by using the inherent attenuation provided by the location of the equipment, such as our building zone concept, or by building a special room to keep the radiation from getting out. Such a room is called a shielded enclosure or, for the old-timers, a "screenroom." It's the same idea as Maxwell Smart's "Cone Of Silence."

(U) Carrying the idea of the shielded enclosure to the extreme, why not shield an entire building? Then you could place equipment without worrying about TEMPEST radiation.

(U) Well, if you have been watching Operations Building 2A going up, you have been witnessing the building of NSA's own "Cone Of Silence." That copper material that goes under the glass facing is for TEMPEST protection. This building will be by far the largest shielded enclosure ever built. The US Intelligence Community is watching this project with much interest. If it works as well as we think it will, full-TEMPEST buildings may well be the thing of the future. There are also plans to TEMPEST-shield the Headquarters and Operations Building 1. The savings in convenience and dollars should be considerable.

(U) A few additional words on TEMPEST radiation. There have been questions about the TEMPEST radiation that's going to be "trapped" inside the buildings by the shielding. "Isn't radiation bad for you?" Well, let me put your mind at ease. TEMPEST radiation is the same type of energy, in the same frequency range, as that used to broadcast radio and television signals, but it is much weaker.

(U) The radiation present in your living room coming from television Channel 2 is many times greater than the radiation from TEMPEST signals. An hour at NSA with TEMPEST will be no more dangerous, but probably a lot less exciting, than an hour at home watching the tempestuous activities of "The A-Team."

EO 1.4.(c)
P.L. 86-36

OCID: 4009885

~~FOR OFFICIAL USE ONLY~~

TEMPEST FOR EVERY OFFICE

P.L. 86-36 by [redacted] S64

John Doe arrives at work in the morning, powers up his computer workstation, and relaxes with a cup of coffee while he reads his morning mail on the CRT screen. Across the hall, Sue Smith finishes editing her project report before routing it to the printer at the front of the room. Meanwhile, Kathy's secretary has just completed a large batch of correspondence that used to take twice as long to prepare.

These are just a few of the "miracles" that we all look forward to in the paperless office of the future. High-technology firms have been gearing up to provide the computers, printers, workstations, and other peripherals for the transition. Experts predict that by using our computer know-how to solve information management problems, we can save millions of dollars in all areas of cost in the office.

Great idea! But what about the special problems that office automation presents to the US Government? One of the problems, of course, is security. To narrow down the scope of this article, let's look at just one part of the security problem: TEMPEST (compromising emanations).

At some point a decision was made that John Doe's workstation would have to meet the government's TEMPEST requirements. The decision may have been made by John Doe himself, by his security Chief, or by the "local TEMPEST authority." A requisition was made for a workstation and some few months later, John Doe sits at his terminal reading and writing with the greatest of ease! The process of procuring a TEMPEST-suppressed terminal has become this simple only in the last few years.

In 1976, on behalf of the National Communications Security Committee (NCSC), the National Security Agency created the Industrial TEMPEST Program (ITP). Until that time, the only way the government could obtain TEMPEST-suppressed equipment was to let a contract for the development of each specific equipment needed. Each contractor was given the classified information necessary to design and test its product. This was an expensive process. As the government's need for information processing equipment grew, the impact of the high cost of these contracts also grew.

The ITP was formed to provide an alternative to this steadily increasing cost of TEMPEST protection. Its purpose is to satisfy the government's need for TEMPEST-suppressed equipment by involving industry in the development of TEMPEST-suppressed products that can be purchased "off the shelf." This is a unique charter for a government program, and the ITP is a unique creation.

The program is based on a no-cost contract between the government and qualified US companies that voluntarily develop, test, and produce TEMPEST-suppressed equipment using their funds rather than government funds. To join the ITP, a company must satisfy a set of qualifications pertaining to US ownership and security clearances and make a clear commitment to develop TEMPEST-suppressed equipment. Additionally, the company's activities must be of obvious benefit to the government. A company remains in the program by working toward the goal of developing TEMPEST-suppressed information processing equipment.

~~FOR OFFICIAL USE ONLY~~

The no-cost contract (known as the ITP Memorandum of Understanding) calls for certain commitments for both government and industry to contribute to the development process.

The government provides classified specifications, technical assistance, technical training in the form of Air Force TEMPEST courses, and the government market for TEMPEST-suppressed equipment. Industry provides those resources needed to put TEMPEST onto the production line. These include development expertise, TEMPEST test capability, R&D expertise and funding, and the manufacturing capability.

The success of the government-industry partnership is undisputed. Since 1976, ITP membership has grown from 9 to 95 companies. The number of government-accredited TEMPEST-suppressed devices has also multiplied. In 1979, when the first list of accredited items, the Preferred Products List (PPL), was published, it listed 11 different products. Today the PPL includes 135 devices, such as word processors, printers, communications terminals, and CRT display units. There are other benefits from this arrangement as well. Advantages to the government include a larger selection of TEMPEST-suppressed products at lower prices; an excellent channel of communication with industry; and firm control over the dissemination of TEMPEST information. Companies in the program gain the opportunity to compete effectively in the TEMPEST marketplace.

Close communications between ITP members and the government has been an important factor in the success of the ITP. As the relationship between ITP members and the government continues to grow and strengthen, we expect to see even better results from the program. Our efforts will be devoted to better communications with ITP members, smoother operation of the program, and even cheaper TEMPEST-suppressed products for the government.

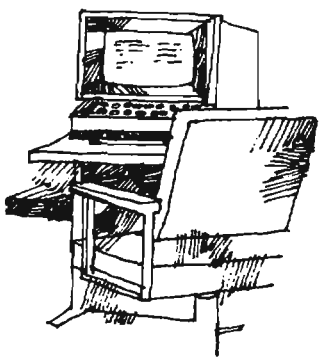
The ultimate goal is for ITP companies to introduce their TEMPEST-suppressed version of a product at the same time that the commercial version hits the marketplace. This will give John Doe and friends the opportunity of obtaining the latest and greatest information processing equipment with TEMPEST protection at the same time that the rest of the world is discovering the same state of the art product in a commercial configuration.

EO 1.4.(d)
P.L. 86-36

Dear Sir

~~(S-CCO)~~ I was particularly interested to read your CRYPTOLOG May 1983 article on the "Computerizing of TA." The analysis of what the TA analyst looks for and needs from ADP and the conclusion in favour of PINSETTER-type software support is remarkably consistent with our own findings in J Division, following a detailed systems analysis exercise conducted throughout 1982. As a result of this we are proposing for J Division a solution, nicknamed [redacted] which will be based on UNIX-PINSETTER work at NSA.

[redacted]



DOCID: 4009885

I Remember JFK (U)

P.L. 86-36

by "HGR"

(U) Now that November 1983 has rolled around, the media can be expected to make a lot of fuss over the fact that it has been 20 years since President John F. Kennedy was assassinated in Dallas, Texas. The commentators and journalists have been making a semi-major event out of the anniversary ("Just like on Pearl Harbor Day, everybody remembers where they were on November 22, 1963, when they first heard the news" and similar inanities), but anniversaries divisible by 5 or 10 always produce a greater outpouring of such deathless prose. So this 20th anniversary of President Kennedy's death will no doubt engender exceptional numbers of articles, radio and TV specials, memoirs, even a book or two, and countless numbers of interviews asking that earth-shaking question "Where were you on that day?" Not that I think that all the to-do is really necessary but Cryptolog and I might as well get on the bandwagon.

~~(FOUO)~~ To get the burning question out of the way, in case anybody cares where I was on Friday, 22 November 1963, let the record show that I was at work somewhere on the second floor of the NSA Building. (At that time there was only one, the 3-story edifice now known as the Operations Building.) Life was going on as usual in one of those offices that always seemed to be running at a fever pitch --"Every day is flap day here!" was the way one person put it--and since our mission did not include keeping track of the president when he was traveling around CONUS, nobody gave much thought to the fact that JFK was going to Dallas that day. But shortly after lunch Al Graves' wife called him and gave him the news.

(U) "HGR" is one of several pseudonyms used by [redacted] P16, who remembered Mabel Babel in our August issue.

~~(FOUO)~~ As luck would have it, the outside phone was on my desk so I got the full impact of his loud "Wha-a-a-a-t?!?" She repeated the news and he uttered a short phrase that I wouldn't dare repeat here and hung up the receiver without even saying "Thanks" or "'Bye!" With a rather perplexed look on his face he then proclaimed to nobody in particular "The President has just been shot!"

~~(FOUO)~~ There was a series of thuds as pencils were dropped by a number of surprised analysts. There were also excited cries of "What did you say?" and "Are you sure?" There was also an occasional "How did you find out?" from SIGINT analysts used to checking source validities. Somebody said, "I won't believe it until I hear it over the Agency loudspeaker system," but to the best of my recollection, such an announcement was not made. For the rest of the day, though, various individuals in the office would call relatives at home to see if there was any later news. A few individuals ran down to the parking lots to listen to news on their car radios. At go-home time President Kennedy was still in the hospital, but the sad news came later.

(U) The funeral took place the following Monday and all government employees got the day off, but for several days after their return to work, the major topic of conversation-

--at least in the office where I was then working--was the lack of any official announcement over the loudspeaker system, with things like "You'd think a communications agency could at least communicate something like that to its employees" being said more times than I care to recall. (For the record, during the next year or so, the Agency did react to the criticism by announcing space shots, presidential signing of Federal pay-raise legislation, etc.)

~~(FOUO)~~ However, there are a few other things about President Kennedy's term that I remember at least as well as his last day. Considering that his term of office included the Bay of Pigs invasion and the Cuban Missile Crisis, events that caused lots of extra work for this Agency and necessitated my working many 12-hour shifts, 6-day weeks (and there were some others even more patriotic who put in 7-day weeks), weekends when I'd work noon to midnight on Sunday and then go home only to be back in the office at 7:30 Monday, I guarantee that it'll be a long time before I forget the Kennedy presidency!

~~(FOUO)~~ There were probably some employees who have put in 24-hour days and although I tried to do it on one occasion, I was thwarted. I could probably go look up the date, but I don't feel like it. However, during the October 1962 Missile Crisis our section had gone on 12-hour shifts and I was on from midnight to noon, but at midday I was in the midst of a long wrap-up report, so I stuck around a few hours longer to finish it, and then someone asked me for a little help on something he was doing, and then something else happened, and then something else, and something else, so I stayed a litle longer. At this point, I figured that since it was almost dinner time, I might as well wait a bit longer and eat in the cafeteria. While eating supper, the idea hit me that since I'd been here for over 18 hours, I might as well try for 24, but Carrie Berry, one of my supervisors, dropped back in the evening to see how things were going. She recalled having seen me that morning--I have one of those faces that it's hard to forget!--and gently suggested that I should hit the road. However, we had heard that the president was going to be making a speech at 8:00 o'clock so I urged her to let me at least stick around to hear it on the portable radio that one of our coworkers had smuggled in. I planned to find some other excuse at the end of the speech, but Miss Berry anticipated me. Within 10 seconds of the the president's last word (while the radio announcer was still saying "You have been listening to President Kennedy speaking live from the White House"), she told me in a very firm tone of voice (that she apparently hadn't to use with me previously) "OK, the speech is over. Now get home!" so I left after only slightly more than 20 hours on the job that day.

(U) But another 1-o-o-o-o-o-ong day in connection with John Kennedy that I'll certainly remember is the day of his inauguration in 1961. The announcement had been made that only Federal employees in the Washington area would be given the day off; subsequently we heard that Fort Meade was not considered part of the DC area. It should be noted that for previous inaugurations the Agency had been housed at Arlington Hall, which was in the Washington area, so I remembered having gotten the day off when Eisenhower had been sworn in. Accordingly, I was annoyed at the thought that we wouldn't be getting the day off for the Kennedy inauguration. Recalling the fact that the Agency had given its employees a few days off the previous winter because of severe snowstorms, a few days before the ceremony, I voiced a silent prayer asking for just enough snow on the 19th so that I'd be able to stay home on the 20th and watch JFK take his oath of office.

(U) Boy, did my prayer get answered! It snowed so heavily on the 19th that the Agency powers that be decreed an early dismissal for all employees about 2:00 p.m. Letting everybody out at the same time on a good day would create a horrible enough traffic jam, but turning the entire crew out at the same time on a snowy day really compounded confusion. It took my carpool over an hour just to get off the NSA parking lot--by comparison, on normal days it took me about 45 minutes to get all the way home to Southeast Washington--and almost another hour just to get over to the Baltimore-Washington Parkway. The pace on the Parkway was mighty slow and the roads in the District of Columbia were clogged with snow and stalled cars so progress was difficult. Fortunately, I had just filled my gas tank the day before or else I might have joined them. Every time we were stopped by a red light one of the carpool members and I would hop out and brush the snow off the back windshield. Shortly after 10 p.m. I staggered into my apartment, cold and weary. Yes, I got to spend the day at home and was able to watch the swearing-in, but I've been afraid to do any praying about the weather ever since.

(U) John Kennedy's inauguration address included the oft-quoted line, "Ask not what your country can do for you; ask what you can do for your country." That speech and that line are the examples of Kennedy oratory that most people remember best, but the linguist in me has even more vivid memories of another JFK speech, the one he made at the Berlin Wall in

DOCID: 4009885

the Spring of 1963. The president was not particularly known for his language abilities, other than his penchant for salty language. (Oh, could that man cuss!) The linguist in the family was his wife Jacqueline, who had grown up with a French governess and was bilingual. (She studied Spanish prior to a presidential trip to South America and acquitted herself admirably in conversations with Latin American dignitaries; that fact, the way she charmed Charles de Gaulle on a presidential mission to Europe, and her remark about "mink underwear" are just about all I remember about her years in the White House.) JFK made one foray into the field of foreign languages, the so-called "Ich bin ein Berliner" speech.

(U) I've listened to recordings of that speech many, many times and the only way that I know that his German words were supposed to be "Ich bin ein Berliner" are because that's the only thing that makes sense in context; it sounds like "Ik benign b'layeh" with the "lay" drawn out for an extra syllable or two. He spoke about how in an earlier times one of the proudest statements a free person could make was "Civis romanum sum" (I am a Roman citizen)--and I must admit that he pronounced the Latin fairly well--and that since World War II "all free men, wherever they live, are citizens of Berlin, and therefore, as a free man, I take pride in the words: Ik benign b'layeh!"

(U) But just before that paragraph he made another attempt to show off a little language knowledge--and truly, a little language knowledge is a dangerous thing. He pointed out that there were people who didn't understand the issue between the free world and Communism; "Let them come to Berlin!" he added. There were others, he said, who considered Communism to be the wave of the future; "Let them come to Berlin!" Twice more he referred to people making simplistic statements made about working with the Communists. About these individuals too he said "Let them come to Berlin!" However, the last time he decided to say it in German, so he said "Lassen sie nach Berlin kommen!" (except that he pronounced it something like "Laaa-s'n zee nack Berlin common!"). The only trouble was that the three previous times he had uttered the magic words the interpreter had rendered them (more correctly) as "Sie soll'n nach Berlin kommen!"

(U) Obviously what had happened was that Kennedy had asked someone "How do you say 'Let them come to Berlin!' in German?" and that person (not necessarily a competent German linguist) had told him "Lassen sie nach Berlin kommen!" which can be translated that way if you mean "Allow them to come" rather than the modal idea of "they should [or "ought to"] come" which the President had in mind. Or it's possible that JFK had studied German in high school or college and had vague recollections of what he had learned . I have used this example many, many times to remind linguists to beware when some friend comes up to them and asks "How do you say so-&-so in Esperanto?" Oh, it sounds very nice to be able to rattle off an answer right away, but a cautious linguist will ask a few background questions, trying to find out the context, the precise shade of meaning, the people who will see or hear the words, etc., etc. If Kennedy's informant had asked to see the whole paragraph, he or she might have deduced that "Sie soll'n, etc." would have been better than "Lassen sie, etc."

(U) The story has a happy linguistic ending, though. After Kennedy had said "Laaa-s'n zee nock Berlin common!" he listened to hear what the interpreter was saying--he obviously hadn't thought to do so the first three times!--and realized that the interpreter had said something altogether different. In a quick flash of that now-famous Kennedy wit, he then said "I would like to thank the interpreter for translating my German into German!" Let the record show that the interpreter was right on the ball though, because he rendered that remark as something like "Ich will den Dolmetscher danken fuer die Uebersetzung meines Deutsches auf besseres Deutsch" (... for translating my German into better German).

(U) Let others remember John F. Kennedy for his civil rights stands, for his meetings with Khruschev, for playing touch football, or for the fact that he left the r off the end of "vigor" ("vigah") but pronounced one on the end of "Cuba" ("Cuber"?), for telling us not ask what our country could do for us, for appointing his brother to the cabinet, or for having a pretty wife. Let others remember JFK in terms of where they were or what they were doing when they learned he'd been assassinated. I may think about those things but, in addition, I assure you that I'll remember JFK for a couple of the lo-o-o--o--o-o-ongest days in my life and for those language-related incidents at the Berlin wall.

OCID: 4009885

THE MANAGEMENT BTOOL OF THE FUTURE (U)

by [redacted] P13

P.L. 86-3

If you have never heard of the "Myers-Briggs Type Indicator" (MBTI for short), you will probably be in the minority over the next few years. This psychometric questionnaire seems likely to become a new fad as a management tool; it has been exploited in a big way by the Japanese, who find it highly valuable in matching people to jobs. For this reason alone, US industries and Federal Agencies will probably use it increasingly in the near future. It is easy to administer and easy to score, and it provides an astonishing degree of useful insight into personality as it affects cooperation with others on team projects, the likelihood of success at various types of jobs, and matching up workers with the different "styles" and philosophies of different organizations or companies.

The MBTI was developed by two women, Isabel Myers and her mother Katherine C. Briggs, during the 1950s, entirely outside the mainstream of psychology. A manual was published in 1962 by the Educational Testing Service, and Myers and Briggs accumulated a large body of data by testing groups of people in a wide range of occupations and populations. Interestingly enough, in view of its current and growing popularity, this instrument remained in obscurity well outside of the establishment of personality and vocational testing for many years. Its developers were not academic psychologists; they didn't "belong to the club." In fact, the "response from organized psychology was certainly cool if not hostile" (to quote the Publisher's Foreword of "Gifts Differing."[2]. The MBTI has only begun to come into its own in the last decade, perhaps even the last five years, as more and more organizations and individuals discover its amazing usefulness.

What is the "MBTI"? It is a questionnaire which can be used to classify people by "type" along four major dimensions. It is based on Carl Jung's theory of personality (as described in his Psychological Types, first published in English in 1923). As might be expected from that remarkable psychological innovator, Jung's personality theory is unique and creative; its flavor and approach to assessing personality carves out a whole new conceptual world, totally different from other theories and assessment schemes. The MBTI questionnaire contains a list of questions eliciting the testee's preferences among various kinds of activities. It can be scored manually in seconds by a simple series of overlays with windows singling out sets of answers that pertain to each of the four main variables being measured. It provides a personality type classification in the form of four letters, for example "ISTJ", "ENFP", or "INTJ". Each of the four places in the classification code represents a choice between two possible preferences: I or E, S or N, T or F, and P or J. The letters stand for terms which seem misleading at first reading; you have to read the descriptions of the personality types, choose all four letters in various combinations, and practice applying them to friends and acquaintances, before you get a good "feel" for what they imply. Once you get the knack, however, I guarantee that you will find them astonishingly enlightening and helpful.

Here is a brief introduction to the type theory, quoted from the Myers book Gifts Differing:

"It is fashionable to say that the individual is unique. Each is a product of his or her own heredity and environment and, therefore, is different from everyone else. From a practical standpoint, however, the doctrine of

uniqueness is not useful without an exhaustive case study of every person to be educated or counseled or understood. Yet we cannot safely assume that other people's minds work on the same principles as our own. All too often, others with whom we come in contact do not reason as we reason, or do not value the things we value, or are not interested in what interests us.

"The merit of the theory presented here is that it enables us to expect specific personality differences in particular people and to cope with the people and the differences in a constructive way. Briefly, the theory is that much seemingly chance variation in human behavior is not due to chance; it is in fact the logical result of a few basic, observable differences in mental functioning.

"These basic differences concern the way people PREFER to use their minds, specifically the way they perceive and the way they make judgements. PERCEIVING is here understood to include the process of becoming aware of things, people, occurrences, and ideas. JUDGING includes the processes of coming to conclusions about what has been perceived. Together, perception and judgement, which make up a large portion of people's total mental activity, govern much of their outer behavior, because perception--by definition--determines what people see in a situation and their judgement determines what they decide to do about it. Thus, it is reasonable that basic differences in perception or judgement should result in corresponding differences in behavior." [pp. 1-2]

Here, in a very brief overview, is a summary of the meanings of different choices for the four letters of the type code or "indicator":

First letter: E (Extroversion) or I (Introversion). The introvert is a person whose main interest lies in his own "inner" world of ideas and concepts. (The term "introvert" has often been distorted or misused to mean a person who is antisocial, shy, reclusive, even neurotic; we must discard that pejorative abuse of the term in considering Jung's theory as used in the MBTI.) The extrovert is a person who directs his interest outward into the external world of people and things. A good criterion in applying this choice is to ask yourself: "Do I frequently feel tired and people-weary after a noisy party or a long day spent interacting with people?" If you answer "yes," you are probably an introvert. If you feel pepped up, raring to go on to another party or stay out all night, you're probably an extrovert. The introvert may have thoroughly enjoyed the interaction; he isn't a misanthrope. He just needs frequent "alone time" and quiet space to catch up with his own inner life and balance the partying and gadding about. The extrovert, in contrast, hates to be stuck by himself in a quiet corner. He gets bored, restless, or sleepy there and soon finds an excuse to get back out into the action. That doesn't mean, however, that he is necessarily a pushy, noisy, insensitive boor (a frequent pejorative implication of the term "extrovert" in popular parlance).

Second letter: N (Intuition) or S (Sensing). This choice defines two sharply contrasting ways of perceiving preferred by different people. Sensing people enjoy exploring the outside world through their eyes, ears, fingers, and noses. They prefer to get their data from the environment and through their senses. Intuitives, on the other hand, prefer to consult their own mental world of associations, symbols, hunches, and ideas to generate data. Sensing people are down-to-earth, objective, pragmatic; intuitives tend to be more creative and theoretical. Sensing people are interested in the past or the here and now; intuitives prefer future possibilities and leaps into the unknown. Note that a person may be an extrovert (preferring to act externally in a dynamic outer world) and also an intuitive (preferring conceptual or theoretical data from his own mind). An introvert may also be a sensing person: objective, matter-of-fact, and practical.

Third letter: T (Thinking) or F (Feeling). This dimension pertains to two contrasting ways of coming to conclusions preferred by different people. Thinking people prefer to use logic, reasoning systematically from A to B to C. Feeling people care more about values: the consequences or meanings of an act or object, and its effects on other persons. Thinking people are more interested in data about things or ideas; feeling people prefer data about human beings and human relationships. Again, we have to guard against a hasty assumption that to be a "feeling" person in this sense means to be illogical or emotional, or that "thinking" necessarily means intelligent. The words are being used here in a very special way, with no inherently good or bad implications.

Fourth letter: P (Perception) or J (Judgement). A final preference that enters into the identification of type is the choice between a perceptive or a judging attitude in dealing with the world. Perceptive people like to continue gathering data and keep their minds open as long as possible, while judging people want things settled and a decision made. Perceptives like to ride with the stream and dynamically follow it wherever it goes; they don't like things to be cut and dried. Judging people want order,

predictability, and seeing things in their proper places; they don't like things to be up in the air or undecided.

These four pairs of choices result in 16 possible sets of four letters, each having its own strengths and weaknesses in the context of certain kinds of jobs. Marriages are apt to last longer and be happier if the couple are compatible in type (i.e., with at least two letters the same and preferably three). If I am an INTJ, and I work for a boss who is an ESFP, we are both going to have some problems getting along (especially if we are sitting at neighboring desks in the same small room!) Many schoolteachers are "SJs"; they have a hard time understanding and coping with the sizable number of perceptives in their classrooms; they want order and common sense while the little "Ps" want to go with the flow and run about gathering data. And so it goes, on and on, through far more examples than I can mention here. I strongly urge anyone interested in human factors to read the two books listed as references at the end of this article and, if possible, get himself and his family "typed." You are likely to find the results amusing and interesting at the very least, and you may well also obtain some substantially useful self-knowledge.

At least one Management Course at the Agency covers the MBTI and the various implications of type in our work environments. In fact, I learned of the MBTI through a coworker who took this course and was greatly impressed by the insights he gained from it. I then took a one-day seminar from Otto Kroeger and Associates, the contractor who taught the Agency Management Course. (See the last reference at the end of this article for the full details.) The questionnaire was sent to me in the mail in advance; I returned my answers by mail, and was assigned a type by the instructors before the day of the seminar. There were about ten attendees, all of whom had been assigned a type in advance by the instructors. During the morning, we were told the history and general theory of the type indicator and the types. We also participated in some very enlightening and amusing little exercises designed to illustrate some of the implications of the types in a very vivid manner, having all the more impact since we did not yet know our types. Since the instructors knew our types, they could assign us to subgroups whose members all shared certain important letters in common. In the afternoon, after we had gone through several of these little games, we were told what our types were.

I will never forget the impact of one exercise, where we were split into three groups and told to work separately to come up with a definition of "leadership." My subgroup had four members. We sat right down and got busy, finishing our task long before the others. I was amazed at the feeling of satisfaction I had: everything went so smoothly with these people. We were all so sensible. We all were on the same wavelength, and it was a joy to work on our little team. Our definition of "leadership" included words like "practical," "objective," and "responsible." And no wonder! We all turned out to be "SJs": sensing judging types. The "NTs" (intuitive thinkers) argued long after their time was up, and their definition of "leadership" featured "intelligent" and "creative." The "NFs" (intuitive feelers) sat on the floor in a huddle; they, too, talked on past the time limit. Their definition focused on ability to communicate and get along with people. It was a revelation to me how uniquely easy and pleasant a task could be in a team of people intentionally matched by type. What benefits might we not reap in many walks of life if we could learn to make conscious and intelligent use of this tool? Perhaps someday children will learn the characteristics of the different types in school and be taught how to make the most of their own and others' predictable strengths and weaknesses. I am still amazed at how completely my own behavior, preferences, and interactions with others are described and predicted by this theory of personality. In fact, I am still discovering new insights based on my own "type" classification. Try it. You can't lose, and you might gain a lot of valuable self-knowledge.

References

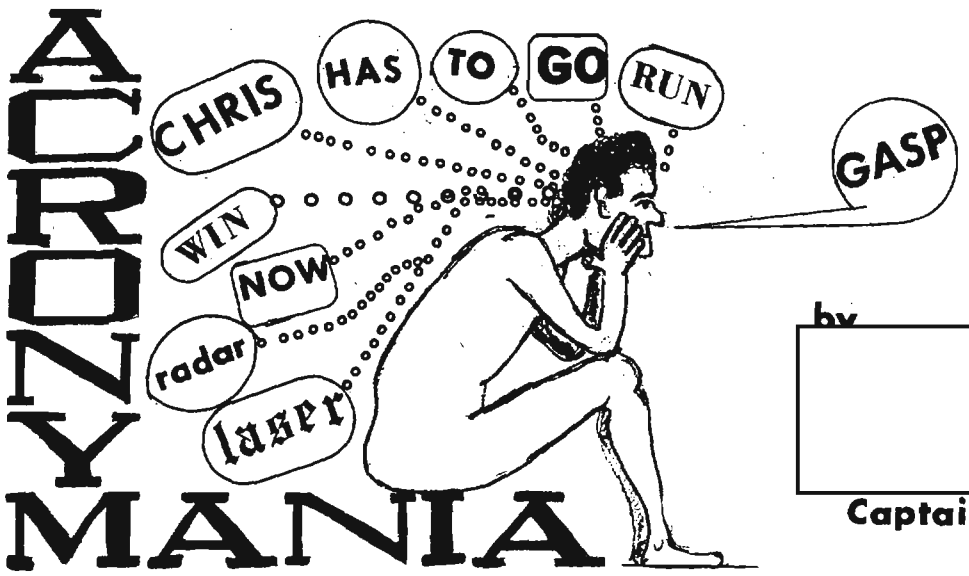
[1] Myers, I.B., Introduction to Type, 2nd edition, Center for Applications of Psychological Type, Gainesville, FL, 1976

[2] Myers, I.B. and P.B., Gifts Differing, Consulting Psychologists Press, Inc., Palo Alto, CA, 1980

[3] Otto Kroeger Associates, 1401 South Barton St., Suite 242, Arlington, VA 22204, (703) 892-4566

DOCID: 4009885

~~FOR OFFICIAL USE ONLY~~



P.L. 86-36

by

Captain, USAF
JOCCP

(U) CHRIS HAS TO GO RUN. This sentence is very innocent-looking. Although it may not be entirely correct grammatically, it is made up of words that form a meaningful sentence and has another claim to fame. All the words in it are acronyms. According to the Acronyms, Initialisms and Abbreviations Dictionary, 8th edition, 1983-84, edited by Ellen T. Crowley:

[] CHRIS = Cancer Hazards Ranking and Information System;

[] HAS = High Angle Strafe;

[] TO = Tuesdays Only;

[] GO = General Order; and

[] RUN = Reduction Unlimited.

(U) Acronyms, unlike ordinary abbreviations, consist of letters (usually initial letters of words, although sometimes two or more letters from one word will be used) that are strung together so as to form meaningful--or, at least, pronounceable--words or names. "Acronymania," as I call the practice, is sweeping America; it is especially prevalent in the military. Many military projects take on names that, most often, have some relationship to the nature of the project. One instance of this, for example, is the Navy term SWAM, an acronym meaning "Shallow Water Attack craft, Medium."

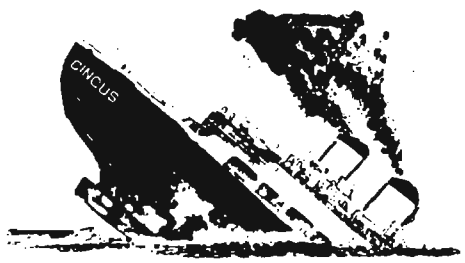
(U) The words RADAR and LASER both started out as acronyms. ("Radar" stands for "radio detection and ranging" while "laser" means light amplification by stimulated emission of radiation.") These words are used so often in normal conversation that they have both been accepted and duly listed in dictionaries.

(U) Although the military creates the lion's share of acronyms, they aren't the only users. There are plenty of acronyms employed in the civilian community too. Some of these actually fit the cause the organization represents. For example, WIN (for Whip Inflation Now) was a popular (if not infamous) button worn briefly during Gerald Ford's administration. (The button may still be seen in the halls of the National Security Agency, being worn by members of Women in NSA.) And what about the organization NOW (the National Organization for Women). The name of the organization drives home the point of immediacy. (At many of their rallies, you'll hear the shout "What do we want? ERA! When do we want it? NOW!") MADD (Mothers Against Drunk Drivers) shows the anger of the members.

~~FOR OFFICIAL USE ONLY~~

(U) Some organizations choose acronyms that point toward the danger of whatever it is that they're trying to combat. Two examples that come to mind are GASP, the Group Against Smog and Pollution) and WAR (Women Against Rape). And let's not forget SHHH, Self-Help for Hard-of-Hearing People.

(U) Comically, some acronyms can actually be confused with real words that may not even come close to the meaning intended. For example, many people refer to a "Short Takeoff and Landing" aircraft as a STOL, pronouncing the acronym an awful lot like the word "stall," which we all know is a word used to describe the condition when an airfoil is incapable of producing lift, causing the aircraft to dive. Or how about the Navy's CINCUS (for Commander-in-Chief, US), pronounced "Sink us!"?



(U) How many times have people gotten confused between NASA, the National Aeronautics & Space Administration, and Nassau, the capital of the Bahamas? You never know if the person you're talking to is discussing a current space shot or telling you about his vacation!

(U) Another case where a real word is also an acronym of unrelated meaning is SIN, which stands for the Society for International Numismatics. For those who don't have a dictionary handy, numismatics simply means coin collecting, which isn't really a sin (although the spouses of such hobbyists may think so).

(U) I was a little worried when I heard about a group on some college campuses called STOP-NSA because I thought they were trying to put our agency out of business. Boy, was I relieved when I learned that it stood for Students to Oppose Participation in the National Student Association!

(U) Of course, some people develop acronyms or see them in places where none was intended. I know several drivers who seem to think that the word STOP you see on those octagonal signs stands for "Start Tromping on Pedal."

(U) We use so many acronyms in our daily work that it's a good thing we don't carry this practice over into the world beyond the fences. Can you imagine what an everyday conversation might sound like if "normal people" peppered their speech with acronyms? It might well sound like the old "Who's on First?" routine. Just a sample of this follows.

"Hi! Are you going to study CHRIS?"

"My name's not Chris, it's Jack!"

"CHRIS is a system, stupid. It's the Cancer Hazards Ranking and Information System, and you better know all about it."

"I can't study anything now. I'm on my way to a SIN meeting."

"You mean you have to go to meetings to do that?"

"No, no, you dodo. SIN is my coin collecting organization meeting. It is held TO."

"Held to what?

"Not held to anything. TO means Tuesdays Only."

"I give up up! I'm ready to go."

"Ready to GO? How do you get ready for a General Order?"

"I didn't say 'GO'; I said 'go'! You know: depart, leave, scram, vamoose, hit the road, decamp, ..."

"Okay, but let's leave with an acronym. How about a KISS?"

"What?!"

"You know. KISS: Keep It Short, Stupid!"

DOCID: 4009885

THE WHITE HOUSE IS SINGING OUR SONG! (U)

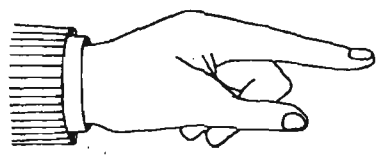
by Albert I. Murphy, E403

(U) The dynamic Lt Col Tom Murawski of the White House staff socked it to us—in a beautiful way. He presented his informative and thoroughly entertaining program on "Just Plain English" in the packed Friedman Auditorium, first on 26 September 1983 for the NSA "heavy hitters" (Grade 15s and above and the equivalent military ranks) and then on the 27th and 28th for the "at large" NSA audiences. And what a show!

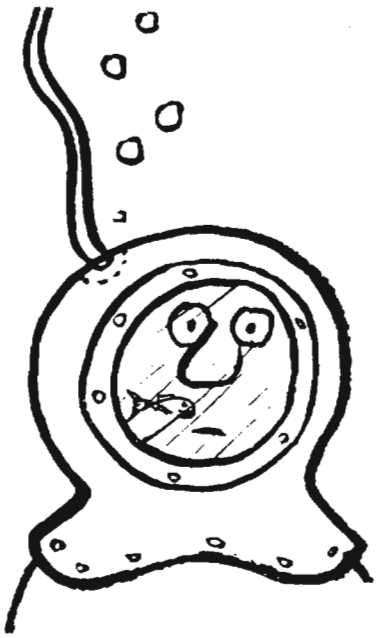
(U) In those three days he convincingly reinforced all the things we at the National Cryptologic School have been trying to do over the past several years in terms of persuading all NSA writers in general, and NSA supervisors and managers in particular, to come down to earth in their writing—to write in a way that's compact, natural, and to the point. He was singing one of our old and familiar songs, and the words came back as clear as your please.

(U) Lt Col Murawski is a tenured professor of English at the US Air Force Academy and is currently serving as an adviser on clear writing to the White House staff. His charge is to teach "Just Plain English" to the major federal agencies. That's precisely what he did here at NSA. He skillfully described the whole array of bad things that are happening in Government writing (we let him see some actual samples of unclassified NSA writings): the gobbledygook, the evasiveness (the passive voice), the bankrupt language, the inappropriate tone—all of it! And he didn't hesitate to identify the groups he viewed as the prime offenders: lawyers, educators (can you believe it?), and military people. ("You've got lots of ex-military people here at NSA," he said. "I can tell.")

(U) We were so pleased with what he had to say and at how he said it that we decided to describe some of the outstanding details of his presentation. But then we thought that, instead of doing that, we'd ask the editors of Cryptolog to republish an article from the January 1982 issue that addressed this problem in much the same way Lt Col Murawski did. The hope was that all writers at the Agency will take heed because what the article said is now strongly endorsed by this potent force on the White House staff. The editors obliged. Please turn the page.



DOCID: 4009885



THE LITERARY BENDS (U)

by Albert J. Murphy, E403

The story goes that a famous author once was approached at a cocktail party by a young aspiring writer who had in his hand a large draft of a (U) novel he had written. The young man, perhaps more brash than polite, asked the author to take the draft, read it, and suggest a title. The author, taken aback by such directness and by the size of the document, thought for a moment, then asked: "Do you mention drums anywhere in the story?" "No sir," replied the young man. "Do you mention trumpets?" Again, "No sir." The maneuver had worked. "Then why don't you call it 'No Drums, No Trumpets'?"

(U) In the business of teaching Introductory Writing (EG-022) and Expository Writing (EG-122) at the National Cryptologic School (NCS), we have encountered some rather pointed feedback from some of our students, which cannot be so easily put aside. The students talk of two worlds of writing at NSA: the ideal world of writing, as taught here at the school, and the real world of writing, as practiced on the job. Eventually, one of them will crystallize the issue by saying, "This course is all well and good. But when I finish it, I know I'm going to be faced with the decision of writing your way for the sake of good writing or of knuckling under to my supervisor's blue pen for the sake of my next promotion." Rightly or wrongly, the haunting question inevitably comes to mind: "Is his or her supervisor under 35 years old and a product of society's convulsing educational system?" We choose never to ask it.

(U) How valid are these rumblings? What is the extent of alleged shortcomings in the way people in management write (we're talking primarily about supervisors and staff editors)? And what are we going to do about it? Based on our own collection of bits of evidence, coupled with this human testimony from the students, we believe that the rumblings have some validity. But since we have neither the mandate, nor the resources, nor the time for a thorough research effort, the best we can do is to present the problem in this vehicle in the hope that the managers in question will read it and do something about it.

(U) Just before the students complete our courses, as part of a normal procedure we alert them to the post-course period of what we call "the literary bends," during which they might find it difficult to apply their newly acquired (or their refreshed) set of rules of good grammar and effective writing. "Don't be surprised," we tell them, "to find your pencil frozen in your hand or your fingers immobile at the typewriter during your first writing tasks on the job." They understand that. Some have reported that that's exactly what happened. Others have had to wrestle with the problem while still in the course. It is unfortunate, however, that we are now compelled to warn them of possible additional difficulties that can occur when a person in the supervisory chain, whether through ignorance, or obstinacy, or, alas, because of misguided pressure from a supervisor at yet a higher level, discourages the students' attempts to apply what we have taught them.

(U) If managers are willing to face up to the reality that some of their people are frustrated in their jobs because, as they perceive it, we don't practice what we preach in the field of writing, then we are well on our way to solving the problem. Perhaps, then, our message to managers ought to be

> Managers:
> By all means enforce good quality control; but in the process, please be aware of this problem, be fair with your people, and be square (that is, be traditional) with the language.

We contend that the modernists are wrong. Like it or not, there is an English Language; and it is governed by a set of rules for correct grammar, effective sentence and paragraph structure, and good writing style. Perish the thought of Congress wanting to change the words of the Constitution to accommodate modern linguistic happenings.

(U) You managers, if you are following this discourse in earnest, should be asking at about this point, "Well, what have you been telling our people in your classes?" Our answer is that we've tried to convey to them the fact that there is beauty in our language, and that the students should find it and use it. We have found that they not only are receptive to this idea, but also at times are resourceful (and not too subtle) in expressing their endorsement. You can experience intellectual beauty, we once told them, by merely pronouncing the names of tribes of American Indians, for they have a majestic quality that evokes, through vivid mental picture of frontier days, much of what is noble in the American character.

> Cheyenne...Pawnee...Apache...
> Comanche...Sioux...Shoshone--

here the students joined in--

> Mohawk...Cherokee...Blackfeet...
> Chippewa...Algonquin...Iroquois.

Then the spell was broken as quickly as it began when one of the students wistfully offered..."the Washington Redskins." We have told them about the importance of good communication, whether in face-to-face conversations, on the telephone, or in writing; and of the potential disasters of failing to communicate. We've advised them not to write without good reason. But once they've decided to write, they should spend some time thinking about what they want to say before committing their thoughts to paper. They've heard us say many times that bad writing is usually the result of poorly thought-out ideas.

Grammar, Spelling and Punctuation

(U) We have compiled an array of real-world writings from NSA in-house correspondence and CRITICOMM messages, which we contend are inconsistent with what we teach. But, in order not to raise the hackles of a lot of people, we will cite only a few that are important to the point we are trying to make, and then only when we think they will do no harm. Recently E asked various in-house elements to submit any comments they might have on an NCS course on reporting, which some of their people attended. It was a bit disconcerting when a staff editor of one of those elements, in his responding memorandum, said, "We don't need grammer in the course. We in the editing chain can handle it." Impertinent of us to mention this, you say? Well, maybe. But what about the problem of credibility? It's there, isn't it? If the element in question recognizes its handiwork here, we hope the people involved will not take umbrage but will view it in the spirit of light criticism and let us make our point. We have taught your people that

1. Dangling and misplaced modifiers are major causes of confusion in communication; to wit, "The second child, Nancy, was the only child of a mother who was divorced in her infancy"; and "If found guilty, the Division of Motor Vehicles will be notified and your license may be subject to suspension."

2. Pronouns must agree in number with their antecedents. A certain ABC television reporter either didn't do his homework or decided to go modern when, in describing a recent hurricane, he said: "Damage will be in the millions, but only one person lost their life."

EO 1.4.(c)
P.L. 86-36

3. Billy Kilmer used incorrect grammar in his beer commercial when he praised his beer for having less calories. He should have said fewer calories because few(er) is used with things you can count and less is used with things you cannot count. ("If there were fewer TVs, there would be less noise.")

4. A writer can quickly reveal himself as less than professional if he is careless with spelling. Consider the following statement that appeared in a real-world NSA CRITICOMM message:

   "SGT (John Doe) IS REQUIRED TO BE INDOCTERNATED FOR (special clearances) PRIOR TO DEPARTURE FROM YOUR STATION."

   An astute, post-publication (unfortunately) comment written across this gem facetiously noted that "This wil hep with hes clarence." Also, we've made it known that irregardless is a self-contradictory non-word, despite the regrettable fact that it is listed in Webster's New Collegiate Dictionary.

5. A comma is required before and when presenting a series of more than two items (matrix, row, and column). One of our students described in class how he was rebuffed by his supervisor for insisting on applying this rule. We suggested he have his supervisor call us to talk about it. We are still waiting for the call.

Managers:
When your people try to apply the rules of good grammar, spelling, and punctuation in their day-to-day writing, they are not trying to out-write you. They are only doing what they learned. So please--let them.

The Sentence

~~(SC)~~ Since your people are not as gifted as General MacArthur was, we have trained them not to write long, Aristotelian sentences. So, when you see them trying to limit their sentences to about twenty words or fewer (to the fullest extent that the content will allow it)-- let them. We've talked them into it. Consider the following long, but not necessarily Aristotelian, opus that appeared in an out-going NSA CRITICOMM message:

[redacted]

We suspect that a period (a full stop) might have been intended after the word producer in the tenth line, but it wasn't evident in the copy of the message we hold. Even if the period had been inserted, the latter sentence, containing at least 105 words, would still tax the patience of the reader.

(U) In order to compose good, expository sentences, our students are following the FACTS formula (the Fast, Accurate, Concise, True, and Simple way). That means they will be trying their best to use the active voice (instead of "the great evader") and a lot of concrete, one-syllable words (we just can't bring ourselves to say "monosyllabic" as opposed to "polysyllabic" in this context). We hope we have burned into their memories the Lensear Write Formula[1] which encourages short sentences, the active voice, and one-syllable words. If you ask them about it, the

chances are good they will be able to recite to you the clear and simple "something special" lead that an obscure reporter wrote on the death of Samuel Clemens in 1910, which must have caught the breath of all who read it: "Tom Sawyer and Huck Finn are orphans tonight. Mark Twain is dead!" Notice the number of one-syllable words.

(U) We encouraged your people to use parallelism correctly and wisely in their writing, to incorporate an effective blend of periodic and loose sentences, to show their maturity in the use of subordinate clauses, and to include in their list of writing "don'ts" the principle that smothered verbs (strong verbs turned into weak nouns, such as -ization, -ment, and -ure words) and passive voice constructions frequently go hand-in-hand. The poorly written sentence "The specialization of many professions is necessitated by the complexity of our society" is best recast to read "Many professions must specialize because our society is complex." The finest sentence that we've come across at the school so far, in terms of sound structure, clear and simple content, and, yes, downright beauty, was written by a student in her autobiography project. She wrote, "When I was little, my father often said that I was the best door slammer this side of the Mississippi River." Is there any wonder why we abhor the likes of the sentence "The possible appearance of a new communications network was observed...."?

Managers:
When your people try to write in clear, simple, and direct language, don't assume that they are undereducated. They're only doing what they learned. So please--let them.

The Paragraph

(U) We have practically ordered your people never to settle for a paragraph that doesn't have the standard properties of UNITY, COHERENCE, ADEQUATE DEVELOPMENT, and CONSISTENT AND APPROPRIATE TONE. Unity calls for one central idea and a single topic sentence; coherence--the paragraph form--is the writer's sequence of thoughts from one sentence to the next, which he achieves through the use of connectives or transitional words and phrases; adequate development--the subject matter of the paragraph--involves the who, what, when, where, and why, whether accomplished through definition, comparisons and contrasts, cause and effect logic, or analysis and classification; and, tone deals with not what the writer says, but how he says it.

~~(C)~~ All four of these properties, we have insisted, are essential for good paragraph structure. But the one that usually causes lengthy discussions in class is TONE. We think this is good, because it tells us that the students are trying to be sensitive to "how it will sound" to the reader by steering away from unwanted tone. So they wrestle with another set of "don'ts": "Don't be offensive ... bossy ... contradictory ... and so on."

Managers: Are you with us?

In one of our classes in Expository Writing a discussion on paragraph tone developed after we explained how the tone of separate paragraphs in a piece of writing, say in a SIGINT report, ought to be consistent with the general tone of the writing. We gave the example of reports forwarded to the NSAPAC REP VIETNAM (NRV) staff in Saigon, in 1971, by one of the ten ARVN Special Technical Detachments (ASTD), which time and again reflected a tone of absolute terror. The perimeter of the site was not secure, and the ARVN people didn't seem to care. When the reports from this ASTD came in, the staff was obliged, not without some pangs of conscience, to change the tone of the reports to fit the dispassionate, objective tone of the monthly status report within which they were incorporated for forwarding to the Director (the Vietnamization Improvement and Modernization [VIM] report). One of the students, who obviously had after-the-fact sympathy for the plight of the writers of those reports (US soldiers assigned to the ASTD), questioned the changing of the tone. After we explained some of the unpleasant realities of the situation (we also apprised her of her handicap as a caring human being), she conceded that the tone of that ASTD's reports had to be changed and that our point on consistent and appropriate paragraph tone was well taken in the class.

DOCID: 4009885

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

Gobbledygook

(U) We have described to your people in considerable detail the perennial enemy of good writing, namely gobbledygook or federalese--the old obscure writing that is usually meant to impress rather than to express. We have convinced them (we hope)

(1) that it is foolish to use high-sounding words, such as utilize, implement, initiate, viable, optimum, and terminate;

(2) that roundabout expressions, such as "It is believed..." and "There is/are..." make for weak writing because they tend to repeat, they are often vague, and they leave the reader with no way of knowing what is meant, thus forcing him to work for nothing;

(3) that we condemn the use of the expression "It is felt that..." because it has three inherent strikes against it--it is roundabout, it is passive, and it is false (one doesn't feel an argument or a contention; one thinks it or one believes it);

(4) that circumlocutions, such as "Owing to the fact that...," "Concerning the matter of...," and "In reference to..." are nothing more than deadwood; and

(5) that illogical, incongruous, or inappropriate metaphors should be avoided.

After analyzing the following real-world statements, we couldn't come up with a reasonably good answer to the question, "What happened to the quality control system?"

"The state of the art, as it exists today...."

"It's a sad day of affairs...."

"(We should be) starting out with a clean foot." (Let's call this one a combined, instead of a mixed, metaphor.)

Those gems are not any worse (or, if you like, any better) than the Golden Oldies taken from letters received at a welfare department in Tennessee some years back (you old-timers might remember them):

"I am very much annoyed to find you have branded my son illiterate. This is a dirty lie as I was married a week before he was born"; "Unless I get my husband's money pretty soon, I will be forced to live an immortal life"; and "I am glad to report that my husband who is missing is dead."

~~(S)~~ [redacted] We also shudder to think of the possible unthinkable consequences of gobbledygooked guidance (from NSA) and gobbledygooked responses (from field elements) on matters about current developments in the world in general and in Eastern Europe and the Middle East in particular. The solution to NSA Crostic No. 35 (Cryptolog, October 1981) contains a poignant comment from [redacted] Plain English that aptly supports all we've been trying to say here. P.L. 86-36

> If we want all Agency personnel to speak and write plain English, perhaps we should first teach Agency personnel English. If we want Agency management to write concise, active, decisive memos, perhaps we should first teach Agency management to be concise, active, and decisive. Let us attack the problem, not just the symptom.

(U) Having stated our case, we fully intend to continue to orchestrate drum rolls and trumpet blares for the cause of getting managers to cooperate in making clear, simple, direct, brief, and appropriate writing happen at NSA.

(1) Gobbledygook Has Gotta Go, U.S. Department of the Interior, Bureau of Land Management, page 7; US Government Printing Office, 1978, 0-269-955.

DOCID: 4009885

CIRCA 1949:

Reminiscences of an Intercept Operator (U)

[redacted]

P.L. 86-36

[redacted]

EO 1.4.(c)
P.L. 86-36

OCID: 4009885

~~FOR OFFICIAL USE ONLY~~

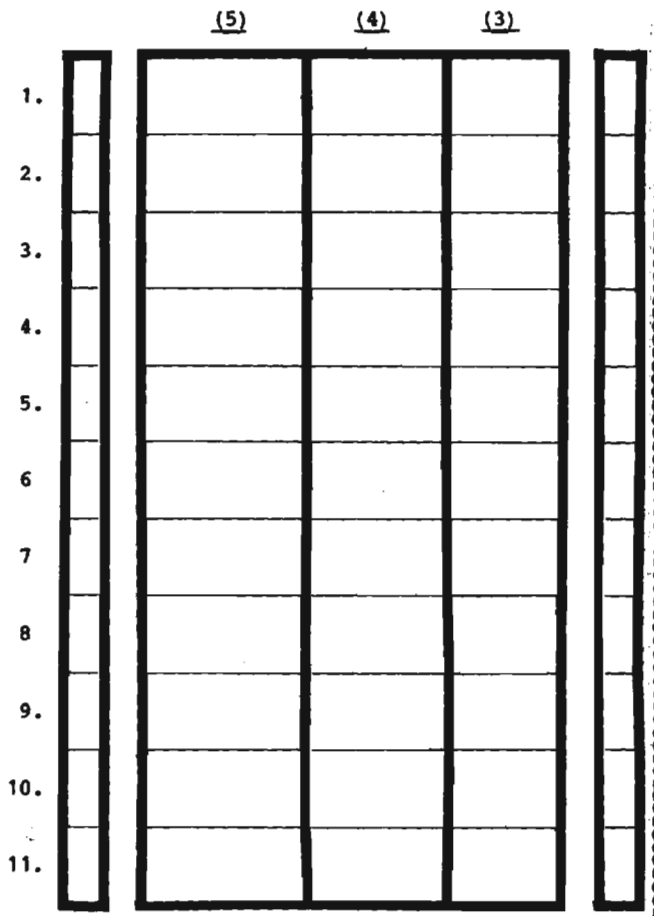
5-4-3 PUZZLE (U)

by
'WATT ZIZNAME,' P1

In the diagram below each row is divided into 5 unequal segments, the center 3 of which are labeled (5), (4), and (3). The digit in parentheses tells you how many letters there are in the word being defined in the list of DEFINITIONS in the right column; each group of explanatory terms has a number corresponding to the row of the diagram and a subsort showing the number of letters in the word being defined.

When you have figured out the 5-letter word being defined, write it in the appropriate box under the (5). Now try to find a 4-letter word that matches the (4) definition given and uses four of the five letters in the word you just wrote. The letters can be rearranged. Now take the omitted letter and write it in the small square on the left end of the appropriate row. Next, take 3 of those 4 letters to make a word that matches the (3) definition, putting the dropped letter in the square at the right end of the row.

If you've found all the correct words and picked out all the right letters, when you read down the column of boxes on the left and then the right, you should see that the 22 letters you've written in those squares spell out a 3-word phrase that should be familiar to you. (The second word is divided between the bottom of one column & the top of the other.)

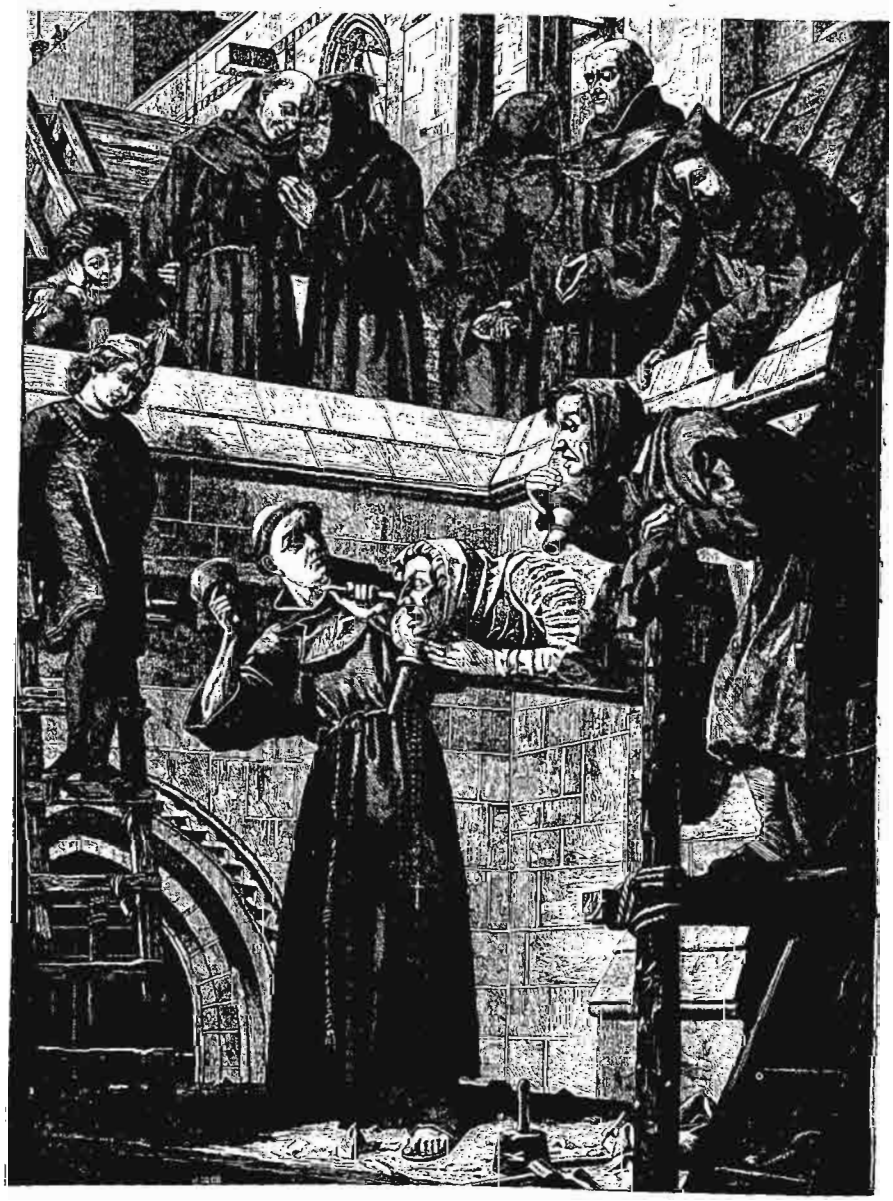


(The solution will appear in the next issue of Cryptolog.)

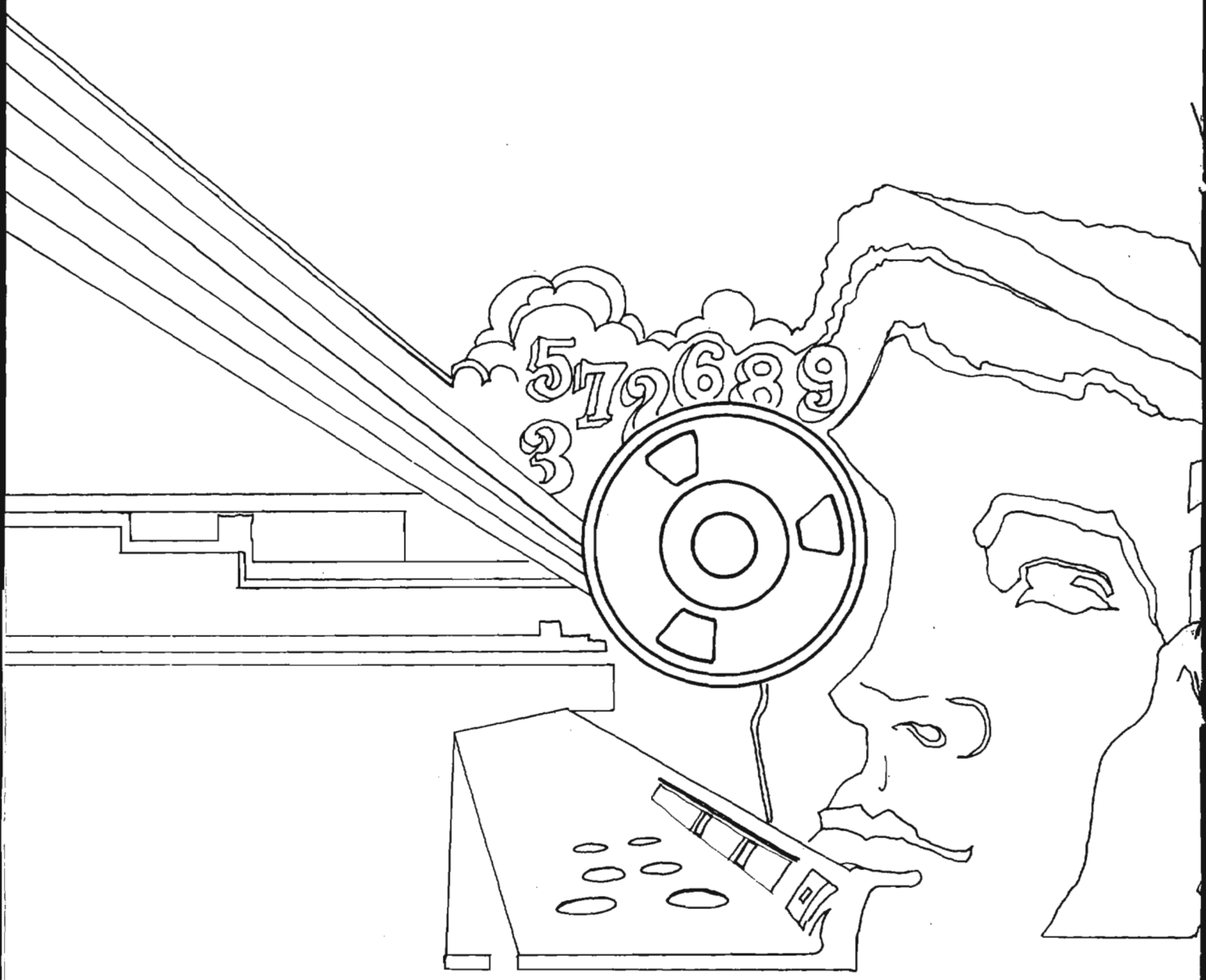
DEFINITIONS

1. (5) beneath; (4) description of the bridge that arched the flood; (3) color of blood; a Square in Moscow.
2. (5) seat; presidency; (4) wealthy; (3) "____ bin ein Berliner!"
3. (5) malice; (4) mince & lemon meringue, for example; (3) between Aug & Oct.
4. (5) Gertrude of "Rose is a rose is a rose is a rose" fame; (4) word after "love" or before "egg"; (3) Latin being.
5. (5) actor Charles or ballplayer Cletus; (4) stable for cows (a Briticism); (3) Johnny _____ , Confederate soldier.
6. (5) what Rembrandt and Titian did and used; (4) Middle Eastern pocket bread; (3) form of bribe allegedly "to insure promptness" that Ambrose Bierce described as "salary we pay to other people's help."
7. (5) raised platform on which performances are presented; kind of coach; (4) obtains; (3) "Ready, ____, go!"
8. (5) Joseph Conrad, Lech Walesa, Madame Curie, and Pope John Paul II among others; (4) sit for an artist; (3) a piece of bread or other food soaked in milk or broth before being eaten; gift for Cerberus.
9. (5) Greek mythological creature, half human & half bird; police car adjunct; (4) strap for making a horse go "Whoa!"; (3) anger.
10. (5) length of a boxer's extended arm when throwing a punch; (4) part of the foot; kind of bishop; curvature; (3) short cheer; Hur's last name.
11. (5) Jones the engineer; (4) affirmative votes; (3) Black, Red or Yellow.

~~FOR OFFICIAL USE ONLY~~



What Is The Caption?


5 7 2 6 8 9
3

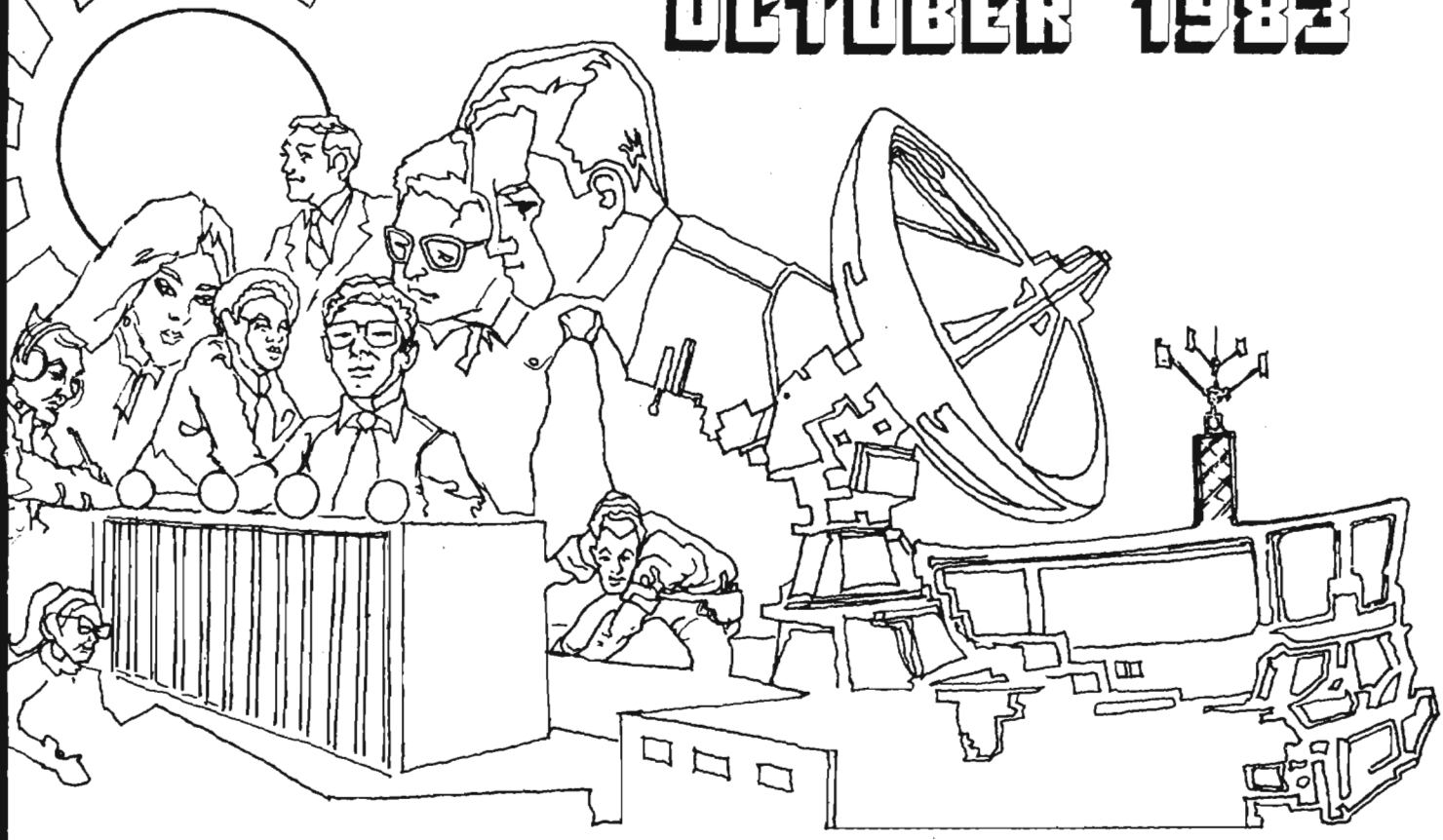
DOCID: 4009884

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

OCTOBER 1983



P.L. 86-36

CRISIS MANAGEMENT: REMARKS (U) ..... Lincoln D. Faurer 1
SOVIET MILITARY GOALS AND THEIR EFFECT
ON NEGOTIATIONS FOR ARMS LIMITATIONS (U) .... [redacted] 2
TIPS ON TOPICAL REPORTING (U) ..... [redacted] 4
THOUSANDS MISS DEMONSTRATION (U) ..... [redacted] 6
LOOKING AROUND: TELECOM 83 (U) ..... [redacted] 12
BANNNERS, COWBOY HATS,
AND ELINT NOTATIONS (U) ..... [redacted] 16

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

OCID: 4009884

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. X, No. 10 OCTOBER 1983

PUBLISHER [redacted]

BOARD OF EDITORS

Editor..... [redacted] (963-3045s)
Asst. Editor... [redacted] (963-1103s)
Production..... [redacted] (963-3369s)

Collection..... [redacted] (963-3961s)
Computer Security
..... [redacted] (968-7313s)
Cryptolinguistics. [redacted] (963-1103s)
Data Systems..... [redacted] (963-4953s)
Information Science
..... [redacted] (963-5711s)
Mathematics..... [redacted] (968-8518s)
Puzzles.....David H. Williams (963-1103s)
Special Research.....Vera R. Filby (968-7119s)

For subscriptions
send name and organization

to: [redacted] P14
(963-3369s)

P.L. 86-36

To submit articles or letters by mail, to: P1, Cryptolog

via PLATFORM mail, send to:
cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no 'O' in 'log')

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

One of the things that is often missing around here is some time to stop and just think a bit about what we are doing. We don't always do that as often as we should. As I begin my third year as editor, it seems to be a good time to pause and reflect about the magazine.

My strongest impression is that the magazine is really the result of the collective efforts of a lot of people. Responsibility for whatever success the magazine has enjoyed must be shared by many.

My predecessors, who built up a going publication process, deserve much of the credit. Building on someone else's work is a lot easier than starting something from scratch.

Then there are those who help during the publication process from manuscript to the final printed and distributed copy that lands on your desk. Without all these friendly folks, we would never make it.

There are the many people who provide the articles, letters, and various items that fill our pages. Over the last decade, most of the in-house technical periodicals have stopped being published, often for lack of material. That has not been a problem for CRYPTOLOG and so I must acknowledge our continuing debt to the authors.

Ultimately, of course, it is you the readers who keep us going. You are a taciturn bunch, I must admit, but you do manage to convey your interest and your appreciation. Without that, there would be little need for the magazine.

WED

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009884

A Few Words About CRISIS MANAGEMENT (U)

from LT. GEN. LINCOLN D. FAURER, Director, NSA/CSS

Director's Remarks on the opening of The Communications Analysis Association (CAA) Symposium on Crisis Management on 24 October 1983

(U) Good morning! I'm pleased to join you in kicking off this symposium on crisis management. I am proud of our agency's Learned Organizations; they permit us to stay in the family while removing ourselves from normal work structures to pursue professional interests.

(U) I would like to make it clear at the outset that I am not an advocate of the "crisis style of management." To the contrary, if we are to cope adequately with the many crises which come our way, we must actively plan and prepare ourselves to deal with a great variety of crisis scenarios.

(U) In the coming week you will be looking at crisis management on a couple of different planes. On one plane, you will be learning how crisis management looks from the vantage point of national policy and decision makers. As we better understand what they need in their efforts to keep bad situations from getting worse, we should be able to provide more useful SIGINT support.

~~(C CCO)~~ On a second plane, you will be looking at how we in this Agency operate in times of crisis to provide that SIGINT support. I think it is appropriate that the Communications Analysis Association, a multidisciplinary organization, has sponsored this examination of crisis management. It is appropriate since our response to every crisis is inevitably a multidisciplinary response. Linguists, cryptanalysts, traffic analysts, signals analysts, and intelligence research analysts all play an important role in every flap. In addition, all kinds of support activities play essential roles. We couldn't begin to do the job without the communicators, engineers, computer operators, and all the others that make our complex production efforts possible. This Agency, more than any other, spends most of its time in a "crisis" posture.

(U) I urge you to take advantage of the opportunities this week will provide to learn more about crisis management and our important role in that process.

EO 1.4.(c)
P.L. 86-36

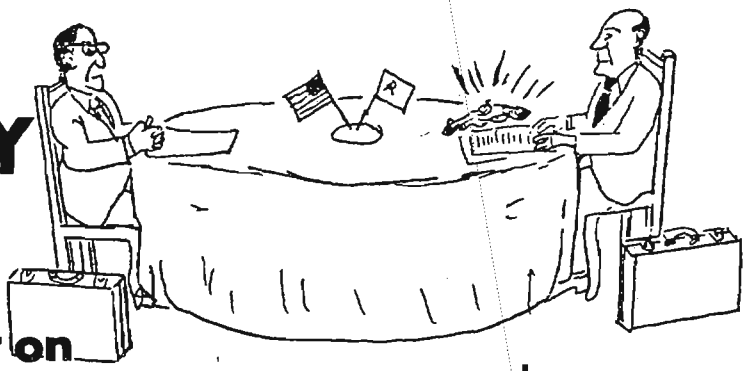
~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4009884

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

SOVIET MILITARY GOALS and Their Effect on Negotiations for ARMS LIMITATION(U)



by

S243

The Soviet Union has used SALT and START negotiations to achieve long-range military goals and to advance its foreign interests. Soviet military goals emphasize border defense through control of neighboring countries, increased influence abroad, and quantitative superiority in military hardware. Whether negotiations or military planning concerns intercontinental ballistic missiles or tanks, the Soviet objective is to end up in a position of strength.

Soviet military planning combines the use of conventional and nuclear warfare to maintain control of the conflict. The Soviets view limited nuclear warfare as a means to hold positions, resupply, contain the enemy, and continue fighting to victory.

One Soviet long-range military goal has been the development of a modern navy. The US naval blockade during the Cuban missile crisis of 1962 is probably the most recent event which showed the Soviets the importance of a strong hardware base, particularly in naval vessels. US Navy units prevented a weak Soviet Navy and merchant ships from docking in Cuba. Unable to break the blockade, the USSR was forced to withdraw its nuclear missiles from Cuban soil. After the conflict, Soviet foreign policy changed to emphasize protection and expansion of its foreign interests. The Cuban Missile Crisis was the last time the Soviets backed down under foreign pressure.

The USSR arrogantly expresses its intention not to allow any outside power or world opinion to affect its foreign policy. Since the 1960s the Soviets have been on a program of constant military hardware building and personnel training, which has only recently showed some signs of diminishing. This tapering off reflects a quantitative advantage gained in a modern navy, tanks, nuclear missiles, and NBC (nuclear, biological, and chemical) equipment and training. The Soviet leadership's lack of concern about world opinion is exemplified by the invasion of Afghanistan and the use of chemical weapons there, as well as by its control of Eastern Europe, particularly Poland.

History has taught the Soviets that tactical surprise and swift troop movement are advantageous in military operations. They admired the rapid troop movements of the Nazi blitzkrieg in World War II and adopted this concept into their military operations. Motorized infantry units and extensive long-range airlift operations during the invasion of Czechoslovakia and Afghanistan are examples of Soviet adaptation of the blitzkrieg concept. In both these invasions the Soviets transferred large numbers of troops and enormous quantities of equipment and supplies in a short period of time. Armor and motorized infantry, supported by bombers and fighter aircraft, are the cornerstone of a Soviet invasion. Tactical goals are to capture and control territory and to surround heavily defended areas. Infantry, artillery, and missiles are used to destroy trouble spots.

~~FOR OFFICIAL USE ONLY~~

Eastern Europe and virtually all the northwestern section of the USSR are well protected by ground, air, naval, and strategic rocket forces. These forces offer a manmade barrier for a border with no natural obstacles. Soviet and Warsaw Pact forces counter NATO and are trained to prevent foreign troops from entering Soviet territory. In negotiations for arms limitations the Soviets attempt to increase their military forces' quantitative gains. They have made reductions only by mothballing older military hardware.

During arms negotiations the Soviets attempt to block implementation of new Western hardware while maintaining their hardware production levels. The Soviets project a superficial appearance to the world of wanting to reduce their levels of military arms. In reality, their objective is to wear down the opposition, using to their advantage world opinion, debates, and demonstrations against any Western arms buildup. The delay in implementing production of the United States' B1 bomber and the MX missile has assisted the USSR in its goal of maintaining a quantitative advantage in strategic weapons. With the production of modern military hardware, including titanium-hulled attack submarines, SS-20 missiles, and FOXBAT long-range bombers, the Soviets have caused the West to reevaluate its strategic defense policies. The Soviet military buildup has caused some Western nations to espouse neutrality in the event of war. Other nations are experiencing internal conflict over how to counter the Soviet military gains. Debates and demonstrations in the US, UK, and West Germany have given the Soviet arms reduction propaganda some credibility and sympathy.

START negotiations will be lengthy and will be criticized as being favorable to the Soviets. An arms limitation agreement will assist the USSR in maintaining a desired quantitative advantage. For example, even if an agreement is made not to place MX missiles in Europe and to remove all Soviet SS-20 missiles east of the Urals, the Soviets would gain. The mobile SS-20s can move into Eastern Europe with little or no warning.

The Soviets are virtually silent about the START negotiations; the West is experiencing debates and demonstrations. Soviet SS-20 missiles are in Eastern Europe; the MX missile is still on the drawing board. Comparison and contrast of Soviet and Western strategic positions lead to an argument about who is superior. The Soviets have progressed from a position of military inferiority to one of equality and, in some cases, superiority over the West. All the Soviet military goals have not been met. However, by using the arms limitations talks, world opinion, and Western desires to end the arms race, there is no reason to expect that the Soviet Union won't meet these goals.

Dear Editor:

Ref [redacted] article on "Management of Coordination." I hope that when the person mentioned on page 8 told him that there are "only two Os in 'coordination,'" he had the presence of mind to point out that there are three Os in "cOOrdinatiOn"!

P.L. 86-36

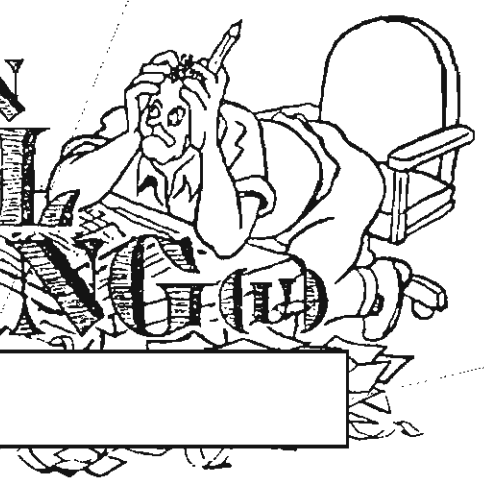
Juan Tuthri

DOCID: 4009884

~~SECRET~~

EO 1.4.(c)
P.L. 86-36

TIPS ON TOPICAL REPORTING (U)



BY [redacted] P.L. 86-3

These few suggestions stem from a presentation the author developed for a National Cryptologic School course [redacted] ~~(C)~~ Having incorporated some minor changes, he believes these tips can be helpful to analysts working on any military problem at NSA.

BE FAMILIAR WITH FORMAL SIGINT REQUIREMENTS

~~(C)~~ These can be found in the National SIGINT Requirements Lists. While important to know, these requirements generally are not crucial in deciding what topics are reportable; almost anything that sounds significant or interesting in a military context is covered by at least one requirement. Furthermore, more often than not there are several requirements in each list with identical priorities, so a person should develop other analytical tools for judging the worth of topics encountered in military traffic. Basically, as intelligence specialists, we need to focus on gems of good information, not overlooking the fact that gems are often found in low-grade ore.

TRY TO KEEP CURRENT WITH UNCLASSIFIED MILITARY LITERATURE

(U) This advice applies especially to magazines but also to books. NSA keeps most important magazines and new books on file in the main library or in specialized technical collections, kept in other locations in the building, in the case of foreign language publications.

(U) No one, of course, can expect to keep track of everything military writings can cover. but a broad knowledge is extremely helpful in defining the issues of real importance in your own mind. Find out what our military brass is thinking. Don't neglect openly available material from Warsaw Pact or other target country sources, either; even the titles of articles can say a lot. Yes, this takes time, perhaps even some personal time reading at home or time which might be deemed "wasted" plowing through thick read files, but this can pay off big sometimes. Consider this as your basic research, very similar to what is expected in every facet of work done in the scientific community.

IDENTIFY THE AREAS OF PRIMARY CONCERN AMONG MILITARY THINKERS AND PLANNERS AT THE PRESENT TIME

(U) This practice has its dangers, though. The tendency in any field of endeavor, but especially in military circles, is to grab a "hot topic" and run with it, neglecting some of the basics that need continuous attention. This often happens when new weapons systems are coming on line. Granting that, intelligence reporters can "make a lot of money" for their organizations by reporting on those current high-interest topics if information becomes available on them; you can be sure any such report, or a briefing based on it, will be received much more avidly by our users than our more run-of-the-mill products.

~~SECRET~~

INFORMALLY PRIORITIZE THE SUBJECTS OF GREATEST INTEREST AS YOU TAKE A LOOK AT THE TRAFFIC IN YOUR CURRENT PROJECT

(U) The National SIGINT Requirements Lists are only general guides to themes of continuing interest, but they cannot stay as current as an analyst who is really on the ball. Sure, there is always the old excuse of too much to do in most offices, where workers slog through piles of traffic that need some sort of attention. But priorities are ultimately set by the same military thinkers whose writings, interviews, and concerns you have been reading about. Get the current priorities straight in your own mind, and you are a jump ahead in the game of producing relevant intelligence.

EO 1.4.(c)
P.L. 86-36

DEVELOP A SPECIALTY

~~(S)~~ There are many generalists among analysts at NSA who know a little about a lot of things. However, it is encouraging to know that with not a great deal of extra effort you can get to be the recognized expert, if you please, in your office or maybe in all of NSA about one or two areas of military knowledge.

[redacted] Receptiveness to new areas of learning is all that is necessary for such a new status; it has nothing to do with grandstanding or empire building.

ACTIVELY SEARCH FOR SOURCE DATA WHICH CAN PROVIDE ANSWERS FOR QUESTIONS ON USERS' MINDS

(U) Unfortunately, we very seldom get transcripts or printouts in which reportable information sort of leaps from the page in a neat, logical, and complete format. When that happens, those writing it up become mere translator-reporters. Translation and reporting are both necessary skills but hardly the stuff from which analytical breakthroughs are made. True analysts are those people who recognize clues and subtle hints in otherwise unintelligible, fragmentary data and manipulate that information into a story of useful intelligence. But analysts have to do their homework, and not just by signing up for more formal classes.

BUILD A NETWORK OF FELLOW ANALYSTS

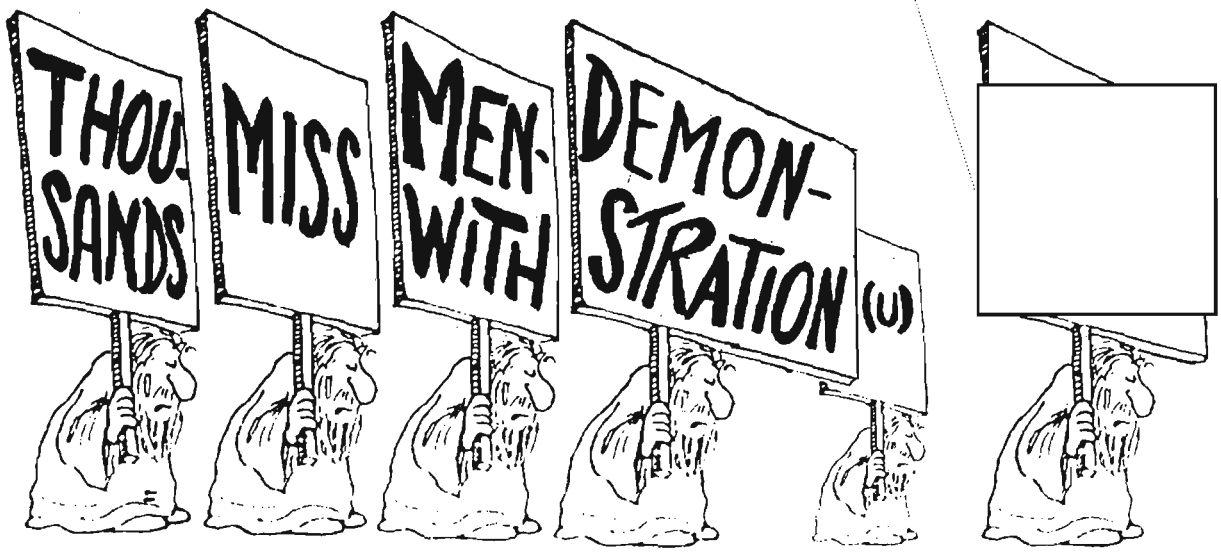
(U) No one can do it all alone. Even competent loners need some help in producing accurate, comprehensive reports. A handy shortcut in research is using the knowledge stored in other people's heads or personal files. Remember, though, that networks require give and take to be effective. Be prepared to share your own expertise with others, within the limits of special clearances and need to know. Fellow analysts also can help you avoid going out on a limb and saying something stupid before your report hits the editors or gets to the formal coordination process.

DON'T OVERLOOK HISTORICAL DATA WHEN WRITING ABOUT THE PRESENT OR PROJECTING TRENDS INTO THE FUTURE

~~(C)~~ Many of us can get so wrapped up in the here and now of intelligence reporting that we neglect to dig into the past. Many old reports, for instance, have a wealth of essentially raw data which was reported "as is"--and rightly so, it should be added--because at that time whoever was working on the problem did not have a complete understanding of some particular aspect. Let's digress a moment to consider an important point. We need to put details into our event and topical reporting for precisely that reason. (This can be done without letting a report degenerate into a formless mass of undigested data.) Reports don't get lost as easily as traffic over the years, and those details can be a gold mine for future analysis of a particular topic. Of course, old traffic should not be neglected if it is possible to make a pull that zeroes in on the topic being developed, especially if an analyst is on to something really hot.

MAINTAIN A HEALTHY CURIOSITY AND DON'T BE AFRAID OF INITIATIVE

~~(C)~~ I saved the most important point for last. As you know, we are working in a big bureaucracy here that seems quite impersonal at times. As long as we choose to remain NSA employees, we'll have to live with that fact. But don't let the bureaucracy become an excuse. That spirit of curiosity, that propensity to delve into new territory, can not only be kept alive but flourish in our business, which, after all, thrives on being snoopy. Many of you would be surprised, too, at how much say an individual analyst has in what he or she reports. Sure, there are always regular demands placed on our time, including things we are specifically ordered or expected to do, but don't hesitate to make noises and try to convince people on up the line that something needs doing if you smell something important in the target you are examining. And don't give up if a pet project gets quashed for some reason. There is always something else to report. Good intelligence comes from dedicated individual analysts dredging up good stuff buried in trivia, not by supervisory decree. Besides, satisfying curiosity and coming up with something new are just plain fun.



"Thousands Miss Menwith Demonstration." So headlined the account of the 4 July 1982 protest at Menwith Hill Station published by the local newspaper, The Harrogate Advertiser. (U) Indeed, the day's events were anticlimactic for those concerned with protecting the Station and discouraging for the protest organizers who attracted less than 10% of the expected 20,000 marchers.

~~(C)~~ By now, Menwith Hill Station might be the most protested-against NSA/CSS facility in the world. From time to time over the past 16 years, small groups have appeared at the front gate supporting a wide variety of causes. Since mid-1980, however, the tempo and the intensity have increased markedly, and we have had to organize ourselves to handle these demonstrations.

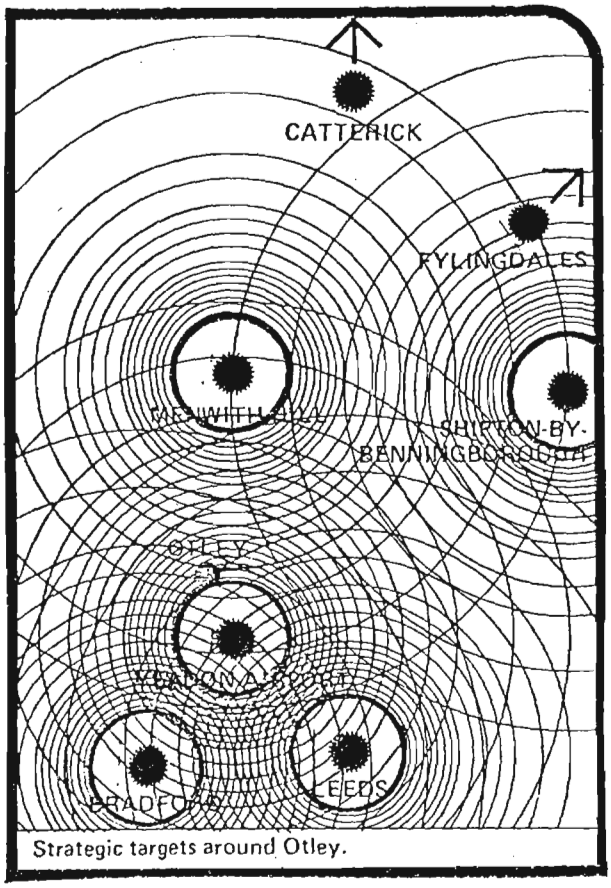
(U) The renewed interest in Menwith Hill was sparked in March 1980 by Duncan Campbell, a British journalist who writes frequently for the New Statesman, a left-oriented magazine. Campbell had previously exposed the British Post Office's "Tinkerbell" operation in which domestic telephones were allegedly being tapped and had caused a major debate in Parliament. In his new article and in subsequent television interviews, Campbell made three points:

- [] that since he had made the British Government stop tapping UK phones, it was obvious the Government had to get someone to do it for them;
- [] that NSA intercepted international lines and Menwith Hill was an NSA station; and
- [] that Menwith Hill was situated near and hooked into Hunter's Stone Tower, a major British Post Office microwave relay tower and was therefore tapping British telephones as well as international lines passing into and out of the UK.

(U) Campbell's accusations were picked up by the British national and local (as well as the US) press in July. The immediate direct response was a very small demonstration by college students from Bradford in the summer of 1980, a few letters to the editor, and follow-up stories in the local Yorkshire newspapers. Considering the potential hostility towards the Station these stories could have generated, we considered ourselves fortunate with so mild a reaction. (The British press plays by different rules: Any accusation is assumed to be true unless specifically denied, and a "No comment" is often treated as a confirmatory statement.)

(U) The publicity apparently then attracted the renewed attention of the Committee for Nuclear Disarmament (CND), one of the largest protest organizations in the UK. CND had selected the "target" theme as the basis on which to organize anti-US demonstrations, usually centered on the Cruise Missile deployment. The target there was well summarized in the December 1980/January 1981 issue of Sanity, the national CND magazine:

"We are a target
because we have nuclear weapons;
"we are a target
because we are an American base;
"we are a target
because we are involved in the NATO Alliance;
"and if we are a target we can't survive."



Strategic targets around Otley.

Figure 1

(U) By early 1981 Menwith Hill was almost an incidental in the national organization's strategy. Far more prominent was the exploitation of a Civil Defense exercise run by the British Government in the fall of 1980. "Square Leg," as the exercise was known, had identified the cities of Leeds and Bradford as Soviet nuclear targets in the event of war with the Soviet Union. When CND literature described the effects of a 5-megaton bomb dropped on Leeds or other nearby targets, Menwith Hill was but one of many targets. (See illustrations 1 and 2.)

(U) However, by early 1981 the local Yorkshire CND had begun to plan a major demonstration directed against Menwith Hill Station. The "target" theme was by now narrowing down to US facilities in the UK with no mention being made of the obvious British "targets," such as RAF Catterick, HMS Forest Moor, or Leeds. When a British base was mentioned, it was only in the context of the base serving American purposes. For example, RAF Fylingdales was described in The Harrogate Nuclear Handbook, published prior to the 4 May demonstration, as "... a crucial link in the U.S.A.'s Early Warning System. This 'Early Warning' would come too late for the U.K." Illustration #3, taken from the Harrogate Nuclear Handbook, demonstrates how the British targets disappeared from CND literature in favor of US targets.

(U) The "target" was further narrowed by the spring of 1981. The issue was now to close down Menwith Hill Station on the premise that if war should break out the Russians would not bomb Yorkshire if there were no Americans there.

(U) This approach can be illustrated by a letter to a local paper by Bob Wilkinson, a member of the New Communist Party in the UK. Wilkinson, who actively assisted in organizing the 4 May 1981 "Peace Picnic" and who later organized the 4 July 1982 "Menwith Hill Picnic," wrote:

> "Our 'allies' have probably their most crucial major retaliatory target eight miles from Skipton, at Menwith Hill. This remarkable top secret base is run by the highly secretive U.S. National Security Agency. Menwith Hill Station, with over 800 employees working round the clock to gather military, political and economic intelligence, is the biggest communications tapping center in the world--reflecting Britain's strategic position in the U.S. world communications network...

"It is the PRIME target for any nuclear strike after an American 'first strike' from a Cruise or Pershing missile ...

"In the interests of the only possible means of survival for the human race there is to be a Peace Picnic at Menwith Hill on May Day. ... Let us put aside all that divides us. Now is the time to act together."

(U) Over 6,000 people marched past Menwith Station on 4 May 1981 behind a very wind-blown banner proclaiming:

CLOSE MENWITH HILL
GIVE PEACE A CHANCE
NUCLEAR-FREE YORKSHIRE

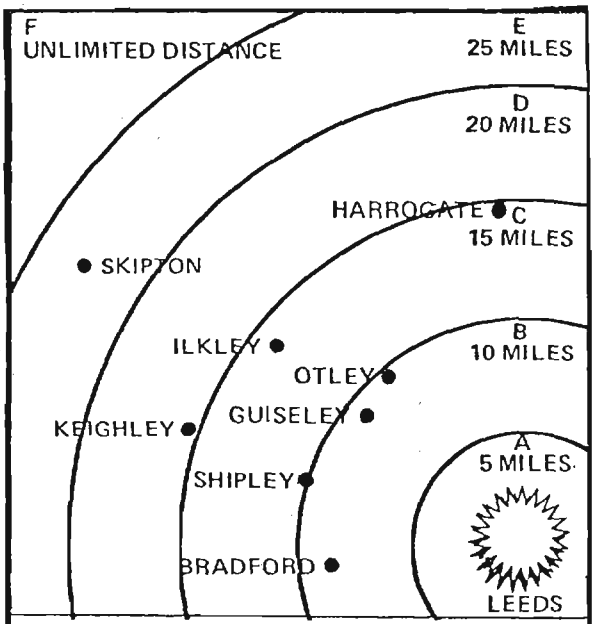
(U) In a nearby field they heard speeches, including one by the Labour Member of Parliament for Keighly, Mr. Bob Cryer, who was the one major "name" attraction present. (Early in the organizing promotion, it was reported that actresses Julie Christie and Susannah York would be present. They were not.) The demonstration was large, peaceful, and successful in drawing media attention. At the close of the day, the organizer said the protesters would return every May Bank Holiday until Menwith Hill was closed down.

(U) There was local opposition to the demonstration. The Harrogate MP condemned it, the Bishop of Ripon refused to become involved, and the parish priest from the organizer's hometown urged a Catholic boycott. One local farmer even managed to "muck" the adjacent field during the speech making.

(U) Following the demonstration, Menwith Hill dropped out of the news. CND actions were concentrated on so-called peace camps at the gates of major USAF bases in the south and the Midlands. On 26 February 1982, after six months of quiet, Menwith Hill hit the front page of the local papers under the headline:

35,000 Target at Menwith "Peace Picnic"

(U) Subsequent articles reported that Bob Wilkinson, the chairman of the organizing committee, had scheduled a massive demonstration during the Station's Independence Day celebrations on 4 July 1982. Significant trade union support was claimed and the national secretary of CND was to be the featured speaker. "Our sole aim," Wilkinson was quoted, "is to get the base closed."



The predicted effects of a 5 megaton bomb exploded over the centre of Leeds.
A Buildings completely destroyed

Figure 2

~~(C)~~ By mid-March, there was a renewed emphasis, perhaps coincidentally, in the tabloids on the number of US bases in the UK. One article began: "Britain is just an aircraft carrier for America's fighting machines in Europe, it is said--a giant parking lot for their strike aircraft, nuclear bombs and spy planes." Probably the CND campaign would have brought substantial publicity to Menwith Hill, but the Station was soon thrust back into sensationalized stories when James Bamford began his publicity campaign for his exposé of NSA, The Puzzle Palace. Bamford's first disclosures concerned the NSA-GCHQ relationship with emphasis on NSA's "Minaret" operation between 1967 and 1973 and GCHQ's assistance therein. There followed a series of articles, including one by Duncan Campbell's associate Linda Melvern, about Anglo-American intelligence cooperation. Menwith Hill received its share of attention in these articles.

(U) The phone-tapping stories reappeared, and were coupled with the "target" theme, which continued to be the main point of emphasis. The Leeds Other Paper published by Leeds Alternative Publications Ltd, (self-styled as a "Trade Union and a worker's cooperative") merged the two themes in its 16 April 1982 issue:

"The Effects Of A One Megaton (airburst) Nuclear Bomb Over Menwith Hill."

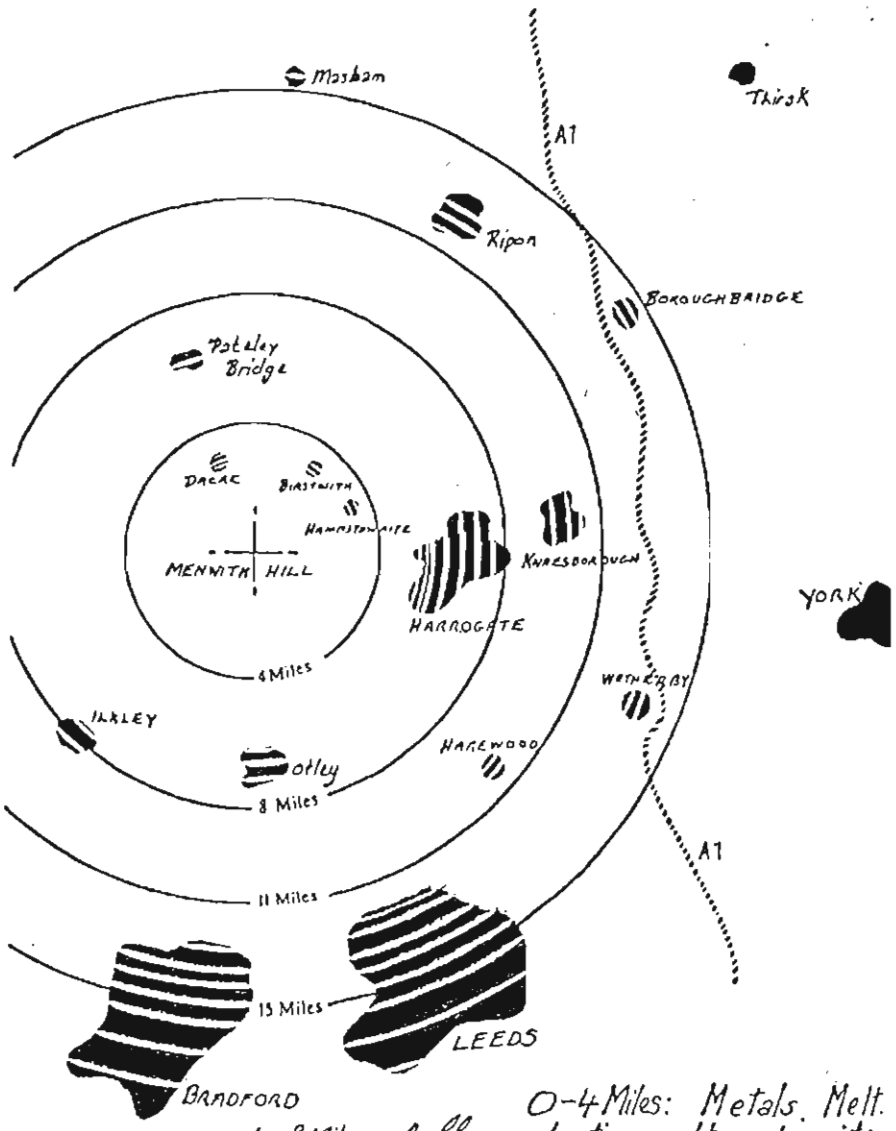


Figure 3

"Council Leaders George Mundie (Leeds) and Derek Smith (Bradford) are giving their support to the picnic. 'Our support for this campaign is twofold. Firstly, we must accept and believe that it is a nuclear target and as such must be removed from our country,' said George Mundie. 'Secondly, we object strongly to the existence of a spy base which is responsible for invading the lives of the people of Britain. ...

"Menwith Hill is a U.S. base comprising the world's most technically advanced and comprehensive spying system. ... For 15 years it has existed to tap the telephones of private citizens, corporations, governments, both nationally and internationally."

(U) By the first of May, the press was reporting that over 30,000 anti-nuclear protesters would converge on the Station. The demonstration was said to have the support of 12 national trade unions and Keighly's MP Mr. Bob Cryer. A 24-hour vigil was now to be added, and the base was to be encircled during the day. According to the organizers, over 3,500 circulars were mailed to trade union branches and shop stewards and 15,000 petition forms had been issued.

(U) Although police liaison indicated the organizers really expected only 20,000 people, all the signs pointed to a massive action at the gates of Menwith on the 4th of July. And as the date approached, the BBC broadcast a story featuring James Bamford, his book, and his allegations, none of which did much that was beneficial to Menwith Hill's image or standing in the community.

(U) A new ingredient was added about this same time, 8,000 miles away. Argentina's armed forces invaded the Falklands and in an instant media interest turned away from the CND. As British forces were organized into a task force, there was an overnight resurgence of patriotism and unequivocal support to the Government in the crisis.

(U) After the US declared for Great Britain, there was a noticeable increase in the general feeling of good will towards Americans in general and, in North Yorkshire, towards Menwith Hill in particular. This was particularly evident during community relations tours when guests offered to their Station hosts their personal appreciation for "the help America is giving us publicly and the help we don't know about."

~~(C)~~ On 15 June, the BBC carried a report called "Falklands Special" that included a segment entitled "The Secret War." Featured was James Bamford, standing in front of NSA/CSS Headquarterss, identified only as an "Electronic Intelligence Analyst"--in other words, he appeared to be an official spokesman for NSA. The following exchange between BBC reporter Tom Mangold and Bamford probably had a stronger effect upon anti-Menwith Hill Station efforts than anyone could have realized at the time:

Mangold: "America's spy satellites tried to help guard the Task Force by giving details of coastal photographs showing the Argentinian Navy, usually in port, weather patterns, and intercepts of coded military traffic. Once the intelligence has been acquired by the satellites, how is it routed to the Task Force Commander?"

Bamford: "Well, it's a very complicated process, and what happens is when the satellite makes its route around the earth it passes over Argentina and the Falkland Islands. It collects its signals intelligence and its photo intelligence, and it stores it on tape, and then it makes about a 45-minute journey northwards on the same trajectory and it passes over England--the first friendly country it passes over. At that point, then the signals are sent down to a ground station--at Menwith Hill Station, the National Security Agency station run by the Americans with some British cooperation, in Yorkshire, near Harrogate. At the ground station the analysts go over the information, produce intelligence out of it, translate it into pictures and sounds, words, and then transmit that information down to Cheltenham, the headquarters of the British Government Communications Headquarters. Once at Cheltenham, the analysts go over what they want to send to the Task Force and they take that information and beam it up to a Defense Satellite--it's called "The Discuss Satellite," a Communications Service satellite, that's just over the Atlantic at 22,300 miles, and in turn that beams it down and the Task Force then receives the information."

(U) There was an immediate and strongly favorable reaction in Yorkshire. Again, this was seen in the Community Relations visits: there was an increase in requests to visit the station and, on those tours already scheduled, the broadcast was mentioned in an appreciative manner. Most of the visit requests came from the Keighly-Bradford area, the hometown of Mr. Cryer, and those groups tended to be supportive, not critical, in their comments during their visits.

(U) As the date of the demonstration approached, there was another complicating factor: a national rail strike had shut down all trains. The impact of that strike is debatable but it probably helped cut attendance. However, by 25 June it was obvious that the demonstration was floundering; only 50 buses had been chartered.

(U) On 27 June a new factor entered: the Station learned that an anti-CND group intended to stage a counter-demonstration by flying over the group trailing a banner stating:

"CND - Communist Neutralist Defeatists."

The spokesman for the group stated he would take away from the media coverage of the demonstration, saying "If the BBC gives the demonstration 25 seconds, at least 5 of it will be on my airplane."

(U) At midnight the demonstration began. A small number of young people started the vigil on schedule. By mid-morning, the police were briefed and the Station waited for the action to begin. So did the organizers. The 12:30 step-off time was delayed to await more protesters, as only about 1,000 were present. Eventually, the police insisted that the march move out and 1,362 men, women, and children began walking behind the lead banner:

MENWITH HILL PEACE PICNIC
GIVE PEACE A CHANCE
CLOSE MENWITH HILL BASE
MAKE YORKSHIRE A NUCLEAR-FREE ZONE

(U) The day was uneventful for the Station, but adding to the demonstrators' woes were the gusty winds and threatening clouds. Just as the climactic ceremony was beginning in front of the gate, horizontal rain (a regular feature at Menwith Hill) struck, driving away all but the organizing officials and their speakers.

(U) One final note: the press coverage proved the anti-CND group correct. Almost as much coverage was given to the airplane and its sign as to the demonstration. Nevertheless, the CND has promised one more demonstration this year and a return visit next 4th of July.

SOLUTION TO NSA-CROSTIC No. 49

[redacted] "[Logic] Design [Exceeding Boolean Capabilities]," CRYPTOLOG, Jan-Feb 1983

"Contemporary digital computer programming makes use of 'languages' which have progressed from the [absolutely] machine-dependent, tedious, 'assembly' stage to a nearly machine-independent, expedient 'high-level' stage."

P.L. 86-36

To: cryptolg at barlc05
From: jim at barlc05 [redacted]
Subject: 1983 wordsmithing award

The 1983 user-friendly award for clarity is awarded to the unknown (probably for good reason) author of the following sentence appearing in the UNIX ED (I) manual page.

"The concatenation of regular expressions is a regular expression which matches the concatenation of the strings matched by the components of the regular expression."

SOLUTION TO NSA-CROSTIC No. 50

"Clear Writing,"
Lieutenant General Lincoln D. Faurer,
Memorandum of 19 October 1983

"Use plain English. Write like you talk by using the active voice. Make your verbs do the work. Use personal pronouns and contractions when they come naturally and the tone allows them."

LOOKING AROUND with

P.L. 86-36

TELECOM 83 [U]

The Telecom 83 meeting combined the largest and most important exhibition of modern telecommunication equipment with a three-part Forum 83 conference on the financial, technical, and legal aspects of telecommunications.

The Telecom meetings are held at four-year intervals and are the premiere conference and exhibition of this kind.

To give a brief quantitative survey, the Exhibition filled two floors of the large Palais des Expositions in Geneva, Switzerland, and a large tent was erected outside to extend the French exhibit. Beyond the tent, a large open space contained dozens of antennas of every kind, many of them operating to satellites or other radio links.

More than 650 companies and nations had exhibits, which covered 90,000 square meters (about one million square feet). Over 700 companies sent teams of people to attend the Forum and to explore the exhibition. The PTTs (Postal, Telephone, and Telegraph Departments) of most nations also sent representatives to look over the equipment, make purchases, and review the technology.

The exhibition was crowded until the last day. It was officially open for seven days, with a preview on 25 October 1983 for the press. Over 100,000 attendees were expected. One effect of the meeting was that every hotel room in Geneva, and for about 50 miles around, was booked up two years before the meeting. Hundreds of visitors were traveling long distances every day to attend the Exhibition and the meetings, and even the planned peace negotiations had to be delayed until the Telecom was over.

Security was very tight, with hundreds of Swiss police and security personnel at the Palais des Exposition and in the streets around that part of Geneva. There was a fear of terrorist activity, because of the Palestinian issue and also because many delegates to a big Socialist meeting being held elsewhere were being quartered in Geneva. Leaflets about the threat were distributed to the exhibitors.

The Forum meetings had high-quality talks and were well attended, even crowded. To illustrate the selectivity, the Technical Forum was offered 400 papers by leading technical organizations in the world and chose 80 of these papers for publication. As a result, the quality of the published papers was very high. One plenary technical paper, by Ian Ross, Director of Bell Laboratories, gave an outstanding prospectus of developments in telecommunications technology; the other plenary papers were of the same quality. The financial and policy papers were also carefully composed and were given, for example, by the Chairman and President of AT&T and by other experts of similar rank. The legal papers were given by prestigious figures, but contained more disagreement than the technical and policy papers.

OCID: 4009884

EXHIBITION NOTES

Some information was gathered in discussions with representatives at the Exhibition stands.

[] The diffusion of telecommunications manufacturing technology was very wide. European and Japanese products were as up-to-date as the latest US products.

[] Small nations, such as Spain and Indonesia, are now manufacturing equipment as well-made as Western Europe, because of turn-key production plants from Europe.

[] Yugoslavia has developed a switch manufacturing capability, based on Silicon Valley (California) technology and other technology transfers, that is extremely up-to-date by Bell Labs (BTL) standards, according to J. Ryan of BTL, who toured their plant and is the BTL expert in switching. The Yugoslavs have overcapacity and are manufacturing modern switches for others.

[] India is producing a wide range of telecom equipment, which appears to be as well-made as European or Japanese equipment.

[] China had a fairly large exhibit, and their best equipment appeared to be of high quality. They have a teleprinter that forms excellent Chinese characters on a screen and also can do excellent matrix printing of the Chinese characters. Any Chinese character can be formed from four teletype letters, based on the radical decomposition. A Chinese operator can learn to type 60 Chinese characters per minute with four weeks of training.

[] Most of the Exhibition literature was very well done from a graphics art viewpoint. This was true of the Chinese, the Saudi Arabians, the Czechs, and other Comecon countries, India, Spain, etc. Only the Soviet exhibit had data sheets that had an engineering rather than a marketing presentation and appearance.

[] The USSR exhibit was fairly large, with over 100 kinds of telecom equipment shown. The Russians also supplied a show with singers, dancers, and musicians, and much of their exhibition was very artistic. However, their equipment appeared to be noticeably less well-made than the other Comecon equipment. They had a computer on a chip, but had to solder the printed wiring to make it work. (The solder points were proudly displayed to me by a Soviet engineer to prove it really was a working 16-bit computer, not a dummy). The connectors however appeared well-made.

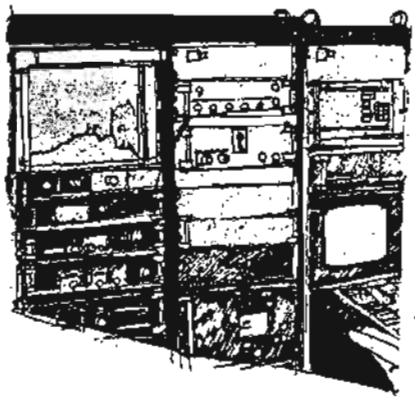
[] There was a wide range of new microwave and optical fiber equipments from many suppliers.

[] ECI, an Israeli company, had a time-assigned speech interpolator (TASI) speech compressor so good that the German Bundespost is adopting it to double their trunk circuit capacity. It will carry voice and data, and is intended to increase traffic capacity faster and more cheaply than microwave links can be built. The Israelis have apparently approached the PRC about marketing it in China to speed up PRC telecom development. It may also have emergency communications uses.

[] The broad emphasis of the show, and of the technical forum, was on producing more services and more "bits down the channel" per hertz and per dollar.

[] There was some cryptographic technology displayed at the exhibition by about ten companies, including a Fujitsu DES device with Public Keying; however there seemed to be almost no spread spectrum equipment.

[] Telecom business skills, as well as manufacturing and operating technology, are being diffused to Third World nations; e.g., a Saudi company bids on Arab and other tenders, after being started up with help from AT&T; Brazilian companies are developing in-house design and marketing competence.



- Turn-key operating networks in the Third World are very questionable. The Finnish company Nokia put a microwave network into the Sudan, which they are sure is not working. The customer, after the turn-key takeover, has not asked for help. Sudanese personnel sent to Finland for maintenance training spoke little or no English, having been selected for bureaucratic reasons. The company is concerned about its reputation. In Indonesia, the same Finnish company has set up a post-turn-key office to provide advice and spare parts sub rosa, so that the customer can claim credit for successful maintenance. In Saudi Arabia, L. M. Ericsson, with a big contract, is setting up the network so they can telemeter its status and performance after the turnover, apparently without the customer's knowledge. This is to protect their reputation. The L. M. Ericsson engineer felt that the Arabs, keen on business, had no interest in technical matters and would be unable to maintain any kind of equipment.

- Foreign manufacturers, in a number of converations, seemed generally unfamiliar with the US telecom market and the marketing concepts of the US telecom suppliers. On the other hand, many US companies seemed very alert to the foreign market. IBM, for example, had sales literature in about a dozen languages, including Japanese. AT&T also had multilingual brochures and data sheets.

- There are uncertainties about the ISDN (Integrated Services Digital Network) development over the next two decades. Market competition and national developments may outrun the ability of the standardizers to agree on what the global ISDN should be. The British announced that they would not wait for the standards. ISDN is supposed to be settled next year, but there is still a lot of uncertainty about both the specifications and whose standards should apply. The result could be a de facto deregulation of future ISDN development.

- The Telecom 83 was apparently successful from the standpoint of making sales, according to various sources. The British had banking services included in their exhibition, to underscore the importance of financing sales.

- The Czech exhibit displayed very little equipment and held its brochures and data sheets closely. Apparently they were not available unless a sale was imminent. On the other hand, the Hungarians, Romanians, East Germans, Bulgarians, and Yugoslavs had equipment and literature readily available.

- One Czech PABX brochure showed equipment that appeared as modern and well-made as US and Japanese equipment, and the brochure was of high quality.

- The French exhibit seemed to be the largest, by a factor of two. The show inside the Hall was as large as the US exhibit, but they put up a huge tent, equally large, outside with more exhibits and a theater, and gave parties.

- Cryptographic equipment was listed by nine companies, but was not visible as apparatus or literature at five of these exhibits. On the other hand, there were three companies that showed new cryptographic products, not indicated in the catalog. Fujitsu had a DES modem. A small Dutch company Text-Lite, had a handheld word processing and data modem, which had DES in a software algorithm, for $600. ITS, an airline communications company, had a Japanese data scrambler to pursue an expansion into banking traffic. The availability of DES from foreign sources in a neat package is significant.

DOCID: 4009884

[] Paradyne, a US and UK company, got a special license to take a DES modem to Geneva for demonstration. They have been successfully testing 15,000 bps on a leased telephone line between UK and Egypt, and 12,000 bps over a switched line between UK and Finland. Those are fairly high bit rates for a 4-KHz circuit.

[] Motorola had a paging system that would deliver short messages to a 2" x 3" receiver for scrolling display. The Swiss also had a similar device, but not working. These new message delivery systems will probably be competitive, and spread fairly quickly in big cities.

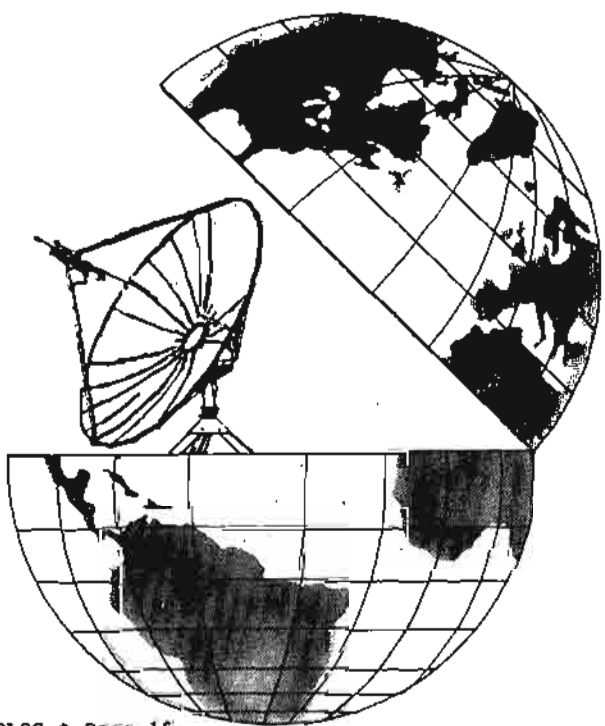
[] Amos Joel, the recently retired Bell Labs switching expert, received an award at Telecom 83 for his contributions to the industry. He had a contract with System Development Corporation (SDC) to make a study of the comparative state of switching technology in different countries. SDC in turn got the contract from DoD. The study was confined to PBXs but that is where the newest technology is going. This study could be useful to various parts of DoD.

[] Dittberner Associates, Inc. has done a 5-volume study for DCA on the telecom networks of 20 countries. The countries are apparently in Europe. This study would complement the Joel study above and would be useful in various parts of DoD.

[] J. Reed, apparently the founder and head of Communications Technology, a California firm that sells military radios to Third World countries, claimed that US export limits on low-grade cryptographic equipment are unfair because the Israeli firm Tadiran and the British company Racal, for example, are selling equivalent equipment in Guatemala, which is costing US companies sales. His company usually uses TCC cryptoequipment, manufactured by the Technical Communications Company. Many of his customers are military and security services, who want security on their radio links, but the delays in US export licenses--apparently not equaled by the Israeli and British governments--make competitive business deals infeasible.

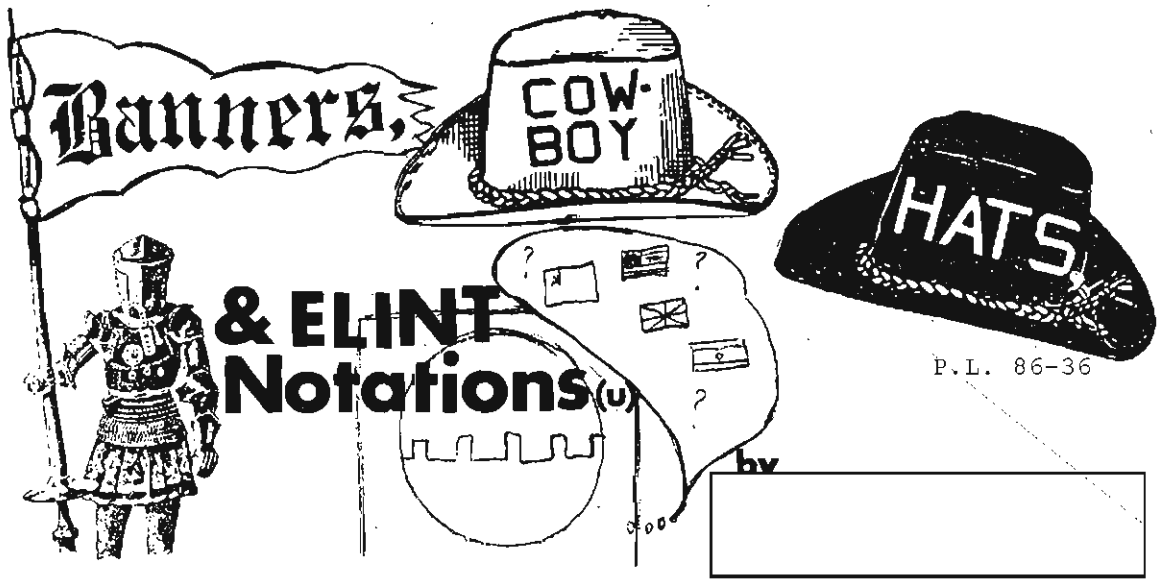
The most striking feature of the Telecom 83 show was the diffusion of the telecom manufacturing technology down into small countries. The Spanish not only build Ericsson switches for their civil net, but also have an Ericsson-designed gridded military net that they are building and operating. It is probably based on a corresponding Swedish military net. They are not yet in a position to compete with the Swedish company or other big manufacturers for foreign markets, but are producing well-made products. Medium-sized Asian countries are also becoming manufacturers. The Brazilians not only have research links to Brazilian universities, but to MIT and its industrial partners as well. Brazilian companies also send students to MIT to get new ideas and technology, and then offer them careers that bring them back to Brazil, to a young company. The Saudis have made a major push into telecommunications, backed by oil money, and a Saudi chaired one of the financial and policy sessions. Despite the problems in Africa and the Arab world in operating the systems, there is a sense of urgency in the Third World and in China that they must expand their telecom nets very rapidly--and also get organic manufacturing capacity. The West Europeans, Comecon nations, Japanese, and US companies are eager to sell them anything they want.

The second striking feature of the Telecom 83 exhibit, apart from its size, was the completely up-to-date and competitive products offered by the European companies, a big advance from four years ago, according to various sources. In essence, the technology transfer has already occurred, and from now on it is a marketing race, in which the US lags in banking, financing, export policies, and government support. This could have strategic impact.



~~FOR OFFICIAL USE ONLY~~

DOCID: 4009884



P.L. 86-36

by

[redacted]

In the film biography "Young Winston," little Winston Churchill arrived at his boarding school for the first time. His professor, in order to make a preliminary evaluation, opened a Latin grammar book and told him to memorize all the case endings of a certain noun. Later, the boy recited his lesson and asked, "But what does it mean, Sir?" The flustered professor answered, "Well of course this is the nominative masculine singular, ... accusative, ... ablative ..." The boy responded politely, "Yes, Sir, but what does it mean?"

(U)

(U) When we use technical designations such as electronic intelligence notations (ELNOTs), we may be as far from explaining what it really means as was Winston's professor. They serve a real purpose, just as the case system did in Latin, but they are simply an intermediate step in the process from concept to communication. They are in themselves no more meaningful to a tactical commander than terms like "ablative" were to a little boy whose native language contained no such feature. Just as grammarians attempted to impose the descriptive terms for a dead language on the evolving Romance and Germanic languages, ELNOTs may not fit the military realities of today without adjustment and flexibility.

~~(C)~~ ELINT must be translated clearly because of its growing importance in the total intelligence picture. ELINT can be made available in near time, unlike imagery, HUMINT, or the products of cryptanalysis.

[redacted]

P.L. 86-36

[redacted]

(U) When the present ELINT notation system was introduced in the mid-1960s, it was tailored to the circumstances of the time. The following presumptions were present at the outset:

P.L. 86-36

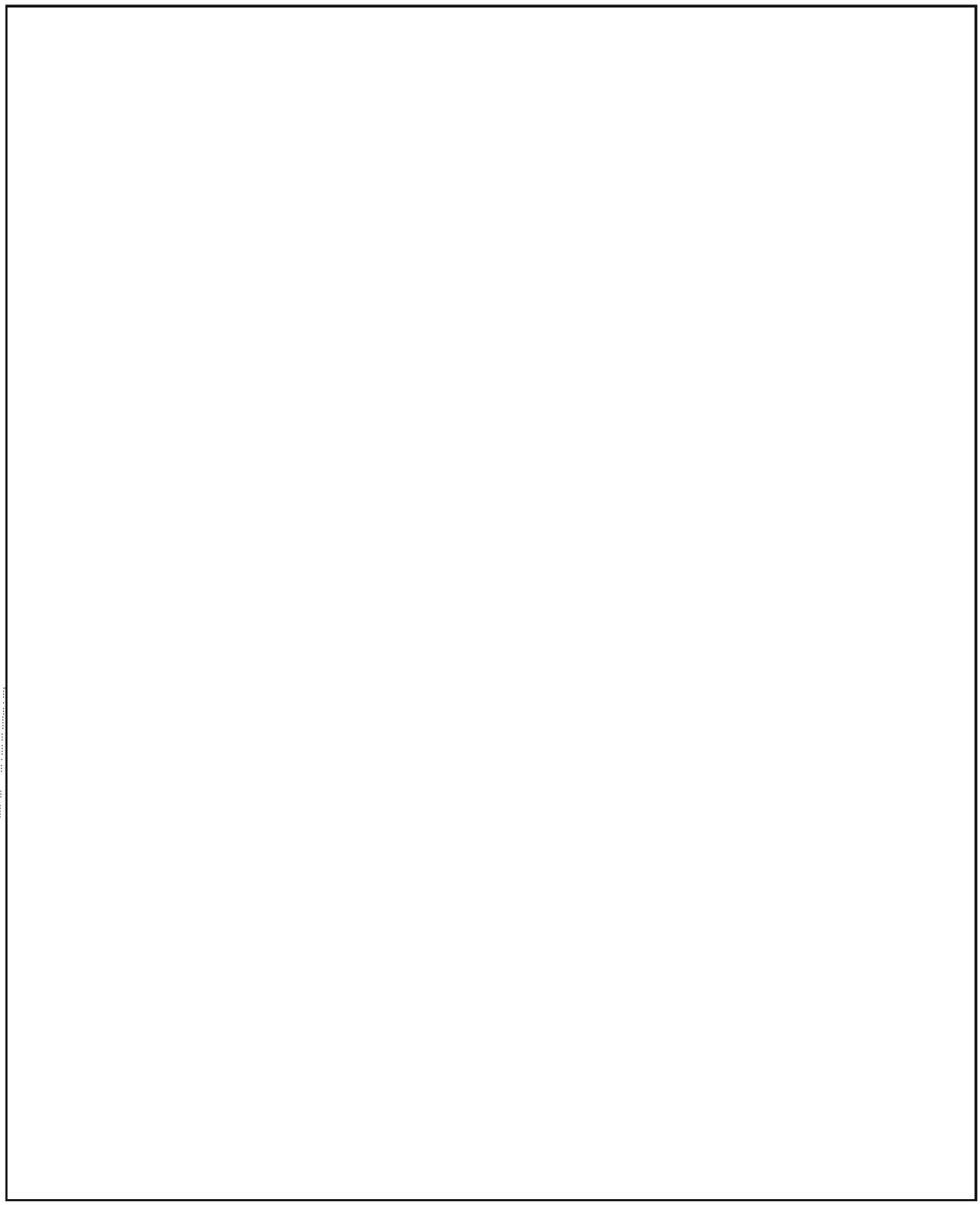
[] Electronic equipment, such as radar, was manufactured in either the Soviet Union and other Warsaw Pact countries (the Communist world) or in the United States, Britain, France (the non-Communist world). Countries with Communist equipment in their inventories were unfriendly, those with non-Communist equipment were friendly.

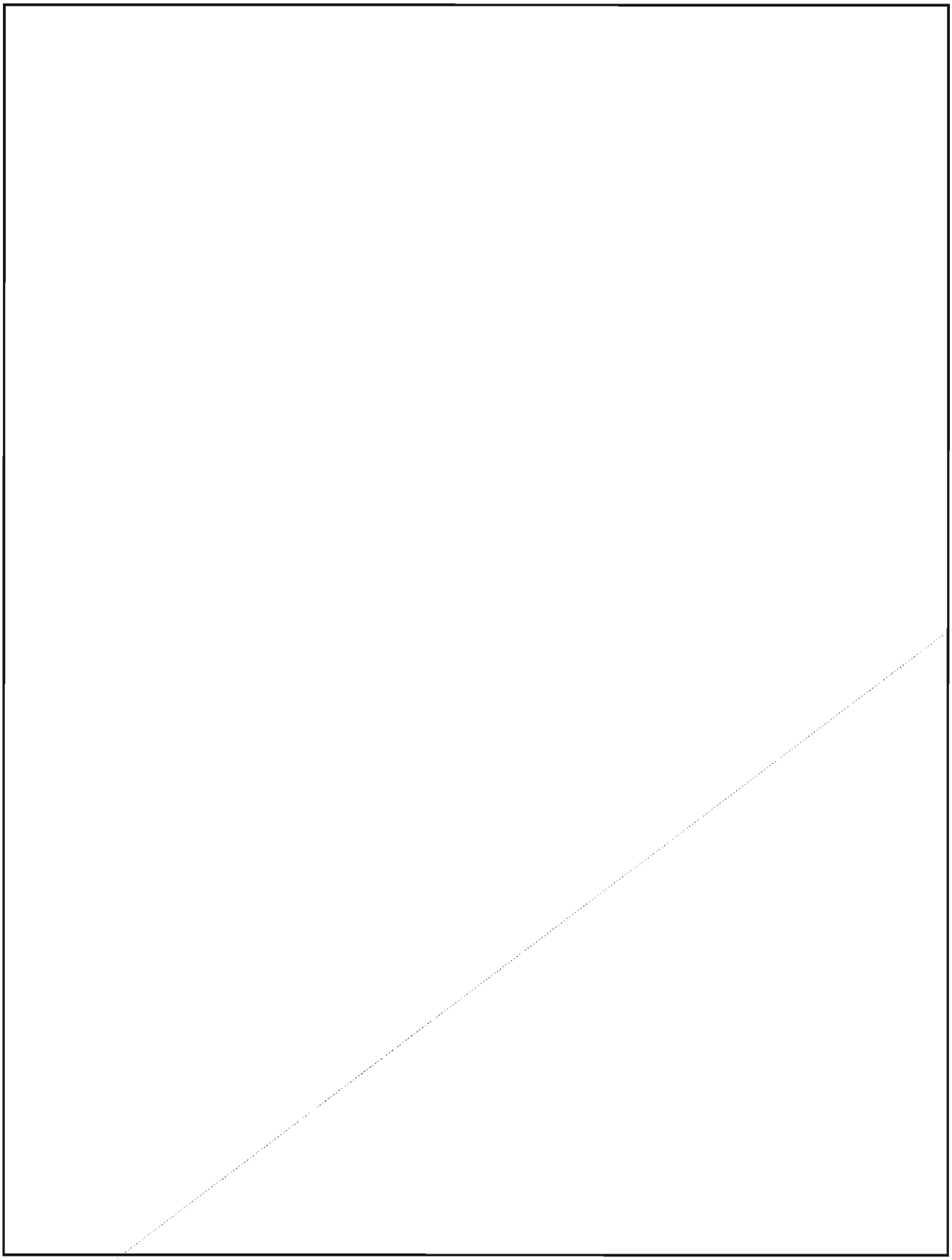
[] Electronic equipment was specialized to a certain basing mode, either airborne, landbased, or shipborne.

~~(C)~~ These presumptions conveniently provided a means of distinguishing friend from foe (like the banners carried in olden times by military units and knights errant) and separated activity into areas of interest. The notations did not reflect function of the equipment nor did they provide any information regarding the threat which the radar (and the weapon associated with it) might pose. An ELINT specialist would distinguish function and threat by his knowledge of the signals on a case-by-case basis.

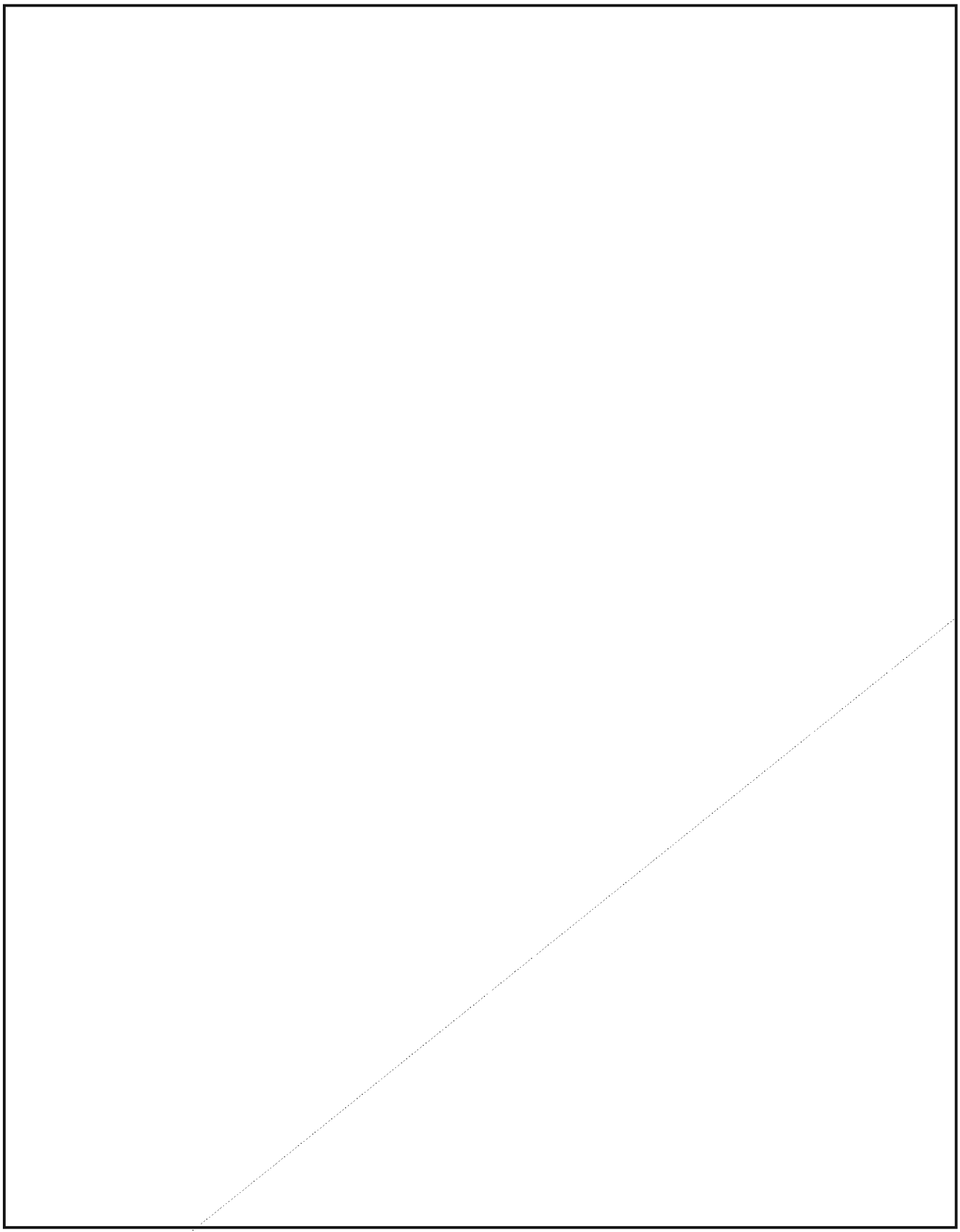
[redacted]

EO 1.4.(c)
P.L. 86-36

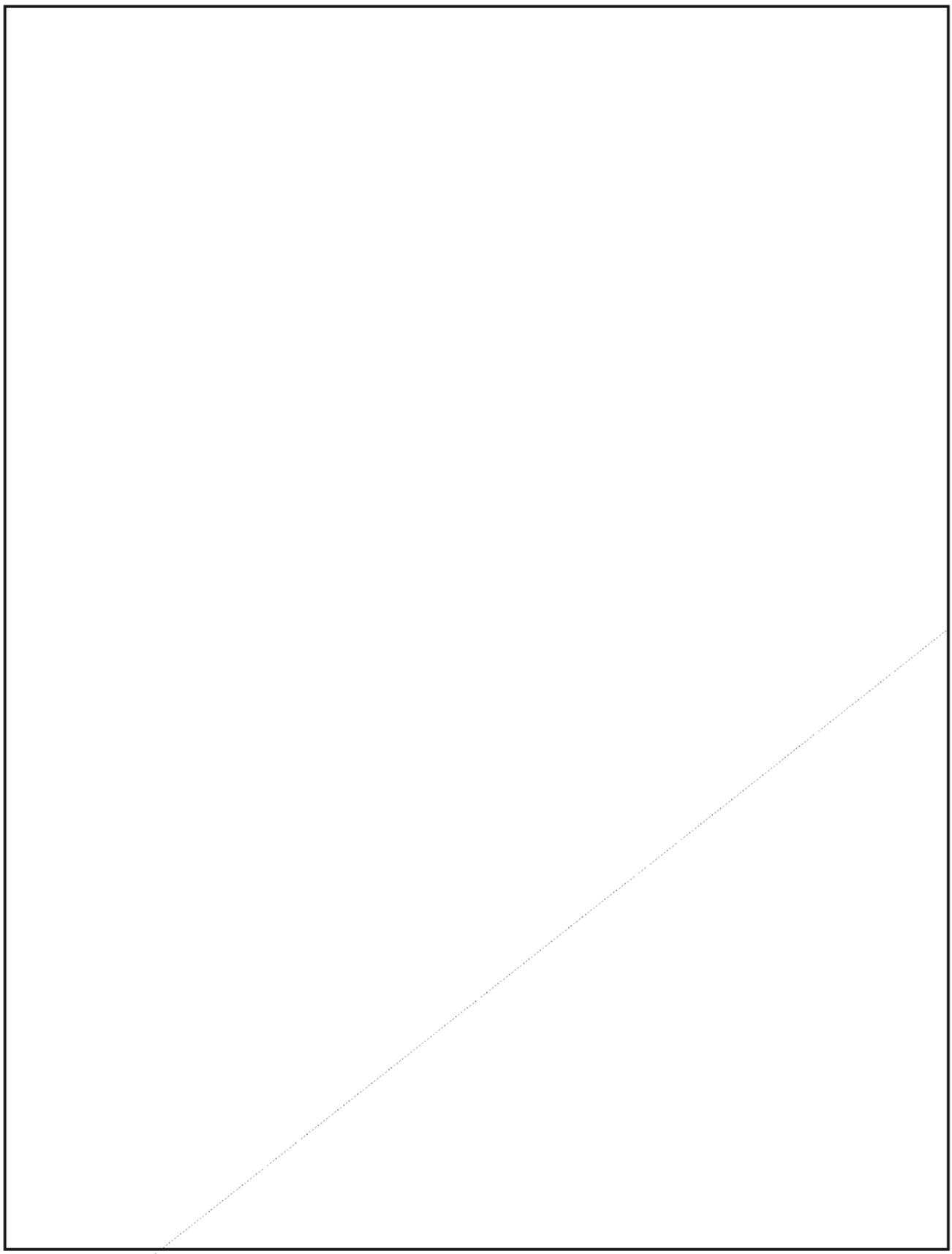




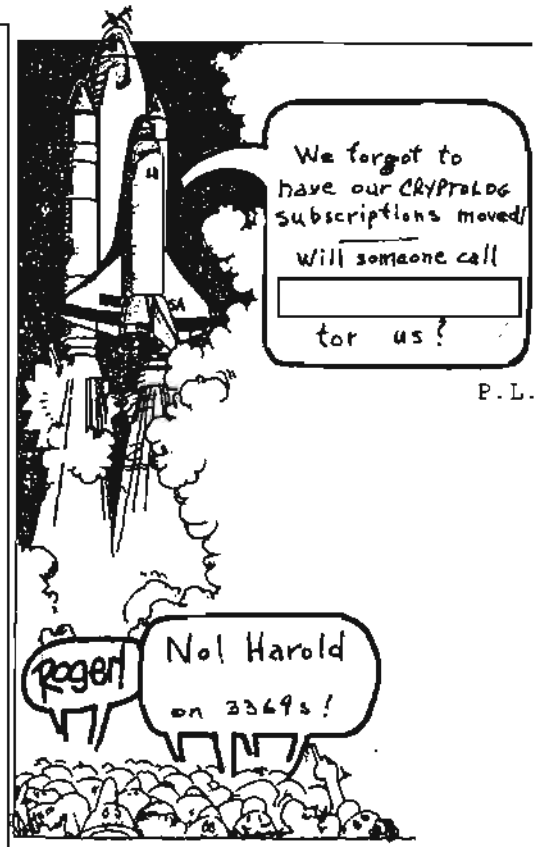
EO 1.4.(c)
P.L. 86-36



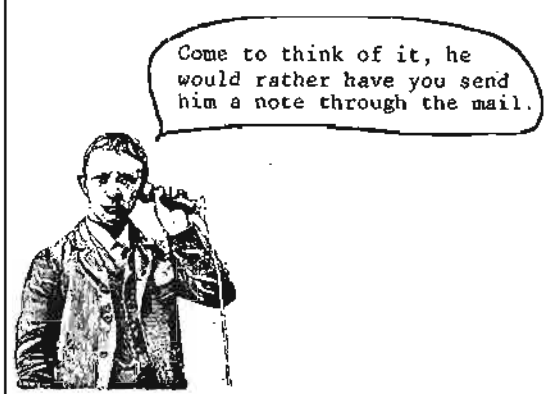
EO 1.4.(c)
P.L. 86-36

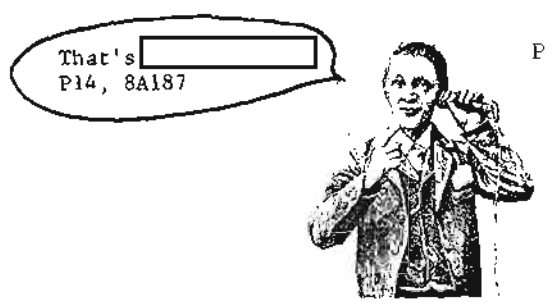


EO 1.4.(c)
P.L. 86-36



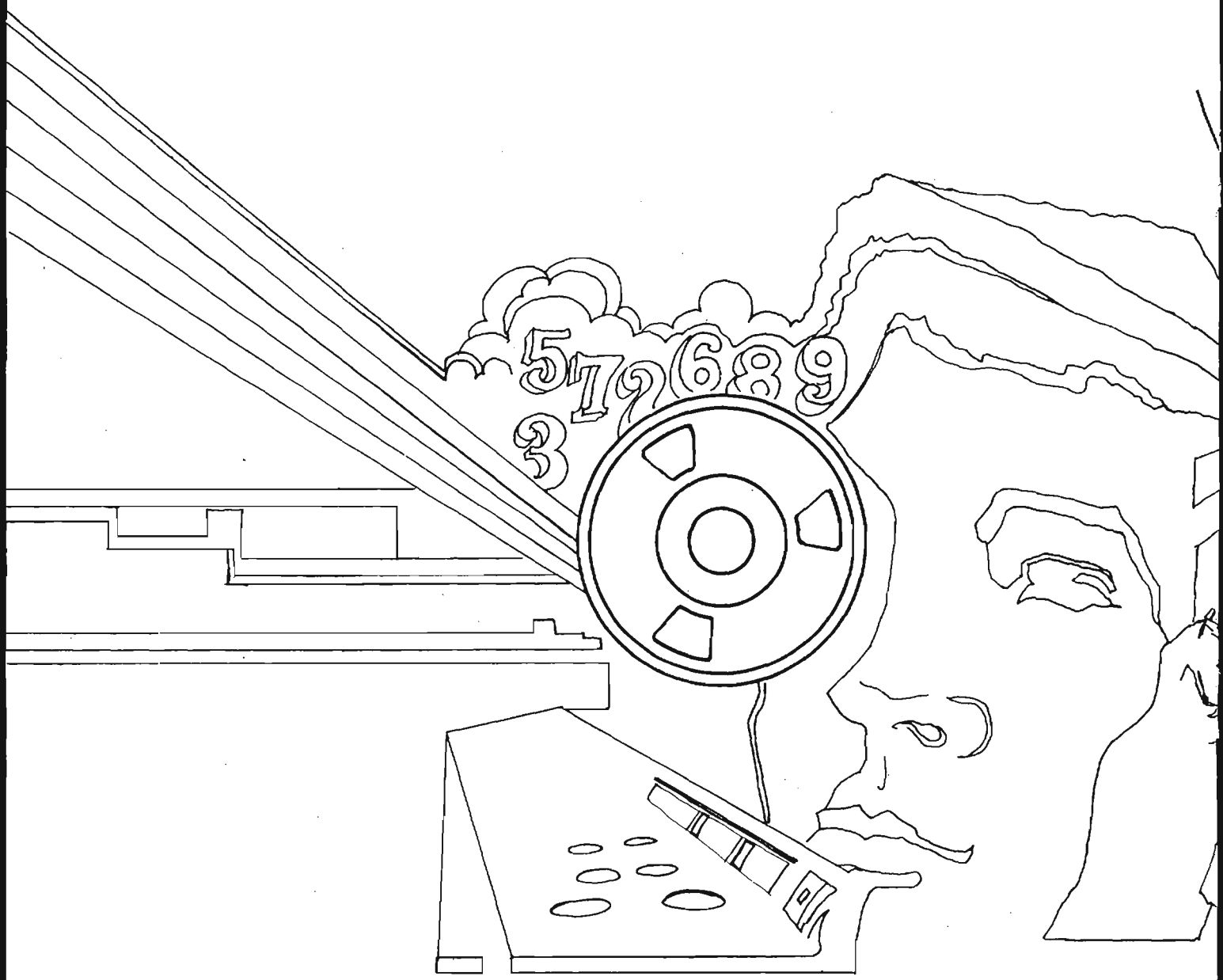
P.L. 86-36





P.L. 86-3

EO 1.4.(c)
P.L. 86-36


5 7 9 6 8 9
3

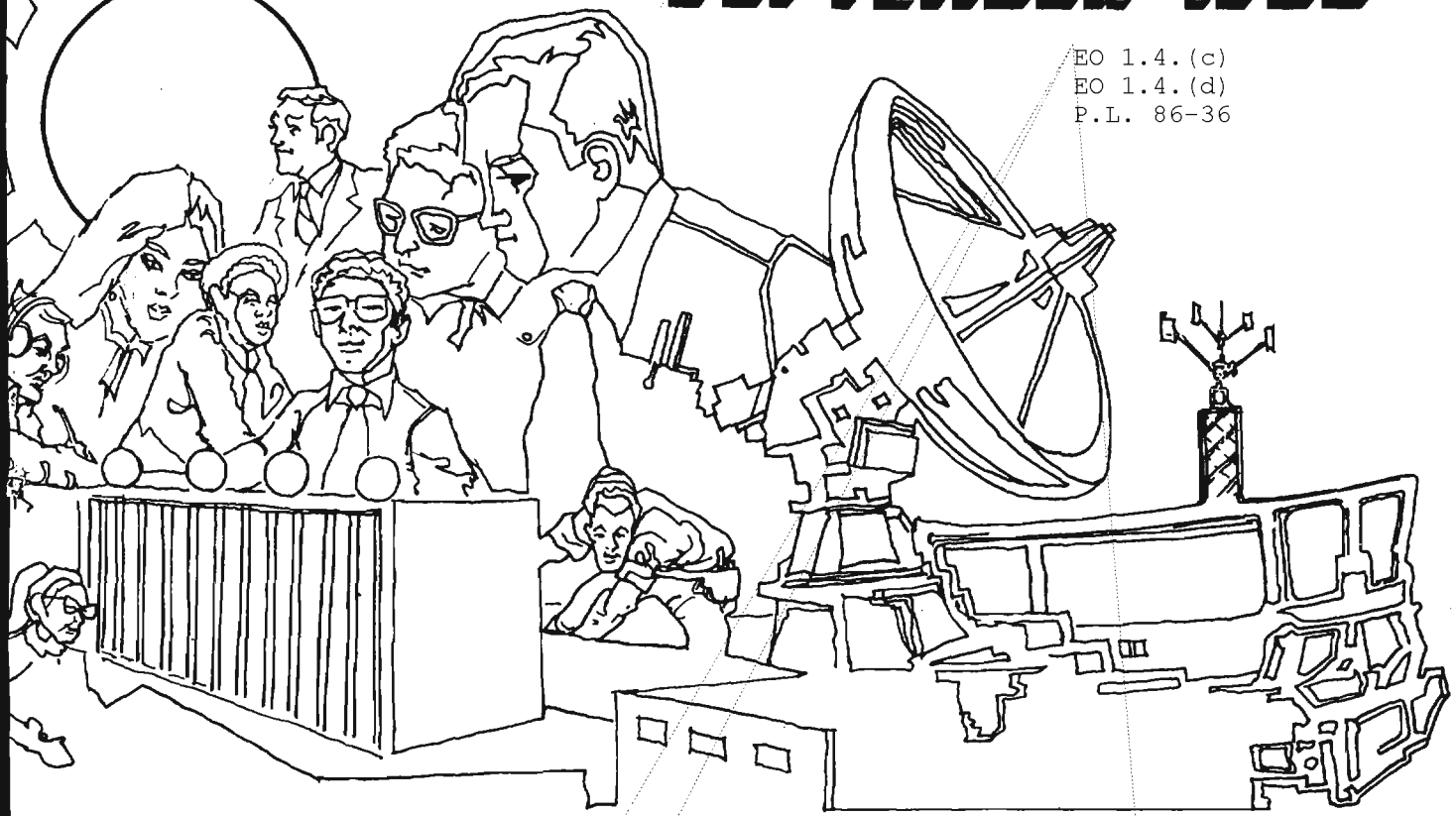
DOCID: 4019697

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

SEPTEMBER 1983



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

[redacted] ..... [redacted] 1
[redacted] 5
DO YOU REALLY MEAN JULIAN? (U) ..... [redacted] 6
MANAGEMENT OF COORDINATION (U) ..... [redacted] 8
ON HOW THE 'GAME' OF THE AGENCY
SHOULD BE PLAYED (U) ..... Ramon Santiago-Ortiz 10
WRANGLER...ONE TOUGH CUSTOMER (U) ..... [redacted] 12
PARPRO: RECONNAISSANCE PROGRAMS (U) ..... [redacted] 15
FOREIGN MICROWAVE RADIO (U) ..... [redacted] 22
NSA-CROSTIC NO. 50 (U) ..... David H. Williams 29

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019697

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. X, No. 9 SEPTEMBER 1983

PUBLISHER [redacted]

BOARD OF EDITORS

Editor..... [redacted] (963-3045s)
Asst. Editor.. [redacted] (963-1103s)
Production..... [redacted] (963-3369s)

Collection..... [redacted] (963-3961s)
Computer Security
..... [redacted] (968-7313s)
Cryptolinguistics. [redacted] (963-1103s)
Data Systems... ..... [redacted] (963-4953s)
Information Science
..... [redacted] (963-5711s)
Mathematics..... [redacted] (968-8518s)
Puzzles.....David H. Williams (963-1103s)
Special Research.....Vera R. Filby (968-7119s)

For subscriptions
send name and organization

to: [redacted] P14
(963-3369s)

P.L. 86-36

To submit articles or letters
by mail, to: P1, Cryptolog

via PLATFORM mail, send to:
cryptolg at bar1cØ5
(bar-one-c-zero-five)
(note: no 'O' in 'log')

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

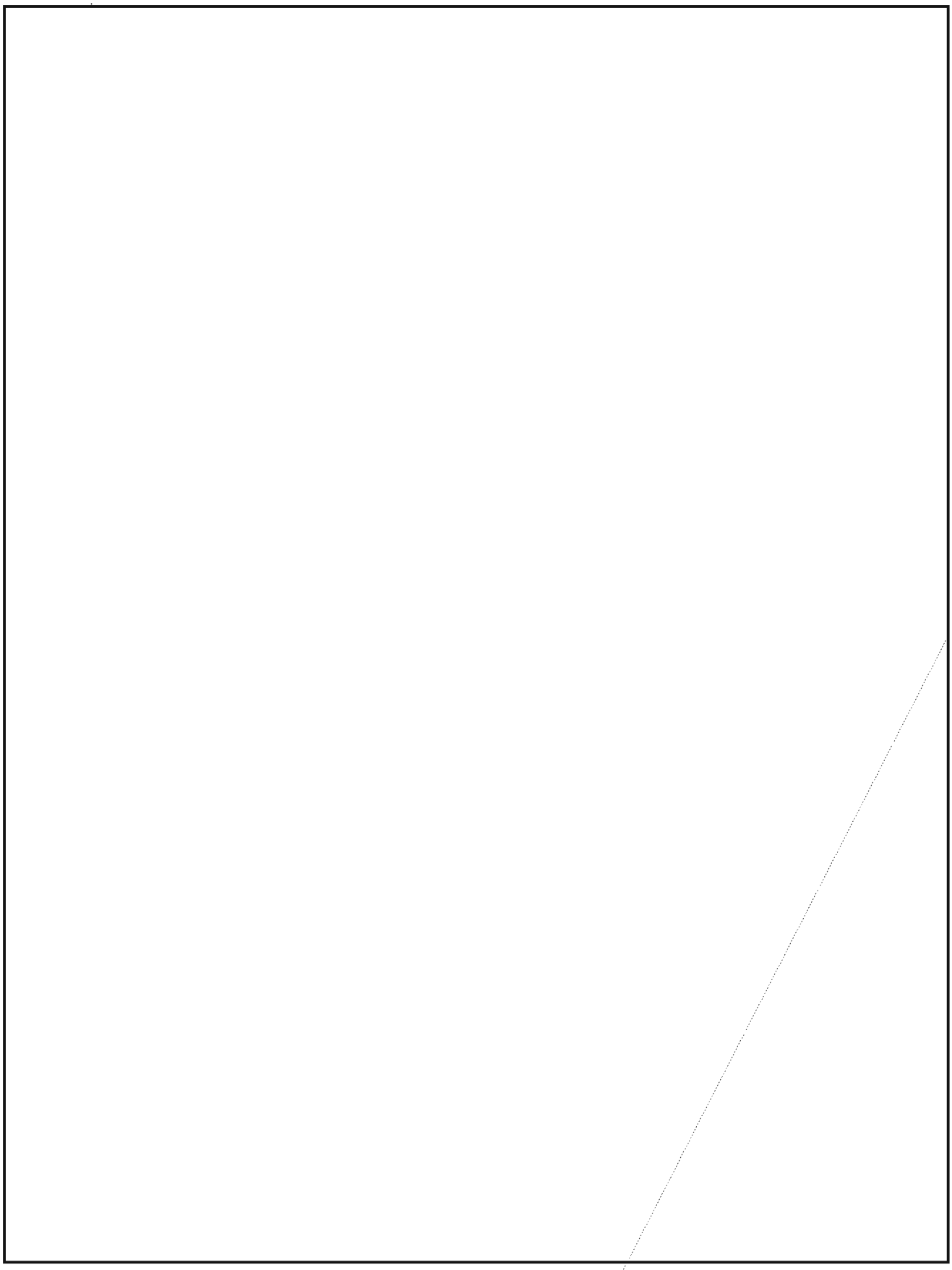
In a nearby university, so the story goes, there was a professor of Marine Biology who was almost legendary for his inability to remember any of the names of his students. He did not even remember the names of his graduate students. One day the Dean asked him, "How is it that you can never remember the names of your students?" "I learned long ago," the professor replied, "that each time I remember the name of a student, I forget the name of a fish."

Our business around here is, at the heart, an intellectual activity. We work at understanding and solving various complex processes and problems, many of which are intentionally devious and difficult.

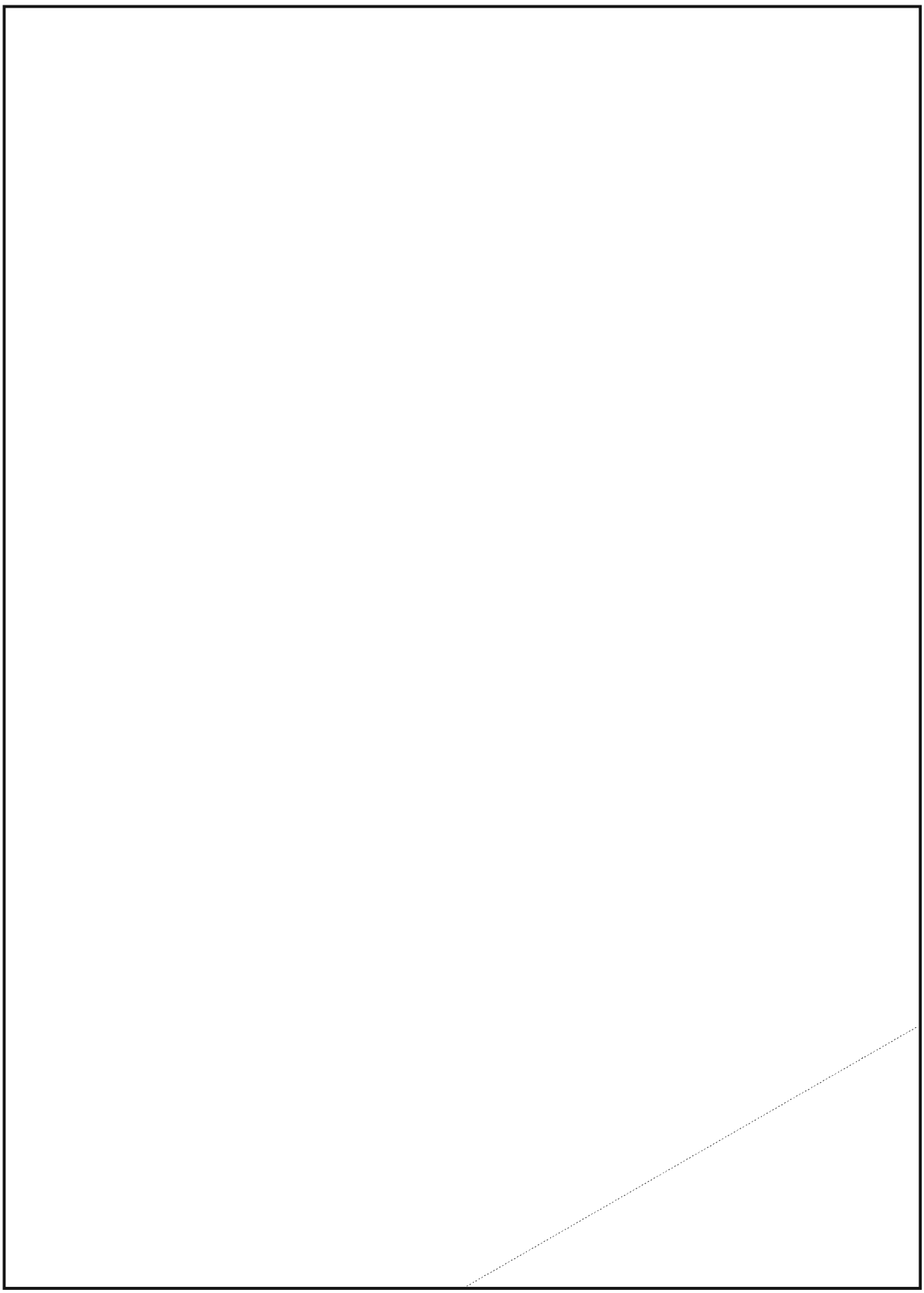
Our system of managing the resources to do all this needs a lot of "fine tuning" (a favorite word of managers) so that the taxpayers, who pay for all of this, will get their money's worth. That is a good and necessary goal, but sometimes our zeal for "fine tuning" produces complicated and bureaucratic mazes that are more efficient in appearance than in substance.

It is all very well to say that we should be smart enough to operate under "sophisticated" organizations and "fine tuned" coordination procedures. And it is also true that most analytic people can, if they turn their minds to it, understand and operate within the most complex operating systems.

Each of us in the analytic business, like the professor, begins each day with only so much "analytic energy" and the more of that energy we spend trying to understand our system--the less we have left over to spend on the target we sometimes call the enemy.

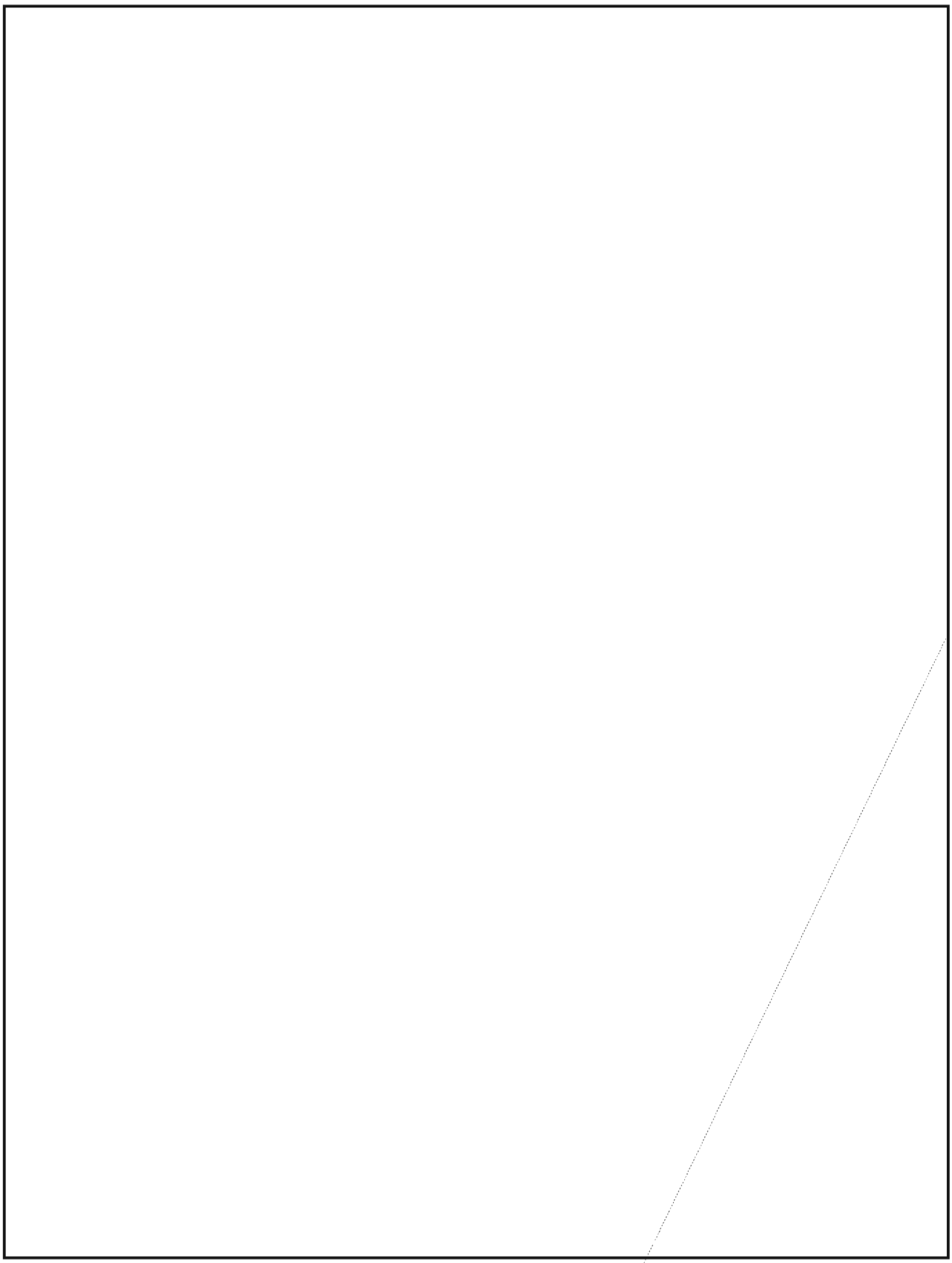


EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

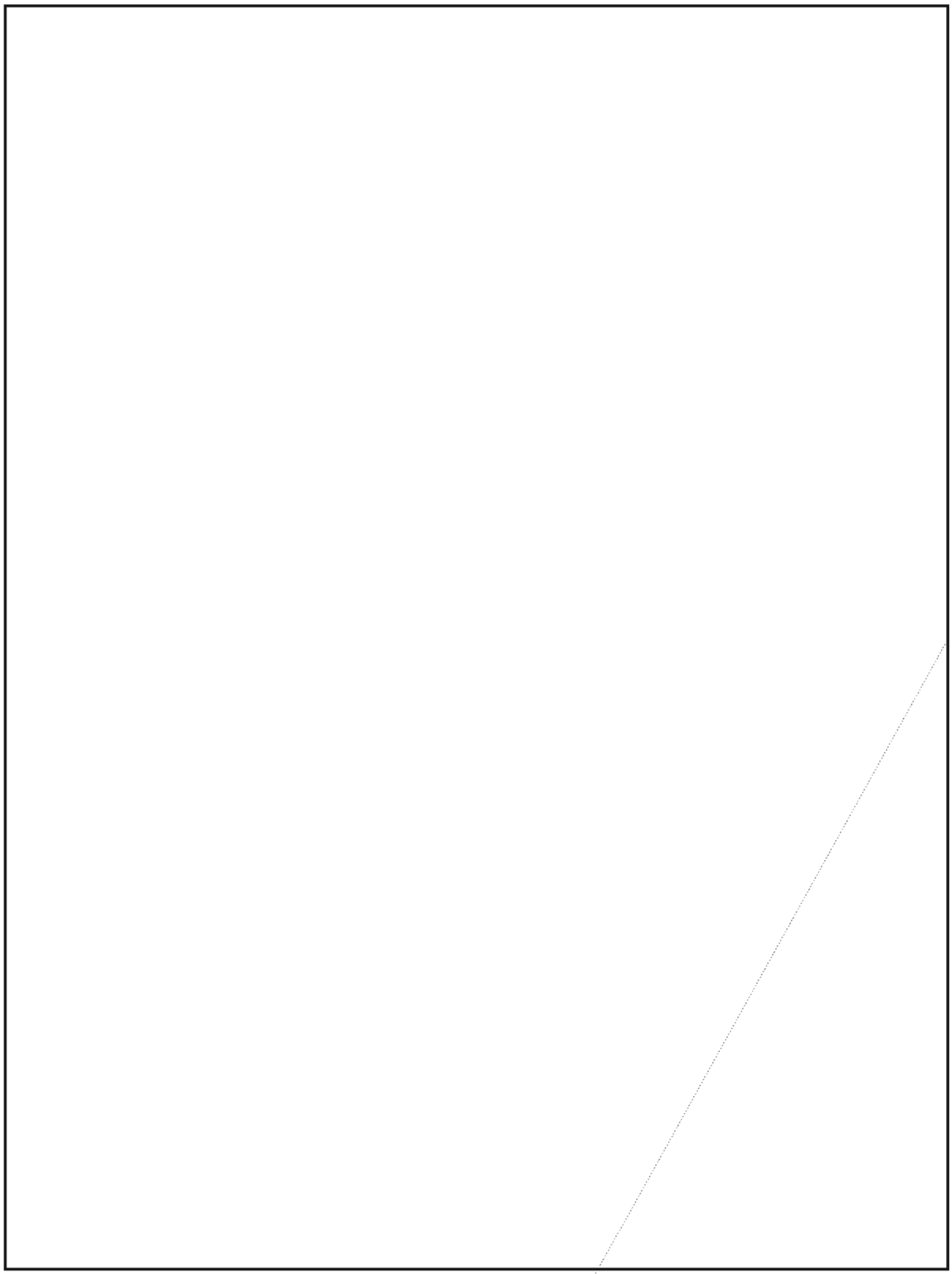


DOCID: 4019697

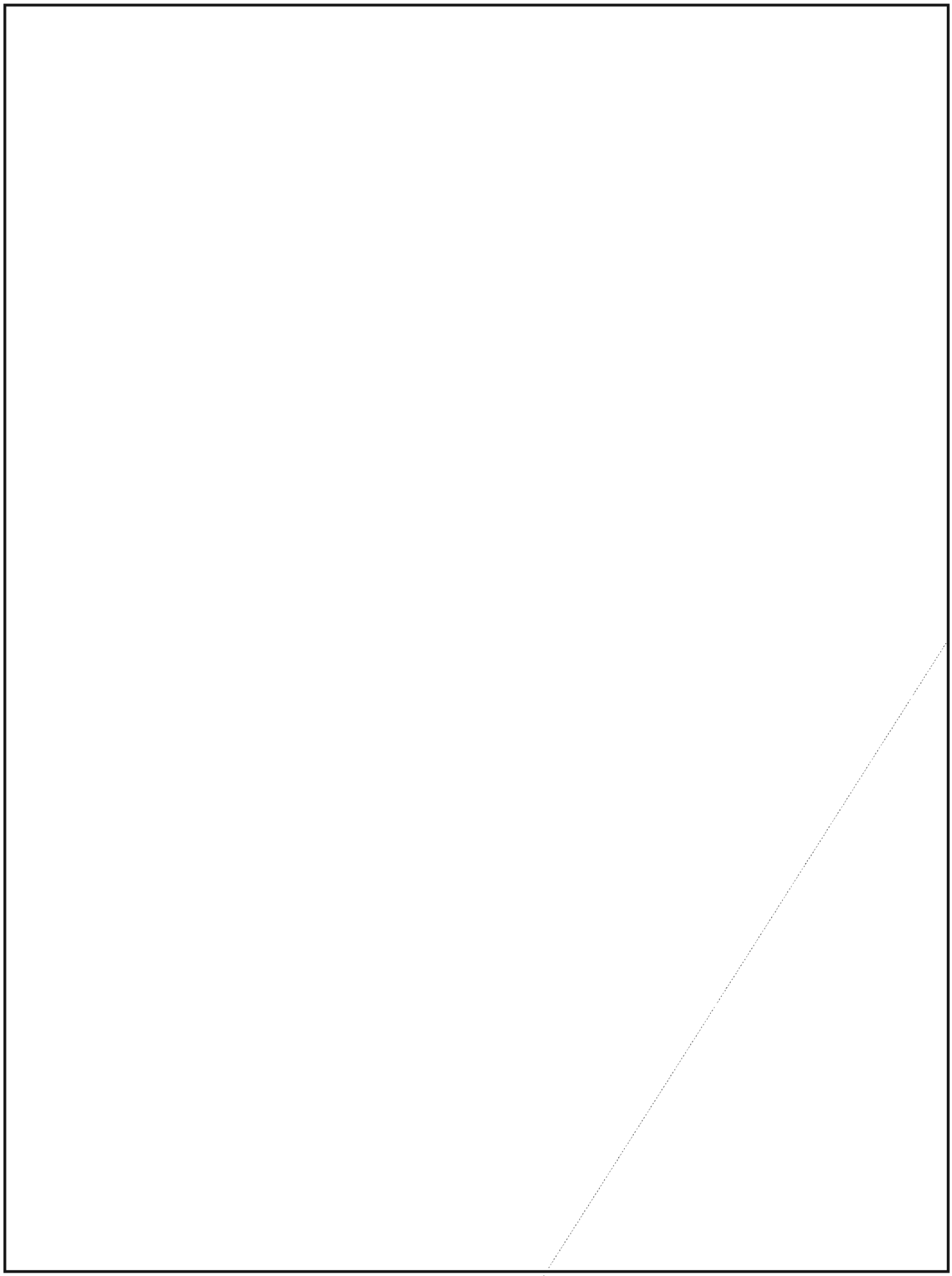
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

DOCID: 4019697

Do You Really Mean JULIAN?

by [redacted] P13

P.L. 86-36

The Data Standards Center (P13D) recently established a new data standard: DE 00105 Ordinal Day The data chain Ordinal Date is of course already a standard, DE 00013. It consists of Year (2N), followed directly by Ordinal Day; e.g.,"83109" to represent 19 April 1983.

If Ordinal Date is already a standard, why worry about one of its components, Ordinal Day? Well, as most NSA people involved in data processing well know, the latter for many years has wrongly been mislabeled "Julian Day." In fact a few years ago, NSA electrical messages used to include a space for entering "Julian Day." Fortunately with the help of sympathetic staff people within T, the NDSC was able to lobby against "Julian Day" so persistently that the term was finally expunged from NSA/CSS electrical message formats. It felt like a major victory!

Accordingly, it now seems appropriate to make "Ordinal Day" an official standard to help lay the ghost of "Julian Day" finally to rest, although that may be easier said than done!

"Julian Date" of course has been equally as persistent as "Julian Day" as a ubiquitous misnomer. Indeed, one of the main reasons for standardizing "Ordinal Date" was to give us some ammunition for suppressing "Julian Date." Incidentally, the ISO (International Standards Organization) has standardized Ordinal Date (ISO 2711), following action by the American National Standards Institute (ANSI) in 1971 to also standardize calendar date and ordinal dates. Both ANSI and the ISO use the term "day of the year" for the data element that encompasses the ordinal days. However, we felt that "Ordinal Day" is perhaps more descriptive of the data element itself.

"Julian Day" and "Julian Date" are of course valid terms, but not in the way that NSA has sometimes employed them. The following information from the Encyclopaedia Britannica summarizes the proper use of these two interlopers.

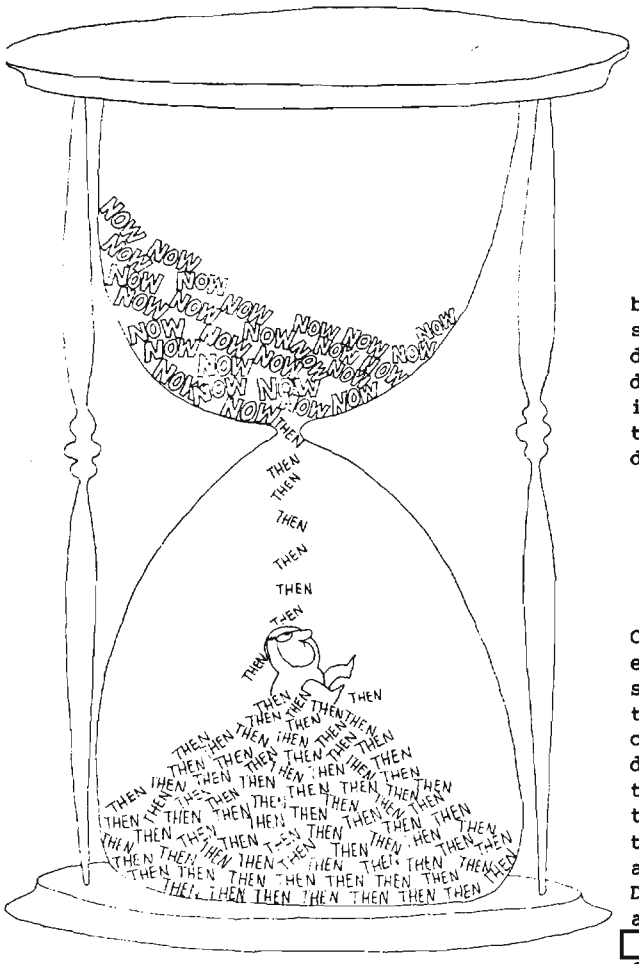
[] JULIAN DATE: The term "Julian Date" refers to a date taken from the Julian Calendar (named for Julius Caesar) that is at present 13 days behind our standard Gregorian Calendar (named for Pope Gregory XIII).

Joseph Justus Scaliger

(1540-1609)

[] JULIAN DAY The concept of numbering days in one-up order is derived from the "Julian Period" system, primarily used by astronomers. (This system was devised by Joseph Scaliger in the 16th century as a universal measure of chronology and named for his father, not for the Roman emperor, although his father, Julius Caesar Scaliger, had been named after the emperor.) "Julian Days" are not numbered one-up through the year, as are "Ordinal Days," but rather throughout the "Julian Period" of 7,980 years that began with Day 1 starting at noon on 1 January 4731 BC (Julian Calendar) and will end at noon on 1 January 3268 AD Julian (which will be 23 January Gregorian) with day 2,914,695.

So you can see neither term represents what quite a few of us NSA people thought it did.



Julius Caesar Scaliger

(1484-1558)

WHAT IS THIS THING CALLED

"an undefined medium in which existing objects appear to develop irreversibly in the changes which they undergo, and in which events and phenomena appear to occur in succession."

The use of "appear to" probably satisfies both physicists and philosophers. However, such a definition would drive a data standardizer right up the wall! In the data standards world, precision and accuracy are premium items, and definitions have to be right to the point. Note, for example, the standard definition for DE 00017, Time:

"An expression of a specific hour and minute of the 24-hour period of the calendar day "

One cannot enjoy the luxury of philosophy, etc., when faced with the demands of a data standard! The above illustrates the point that the definition of a term, and that of a corresponding data standard (if any), can differ to a considerable degree. By the way, the NDSC has a big investment also in SIGINT terminology as well as data standards. The terminology team in P13D has already published authoritative glossaries on Traffic Analysis, Direction Finding, and SIGINT Collection, as annexes to USSID 412. Contact [redacted] (on 968-8161s) for information about any of the above.

P.L. 86-36

DOCID: 4019697

~~FOR OFFICIAL USE ONLY~~

MANAGEMENT OF COORDINATION (U)

by [redacted]
Captain, USAF
JOCCP

(U) The three little words that always make me cringe are "Coordinate this please." Coordination is really time-consuming and, if taken in regular doses, has got to be the main cause of nervous breakdowns among Agency employees.

Webster's definition of "coordination" includes the word "harmonious" but real staff coordination is anything but that. "Acrimonious" would be more appropriate. I often take a deep breath before walking into an office with a piece of "For Coordination" correspondence that appears controversial. I don't think that anything is as frustrating as wandering the equivalent of five miles through a labyrinth of hallways to get three small initials on a piece of paper. No, wait! I can think of something even more frustrating.

You walk around those hallways searching out the final office chief to get him/her to put the final "blessing" on your (by now) cannibalized (otherwise known as "edited") product and he/she disagrees with the whole principle of the paper and tells you that he/she will not concur. ("I non-concur," is usually the expression used.) I sometimes would give my right arm for one of two things in this type of situation:

[] a pistol (preferably one of high caliber) or

[] a high tree (with a conveniently placed strong horizontal limb) and a strong rope.

It would not be extremely disappointing to receive one or two "suggested changes," but each "coordinatee" has his/her own method of inserting these "recommendations." Each one has an unmistakable style, but they can usually be divided into three basic categories:

1. The "arrow maker," who usually goes around placing arrows below (or above or in the margin near) the sentence or word in question. (Sometimes I would like to suggest where to put some of those arrows and now I know why Custer got it in the end.)

2. The inimitable user of Xs, who uses rather large Xs to blot out whole paragraphs, sometimes destroying continuity and making your paper look something like a cross (pun intended!) between a fingerpainting by a mentally disturbed kindergarten student and a colony of eartheworms making love to one another. (The best remedy for X-makers is to provide a pen for them to use, making sure that it is a very soft felt-tip marker--which frustrates their editing--or a pen just about ready to run out of ink. This intimidation process may hamper their efforts and they may give up in disgust, telling you that your paper is fine.)

3. The "thinker," who sits there and ponders the paper, regardless of whether it is a two-liner or a two-pager) and corrects grammar ("It's 'you and I,' not 'you and me'!") or spelling ("There are only two Os in 'coordinate'!"). The best way to counter the thinker is to put several "one-dollar" words in the paper the best one being "propinquity." This word isn't often used in Agency papers and the "coordinatee" may take one of two actions when

~~FOR OFFICIAL USE ONLY~~

confronted with it: He/she may try to show knowledge of the word thereby forcing immediate agreement to the point in which the term appears; or he/she may take the time to look it up (or possibly ask you for a definition in the hope that you really don't know), thereby disrupting his/her thought processes. (Of course, nothing from nothing is nothing.) By the way, "propinquity" means "nearness."

The following main points are absolutely essential when embarking on a coordination trek:

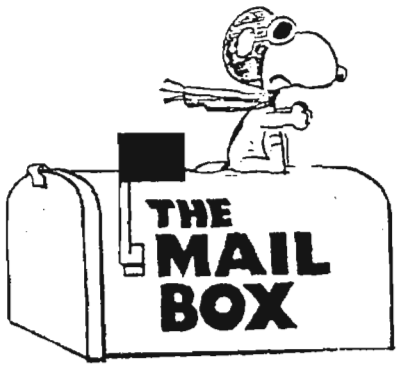
1. HAVE AN OPEN MIND. Be as objective as possible when someone edits your paper, even when you are thinking about ripping your hair out or applying cattle prods to the other person's anatomy;

2. ALWAYS BE AGREEABLE TO CHANGE. If you fight editing changes, this may lead to more "pen massacre" on your work. (It's similar to when your father or or mother used to catch you doing wrong: If you argued, the paddle seemed lighter and hurt more.)

3. KEEP YOUR COOL! Leaning over the desk and breaking the editor's pen, glasses, nose, or arm may make you feel better, but it certainly will not solve the problem. Besides, you can't get initials from a person in intensive care. (Refer to Rule #2 in such cases.)

4. REMEMBER THAT MURDER IS POSSIBLY PUNISHABLE BY DEATH. Except in this case where the charge may be reduced to justifiable manslaughter.

If you keep these rules in mind, coordination will be as much fun for you as it is for the many inmates of Sing Sing or the patients at Saint Elizabeths. Just remember that, if all else fails, your mother always liked you--but she never had to put her initials on anything you wrote.



Dear Sir:

I read with interest the article in the June/July 1983 issue of CRYPTOLOG entitled REDBARON, ROADRUNNER, & BRONZSTAR: What's in a Name? The article points out a problem that this organization has been struggling with for some time. That is the attempt to educate project officers within the Agency about NSA/CSS Regulation No. 10-5, Assignment and Handling of Cover Terms.

This regulation states that approval to use covernames must be obtained from the NSA Cover Term Officer (CTO) who determines the eligibility of specific words for use as covernames. It also states that covernames of similar or related type will not be assigned to projects or operations that are themselves similar or related. Nor will they be a term that will tend to reveal the meaning of the activity (e.g., abbreviations or acronyms).

Not going by the rules in the assignment of covernames can lead to compromise of not only one project but a whole series of projects if they are not protected properly. Assigning covernames to projects without going through the CTO can also lead to duplication of usage and eventually impairment of the Cover Term program itself.

Of equal importance is the fact that the definitions of these covernames are rigidly controlled. Responsibility for releasing these definitions is vested in Q4. Even the terms themselves are controlled. Lists of individual covernames cannot be acquired without first getting the approval of T5.

I urge your readers who use covernames for projects, equipments, exercises, or operations to become familiar with NSA/CSS Reg. 10-5 to insure that they comply with its requirements. If they have any questions about the procedures to follow regarding the use of covernames they can call the NSA Cover Term Officer, [redacted] on x968-8726s.

[redacted]
Chief, T511

P.L. 86-36

ON HOW THE "GAME" OF THE AGENCY COULD BE "PLAYED" (U)

by RAMÓN SANTIAGO-ÓRTIZ, G42

P.L. 86-36

In my lifetime I have watched many baseball games, played quite a number of them, and even coached a few, so my connection with the sport consists of more than just the article "The Language of Beisbol" (Cryptolog, August 1974) that I co-authored with [redacted]

As most people know, baseball has been called the national pastime of the US of A, but I strongly believe that baseball is more than just a mere game. I think it can serve as a guide to life. We have seen teams suddenly score several runs and come from 'way behind to win a game in the last of the ninth inning; from this we can learn never to give up, to constantly keep on trying. "Sure extra-base hits" suddenly become outs because some outfielder scampers a little faster, leaps a little higher, or throws a little harder than people thought he could. Teams have protracted winning streaks or lo-o-o-o-ong slumps, just the way that individuals have good days and bad days. And so on, and so on and so on.

Not surprisingly I have often thought that the "game" in the Agency for which I work should be played just like baseball too. Unlike the Agency, in baseball the guys who play on the field--the ones who produce the hits or make the catches, who slide and get their uniforms dirty, who get injured sometimes badly--these "soldiers in the trenches" do get better salaries and greater recognition than the team managers because they do the tough, dirty work. I think that NSA should follow a similar practice.

The truth is that most of my experience has been in G Group, involved with Spanish-language problems, particularly with voice problems. But even if what I have seen and heard there is not 100% applicable to other parts of NSA, it is sufficiently widespread within G Group (which is, after all, an important part of the Agency) to warrant mention....and to justify my comments.

One way that the Agency could profit by following baseball is in the treatment of managers. A baseball skipper is praised for his team's successes and blamed for his team's failures and losses. It is not unusual for a team's owner to fire the manager when the team has lost a large number of its recent games, regardless of how many games had been won the month before. No excuses, no delays; just "get rid of the bum" and get another manager, who might do better. And, if the new guy doesn't improve the situation, fire him and get somebody else! Good performers do not need to worry!

After all, managers don't win the games; the players do. For every case where a baseball manager has made a clever game-winning change in the line-up or spotted a rule infraction that negated an opponent's advantage, you can find cases of substitutions that backfired: relief pitchers who walked in the winning run pinch hitters who struck out, etc. Why do managers, in the whole US government, no matter how "good" or "bad," seem to get most or all of the "goodies"?

DOCID: 4019697

I suppose that there may be a number of ineffective managers at NSA who, instead of being fired, get shifted to other managerial positions (spreading their incompetence around), sometimes even higher positions? The justification for their advancement would be the outstanding job done by the members of their "team" but, unfortunately, the "players" whom that manager supervised, the ones who turned in the outstanding performances for which the manager was rewarded, are left behind, unsung, unmentioned, unrewarded, unpromoted, etc.

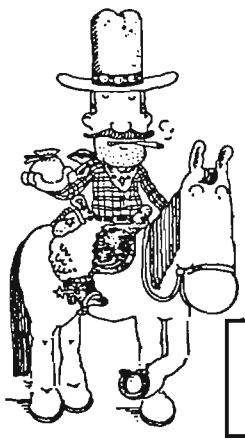
I do not claim, or even wish, that the managers in the Agency should be as good at their jobs as the analysts and technicians whom they supervise That is not their mission in the Agency unless they are "working managers" who put on a set of earphones, man a position, and get into the fray with the rest of the "troops." Only a small percentage of them do so. Once there were a few "player-managers" in baseball, but the fans didn't expect a player-manager's batting average to be the highest on the team. They did, however, expect him to contribute hits and fielding plays to help his team win games. Similarly, a working manager in an Agency voice shop may not have the keenest ear or the biggest vocabulary but he should be able to do a creditable job helping his "team" win their "big game" with his managerial skills.

It is very easy for a manager to say, "Pedro, do this!" or "Pancho, do that!"--even easier if Pedro and Pancho here at NSA, like Yaz, Pete, Reggie, and Gaylord on the ballfield, have been for many years playing the game well with minimal supervision or help from their manager.

There is a particularly great discrepancy here, though, when Pedro and Pancho, after 18 years in the Agency are still grade 12, but most of their non-linguist co-workers have gone on to greater glory. Pedro and Pancho happen to be bilingual native Spanish linguists at NSA, as is Pablo, their manager. If they were "performers" in the major leagues, their performances would have been comparable to batting .340 lifetime with a .989 fielding average and their salaries would have been increased accordingly after each successful season because in the major leagues it doesn't matter if your name is Joe Doe or Pancho Perez, just as long you hit well and field well.

There is something else that I think NSA can borrow from the national pastime. Baseball is willing to make changes, adopt innovations (e.g., the expansion of the leagues, recognition of free agent status, the designated hitter, annual rules revisions, etc). NSA should be willing to make changes too, even if only to see if such "rule revisions" might be better than the existing procedures. In the August 1977 issue of Cryptolog I wrote an article ("Telling It Like It Is") in which I pointed out some of the problems faced by the Agency's Hispanic linguists. Isn't it pathetic that now, six years later, I can write this article since very little has changed? (The only good thing that has happened to linguists in the interim is the introduction of the FLIP [Foreign Language Incentive Program] bonuses).

Former baseball player Joe Garagiola once referred to the impartiality of baseball umpires by saying something like "An umpire doesn't care if a black arm is throwing the ball past a Jewish batter's bat to an Italian catcher's mitt. He's only interested in whether the pitch is a ball or a strike." Maybe we at NSA could use a few such umpires who are concerned with the quality of the job that's being done, not with the ethnic background of the person or persons doing it...and with rewarding those who are doing their jobs really well



Wrangler: One Tough Customer (U)

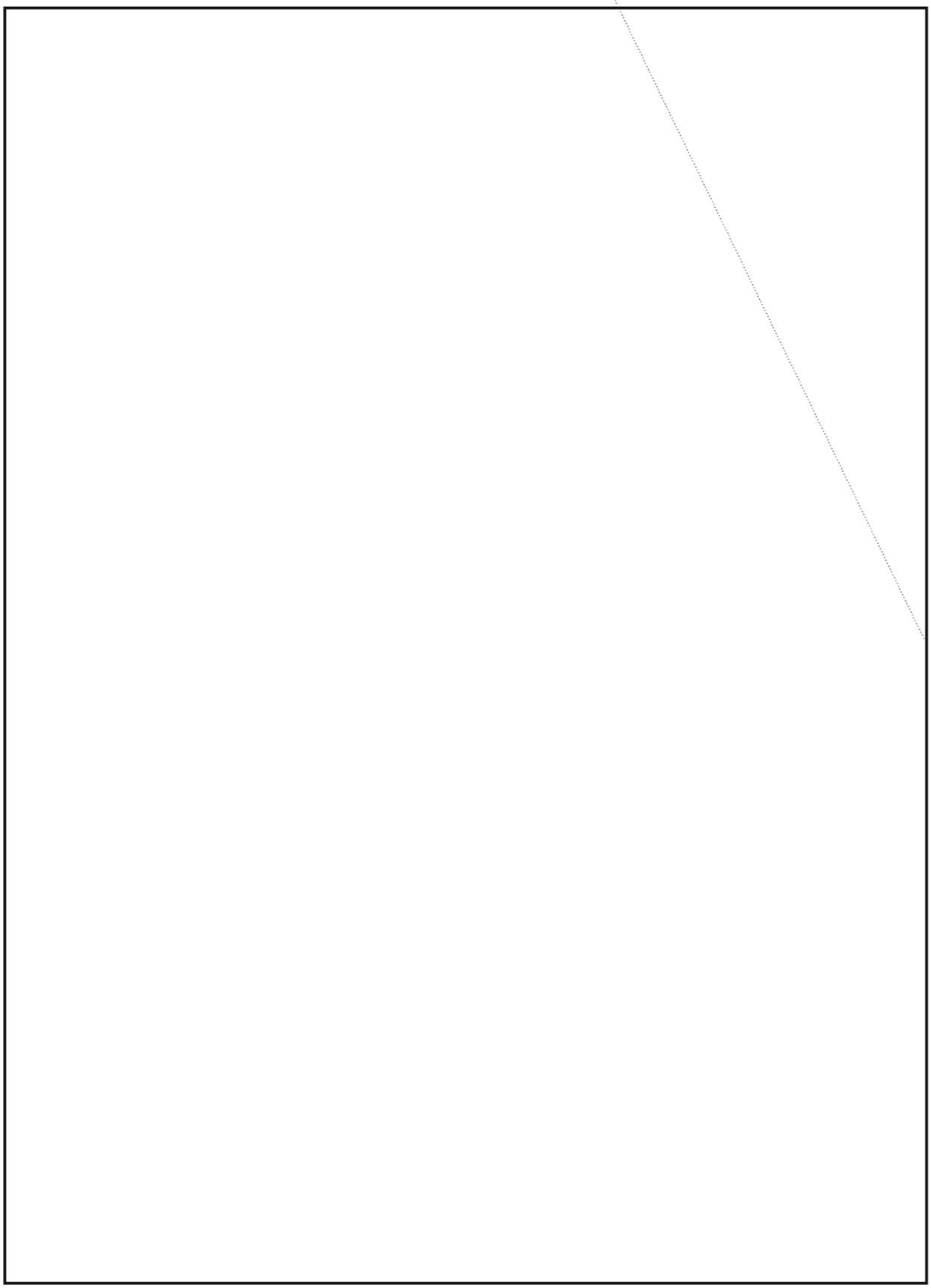
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

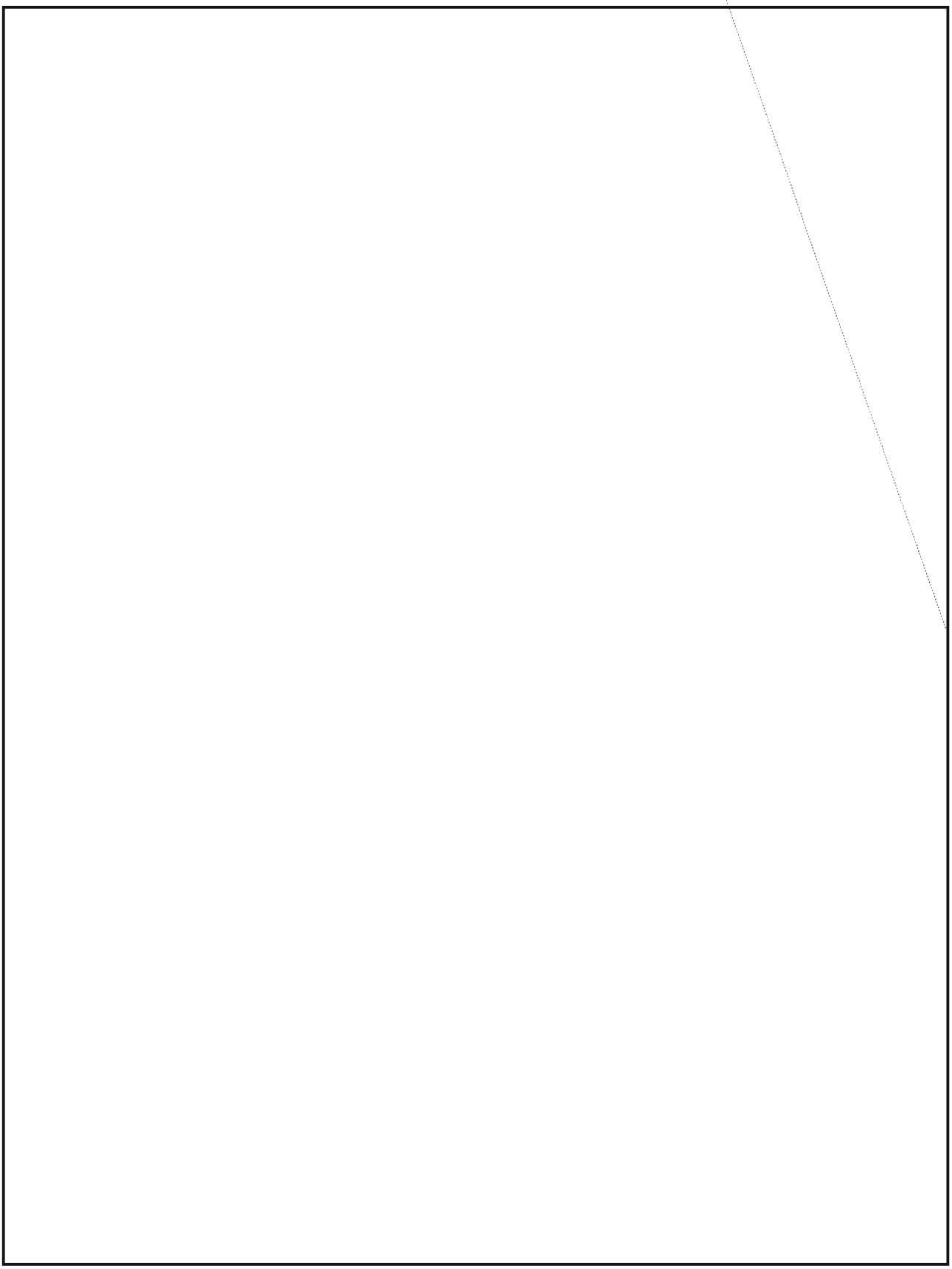
DOCID: 4019697

~~SECRET~~

EO 1.4.(c)
P.L. 86-36



~~SECRET~~



DOCID: 4019697

UNITED STATES AIR FORCE STRATEGIC AIR COMMAND'S RC-135, U-2, SR-71 RECONNAISSANCE PROGRAMS (U)

P.L. 86-36

by [redacted]
Captain, USAF JOCCP

PURPOSE

(U) This paper describes the RC-135, U-2R/TR-1, and SR-71 Peacetime Airborne Reconnaissance Program PARPRO missions from a Strategic Air Command crewmember's perspective. This viewpoint will provide insight into the capabilities and limitations of these air-breathing, airborne reconnaissance systems.

EO 1.4.(c)
P.L. 86-36

BACKGROUND

~~(S)~~ Strategic Air Command (SAC) reconnaissance programs represent the Air Force contribution to worldwide flexible SIGINT support of the intelligence community and our military commanders. With proper support, reconnaissance platforms can fly global missions on very short notice. Although initially tasked prior to overseas deployment, they have the flexibility to fulfill additional requirements once deployed. [redacted]

However, these manned reconnaissance missions provide indispensable intelligence, with the flexibility to satisfy both wartime and peacetime cryptologic needs.

~~(C)~~ Through the Strategic Reconnaissance Center (SRC) at SAC Headquarters in Omaha, Nebraska, SAC acts as the controlling authority for all USAF PARPRO operations. SAC has the responsibility for the operation and maintenance of the PARPRO airframes, while interception equipment maintenance is performed by a combination of SAC and Electronic Security Command (ESC) Personnel and civilian contractors.

~~(C)~~ The SRC coordinates proposed reconnaissance operations with the Joint Chiefs of Staff/Joint Reconnaissance Center (JCS/JRC), NSA, and theater commanders. [redacted]

~~(S)~~ The U-2/TR-1, SR-71, and RC-135, though radically different in design and capabilities, have some similarities:

- [] All are tasked with peripheral area reconnaissance of worldwide target countries;
- [] All are flown by SAC; and
- [] All airborne systems must satisfy dual requirements.

[redacted]

EO 1.4.(c)
P.L. 86-36

TYPICAL CREW COMPLEMENT

	SAC PERSONNEL		ESC PERSONNEL	
AIRCRAFT	Pilot	Maintenance		Maintenance
SR-71	1	-		-
U-2/TR-1	1	-		-
RC-135V/W	2	1		2
RC-135M	2	-		2
RC-135S	2	2		1
RC-135U	2	2		1

EO 1.4.(c)
P.L. 86-36

FIGURE 1. ~~(S)~~

OPERATIONAL BASES

PLATFORM		MOB	
SR-71		Beale AFB, CA	
U-2R/TR-1		Beale AFB, CA	
RC-135V/W		Offutt AFB, NE	
RC-135U		Offutt AFB, NE	
RC-135M		Offutt AFB, NE	
RC-135S		Eielson AFB, AK	

FIGURE 2. ~~(S)~~

~~(C-CCO)~~ A breakdown of the respective aircraft crew positions and command responsibility is shown in Figure 1. The pilots, navigators, and electronic warfare officers ("RAVENS") are all rated flying officers under SAC jurisdoction. Virtually all other crewmembers are enlisted and are assigned to ESC or SAC. Air Force Specialty Codes employed for ESC crews are 205XX (Special Signals Analysis), 207XX (Manual Morse, Radioprinter), 208XX (Linguist), and 328XX (Maintenance). All crewmembers are Category III-cleared, and selected members of the ESC crew have compartmented clearances. SR-71 and U-2R/TR-1 crews usually do not have COMINT clearances.

MISSION/AIRFRAMES

~~(S)~~ All SAC aircraft and crewmembers operate under a concept of employment involving Operating Base (MOBs) and Forward Operating Bases (FOBs). That is, training and major aircraft maintenance for all SAC reconnaissance squadrons are performed at the MOB within the US. For the U-2R/TR-1 and SR-71, the MOB is located at Beale AFB, California (9th SRW). For the RC-135S models, the MOB is Offutt AFB, Nebraska (55th SRW), and for the RC-135 it is Eielson AFB Alaska (6th SRW). From the MOB the SAC crews are deployed for 90 to 160 days per year to FOB locations. SAC RC-135M/V/W ELINT crewmembers (RAVENS) are sent to all FOB locations, and thus become qualified for all areas of the world, unlike ESC personnel, who are permanently stationed in the FOB and MOB countries and accordingly specialize in only their particular geographic area. A chart depicting the MOB and FOB locations associated with each system is found in Figure 2. Although these aircraft normally operate from the FOBs shown, they are able to deploy to many other locations on short notice. Figures 3 through 5 present specific missions and capabilities of each platform. Note that the different models of the same aircraft type have a different airframe/electronic fit (i.e., internal configuration, equipment, engines, and seat placement are different).

[redacted]

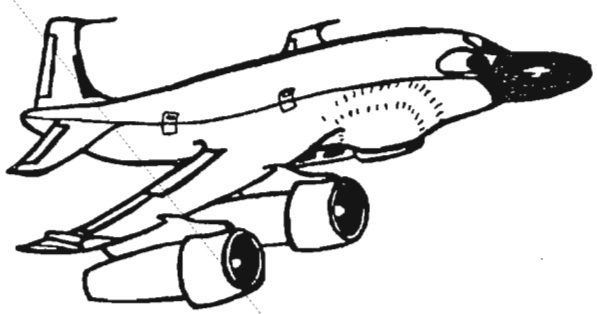
WHITE WOLF REVIEW

~~(S-CCO)~~ WHITE WOLF (WW) is the Advisory Support Program instituted by JCS to provide protection for PARPRO aircraft flying in or near potentially dangerous territory.

[redacted]

OPERATIONAL FACTORS

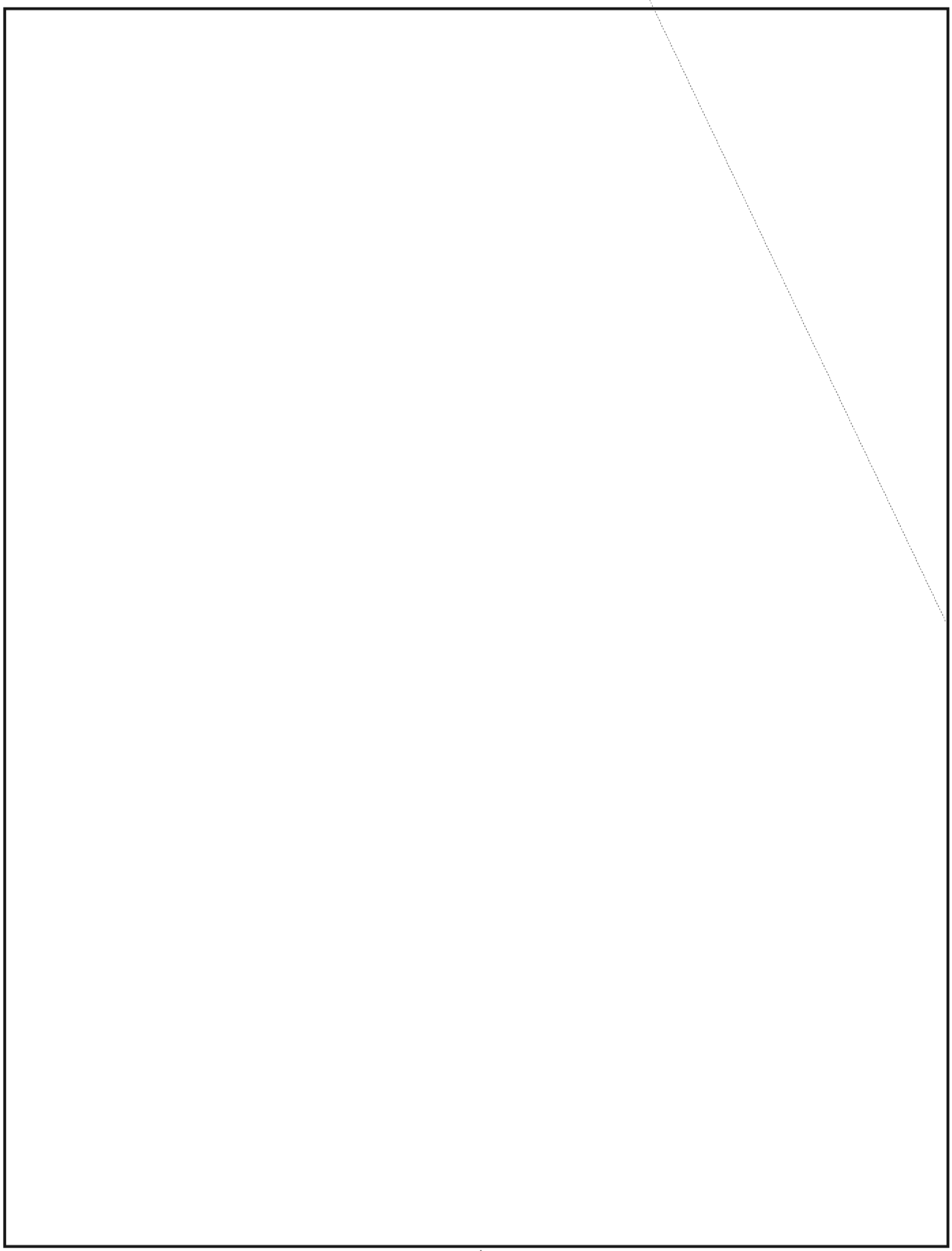
(U) The following information concerning factors affecting the crew is based on the author's experience and provides insight into manned ELINT collection missions. The crewmembers' duty day includes more than the actual flight time. There are five briefings and aircraft checkouts. The flight time limitation for a normal crew is 24 hours. If the crew is augmented (by adding one pilot to the crew of an RC-135) the aircraft may legally stay aloft for 30 hours. Normal mission length is 8 to 18 hours for the RC-135, 8 hours for U-2R/TR-1, and 6 hours for the SR-71. No crew may legally fly more than 125 hours a month or more than 330 hours in a 90-day period. A crew also must be provided the opportunity for 12 hours of rest between flights. These limits are set for safety and health reasons: a crew that flies in excess of 100 hours in a 10- to 30-day period can be physically exhausted by the intensity of the job and and by the physical strain induced by a noisy (120 dB) environment.



EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36



~~SECRET SPOKE~~

(U) Extensive facilities are required to support the aircraft and crew. For example, the SR-71 requires special fuel and special airborne tankers that actually heat the fuel so that it does not turn from liquid to a gelatinous state prior to refueling. All aircraft need specialized maintenance support to include test equipment, military technicians, and civilian contractors. With the complexity of these airborne systems (sometimes one-of-a-kind equipment), quality maintenance support is sometimes difficult to attain. Insufficient spare parts is a common problem. Quarters and messing facilities have to be available for the crew and support personnel because of the MOB/FOB concept. When quarters close to the operations are not available, the additional time spent in transit to and from a base can impact on a crew's rest.

(U) The RC-135 and SR-71 usually need air refueling (i.e., tanker) support. If two tankers are required, then three crew and three tankers must be available in case one aircraft aborts. All PARPRO mission refueling tankers have a spare aircraft and crew scheduled as a backup.

(U) Weather can also be a major factor. Missions are sometimes delayed or canceled due to adverse weather. Crosswinds are a factor in the launch decision, and airfield weather visibility (e.g., due to fog) cannot be less than approximately half a mile horizontal and and 150 feet vertical. Moisture and temperature extremes frequently cause problems with complex onboard electronic equipment.

ADDITIONAL CONSIDERATIONS

(U) On the RC-135 the average time required after takeoff to turn on, check, and calibrate the equipment is 30 minutes. Often computer systems dump the program and need to be brought up several times or restarted during a mission. This occurs as a result of vibration, temperature extremes, and power fluctuations inherent in airborne platforms.

~~(C)~~ PARPRO missions may continue with degraded equipment or totally inoperative stations as long as minimum advisory support capability exists. The maintenance technicians on an RC-135 can work miracles in the air, but many times broken equipment cannot repaired due to a lack of a correct (spare) "black box" or the inaccessibility of equipment.

[redacted]

EO 1.4.(c)
P.L. 86-36

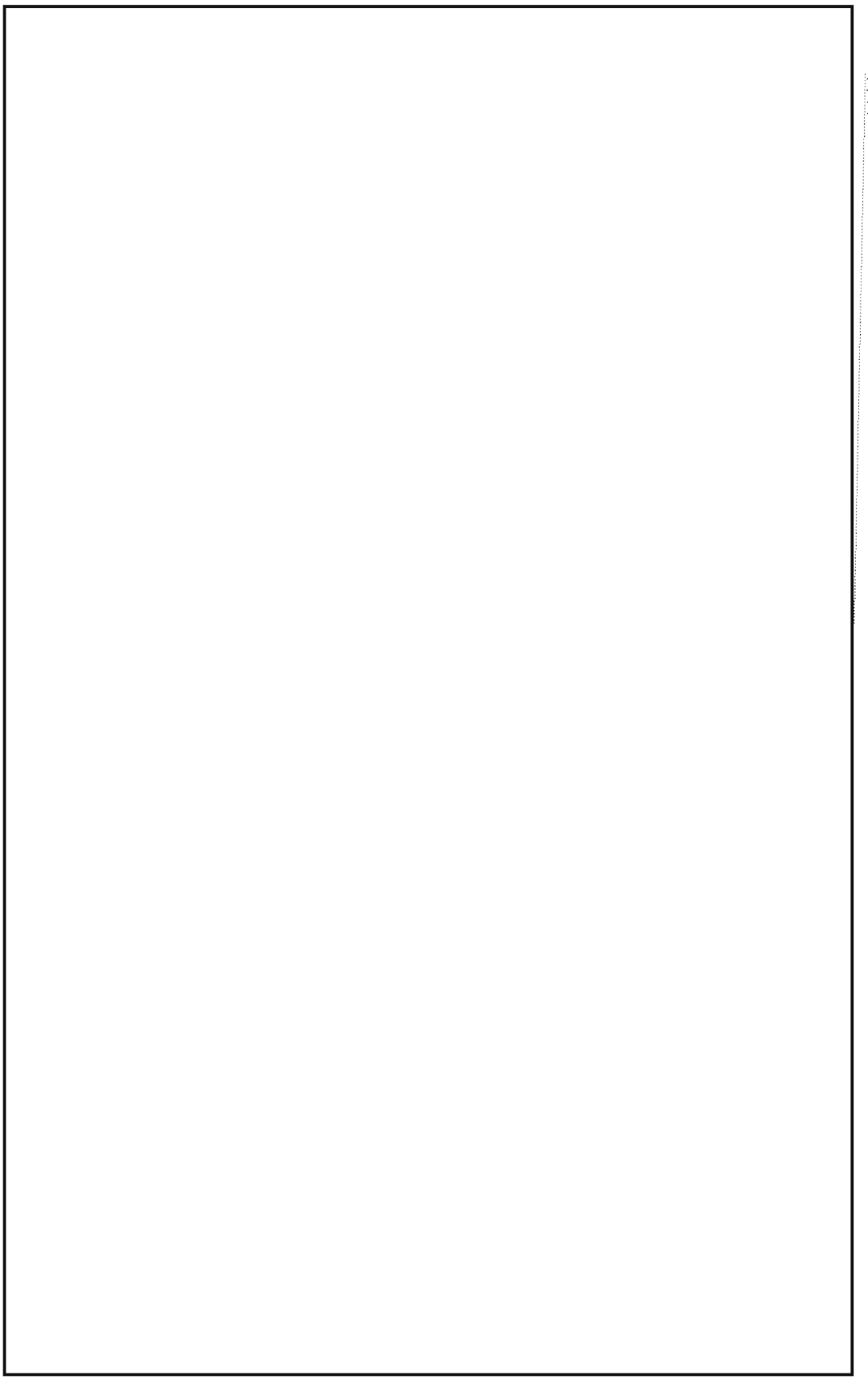
~~(SC)~~ Stress on the crew is amplified by the proximity of hostile interceptors and ground-based and shipborne weapons systems. (Hostile pilots have been known to fly as close as 10 feet to mission aircraft.) All intercepting aircraft are armed while all reconnaissance platforms, with the exception of the SR-71, are without any defensive electronic countermeasures or munitions. RC-135s do not even carry Radar Warning Receivers (RWRs). The crewmembers view the lack of an RWR with concern.

[redacted]

EO 1.4.(c)
P.L. 86-36

CONCLUSION

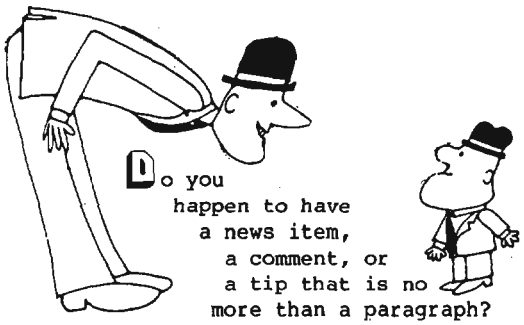
~~(C)~~ In this article I have presented some facts and opinions about PARPRO that may not be common knowledge. The missions collect intelligence in much the same way as other systems. However, the missions also have some radical differences, and the risk factor is much higher. There are many factors that affect the SAC PARPRO missions that are not present in conventional collection systems, including a lack of NSA control. Hopefully, this paper will facilitate an understanding of, and an appreciation for, the special capabilities and some of the limitations of the PARPRO missions. This additional knowledge may allow more optimum tasking and efficient management of these systems.



EO 1.4.(c)
P.L. 86-36

DOCID: 4019697

Contributions Solicited



Do you happen to have a news item, a comment, or a tip that is no more than a paragraph?

Or perhaps you have an article of several thousand words? Never mind how big it is! Long or short, if it has something worthwhile to say, we'll probably print it. Of course, a shorter item has a much better chance of getting read.

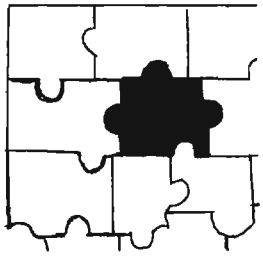
First-person articles or stories about your own experiences are welcome, so long as they relate in some way to our work.

[redacted]

EO 1.4.(c)
P.L. 86-36

Want anonymity? A thoughtful piece on a subject of interest to a fairly large number of readers will be considered for anonymous publication, if the author requests it. If you want to use a pseudonym, that is OK too....but the writer must identify himself or herself to the editor in an accompanying memo or by phone. Needless to add, a personal or trivial complaint (e.g., "My supervisor takes government paper clips home from the office") will not be considered.

Something missing? If you feel that your work or your interests are not being well represented in Cryptolog, it is probably because you and your friends are not contributing. The editors sincerely want to cover the whole territory of NSA's interests, but articles don't grow on trees, y'know! Somebody who knows the subject matter has to write them!

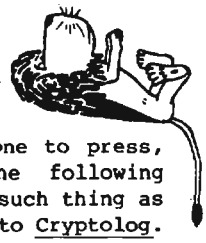


Your contribution does not have to be typed. We'll give preference to content over form every time. However, especially in the case of a long piece, the editorial eye will appreciate any effort you can make to get your article typed (and we'll even forgive a strikeovers and misspellings). Nowadays, of course, if you have access to a terminal connected to the Agency network, you can simply send it to us at cryptolg@bar1c05 and we can do our editing right at the terminal. But we have also accepted an item handwritten on a used lunch-bag.

Photographic illustrations can be reproduced in Cryptolog at the same quality as in the NSA Newsletter.

Sensitive materials?? No way!!!! We'll publish articles all the way up to TOP SECRET CODEWORD, but we have to draw the line at compartmented or otherwise exclusive sources.

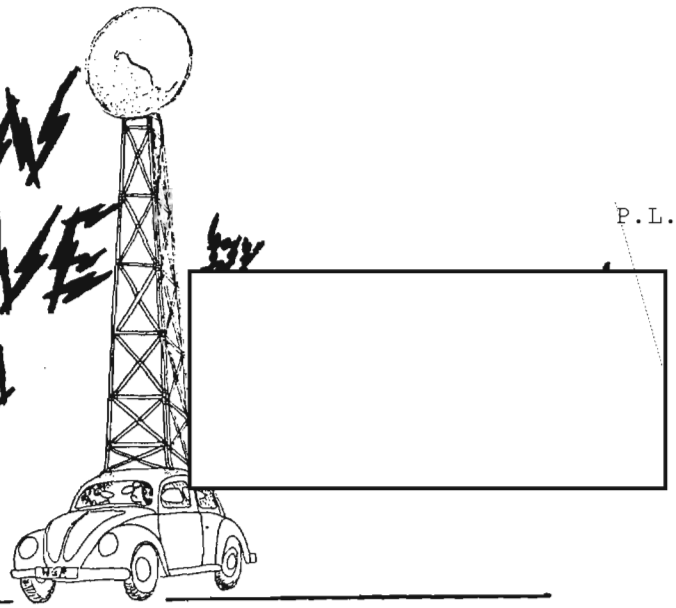
Need assistance? You may have a half-finished article, or an outline, or some incomplete notes, or maybe just an idea about an item you'd like to write, something you feel has possibilities but you aren't quite sure what to do with it. A quick call to the appropriate departmental editor (or the Assistant Editor, ext 1103) will probably get you the aid and comfort you need. It may even give you the inspiration to finish your magnum opus!



Our deadline? Theoretically we should have one, but we don't. After all, Cryptolog is a monthly publication, so if we get your article just after one issue has gone to press, you'll be in time for the following month's edition. There's no such thing as a bad time to submit an item to Cryptolog.

DOCID: 4019697

FOREIGN MICROWAVE RADIO



by

[redacted]

P.L. 86-36

(U) Hungary is the center for microwave radio technology in the Eastern Bloc, doing both R&D and production of new microwave radio equipment for Russia and the other Bloc nations, according to Dr. Ferdo Ivanek of Farinon Corp. In a recent talk to an IEEE Microwave Technology class at the University of Maryland, Dr. Ivanek showed some slides of the new 120-mm "Slimline" equipment that the Hungarians are building and remarked that they do very good work and publish their results. Journals such as Budavox and HiradÁstechnika carry articles on new data, switching, and telephony systems (in Hungarian).

(U) Before World War II the Hungarians were doing advanced work in commercial radio equipment, although the Czechs were ahead in consumer electronics. Bombing and other war operations apparently did not severely damage the Hungarian industrial base so that they were able to catch up with Western developments. The Hungarians have recently developed a baseband equalization processor to correct channel distortions of microwave baseband signals, with the result that they can now transmit 1,800 voice channels over the same radio bandwidth that formerly carried a 900-channel FM signal. In their laboratories they commonly develop very modern equipment, using components and other microwave devices imported from the West or Japan. However, Dr. Ivanek pointed out, the Soviet policy of economic autarky insists that all radio production equipment must use domestically produced components which are manufactured in the Soviet Bloc. Because the Bloc nations are not able to manufacture the most modern components, a 10-year lag occurs while the manufacturing problems are being solved, and the equipment is obsolescent by the time it gets into large-scale production.

(U) The demand for autarky produces a backlog of unsatisfied needs, so that at times the USSR and its satellites must go on a "buying spree" to get vitally needed equipment. The USSR is currently buying a considerable amount of telecommunication equipment abroad. According to one comment in the class, the USSR has bought some L. M. Ericsson AXE switches and has written unusually favorable comments about these switches. Dr. Ivankek said that Tellettra, a Fiat subsidiary, had sold the USSR a large 4-GHz trans-Siberian radio relay system.

(U) The demand for autarky not only limits the market for equipment, but Dr. Ivanek expressed the strong opinion that the Soviet Bloc nations would have their own clocks and timing standards for the digital nets they were developing rather than derive timing from the Western European PTT nets.

(U) One of the implications of Dr. Ivanek's comments about the leading role of the Hungarians in this area of microwave technology is that the Hungarians may be able to sell equipment to the Western market which will later be used in the Soviet Bloc nations, after the inevitable lag in solving the manufacturing problems of producing domestic components. Further, the Hungarian literature and the appearance of the Hungarian vendors at trade shows such as Telecom 83 may give valuable information about microwave radio technology that will later appear in the USSR and other Bloc nations. A survey of some foreign technical data showed 33 papers on Hungarian microwave equipment. In addition, abstracts of Hungarian papers are available from computer data bases.

(U) The major differences, from a business point of view, between the US and the foreign

microwave radio market are, according to Dr. Ivanek:

1. Market size;
2. Equipment characteristics;
3. Monopolies vs deregulation;
4. Technical standards;
5. Domestic industrial capability; and
6. Commercial versus military applications.

(U) In market size, the once fragmented European market has caught up with the North American market, and the Asian market is expected to catch up with the North American by 1990. Latin America by 1990 will have about 30 million subscriber lines, roughly equal to the 1970 Asian market. The African and Oceanian switched public telephone plant will remain small compared to all the others. (Dr. Ivanek drew on a Telecom 79 report by Kamman et al of A. D. Little which forecast the telecom market.)

(U) Number of telephones (millions)

Year	1970	1980	1990
North America	80	110	140
Europe	50	110	210
Asia	30	60	140
Latin America	10	17	30
Oceania, Africa			10

(U) Operating Revenues (billions of 1979 $)

Year	1975	1980	1990
NA	35	67	122
Eur	26	57	164
Asia	17	38	80
LA	2	4	9
Oceania	1.6	3	4
Africa	.6	1.5	4
	81.6	171	383

(U) Shipments of Telecom Equipment (in billions of 1979 $)

	1970-80	1980-90
NA	62	103
Eur	76	196
Asia	40	59
LA	6	15
Africa	1.6	5
Oceania	3	7
	198.6	385

(U) Shipments by Equipment Type (in billions of $)

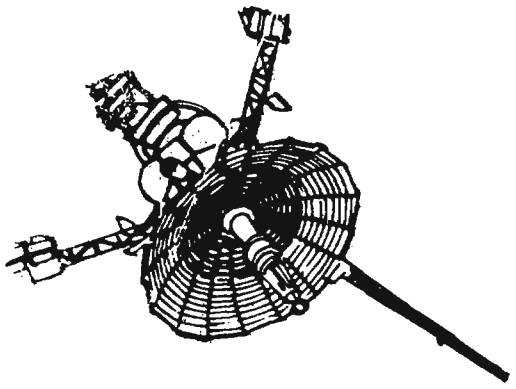
	1970-80	1980-90
C.O. switching	47	92
Long-Haul Xmsn	27	53
Local Dist.	60	117
Station Apparat.	35	68
Other	17	35
	186	365

(U) Of this extensive plant, worldwide sales of microwave radio transmitters and receivers will comprise about $10 billion per decade, or $1 billion annually (in 1979 dollars).

(U) Only a small part of the European market is open to competitive selling, because of the power of the PTTs to control telecommunication procurement and design. US industry has a lesser commitment to export sales than manufacturers in Europe and Japan. For example the exports of French microwave radio relay equipment over the past decade have been almost the same volume as the sales to the PTT, despite an intensive program of microwave installation inside France. The CNET (the French version of Bell Labs) sponsors development projects with the French companies SAT and Thompson-CSF to build the same equipment. In some product categories the two companies are given monopoly positions, while in others they compete head on. Part of the CNET microwave development plan includes equipment by SAT or Thompson CSF which is exclusively for export--there is no internal French market, yet the government, through CNET, subsidizes the development. The French government also does careful market research for telecom equipment.

(U) The German PTT (Bundespost) does not go as far as the French in sponsoring export activities but it does keep the door open for marketing of German equipment through participation in the CCIR (the International Consultative Committee of Radiocommuncations), where international standards for equipment are set in a way that helps German exports.

(U) Examples of markets developed by the French are Mexico and Brazil, which use CCITT equipment and standards and no longer follow North American standards. Latin America, Asia. Africa, Oceania, and Europe all have adopted CCITT standards. Only the US, Canada, Japan. Soth Korea, and Taiwan still use primarily North American telecom standards. This seriously limits the exports of US radio equipment, switches, digital systems, modems, and all the rest of modern telecommunication apparatus.



(U) At CCIR and WARC meetings, the US delegations, formed primarily of business people (whose technical expertise is usually much greater than that of US government officials), the US technical people are very capable in the satellite communications area and are very influential in the outcome of the conferences. In the terrestrial radio area (which is the main medium for telecommunications), the US delegations are apparently not as capable as the foreign delegations (possibly because they don't work to CCITT technical standards). Dr. Ivanek thought that the US radio industry, composed of many competing companies, needed some coordinating structure, similar to the centralized research entities that Electronic Industries Association (EIA) and Microelectronics and Computer Technology Corporation (MCC) have formed for components and microcircuitry, in order to compete more effectively in the world market.

(U) In addition to making these general observations on foreign microwave, Dr Ivanek displayed a number of slides of specific equipments from various foreign manufacturers to illustrate current developments.

(U) To begin, there was a slide of the first microwave link, developed in 1934. The British and French PTT collaborated in a cross-Channel one-hop link. It used a triode for power and operated at about 2 GHz. A parabolic antenna about 3 meters in diameter was used, predating the postwar European microwave nets by almost 20 years.

(U) A map of the French microwave network, in its current state, showed a large number of disconnected star nets. The digital trunks operate at 52, 34, 2 x 34, and 140 Mbps. These trunks connect into digital switches (which the French pioneered) into regional centers. The French are introducing digital microwave from the bottom up, on a regional basis, where the existing equipment is ready for replacement. In the Lyons area they have 2-, 8-, and 34-MBps trunks. They also have new 15-GHz nets operating at 2, 8, and 34 Mbps. They use the digital trunks to connect the E-10 digital switches. The nets are stars. There is no French equivalent of a Long Lines grid or trunk system such as AT&T uses. When the French begin to interconnect their regional centers, they will use both digital radio relay and optical fiber, according to Dr. Ivanek, since the failure modes of the two media are quite different.

(U) The UK has digital microwave nets at 140 MBps at 11 GHz. Germany has digital trunks at 2, 13, and 15 GHz. Italy has digital nets similar to the French. Switzerland has digital nets for data transmission (where the other nets are for voice or data).

(U) Analog microwave radio is still flourishing, and the Japanese have developed a 5400-channel SSB system at 6 GHz, very similar to the 6000-channel Bell System. The Germans and French are working on similar SSB systems, but have not yet introduced them.

(U) In Switzerland they have built up microwave feeder links to cable TV distribution systems. The feeder links operate at 2.5 GHz and the distribution net works at 11 and 12 GHz. The Swiss can put two independent TV baseband signals on a single radio carrier by frequency multiplexing so the distribution system is very efficient.

(U) A map of the African microwave net PANAFTEL, from the ITU, showed substantial development in subsaharan Africa. This large network had resulted from a substantial amount of ITU assistance.

(U) The development of microwave in the PRC was covered in a January 1983 issue of Microwave System News.

(U) India has been manufacturing some of its own microwave equipment, and there was slide of a portable remote satellite earth station mounted on a truck, which the Indians had developed themselves. There was a slide of some new "Slimline" 120-mm-wide racks of equipment which the Indians were manufacturing.

(U) This new Slimline equipment, pioneered 20 years ago by the Germans (to save space in switching centers and microwave terminals), is also used in Yugoslavia and Eastern Europe. The French use it widely. In the US, only two companies make Slimline. Western Electric makes a 5-inch-wide "American" Slimline series while Farinon make CCITT-specified 120-mm Slimline equipment.

(U) As the US market is opened up by deregulation, the US telecommunications companies are gradually accepting some European designs. This reverses a long trend from 1945 till now in which US microwave circuitry was exported and became the standard in most countries. There are still many US-standard microwave equipments installed and operating as analog circuits in many countries. The change to digital transmission will see CCITT equipment dominate. Some US manufacturing companies are developing CCITT versions of their existing tested equipment (e.g., the GTD 120E and GTD 1000E PABXs are being adapted to 32-channel PCM CCITT and CEPT standards.) The microwave technologies and manufacturing methods developed by the US companies have been widely adopted overseas, but the end products differ. In analog microwave systems the interface problems are not as severe because the frequency multiplexing plans are in common use by many different manufacturers. In digital microwave systems there is a great deal of product differentiation in the technical characteristics, especially among competing US manufacturers, so that digital interfaces are more difficult to handle.

(U) US users of high powered microwave transmitters depend on foreign suppliers of TWTs (traveling wave tubes), e.g., Siemens and Thompson CSF. The TWTs are smaller and much more efficient than arrays of solid state power amplifiers; e.g., the solid state unit would consume 100 watts of power to radiate 10 watts, while a TWT would need only 20 watts to radiate 10 watts. The extra power must be dissipated as heat, and in space applications power limitations are also critical.

(U) US users of GaAs (Gallium Arsenide) components must also depend on foreign suppliers, particularly Japan. The GaAs FET (Field Effect Transistors) are crucial to microwave receiver designs and other analog microcircuits. Western Electric produces its own GaAs FETs but the other US users must obtain their components from Japan because WE has not put its components on the commercial market.

(U) Technical standards play a central role in the development and sale of microwave equipment. The CCIR is the principal agency for setting radio standards. It is slow but effective. There is no voting in the CCIR and decisions are arrived at by consensus, so that persuasion by technical representatives of the various countries is the method used to get decisions. The Japanese, who are major producers of advanced microwave equipment, are very active in the CCIR. The CCIR studies in microwave began in 1948 in Sweden. In 1951 in Germany a study on wideband radio relay, for TV distribution, was undertaken. Successive CCIR meetings in London in 1953 and Warsaw in 1956 continued this work. The main purpose of terrestrial microwave in Europe (and the US) at first was the distribution of TV broadcasting. The wideband microwave systems predated wideband tape recorders, so central studios could transmit over a network to local VHF broadcasting stations. Multichannel telephony came later, as filters and other components were developed. The USSR, although a CCIR member, would never agree to 5-MHz baseband for wideband TV transmission and, as a result, the TV baseband in COMECON is 6 MHz. This apparently was to prevent any TV interfaces between Western and Eastern Europe, according to Dr. Ivanek.

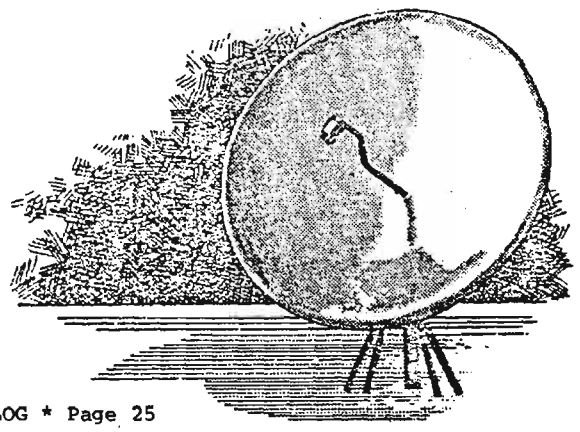
(U) Among operating microwave systems, the Japanese 400-Mbps system at 20 GHz is the highest capacity digital system in use, while the Western Electric 6000-channel AR6 is the highest capacity analog system in use.

(U) The very high efficiency of the SSB analog systems could have a significant effect on communication satellites, which are widely expected to become "all digital" by 2000. Because of bandwidth limitations in the lower microwave frequencies (under 10 GHz), the SSB analog FDM systems may be much more efficient than digital systems for most telephony.

(U) India, which lost an INSAT satellite recently, is preparing a ground station network in anticipation of a future satellite.

(U) Brazil, according to Dr. Ivanek, has serious intentions for a major domestic satellite program, using several satellites under its own operational control.

(U) AEG Telefunken has developed an 11/14 GHz (i.e., 11-12 GHz and 14-15 GHz bands for satellite transmission) regenerative repeater for digital microwave. This eliminates the need to demodulate the radio signal to an IF (intermediate frequency). This will allow onboard baseband switching on a satellite. The system is designed to operate at 120 Mbps differential QPSK (4-phase shift keying) demodulation. The hardware already exists.



(U) In France the CNET uses SAW (Surface Acoustic Wave) devices in satellite communications, for filters, digital modulators, up converters, down converters, demodulators and receiving filters. The SAW circuits are very compact, about the size of a 1-franc coin, and the link operates at 2 Mbps.

(U) In Japan a commercial satellite uses spread spectrum for two voice channels. The PN (pseudo noise) code is generated by an 8-stage register at 16.6 Mbps which transmits an information band of 65 Kbps. The Japanese also use spread spectrum for equatorial communications.

(U) An SR system in Canada uses an analog PPM TDM system at 1.5 GHz for rural communications. The system can accommodate 120 subscribers. The terminal units and transceivers are hung on a pole at the subscribers' premises.

(U) In France at Thezillieu an IRT 1500 TDMA system at 1.5 GHz is in use. The IRT 1500 (Integrated Rural Telephone) systems uses FSK for 832-Kbps transmission to 128 subscribers at 63 stations. Hops as long as 40 Km are in use.

(U) The Japanese NTT has developed a microwave overlay system that consists of a rooftop or desktop 26-GHz microwave system. The desktop model has a telephone and a shiny 12-inch parabolic antenna that sits on a desk or table. The radio links will operate over 7-Km hops at 2 Mbps. A voice channel over the radio link uses 64 Kbps per subscriber. The transmission power is 27 dBm, and the frequency stability is 0.0001. Modulation is DFSK and the system will carry 100 channels. NEC is to produce this new system. The purpose of the desktop 26-GHz system is to provide an urban area overlay system which will allow office computers and desktop computers to interconnect between tall buildings. The existing twisted pair cable systems will not carry the high data rate, so the microwave equipment allows dedicated nets to overlay the civil plant. The Japanese have tested the system and are confident that it will operate reliably through the rainy environment in Japan. This implies that the 26-GHz digital desktop microwave system will work almost anywhere in an urban area, and will allow dedicated digital nets to be set up in any city without waiting for improvements in the existing public networks. There is even a portable voice channel service set, so that a technician can test a new or existing station without using the fixed equipment. This should be a very flexible modern system, especially for dedicated nets.

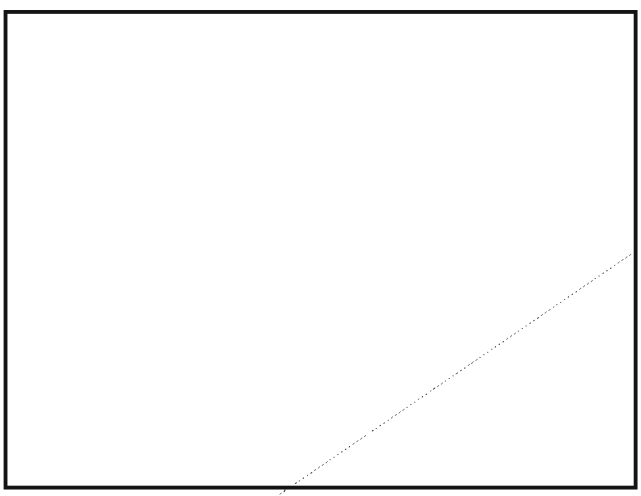
(U) Summing up, the foreign developments in microwave are as good technically as modern US equipment. Some of the new foreign systems are very well designed from a marketing standpoint. The spread of CCITT standards to almost every nation except the US and Canada gives the foreign microwave manufacturers much easier access to the world market. The US companies have been sluggish in responding to this technologic and regulatory change.

Analysis

(U) Hungarian equipment and technical literature could be a fruitful source of information about microwave systems which will be used in COMECON. The apparent 10-year lag time in developing the component manufacturing capability would give some lead time for the development of SIGINT systems to deal with the new microwave technology. In addition, export control policies could be designed to lengthen the lag time for COMECON manufacture and use by blocking access to the manufacturing technology for critical components used by the Hungarians in their development models. The Hungarians may also be concerned with digital switching and protocols since the digital microwave must interface into the switches.

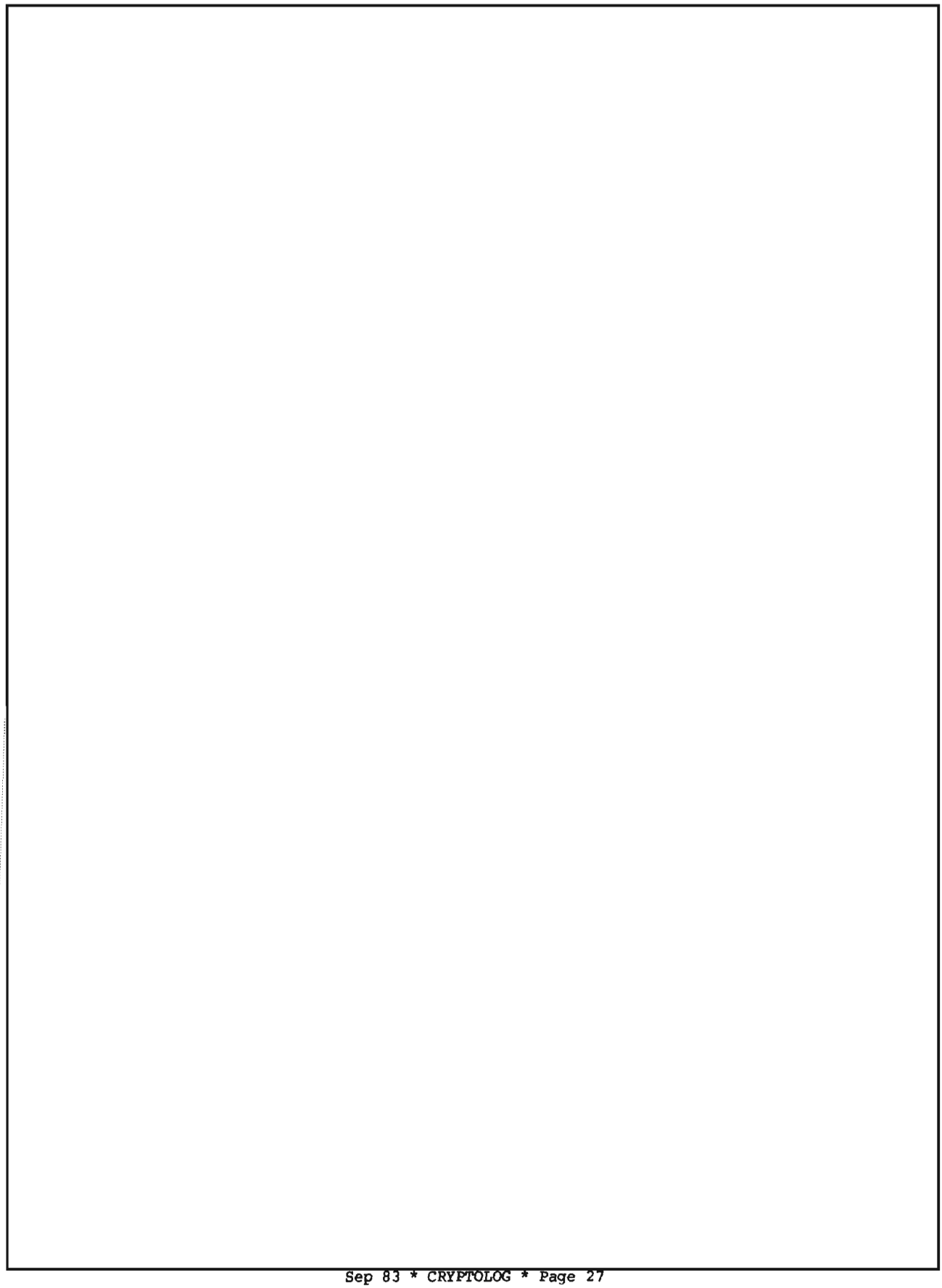
(U) The possibilities of the Hungarian telecommunications industry as a bellwether of Soviet telecommunications could be explored by literature searches, interviews with Dr. Ivanek, and various conventional methods of gathering information.

(U) The expected massive growth of telephony in Europe and Asia points to fruitful SIGINT opportunities. The telephone growth will be directly related to rapid economic growth in those areas. The substantial spending on local distribution ($117 billion) during 1980-90 implies that the local nets will be valuable access points for SIGINT.



EO 1.4.(c)
P.L. 86-36

DOCID: 4019697



EO 1.4.(c)
P.L. 86-36

DOCID: 4019697

~~FOR OFFICIAL USE ONLY~~

NSA-Crostic #50

Here's one in the cryptic vein

A. Bethlehem, before it became a big city (2 wds)

5 18 100 68 128 79 28 137 71 177

B. Scopes trial movie is whither I intend to go (3 wds)

105 89 114 9 186 160 39 19 147 56 144 22

112 132

C. For no reason he brought needles, sly dog

121 20 47 182 127 151 108 145 12 25

D. Is he crabby? Why no, just a whiner

97 63 57 165 54 32 183

E. Judy Garland's best-known song (2 wds foll. by Word U)

155 46 152 173 133 185 111

F. Light up for prospector's fortunate find (2 wds)

30 156 51 74 33 35 146 159 176 150 24

G. Cranny leader

37 106 67 31

H. "_____ of Texas" (4 wds)

96 70 41 153 50 163 104 15 189 110 77 122

157 136

I. Death row inmate anticipates Toffler book (2 wds)

169 34 113 174 17 3 76 40 180 117 23

J. Fall of a Mau Mau nut

130 59 123 75 53 107

K. Are inflexible prigs uncommon? I say yes

1 92 43 49 149 184 181 98 119 13 81 162

8 178

L. Castle bird

87 72 118 55

M. Australian server

115 48 143 99 10 135

N. Why do you brag at a large turnip?

166 27 161 187 64 29 11 126

O. See hopes for African tomb-builder

103 134 148 82 86 2

P. For you plus me it can be rash

141 124 78 91 188

Q. Palindromic body part

139 116 120

R. Ida ran a hotel off the coast of Ireland

102 73 94 131

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019697

S. Familiar thoroughfare for Bob, Bing and Dottie — 80 90 140 66

T. Interrogative — 179 69 171

U. See Word E — 101 6 45 83 170 88 16

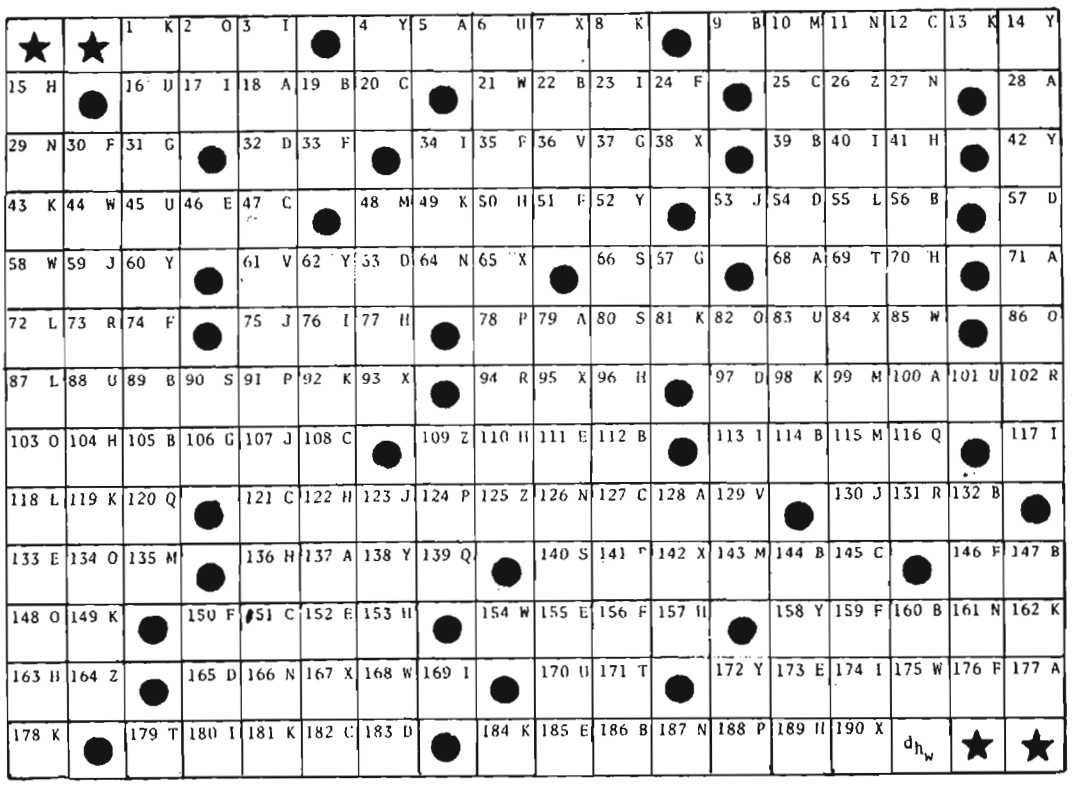
V. Intravenous feeding at Harvard or Yale? — 36 61 129

W. Bring back lonely tea bag for headache — 44 154 21 168 175 58 85

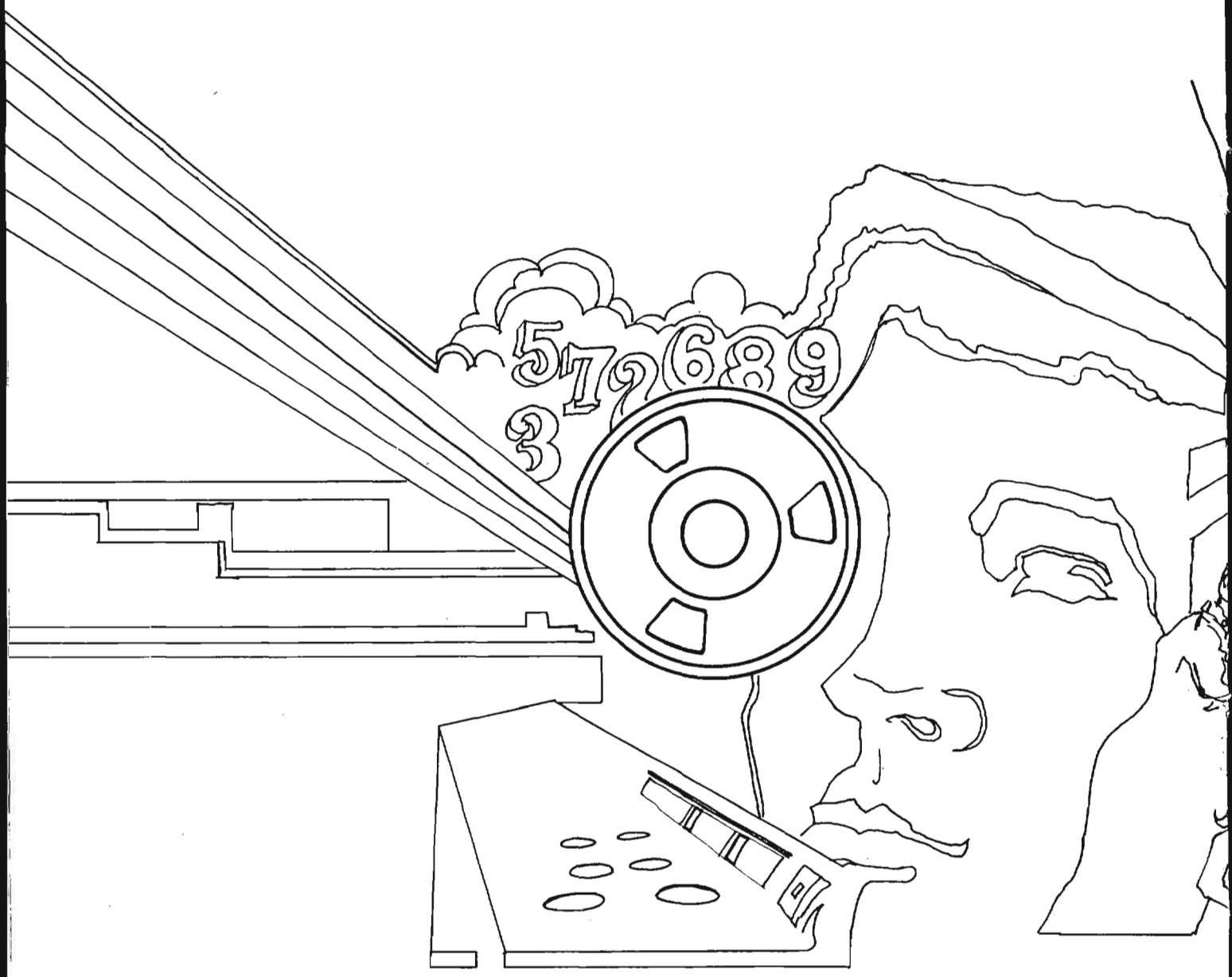
X. Mica is in glasses or cups — 167 190 7 95 38 142 84 65 93

Y. Renew spa personnel's *Times* subscription — 138 52 158 14 4 42 172 62 60

Z. Develop tier between F and H — 164 125 26 109



P1-Jan 84-83-42192


5 7 2 6 8 9
3

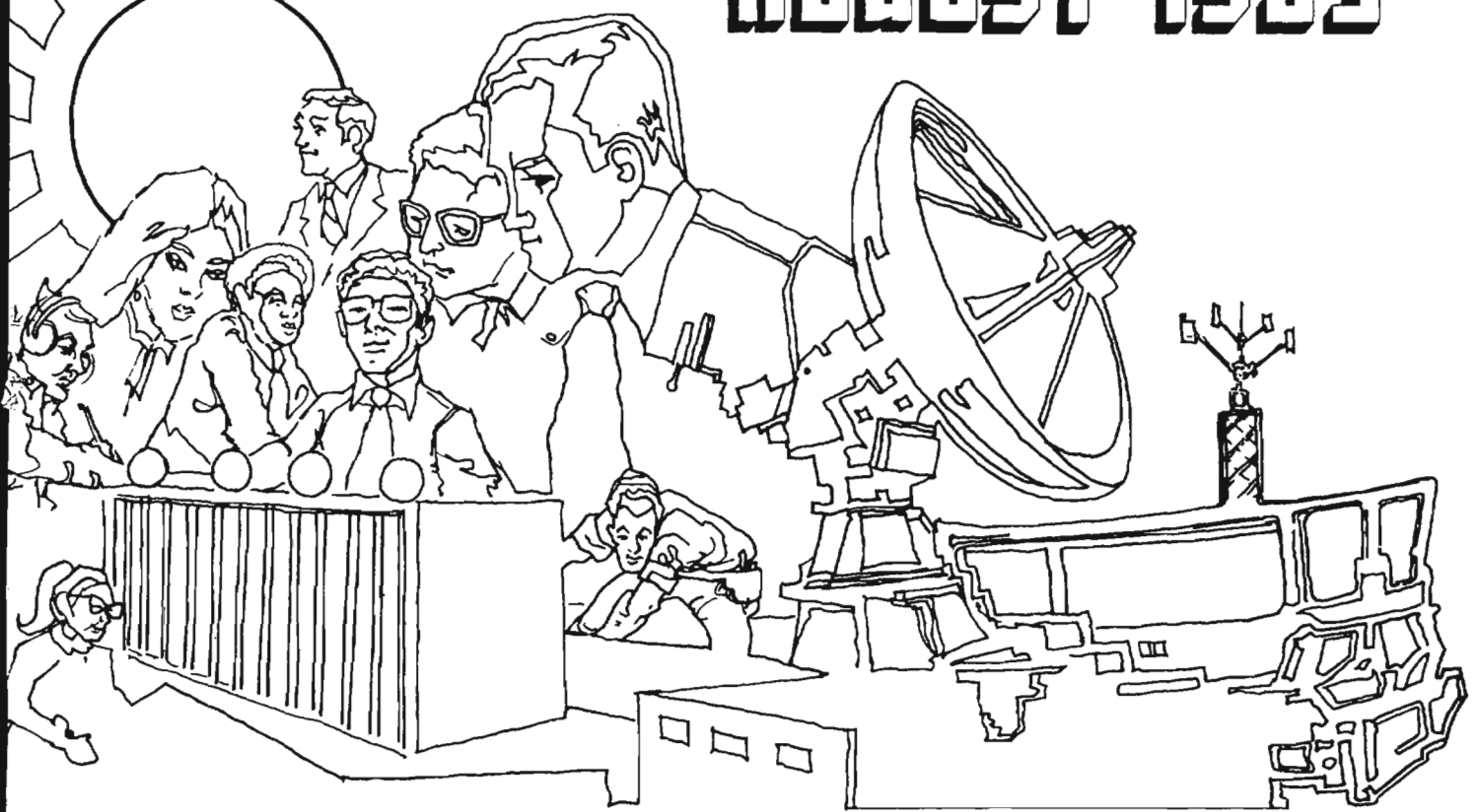
DOCID: 4009865

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

AUGUST 1983



P.L. 86-36

THE CASE OF THE 'FOWLED-UP' CRITIC (U) ..... [redacted] 1
DOES YOUR OFFICE MAKE YOU SICK? (U) ..... [redacted] 7
LETTERS TO THE EDITOR (U) 9
I REMEMBER MABEL BABEL (U) ..... [redacted] 11
REVIEW: THE BATTLE FOR THE FALKLANDS (U) ..... [redacted] 14
NSA-CROSTIC NO. 49 (U) ..... David H. Williams 20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating~~

~~SECRET~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009865

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. X, No. 8 AUGUST 1983

PUBLISHER [redacted]

BOARD OF EDITORS

Editor..... [redacted] (963-3045s)
Asst. Editor... [redacted] (963-1103s)
Production..... [redacted] (963-3369s)

Collection..... [redacted] (963-3961s)
Computer Security
..... [redacted] (968-7313s)
Cryptolinguistics. [redacted] (963-1103s)
Data Systems..... [redacted] (963-4953s)
Information Science
..... [redacted] (963-5711s)
Mathematics..... [redacted] (968-8518s)
Puzzles.....David H. Williams (963-1103s)
Special Research.....Vera R. Filby (968-7119s)

For subscriptions
send name and organization

to: [redacted] P14
(963-3369s)

P.L. 86-36

To submit articles or letters
by mail, to: P1, Cryptolog

via PLATFORM mail, send to:
cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no 'O' in 'log')

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

We are always looking for articles, letters, and technical material that might be suitable for publishing in Cryptolog. We think of the magazine as a technical bulletin board so that people at one end of the building can keep up with what is going on at the other end of the building.

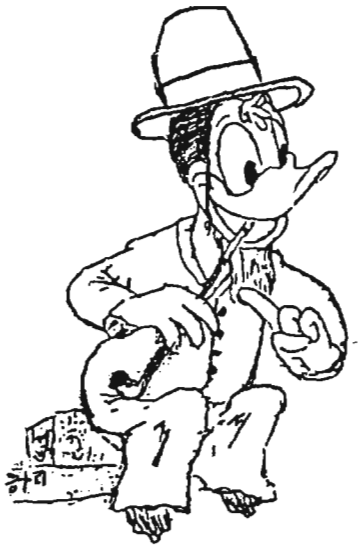
There are some restrictions on material we can use. First, we must know who the author is. We will consider publishing material anonymously, but either the editor or the assistant editor must know who the author is. We stress this because we have received some material without the author's name, but it will not be published (no matter how interesting) unless the author(s) contact one of us. Sorry about that.

Another restriction involves reviews and comments about current books that discuss the Agency. We have received such items from time to time but have had to reject them, usually for legal reasons.

Aside from the legal aspects, there are practical reasons for avoiding the subject. Let's say that Constant Blabber puts a bunch of ridiculous stuff about NSA into his latest book. We review it and point out the errors. Then he brings action to get copies of everything we have that mentions him or his dumb book. If we happen to have your manuscript in hand, and it mentions ole Constant, then your item is fair game for him, too.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009865



The Case of the 'Fowled-Up' Critic(U)

P.L. 86-36

by [redacted] Q42

(U) The old adage "Things are seldom what they seem" is nowhere more true than in the fascinating world of SIGINT. This is particularly applicable to military SIGINT targets, to which this article is restricted.

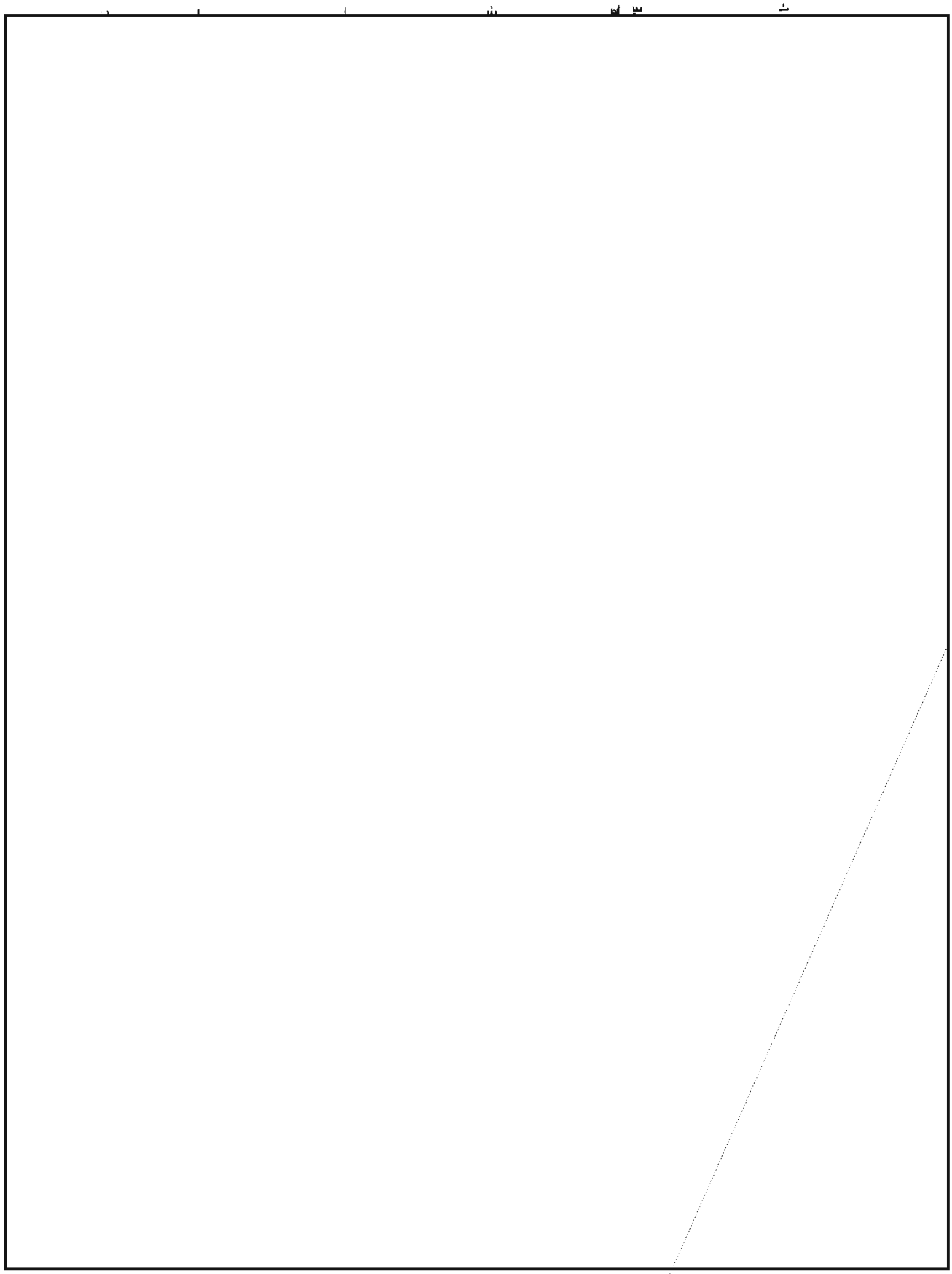
(U) For some time now, I have thought about describing in anecdotes ways in which natural phenomena can conspire to complicate the lives of SIGINT analysts and reporters--and of the users whom they support. The main intention here is not only to amuse but also to show that the answers to seemingly complicated SIGINT questions often lie in the strangest, yet most "natural" places. In fact, sometimes the answers are so simple as to be labeled "ridiculous" by many, but they are nevertheless true. A second intention is to demonstrate the value of judicious use of collateral sources in explaining events which, based on SIGINT alone, may present an entirely different view.

(U) Although I have selected humorous titles for the two episodes in this short series, the SIGINT facts are presented exactly as they occurred, as are the collateral additions. Intrigued? I hope so! Read on!

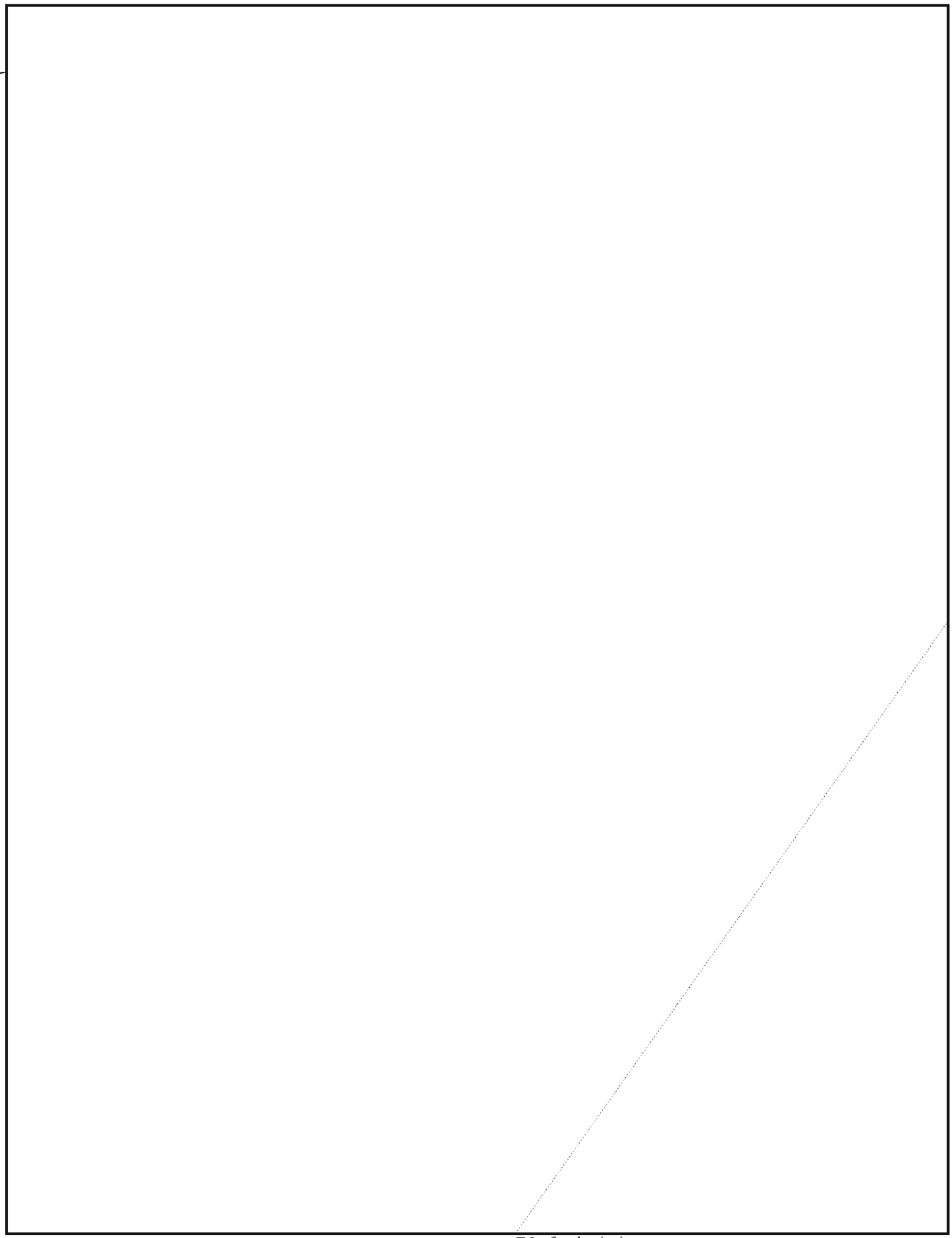
[redacted]

[redacted]

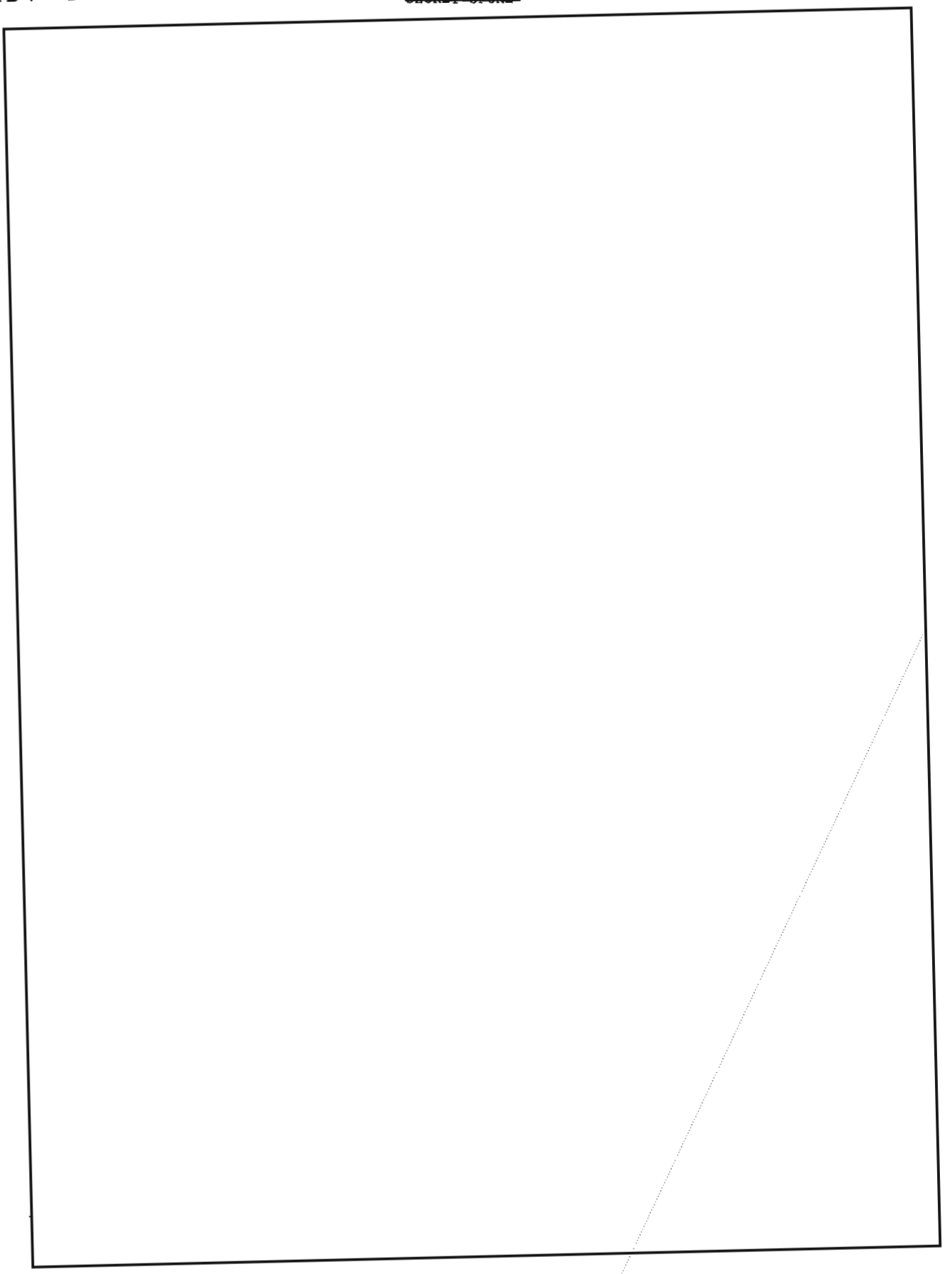
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



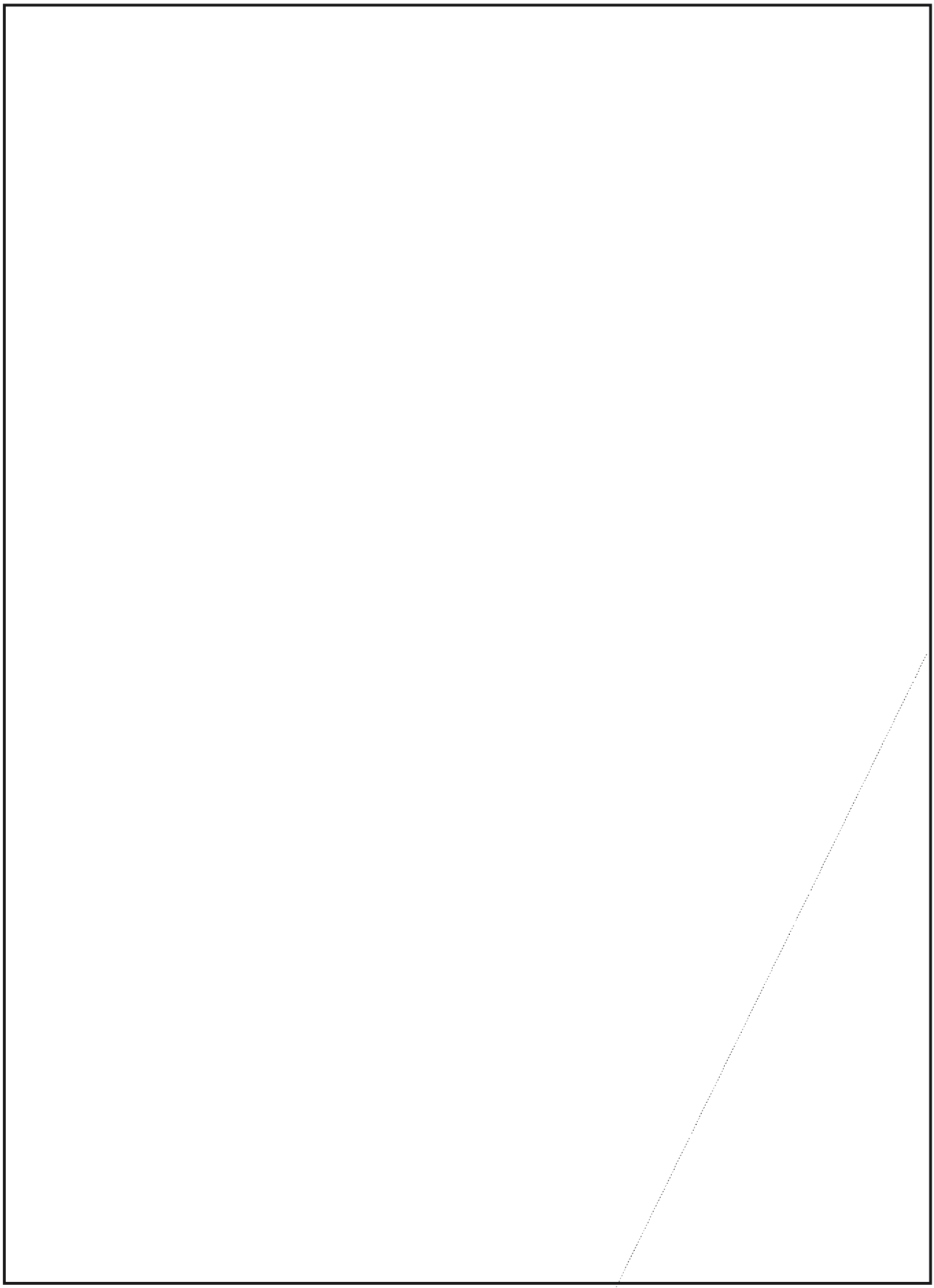
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



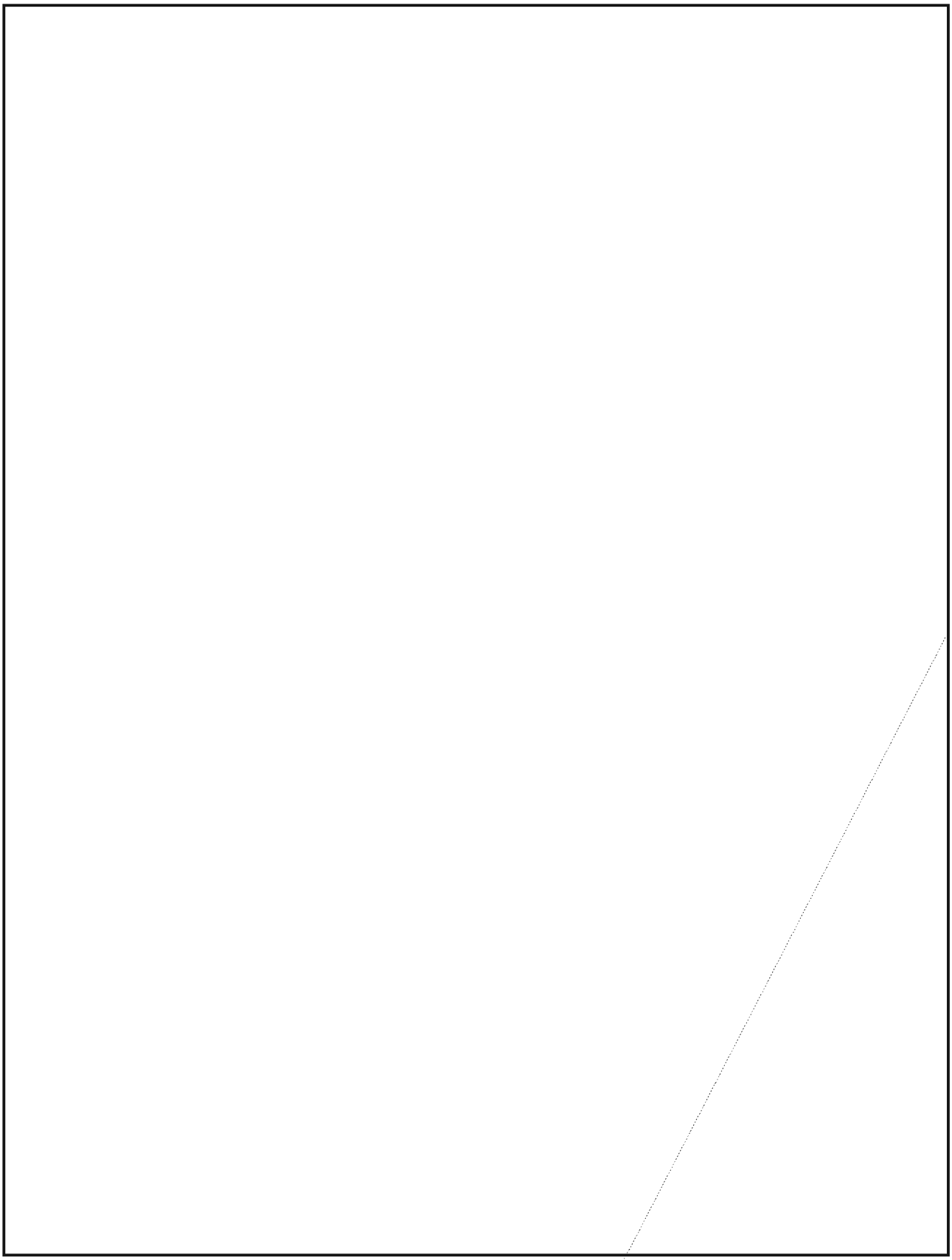
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

DOCID: 4009865

DOES YOUR OFFICE MAKE YOU SICK? (U)

by [redacted]

P.L. 86-36

That's the title of a popular article in a recent issue of American Health magazine (Vol. II, number I, Jan/Feb 1983, p. 79), by Sheila S. Moramarco. It describes an embarrassing series of incidents in the Environmental Protection Agency's new building: employees in a variety of work areas came down with mysterious illnesses involving profuse sweating, lethargy, excessive menstrual flow, and skin mottling, among other bizarre symptoms. The problems could not be traced to any single type of source in the different offices. The EPA is housed in a "three-story glass and concrete building with 12-floor high-rises on each end. Sealed against the weather with windows that don't open, with air-conditioning, heating and lighting that are centrally controlled, this office is a typical 'tight building' ... Ironically, the E.P.A. had given its employees a work environment--an office building improvised from a shopping mall--distinguished by stale, polluted air and a haphazard ventilation system incapable of ridding the building of toxic chemicals. But what happened at E.P.A. was not an isolated incident. The pattern of the erratic, mysterious illness ... is common enough in such offices to merit a medical name: 'tight-building syndrome.'"

This syndrome is likely to affect individual workers in widely scattered offices that have nothing obvious in common, while sparing other workers sitting at neighboring desks. Its symptoms are a grab-bag typically including skin rash, respiratory distress, eye irritation, lethargy, nausea, dizziness, and menstrual irregularities. The article quotes the following summary by Judith Gregory, research director of the Working Women Education Fund in Cleveland: the ailments "are generally the result of a combination of factors ... They may include irritating or toxic indoor pollutants; biological agents such as fungi, spores, or bacteria; inadequate fresh air--and high levels of job stress." What it seems to amount to is that the air-tight environment concentrates any irritants that happen to exist in a given work area and raises the probability that individual employees who are at risk for any reason--stress, physiological weaknesses or predisposition, etc.--will be affected. A somewhat similar situation has been coming to light in homes tightly insulated to save energy over the last few years.

What are some of the commonest chemical problems in offices that may be exacerbated in "tight" workplaces? The most widespread pollutant, according to the article, is formaldehyde. This substance is a common ingredient in building materials and office supplies and it has a strong tendency to leak into the air; thus it is an inescapable constituent of stale office air. It can cause eye, nose, and throat irritation, breathing difficulty, dizziness, nausea, fatigue, and confusion. A level of six parts per million, three times the level allowed by OSHA, was found in one office building in a study triggered by employee complaints. Many people are affected by formaldehyde even at or well below the level permitted by OSHA standards. Worse still, formaldehyde is known to cause cancer in animals, though we aren't yet certain that it does so in humans.

DOCID: 4009865

Ozone is another common problem in office air. It is "an unstable form of oxygen produced when air is exposed to high voltage or ultraviolet light." Ozone can cause severe irritation to the lungs, nose, and throat, permanently damage the respiratory system, damage blood cells, and impair vital enzymes. "High-energy office machines, photocopiers in particular, can build up dangerous levels of ozone" in inadequate ventilation.

Asbestos is another culprit, due to its widespread use in insulating and fireproofing materials before 1970. In many buildings where insulation is deteriorating, the air is laden with asbestos dust. EPA considers that any degree of contamination by asbestos is dangerous, however small. It can cause cancer of lungs, stomach, colon, and rectum, as well as a chronic lung disease called asbestosis.

Radon is a radioactive gas which has been estimated to cause 10% of US lung cancer cases. It is inhaled with dust particles in the air. It comes from tiny amounts of radium normally contained in brick, rock, and concrete. In well-ventilated spaces it does not present a hazard, since it can escape without building up. But when ventilation drops by half, the radon level doubles.

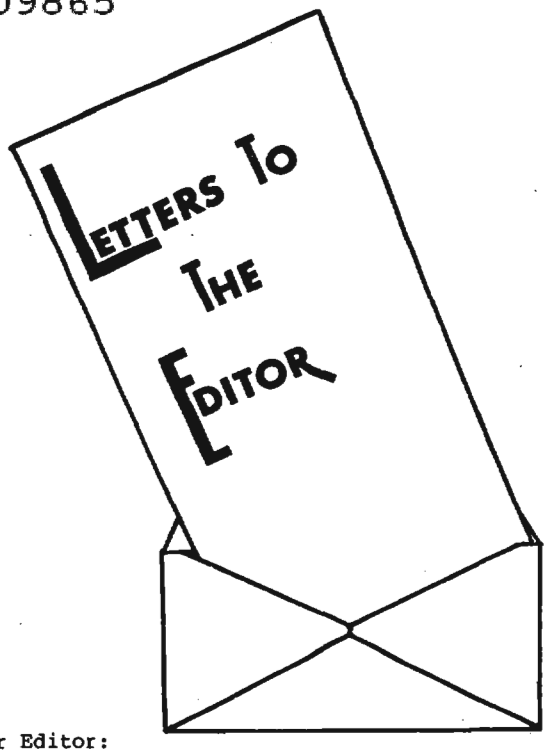
Job stress may make individuals more vulnerable to these pollutants, concentrated by the "tight-building" environment and poor ventilation. Workers who have some feeling of control, enjoyment, and reward in their jobs and a hope of stability for the future are defended to some extent from the environmental stressors. This may go far toward explaining the higher incidence of "tight-building syndrome" in clerical and secretarial workers and, specifically, among women.

Office copiers are among the major causes of health problems for office workers. Studies have shown, according to this article, that "both the materials and the process used in photocopying can cause serious health problems." A worker who fails to close the cover during exposure gets a dose of strong light that could produce eye and skin problems. The paper used in making copies can cause allergic dermatitis. Chemicals in photocopier toners (nitropyrene, trinitrofluorenone, and hydrocarbons) may be bad for skin and eyes, though there is no definite proof of damage as yet. Copiers in small rooms with poor ventilation can build up ozone levels well above the .1 part per million considered safe by OSHA.

Is this a description of your work area: "stuffy, dirty air; no air moving near the air vents; dust and fibers accumulating visibly on tops of cabinets and desks; windows that can't be opened; ventilation or air conditioning we can't adjust or control"? If so, it is imperative that you look into the situation and get something done about improving the ventilation. Is there a copier or some other machine or activity that may cause noxious fumes in the same space with you? That's another sure sign that you should make certain your office is well ventilated, or get yourself moved as far away from the pollution source as you can (preferably into another room). And, while the American Health article did not mention smoking, many authorities now seem to agree that tobacco smoke (whether actively ingested or passively suffered because of others' habits) is a serious health hazard.

Judging by what I have seen, all too many of us must work in poorly ventilated areas. We have rearranged walls and doors, restructured office spaces, and moved furniture around so often and so randomly that no system of ventilation could cope with the present situation in our buildings. Too many of us have deliberately sealed off air vents to stop "drafts" or inadvertently obstructed air movement with stacks of furniture, boxes, etc. Maybe it's time we looked around and began to take seriously warnings like those in this article.

DOCID: 4009865



Dear Editor:

I feel constrained to point out a few errors I noted in [redacted] article "Government of the People, by the Party, for the Leadership" in the April 1983 issue of Cryptolog.

Firstly, the Party Congresses are held, appropriately, in the DVORETs S"EZDOV (The Palace of Congresses), not a DOM SOVETOV. Perhaps Bill is thinking of the DOM SOVETSKOJ ARMII or the DOM SOYuZOV.

Secondly, the correct title of the Soviet chief of state is "Chairman of the Presidium of the Supreme Soviet"; the term "PREZIDENT" is mainly reserved for foreign use.

Thirdly, the post to which Andropov was quickly elected was, of course, that of General Secretary of the Central Committee of the Communist Party of the Soviet Union, not the post mentioned above. Andropov did not assume the post of Chairman of the Presidium until June of 1983.

I'm not sure what Bill had in mind when he says that Brezhnev served as First (sic) Secretary since 1970. He took over as party chief in 1964 when the post was known as First Secretary, but the title was changed to that of General Secretary by the 23rd Party Congress (1966).

In discussing the Main Political Directorate, he mentions that its chief, Epishev, is directly accountable to the Politburo. He might have added that, according to several open-source publications, the Main Political Directorate functions as a Central Committee Department, thereby giving the missing link in the flow chart of Soviet decision-making.

This is all not to disparage a most useful recitation of the differences between the formal structure and public ritual on the one hand, and the reality of power relationships on the other. Bill McGranahan and Marc Brenner are to be commended on pointing out to Cryptolog's readers that all is not as it seems in the USSR. Then again, aren't we reminded enough of that in our daily work?

[redacted]

P.L. 86-36

[redacted] replies:

The first objection is the worst one because the man is right: I was wrong on the name of the darn building. I still have ticket stubs telling me that I saw "The Fountain of Bakchisaraj" at the DVORETS S"EZDOV--and I read through the article umpteen times looking for mistakes like that and still blew it. As my editors have told me, this happens to the worst of us.

In the second case, I understand the question but I fail to see a problem. In that part of the article I am describing how we foreigners can be a bit confused when the Soviets remind us that their government has a president too (and [redacted] himself says that "the term 'PREZIDENT' is mainly reserved for foreign use"). It is true that I did not give this formal title explicitly, although I believe that you will find it was very strongly implied in the body of the paragraph:

> "These representatives and deputies ... elect the Presidium of the Supreme Soviet which handles the Supreme Soviet's business when the body is not in session. The chairman of the Presidium is very similar to the European, idea of a president; he has very little power but he is the official representative of the Supreme Soviet and the Chief of State."

I'm afraid I don't understand the third objection at all, because I never said that Andropov became "PREZIDENT." In fact, things were happening so swiftly that I purposely avoided referring to Andropov by any specific title, since the occupant could change again by the time the article went to press and once again I would be struck with dated material. I referred simply to Andropov's "accession to power" and left it at that. Hopefully, as the situation crystallized, a more permanent line-up of personalities and positions would take shape and the readers would be able to use our description of the Party and the government to visualize a little more clearly who is in charge and how he gets things done.

In conclusion, I would like to stress that since the article was intended as a primer of the Communist Party of the Soviet Union and that country's government, I could not be complete in extent--or in time! Granted there will be differences of opinion as to what crucial and what is peripheral; but if any of my attempts to make these systems more understandable have actually caused distortion or confusion, I am most grateful to [redacted] for having pointed them out.

P.L. 86-36

From: hgr at BAR1C05
Subject: letter to the editor
To: cryptolg

Dear Editor of Cryptolog:

I have a question about Zebulon Zilch's article, "My Staff--It Comforts Me." Does that illustration at the end, the one showing a shepherd separating the sheep from the goats, represent the Z Staff performing a similar function? Or does the shepherd represent DIRNSA using a "staff" to divide the bah-sayers from the nah-sayers?

[redacted] P16

Editor's Note: We submitted your question to Zebulon Zilch, who wrote the article, and his reply was "Yes!"

Dear Editor:

Thanks for your "Our of My Depth" feature in the May Cryptolog. While it was entertaining, it was far from realistic. With only 3 garbles among the 673 digits, it has a "cleanliness rate" exceeding 99.5%! Where's the challenge?

[redacted] P.L. 86-36

SOLUTION TO NSA-CROSTIC 48

From "AMERICAN MAGIC," by Ronald Lewin

"The Voynich Manuscript is worth a mention because it provides a perfect paradigm, a deeply instructive example of everything unacceptable for the wartime cryptanalyst."

P.L. 86-36

*** N O T I C E ***

The CRYPTOLOG Special Issue (CISI Essay Contest), dated January-February 1983, has been favorably received and as a result a number of requests have come in for copies. An appeal is herewith made to the recipients who have finished with their copy to return it to P14 (Attn: [redacted] for further distribution. Thank you.

P.L. 86-36

---

*CORRECTION*CORRECTION*CORRECTION*CORRECTION*

SCI MEANS
"SENSITIVE COMPARTMENTED INFORMATION"

(U) Somehow an error crept into [redacted] article "Do You Know the Differences?" in the June-July 1983 Cryptolog. The term SCI is expanded on page 7 as "Special Compartmented Intelligence," which is incorrect. The abbreviation really stands for "Sensitive Compartmented Intelligence," as in the chart on page 8. We hope that no undue confusion was caused by this discrepancy.

P.L. 86-36

P.L. 86-36

[redacted]

P.L. 86-36

There's one individual who was glad to see the editorial comment following [redacted] letter in the May 1983 Cryptolog because, as one who knew and worked closely with Miss Mabel Babel, yours truly definitely feels that she really deserves some recognition. If the new NSA/CSS building is called "The Tower of Babel," this writer thinks that that might be a worthy tribute to a loyal, dedicated government employee. Accordingly, I do hope that you won't mind my taking a few moments to reminisce about our "Miss Babel." No one ever called her "Mabel"--and woe unto the poor benighted soul who pronounced her family name as "babble"! She remains one of my most unforgettable characters at NSA, a place where characters (both forgettable and unforgettable) abound. It is devoutly hoped that some of the other oldtimers who remember that marvelous woman will be inspired to put some of their memories in writing too.

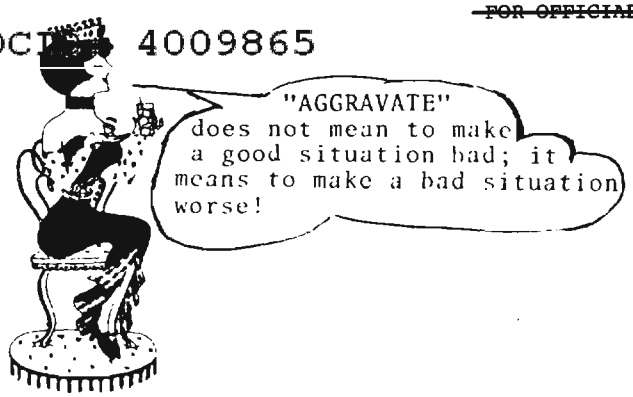
One particularly memorable thing about Mabel Babel was that she never used the pronouns "I" or "my" in speech or writing. Of course, she didn't often talk about herself, but on those rare occasions when someone else would steer the conversation around to her, she would speak as if she were talking about someone else. Like Julius Caesar before her or Ellery Queen and Miss Manners since, she referred to herself only in the third person: "Well, in Miss Babel's humble opinion ..." (although her opinions were anything but humble) or "Things would be done differently if Miss Babel were in charge."

Having been brought up in a diplomatic environment, she usually referred to her interlocutors (a good word I learned from her) as "Your Excellency," not just plain "you." It certainly made a junior linguist feel important to be so addressed by such an august personnage, even though the sentence was something like "Miss Babel seems to have found a minor discrepancy in your excellency's translation" or "May Miss Babel humbly suggest that your excellency henceforth refrain from rendering this word in that fashion?"

She was probably the only person I ever met who could use the words "eschew" and "vouchsafe" in ordinary conversation, and she was the fist person I ever heard use "counterproductive" in mixed company. Another of her rules seemed to be "Never use the indicative mood if you can possibly use the subjunctive." One of the other people in the section put his finger on Miss Babel's propensities when he admiringly said "She talks the way other people write."

Mabel Babel was a short woman who used a chair with several cushions on it and some of us semi-jokingly referred to it as her "throne," since it was from that seat that so many of her "imperial" decrees emanated. That was where she would sit when reading or checking people's work. But she had another desk on the other side of the room that she used for typing. She always kept at least one pencil poked into her hair (which remained black despite the passage of the years) for her corrections and notations, inscribed in her inimitable, fine, legible Spencerian handwriting with its precise angling and an abundance or plethora of loops and curlicues, but she used the Spencerian only when checking other people's work. Whenever she drafted a document, she would type it on a beat-up old Remington manual that no one else in the office dared to touch. Because she was so short, she would take the section's unabridged dictionary off a nearby table and place it on a convenient chair so that she would be high

DOC[redacted] 4009865



A Pronouncement from "The Throne"

enough and at the proper angle to attack the keyboard. I recall one day when I, still one of the most junior of junior linguists, was writing some document and needed to look something up in the unabridged, so I politely walked over and asked, "Excuse me, Miss Babel, but I'd like to look up a word in the dictionary." Giving me a look that would freeze Lake Superior, she firmly replied "Can't you see? Miss Babel is sitting on it!" Case closed (and she hadn't even called me "Your Excellency")!

But about half an hour later, another occasion arose when I needed to consult the Webster's, so I mustered up all the courage I could and again begged her permission to use the book. An even frostier look accompanied an even more determined repetition of "Can't you see? Miss Babel is sitting on it!" Somehow I found the nerve to reply "But, Miss Babel, I always thought that a dictionary was for developing the other end of the spine."

With a discreet "Haha," Mabel Babel slid off the dictionary and, as I approached to use it, said "Go ahead--but just one word!"

That dictionary incident was the closest that anyone could ever remember to an argument that Miss Babel lost (and even her "just one word!" left her in control of the situation). If she did make a mistake, she did not like to have it pointed out to her and she usually had a perfectly good explanation of why it wasn't really incorrect, so that the person who pointed out the supposed mistake was really the one in error.

For example, one time when I had used the expression "from whence" in a text, she dutifully tried to tell me that this was redundant, that that "whence" was not a synonym of "where" but a preposition that meant "from that place," and that therefore the two words were not interchangeable. I tried to say that I couldn't quite agree with her and in my own defense I argued that "Shakespeare, Fielding, Thackeray, and even the King James Bible committee all used 'from whence' in their writings," figuring that she couldn't argue with an all-star lineup like that. Completely unfazed, she replied, "Well, they wouldn't have used that locution if Miss Babel had been checking their output!" She also chastised me for mentioning Shakespeare and Fielding in the same breath, since in her view no other writer came even close to the Bard of Avon. (Some of us speculated that in her youth she may have known him personally.)

Speaking of the word "whence" reminds me that she was one of only two people I ever knew who really pronounced WH- words with a "HW" sound, so that when she said "whether" it didn't sound like "weather." (The other such person was Doctor Sidney Fairbanks, whom I'm sure some readers here at the Agency also remember fondly.)

But, whether pronouncing them or writing them, she had a wonderful way with words, which to her were like old friends. She referred to this trait of her character as "a love affair with language." She could and would discuss etymologies, derivations, and usages the way some people talk about sports, the weather, or their grandchildren. In a manner of speaking, I guess you might say that since Miss Babel was a spinster, her words were her grandchildren.

For instance, I recall the first time that I came across the French word démarche in a text I was translating. One dictionary gave "procedure, step, application, overture" as possible meanings and I forget which one I picked (probably "overture") but I wasn't really happy with it. Shortly thereafter, Miss Babel pointed out to me that well-bred translators don't have to look for good translations of that word; they just leave it as démarche, ending up with "Miss Babel is surprised that your excellency didn't know that."

A few days later when I was working on a Spanish text and translated the word gestión as "negotiation," she reminded me, "Does your excellency have any recollection of Miss Babel's discussion of démarche a few afternoons ago? Well, démarche is an equally satisfactory rendition for the Spanish word gestión. Here is a brief aide mémoire on the subject for your excellency's perusal," and she handed me a 3-by-5 card--she loved to jot things down on 3-by-5 cards and hand them to transgressors to make sure they remembered her teachings; we called the cards "Babelgrams" when she wasn't within earshot--with the message:

1. Refrain from translating the French word démarche. It is a perfectly acceptable word in English.

DOCID: 4009865

2. Do not (repeat "not") forget that there is an acute accent over the first e in démarche.

3. The word démarche is also recommended as a rendering of the Spanish noun gestión.

Along with the Babelgram came a lovely lecture on the valuable word démarche, a noun that can mean anything from saying "Gesundheit" when someone sneezes up to (and beyond) sending several armored divisions into a neighboring country. It was the extreme variety of meanings that the word could have (a polite way of saying "vagueness") that made it appeal to government linguists. She also went into great detail to explain the differences between "making a démarche" and "taking a démarche" (but I blush to admit that I've forgotten the distinction) and railed about how many careless people write the word without the accent over the e, expressing rage and indignation over the fact that Webster's dictionary even sanctioned writing the word without an accent. I distinctly remember her indignation as she proclaimed "Why, Miss Babel would as soon commit adultery as write write démarche without its accent!" Somehow I couldn't picture her doing either.

Another of her pet peeves was the misplaced "only." When one of the local breweries back in the 1950s started using returnable bottles for which the buyer left a returnable deposit, they included in their ads a little picture of kilted Scotch gent saying "Ya only pay for the beer!" Although not a beer-drinker, Miss Babel felt constrained to write them an indignant letter pointing out that what their Caledonian was implying was that one only pays for the beer but doesn't get it, doesn't take it home, doesn't drink it, doesn't enjoy it, or do anything else with it. "What he should be saying," she concluded, "is 'Ya pay only for the beer!' or 'Ya pay for only the beer!'" Within a week after she sent the letter, we were pleased to note, the brewery stopped using the picture and the solecism, although I later heard that they also received a lot of letters from people named MacTavish, MacGregor, MacDonald, Mac Leod, etc., objecting to the use of the Scotsman.

Another time, when one of the translators included a reference to a person "who only died last week," she imperiously asked, "And what did he do this week to top that?" before changing it to "died only last week." To people who tried to argue "Well, you know what I mean," she would reply "But if your excellency wrote correctly everyone would know what your excellency means and they would know it immediately!"

One time when I had put the word "only" in a place where she thought it didn't belong, I attempted to defend myself by saying that this was the way that most people spoke and where I put the word was where the average person would do so in normal conversation, adding that I didn't think anyone would misunderstand the meaning. She handed me another 3-by-5 card on which she had written the sentence

I hit him in the eye yesterday.

and challenged me to put the word "only" in all eight conceivable places. "Does your excellency really believe that all eight of those sentences mean the same thing?" she asked and walked away triumphantly before I could answer.

She expected others to have her high standards of language usage and proper behavior and was extremely annoyed when anyone used bad language in her presence or spoke evil of a co-worker in her presence. "Miss Babel would not have expected that your excellency would say such things!"

There is another story, probably apocryphal, that deals with her high standards and her feeling that she was never the one who was wrong. According to this tale, Miss Babel was on a tour of the Naval Observatory in Washington and was shown the gigantic telescopes that are used to track the movement of one particular star. Those movements, the guide said, are calculated to split-second accuracy and it is known precisely to a millionth of a second when the star would pass directly in front of one of those telescopes, which was connected to an electronic device that would observe the exact instant when the star's image landed on a hair-thin wire on a specially-rigged table that was connected to a master clock on the wall. The guide went on to explain how the clock was built in such a way that it would reset itself to the precise nanosecond when the calculations called for the star's passage, adding "and then from this room, that clock sends out radio signals to radio and television stations, railroads, airlines, military bases, and many other users all across the nation for whom absolute accuracy in time is essential. In other words, this clock is the one that tells all of America just what time it actually is!" At this point, we are told, Mabel Babel, who didn't own a wristwatch, opened her purse and took out a huge pocket watch (a legacy from her dear father), looked at it, and said "Yes, and your clock is only two minutes fast!"

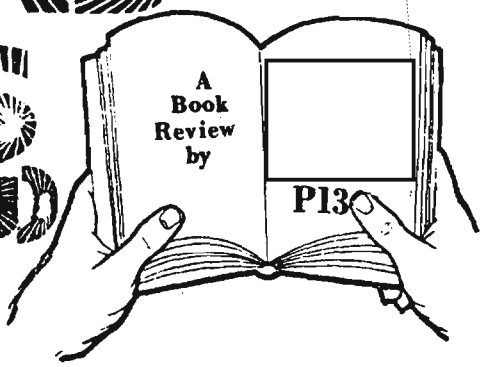
Even if the story isn't true, that's the kind of person she was, which is one of the reasons why [redacted] will remember Mabel Babel!

P.L. 86-36

DOCID: 4009865

THE BATTLE FOR THE FALKLAND ISLANDS (U)

P.L. 86-36



PUBLISHED BY
W. W. NORTON & CO., NEW YORK, 1983

Did a security leak from the British Parliament cause the Falklands War? Did secret intelligence from SIGINT and other sources deceive the British government into thinking the Argentines would never invade? Why did the British Navy begin planning a full-scale amphibious task force operation to reconquer the Falklands a week before the Argentines invaded? Why were telecommunications between the Falklands and London completely out of operation for half a day just as the Argentine landings were taking place?

Max Hastings and Simon Jenkins raise, and to some extent answer, a number of intriguing political and military questions about the Falklands crisis which are a revealing commentary on modern diplomacy, democracy, and war.

The book emerged from an agreement between Jenkins, the political editor of the Economist, and Hastings, a war correspondent for the Standard, made the day before the task force sailed on 5 April 1982, that if a war broke out Jenkins would cover events in London and Hastings would cover the battle. Six months after the war ended they wrote the book and jointly developed its conclusions, using not only the information available during the Falklands war but interviews after the war with almost all of the central figures on both sides of the Atlantic (including Argentina), to try to reconstruct what actually happened, how it happened, and why.

The book is a thesaurus of interesting details, many of which did not crop up in the current reporting; e.g., during the land battle on East Falkland, two reporters discussed the operational plan for a coming battle over the Falklands telephone system. The British military authorities were not sure the Argentines were monitoring the telephone circuits, but they were displeased and banned all reporters from all operational briefings after that. Just before the key battle at Goose Green, fought to satisfy domestic political needs in England rather than for any military need in the South Atlantic, the BBC World Service announced that the Parachute Regiment was advancing onto Goose Green. The Argentines, hearing the broadcast, alerted their defenses, and were ready and waiting. Regimental Commander H. Jones was killed, and casualties were noticeably higher because of this BBC report (p. 239). The writers concluded that the competitive pressure for scoops and newspaper sales, combined with the jockeying for party advantage, led to a lot of disclosures in the British media which only helped the Argentines. Quite an admission from professional journalists.

Jenkins' insight into the London political scene gives an illuminating counterpoint to Hastings' reporting of the battle itself. One of the key military matters was the failure of the Navy to gain air supremacy before the amphibious landings took place; the air battle only then began in earnest because the Navy had stayed out of reach of the Argentine planes after early ship losses such as HMS Sheffield. Another key matter, according to the book, was the dearth of accurate or useful intelligence of a military or political kind. The authors claim that the US did not provide the UK with even a single satellite photograph during the entire Falklands episode (p. 322).

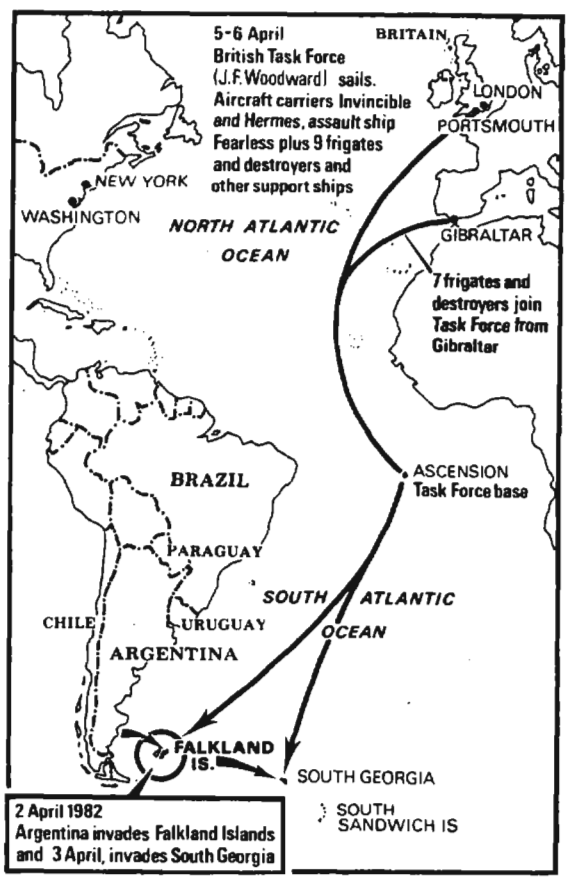
SIGINT is mentioned, but only in passing, with the gratuitous revelation that a US intercept site in southern Chile was an important source (pp. 58 and 142). Order of battle information was known in London from some source, but the local commanders were apparently not told whom they were facing or

where they were located (p. 252). The fact that the war occurred at all was an enormous failure in both intelligence and diplomacy by Britain, Argentina, and the US. The British did not believe the Argentines would invade without a long ritual of warning, while the Argentines never believed that the British would go all the way to the South Atlantic to recapture islands they had been trying to hand over to the Argentines for 17 years. The British Navy utterly misjudged the air and missile threat. The Argentine government utterly misjudged the American, Russian, and UN reaction to their bloodless occupation of the Falklands. The Americans were astonished by the readiness to fight on both sides.

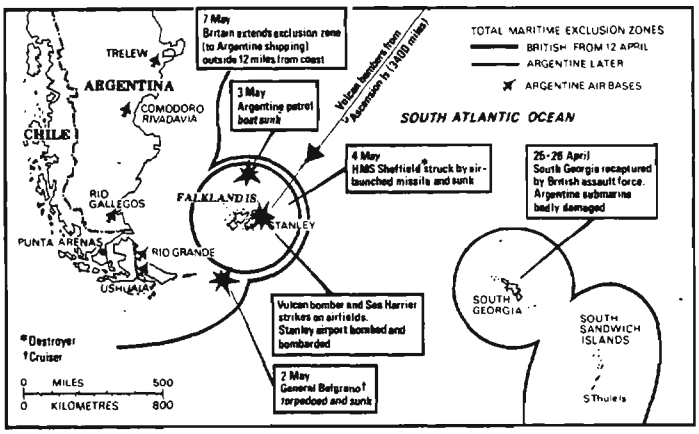
The book describes the war as a "freak of history," noting that the British training and tactics that worked against the heavily armed Argentine troops, by disrupting their defensive posture, would not work at all in Western Europe. The Navy, which was about to be dismembered before the war, lost ships and men, but emerged much stronger in defending its role and its budget. The Argentines, in the opinion of the writers, were disadvantaged by their use of US tactical doctrine, which made them dependent on masses of material and motor transport rather than on troop training and competent officers. When they surrendered, they had been unable to feed their troops, but huge stockpiles of new weapons and food were clustered in Port Stanley, unused. Supplies, and the ability to move them in quantity over a beachhead when the enemy held air superiority, were crucial to the British campaign, but the politicians in London were oblivious to this problem, and chafed for immediate attacks. The ground commander, Major General Thorpe, spent most of the war sailing south on the QE2, arriving with his staff only after the most critical battles had been fought, because there was apparently no way to get them to the scene quickly.

Among the points made in the book, the UK forces--many of which had not seen real action since World War II--were all eager to demonstrate what they could do, while the Argentine army had no concept of how to fight a real war. Only the Argentine air force, which was reluctant over the Malvinas occupation, fought well, and they nearly defeated the British Navy. The Argentine ground forces failed to counterattack the landing on the critical first day, even though their air force had broken through the British navy defenses and were disrupting the operations in San Carlos Bay. During the ensuing land battle Argentine officers did not stay with their men, while the British NCOs and officers led their troops. (A sergeant and a lieutenant colonel of the Parachute Regiment both got the Victoria Cross posthumously, and there were many other medals.) The British were always confident of winning the land battle but the sea battle was much closer than expected, primarily because of inadequate defense against air attack and missiles.

Before the war, the British government felt that the Falklands were expendable compared to British trade interest in South America, and tried to solve the problem by manipulating the islanders (p. 16). The Argentine Junta thought a military takeover of the Falklands would cause no more fuss than the Indian takeover of Goa. Special Intelligence, including SIGINT, predicted a crisis in 1977 which did not materialize and, after this false alarm, was reluctant to cry wolf in 1982 (p. 36). The Foreign Office was better at dealing with foreign governments than with its own and could not get support in Parliament for a transfer of sovereignty. Nevertheless, the Thatcher government denied British passports to Falklanders who did not have a native-born British parent, and this was seen by the Argentines as an adbication of British interest.



DOCID: 4009865



The Franks Report, the official British inquiry into the background of the Falklands conflict (which concluded that the government was not to blame for the invasion but had not been kept accurately informed by the intelligence assessments), claimed that the secret intelligence before the war was a poorer indicator of Argentine invasion plans than articles by knowledgeable insider journalists in the Argentine press. The invasion occurred on 2 April, but on 28 March the JIC (Joint Intelligence Committee) said no invasion was imminent. The government intended to send submarines to the coast of Argentina covertly, negotiating until they arrived, then announce the submarine threat to deter an Argentine invasion fleet from leaving port. However, the Parliament leaked the plan on 29 March, before the HMS Spartan actually sailed. The Argentines immediately put to sea, to accomplish the invasion before the submarines arrived. Apparently, this political leak was the trigger for Argentine action (p. 64). The cabinet, knowing from SIGINT that the invasion would occur on 2 April, was asleep when it took place. The Argentine media broadcast the impending invasion before it occurred. The communications between the Falklands and UK were inoperable during the invasion, and the government learned the results from the Argentine media reports (p. 74).

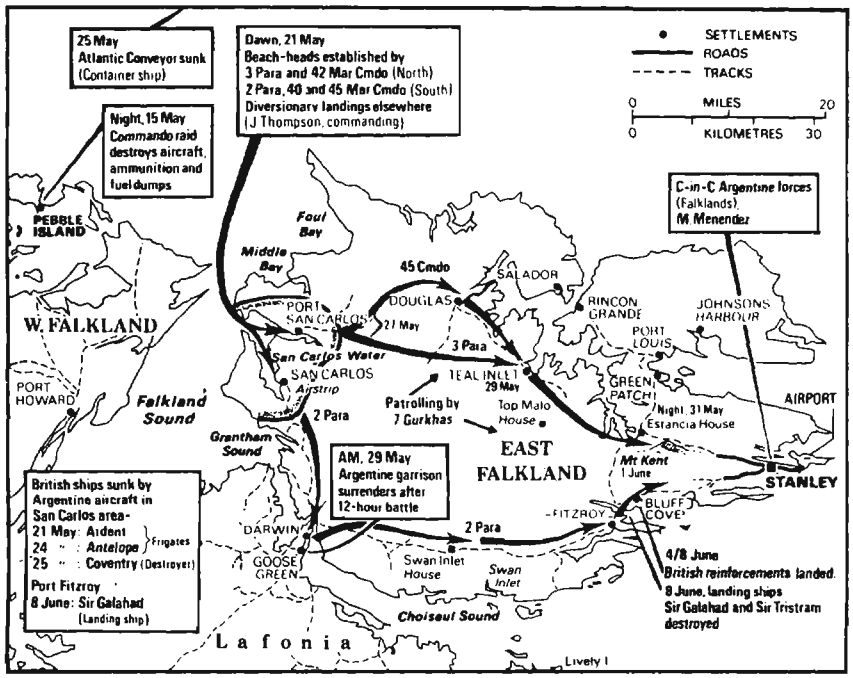
Once the public feeling in Britain had been aroused by the invasion, the Task Force had to put to sea by 5 April before the sense of national purpose evaporated (p. 92). The Royal Navy had planned the large naval operation on 29 March, recognizing immediately that naval power and shipping were the crucial elements in the combat and logistics of such a distant crisis (Chapters 4 and 5). British diplomacy, fumbling before the invasion, moved quickly to marshal international support and a UN Resolution 502 against Argentina (p. 101). The UK feared the Americans would be as unreliable over the Falklands as they had been over Suez, but US support was extremely good (p. 142).

The British Navy expected a walkover but was nearly annihilated (p. 115). Many Navy officers could not believe that there would be no AEW (Airborne Early Warning) protection for the Task Force (p. 117). AWACS support to the British was denied to prevent US direct involvement (p. 142). There were many interservice communication problems on the British side because the autocratic Navy chain of command was very different from the flexible Army staffwork (p. 122). The politicians and civil servants in Britain were kept ignorant of the operational concerns and difficulties of the impending war (p. 124). This made them critical and impatient of delays and reverses.

The sinking of the Belgrano was a political defeat for the British because it was not seen as strict self-defense (p. 149). Because of the lack of AEW, the Sheffield was not firing chaff clouds to offset a possible missile attack, and the missile was launched only a few miles from the ship by a low flying Argentine plane. Until that moment every man in the fleet had been living with the image, rather than the reality, of war.

The early warning against the land-based aircraft was given by a combination of submarine sightings and SAS teams ashore (pp. 157, 162, and 207). Apparently radar and SIGINT detection of the takeoffs were not available. The British strategy of crushing the Argentine air force before the amphibious operation was negated by the Argentine refusal to risk their aircraft against the dangerous Harriers until the British forces committed themselves to a beachhead (p. 161). Since they could not sail home without a land battle, the British government and service chiefs cast aside the rules for amphibious warfare and went ahead without air supremacy. After the loss of the Sheffield, the politicians began to lose confidence in the Navy and sought negotiations after a 5 May emergency session, but Argentine Foreign Minister Costa Mendes mishandled the opportunity and the war was resumed (pp. 167-8).

The British forces got no intelligence of value from the Falklands population during the occupation (p. 177). SAS teams had no burst-transmitting radios and had to keep to terse reports to avoid the "Argentines' excellent modern interception equipment" (p. 181). Despite Soviet surveillance ships and satellites, the Argentines after the war denied that they got any intelligence from the USSR (p. 182). British geographic intelligence came fortuitously from a Royal Marine officer who commanded the Marine detachment there in 1978 and had written a navigational guide to



The Two-Pronged Attack towards Port Stanley

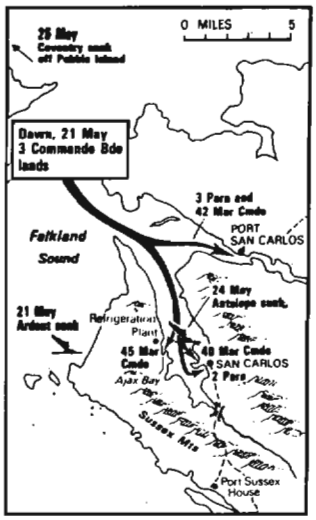
the islands. The Marines sent to land on the beachhead had been trained for arctic warfare in Norway, a fortunate coincidence, but there was only one Spanish-speaking member of the brigade. The invasion plan was based on the use of large helicopters to move men quickly to Port Stanley from the distant beach head at San Carlos, but the Argentines sank the ship carrying them and the troops had to march overland in a blizzard and freezing rain. Argentine attacks on British ships in San Carlos Bay would have been even more destructive had not US export laws blocked the sale of a technical manual that showed how to arm the bombs to explode after a short flight (p. 228). This export limitation on technical data (which no other nation practices) saved hundreds of British lives.

Communications were often very good or very bad. Over 100,000 messages were passed on the command ship Fearless before the war ended. Although not mentioned in the book, the merchant ships requisitioned for logistic support lacked cryptoequipment so that their messages were passed in the clear by HF [1]. The British troops put all their cryptoequipment on one landing craft, which the Argentines sank, so they had to learn to use manual systems and codes in the middle of a battle [2]. When the Argentines surrendered, a portable satellite terminal was used to transmit the details between London and the negotiating table in Port Stanley. MGen Moore on the QE2 had an expensive Scott Satellite communications system to enable him to command the battle remotely, but it didn't work, and he only arrived to give orders at the last stage of the battle (p. 269).

The failure of a shipboard satellite station to work under war conditions is a point that should be borne in mind, for MGen Moore had to depend on HF circuits during the critical first week of the land battle.

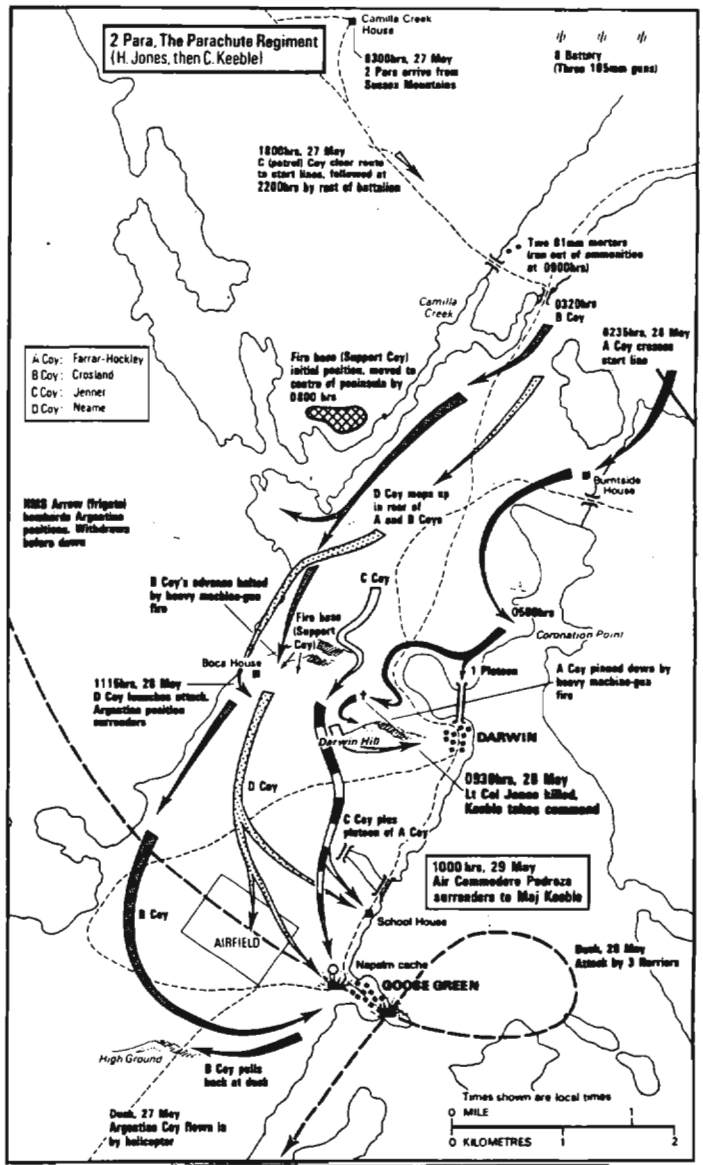
The battle at Goose Green, fought to satisfy domestic political needs in England, would have been a slaughter had the Argentines used their advantages in numbers, equipment, and position. The defenders were three times stronger than the attackers (p. 251). London knew from SIGINT the exact order of battle in the Falklands, hence knew the strength at Goose Green, but did not pass that information to the attacking paratroops (p. 252). Fighting in open terrain, some of the British paratroops abandoned their submachine guns and picked up the Argentine rifles, which had greater range and hitting power (p. 244). Naval gunfire and artillery flown in by helicopter were used initially, but hand-carried rockets and mortars then became crucial to breaking the well-prepared Argentine defenses (pp. 241-7). The Argentines had supplies of napalm but the British had been using white phosphorus, a chemical weapon with equally horrifying effects (p. 321).

After Goose Green, the marines and paratroops marched 40 miles across the Falklands in a freezing rain because all the helicopters were needed to move supplies and wounded. The marchers began 27 May and arrived at Mount

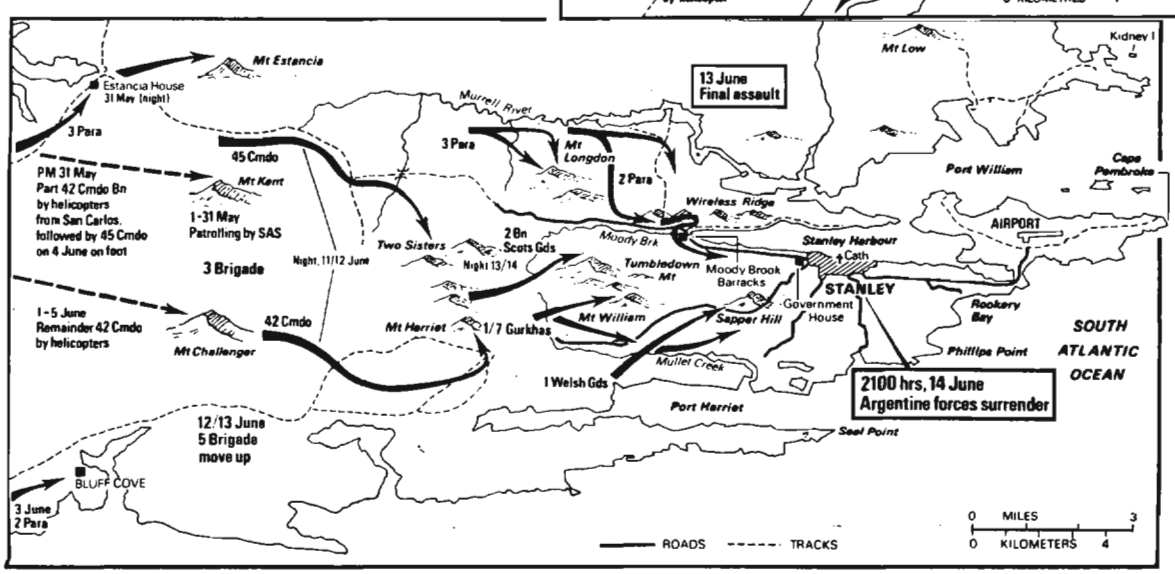


The Landing at
Port San Carlos

The Battle for Goose Green



The Battle for Stanley



Kent on 4 June. The final attack on Stanley was made on 13 June. The weather and exposure produced a lot of trench foot and frostbite, and the cardinal problem was to get the final battle started before the elite troops were reduced by the continuous cold and wet. A small force captured Mount Kent on 31 May in a helicopter night attack made possible by US-supplied night vision equipment.

For various reasons, a Welsh regiment was on board the landing ship Galahad at Fitzroy, waiting for small craft to ferry them across a cove on 8 June, when four Argentine aircraft attacked. A bomb ignited gasoline aboard the Galahad; 51 soldiers on board were killed and many others suffered severe burns. The Harrier CAP had been drawn off Fitzroy by an attack which minutes earlier damaged the frigate Plymouth. The Welsh troops had been aboard the Galahad for five hours without disembarking. Afterwards this was called a calculated risk (p. 282). Because it was bad news, when good news was awaited, the Fitzroy incident was perceived in London as a political disaster (p. 282). This reflects the close interaction between domestic politics and military events in a remote-area war.

Because the air dimension was so critical to the Falklands War, the whole battle hung on a small number of exhausted Harrier and helicopter pilots and maintenance crews who kept their few aircraft flying and fighting week after week. The British ground forces found that night operations by their highly trained troops were quite effective against the entrenched but demoralized Argentines (p. 292). These were usually launched through minefields. On 12 June the last British attack at Tumbledown Mountain outside Stanley was accompanied by 6,000 rounds of artillery fire and naval gun support (p. 305). This produced a major Argentine retreat. The Argentine officers were apparently not around to control the situation (p. 307). Improvised psychological warfare, using the one Marine who spoke Spanish, quickened the surrender.

Starting with a solid core of well-drilled tactical skills, equipment, long-service troops, and vigorous officers, the British forces were compelled by the climate and the losses of ships and equipment to improvise and take many risks. It was a very "iffy" battle, which might have been a major naval disaster. The cost-cutting scheme of tailoring military and naval forces to a very specific NATO scenario proved very expensive in the end. The war cost about 1,000 casualties, six ships sunk and ten damaged, and nine aircraft lost, representing about a billion pounds sterling in lost and damaged equipment. The operation cost about 700 million pounds (p. 317). The lack of adequate reserves of equipment, such as helicopters, put the campaign at great risk even though the Argentines had never fought a war and had no idea of how to use the resources they had.

Overall the book is fairly critical about the actions of the British government before and during the war, but generally adulatory about the fighting forces. Hastings apparently had very good rapport with the military services and huddled in foxholes with the forward combat elements during much of the land battle. When the cease-fire occurred, he was one of the first people into Stanley, still wearing his camouflage paint and battle kit. An earlier book on the Falklands war by the Sunday Times Insight team was much more critical of the British combat operations, and also of Hastings, who was regarded as an uncritical loyalist. While Hastings and Jenkins criticized the press for the way they handled the war, the earlier book criticized the war for the way it handled the press.

Conclusion

Unlike the precision operations of the Israelis in wiping out targets in the Middle East by perfect use of intelligence and weapons, the Falklands War was a battle of unplanned contingencies, politics intermixed with tactics, horrendous security leaks, interservice quarrels (on both sides), tangled and unreliable communications, profound lack of knowledge of the enemy, fumbled opportunities, and enormous stresses on the commanders and the men, who knew the war could be lost in half a day. Despite the fact that it was a "freak of history,"--viz: the first colonial war fought with modern weapons, electronics, and communications during a virtual Antarctic hurricane--the Falklands War was highly revealing about the operations of the military forces and the complicated tug-of-war between military reverses, tactical delays, media reports, and the vacillations and political jockeying in the opposing capitals. These political-military interactions are described quite well in this book. As more information comes to the surface, the ironies, surprises, and afterthoughts of this precarious struggle, where both parties fought at the limits of their military reach, may contain more object lessons on the nature of modern conventional war in remote areas than any battle in the last 40 years.

NOTES

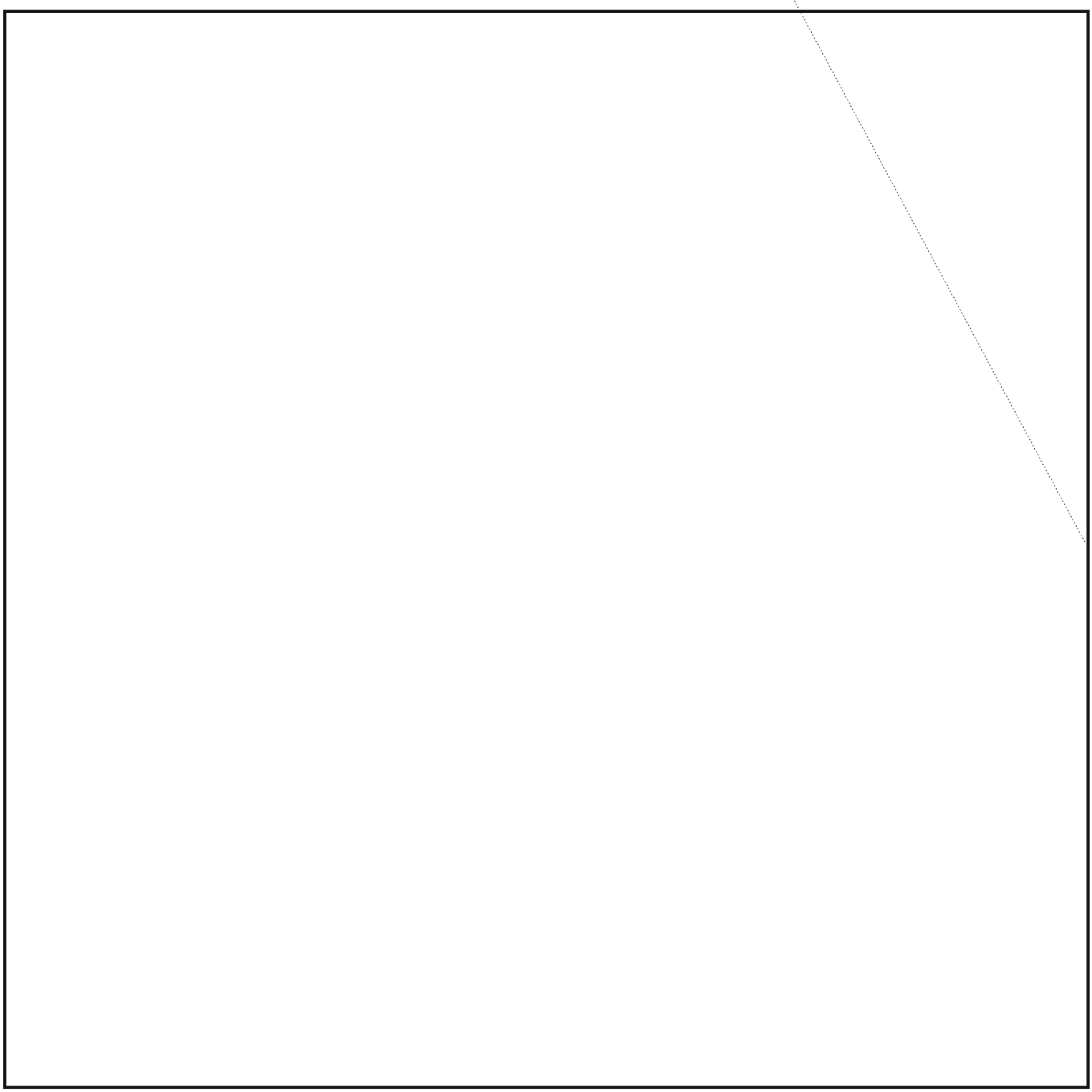
[1] SIGNAL, Dec 82, p. 84. "War in the South Atlantic--The Naval Communicator's Challenge."

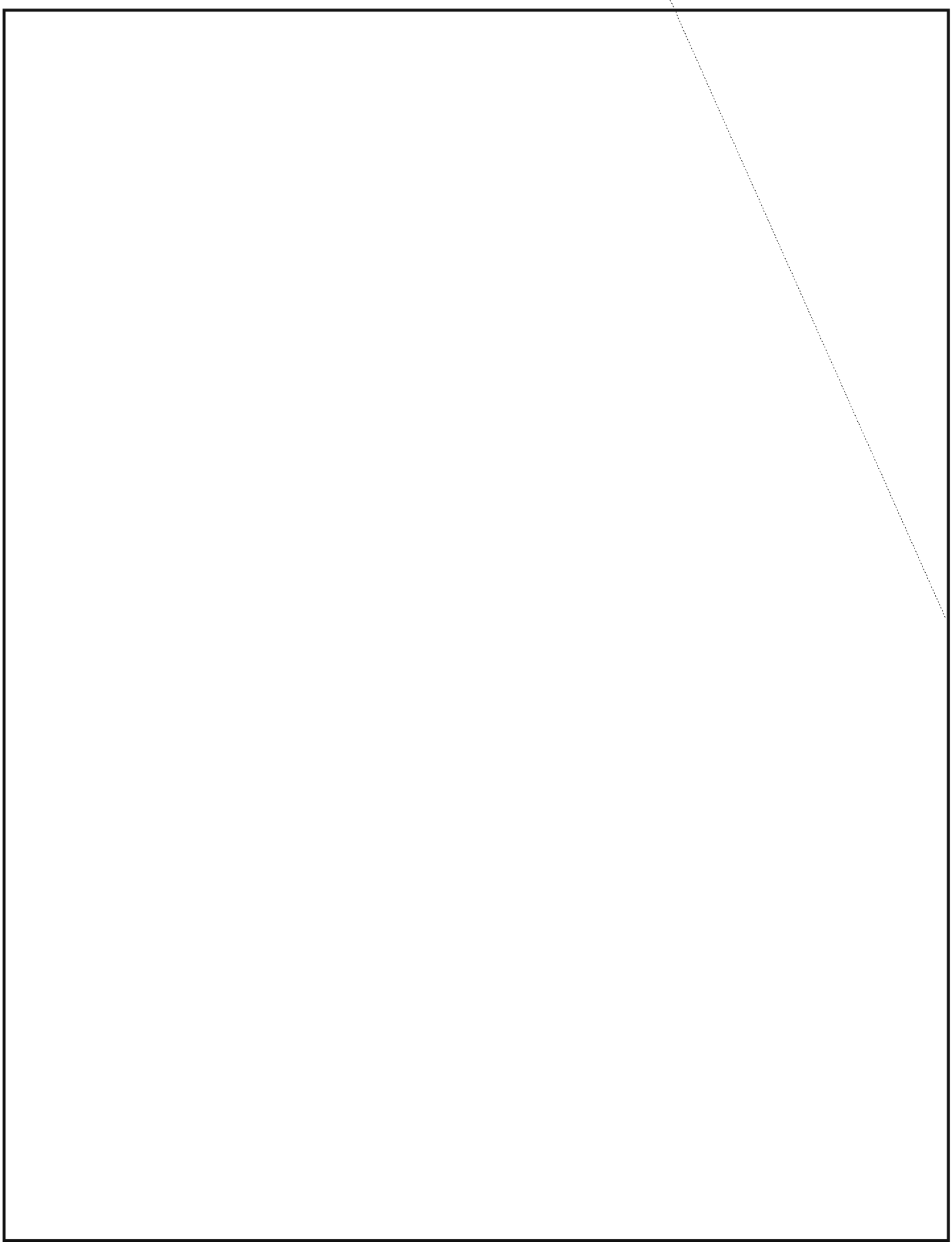
[2] SIGNAL, May 83, p. 105. "Falklands Islands War--A Signaller's Viewpoint."

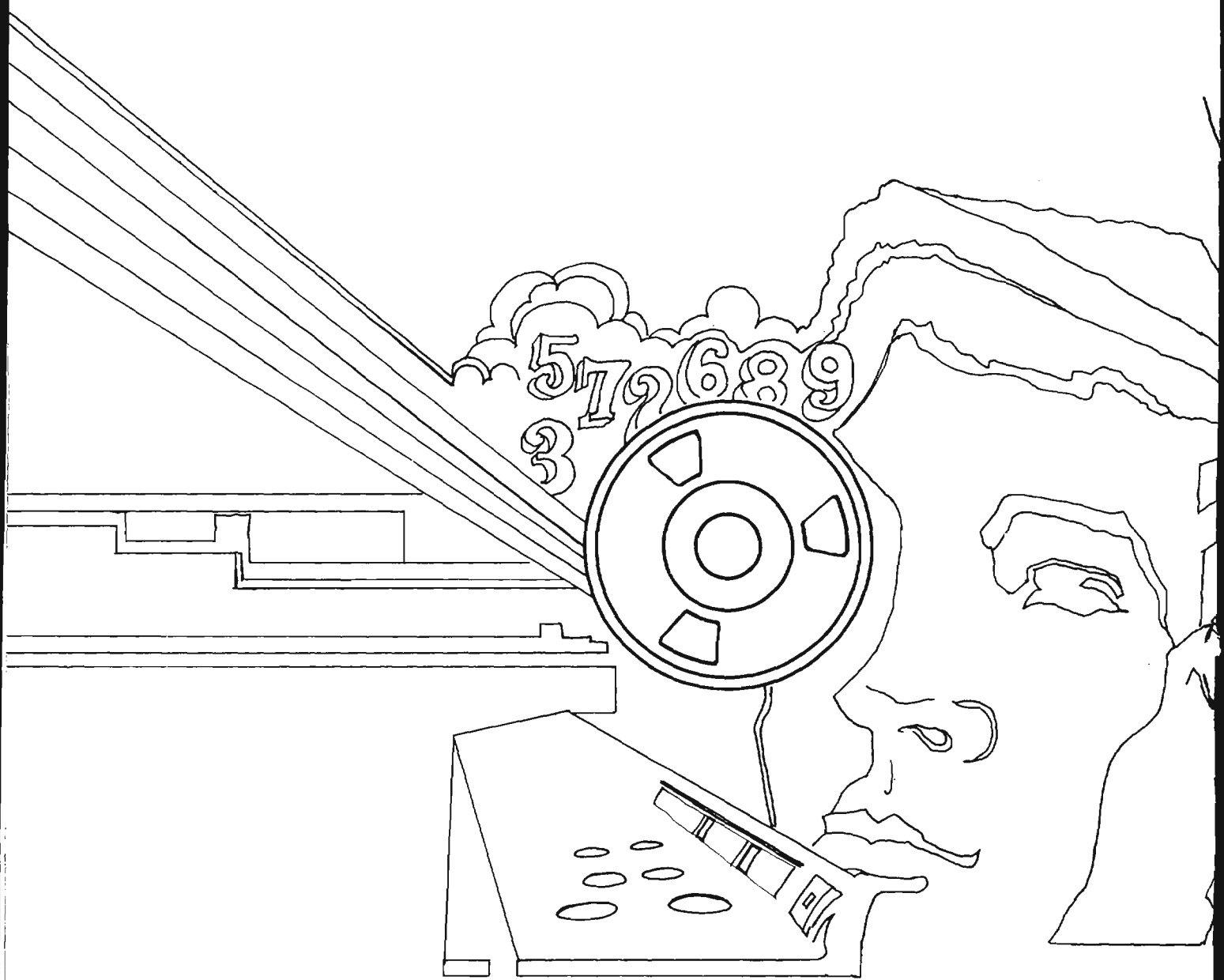
DOCID: 4009865

NSA Crostic No. 49

P.L. 86-36






5 7 9 6 8 9
3

DOCID: 4009863

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JUNE-JULY 1983

EO 1.4.(c)

WHY PASCAL? (WHY NOT?) (U)..... [redacted] 1
REDBARON, ROADRUNNER, BRONZSTAR:
WHAT'S IN A NAME? (U)..... [redacted] 4
LETTER TO THE EDITOR..... [redacted] 6
DO YOU KNOW THE DIFFERENCES? (U)..... [redacted] 7
SOME TIPS ON GETTING PROMOTED (U)..... [redacted] 10
[redacted] 19
PUNCHING THE BIOLOGICAL TIMECLOCK (U)..... [redacted] 22
[redacted] ..... [redacted] 24
LETTER TO THE EDITOR..... [redacted] 26
NSA-CROSTIC NO. 48 (U).....Vera R. Filby.....28

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

P.L. 86-36

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2
DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009863

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. X, No. 6-7 JUNE-JULY 1983

PUBLISHER [redacted]

BOARD OF EDITORS

Editor.....[redacted] (968-8322s)
Asst. Editor...[redacted] (963-1103s)
Production.....[redacted] (963-3369s)

Collection.....[redacted] (963-3961s)
Computer Security
.....[redacted] (968-7313s)
Cryptolinguistics.[redacted] (963-1103s)
Data Systems.....[redacted] (963-4953s)
Information Science
.....[redacted] (963-5711s)
Mathematics.....[redacted] (968-8518s)
Puzzles.....David H. Williams (963-1103s)
Special Research.....Vera R. Filby (968-7119s)

For subscriptions
send name and organization

to: P1, Cryptolog
or call [redacted] 963-3369s

P.L. 86-36

To submit articles or letters
by mail, to: P1, Cryptolog

via PLATFORM mail, send to:
cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no '0' in 'log')

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

There is a story going around which is probably not true. At least, there is no official confirmation of it, and discrete inquiries have produced only denials. Nevertheless, after some investigation, we have decided to pass the item along and let you decide for yourself.

The story concerns the new building, and a new design concept: the containerized office! The building is carefully arranged so that, when an organization needs to be moved, the offices are individually lifted out of position and then slid into their new location, without disturbing the contents of the office itself. All electrical connections, including phones and computer terminals, simply plug in as the module is fitted into place.

We had a look at the new building and we must admit that the possibility is intriguing. Those two big cranes could do the job quite nicely, one removing the 'out' office and the other handling the 'in' office. When a crisis developed and reorganization was critical, one could even imagine moving 'on the fly' without disturbing the occupants. Each office could have prominently displayed "FASTEN YOUR SEAT BELTS" signs and the group chief could make a brief announcement over the intercom about the move and the ETA at the new location.

From a certain angle, the new building looks a bit like a giant data base. Perhaps the entire "mover" system can be run from a remote terminal somewhere. If so, we trust it will be one of the faster ones.

WED

DOCID: 4009863

WHY PASCAL? (U)

P.L. 86-36

by

[redacted]

"It is practically impossible to teach good programming to those who have had a prior exposure to BASIC; as potential programmers they are mentally mutilated beyond hope of recognition."

Now, now, before you come dashing up to my office to mutilate me please note that there are quotes around that statement. I did not say it. Actually it was made by professor Edsger W. Dijkstra, a Dutch physicist and computer scientist. One could infer from this that he didn't care too much for BASIC.

Well, what is wrong with BASIC? Most of the personal computers have it. Most all new data systems people know it. You can get a personal computer to do almost anything you want by programming in it. Those of us who use them really aren't mentally mutilated, are we? Well, ARE WE?!

P13 has been experimenting with powerful personal computers for a couple of years now in an effort to make the job of the analyst a little easier, and maybe even a bit more enjoyable. Our programming has been done in BASIC because BASIC came with the machines and there was no obvious reason to use anything else.

As personal computers have become faster and acquired more memory, and as other languages have become available, it seemed that the time had come to investigate some of them. For the past few months I have been looking into the use of Pascal on the IBM-PC, and would like to share some of my thoughts with you.

First of all, it is necessary that you understand a very important difference between BASIC and Pascal. Basic, as it is purchased for most machines, is an "interpreted" language and Pascal is a "compiled" language.

With an interpreted language, a programmer need only type the program into the computer, and give the command for the program to run. An interpreter then looks at the first statement, checks to be sure it makes sense, translates it into code that is recognizable to the machine, and then executes it. This procedure continues until the program is completed.

If the statement doesn't make sense, a message will appear on the screen telling the user that he has an incorrect statement and the program halts. The user can make the correction and restart the program.

So far so good, but how does this differ from Pascal? Well, when you are through writing your Pascal program you type in a command calling the compiler. This compiler takes your entire program and attempts to translate it into a machine recognizable form. When the translation is complete, you may then run the program. On the IBM-PC compilation of even a relatively small program can take as long as a few minutes. If there are errors, the program may, of course, not compile.

The important thing to remember here is that as soon as you write your BASIC program you can make an attempt at running it. Pascal requires that you compile your program. When writing a new Pascal program you may very well attempt numerous compilations before you are in a position to try to run it. This can get very frustrating and may very well cause you to begin to feel the urge to fold, spindle, or otherwise mutilate your disk--or maybe even the computer itself.

In general, a correctly written compiled program will run noticeably faster than an interpreted program but, when you are actually doing the writing, it is more productive to be using an interpreted language.

So, why Pascal? Well, if you are writing a program that you very well know might be used once or twice at most, then you clearly don't want to use Pascal. You may spend too much time trying to compile it. If, on the other hand, you were asked to write a program that will probably be used for years and will, of course, need to be maintained, then Pascal would be a good choice.

A few examples will illustrate my point. Suppose you were asked to write a program that would store in a personnel file the names and addresses of the people in your office. Suppose you want to allow 20 characters for the name, 14 for the address which could contain 4 digits for the street number and 10 for the street name, 10 characters for the city, 2 for the state, 5 for the ZIP code, and 7 for the phone number, for a total of 58 characters.

In BASIC, variable names can only be two characters long so you would probably use a string PE$ (for personnel) which would be 58 bytes long. Into this string you could place a NA$ for name, AD$ for address, SN$ for street name, CI$ for city, ST$ for state, ZI$ for ZIP and PH$ for phone. (BASIC requires a '$' in the names of character strings.) When you concatenate these strings, you get your record.

In this BASIC program you naturally would write some error-checking code to be sure that the user did not put in more than two characters for the state name, seven for the phone number, 10 for the city, etc.

Now, a year or two goes by and someone decides that the address should have room for at least 5 digits, the phone 10 digits (you want to show the area code), and the name 15 characters. You must go through your BASIC program and try to remember which variables you used for name, phone, etc. It may be obvious now that PH$ must stand for phone, but a year from now when you are asked to change the telephone number length, are you going to remember that TELEphone (TE$?) this year was phone (PH$) last year? Maybe not. What about PE$? What is the new field length?

Pascal will make it more difficult for you to confuse yourself. Pascal requires that all data types, such as the string of characters containing the name, phone, etc, be identified at the beginning of the program, and that all of your constants, data types, and variables be declared very specifically. The beginning of your Pascal program would look like this:

```
TYPE
  PERSONNEL =
    RECORD
      name: PACKED ARRAY[1..20] of char;
      number: PACKED ARRAY[1..4] of integer;
      street: PACKED ARRAY[1..10] of char;
      city: PACKED ARRAY[1..10] of char;
      state: PACKED ARRAY[1..2] of char;
      zip: PACKED ARRAY[1..5] of integer;
      phone: PACKED ARRAY[1..7] of integer
    END;
```

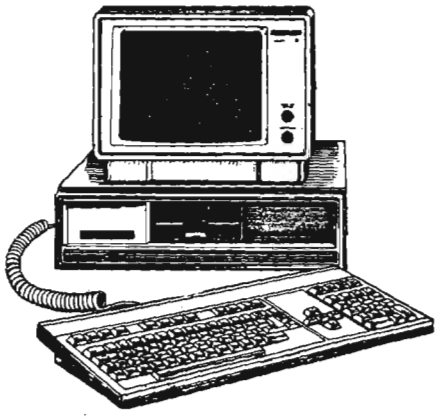
A BASIC string is a Pascal "PACKED ARRAY".

A year from now, if you wanted to allow 10 digits in the phone number...no problem, you simply go to the TYPE declaration, look up "phone" and change the PACKED ARRAY from 7 to 10.

OK, so Pascal does seem to allow easier maintenance of data; what else? Pascal allows a program to be broken up into separate procedures. These individual procedures could each be programmed to do one simple task. A driver program would then sequentially call the procedures. For example, in the above program, the driver might look like this:

```
PROGRAM info;

TYPE
  PERSONNEL =
    RECORD
      name: PACKED ARRAY[1..20] of char;
      number: PACKED ARRAY[1..4] of integer;
      street: PACKED ARRAY[1..10] of char;
      city: PACKED ARRAY[1..10] of char;
      state: PACKED ARRAY[1..2] of char;
      zip: PACKED ARRAY[1..5] of integer;
      phone: PACKED ARRAY[1..7] of integer
     END;

BEGIN;
  get_name;
  get_address;
  get_phone
END.
```

The procedure get_name would prompt the user to type in the person's name and would then store it in the PACKED ARRAY 'name'. The other procedures would do similar small tasks.



That's it! If next year someone decides that information as to marital status is needed, you could add a new procedure "status", which would prompt the user with a yes/no question as to whether or not the individual is married. Into your RECORD area you could insert "status: boolean". No problem.

In BASIC you would have to figure out a location in your program to insert the status information. What variables do you use? ST$ sounds good--or did you use that for state? You had better be careful. If you were writing in BASIC you didn't declare your variables anywhere; you simply started using them. In contrast, the variable names in Pascal can be meaningful and the ones used in the procedure get_phone, for example, do not affect the ones in get_address. You can use the same names if you want.

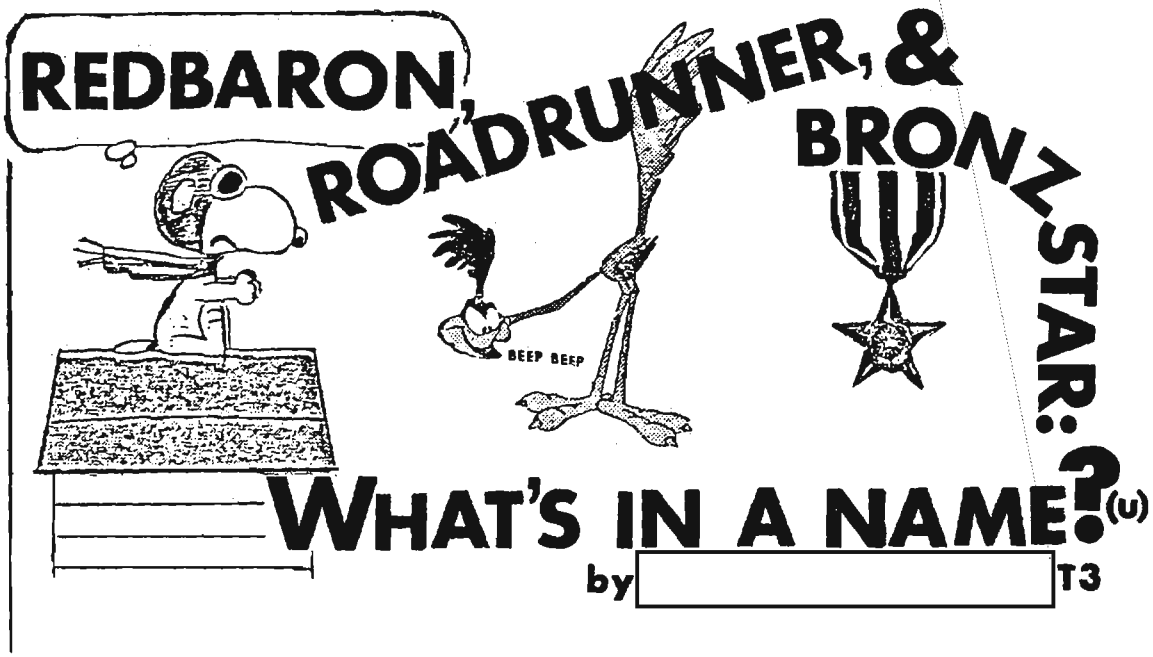
Pascal is not very forgiving. You MUST introduce all of your variables, constants, etc. at the beginning of the program. BASIC does not require this and unless a user is very careful with his error-checking, he can more easily insert incorrect data into a BASIC program than he could into a Pascal one; or a programmer might use the same variable name for two different variables. BASIC will easily allow this.

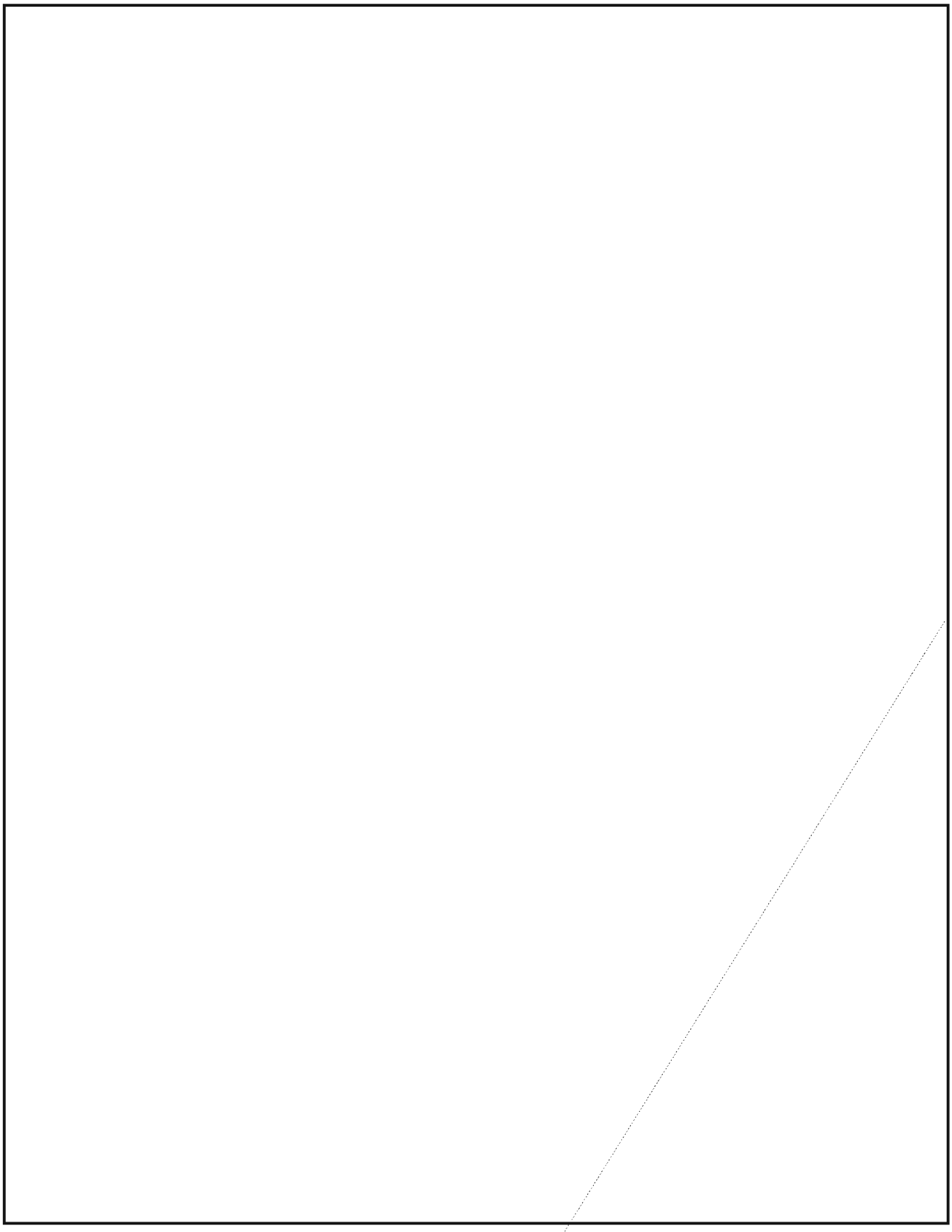
Pascal tends to be self-documenting. The individual procedures are generally quite short with the procedure and variable names very meaningful. Some versions of BASIC do allow variables of more that 2 characters but only the first 2 are recognized by the interpreter; therefore STate and STatus would be identical variables to the machine. So, the get_address procedure might put MD for Maryland in the variable that you are calling State and then the Status procedure might modify that exact same variable to 'yes' or 'no'.

This could put the programmer into a bewildered status, or a state of confusion.

It is for the above reasons that those of you who are using personal computers should consider using Pascal.

Remember, you do not want to become mentally mutilated!


REDBARON, ROADRUNNER, & BRONZSTAR:
BEEP BEEP
WHAT'S IN A NAME?! (U)
by T3



P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

Correspondence

Dear Sir:

P.L. 86-36

I was particularly interested in the [redacted] article on Video Teleconferencing in the March 1983 issue. I believe we would be totally remiss in limiting the justification for such a system on teleconferencing alone. Requirements for training at field locations around the world are growing at a rapid pace and the NCS budget for travel is growing accordingly. It is therefore apparent to me that a dual-purpose system is needed.

P.L. 86-36

Our experience with the Instructional Television System (ITV) has proven that the technique is extremely effective. Agency student participants, when surveyed on their reaction to the system, have been extremely positive in their responses. We did experience minor procedural problems during the early stages of our involvement but these seem to have been corrected.

I would therefore propose that the justification for a worldwide video teleconferencing system be beefed up with the addition of ITV. It seems to me that it would provide us with a much bigger bang for the buck.

[redacted]

Dean, E4

P.L. 86-36

DOCID: 4009863

DO YOU KNOW THE DIFFERENCES? (U)

P.L. 86-36

by [redacted] C223

Sensitivity markings, including Compartment/Category and Classification/Caveat labels, often seem to be confused with one another, as well as with the slew of acronyms and buzz words that proliferate in the everyday jargon here at the National Security Agency. Some of this confusion, such as the confusion between SI (Special Intelligence) and SCI (Special Compartmented Information) for example, does not necessarily pose an enormous problem for most NSA employees since many jobs here do not require a knowledge of the distinction between these particular abbreviations. For the employees of the newly established DoD Computer Security Center (DoDCSC), however, such distinctions are not trivial.

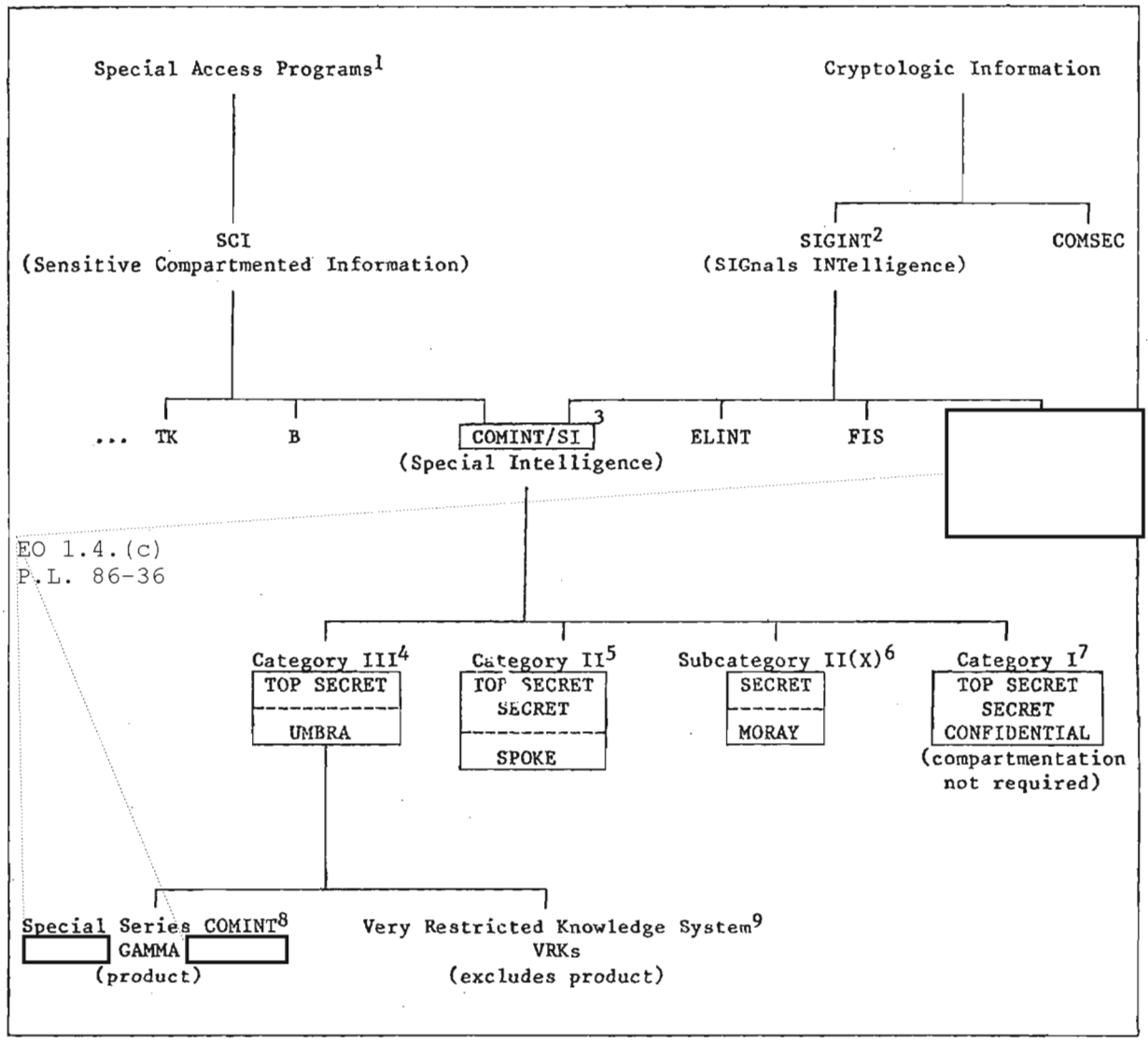
(U) Specifically, the C2 organization (Office of Applications Systems Evaluations within the DoDCSC) is directly involved with the formal evaluations of both operational and developmental computer systems, inside and outside the NSA environment. The C21 division is responsible for providing ADP security guidance during the development of systems, while C22 evaluates systems that are about to become operational or are already fully operational.

~~(C)~~ Generally speaking, computer processing systems are evaluated in different ways depending on the users and the types of information that pass through the system during its operational existence. Typically, any intelligence processing system may be described as operating in one of several modes, as defined by the Director of Central Intelligence Directive (DCID) Security Policy on Intelligence Information in Automated Systems and Networks (formerly DCID 1/16), which establishes policy for computer security in the Intelligence Community. The most stringent category of ADP security is that of Compartmented Mode.

> SCI may be processed and/or stored in an ADP system operating in the Compartmented Mode; that is, the system is processing two or more types of SCI, or any one type of SCI with other than SCI, and system access is secured to at least the TOP SECRET level, but all system users need not necessarily be formally authorized access to all types of SCI being processed and/or stored in the system.
> (p. 5, paragraph II.2.C(1))

(U) A recent C22 evaluation dealt with a computer system that is considering placing GAMMA-controlled information in an existing system data base. Thus, GAMMA had to be defined using the terms that were thought to be appropriate so that the system in question could be properly mapped into one of the

OCID: 4009863



1. Reference EO 12356, Section 4.2
2. Reference SISR Volume I Section I
3. Reference SISR Volume 1
4. Reference SISR Volume I, Section II, Part I (2.a.) & USSID 3, Annex A, Appendix 1
5. Reference SISR Volume I, Section II, Part I (2.b.) & USSID 3, Annex A, Appendix 2
6. Reference SISR Volume I, Section II, Part I (2.c.) & USSID 3, Annex A, Appendix 3
7. Reference SISR Volume I, Section II, Part I (2.d.) & USSID 3, Annex A, Appendix 4
8. Reference SISR Volume I, Section II, Part I (3.) & USSID 3, Annex E
9. Reference USSID 16

several modes of operation defined in the DCID. Unfortunately, it was surprisingly difficult to determine whether GAMMA was an SCI Compartment, a VRK, a special handling caveat, or something else. As it turns out, I was asked to find out what formal relationship GAMMA has to the information hierarchy within the Intelligence Community.

~~(C)~~ The attached diagram represents a picture of the various levels of information within the Intelligence Community. Elements that lie directly beneath a higher-order element and that are connected by a horizontal line may be considered subsets of the higher-order element (i.e., TK, B, and COMINT/SI are all information subsets of SCI). No attempt has been made to show any of the subelements under SCI or SIGINT, except for the COMINT/SI subelement, which has been expanded out of necessity.

(U) Probably the most confused abbreviations that are used regularly at NSA include SI, SCI, and SIGINT. Consequently, these are the only ones expanded on the chart.

(U) The term SCI explicitly includes all Sensitive Compartmented Information on an Intelligence Communitywide basis. SIGINT (SIGnals INTelligence), since it is not a subset or a type of SCI, is not a Compartment. On the other hand, SI is an SCI Compartment, and yet it is also a formal subset element of SIGINT. This is why there are two horizontal lines attached to the COMINT/SI information element.

(U) COMINT and SI are the same; that is, SI is synonymous with COMINT. Apparently, the term SI has been used in the past as an unclassified way of designating COMINT activity. Now, since the word COMINT has been declassified, the term SI is somewhat obsolete. Most of the confusion surrounding SI probably stems from its past use in two entirely different contexts. In the first context, SI has been commonly used, although incorrectly, as a broad way of designating all Compartmented Information (i.e., SCI). In the second context, SI has been used (correctly) as a cover term to designate specifically the SCI Compartment COMINT. At any rate, SI stands for Special Intelligence--not Sensitive Information or Signals Intelligence. Since SI is technically a Compartment, it resides within SCI; note, however, that SI is also an information subset within SIGINT that is not in and of itself a formal Compartment or type of SCI.

~~(C-CCO)~~ The specific C22 evaluation that triggered this clarification project in the first place determined that GAMMA is an information subset within the Special Series COMINT element located hierarchically beneath COMINT Category III. COMINT is the Compartment and GAMMA is presumably a Special Series Compartment, or subcompartment, if you will. This distinction raises several interesting questions:

[] Should computer systems already processing Compartmented information (COMINT material, for example) be required to meet higher computer security specifications if substantially more sensitive information from within the same Compartment (e.g., GAMMA-controlled information) is placed on the system, while all users are not authorized access to the Subcompartmented information?

[] Are the controls that SCI Compartments are currently required to meet necessarily sufficient for all subcompartmented information contained within these Compartments? In other words, are the regulatory computer security controls restricting everyday COMINT access, by definition, refined enough to correctly handle the substantially more sensitive GAMMA information retrieval process?

[] Should not subcompartmented information elements require stricter computer security controls than their parent Compartments?

Hopefully so. Unfortunately, the pertinent DCID's most stringent set of computer security controls is not only in a broad and general policy format, but also stops at the SCI Compartment level. Perhaps, several layers of detailed regulatory controls should be incorporated to cover all types of highly restricted material, including all levels of Subcompartmented information.

(U) It would be great if NSAers talked the same language by using the appropriate acronyms, abbreviations, and other sensitivity terms precisely. Being a recent college hire, I know how overwhelming the multitude of acronyms, Compartments, Classification/Caveat markings, and other assorted sensitivity handling labels can be--especially to new employees. Hopefully, this article will lead to the necessary actions to make clearer language possible at NSA. Any corrections, comments, or other useful information pertaining to this subject will be greatly appreciated. I can be reached via PLATFORM mail ("rankin @ cayley" or "rankin @ gandalf") or on secure extension 968-8584.

P.L. 86-36

Over the nine-year history of Cryptolog, one article stands out as the most popular: Some Tips On Getting Promoted, by [redacted] published in December 1978. Many hundreds of copies of the article have been given out, and requests continue to come in.

Because of the article's continued popularity, and because our supplies of reprints were exhausted, we went back to the author and suggested that we rerun the article along with any necessary changes and she has graciously consented.

The article was written as a result of the author's experience as a member of the 1978 NSA Grade 14 Promotion Board. In 1980 she was Chairman, with vote, of the NSA Grade 15 Promotion Board. For the last two years, she has been a member of the Advisory Panel on Executive Development, which has selected members for the Senior Cryptologic Executive Development Program (SCEDP). Both groups use the employee's promotion file as an important document to study during the selection process. And one of the major items in that file is the Personnel Summary.

The author documents how important the Personnel Summary was, and still is, to the promotion process at NSA. Because so few NSA employees seem to understand this, judging by the state of their Personnel Summaries, this article is as valid today as it was then. It is not exaggerating to say that your Personnel Summary is critical to your professional life at NSA.

The original article is being reprinted here intact. Footnotes have been used to make the few changes necessary to ensure currency and accuracy.

This article reminds you that it is your responsibility to write your Personnel Summary and keep it up to date. It also gives some guidance to help you do it. I hope you will read and heed its message.

Editor

DOCID: 4009863

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

S14

12. PUBLICATIONS (List titles; do not confuse this with reports prepared as a regular part of the job) | DATE

SOME TIPS ON GETTING PROMOTED

Article based on talk given in April 1978 to WIN (Women in NSA)

CRYPTOLOG, Dec 1978

Promotion. The word inevitably stirs response of some kind in every red-blooded NSA employee: hope, pleasure, challenge; despair, frustration, disappointment; even inertia, resentment, resignation. Despite disparate views on promotion, most people share -- openly or secretly -- a common desire to be promoted. And many also share, I think, a common lack of understanding about the promotion process here at NSA and a lack of knowledge about the part they play in it.

(1) This article mainly addresses promotions to grades 13 through 15* and discusses two subjects which are fundamental to those promotions -- Personnel Summaries and Promotion Files. Both are critically important to you, the employee, because they are critically important to the promotion process here at NSA. Witness these two points:

- *your Promotion File represents you to a promotion board,* and
- *you personally write only one document in that file -- your Personnel Summary.*

Promotion Files described in this article are the ones regularly kept only for people of grades 12 through 14, for use by the three NSA-wide Boards that handle promotions for grades 13 through 15. These Promotion Files are described in the final section of this article. Promotions below grade 13 are handled by local organizations whose practices vary on maintenance of personnel files and their use in the promotion process.

Personnel Summaries, on the other hand, are important to everyone, regardless of grade. For grades 12 through 14, the formal promotion process requires that every Promotion File, hence every Personnel Summary, be reviewed during every promotion cycle. For grades up through 12, some local promotion boards use them as well. (2) I recently* chaired a local promotion board in my parent organization, S1, and we routinely reviewed Personnel Summaries of grades 2 through 11 each time we met. Personnel Summaries have still other uses: for overseas assignments; for transferring to a new job; for some types of training. Whenever, in fact, official information on you and your career is needed, the Personnel Summary may be used. The first and major part of this article presents tips on how you should write your all-important Personnel Summary.

The ideas in this article are my own. I am not an expert on personnel matters and do not mean to appear to be. Though I am currently serving on the Agency Grade 14 Promotion Board,* (3) my experience there has simply confirmed long-held impressions and reinforced my belief about the critical importance of the two topics covered in this article.

Personnel Summaries

Many consider Personnel Summaries to be the bane of their existence. Some don't take them seriously. Others fill them out casually. And most of us write them because we're forced to. Whatever you feel about Personnel Summaries, you should recognize why a Personnel Summary is important, who is responsible for filling it out, when it should be filed, and how to get it filed.

Why Important?

Why is your Personnel Summary important? Because it is an essential document in your Promotion File, the one that describes your complete NSA life: your jobs, your accomplishments, your training, your awards. It is no secret what things are deemed desirable for promotion. The information you provide in your Personnel Summary constitutes a list of the very things judged important when selecting people for promotion, *to any grade.* Your Promotion File represents you to the Board; it is one of the most important sources of information about you available to them. Board members cannot be expected to have personal knowledge of you in a large Agency like NSA. True, if you are fortunate enough to be nominated for promotion, then a written recommendation about your accomplishments and qualifications is included in your Promotion File. Otherwise, *your Personnel Summary is it!* Since every Promotion File contains one and you write it, it is your chance to describe what you have done. No one knows it better. And if you do not say it, it may not get said at all.

Who Is Responsible?

Who is reponsible for your Personnel Summary? *You* are! You are responsible for filling it out initially (within 90 days after promotion to grade 12 through 14) and then for updating it. Do not expect your office to remind you. It is your responsibility. Though Personnel Summaries are not required for them, I also urge people in grades *below 12* to fill out Personnel Summaries and to update them periodically. Get into the habit now, for it is easier to do it routinely and gradually than suddenly in one big lump when you do become a 12. Also, I think it shows supervisors that

~~FOR OFFICIAL USE ONLY~~

you are a person of initiative with serious career intentions.

When to File

As I mentioned in the previous paragraph, you are required to update your Personnel Summary within 90 days after promotion to grades 12 through 14. I recommend you also do it whenever a major event occurs, such as when you: transfer to a new organization or job; become a supervisor or assume major new duties; receive a major award, professional certification, or educational degree. Otherwise, plan to do it annually, in synchrony with the promotion board cycles. Currently the grade 13 Board meets four times a year; the grade 14 and 15 Boards meet twice. If your updated Personnel Summary is *in your file* by 1 January or 1 July, you will satisfy all Boards. (Since Promotion Boards are appointed for a calendar year, I recommend January.) I simplify updating my own Summary by following a practice I use to keep track of income tax deductions: whenever anything of importance occurs, I jot it down on a slip of paper with the date and stick the paper into a file. When the time comes to update, I have all the information at hand and the job is nearly done.

Tips on How to Write a Personnel Summary

The following paragraphs describe ways to write a Personnel Summary. These are my personal ideas, and some people -- even you -- may not agree with them. So be it. But I hope to stimulate you to think seriously about Personnel Summaries and to try to help you to write a better one. My aim is to give you a start and hope that you will take it from there.

My best general advice is to be succinct. Say what you have to say briefly, concisely and clearly. Do not write the Great American Novel and ramble on for 20 pages. On the other hand, avoid being too brief and selling yourself short. (I am surprised at the number of people who write one-liners!) Do not try to upstage Agatha Christie and write a mystery story, but avoid too much excruciating detail. Write your Personnel Summary so that a busy person, who is reading hundreds of Promotion Files, can understand and appreciate it quickly and, you hope, be impressed enough to single out your file for special consideration.

Personnel Summaries are written on Form P3267 (REV Feb 76)★which is available in your office or from the NSA Supply Room. The first page contains seven items. Fig. 1 shows the first four:

(4)

AS OF (date)	1. NAME (as it appears on official records) (Last, all capital letters)	(first)	(middle)
Dec 1978	Smith	Jane	Anne

2. EMPLOYEE IDENTIFICATION (SSN)	3. CRYPTOLOGIC SERVICE MILITARY (i.e., ASA, AFSS, NSG, NSA) (years)	(months)	CIVILIAN (years)	(months)	4. TOTAL FEDERAL SERVICE
123-45-6789	3	2	12	9	15 yrs 11 mos

Fig. 1

The "As of" date should never be over a year old. Some files contain Personnel Summaries so ancient that the paper has turned yellow! An out-of-date summary raises some rather unflattering -- to you -- questions in the mind of the reader. Are you lazy? Are you so disorganized you cannot remember to update it? Don't you care?

One sees many Personnel Summaries with only the dates changed -- the correction tape over the date is obvious in the reproduced copy. This is often done, and rightly so, to save retyping when there are no major changes to report. But what if there *are* important changes in your job and you don't record them? Look below at Item 6, "Experience" (Fig. 2), taken from a *supposedly* current Personnel Summary:

6. NSA/CSS OR SCA CIVILIAN EXPERIENCE				
TITLE	GRADE	DATE OF ACTION	AGENCY	ORGANIZATION
A. CURRENT ASSIGNMENT (Functional/Job Title, e.g., Chief, Data Storage Equipment Division; if none, use job title reflected on 3150 or SF 50)				
Traffic Analyst	12	Jan 1976		B111
B. TITLE OF LAST PROMOTION				
Traffic Analyst	12	Apr 1970		B9
C. INITIAL ASSIGNMENT				
Analyst	5	Jun 1958		ALLO

Fig. 2

DOCID: 4009863

To the eye, Item 6 in Fig. 2 looks fine. However, this person is no longer a Traffic Analyst in B111. He has transferred to a new job -- a supervisory one -- and he is now Chief, Processing and Analysis Division, X35. *But how is the Board to know?* The problem is magnified if this person is nominated for promotion. The documentation that accompanies the nomination describes the person's *current* job, with the result that the two documents -- the nomination and the Personnel Summary -- do not match. How does that look to a Board? Again, what does it say about you and your sense of responsibility?

When listing your current job title in Item 6, be sure to use the *functional* job title if you have one. For example: D/Chief, Data Storage Division; Project Manager for XXXX; Russian Language Instructor. Otherwise, use job titles as shown on the form.

Now let's go back to Item 5, your educational record (Fig. 3):

5. EDUCATION *(List most recent first)*

SCHOOL *(Include Joint or Senior Service Colleges; also, any substantial work done toward a degree, but for which no degree was awarded)*	DEGREE	MAJOR FIELD	DATES *(If great span of time involved, indicate reason, e.g. (Night))*
University of Maryland	MA (20 credits)	International Relations	1976-78 Nights
Armed Forces Staff College	Diploma	--	1975
University of Maryland (Cum Laude, Phi Beta Kappa, Honors in History)	BA	History and Political Science	1971-1973
Anne Arundel Community College	Assoc.	History	1960-71
Bowie High School	Diploma	College Prep	1969

Fig. 3

List these in reverse chronological order, with the most recent first. Include all education for which you earned a degree and use "Diploma" to indicate completion of a joint or service school. Also include substantial work toward another degree. If any of these took extended time, indicate why (as "Nights"). And I suggest you state any graduation honors here, to highlight them.

Item 7, "Commendations and Awards," should also be in reverse chronological order. Fig. 4 shows some examples of the kinds of things to include.

7. COMMENDATIONS AND AWARDS *(e.g. Meritorious Civilian Service Awards, Outstanding Performance Appraisals, Letters of Commendation from Chiefs of major organizations or higher) (List most recent first)*	DATE
Letter of Appreciation, Chief A	1978
Level 7 Performance Rating	1977
Outstanding Performance Ratings	1975, 73, 69
QSI	1974
SSWP	1968
Meritorious Civilian Service Award	1965
NCS Teacher of the Year	1960
First Prize, CLA Essay Contest	1959
NSA Scholarship	1958

Fig. 4

Include Letters of Appreciation only if they are from an Office Chief or higher (for grades below 12 I think this rule may be relaxed) and be sure that copies of such letters are in your Promotion File. List level-7 performance ratings, but not level-6. Also list any special Agency awards or scholarships you may have received. Professionalization certifications belong in Item 16, and extracurricular activities should be entered in Item 14 -- do not include them here.

(5)

Page 2 of Form P3267 contains two items. At the top, Item 8 provides space for summarizing your "Current Assignment" (Fig. 5). Begin this paragraph by giving your functional job title, the name of your immediate organization, date of appointment, and names of ascending key organizations.

8. SUMMARY OF CURRENT ASSIGNMENT

D/Chief, Support Staff (Z13), Office of Facilities (Z1), Computer Services Organization (Z).

Since April 1973 Mrs. Jones has been responsible for managing. . .

Fig. 5

CID: 4009863

Then list your major responsibilities, following these recommendations:

- Use narrative style (not outline form),
- Use complete sentences,
- Use third-person forms (not "I was responsible for...," but "Mrs. Jones was responsible for...")

Note that your supervisor's signature is required in Item 8 as verification.

Item 9, at the bottom of page 2, is the "Summary of All Previous Civilian and Military Service of a Cryptologic Nature." This is probably the most difficult part of the form to fill out. The longer your career, the more you have to tell about. If there is not enough space provided in Item 9 to hold all the information requested, you should use as many additional plain sheets as necessary, labeling each with your name, SSN, and page number.

This is likely to be the longest section, so it is important to try to make it clear and readable. You do not have to be an accomplished writer or even to have any special writing skill. Just be direct, factual, and as concise as possible. Follow instructions given above for Item 8 (use narrative style, complete sentences, third-person forms). In addition, follow these suggestions:

- Use *chronological* order ("Begin with oldest assignment and end with most recent"). Note that this is *not* "reverse chronological order," as in some of the other items;
- Use one paragraph per job;
- Start paragraph with vital information: dates, functional job title, immediate organization and up;
- Identify organizations, projects, systems, etc.

Notice that I said to identify "organizations, projects, systems, etc." Otherwise, you end up writing a mystery story, like this one:

> "From August 1960 to January 1964, Mr. Smith was Chief of A13 where he was responsible for managing all aspects of Project SUCHNSUCH. He also provided technical assistance to several important systems under study by another division: XYZQ and ABCJ."

The only really clear thing in this paragraph is the date! Who remembers what A13 was in the early 1960s? What in heaven's name was SUCHNSUCH? What were systems "XYZQ and ABCJ"? And so on! How much clearer, and how much more professional if this had been written instead (Fig. 6a):

9. SUMMARY OF ALL PREVIOUS CIVILIAN AND MILITARY SERVICE OF A CRYPTOLOGIC NATURE (List in chronological order - begin with oldest assignment and end with most recent; indicate location, functional/job title and dates)

From August 1960 to January 1964, Mr. Smith was Chief of the Nonesuch Reporting Division (A13) in the Office of Overall Reporting (A1) in the General Analysis and Reporting Group (A). He was responsible for managing all aspects of Project SUCHNSUCH (full-text automation of Nonesuch reports) and provided technical assistance to several important systems under study by another division: XYZQ (system for automating. . .) and ABCJ (system for . . .).

Fig. 6a

If you wish, you may use a space-saving format, with an offset header (for dates, jobs, and organizations) followed by a colon and and a list, as in Fig. 6b:

9. SUMMARY OF ALL PREVIOUS CIVILIAN AND MILITARY SERVICE OF A CRYPTOLOGIC NATURE (List in chronological order - begin with oldest assignment and end with most recent; indicate location, functional/job title and dates)

August 1960 to January 1964
Chief, Nonesuch Reporting Division (A13), Office of Overall Reporting (A1), General Analysis and Reporting Group (A):

Mr. Smith was responsible for managing: SUCHNSUCH (full-text automation of Nonesuch reports), all reporting on . . ., and providing technical assistance to another division on several important systems, such as XYZQ (system for automating . . .) and ABCJ (system for . . .).

Fig. 6b

These may seem like small things to you, but they have a big impact on improving the readability of your Personnel Summary. You do want people to read it, don't you? As the final test, I recommend that you ask a friend to read your Personnel Summary critically to

DOCID: 4009863

see if it is indeed clear and to the point. Preferably that friend should pretend that you are *not* a friend, but a complete stranger who wants to know everything about you. Does your Personnel Summary present you as a clear-writing (and, presumably, clear-thinking), forceful, direct person, or as an imprecise, vague person carrying out "various" unexplained duties? Rewrite your Summary, and especially Item 9, until anyone who reads it -- not just your friends who have known you for years -- can get a clear picture of what you have done and why you are promotable.

Page 3 of the form contains four items, the top three of which are often ignored -- or so it seems when they are so frequently left blank: "Field Assignments," "Related Experience" and "Publications." If you have pertinent information on any of these, put it in.

For Item 10, "Field Assignments". (Fig. 7), be sure to give both the organizational and functional titles and the inclusive dates. These items are in *reverse* chronologcal order. Incidentally, regular updating of Personnel Summaries seems to be a special problem for people assigned to the field. Their Personnel Summaries are rarely updated while they are away from Fort Meade/FANX and consequently the promotion boards often have no knowledge whatever about what the person is doing during an important 2- or 3-year period. I urge people to file yearly updated Personnel Summaries while they are on field assignments.

10. CRYPTOLOGIC COMMUNITY FIELD ASSIGNMENTS (CONUS and Overseas) (List most recent first)			
ORGANIZATION	LOCATION	FUNCTIONAL/JOB TITLE	DATES
F06	Timbuck	Station Chief	1975-78
F99	Eden	Engineer	1969-72
F17	Nowhere	Analyst	1965 (Jan-Mar)

Fig. 7

For Item 11, "Other Civilian/Military Experience" (Fig. 8), include those things that show you possess skills that may apply to your NSA job, such as teaching, managing, and organizing. These are also in reverse chronological order. For example:

11. OTHER CIVILIAN/MILITARY EXPERIENCE WHICH MAY BE RELATED TO AN NSA/CSS OR SCA POSITION			
ORGANIZATION	LOCATION	FUNCTIONAL/JOB TITLE	DATES
Army Reserve	Ft. Meade, Md.	Platoon Leader	1971 to present
G.W. Univ.	Washington, D. C.	Lecturer in Computer Science	1968-1970
Summer Camp	Arlington, Va.	Director	1965

Fig. 8

Item 12 is "Publications" (Fig. 9). I am disappointed that so few files list any publications. Since publications *are* included in the Personnel Summary, NSA must consider writing to be an important skill. Managers, for example, spend a lot of time writing. And good writing comes from practice. Fortunately for us, NSA offers many opportunities to publish. If you have been looking for places to express your views, here they are:

(6) *NSA Technical Journal*★
Cryptologic Spectrum★
(7) CRYPTOLOG
Field Information Letter★
Essay Contests (Learned Organizations -- CMI, CLA, CAA)
CISI Spring Conference
Cryptologic History Series
NCS courses
Informal Agency newsletters such as *SOLIS Newsletter* and the previously published *Bits and Bytes, Dragon Seeds, Keyword, Quarterly Review for Linguists.*

The editors of all these publications welcome your contributions. Try to have some published works and major reports (though not regular ones produced as part of your job) to list on your Personnel Summary. It just may help to attract attention to your File!

12. PUBLICATIONS (List titles; do not confuse this with reports prepared as a regular part of the job)	DATE
"Project SUCHNSUCH -- A Personal View" -- article based on talk given in April 1978 to Computer and Information Sciences Institute (CISI)	CRYPTOLOG, Dec 1978

Fig. 9

The next three sections, all part of Item 13 on the form, are meant to show "Highlights in the Area of Self Development" in your professional life -- past, present, and future. The format is the same for all three sections. Fig. 10 gives some examples for "A. Past." List here the things that are completed, such as past membership in professional societies and education not already listed in Item 5. Courses taken at NSA belong here. Follow the example and identify the courses by title and course number. In the rightmost column, you can indicate things like "Top student" or special honors. You can leave this column blank if nothing applies.

13. HIGHLIGHTS IN THE AREA OF SELF DEVELOPMENT: *(Chronologically list all formal NSA/CSS/SCA, college level or technical courses (military or civilian) as well as membership in either NSA/CSS/SCA or external professional societies) (Exclude those for which a degree was subsequently awarded)*

	SUBJECT/SOCIETY	PLACE	DATES (from - to)	DURATION OR LENGTH	DEGREE	SPECIALTY/ OFFICE HELD
A. PAST	Zeta Eta Eta (French Honorary	University	1965-68	--	--	President, 1967
	MS-111 (Briefing Skills)	NSA	1968	49 hrs	S	--
	MG-444 (Management Analysis	NSA	1971	120 hrs	A	Top student
	CMI	NSA	1971-present	--	--	Member

Fig. 10

The first two items on page 4, the last page of the form, are "B. Present" and "C. Future" highlights in your self-development (sections not reproduced here). These sections are to be filled out in the same manner as "A. Past." Future plans might include such things as your plans to attain another specified certification, change career fields, join a professional society.

Item 14, "Other Achievements" (Fig. 11), provides space for showing your self-development in your nonprofessional life. Many people leave this blank. If you do, I think you are missing a big opportunity to provide a rounded picture of yourself to the Promotion Board. If you are active in areas like those listed below, I encourage you to list them. Show by your non-job-related activities that you have other interests -- and other talents.

14. OTHER ACHIEVEMENTS *(In brief, list all NSA/CSS/SCA affiliate endeavors, which are not necessarily a part of your assigned duties, i.e., Civilian Welfare Council, GEBA, NSA/CSS/SCA club, etc; Civic or Community efforts may be included)*

ACTIVITY	INCLUSIVE DATES	CAPACITY IN WHICH SERVING/SERVED
NSA:		
Civilian Welfare Council	1967-1969	B Group representative
Credit Union	1970-1973	Member, Board of Governors
GEBA	1976-present	Member, Board of Directors
NSA Jazz Band	1970-present	Member
Travel Club	1972-present	Member; President, 1976-78
United Givers Fund Campaign	1977	Keyman, B Group
Community:		
Church, Scouts, recreational activities, civic associations, PTA	(Provide appropriate information)	

Fig. 11

Item 15 (not reproduced here) provides space for you to list your job-related or self-improvement "Reading Achievements" -- in-house publications, professional journals, foreign-language material. Please do not list your pleasure reading, especially not "Playboy." Board members have seen that one so often, they are weary of it!

"Professionalization" certifications are to be listed in Item 16 (Fig. 12). If you have more than one, be sure to list them all, with the dates awarded. If you are about to receive still another, note this in parentheses, as shown:

16. PROFESSIONALIZATION *(List professional certification(s))*

CERTIFICATION		
TITLE	DATE	CERTIFYING PANEL (S)
Cryptanalyst	12 Jun 1970	Cryptanalysis Career Panel
Education and Training Officer	1 Sep 1973	Education Career Panel
Traffic Analyst (Lack only Part 3 of PQE for certification -- scheduled to take test in Nov 77)		

Fig. 12

DOCID: 4009863

Finally, sign the form, date it, and affix the proper security classification. Take this last responsibility seriously and do it carefully, seeking help from experts if you need it. Underclassifying or overclassifying looks bad to a Board because Boards expect that by grade 12 you should know how to classify correctly or know where to find help.

(8) Instructions for filling out Personnel Summaries are contained in the *NSA Personnel Management Manual*, Chapter 302B (Jul 76)★ which every major office has. Your own office will handle the filing of your Personnel Summary for you. It will reproduce multiple copies of it, some for retention in local organizational files, one for you, and (for grades 12 through 14), some for sending through channels to your Promotion File in M3.

Promotion Files

(9) Promotion Files are not to be confused with Personnel Files★ often called "201 Files." The Office of Personnel, specifically M3, maintains both. There is an official Personnel File for every NSA employee. It documents all formal activity in connection with your NSA life: hiring, performance appraisals, training, job or organizational changes, etc. There are official Promotion Files only for employees in grades 12 through 14. Local organizations often maintain abbreviated versions of the 201 File on all their employees (and some may also keep a Promotion File). Official Promotion Files are the files that are being discussed here -- the files used by the three Agency Promotion Boards when considering people for promotion to grades 13 through 15.★ (10) I am going to tell you what should be in your Promotion File, how you can make arrangements to see yours, and how you can update it.

Your Promotion File should contain:

- Personnel Summary (current within one year);
- Certification documentation (in the form of a computer printout or a letter from the certifying Panel);
- Recommendation for promotion from Key Component, if you are recommended. (Since Promotion Files are shown to you intact, with nothing removed, you can see the recommendation on you if there is one, or know you are not currently being recommended if there is not.)

In addition, your Promotion File should contain, *for your current grade only* (information from previous grades is purged):

- Performance appraisals;
- Inventory of Attributes (If you are a 12 or above, this is part of your official Performance Appraisal. However, you may never have seen it or even know it exists because, until recently, it was a private document and was generally not shown to employees. Nowadays the sheet is green but it used to be yellow, and many files still contain copies of "yellow sheets")★ (11)

Fig. 13 shows the form for the Inventory of Attributes. Rating is on a scale of 00 through 99, and space is provided on the right for narrative comments. Like the information in a Personnel Summary, the items in the Inventory of Attributes

(24)	A. Innovativeness: Consider how well the individual provides problem solutions, shows ingenuity and creativity and pioneers in seeking new ways to complete work faster and more accurately.	
(25)	B. Effectiveness in working with people: Consider how well the individual meets and deals with others, his/her effectiveness in establishing and maintaining working relationships with peers, subordinates and supervisors.	
(26)	C. Drive and Initiative: Consider the extent to which the individual demonstrates attributes such as forcefullness, aggressiveness and enthusiasm.	
(27)	D. Personal Characteristics: Consider all personal characteristics as they affect the individual's job performance.	
Present (28) / Higher (29)	E. Subject-matter knowledge: Consider the individual's depth and breath of knowledges and skills required at his/her present and next higher grade.	
(30)	F. Advancement potential: Consider how the individual compares with others for advancement to a position of greater responsibility and his/her overall capability for progression within the career field.	

Fig. 13

DOCID: 4009863

P.L. 86-36

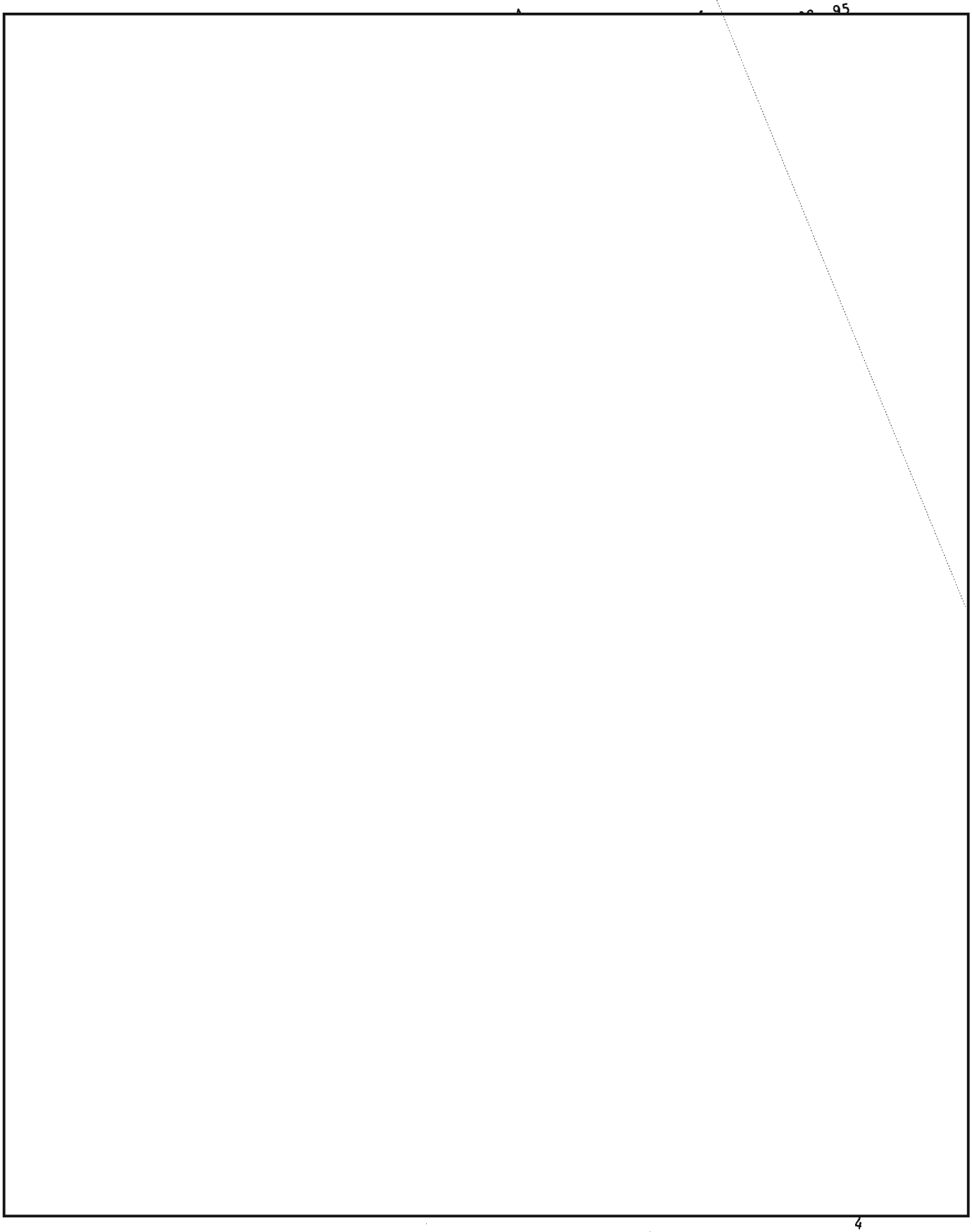
How I Almost Helped Win the FALKLAND ISLANDS War (U)

by Pfc(Ret) [redacted] P16

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

60
95



4

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

TWO NEW LANGUAGE AIDS (U)

[redacted]

[ ] Chinese-English Glossary of Linguistic Terms (U)
(work is UNCLASSIFIED and available in hard copy and on microfiche)

(U) Agency employees who need either one can secure a copy of the Chinese aid [redacted] They're both in P16 and their phone number is 963-1103s.

P.L. 86-36

P.L. 86-36

SOLUTION TO NSA-CROSTIC 47

Memorandum [to M36], by [redacted]

"I have put considerable thought into the Senior Technical Expert Program (STEP) since we spoke last week. The following ideas differ hardly at all from those I espoused then, but the clarity with which I can state them may have improved."

Mr. Smith

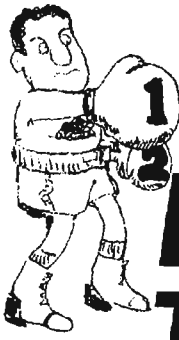
I have been reading Cryptolog for a number of years, but have had to get it by finding an abandoned copy or out of a burn bag. Now that I've switched organizations, I rarely see a copy in either of the above-mentioned categories. Thus, could you please add my name to your distribution list?

Thank you in advance

[redacted]

P.L. 86-36

DOCID: 4009863



Human Factors

Punching the BIOLOGICAL TIME CLOCK (U)

by

[redacted]

P.L. 86-36

According to an article by Wray Herbert in Science News (Vol, 122, No. 5, July 31, 1982) it was 4 AM when the accident at the Three Mile Island power plant occurred and the employees on duty had just that day "rotated" shifts, switching from the day shift to the night shift. Poor human performance has since been implicated as a major cause of the accident. Abnormally high accident rates in other industries--trucking and Navy, for example--have also been linked to human error. And, increasingly, researchers have been looking to unnatural shift rotation as a possible cause of occupational mishaps.

Scientists have now applied some basic principles of circadian rhythm, the natural sleep-wake cycle, to the design of an actual industrial work schedule and have reported that a more natural rotation pattern improves worker satisfaction and health and also causes an improvement in job performance.

According to Charles A. Czeisler of Harvard University and the Boston-based Center for Design of Industrial Schedules, one in four American workers works something other than a standard day shift, and many of those who rotate shifts do so in a way that violates the natural timing of sleep and wakefulness. The workers at Great Salt Lake Minerals and Chemicals Corporation in Utah, the site of the experiment, had for 10 years rotated every week to the preceding shift--from days to nights to evenings to days, etc. With the cooperation of the company, Czeisler and his colleagues--Martin C. Moore-Ede of Harvard Medical School and Richard M. Coleman of Stanford Medical School--changed the schedules of 85 workers: 33 began rotating to a later shift every week and 52 rotated to a later shift every three weeks. The researchers compared the subjects to 68 non-rotating shift workers on measures of job satisfaction, health, personnel turnover, and productivity.

The results revealed that 70% of the workers preferred forward rotation; those who rotated weekly showed a 49% improvement in satisfaction, while those who rotated every three weeks showed an 87% improvement. The latter group also showed an improvement in health, though they still fell short of the controls. In addition, personnel turnover decreased and productivity increased 22 percent, a gain that was maintained nine months following the study. The company has since adopted the new rotation schedule for the entire plant.

The circadian principles underlying the schedule design are fairly simple, Czeisler said. Because the natural sleep-wake cycle, controlled by oscillations in deep body temperature, tends to run about 25 hours, the natural tendency is to go to sleep later and later. But most people have the capacity to adapt to a change of one or two hours a day (delay or advance) without becoming "desynchronized." In fact, people are constantly advancing their sleep by an hour a day to conform to the earth's 24-hour schedule. But when people rotate shifts, Czeisler said, the change in sleep cycle is too dramatic; the system becomes desynchronized and begins to "free-run," to drift forward on its natural 25-hour cycle until it is back on phase.

As long as the system is out of phase, the trough of the alertness cycle occurs during waking hours, explaining shift workers' complaints about exhaustion; the same desynchronization is the cause of jet lag. Because the internal 25-hour clock tends naturally to delay sleep, it is much easier to adapt to a shift rotation that requires sleep delay: a forward rotation. Backward rotation (like eastward jet travel) requires that sleep be advanced, which in turn forces the internal sleep-wake cycle to drift all the way around the clock to get back in phase, a process that, at an hour a day, may take a week or

more. Some workers, Czeisler said, complain of never adjusting to a new shift; even with forward rotation it requires a few days to become resynchronized, explaining why the 21-day schedule was more satisfactory and productive than the 7-day schedule.

According to Czeisler there is no single ideal schedule for all of industry, but it is essential that these basic physiological principles be considered in the design of any schedule that could interfere with sleep. The newly-formed Center for Design of Industrial Schedules, he said, will be examining regulations that involve work scheduling where safety is an issue--Federal Aviation Administration and Nuclear Regulatory Commission regulations, for example.

According to Charles Ehret, a biologist at Argonne National Laboratory in Illinois, FAA and NRC regulations currently pay no attention to circadian principles. Based on his own survey of the American power industry, he said that at least half the power plants were rotating their workers the wrong way, causing sleep deprivation and dangerous desynchronization. "We cannot pinpoint the circadian contribution to the accident at TMI or to any single maritime or aircraft accident," he said, "but there's no doubt that cognitive function, visual acuity, and psychometric performance are 'way, 'way down under these circumstances."

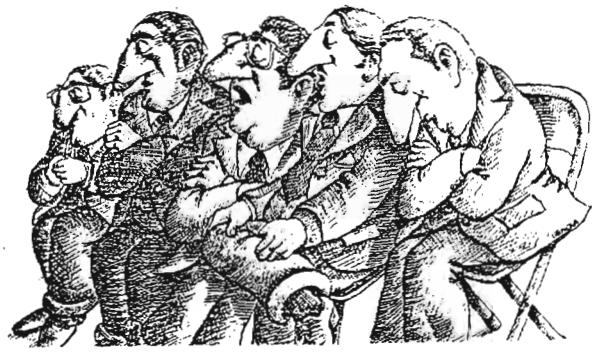
The reason I have devoted so much space to the text of this article is that it certainly has applications for NSA, where there are so many around-the-clock operations which necessitate shift rotation by their personnel. But, to the best of my knowledge, none of those 24-hour shops uses a forward-rotating shift schedule. Some time ago an NSA element did experiment with forward-rotating shifts. The new shift arrangement was not well received overall. Several organizations terminated the test after a three-month trial period. The main reasons for the dissatisifaction were:

[] the employees did not feel any better (despite prediction that they would), and

[] the new shift arrangement created one very short break, in contrast to a very long break under the old scheme.

Under the old shift rotation plan, there were two 72-hours breaks and one 48-hour break. The 48-hour break means coming in off a mid, sleeping during that day, and returning to work on days 48 hours later. The effect is just one day off. That short break was, at best, inconvenient and some workers complained that it did not provide adequate rest between shift changes. It should also be noted that the shift rotation cycle in this experiment was every six days, not the three weeks recommended by the Science News article. Maybe we should give the longer cycles a try.

Based on an article in Human Factors Letter #1-83.



EFFECTS OF HAVING TO GET YOUR SLEEP IN THE DAYTIME

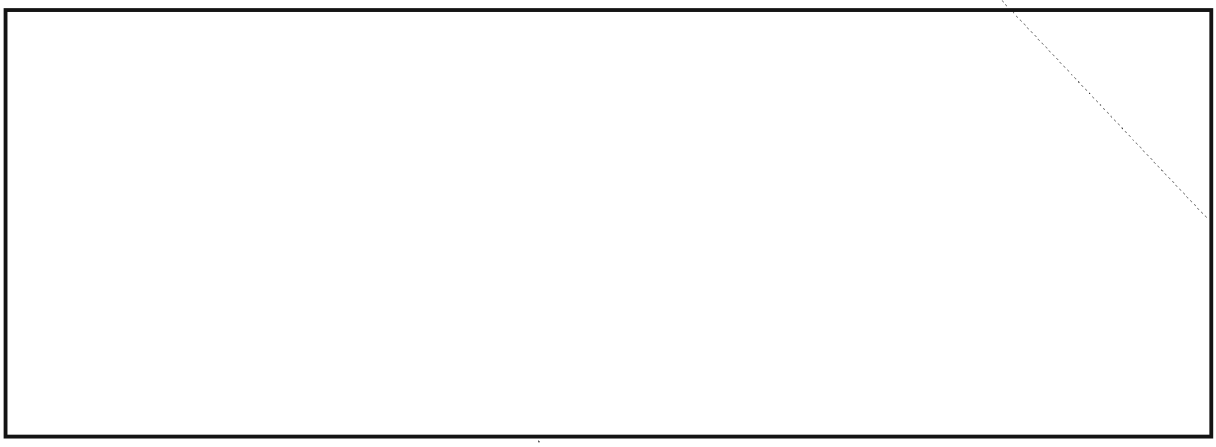
by [redacted] P13

P.L. 86-36

A recent article in the Journal of the Human Factors Society describes a study of some effects of shift work ("The Sleep and Performance of Shift Workers," A. J. Tilley, et al., Human Factors, Vol. 24, No. 6, December 1982, pp. 629-641). This study differs from most previous studies in that it monitored and recorded the sleep of workers in their own homes, rather than in a lab or only indirectly via questionnaires. The abstract provides the following summary of results:

"The sleep and performance of 12 male shift workers, operating a discontinuous, weekly-alternating, three-shift system, were monitored over the course of one complete shift cycle. Compared with nocturnal sleep, day sleep was shorter in duration and was degraded in quality, and its sleep stages were temporally disrupted. Simple unprepared reaction time and four-choice reaction time were impaired at night, and simple reaction time deteriorated as a function of the number of days into the shift and the time on task. Sleep and performance changes can be primarily attributed to circadian factors; however, the deterioration in performance from night to night and with time on task is probably due to an accumulative sleep deficit. As far as sleep and performance are concerned, the best shift system is probably one having a short rotation cycle, with afternoon shifts or rest days preceding and following the night shift."

EO 1.4.(c)
P.L. 86-36

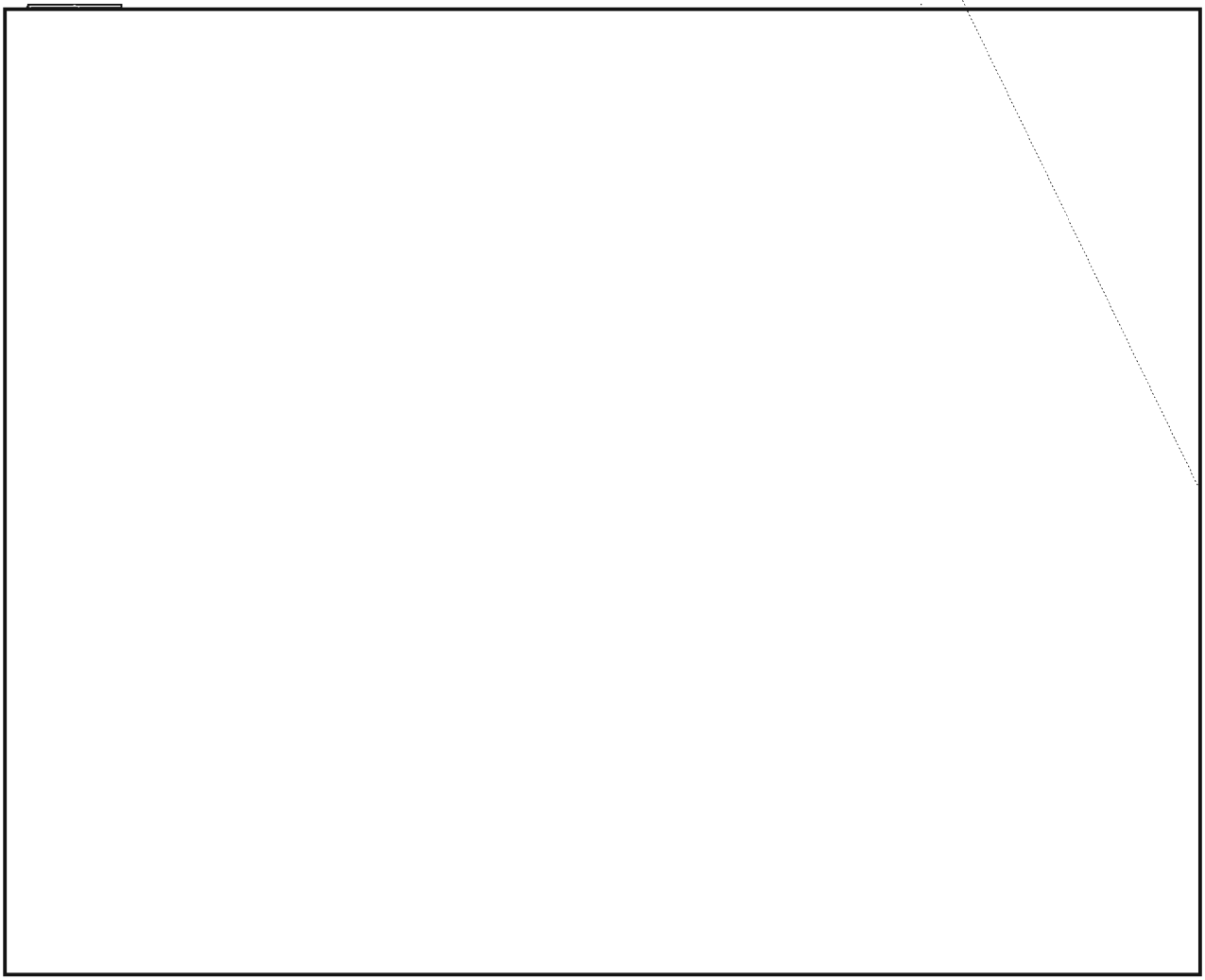


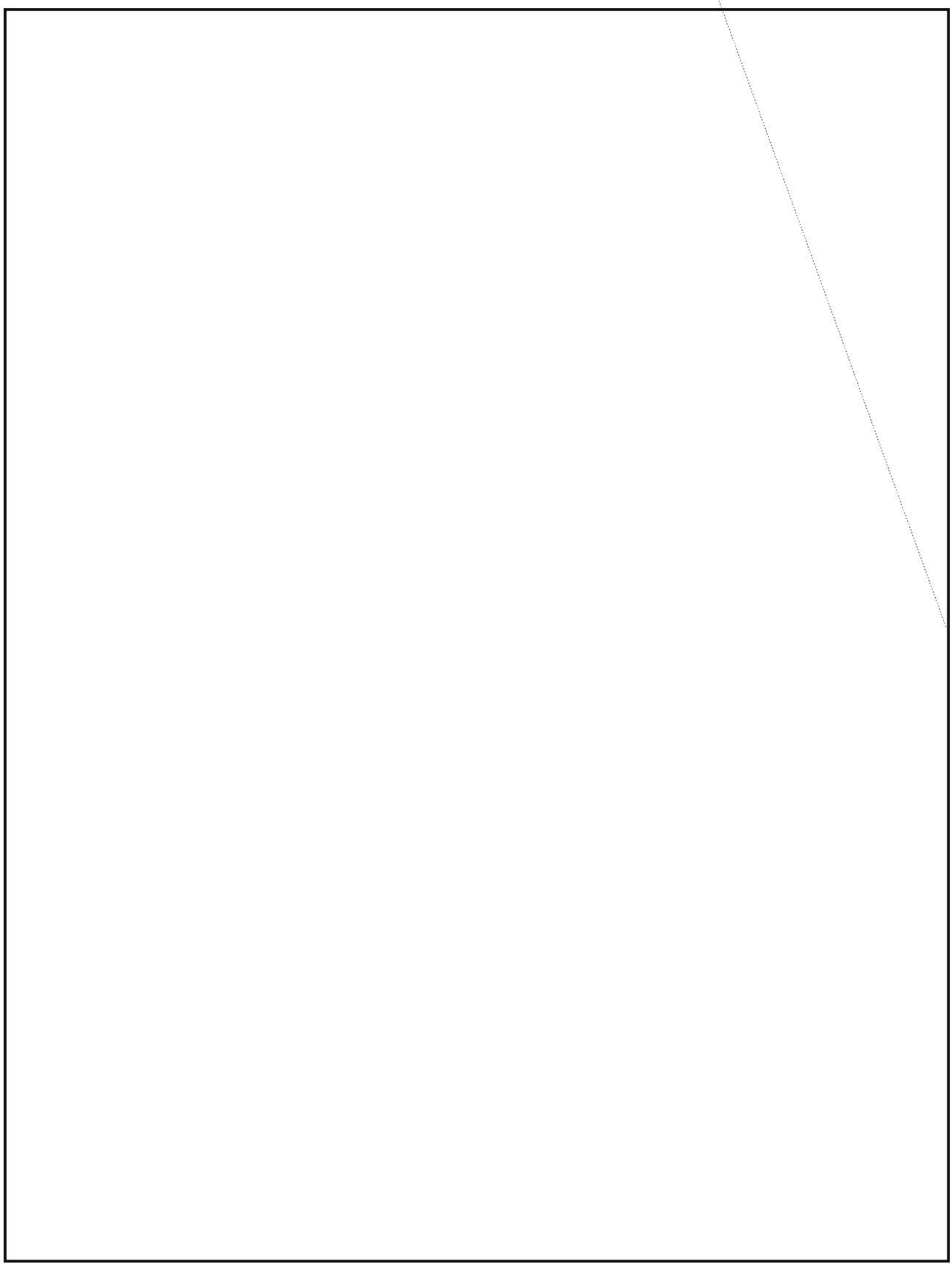
P.L. 86-36

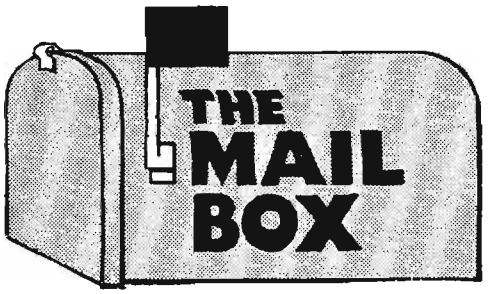
by [redacted] A25

EO 1.4.(c)
P.L. 86-36

& [redacted] T5321







Dear Editor:

Security of classified information is the business of all Americans who have access to it. A problem exists in this area, however, in that not all who have access to such information are educated on the need to protect it. The exposure given to US intelligence agencies in the popular media has made education in classified material security and COMSEC imperative.

A new "NSA Security Agreement" requires the signature of all current, and presumably future, employees of NSA. According to the instructions for completing the form, the Agreement follows the determination by the Director of Central Intelligence that

> "all agencies and departments granting access to Sensitive Compartmented Information (SCI) ... must implement a program to better protect ... vital intelligence assets from unauthorized disclosure."

The explanation goes on to say that NSA's program "includes a security agreement that requires persons with SCI access to submit for prior review any information or material for public disclosure." It appears that the requirement for this agreement was precipitated by recent publicity about NSA.

It is difficult for any employee to argue with the need to protect sensitive information in ways such as those specified in the Agreement. But the question inevitably arises in the minds of those of us with less extensive Weltanschauungen, "Why must we so carefully protect material from sensitive sources when those for whom we gather and analyze it (especially elected officials on Capitol Hill and members of their staffs) discuss it openly?"

Implicit in this question is a perhaps justifiable resentment that many of us harbor against those outside the intelligence community who leak the information we try so hard to protect. As a former staffer in the House of Representatives, I can vouch for the lack of concern (which borders on total disregard) for the need to physically protect classified information from unauthorized disclosure. My concern here is not for those people who work regularly with the intelligence community, such as the Senate and House Select Committees on Intelligence, but rather with the many hundreds of others who can and do have access to sensitive intelligence but who have little understanding of the protection it needs. It is not unusual for classified materials to be left lying on desks in the completely non-secure House and Senate office buildings for minutes, hours, or even over weekends. Often the highest degree of protection offered to this information is to place it in an unlocked desk drawer. Our resentment is unproductive, however, unless it produces workable methods to stop such disclosures and the resolve to implement those changes.

But even if we have both the methods and the determination to correct the problem of leaks of sensitive information, we must still face a most difficult dilemma. We must balance the necessity for some elected officials to have access to classified information against the need to ensure that they are willing and able to maintain its secrecy. Simply by virtue of being elected to Congress or having made large contributions to the party that controls the White House, Senators, Representatives, and Administration appointees have access to almost any information they desire. That they were elected to positions of public trust and confidence implies that they are trustworthy. But the speciousness of this logic is quickly seen if we remember the many Members of Congress who have been censured or indicted for serious crimes over the years, or if we remember Teapot Dome and Watergate. There are enough recent examples of bribery and obstruction of justice, as well as other crimes, to indicate to me that election or appointment to office does not automatically make someone trustworthy.

Another problem, just as thorny, is the access to classified information that many members of congressional staffs and lower-level political appointees obtain almost automatically. There are, of course, valid reasons for some staffers to have access to sensitive information. But most of the people who come to Washington to work on Capitol Hill have had no previous experience in federal government, much less experience with classified material. To many of these people, a security clearance, and the attendant access

to classified material, is more of a status symbol than anything else. The higher the clearance level, the greater a person's status among others who, likewise, previously had no access to classified information.

In order to achieve at least one measure of status, many staffers with little or no real need for access persuade their elected bosses (with little difficulty) to request clearances for them. Virtually all these staffers seem to receive clearances in short order. This indicates to me that Defense Department investigators find nothing in these applicants' backgrounds to preclude them from receiving clearances or that only cursory investigations on them are conducted. I find it difficult to believe that all Capitol Hill applicants for clearances are models of trustworthiness. The swiftness with which their background investigations are completed implies that trustworthiness in not the sole reason they are granted clearances.

There are more than 16,ØØØ members of personal and committee staffs in the Senate and House of Representatives--and who knows how many political appointees in the executive branch? The Defense Investigative Service (DIS), the agency responsible for conducting background investigations for the Capitol and parts of the executive branch, is deluged with requests for clearances. Since the DIS has such a large investigative responsibility, it necessarily must put its responsibilities in some order of priority. The highest priority seems to go to pre-employment for the intelligence community. Here investigators must make a tough decision: If they grant clearances following a pro forma investigation, they are open to charges of negligence if people to whom clearances are granted later prove to be untrustworthy. If the investigators press the nominating Member of Congress to further justify the need for one of his or her staff to have a clearance, they could be accused of damaging Executive Branch relations with Congress. If investigators press Administration officials to further justify the need for a staff clearance, they can be accused of not being "team players" within the Executive Branch.

Conducting pre-employment investigations for the intelligence community may be the best use of scarce DIS resources. Most leaks of national security information usually seem to come not from the intelligence community but from other executive branch agencies and from the legislative branch. Given this, it appears that either clearances have been improperly granted or that those outside the intelligence community need to be made aware of the need to protect this information.

I think that the DIS, generally, is doing a good job in conducting background investigations on legislative staffers, although it could perhaps adhere more closely to established standards for granting clearances. It could require satisfactory completion of a full background investigation before granting a SECRET clearance.

But even though investigations may be part of this problem, the major issue is not so much the ease or difficulty with which people might receive clearances, but the lack of training given on the need to protect the information to which they are given access. Whereas new NSA employees are given a rigorous orientation on the need for security, I know from my own experience that none is given to legislative staffers when they are granted their clearances. In all probability, the same situation exists in the Executive Branch for political appointees. This, in itself, is scandalous. But when this lack of security awareness leads to the inadvertent disclosure of sensitive information, it carries with it many dangerous implications for the nation.

What can we do to remedy this problem? We can politely but firmly insist that other Executive Branch agencies and Congress uphold their end of the national security bargain by immediately implementing comprehensive security education programs among those who are or have been granted access to classified information. It may be naive to think that education alone will change the minds of potential leakers but existing policies and attempts to stop leaks have, for the most part, failed. And the recent Executive Order threatening Administration employees with polygraph testing and possible job action will probably have little noticeable effect on leaks; those intent on damaging the national security will do so, albeit more circumspectly, regardless of potential consequences. We must, then, concentrate on the unknowing (but nonetheless damaging) disclosures made by those who are merely unaware of the implications of the trust their security clearances carry. Security education might help in these cases. We owe it to ourselves to try all possible courses in search of new ways to put a halt to unauthorized disclosures.

Given the transient nature of politically appointed staff people in most of the federal government, security education programs might seem like trying to sweep back the sea. But, with our national security at stake, can we afford to do less?

[redacted] G732

P.L. 86-36

DOCID: 4009863

~~FOR OFFICIAL USE ONLY~~

NSA-Crostic 48

by Vera R. Filby

A. Palindromic plotter

B. Unhidden treasure

C. In Oslo or in backward yawn

D. It's sharp to ice crab

E. Hilarious response to the French grunt

F. VASCAR couldn't do without it (2 wds)

G. Mr. Strauss and actress Sharon combine to float upward

H. Let the Roman behold

I. *Sotto voce*

J. He keeps saying the writer ate sausage

K. Ultimate degree

L. It's between a W and a Y

M. He sang about all those trombones (2 wds)

N. A something, but what?

O. Outer way

P. Verb uninflected in form, to be brief

Q. Often followed by overrun

R. Pop raved, but then said OK

56 89 50 125 63

47 4 42 120 101

137 119 80 23 53 75

62 9 3 132 115 103 59

139 64 81 105 10

65 5 134 19 92 86 99 30

57 118 117 38 127

116 71 97 21 79 69 44 123

111 16 82 93

124 102 18 41 73 51 25 133

8 142 58 17 108 32 130 78

31 20 27

39 35 7 96 88

68 14 141 33 131 90 114 77

37 13 60 76 83 140

46 94 40 135 72

128 107 95

110 34 52 121

138 91 112 126 24 85 98 70

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

S. This dancer won the 1953 Preakness and Belmont — 104 28 113 84 48 55

T. Tales of long ago — 129 100 26 2 15

U. Second fruity computer (2 wds) — 136 61 54 74 87 49 43

V. Andy, Min, Chester and Uncle Bim — 67 106 11 45 22

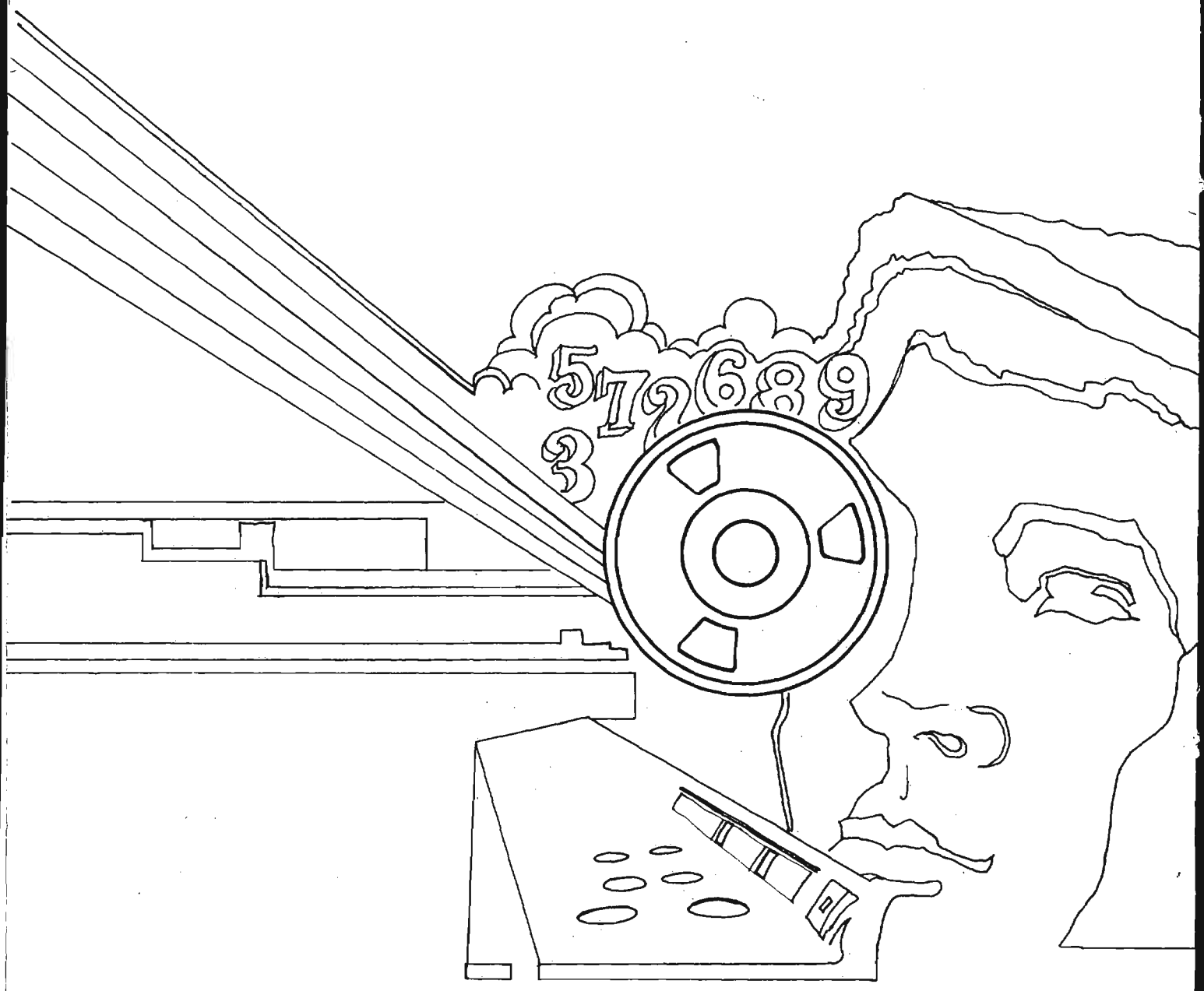
W. HAL + 111 (according to *2001: A Space Odyssey*) — 66 36 29

X. Girl's nickname inscribed in clinic at Hyattsville — 109 12 1 122 6

1 X	2 T	3 D	■	4 B	5 F	6 X	7 L	8 J	9 D	10 E	■	11 V	12 X	13 N
14 M	15 T	16 H	17 J	18 I	19 F	20 K	■	21 G	22 V	■	23 C	24 R	25 I	26 T
27 K	■	28 S	■	29 W	30 F	31 K	32 J	33 M	34 Q	35 L	■	36 W	37 N	38 F
39 L	40 O	41 I	42 B	■	43 U	44 G	■	45 V	46 O	47 B	48 S	49 U	50 A	51 I
52 Q	■	53 C	■	54 U	55 S	56 A	57 F	58 J	59 D	60 N	■	61 U	62 D	63 A
64 E	65 F	66 W	67 V	68 M	■	69 G	■	70 R	71 G	72 O	73 I	74 U	75 C	■
76 N	77 M	78 J	79 G	80 C	81 E	82 H	83 N	84 S	85 R	86 F	■	87 U	88 L	89 A
90 M	91 R	92 F	93 H	■	94 O	95 P	■	96 L	97 G	98 R	99 F	100 T	101 B	102 I
103 D	104 S	105 E	■	106 V	107 P	108 J	109 X	110 Q	111 H	112 R	113 S	114 M	115 D	116 G
117 F	■	118 F	119 C	120 B	■	121 Q	122 X	123 G	■	124 I	125 A	126 R	127 F	128 P
129 T	130 J	■	131 M	132 D	133 I	134 F	135 O	136 U	137 C	138 R	139 E	140 N	141 M	142 J

~~FOR OFFICIAL USE ONLY~~

P1-Oct 83-S3-37033


5
7
9
6
8
9
3

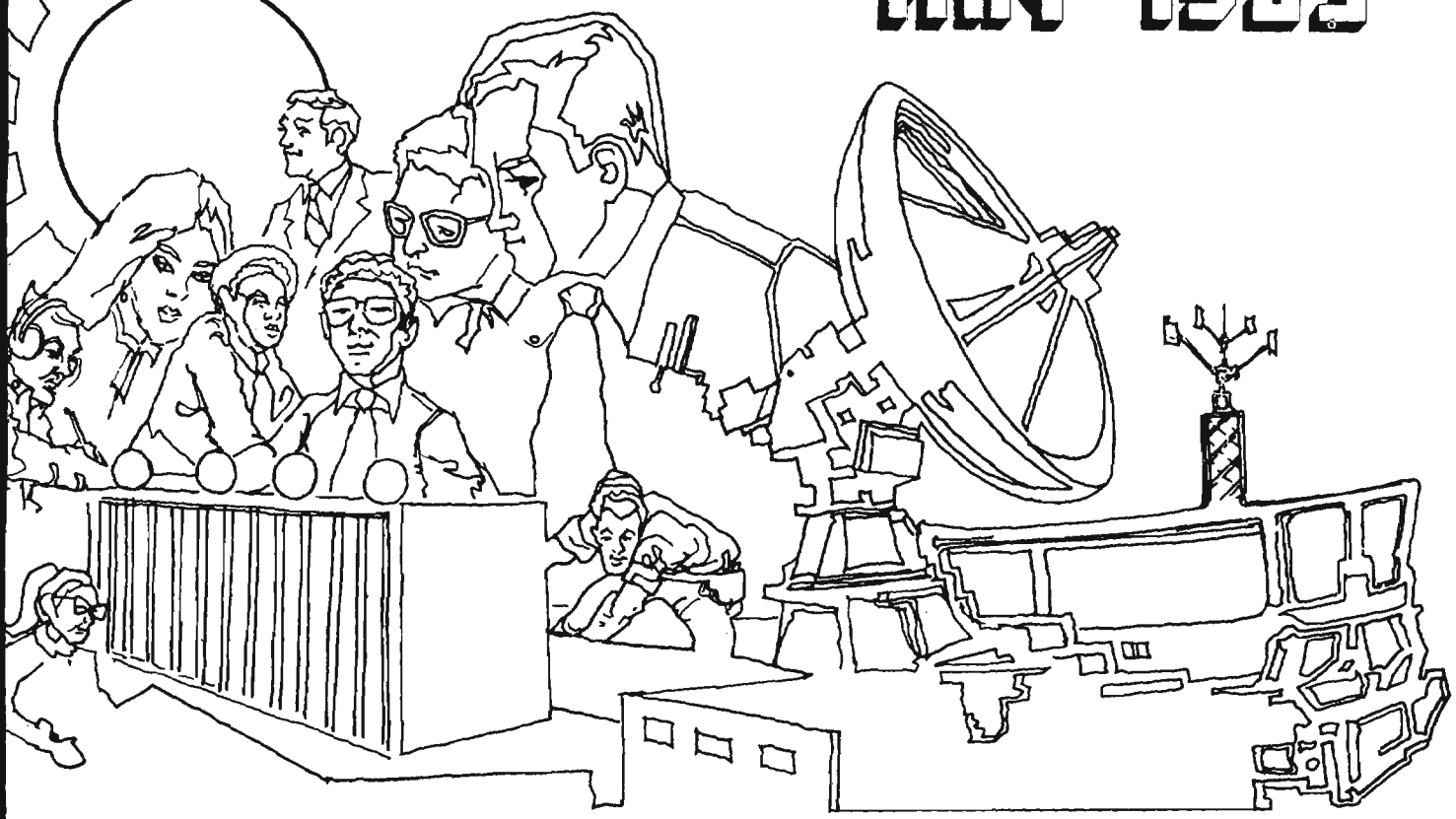
DOCID: 4009861

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MAY 1983



P.L. 86-36

CONFESSIONS OF A BRIEFER (U)..... [redacted] 1
STILL MORE ABOUT PASSWORDS (U)..... [redacted] 5
CRYPTOGRAPHY AT GLOBECOM 82 (U)..... [redacted] 7
REVIEW: DIGITAL TELEPHONY (U)..... [redacted] 11
CUMULATIVE INDEX, PART THREE: KEYWORDS (U).....13
OUT OF MY DEPTH (U).....33
THE INTELLIGENCE WATCH OFFICER (U)..... [redacted] 35
COMPUTERIZING TRAFFIC ANALYSIS (U)..... [redacted] 36
NSA-CROSTIC NO. 47 (U).....David H. Williams.....44

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2
DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case #54778

DOCID: 4009861

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. X, No. 5 MAY 1983

PUBLISHER [redacted]

BOARD OF EDITORS

Editor..... [redacted] (968-8322s)
Asst. Editor... [redacted] (963-1103s)
Production..... [redacted] (963-3369s)

Collection..... [redacted] (963-3961s)
Computer Security
..... [redacted] (968-7313s)
Cryptolinguistics. [redacted] (963-1103s)
Data Systems..... [redacted] (963-4953s)
Information Science
..... [redacted] (963-5711s)
Mathematics..... [redacted] (968-8518s)
Puzzles.....David H. Williams (963-1103s)
Special Research.....Vera R. Filby (968-7119s)

For subscriptions
send name and organization

to: CRYPTOLOG, P1
or call [redacted] 963-3369s

P.L. 86-36

To submit articles or letters
via PLATFORM mail, send to

cryptolg at bar1cØ5
(bar-one-c-zero-five)
(note: no 'O' in 'log')

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

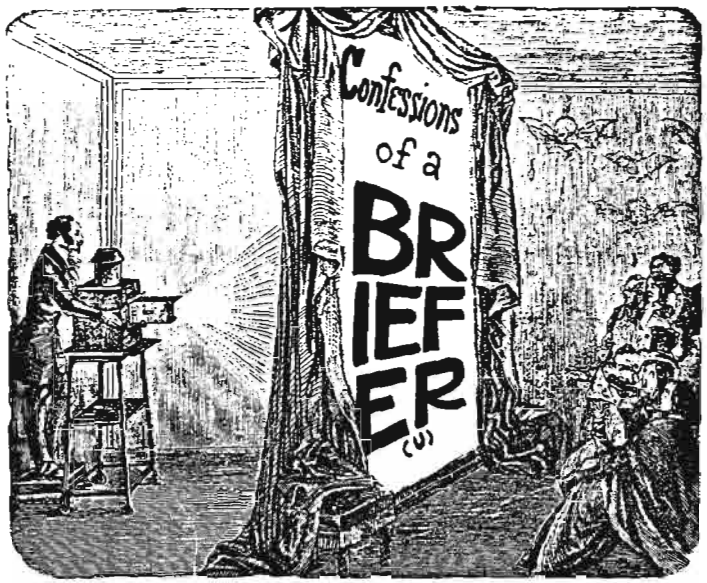
At my bank, having direct mail deposit qualifies me for certain privileges, but when I applied for them, I was told I was NOT a "direct mail depositor." I disagreed; my paycheck is sent directly to them, and has been for some time. Then, I discovered the key: my account is joint with my wife, and the computer lists her name FIRST. So when they retrieve data about MY accounts....

Some years ago, when I dabbled in real estate, I had several fat listing books, and kept them in order by area, price, and number of bedrooms. The listings were typed, and often contained errors. Some were easy to spot. If the tax district or the number of bedrooms was wrong, it was easy to make a pencil change on my copy and move the listing to the right place in the books.

I notice that real estate agents are computerized these days. They go to a terminal, key in a price range, number of bedrooms, geographic area, etc., and out comes a string of listings. Who makes the corrections? I doubt that anyone does. It wouldn't surprise me to hear that some real estate people "hide" new listings, when submitting them to "Multiple List" data bases, by putting typos into key data fields, to give their own agents "the first shot" at a new listing. Between accidental and intentional typos, I wonder how much of the existing data actually gets to the requestor.

Please don't write in and tell me about good programming practices. That's not my point. Both we and our targets are coming to rely more and more upon data retrieval for our information. Anybody who can read and type can call up data on most of these systems, but only the more innovative people will be able to squeeze out of the system the "hidden" data. Knowing how to do this could depend upon understanding how people behave when they use a data base, and also how the data base itself really works. It could, in fact, become a new cryptologic skill field.

DOCID: 4009861



P.L. 86-36

by [redacted] B109

"Wake up, Jim. The briefing's over."

"Huh, what did you say? Oh, I guess I must have drifted off. Sure is hard to stay awake in a dark briefing room after lunch. Say, Fred, did you get copies of that guy's slides for me to read back in the office so I can find out what Project RATTLECAN is all about?"

Does this exchange sound familiar? If not, then this article is not really for you. (Keep on reading though; you might learn something that will be useful later.) But if you are one of those who have been bored to sleep on numerous occasions as some well-meaning project officer or analyst read an endless succession of slides to you, perhaps this article will contain some thoughts that may help you avoid inflicting similar boredom on others. It may even make your briefings more effective.

One of the most basic causes of poor briefings here at NSA (and elsewhere as well, I am sure) is the mistaken view that briefings are a good, concise way to transfer information to people. Absolutely nothing could be further from the truth. Yet we constantly use briefings to "bring people up to speed" on a wide range of detailed and complex topics. The subtle deceit of briefings is particularly interesting when someone has received a "Good brief!" from his audience. Just ask the briefee afterwards how many tanks the Zendian Army has, or how many communications circuits are at Field Station Xapa, or some other detailed question on the topic and most likely you will get some answer like "Well, I don't recall exactly, but I'll call Tommy Talker who briefed me on it and he'll have the answer." In this case Mr. Briefee may not have the facts but he did get the message.

The fallacy of using briefings to bring people "up to speed" is that briefings are not a good medium for the presentation of a lot of objective, factual data. They are, however, an excellent medium for affecting people's attitudes and emotions. In our society we have so thoroughly suppressed our emotions (e.g., "Grown men don't cry") that we would tend to deny that we are even subject to a play on our emotions, especially in some intellectual palace like the National Security Agency. Unfortunately, this leaves us extremely vulnerable to approaches from a nonintellectual angle and the briefer who discovers this vulnerability, either by accident or as an active intellectual discovery, can use this approach to produce consistently "good briefs." This is a fact long known to Madison Avenue and it is equally true here at the Agency.

When you have had a good briefing, what are the things that you most readily recall? In all likelihood it will include items such as the command and presence of the briefer and the quality of the graphics. You will remember the organization that sponsored the briefing and those memories will be of a competent and professional outfit. You will know that the topic briefed is:

[] very grave;

[] requires immediate action by your organization;

[] is in competent hands; or

[] needs more resources in the out years.

But you will not recall specifically why you have those feelings.

All this having been said, then, how can we use this knowledge in building a "good brief"? The most basic step is to decide what emotional message, feeling, or attitude you want to inculcate in the listener. Generally, the attitude or emotion will be one favorable to the topic and organization presenting the brief. For instance, a project officer will generally want to leave listeners impressed with the importance of the project so that future requests for support will be favorably endorsed. In short, although briefings are generally thought of as being informational, most briefings are sales pitches. Once the basic message of the briefing is established, all other work should support that message.

In briefing there is no substitute for the competent briefer, a person who speaks with all the self-assurance of a Nobel Laureate but who at the same time compliments and involves the listeners; one who does not preach to them. For some people these qualities are natural, but for most they can be acquired. The secret is lots of practice and the knowledge that you know more about your topics than your listener.

Armed with this confidence, the briefer should never use a script. If you know what you are talking about, you don't need a script. If you don't know what you're talking about, you shouldn't be briefing. Bishop Fulton Sheen never used any notes on his very successful TV show during the 1950s. When asked about this once, he cited a remark he had heard as a child. An old woman walking out of church was complaining because the bishop had read his sermon from notes. Her question, which impressed Sheen, was "How the devil can he expect us to remember what he's saying when he can't remember it himself?"

Freedom from the script allows the briefer to give the appearance of being extemporaneous as he or she responds to the quips, comments, and questions of the briefee(s). It also permits the briefer to tailor the brief readily to the background and interest of the listener. Finally, the freedom from the script allows the briefer to establish a pace or rhythm for the briefing that enhances the authority and assurance of the presentation.

With the script eliminated, the only tangible form left to the briefing is the graphics. These are as critical as the presence of the briefer and, in fact, can often make the briefer seem more professional and the briefing come across better. In the choice of graphics it is especially important to keep in mind the emotional appeal of the brief. The Chinese writer who said that one picture was worth a thousand words knew what he was talking about, and the proper choice of graphics can save a lot of talk and questions.

For example, consider the graphics in Figures 1 and 2. "Zendian Army Power" (Figure 1) is just a compilation of numbers. The briefee will read it rather than listen to the briefer--and you'd better hope that the briefee doesn't have some spurious knowledge or he might make some comment like "I thought the Zendians had Type Q tanks instead of Type Ys." This sort of question could well be enough to throw an inexperienced briefer off pace or, worse yet, lead to intellectual questioning of every statement.

Figure 1 has has yet another critical flaw: In column 1 the numbers don't add up to the total shown. If the listener notices this, he/she will spend the rest of the briefing adding up any numbers that appear, looking for other errors.

FIGURE 1: ZENDIAN ARMY POWER

	TROOPS	TANKS	HEAVY ARTY	MED ARTY	APC	HELOS
I CORPS	55,000	250	200	500	600	45
*						
III CORPS	58,000	300	212	550	600	43
IV CORPS	61,000	312	220	560	500	48
V CORPS	58,000	270	220	550	550	45
ABN CORPS	25,000	**	---	200	---	350
TOTAL	247,000	1132	632	2360	2250	531

* There are no units in the Zendian Armed Forces with the designator 2 or II because the Zendians consider this number bad luck.

** There are no tanks per se in the Airborne Corps but there are approximately 200 of the so-called "Y-type tanks" that are in reality a lightweight high-speed tracked anti-tank gun.

OCID: 4009861

Figure 2

Figure 3

DOCID: 4009861

Figures 2 and 3 (previous page) are good examples of effective graphics. Both of them evoke a strong emotional response. In fact, either of these pictures could well move the listener to a rendition of war stories about when he/she drove tanks, rode in helicopters, or had some related experience. This will imbue feelings of camaraderie between the briefer and briefee that will make the briefee much more amenable to the briefer's message.

These two pictures have some other practical advantages:

[] they will serve to cue the briefer;

[] they will not limit the remarks the briefer may wish to make

[] they don't contain the intellectual snags that are found in Figure 1; and

[] perhaps best of all, they will not have to be changed or updated unless the Zendians get rid of that tank or helicopter.

(When using slides like this, however, make certain that it is really a picture of what you say it is or it will be almost as bad as having numbers that don't add up.)

By concentrating on influencing emotions or feelings, we do not ignore the facts. We just use them in a different manner. Rather than being sort of inert things, the facts that we have to use are woven into the fabric of the brief in a way that supports the basic message. One way to do this is with "amazing facts." We all have a store of "amazing facts" but probably don't realize it. For example, the fact that the Zendian Navy has 89 operational submarines will probably mean very little to anyone but an avid naval buff, but the same fact cast in a different context becomes an "amazing fact": "The Zendian Navy has the largest submarine force in the third world!" Bar, pie, and line charts are all effective ways of presenting amazing facts such as this.

While you never want to read your slides to your listeners, there are times when you may want to let your listeners read the slides themselves. This provides a change of pace for both briefer and briefee. It's a quick way to slip over what otherwise may be a long narrative and it involves the briefee in the briefing process more actively. Such graphics should never be long textual passages. The proper form is short "bullets," ideally only one or two words each. (See Figure 4.)

UNITARY PLANNING
I&W EMPHASIS
SURVIVABLE COMMUNICATIONS
COMPUTER INTEROPERABILITY
PRODUCTION ENHANCEMENT
COMBINED WORKFORCE

Figure 4

The briefer can introduce this type of graphic with some line such as "These are the characteristics of ..." (whatever the subject is). The briefer should watch the faces of his audience and move on to the next graphic as soon as the the expressions of the listeners show that they have read the graphic.

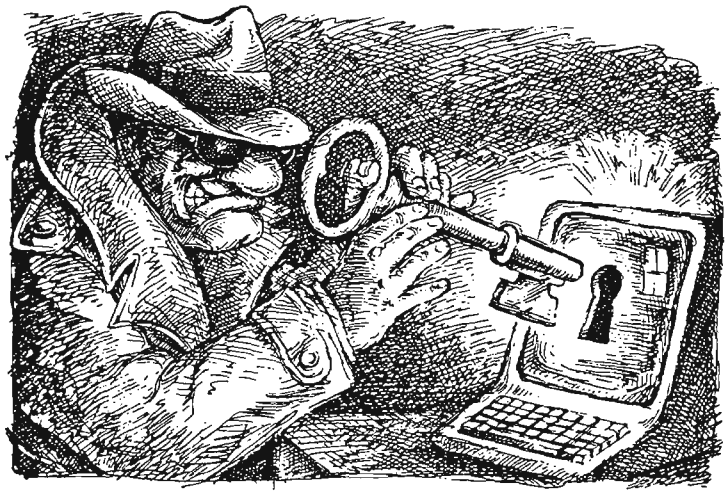
In summary, the key to effective briefing is to remember that briefings should be used to form attitudes or affect emotions, not only to transfer objective facts. The effective brief should have one central underlying attitudinal or emotional message that it is attempting to deliver and all aspects of the briefing must support this. The briefer should not use a script and the graphics should be simple and chosen with an eye to their emotional impact. Facts used in the briefing are much more effective when placed in some sort of comparative context. Slides to be read should be read by the briefee not the briefer.

Good luck! Good brief!

"Epilogue"

In closing, I believe it is necessary to comment on the ethics of briefing. It is evident that, armed with information about the weakness of our psyche, an unprincipled bureaucrat can take considerable advantage of his or her colleagues. At present the only sure counter to this is the individual integrity of the briefing organization which must use its power only for pure motives. Unfortunately, a full discussion of the ethics of briefing is beyond the scope of this article, but perhaps some reader may feel an urge to expand on that topic.

STILL MORE ABOUT PASSWORDS (U)



[redacted] P13

P.L. 86-36

A USER VIEWPOINT

The password controversy continues. On the one hand, [redacted] and others have stressed the need for greater security to avoid potential compromise. On the other hand, [redacted] and others have made a strong case for short, easy-to-type and memorable passwords to avoid needless errors and frustration on the part of the user. I am in sympathy with both causes, although I violently object to [redacted] closing paragraph (CRYPTOLOG, Mar 83, p. 38): he states that an easily remembered password is easy to type regardless of length, and that he doubts that a non-typist (i.e., one who does NOT find a long, memorable password easy to type) will use a terminal for very long. I would argue just the opposite. The probability of error rises progressively with each additional character added to the password, especially since characters are not being echoed on the screen. Also, my personal observation has been that the majority of non-secretarial users--linguists, programmers, and managers among them--are in fact either non-typists or poor-to-fair typists, myself included; yet terminal usage among these groups is increasing rather than decreasing, as more and more people become aware of the advantages which a computer terminal can provide to the professional user.

Having said this, let me state that I think the problem is easily solvable in a manner which should satisfy both viewpoints. Instead of viewing the problem theoretically--short passwords are good, but breakable; large alphabets, pass phrases, and "passcodes" are good, but will result in higher error rates--we should take the Agency environment into account. Many Agency computer systems have a feature which automatically "kicks out" anyone who unsuccessfully tries a user ID-password combination three or four times in a row. Those which do not can be easily modified to allow this capability. If the office security manager is alerted to terminals on which three unsuccessful ID-password combinations have been tried, I doubt very much that a hostile entity would have any success in breaking even a five- or six-letter, single-case, mnemonic password before being apprehended. At the same time, a poor typist gets several chances at entering the combination correctly before setting off the alarm. This system thus provides the best of both worlds: a user-friendly password environment which is, for all intents and purposes, immune to exploitation.

[redacted]

P.S. A challenge to all UNIX users: how many of you can type "Low flying bees eat wax beans" (to use [redacted] example of a pass phrase) and get it right the first time? It's easy to find out: set terminal type to STTY -ECHO ; type in the phrase enclosed in single quotes, i.e., 'Low flying bees eat wax beans' and hit <RETURN>. A system message will appear as follows:

flying bees eat wax beans: not found
(or whatever you REALLY typed)

After you're done experimenting, STTY ECHO will make your characters visible again. (At an informal testing in the KEPLER laboratory, I got the phrase right 3 out of 7 times; however, I fall under the "non-typist" category.)

THREE GOOFS AND YOU'RE OUT

On [the system I use], a user signs on with user initials and then is required to type in a password. If the person "fails," they may try again and again and again.... To prevent exhaustive searches, why not flag to the systems operator any console that tries say three times? Or lock that terminal out?

[redacted] P.L. 86-

DOCID: 4009861

PASSWORDS: FRIEND OR FOE?

Speaking of passwords, what is an acceptable balance between security and convenience? I have found what I believe to be a rather comfortable and simple solution (but then I'm sure SOMEONE will disagree). I simply choose a word...such as walnut, then alter or mispell it (walllnut, wawlnut...etc.). Not enough to make it difficult to remember, but definitely making it more secure and harder to guess.

[redacted] P.L. 86-3

MORE ON PASSWORDS AND HUMAN FACTORS
(from COMPSECNEWS, June 1983)

One of the frequently heard complaints from persons who changed to more clever passwords containing special symbols or mixtures of upper and lower case, was that when bringing some of the terminals up cold, and prior to loading the terminal emulator, they could not login. True that each keycap may not send the same character before an emulator load as it will after, but when those infrequent occasions arise, you can still prpbably login if you only knew what keys to press. For example, one system I know of uses the "back tab" key to produce the "/" prior to emulator load. Obviously an inconvenience, but most users do not regularly have to perform initial terminal loads.

Other systems that I have seen have accounts called "LOAD." These accounts do not require the person who logs in to enter a password, only to choose a desired emulator. After the selected emulator is loaded, the real user login is then required. If your system does not have this feature, complain to the system Guru. Incidentally, notice that an emulator load is all that the "LOAD" account can do.

Another comment had to do with the login-id being secret. The suggestion centered around doing away with initials as the login-id, and using a secret account name in addition to a secret password. Maybe a useful idea, but one point missed by this comment was that the current login algorithm used on most of the systems does not reveal what is wrong when the login fails. For example, notice of login failure only appears after the id and the password has already been given. Another problem with this suggestion is we already have a requirement to identify individual use of sensitive computers. Work is currently underway to assign each and every user of our computer systems a unique id that will be the same regardless of which computer system is used. The adopted format will follow first two initials followed by the first five letters of the last name. A central registry is being established to resolve conflicts.

[redacted] (June 1983) P.L. 86-3

Keep your comments coming! In particular, I would like to see more comments from users about the consequences for them of various access restrictions, password procedures, etc. How have some practices on the systems YOU use hindered or helped YOU in your work? I know that it is fun for a lot of you ingenious people out there to think up new password schemes and gimmicks, but the computer security experts are pretty inventive and ingenious too. What they need, more than new techniques and ideas, is some clear feedback from users about the COSTS and BENEFITS of different kinds of procedures currently in use. If they get a clear indication from users that certain methods of implementing access restrictions impose a relatively high cost on users, they will be motivated to use their ingenuity to find other and better methods that are just as secure but less costly to the user. I was interested to note, in the COMPSECNEWS item above, the assumptions that

1) users rarely had to load terminals "cold"; and
2) coping with keys that send different characters before and after emulator loading constituted a minor inconvenience at most.

What do you think about those assumptions?

As a hunt-and-peck typist, I find odd-ball special characters are a MAJOR stumbling block, even when the keycaps agree with the character that gets sent. Even the shift key and "CTRL" key are frequent error-makers for me. Also, my impression is that users have to down-line-load Delta Data terminals more frequently, at least for some systems, than the COMPSECNEWS editor assumes. In fact, if I had to cope with that problem, even having to load a terminal once a week would be far too often for me! The "LOAD" account mentioned in the article seems to me a much more promising and user-friendly approach than "if you only knew which key to press."

For a programmer, or someone thoroughly familiar with the terminal and software, perhaps keys that send different odd-ball sets of characters at different times may present only a minor annoyance; in fact, computer folk seem to thrive on and positively welcome such problems. Most others, however, are very unlikely to agree with them. Computer specialists, and computer security specialists in particular, need to be reminded that situations constituting brief nuisances or even amusing challenges for them can be stressful and exasperating for other kinds of users.

-M.E.D.

DOCID: 4009861

LOOKING AROUND with

Cryptography at GLOBECOM 82

P.L. 86-36

Review:

Digital Telephony (U)

A DES-type algorithm, using 800-bit vectors in place of the 48-bit vectors of DES, was proposed at GLOBECOM 82 (the 1982 Global Communications Conference) for the encipherment of medical records. The key would be 160,900-bits long. The Belgian author of the paper, Desmedt, claimed that this would protect medical records during the life of the person concerned. In reply to a question, he admitted that he did not know how to keep the 160,900-bit key itself secure and intact for the 100-year period.

(U)

(U) The Desmedt paper on super-DES was one of five papers on cryptography presented at GLOBECOM 82 in December. In addition, there were five other sessions on coding, primarily speech coding, which proposed reducing bit rates for video and voice and facsimile. Compression techniques and the ability to recover from channel errors are critical to the use of digital encryption techniques.

(U) One of the surprising papers was about a detailed experiment with analog encryption at Bell Labs. Apparently low bit rate encryption causes so much loss of voice quality, especially over low-quality lines which cannot support 9600-bps rates, that there is a growing demand for encryption which sends analog waveforms. The Bell Labs work has been done by computer processing, but they expect to develop a real-time circuit, after which their VLSI chip designers will examine the cost of single-chip analog encryption. That could have a revolutionary effect on secure voice and on cryptanalytic priorities.

(U) Two other surprises were the sophisticated insight into the strengths and weaknesses of various public key schemes, especially the flaws of the Hellmann-Merkle algorithm, and the importance of the recent Racal-Milgo patent on finding large primes for the RSA public key algorithm. Several speakers stated that the RACAL-MILGO algorithm had made the integration of DES and the RSA algorithm feasible as the basis of a switched ad hoc public cryptographic network.

(U) This demonstrated interest in the feasibility of the RSA algorithm as a means of keying DES links is more interesting in the light of the Inman interview (Science, Dec 82), which identified RSA as a secure method.

(U) The leadoff paper by J. Michael Nye, a self-styled cryptographic "expert," described the methods and cost of intercepting telecommunications in the US and gave a list of 26 domestic cryptographic suppliers offering 104 products and 13 foreign vendors offering 81 products in the US market. The list of suppliers and products is growing, and the impact of Personal Computer encryption is yet to be felt. This is a very big change from ten years ago, when only a few companies supplied cipher equipment to the US market. Most of the products are for fixed telephone service, but as the new technology of cellular radio develops over the next decade, the market for voice encryption, to protect the 900-MHz mobile circuits from interception will increase to millions of vehicle radios.

(U) Cox, Jayant, and McDermott of Bell Labs gave a paper on a time-frequency segment permutation analog encryption which they believe is very secure against cryptanalytic attack, without loss of voice quality or syllable intelligibility. The delay for the scrambling and descrambling is no more than 256 to 512 milliseconds for 16-msec speech segments. Each 16-msec segment, sampled at 8000 Hz to give 128 samples, is converted to sub-bands by digital filtering, and the sub-band vectors are then permuted. The digital vectors are stored in a buffer with a memory capacity up to 512 msec. A cryptographic keystream decides on the segment permutation, and also decides which time segment will be sent. Any time segment can be delayed up to 256 msec. The input test data were voiced digits in random order, used to avoid the redundancies of normal conversational speech.

(U) The cryptographic scheme is to fill the buffer with 16-msec segments, then send all of them in some pseudorandom order until the buffer is transferred to the receiving end. Then the buffer is refilled and the scrambling and transmission begin on the next multi-segment block of speech. It is not clear from the published paper whether the segment transposition key is the same or changes from block to block.

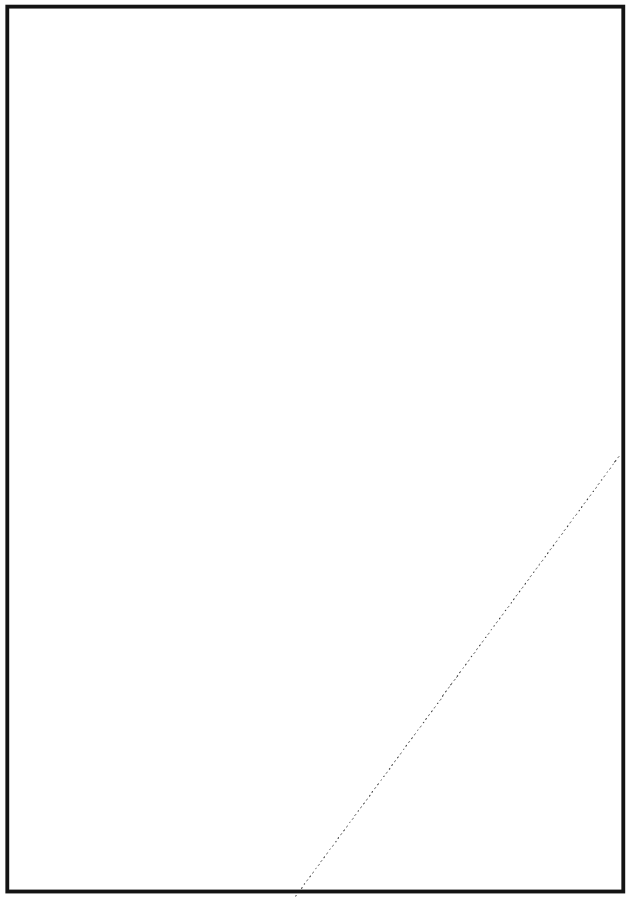
(U) The scrambler was implemented on the BTL Digital Signal Processor, and tests showed that it gave better intelligibility than simple frequency inversion scrambling. The scrambled signal envelope sounds like "birds chirping." To maintain synchronization, a series of pulses is sent down the channel whenever the scrambling buffer is reinitialized, and these high pitched pulses send like "cricket chirps" interleaved with the signal.

(U) Although the system is described as an "analog" scrambler, it is clearly a 5-stage analog-digital process, in which most of the processing at each end is digital, but the transmitted signal is an analog waveform. It has been tested over the Murray Hill phone system, with addition of simulated white noise and phase roll (a channel impairment).

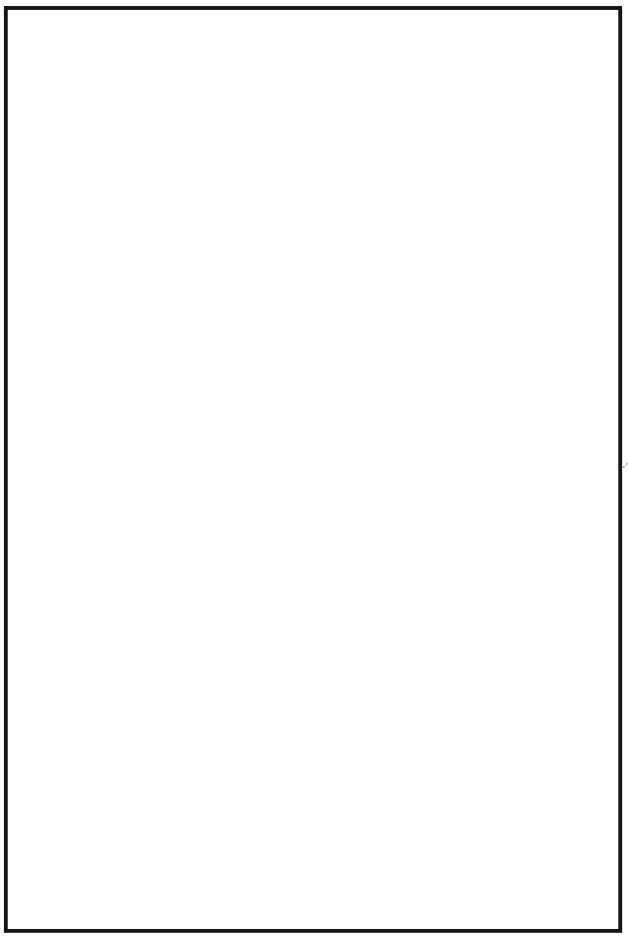
(U) Because sample-to-sample fidelity is important to speech reconstruction, i.e., the sampled speech at the receiver must match the samples that are supplied to the digital-to-analog (D/A) converter at the transmitter, it is necessary to equalize the channel to compensate for channel distortions and to synchronize the instants of sampling at each end. The synchronization pulses (cricket chirps) are used to establish and maintain sample timing and are also used for channel equalization (since they give the impulse response of the channel).

(U) The main thrust of the designers' work was to get good intelligibility. They now want to reduce the software algorithm to a hardware device, and VLSI design can follow from there. The audience showed substantial interest in this scheme.

(U) Despite the rapid introduction of digital channels, for many years to come, most of the world's telephone connections will be made over copper circuits that will not support high bit rate digital speech. One of the driving forces behind the development of digital transmission and local loops is the desire for high-quality secure speech. If the hybrid analog-digital scrambling gives good enough speech quality, and no particular security weaknesses become known, the market pressure to develop digital services to the 64,000-bps level IDN (= Integrated Digital Network) may reduce (since customers won't have to buy them) and this could affect an important part of the digitization of the telephone network.



EO 1.4.(c)
P.L. 86-36

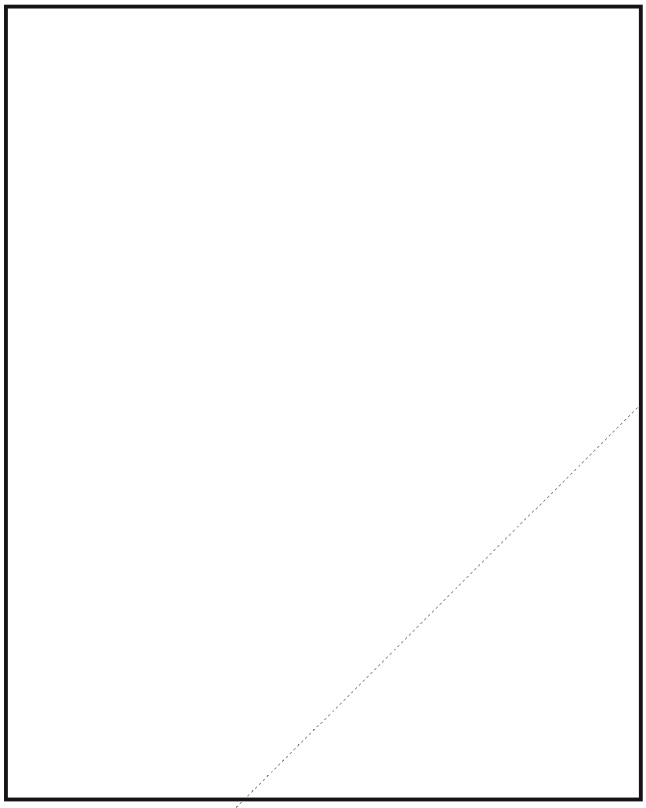


(U) The Desmedt paper on Super-DES began with a critique of existing cryptographic methods, interleaved with some familiar commentary on NSA intervention in the DES design. A point of interest is the statement that the Geneva Management Group in 1981 concluded that DES was not adequately secure. Desmedt argues that encryption algorithms that iterate the basic operations many times provide higher security than the individual operations (e.g., substitution, transposition) but are impractical to implement on VLSI chips. He also argues that a DES-breaking special machine may be costly today, but in 20 years could be cheap enough to break messages enciphered on DES now. He also acknowledges that no "shortcut" solution to DES is known. Hellmann's insinuation that a "trapdoor" was built into DES by NSA is referred to. The problem of public key algorithms such as the Merkle-Hellmann scheme is described as either they have known weaknesses or they may have unknown weaknesses. What is notable about all of this critique is that the authors are professors of mathematics in Belgium and they are very up-to-date in the state of cryptology in the public domain. (One of them spent 1978-79 at UCLA, Berkeley, doing pertinent research.)

This is undoubtedly a reflection of the rapid transborder flow of technical information between academicians and the arrival of increasingly capable people into the arena of public cryptology. Without doubt, the technical quality of the work will increase and will threaten SIGINT.

EO 1.4.(c)
P.L. 86-36

(U) The particular cryptographic scheme that Desmedt et al propose is a version of DES in which blocks of data of 1,600 bits are enciphered, under the control of a 160,900-bit key. The S-boxes of DES are replaced by one-way knapsack functions. This revised "S box," instead of operating on eight bits, operates on 200 bits, and there are eight of them operating in parallel. Each of the new "S boxes" is initialized with 100 integers of 20 bits, so that it contains 20,000 bits. There are eight "S Boxes," which use up 160,000 bits of the key. Because of the trapdoor function, even if the 160,000 bits were known and all the S-box outputs were known, it would still be very difficult to compute the 800-bit input. However, the 160,000-bit key is not known. It is kept secret. That makes it even harder to compute the input from the output. The 200-bit outputs are expanded up to 208 bits and then hashed down to 100 bits to give the 800-bit output. This complicated process is iterated a number of times. A stream or block mode with this algorithm is possible.



EO 1.4.(c)
P.L. 86-36

(U) Yiu and Peterson of Hewlett-Packard gave a paper on a single-chip VLSI Public Key algorithm. The algorithm is Hellmann's discrete exponential scheme using Galois Field arithmetic. The chip has 12,000 transistors and is designed for a 4-MHz clock rate. The Public Key algorithm would be used in conjunction with DES, to distribute keys for the DES algorithm. The purpose of the chip design was to give higher speed and lower cost for encryption. The use of Galois Field arithmetic eliminates the need for carry or borrow operations, and the arithmetic operations can be executed by linear feedback shift registers. The developers expect to use the chip in a computer network, but the company, according to Yiu, has no commitment to market it.

(U) Doctor Yiu mentioned the recent Racal Milgo patent for finding large prime numbers in a few seconds as an important breakthrough in implementing Public Key networks. The patent, No. 4,351,982, claims that it reduces microprocessor computation time to find a set of 200-bit primes from 1,200 hours to two hours. Desmedt stated in his talk that the RACAL MILGO datacryptor took only 17 seconds to distribute key (but it was not clear that it would find RSA primes in that short time). Hollander of BTL (Bell Telephone Labs) has a patent application that purports to find large primes very quickly. The Japanese are developing a chip that will do RSA encryption at 50,000 bps. The work is a joint project of NTT, NEC, Hitachi, Fujitsu, and Oki. Sandia has developed an algorithm that will do multiplication modulo C in $\log2(C) + 7$ clock pulses, which is an improvement over the conventional modular multiplication, which takes N x N clock pulses for an N-bit modulus. The Sandia method would take only N + 7 clock pulses. It is aimed at RSA encryption using 512-bit prime numbers. At 20-MHz clock speed they expect to be able to encrypt at 25 Kbp/s. Now that the RSA Public Key algorithm has been publicly identified by a former NSA Director as secure, there will undoubtedly be intensified work to make it easier to use to set up DES links. The high utility of being able to dial up any other party and set up a secure link, without prior key distribution, is irresistible from both intellectual and marketing viewpoints.

(U) A paper on the AMD DES chip was given by Brown, an AMD executive. This was followed by some discussion of the merits of DES. Both Yiu and Brown felt that DES was in fact secure, and that the criticism that Desmedt and other authors had raised were not supported by any facts. No one had been able to read or exploit DES, and it had the advantage of a standardized tested algorithm. The AMD DES chip was capable of 1.7 Mbytes/sec, so that it could be used for disc controllers. It cost $75 for a single unit.

(U) Another paper at the cryptographic meeting was an Italian scheme by CSELT for a "robust" 4800-bps speech coder. Audio tapes showed it to be resonant and of low quality. The paper did not seem to offer any important new work. However, the topic of speech coding and other compression coding was treated at five other sessions. There were 31 papers on voice and image compression, of which 16 were by foreign authors. The sessions were:

[] A8 : Low bit rate speech coding

[] B6 : Image processing

[] D4 : European videoconferencing

[] E6 : Advances in speech coding

[] F7 : Speech processing

(U) The interest in compressed speech in sessions A8, E6, and F7 was initially to allow narrowband encrypted voice signals. Now a number of other applications, including low-cost bandwidth conservation and interim storage of voice, have emerged from the capability to compress speech.

(U) The interest in compressed video is for both teleconferences and private TV broadcasts (e.g., Pay-TV, TV relay by satellite, and Direct Broadcast Satellites (DBS)). The common carriers and the broadcasters both see commercial advantages in being able to send TV signals that can be securely encrypted. Because bits/sec cost money, the customers want the pictures compressed.

(U) In Europe there is a multinational effort to develop a standardized videoconference system, with a standard video coder. Some of this is for satellite applications, to thwart interception, but most of it will

probably pass overland on radio relay and optical fibers. The compression allows cheaper conferences and security, and the standardization will allow the Europeans to intercommunicate and keep US companies out of the equipment market.

(U) There are now hundreds of papers published on vocoders, fax coders, encryption, video coding, etc. Many of the papers are foreign, but the Europeans in particular have been handicapped in the speech area, for example, by the lack of specialized journals which consolidate the work. As as result, they look to the US journals, especially the IEEE publications, as the focus of the current work. This also makes it difficult for US parties to keep up with the foreign work because it is spread across a number of journals and is often published in German, French, Italian, Swedish, Japanese, etc. However, the foreign literature is growing, and will become a more important source of new work in cryptography and coding.

(U) The Europeans, arriving on the scene after the US has identified the problems and paid for the basic research, will be able to converge on coding and encryption standards to serve many of their PTT plans, without the competition, confusion, public controversy, and divided purposes that have arisen in the US in both Government and civil coding and encryption. By the end of the decade, they may have passed the US in these fields, just as they have surpassed the US in a number of other selected technologies and industries.

References:

1. GLOBECOM 82 Conference Record

2. US Patent 4,351,982 (RACAL MILGO)

3. E.F. Brickell, A Fast Modular Algorithm with Application to Two Key Cryptography, Sandia National Labs. Re DE-AC04-76DP00789

4. Simmons, G., and M. Norris, How to Cipher Faster Using Redundant Number Systems, Sandia National Laboratories, Aug 1980.

5. Miyaguchi, A., S. Mizuta, K. Furuie, T. Tsujiguchi, and H. Mizuta, Combination Type Computer Circuits for Code Handling, NEC, 1981.

6. NTIS Search Vocoders, V1,2, 1982.

7. Inman, Bobby, Science, V218, 24 Dec 1982, p. 1290.

8. NTIS PB-806860 Vocoders 1970-82, abstracts from the Engineering Index. Apr 82. Contains foreign vocoder abstracts. (In P1 library)

9. NTIS PB-82-806852, Apr 82. Vocoders. Citations from NTIS data base. US literature (In P1 library)

10. NTIS PB 82-863671, Mar 82, Facsimile Communications, Citations from INSPEC data base. (Contains many foreign literature references)

Digital Telephony
by John C. Bellamy, Wiley, 1982.

~~(C)~~ Is "plesiochronous"a familiar word? It soon will be, if you are concerned with international digital networks. A plesiochronous network does not synchronize the network, but merely uses clocks at each node that are accurate enough to keep the bit slip rate low enough not to interfere with operation. The US domestic digital network is synchronized, to save the cost of the node clocks, but the CCITT has established clock standards to interface different national networks by plesiochronous gateway connections. Because the national networks run at slightly different rates, [redacted] and COMSEC will have to anticipate this plesiochronous structure.

EO 1.4.(c)
P.L. 86-36

(U) Network synchronization schemes are just one small part of John Bellamy's new book on digital telephony. The author, who received his PhD in EE in 1971, worked as a manager at the Collins Division of Rockwell International in transmission systems, then as a member of the technical staff at Arthur A. Collins, Inc., the R&D firm that hived off from Collins Radio when Rockwell took them over. He is now an R&D manager at the Communications System Division of United Technologies, so he has substantial practical experience with modern telecommunications engineering. It is notable that Collins builds digital radio equipment so well that Western Electric dropped some of its own projects and buys from them. In addition to his industry experience, Dr. Bellamy has been an Adjunct Professor of Electrical Engineering and Computer Science at Southern Methodist University since 1976, so he is used to

organizing, simplifying, and teaching engineering technology.

(U) His book is a well-written tutorial on telephony and digital telecommunication. Although digital transmission was developed with computer and data traffic in mind, the main traffic volume will be voice for a long time. Analog transmission and networks will also be around for a long time, but digital telephony is of particular interest where encryption is wanted (as he says on page 75) because of the paucity of good analog encryption.

(U) The book covers digital networks from a general overview of the analog network in the US, through voice digitization algorithms (PCM, DPCM, APC, vocoders, etc), fundamentals of digital transmission, switching and multiplexing, through digital modulation, network synchronization and control, to high-level descriptions of several digital networks and a discussion of the future of digital telephony. Among other things, the book has a 16-page glossary of pertinent terms, such as burst isochronous, Centrex service, despotic network, elastic store, HDB3 code, justification ratio, mesochronous, muldem, permanent virtual circuit, plesiochronous, robbed digit signaling, state store, transhybrid loss, traveling class mark, and waiting time jitter. These terms are indispensable refinements in educated discussions of networks. (This glossary will soon be in the NSA terminology base).

(U) Some points of interest in the book:

[] One of the principal difficulties in making the large telephone network operate is the variety of signals and signaling functions, all of which have to be translated by interfaces or made compatible.

[] Common Channel signaling in the Bell System is highly centralized, making the entire network vulnerable to failures in the CCIS packet traffic.

[] If a CCIS node fails to store and forward certain network information correctly, the network will gradually lock up because disconnects do not occur automatically.

[] Digital microwave radio is cheaper than T-carrier for distances as short as eight miles, and the major impetus for digital radio has been the introduction of digital switches, not the demand for digital traffic, which can pass over the analog network.

[] Fifteen different types of digital central office switches are in service in the US, and more are expected as foreign suppliers enter the US market. The disadvantages of digital networks are increased bandwidth, A/D and D/A conversion, time synchronization, topologically restricted multiplexing, and incompatibility with the large analog plant.

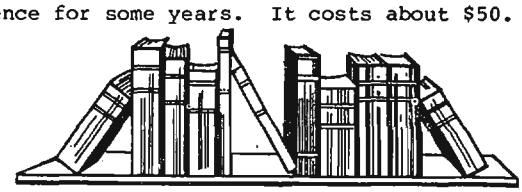
[] Voice digitization, nominally 64,000 bps, can be as great as 400,000 bps for specialized services such as broadcast transmission.

[] About ten different speech coding schemes are described.

(U) In the chapter on digital switching, the advantage of time-domain switching is shown to be the ease of getting switches that don't suffer from blocking. There is quite a lot of information in the switching chapter. The chapter on network synchronization examines many of the timing problems and the solutions such as bit slips, elastic stores, pulse stuffing, and packetization. The chapter on digital networks leads from ARPANET to the ISDN (integrated services digital networks). Circuit-switched nets are shown to be more efficient for voice transmission than packet-switched nets, but digital speech interpolation can increase the effective number of channels on a trunk if the circuit switching is fast enough. Current circuit switching can operate fast enough so that even the beginnings of syllables are not lost. The final chapter is on traffic analysis, as the traffic engineers and designers do it.

(U) The book is well written and well illustrated, with references and exercises. Because of the integration of transmission and encryption, as well as the continuous growth and switchover into digital networks in every country, a knowledge of the engineering and technology of digital networks will be an essential part of a cryptologic repertoire. Bellamy's book is a good beginning to this knowledge. The enciphered speech cryptanalytic experts in R52 ordered desk copies after reviewing the book.

(U) Summing up, Digital Telephony is timely, gives good coverage of digital networks, and should be a useful text and reference for some years. It costs about $50.



DOCID: 4009861

CUMULATIVE INDEX (U)

EO 1.4.(c)
P.L. 86-36

Part Three: Keywords

The following cumulative index of CRYPTOLOG (Vols. I through IX, 1974-1982) was produced using UNIX/PINSETTER tools on MYCROFT and BARDOLPH1. The index is in three parts, and is being published in three successive issues. Part one is an index by author; part two is an index by title; and part three is an index by keyword. Items in multiple issues (February-March 1975, for example) are indicated by the first month (i.e., by Feb 75).

AAAS
Feb 82 Gayler - AAAS, 1982; [redacted]
Feb 82 Software - AAAS, 1982; [redacted]

ABNER
Aug 77 Early Days in NSA Computing; Chauvenet L.R.
Nov 77 Letter: [redacted] Article; Snyder S.S.
Jun 78 Equipment Maintenance on ABNER; [redacted]

Acronyms
Apr 80 OH, K!; [redacted]

Africa
Nov 77 How Many African Countries Can You Spot?; [redacted]

Afrikaans
Sep 74 Language in the News; [redacted]

AG-22/IATS
Mar 76 Musings About the AG-22/IATS; Phillips C.J.
May 76 What's Wrong with AG-22/IATS?; [redacted] D.R.
Jun 76 Comments on AG-22/IATS; [redacted]
Jun 76 Comments on AG-22/IATS;
Jun 76 Comments on AG-22/IATS;
Jun 76 Comments on AG-22/IATS;
Jun 76 Comments on AG-22/IATS;
Jun 76 Comments on AG-22/IATS;
Jun 76 Comments on AG-22/IATS;
Jun 76 Comments on AG-22/IATS;
Sep 76 More Comments on the AG-22/IATS: [redacted] B.
Oct 76 Another Word on AG-22/IATS; [redacted] M.A.
Apr 77 The Last Word on IATS?; Phillips C.J.
Jun 77 AG-22/IATS: A View From the Bridge; [redacted]
Sep 77 Another Last Word on IATS; [redacted] P.A.
Oct 77 Letter: AG-22 Page Print; 'Reader'

American Magic
Apr 82 Review: The American Magic; [redacted]

Amerind
Sep 74 Language in the News; [redacted]

AOC News
May 82 Is There An Old Crow In Your Future?; [redacted]

Appraisal System
Nov 78 Letter: Appraisal System: 'Anon.'
Nov 78 Letter: Appraisal System; [redacted]

Arabic
Sep 74 Language in the News; [redacted]
Dec 74 Language in the News;
Apr 75 Language in the News; Tetrault E.W. [redacted]
Sep 74 COMINT Analysis of [redacted]
Dec 74 Letter: [redacted] Article; 'Anon.'

Archives
Jun 78 Never Again!: Gurin J.
Nov 78 Never on My Watch; [redacted]

Arms Control
Feb 82 Gayler - AAAS, 1982; [redacted]

Artificial Intelligence
May 77 Another Controversial Book on Artificial Intelligence: [redacted]
Sep 77 The Doctor Is In(capable of Diagnosing); Chauvenet L.R.

Asia
Aug 76 Integrated Analysts for Asia; [redacted] W.D.

Ask Art
Apr 79 Letter: Ask Art; 'Sue'

Assignments
Jan 80 Coming Home; [redacted]

Automation
Oct 75 Automation of a TA Process; Murphy T.
Sep 77 [redacted] D.L.

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Awards
Aug 74 Learned Organizations--1974 CLA Essay Contest, 1974 CMI Essay Contest; CISI Prizes and Honors, Spring 74;
Jan 76 Lenin and State Prizes: Now You See Them, Now You Don't!; [redacted]
Jan 78 Thanks for the Attaboy!; [redacted]
Apr 78 Prizewinners in Three Holes;
Jan 80 CLA News: Sydney Jaffe Award;
Sep 82 Letter: Kudos; [redacted]

Blue Russian
Nov 75 Golden Oldie: Blue Russian; [redacted] J.F.

Bookbreakers
Sep 74 Cryptanalysis and Code Recovery; Mountjoy M.
Apr 75 Letter: Professionalization of Bookbreakers; [redacted]
May 75 Letter: [redacted] Letter; [redacted]
May 75 Letter: [redacted] Letter;
Jun 75 Letter: Bookbreakers; Professionalization of Country Specialists; [redacted]
Jun 75 Letter: Myers Letter; 'Anon.'
May 76 Conversation With a Bookbreaker; 'Anon.'
Mar 77 [redacted]
Jul 77 Bookbreakers Forum; [redacted]
Jul 77 [redacted] Buck S.H.
Jan 78 New and Improved Aid for Bookbreaking; [redacted]
Jun 78 Bookbreakers Forum; [redacted]
Nov 78 Linguistics and the Code Reconstructor; Buck S.H.
Apr 79 Bookbreakers Forum;
Apr 80 ... And In A More Modern Vein; [redacted] V.
Apr 82 Bookbreakers Forum On Machine Aids; [redacted]

Book Review
Feb 75 Review of 'Guide to Russian Technical Translation' by Salemme; [redacted]
Jun 75 The Navajo Code Talkers;
Dec 75 A Personal Comment on Winterbotham's 'The ULTRA Secret': Tiltman J.H.
May 77 Another Controversial Book on Artificial Intelligence; [redacted]
Jan 78 'Bodyguard of Lies' (Book Review); McConnell H.
Jan 78 'The Man Who Broke Purple' (Book Review); Filby P.W.
Oct 78 Feeding the Germans Misinformation (Book Review); Filby P.W.
Nov 81 Review: What Do You Think?; [redacted] M.E.
Dec 81 Review: In The Name of Efficiency; [redacted]
Mar 82 A Historian Looks at SIGINT; Filby V.R.
Apr 82 Review: The American Magic; [redacted]
Sep 82 Normandy: 1944; [redacted]

Broad Spectrum
May 82 Full or Broad Spectrum Lighting; [redacted]

Budgeting
Jul 77 ZBB? What In the World Is That?; [redacted] W.E.

By-Lines
Feb 78 By-Lines Don't Cost--They Pay!; [redacted]

C-LINERS
Mar 77 Letter: C-LINERS Article; 'Appalled'

CAA News
Dec 75 Learned Organizations--CLA Essay Contest; CAA News;
Jul 77 CAA News: What Ever Happened to the CAA?; [redacted]
Aug 77 CAA News: What Are They Up to Anyway?; [redacted]
Sep 77 CAA News: Whom?; [redacted]
Oct 77 CAA News; [redacted]
Nov 77 CAA News; [redacted]
Dec 77 CAA Message and News; [redacted]
Jan 78 CAA News; W.E.S.
Feb 78 CAA News; W.E.S.
Mar 78 CAA News; W.E.S.
Apr 78 CAA News; W.E.S.
May 78 CAA News; W.E.S.
Jun 78 CAA News; W.E.S.
Jul 78 CAA News; W.E.S.
Sep 78 CAA News; W.E.S.
Oct 78 CAA News; W.E.S.
Nov 78 CAA News; W.E.S.
May 79 CAA News;
Jun 79 CAA News;
Aug 79 CAA News; [redacted]
Oct 79 CAA News: Conference on Communications Analysis; [redacted]
Mar 77 [redacted] D.A.

Calendar
Dec 74 A Proposal for Calendar Reform; Leahy F.T.

Callsigns
Dec 74 An Approach to Callsign Analysis; Jackson W.J.
May 78 Callsigns and WARC-79; [redacted]
May 78 TA Implications of FCC Proposal; [redacted]
Sep 78 [redacted]

CAMINO
Feb 75 CAMINO News; [redacted]

Career Fields
Jun 76 How Things Have Changed!; [redacted]
Jan 78 The Changing Face of NSA; 'Anon.'

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Jan 81 Why Do They Leave?; [redacted]
Nov 82 The Costs of Muddling Through; Gould R.E.

Career Panels
Aug 74 A Short Directory of Career Panels;
Feb 79 Language Career Panel: Clarification of Nov 78 Item:

CARRIAGE
Sep 74 Project CARRIAGE: Worldwide HFDF Modernization Plan; Webster J.B.

Catalogs
Oct 81 Technical Support Catalogs; [redacted] K.J.

Celtic
Jun 78 Celtic Languages Today; [redacted]

Censorship
Nov 75 When Censorship Backfires; [redacted]

Central Information
Apr 75 A Guide to Central Information, C5;

Central Research
Nov 82 Central Research and The Paper Blob: [redacted]

Certification
Mar 76 A Comparison of NSA and ATA Certification Standards; [redacted]
Sep 76 Is There Life After Certification?; [redacted]

Changing Environment
Jan 80 There's a New World Coming - Are You Ready?; [redacted]

Chinese
Sep 74 Language in the News; [redacted]
Oct 74 Character Building in the People's Republic of China; Hamlett G., Reed M.
Oct 74 Even a 5-year-old Child ...; Tetrault E.W.
[redacted]
Jun 76 An Evaluation of a Scientific Chinese Machine Translation; [redacted]
Jun 76 Notes on Translation from the Chinese; [redacted]
Nov 77 Backing into Language Acquisition; [redacted]
Mar 78 [redacted]
Jun 78 [redacted]
Jul 78 Letter: [redacted] Article; [redacted]
Jul 78 Tell Me I'm Just a Sinobibliophobe; [redacted]
Dec 82 [redacted]

Ciphers
Feb 75 Basic Patterns of [redacted] Codes and Ciphers; [redacted]
Feb 76 What Is Cipher Text?; [redacted]
May 76 A Simple Cipher Story; [redacted]
Sep 76 Another Cipher by ...; [redacted]
Jun 77 Old Russian Manuscript Ciphers: [redacted]

Cipher Devices
Apr 79 But, Mr. Boak, Did You Ever Try To Get Rid of One in a Hurry?; D.H.W.

Cipher Systems
Oct 75 Computers, Comms, and Low-Grade Ciphers: [redacted]

CIRC
Jan 80 CIRC: An Intelligence Data Base; [redacted]

CISI News
Aug 74 Learned Organizations--1974 CLA Essay Contest, 1974 CMI Essay Contest; CISI Prizes and Honors, Spring 74;
Dec 74 Learned Organizations--CISI Forms Special Interest Group on Human Factors; [redacted]
Jan 75 Learned Organizations--IAI News, CISI News; CLA is Ten Years Old!; CMI News;
Mar 79 CISI News;
May 79 CISI News: Spring Conference;

Classic Cables
Mar 79 Classic Cables;
Apr 79 Classic Cables;
May 79 Classic Cables;
Apr 81 Classic Cables;

Classification
May 75 Codeword or COMINT Channels?; [redacted] H.
Jan 77 Letter: Use of Term 'Compartmented'; [redacted]
Jul 77 Classification Corner; [redacted]
Sep 77 Classification Corner: XGDS-2; [redacted]
Oct 77 Classification Corner: A Bigger Picture; [redacted]
Oct 77 Classification Corner: Who Said?; Kermisch H.
Jan 79 It's Party Time!; [redacted]

CLA News
Aug 74 Learned Organizations--1974 CLA Essay Contest, 1974 CMI Essay Contest; CISI Prizes and Honors, Spring 74;
Jan 75 Learned Organizations--IAI News, CISI News; CLA is Ten Years Old!; CMI News;
Apr 75 Language in the News; Tetrault E.W.
May 75 Learned Organizations--CLA News; IAI News;
Jul 75 Learned Organizations--CLA News; CMI News;
Dec 75 Learned Organizations--CLA Essay Contest; CAA News;

P.L. 86-36
EO 1.4.(c)
P.L. 86-36

Sep 76 Learned Organizations--1976 CLA Essay Contest; 1976 CMI Essay Contest;
Mar 78 CLA News;
Sep 78 CLA News;
Feb 79 CLA News: Russian Institute;
Oct 79 CLA News;
Jan 80 CLA News: Sydney Jaffe Award:
Jan 81 NCS-CLA Symposium;

Clustering
Apr 78 A Little PEP Talk; [redacted]

CMI News
Aug 74 Learned Organizations--1974 CLA Essay Contest, 1974 CMI Essay Contest; CISI Prizes and Honors, Spring 74;
Jan 75 Learned Organizations--IAI News, CISI News; CLA is Ten Years Old!; CMI News;
Jul 75 Learned Organizations--CLA News; CMI News;
Sep 76 Learned Organizations--1976 CLA Essay Contest; 1976 CMI Essay Contest;
Jan 79 CMI News;
Aug 79 CMI News; [redacted]

EO 1.4.(c) P.L. 86-36

Codes
Sep 74 Cryptanalysis and Code Recovery; Mountjoy M.
Feb 75 Basic Patterns of [redacted] Codes and Ciphers; [redacted]
Jun 75 The Navajo Code Talkers;
Jun 76 The Marquis and the Medium; [redacted]
Nov 78 Linguistics and the Code Reconstructor; Buck S.H.
Mar 82 [redacted]

EO 1.4.(c) P.L. 86-36

Collection
Aug 74 What Is a Collector?; [redacted]
Dec 74 The New Collection Criteria; [redacted]
Aug 75 Abdul and His 40 Tanks; Mason F.O.
Feb 76 The [redacted] System; [redacted]
May 76 Some Principles of Cover and Deception; [redacted]
Jun 76 The [redacted] Collection System: Murphy T.
Aug 76 NSA Cryptologic Collection;
Oct 76 Another Word on AG-22/IATS; [redacted] M.A.
Jan 77 Where Were We?; Mason F.O.
Nov 77 Director's Memorandum: [redacted] Guidance'; Inman B.R.
Nov 77 Objective Satisfaction Score: Collection Performance; [redacted]
Jan 78 An Early NSA Proposal for Satellite Remoting; [redacted] Nolte W.M.
Jan 78 What Ever Happened to COPES?; [redacted] W.E.
Feb 78 Collection-Support TA is Not for Everyone; [redacted]
Jun 78 [redacted]
Jan 81 KITTIWAKE; [redacted]

Color Code
Sep 74 Gary's Colors; Garofalo C.A.
Feb 82 Golden Oldie: Simplicity in Color; Garofalo C.A.

Comic Strip
Sep 77 Al Balloni, Editor; A.J.S.
Jan 79 Al Balloni, Editor; A.J.S.

EO 1.4.(c) P.L. 86-36

COMINT
Sep 74 COMINT Analysis of [redacted]
Jan 75 The Case for COMINT Readers; [redacted] H.G.
Apr 76 Golden Oldie: Hidden Losses in COMINT Production; Gould R.E.
May 76 COMINT in the Russian Navy, WWII; [redacted]
Jan 78 COMINT, COMSEC, and Hilbert's Tenth; [redacted]
Feb 79 The COMINT Chain 'Gang'; [redacted]

Communications
Oct 75 Computers, Comms, and Low-Grade Ciphers: [redacted]
Apr 80 [redacted]

EO 1.4.(c) P.L. 86-36

Communications Changes
Apr 75 A Comm Change at Ramasun Station; [redacted]
Oct 82 Golden Oldie: The Reality of Communications Changes; [redacted]

P.L. 86-36

Computers
Aug 74 Right-to-Left Text Sorts Are Not Impossible; [redacted]
Dec 74 Flag-Waving Programmer; John G.
Jan 75 The Yawn of the Computer Age or When Your Terminal is Terminal; [redacted]
Jun 75 Professionalizing in Computer Systems; [redacted]
Aug 75 Computer Network Resources In C5;
Oct 75 Computers, Comms, and Low-Grade Ciphers: The Southeast Asian Exploitable Message Processing System; [redacted]
Apr 76 What's the Best Location for the Computer Applications Function?; [redacted] C.E.
Jun 76 Computers In The ELINT and Telemetry Business; [redacted]
Mar 77 A View of the Central Computer Complex in the Late 1970s and Early 1980s; Phillips C.J.
Mar 77 An Overview of Project [redacted] Coyle J., [redacted]
Apr 77 Contemplating Computing; [redacted]
May 77 Universes, Galaxies, Stars, Bars, and Other Concepts; Phillips C.J.
Aug 77 Early Days in NSA Computing; Chauvenet L.R.
Apr 78 Remedial Software Engineering; [redacted] J.F.
May 78 The Joys of UNIX; [redacted]
Oct 78 Data Security and Human Error; [redacted] J.M.
Jun 79 Teaching Computer Science To Linguists; [redacted]

P.L. 86-36

EO 1.4.(c) P.L. 86-36

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Jan 80 Analysts of NSA, Arise!;
Nov 81 How to Create A User-Unfriendly System:
Nov 81 The PPC Is Coming!;
Dec 81 In Pursuit of: Faster Horses, Younger Women, Older Whiskey and More Money; D.L.
Dec 81 PLATFORM: How Did You Say That Works?;
Feb 82 Human Factors Corner: Some Advice to Users of Unfriendly System;
Feb 82 Software - AAAS, 1982;
Mar 82 A Personal Computer: A Current Cryptanalysis Support Tool:
Mar 82 Human Factors Corner: Consumer vs. Computer: A Review;
Apr 82 Personal Computer Application;
Apr 82 Word Processing In A4;
Sep 82 TSS Revolution;
Oct 82 Human Factors Corner: Text Editors;
Oct 82 What's The Good (Pass)Word?;
Dec 82 Going On-Line With Information Aids; Gurin J.

Computer Aids
Apr 76 Computer-Aided Transcription of

Computer Security
Mar 79 Computer Operating System Vulnerabilities;
Jun 82 Some Reflections On The Reality of Computer Security; Hanyok R.J.
Oct 82 What's The Good (Pass)Word?;
Dec 82 Passwords;

Computer TA
Apr 80 A Traffic Analyst Looks at Computers;

COMSEC
Jun 75 COMSEC Familiarization: Do You Need It?;
Jan 78 'Bodyguard of Lies' (Book Review);
Jan 78 COMINT, COMSEC, and Hilbert's Tenth;
Apr 79 COMSEC/SIGINT Relations; Boak D.G.
Nov 82 COMSEC Challenges;

COPES
Nov 76 Check Your Morse Front-End Alignment; 'Anon.'
Jan 78 What Ever Happened to COPES?; W.E.
Jun 78 Letter: Article; Gilbertson E.A.
Sep 78 Letter: Gilbertson Letter;

Coverterms
Apr 75 Coverterms; Filby V.R.

Jul 77 Which Tape Has the Intelligence? Project Gurin J.

CRITIC
Nov 78 Wedding Bells and That Old Gang of Mine; Sawyer E.L.

CRT
Mar 78 A Linguist Looks at the Tube; R.S.
Mar 78 The Hand Is Not Quicker Than the Eye;
Aug 82 Human Factors Corner: Video Display Terminals and Vision of Workers; M.E.

Cryptanalysis
Sep 74 Cryptanalysis and Code Recovery; Mountjoy M.
Oct 74 An October Overlap;
Nov 74 Answer to An October Overla : J.E.
Nov 74 New Trends in the Teaching of Cryptanalysis;
Dec 74 Puzzle: Secret Messages, 'Military Cryptanalytics';
May 75 TA, Handmaiden of CA; Mason F.O.
Jul 75 Re-psychling the Code Clerk;
Jul 75 Too Many Garbles;
Aug 75 Twenty Years of Transposition; J.E.
Aug 75 Typewriter Random -- A New Look;
Oct 75 Letter: Typewriter Keyboard;
Oct 75 F.
Feb 76 What Is Cipher Text?;
May 76 A Simple Cipher Story;
Aug 76 The Hierarchical Clustering of Cryptanalytic Data;
Nov 76 Teacher Learns a Lesson;
Aug 77 Want to Play with a Pickfair Square?;
Dec 77
Jan 78 'The Man Who Broke Purple' (Book Review); Filby P.W.
Apr 78 Looking at Mr. Isaac L.
May 78 The Future of Cryptanalysis; Lutwiniak W.
Jun 78 L.S.
Jan 82 Letter: Cryptanalysis Article; A.
Mar 82
Dec 82 Does Anybody Here Remember PURPLE?;

Cryptanalysts
Aug 74 What Should You Expect? or, The Analysis of Cryptanalysts;
Jun 76 How Things Have Changed!;

P.L. 86-36
P.L. 86-36
P.L. 86-36
P.L. 86-36
P.L. 86-36
EO 1.4.(c)
P.L. 86-36
P.L. 86-36
EO 1.4.(c)
P.L. 86-36

Crypto-TA
Jun 75 More on Squaring the Page (A Crypto-TA Function); Mason F.O.
Apr 79 A Somewhat Larger Problem: [redacted] W.E.
Aug 82 An Old Problem; [redacted]
Oct 82 Answer: An Old Problem; [redacted]

Cryptograms
Sep 74 Secrets of the Altars--The Moustier Cryptograms; [redacted]

Cryptographic
Apr 75 Psyching the Code Clerk: [redacted] Callimahos L.D.

CRYPTOLOG
Aug 74 CRYPTOLOG A Letter of Introduction; Wolff H.E.
Dec 74 CRYPTOLOG Index for 1974;
Jan 75 CRYPTOLOG Index for 1974;
Dec 75 CRYPTOLOG Index for 1974-1975;
Nov 76 Letter: Cumulative Index; Bostick C.W.
Dec 77 CRYPTOLOG Index for 1977;
Mar 78 An Idea for an Article; Miller D.E.
Dec 78 CRYPTOLOG Index for 1978;
Jan 79 Letter From the Publisher; Lutwiniak W.
Mar 79 Readers' Survey; D.H.W.
May 82 CRYPTOLOG Numbering;

Cryptologic Mission
Feb 79 Let's Not Forget Our Cryptologic Mission: Gurin J.
Apr 79 Letter: Gurin Article (Feb 79); [redacted]

Cryptology
Jan 76 Football and Cryptology; [redacted]
Feb 78 First Lady of Navy Cryptology; [redacted] R.P.

Cryptosystems
Oct 75 The Do Xa Pads; Wiley E.
Sep 78 [redacted]

Crypto Devices
Aug 82 AFCEA 82 and ICC-82: New Crypto Devices; [redacted]

CSI News
Dec 75 Establishment of CSI Newsletter;

Cyrillic
Jun 76 Transliteration or Cyrillic?; [redacted] G.

Data Bases
Jan 75 How Clean Does a Data Base Need to Be?; [redacted]
Feb 79 Literature Search On-Line; Miller M.E.
Jan 80 CIRC: An Intelligence Data Base; [redacted]
Nov 82 Central Research and The Paper Blob; [redacted]

[redacted]

Data Flow
Apr 80 Data Flow--Challenge of the 1980s; Phillips C.J.

Data Security
Oct 78 Data Security and Human Error; [redacted] J.M.

Data Sorting
Aug 74 Right-to-Left Text Sorts Are Not Impossible; [redacted]

Data Standards
Nov 74 Data and Definitions: Calling Things by Their Rightful Names; [redacted]
Nov 78 Data Standards Center; Pattie M.T.
Dec 78 a/k/a Sam; [redacted]
Feb 79 Data Standards Without Tears; [redacted] P.Q.
Feb 79 Well, Maybe a Sniffle or Two...; Pattie M.T.
Mar 79 Data Standards Without Tears: A Comment; [redacted]
Mar 79 Letter: Data Standards; [redacted]
Jun 79 ... Mr. Pattie Replies; Pattie M.T.
Jun 79 Data Standards Without Teeth; [redacted] P.Q.
Aug 79 An August Baudy; [redacted]
Jan 82 Data Field Naming/Coding Conventions at NSA; [redacted]
Aug 82 All I Ever Wanted To Know About DES; [redacted]

Dates
Jul 77 Dating Game; Williams D.H.
Aug 77 Postscript to 'Dating Game'; [redacted]

Deception
Feb 76 How Do We Know It's True?; Filby V.R.
May 76 Some Principles of Cover and Deception; [redacted]
Jun 76 'Right On, Vera!'; [redacted]
Jun 79 [redacted] M.R.

Degarbling
Sep 77 [redacted] D.L.
Dec 77 Letter: [redacted] Article; [redacted]

DESKPAD
Nov 75 DESKPAD: A Programmers's Tool; [redacted] H.

DIALOG
Aug 77 DIALOG Available at NSA;
Feb 79 Literature Search On-Line; Miller M.E.

Dictionaries
Feb 75 Glossaries versus Dictionaries: Which Should It Be?; Gurin J.
Feb 75 The Devil's Dictionary;

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

P.L. 86-3

P.L. 86-3

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

Aug 76 Note on FRANCOPHONEGLOS;
May 78 Project UTENSIL: The DDO Data Dictionary/Directory; [redacted]

Documentation
Sep 77 Is There a Doctor in the House?; [redacted]
Jan 80 System Acquisition Document Review; [redacted]
Jun 82 Human Factors: Responsible Documentation; [redacted]

Economic Intelligence
Oct 81 Economic Intelligence: Problems and Prospects; [redacted]

Editor's Note
May 76 Scraps from the Editor's Desk; Salemme A.J.
Feb 79 [redacted] and a Little Bit of Luck; Williams D.H.

Editorial Comment
Feb 78 No, Winnie, You've Got It Upside Down Too!; A.J.S.
Jun 82 Letter: Editorial Comment; [redacted] P.A.

Efficiency
Dec 81 Review: In The Name of Efficiency; [redacted]

ELINT
Nov 74 [redacted] What? Where? Why?; [redacted] G.A.
Apr 75 The Uses of ELINT; [redacted]
May 75 Letter: Bloom Article; [redacted]
Apr 76 Will the Real ELINT Please Stand Up; [redacted]
Jun 76 Computers In The ELINT and Telemetry Business; [redacted]
Aug 76 Yes, Don, There is an ELINT!; [redacted] W.L.
Nov 76 Letter From Canada; [redacted]

Emitter Identification
May 79 Emitter Identification Techniques; [redacted]

English
Dec 74 Language in the News; [redacted]
Jun 75 Where Does 'Does' Come From?; Tetrault E.W.
Aug 75 Language in the News;
Nov 76 The Uses of Elegant English; [redacted] J.R.
May 77 Choose Ye!; [redacted]
May 77 Plain English; [redacted]
Jun 77 Vich Iss R-r-right?; A.J.S.
Nov 77 What Ever Does 'However' Mean?: [redacted]
Jan 78 The Joys and Frustrations of Plural-Dropping; A.J.S.
Mar 79 Fairbanks on English; Fairbanks S.
Apr 79 More Fairbanks on English; Fairbanks S.
May 79 More Fairbanks On English; Fairbanks S.
Jun 79 How Are Your Stamina?; Fairbanks S.
Jul 79 Wilt Thou, Angelina ...?; Fairbanks S.

Equipment
Jun 78 Equipment Maintenance on ABNER; Bernard R.
Oct 78 Will It Really Do the Job?; [redacted]
Apr 79 But, Mr. Boak, Did You Ever Try To Get Rid of One in a Hurry?; D.H.W.
Oct 79 Another Source; [redacted]
Oct 79 Snowballs On The Roof; Filby V.R.
Aug 82 AFCEA 82 and ICC-82: New Crypto Devices; [redacted]

Equivalency Tests
Nov 75 NCS Offers Course-Equivalency Tests;
Apr 76 NCS Offers Course-Equivalency Tests, Clarification;

Evaluation
Oct 77 K1: SCA Field Management and Evaluation; [redacted]
Jul 79 EXPERT; [redacted]

EW
Jun 75 The Role of the Electronic Warfare Advisory Element (EWAE) of NSA; [redacted]
Oct 76 Russian SIGINT and Electronic Warfare; [redacted]

EXPERT
Jul 79 EXPERT; [redacted]

Exploitation
Feb 78 [redacted] Schlauch R.H.
Jul 79 EXPERT; [redacted]

Field Stations
Apr 75 A Comm Change at Ramasun Station; Reese J.C.
Oct 75 The Danang Processing Center; [redacted] A.
Jan 76 Leo in October; Murphy A.I.
Apr 76 One Day in Danang; [redacted]
Jun 76 Letter: [redacted] Article; Murphy A.I.
Jan 77 Where Were We?; Mason F.O.

Forms
Sep 77 Speaking of Logging ...; [redacted]

FRANCOPHONEGLOS
Aug 76 Note on FRANCOPHONEGLOS;

French
Aug 74 Nice Busman's Holiday for One NSA Employee; [redacted]
Sep 74 Language in the News; [redacted]
Aug 76 Language in the News;

EO 1.4.(c) P.L. 86-36

EO 1.4.(c) P.L. 86-36

P.L. 86-36

P.L. 86-36

P.L. 86-36

EO 1.4.(c) P.L. 86-36

P.L. 86-36

EO 1.4.(c) P.L. 86-36

P.L. 86-36

French Connection
Dec 76 The French(fried) Connection: Gino the Genie; [redacted]

Frequencies
Jan 79 The Return to HF; [redacted]
Jan 82 HF - The Rebirth: [redacted]
Jun 82 Amateur Spread Spectrum; [redacted]

[redacted]
Feb 76 The [redacted] System; [redacted]
Oct 77 Update on [redacted]

Games
Oct 76 A Vexing Agency-Wide Problem; Mason F.O.
Nov 76 Answer to 'Vexing ... Problem'; Mason F.O.

EO 1.4.(c)
P.L. 86-36

Geography
Dec 74 Maps in Mind--A Photoessay; [redacted]
Dec 74 Puzzle: Citizens of the World;
Nov 77 How Many African Countries Can You Spot?; [redacted]
Apr 78 +Conoces Bien la Geografia?; [redacted]
Oct 78 Know Your Geography; [redacted]
Dec 78 How Do You Spell Peking?; [redacted]
Feb 79 Know Your Geography; [redacted]
Apr 80 Geographic Trivia;

German
Sep 76 Language in the News;
Nov 77 Backing into Language Acquisition; [redacted]

P.L. 86-36

Glossaries
Aug 74 The New Traffic Analysis Glossary;
Oct 74 Golden Oldie: An Unofficial Glossary of Weasel Words;
Feb 75 Glossaries versus Dictionaries: Which Should It Be?; Gurin J.
Feb 76 Expletives Deleted: Glossing Over a Glossary; [redacted]
Aug 77 Expletives Deleted?; Salemme A.J.

[redacted]
Jun 76 The [redacted] Collection System; Murphy T.
Oct 76 Letter: [redacted] Article [redacted]

EO 1.4.(c)
P.L. 86-36

Graphics
Dec 75 Graphic Analysis of Linear Recursive Sequences; [redacted]
Dec 76 Graphic Names; [redacted]

GUPPY
Feb 75 Replacement of the GUPPY Library; [redacted]

Hebrew
Sep 74 Language in the News; [redacted]

HELIPAD
May 79 Project HELIPAD: An Epitaph; [redacted] M.L.

P.L. 86-36

HF
Jan 79 The Return to HF; [redacted]
Jan 82 HF - The Rebirth; [redacted]

HFDF
Sep 74 Project CARRIAGE: Worldwide HFDF Modernization Plan; Webster J.B.
Nov 74 [redacted] What? Where? Why?; [redacted] G.A.

EO 1.4.(c)
P.L. 86-36

Hiring
Oct 74 News from NCS--Agency Resumes Hiring of LICs; NCS Offers Course in 'SIGINT Appreciation';
Dec 75 Linguists From The Melting Pot; Gould R.E.

P.L. 86-36

History
Feb 75 The Gulf of Tonkin Incident; [redacted] W.D.
May 76 COMINT in the Russian Navy, WWII; [redacted]
Sep 78 Soviet COMINT and the Civil War; [redacted]
Nov 78 Cast a Double Shadow: The Trojan Horse of SIGINT; [redacted]
Jan 79 W.W.II Japanese Translation at Arlington Hall Station;
Mar 79 Pursuit of the [redacted] [redacted] E.L.
Sep 82 Normandy: 1944; [redacted]
Dec 82 Does Anybody Here Remember PURPLE?; [redacted]

EO 1.4.(c)
P.L. 86-36

Human Factors
Jun 77 Human Factors and Systems Design: An Estranged Relationship?; [redacted]
Oct 77 Human Factors and the Use of Microfiche Readers at NSA; Snow D.
Jan 79 Human Factors Newsletter;
Jan 82 Human Factors Corner: Information System; [redacted]
Feb 82 Human Factors Corner: But What Do I Do With My Papers?; [redacted]
Feb 82 Human Factors Corner: Some Advice to Users of Unfriendly System; [redacted]
Mar 82 Human Factors Corner: Consumer vs. Computer: A Review; [redacted]
May 82 Human Factors Corner: Data Gathering, How Do We Spend Our Day?; [redacted]
Aug 82 Human Factors Corner: Video Display Terminals and Vision of Workers; [redacted] M.E.
Oct 82 Human Factors Corner: Text Editors; [redacted]
Nov 82 Human Factors Corner: How Do People Organize Cooperative Work?; [redacted]
Dec 82 Passwords; [redacted]

IAI News
Jan 75 Learned Organizations--IAI News, CISI News; CLA is Ten Years Old!; CMI News;
May 75 Learned Organizations--CLA News; IAI News;

P.L. 86-36

Indicators
Dec 82 Development and Correlation of Indicators;

Information
Jan 82 Human Factors Corner: Information System
May 82 The NSA Information Desk: 'No Comment';

INKSTAND
Jun 77 SIGINT Welcomes INKSTAND;

Intelligence
Dec 75 What Are We About? (Fragments, Figments, or What?);
Apr 76 Letter: Comments on Letter on What Are We About?;
Apr 76 Letter: What Are We About? Article;

Intelligence Community
Aug 77 New Directions for the U.S. Intelligence Community; Gaddy D.W.

Intern Program
Sep 74 A Long Hard Look at the Intern Program--Program Philosophy; Recruitment (Part One); 'Exinterne'
Oct 74 A Long Hard Look at the Intern Program--Selection and Orientation (Part Two); 'Exinterne'
Nov 74 A Long Hard Look at the Intern Program--Motivation and Morale (Part Three); 'Exinterne'
Dec 74 A Long Hard Look at the Intern Program--What Happens to the Graduate? (Part Four); 'Exinterne'
Feb 75 Letter: Exinterne Articles; Tetrault E.W.
Apr 75 Letter: Exinterne Articles;

Interpreters
Feb 75 The Faithful Echo--The Role of the State Department Interpreter;
Oct 77 The Perils of Being a State Department Interpreter;
Feb 78 The Unseen Go-Between; Gurin J.

IRA
Aug 77 What Is an Information Research Analyst?;

Oct 79

IRONHORSE
Oct 75 IRONHORSE: A Tactical SIGINT System;
Oct 76 Letter: IRONHORSE Article:

ISHTAR
Jan 75 The SIGINT Users' Handbook or: What's an ISHTAR?;

Japanese
Nov 76 Toujours La Politesse (Japanese); Buck S.H.
Jul 77 The Transcription Skill: Concepts and Teaching Methodologies;
Jan 79 W.W.II Japanese Translation at Arlington Hall Station;

JPRS
Sep 77 JPRS Language Reference Aids;

Keyword Spotting
Mar 77 Letter: Keyword Spotting; Gurin J.

KITTIWAKE
Jan 81 KITTIWAKE;

Dec 78

Dec 78

KRYPTOS News
Feb 82 KRYPTOS: A New Society;
Dec 82 KRYPTOS News;

Language
Aug 74 Nice Busman's Holiday for One NSA Employee; Dudley B.
Aug 74 The Language of Beisbol in Everyday Talk; , Santiago-Ortiz R.A.
Sep 74 Language in the News;
Oct 74 Character Building in the People's Republic of China:
Oct 74 Even a 5-year-old Child ...; Tetrault E.W.
Nov 74 Purity of the Russian Language--Slavophiles vs. Westernizers;
Dec 74 Language in the News:
Dec 74 The Old Section;
Jan 75 The Case for COMINT Readers; H.G.
Feb 75 The Faithful Echo--The Role of the State Department Interpreter;
Apr 75 Language in the News; Tetrault E.W.
Jun 75 The Navajo Code Talkers:
Jun 75 Where Does 'Does' Come From?; Tetrault E.W.
Aug 75 A Fix for the Language Problem?;

Aug 75 Language in the News:
Oct 75 Language Lessons Learned: A Personal Memoir;
Oct 75 Tactical Language Exploitation: A Lesson Learned?;
Nov 75 Golden Oldie: Blue Russian; J.F.
Feb 76 Expletives Deleted: Glossing Over a Glossary;
Mar 76 1976 Language Meetings and Conferences;
Mar 76 A Comparison of NSA and ATA Certification Standards;

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

 P.L. 86-36

DOCID: 4009861

EO 1.4.(c)
P.L. 86-36

Mar 76 To Pull a 'Ponyal'; [redacted]
Apr 76 Computer-Aided Transcription of [redacted]
Apr 76 How Do Adults Learn Language?; [redacted]
Apr 76 Language in the News: Language Rule;
May 76 Hypnosis and Self-Hypnosis in Language Learning; Buckley D.
May 76 What Language Problem?; Pattie M.T.
Jun 76 An Evaluation of a Scientific Chinese Machine Translation; [redacted]
Jun 76 Notes on Translation from the Chinese; [redacted]
Aug 76 Language in the News;
Aug 76 Research in Speech Perception (Dr. Ruth Day); Tetrault E.W.
Sep 76 Language in the News;
Oct 76 Language Skill File; [redacted] Mooney K.
Oct 76 Some Ideas about Mechanized Language Working Aids; [redacted]
Nov 76 Golden Oldie: The Things They Say; Miller D.E.
Nov 76 The Uses of Elegant English; [redacted] J.R.
Nov 76 Toujours La Politesse (Japanese); Buck S.H.
Dec 76 What's In a Name?; [redacted]
Jan 77 Letter: [redacted] Article; Kenny M.M.
Apr 77 'It's Got to Get Out Today!'; Blank F.
Jul 77 [redacted] Buck S.H.
Jul 77 Tool Languages; [redacted]
Aug 77 Expletives Deleted?; Salemme A.J.
Sep 77 [redacted] D.L.
Sep 77 JPRS Language Reference Aids; [redacted]
Sep 77 The [redacted] Seminar Program; [redacted] W.L.
Nov 77 Backing into Language Acquisition; [redacted]
Nov 77 Language Processing Forum; [redacted]
Nov 77 Letter: Salemme Article; [redacted]
Nov 77 Letter: Salemme Article; [redacted]
Dec 77 What Made Them Do It? (Language Self-Study); [redacted]
Jan 78 Thanks for the Attaboy!; [redacted]
Feb 78 [redacted]
Feb 78 The Unseen Go-Between; Gurin J.
May 78 Uncle-a Sam Wantsa You!; [redacted]
Jun 78 Celtic Languages Today; [redacted]
Jul 78 Is A Translator a Professional?; [redacted]
Sep 78 Letter: Pattie Article; Buckley D.
Sep 78 Soviet COMINT and the Civil War; [redacted]
Sep 78 What's In a Non-Name?; [redacted]
Oct 78 And-a You Betta Have Moti-vaysh!; [redacted]
Dec 78 Agency Summer Language Study; Buckley D.

Jan 79 Golden Oldie: On First Opening Kenney's 'Statistics'; Mountjoy M.
Jan 79 Henry Cement and other Phantoms of the Opera(tions); [redacted]
Feb 79 Language Career Panel: Clarification of Nov 78 Item;
Mar 79 VORD is a Better Idea; [redacted]
May 79 Run This Through Your Transcription Machine; [redacted]
May 79 Where Do Good Transcribers Come From?; [redacted]
Jun 79 Letter: 'Sixth Language'; [redacted] P.A.
Jun 79 Sign Language;
Jun 79 The Baltic Encoders; [redacted]
Jul 79 Gears of the Mouth; [redacted]
Jul 79 Letter: [redacted] Article (Apr 79); [redacted]
Jul 79 Wilt Thou, Angelina ...?; Fairbanks S.
Aug 79 Language Proficiency Certificates for Military Personnel; [redacted]
Oct 79 NCS Summer Language Program;
Apr 80 LIME-A, OHIO; LEEM-A, Peru; Salemme A.J.
Apr 80 P16 Language and Cryptologic Library; [redacted]
Jan 81 Why Do They Leave?; [redacted]
Apr 81 Grading The Russian PQE; [redacted]
Jan 82 Letter: [redacted] Article; Chauvenet L.R.
Feb 82 Native Scripting of Languages; [redacted]
Apr 82 Partial Machine Translation: Final Report; Pratt D.L., [redacted]
Nov 82 The Costs of Muddling Through; Gould R.E.

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Language Identification
Jan 80 LIP; [redacted]

Leadership
Oct 82 Leadership: A Personal Philosophy; [redacted]

P.L. 86-36

Lexicography
Sep 74 Some Thoughts on Lexicography; Buck S.H.
Feb 75 Glossaries versus Dictionaries: Which Should It Be?; Gurin J.
Jul 77 [redacted] Buck S.H.

EO 1.4.(c)
P.L. 86-36

Library
Feb 75 Replacement of the GUPPY Library; [redacted]
Aug 76 NSA Cryptologic Collection;
Jun 79 Letter: Library Changes; [redacted]
Jun 79 Letter: Library Changes; [redacted]
Apr 80 P16 Language and Cryptologic Library; [redacted]

Linguistics
Nov 78 Linguistics and the Code Reconstructor; Buck S.H.

P.L. 86-36

Linguists
Apr 75 Machine Course for Linguists; Tetrault E.W.
May 75 Are We Wasting Linguistic Time?; [redacted] M.R.
Aug 75 Linguists -- We Need An 'Experts Yellow Pages'!; [redacted]
Oct 75 Linguists -- You Have an Expert to Call!: [redacted]
Dec 75 Linguists From The Melting Pot; Gould R.E.
Sep 76 Machine-Produced Aids for the Linguist, Part I; Salemme A.J.
Oct 76 Machine-Produced Aids for the Linguist, Part II; Salemme A.J.
Dec 76 Let's Give the Linguists a Bigger Piece of the Pie!; [redacted]
Jan 77 What If the Linguists Disappeared?; Myers L.S.
Mar 77 A Few Thoughts on the NSA Linguist; 'Anon.'
Mar 77 Letter: Butcher Article; Buckley D.
Apr 77 Letter: Buckley Letter; Tetrault E.W.
Jun 77 Letter: Buckley Letter [redacted]
Sep 77 Letter: Lebanik Letter; Buckley D.
Mar 78 A Linguist Looks at the Tube [redacted] R.S.
Jun 78 As I Was Saying Two Years Ago ...; Pattie M.T.
Jun 79 Teaching Computer Science To Linguists; [redacted]
Aug 79 On Coming of Age at NSA: Confessions of an Ex-Linguist; [redacted]
Oct 79 Letter: [redacted] Article (Aug 79); Taylor D.L.
Jan 80 LIP; [redacted]
Jan 80 NSA/CSS Military Linguist Program;
Apr 80 Help Wanted; [redacted]
Aug 82 Linguist Machine; [redacted]

LIP
Jan 80 LIP; [redacted]

Lithuanian
Jun 79 The Baltic Encoders; Reiskis A.

Lycian
Sep 74 Language in the News; [redacted]

Machine
Apr 82 Partial Machine Translation: Final Report; [redacted]

Machine Aids
Apr 75 Machine Course for Linguists; Tetrault E.W.
Sep 76 Machine-Produced Aids for the Linguist, Part I; Salemme A.J.
Oct 76 Machine-Produced Aids for the Linguist, Part II; Salemme A.J.
Oct 76 Some Ideas about Mechanized Language Working Aids; [redacted]
Apr 82 Bookbreakers Forum On Machine Aids; [redacted]

Machine Intelligence
Jul 75 Machine Intelligence--Promise or Delusion?; [redacted]

Machine Translation
Jun 76 An Evaluation of a Scientific Chinese Machine Translation; [redacted]

Management
Aug 74 Golden Oldie: The Management Survey of the Philharmonic;
Sep 77 Knowledge Resource Management at NSA; [redacted]
Mar 78 A Donkey in Your WHAT?; [redacted]
Jul 78 The Bucky Balance; [redacted]

Management Directives
May 75 Hooray for PMDs!; [redacted]

Managers
Feb 78 Senior Military Cryptologic Supervisors Course; [redacted]
Apr 78 Accentuate the Negative; [redacted]

Maps
Dec 74 Maps in Mind--A Photoessay; [redacted]

MAROON SHIELD
Nov 77 Director's Memorandum: [redacted] Guidance': Inman B.R.

EO 1.4.(c)
P.L. 86-36

Mathematics
Jul 78 Tell Me I'm Just a Sinobibliophobe; [redacted]

Mechanized Translation
Jul 75 RAPIDTRAN: [redacted]

Meetings
Mar 82 Rules For The Camel Corps; [redacted] C.

Memorable Memo
Aug 79 Memorable Memos;

Messages
Feb 82 A Time for Change; [redacted]
Jun 82 Golden Oldie: Reporting Message Volumes; [redacted]

Meteorburst
Mar 82 Meteorburst Communications; [redacted]

Microcomputers
May 82 The Micro Revolution: Arthur Young Study Comment [redacted]

Micrographics
Sep 76 The Bible and the Washington Monument; Snow D.
Oct 77 Human Factors and the Use of Microfiche Readers at NSA; Snow D.
Dec 77 Conversation With a Micrographics Pioneer; [redacted]

P.L. 86-36

Oct 78 Back to Square One!; [redacted]
Oct 78 Reduction Ratios in Micrographics; Snow D.

Military
Jul 78 The Soviet General Staff; [redacted]

Minicomputers
Jun 78 A Computer Scratch Pad at Home or at Work?; [redacted]
Jun 78 Minnie's Mini; Kenny M.M.

EO 1.4.(c)
P.L. 86-36

Missiles
Nov 77 [redacted]

Molecule Superseries
Feb 75 Golden Oldie: Establishment of Molecule Superseries; [redacted]

EO 1.4.(c)
P.L. 86-36

MORETOWN
Mar 78 [redacted]
Jul 78 Letter: [redacted] Article; [redacted]

MOSES
Jun 79 The Story of MOSES; Gardner D.G.

MSI
Dec 75 The Great Soviet Shipbuilding Mystery; Williams D.H.

Multichannel
Oct 78 [redacted]

Multivariate Techniques
Mar 77 [redacted] D.A.

EO 1.4.(c)
P.L. 86-36

Navy
Feb 78 Soviet Navy Command Post System; [redacted]

NCS
Oct 74 News from NCS--Agency Resumes Hiring of LICs; NCS Offers Course in 'SIGINT Appreciation';
Apr 75 Language in the News; Tetrault E.W.
Nov 75 NCS Offers Course-Equivalency Tests;
Apr 76 NCS Offers Course-Equivalency Tests, Clarification;
Oct 79 NCS Summer Language Program;
Jan 81 NCS-CLA Symposium;

Negative Intelligence
Oct 78 A Method for Measuring Negative Intelligence; [redacted]

Network
Aug 75 Computer Network Resources In C5;

NSA
May 76 A Soviet View of NSA; [redacted]
Dec 78 A VIP Tour through the Attic of NSOC; [redacted]

P.L. 86-36

Oct 79 Snowballs On The Roof; Filby V.R.
Apr 80 What To Do About 'FANX'; [redacted]
May 82 The NSA Information Desk: 'No Comment'; [redacted]
Oct 82 Not Secret Anymore; [redacted]

On-Line Aids
Dec 82 Going On-Line With Information Aids; Gurin J.

On-Line Data
Aug 77 DIALOG Available at NSA;
Feb 79 Literature Search On-Line; [redacted]

OPELINT
Nov 81 OPELINT Is Alive and Well In B Group; [redacted]

P.L. 86-36

Order of Battle
Dec 77 [redacted]
Mar 78 Letter: Rosenbluh Article; [redacted] K.E.

Organizations
Dec 78 To Whom It May Concern; Grant L.G.
Feb 79 Letter: Grant Article (Dec 78); Pattie M.T.
Apr 81 Middle-Age Spread; [redacted]

P.L. 86-

Organize Work
Nov 82 Human Factors Corner: How Do People Organize Cooperative Work?; [redacted]

Overheard
Oct 78 Overheard in the Burnbag Line;
Apr 82 Overheard While Standing in the Burnbag Line;

Pattern Recognition
Dec 77 What Is Pattern Recognition?; [redacted] D.A.

PEP
Apr 78 A Little PEP Talk; [redacted]

PERCIVAL
Nov 76 Check Your Morse Front-End Alignment; 'Anon.'

Performance
Feb 82 The Internal Performance Evaluation: Friend or Foe?; [redacted]

Performance Appraisals
Jan 80 Between The Lines of Your Performance Appraisal; [redacted]

Personalities
Jul 77 Match Them Up!; [redacted]
Jan 79 Golden Oldie: On First Opening Kenney's 'Statistics'; Mountjoy M.
Jan 79 Henry Cement and other Phantoms of the Opera(tions); [redacted]
Oct 79 The Roads Around Us; Chauvenet L.R.

P.L. 86-36

Personality
Sep 77 Tribute to the Guru; 'Class 32'

Personal Computers
Mar 82 A Personal Computer: A Current Cryptanalysis Support Tool; [redacted]
Apr 82 Personal Computer Application: [redacted]
Jun 82 Letter: Personal Computer Article; [redacted]

Personnel
Feb 78 First Lady of Navy Cryptology; [redacted] R.P.
Jan 79 How do You Tell These Two Clowns Apart?;

Plaintext
May 82 Letter: Plaintext; [redacted]

PLATFORM
Mar 77 An Overview of Project [redacted]
Dec 81 PLATFORM: How Did You Say That Works?; [redacted]

PL1
Nov 78 Formatting PL/1 Source Code; [redacted] K.J.

PMD
May 75 Hooray for PMDs!; [redacted]

PMT
Apr 82 Partial Machine Translation: Final Report; [redacted]

Poems
Jan 77 Executive Order 11652; 'Leiner'
Jan 81 Some Things Never Change;
Feb 82 A Wail, A Complaint, and a Melange; Snyder S.S.

Polyhedrons
May 77 The Polyhedral War; [redacted]
Aug 77 Letter: [redacted] Article; 'Weeson'

Portuguese
Sep 74 Language in the News; [redacted]
Jan 78 Thanks for the Attaboy!; [redacted]

PQE
Jan 75 The Case for COMINT Readers; [redacted] H.G.
Dec 76 Why Can't They Design a Good SR Test?; Bjorklund K.
Apr 77 Some Thoughts on the Russian PQE; [redacted]
Jun 77 Letter: Clark Article; [redacted]
Feb 79 In Defense of The Indefensible: Notes on the Russian PQE; Tetrault E.W.
Apr 81 Grading The Russian PQE; [redacted]
Jan 82 Letter: [redacted] Article; Chauvenet L.R.

Dec 82 Questions In Search of a PQE; 'Schmedlapp'

Predictions
Feb 76 The Prebendary and the Prophet; [redacted] R.
Dec 76 But It Looks Like the Real Thing; [redacted]
Mar 77 Letter: [redacted] Interview; [redacted] H.L.

Production
Apr 76 Golden Oldie: Hidden Losses in COMINT Production; Gould R.E.

Professionalization
Dec 74 The New Collection Criteria; [redacted]
Apr 75 Letter: Professionalization of Bookbreakers; [redacted]
Jun 75 Letter: Bookbreakers; Professionalization of Country Specialists; [redacted]
Jun 75 Professionalizing in Computer Systems; [redacted]
Apr 77 Some Thoughts on the Russian PQE; [redacted]
Oct 78 Continuing Professionalization; [redacted]
Apr 79 Fear of Testing, and What To Do About It; [redacted]

Proficiency
Aug 79 Language Proficiency Certificates for Military Personnel; [redacted]

Promotions
Nov 77 A Proposed Cure for the Time-in-Grade Syndrome; [redacted]
Mar 78 A Proposed Cure for the 'Performance Syndrome'; [redacted]
Dec 78 Some Tips on Getting Promoted; [redacted] V.C.
Feb 79 Letter: [redacted] Article (Dec 78); Bostick C.W.
Aug 79 ... But On The Other Hand;
Aug 79 NSA Promotion Boards: How They Work; [redacted]
Jan 81 How to Improve Your Promotion Potential; [redacted]
Jun 82 Who Wants A Promotion, Anyway?; [redacted]
Aug 82 What Promotion Boards Want; [redacted]

Publications
Jan 75 The SIGINT Users' Handbook or: What's an ISHTAR?; [redacted]
May 76 About the NSA SIGINT Summary; Hunt W.
Sep 76 Foreign Publications Procurement Program; [redacted]
Mar 77 Revised Technical SIGINT Manual in Preparation; Filby V.R.
May 78 Project UTENSIL: The DDO Data Dictionary/Directory; [redacted]
Dec 78 'No, No, Nanette!' Means Yes?; A.J.S.
Jan 79 Human Factors Newsletter;

P.L. 86-36

Jul 79 Russian Handbook of Spoken Usage, Vol 3;
Jan 80 System Acquisition Document Review; [redacted]
Mar 82 Old Phone Books Never Die; Nolte W.M.

Punctuation
Nov 74 The Apostrophe: Some Thought's;
Oct 76 The Winnah: Kid Apostrophe!;
Aug 79 Punctuation: More Than Meets The Eye; [redacted]

PURPLE
Dec 82 Does Anybody Here Remember PURPLE?; [redacted]

Puzzle
Aug 74 Puzzle: Stinky Pinky;
Aug 74 Puzzle: Telephone Directory;
Oct 74 An October Overlap; [redacted]
Oct 74 Puzzle: Telephone Recall;
Nov 74 Answer to An October Overla ; [redacted] J.E.
Dec 74 Puzzle: Citizens of the World;
Dec 74 Puzzle: Secret Messages, 'Military Cryptanalytics';
Jan 75 Puzzle: Crossed Codewords; [redacted]
Feb 75 Letter: Citizens of World Puzzle; [redacted] G.P.
Feb 75 Puzzle: Can You Make Out the Name?; [redacted]
Apr 75 Answer to Can You Make Out the Name!; [redacted]
May 75 Puzzle: How Many Words in 'CRYPTOLOG'; [redacted]
Jun 75 Puzzle: [redacted]
Aug 75 Puzzle: CRY-PTO-LOGrolling;
Oct 75 NSA-Crostic No. 1; A.J.S.
Jan 76 NSA-Crostic No. 2; A.J.S.
Apr 76 NSA-Crostic No. 3; A.J.S.
Jun 76 NSA-Crostic No. 4; A.J.S.
Oct 76 NSA-Crostic No. 5; A.J.S.
Nov 76 TEXTA 'Word Seek'; [redacted]
Jan 77 NSA-Crostic No. 6; A.J.S.
Apr 77 NSA-Crostic No. 7; Chauvenet L.R.
Jul 77 NSA-Crostic No. 8; A.J.S.
Jul 77 Puzzle: Match Them Up!: [redacted]
Sep 77 NSA-Crostic No. 9; Williams D.H.
Nov 77 How Many African Countries Can You Spot?: [redacted]
Nov 77 NSA-Crostic No. 10; A.J.S.
Jan 78 NSA-Crostic No. 11; Williams D.H.
Feb 78 Puzzle: Three Holes;
Mar 78 Answer to Three Holes;
Mar 78 NSA-Crostic No. 12; A.J.S.
Mar 78 Word Seek; [redacted]
Apr 78 +Conoces Bien la Geografia?; [redacted]
Apr 78 NSA-Crostic No. 13; Williams D.H.
Apr 78 Prizewinners in Three Holes;
May 78 NSA-Crostic No. 14; 'Sardonyx'
Jun 78 NSA-Crostic No. 15; A.J.S.
Jul 78 NSA-Crostic No. 16; Williams D.H.
Sep 78 NSA-Crostic No. 17; A.J.S.
Oct 78 Know Your Geography; [redacted]
Oct 78 Letter: NSA-Crostic; [redacted]
Oct 78 Letter: NSA-Crostic; Filby V.R.
Oct 78 NSA-Crostic No. 18; Williams D.H.
Oct 78 Puzzle: Who and Whom?; [redacted]
Nov 78 NSA-Crostic No. 19; Williams D.H.
Dec 78 NSA-Crostic No. 20; Williams D.H.
Jan 79 NSA-Crostic No. 21; Williams D.H.
Feb 79 Know Your Geography; [redacted]
Feb 79 NSA-Crostic No. 22; D.H.W.
Mar 79 NSA-Crostic No. 23; Salemme A.J.
Apr 79 NSA-Crostic No. 24; D.H.W.
May 79 NSA-Crostic No. 25; D.H.W.
Jun 79 NSA-Crostic No. 26; D.H.W.
Jul 79 NSA-Crostic No. 27; D.H.W.
Aug 79 NSA-Crostic No. 28; D.H.W.
Oct 79 NSA-Crostic No. 29; D.H.W.
Jan 80 NSA-Crostic No. 30; D.H.W.
Apr 80 NSA-Crostic No. 31; D.H.W.
Jan 81 NSA-Crostic No. 32; D.H.W.
Apr 81 NSA-Crostic No. 33; D.H.W.
Oct 81 NSA-Crostic No. 35; D.H.W.
Nov 81 Cryptic Crossword; [redacted]
Dec 81 NSA-Crostic No. 36; D.H.W.
Jan 82 NSA-Crostic No. 37; D.H.W.
Feb 82 NSA-Crostic No. 38; D.H.W.
Mar 82 Cryptic Crossword; [redacted]
Mar 82 Letter: Strangest Bust of the Month; Dibben A.
Apr 82 NSA-Crostic No. 39; D.H.W.
May 82 Bust Answer; [redacted]
May 82 NSA-Crostic No. 40; D.H.W.
Jun 82 NSA-Crostic No. 41; D.H.W.
Aug 82 NSA-Crostic No. 42; D.H.W.
Oct 82 NSA-Crostic No. 43; D.H.W.
Nov 82 NSA-Crostic No. 44; D.H.W.
Dec 82 NSA-Crostic No. 45; [redacted]

Qualifiers
Nov 76 Clarity, Thy Name is Qualifier; Mollick J.J.

Radio Electronic
Jun 79 [redacted] M.R.

Radio Fingerprinting
Apr 80 AIT; [redacted]

RAGPIE
Jan 78 But Why Do We Do It?; [redacted]

RAPIDTRAN
Jul 75 RAPIDTRAN: [redacted]

Readiness
Jul 79 Naval Readiness: A Basis for Comparison; [redacted]

Reference Aids
Sep 77 JPRS Language Reference Aids; Spiegelthal E.S.

Reflections
Nov 74 Reflections on a Translator's Conference; [redacted]

P.L. 86-36

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

P.L. 86-36

EO 1.~~4(c)~~
P.L. 86-36

P.L. 86-36

Jan 79 Reflections and Recommendations; Filby V.R.

Reminiscences
Mar 77 A View of the Central Computer Complex in the Late 1970s and Early 1980s; Phillips C.J.
Apr 81 The Poet's Corner;
Aug 82 I Remember; [redacted]
Nov 82 An Old Timer Is One Who; [redacted]

Reporters
Aug 74 Calling All SRAs! -- SRA Symposium; [redacted]

Reporting
Aug 74 A Spot by Any Other Name; Filby V.R.
Oct 74 Letter: [redacted] Article: [redacted]
Apr 75 Oral Reporting: A New Challenge for NSA; [redacted]
EO 1.4.(c) Jun 75 Letter: Volenick Article; [redacted]
P.L. 86-36 Dec 77 [redacted]
Jan 78 Letter: [redacted] Article: [redacted]
Sep 78 A Matter of Style; [redacted]
Jan 79 Reflections and Recommendations; Filby V.R.
Nov 81 Futuristic Reporting; [redacted]

Resources
Sep 77 Knowledge Resource Management at NSA; [redacted]
Apr 78 Accentuate the Negative; [redacted]

Reutilization
Oct 79 Another Source; [redacted]

Russian
Sep 74 Language in the News; [redacted]
EO 1.4.(c) Oct 74 The [redacted] Exercise: A Case Study
P.L. 86-36 in Special Research Analysis; Filby V.R.
Nov 74 Purity of the Russian Language-- Slavophiles vs. Westernizers; [redacted]
Feb 75 Review of 'Guide to Russian Technical Translation' by Salemme; [redacted]
Mar 76 To Pull a 'Ponyal'; [redacted]
May 76 COMINT in the Russian Navy, WWII; [redacted]
Apr 77 Some Thoughts on the Russian PQE; [redacted]
May 77 Why Are These People Smiling?; [redacted]
Jun 77 Letter: Clark Article; [redacted]
Jun 77 Old Russian Manuscript Ciphers; [redacted]
EO 1.4.(c) Sep 77 [redacted]
P.L. 86-36 D.L.
Nov 77 Backing into Language Acquisition; [redacted]
Dec 77 Letter: [redacted] Article [redacted]
Jul 78 I Remember SPELLMAN; Salemme A.J.
Feb 79 In Defense of The Indefensible: Notes on the Russian PQE; Tetrault E.W.
Jul 79 Gears of the Mouth; [redacted]
Jul 79 Russian Handbook of Spoken Usage, Vol 3;
Apr 80 Help Wanted; Engle T.L.
Apr 81 Grading The Russian PQE; [redacted]
Jan 82 Letter: Delaney Article; Chauvenet L.R.

Satellites
Nov 75 [redacted]
W.L.
Jan 78 An Early NSA Proposal for Satellite Remoting; [redacted], Nolte W.M.

P.L. 86-36

Screening Radiation
Aug 79 Letter: Screening Radiation; [redacted] W.E.
Aug 79 Letter: [redacted] Letter (Aug 79); [redacted]

SCREENWRITER
Mar 78 A Linguist Looks at the Tube; [redacted] R.S.
Apr 78 Letter: [redacted] Article; 'Fennwatcher'

SDO
Dec 81 Sleep Well: Your SDO Is On Duty; Sawyer E.L.

P.L. 86-36

Secure Communications
Jun 75 The Navajo Code Talkers;
Jun 79 The Baltic Encoders; Reiskis A.

Security
Apr 77 The 'Ice Age' and International Security; [redacted]
Jul 77 Letter: Westwood Article; [redacted]
Jul 79 Source Protection: Our Agency's Insurance Policy; [redacted]
Dec 81 Sleep Well: Your SDO Is On Duty; Sawyer E.L.

Self-Paced Instruction
Aug 74 Self-Paced Instruction: The Future is Now!; [redacted]

P.L. 86-36

SIGINT
Feb 76 How Do We Know It's True?; Filby V.R.
Apr 76 On Being Truthful; Gaddy D.W.
Oct 76 More Thoughts on 'Questionable' SIGINT; [redacted]
Oct 76 Russian SIGINT and Electronic Warfare; [redacted]
Jun 77 SIGINT Welcomes INKSTAND; [redacted]
Oct 77 Partners in the Exciting Future of SIGINT; Rosenblum H.E.
Nov 78 Cast a Double Shadow: The Trojan Horse of SIGINT; [redacted]
Apr 79 COMSEC/SIGINT Relations; Boak D.G.
Dec 81 Exercise Support; [redacted]
Mar 82 A Historian Looks at SIGINT; Filby V.R.

SIGINT 1990
Sep 82 SIGINT: 1990, Part One; [redacted]
Oct 82 SIGINT: 1990, Part Two;
Nov 82 SIGINT: 1990, Part Three; [redacted]

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

EO 1.4.(c)
P.L. 86-36

SIGINT 80s
Jan 81 SIGINT In The 80s: Two Views; [redacted] Lutwiniak W.

SIGINT Alert
Dec 78 [redacted]

SIGINT Exploitation
Apr 78 SIGINT Exploitation, 1990; [redacted]
Jul 78 Letter: [redacted] Article; Gurin J.

SIGINT Handbook
Jan 75 The SIGINT Users' Handbook or: What's an ISHTAR?; [redacted]

SIGINT Reporting
Aug 76 Initiatives in SIGINT Reporting; [redacted]

SIGINT Summary
Mar 77 More about the NSA SIGINT Summary; [redacted]
Jun 77 More about More about the NSA SIGINT Summary; Boucher M.J.

Signals Processing
Oct 74 The Mission of the Signals Processing Requirements Panel; [redacted]

Signs
Jun 79 Sign Language;

SIMP
Jun 75 Golden Oldie: SIMP Tables;

Software
Nov 75 DESKPAD: A Programmers's Tool; [redacted] H.
May 78 The Joys of UNIX; D'Imperio M.E.
Nov 78 Formatting PL/1 Source Code: [redacted] K.J.
Feb 82 Software - AAAS, 1982; [redacted]

SOLIS
Dec 78 How Do You Spell Peking?; [redacted]
Dec 78 [redacted]
Jan 79 SOLIS: A Vehicle in Search of an Engine; [redacted]
May 79 Chapenko, Shapenko: What Difference Does It Make?; [redacted]

SOLITS
Nov 75 In Praise of SOLITS; Grant L.G.

Soviet
Aug 75 Processing [redacted] Communications; [redacted]
Nov 75 [redacted] W.L.
Dec 75 The Great Soviet Shipbuilding Mystery; Williams D.H.
Jan 76 63 Days--The Soviets in Space; [redacted]
May 76 A Soviet View of NSA; [redacted] J.
Oct 76 Russian SIGINT and Electronic Warfare; [redacted]
Oct 76 Work Quotas for Soviet Translators; [redacted]
Nov 77 [redacted]
Feb 78 Soviet Navy Command Post System; [redacted]
Jul 78 The Soviet General Staff; [redacted]
Sep 78 [redacted]
Sep 78 Soviet COMINT and the Civil War; [redacted]
Apr 80 [redacted]

Space Program
Jan 76 63 Days--The Soviets in Space; [redacted] J.
Dec 76 Apollo-Soyuz Test Project; [redacted] J.E.
Sep 78 [redacted]

Spanish
Aug 74 The Language of Beisbol in Everyday Talk; [redacted] Santiago-Ortiz R.A.
Sep 74 Language in the News; [redacted]
Jan 75 The Case for COMINT Readers; [redacted] H.G.
Aug 77 Telling It Like It Is; Santiago-Ortiz R.A.

Special Research
Dec 76 Why Can't They Design a Good SR Test?; Bjorklund K.

Spelling
Jun 77 Vich Iss R-r-right?; A.J.S.
Dec 78 How Do You Spell Peking?; [redacted]
Dec 78 [redacted]
May 82 Letter: Plaintext; [redacted]

SPELLMAN
Jun 78 Never Again!; Gurin J.
Jul 78 I Remember SPELLMAN; Salemme A.J.
Sep 78 Letter: Salemme Article; Williams D.H.
Oct 78 More B.S. (Before Spellman); [redacted] C.H.
Feb 79 P.S.; [redacted]
Jul 79 Shootout at the SIGINT Corral; [redacted] P.S.

Spread Spectrum
Jun 82 Amateur Spread Spectrum; [redacted]

SRA
Aug 74 Calling All SRAs! -- SRA Symposium; [redacted]
Oct 74 Letter: Sapp Article: [redacted]
Oct 74 The [redacted] Exercise: A Case Study in Special Research Analysis; Filby V.R.

P.L. 86-36
EO 1.4.(c)
P.L. 86-36

~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

P.L. 86-36

Sep 77 Whither the SRA?;

SRI
Apr 77 Flash! 115th SRI Located!; Salemme A.J.

EO 1.4.(c)
P.L. 86-36
Feb 78

Swahili
Sep 74 Language in the News;

SYMBIOSIS
Jun 75 Project SYMBIOSIS; 'Anon.'

System Design
Jun 77 Human Factors and Systems Design: An Estranged Relationship?;

System Development
Mar 82 Towards Better System Development;

T-Vision
Jan 79 T-Vision: The Reference Analyst's Medium of the Future;

Tale
Sep 74 Golden Oldie: King Eusyb and Queen Deodi;
Oct 81 The Stairwell Society;
Jan 82 Letter: Stairwell Society Article;

Target Location
Jun 78 Golden Oldie: Unidentified Unit at Unknown Location;

TDY
Jan 82 All The Alligators Aren't On Sport Shirts;

Teaching Methodolgies
Jul 77 The Transcription Skill: Concepts and Teaching Methodologies;

Technical Exercises
Sep 77 'Simonoff Says!'; A.J.S.

Technical Information
Jun 79 The Story of MOSES;

Technical Manual
Nov 74 Guidesmanship--or How to Write Technical Manuals Without Actually Giving Anything Away;
Mar 77 Revised Technical SIGINT Manual in Preparation; Filby V.R.

Technical Support
Oct 81 Technical Support Catalogs; K.J.

Telemetry
Jun 76 Computers In The ELINT and Telemetry Business;
Nov 77

P.L. 86-36

Telephone
Apr 78 Telephone Problem Here;
Mar 82 A Brief Treatise on Five Laws of Telephonic Communications; Nolte W.M.

Telex
Jan 75 UNNA,

EO 1.4.(c)
P.L. 86-36

Terminology
Aug 74 A Spot by Any Other Name; Filby V.R.
Nov 74 Data and Definitions: Calling Things by Their Rightful Names;
Aug 79 An August Baudy;
Nov 81 Say What You Mean; Gaddy D.W.
Jan 82 Data Field Naming/Coding Conventions at NSA;

P.L. 86-36

TEXTA
Aug 74 TDB: The TEXTA Data Base; Jackson W.J.
Nov 76 TEXTA 'Word Seek';
Jul 78 Ye Gads! Another Country Trigraph System;
Oct 78 Letter: rticle; Pattie M.T.
Dec 81 TEXTA: What Is It? Where Is It Going?;

Sep 77 The Seminar Program; W.L.

Third Party
Apr 81 Third Party Relationships;

Jul 77 Buck S.H.

EO 1.4.(c)
P.L. 86-36

TIDE
Dec 81 TIDE: A Brief History;

Time Usage
May 82 Human Factors Corner: Data Gathering, How Do We Spend Our Day?;

TIPS
Sep 76 TIPS is Still Alive and Well;

Traffic Analysis
Aug 74 The New Traffic Analysis Glossary;
Sep 74 Gary's Colors; Garofalo C.A.
Dec 74 An Approach to Callsign Analysis;
Apr 75 A Comm Change at Ramasun Station;
May 75 TA, Handmaiden of CA; Mason F.O.
Jun 75 More on Squaring the Page (A Crypto-TA Function); Mason F.O.
Aug 75 Abdul and His 40 Tanks; Mason F.O.

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

EO 1.4.(c)
P.L. 86-36

Aug 75 Processing [redacted]
Communications; [redacted]
Oct 75 Automation of a TA Process; Murphy T.
Nov 76 How to Make a Railroad Disappear;
[redacted]
Jan 77 Letter: Mason Article; [redacted]
Apr 77 Letter: Mason Article: Boucher M.J.
Apr 77 Letter: Mason Article; [redacted]
Apr 77 Letter: Mason Article; McGrillies J.R.
May 77 A Story With a Moral; [redacted]
Jun 77 Letter: Mason Article; [redacted]
Oct 77 Which Numbering System Should We Use?;
'Asken'
Nov 77 A Little TA Problem; [redacted]
Dec 77 [redacted]
Feb 78 Collection-Support TA is Not for
Everyone; [redacted]
Apr 78 Telephone Problem Here; [redacted]
May 78 TA Implications of FCC Proposal:
[redacted]
Sep 78 [redacted]
[redacted]
Nov 78 A Small Problem; [redacted]
Jan 79 Second Sighting; 'Donym'
Mar 79 Let's Not Lose Our TA Skills; [redacted]
G.
Apr 79 A Somewhat Larger Problem; [redacted]
W.E.
Jun 79 Letter: [redacted] Article; Bjorklund K.
Jun 79 Traffic Analysis of the Future;
[redacted]
Jul 79 Letter: Bjorklund Letter (Jun 79);
Broglie E.F.
Jul 79 Letter: Bjorklund Letter (Jun 79);
Buckley D.
Aug 79 Letter: Buckley a [redacted] (Jul 79);
[redacted]
Jan 80 There's a New World Coming - Are You
Ready?; [redacted]
Feb 82 Golden Oldie: Simplicity in Color;
Garofalo C.A.
Mar 82 Letter: A Toy Problem; Tiren D.J.
Apr 82 Golden Oldie: Tracks in the Sands of
Time; Mason F.O.
May 82 A History Lesson; [redacted]
May 82 True Base: Two Tales [redacted]
Jun 82 A Personal Footnote;
Jun 82 Golden Oldie: Reporting Message
Volumes; [redacted]
Oct 82 Answer: An Old Problem; [redacted]

Traffic Analysts
Aug 76 Integrated Analysts for Asia; [redacted]
W.D.
Jan 77 Letter: 'Firebrand' Letter on [redacted]
Article; [redacted]
Apr 77 Letter: [redacted] Article; [redacted]
Apr 77 Letter: [redacted] Article;
Jul 77 Letter: [redacted] Article;
Jul 77 Letter: [redacted] Article;
Oct 77 Golden Oldie: Analyzation of Data:
Curtin R.
Mar 79 Attention Military Traffic Analysts;
Apr 80 A Traffic Analyst Looks at Computers;
[redacted]

Apr 81 Traffic Analysis: Specialty Without
Portfolio; [redacted]

Training
Aug 74 Self-Paced Instruction: The Future is
Now!; [redacted]
Nov 74 New Trends in the Teaching of
Cryptanalysis; [redacted]
Apr 76 How Do Adults Learn Language?;
[redacted]
May 76 Hypnosis and Self-Hypnosis in Language
Learning; [redacted]
Nov 77 Backing into Language Acquisition;
[redacted]
Dec 77 What Made Them Do It? (Language Self-
Study); [redacted]
Dec 78 Agency Summer Language Study: [redacted]
D.
Jun 79 Teaching Computer Science To
Linguists; [redacted]
Oct 79 NCS Summer Language Program;

Transcriber Analyst
May 79 Transcriber-Analyst Relations; Miller
D.E.

Transcription
Mar 76 To Pull a 'Ponyal'; [redacted]
Apr 76 Computer-Aided Transcription of
[redacted]
May 77 Why Are These People Smiling?;
[redacted]
Jul 77 Which Tape Has the Intelligence?
Project [redacted] Gurin J.
Aug 77 Telling It Like It Is; Santiago-Ortiz
R.A.
Jul 78 I Remember SPELLMAN; Salemme A.J.
Oct 78 You Can't Tell the Wheat from the
Chaff Without a Program; Gurin J.
May 79 Run This Through Your Transcription
Machine; [redacted]
May 79 Where Do Good Transcribers Come From?;
[redacted]
Oct 79 The 2000-Year-Old Transcriber;
[redacted]

Translation
Feb 75 Review of 'Guide to Russian Technical
Translation' by Salemme; [redacted]
Jul 75 RAPIDTRAN: [redacted]
[redacted]
Mar 76 A Comparison of NSA and ATA
Certification Standards; [redacted]
Jun 76 Notes on Translation from the Chinese;
[redacted]
Sep 76 Semantic Voids: Don't Shoot the
Translator; Mason D.
Nov 76 How to Make a Railroad Disappear;
[redacted]
Apr 77 'It's Got to Get Out Today!'; Blank F.
Nov 77 What Ever Does 'However' Mean?;
[redacted]
Apr 78 ATA Letter to President Carter;
Tinsley R.L.
May 78 Uncle-a Sam Wantsa You!; [redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

P.L. 86-36

Jul 78 Has It Ever Been Translated Before?:
Nov 78 Letter: Article;
Jul 79 Gears of the Mouth; Lasley D.
Jul 79 Seminar on Translation Problems:
Jan 81 Translator In Your Pocket;
Aug 82 Linguist Machine;

Translation Grading
Mar 76 An Objective Approach to Scoring Translations;
Aug 76 NSA's System for Grading Translations;

Translator
Aug 74 Nice Busman's Holiday for One NSA Employee; Dudley B.
Nov 74 Reflections on a Translator's Conference;
Oct 76 Work Quotas for Soviet Translators;
Nov 76 Golden Oldie: The Things They Say; Miller D.E.
Jul 78 Is A Translator a Professional?;
Jan 79 W.W.II Japanese Translation at Arlington Hall Station;

Transliteration
Jun 76 Transliteration or Cyrillic?; G.
May 79 Chapenko, Shapenko: What Difference Does It Make?;

Trigraph
Jul 78 Ye Gads! Another Country Trigraph System;

Trivia
Jun 79 Letter: 'Sixth Language'; P.A.
Jul 79 Letter: Linguatrivia;
Apr 80 Geographic Trivia;

True Base
May 82 True Base: Two Tales;

TSS
Apr 82 Word Processing In A4;
Sep 82 TSS Revolution;

EO 1.4.(c) P.L. 86-36

Typewriter
Aug 75 Typewriter Random -- A New Look;
Oct 75 Letter: Typewriter Keyboard;

T Organization
Mar 78 Some Background on the C/T Merger; Smith F.
Sep 78 T Establishes Human Resource Development Panel;

ULTRA
Dec 75 A Personal Comment on Winterbotham's 'The ULTRA Secret'; Tiltman J.H.
Dec 75 Mum's Still the Word! ('The ULTRA Secret');
Dec 75 Weapon That Helped Defeat Nazis (Winterbotham's 'The ULTRA Secret'); Filby P.W.
Feb 78 More Beans; Filby V.R.
Oct 78 Feeding the Germans Misinformation (Book Review); Filby P.W.

UNIX
May 78 The Joys of UNIX;
Nov 81 How to Create A User-Unfriendly System:
Dec 81 In Pursuit of: Faster Horses, Younger Women, Older Whiskey and More Money; D.L.
Feb 82 Human Factors Corner: Some Advice to Users of Unfriendly System;
Feb 82 Letter: UNIX Article;
Oct 82 Human Factors Corner: Text Editors;
Oct 82 What's The Good (Pass)Word?:

UNIX How To
Mar 82 But Life Is Supposed To Be Hard; J.
May 82 Letter: Article;
Sep 82 More Free Goodies:

UNIX Shell
Apr 82 Shell Game;
May 82 Letter: Shell Game Article;
Jun 82 Letter: Shell Game Article; J.W.
Jun 82 Letter: Shell Game Article; P.A.
Jun 82 Loooong Shell;
Aug 82 Shell Game;
Nov 82 Letter: Shell Game Article;
Dec 82 Shell Game: AJSQUE;
Dec 82 Shell Game: Counter; W.E.S.
Dec 82 Shell Game: PWB WHEN;

UNNA
Jan 75 UNNA,

URSI
Dec 81 The 1981 URSI XX General Assembly;

UTENSIL
May 78 Project UTENSIL: The DDO Data Dictionary/Directory;

Validity
Dec 75 What Are We About? (Fragments, Figments, or What?);
Feb 76 How Do We Know It's True?; Filby V.R.
Apr 76 Letter: Comments on Letter on What Are We About?;
Apr 76 Letter: What Are We About? Article;
Apr 76 On Being Truthful; Gaddy D.W.
May 76 Some Principles of Cover and

P.L. 86-36

~~SECRET~~

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

Deception; [redacted]
Nov 76 Clarity, Thy Name is Qualifier; Mollick J.J.

Videocasette
Apr 81 DIA Videocasette Program;

Video Encryption
Jan 82 Video Encryption: A Report From EASCON 81; [redacted]

Vietnam
Feb 75 The Gulf of Tonkin Incident; [redacted] W.D.
Jul 75 Re-psychling the Code Clerk; [redacted]
Aug 75 Twenty Years of Transposition; [redacted] J.E.
Oct 75 1972-1973: A Vietnam Odyssey EO 1.4.(c) Stepp L.C., [redacted]
Oct 75 Computers, Comms, and Low-Grade Ciphers: [redacted]
Oct 75 NSA in Vietnam: Proud and Bitter Memories; [redacted]
Oct 75 One Chance in Three--But It Worked; [redacted]
Oct 75 The Danang Processing Center; [redacted] A.
Oct 75 The Do Xa Pads; Wiley E.
Oct 75 [redacted] F. EO 1.4.(c)
Jan 76 Leo in October; Murphy A.I.
Mar 76 Letter: Proud and Bitter Memories Article; [redacted]
Mar 76 Letter: Proud and Bitter Memories Article: [redacted]
Apr 76 One Day in Danang; [redacted]
Jun 76 Letter: Cameron's Article; Murphy A.I.
Mar 79 Pursuit of the [redacted] E.L.
May 79 Project HELIPAD: An Epitaph; [redacted] M.L.

EO 1.4.(c)
P.L. 86-36

VORD
Mar 79 VORD is a Better Idea; [redacted]

Voynich Manuscript
Aug 75 The Voynich Manuscript-Third Theory; Miller D.E.
Apr 76 The Voynich Manuscript Revisited; [redacted]

P.L. 86-36

WARC-79
May 78 Callsigns and WARC-79; [redacted]

Warnings
Dec 76 But It Looks Like the Real Thing; [redacted]
Mar 77 Letter: Bunker Interview; [redacted] H.L.
Dec 82 Development and Correlation of Indicators; [redacted]

WARSAW Pact
Jul 75 The Warsaw Pact [redacted]

EO 1.4.(c)
P.L. 86-36

[redacted] P.L. 86-36

Waveguide Analysis
May 76 Waveguide Analysis; [redacted]

Weasel Words
Oct 74 Golden Oldie: An Unofficial Glossary of Weasel Words;

Working Aids
Jan 75 The Case for COMINT Readers; [redacted] H.G.

Writing
Nov 74 Guidesmanship--or How to Write Technical Manuals Without Actually Giving Anything Away; Thal W.E.
May 77 Plain English; [redacted]
Aug 77 Let Me Repeat--And Make Myself Perfectly Clear: Jenks P.
Jan 78 The Joys and Frustrations of Plural-Dropping; A.J.S.
Dec 78 'No, No, Nanette!' Means Yes?; A.J.S.
Mar 79 Fairbanks on English; Fairbanks S.
Apr 79 More Fairbanks on English; Fairbanks S.
May 79 More Fairbanks On English; Fairbanks S.
May 79 More Than Words Can Say; Gurin J.
Jun 79 How Are Your Stamina?; Fairbanks S.
Jan 82 The Literary Bends; Murphy A.I.
Feb 82 Native Scripting of Languages; [redacted]
Mar 82 Letter: The Literary Bends Article; Murphy A.I.

P.L. 86-36

P.L. 86-36

[redacted]
Apr 78 Looking at Mr. [redacted],
[redacted]
Nov 78 A Dialogue Between Ms. User and Dr. Analysis; [redacted]

EO 1.4.(c)
P.L. 86-36

From: fma at stept03 [redacted]
Subject: SHELL
Reference: CRYPTOLOG, March 83, page 32

[redacted]

[redacted] T441, 963-5553

EO 1.4.(c)
P.L. 86-36

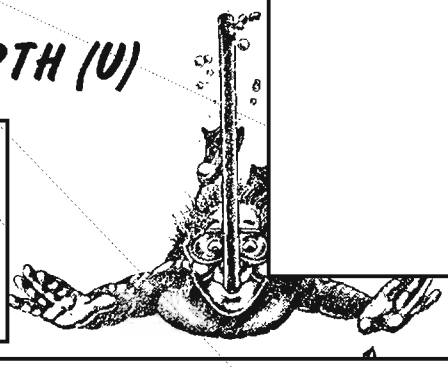
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4009861

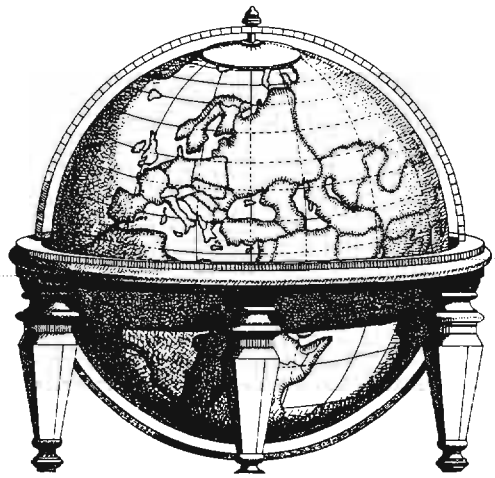
EO 1.4.(c)
P.L. 86-36

OUT OF MY DEPTH (U)



The Intelligence Watch Officer (U)

by [redacted] T52



P.L. 86-3

EO 1.4.(c)
P.L. 86-36

(U) Want an interesting job? Do you want to be busy--sometimes too busy to eat even when you've brown-bagged? If you are interested in current events and want to know what is going on in the world or what is going to happen next, you may be interested in the Intelligence Watch Officer (IWO) position in the National SIGINT Operations Center.

(U) The author served as Intelligence Watch Officer on Team 3 (P33) in NSOC from September 1981 to January 1983.

[redacted]

[redacted]

[redacted]

[redacted]

(U) If you are interested in more information on the Intelligence Watch Officer position in NSOC, contact T5, x3265s.

EO 1.4.(c)
P.L. 86-36

(U) During non-regular duty hours, the IWO acts for T5 in receiving and responding to requests for information from NSOC, field sites and 24-hour NSA work areas. The IWO attempts to answer all requests instead of referring them to a day shop for action. This frequently necessitates trips to the NSA Geography and Map Library, the Main Library, or to Central Research to research and retrieve a map or citation to answer the query. The IWO has a one-way pager to carry when away from NSOC for any length of time--he maintains constant contact with NSOC when necessary to receive new requests or operational requirements.

P.L. 86-36

Sir,

~~(C)~~ I would like to raise a "full glass" in a toast to [redacted] on his article concern-

[redacted]

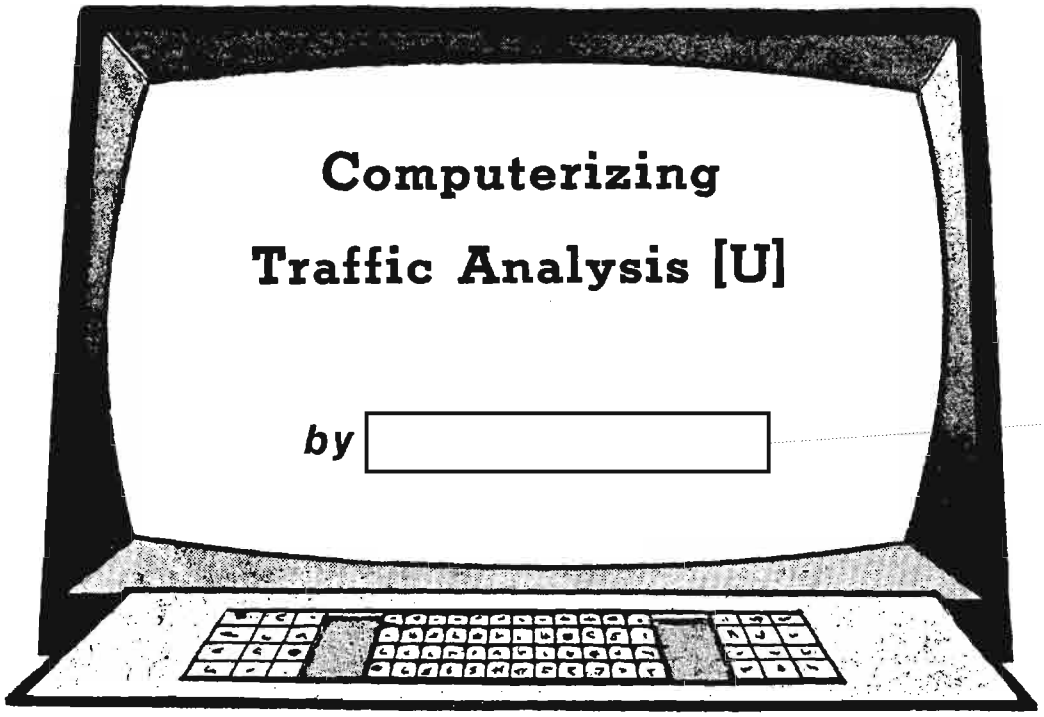
[redacted]

P.L. 86-36

[redacted]

EO 1.4.(c)
P.L. 86-36

OCID: 4009861



Computerizing Traffic Analysis [U]

by [redacted]

P.L. 86-3

(U) The traffic analyst finds himself turning to data systems because he often has mountains of data to examine, because the people who receive TA results usually want their information very rapidly, and because almost all the data the traffic analyst wants to see is already inside a computer somewhere.

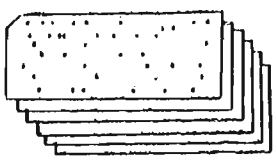
(U) Most traffic analysts who try to look at data systems develop a kind of schizophrenia. On the one hand, the TA data that comes in today has to be processed and analyzed today because there will be another batch of data coming in tomorrow. This means that the traffic analyst has to use today's data system to handle today's data. On the other hand, it does seem to us traffic analysts that data systems people would much rather talk about tomorrow's system--the one that isn't here yet, the one that won't have all these glitches and problems that today's system has.

(U) The traffic analyst who is in the trenches on a current operational problem would easily trade all the glowing promises of some brighter tomorrow for a quick fix on some of the glitches in today's system that will keep him from bleeding to death right now. That isn't my subject today--I really want to talk about the future. But as I thought about standing up here in front of all you data systems people, I couldn't resist putting in a plug for the working traffic analyst; he needs your help, both today and tomorrow.

This paper was presented at the November 1982 Meeting of CISI.

THE PROLOGUE IS PAST

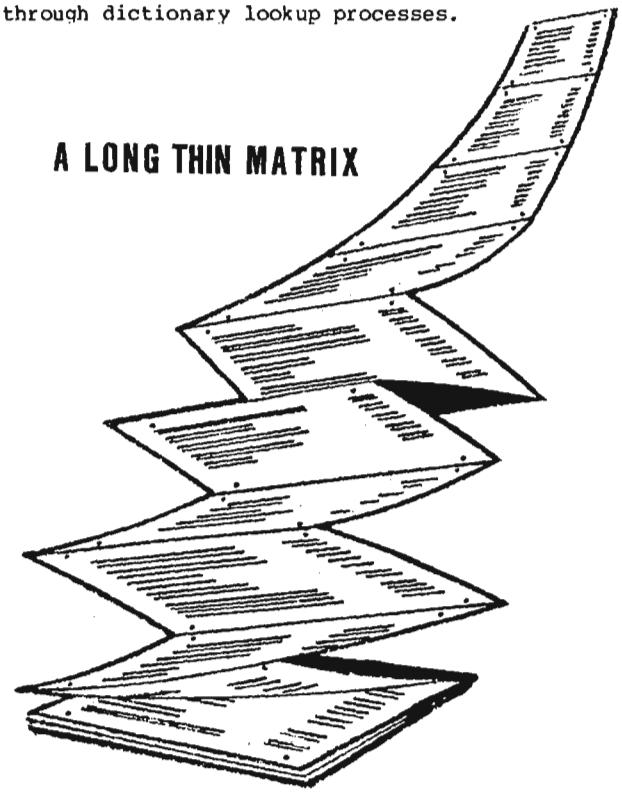
(U) I might be well to begin with a little history, or at least history as I remember it. My first recollection of what we now call data systems was a lot of 80-column cards and a card sorter. That was about 35 years ago. Watching those cards go through that sorter was rather hypnotic. The possibilities seemed limitless then--if we could only find a cheap and easy way to get the data onto the cards. I think the equipment was called Electronic Accounting Machines (EAM), and the people who supported the traffic analysts were called Methods Analysts (in the 1940s and early 50s).



(U) Since our data consisted of a matrix with 80 columns and many rows (one row for each card), our output consisted of that same matrix with its columns and rows transposed in some way. Later, we added the ability to look up words or strings in a dictionary and insert the result back into the matrix.

(U) Many years and computer systems later, in the mid-1960s, this was still the primary data systems support to traffic analysts: a transposed matrix (now often wider than 80 columns) with a dictionary lookup. There were attempts to go beyond this. Most of the things we tried were made to fit one specific problem, and never developed into general TA tools. We developed ponderous, monolithic record formats whose structure provided a special place for each variety of data we thought we would find in the traffic. What I remember most vividly are long, soporific meetings where all we ever seemed to talk about was what format the data was going to be in. We spent untold amounts of energy and resources getting all of our data into these unyielding, user-murky systems, and there was often little energy and resources left over to develop any user-friendly output.

(U) The result of this, in many areas, was that the output received by the traffic analyst was not much more than his original raw traffic, transposed both horizontally and vertically, and with some information added through dictionary lookup processes.



The form in which the output was delivered to the analyst was often decreed by someone remote from the analyst--someone who never had to actually live with the output--and it was rarely if ever changed to fit the current needs of the local problem or individual analyst.

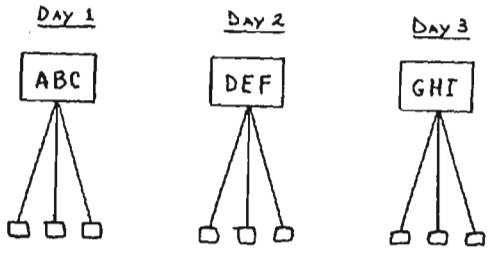
(U) It is still possible, even today, to see analysts sitting down with computer output and handlogging data from that computer output onto a form for their own personal use. In at least two areas, one might then see that same handwritten log being used a little later to punch cards for further computer processing!

WHAT IS THE TRAFFIC ANALYST TRYING TO DO?

(U) The traffic analyst is trying to draw a picture of his communications target. He usually wants this picture to show how his target looks when it is operating normally. Once he knows what his target's normal behavior is, then he is in a position to detect variations, and report them to intelligence consumers.

CONTINUITY

(U) Traffic analysts are usually looking for something they call continuity. When faced with a target that has daily-changing callsigns, the traffic analyst seeks to learn which of today's callsigns matches what callsign used yesterday.



CONTINUITY

DATE:	1	2	3	4
STN 1:	ABC	DEF	GHI	...
STN 2:	...	...		
...	...			

If I can say that the station that used callsign ABC on the first day is the same station that used callsign DEF on the second, then I can say that DEF (on the 2nd day) is continuity of ABC (on the 1st). On the third day, if I can say that GHI was used by that same station, then I can add GHI (on day 3) as another link in a growing chain of continuity. Many of our TA targets do change their callsigns, frequencies, addresses, and other features on a regular basis. They do it to

make collection and identification more difficult, and it is the job of the traffic analyst to defeat these changes by the development of continuity.

TWO KINDS OF TRAFFIC ANALYSIS

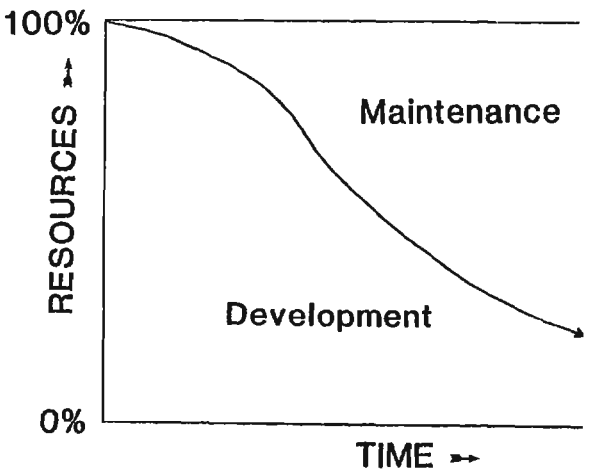
(U) There are two forms of traffic analysis on most problems: development and maintenance. To borrow an example from cryptanalysis, the attack against a cipher system often goes through two phases:

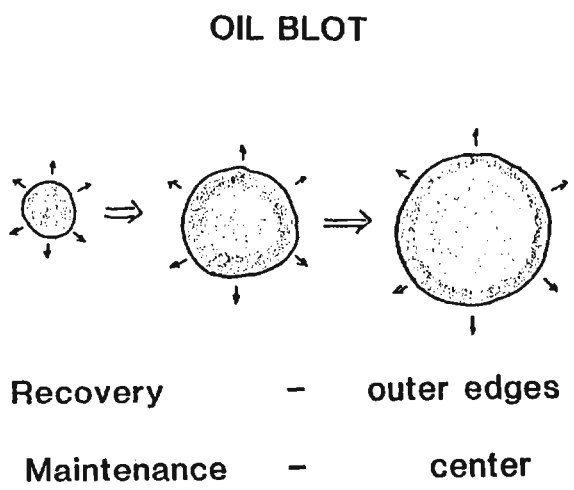
- [] first, diagnosing and recovering of the general cipher system, and
- [] second, exploiting and processing the recovered system, which often involves solving daily keys or settings.

So too, in traffic analysis, one can consider that there is a development (or recovery) phase and a maintenance (or exploitation) phase, which may or may not include product reporting. However, in traffic analysis, the two phases often occur at the same time.

(U) In some ways, the traffic analysis process resembles a spreading oil blot. Out on the edges, new target territory is being conquered; new target communications structures are being discovered and cataloged; new methods of identifying and distinguishing various communications are being developed. But back in the central part of the oil blot, the territories previously conquered must be kept track of; the continuity of target communications structures previously recovered must be maintained.

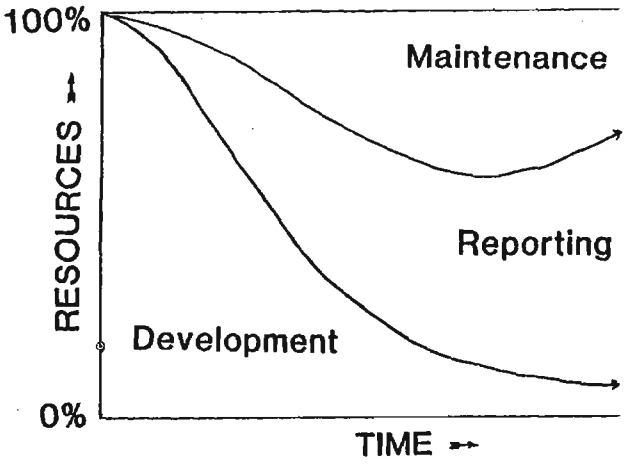
(U) The more territory one conquers, the thinner the center of the oil blot becomes. The more communications structures one recovers, the more continuities there are that now must be kept track of. As the maintenance effort grows, it will use more of the available resources, draining them away from the recovery part of the effort, and at some point it will have absorbed enough of the resources so that a point of "no growth" is reached and, for all practical purposes, recovery of new structures stops. If expansion doesn't stop, the center of the oil blot will break; if development doesn't stop, the maintenance effort will fall behind and begin to lose track of continuities, which will then have to be discovered and developed all over again. This tension over resources between maintenance and development is similar to the one between software maintenance and software development.





(U) Sometimes the personality of the manager plays a part in just where this point of "no growth" takes place. Some managers are more at home in the settled, stable atmosphere of the center, where things don't change much from day to day. These managers tend to concentrate their attention on building a smooth-running system at the center, and may put a larger proportion of their resources into that area, so that the "no growth" point is reached more quickly. Other managers thrive in the rough and tumble frontier atmosphere out on the edges of the problem, where each day is likely to bring some new and different challenge. These managers tend to concentrate their attention on the recovery effort, sometimes at the expense of the more humdrum maintenance.

DOCID: 4009861



REPORTING

(U) Some traffic analysis problems have a lot of potential for reporting--for providing the intelligence consumer with a blow by blow account of what the target is doing. Targets that involve ships and aircraft often have this potential because they move around from place to place, and the analysts often find much of their time taken up with reporting which ships and aircraft were active today, in what areas and performing what missions. Where this reporting potential is high, it tends to draw off resources from both development and maintenance. Managers whose problems have a strong reporting emphasis (especially time-sensitive reporting) will generally try to pull resources from development rather than from maintenance, because losing the continuities means losing the raw material for the reporting effort. Losing the development effort is generally seen as the lesser of two evils.

(U) As an aside, I should say here that the reporting side of traffic analysis is generally well ahead of the technical side in the use of computers. Since my primary interest in this paper is the working-level traffic analyst, I will be concentrating on the technical side, and I do not propose to discuss the reporting aspects of TA except as they touch on the technical side.

TRAFFIC ANALYSIS GOALS

(U) From the standpoint of the two kinds of traffic analysis--development and maintenance --we can express the general goals in the following ways:

TA DEVELOPMENT GOALS

(U) We rarely collect or analyze all of the communications of any given target. We are almost always working on a sample of the target. At any given time, there is some residue of the target that we do not maintain continuity on, and bits and pieces of that residue find their way into our unidentified or search pile--the file of incoming traffic which looks as if it belongs to our target but doesn't exactly fit any of our known continuities. Development TA concentrates on that pile, trying to dig out new target nets and continuities. This unidentified pile is almost like "background noise"; it is always there, whether we talk about it or not. If we are still growing (if the oil blot is still expanding), then our development goal is to dig more of the target out of the unidentified pile. If we have reached the "no growth" point, then our development goal is to be able to recognize and develop any new communications that the target might put on the air--communications that ought to stand out against the "normal noise" in the unidentified pile.

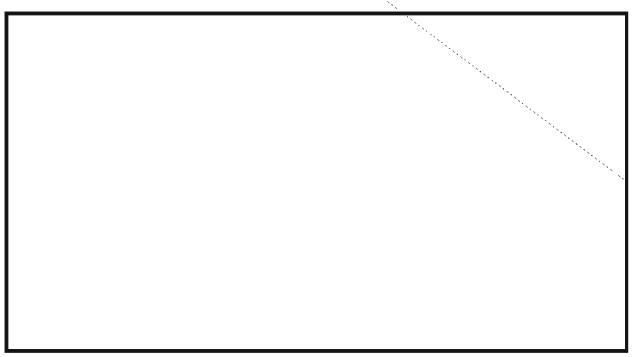
TA MAINTENANCE GOALS

(U) During the maintenance phase, we want to be able to hang on to the continuity that we have already recovered. We want to do this:

- [] to support whatever analysis efforts are currently engaged on the target (such as cryptanalysis, language, reporting, etc.), and
- [] to support whatever collection effort is working against the target.

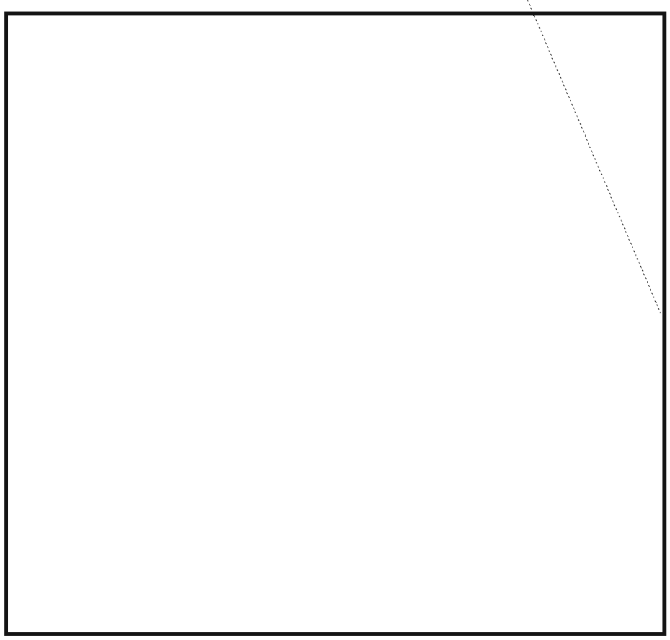
(U) To do the first support requirement properly, we need to be able to correctly distinguish and identify each of our continuities as the traffic arrives at the point of analysis, i.e., after it has been collected.

P.L. 86-36



HOW CAN COMPUTER POWER BE APPLIED TO THE TA PROBLEM?

~~(S-CCO)~~ In order to consider how the power of the modern computer might be applied to traffic analysis, we need to look at the model of TA that emerges from these two phases: development TA and maintenance TA. Although I have described them as if they were distinct and separate, they really ought to be thought of as a conjugate pair, because they tend to occur together on most problems. It is also possible for certain problems to be best described as a hybrid of these two forms: during the war in Vietnam, one out of every three pieces of intercepted traffic was unidentified, largely because of the rapidly-changing nature of the target. The point I want to leave with you today is that any attempt to provide the traffic analyst, either here in this building or anywhere in the world, with a Traffic Analysis Workbench System must reckon with the fact that the problem he is working will always be some mixture of these two forms of traffic analysis. We also need to consider that a TA problem can quickly change from one form to the other.



~~(C)~~ We decided to see if we couldn't find a way for computers to help us with the more stable maintenance problem. I remember spending several weeks laying out the logic and processes on the problem. And I remember being told, at the end of the project, that there wasn't nearly enough memory available to do what I needed.

	MAINTENANCE	DEVELOPMENT
Problem type:	continuity-keeping bookkeeping "Anything changed?"	continuity-seeking pattern searching "What's new?"
How dynamic?	slowly changing	rapidly changing
Foreknowledge:	high	low
State of solution:	~solved	~unsolved
Control:	semi-automatic	hands-on
Interaction:	human-efficient	human-intensive
Techniques:	target specific knowledge-based?	human specific "mix-n-match"
Worst case:	"below the salt"	start from scratch

A COMPARISON OF TWO FORMS OF TA

DOCID: 4009861

A COMPARISON OF TWO FORMS OF TA

(U) Let's look at these two forms of TA a little more closely. How do they compare when we look at them from the viewpoint of providing today's (and tomorrow's) traffic analyst with a computer support toolkit, while using a terminal workstation in an NSA worldwide networking environment?

(U) In development TA (the garrison communications in our example), we have a bookkeeping problem,

- [] where the emphasis is clearly on keeping track of a lot of known continuities;
- [] where we expect the changes in the target characteristics to be relatively modest;
- [] where the technical means of keeping up with the target (i.e., callsign and frequency systems, address tables, etc.) are largely solved or understood; and
- [] where we have good prospects of being able to project the appearance and behavior of the target from day to day.

(U) In development TA (the training communications in our example), we have a pattern-searching problem,

- [] where the emphasis is on sifting through masses of low-yield ore, looking for something that forms a continuity;
- [] where the next success may look nothing like the last one; and
- [] where the chances of finding that needle in the haystack may depend as much on the personality of the searcher as on the content of the haystack.

If we can't keep continuities, (i.e., are not able to), then the target stays in the development phase, no matter how much we know about it. Someone once said that TA continuities take either 95% of our resources, or 5%. That number may not be right, but the idea is. Being able to keep track of the continuities is the key to whether the problem is development or maintenance in nature. A daily-changing callsign system looks to us as if it is rapidly changing if we haven't solved the system, but once the system is solved, we then perceive it to be slowly changing. It is a matter of viewpoint.

(U) In maintenance TA, we work largely with what the target gives us. A package of techniques to grapple with a callsign system may work well enough on a problem where the callsigns are the key to our keeping track of continuity, but may be almost useless on another problem where the callsign system isn't solved and we must rely on other things, such as serial numbers or addresses.

(U) In development TA, on the other hand, a particular technique may pull one new structure out of the search pile and then never again find anything. The development analyst may need to continually devise new attacks and new methods; to him, the search pile is a featureless mass and it is his job to sort out the various pieces and find ways to distinguish one piece from another with some reliability.

(U) The maintenance TA problem probably needs a package that will

- [] look over the incoming material for the day;
- [] make reasonable guesses about continuities (including garbles);
- [] flash a warning light at the traffic analyst when things look very wrong or when it is confused by something; and
- [] provide a clean and readable summary of its results to the analyst for review.

It ought to keep up with both short-term and long-term trends, and should be especially attentive about "missing persons," portions of the target which haven't been seen for a while.

(U) The development TA problem, on the other hand, needs a toolkit that will provide the analyst with a range of diagnostic, computational, and pattern-searching techniques that can be brought to bear on the problem, in whatever mix the analyst needs at the moment.

WORST CASE

(U) I have shown what might be called the "worst case" for each of these forms of traffic analysis.

(U) In maintenance TA, one sometimes finds that a problem must somehow be worked, but that it has no real resources and not enough clout to get any. Now, in the best of all worlds, where everything is done right and for the right reasons, such problems should not exist. If a problem is worth working on at

all, it is worth the resources needed to get the job done. However, in the real world, those problems that are "below the salt" will always be working with whatever support they can beg, borrow, or scrounge. Providing a general package for such problems would pay for itself a hundredfold in the first few years. At the minimum, package needs to be able to "ring an alarm bell" when the target starts to disappear, or becomes more active, or changes in some other way.

~~(S-CCO)~~ In development TA, the worst case might be the situation where nothing is known. That is not as uncommon as some people might think. [redacted] When we pull together an analysis effort for a sudden war or brushfire, the analysts are usually drawn from other problems around the building; it would be nice if they didn't have to add "learning a new system" to all the other problems they will face on the new target. Therefore, the toolkit for such situations must be quite general and all-purpose.

TWO SYSTEMS OR ONE?

(U) What I have been describing so far may sound like two different systems, but what I am proposing is one system, with two parts. I have already said that these two phases or aspects of TA occur together, and I should add that on more than one problem, they are frequently done by the same people. New continuities are recovered by the development TA process, and then handed over to the maintenance TA effort to be kept track of. Information is often derived by the maintenance effort that will help the development effort. What the traffic analyst needs is one system that has enough flexibility for him to move whichever way his TA problem takes him. It would also be useful if the language we use is one that isn't going to change every few years because some equipment in the basement is being upgraded.

PINSETTER

(U) Several years ago, we began to work on the concept of a Traffic Analysis Workbench System, with the covername PINSETTER. Some of what I have described here comes out of that experience. PINSETTER has been described elsewhere, so I will not spend time on it here. However, I will share with you some of my personal conclusions about PINSETTER, especially those which seem to be pertinent to the future.

(U) There are aspects of traffic analysis which resemble word processing, and a good screen editor seems to go a long way toward putting the analyst in contact with his traffic, letting him rearrange it and touch up the rough edges and garbles the way he (the owner) wants them. It lets him look at the data before he decides what processing to apply to it. It also puts him in a good position to generate reports about his problem, especially the technical reports with technical data embedded in narrative text.

(U) A good toolkit, similar to UNIX and the PINSETTER extensions, is invaluable in providing the traffic analyst with the ability to tailor-make his own flexible processes for large scale manipulation of his traffic.

EO 1.4.(c)
P.L. 86-36

(U) Many of the practical results of PINSETTER, results that found their way into daily applications on specific targets, were not limited to traffic analysis. It became a regular occurrence to hear people from other cryptologic disciplines tell us that much of the UNIX/PINSETTER package for traffic analysts was what they needed, too.

PROBLEMS THAT NEED SOLVING

(U) Among the many problems that need to be solved, I would like to mention two. Both of these are areas that are critical to the future TA Workbench System.

ARCHIVES

(U) Some of our continuities form chains that stretch back to the end of World War II. One of the things that Data Systems people don't like to hear is that we need storage for data whose lifetime must be measured in years, and perhaps decades. Some years ago, there came a time when all of our incoming data went solely into the computers in the basement. It was the culmination of the dreams of a number of people: to take the raw traffic away from the analyst! I don't challenge that decision. It is history. But I must say that on many TA problems around the agency, there are no good records on our known continuities from that date forward, unless there were analysts still keeping some sort of hand records. The philosophy on most computer hosts is that any records not accessed within some period (usually a year or less) are taken off the system.

(U) Even if the data is put onto tape, the medium will deteriorate. Once on tape, the data is "out of sight and out of mind." The software that understands that data will sooner or later disappear or be "improved." Nevertheless, the analysts on that problem are still responsible for that period of time, and may still have to field questions about their

targets for that time period. So far, we have dodged this bullet, but sooner or later we will have to face the need for long term archives.

INFREQUENT USE OF PROCESSES

(U) The second problem involves the question of software that is only infrequently used. For example, suppose that one of our larger targets has a major communications change every five or six years. The effect of this change is so great that it interrupts intelligence reporting on that target until the new communications structures are understood and recovered. Each time the change occurs, an intensive effort is therefore mounted to recover our continuities in the shortest possible time.

(U) In the old days, when the special effort was over, everything was bundled up and packed away for retrieval when the next change came along. But how do we handle this now that we have modern data systems support? After five or six years, how much of the software is still useful? Chances are that the data base has been changed, as well as the host on which it resides.

(U) Another example might be the diagnostic techniques to attack a particular kind of callsign system. Once the system in question is solved, how should we preserve the software so that it doesn't need to be reinvented the next time such a system is encountered? Suppose we don't find a similar system for five, or six, or even ten years?

CONCLUSION

(U) I don't offer either my observations or my experiences as criticisms, but rather as areas of traffic analysis support which need to be solved. I have tried to avoid mentioning specific hardware or software, except as examples. A man named Bob Biles taught me long ago that users should never tell computer people what equipment to use.

(U) Perhaps traffic analysis has lagged behind other cryptologic disciplines in making full use of modern data systems. But that is changing, thanks to the patience, ingenuity, and hard work of many of you here today. I still keep a supply of pencils around, and I still have a pencil sharpener on my desk--but I have noticed that I don't really use them very much any more.

Dear Editor:

(U) In sympathy with countless NSAers who, through the years have been antagonized, baffled, challenged, demoralized, etc., by countless forms of human and machine language (not to mention the devil's own creation, governmentese), I propose that our new OPS Bulding 2A be christened--at least informally--"The Tower of Babel"!

JOHN J. MOLLICK, B41

[Editor's Note: In keeping with the tradition of naming the streets, auditoriums, etc., in the NSA complex after outstanding individuals, we could always claim that the building had been named after the late, lamented Mabel Babel (19??-1979), one of the Agency's foremost linguists, who spoke fluent governmentese as her native tongue. Her classic work, A Governmentese-English, English-Governmentese Dictionary (now out of print), is still the classic work in the field.]

Mabel Babel

P.L. 86-36

SOLUTION TO NSA-CROSTIC No. 46

[redacted] Memo from the Editor [of CRYPTOLOG to CRYPTOLOG's Puzzle Editor]

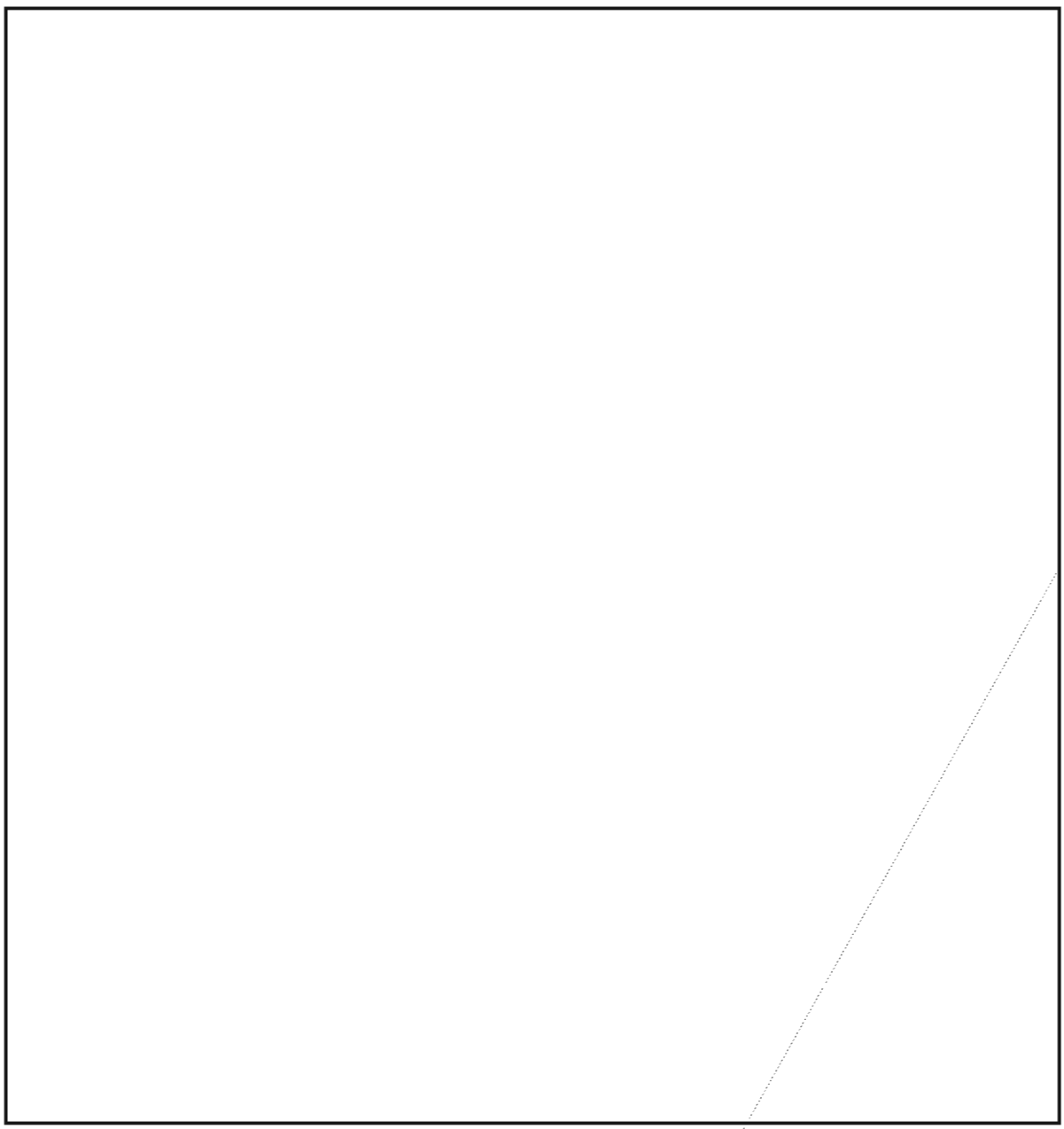
"Our Jan-Feb issue will be devoted to the CISI Essay Contest. It would be useful to have a puzzle that has data systems as a base, if you can find a suitable text. Also, I have been contemplating running an April Fool issue. You might be thinking about that..."

OCID: 4009861

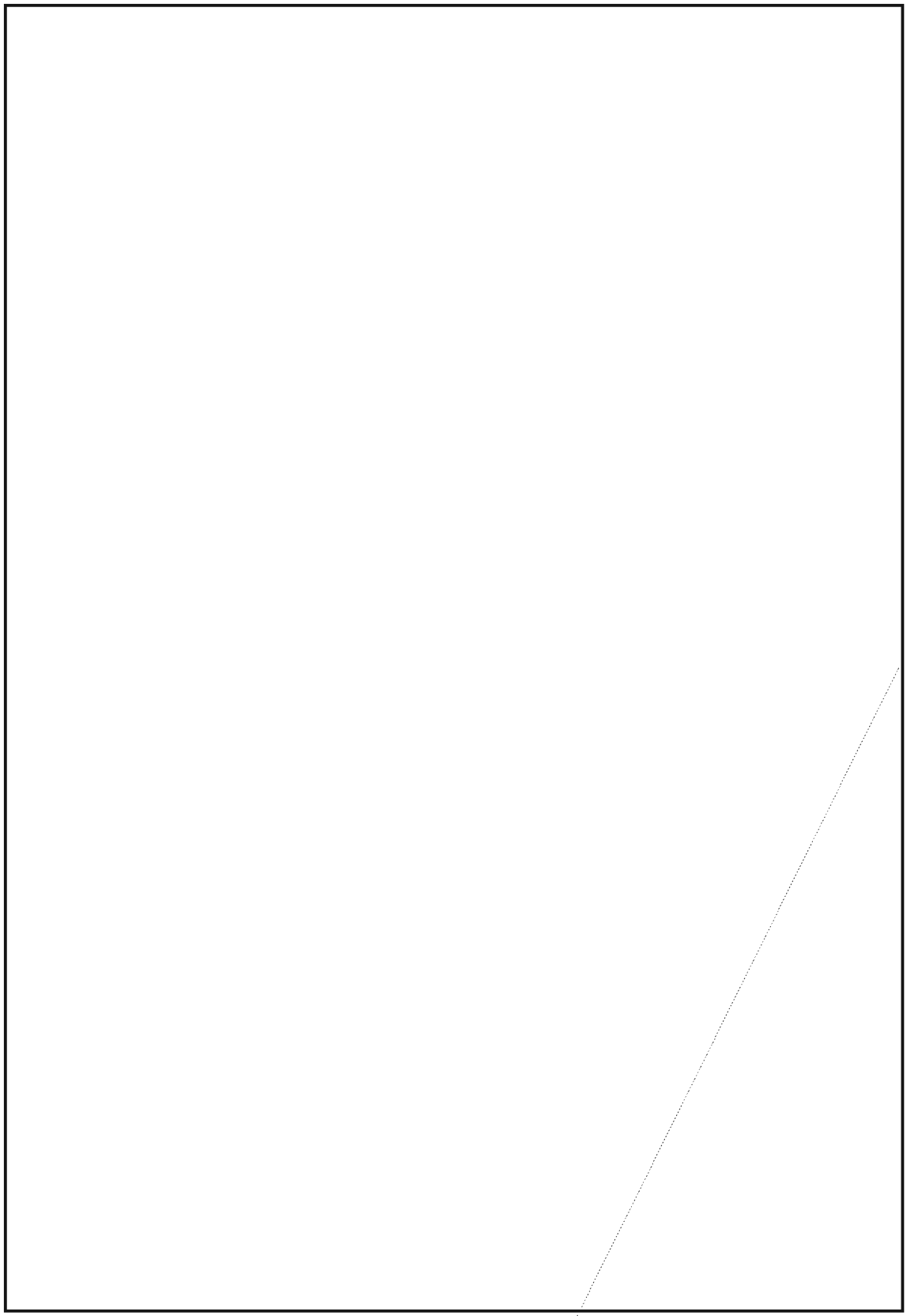
NSA-Crostic 47

by DHW

N.S. Norway (1889—1960) was an aeronautical engineer, active during the pioneer days of British aviation. He was also a prolific novelist. Many of his best works are set in the country which became his post-WWII home. Mr. Norway is Word V in this puzzle.

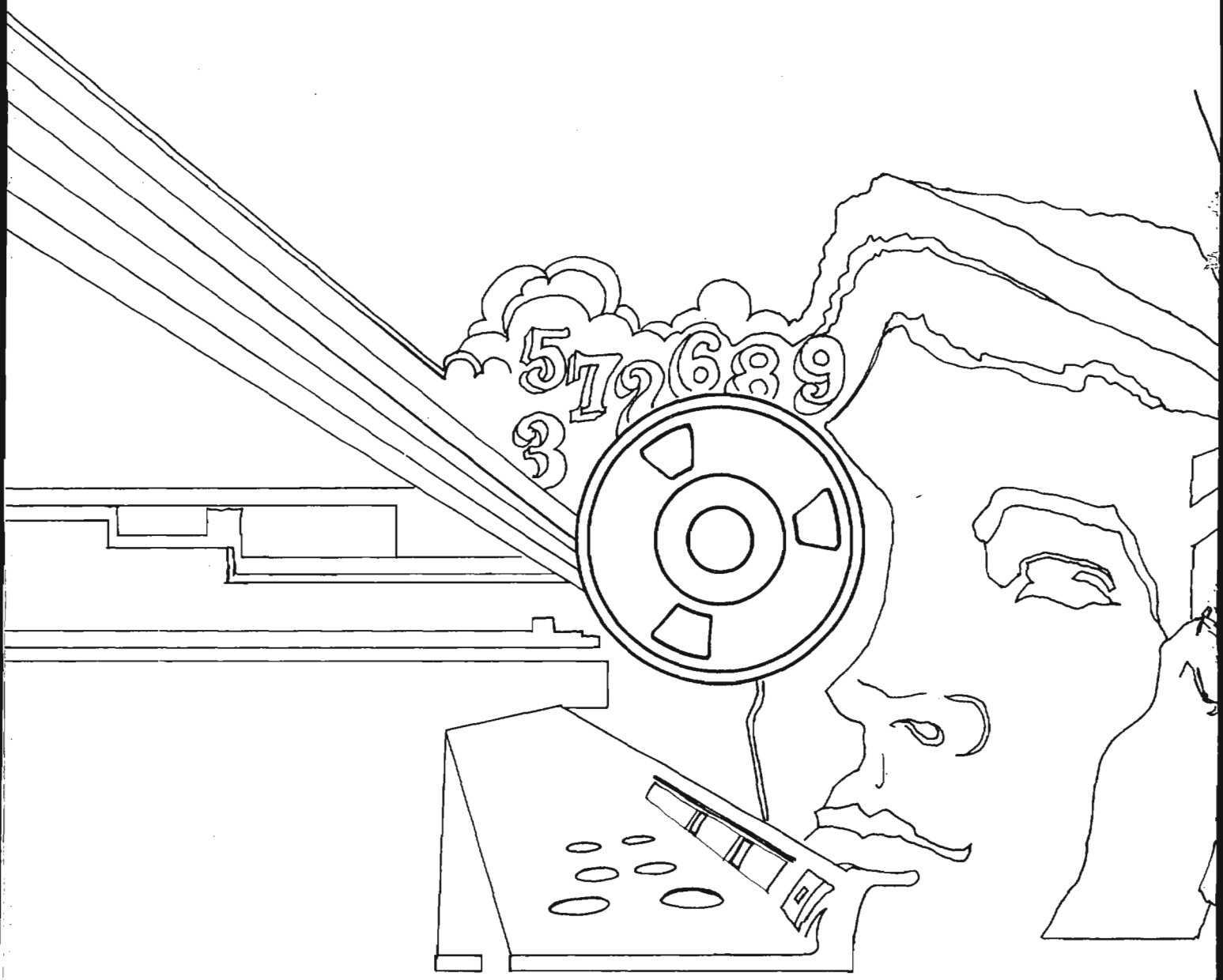


P.L. 86-36



P.L. 86-36

P1-AUG 83-83-35267


5 7 2 6 8 9
3

DOCID: 4019695

P.L. 86-36

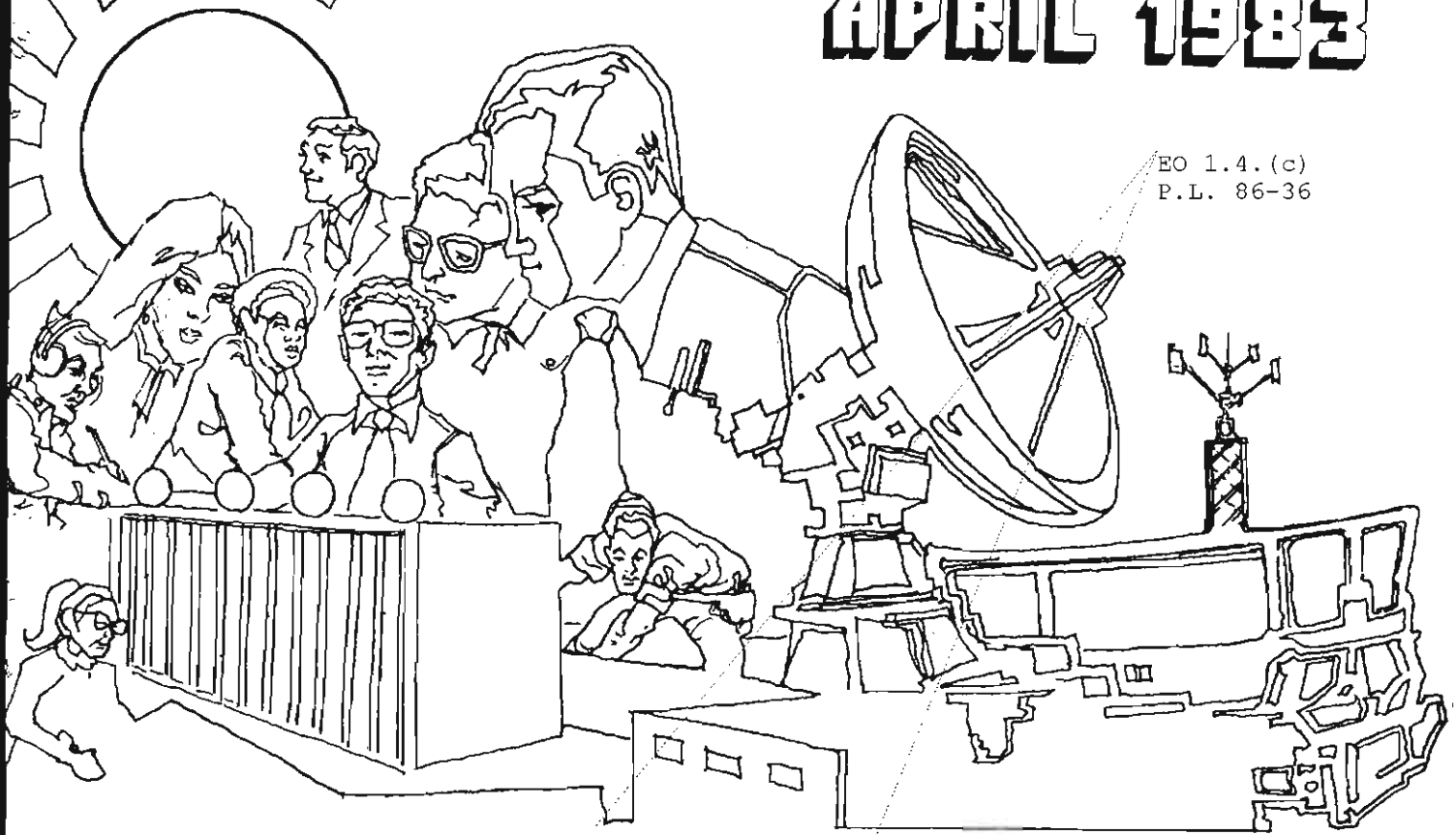
~~TOP SECRET~~

P16 [redacted]

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

APRIL 1983



EO 1.4.(c)
P.L. 86-36

UIS: USER INTERFACE SYSTEM (U)
PART ONE: CONCEPT (U) [redacted] 1
PART TWO: ARCHITECTURE (U) [redacted] 11
CUMULATIVE INDEX, PART TWO: TITLES (U) 19
GOVERNMENT OF THE PEOPLE, BY THE PARTY, FOR THE LEADERSHIP (U) [redacted] 30
SPECIFYING COLORS FOR COMPUTER GRAPHICS (U) [redacted] 37
[redacted] ..... [redacted] 39
[redacted] ..... [redacted] 48
NSA IN THE SPACE AGE (U) [redacted] 51
MY STAFF--IT COMFORTS ME (U) 'Zebulon Zilch' 55
WORD PEOPLE AT NSA (U) 'Dickson Airy' 59
NSA-CROSTIC NO. 46 (U) David H. Williams 60

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019695

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. X, No. 4 APRIL 1983

PUBLISHER [redacted]

BOARD OF EDITORS

Editor..... [redacted] (968-8322s)
Asst. Editor... [redacted] (963-1103s)
Production..... [redacted] (963-3369s)

Collection..... [redacted] (963-3961s)
Cryptolinguistics [redacted] (963-1103s)
Information Science
..... [redacted] (963-5711s)
Machine Support..... [redacted] (963-4953s)
Mathematics..... [redacted] (968-8518s)
Puzzles.....David H. Williams (963-1103s)
Special Research.....Vera R. Filby (968-7119s)

For subscriptions
send name and organization

to: CRYPTOLOG, P1
or call [redacted] 963-3369s

P.L. 86-36

To submit articles or letters
via PLATFORM mail, send to

cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no '0' in 'log')

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

The other day we saw a phrase that we haven't seen for a while: "paperless office." It was a popular term a while back, and was sometimes called the "paperless society." It was used to refer to that future day when all paper would be replaced by some other media, such as cathode ray tubes (TV) or other display devices.

Just to see if something was happening that we hadn't heard about, we took a stroll through the local supply room. The shelves were still filled with paper supplies, and with things that make marks on paper. Looseleaf notebooks seem to disappear from the shelves as fast as the supply folks can stock them. One can still hear serious debate about which brand of "white out" does the best job. Erasers, paper clips, rulers, IN (and OUT) baskets, sheets of press-on letters, scissors...the list goes on and on. Paper does not seem to be on the way out just yet. Not around here, anyway.

There is a growing sentiment that we will never reach that paperless state. It is not, after all, a question of technology. In a recent survey of computer editing systems, the authors finished with the somewhat guilty admission that, in the preparation of their report, they had consumed just under a mile of paper. We have no statistics to support it, but we have the distinct impression that we are using more paper per capita, not less.

New technology does not have to replace the old; it sometimes finds its niche alongside the old. Office automation seems to be aimed at getting machines to write down, on paper, what used to be written down by some other method, on paper. Some people think office automation will use more paper, not less.

The next time you wander through your favorite supply room, take a close look at the tiers of forms arrayed there. Do you think they will ever go away?

DOCID: 4019695

P.L. 86-36

by [redacted] T44

and [redacted] T44SA

UIS
USER INTERFACE SYSTEM

PART ONE: CONCEPT

by [redacted]

P.L. 86-36

The National Security Agency Scientific Advisory Board just published a Report on Networking Architecture which should be of special interest ~~(FOUO)~~ to you if you are a user of terminals and computers. It recommends that we develop an architecture which makes it possible to put effective access to data and computing within reach of every analyst who can use it. I would broaden that to include programmers, managers, technical staffs, and the hundreds--perhaps thousands--of people who deal with finance, training, travel, supply, and other essential support services both here and in the field. UIS (Users' Interface System) is that architecture and the subject of this talk.

~~(FOUO)~~ It seems to me that there are at least three questions worth asking about UIS:

- First, what is UIS? In many respects, this is the easiest question to answer and we will do that in the next hour.

- Second, why should you care about something called UIS, anyway? The answer is you shouldn't if you work in total isolation and don't have anything to do with what most of the Agency does. If, however, you--like most of us--have some part in the total information flow from collector to customer and believe--as I do--that there is still room for improvement in how you as a user access, handle, and process the information you deal with, then you have a vital interest in UIS.

A joint paper presented at the October 1982 Meeting of CISI.

- Third, what's a UIS good for? A couple of years ago we went all over the Agency and asked people what they thought they needed to do their job better or make their job easier. This is what UIS is all about and we will be talking much more about that, both in the next hour and in the weeks and months ahead.

~~(FOUO)~~ Let me digress for just a moment so that much of what I say later will make more sense. I happen to believe that the way we usually state our requirements for what we need is largely inadequate. We as users (and we're all users in one way or another) often have some specific end result in mind such as the way we want to see things on a screen, the way traffic should look when we get it, the processing steps needed to handle it, who gets it next, and so on. From talking with analysts in A, B, and G, I am convinced they understand and exploit the use of computers for their work very, very well. In other words, we have some pretty clear ideas about just what it is we do today, what we need to do it, and in many cases, what the hardware and software ought to provide us to let us do more, or do it better. When we try to project our future needs, however, it is often with the mistaken idea that we should be able to specify and build a turnkey solution with the

DOCID: 4019695
P.L. 86-36

same degree of certainty--the "big bang" theory of building systems. Instead, we end up with a detailed specification of a changeable, uncertain, future need. We run into trouble because the system development process and the analytic process are very similar. They are both learning experiences: prototyping, testing hypotheses, and feedback are vital. We build upon the results of our experiences both successful and unsuccessful. It really is more of a process than an event. [redacted] described it well in his talk to CISI last May when he talked about the importance of prototyping and feedback--and the shortcomings of the requirements process--developing TSS software for analysts. [1]

~~(FOUO)~~ Somehow we have gotten into the practice of specifying requirements in global, abstract, artificial, functional, and sometimes meaningless terms when we attempt to fully define a solution "up front" to a problem we don't fully understand yet. The end result, I think, is that the system designer is often unclear about what he is trying to build and the user, the analyst, the customer, is unclear about what he is getting. The user thinks the screen is going to be formatted one way and the designer does it some other way because the requirement simply says there will be so many protected or unprotected fields of information, certain "functional" capabilities for manipulating the information, and perhaps a performance specification of some sort--all of which has little meaning in the only terms that count--namely satisfying the end user.

~~(FOUO)~~ Both the customer and the designer have done their best, given the requirements, and yet the result is not satisfactory.

~~(FOUO)~~ The best recent example of dealing with the right kinds of requirements in the right way is the A21 graphics project.

~~(FOUO)~~ To overcome the language barrier between analysts and systems designers, more than 1,500 mock-ups were constructed so there could be no doubt about what the analyst expected to see and what the designer expected to produce. There was a solid basis for building the system based on a common understanding of the specific desired end result.

~~(FOUO)~~ What does this have to do with UIS? We need to do more prototyping. We need to involve the user thoughout. We need to be building systems which readily adapt to changing needs--not ignore or refute them--or even worse, require the end user to continually adapt to a rigid system conceived years earlier. UIS is designed to change and adapt to change where it matters most: with the end user--with people. I am interested in the end result of UIS, which we are going to describe, and not in some abstract philosophical concept. I am going to be asking you to consider UIS in terms of your job as an analyst, a programmer, a manager, or whatever. I am going to invite you to offer any suggestions you might have now or later and I hope you will want to work with us as we begin to develop UIS and make it real. I would ask you to think in terms of end results--in the most practical terms that you can of what you really need and how you would like to see it work.

~~(FOUO)~~ By the end of this century we will have a complex network of people, computers, and communications to do the SIGINT job and virtually everyone will be a part of it in

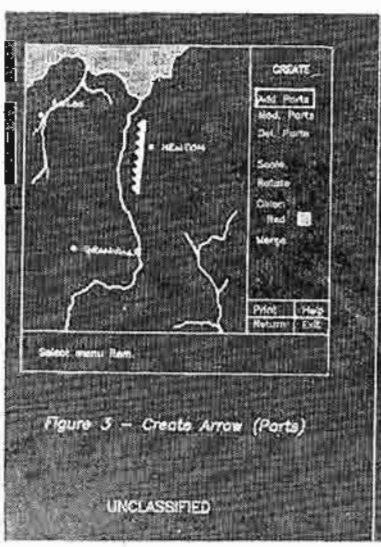


Figure 3 – Create Arrow (Parts)

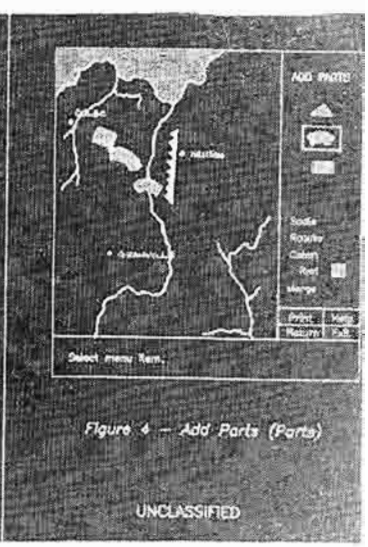


Figure 4 – Add Parts (Parts)

some way. UIS is the next vital step in the evolution that began with timesharing many years ago, continued with the development of the PLATFORM network and the GTSS/UNIX Terminal Subsystems, and the now-ubiquitous (almost) user terminal. The end of the century isn't that far off.

~~(FOUO)~~ Having set the stage, I will talk about UIS especially from the user's point of view (to the extent that I can) and [redacted] will talk about the UIS architecture itself (how it's glued together) and our plans for an actual prototype beginning this year.

P.L. 86-36

Goals, Definitions and Architecture

~~(FOUO)~~ UIS is the means of bringing closer to the user convenient, affordable, interactive, and personal access to the Agency's computing, communications, and data base resources.

~~(FOUO)~~ The stated "formal" goal of UIS is to enhance user productivity by providing timely delivery of information and immediate access to required data, computing, and human resources.

~~(FOUO)~~ Who is the UIS "user" anyway and what is his job? This model of the SIGINT data flow system contains many functions (except for the "support" functions I mentioned earlier), all of which are performed by what I consider to be potential UIS users.

~~(FOUO)~~ To place the UIS concept in perspective in relation to the flow of data through the Agency, this generalized model of the real-time SIGINT system (used by Mr. George Cotter in a recent CISI briefing) shows, in the horizontal direction, the flow of data from collectors to processors to product data bases to consumers and, in the vertical direction, the interaction of users with the data flow and the processors. NFAS (NSA Forwarding and Access System), the subject of a later briefing, is our networking architectture which is concerned with the horizontal axis of this model; UIS applies to the vertical direction.

~~(FOUO)~~ A blow-up of the right-hand portion of Mr. Cotter's model is a fair representation of the UIS architecture.

~~(FOUO)~~ Simplifying this diagram and putting other labels on the boxes produces an architectural model of UIS. [redacted] will treat this in more detail in his portion of the talk.

P.L. 86-36

Technology Issues

~~(FOUO)~~ UIS, in continuing the trend of the past decade to move data and processing power closer to the end user, will take advantage of state-of-the-art technology as it becomes commercially viable.

~~(FOUO)~~ The key to UIS--the personal computer--will soon have greatly increased computing power, internal memory, and disk storage capacity. Other devices included in UIS are graphics computers, word processors, and office automation equipment. (Throughout this talk I will intentionally use the term "personal computer" to include these variations.)

~~(FOUO)~~ Coupling this end-user power with networking and switching technology will place, under the direct control of the end user, the capability for him to control nearly all of his processing and data access requirements.

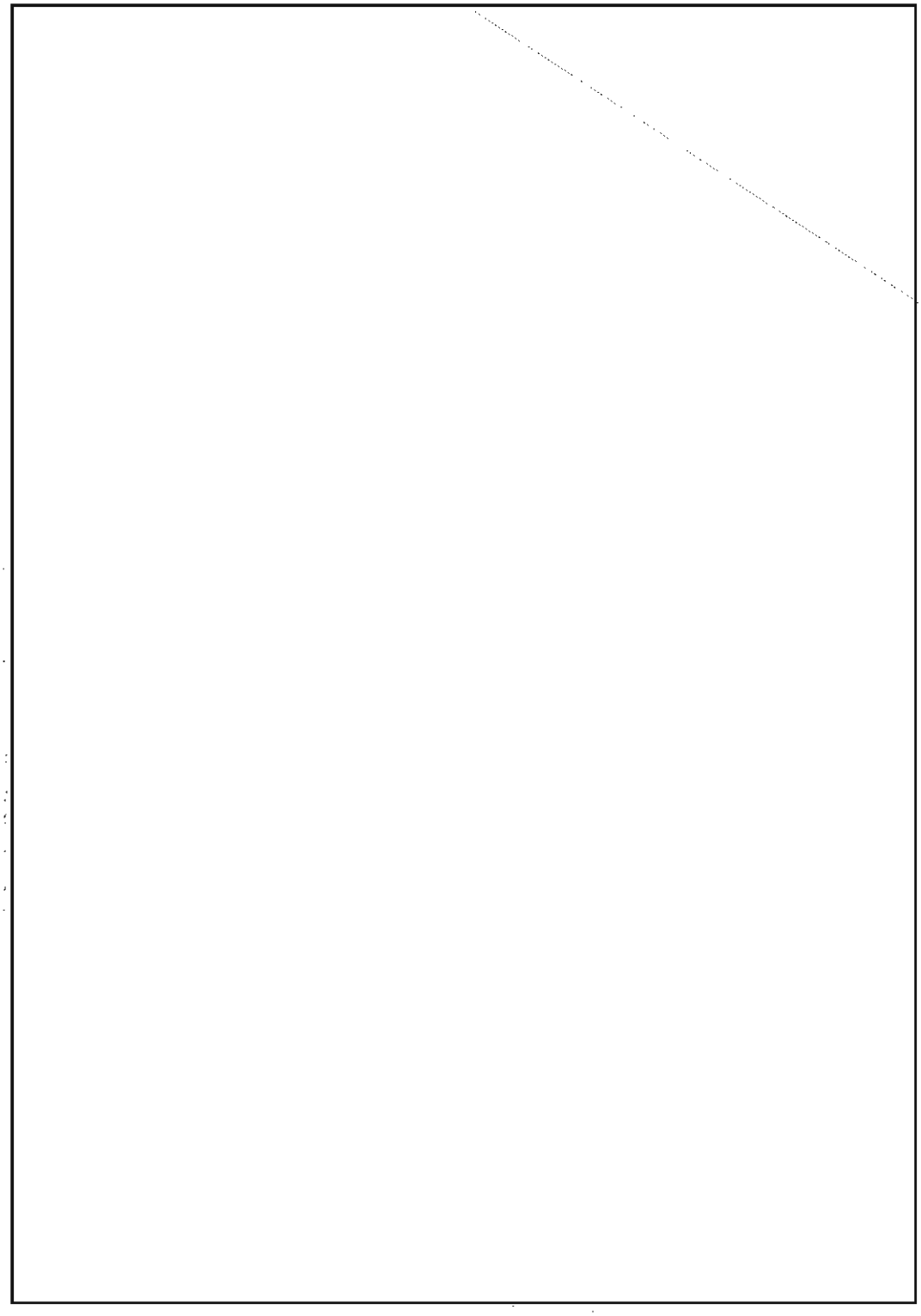
~~(FOUO)~~ Networking and packet switching technology will allow the user to access data bases and processing on other Agency mainframe computers, to communicate with other users, and in general to expand his horizons beyond his desktop to the entire SIGINT system.

~~(FOUO)~~ UIS host computers will provide a complete set of user services such as access to PLATFORM and PLATFORM resources. Additionally, the UIS host will provide data storage and management facilities, data conversion and reformatting services, mail, file archiving, security, and other support for various communities of users and a variety of general utilities.

~~(FOUO)~~ The resulting "layered" or distributed processing environment made up of personal computers, UIS host computers, and mainframe computers will form the basis for a dramatic change in the way most of us will work.

The Key to UIS

~~(FOUO)~~ The personal computers--or, as they are known in UIS parlance, Terminal Workstations (TWSs)--are the primary elements which will bring about the change from existing methods of working to the UIS environment. Only recently has the cost of personal computers decreased sufficiently to make them an affordable resource for most Agency personnel. Experts predict that the price per terminal will fall to a point within the next five years that a productivity improvement of only 8 to 10 percent will justify the investment of one-third of a person's average annual salary.



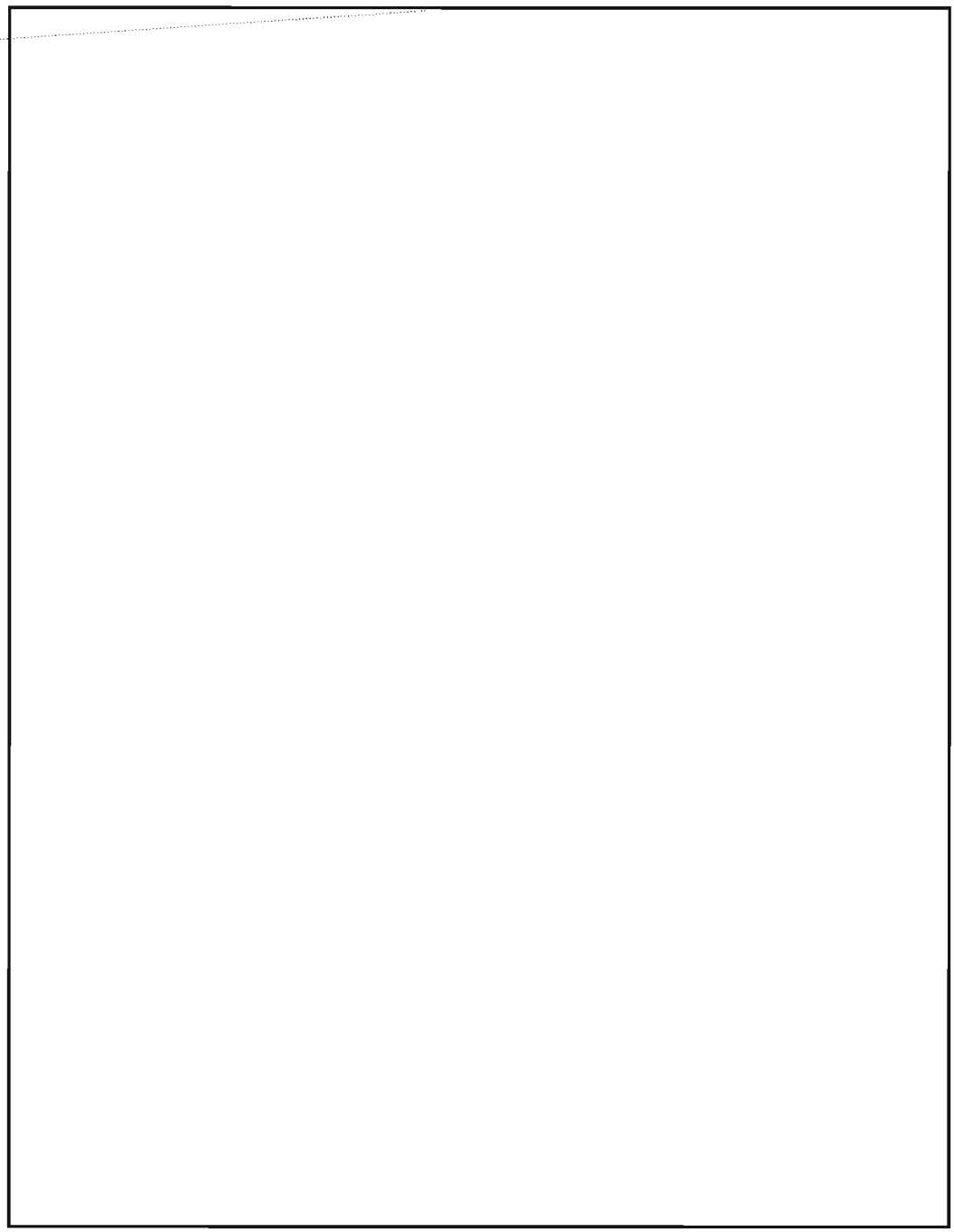
EO 1.4.(c)
P.L. 86-36

DOCID: 4019699

DOCID: 4019693

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



DOCID: 4019695

Today that's about $9,000. However, it is the opinion of these same experts that a significant (15-50%) productivity gain can be realized from a large portion of the Agency's workforce as they convert to a UIS environment.

~~(FOUO)~~ Just what is meant by a Terminal Workstation in UIS terms? Briefly, a TWS is a personal computer with sufficient local memory, disk space, display capacity, and communications support to provide the user with local computing power and, when needed, to connect him to a more powerful machine--a UIS host or the PLATFORM network and the Main Computer Complex. The TWS will be running under UNIX or at least a UNIX-compatible multitasking executive. The UNIX user interface, the file structures, the interprocess communication, and the shell environment are all essential elements. Additionally, the TWS will support, at a minimum, the C compiler and the BASIC interpreter. PASCAL may also be desirable as well. The current recompetition for a replacement of the Agency standard terminal (the Delta Data 7000T) is designed to acquire a personal computer of the type just described.

~~(FOUO)~~ Personal computers (although not with the capacity or the compute power described above) have been in use at the Agency and have been experimented with for at least three years as part of a program initiated by Mr. Kermith Speierman to explore this new dimension in computing. During this period much has been accomplished, spearheaded by the P1 organization, primarily in the areas of cryptanalysis and traffic analysis. Most of this work has been designed to determine just how useful a personal computer can be in running programs previously available only on large mainframe computers or to do work done by hand at the analyst's desk. All of this early experimentation was done primarily in a stand-alone mode (Stage I, if you will) although several of the personal computers have been hooked up to Terminal Subsystem (TSS) hosts (PDP-11/70s) and thus were able to access data bases on other systems. Analysts have used this facility to transfer data to the personal computer. This was Stage II in the evolution of the application of personal computers.

~~(FOUO)~~ UIS will lay the basis for development of Stages III and IV. People do not work in isolation. Sharing of files and programs and communicating with each other is necessary. The prototype of the Stage III working environment is being developed in the TSS of today. UIS will build on this work, marry it to the power of the personal computer, and provide a new host with enhanced capabilities. Stage IV will be accomplished when analysts worldwide through UIS terminal workstations can directly affect (and be directly affected by) the flow of data from the collectors to the product data bases and on to the consumer.

~~(FOUO)~~ Moving increased computing power nearer to the end user will cause a steady, but inevitable and vast, evolution to occur in the way data is stored, processed, and accessed. The nature of the Terminal Workstation is so different from the directly-connected terminals now in use, that we will be forced to rethink our most basic and traditional ways of moving, storing, and manipulating information. I cannot emphasize this point enough! The TWS reduces the dependence of large numbers of users on central processors and central data bases. Data processing and data storage and access can now be scattered in a large number of locations accessible to large numbers of people and processes. The tough challenge that DDT faces in implementing UIS is matched by the equally tough challenge faced by DDO (in particular) of applying the technology to best advantage once implemented. There is already a good deal of work going on in P1, A3, A6, B2, B5, B6, G3, and elsewhere which is leading in this direction.

The User's View: A UIS Scenario

~~(FOUO)~~ Several times in this talk, assertions have been made that UIS will cause a change in the way the user works; will cause a change in the way we move, store and manipulate data; and will challenge all of us to derive the maximum benefit from the implemented technology. To dramatize the differences between the system today and the system as it should be under UIS, a scenario describing the way a user might operate under UIS follows. The person described is a composite, if you will, of all the analysts, reporters, transcribers, flow managers, programmers, secretaries, office staffs, and managers who will be users of UIS Terminal Workstations of various kinds. But, within the scenario describing our general analyst's day, will be some of the things you might do.

~~(FOUO)~~ Our UIS TWS user arrives at his desk and powers up his personal computer. The system will ask for his personal ID and password. Once the system is satisfied that the user is who he claims to be, the user will not have to identify himself to any other computer he may wish to connect to during the day; his TWS will pass his verified identity to any other computer requiring it at the time of connection. The other computer needs only to determine that the person requesting access has been granted access permission. Specific file access on another system might require other

DOCID: 4019695

security measures that would occur after the connection was granted.

MAIN MENU

1. HELP
2. TEXT EDITING
3. TA FUNCTIONS
4. CA FUNCTIONS
5. TRANSCRIBER FUNCTIONS
6. REPORTER FUNCTIONS
7. PROGRAMMING FUNCTIONS
8. RESEARCH FUNCTIONS
9. OFFICE SYSTEM
.
.
.
21. SYSTEM FUNCTIONS

ENTER # OF SERVICE
& PRESS RETURN KEY:? (2)

~~(POOR)~~ Now that the UIS user has gained access to his personal computer and through it to that portion of the rest of the SIGINT system that he needs access to, he will be presented with a menu tailored to those functions that he routinely performs. At the top of the menu will be a HELP command and at the bottom of the menu will be a selection that will allow him access to the general system commands--the equivalent of a percent sign (%) for those of you familiar with UNIX. Our user will select from this menu some function he wants to start his day. Typically, this would be a review of his personal calendar or a scan of all the messages sent to him by other users or by other computers since he last looked.

~~(POOR)~~ Throughout the day he will interact with the rest of the system to send and receive mail and messages, transfer files to and from the MCC (the Main Computer Complex) or local UIS host systems, etc. However, the majority of his day will be spent using the data storage capacity and compute power of his personal computer, largely independent of the MCC.

TEXT EDITING MENU

1. HELP
2. MEMORANDUM FORMAT
3. NOTE FORMAT
4. RECORD MESSAGE FORMAT (UMPS)
5. SPECIALIZED FORMATS
6. CREATE A FILE
7. EDIT AN EXISTING FILE
8. VIEW A FILE
9. VIEW A DIRECTORY OF FILES
10. PRINT A FILE
.
.
.
20. RETURN TO MAIN MENU
21. SYSTEM FUNCTIONS

ENTER # OF SERVICE
& PRESS RETURN KEY:? (20)

~~(POOR)~~ Up to this point most of the functions our user will need are probably common to the vast majority of UIS users. One important function in this category is text processing. Since we all deal with text in some way or other through most of the day, a text-processing capability within the terminal is of prime importance. Wouldn't it be great if the many documents we produce each day (including end product, messages, reports, transcripts, plans, programs, etc., etc.) would have to be typed only one time! And if others could review and/or edit them easily and conveniently without always reducing them to hard copy? Text processing needs to be as readily available as the No. 2 pencil and as flexible as the pocket calculator.

~~(POOR)~~ From here on, the functions our UIS user selects from his menu become more specific, reflecting the duties of his job. The power of the personal computer allows us to tailor common, standard, modular functions into individual menus for each TWS user.

ANALYSIS MENU

1. HELP
2. SCAN/EDIT TRAFFIC PROCESS
3. EDIT TA LOGS
4. TEXT EDITING
.
.
.
20. RETURN TO MAIN MENU
21. SYSTEM FUNCTIONS

ENTER # OF SERVICE
& PRESS RETURN KEY:? (20)

~~(FOUO)~~ He might select from his menu the function that would allow him to scan the traffic that has accumulated for the past 24 hours and edit some of it, discard some of it, or copy some of it for later use as part of a report.

MAIL MENU

1. HELP
2. SEND MAIL
3. VIEW MAIL RECEIVED
4. TELECONFERENCE
.
.
.
20. RETURN TO MAIN MENU
21. SYSTEM FUNCTIONS

ENTER # OF SERVICE
& PRESS RETURN KEY:? (20)

~~(FOUO)~~ He might select from his menu the function that would allow him to send an informal message to another analyst halfway around the world or to read messages sent by that analyst to him. Given that time differences are not too great, he might even enter into an interactive conversation with the other analyst.

SPECIALIZED REPORT FORMAT MENU

1. HELP
2. RECORD MESSAGE (UMPS) FORMAT
3. USSID ### FORMAT
4. KLIEGLIGHT FORMAT
5. TECHSUM FORMAT
6. PROCUREMENT REQUEST FORMAT
7. PERSONNEL SUMMARY FORMAT
8. LEAVE REQUEST FORMAT
9. TRAINING REQUEST FORMAT
.
.
.
20. RETURN TO MAIN MENU
21. SYSTEM FUNCTIONS

ENTER # OF SERVICE
& PRESS RETURN KEY:? (20)

~~(FOUO)~~ He might select from his menu the function that would provide templates of any one of the hundreds of formatted reports we produce daily. After filling in the necessary information and correcting any errors, he would transfer it electronically to one or several people for coordination/comment. Getting the commented versions back electronically, he would make necessary changes and transfer the report to the person authorized to release it. Upon release, the report would be distributed electronically to all designated recipients, people who would read the report and take action or computers that would use the report as an update to some data base.

PROGRAMMERS MENU

1. HELP
2. C
3. BASIC
4. COMPILE
5. TEXT EDITING
.
.
.
20. RETURN TO MAIN MENU
21. SYSTEM FUNCTIONS

ENTER # OF SERVICE
& PRESS RETURN KEY:? (20)

~~(FOUO)~~ If our user is a programmer, he might select from his menu the function that would allow him to generate a program or to revise a program which he had entered earlier. He would have the necessary support functions to enable him to design and plan the program, properly format the input, and document the results. Given that the language he used to program was one recognized by the TWS (BASIC, C, PASCAL, etc.), he could ensure that the program was syntactically correct before connecting to the host or main frame for compiling or execution.

REMOTE ACCESS MENU

1. HELP
2. CONNECT TO SOLIS
3. CONNECT TO ULTRAMARINE
4. CONNECT TO CARILLON
.
.
.
20. RETURN TO MAIN MENU
21. SYSTEM FUNCTIONS

ENTER # OF SERVICE
& PRESS RETURN KEY:? (20)

~~(FOUO)~~ Our typical user might select from his menu the function that would allow him to conveniently and interactively access several computers where information was stored. Required information could also be brought back to the TWS and used to answer a query, become part of some report, or simply be a working aid of some sort.

OFFICE SYSTEMS MENU

1. HELP
2. CALENDAR
3. MESSAGES/MAIL
4. MEMOS
5. PHONE BOOK
6. TEXT EDITING
7. SPELLING CHECK
8. NOTES
9. ACTION/SUSPENSE FILE
.
.
.
20. RETURN TO MAIN MENU
21. SYSTEM FUNCTIONS

ENTER # OF SERVICE
& PRESS RETURN KEY:? (20)

~~(FOUO)~~ A manager might select from his menu the function that would allow him to examine his calendar for the day and a suspense/action file of items that should be completed. A request for any mail (to include administrative messages, personal notes, reports for comment/concurrence, etc.) would bring a list of items to his attention appropriately prioritized by his secretary or staff. His decision-making process is helped throughout the day by selecting from the menu functions that allow him convenient access to data containing technical, budget, planning, personnel, and management information.

~~(FOUO)~~ At any time during the day, if the TWS is powered on, any computer in the SIGINT system could send information directly to the TWS. When received, the user would be notified and he could take appropriate action. This facility could be used to update the user's work queues, to alert the user to the arrival of high interest traffic or mail or an incoming OPSCOMM, or failure of a critical program in the flow. It is a means to get real-time, human interaction into the flow of the SIGINT process. These brief and highly simplified scenarios highlight several advantages that the UIS concept has over today's operation:

[] UIS is capable of being tailored very specifically to each user while, at the same time, taking advantage of general utilities common to all users.

[] UIS does not depend on the 100% availabilty of the MCC or UIS Host systems for the user to do useful work.

[] UIS Terminal Workstations will provide powerful computer capabilites and data storage facilities conveniently and directly available to the user.

[] UIS will provide convenient access to the rest of the SIGINT system when required.

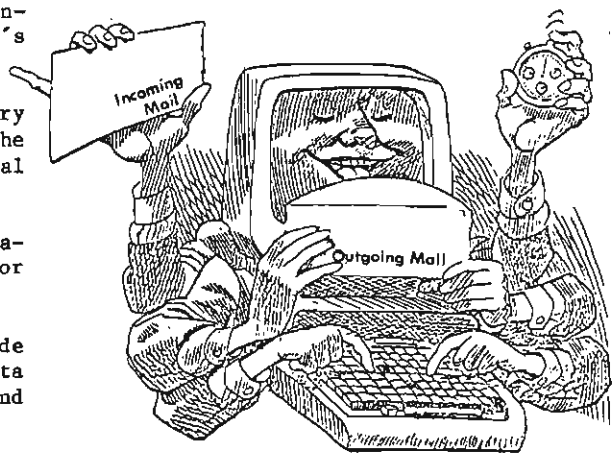
[] UIS will not only allow the user to affect the system but allow the system to directly affect the user, thus establishing a continuous feedback loop between the user and the system.

Planned Evolution

~~(FOUO)~~ It is not enough to provide an architecture and an operational concept. This briefing and the many papers that have been written (and will be written) are designed to present the UIS concept to a wide audience so that systems designers can begin to incorporate UIS concepts in their designs. But it is not enough to hope that the UIS concept will be implemented through the efforts of many project managers. There is technology that must be developed (or acquired) and demonstrated. The UIS technology and techniques must be demonstrated in an operational prototype and the real challenge of the problems posed by a distributed data processing environment must be solved. T44, with DDT's approval and with considerable help from other organizations throughout the Agency, hopes to introduce a UIS prototype within the coming year where the system designer and the user can collaborate to produce a functioning UIS environment. We have already begun to work with PI analysts and others to see which "real" analytic problems we should be addressing first. If any of you would care to make any suggestions or want to know more about what we are doing, I invite you to get in touch with me. [redacted] will be describing some of our early plans for the prototype in the second half of this briefing.

P.L. 86-36

1. [redacted] TSS Revolution, Cryptolog, Sep 1982, pp. 8-12.



P.L. 86-36

PART TWO: ARCHITECTURE

by [redacted]

~~(FOUO)~~ Now that Tom has told you what UIS is for and how it has gotten to where it is, I will tell you how it is made up. I intend to cover the Architecture (how it all fits together); the technology which makes it possible at this point in time; the components (some of which already exist) which make up UIS; our approach to making UIS real in all its aspects; and especially the UIS Prototype, which is our initial move in getting UIS where we want it to be.

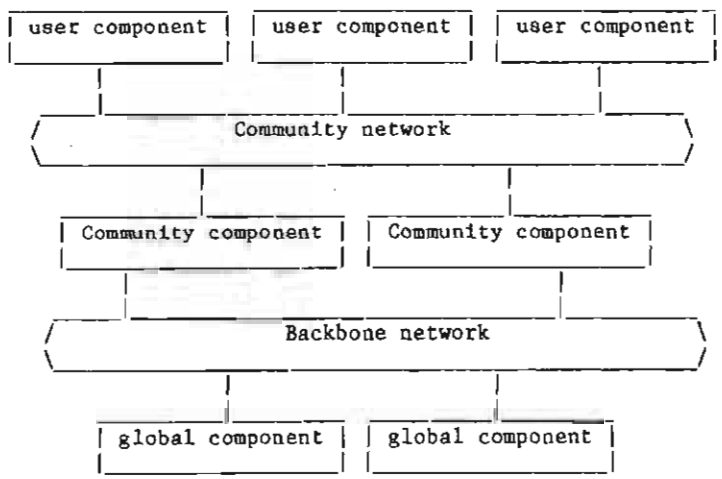
~~(FOUO)~~ This is the basic UIS Architecture. It consists of three main levels of components, with interconnection between these levels.

~~(FOUO)~~ At the outer level (closest to the user) we have the User Component which is where all private data and applications reside. This is the user's private workspace, to be treated rather like a desk, chair, phones, file, and scratchpad would be used today; it will provide as much data storage and computer power as we can afford.

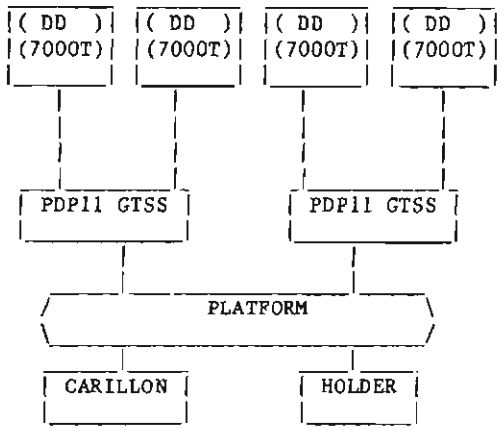
~~(FOUO)~~ At the intermediate level we have the Community Components, which is where the individual user comes into contact with his fellow workers. It is here that data needed by more than one user is stored (e.g., a calendar which an executive shares with his secretary, or a frequently-used operational data base). In addition to the sharing function it is at this level that support to users, above and beyond that which the User Component can provide, is available (e.g., file archiving, high-quality printers, extended computing power).

~~(FOUO)~~ At the innermost level are the Global Components, the major computer complexes in the basement. These must be accessible by the user through the other elements of UIS, and we do not envisage that they will change significantly because of UIS.

~~(FOUO)~~ There are two levels of connectivity, the Community Network, the element which connects the user to his Community Component and to other users, and the Backbone Network which connects all major components. While there is only one (logical) Backbone Network, there are many Community Networks. The function of these components will become clearer later in the briefing.



UIS ARCHITECTURE CONCEPT



UIS ARCHITECTURE NOW

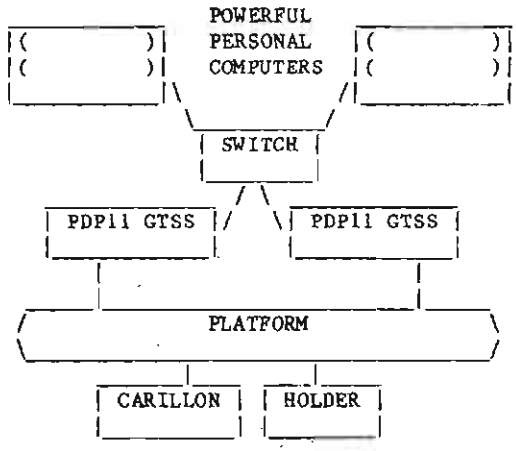
~~(FOUO)~~ If all this sounds too ethereal, let us look at what we have today and see how closely it corresponds to this architecture. As you can see the Global Components are in place, as is the Backbone Network, in the form of the PLATFORM network. The Community Components are represented by the existing PDP 11-based GTSSs, which are the starting point for the full Community Components but also contain the Community Network and User Component facilities, because these are only point-to-point lines and "dumb" terminals respectively.

~~(FOUO)~~ The next few slides show how we expect to develop from where we are now to where we hope to be at the end of UIS.

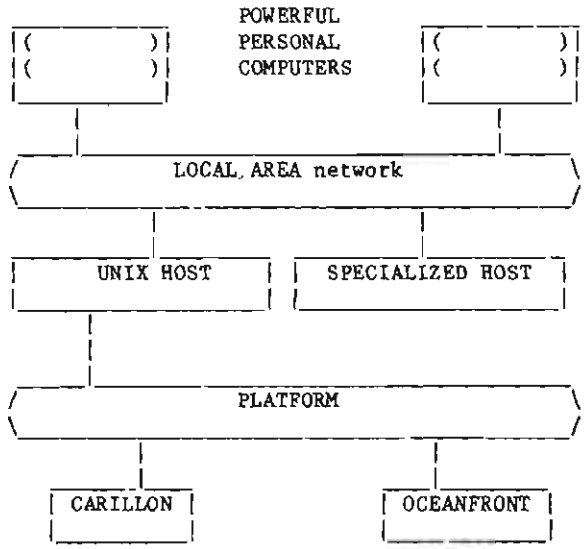
~~(FOUO)~~ The first item to be tackled is to replace the "dumb" terminals with Powerful Personal Computers (PPCs) and thus greatly expand the local processing and storage available to each user, literally on his desk. This process has already begun with the use of a variety of PCs in many different organizations within NSA. I'll talk more about the technical characteristics of these devices later but as far as the user is concerned the Powerful Personal Computer, implemented as what we call the Terminal Work Station, is the basis for the User Component. It will provide the user with local, affordable, available, and private computing resources--it is his own machine, with sufficient storage for his private data, processing power (and, of course, software) to satisfy, say, 90% of his computing requirements and, when the Terminal Workstation needs it, access to larger computers, to other data, and to the worldwide network of users.

~~(FOUO)~~ As a starting point, the Terminal Work Station will run the UNIX operating system and so will have available to it many of the applications currently used on the PDP 11 GTSSs--one notable exception being the RAND Editor, which will be replaced by a Word Processing package native to the TWS itself.

~~(FOUO)~~ As a first step towards introducing the concept of a Community we shall reduce the reliance on a single host by means of a simple switching function, implemented either as a digital switch or using some early offerings in Local Networking.



UIS ARCHITECTURE
THE POWERFUL PERSONAL COMPUTER

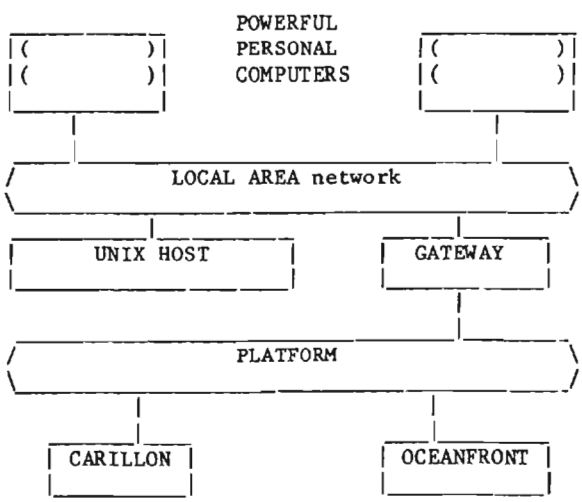


UIS ARCHITECTURE
COMMUNITY NETWORK AND SUPPORT

~~(FOUO)~~ This extended local power has to be linked to the Community-level components in a much faster and more flexible way than we have at present. This will be achieved by means of the emerging Local Area Networking technology (of which more later). We are looking here for more than mere connectivity; we are looking for some measure of intelligence in making decisions as to which hardware component at the Community level a User Component needs to connect to. (If a user wants to archive a file, it is no good connecting him to the print server!)

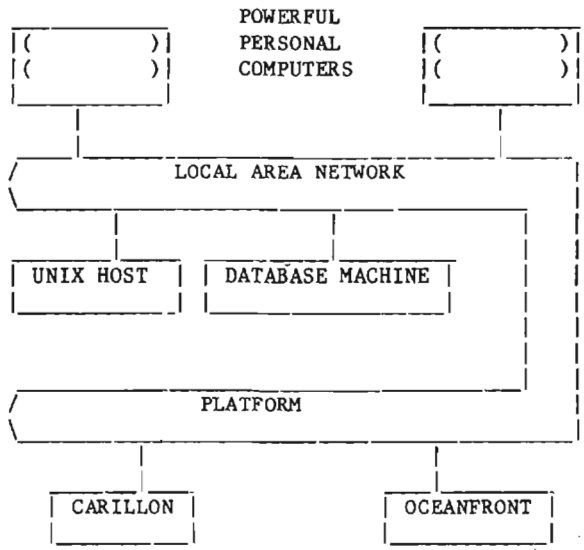
~~(FOUO)~~ The development of the Community Component will be somewhat slower, relying initially on the existing TSSs and their look-alike replacements. By supporting UNIX in both the PPCs and the Host, the transition from Host software to Terminal software will be accomplished over a period of time. This will be hastened by the inclusion at the Community level of certain specialized processors, of which the most obvious are the Database Machines as typified by the Britten-Lee IDM-500, with which T3 is currently experimenting.

~~(FOUO)~~ Extending the idea of reducing our dependence on a single host, we shall introduce at this stage the idea of a file server which holds Community files; when a user requires processing and data, he is allocated to any available machine and the file server stages the required data to that machine. One may even wish to consider whether interactive connection between the User and Community levels should be replaced by a transactional protocol. In the long term one can conceive of the Community Component as evolving from a set of General-Purpose Processors to become a collection of specialized processors.



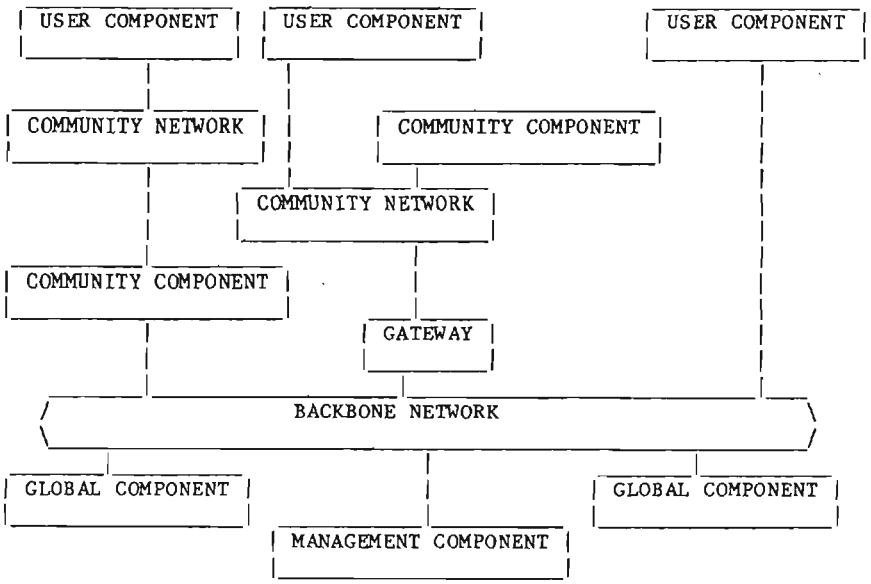
UIS ARCHITECTURE
ACCESS TO GLOBAL RESOURCES

~~(FOUO)~~ A major limitation of the previous phase of the development is the necessity of passing through a general-purpose processor to get to the Global Components. This would be made easier by including a special-purpose machine at the Community level with the job of handling the gateway function from the User to the Global levels. This in itself is a major undertaking.



UIS ARCHITECTURE
THE USER'S DREAM

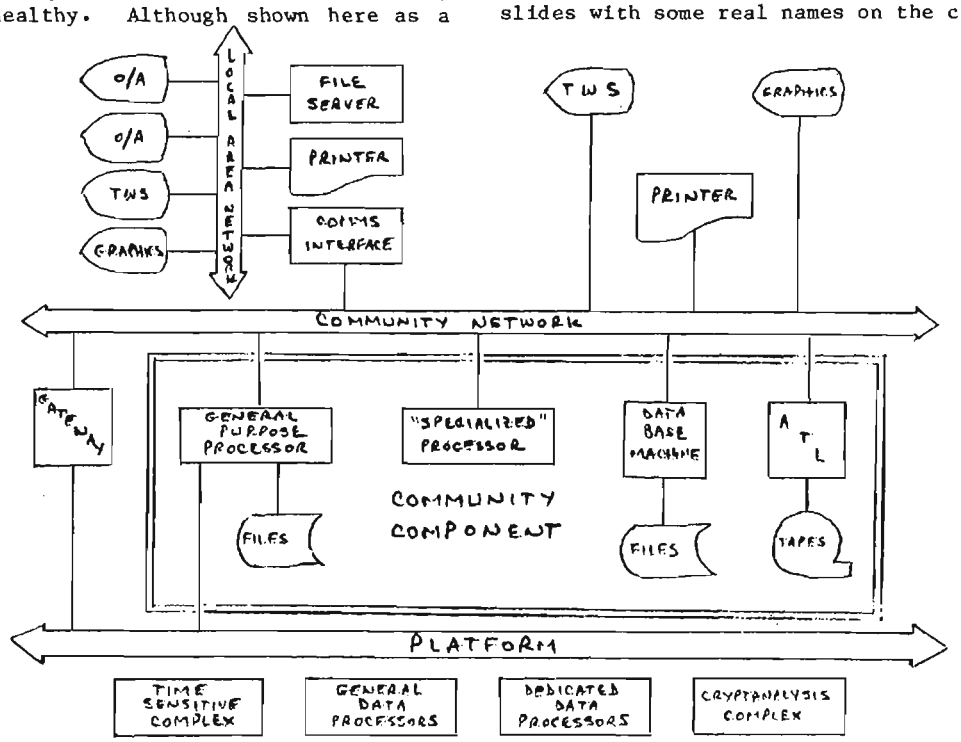
~~(FOUO)~~ If we continue with this trend, the Community and Backbone Networks merge. It may be, however, that this is more a Utopian dream than an achievable goal, though it must always be our aim to make the network appear to the user to be one cohesive whole rather than a set of mazes to be negotiated only with skilled navigating.



~~(FOUO)~~ Clearly these phases will overlap considerably so what we actually end up with is a configuration more like this one; the elements of the previous slides can still be seen as individual entities however.

~~(FOUO)~~ A new element, one which is vital to UIS but which I won't say much about today (mainly because we haven't defined it very well yet), is the Management component. This is where the system is monitored, controlled, and kept healthy. Although shown here as a single box it is likely to be a fully distributed function (when we can figure out how to build it).

~~(FOUO)~~ A typical UIS Community will look rather like this (below). As well as the elements described so far there will be specialized User Components supporting Graphics, interfaces to dedicated Office Automation networks, and local print facilities. This is just a redrawing of the earlier conceptual slides with some real names on the components.

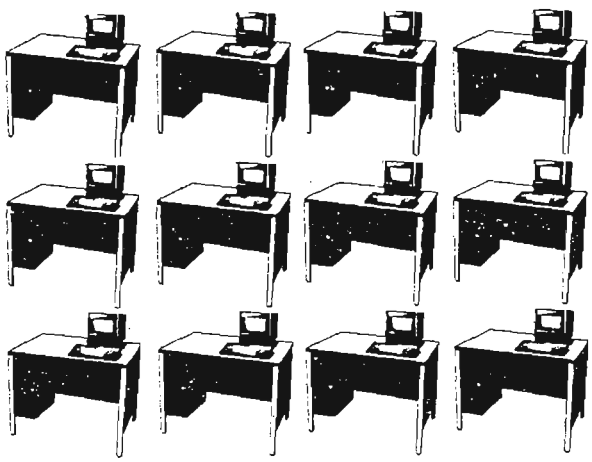


TECHNOLOGY/COMPONENTS

~~(FOUO)~~ Having looked at the architecture, we turn to the question of why now is the right time to be making a big push for the UIS idea. After all, there is nothing particularly revolutionary in the ideas; they develop out of existing systems and the natural course of technological advances.

~~(FOUO)~~ The important thing at this time is that the technology is now becoming available to allow us to move usable processing nearer to the user in a cost-effective manner. This is a continuation of a long transition from central batch processing, through remote access, GTSS systems, and networking to the emerging use of personal computers. The key technologies needed to realize the UIS concept are Powerful Personal Computers and Local Area Networks. Community Support Processors, while not in themselves new technology (they are developing in a steady progression from the existing GTSSs), are essential components of UIS and their form and function will be modified by the increased use of the PPCs and LANs. Global Networking we already have and will need to exploit and expand to support the UIS method of working.

~~(FOUO)~~ Let's now look at some of these technologies in a little more detail.



TECHNOLOGY/COMPONENTS
Powerful Personal Computer

- Keyboard/Screen
- Powerful Microprocessor
- At least 256Kb Memory
- 10 Mb+ Winchester Disc
- Communications Interface/Software
- Tempest
- UNIX
- Word Processor Software
- Data Base Support

~~(FOUO)~~ The PPC which we can now purchase for around $10,000 satisfies the definition given here. It is no accident that the specifications of the UIS Terminal Workstation and the Agency standard terminal to replace the DD7000, known and loved by so many Agency personnel, are so similar.

~~(FOUO)~~ You will notice that the memory requirements (both main memory and back-up storage) are large--some people say too large; this is a natural (and relatively cheap) response to the information explosion. We have never had enough storage on any computer (and probably never will have) but at least the responsibility for the organization of this storage is totally with the user.

~~(FOUO)~~ TEMPEST is a restrictive but necessary requirement.

~~(FOUO)~~ As we have mentioned earlier, we are looking to a PPC which supports the UNIX operating system or something which looks very much like it. This will give the dual advantages of portability of the current TSS software and of user familiarity.

~~(FOUO)~~ The communications interface, properly supported by vendor software, is another key element allowing the user to access the remainder of his world.

~~(FOUO)~~ We are looking for an extensive amount of vendor-supplied software in addition to the ability to transport UNIX-based software from the GTSSs.

~~(FOUO)~~ A device such as that described here could not have been purchased a year ago.

TECHNOLOGY/COMPONENTS
Local Area Network

- Hardware is available and cost effective
- Software is developing
- Tempest

~~(FOUO)~~ Local Area Networking technology (needed for the Community Network) is somewhat less mature than PPC technology. It is growing apace and many vendors are pushing their hardware. Clearly, this is the technology we need and will get; equally clear, however, is that we can't buy the software (mainly the implementation of protocols) needed to give us the necessary functionality.

~~(FOUO)~~ To UIS the Community Network has more than just a switching function; it is the means by which the User projects his image to the world. For instance, most current PPCs come with an asynchronous communications interface running at around 9.6 Kb; this makes the PPC look to hosts like a dumb terminal. What we need, however, is to make the PPC look like what it is: a computer with high-speed file transfer and other sophisticated capabilities. The ability to drive data into the TWS without the user having to control the transfer is a key UIS function, needed to support overnight offloading of data from the more centralized processors, for instance. Clearly, this goes well beyond what is currently available in the Local Area Network marketplace, and requires changes in the connection strategy of the PPCs and the Hosts as well as the LAN technology--but it is still part of what a user considers as the network.

TECHNOLOGY/COMPONENTS
Community Support Processors

- PDP 11/70 now
- Replacement Host
- Support for 100 terminals
- How many PPCs?

~~(FOUO)~~ The existing GTSS has served us well and will continue to do so, as will its immediate successor which is now being competed for. Existing applications will continue to be run but will steadily be replaced by applications in the PPC--these may be copies of the same software in the TSS--and by specialized processors.

~~(FOUO)~~ Current PDP 11/70s support up to 32 directly-connected users; the replacement Host will support perhaps 100. By implementing UIS we hope to extend the support to several hundred, of whom only a small proportion are actually using Community resources at any one time, thereby enabling Communities to be exactly what they need to be--all users who work together--no longer being restricted to the 32 terminal users of each system.

~~(C)~~ Incidentally, you may notice that we haven't explicitly defined what we mean by a Community. This is about the closest we have come. This is not an oversight. We believe that UIS should allow the Users to decide what they want to constitute a Community, which may be as small as an individual office or as big as all analysts

EO 1.4.(c)
P.L. 86-36

TECHNOLOGY/COMPONENTS
Global Networks

- PLATFORM
- Theater Networks
- Global Interconnection

Global Components

- Little or no change

~~(FOUO)~~ Global Networking is already with us, in fact has been for many years, and we see an evolutionary progression towards greater survivability, increased throughput and timeliness, and greater functionality. This is required for reasons other than UIS and will be accomplished through the use of theater networks and a global interconnection of networks.

~~(FOUO)~~ We do not see any major changes to the Global processors in the immediate future, though they will undoubtedly be affected in the long term as we eliminate directly connected user terminals.

THE PROTOTYPE AND BEYOND

~~(FOUO)~~ So where do we start on these grandiose plans?

~~(FOUO)~~ The obvious place is the Terminal Workstation, which is what the user will perceive as the interface to the whole processing system.

~~(FOUO)~~ I have talked about the things we need on the Powerful Personal Computer and Tom talked about the facilities provided to users on the user component. It is the implementation of the User Component on a PPC, as the Terminal Workstation, which is the first real challenge of UIS. The PPC, even with extensive vendor software, is not enough. We have to add specific NSA software; we have to make it attractive and secure to store data on this local device and to manipulate it locally, to make it easier to access other machines (without knowing a litany of FTP commands for instance), and to generally be friendly to the person manipulating the keyboard.

~~(FOUO)~~ It is not until we have done all of these things that we can begin to claim that we have implemented the User Component of UIS.

~~(FOUO)~~ To gain experience in the technology and, more importantly, to be able to demonstrate that the ideas we have presented today make sense, are achievable, and are attractive to the end users, we are building a prototype system in T44.

~~(FOUO)~~ We have already gained some experience by using Xerox 820s, originally purchased as programmable word processors but subsequently adapted by us to support other office functions and communications to PLATFORM. This experience has proven invaluable in enabling us to specify a much more powerful and flexible device for the true prototyping effort.

~~(FOUO)~~ This prototype is a joint venture with P1 personnel, who also have considerable experience in the use of personal computers. The intent is to bring in up to 12 Powerful Personal Computers and turn them into Terminal Workstations, as described earlier.

~~(FOUO)~~ We have chosen terminals made by WICAT for use in the prototype as they fall within an acceptable price range and are the earliest models to have all, or nearly all, of the features we need.

~~(FOUO)~~ Under the UIS umbrella we shall also be getting experience with Local Area Networking. We are, for instance, working with T15 to improve the operation of the numerous TSSs in the basement by pooling of peripherals. We shall also use this type of technology to connect the WICAT terminals to a number of NASs and TSSs, such as CARONA and STEPSTONE-T03.

~~(FOUO)~~ As we get these components in place and start to use them, we shall undoubtedly run into snags, so we must remain flexible in our approach and try to solve the problems as they arise. (We have already changed our minds at least twice on how to connect the TWS to the Community level and on how many WICATs to buy.)

~~(FOUO)~~ This prototype, which we expect to have operational by August 1983, will be used to demonstrate the functions shown here.

A P P R O A C H

TERMINAL WORK STATION
|
|
V
LOCAL AREA NETWORK
AS A COMMUNITY NETWORK
|
|
V
EFFECT ON TSS & ITS
REPLACEMENT--COMMUNITY COMPONENT
|
|
V
GLOBAL CONSIDERATIONS

~~(FOUO)~~ Within the WICAT we shall demonstrate Office Automation functions such as Word Processing, memo generation, and calendar and phone directory maintenance; some CA applications taken from existing PCs; and parts of some TA applications taken from the PINSETTER suite.

~~(FOUO)~~ Our means of making the terminal user-friendly is to use a menu-driven approach, with the user prompted for the

minimum amount of information. On our existing Xerox 820s, for instance, we perform transfers to and from CARONA through a NAS and only ask the user for the file names on each system and his CARONA password--rather different from the FTP sequence needed if the user is sitting at a dumb terminal.

~~(FOUO)~~ Networking applications will include electronic mail (messages generated on the local TWS but distributed using the existing software in the TSS) and dissemination of the TA files to the individual analysts.

~~(FOUO)~~ Additionally, the prototype will be used to investigate some of the areas which are less well defined, such as:

- distributed data;
- extension of TWS power;
- new applications;
- use of new technologies;
- management of users; and
- protocol issues.

~~(FOUO)~~ Some of the specific things we have in mind for this further stage are:

- How to use the Britten-Lee IDM 500 Data-Base Machine as a specialized Community Component;
- Alternative User Components, such as the Xerox 860s and Stars under the Office Automation program and the AYDEN CORE Graphics in support of A21 (as a prototype of Jerkin);

~~(FOUO)~~ Most of the other items on this slide are in the nature of a wishlist at present; they will become better defined as we get the things from the previous slide implemented and have more resources to devote to the investigational, rather than demonstrational, aspects of the prototype.

~~(FOUO)~~ Having concentrated firstly on the outermost layer (the TWS), we intend to move steadily inward to implement secondly the Community Network using a full-function Local Area Network, as described earlier. This will greatly improve performance and flexibility over the existing point-to-point connection. The effect on the TSS caused by these developments will be the third area to receive attention--by the time this happens specialized processors will be maturing, applications will be moving out to the TWS, and greater functionality will be available, thereby allowing a significant step forward to be made. Finally we shall see if there are any effects on the Global Network and the Global Components.

~~(FOUO)~~ In parallel with this mainstream development we shall be studying the problems of access, security, accounting, control, and other management implications of an increasingly distributed environment.

SUMMARY

~~(FOUO)~~ In closing, I should like to return to Tom's original questions.

What is UIS?

~~(FOUO)~~ Well, I hope we have explained the Concepts, the Architecture, and the Components sufficiently to answer this question.

Why should you care?

~~(FOUO)~~ You should care because this is the way the Agency will be doing its business by the end of the century, and if you don't want to get left behind you should make sure you have your UIS personal computer with its considerable local computing power and practically limitless communications ability.

What is UIS good for?

~~(FOUO)~~ Our answer is that it is good for everything which involves a person, and one or more of: data, computing, or communications. If you didn't recognize anything familiar in the scenarios Tom went through, you are probably in the wrong meeting. If you recognized more than a little of what you need to do your job, then please watch as we try to answer the question more accurately and in more detail by gaining experience with real users and with their reactions to the prototype. If you can see immediate, useful, and powerful applications to your work area, please give us a call.

Cumulative Index
Part Two: Titles (U)

The following cumulative index of CRYPTOLOG (Vols. I through IX, 1974-1982) is in three parts, and is being published in three successive issues, by author, by title, and by keyword. Items in multiple issues (February-March 1975, for example) are indicated by the first month (i.e., by Feb 75).

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Abdul and His 40 Tanks; Aug 75; Mason F.O.
About the NSA SIGINT Summary; May 76; [redacted]
Accentuate the Negative; Apr 78; [redacted]
Agency Summer Language Study; Dec 78; Buckley D.
AG-22/IATS: A View From the Bridge; Jun 77; [redacted]
AIT; Apr 80; [redacted]
a/k/a Sam; Dec 78; Meyer W.P.
Al Balloni, Editor; Sep 77; A.J.S.
Al Balloni, Editor; Jan 79; A.J.S.
All I Ever Wanted To Know About DES; Aug 82; [redacted]
All The Alligators Aren't On Sport Shirts; Jan 82;
Amateur Spread Spectrum; Jun 82; [redacted]
[redacted] Nov 77; [redacted]
Analysts of NSA, Arise!; Jan 80; [redacted]
And-a You Betta Have Moti-vaysh!; Oct 78; [redacted]
Another Cipher by ...; Sep 76; [redacted]
Another Controversial Book on Artificial Intelligence; May 77; [redacted]
Another Last Word on IATS; Sep 77; [redacted] P.A.
Another Source; Oct 79; [redacted]
Another Word on AG-22/IATS; Oct 76; [redacted] M.A.
Answer to Can You Make Out the Name!; Apr 75; [redacted]
Answer to Three Holes; Mar 78;
Answer to 'Vexing ... Problem'; Nov 76; Mason F.O.
Answer: An Old Problem; Oct 82; [redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Apollo-Soyuz Test Project; Dec 76; [redacted] J.E.
The Apostrophe: Some Thought's; Nov 74;
An Approach to Callsign Analysis; Dec 74; Jackson W.J.
Are We Wasting Linguistic Time?; May 75; Irwin M.R.
As I Was Saying Two Years Ago ...; Jun 78; Pattie M.T.
ATA Letter to President Carter; Apr 78; Tinsley R.L.
Attention Authors and Publicity Chairmen; Mar 82;
Attention Military Traffic Analysts; Mar 79;
An August Baudy; Aug 79; [redacted]
[redacted] Sep 77; Pratt D.L.
Automation of a TA Process; Oct 75; Murphy T.

P.L. 86-36

P.L. 86-36

Back to Square One!; Oct 78; [redacted]
Backing into Language Acquisition; Nov 77; [redacted]
The Baltic Encoders; Jun 79; Reiskis A.
Basic Patterns of [redacted] Codes and Ciphers; Feb 75; [redacted]
Between The Lines of Your Performance Appraisal; Jan 80; [redacted]
The Bible and the Washington Monument; Sep 76; Snow D.
[redacted] Mar 77; Jul 77; [redacted]
Bookbreakers Forum; Jun 78;
Bookbreakers Forum; Apr 79;
Bookbreakers Forum On Machine Aids; Apr 82; [redacted]
[redacted] Jul 77; Buck S.H.
The Bucky Balance; Jul 78; [redacted]
Bust Answer; May 82; [redacted]
But It Looks Like the Real Thing; Dec 76; [redacted]
But Life Is Supposed To Be Hard; Mar 82; [redacted] J.
But, Mr. Boak, Did You Ever Try To Get Rid of One in a Hurry?; Apr 79; D.H.W.
But Why Do We Do It?; Jan 78; [redacted]
By-Lines Don't Cost--They Pay!; Feb 78; Mollick J.J.

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

CAA News: What Ever Happened to the CAA?; Jul 77;
CAA News: What Are They Up to Anyway?; Aug 77;
CAA News: Whom?; Sep 77;
CAA News; Oct 77;
CAA News; Nov 77;
CAA Message and News; Dec 77;
CAA News; Jan 78; W.E.S.
CAA News; Feb 78; W.E.S.
CAA News; Mar 78; W.E.S.
CAA News; Apr 78; W.E.S.
CAA News; May 78; W.E.S.
CAA News; Jun 78; W.E.S.
CAA News; Jul 78; W.E.S.
CAA News; Sep 78; W.E.S.
CAA News; Oct 78; W.E.S.
CAA News; Nov 78; W.E.S.
CAA News; Jun 79;
CAA News; May 79;
CAA News; Aug 79;
CAA News: Conference on Communications Analysis; Oct 79;
Mar 77; D.A.
Calling All SRAs! -- SRA Symposium; Aug 74;
Callsigns and WARC-79; May 78;
CAMINO News; Feb 75;
The Case for COMINT Readers; Jan 75; H.C.
Cast a Double Shadow: The Trojan Horse of SIGINT; Nov 78;
Celtic Languages Today; Jun 78;
Central Research and The Paper Blob; Nov 82;
The Changing Face of NSA; Jan 78; 'Anon.'
Chapenko, Shapenko: What Difference Does It Make?; May 79;
Character Building in the People's Republic of China; Oct 74;
Check Your Morse Front-End Alignment; Nov 76; 'Anon.'
Dec 82;
Choose Yet; May 77;
CIRC: An Intelligence Data Base; Jan 80;
CISI News; Mar 79;
CISI News: Spring Conference; May 79;
CLA News; Mar 78;
CLA News; Sep 78;
CLA News; Oct 79;
CLA News: Sydney Jaffe Award; Jan 80;
CLA News: Russian Institute; Feb 79;
Clarity, Thy Name is Qualifier; Nov 76; Mollick J.J.
Classic Cables; Apr 79;
Classic Cables; Mar 79;
Classic Cables; May 79;
Classic Cables; Apr 81;

P.L. 86-36

P.L. 86-36

Classification Corner; Jul 77;
Classification Corner: XGDS-2; Sep 77;
Classification Corner: A Bigger Picture; Oct 77;
Classification Corner: Who Said?; Oct 77;
CMI News; Jan 79;
CMI News; Aug 79;
Codeword or COMINT Channels?; May 75; H.
Collection-Support TA is Not for Everyone; Feb 78;
Coming Home; Jan 80;
COMINT Analysis of Sep 78;
The COMINT Chain 'Gang'; Feb 79;
COMINT, COMSEC, and Hilbert's Tenth; Jan 78;
COMINT in the Russian Navy, WWII; May 76;
A Comm Change at Ramasun Station; Apr 75;
Comments on AG-22/IATS; Jun 76;
Comments on AG-22/IATS; Jun 76;
Comments on AG-22/IATS; Jun 76;
Comments on AG-22/IATS; Jun 76;
Comments on AG-22/IATS; Jun 76;
Comments on AG-22/IATS; Jun 76;
Comments on AG-22/IATS; Jun 76;
Comments on AG-22/IATS; Jun 76;
A Comparison of NSA and ATA Certification Standards; Mar 76;
Computer-Aided Transcription
Apr 76;
Computer Network Resources In C5; Aug 75;
Computer Operating System Vulnerabilities; Mar 79;
Computers In The ELINT and Telemetry Business; Jun 76;
Computers, Comms, and Low-Grade Ciphers: The
Oct 75;
A Computer Scratch Pad at Home or at Work?; Jun 78;
Some Reflections On The Reality of Computer Security; Jun 82; Hanyok R.J.
COMSEC Challenges; Nov 82;
COMSEC Familiarization: Do You Need It?; Jun 75;
COMSEC/SIGINT Relations; Apr 79; Boak D.G.
+Conoces Bien la Geografia?; Apr 78;
Human Factors Corner: Consumer vs. Computer: A Review; Mar 82;
Contemplating Computing; Apr 77;
Continuing Professionalization; Oct 78;
Contributions Solicited; Sep 74;
Conversation With a Micrographics Pioneer; Dec 77;
Conversation with a Bookbreaker; May 76; 'Anon.'
The Costs of Muddling Through; Nov 82; Gould R.E.
Coverterms; Apr 75; Filby W.R.

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

P.L. 86-36

Cryptanalysis and Code Recovery; Sep 74; Mountjoy M.
Cryptic Crossword; Nov 81; [redacted]
Cryptic Crossword; Mar 82; [redacted]
AFCEA 82 and ICC-82: New Crypto Devices; Aug 82; [redacted]
CRYPTOLOG Index for 1974; Dec 74;
CRYPTOLOG Index for 1974; Jan 75;
CRYPTOLOG Index for 1974-1975; Dec 75;
CRYPTOLOG Index for 1977; Dec 77;
CRYPTOLOG Index for 1978; Dec 78;
CRYPTOLOG A Letter of Introduction; Aug 74; Wolff R.E.
CRYPTOLOG Numbering; May 82;

The Danang Processing Center; Oct 75; [redacted] A.
Data and Definitions: Calling Things by Their Rightful Names; Nov 74; [redacted]
Data Field Naming/Coding Conventions at NSA; Jan 82; [redacted]
Data Flow--Challenge of the 1980s; Apr 80; Phillips C.J.
Data Security and Human Error; Oct 78; [redacted] J.M.
Data Standards Center; Nov 78; Pattie M.T.
Data Standards Without Tears; Feb 79; [redacted] P.Q.
Data Standards Without Tears: A Comment; Mar 79; [redacted]
Data Standards Without Teeth; Jun 79; [redacted] P.Q.
Dating Game; Jul 77; Williams D.H.
Development and Correlation of Indicators; Dec 82; [redacted]
DESKPAD: A Programmers's Tool; Nov 75; [redacted] H.
The Devil's Dictionary; Feb 75;
DIA Videocasette Program; Apr 81;
DIALOG Available at NSA; Aug 77;
A Dialogue Between Ms. User and Dr. Analysis; Nov 78; [redacted]
Diego Garcia? What? Where? Why?; Nov 74; [redacted] G.A.
Director's Memorandum: 'MAROON SHIELD Guidance'; Nov 77; Inman B.R.
The Doctor Is In(capable of Diagnosing); Sep 77; Chauvenet L.R.
Does Anybody Here Remember PURPLE?; Dec 82; [redacted]
A Donkey in Your WHAT?; Mar 78; [redacted]
The Do Xa Pads; Oct 75; Wiley E.

Early Days in NSA Computing; Aug 77; [redacted] L.R.
An Early NSA Proposal for Satellite Remoting; Jan 78; Horo J.E., Nolte W.M.
Economic Intelligence: Problems and Prospects; Oct 81; [redacted]
Emitter Identification Techniques; May 79; [redacted]
Equipment Maintenance on ABNER; Jun 78; [redacted]

EO 1.4.(c)
P.L. 86-36

[redacted] Dec 77; [redacted]
Establishment of CSI Newsletter; Dec 75;
An Evaluation of a Scientific Chinese Machine Translation; Jun 76; [redacted]
Even a 5-year-old Child ...; Oct 74; Tetrault E.W.
Executive Order 11652; Jan 77; 'Leiner'
Exercise Support; Dec 81; [redacted]
EXPERT; Jul 79; [redacted]
Expletives Deleted: Glossing Over a Glossary; Feb 76; [redacted]
Expletives Deleted?; Aug 77; Salemme A.J.

P.L. 86-36

Fairbanks on English; Mar 79; Fairbanks S.
The Faithful Echo--The Role of the State Department Interpreter; Feb 75; [redacted]
Fear of Testing, and What To Do About It; Apr 79; [redacted]
Feeding the Germans Misinformation (Book Review); Oct 78; Filby P.W.
A Few Thoughts on the NSA Linguist; Mar 77; 'Anon.'
First Lady of Navy Cryptology; Feb 78; [redacted] R.P.
A Fix for the Language Problem?; Aug 75; [redacted]
Flag-Waving Programmer; Dec 74; John G.
Flash! 115th SRI Located!; Apr 77; Salemme A.J.
Football and Cryptology; Jan 76; [redacted]
Foreign Publications Procurement Program; Sep 76; Link L.
Formatting PL/1 Source Code; Nov 78; [redacted] K.J.
The French(fried) Connection: Gino the Genie; Dec 76; [redacted]
The [redacted] System; Feb 76; [redacted]
Full or Broad Spectrum Lighting; May 82; [redacted]
The Future of Cryptanalysis; May 78; Lutwiniak W.
Futuristic Reporting; Nov 81; [redacted]

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Gary's Colors; Sep 74; Garofalo C.A.
Gayler - AAAS, 1982; Feb 82; [redacted]
Gears of the Mouth; Jul 79; Lasley D.
Geographic Trivia; Apr 80;
Glossaries versus Dictionaries: Which Should It Be?; Feb 75; Curin J.

P.L. 86-36

Golden Oldie: The Management Survey of the Philharmonic; Aug 74;
Golden Oldie: King Eusyb and Queen Deodi; Sep 74; [redacted]
Golden Oldie: An Unofficial Glossary of Weasel Words; Oct 74;
Golden Oldie: Establishment of Molecule Superseries; Feb 75;
Golden Oldie: SIMP Tables; Jun 75;
Golden Oldie: Blue Russian; Nov 75; [redacted] J.F.
Golden Oldie: Hidden Losses in COMINT Production; Apr 76; Gould R.E.
Golden Oldie: The Things They Say; Nov 76; Miller D.E.
Golden Oldie: Analyzation of Data; Oct 77; [redacted]
Golden Oldie: Unidentified Unit at Unknown Location; Jun 78;
Golden Oldie: On First Opening Kenney's 'Statistics'; Jan 79; Mountjoy M.
Golden Oldie: Reporting Message Volumes; Jun 82; [redacted]
Golden Oldie: Simplicity in Color; Feb 82; [redacted]
Golden Oldie: Tracks in the Sands of Time; Apr 82; Mason F.O.
Golden Oldie: The Reality of Communications Changes; Oct 82; [redacted]
The [redacted] Collection System; Jun 76; [redacted] T.
Grading The Russian PQE; Apr 81; [redacted]
Graphic Analysis of Linear Recursive Sequences; Dec 75; [redacted]
Graphic Names; Dec 76; [redacted]
The Great Soviet Shipbuilding Mystery; Dec 75; Williams D.H.
A Guide to Central Information, C5; Apr 75;
Guidesmanship--or How to Write Technical Manuals Without Actually Giving Anything Away; Nov 74; [redacted]
The Gulf of Tonkin Incident; Feb 75; [redacted] W.D.

H

EO 1.4.(c)
P.L. 86-36

The Hand Is Not Quicker Than the Eye; Mar 78; [redacted]
Has It Ever Been Translated Before?; Jul 78; [redacted]
Help Wanted; Apr 80; [redacted]
Henry Cement and other Phantoms of the Opera(tions); Jan 79; [redacted]
HF - The Rebirth; Jan 82; [redacted]
The Hierarchical Clustering of Cryptanalytic Data; Aug 76; [redacted]
A Historian Looks at SIGINT; Mar 82; Filby V.R.
A History Lesson; May 82; [redacted]
Hooray for PMDs!; May 75; [redacted]
How Are Your Stamina?; Jun 79; Fairbanks S.
How Do Adults Learn Language?; Apr 76; [redacted]
How Do We Know It's True?; Feb 76; Filby V.R.
How Do You Spell Peking?; Dec 78; [redacted]
How do You Tell These Two Clowns Apart?; Jan 79;
How Many African Countries Can You Spot?; Nov 77; [redacted] Dec 77; Rosenbluh H.G.
How Things Have Changed!; Jun 76; [redacted]
How to Create A User-Unfriendly System; Nov 81; [redacted]
How to Improve Your Promotion Potential; Jan 81; [redacted]
How to Make a Railroad Disappear; Nov 76; [redacted]
How Clean Does a Data Base Need to Be?; Jan 75; [redacted]
Human Factors: Responsible Documentation; Jun 82; [redacted]
Human Factors and Systems Design: An Estranged Relationship?; Jun 77; [redacted]
Human Factors and the Use of Microfiche Readers at NSA; Oct 77; Snow D.
Human Factors Newsletter; Jan 79;
Human Factors Corner: Information System; Jan 82; [redacted]
Human Factors Corner: Some Advice to Users of Unfriendly System; Feb 82; [redacted]
Human Factors Corner: But What Do I Do With My Papers?; Feb 82; [redacted]
Human Factors Corner: Data Gathering, How Do We Spend Our Day?; May 82; [redacted]
Human Factors Corner: Video Display Terminals and Vision of Workers; Aug 82; [redacted]
Human Factors Corner: Text Editors; Oct 82; [redacted]
Human Factors Corner: How Do People Organize Cooperative Work?; Nov 82; [redacted]
Hypnosis and Self-Hypnosis in Language Learning; May 76; Buckley D.

EO 1.4.(c)
P.L. 86-36

I

[redacted] Dec 78; [redacted]
I Remember SPELLMAN; Jul 78; Salemme A.J.
The 'Ice Age' and International Security; Apr 77; [redacted]
An Idea for an Article; Mar 78; Miller D.E.
In Praise of SOLITS; Nov 75; Grant L.G.
In Defense of The Indefensible: Notes on the Russian PQE; Feb 79; Tetrault E.W.
In Pursuit of: Faster Horses, Younger Women, Older Whiskey and More Money; Dec 81; [redacted] D.L.
[redacted] Nov 75; [redacted] W.L.
The NSA Information Desk: 'No Comment'; May 82; [redacted]
Initiatives in SIGINT Reporting; Aug 76; [redacted]
Integrated Analysts for Asia; Aug 76; [redacted] W.D.

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

P.L. 86-36

P.L. 86-36

EO 1.4.(c)
OCID: P4019695

P.L. 86-36

P.L. 86-36

[redacted] Mar 78; [redacted]
IRONHORSE: A Tactical SIGINT System; Oct 75; [redacted]
Is A Translator a Professional?; Jul 78; [redacted]
Is There a Doctor in the House?; Sep 77; [redacted]
Is There Life After Certification?; Sep 76; [redacted]
It's Party Time!; Jan 79; [redacted]

J

The Joys and Frustrations of Plural-Dropping; Jan 78; A.J.S.
The Joys of UNIX; May 78; [redacted]
JPRS Language Reference Aids; Sep 77; [redacted]

K

KITTIWAKE; Jan 81; [redacted]
Know Your Geography; Oct 78; [redacted]
Know Your Geography; Feb 79; [redacted]
Knowledge Resource Management at NSA; Sep 77; [redacted]
KRYPTOS News; Dec 82 [redacted]
KRYPTOS: A New Society; Feb 82; [redacted]
K1: SCA Field Management and Evaluation; Oct 77; [redacted]

L

P16 Language and Cryptologic Library; Apr 80; [redacted]
The Language of Beisbol in Everyday Talk; Aug 74; [redacted], Santiago-Ortiz R.A.
Language Career Panel: Clarification of Nov 78 Item; Feb 79;
Language in the News; Sep 74; [redacted]
Language in the News; Dec 74; [redacted]
Language in the News; Apr 75; Tetrault E.W.
Language in the News; Aug 75;
Language in the News: Language Rule; Apr 76;
Language in the News; Aug 76;
Language in the News; Sep 76;
Language Lessons Learned: A Personal Memoir; Oct 75; [redacted]
1976 Language Meetings and Conferences; Mar 76;
Language Processing Forum; Nov 77; [redacted]
Language Proficiency Certificates for Military Personnel; Aug 79; [redacted]
Language Skill File; Oct 76; [redacted]
The Last Word on IATS?; Apr 77; Phillips C.J.
Leadership: A Personal Philosophy; Oct 82; [redacted]
Learned Organizations--1974 CLA Essay Contest, 1974 CMI Essay Contest; CISI Prizes and Honors, Spring 74; Aug 74;
Learned Organizations--CISI Forms Special Interest Group on Human Factors; Dec 74; [redacted]
Learned Organizations--IAI News, CISI News; CLA is Ten Years Old!; CMI News; Jan 75;
Learned Organizations--CLA News; IAI News; May 75;
Learned Organizations--CLA News; CMI News; Jul 75;
Learned Organizations--CLA Essay Contest; CAA News; Dec 75;
Learned Organizations--1976 CLA Essay Contest; 1976 CMI Essay Contest; Sep 76;
Lenin and State Prizes: Now You See Them, Now You Don't!; Jan 76; [redacted]
Leo in October; Jan 76; Murphy A.I.
Let Me Repeat--And Make Myself Perfectly Clear; Aug 77; Jenks P.
Let's Give the Linguists a Bigger Piece of the Pie!; Dec 76; [redacted]
Let's Not Forget Our Cryptologic Mission; Feb 79; Curin J.
Let's Not Lose Out TA Skills; Mar 79; [redacted] G.
Letter From Canada; Nov 76; [redacted]
Letter From the Publisher; Jan 79; Lutwiniak W.
Letter: [redacted] Article; Oct 74; [redacted]
Letter: [redacted] Article; Dec 74; 'Anon.'
Letter: Citizens of World Puzzle; Feb 75; [redacted] G.P.
Letter: Exinterne Articles; Feb 75; Tetrault E.W.
Letter: Exinterne Articles; Apr 75; [redacted]
Letter: Professionalization of Bookbreakers; Apr 75; [redacted]
Letter: [redacted] Article; May 75; [redacted]
Letter: [redacted] Letter; May 75; [redacted]
Letter: [redacted] Letter; May 75; [redacted]
Letter: [redacted] Letter; Jun 75; 'Anon.'
Letter: Bookbreakers; Professionalization of Country Specialists; Jun 75; [redacted]
Letter: [redacted] Article; Jun 75; [redacted]
Letter: Typewriter Keyboard; Oct 75;
Letter: Proud and Bitter Memories Article; Mar 76; [redacted]
Letter: Proud and Bitter Memories Article; Mar 76; O'Neill K.
Letter: What Are We About? Article; Apr 76; [redacted]
Letter: Comments on [redacted] Letter on What Are We About?; Apr 76; [redacted]
Letter: [redacted] Article; Jun 76; Murphy A.I.
Letter: IRONHORSE Article; Oct 76; [redacted]
Letter: [redacted] Article; Oct 76; [redacted]
Letter: Cumulative Index; Nov 76; Bostick C.W.
Letter: 'Firebrand' Letter on [redacted] Article; Jan 77; [redacted]
Letter: [redacted] Article; Jan 77; Kenny M.M.
Letter: Mason Article; Jan 77; [redacted]

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

P.L. 86-36

DOCID: 4019695

P.L. 86-36

Letter: Use of Term 'Compartmented'; Jan 77; [redacted]
Letter: [redacted] Interview; Mar 77; [redacted] H.L.
Letter: [redacted] Article; Mar 77; Buckley D.
Letter: C-LINERS Article; Mar 77; 'Appalled'
Letter: Keyword Spotting; Mar 77; Gurin J.
Letter: [redacted] Article; Apr 77; [redacted]
Letter: [redacted] Article; Apr 77; [redacted]
Letter: Buckley Letter; Apr 77; Tetrault E.W.
Letter: Mason Article; Apr 77; Boucher M.J.
Letter: Mason Article; Apr 77; [redacted]
Letter: Mason Article; Apr 77; McGrillies J.R.
Letter: Buckley Letter; Jun 77; [redacted]
Letter: [redacted] Article; Jun 77;
Letter: Mason Article; Jun 77;
Letter: [redacted] Article; Jul 77;
Letter: [redacted] Article; Jul 77;
Letter: [redacted] Article; Jul 77; [redacted]
Letter: [redacted] Article; Aug 77; 'Weeson'
Letter: [redacted] Letter; Sep 77; Buckley D.
Letter: AG-22 Page Print; Oct 77; 'Reader'
Letter: [redacted] Article; Nov 77; Snyder S.S.
Letter: Salemme Article; Nov 77; [redacted]
Letter: Salemme Article; Nov 77;
Letter: [redacted] Article; Dec 77; [redacted]
Letter: [redacted] Article; Jan 78; [redacted]
Letter: [redacted] Article; Mar 78; [redacted] K.E.
Letter: [redacted] Article; Apr 78; 'Fennwatcher'
Letter: [redacted] Article; Jun 78; Gilbertson E.A.
Letter: [redacted] Article; Jul 78; Gurin J.
Letter: [redacted] Article; Jul 78; [redacted]
Letter: Gilbertson Letter; Sep 78; [redacted]
Letter: Pattie Article; Sep 78; Buckley D.
Letter: Salemme Article; Sep 78; Williams D.H.
Letter: NSA-Crostic; Oct 78; [redacted]
Letter: NSA-Crostic; Oct 78; Filby V.R.
Letter: [redacted] Article; Oct 78; Pattie M.T.
Letter: Appraisal System; Nov 78; 'Anon.'
Letter: Appraisal System; Nov 78 [redacted]
Letter: [redacted] Article; Nov 78; [redacted]
Letter: Ask Art; Apr 79; 'Sue'
Letter: Library Changes; Jun 79; [redacted]
Letter: Library Changes; Jun 79;
Letter: 'Sixth Language'; Jun 79 P.A.
Letter: [redacted] Article; Jun 79; Bjorklund K.
Letter: Bjorklund Letter (Jun 79); Jul 79; [redacted]
Letter: Bjorklund Letter (Jun 79); Jul 79; Buckley D.
Letter: [redacted] Article (Apr 79); Jul 79; [redacted]
Letter: Buckley a[redacted] (Jul 79); Aug 79; [redacted]
Letter: Data Standards; Mar 79; [redacted]
Letter: Grant Article (Dec 78); Feb 79; Pattie M.T.
Letter: Gurin Article (Feb 79); Apr 79; [redacted]
Letter: [redacted] Article (Dec 78); Feb 79; Bostick C.W.
Letter: Linguatrivia; Jul 79; [redacted]

Letter: [redacted] Article (Aug 79); Oct 79; Taylor D.L.
Letter: Screening Radiation; Aug 79; [redacted] W.E.
Letter: [redacted] Letter (Aug 79); Aug 79; [redacted]
Letter: [redacted] Article; Jan 82; Chauvenet L.R.
Letter: Stairwell Society Article; Jan 82; [redacted]
Letter: Cryptanalysis Article; Jan 82; [redacted] A.
Letter: UNIX Article; Feb 82; [redacted]
Letter: Strangest Bust of the Month; Mar 82; [redacted]
Letter: The Literary Bends Article; Mar 82; Murphy A.I.
Letter: A Toy Problem; Mar 82; Tiren D.J.
Letter: Plaintext; May 82; [redacted]
Letter: [redacted] Article; May 82; [redacted]
Letter: Shell Game Article; May 82 [redacted]
Letter: Editorial Comment; Jun 82; [redacted] P.A.
Letter: Personal Computer Article; Jun 82; [redacted]
Letter: Shell Game Article; Jun 82; [redacted] P.A.
Letter: Shell Game Article; Jun 82; [redacted] J.W.
Letter: Kudos; Sep 82; [redacted]
Letter: Shell Game Article; Nov 82; [redacted]
LIME-A, OHIO; LEEM-A, Peru; Apr 80; Salemme A.J.
A Linguist Looks at the Tube; Mar 78; Johnson R.S.
Linguists From The Melting Pot; Dec 75; Gould R.E.
Linguists -- You Have an Expert to Call!; Oct 75; [redacted]
Linguists -- We Need An 'Experts Yellow Pages'!; Aug 75; [redacted]
Linguist Machine; Aug 82; [redacted]
Linguistics and the Code Reconstructor; Nov 78; Buck S.H.
LIP; Jan 80; [redacted]
The Literary Bends; Jan 82; Murphy A.I.
Literature Search On-Line; Feb 79; [redacted]
A Little PEP Talk; Apr 78; [redacted]
A Little TA Problem; Nov 77; [redacted]
A Long Hard Look at the Intern Program--Program Philosophy; Recruitment (Part One); Sep 74; 'Exinterne'
A Long Hard Look at the Intern Program--Selection and Orientation (Part Two); Oct 74; 'Exinterne'
A Long Hard Look at the Intern Program--Motivation and Morale (Part Three); Nov 74; 'Exinterne'
A Long Hard Look at the Intern Program--What Happens to the Graduate? (Part Four); Dec 74; 'Exinterne'
Looking at Mr. [redacted] Apr 78; [redacted]

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

P.L. 86-36

M

EO 1.4.(c)
P.L. 86-36

Machine Course for Linguists; Apr 75; Tetrault E.W.
Machine Intelligence--Promise or Delusion?; Jul 75; [redacted]
Machine-Produced Aids for the Linguist, Part I; Sep 76; Salemme A.J.
Machine-Produced Aids for the Linguist, Part II; Oct 76; Salemme A.J.
Partial Machine Translation: Final Report; Apr 82; [redacted]
Maps in Mind--A Photoessay; Dec 74; [redacted]
The Marquis and the Medium; Jun 76; Dawson R.
Match Them Up!; Jul 77; [redacted]
A Matter of Style; Sep 78; [redacted]
Memorable Memos; Aug 79;
Meteorburst Communications; Mar 82; [redacted]
A Method for Measuring Negative Intelligence; Oct 78; [redacted].
The Micro Revolution: Arthur Young Study Comment; May 82; [redacted]
Middle-Age Spread; Apr 81; [redacted]
NSA/CSS Military Linguist Program; Jan 80;
Minnie's Mini; Jun 78; Kenny M.M.
The Mission of the Signals Processing Requirements Panel; Oct 74; [redacted]
More about More about the NSA SIGINT Summary; Jun 77; Boucher M.J.
More about the NSA SIGINT Summary; Mar 77; [redacted]
More B.S. (Before Spellman); Oct 78; [redacted] C.H.
More Beans; Feb 78; Pilby V.R.
More Comments on the AG-22/IATS; Sep 76; [redacted] B.
More Fairbanks on English; Apr 79; Fairbanks S.
More Fairbanks On English; May 79; Fairbanks S.
More Free Goodies; Sep 82; [redacted]
More Than Words Can Say; May 79; Gurin J.
More Thoughts on 'Questionable' SIGINT; Oct 76; [redacted]
More on Squaring the Page (A Crypto-TA Function); Jun 75; Mason F.O.
[redacted] Oct 78; [redacted]
Mum's Still the Word! ('The ULTRA Secret'); Dec 75; [redacted]
Musings About the AG-22/IATS; Mar 76; Phillips C.J.

EO 1.4.(c)
P.L. 86-36

N

The Navajo Code Talkers; Jun 75;
Native Scripting of Languages; Feb 82; [redacted]
Naval Readiness: A Basis for Comparison; Jul 79; [redacted]
NCS-CLA Symposium; Jan 81;

P.L. 86-36

NCS Offers Course-Equivalency Tests; Nov 75;
NCS Offers Course-Equivalency Tests, Clarification; Apr 76;
NCS Summer Language Program; Oct 79;
Never Again!; Jun 78; Gurin J.
Never on My Watch; Nov 78; [redacted] Jan 78; [redacted]
New Directions for the U.S. Intelligence Community; Aug 77; Gaddy D.W.
The New Traffic Analysis Glossary; Aug 74;
New Trends in the Teaching of Cryptanalysis; Nov 74; [redacted]
The New Collection Criteria; Dec 74; [redacted]
There's a New World Coming - Are You Ready?; Jan 80; [redacted]
News from NCS--Agency Resumes Hiring of LICs; NCS Offers Course in 'SIGINT Appreciation'; Oct 74;
Nice Busman's Holiday for One NSA Employee; Aug 74; Dudley B.
1972-1973: A Vietnam Odyssey; Oct 75; [redacted]
No, Winnie, You've Got It Upside Down Too!; Feb 78; A.J.S.
[redacted] Sep 78; [redacted]
Normandy: 1944; Sep 82; [redacted]
Note on FRANCOPHONEGLOS; Aug 76;
Notes on Translation from the Chinese; Jun 76; [redacted]
NSA Cryptologic Collection; Aug 76;
NSA in Vietnam: Proud and Bitter Memories; Oct 75; [redacted]
NSA-Crostic No. 1; Oct 75; A.J.S.
NSA-Crostic No. 2; Jan 76; A.J.S.
NSA-Crostic No. 3; Apr 76; A.J.S.
NSA-Crostic No. 4; Jun 76; A.J.S.
NSA-Crostic No. 5; Oct 76; A.J.S.
NSA-Crostic No. 6; Jan 77; A.J.S.
NSA-Crostic No. 7; Apr 77; Chauvenet L.R.
NSA-Crostic No. 8; Jul 77; A.J.S.
NSA-Crostic No. 9; Sep 77; Williams D.H.
NSA-Crostic No. 10; Nov 77; A.J.S.
NSA-Crostic No. 11; Jan 78; Williams D.H.
NSA-Crostic No. 12; Mar 78; A.J.S.
NSA-Crostic No. 13; Apr 78; Williams D.H.
NSA-Crostic No. 14; May 78; 'Sardonyx'
NSA-Crostic No. 15; Jun 78; A.J.S.
NSA-Crostic No. 16; Jul 78; Williams D.H.
NSA-Crostic No. 17; Sep 78; A.J.S.
NSA-Crostic No. 18; Oct 78; Williams D.H.
NSA-Crostic No. 19; Nov 78; Williams D.H.
NSA-Crostic No. 20; Dec 78; Williams D.H.
NSA-Crostic No. 21; Jan 79; Williams D.H.
NSA-Crostic No. 22; Feb 79; D.H.W.
NSA-Crostic No. 23; Mar 79; Salemme A.J.
NSA-Crostic No. 24; Apr 79; D.H.W.
NSA-Crostic No. 25; May 79; D.H.W.
NSA-Crostic No. 26; Jun 79; D.H.W.
NSA-Crostic No. 27; Jul 79; D.H.W.
NSA-Crostic No. 28; Aug 79; D.H.W.
NSA-Crostic No. 29; Oct 79; D.H.W.
NSA-Crostic No. 30; Jan 80; D.H.W.
NSA-Crostic No. 31; Apr 80; D.H.W.
NSA-Crostic No. 32; Jan 81; D.H.W.

P.L. 86-36
EO 1.4.(c)
P.L. 86-36
P.L. 86-36

EO 1.4.(c)
DOCID: 4019695

P.L. 86-36

NSA-Crostic No. 33; Apr 81; D.H.W.
NSA-Crostic No. 35; Oct 81; D.H.W.
NSA-Crostic No. 36; Dec 81; D.H.W.
NSA-Crostic No. 37; Jan 82; D.H.W.
NSA-Crostic No. 38; Feb 82; D.H.W.
NSA-Crostic No. 39; Apr 82; D.H.W.
NSA-Crostic No. 40; May 82; D.H.W.
NSA-Crostic No. 41; Jun 82; D.H.W.
NSA-Crostic No. 42; Aug 82; D.H.W.
NSA-Crostic No. 43; Oct 82; D.H.W.
NSA-Crostic No. 44; Nov 82; D.H.W.
NSA-Crostic No. 45; Dec 82; Dawson R.
NSA Promotion Boards: How They Work; Aug 79; [redacted]
NSA's System for Grading Translations; Aug 76; [redacted]

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

P.L. 86-36

An Objective Approach to Scoring Translations; Mar 76; [redacted]
Objective Satisfaction Score: Collection Performance; Nov 77; [redacted]
An October Overlap; Oct 74; [redacted]
Answer to An October Overla ; Nov 74; [redacted] J.E.
Odds and Ends; Jun 82; EO 1.4.(c)
OH, KI; Apr 80; [redacted] P.L. 86-36
Is There An Old Crow In Your Future?; May 82; [redacted]
The Old [redacted] Section; Dec 74; [redacted]
Old Phone Books Never Die; Mar 82; Nolte W.M.
An Old Problem; Aug 82; [redacted]
Old Russian Manuscript Ciphers; Jun 77; [redacted]
An Old Timer Is One Who; Nov 82; [redacted]
On Being Truthful; Apr 76; Gaddy D.W.
On Coming of Age at NSA: Confessions of an Ex-Linguist; Aug 79; [redacted]
Going On-Line With Information Aids; Dec 82; Gurin J.
One Day in Danang; Apr 76; [redacted]
One Chance in Three--But It Worked; Oct 75; Gerhard W.
OPELINT Is Alive and Well In B Group; Nov 81; [redacted]
Oral Reporting: A New Challenge for NSA; Apr 75; [redacted]
Overheard in the Burnbag Line; Oct 78;
Overheard While Standing in the Burnbag Line; Apr 82;
An Overview of Project [redacted] Mar 77; [redacted]

Partners in the Exciting Future of SIGINT; Oct 77; Rosenblum H.E.
Passwords; Dec 82; [redacted]
The Internal Performance Evaluation: Friend or Foe?; Feb 82; [redacted]

P.L. 86-36

The Perils of Being a State Department Interpreter; Oct 77;
A Personal Comment on Winterbotham's 'The ULTRA Secret'; Dec 75; Tiltman J.H.
Personal Computer Application; Apr 82; [redacted]
A Personal Computer: A Current Cryptanalysis Support Tool; Mar 82; [redacted]
A Personal Footnote; Jun 82; [redacted]
Plain English; May 77; [redacted]
PLATFORM: How Did You Say That Works?; Dec 81; [redacted]
The Poet's Corner; Apr 81;
The Polyhedral War; May 77; [redacted] Diesso M.
Postscript to 'Dating Game'; Aug 77; [redacted]
The PPC Is Coming!; Nov 81; [redacted] Jun 78; [redacted]
The Prebendary and the Prophet; Feb 76; Dawson R.
Prizewinners in Three Holes; Apr 78;
Processing [redacted] Communications; Aug 75; [redacted]
Professionalizing in Computer Systems; Jun 75; [redacted]
Progress-1: [redacted] Sep 78; [redacted]
Project CARRIAGE: Worldwide HPDF Modernization Plan; Sep 74; Webster J.B.
Project HELIPAD: An Epitaph; May 79; [redacted] M.L.
Project SYMBIOSIS; Jun 75; 'Anon.' P.L. 86-36
Project UTENSIL: The DDO Data Dictionary/Directory; May 78; [redacted]
A Proposal for Calendar Reform; Dec 74; Leahy F.T.
A Proposed Cure for the 'Performance Syndrome'; Mar 78; [redacted]
A Proposed Cure for the Time-in-Grade Syndrome; Nov 77; [redacted]
P.S.; Feb 79; [redacted]
Psyching the Code Clerk; [redacted] Apr 75; Callimahos L.D.
To Pull a 'Ponyal'; Mar 76; [redacted]
Punctuation: More Than Meets The Eye; Aug 79; [redacted] P.L. 86-36
Purity of the Russian Language--Slavophiles vs. Westernizers; Nov 74; [redacted]
Pursuit of the [redacted] Mar 79; [redacted] E.L.
Puzzle: Stinky Pinky; Aug 74; P.L. 86-36
Puzzle: Telephone Directory; Aug 74; EO 1.4.(c)
Puzzle: [redacted] Oct 74;
Puzzle: Secret Messages, 'Military Cryptanalytics'; Dec 74; P.L. 86-36
Puzzle: Citizens of the World; Dec 74;
Puzzle: Crossed Codewords; Jan 75; [redacted]
Puzzle: Can You Make Out the Name?; Feb 75; [redacted]
Puzzle: How Many Words in 'CRYPTOLOG'; May 75;
Puzzle: [redacted] Jun 75; [redacted]
Puzzle: CRY-PTO-LOGrolling; Aug 75; EO 1.4.(c) P.L. 86-36

P.L. 86-36

Puzzle: Match Them Up!; Jul 77;
Puzzle: Three Holes; Feb 78;
Puzzle: Who and Whom?; Oct 78;

Questions In Search of a PQE; Dec 82;

EO 1.4.(c)
P.L. 86-36

Jun 79;
M.R.
RAPIDTRAN:
Jul 75;
Readers' Survey; Mar 79; D.H.W.
Reduction Ratios in Micrographics; Oct 78; Snow D.
Reflections and Recommendations; Jan 79; Filby V.R.
Reflections on a Translator's Conference; Nov 74;
Remedial Software Engineering; Apr 78; J.F.
I Remember; Aug 82;
Replacement of the GUPPY Library; Feb 75;
Re-psychling the Code Clerk; Jul 75;
Research in Speech Perception (Dr. Ruth Day); Aug 76; Tetrault E.W.
The Return to HF; Jan 79;
Review of 'Guide to Russian Technical Translation' by Salemme; Feb 75; A.J.
Review: In The Name of Efficiency; Dec 81;
Review: The American Magic; Apr 82;
Review: What Do You Think?; Nov 81; M.E.
Revised Technical SIGINT Manual in Preparation; Mar 77; Filby V.R.
Right-to-Left Text Sorts Are Not Impossible; Aug 74;
The Roads Around Us; Oct 79; Chauvenet L.R.
The Role of the Electronic Warfare Advisory Element (EWAE) of NSA; Jun 75;
Rules For The Camel Corps; Mar 82; C.
Run This Through Your Transcription Machine; May 79;
Russian Handbook of Spoken Usage, Vol 3; Jul 79;

Say What You Mean; Nov 81; Gaddy D.W.
Scraps from the Editor's Desk; May 76; Salemme A.J.
Second Sighting; Jan 79; 'Donym'
Not Secret Anymore; Oct 82;
Secrets of the Altars--The Moustier Cryptograms; Sep 74
Self-Paced Instruction: The Future is Now!; Aug 74;
Semantic Voids: Don't Shoot the Translator; Sep 76;
Seminar on Translation Problems; Jul 79;
Senior Military Cryptologic Supervisors Course; Feb 78;
Shell Game; Apr 82;
Shell Game; Aug 82;
Shell Game: Counter; Dec 82; W.E.S.
Shell Game: AJSQUE; Dec 82;
Shell Game: PWB WHEN; Dec 82;
Loooong Shell; Jun 82;
The Exercise: A Case Study in Special Research Analysis; Oct 74; Filby V.R.
Shootout at the SIGINT Corral; Jul 79; P.S.
A Short Directory of Career Panels; Aug 74; Dec 78;
SIGINT Exploitation, 1990; Apr 78;
SIGINT In The 80s: Two Views; Jan 81; Rich R.E., Lutwiniak W.
Russian SIGINT and Electronic Warfare; Oct 76;
The SIGINT Users' Handbook or: What's an ISHTAR?; Jan 75; Oliver D.B.
SIGINT Welcomes INKSTAND; Jun 77;
SIGINT: 1990, Part One; Sep 82;
SIGINT: 1990, Part Two; Oct 82;
SIGINT: 1990, Part Three; Nov 82;
Sign Language; Jun 79;
A Simple Cipher Story; May 76; Meyer W.P.
Oct 79;
Sleep Well: Your SDO Is On Duty; Dec 81; Sawyer E.L.
63 Days--The Soviets in Space; Jan 76; J.
A Small Problem; Nov 78;
Snowballs On The Roof; Oct 79; Filby V.R.
Software - AAAS, 1982; Feb 82;
SOLIS: A Vehicle in Search of an Engine; Jan 79;
Some Background on the C/T Merger; Mar 78; Smith F.
Some Ideas about Mechanized Language Working Aids; Oct 76;
Some Principles of Cover and Deception; May 76;
Some Things Never Change; Jan 81;
Some Thoughts on Lexicography; Sep 74; Buck S.H.
Some Thoughts on the Russian PQE; Apr 77; Clark G.L.
Some Tips on Getting Promoted; Dec 78; V.C.
A Somewhat Larger Problem; Apr 79; W.E.
Source Protection: Our Agency's Insurance Policy; Jul 79;

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Soviet COMINT and the Civil War; Sep 78; [redacted] Apr 80; [redacted]
The Soviet General Staff; Jul 78; [redacted] Feb 78; [redacted]
A Soviet View of NSA; May 76; [redacted]
Speaking of Logging ...; Sep 77; [redacted]
A Spot by Any Other Name; Aug 74; Filby W.R.
The Stairwell Society; Oct 81; [redacted] Feb 78; [redacted]
The Story of MOSES; Jun 79; [redacted]
A Story With a Moral; May 77; [redacted]
System Acquisition Document Review; Jan 80; [redacted]

P.L. 86-36

T

Towards Better System Development; Mar 82; [redacted]
T Establishes Human Resource Development Panel; Sep 78;
T-Vision: The Reference Analyst's Medium of the Future; Jan 79; [redacted]
TA, Handmaiden of CA; May 75; Mason F.O.
TA Implications of FCC Proposal; May 78; [redacted]
Tactical Language Exploitation: A Lesson Learned?; Oct 75; [redacted]
Teacher Learns a Lesson; Nov 76; [redacted]
Teaching Computer Science To Linguists; Jun 79; [redacted]
Technical Support Catalogs; Oct 81; [redacted] K.J.
A Brief Treatise on Five Laws of Telephonic Communications; Mar 82; Nolte W.M.
Telephone Problem Here; Apr 78; [redacted]
Tell Me I'm Just a Sinobibliophobe; Jul 78; [redacted]
Telling It Like It Is; Aug 77; Santiago-Ortiz R.A.
TEXTA: What Is It? Where Is It Going?; Dec 81; [redacted]
TEXTA 'Word Seek'; Nov 76; [redacted]
TDB: The TEXTA Data Base; Aug 74; Jackson W.J.
The [redacted] Seminar Program; Sep 77; [redacted] W.L.
Thanks for the Attaboy!; Jan 78; [redacted]
Third Party Relationships; Apr 81; [redacted] Sep 78; [redacted]
TIDE: A Brief History; Dec 81; [redacted]
A Time for Change; Feb 82; [redacted]
TIPS is Still Alive and Well; Sep 76; [redacted]
Too Many Garbles; Jul 75; [redacted]
Tool Languages; Jul 77; Murphy J.D.
Toujours La Politesse (Japanese); Nov 76; Buck S.H.
To Whom It May Concern; Dec 78; Grant L.G.

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

Traffic Analysis: Specialty Without Portfolio; Apr 81; [redacted]
A Traffic Analyst Looks at Computers; Apr 80; [redacted]
Traffic Analysis of the Future; Jun 79; [redacted]
Transcriber-Analyst Relations; May 79; Miller D.E.
The Transcription Skill: Concepts and Teaching Methodologies; Jul 77; [redacted]
Translator In Your Pocket; Jan 81; [redacted]
Transliteration or Cyrillic?; Jun 76; [redacted] G.
Tribute to the Guru; Sep 77; 'Class 32'
True Base: Two Tales; May 82; [redacted]
TSS Revolution; Sep 82; [redacted]
Twenty Years of Transposition; Aug 75; [redacted] J.E.
Typewriter Random -- A New Look; Aug 75; [redacted]
The 2000-Year-Old Transcriber; Oct 79; [redacted] and a Little Bit of Luck; Feb 79; Williams D.H.

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

U

[redacted] Jun 78; [redacted] L.S.
Uncle-a Sam Wantsa You!; May 78; [redacted]
The 1981 URSI XX General Assembly; Dec 81; [redacted]
The Uses of Elegant English; Nov 76; [redacted] J.R.
The Uses of ELINT; Apr 75; [redacted] Mar 82; [redacted]
Universes, Galaxies, Stars, Bars, and Other Concepts; May 77; Phillips C.J.
UNNA [redacted] Jan 75; [redacted]
The Unseen Go-Between; Feb 78; Gurin J. [redacted] Oct 77; [redacted]

EO 1.4.(c)

V

P.L. 86-36

A Vexing Agency-Wide Problem; Oct 76; Mason F.O.
Vich Iss R-r-right?; Jun 77; A.J.S.
Video Encryption: A Report From EASCON 81; Jan 82; [redacted]
A View of the Central Computer Complex in the Late 1970s and Early 1980s; Mar 77; Phillips C.J.
A VIP Tour through the Attic of NSOC; Dec 78; [redacted]
VORD is a Better Idea; Mar 79; [redacted]
The Voynich Manuscript-Third Theory; Aug 75; Miller D.E.
The Voynich Manuscript Revisited; Apr 76; [redacted] Oct 75; [redacted] F.

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

W

A Wail, A Complaint, and a Melange; Feb 82; Snyder S.S.
Want to Play with a Pickfair Square?; Aug 77;
The Warsaw Pact [redacted] Jul 75; [redacted]
Waveguide Analysis; May 76; [redacted]
Weapon That Helped Defeat Nazis (Winterbotham's 'The ULTRA Secret'); Dec 75; Filby P.W.
Wedding Bells and That Old Gang of Mine; Nov 78; Sawyer E.L.
Well, Maybe a Sniffle or Two...; Feb 79; Pattie M.T.
What Are We About? (Fragments, Figments, or What?); Dec 75; [redacted]
What Ever Does 'However' Mean?; Nov 77; [redacted]
What Ever Happened to COPES?; Jan 78; [redacted] W.E.
What If the Linguists Disappeared?; Jan 77; [redacted]
What Is a Collector?; Aug 74; [redacted]
What Is an Information Research Analyst?; Aug 77; [redacted]
What Is Cipher Text?; Feb 76; [redacted]
What Is Pattern Recognition?; Dec 77; [redacted] D.A.
What Language Problem?; May 76; Pattie M.T.
What Made Them Do It? (Language Self-Study); Dec 77; [redacted]
What Promotion Boards Want; Aug 82; [redacted]
What Should You Expect? or, The Analysis of Cryptanalysts; Aug 74; [redacted]
What To Do About 'FANX'; Apr 80; [redacted]
What's the Best Location for the Computer Applications Function?; Apr 76; [redacted]
What's The Good (Pass)Word?; Oct 82; [redacted]
What's Wrong with AG-22/IATS?; May 76; [redacted] D.R.
What's In a Name?; Dec 76; [redacted]
What's In a Non-Name?; Sep 78; [redacted]
When Censorship Backfires; Nov 75; [redacted]
Where Do Good Transcribers Come From?; May 79; [redacted]
Where Does 'Does' Come From?; Jun 75; Tetrault E.W.
Where Were We?; Jan 77; Mason F.O.
Which Numbering System Should We Use?; Oct 77; 'Asken'
Which Tape Has the Intelligence? Project CRISELOR; Jul 77; Gurin J.
Whither the SRA?; Sep 77; [redacted]
Who Wants A Promotion, Anyway?; Jun 82; [redacted]
Why Are These People Smiling?; May 77; Harrison M.A.
Why Can't They Design a Good SR Test?; Dec 76; Bjorklund K.
Why Do They Leave?; Jan 81; [redacted]
Will It Really Do the Job?; Oct 78; [redacted]
Will the Real ELINT Please Stand Up; Apr 76; [redacted]
Wilt Thou, Angelina ...?; Jul 79; Fairbanks S.
The Winnah: Kid Apostrophe!; Oct 76;
Word Processing In A4; Apr 82; [redacted]
Word Seek; Mar 78; [redacted]
Work Quotas for Soviet Translators; Oct 76; [redacted]
W.W.II Japanese Translation at Arlington Hall Station; Jan 79;

P.L. 86-36
EO 1.4.(c)

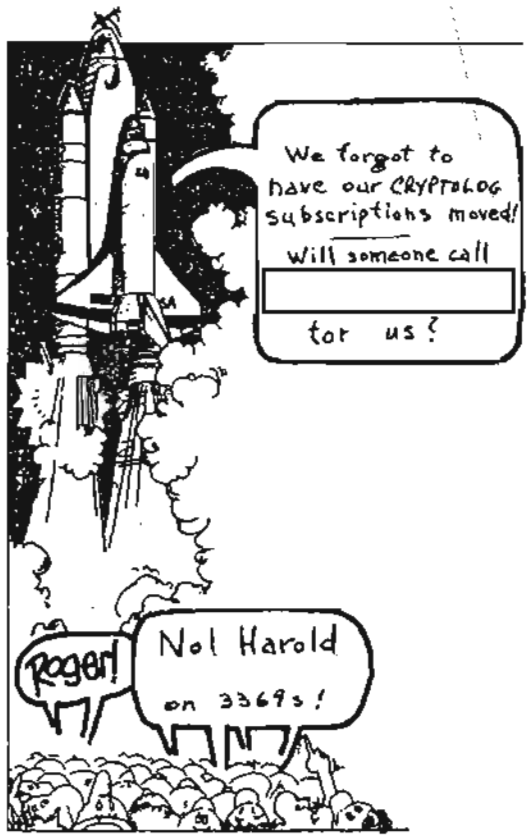
Y

The Yawn of the Computer Age or When Your Terminal is Terminal; Jan 75; [redacted]
Ye Gads! Another Country Trigraph System; Jul 78; [redacted]
Yes, Don, There is an ELINT!; Aug 76; [redacted] W.L.
You Can't Tell the Wheat from the Chaff Without a Program; Oct 78; Gurin J.

Z

P.L. 86-36

2BB? What In the World Is That?; Jul 77; [redacted] W.E.



P.L. 86-36

DOCID: 4019695

Government of the People, by the Party, ★ for the Leadership

BY

P.L. 86-36

The American student who spends a summer or a semester in the Soviet Union is usually quite impressed when he or she is given the customary tour of the Kremlin and is told about the Soviet government. It seems very similar to what one finds in the Western democracies. There is a bicameral assembly called the Supreme Soviet which meets in the ultramodern DOM SOVETOV, the House of Congresses. The Supreme Soviet, like the US Congress or British Parliament, is bicameral in that it consists of two bodies: the Soviet of Union, to which representatives are apportioned by population (one for every 330,000 citizens), and the Soviet of Nationalities, in which every political entity has a constitutionally determined number of deputies (32 for each republic, 11 for each autonomous republic, etc). These representatives and deputies are elected by the citizens of the Soviet Union and they, in joint session, elect the Presidium of the Supreme Soviet which handles the Supreme Soviet's business when the body is not in session. The chairman of the Presidium is very similar to the European idea of a president; he has very little power but he is the official representative of the Supreme Soviet and the Chief of State (PREZIDENT).

NOTE: This article was written before Brezhnev's death, but the situation is still so fluid that any statements made about Andropov might be obsolete before this article gets published.

Leonid Brezhnev was Chairman of the Supreme Soviet from 1977 until his death in November, 1982, and his successor Yuri Andropov was quickly elected to the post. (See NOTE.)

The Supreme Soviet also officially appoints the members of the Council of Ministers. This is the highest executive and administrative organ in the USSR and its chairman functions in a manner similar to a European Prime Minister. He is the person charged with the efficient functioning of the immense government bureaucracy and the proper coordination of the ministries sanctioned by the Soviet constitution. Alexei Kosygin was the Chairman of the Council of Ministers for almost 20 years; since his death the post has been filled by Nikolay Tikhonov.

For a simplified illustration of how the elective and appointive processes work, see Figure 1.

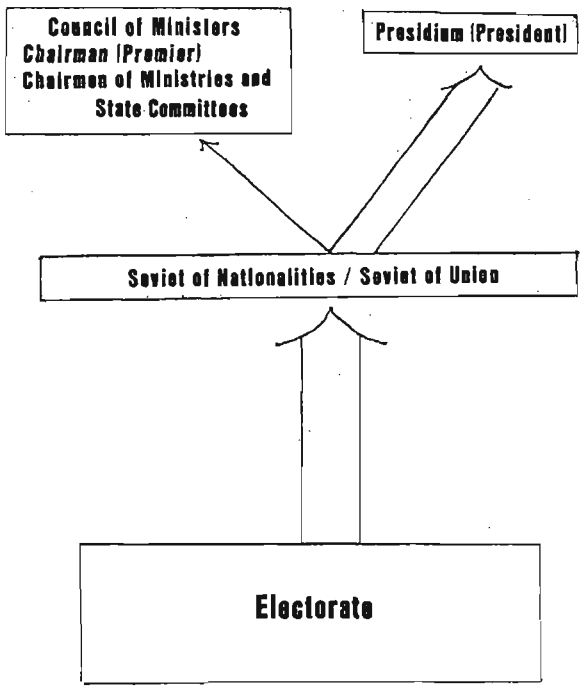


Fig. 1: The Government of the USSR (Theory)

But there are some very fundamental differences between the actual operation of the Soviet government and the way that Western democracies function. One of these differences should eventually become apparent to even the most apolitical visitor: The Soviets have equipped the DOM SOVETOV with a huge stage and orchestra pit and the use the House of Congresses for ballets when the Supreme Soviet is not in session. After three or four months of spectacular performances, our student might begin to wonder if the Soviet congress is ever in session. If he or she is in Moscow on a one-year program, that curiosity would really grow, for the entertainment never seems to stop for very long.

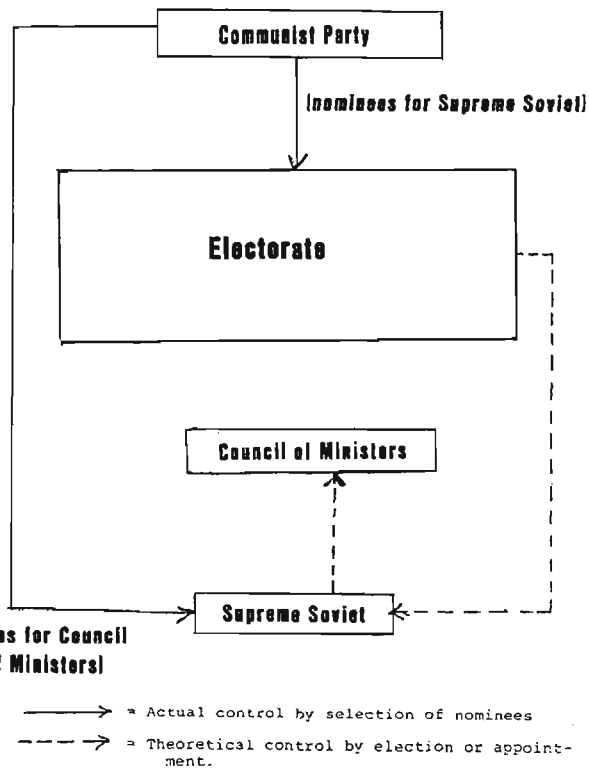
The explanation of this puzzle lies in the nature of the Supreme Soviet's deputies and their duties. They <u>are</u> elected by the citizenry, but the <u>selection</u> of the candidates is made by the Communist Party and those candidates are elected without opposition.

Secondly, when the representatives and deputies do meet in solemn session, it is to ratify and formally approve actions, positions, and appointments that have already been made by the Communist Party leadership. There is no discussion or debate; still less is there any introduction of new alternative items on the agenda at the behest of the representatives' constituents.

Finally, since the actual functions of the Supreme Soviet are so restricted, its sessions are very short, usually lasting only a few days. Thus the actual government functions very nicely with its official legislative branch out of session about 350 days of the year.

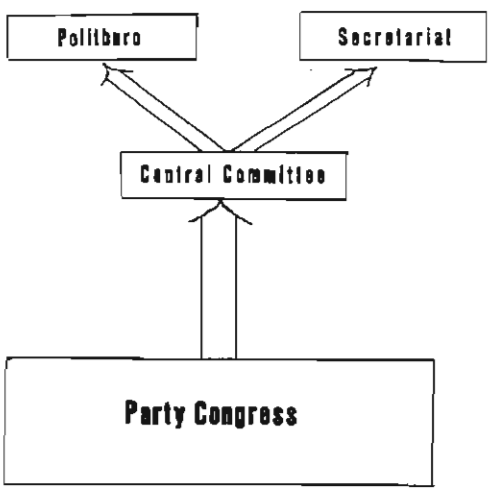
The Soviet government in practice is shown in Figure 2.

Fig. 2: Actual operation of the Soviet government



It would not be fair to say that the Soviet government is a facade designed to impress foreigners, for parts of it are the results of national experience that far antedated the Revolution. For over a thousand years the Russians have had authoritarian governments; changes, when they came, were decreed by the tsar, not demanded by outraged citizens. Representatives of the people, when they appeared, came to present a problem, not to make a decision or demand the enforcement of some regulation. Lenin's contribution to this tradition was an absolute requirement for discipline within his party. At the time of the Revolution this was a matter of survival. Without the discipline that Lenin had inspired, the Bolsheviks would have soon disintegrated into impotent bands of squabbling revolutionaries.

The trappings of democracy are important, albeit cosmetic. They provide an aura of participation in the formalities of government to the Soviet citizen without giving him any actual power or responsibility. These are the jealously guarded prerogatives of the Communist Party.



Symbols: ⟹ = elects

Fig. 3: Theoretical structure of the Communist Party

THE COMMUNIST PARTY

In theory the Communist Party structure is basically democratic, with the members at all levels being elected by those under them. The official apex of the Party structure is the Central Committee, which had 319 full members in 1981. The administrative control of the Party's own agencies and operations is in the hands of the Secretariat and the day-to-day execution of the Central Committee's mandates is entrusted to a standing committee called the Political Bureau or the Politburo. (See Figure 3.)

In practice, however, the flow of power and control within the Party is unidirectional--from the top. The Politburo is the apex of party control and the prime formulator of party policy. It is a collegiate body, containing within itself those key government officials and ministers who will actually implement its decisions. It is the Politburo that introduces the legislation or changes in the Constitution that will be ratified by the Supreme Soviet. And it is the Politburo which determines its own membership and that of the Secretariat.

The Secretariat is the most powerful administrative and executive organ in the Party. Besides directing all of the Party's internal and external affairs, the Secretariat also decides which Party members will stand for unopposed election to the Central Committee. (see Figure 4.)

There is little chance for serious conflict between these two bodies because many of the secretaries of the Communist Party are also members of the Politburo and, traditionally, the First Secretary of the Communist Party is also *primus inter pares* on the Politburo. Oddly enough, it is within the Politburo that free debate and discussion can intrude. The members of the Politburo can and do elect their own leader; Brezhnev's forte over the years was his ability to find consensus within this group.

Brezhnev served as First Secretary of the Communist Party, starting in 1970. Therein lay the source of his power, for within the Party he was the prime policy maker, the chief executive, and the ultimate nominator to party and government positions.

While there were policy discussions within the Politburo, all of the participants follow

the same ground rules and, by the end of Brezhnev's regime, most of them owed their exalted position to his influence. Opposition, if voiced, would tend to be circumspect. Furthermore, once decisions were made, both party instinct and self-preservation required an absolutely solid front to the rest of the world and to the party/governmental structure below them.

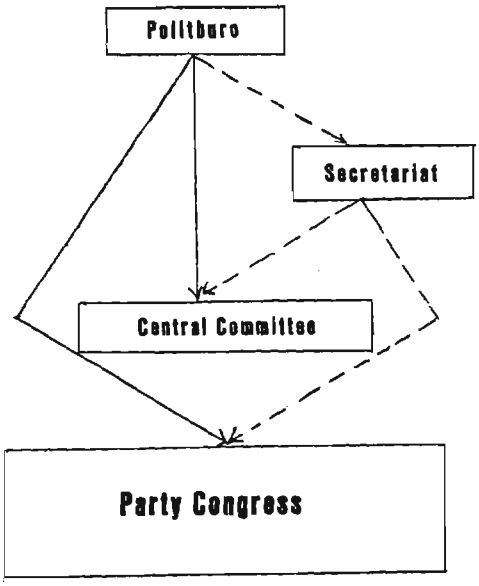
As the General Secretary of the Communist Party, Brezhnev did not need to negotiate. Everyone nominated for a Party or governmental position, whether he or she was to be appointed or go through the formality of an election, fell under his purview.

With that much power concentrated in his hands, one may wonder why Brezhnev even bothered to become PREZIDENT. Indeed, for may years the post was considered a dead end for careers and was used as an upper-echelon dumping ground where an old apparatchik could be deposited with many honors but no influence. Brezhnev may have had some personal reasons: he had the power, so why shouldn't he have had the honors too? However, being president had other advantages, especially in the area of protocol. When he was only the General Secretary of the Communist Party, Brezhnev had run into some awkward situations, especially when visiting Western nations; his only civil position was merely that of a humble delegate to the Supreme Soviet (from a district of his own choosing) and thus he had to go through the motions of deferring to the Premier or the President when one of those chiefs of government was a member of the official party. As Chief of State, he was able to receive 21-gun salutes and to review honor guards without encumbering himself with any onerous additional responsibilities.

PARTY CONTROL OF THE GOVERNMENT

While the domination exercised by the Communist Party over a supposedly democratic society may be abhorrent to the Western mind, there is no doubt about its status under Soviet law. Article 6 of the Soviet Constitution states:

> The leading and guiding force of Soviet society and the nucleus of its political system, of all state and public and social organizations, is the Communist Party of the Soviet Union. The CPSU exists for the people and serves the people.



Symbols: - - -> = Control by selection of nominees
——> = Control by selection of policy

Fig. 4: Actual operation of the Communist Party

> The Communist Party, armed with the teachings of Marxism-Leninism determines the general perspectives of the development of society and the course of the home and foreign policy of the USSR, directs the great constructive work of the Soviet people, and imparts a planned, systematic and theoretically sound character to their struggle for the victory of Communism.
>
> All Party organizations shall function within the framework of the Constitution of the USSR.

This is a key article in the Soviet Constitution and merits careful reading because:

1. While the CPSU is defined as existing for the people and serving the people, nowhere does it say that it is elected by or answerable to them.

2. It imparts blanket authorization to the CPSU to direct all state, public, and social organizations with the society and to determine internal and external policy without authorizing any group or agency

external to the Party to decide what should be included under these terms. If the party decides that stamp collectors constitute a social organization needing party direction, willy-nilly they will get that direction.

3. While many admirable rights are provided for individuals and groups under this constitution, the exercise and ultimate specification of these rights will be under the guidance of the Communist Party. Furthermore, the enforcement of these rights will be by agencies which will be under Party control.

There can be no doubt about the official status accorded to the Communist Party under the constitution. It has been given a license to kill. The only question that remains is how it exercises this power.

Figure 5 shows the various echelons of Soviet government and Party organizations. At first glance it would seem that we are dealing with two corresponding but separate entities, but this is not so. At each echelon the party exerts its power laterally to the corresponding governmental level and down to the subordinate Party organizations.

The Party exercises its control laterally through a combination of appointments and dual responsibilities. To begin with, all government officials at the upper levels are Party members and are subject to Party discipline. Furthermore, their appointment (or nomination to elective office) was authorized and approved by the Party bureau or secretariat. This is the situation that obtains throughout the ministries and directorates and committees under the Council of Ministers. However, there are some key positions that the Party officials have appropriated for themselves, resulting in one individual wearing two hats: one as a Party functionary and another as a government official. Leonid Brezhnev was a good example of one man riding two teams of horses: he was the General Secretary of the Communist Party and the dominant member of the Politburo; he was also the representative of the Bauman District in Moscow to the Soviet of Union and, last but not least, Chairman of the Presidium of the Supreme Soviet (PREZIDENT). Within the Party, Andrei Gromyko is a full member of the Politburo, as well as the Minister of Foreign Affairs and a member of the Council of Ministers. Another such minister who is also very prominent in the Politburo is Minister of Defense Dmitri Ustinov.

Yet the Politburo is unique in its composition. Its membership is completely open, both in number and official status. If the Politburo decides that someone's input is necessary or useful, he will be elevated to membership, at least as a candidate. Its present membership includes national, oblast, and city officials. For example, Vladimir V. Shcherbitskij is the Ukrainian Party Secretary, Grigorij V. Romanov is the First Secretary of the Leningrad Oblast party organization, and Viktor V. Grishin is the Moscow City First Secretary.

Also, since the Politburo is first and foremost a standing committee of the Party, a member does not have to hold a high governmental post in order to exert considerable influence. We have already seen that Brezhnev's governmental post was quite humble long after he had effectively taken control of the country. Similarly, the late Mikhail Suslov, who was in the Politburo for a quarter of a century and exerted enormous influence, served for years as the chairman of an obscure commission in the Council of Union.

PARTY CONTROL OF THE MILITARY

The Soviet military establishment appears to be similar to those of Western nations in that it is a ministry of the civilian bureaucracy. It is headed by a minister who is subordinate to the Premier and Chairman of the Council of Ministers. Like all the other state public and social organizations in the Soviet Union, it is under the guidance and leadership of the Communist Party according to the provisions of Article 6 of the Soviet Constitution.

However, there are other historical and social factors that make the military different. The party, whether headed by Lenin or Stalin or Khrushchev, has long realized that the military is one organized, disciplined, and armed organization with loyalties of its own that could be a real threat to Party control; for this reason they have kept it under particularly close scrutiny and have been reluctant to put the military in policy-making positions. While professional military men have been appointed Minister of Defense, the only one to be allowed into the Politburo since Stalin was the late Marshal Grechko, except for Marshal Zhukov, who was a member for a few months after Khrushchev seized power but was quickly eased out.

This is also one situation where personalities can make discerning the tail from the dog

DOCID: 4019695

difficult. Dmitri Ustinov, as Minister of Defense, is officially answerable to the Premier, Nikolaj Tikhonov. But, within the Politburo, Ustinov outranks the Chairman of the Council of Ministers, both in seniority and patronage.

The Soviet military differs from its western counterparts in that the Party does not have its functionaries actually running military positions or directorates. They realize that such an intrusion would seriously affect operational efficiency. But in other ways surveillance, if not control, follows the familiar pattern. To begin with, virtually all officers of field rank (major or equivalent) and above are members of the Communist Party, with a significant number holding elective positions in the government and the Party. This puts them under Party discipline and gives them Party obligations that could dilute their interests and obligations. As in the civilian sector, there is a separate Party organization following the military structure down to company level. (See Figure 6) This constitutes a separate chain of command. The man at the top, Gen-Army Yepishev, is accountable directly to the Politburo although he is administratively subordinate to the Minister of Defense and reports to him on the status of troop morale, discipline, and political work.

There is always the possibility, of course, that the Party watchdogs might develop a cozy, overly sympathetic relationship with the objects of their scrutiny. To avoid this, the Party has built almost baffling layers of redundancy into its surveillance: the Komsomols, the local Party organizations, and the military councils back up the military Party chain. The Procuracy and the Party Control Committees have their own direct lines to the Politburo....and keeping book on how well all of them are performing are the ubiquitous agents of the KGB (Committee for State Security). If anyone anywhere in the military is doing or thinking something heretical, someone will be informing the Party leadership.

CONCLUSION

Much more detail would have to be added to begin describing the civil, military, and Party structure of the Soviet Union completely: the lists of ministries and bureaus and committees and commissions in the Soviet Union and its member republics are almost endless. The various commands, directorates, and departments within the Ministry of Defense are perhaps even more confusing. But most of this is simply an extension or refinement of what has been presented here. The Soviets are remarkably consistent in this regard.

As this article was being written, it was announced in open sources that Andrej P. Kirilenko had retired from the Politburo. Shortly thereafter, the death of Leonid Brezhnev occurred followed by the accession to power of Yurij Andropov. But the nature of the Communist Party and the way it controls Soviet society will remain constant; the offices of PREZIDENT and General Secretary will not change. Indeed, a basic understanding of this system will be even more necessary as the survivors and their factions within the Politburo scramble for power in post-Brezhnev Russia. Without this understanding, you not only do not have a scorecard; you don't even know the rules of the game!

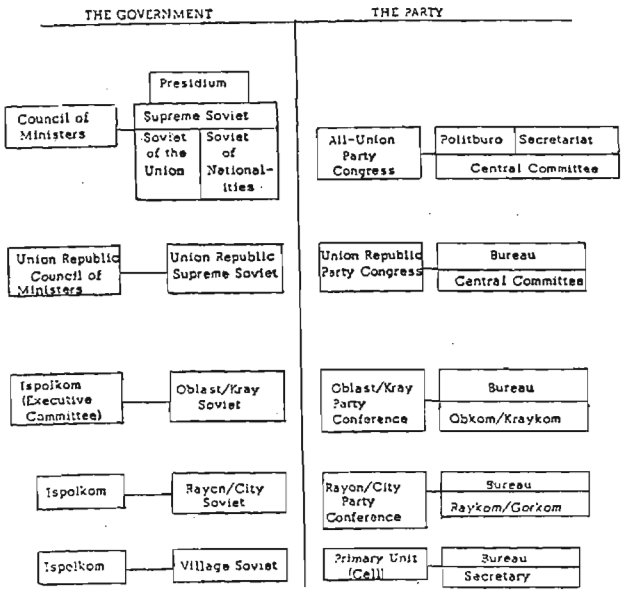


Fig. 6: Party and Government Echelons

AFTERWORD

The author would like to express his gratitude for the advice and assistance he received from Marc Brenner of the National Cryptologic School, who read the original drafts and provided invaluable source materials and who supplied the material for Figures 1 through 4. He also read over the original manuscript (prepared as a report while the author was serving as a Foreign Area Officer for the Army ITAC at FANX).

OCID: 4019695

Organization of the Main Political Directorate of the Soviet Army and Navy (MPD)

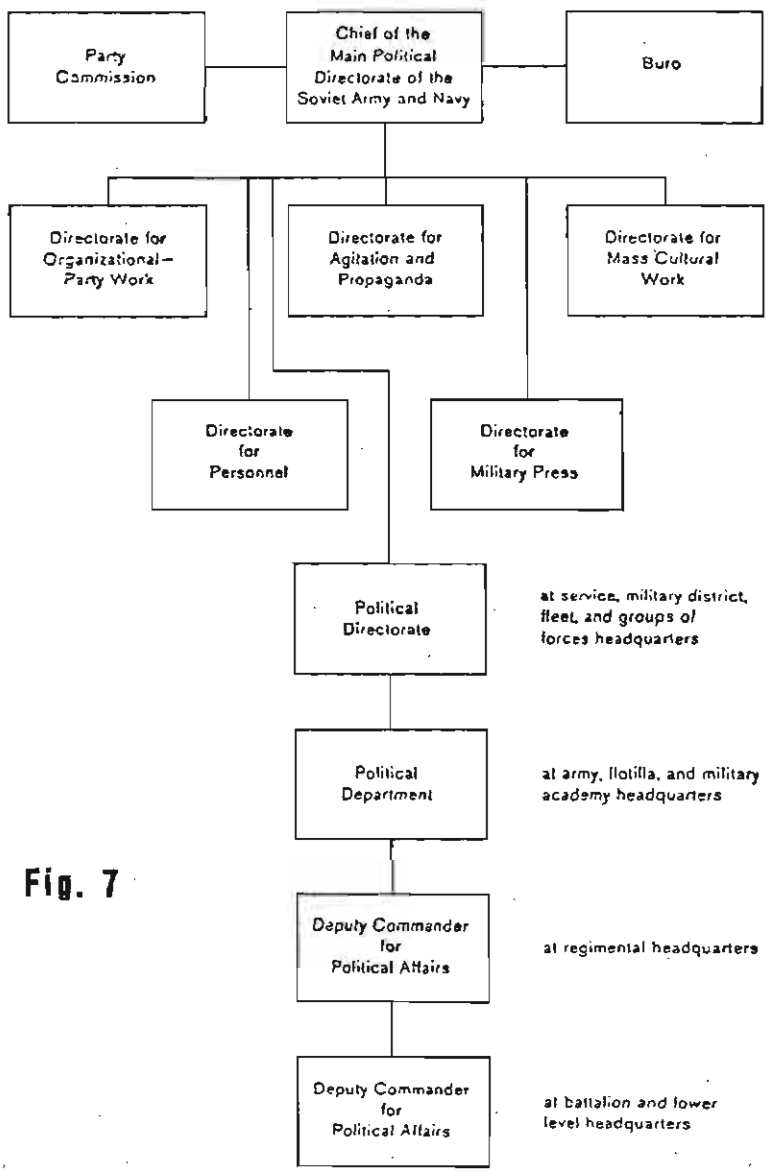


Fig. 7

OCID: 4019695

~~FOR OFFICIAL USE ONLY~~

SPECIFYING COLORS FOR COMPUTER GRAPHICS

by [redacted], P13

P.L. 86-36

The user of a color graphics system is frequently faced with the need to describe or name various colors he wishes to use for CRT displays. It is important for the user to be able to specify the exact hue, saturation, and lightness he wishes the colors to have. It is also necessary to specify the colors in such a way that typical color graphics systems can realize and display them. An article in the August issue of Communications of the ACM describes two color notation systems in general use for this purpose, and contrasts them from a human factors point of view against a third system devised by the authors (T. Berk, et al., "A Human Factors Study of Color Notation Systems for Computer Graphics," Comm. ACM, Vol 25, No. 8, August 1982, p. 547).

A typical color graphics system can realize up to 4,096 different colors. There must be some system of description or notation, however, to permit the user to select and specify the color that comes closest to what he has in mind. The notation system must also let him vary the parameters of a displayed color until he gets what he wants. Two commonly-used color notation systems for graphics are the RGB and HLS methods. The RGB system requires a user to specify a color in terms of its red, green, and blue primary components, corresponding to intensities of the electron beams that excite red, green, and blue phosphors on the color CRT. This means, essentially, that the user must describe his colors in a way closest to the internal workings of the system and farthest away from his natural (cultural and linguistic) ways of seeing and naming colors. To make matters worse, the RGB expression for a color consists of a triple of real numbers between 0 and 1, for instance [0.73, 0.63, 0.05]. This is a very cumbersome and unnatural way to describe a color for most people.

The HLS system allows the user a more natural way of specifying colors, in terms of hue, lightness, and saturation. Unfortunately, the mode of representation still depends on a triple of real numbers. For example, the same color used in the example of RGB above (a shade of yellow) would be shown as [0.142, 0.73, 0.93] in HLS. What is needed is a notation that provides the user with a natural and convenient way not only of describing the color he has in mind, but also of entering it into the system in some higher-level language so that it may be converted behind the scenes to the RGB-type internal representation required by the graphics system.

Well, how do people think and talk about colors when they are NOT using color graphics? In fact, color names (and, in some cases, even the number of different colors distinguished) are a matter of language and custom, varying among different cultures. Some cultures, for example, do not distinguish green from blue as we do, but call the whole range of hues between our green and blue by one name. As English speakers, we take for granted certain specific ways of describing and relating colors in a kind of "color space" with several dimensions along which we perceive colors to vary. When we are talking to other people

~~FOR OFFICIAL USE ONLY~~

OCID: 4019695

about colors, we can make use of a large vocabulary of specialized color words like "beige," "mauve," or "magenta," or phrases such as "Kelly green" or "burnt umber." As the paint salesman can testify, it is hard to communicate color changes or relationships accurately and operationally using this set of words ("Make it more beige." "I want a kind of tangerinish color but more toward the gold, kind of like a winter sunset!") But we also have another more logical linguistic system for color descriptions using a small number of color names which may be preceded by one or more adjectives, e.g., "vivid blue," "reddish yellow," "very dark purple." In this system, we might say "Make it more reddish" or "Make it lighter" to describe a change that would move a perceived color closer to a target area in our "color space."

Berk et al. have devised a third formal notation for colors, the CNS system. It is intentionally designed to be as close as possible to the natural English method of using color names and adjectives. The CNS system is based on a color lexicon of the Inter-Society Color Council and the National Bureau of Standards (ISCC-NBS). The syntax of CNS is shown below, with some sample color descriptions:

```
<color name> ::= <achromatic name> | <chromatic name>
<achromatic name> ::= [<lightness>] GRAY | BLACK | WHITE
<chromatic name> ::= <lightness> <saturation> <hue> |
                     [<saturation>] [<lightness>] <hue>
<lightness> ::= VERY DARK | DARK | MEDIUM | LIGHT | VERY LIGHT
<saturation> ::= GRAYISH | MODERATE | STRONG | VIVID
<hue> ::= <generic hue> | <halfway hue> | <quarterway hue>
<generic hue> ::= RED | ORANGE | BROWN | YELLOW | GREEN |
                  BLUE | PURPLE
<halfway hue> ::= <generic hue> - <generic hue>
<quarterway hue> ::= <ish form> <generic hue>
<ish form> ::= REDDISH | ORANGISH | BROWNISH | YELLOWISH |
               GREENISH | BLUISH | PURPLISH
```

Either or both lightness and saturation may be omitted and, in their absence, "MEDIUM" and "VIVID" are assumed. Only hues which are next to each other in the list may be combined to form halfway and quarterway hues. A total of 627 color descriptions can be generated.

Examples

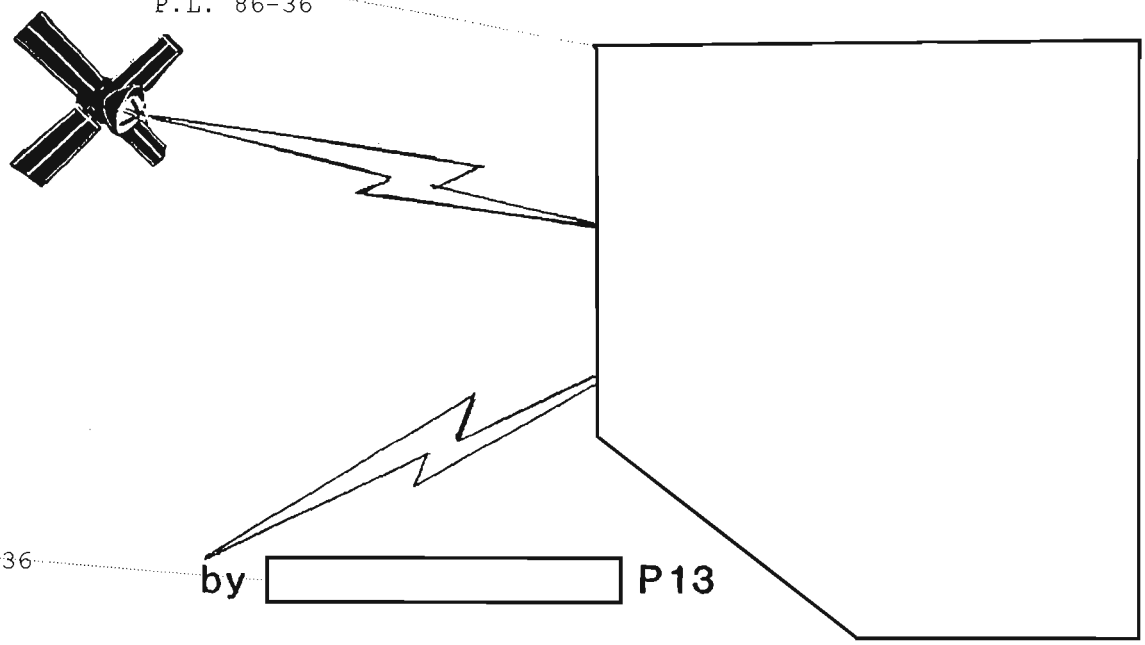
achromatic:
DARK GRAY; BLACK; VERY LIGHT GRAY; WHITE.

chromatic:
YELLOW, YELLOWISH-GREEN; YELLOW-GREEN;
MODERATE BLUE; LIGHT GRAYISH RED-ORANGE.

A human factors experiment was carried out to compare the accuracy with which people could describe colors using the three systems RGB, HLS, and CNS. The 37 subjects were computer science students at the Florida International University. An approximately equal number of students were taught each of the three systems, and then asked to give specifications for 20 different test colors on glossy pigment samples from the Macbeth Color Checker Color Rendition Chart. For each response, a distance was computed (measured in NBS Color Difference Units) between the color on the chart and the color the student's description would generate. The larger this distance turned out to be, the less accurate was the description. A 3x20 two-way analysis of variance found the effect of the notation system to be statistically significant ($p<0.001$). The RGB users were least accurate, HLS were next, and CNS were most accurate.

The authors note that CNS provides users with a relatively limited choice of discrete small regions along the three dimensions of the color space, while RGB and HLS provide a much larger and apparently more flexible set of choices. It might be expected, therefore, that users would have more trouble describing colors accurately using CNS. In fact, the opposite was true. Clearly, the naturalness of the CNS method more than offset any lacks it might have had in "power" or "flexibility." Berk et al. close their brief technical note with a summary that has wide-ranging implications for software design far beyond the limited area of color graphics: "In sum, the results of this experiment confirm the importance of human factors considerations in software development. In this instance, it has been shown that giving a user choice from a small set of values that are carefully chosen and based on human factors principles can produce better accuracy than providing a much larger and apparently more flexible set of values that are not based on such principles."

DOCID: 4019695 EO 1.4.(c) P.L. 86-36



P.L. 86-36 by P13

A Globecom 82 meeting described a number of related projects to provide rural African villages as small as a few hundred people with modern satellite communications. (U) The ITU (International Telecommunications Union) has sponsored and coordinated a number of these projects, and there have been meetings in Addis Ababa, Bangkok, Geneva, and Paris in the past few years on this topic. Significantly, the West German Ministry of Economic Development has set aside $500 million to finance the development of African telecommunications (and, incidentally, to create a market for German high-technology products). Traffic forecasts estimate as much as 15,000 erlangs of traffic to be carried over 20,000 two-way satcom circuits. An initial satellite, with 12 transponders which could each carry 600 two-way voice circuits (500 erlangs of traffic per transponder) could be in service in 1986 if the earth station problems could be solved. An erlang is an international (dimensionless) unit of the average traffic intensity of a facility during a period of time, normally an hour. The number of erlangs is the ratio of the time during which a facility is occupied (continuously or cumulatively) to the time this facility is available for occupancy.

(U) If this African domsat project is carried out, it could create a major change in global telecommunications during the next decade.

(U) Because rural Africa has virtually no surplus wealth, it would ordinarily be impossible to finance telephone links to the towns by either landline or satellite. On the other hand, the demand for telephone service is intense; in market towns the Africans will wait in queues all day to make a call from a public phone. Current telephone plant in rural Africa, where 85 percent of the population lives, is about 160,000 phones to serve a population of 250 million people. In essence, the sub-Saharan African countries can scarcely provide telephone service in their major cities and communications into the rural area, except for sound broadcasting, are generally limited and uncertain.

(U) The existence of the West German fund had put African telecommunications in a new light because it is now possible to capitalize a large-scale project. Apparently the aim of the German Government is to apply the money as part of its foreign aid program and, at the same time, create a market for the products and services of their very capable telecommunications manufacturers. Some of the money has already been used to fund ITU studies of rural African telecommunications and if the German scheme is enacted, the whole pattern of domestic intracountry African communications will undergo rapid and drastic change.

(U) Because demand-assigned single-channel voice circuits over satellite relay are favored as the best solution to rural telephony, the proposed transformation would eventually connect several hundred thousand villages and towns all over sub-Saharan Africa through a satellite relay. Three or four narrow spot beams would cover the continent from the southern edge of the Sahara to the border of South Africa. Thin-route terrestrial links, e.g., VHF single-channel radio links, would connect the smallest villages to the hamlets where the earth stations were located.

Between 10 and 50 percent of the rural traffic would connect into the major cities, so that the traffic content would reflect the complete infrastructure and internal activities of the countries and the wide range of languages and dialects that flourish throughout the continent.

Rural Communications

(U) The problem of rural African communications has been under study by the ITU and by private interests for some time.[1-10] One proposed satellite would use three 7° spot-beams at 4-to-6 GHz to cover most of Africa. Variations on this would use one 12° beam or four 4.5° beams. The narrower the beams the less power needed both in space and on the ground, but satellite complexity increases. The satellite, which would cost $200 million, would have to have high power and high sensitivity to allow the use of small, "cheap" earth stations. Some of the design ideas are very similar to concepts presented by Lusignan and his team at the Stanford University Communication Satellite Planning Center. (Libya and Mexico have adopted the CSPC software for their network planning.) The three downlink beams would operate at 4.0 GHz with 20 watts of power (eirp), "backed off" 5 dB. Because of the high elevation angles the downlink rain loss would be negligible at 4.0 GHz.

(U) The uplinks to the satellite would operate at 6.2 GHz with 3-meter antennas. For the 3-beam system, uplink power would be 0.5 watts and the antenna gain of 43.6 dB would give an earth-station eirp of 39.6 dBW.

(U) The earth stations are the crucial element of the system because of the need for low cost, ruggedness, and extreme reliability. The lack of electric power in the small towns and villages, for the forseeable future, is a critical factor in feasibility. More than half the African population lives in tiny villages with neither transportation nor lighting.

Table: Distribution of Rural African Population

Size of Village	Number of Villages	Mean Pop.	Total Pop.
0 - 400	324,000	200	64 million
400 - 1000	106,000	700	74 "
1000 - 4000	35,380	2,500	88 "
4000 -10000	3,503	7,000	24 "
Total	469,000		250 million

(U) Terrestrial nets already serve 160,000 phones. A combination of terrestrial nets, e.g., VHF single-channel radio links and satellite links in larger villages, would be used to serve a total population of 250,000 phones. The smallest villages would have no telephones. The traffic demand is estimated at .05 erlangs for the 700-person village (about one 3-minute call per hour during the busy part of the day). This aggregates over the thousands of villages to about 3,500 erlangs of traffic in the rural area, supplemented by 10 to 50 percent additional traffic to the urban centers. Traffic from the larger towns would increase this volume to about 18,000 erlangs.

Table: Distribution of Rural Traffic

Size of Village	Traffic Demand	Number of Phones	Total Demand	Demand (+50% Urban)
0 - 400	-			
400 - 1000	.05 erlangs	106,000	5,300	7,950
1000 - 4000	.15 "	106,000	5,300	7,950
4000 - 10000	.50 "	38,000	1,760	2,625
		250,000	12,360	18,525

(U) Because the economies and tribal relations frequently extend across the arbitrary borders of African nations, the rural traffic will often be transborder traffic unless the national PTTs prohibit this. Equipment will limit traffic growth, even if funding is available, for a typical transponder can carry only 600 two-way circuits and, to keep blocking below 1 percent, only 500 can be used for peak traffic. Another 10 circuits would be used for channel assignments and requests. DAMA (Demand-Assigned Multiple Access) will provide geographical flexibility, but a typical satellite with 12 transponders can carry only 6,000 erlangs of traffic. If such a satellite was launched in 1985-6, it would probably reach saturation in the early 1990s and a second satellite with 12 more transponders (or a new satellite with 24 transponders to replace the 1986 relay) would be needed. The DAMA system would be centralized, with centralized billing. This would give the national PTTs virtually complete control of all the earth stations, tariffs, and interconnections. There would presumably be a regional satellite operating agency serving the member nations as an "Africa COMSAT."

Table: Service from 12 Transponders

Size of Village	Number of Telephones	Number of Villages to be Connected
0 - 400	-	-
400 - 1000	31,000	31,000
1000 - 4000	31,000	10,000
4000 - 10000	10,000	1,000

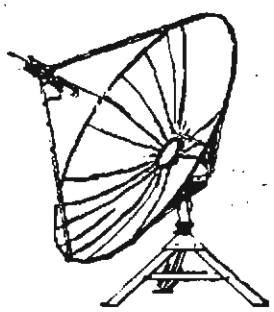
(U) This amounts to providing service to about one third of the villages of each size above 400 people, but over 300,000 smallest villages are left out of the satellite system in this initial system.

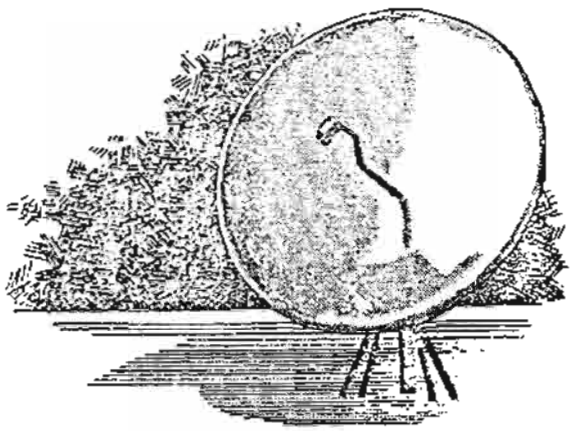
Earth Stations

(U) Once a satellite is put into operation, the spread and usefulness of the network depends on low-cost, reliable earth stations. A critical parameter for the SCPC design is frequency stability in both satellite and earth stations. Frequency accuracy of one part in 10 million is required in both the space and ground segments. Because the earth station will have to operate over a wide temperature range (as much as 50° Celsius), a reference standard is needed in each earth station. The earth station must have frequency agility to tune over 800 MHz in 30-KHz steps with errors no greater than 400 Hz and 600 Hz on the down and up links. Power is critical, for diesel generators are not considered a feasible power source in remote villages; the lacks of fuel, maintenance, and skilled operators are major problems. The earth station reliability criterion is that maintenance calls must be more than a year apart. This is a stringent requirement, but it is primarily a technical problem. The alternative would be a complex training program. The difficulty of training, operation, and maintenance for any kind of telecommunication equipment and power supply in rural Africa can be characterized in part by noting that with 1,700 local languages, instruction and advice and reference manuals of cassettes would have to be translated into hundreds of different languages.

(U) Small two-way earth stations with 3-meter dishes currently cost more than $100,000, not including power. Because terrestrial circuits must be connected into the earth station to serve feeder links to smaller villages, it must have a PABX (Private Automatic Branch Exchange). Each earth station can handle up to 10 telephone circuits if power is available. A difficult interface problem occurs where the earth station must connect into an existing telephone system, e.g., in a medium-sized town, because old-fashioned manually-operated switchboards with R2 signaling must be interconnected to the high-technology low-power terminal electronics.

(U) The advocates of GLODOM (Global Domestic) rural satellite systems are trying to reduce earth station electronics costs to $15,000, but even if they succeed the total cost for 3-meter earth stations will probably not go below $30,000. If the German government does provide $500 million for rural Africa's telecommunications and the space segment costs $200 million, some 10,000 earth stations could be funded in the initial phase with the remaining $300 million. This would equip only 7 percent of the villages and towns of more than 400 persons, but terrestrial nets could extend the coverage to many adjacent villages.





(U) Once an "early bird" Africasat network began to deliver services to the rural area, the extension of services would probably become a significant domestic political matter in Africa and the governments would apply persuasion to other nations to get additional funding in the form of loans, grants, etc., to extend the network. (At a 1980 meeting in the US one African Minister of Communications declared that telecommunications should be defined as a "basic human right," and the countries expect transfers of wealth and technology to provide these "rights.")

(U) Experience in South America has shown that once the primitive HF voice circuits are replaced by good-quality satellite voice circuits, the demand for long-distance traffic expanded sixfold overnight. African rural life centers around the market towns, where barter, trading, and other vital business transactions occur. Once telephone service to the larger towns and cities is available, a "hiding demand" for telephony is likely to be unleashed which presently cannot be seen in any conventional traffic studies. In a sense, the lack of transport and energy in the rural areas creates a greater demand for communications--a phenomenon manifested in the wide dispersion of sound broadcasting to over 19 million radio receivers.

(U) In addition to business traffic, growth in government traffic, personal traffic, and public service traffic also represent hiding demands, capable of explosive growth. In Australia medical services are provided to remote areas by HF radio circuits, with verbal descriptions of symptoms sent one way and medical advice and designations of specific treatments sent to the outstation. In the African context, telephony can be used to provide specific information and questions on agriculture, health, public health, weather, emergencies, etc., to improve health and the rural economy. This type of specific information is worth the cost of the call to the farmer, herdsman, or sick person.

(U) An important point that has not yet been resolved in planning rural African telecommunications is, even if a foreign grant capitalizes the initial plant, where will the operation and maintenance monies come from? In the case of potentially rich countries, which have oil or mineral resources, business customers and general revenues can be used to cross-subsidize the rural O&M costs. In the LDCs (Least Developed Countries), the only source of revenue is borrowing and the Western banks are becoming wary of the loans. On the other hand, World Bank studies have shown that telephone stations, even in poor countries, soon yield net revenues to the PTTs because of the value of the calls relative to other expenditures.

(U) Major telecommunications companies have been very skeptical about the business prospects for rural African satellite systems. The World Bank has also been skeptical of satellites.[11] The high cost of even small earth stations for conventional satellite systems has made satcoms appear a hopeless investment prospect for some of the poorest nations in Africa. However, the use of sensitive receivers on the satellite, with narrow spot beams, comes closer to making small earth stations a feasible investment. More important, there have now been several years of studies and conferences under ITU auspices,

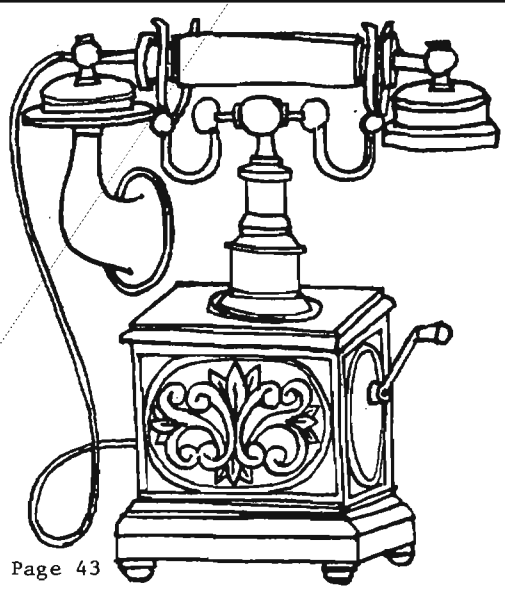
and the political leaders of both rich and poor nations are now thinking of telecommunications as a need which must be fulfilled by transfers from rich nations to Africa, without regard to return on investment.

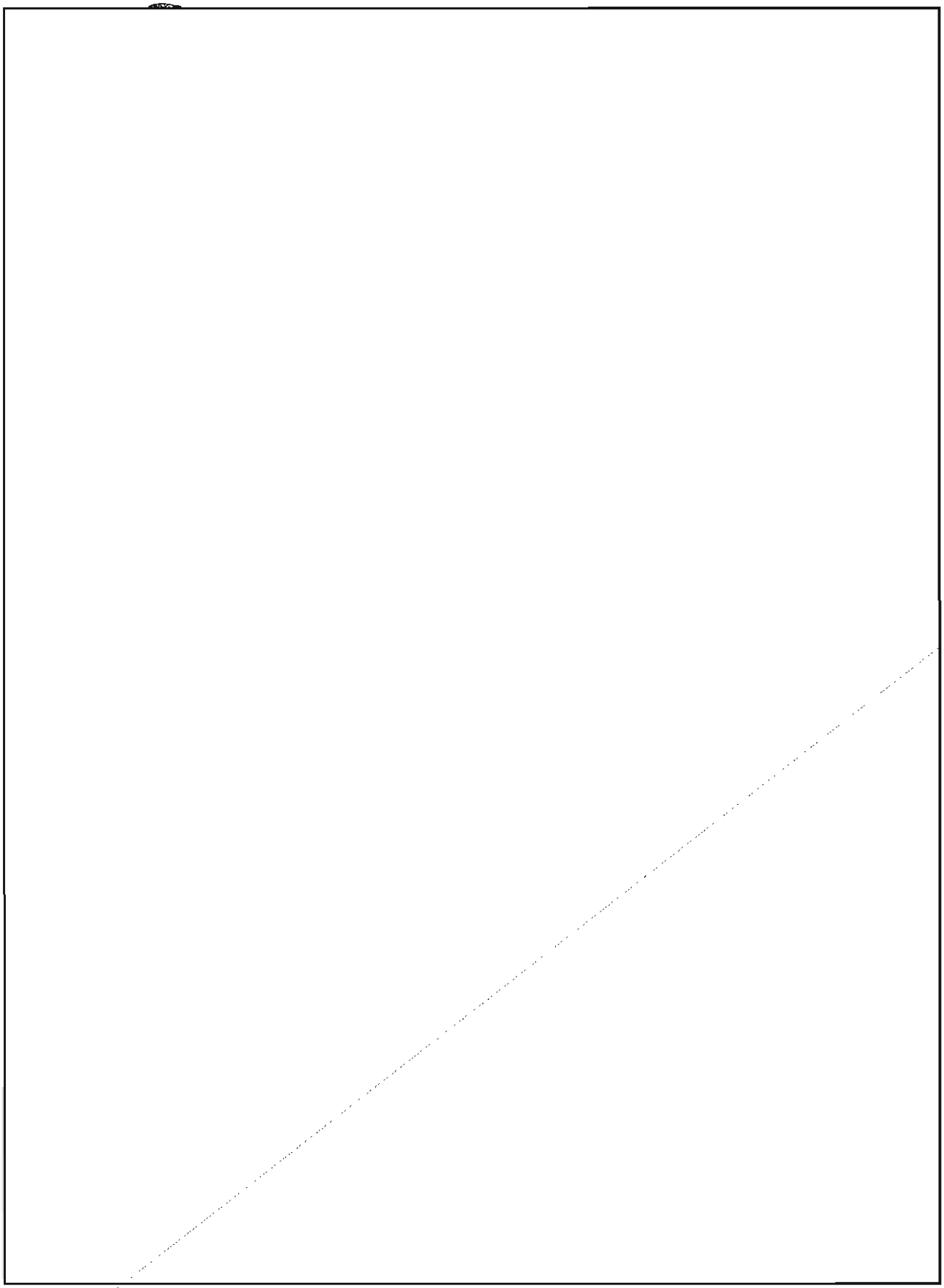
(U) Africa itself is becoming increasingly significant to the economies, politics, and strategic interests of the rich nations. The section of Africa running East-West from Namibia to Swaziland, known as "High Africa," is considered to be the "Saudi Arabia" of the mineral world. By 1990 the US and many other advanced nations will be unable to produce steel economically unless they get manganese from Africa or the USSR. Many other vital minerals, (e.g., cobalt, chromium, uranium) will also have to be obtained from Africa. The USSR and several satellite nations have spread economic and political fieldworkers into many African rural areas. There are also military and trade rivalries spreading between the African nations and being imposed on Africa from other parts of the world.

~~(FOUO)~~ Many of these economic and political influences will be manifested in the small towns and rural areas, as well as in the cities. Thus, there are East Germans, Czechs, Russians, Cubans, and other Soviet-bloc fieldworkers in various African countries. In parts of Africa the British and French have considerable presence, dating from their colonial period. Revolution and guerrilla warfare also express themselves in the rural areas. The continuous tension between white South Africa and the politically volatile Black African nations just northward lies, not by accident, along the mineral-rich area of High Africa. Politics, enormous potential wealth, dynamic change, and high strategy are woven across the continent, much of which is almost unchanged by the last thousand years of history.

~~(C-CCO)~~ One of the striking features of communications in rural Africa is that almost all of Africa, outside the main cities, is inaccessible to the West. As R. Richter notes in her book Whose News? (p. 241), the African governments are very reluctant to let any reporters, even their own, get out of the cities to see what is happening in the rural areas, where most of the population lives. One by-product of the Africasat is that the urban Africans would be able to find out more of what was happening outside the cities, and this is apt to make the traffic content more valuable because of the dearth of other sources of information.

P.L. 86-36
EO 1.4.(c)

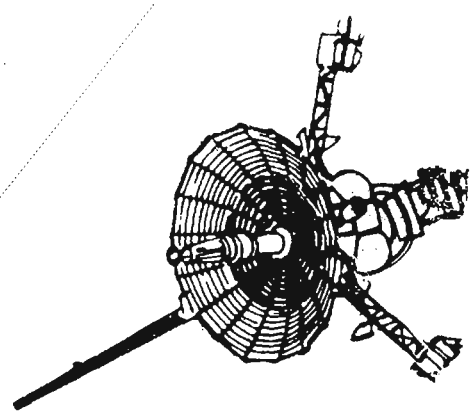


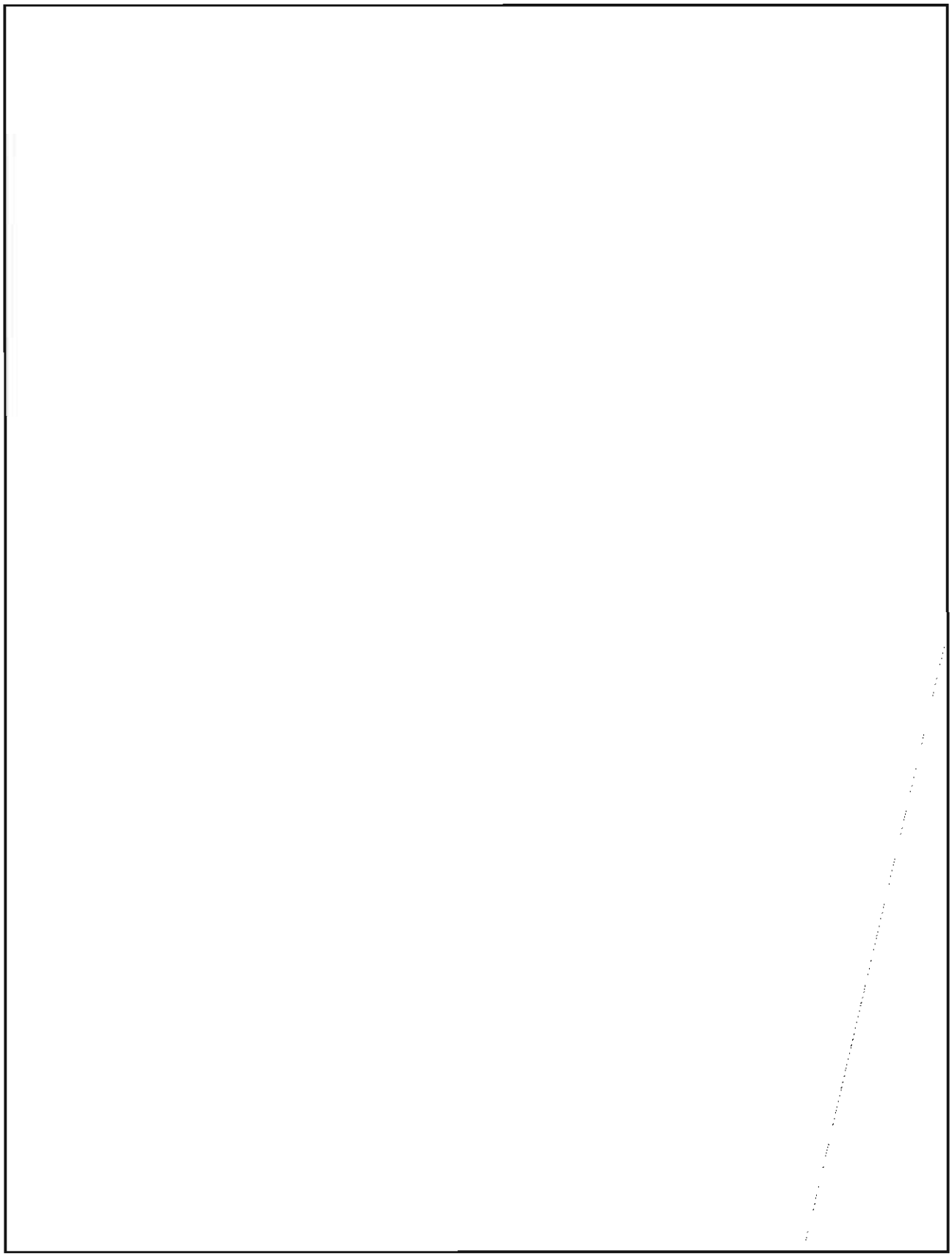


EO 1.4.(c)
P.L. 86-36
~~NOT RELEASABLE TO CONTRACTORS~~ ~~TOP SECRET UMBRA~~

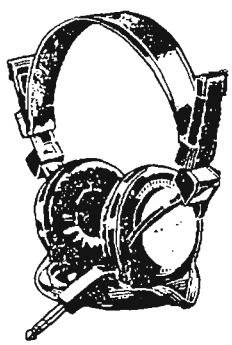
(U) The principal international languages in Africa are Arabic, French, English, and Portuguese. These would be spoken at a high level, or across long distances, as governmental and business languages. Within Africa there are a number of "lingua francas" such as Hausa or Swahili, which are spoken as second or third languages by millions of Africans who originally learned localized vernaculars. In Southern Africa the lingua francas are Fanagalo, Tswana, Lozi, Umbundu, Lwena, town Bemba, and Nyanja. Vernaculars in the same area include the Khoisan click languages such as !Kung, Hiechware, Kam, Nama Hottentot, Korana Hottentot, and Bantu languages such as Zulu, Xhosa Tswana, Kololo, and Chokwe-Lunda.[13] In Eastern Africa Swahili, Ganda, and Amharic serve as lingua francas, while Somali is the vernacular over a large area at the Horn of Africa. (But a dialect of Somali is used as the lingua franca between the different Somali dialects.) Other well-known lingua francas are Luba (or Chiluba), Kituba, and Lingala in the Congo basin, while the Niger-Congo family contains several dozen vernacular languages used in the same area. In western Central Africa Bulu, Yaunde, Duala, Bali, Adamawa-Ful, and Sango serve as lingua francas. On the West African coast Yoruba, Ewe, Twi, Ga, Mende, Temne, Susu, and Wolof are used as lingua francas. In the w
Sudan Hausa, Songhai, Mosi, Mandingo, Ma
Dyula, Bambara, and Kangbe serve the same function. Bambara, for example, is widely used as a soldiers' language and was used by the French for military recruiting. Many of the languages are known by various different names, and there are different spellings and even different alphabets for some languages. The Click Languages use various punctuation symbols such as !, #, and & to express different click sounds. To summarize, the language situation is very diverse and complicated, and the impact of modern telecommunications will change the linguistic situation fairly rapidly.

EO 1.4.(c)
P.L. 86-36





EO 1.4.(c)
P.L. 86-36



References:

1. Nickelson, R. L.,"Appropriate Satellite Systems for Rural Telecommunications," C5.1, GLOBECOM 82 Conference Record.

2. Laufenberg, W., "A Satellite Telecommunication System for Remote Areas in Africa," C5.2, GLOBECOM 82 Conference Record.

3. Fraser, J. M., "Interfaces in Rural Satellite Telephone Systems," C5.3, GLOBECOM 82 Conference Record.

4. Johannsen, K. G., "Rural Satellite Communication System Network Consideration C5.4, GLOBECOM 82 Conference Record.

5. Tustison, G. F., "An Earth Station Design for Rural Telecommunication," C5.5, GLOBECOM 82 Conference Record.

6. ITU Report, "Appropriate modern telecommunication technology for integrated rural development in Africa," Geneva, November 1981.

7. Pierce, W., and N. Jaquier, "Telecommunications and Development, general synthesis report of the ITU-OECD Project on the contribution of telecommunications to economic and social development," Geneva and Paris, April 1982.

8. Meyer, J. A., "Digital Meteorburst Communication," INTELCON 80 Conference Record.

9. CCIR Draft Report, "Requirements of a Rural Domestic Satellite System," Question 23/4, 26 June 1981.

10. Space Technology and Africa; OTRAG: why we are in Africa. Special Study, Africa, Dec 1977, No. 76. pp.49-57. Africa Journal Ltd., London.

11. Saunders, R., World Bank, statement to the author at INTELCON 80, Nov 1980.

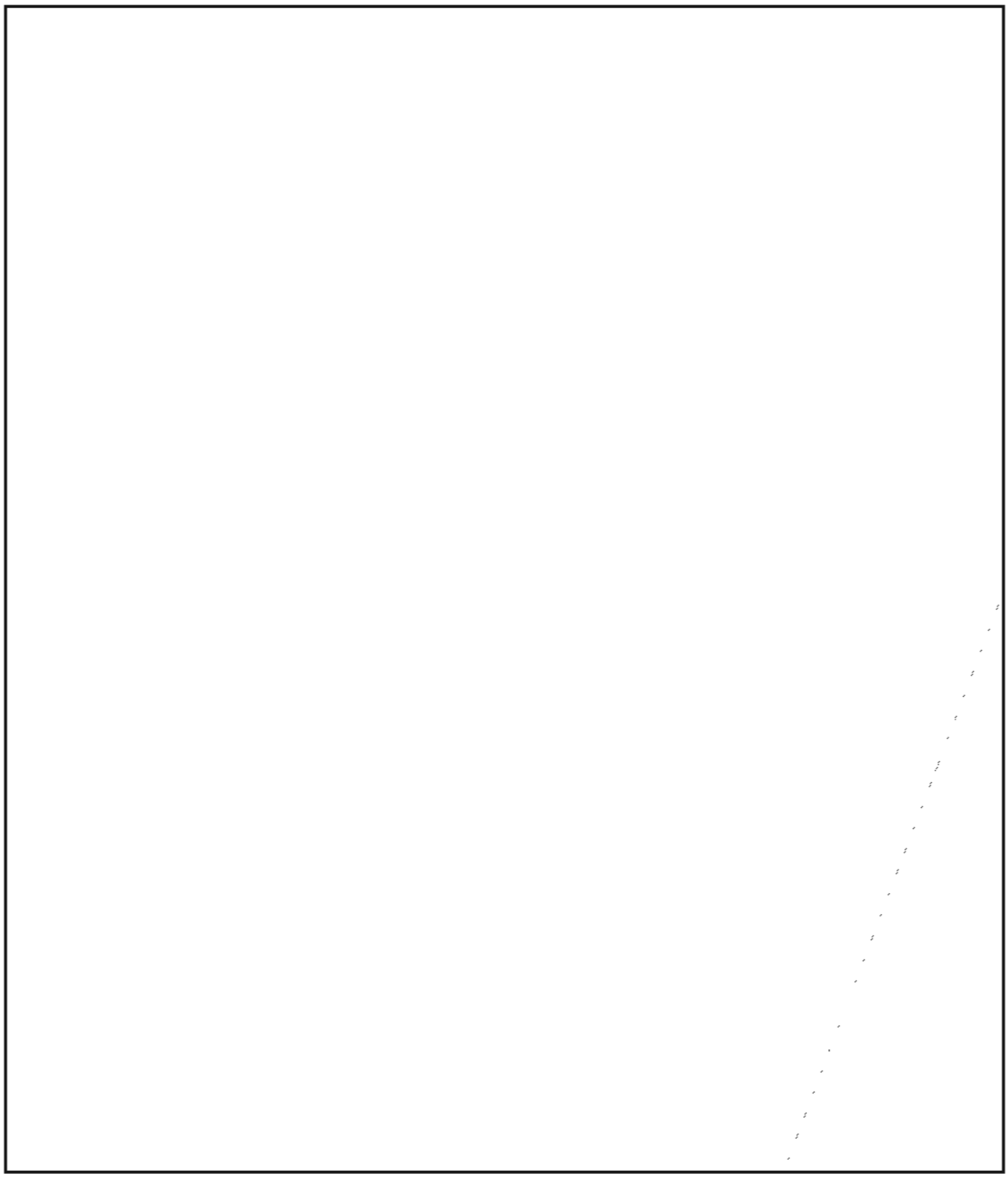
12. Heine, B., Status and Use of African Lingua Francas, Weltforum Verlag, Munich, 1970.

13. Greenberg, J. H., Studies in African Linguistic Classification, Compass, New Haven, 1955.

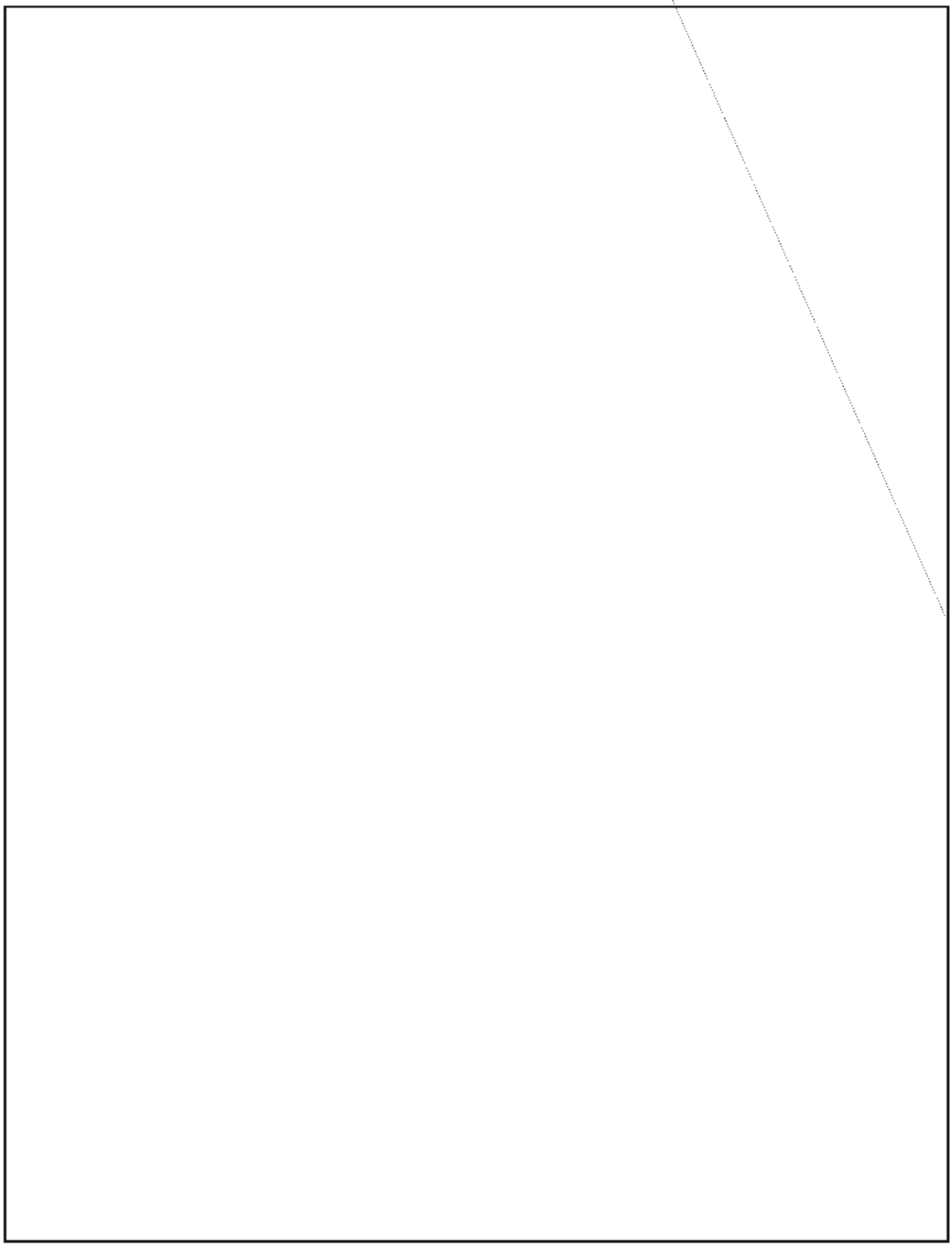
14. Leistner, D. "Rural communications - a topical problem in communication engineering for the next decade," Fernmeldtechnik (Germany) Vol. 22, No.2, pp.51-55 (1982). In German.

15. CCITT Handbook "Rural Telecommunications," ITU, Geneva, 1979.

P.L. 86-36
EO 1.4.(c)



P.L. 86-36
EO 1.4.(c)



DOCID: 4019695

¡Atención!

FBIS LATIN AMERICAN REFERENCE AID

(U) A revised guide to more than 5,000 abbreviations and acronyms that appear in the Latin American press, often without expansion, has been compiled by FBIS Production Group linguists. The 1983 "Abbreviations and Acronyms in the Latin American Press," which supercedes a smaller 1979 volume, includes as new entries Nicaraguan organizations created since the Sandinista revolution and abbreviations from the English-language press of the Eastern Caribbean. Alphabetical listings include the names of political organizations, government entities, professional and labor associations and companies in 41 Latin American countries and territories. The 414-page book was compiled for translators and others who read Spanish, Portugueses, or French but are not familiar with many of the local and regional abbreviations found in newspapers and periodicals.

(U) The reference aid was printed by the Joint Publications Research Service as publication No. 83345. It is available to US Government consumers through regular acquisition channels.

(U) "He came close last year, but close only counts with skunks, horseshoes, and hand grenades."

(Miss Oklahoma commenting on a computer expert's failure to correctly predict the Miss America of 1981)

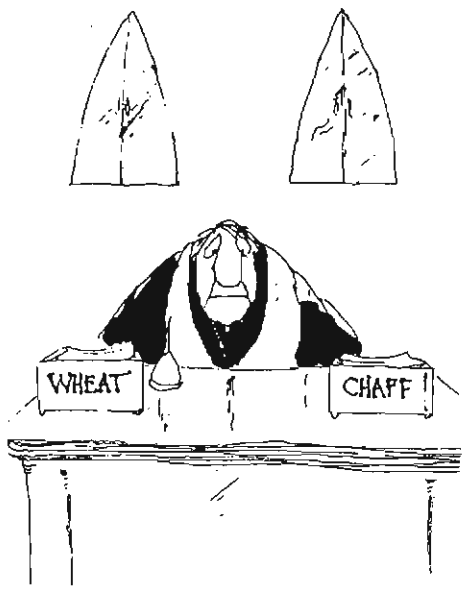
SOLUTION TO CRYPTIC CROSSWORD #3

ACROSS

1. olfactory (ol + factory)
6. pawns (pa + WNS)
9. formula (anag.)
10. nankeen (Nan + keen)
11. plead (sample a delicacy)
12. idealists (idea + lists)
13. icebound (anag.)
15. coma (frantic Onani)
19. guns (rev. spell.)
20. prurient (u + printer: anag.)
23. Dubliners (dub + liners)
24. nicer (ni + cer)
26. evident (anag.)
27. maidens (ma + I + dens)
28. digit (dig + it)
29. renegades (anag.)

DOWN

1. offspring (off + spring)
2. forge (double def.)
3. cauldron (pun: called Ron)
4. ovations (innovations - inn)
5. yonder (Roy + Ned: anag.)
6. panels (pleasant - AT: anag.)
7. whetstone (anag.)
8. sinks (double def.)
14. ennobling (eNNOBling)
16. asterisks
17. freshmen (reFRESHMENts)
18. bringing (bRINGing)
21. wisest (wISest)
22. setter (Somerset terminal)
23. dread (D + read)
25. creed (C + reed)



DOCID: 4019695

NSA IN THE SPACE AGE (U)

by [redacted] R093

P.L. 86-36

The single greatest problem confronting NSA seems to have been the need to keep pace with space developments. Despite repeated efforts, however, it is apparent that only a concerted, highest priority, Agencywide initiative might succeed to counter our failing space applications programs. In anticipation of such an initiative, I would like to make several suggestions which should be studied in addressing this physical space problem. (Yes, physical space.)

Perhaps the most important hurdle that we must overcome is the traditional thinking that each Agency employee is entitled to his or her own personal desk, reserved three hundred and sixty-five (365) days a year. Let us look at the facts. The average employee has twenty-two (22) days of "use or lose" leave annually. This represents nine percent (9%) of the work year. In addition, all employees receive thirteen (13) days of sick leave annually, equivalent to five percent (5%) of the work year. Thus, a cumulative fourteen percent (14%) space saving is possible by the simple approach of assigning desks on a "first come, first served" basis each day.

Once the logic of that solution is accepted and the procedure is implemented, additional potential savings become almost limitless. Training, which averages around three (3) weeks per year per employee, makes possible an additional six percent (6%) space savings, while TDY/travel absences contribute another four percent (4%) on average.

But why stop there? Making desks available on a "first come, first served" basis at all times during each day permits even more space savings while encouraging efficiencies. Take lunch and coffee breaks, for example. Staggering these events, which total almost one (1) hour per day, can save an additional five percent (5%) in space requirements. And how about other occasions when employees need to be away from their desks? Walks to water fountains, reproduction machines, the "powder room," and the boss's office all contribute to lowering the need for standby desks. There are also meetings, planning sessions, and coordination conferences. Then there are the visits to the bank, the credit union, the barbershop, and the drugstore. These absences have been conservatively estimated to consume a full nine percent (9%) of the average work day. On the one hand, losing your desk during these absences would permit further space savings. On the other, it might tend to foster efficiences as employees could compete for desk space by coming to work earlier and by staying at their desks longer at a stretch.

Up to this point, the suggestions have been relatively straightforward. So consider now, please, a few of the more innovative approaches under study throughout the Agency. One particularly forward-looking example involves the R Staff. For a year now, the emphasis has been on recruiting people of--shall we say?--diminished stature. It is quite evident that these people are able to remain comfortable in less than customary space allocations. Phase II of this experiment in R is now about to begin. We have become quite conditioned in this Agency to the proliferation of partitions vertically dividing our space. But now, the R Staff is embarking upon a new era involving the horizontal division of space. That's right: a single floor will have platforms installed so that, in effect, it can serve as two (2) floors of space. This will permit desks to be effectively stacked two (2) high--bunk desks, you might say. Theoretically, this could yield a fifty percent (50%) space saving, although present implementation goals call for a more modest thirty percent (30%) saving in the first fiscal year. Interestingly, there

DOCID: 4019695

would be no problem with GSA space-per-employee standards which are expressed in terms of "square feet" rather than the more telling "cubic feet" measure. Thus far, the only negative effect of this experiment has been the dismal record of the R Staff basketball team.

The T Organization is also embarking on its own innovative experiment to solve the space problem. Soon, the so-familiar gray and black phones that adorn almost every desk will disappear. Replacing them will be a limited number of phonebooths strategically, but sparingly, placed in work areas. The estimated benefits are several. First, security will be improved because of the privacy inherent in a closed booth. Complementary to and concomitant with this benefit, the noise level in the office environment will be reduced. Second, since there will be no seats in the booths and since there will be queues of fellow employees waiting to use the phones, telephone conversations will be limited to essentials. Third--and this relates to the earlier initiative of "first come, first served" desks--it will free up more office space as employees using phones would have to abandon their desk space. Latest operations research studies indicate that the average Agency employee now spends fully twelve percent (12%) of effective worktime on the telephone.

The Operations and the Installations and Logistics organizations are not standing still in the face of this space challenge either. Everyone realizes that there is quite a bit of wasted open space between the Headquarters Building and the Operations Building. Well, in a cooperative endeavor, L will drape an inflatable roof over the area after walling up the two openings on either side of Gatehouse 1 (One). The Operations organization will do its part by channeling unused electrons from collection efforts into the area. In much the same way that hot air currents are used to sustain the roof of the Hubert H. Humphrey stadium dome (aptly named after a politician), our roof will be sustained by the continuous flood of these returning electrical currents. After proper subdivision and incorporation of some of the stacking and bunk desk technology developed by R, this initiative will yield a twenty percent (20%) space bonus! To their credit, however, the L Organization will not stop there. Careful surveys on restroom usage indicate a significantly wasteful amount of space has been allocated needlessly. Applying standards pioneered at the Capitol Center during rock concert sellouts, L has mapped out a plan to convert seventy-five percent (75%) of these underused areas into office space.

The next space-saving innovation is already being practiced throughout the whole Agency although in a less than optimal manner. Patterned on the children's game, musical chairs, it involves periodic reorganization and relocation of functions and personnel. By a coordinated continuation of these activities, fully ten percent (10%) of the work force can be kept literally without an assigned office space as desks and support equipments sit in moving trucks, on loading docks, or in hallways. A side benefit of this action, incidentally, is improved security through drastic records reduction. Personnel required to move would have an incentive to clean out desks and purge old records, files, and tapes. In addition, movers would be instructed to lose at least two (2) boxes per move instead of their current quota of only one (1) box per move. Of course, this then frees up even more space.

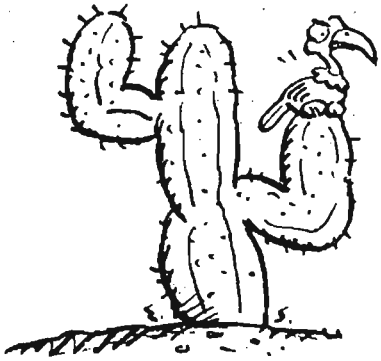
It goes almost without mention that all records are being reduced to either microfiche or electrical impulses on storage media. We still won't ever be able to put our hands on the information we need, but at least our records will take up thirty percent (30%) less space in the process of remaining functionally useless. And, naturally, the advances of space-age electronics will help solve our physical space problems too. In twenty-five (25) years, a computing capability that once filled a whole room is now housed in a one-by-three-inch (1-by-3") box. As these size reductions continue, our only problem will be in finding operators small enough to use the devices.

There are many other ideas under study, such as using a "lazy Susan" office configuration to eliminate all need for walkways, substituting writing stands for desks, and placing benches along main corridors. Also being considered is resorting to a multi-shift operation where all staffs will work mids. Staffs seem to operate in the dark anyway and they'll have little more than each other to bother at that hour. This and the other of the more experimental considerations may very well find their way into use in the near future.

But for now, if you have kept careful track, you noticed that the Agency has proven techniques to effect a ninety-seven percent (97%) space reduction already. The remaining three percent (3%) of the space that we will continue to need is roughly equivalent to the first floor of Operations Building One (1). We shall, therefore, retain direct use of that space. The rest will be sublet to those unfortunate Federal agencies and departments that still have not entered the Space Age. So, get ready to stretch out in plush surroundings and be thankful that once again your every need will soon be satisfied.

DOCID: 4019695

by Marian D. Librarian



BOOK REVIEW:

FRONTIER DENTIST by Phil N. Drill.

The story of Doctor Perry O'Dontics (1826-1851), a young graduate of the Painless Parker School of Dentistry, who went west with the 49-ers and performed the first extraction in the territory of California.

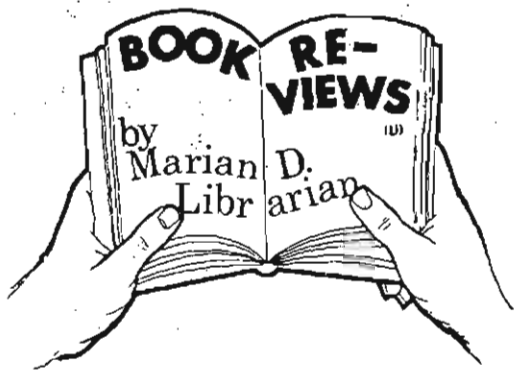
The book describes the problems that he encountered, especially that of ministering to unwilling prospectors who were afraid that he'd steal their gold while they were under anesthesia. How he won their confidence and trust could serve as an example to SIGINT managers dealing with other agencies that have a certain distrust of NSA and its product. The description of how the doctor improvised when he ran out of dental floss, making his own out of buffalo entrails, could also serve as an example to field station managers in remote sites.

(I am reminded of the commander of USM 9999 in a small town in the Italian Alps who kept requesting telephone wire from headquarters so that he could do his job better, finally using 14 tons of spaghetti made by the women of the nearest village. This worked fine for about two weeks, but as luck would have it, shortly thereafter the migrating season of the pasta birds began and as they flew over his station, they ate the spaghetti, forcing him to improvise using bird entrails instead of wire.)

It was interesting to see how the doctor even persuaded some of the miners and prospectors to give up some of their gold dust to be used as fillings for their cavities. In fact, it was Dr. Perry O'Dontics who coined the phrase, "There's gold in them thar fills!"

The last chapter of the book describing the problems that arose when another dentist, Dr. "Yank" Molarz, moved into the camps and took away some of Dr. O'Dontics' patients reminded me of some incidents during World War II when SIGINT organization from Army and Navy units that happened to be in the same general area fought over the same intercept and the intelligence derived from that intercept. The fact that the competition ended in the early death of Perry O'Dontics should serve as a lesson to units that indulge in internecine conflict, especially since there were enough teeth in the California for both dentists.

OCID: 4019695



BOOK REVIEW:

MAN DOES NOT LIVE BY MATZOS ALONE:

The Story of the Manischewitz Kosher Foods Family and Their Company, by I. Nasch.

The Manischewitz empire is so vast today that it's hard to believe that it once consisted of only Moishe Manischewitz (a humble baker in 18th-century Oyvey, Germany) and his two sons, Matthew and Mark. But it's true and this book traces the history of the company through the generations, showing how the same basic techniques that old Moishe used with his family have been maintained through the centuries. Some of these techniques could serve as models for SIGINT managers--especially if the Agency expands in the future.

There are other similarities that can be pointed out. It is worth noting that old Moishe Manischewitz and all his successors have had to comply with two sets of laws, those of the country in which they work and the rules governing kosher foods (often more stringent than national). The way that Moishe indoctrinated his sons (and later some of the other young men of the village) could serve as a model for the NSA intern program.

Although for generations the company specialized only in matzos, the flat unleavened bread traditionally eaten by Jews at Passover, it is interesting to note that Moishe's grandson Luke introduced diversification into the line with non-Passover foods, overcoming the objections of many members of the family (including his own grandmother, Goldie, Moishe's widow). This reminds me of the situation just before World War II, when NSA's predecessor decided to try intercepting types of traffic other than Morse code, much to the despair of old-timers, who insisted that the time and effort needed to intercept printer and voice would be prohibitive and would detract from the effort being devoted to Morse.

Oddly enough, a generation later, when some of the other products that Luke introduced proved to be money-makers, Luke's son Manny suggested that the company specialize in them and drop matzos from their line. Many of the members of the family protested this (just as there have always been SIGINT people who propose that we stop worrying about Morse code and devote our efforts to other means of communication), but time has shown that there is a need for both the old products and the new (just as NSA has been extracting intelligence from Morse and the newer varieties of transmission).

DOCID: 4019695

MY STAFF— It Comforts Me!

by ZEBULON ILCH'

Act I, Scene 1

Place: The inner sanctum of the Secretary of Defense in the Pentagon.
Time: A few decades hence, on the morning of 17 April.

"Excuse me, Sir. Here's that staff study you ordered," said the young lady as she dropped a pile of paper on the desk of Warren Piece, the Secretary of Defense.

"Holy Mackerel!" shouted the Secretary [except that he used a much stronger term] as he scanned the document. "Do you realize what your statistics show? For each soldier, sailor, airman, and Marine in the armed forces, we have 28 civilian staffers in Defense Department agencies! That's preposterous. We don't need more than 10 or 12 staffers per combatant. I'll issue an order at once cutting down on the number of staff personnel. Miss Spelle, take a directive!"

Act I, Scene 2

Place: The inner sanctum of the Director of NSA
Time: Same year, a week or two later

"I wouldn't have called this meeting unless I thought it was urgent, said Admiral T. V. Sett, Director NSA/Chief CSS, to a gathering of Chiefs of key components "and this memo from SecDef is just that! He's highly annoyed [except DIRNSA used a more picturesque expression] about the number of staffs in DoD. What's even worse is he singles out NSA/CSS as one of the worst offenders. For every person we have actively engaged in collecting, decrypting, and translating messages, we have 37 people engaged in staffwork. That's way above the Department average of 28. So, we've got to cut down on the number of staffs and staffniks in the Agency....and we've got to do it ASAP!"

There was a simultaneous nodding of every single head belonging to a key component chief (KCC), but none of them said anything. Each one mentally recounted the number of individual staffs in his particular bailiwick, mentally tabulated the number of individuals on each of them, recounted the types of studies they prepared, recalled the number of times that a well-staffed background study had saved his or her (the KCC's) neck, and came to the realization that removing even one staffnik would be tantamount to excising his or her (the KCC's) own appendix without an anesthetic.

Finally, Hugh S. Essar, the Chief of A Group spoke up. "Sir, I can well understand the SecDef's feeling and I can agree with him that there are a number of DoD agencies where the number of staffniks is out of proportion to the amount of work they perform. But I venture to say that at NSA/CSS, such is not the case. The reason that NSA carries out its mission so well is that no precipitate actions are taken without proper in-dept background studies of the causes and effects of all sorts of actions and activities. Speaking in behalf of myself and the organization I head, I can confidently state, Sir, that I cannot--absolutely not!--dispense with even one of the hard-working, loyal members of any of the staffs in A Group."

"I feel the same way about my staffniks," said DeFarr East, Chief of B Group. "Because

OCID: 4019695

of the multiplicity of tasks assigned to our organization and the impossibility of any supervisor, except the Group Chief, knowing the details of all of them, it is essential--absolutely essential!--for B Group to maintain all of the staffs it has at present."

"I can wholeheartedly agree with the remarks of my colleagues," said Al Lowe, Chief of G Group. "Everything they have said is equally true of my organization, only more so! Why, my Group has a greater variety of targets, crypt systems, report series, and product issued than their groups combined according to a recent study by a G Group staff. Without trying to disparage the other KCCs' organizations, I would say that proper staffing is the major cause of G Group's outstanding reputation."

"Let's not forget the need of adequate staffwork in the maintenance of a proper educational system," chimed in Reed N. Wrighton, Commandant of the NCS. "I recently received a staff study that shows that for every person in E who is actually involved in teaching classes, we have only 16 individuals engaged in the necessary background staffwork. Since this figure is considerably below the DoD average--and even farther below the Agency average--I would be loath and reluctant to dispense with any of my staffs."

And so it went around the table as each KCC in order, from the Chief of A Group down to the Chief of Y Group, defended the need for his or her staffniks and expressed a deep-seated unwillingness to give up any devoted staffniks.

"I was afraid that this would happen," said DIRNSA, "but we have no choice. SecDef has said that we must cut down on the number of staffs and staffers, so cut we must! Accordingly, since none of you will bite the blankety-blank bullet yourselves, I must take the following action: I am this day establishing a new organization to eliminate unnecessary staffs--and I'm sure that there must be one or two unnecessary ones in a large organization like this--in NSA. Since we have used up all of the letters of the alphabet through Y, this new body will be called the Z Staff, and it will report directly to me....and I hasten to add that in order to avoid incurring SecDef's wrath, I'll be quite ready to concur with most of its recommendations for eliminations. To head this new entity, I am appointing Frank N. Stein, my Chief of Staff, as the Chief of Z. He will head an organization made up of one staff person from each key component, whom he will personally select, to help him in his work. Meeting dismissed."

Act II, Scene 1.

Time: Two or three weeks later (give or take a fortnight or two).
Place: The inner sanctum of Z Group on the Ninth Floor of the NSA Building

Frank N. Stein called the first meeting of his Z Staff to outline their duties and work out their modus operandi. "Before we can eliminate any staffs, we have to know where they are. Because of your backgrounds, you men and women--but mostly men!--are in a position to know just what staffs exist in each agency key component. Now I know there will be a lot of loyalty in each of you to protect some of your buddies back in A, or G, or K, or Q, but let me remind you all that you are now members of Z. Henceforth, your only loyalty is to the Z Staff (not to be confused with The A Team). Don't forget: by eliminating your old job you are making your own future more secure."

"But I've been a staffnik for years," remarked Conn Currence. "If I eliminate my job back in C Group, what else can I do after we finish this project?"

"The nice part about the Z Staff's mission," replied Stein (who, like a good staffnik, always spoke in memorandum format) "is that:

(1) we'll be investigating all facets of the Agency so a good Z operative can eliminate the positions of certain key individuals without necessarily doing away with the staff functions performed by those persons, so that when and/or if Z Group's mission is ever completed, there will most likely be a need for a trained staffer to perform that job.

(2) SecDef's anti-staffing memo does not--repeat not--set any deadline for the reduction of staffs, so we don't have any short fuses to worry about.

(3) DIRNSA's directive establishing Z Group is likewise without any time constraints, so if we budget our man-hours properly, we can conceivably make a lifetime project out of this study, maintaining of course that an in-depth analysis of this sort cannot be rushed."

"That's a relief," said Currence, "but won't somebody get angry if we don't get rid of some staffs?" Several other Z-niks nodded and said "Yeah, won't they?"

"I didn't say that we don't do anything," replied Stein. "I just said that we mustn't rush things. I think our motto should be

'with all due and deliberate speed' (which sounds like it means something but is vague enough so that no one really sure just what it does mean). I also propose that we organize our work alphabetically, devoting our first efforts to A Group, which ought to take us quite a long time. Then we can work on B Group, and so on."

"Maybe we ought to do a staff study on this and consider all the alternatives, Chief," suggested Sam Urai, a former B Group staffer. The roar of voices seconding this recommendation was deafening, so Stein gave them four weeks to concretize their feelings and put their recommendations in writing."

Act II, Scene 2

Place: Same
Time: At least two months later.

"I've called this meeting today," declaimed Frank N. Stein, "to report on my findings with respect to your recommendations about the method for Z Group's operation to proceed. I have read over the staff studies submitted by each of you and I must say that I am thoroughly convinced that I have selected a fine bunch of men and women to constitute the Z Staff. Your comments about my suggestion to proceed through NSA alphabetically by organizational designator ranged from total agreement to absolute disagreement, each duly supported by impeccably logical reasoning (often drawing completely opposite conclusions from the same data), and there were a few of them that I've read and reread several times and still can't figure out whose side they're on. Excellent work, Z Staffers!

"Accordingly, we will now go ahead with our work, proceeding alphabetically by organization designator. Our first target will be A Group and our mission is to eliminate as many staff positions as possible.

Act II, Scene 3

Place: Same
Time: Over a year later

"Well, Z Staff," said Frank N. Stein, "we seem to be making progress in our analysis of A Group. To date we have discovered three staff jobs that can be eliminated, but we seem to be encountering resistance from many agency employees, which is making our job harder. Accordingly, I have today requested that the Director authorize the expansion of the Z Staff by at least a dozen billets and I am happy to say that he concurred without even recommending a study. I'd like to introduce the first three new members of this staff, all of whom formerly worked on A Group staffs until recently. Because of their vast experience in A Group, they should be of great assistance in helping us find positions to eliminate and well-trained individuals to help us in our deliberations."

INTERMISSION

[during which a new President is elected and, consequently, a new Secretary of Defense moves into the Pentagon. Since his Chief had been elected on a program to eliminate waste in government, he heartily endorses his predecessor's anti-staffnik directive. The new Director of NSA/CSS, General Al Arm, inspired by the Secretary's statement, orders across-the-board promotions for all members of his staff-cutting staff.]

Act III, Scene 1

Place: The Friedman Auditorium, NSA
Time: Over a year later

"I've had to call this meeting of the Z Staff here because there are just too many of us to sit around the office and report on our progress," said Frank N. Stein happily. "We have been having great success with eliminating the staffs in A Group. Fortunately, the chiefs of other key components have seen that we mean business so they have voluntarily reduced the number of staffs within their organizations, which makes our task somewhat easier. Some of them have appointed an alarming number of Special Personal Assistants for specialized functions and some of these SPAs have Special Assistants of their own to help them. A special six-month Z Group staff study has definitely determined that these Special Assistants do not technically constitute staffs and therefore we don't have to eliminate them.

"We've also been fortunate in having a number of qualified staffers who, fearing that their jobs might be done away with, have volunteered to serve on the Z Staff. Our numbers have increased greatly and this has enabled us to complete our functions in A Group. So today we can start the task of eliminating the staffs in B Group. I wish you as much success in your labors there as we have had in A Group.

"As many of you know, I have been eligible for retirement for several months now, but I couldn't leave Z Group until we had achieved our first important milestone, and the elimination of A Group's staffs is that milestone. Accordingly, in addition to the news about A Group, there are three other reasons for this meeting:

DOCID: 4019695

(1) To formally announce my retirement from government service, the National Security Agency, and regrettably from Z Group, where I have made so many friends and accomplished so much;

(2) To introduce my successor, the new Chief of Z, Gilbert O'Teen, and hope that you'll give Gil the same support and backing that you gave me during my tenure as Chief; and

(3) To announce that although I am officially retiring, I have been persuaded to continue working with Z Staff as a Retired Annuitant, so I'll still be available for consultation, advice, concurrence, and consultation. I will be, as the saying goes, 'Forgotten but not gone!'"

Young Gil O'Teen, the new Chief, spoke briefly, urging the members of Z Staff to continue their dogged pursuit of unnecessary staff positions throughout the other components of the Agency and announced that since there were so many members of the organization, he was appointing several Special Personal Assistants to help him with the day-to-day management and paperwork of Z. Several of the people he named were individuals who were not previously Z-niks.

ANOTHER INTERMISSION

[during which young Gil O'Teen matured and Z Staff continued to grow and to eliminate staffs from other Agency components.]

ACT IV, Scene 1
Place: The Baltimore Civic Center
Time: Several years later

Gil O'Teen, a bit gray at the temples, has called a meeting of the Z Staff to congratulate them on their great accomplishments in eliminating staffs from assorted Agency elements. He is telling them, "It seems like only yesterday when we started to root out the growing 'staff infection' that was affecting our beloved Department of Defense. I can still recall vividly the opposition that we received when we started working on A Group's excess staffers, opposition that continued on through B and C groups. We had to tread delicately with D because there was some fear that the Director might retaliate, but fortunately the General was a firm believer in Special Personal Assistants to the Director and Z Group was able to convince him to appoint a few more--I don't think that 427 SPADs is too many for an important individual like DIRNSA. When General Arm was replaced by our first female Director, General Anne S. Thesia, she managed to cut the number down to 399 SPADs but has no staffs to speak of. The other groups, E through T, got the message and readily eliminated staffs and staffers with the help of Z Group. We discovered that U Group had no staffs for us to eliminate, but V, W, and X Groups did. However, with all the experience we had gained in our earlier efforts, we had little trouble eliminating their excess staffniks. Today we have gathered, all 900 members of Z Group, to celebrate the removal of the last vestige of staffs from Y Group. I have here in my hand the document for the DIRNSA's signature and subsequent submission to SecDef announcing the removal of all the staffs from NSA/CSS except for the Z Staff, which is charged with seeing that the scourge of staffs does not again arise in the Agency. Now we can all breathe happier in the knowledge that our collectors, processors, analysts, reporters, and linguists are doing their jobs as they are supposed without the heavy financial burden of paying so many staffniks.....and Z Group will continue to see that the Agency does not slip back into its previous staff-ridden days! Keep up the good work, members of Z Staff!"

ACT IV, Scene 2

Place: The Office of the Secretary of Defense
Time: One Month After the Previous Scene

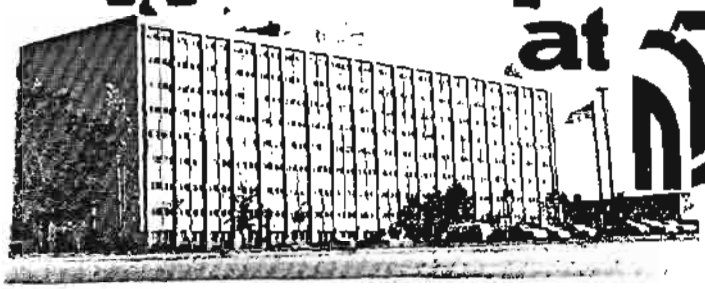
The Secretary of Defense commends General Anne S. Thesia because NSA/CSS is the first DoD agency to cut its number of staffniks so sincerely. He promotes General Thesia, making her the Army's first 6-star general, and appoints a staff to examine how NSA/CSS did such a thorough job so that recommendations can be made to other agencies.

THE END

DOCID: 4019695

~~FOR OFFICIAL USE ONLY~~

WORD PEOPLE at NSA (U)



by 'Dickson Airy'

#1: CHESLEY

Term: chesley (verb)

Meaning: to get out of a difficult situation by convincing others that you are a victim of circumstance, whether you really are or not.

Background: G.V.R. Chesley was, until recently, a venerable analyst for a major production group of the National Security Agency; his 30-year award testified to his "inestimable value." However, it is not for that value that he is remembered, as inestimable as it was. This account, as useful as it is, leaves questions unanswered. What was the role of the Stairway Society (see CRYPTOLOG, October, 1981) in this affair? Could they have been a hidden factor in these events? Curiously, there is no surviving record of what G.V.R. stood for; all his co-workers remember are the initials. No one can recall every hearing what they stood for, or why Chesley never used his full name. Perhaps some kind reader could shed some light on these details for the sake of historical accuracy.

Chesley was in the process of being disciplined by his supervisor, Hardin Tuff, for being absent from his desk for four hours. Chesley claimed at the time that he was on the sixth floor taking care of some personnel business; as he came back down in the elevator, he found that the crush of oncoming passengers prevented his getting off at the first floor. He rode the elevator up and down, up and down, up and down, up and down, for several hours, each time being prevented from getting out at the first floor by incoming passengers. At last he grew faint and his paleness attracted the attention of several other passengers, who successfully extricated him from the elevator car with a variation of the flying wedge.

Some people have such an impact upon those around them that their name passes into the language as a word of common usage. Bloomer, Boycott, Mae West, McAdam, etc., have all been memorialized in this way. There are many NSA people who have done things worthy of being memorialized, and their names have already become part of our day-to-day vocabulary. We believe that some note should be taken of these people and their contributions, and therefore we encourage our readers to share their stories about word-worthy co-workers. We offer here the story of one of our fellow laborers; although he is no longer with us, his name lives on in our midst.

Tuff expressed disbelief and suggested that he could have gotten off at another floor and walked down. Chesley produced a letter from a physician indicating that he was allergic to the paint used in the stairwells.

When Tuff challenged the authenticity of the letter, protracted and emotional discussions ensued. Feeling the need for onsite demonstrations, both men went to the stairwell, where Chesley began to sneeze violently. This startled his supervisor, who fell down the stairs, breaking his left leg and arm, whereupon Tuff applied for, and was granted, retirement on the grounds of disability.

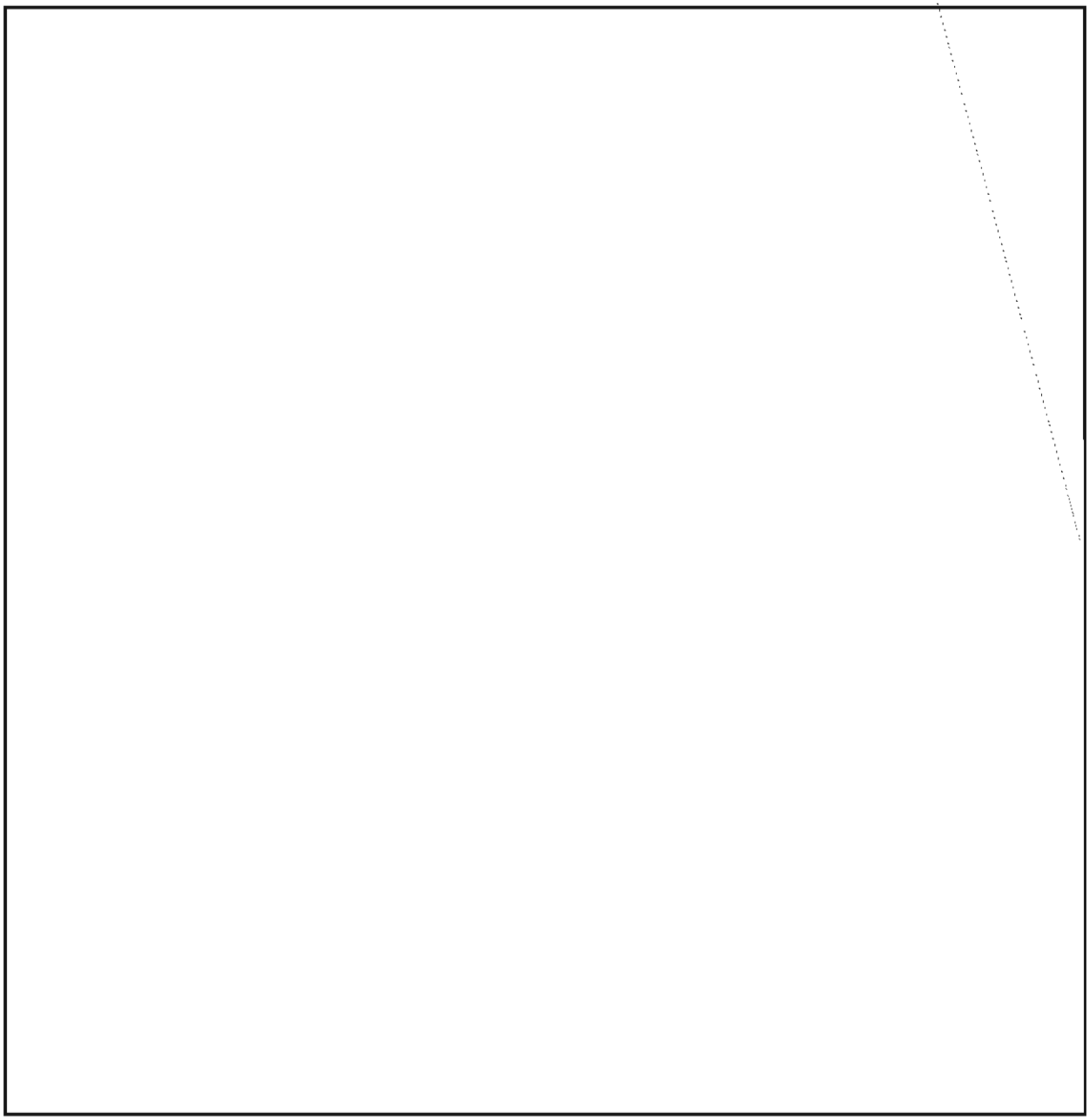
Chesley's new supervisor Al B. Careful, who turned out to be deathly afraid of germs, and therefore of being sneezed upon, reviewed the case and decided to drop the charges.

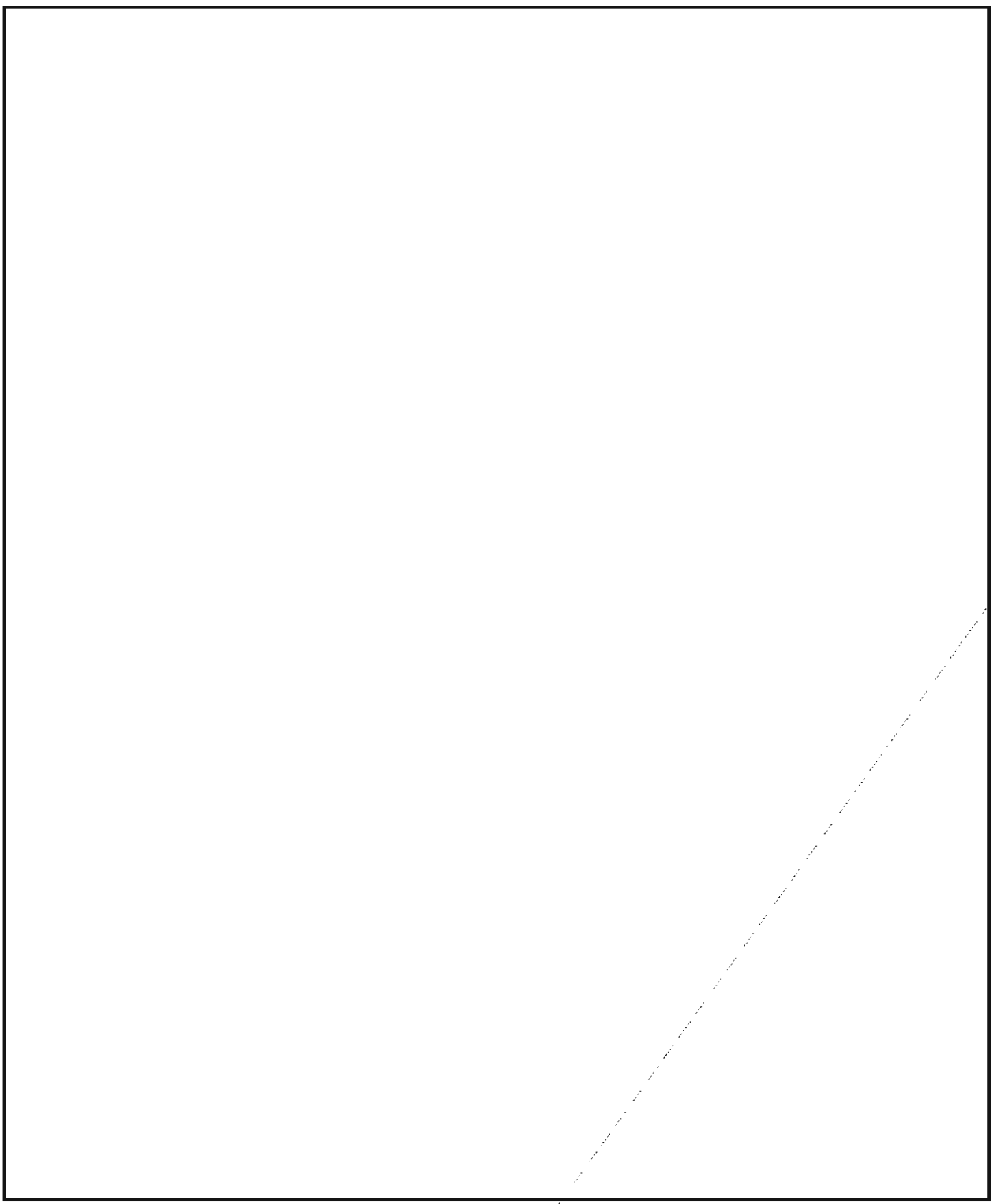
~~FOR OFFICIAL USE ONLY~~

DOCID: 4019695

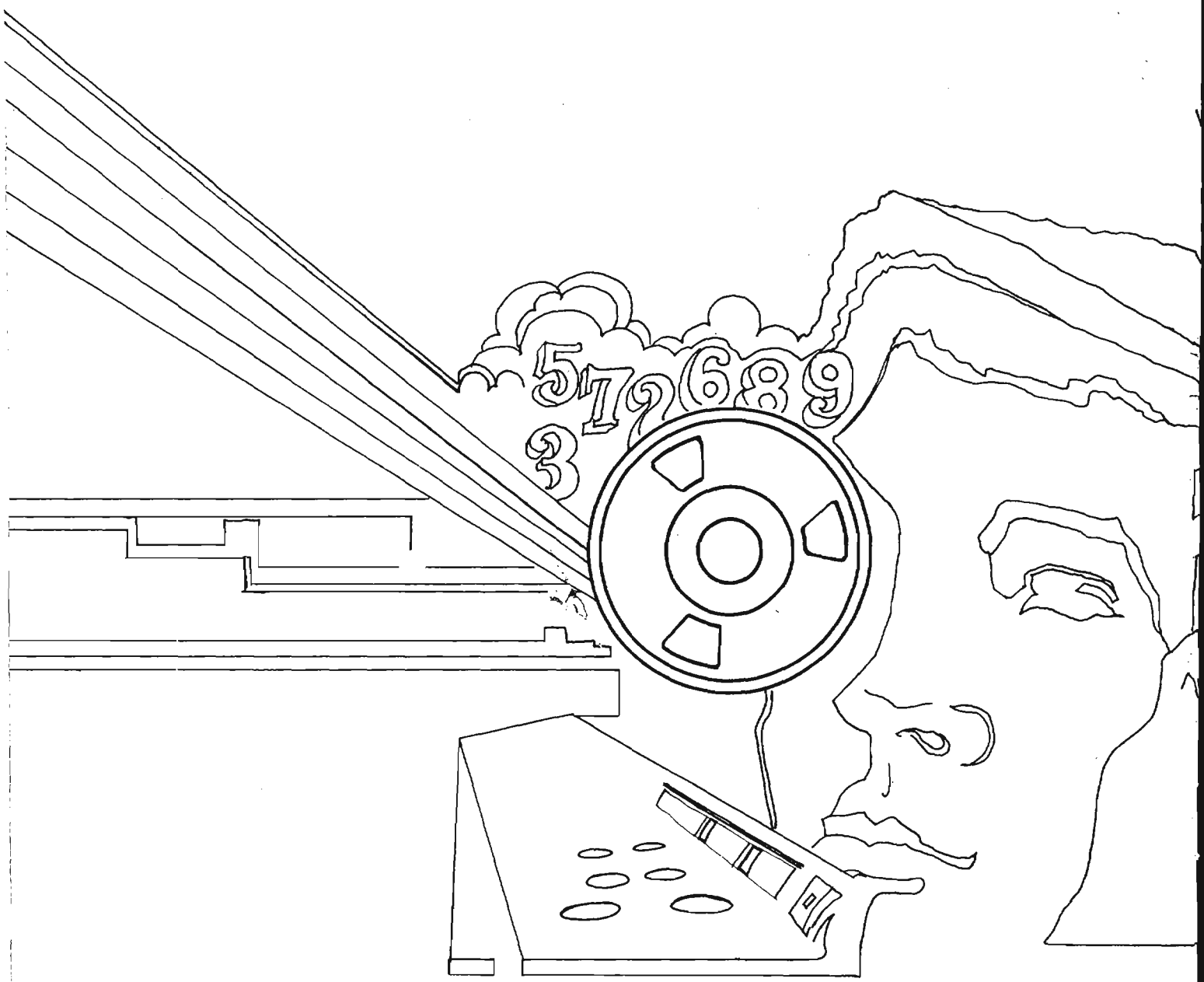
NSA-CROSTIC No. 46
by dhw

This is a belated April Fools' Day puzzle. Solvers may be assured, however, that there is no trickery whatsoever in any of the definitions.





P.L. 86-36


5 7 2 6 8 9
3

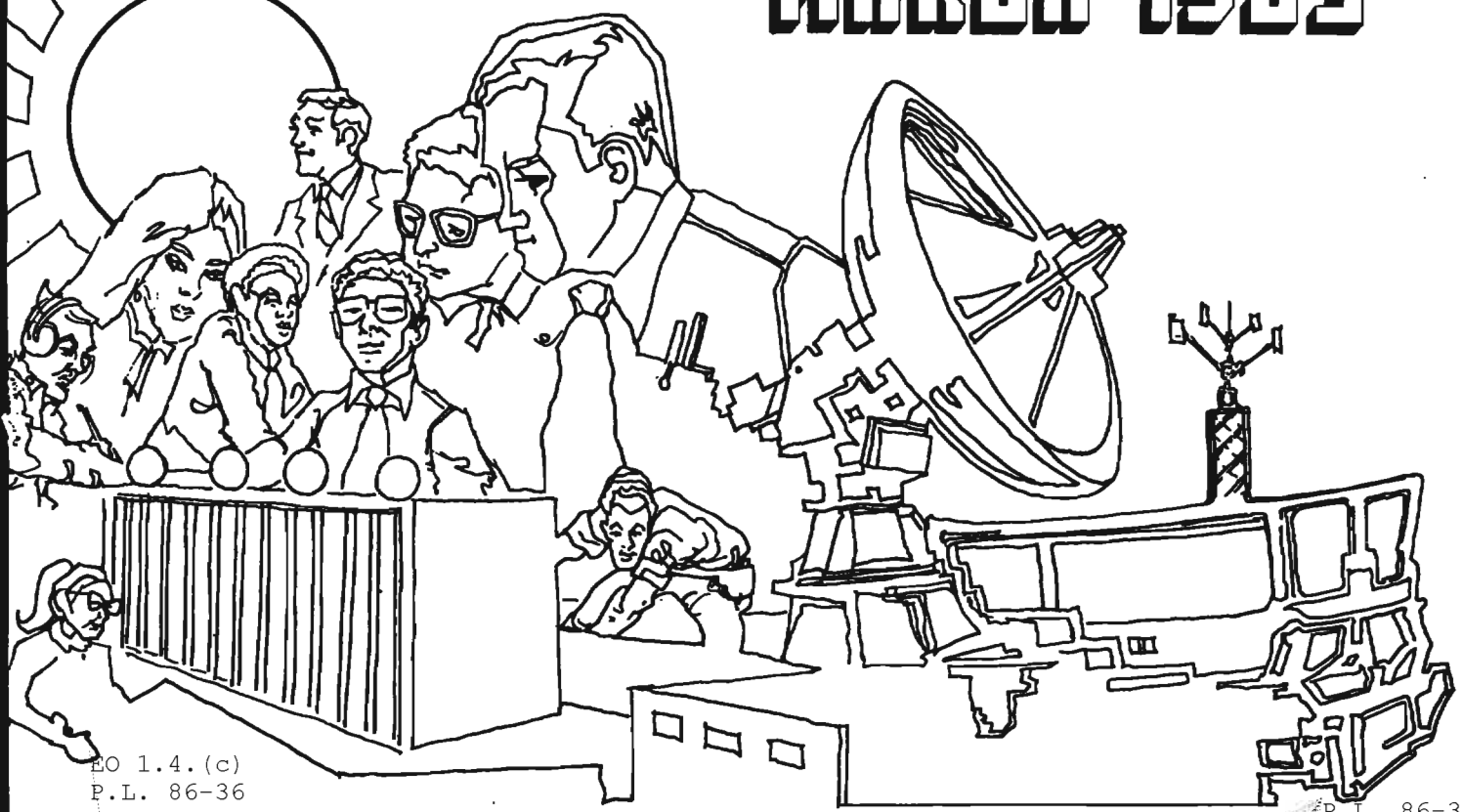
DOCID: 4019691

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MARCH 1983



EO 1.4.(c)
P.L. 86-36

P.L. 86-36

VIDEO TELECONFERENCING: NSA APPLICATIONS (U)....[redacted].....1
IS THE GLASS HALF EMPTY OR HALF FULL? (U).....[redacted].....11
CUMULATIVE INDEX, PART ONE: AUTHORS (U).....16
STUDENTS! (U).....30
[redacted].....30
CRYPTIC CROSSWORD #3 (U).....[redacted].....31
SHELL USING IF.....[redacted].....32
E.T. AT NSA.....32
SIGINT CHALLENGE: A SCENARIO (U).....[redacted].....33
KRYPTOS SPRING MEETING (U).....34
MORE ON PASSWORDS (U).....[redacted].....35
TDY TRAVAIL (U).....Vera R. Filby.....40
WEATHER: A KEY INTELLIGENCE INDICATOR (U).....[redacted].....43

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019691

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. X, No. 3 MARCH 1983

PUBLISHER [redacted]

BOARD OF EDITORS

Editor..... [redacted] (968-8322s)
Asst. Editor... [redacted] (963-1103s)
Production..... [redacted] (963-3369s)

Collection..... [redacted] (963-3961s)
Cryptolinguistics. [redacted] (963-1103s)
Information Science
..... [redacted] (963-5711s)
Machine Support..... [redacted] (963-4953s)
Mathematics..... [redacted] (968-8518s)
Puzzles.....David H. Williams (963-1103s)
Special Research.....Vera R. Filby (968-7119s)

For subscriptions
send name and organization

to: CRYPTOLOG, P1
or cal [redacted] 963-3369s

P.L. 86-36

To submit articles or letters via PLATFORM mail, send to

cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no '0' in 'log')

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

Style is an elusive thing. I remember a coworker who had an elegant way of speaking, but when I tried to analyze how he did it, I could never pin down anything central or basic. It just seemed that he had a good grasp of a lot of peripheral details. The only way I can describe him is to say that he never spoke in "rough draft." And I envied him for that ability.

What brings my coworker to mind is a question of style that has been bouncing around here at CRYPTOLOG. What kind of a magazine do you, the readers, want?

We get feedback, of course. On the very same day, we received one note that wondered why we don't put in the weird and nutty titles any more, and another that thanked us for switching to titles that were clean and easy to read. Call that a draw.

Here is a specific question for you about CRYPTOLOG. At one end of the scale, there are the clean, crisp page layouts with lots of white space and a generally "glossy" look, which is to journalism students what structured programming is to computer students. At the other end of the scale is what someone has called "early Whole Earth Catalog." Where should CRYPTOLOG be on that scale? What do you think? Let us know.

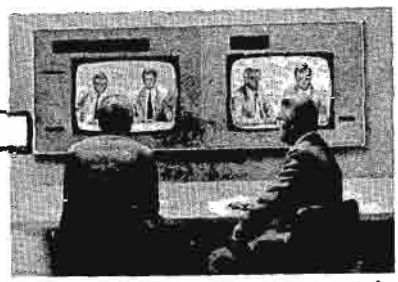
WED

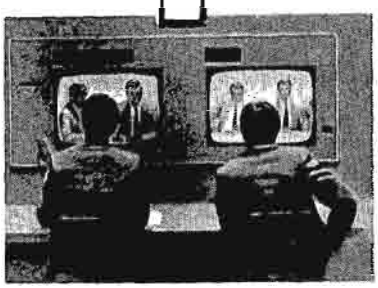
Note:
The January 1983 issue may be late in arriving, because of its size. It should be changed from "January" to "January-February" and from "No. 1" to "No. 1-2"

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019691

VIDEO TELECON-FERENCING AT NSA





by

T43

P.L. 86-36

INTRODUCTION

(U) As early as the 1880s the concept of electrically transmitting and receiving transient visual images through the air as electromagnetic waves had been explored. Paul Nipkow, a German scientist, pioneered a scanning device in 1884 that sent pictures short distances. By 1928 scientists had perfected Nipkow's invention. On September 11, 1928, an experimental television station, W2XAD, provided visual stimuli which were meshed with the audio track of radio station WGY to present the first production on television. In 1936 the National Broadcasting Company (NBC) was the first to combine the audio and visual signals into a single transmission medium.

(U) Today the concept of transmitting and receiving visual images is not unlike that of yesteryear. However, its magnitude and applications are far more sophisticated and extensive. The emphasis today is placed on television to operate in a two-way, full-duplex configuration which will allow groups of people in geographically separate locations to interact in both the audio and visual modes simultaneously. This technique, referred to as Video Teleconferencing, is currently being used by a number of corporations, government organizations, and educational institutions as a substitute for, or supplement to, travel.

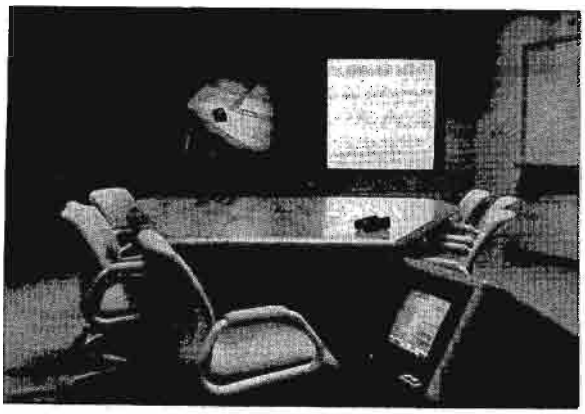
(U) With the costs of travel escalating and government funding declining, it is time for the National Security Agency to research and analyze the feasibility of adopting Video Teleconferencing for use in selected Agency applications.

BACKGROUND

Concept of Video Teleconferencing

(U) Video Teleconferencing is a means of conducting a visual and audible conference between two or more groups of people who are geographically separated, while maintaining all the realism of a face-to-face meeting. In addition to allowing the other participants to be seen and heard, video conferencing can permit in its system configuration the simultaneous exchange of hardcopy and graphic information. Video Teleconferencing is a relatively new term in the field of communications; however, the original process of transmitting and receiving audio-visual signals was developed in the late 19th century.

(U) Face-to-face conversations between people is considered by many to be the most productive communication tool. Because of geographical separation, time constraints, and travel costs, face-to-face meetings are not always practical. Implementation of a video



conferencing system could provide a reduction in undesirable travel, greater flexibility in scheduling meetings, and better structured, higher quality conferences.

(U) Studies in the use of video teleconferencing suggest that, "Video conferencing is effective for task-oriented meetings that are short, structured, have a specific purpose and involve a limited number of participants who know each other."[1]

Video Teleconferencing as a Replacement for Travel

~~(C)~~ In recent years the cost of travel has increased at an annual rate of 35 percent.[2] NSA is not immune to those escalating costs in travel. In 1981, NSA's expenditures for temporary duty (TDY) trips, both Operational and Maintenance (O&M) and Research and Development (R&D), totaled $13.8 million.[3] Putting this astronomical figure into perspective, it equates to $865.00 for every civilian employed at the NSA headquarters (15,953).[4]

(U) Many major corporations are adopting video teleconferencing as a substitute for travel in an attempt to offset soaring costs. Atlantic Richfield, for example, estimates that its annual travel expenses have risen from $20 million to $50 million in recent years. These awesome figures have persuaded Atlantic Richfield to adopt video teleconferencing with the hope of cutting corporate travel costs by 20 percent. Westinghouse activated a video teleconferencing link between Baltimore and Edwards Air Force Base in California in late 1982. Sperry Univac, another major corporation, has been using freeze-frame video since 1978 between its headquarters in Pennsylvania, Minnesota, and Utah.

(U) The saving in travel funds is a major consideration for these companies. In view of NSA's huge travel expenditures for 1981, the adoption of video teleconferencing should be considered. However, the monetary saving is not the only benefit to be realized in adopting video conferencing. Meetings can be scheduled more frequently and on shorter notice since travel time associated with such meetings could be reduced. Attendance is more flexible. Many more participants, who otherwise might be unable to attend a face-to-face meeting, would be allowed to take part. The "catch-up" syndrome, time required by travel participants to catch up on daily tasks that have built up during the TDY period, could be eliminated. These latter benefits are difficult to quantify monetarily, but they remain justifiable considerations in the decision to implement video teleconferencing.

Psychological Aspects of Video Teleconferencing

(U) Although video teleconferencing could provide a more elaborate means of conducting geographically separated meetings while, at the same time, proving to be an invaluable asset in corporate savings, its implementation may create obstacles that participants must overcome to to achieve total effectiveness. With the introduction of video teleconferencing as a replacement for the actual in-person assemblage, one must be able to present oneself and one's environment. Some may find it difficult to project ideas in a natural manner while in an artificial setting. Recent studies suggest possible video conferencing difficulties if the participants are strangers or of differing ranks and grade levels.

> "...when only a voice channel is available, communicators create an image of the person speaking, which while it may not accurately represent that person, is complete in itself. A low definition video representation may be sufficient to interfere with the information of such an image while being too ambiguous to create a satisfactory image in its own right. Maintaining friendly relations, is reported as being less difficult, suggesting that the video image is sufficient to act as a reminder stimulus if the person is already known, although people using teleconference for regular meetings still experience the need to meet face-to-face about once every.three or four meetings."[5]

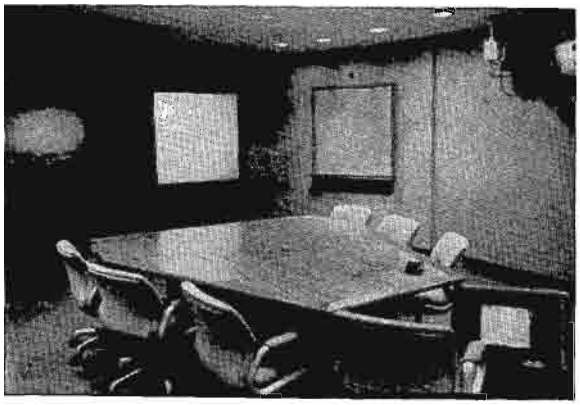
(U) During video conferences, first impressions are made via auditory and visual channels exclusively. The initial handshake and

working lunches would be eliminated through video conferencing usage. Some may find these factors a boon or a hindrance, depending on past conference experiences and conference goals. Subtle mood changes and all other sensory modalities would likely be lost through the video conferencing approach. It has been said that, "People don't like to change the way they do things. They like to press the flesh, watch the fellow's reaction to what they say, swap stories and all the rest."[6]

(U) The video teleconferencing method of communcating would allow for immediate feedback of material presented, as well as allow for group dynamics to take a part in the decision-making. Aetna Life & Casualty is reported as having realized more efficient video teleconferencing sessions than face-to-face meetings in some instances. The conferees appear more determined and eager to capitalize on the video conferencing facilities once they are scheduled. Thus, less time is spent on small talk. Results of recent psychological surveys evaluating the acceptance of video teleconferencing versus phone meetings, revealed video conferencing to be more suitable for cooperative tasks and not applicable when the opinions are the participants are at variance.

> "...teleconferencing was both effective and acceptable for meetings involving information exchange, routine decision-making, and cooperative problem-solving, but not as good for getting to know people, bargaining and negotiation tasks involving serious conflict."[7]

(U) In addition, these survey results indicated the majority of video users can accomplish meeting objectives efficiently through the use of a video teleconferencing system.



(U) The psychological aspects of video teleconferencing may take some getting used to, even after the technical elements and financial milestones are eliminated. However, with increased use of video teleconferencing, it is believed that any personal psychological barriers that may exist will be diminished.

TECHNICAL CONSIDERATIONS IN ADOPTING VIDEO TELECONFERENCING

Design Elements

(U) "Providing a Video-conferencing system design that will satisfy the user's requirements of meeting efficiency and effectiveness is a big order."[8] The general design of a video conference room is more or less straightforward. Its basic layout is not unsimilar to that of a local television studio comprising an eye-appealing environment, cameras, microphones, monitors, and a control console. To enhance a video teleconferencing operation, the inclusion of additional equipment would be required. This additional equipment could include facsimile equipments for the simultaneous exchange of hardcopy documentation, telephones for private voice exchange and coordination, video recorders for future reference of the proceedings, and an electronic blackboard for graphic depiction of information. A teletypewriter terminal should also be given consideration in the design effort. This could eliminate the need for facsimile. The principal objective of the facsimile and teletypewriter device(s) is to provide a means of transmitting quick copies of documents held at one end of the system so that all conferees can pursue and discuss in detail the same document at the same time. Still another device that should be considered, at least at the NSA headquarters, is a computer terminal. This terminal would be most desirable as information or date pertinent to a particular subject under discussion during a meeting may only be available from computer data bases.

(U) Although the design effort can incorporate a multitude of additional equipments to enhance the success of the conference, the primary goal is to provide a clear picture and good fidelity between the participants. It is imperative to perfect these areas so that they closely resemble a traditional face-to-face conference.

Transmission Techniques

(U) Various means of holding "electronic" meetings are available to corporate managers today. One type of electronic meeting which

is receiving the most attention is the video teleconference. Implementing a video conference system relies heavily on the availability and cost of suitable bandwidth to meet the particular needs of the company. The two conventional modes used for video conferencing today are wideband video conferencing and narrowband video conferencing.

(U) Wideband video conferencing is teleconferencing combined with the use of a one-way or two-way wide bandwidth (1.544 megabits or above) communication link to transmit and receive simultaneous motion or real-time television pictures. Narrowband video conferencing is the use of one or more narrow bandwidth (less than 1.544 megabits) communications links to transmit and receive still or freeze-frame television pictures.

(U) A variety of firms, both foreign and domestic, are frequently mentioned in current literature as being heavily involved in providing wideband video conferencing. Some of these companies include Nippon Telephone and Telegraph (NTT) of Tokyo, Northern Telecom (NT) of Toronto, International Telephone and Telegraph (ITT), Radio Corporation of America (RCA), and Satellite Business Systems (SBS). There are three wideband full-motion video teleconferencing configurations available. They are:

[] full-motion one-way video;

[] full-motion one-way video/two-way audio; and

[] full-motion two-way video/two-way audio.

(U) Full-motion one-way video is suitable for educational meetings where basic information is being presented to conference participants in remote locations and complete interaction is not necessary. Full-motion one-way video/two-way audio allows transmitted presentations to a group of conferees at a remote location or several locations with the ability for complete audiointeraction. This form of video conferencing is used for education, sales, training, or any other meeting that presents information to a widely dispersed group of people.

(U) Full-motion two-way video/two-way audio is the most complete form of video teleconferencing. Total interaction, both visual and audio, by participants in this configuration is the closest thing to a face-to-face meeting. Wideband video most closely resembles the traditional face-to-face gatherings and provides immediate feedback on presented information. The facial expressions and all other movements of the speaker and conferees are there for all to see. This mode of operation is not unlike that of television today. "There is a feeling of psychological presence,"[9] with wideband video.

(U) Narrowband video conferences use bandwidth that cannot pass video information fast enough to support motion pictures. Since narrowband video links normally travel over ordinary voice-grade telephone lines, their use represents a less costly investment with regard to bandwidth required. These lines can transmit video signals at an average rate of one frame every 70 seconds. This type of system is commonly referred to as "slow-scan" or "freeze-frame" television. The use of the narrowband method in establishing a participant's presence provides sufficient psychological feedback for continuing information on the overall situation at other locations.

> "Pictures transferred under these conditions are somewhat poorer than the full video [wideband] we have all experienced in live television. In a conference situation, slow-scan [narrowband] picture transmission is very often adequate and useful, depending on the live interaction required."[10]

(U) Studies of both narrowband and wideband video systems revealed that some subscribers of narrowband video are still satisfied that the freeze-frame image is adequate. Others feel that full-motion video, realized through the wideband technique, is required to establish a user presence and provide a more productive and effective meeting.

Single and Multi-Point Conferences

(U) Another consideration when implementing a video teleconferencing system would revolve around the selection of either single- or multiple-point configurations. The magnitude of the organization and the diffuseness of its field headquarters and stations would be primary considerations in this decision.

~~(C)~~ A single point-to-point schema would allow for video communications between two locations only, such as NSA, Fort Meade, with Hq NSAPAC, Pearl Harbor. This arrangement is depicted graphically in Figure 1. Such a system limits participants as well as conference station locations. However, a strategically located studio in the Pacific or European theaters linked with NSA Headquarters would allow for easier access by field station managers and other participants from nearby field stations than would travel to Fort Meade.

(U) A multiple-point conference configuration entails the selection of three or more field stations. These stations can be, but are not necessarily, confined to the same geographic area. This mode of operation would provide the means of conducting business with more participants on an extended spectrum simultaneously. For example, consider a multiple-point conference arrangement connecting NSA, Fort Meade, and Hq NSAPAC, Pearl Harbor, with field stations [redacted]. The NSA Fort Meade junction would serve as the nodal point or controlling facility for all of the conferences. Possible multiple-point system schematics are shown in Figures 2 and 3.

EO 1.4.(c)
P.L. 86-36

NSA APPLICATIONS OF VIDEO TELECONFERENCING

Considerations in Implementation

(U) Prior to any decision by NSA management to implement video teleconferencing systems, careful and thorough analysis must be conducted to ascertain the following:

[] Could travel expenditures be reduced to offset the procurement and maintenance costs of the system?

[] Could mission elements realize a marked increase in productivity through the use of video teleconferencing?

[] Could NSA employees adapt to the use of video teleconferencing as a replacement for face-to-face meetings?

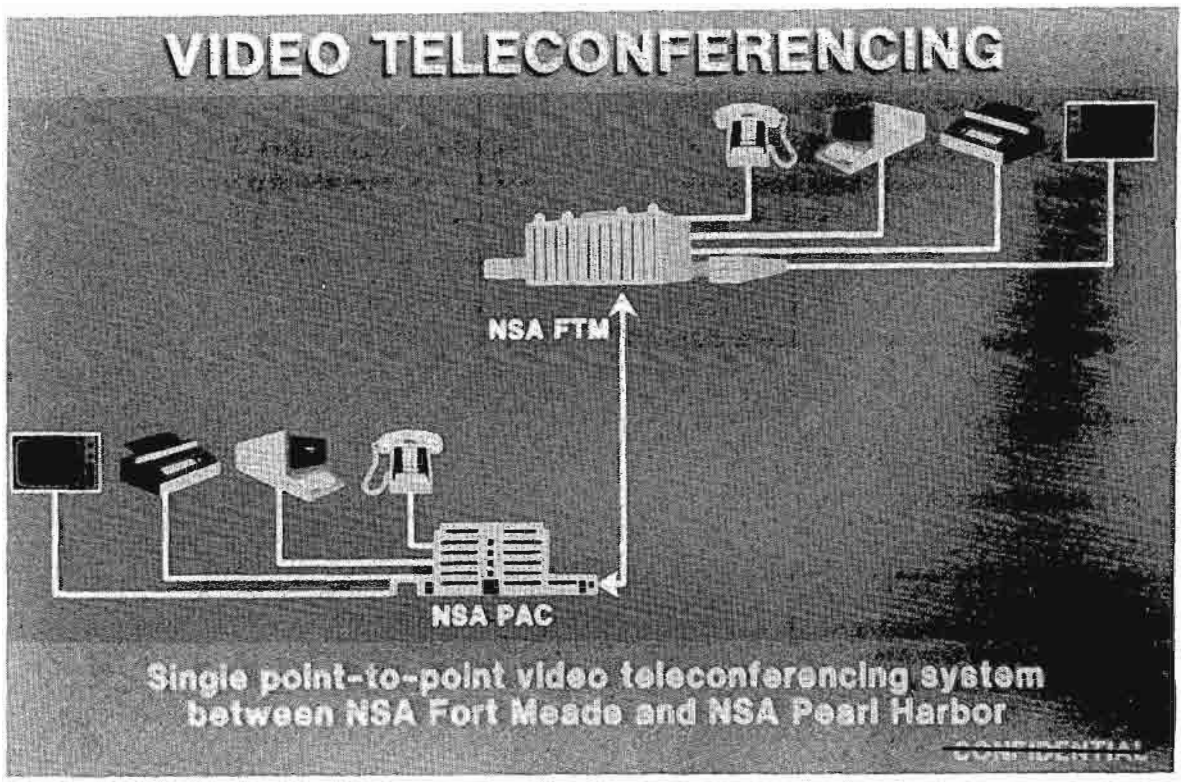
[redacted]

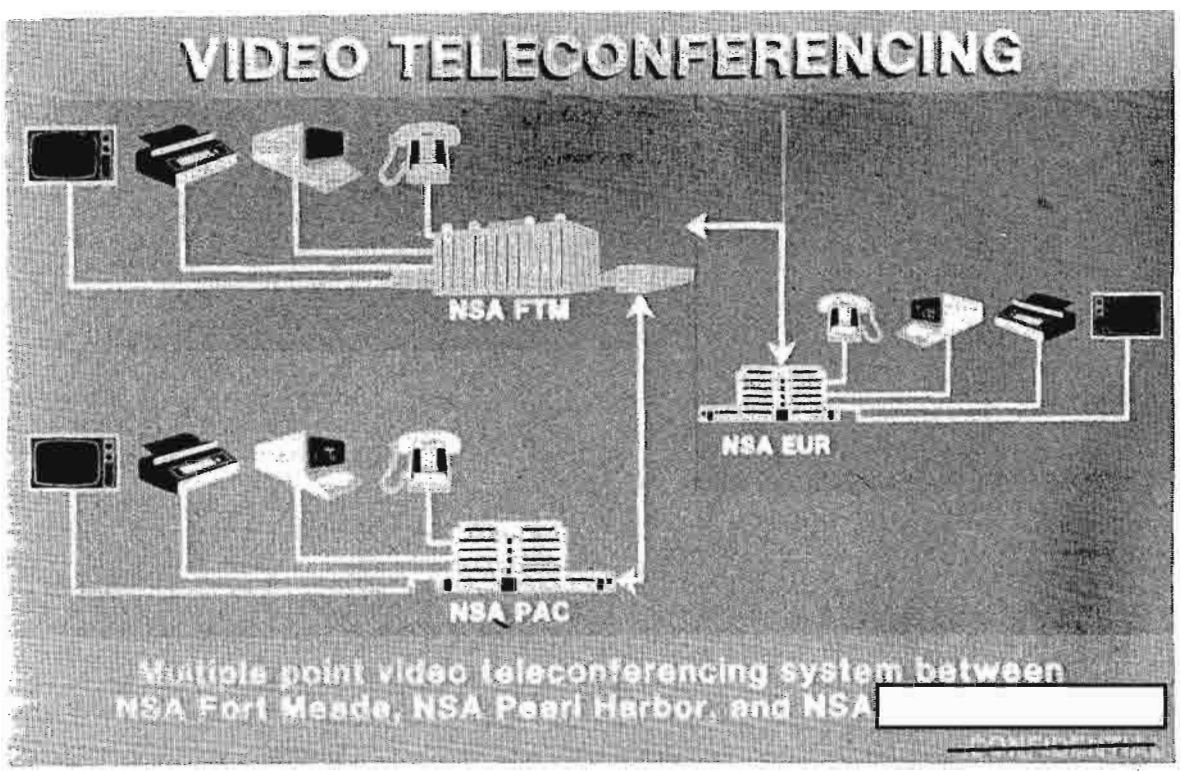
EO 1.4.(c)
P.L. 86-36

[redacted]

Table 1 ~~(C)~~

~~(C)~~ If NSA elects to adopt video teleconferencing as an alternative to travel, it is possible that the Agency could realize a savings similar to that projected by Atlantic Richfield of 20 percent annually. Using this hypothesis, NSA might have realized a savings of $3.8 million by the end of 1982 if a video conferencing system had been fully operational. Savings by the end of 1983 could reach the $5 million mark. However, in any given year that the system is tasked for implementation, the majority of the majority of the initial travel savings would be consumed in procurement, installation, and training costs. But, given a two-year operational period from the time of the initial operating capability (IOC), NSA would begin to realize a substantial return on its investment. A minimal portion of the yearly return, estimated at 15 percent per annum, could then be applied toward the operational and maintenance (O&M) costs of such a system. Savings in travel at a rate of 20 percent annually (Atlantic Richfield) and the estimated operational and maintenance costs of 15 percent per annum to be realized by NSA with the adoption of video conferencing are shown in Table 2.





EO 1.4.(c)
P.L. 86-36

Table 2 ~~(C)~~

(U) If NSA communications were entirely dependent on written messages, instead of video teleconferencing or travel, each project worker would have to be concrete and specific in his or her project presentation and explanation. The real-time feature of video teleconferencing would be lost through travel and written messages. Video conferencing would eliminate some of the formal written communique. Chances of having all needed personnel at a video project meeting would be greater. Users would have at their disposal a means of presenting the target area graphically. Productivity, then, should definitely be an outcome of structured, well organized, timely video teleconferencing.

(U) A study conducted by Satellite Business Systems (SBS) indicates that 54 percent of video users were as successful with business meetings through video conferencing as they were through face-to-face meetings, 31 percent were not as successful, 10 percent were more successful, and 5 percent were much less successful.[12] A total of 64 percent of video users proved to be as satisfied or more so with the use of video conferencing than with face-to-face meetings.

(U) It is impossible to predict the NSA user acceptance or rejection of a video system. It can be expected that some individuals at NSA will be reluctant to accept video teleconferencing as a new communications tool and a replacement for face-to-face meetings. They may question video's structured, impersonal nature. Some at NSA may not function as efficiently under the time constraints imposed by video. Still others may miss the change of pace and morale enhancement provided by travel.

(U) However, if NSA video participants' opinions parallel those of users in previous studies, it could be expected that a majority of video users would be satisfied with conference results using this new method of communications. User acceptance may be enhanced through practice sessions, frequent use, positive reinforcement, and a relaxed atmosphere.

EO 1.4.(c)
P.L. 86-36

The meeting isn't over yet!

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Advantages & Disadvantages in Adopting Video Teleconferencing

~~(C)~~ Up to this point, few negative aspects other than the possible psychological barriers to NSA Participants have been cited. It is necessary that additional shortcomings for NSA be mentioned. Scheduling conference times to suit wide time-zone differences between NSA Headquarters and European or Pacific field stations is a major stumbling block. Participant flexibility is crucial in such situations.

This figure may be discouraging, but still an overall savings in travel would be realized. Finally, conference participants who are not fully prepared for scheduled video conference time would create an immediate loss of money, time, and productivity. It then becomes essential for NSA management to alert all conferees that such waste will not be tolerated.

(U) Although many of the advantages to be realized through the adoption of videoteleconferencing have already been expounded on through studies of corporations' successfully use of the video link, they must be restated in terms of NSA usage. Cost efficiency, timeliness in decisions, improved work coordination and productivity enhancement may all be possible for NSA. In addition, more employees would be able to attend and more flexible meetings would result.

Resources (Bandwidth & Equipment)

(U) To establish a video teleconferencing system at NSA Headquarters and other sites, it would be necessary to reserve exclusively one existing conference room at each. The permanent features of the room would include, but are not limited to, fixed-position cameras, a facsimile device, telephones, a blackboard (preferably electronic), a computer terminal (for use at Headquarters) interfacing with one of the major NSA complexes, television monitors, and microphones. It would also be necessary to modify the room to ensure proper acoustics. At the present time, the actual video equipment is available at the Agency, but its use is reserved exclusively for the NSA television production studio. Other needed equipment presently exists at NSA, but it also is currently on use to satisfy in-house production and mission requirements. Therefore, procurement action for all video teleconferencing and associated equipments would be necessary. Once purchased, this equipment would be dedicated for the sole use of NSA video teleconferencing. Identical equipment would be required at all selected video conferencing field stations. In addition to video conferencing equipments, communications interfacing equipment would be required to transfer signals. This equipment includes cryptographic devices to secure transmissions, modulators/demodulators, multiplexers, expanders, translators (transceivers), and line drivers.

Financial and Manpower Analysis

(U) Types of video teleconferencing system arrangements are numerous and varied. A number of components determine the actual system cost. The variants include television production, length of broadcast, audio system, number of receiving locations, projection equipment, and the actual conferencing room. A basic slow-scan configuration consisting of a transceiver, a camera with appropriate lenses, black-and-white monitors, and associated accessories for one location costs approximately $25,000.[15] This particular system would provide freeze-frame video with a high resolution of 78 seconds, switchable to a medium resolution of 35 seconds. In contrast, a full-motion (real-time) video color system's cost would begin at approximately $50,000 per location.[16] Initial video system costs do not include transmission medium expenditures, operator training, or the interfacing communications equipment. Prices remain fairly consistent between specific equipment suppliers, such as Videonet Incorporated, Colorado Video, and American Satellite. For NSA to determine the amount of funding required to install a dedicated video conferencing system, an in-depth study of desired equipment would be necessary. Only after specific equipment is selected, could a total system expenditure be finalized.

(U) It is estimated that one trained television production technician would be needed at each location.[17] NSA currently employs 6 to 10 skilled television production technicians at Fort Meade. Their expertise in the video area could possibly provide in-house training for future video system controllers. However, field station personnel would be required to travel to NSA, or trained technicians could be sent to various video-established locations to provide the needed production training. Fellowship programs could be established, which could also allow NSA staff members to become educated in the area of video conferencing production. There are too many variables, beyond system and bandwidth costs, at this time for a bottom-line dollar figure to be rendered.

Immediate & Long-Range Applications

~~(C)~~ An immediate application of video teleconferencing at NSA could connect NSA Headquarters with the Friendship Annex and various government agencies in the Washington DC area. Bandwidth is presently available for such communication links. To introduce video at NSA, it is recommended that both slow-scan and full-motion capabilities be utilized independently on a trial basis. The Agency would then be able to evaluate system functioning and determine future video teleconferencing needs.

(U) If video is evaluated as a reliable and productive NSA communication tool, future applications should include connections with NSA field headquarters in Europe and the Pacific. In time, it is not unrealistic to expect that with favorable acceptance of the video link, video teleconferencing connections could multiply to include numerous selected NSA field stations worldwide.

CONCLUSION

(U) It becomes apparent through researching the field of video teleconferencing that it is, in fact, a tremendous communications tool which can be used for the enhancement of conference productivity and travel reduction. It is hoped that NSA will approach video teleconferencing with total openness. As this research has shown, many managers from a wide spectrum of corporate disciplines are using video teleconferencing today and are realizing increased productivity as well as reduced travel budgets. Monetary savings with video teleconferencing is considered to be the most popular for its use. Across-the-board dollar

figures can be produced to support a video system. Savings of time have also been found to be a major asset gained through the use of a successful video teleconferencing system. Management's efficient use of time is at the heart of productivity. Through video teleconferencing, quicker and more efficient response times and decisions are realized. Therefore, savings in time can always be regarded as a credible justification, along with monetary savings, for the implementation of video teleconferencing. It cannot be overemphasized that, for management, video teleconferencing can provide shorter, more productive meetings with less turn-around time on projects.

(U) With the adoption of a video teleconferencing at NSA and selected field stations, there must be a total commitment on the part of the Agency to the concept of video conferencing. Favorable attitudes toward teleconferencing must also exist. A clearly defined conference format must be developed and adhered to, to ensure system success. Highly reliable communication links and easy-to-use and accessible video conferencing equipment must be provided. A quality video teleconferencing system could possibly convert doubters into avid users and possible advocates. Increased productivity will likely be an incentive for increased video system use. Although it is not realistic to expect all travel to cease, closer scrutiny of travel requests should be conducted. This would be necessary if NSA is to realize a positive return on its investment in a video teleconferencing system.

(U) When all the facts concerning video teleconferencing are weighed, I think that the scales will tip in favor of NSA's adoption of a video teleconferencing system.

Footnotes:

1. File, Karen N., "Teleconferencing: A Case Study," Office, November, 1981, p. 88.
2. Johantgen, Beverly, "Video Teleconferencing--A Brave New World," Computer World, 17 March 1982, p. 12.
3. Interview with [redacted] Finance Office, National Security Agency, Ft. George G. Meade, Md., 24 May 1982.
4. Interview with [redacted] Office of Personnel Administration, National Security Agency, Ft. George G. Meade, Md., 6 October 1982.
5. Albertson, Lesley A., "Telecommunications as a Travel Substitute: Some Psychological, Organizational, and Social Aspects," Journal of Communications, Spring 1977, p. 33.
6. Perham, John, "Business' New Communications Tool," Dun's Review, February 1981, p. 81.
7. "Telecommunications and Energy Policy," Telecommunications Policy," Vol I, No. 1, cited by Jeff Charles, "Approaches to Teleconferencing Justification: Towards a General Model," Telecommunications Policy, December 1981, p. 297.
8. Munsey, Wallace, "Wide-band versus Narrow-band Video-conferencing: The User Must Decide," Telecommunications, February 1981, p. 50.
9. Ibid., p. 48.
10. Johantgen, op. cit., p. 12
11. [redacted] interview, 24 May 1982.
12. Rush, C.T., "Evaluation Report on Project PRELUDE, Experiment No.26 in the Communications Technology Satellite Program." PRELUDE-Communications of the 80's, May 1978.
13. Interview with James Keller, Plans and Requirements, National Security Agency, Fort George G. Meade, MD, 6 June 1982.
14. Interview with [redacted] Facilities Control Office, National Security Agency, Fort George G. Meade, MD, 25 October 1982.
15. Interview with James Dole, Colorado Video Incorporated, AFCEA Conference, Washington, DC, 16 June 1982.
16. Ibid., Interview, 16 June 1982.
17. Interview with Tim Gately, Television Production, National Security Agency, Fort George G. Meade, MD, 25 October 1982.

P.L. 86-36

DOCID: 4019691

IS THE GLASS HALF EMPTY OR HALF FULL?(U)

by [redacted]

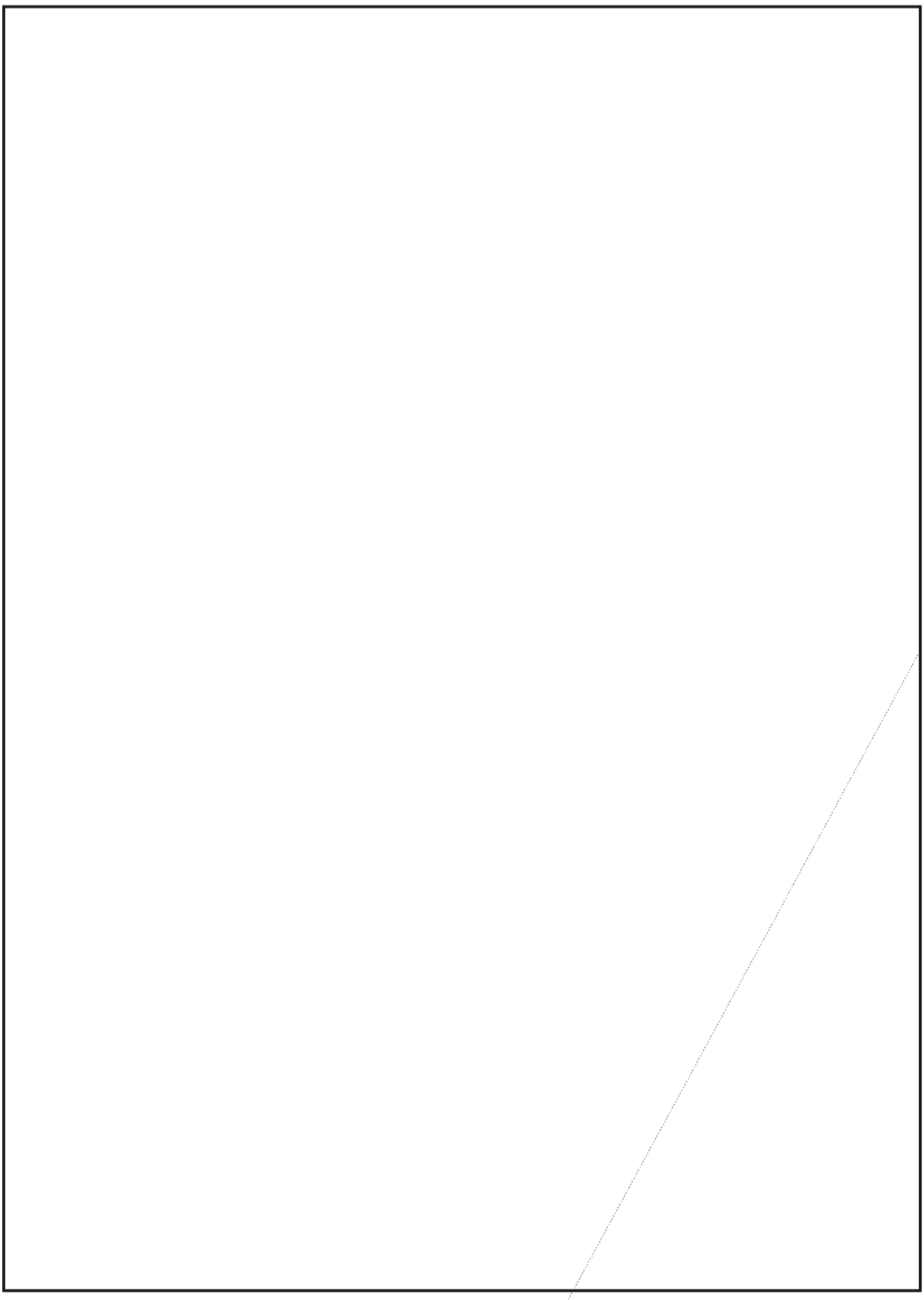
[redacted] P.L. 86-36

EO 1.4.(c)
P.L. 86-36

(U) Being prone to kicking dead horses, I decided that the title for this article should be based on the well-worn philosophical anecdote of the pessimist who perceives a glass of water half-empty, while the optimist is certain that the same glass is half-full. Of course the fact I am basically lazy, and that this title met my self-inflicted requirement that nothing should be overtaxing to my thought processes, played some role in helping to select the title. My one problem with it is that I have a difficult time convincing myself that a glass with any amount of water deserves contemplation at all. As with all of us, I am most happy with a glass that is all full or all empty. Unfortunately, reality is rarely represented in clear-cut choices and that blasted, undefinable glass is always there to make life difficult.

[redacted]

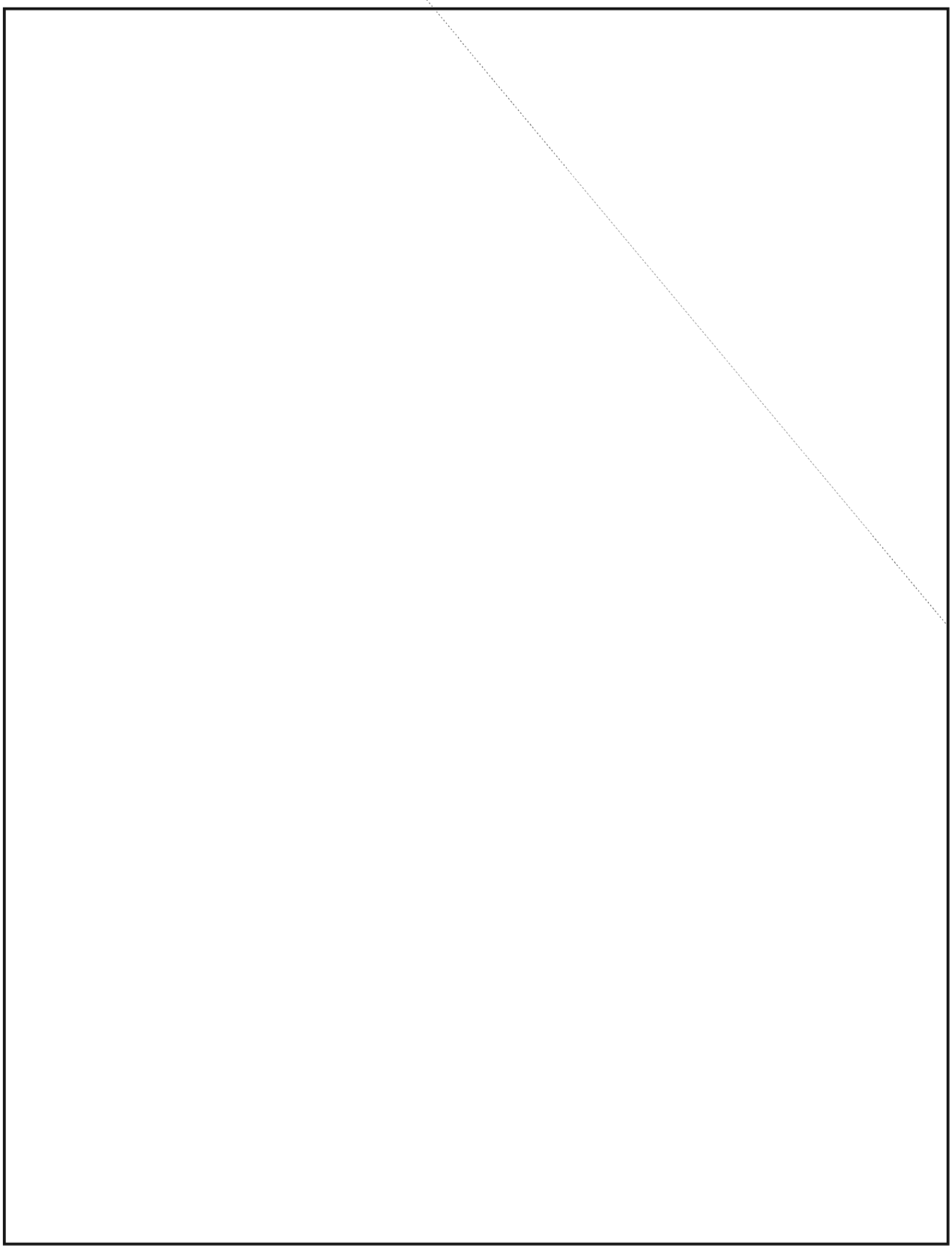
[redacted]

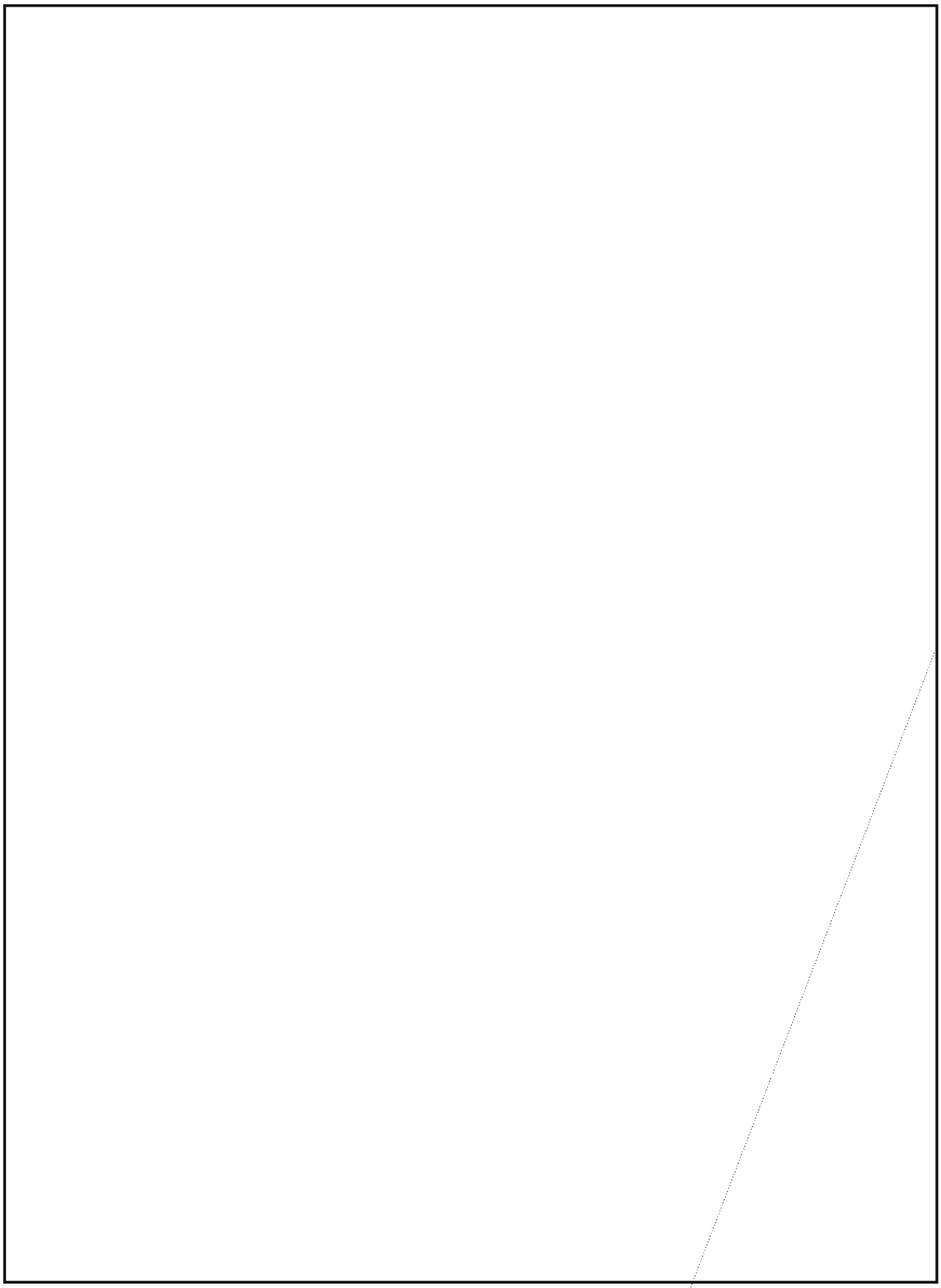


EO 1.4.(c)
P.L. 86-36

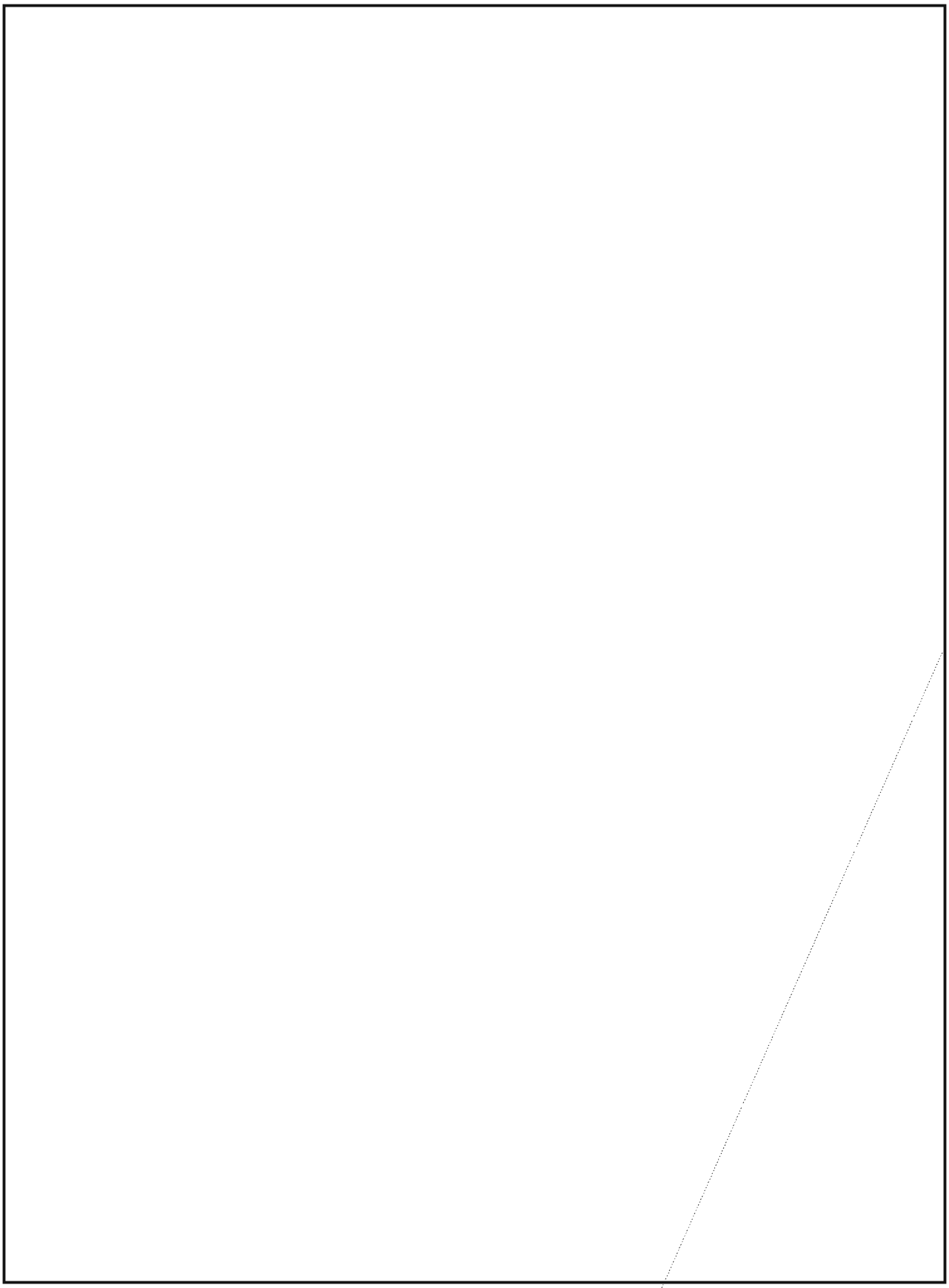
DOCID: 4019691

E0 1.4.(c)
P.L. 86-36



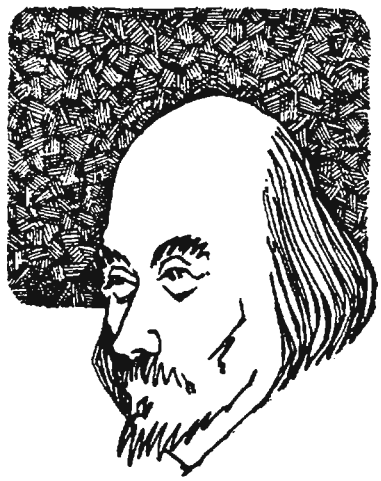


EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

OCID: 4019691



CUMULATIVE INDEX

(U)

Part One: AUTHORS

Aug 74 A Short Directory of Career Panels
Aug 74 Golden Oldie: The Management Survey of the Philharmonic
Aug 74 Learned Organizations--1974 CLA Essay Contest, 1974 CMI Essay Contest; CISI Prizes and Honors, Spring 74
Aug 74 Puzzle: Stinky Pinky
Aug 74 Puzzle: Telephone Directory
Aug 74 The New Traffic Analysis Glossary
Sep 74 Contributions Solicited
Oct 74 Golden Oldie: An Unofficial Glossary of Weasel Words
Oct 74 News from NCS--Agency Resumes Hiring of LICs; NCS Offers Course in 'SIGINT Appreciation'
Oct 74 Puzzle: Telephone Recall
Nov 74 Golden Oldie: A Medal for Horatius...
Nov 74 The Apostrophe: Some Thought's
Dec 74 Cryptolog Index for 1974
Dec 74 Puzzle: Citizens of the World
Dec 74 Puzzle: Secret Messages, 'Military Cryptanalytics'
Jan 75 Cryptolog Index for 1974
Jan 75 Learned Organizations--IAI News, CISI News; CLA is Ten Years Old!; CMI News
Feb 75 Golden Oldie: Establishment of Molecule Superseries
Feb 75 The Devil's Dictionary
Apr 75 A Guide to Central Information, C5
May 75 Learned Organizations--CLA News; IAI News
May 75 Puzzle: How Many Words in 'CRYPTOLOG'
Jun 75 COMSEC Familiarization: Do You Need It?
Jun 75 Golden Oldie: SIMP Tables
Jun 75 The Navajo Code Talkers
Jul 75 Learned Organizations--CLA News; CMI News
Aug 75 Computer Network Resources In C5
Aug 75 Language in the News

The following cumulative index of CRYPTOLOG (Vols. I through IX, 1974-1982) was produced using UNIX/PINSETTER tools on MYCROFT and BARDOLPH1. The index is in three parts, and is being published in three successive issues. Part one is an index by author; part two is an index by keyword; and part three is an index by title. Items in multiple issues (February-March 1975, for example) are indicated by the first month (i.e., by Feb 75).

Aug 75 Puzzle: CRY-PTO-LOGrolling
Oct 75 Letter: Typewriter Keyboard
Nov 75 NCS Offers Course-Equivalency Tests
Dec 75 Cryptolog Index for 1974-1975
Dec 75 Establishment of CSI Newsletter
Dec 75 Learned Organizations--CLA Essay Contest; CAA News
Mar 76 1976 Language Meetings and Conferences
Apr 76 Language in the News: Language Rule
Apr 76 NCS Offers Course-Equivalency Tests, Clarification
Aug 76 Language in the News
Aug 76 NSA Cryptologic Collection
Aug 76 Note on FRANCOPHONEGLOS
Sep 76 Language in the News
Sep 76 Learned Organizations--1976 CLA Essay Contest; 1976 CMI Essay Contest
Oct 76 The Winnah: Kid Apostrophe!
Jan 77 Golden Oldie: A Medal for Horatius...
Aug 77 DIALOG Available at NSA
Aug 77 Want to Play with a Pickfair Square?
Oct 77 The Perils of Being a State Department Interpreter
Dec 77 Cryptolog Index for 1977
Feb 78 Puzzle: Three Holes

Mar 78 Answer to Three Holes
Mar 78 CLA News
Apr 78 Prizewinners in Three Holes
Jun 78 Golden Oldie: Unidentified Unit at Unknown Location
Sep 78 CLA News
Sep 78 T Establishes Human Resource Development Panel
Oct 78 Overheard in the Burnbag Line
Dec 78 Cryptolog Index for 1978
Jan 79 CMI News
Jan 79 How do You Tell These Two Clowns Apart?
Jan 79 Human Factors Newsletter
Jan 79 W.W.II Japanese Translation at Arlington Hall Station
Feb 79 CLA News: Russian Institute
Feb 79 Language Career Panel: Clarification of Nov 78 Item
Mar 79 Attention Military Traffic Analysts
Mar 79 CISI News
Mar 79 Classic Cables
Apr 79 Bookbreakers Forum
Apr 79 Classic Cables
May 79 CAA News
May 79 CISI News: Spring Conference
May 79 Classic Cables
Jun 79 CAA News
Jun 79 Sign Language
Jul 79 Russian Handbook of Spoken Usage, Vol 3
Jul 79 Seminar on Translation Problems
Aug 79 ... But On The Other Hand
Aug 79 Memorable Memos
Oct 79 CAA News: Conference on Communications Analysis
Oct 79 CLA News
Oct 79 NCS Summer Language Program
Oct 79 [redacted]
Jan 80 CLA News: Sydney Jaffe Award
Jan 80 NSA/CSS Military Linguist Program
Apr 80 Geographic Trivia
Jan 81 NCS-CLA Symposium
Jan 81 Some Things Never Change
Apr 81 Classic Cables
Apr 81 DIA Videocasette Program
Apr 81 The Poet's Corner
Jan 82 All The Alligators Aren't On Sport Shirts
Mar 82 Attention Authors and Publicity Chairmen
Apr 82 Overheard While Standing in the Burnbag Line
May 82 Cryptolog Numbering
Jun 82 Odds and Ends

'Anon.'
Dec 74 Letter: [redacted] Article
Jun 75 Letter: [redacted] Letter
Jun 75 Project SYMBIOSIS
May 76 Conversation With a Bookbreaker
Nov 76 Check Your Morse Front-End Alignment
Mar 77 A Few Thoughts on the NSA Linguist
Jan 78 The Changing Face of NSA
Nov 78 Letter: Appraisal System

'Appalled'
Mar 77 Letter: C-LINERS Article

'Asken'
Oct 77 Which Numbering System Should We Use?

'Donym'
Jan 79 Second Sighting

'Exinterne'
Sep 74 A Long Hard Look at the Intern Program--Program Philosophy; Recruitment (Part One)
Oct 74 A Long Hard Look at the Intern Program--Selection and Orientation (Part Two)
Nov 74 A Long Hard Look at the Intern Program--Motivation and Morale (Part Three)
Dec 74 A Long Hard Look at the Intern Program--What Happens to the Graduate? (Part Four)

'Fennwatcher'
Apr 78 Letter: [redacted] Article

'Leiner'
Jan 77 Executive Order 11652

'Mouse'
Aug 77 Letter: Subscription

'Reader'
Oct 77 Letter: AG-22 Page Print

'Sardonyx'
May 78 NSA-Crostic No. 14

'Schmedlapp'
Dec 82 Questions In Search of a PQE

'Sue'
Apr 79 Letter: Ask Art

'Weeson'
Aug 77 Letter: [redacted] Article

'Class 32'
Sep 77 Tribute to the Guru

A.J.S.
Oct 75 NSA-Crostic No. 1
Jan 76 NSA-Crostic No. 2
Apr 76 NSA-Crostic No. 3
Jun 76 NSA-Crostic No. 4
Oct 76 NSA-Crostic No. 5
Jan 77 NSA-Crostic No. 6
Jun 77 Vich Iss R-r-right?
Jul 77 NSA-Crostic No. 8
Sep 77 'Simonoff Says!'
Sep 77 Al Balloni, Editor
Nov 77 NSA-Crostic No. 10
Jan 78 The Joys and Frustrations of Plural-Dropping
Feb 78 No, Winnie, You've Got It Upside Down Too!

EO 1.4.(c)
P.L. 86-36

P.L. 86-

DOCID: 4019691

P.L. 86-36

Mar 78 NSA-Crostic No. 12
Jun 78 NSA-Crostic No. 15
Sep 78 NSA-Crostic No. 17
Dec 78 'No, No, Nanette!' Means Yes?
Jan 79 Al Balloni, Editor

[redacted]
Feb 75 The Gulf of Tonkin Incident
Oct 75 Tactical Language Exploitation: A Lesson Learned?
Aug 76 Integrated Analysts for Asia
Jul 77 Letter: [redacted] Article
Oct 81 The Stairwell Society

[redacted]
Feb 78 Senior Military Cryptologic Supervisors Course

[redacted]
Mar 78 [redacted] EO 1.4.(c) P.L. 86-36

[redacted]
Dec 75 Graphic Analysis of Linear Recursive Sequences

[redacted]
Aug 74 Self-Paced Instruction: The Future is Now!

[redacted]
Jul 78 Is A Translator a Professional?

[redacted]
Apr 80 OH, K!

Barrer D.Y.
Sep 78 Letter: Gilbertson Letter

[redacted]
Jul 75 Re-psychling the Code Clerk

[redacted]
Apr 75 Letter: Professionalization of Bookbreakers

[redacted]
Jul 77 The Transcription Skill: Concepts and Teaching Methodologies

[redacted]
Jun 78 Equipment Maintenance on ABNER

[redacted]
Jul 78 The Soviet General Staff

[redacted]
May 82 Letter: Plaintext

Bjorklund K.
Dec 76 Why Can't They Design a Good SR Test?
Jun 79 Letter: [redacted] Article

[redacted]
Apr 77 'It's Got to Get Out Today!'

[redacted]
Apr 75 The Uses of ELINT

Boak D.G.
Apr 79 COMSEC/SIGINT Relations

[redacted]
Jun 79 Letter: Library Changes

[redacted]
Jun 75 The Role of the Electronic Warfare Advisory Element (EWAE) of NSA
Mar 76 Letter: Proud and Bitter Memories Article
Jun 76 Computers In The ELINT and TELEMETRY Business

[redacted]
Dec 74 The Old [redacted] Section EO 1.4.(c) P.L. 86-36

Bostick C.W.
Nov 76 Letter: Cumulative Index
Feb 79 Letter: [redacted] Article (Dec 78)

Boucher M.J.
May 75 Letter: [redacted] Article
Apr 77 Letter: Mason Article
Jun 77 More about More about the NSA SIGINT Summary

[redacted]
Apr 82 Word Processing In A4

[redacted]
Dec 82 KRYPTOS News

[redacted]
Dec 74 Maps in Mind--A Photoessay

[redacted]
Jul 79 Letter: Bjorklund Letter (Jun 79)

[redacted]
Apr 77 Contemplating Computing

[redacted]
Oct 78 And-a You Betta Have Moti-vaysh!
Apr 79 Fear of Testing, and What To Do About It

[redacted]
Jul 78 The Bucky Balance

[redacted]
May 76 Hypnosis and Self-Hypnosis in Language Learning
Mar 77 Letter: [redacted] Article
Sep 77 Letter: [redacted] Letter
Sep 78 Letter: Pattie Article
Dec 78 Agency Summer Language Study
Jul 79 Letter: Bjorklund Letter (Jun 79)

P.L. 86-36

Buck S.H.
Sep 74 Some Thoughts on Lexicography
Nov 76 Toujours La Politesse (Japanese)
Jul 77 [redacted]
Nov 78 Linguistics and the Code Reconstructor

[redacted]
Aug 74 What Is a Collector?
Dec 74 The New Collection Criteria
Apr 76 Will the Real ELINT Please Stand Up
Aug 79 An August Baudy

[redacted]
Dec 76 But It Looks Like the Real Thing

[redacted]
Nov 76 Letter From Canada

[redacted]
Mar 76 A Comparison of NSA and ATA Certification Standards
Oct 76 Work Quotas for Soviet Translators
Dec 76 Let's Give the Linguists a Bigger Piece of the Pie!
Nov 77 What Ever Does 'However' Mean?
Oct 78 More B.S. (Before Spellman)

[redacted]
Jan 76 63 Days--The Soviets in Space
Sep 78 [redacted]

EO 1.4.(c)
P.L. 86-36

Callimahos L.D.
Apr 75 Psyching the Code Clerk: [redacted]

[redacted]
Oct 75 The Danang Processing Center
Apr 76 One Day in Danang

[redacted]
Jun 76 Comments on the AG-22/IATS

[redacted]
Apr 78 Remedial Software Engineering

[redacted]
Nov 76 The Uses of Elegant English

[redacted]
Nov 81 OPELINT Is Alive and Well In B Group

Chauvenet L.R.
Apr 77 NSA-Crostic No. 7
Aug 77 Early Days in NSA Computing
Sep 77 The Doctor Is In(capable of Diagnosing)
Oct 79 The Roads Around Us
Jan 82 Letter: Persephone Terpsichore Article

P.L. 86-36

P.L. 86-36

[redacted]
Mar 76 An Objective Approach to Scoring Translations
Apr 76 The Voynich Manuscript Revisited
Aug 76 NSA's System for Grading Translations
Mar 79 VORD is a Better Idea

[redacted]
Oct 77 [redacted]

[redacted]
Apr 77 Some Thoughts on the Russian PQE
Aug 79 Punctuation: More Than Meets The Eye

EO 1.4.(c)
P.L. 86-36

[redacted]
Oct 75 IRONHORSE: A Tactical SIGINT System

P.L. 86-36

[redacted]
Nov 76 How to Make a Railroad Disappear

[redacted]
Jan 77 Letter: Use of Term 'Compartmented'

[redacted]
Nov 75 DESKPAD: A Programmers's Tool
Feb 76 The [redacted] System

EO 1.4.(c)
P.L. 86-36

[redacted]
May 82 Is There An Old Crow In Your Future

[redacted]
Apr 82 Partial Machine Translation: Final Report

[redacted]
Jan 80 LIP

[redacted]
Feb 82 The Internal Performance Evaluation: Friend or Foe?

[redacted]
May 76 What's Wrong with AG-22/IATS?

P.L. 86-36

[redacted]
Sep 77 Knowledge Resource Management at NSA

[redacted]
Apr 76 How Do Adults Learn Language?

[redacted]
Feb 78 [redacted]

EO 1.4.(c)
[redacted]L. 86-36

[redacted]
Feb 76 Expletives Deleted: Glossing Over a Glossary

[redacted]
Aug 76 The Hierarchical Clustering of Cryptanalytic Data
Mar 77 CADRE Reveals What Data Conceals
Dec 77 What Is Pattern Recognition?
Apr 78 A Little PEP Talk
Nov 78 A Dialogue Between Ms. User and Dr. Analysis

P.L. 86-36

DOCID: 4019691
P.L. 86-36

May 79 Emitter Identification Techniques

[redacted]
Nov 81 Cryptic Crossword
Mar 82 Cryptic Crossword
Mar 82 Rules For The Camel Corps

[redacted]
Oct 75 Linguists -- You Have an Expert to Call!

[redacted]
Dec 77 What Made Them Do It? (Language Self-Study)

[redacted]
Mar 77 An Overview of Project [redacted]

Craig D.K.
Sep 74 COMINT Analysis of [redacted]
Oct 81 Economic Intelligence: Problems and Prospects

EO 1.4.(c)
P.L. 86-36

[redacted]
Dec 74 Learned Organizations--CISI Forms Special Interest Group on Human Factors
Jun 77 Human Factors and Systems Design: An Estranged Relationship?

[redacted]
Oct 78 Letter: NSA-Crostic

Crowell B.
Jun 78 A Computer Scratch Pad at Home or at Work?

[redacted]
Oct 77 Golden Oldie: Analyzation of Data

[redacted]
Feb 75 CAMINO News
Jul 75 Machine Intelligence--Promise or Delusion?
Oct 76 Some Ideas about Mechanized Language Working Aids
May 77 Another Controversial Book on Artificial Intelligence
May 78 The Joys of UNIX
Nov 81 How to Create A User-Unfriendly System
Nov 81 Review: What Do You Think?
Dec 81 Review: In The Name of Efficiency
Jan 82 Human Factors Corner: Information System
Feb 82 Human Factors Corner: But What Do I Do With My Papers?
Feb 82 Human Factors Corner: Some Advice to Users of Unfriendly System
Mar 82 Human Factors Corner: Consumer vs. Computer: A Review
May 82 Human Factors Corner: Data Gathering, How Do We Spend Our Day?
Jun 82 Human Factors: Responsible Documentation
Aug 82 Human Factors Corner: Video Display Terminals and Vision of Workers
Oct 82 Human Factors Corner: Text Editors
Nov 82 Human Factors Corner: How Do People Organize Cooperative Work?
Dec 82 Passwords

D.H.W.
Feb 79 NSA-Crostic No. 22
Mar 79 Readers' Survey
Apr 79 But, Mr. Boak, Did You Ever Try To Get Rid of One in a Hurry?
Apr 79 NSA-Crostic No. 24
May 79 NSA-Crostic No. 25
Jun 79 NSA-Crostic No. 26
Jul 79 NSA-Crostic No. 27
Aug 79 NSA-Crostic No. 28
Oct 79 NSA-Crostic No. 29
Jan 80 NSA-Crostic No. 30
Apr 80 NSA-Crostic No. 31
Jan 81 NSA-Crostic No. 32
Apr 81 NSA-Crostic No. 33
Oct 81 NSA-Crostic No. 35
Dec 81 NSA-Crostic No. 36
Jan 82 NSA-Crostic No. 37
Feb 82 NSA-Crostic No. 38
Apr 82 NSA-Crostic No. 39
May 82 NSA-Crostic No. 40
Jun 82 NSA-Crostic No. 41
Aug 82 NSA-Crostic No. 42
Oct 82 NSA-Crostic No. 43
Nov 82 NSA-Crostic No. 44

[redacted]
Feb 79 Data Standards Without Tears
Jun 79 Data Standards Without Teeth

[redacted]
Sep 76 More Comments on the AG-22/IATS

Dawson R.
Feb 76 The Prebendary and the Prophet
Jun 76 The Marquis and the Medium
Dec 82 NSA-Crostic No. 45

[redacted]
Apr 81 Grading The Russian PQE

[redacted]
Jun 82 Who Wants A Promotion, Anyway?

[redacted]
Feb 76 What Is Cipher Text?
Jan 82 Letter: Cryptanalysis Article
Mar 82 Letter: Strangest Bust of the Month

[redacted]
May 77 The Polyhedral War

[redacted]
Jul 77 Letter: [redacted] Article

P.L. 86-36

DOCID: 4019691

~~SECRET~~

P.L. 86-36

[redacted]
May 75 Hooray for PMDs!

[redacted]
Oct 75 [redacted]

[redacted]
Oct 74 The Mission of the Signals Processing Requirements Panel

Dudley B.
Aug 74 Nice Busman's Holiday for One NSA Employee

EO 1.4.(c)
P.L. 86-36

[redacted]
Oct 76 Another Word on AG-22/IATS
Nov 81 Futuristic Reporting

[redacted]
Aug 74 What Should You Expect? or, The Analysis of Cryptanalysts
Sep 74 Secrets of the Altars--The Moustier Cryptograms
Oct 74 An October Overlap
Nov 74 Answer to An October Overlap
Aug 75 Twenty Years of Transposition

[redacted]
Oct 77 K1: SCA Field Management and Evaluation

[redacted]
Dec 81 Exercise Support

[redacted]
Aug 77 What Is an Information Research Analyst?

[redacted]
May 76 Waveguide Analysis

[redacted]
Feb 75 Puzzle: Can You Make Out the Name?
Apr 75 Answer to Can You Make Out the Name!

Engle T.L.
Jun 75 Puzzle: [redacted]
Apr 80 Help Wanted

[redacted]
May 82 Letter: Shell Game Article

EO 1.4.(c)
P.L. 86-36

[redacted]
Jun 77 SIGINT Welcomes INKSTAND

[redacted]
Aug 82 What Promotion Boards Want

Fairbanks S.
Mar 79 Fairbanks on English
Apr 79 More Fairbanks on English
May 79 More Fairbanks On English
Jun 79 How Are Your Stamina?
Jul 79 Wilt Thou, Angelina ...?

[redacted]
Nov 74 [redacted] What? Where? Why?

[redacted]
Apr 76 What's the Best Location for the Computer Applications Function?

EO 1.4.(c)
P.L. 86-36

[redacted]
Jan 81 How to Improve Your Promotion Potential

[redacted]
Nov 78 Letter: [redacted] Article

Filby P.W.
Dec 75 Weapon That Helped Defeat Nazis (Winterbotham's 'The ULTRA Secret')
Jan 78 'The Man Who Broke Purple' (Book Review)
Oct 78 Feeding the Germans Misinformation (Book Review)

Filby V.R.
Aug 74 A Spot by Any Other Name
Oct 74 The [redacted] Exercise: A Case Study in Special Research Analysis
Apr 75 Coverterms
Feb 76 How Do We Know It's True?
Mar 77 Revised Technical SIGINT Manual in Preparation
Feb 78 More Beans
Oct 78 Letter: NSA-Crostic
Jan 79 Reflections and Recommendations
Oct 79 Snowballs On The Roof
Mar 82 A Historian Looks at SIGINT

EO 1.4.(c)
P.L. 86-36

[redacted]
Apr 82 Personal Computer Application
May 82 The Micro Revolution: Arthur Young Study Comment

[redacted]
Aug 75 Typewriter Random -- A New Look
Nov 76 Teacher Learns a Lesson

[redacted]
Jan 80 Coming Home

[redacted]
Jan 76 Football and Cryptology
Nov 77 Letter: Salemme Article
Jun 79 Letter: Library Changes

[redacted]
May 82 Full or Broad Spectrum Lighting

[redacted]
Mar 77 More about the NSA SIGINT Summary

Gaddy D.W.
Apr 76 On Being Truthful
Aug 77 New Directions for the U.S. Intelligence Community
Nov 81 Say What You Mean

P.L. 86-36

P.L. 86-36

~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

[redacted]
Jan 78 Thanks for the Attaboy!
May 78 Uncle-a Sam Wantsa You!
Jan 79 Henry Cement and other Phantoms of the Opera(tions)
Feb 79 The COMINT Chain 'Gang'
Jun 79 The Story of MOSES

Garofalo C.A.
Sep 74 Gary's Colors
Feb 82 Golden Oldie: Simplicity in Color

Gerhard W.
Oct 75 One Chance in Three--But It Worked

[redacted]
Oct 76 More Thoughts on 'Questionable' SIGINT
Jan 77 Letter: 'Firebrand' Letter

[redacted]
Nov 82 Central Research and The Paper Blob

Gilbertson E.A.
Jun 78 Letter: [redacted] Article

[redacted]
Jul 78 Ye Gads! Another Country Trigraph System

[redacted]
Oct 75 NSA in Vietnam: Proud and Bitter Memories
Dec 77 CAA Message and News
Jun 82 Golden Oldie: Reporting Message Volumes

P.L. 86-36

[redacted]
Nov 78 Letter: Appraisal System

[redacted]
Dec 77 Letter: Pratt Article
Dec 82 [redacted]

EO 1.4.(c)
P.L. 86-36

Gould R.E.
Dec 75 Linguists From The Melting Pot
Apr 76 Golden Oldie: Hidden Losses in COMINT Production
Nov 82 The Costs of Muddling Through

[redacted]
May 77 A Story With a Moral
May 77 Letter: 'Horatius'
Sep 77 Is There a Doctor in the House?

Grant L.G.
Nov 75 In Praise of SOLITS
Dec 78 To Whom It May Concern

[redacted]
Nov 82 Letter: Shell Game Article

[redacted]
Apr 76 Letter: What Are We About? Article

P.L. 86-36

[redacted]
Aug 82 Linguist Machine

Gurin J.
Feb 75 Glossaries versus Dictionaries: Which Should It Be?
Mar 77 Letter: Keyword Spotting
Jul 77 Which Tape Has the Intelligence: Project [redacted]
Feb 78 The Unseen Go-Between
Jun 78 Never Again!
Jul 78 Letter: [redacted] Article
Oct 78 You Can't Tell the Wheat from the Chaff Without a Program
Feb 79 Let's Not Forget Our Cryptologic Mission
May 79 More Than Words Can Say
Dec 82 Going On-Line With Information Aids

[redacted]
Jun 75 Letter: Bookbreakers; Professionalization of Country Specialists

[redacted]
Oct 74 Character Building in the People's Republic of China

[redacted]
May 76 COMINT in the Russian Navy, WWII
Oct 76 Russian SIGINT and Electronic Warfare
Jun 77 Old Russian Manuscript Ciphers
Sep 78 Soviet COMINT and the Civil War

[redacted]
Jun 75 Letter: [redacted] Article
Dec 78 [redacted]

[redacted]
Dec 78 How Do You Spell Peking?

EO 1.4.(c)
P.L. 86-36

Hanyok R.J.
Jun 82 Some Reflections On The Reality of Computer Security

[redacted]
Jan 75 Puzzle: Crossed Codewords

Harrison M.A.
May 77 Why Are These People Smiling?

[redacted]
Jun 78 [redacted]

[redacted]
Dec 81 PLATFORM: How Did You Say That Works?

EO 1.4.(c)
EO 1.4.(d)

[redacted]
Sep 82 TSS Revolution

[redacted]
Feb 82 Letter: UNIX Article

[redacted]
Nov 77 Letter: Salemme Article

P.L. 86-36

[redacted]
Apr 81 Third Party Relationships

[redacted]
Dec 76 Apollo-Soyuz Test Project

[redacted]
Jun 82 Letter: Shell Game Article
Jun 82 Loooong Shell

Horn J.E., Nolte W.M.
Jan 78 An Early NSA Proposal for Satellite Remoting

[redacted]
Jan 80 System Acquisition Document Review

[redacted]
Nov 74 Data and Definitions: Calling Things by Their Rightful Names

[redacted]
Apr 78 SIGINT Exploitation, 1990

Hunt W.
May 76 About the NSA SIGINT Summary

[redacted]
Dec 75 Mum's Still the Word! ('The ULTRA Secret')

[redacted]
Jun 76 Comments on the AG-22/IATS
Jan 78 But Why Do We Do It?
Mar 78 A Donkey in Your WHAT?

[redacted]
Jul 79 Letter: [redacted] Article (Apr 79)

Inman B.R.
Nov 77 Director's Memorandum: [redacted] Guidance'

Irwin M.R.
May 75 Are We Wasting Linguistic Time?

[redacted]
Apr 78 Looking at Mr [redacted]

EO 1.4.(c)
P.L. 86-36

Jackson W.J.
Aug 74 TDB: The TEXTA Data Base
Dec 74 An Approach to Callsign Analysis

[redacted]
Oct 76 Letter: IRONHORSE Article

[redacted]
Jan 81 Why Do They Leave?

[redacted]
Nov 74 New Trends in the Teaching of Cryptanalysis
Dec 78 Some Tips on Getting Promoted
Aug 79 NSA Promotion Boards: How They Work

P.L. 86-36

Jenks P.
Aug 77 Let Me Repeat--And Make Myself Perfectly Clear

[redacted]
May 82 The NSA Information Desk: 'No Comment'

[redacted]
Mar 78 A Linguist Looks at the Tube

[redacted]
Dec 74 Flag-Waving Programmer

[redacted]
Dec 78 [redacted]
Jan 79 SOLIS: A Vehicle in Search of an Engine

[redacted]
Apr 81 Traffic Analysis: Specialty Without Portfolio

EO 1.4.(c)
P.L. 86-36

[redacted]
Jan 77 Letter: Mason Article

[redacted]
Oct 78 A Method for Measuring Negative Intelligence

[redacted]
Nov 74 Purity of the Russian Language--Slavophiles vs. Westernizers

[redacted]
Jul 79 Source Protection: Our Agency's Insurance Policy

P.L. 86-36

[redacted]
Sep 77 Speaking of Logging ...

Kenny M.M.
Jan 77 Letter: [redacted] Article
Jun 78 Minnie's Mini

[redacted]
May 75 Codeword or COMINT Channels?
Jul 77 Classification Corner
Sep 77 Classification Corner: XGDS-2
Sep 77 XGDS-2 (Classification Corner)
Oct 77 Classification Corner: Who Said?
Jan 79 It's Party Time!

[redacted]
Oct 76 Language Skill File

[redacted]
Sep 78 [redacted]

[redacted]
Nov 75 When Censorship Backfires
Jan 76 Lenin and State Prizes: Now You See Them, Now You Don't!
May 79 Chapenko, Shapenko: What Difference Does It Make?

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

DOCID: 4019691

P.L. 86-36

[redacted]
Aug 76 Initiatives in SIGINT Reporting

[redacted]
Dec 82 Development and Correlation of Indicators

[redacted]
Jul 78 Letter: [redacted] Article
Jan 80 Between The Lines of Your Performance Appraisal

[redacted]
Nov 74 Reflections on a Translator's Conference

[redacted]
Sep 78 A Matter of Style

Landi W.E.
Apr 77 Letter: Mason Article

[redacted]
Oct 78 Back to Square One!
Jan 81 Translator In Your Pocket

[redacted]
Nov 77 Language Processing Forum
Feb 82 Native Scripting of Languages

[redacted]
Apr 80 AIT

Lasley D.
Jul 79 Gears of the Mouth

[redacted]
Nov 77 Objective Satisfaction Score: Collection Performance

[redacted]
Jul 77 Letter: [redacted] Article

[redacted]
Dec 74 A Proposal for Calendar Reform

[redacted]
Jun 77 Letter: [redacted] Letter

[redacted]
Mar 82 But Life Is Supposed To Be Hard
Sep 82 More Free Goodies

[redacted]
Mar 79 Computer Operating System Vulnerabilities

[redacted]
Jan 75 The Yawn of the Computer Age or When Your Terminal is Terminal

[redacted]
Sep 76 Foreign Publications Procurement Program

P.L. 86-36

[redacted]
May 82 Letter: [redacted] Article

[redacted]
Nov 77 [redacted]

[redacted]
Oct 79 Another Source

EO 1.4.(c)
P.L. 86-36

[redacted]
Dec 81 TIDE: A Brief History

[redacted]
Sep 74 Golden Oldie: King Eusyb and Queen Deodi

[redacted]
Feb 82 A Time for Change

Lutwiniak W.
May 78 The Future of Cryptanalysis
Jan 79 Letter From the Publisher

Lutwiniak W., [redacted]
Jan 81 SIGINT In The 80s: Two Views

[redacted]
Sep 82 Letter: Kudos

[redacted]
Sep 76 Semantic Voids: Don't Shoot the Translator

Mason F.O.
May 75 TA, Handmaiden of CA
Jun 75 More on Squaring the Page (A Crypto-TA Function)
Aug 75 Abdul and His 40 Tanks
Oct 76 A Vexing Agency-Wide Problem
Nov 76 Answer to 'Vexing ... Problem'
Jan 77 Where Were We?
Apr 82 Golden Oldie: Tracks in the Sands of Time

[redacted]
Jun 75 Professionalizing in Computer Systems

[redacted]
Feb 75 Basic Patterns of [redacted] Codes and Ciphers

EO 1.4.(c)
P.L. 86-36

[redacted]
Apr 77 Letter: [redacted] Article

[redacted]
Mar 77 An Overview of Project [redacted]

[redacted]
Jan 78 'Bodyguard of Lies' (Book Review)

[redacted]
Oct 79 The 2000-Year-Old Transcriber
Apr 80 What To Do About 'FANX'

P.L. 86-36

[redacted]
Jun 76 Comments on the AG-22/IATS

McGrillies J.R.
Apr 77 Letter: Mason Article

[redacted]
Jul 77 Match Them Up!
Jul 77 Puzzle: Match Them Up!
Nov 77 How Many African Countries Can You Spot?
Apr 78 +Conoces Bien la Geografia?
Oct 78 Know Your Geography
Feb 79 Know Your Geography

[redacted]
Aug 75 Linguists -- We Need An 'Experts Yellow Pages'!

[redacted]
May 78 Callsigns and WARC-79
Jan 79 The Return to HF
Dec 81 The 1981 URSI XX General Assembly
Jan 82 HF - The Rebirth
Jan 82 Video Encryption: A Report From EASCON 81
Feb 82 Gayler-AAAS, 1982
Feb 82 Software - AAAS, 1982
Mar 82 Meteorburst Communications
Apr 82 Review: The American Magic
May 82 A History Lesson
Jun 82 Amateur Spread Spectrum
Aug 82 AFCEA 82 and ICC-82: New Crypto Devices
Sep 82 Normandy: 1944
Sep 82 SIGINT: 1990, Part One
Oct 82 SIGINT: 1990, Part Two
Nov 82 SIGINT: 1990, Part Three

Meyer W.P.
May 76 A Simple Cipher Story
Sep 76 Another Cipher by ...
Dec 78 a/k/a Sam
Aug 82 I Remember
Nov 82 An Old Timer Is One Who

P.L. 86-36

[redacted]
Feb 82 KRYPTOS: A New Society

Miller D.E.
Aug 75 The Voynich Manuscript-Third Theory
Nov 76 Golden Oldie: The Things They Say
Mar 78 An Idea for an Article
May 79 Transcriber-Analyst Relations

Miller K., Isaac L.
Apr 78 Looking at Mr. [redacted]

[redacted]
Feb 79 Literature Search On-Line

[redacted]
Sep 76 Is There Life After Certification?
Nov 76 Clarity, Thy Name is Qualifier
Feb 78 By-Lines Don't Cost--They Pay!

EO 1.4.(c)
P.L. 86-36

[redacted]
Oct 76 Language Skill File

[redacted]
Jul 79 Shootout at the SIGINT Corral

[redacted]
Apr 79 Letter: Gurin Article (Feb 79)

[redacted]
Dec 76 The French(fried) Connection: Gino the Genie

[redacted]
Jun 78 Celtic Languages Today

Mountjoy M.
Sep 74 Cryptanalysis and Code Recovery
Jan 79 Golden Oldie: On First Opening Kenney's 'Statistics'

[redacted]
Nov 76 TEXTA 'Word Seek'
Mar 78 Word Seek

[redacted]
Sep 76 TIPS is Still Alive and Well
Mar 79 Data Standards Without Tears: A Comment
Jan 82 Data Field Naming/Coding Conventions at NSA

Murphy A.I.
Jan 76 Leo in October
Jun 76 Letter: [redacted] Article
Jan 82 The Literary Bends
Mar 82 Letter: The Literary Bends Article

[redacted]
Jul 77 Tool Languages

EO 1.4.(c)
P.L. 86-36

Murphy T.
Oct 75 Automation of a TA Process
Jun 76 The [redacted] Collection System

[redacted]
May 75 Letter: [redacted] etter
Jan 77 What If the Linguists Disappeared?
Jun 78 [redacted]

[redacted]
Oct 75 Linguists -- You Have an Expert to Call!

[redacted]
Nov 78 Never on My Watch

EO 1.4.(c)
P.L. 86-36

[redacted]
Nov 77 A Proposed Cure for the Time-in-Grade Syndrome
Apr 78 Accentuate the Negative
Mar 79 Let's Not Lose Our TA Skills
Jan 80 There's a New World Coming - Are You Ready
Apr 81 Middle-Age Spread

P.L. 86-36

P.L. 86-36

[redacted]
Apr 77 Letter: [redacted] Article

Nolte W.M.
Mar 82 A Brief Treatise on Five Laws of Telephonic Communications
Mar 82 Old Phone Books Never Die

Nolte W.M., [redacted]
Jan 78 An Early NSA Proposal for Satellite Remoting

[redacted]
Jun 76 Comments on the AG-22/IATS

[redacted]
Oct 75 1972-1973: A Vietnam Odyssey

O'Neill K.
Mar 76 Letter: Proud and Bitter Memories Article

O'Sullivan P.A.
Jun 79 Letter: 'Sixth Language'

[redacted]
Mar 78 A Proposed Cure for the 'Performance Syndrome'

Oliver D.B.
Jan 75 The SIGINT Users' Handbook or: What's an ISHTAR?

[redacted]
Aug 79 On Coming of Age at NSA: Confessions of an Ex-Linguist

[redacted]
Oct 82 Golden Oldie: The Reality of Communications Changes

[redacted]
Jun 76 Comments on the AG-22/IATS
Feb 78 Collection-Support TA is Not for Everyone
Oct 78 Continuing Professionalization

[redacted]
Dec 82 Does Anybody Here Remember PURPLE?

[redacted]
Sep 77 The [redacted] Seminar Program

Pattie M.T.
May 76 What Language Problem?
Jun 78 As I Was Saying Two Years Ago ...
Oct 78 Letter: [redacted] Article
Nov 78 Data Standards Center
Feb 79 Letter [redacted] Article (Dec 78)
Feb 79 Well, Maybe a Sniffle or Two...
Jun 79 ... Mr. Pattie Replies

[redacted]
Jun 76 Comments on the AG-22/IATS

P.L. 86-36

[redacted]
May 79 Project HELIPAD: An Epitaph

[redacted]
Oct 82 What's The Good (Pass)Word?

Phillips C.J.
Mar 76 Musings About the AG-22/IATS
Mar 77 A View of the Central Computer Complex in the Late 1970s and Early 1980s
Apr 77 The Last Word on IATS?
May 77 Universes, Galaxies, Stars, Bars, and Other Concepts
Apr 80 Data Flow--Challenge of the 1980s

P.L. 86-3

[redacted]
Nov 82 COMSEC Challenges

EO 1.4.(c)
P.L. 86-36

[redacted]
Feb 75 The Faithful Echo--The Role of the State Department Interpreter

[redacted]
Mar 82 A Personal Computer: A Current Cryptanalysis Support Tool

[redacted]
Sep 77 [redacted]
May 82 Burst Answer

[redacted]
Apr 82 Partial Machine Translation: Final Report

P.L. 86-36

[redacted]
Jul 75 RAPIDTRAN: [redacted]
Oct 75 Language Lessons Learned: A Personal Memoir
Mar 77 Letter: Bunker Interview
Sep 78 What's In a Non-Name?

[redacted]
May 79 Run This Through Your Transcription Machine

EO 1.4.(c)
P.L. 86-36

[redacted]
Oct 74 Character Building in the People's Republic of China

[redacted]
Aug 76 Yes, Don, There is an ELINT!

[redacted]
Apr 75 A Comm Change at Ramasun Station

Reiskis A.
Jun 79 The Baltic Encoders

[redacted]
Sep 77 Another Last Word on IATS
Jan 81 KITTIWAKE
Jun 82 Letter: Editorial Comment
Jun 82 Letter: Shell Game Article

P.L. 86-36

P.L. 86-36

Nov 75 Golden Oldie: Blue Russian

Lutwiniak W.
Jan 81 SIGINT In The 80s: Two Views

Mar 78 Letter Article

Apr 80 P16 Language and Cryptologic Library

Jun 76 Comments on the AG-22/IATS

Dec 81 In Pursuit of: Faster Horses, Younger Women, Older Whiskey and More Money
Dec 82 Shell Game: AJSQUE

Sep 74 AFRIKAANS--Language in the News
Sep 74 AMERIND--Language in the News
Sep 74 HEBREW--Language in the News
Sep 74 Language in the News
Dec 74 Language in the News
Jan 75 The Case for COMINT Readers
Jul 75 Too Many Garbles
Dec 77
Oct 78 Puzzle: Who and Whom?
Jul 79 Letter: CRYPTOLOG Art
Mar 82
Oct 82 Not Secret Anymore

Santiago-Ortiz R.A.
Aug 74 The Language of Beisbol in Everyday Talk

EO 1.4.(c)
P.L. 86-36

Rosenblum H.E.
Oct 77 Partners in the Exciting Future of SIGINT

P.L. 86-36

Dec 76 Graphic Names

EO 1.4.(c)
P.L. 86-36

Mar 76 To Pull a 'Ponyal'

Feb 78

Salemme A.J.
May 76 Scraps from the Editor's Desk
Sep 76 Machine-Produced Aids for the Linguist, Part I
Oct 76 Machine-Produced Aids for the Linguist, Part II
Apr 77 Flash! 115th SRI Located!
Aug 77 Expletives Deleted?
Jul 78 I Remember SPELLMAN
Mar 79 NSA-Crostic No. 23
Apr 80 LIME-A, OHIO; LEEM-A, Peru

Dec 82 Shell Game: PWB WHEN

Jan 80 LIP

Santiago-Ortiz R.A.
Aug 77 Telling It Like It Is

Santiago-Ortiz R.A.,
Aug 74 The Language of Beisbol in Everyday Talk

EO 1.4.(c)
P.L. 86-36

Aug 74 Calling All SRAs! -- SRA Symposium

Sawyer E.L.
Nov 78 WEDDING BELLS and That Old Gang of Mine
Mar 79 Pursuit of the
Dec 81 Sleep Well: Your SDO Is On Duty

Feb 78

Jul 78 The Soviet General Staff

P.L. 86-36

Feb 78 First Lady of Navy Cryptology

Jun 76 An Evaluation of a Scientific Chinese Machine Translation
Oct 77 Classification Corner: A Bigger Picture
Nov 78 Formatting PL/1 Source Code
Jun 79 Teaching Computer Science To Linguists

May 77 The Polyhedral War

Jul 78 Has It Ever Been Translated Before?

Nov 75

EO 1.4.(c)
P.L. 86-36

Jan 79 T-Vision: The Reference Analyst's Medium of the Future

May 77 Plain English

Jul 77 Letter: Subscription

Oct 76 Letter: Article

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

DOCID: 4019691

[redacted] EO 1.4.(c)
Jul 79 Letter: Linguaprivia P.L. 86-36

[redacted]
Apr 76 Computer-Aided Transcription [redacted]

Smith F.
Mar 78 Some Background on the C/T Merger

[redacted]
Jun 76 'Right On, Vera!'

Snow D.
Sep 76 The Bible and the Washington Monument
Oct 77 Human Factors and the Use of Microfiche Readers at NSA
Oct 78 Reduction Ratios in Micrographics

[redacted]
Jan 80 CIRC: An Intelligence Data Base

[redacted]
Jun 82 Letter: Personal Computer Article

Snyder S.S.
Nov 77 Letter: [redacted] Article
Feb 82 A Wail, A Complaint, and a Melange

[redacted]
Jun 76 How Things Have Changed!

[redacted]
Apr 75 Letter: Exinterne Articles

[redacted]
Aug 79 Letter: Buckley and [redacted] (Jul 79)

[redacted]
Dec 77 [redacted]

[redacted]
Jun 76 Notes on Translation from the Chinese
Dec 76 What's In a Name?
Aug 77 Postscript to 'Dating Game'
Sep 77 JPRS Language Reference Aids
Nov 77 Backing into Language Acquisition
Jan 78 COMINT, COMSEC, and Hilbert's Tenth
Jul 78 Tell Me I'm Just a Sinobibliophobe

[redacted]
Dec 78 A VIP Tour through the Attic of NSOC

[redacted]
Mar 82 Towards Better System Development

[redacted]
Aug 79 Letter: [redacted] Letter (Aug 79)

[redacted]
Jun 77 Letter: Mason Article

[redacted]
Jun 79 [redacted]

[redacted]
Oct 75 1972-1973: A Vietnam Odyssey

[redacted]
Aug 82 An Old Problem

[redacted]
May 78 TA Implications of FCC Proposal

[redacted]
Jan 75 How Clean Does a Data Base Need to Be?
Jun 76 Comments on the AG-22/IATS
Jul 77 CAA News: What Ever Happened to the CAA?
Aug 77 CAA News: What Are They Up to Anyway?
Sep 77 CAA News: Whom?
Oct 77 CAA News
Nov 77 A Little TA Problem
Nov 77 CAA News
Jan 78 Letter: [redacted] Article
Jan 78 What Ever Happened to COPES?
Mar 78 The Hand Is Not Quicker Than the Eye
Apr 78 Telephone Problem Here
Sep 78 [redacted]
Nov 78 A Small Problem
Mar 79 Letter: Data Standards
Apr 79 A Somewhat Larger Problem
Jun 79 Traffic Analysis of the Future
Aug 79 CAA News
Aug 79 Letter: Screening Radiation
Apr 80 A Traffic Analyst Looks at Computers
Dec 81 TEXTA: What Is It? Where Is It Going?
Apr 82 Shell Game
May 82 True Base: Two Tales
Jun 82 A Personal Footnote
Aug 82 Shell Game
Oct 82 Answer: An Old Problem

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

[redacted]
Jun 77 Letter: [redacted] Article
May 79 Where Do Good Transcribers Come From?

[redacted]
Aug 75 Processing [redacted] Communications

[redacted]
Feb 75 Replacement of the GUPPY Library

EO 1.4.(c)
P.L. 86-36

[redacted]
Nov 81 The PPC Is Coming!

[redacted]
Oct 79 Letter: [redacted] Article (Aug 79)

Tetrault E.W.
Oct 74 Even a 5-year-old Child ...
Feb 75 Letter: Exinterne Articles
Apr 75 Language in the News
Apr 75 Machine Course for Linguists

P.L. 86-36

P.L. 86-36

Jun 75 Where Does 'Does' Come From?
Aug 76 Research in Speech Perception (Dr. Ruth Day)
Apr 77 Letter: [redacted] Letter
Feb 79 In Defense of The Indefensible: Notes on the Russian PQE

[redacted]
Nov 74 Guidesmanship--or How to Write Technical Manuals Without Actually Giving Anything Away
May 77 Choose Ye!
Jul 77 ZBB? What In the World Is That?
Oct 78 Will It Really Do the Job?

EO 1.4.(c)
P.L. 86-36

[redacted]
Oct 75 Computers, Comms, and Low-Grade Ciphers: [redacted]

[redacted]
Aug 75 A Fix for the Language Problem?

[redacted]
Oct 78 [redacted]

Tiltman J.H. EO 1.4.(c)
Dec 75 A Personal Comment on Winterbotham's 'The ULTRA Secret'

P.L. 86-36

[redacted]
Apr 80 [redacted]

EO 1.4.(c)
P.L. 86-36

Tinsley R.L.
Apr 78 ATA Letter to President Carter

Tiren D.J.
Mar 82 Letter: A Toy Problem

[redacted]
Jun 76 Transliteration or Cyrillic?

[redacted]
Feb 75 Review of 'Guide to Russian Technical Translation' by Salemme
May 76 A Soviet View of NSA

P.L. 86-36

[redacted]
Aug 79 Language Proficiency Certificates for Military Personnel

[redacted]
May 75 Letter: [redacted] Letter
Mar 77 [redacted]
Jul 77 Bookbreakers Forum
Jan 78 [redacted]
Jun 78 Bookbreakers Forum
Apr 80 ... And In A More Modern Vein
Apr 82 Bookbreakers Forum On Machine Aids

[redacted]
Aug 79 CMI News

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

[redacted]
Oct 78 Data Security and Human Error

[redacted]
Apr 75 Oral Reporting: A New Challenge for NSA

W.E.S.
Jan 78 CAA News
Feb 78 CAA News
Mar 78 CAA News
Apr 78 CAA News
May 78 CAA News
Jun 78 CAA News
Jul 78 CAA News
Sep 78 CAA News
Oct 78 CAA News
Nov 78 CAA News
Dec 82 Shell Game: Counter

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

[redacted]
Jan 75 UNNA, [redacted]

[redacted]
Jul 75 The Warsaw Pact [redacted]

[redacted]
Oct 82 Leadership: A Personal Philosophy

P.L. 86-3

Webster J.B.
Sep 74 Project CARRIAGE: Worldwide HFDF Modernization Plan

[redacted]
Jun 77 AG-22/IATS: A View From the Bridge

[redacted]
Oct 74 Letter: [redacted] Article
Dec 75 What Are We About? (Fragments, Figments, or What?)
Apr 76 Letter: Comments on [redacted] Letter
May 76 Some Principles of Cover and Deception
Apr 77 The 'Ice Age' and International Security
Sep 77 Whither the SRA?
Nov 78 Cast a Double Shadow: The Trojan Horse of SIGINT
Jul 79 Naval Readiness: A Basis for Comparison

Wigglesworth D.
Dec 77 Conversation With a Micrographics Pioneer

[redacted]
Jul 79 EXPERT

Wiley E.
Oct 75 The Do Xa Pads
Jan 82 Letter: Stairwell Society Article

P.L. 86-36

Williams D.H.
Dec 75 The Great Soviet Shipbuilding Mystery
Jul 77 Dating Game
Sep 77 NSA-Crostic No. 9
Jan 78 NSA-Crostic No. 11
Apr 78 NSA-Crostic No. 13
Jul 78 NSA-Crostic No. 16
Sep 78 Letter: Salemme Article
Oct 78 NSA-Crostic No. 18
Nov 78 NSA-Crostic No. 19
Dec 78 NSA-Crostic No. 20
Jan 79 NSA-Crostic No. 21
Feb 79 [redacted] and a Little Bit of Luck

EO 1.4.(c)
P.L. 86-36

[redacted]
Oct 81 Technical Support Catalogs

[redacted]
May 78 Project UTENSIL: The DDO Data Dictionary/Directory

Wolff H.E.
Aug 74 Cryptolog A Letter of Introduction

[redacted]
Aug 82 All I Ever Wanted To Know About DES

P.L. 86-36

[redacted]
Aug 74 Right-to-Left Text Sorts Are Not Impossible
Feb 75 Letter: Citizens of World Puzzle
Feb 79 P.S.

[redacted]
Nov 77 Language Processing Forum
Feb 82 Native Scripting of Languages

[redacted]
Jan 80 Analysts of NSA, Arise!

STUDENTS!

(U)

(U) On 29 November 1982 NCEUR announced its Independent Study Program as a way to facilitate the enrollment in and completion of National Cryptologic School (NCS) independent courses for cryptologic personnel in Germany. This is to cut the lag in mailing time between the NCS and sites in Germany. The NCEUR Training Office will also issue NCS Course Completion Certificates to individuals who satisfactorily complete an Independent study course obtained from NCEUR.

(U) Also available from NCEUR will be Russian and Czech videotapes to support language refresher and development training as well as videotapes on equipment maintenance, operations, collecions, management, security, etc.

[redacted]

[redacted]

(U) PAC-II is a project planning and control system developed by International Systems, Inc. PAC-II was designated the Agency standard automated project management system by memorandum DDPR/006/81 and is intended to help Agency project leaders with planning, scheduling, resource allocation, budget tracking, task assignment, over/under projections, etc. PAC-II allows inter-task dependencies and includes extensive facilities for playing "What if?" The system includes a 5-year scheduling capability and provides for tailoring the defaults to specific work schedules, holiday patterns, skill mixes, etc. More than 40 standard reports (Gantt charts, budget summaries, projected completions, etc.) are available. There is no Agency software development involved in PAC-II.

[redacted]

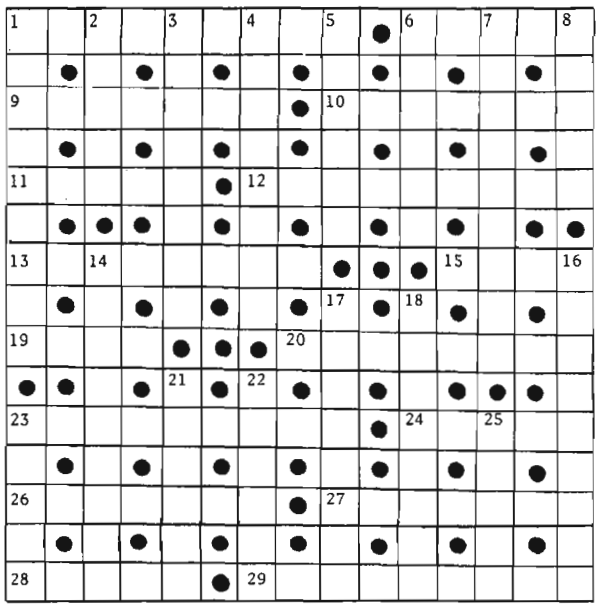
DOCID: 4019691

~~FOR OFFICIAL USE ONLY~~

CRYPTIC CROSSWORD #3

by [redacted]

P.L. 86-36



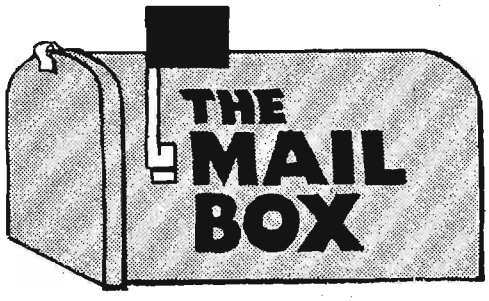
ACROSS

1. Smelly end of Tylenol production plant? (9)
6. Dad gets directions for the chess pieces (5)
9. Foul ram demolishes baby food! (7)
10. Little Miss Fabray eager for Chinese material! (7)
11. To sample a delicacy has inner appeal (5)
12. Dreamers' series of mental impressions (9)
13. I bounced wildly, then became frozen in place (8)
15. Frantic Omani prince shows lack of consciousness (4)
19. Cozy retreat for shooters (4)
20. We heard you teamed up with insane printer to be lewd (8)
23. Do some Irishmen nickname ships? (9)
24. In back, half dancer is comparatively more fastidious (5)
26. The obvious ten dive over! (7)
27. Loose ends trail behind! I am returning for young ladies! (7)
28. Finger that one! (5)
29. Traitors see danger all around! (9)

DOWN

1. Children averse to March, April and May? (9)
2. Counterfeit following valley (5)
3. Telephoned Reagan, we hear, to make pot (8)
4. Topless new developments bring forth applause and more applause! (8)
5. Roy is scuffling with Ned over there! (6)
6. It's pleasant without 80 mixed-up discussion groups (6)
7. We sent hot mixture to the grinder! (9)
8. Goes under the basins? (5)
14. Becoming more dignified, Neil G Motley captures backward German city (9)
16. Stars take chances on seat collapsing! (9)
17. Snacks center for the new students? (8)
18. Conveying the band into Crosby? (8)
21. The most sage is found in states beyond the Rockies (6)
22. The dog is in the Somerset terminal! (6)
23. Five hundred perused *A Great Anxiety* (5)
24. Doctrine of Celsius' grass (5)

~~FOR OFFICIAL USE ONLY~~

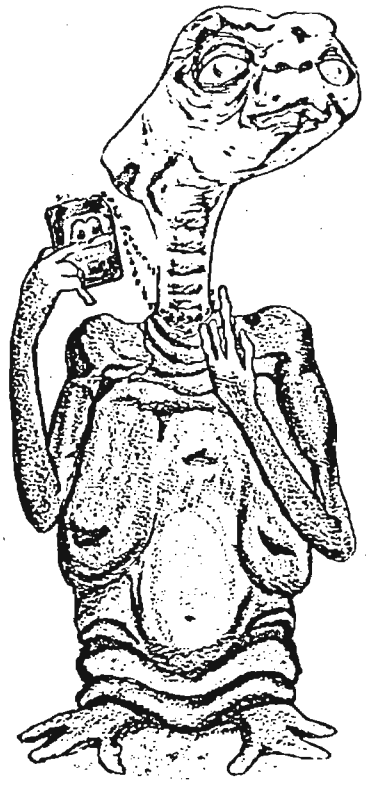


You may have thought that some of your coworkers behaved like beings from another planet, and there may very well be some extra-terrestrials among us! As a matter of fact, the new edition of the Agency telephone directory lists 25 ETs on the NSA payroll.

Of these 25 ETs, 22 are civilian (14 men, 8 women) and 3 are in the military (2 in the Army, 1 in the Navy). It should be pointed out that 23 of the 25 aren't really 100% ETs since they have middle initials and three of them have "Jr." tacked on to the end of their names, but there are two persons listed with pure "E.T." initials:

[redacted] P.L. 86-

However, [redacted] is on a field assignment, so [redacted] of Q4 is the only "real E.T." in the NSA Headquarters complex. That's quite an honor and we congratulate him. We just hope that now that this item is appearing in Cryptolog, he doesn't get a spate of notes on his desk saying, "E.T., phone home!"



[redacted]

Cheers,
[redacted] P14 (working in B111, x5741s)

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

SIGINT CHALLENGE

A SCENARIO (U)

EO 1.4.(c)
P.L. 86-36

by [redacted] W3

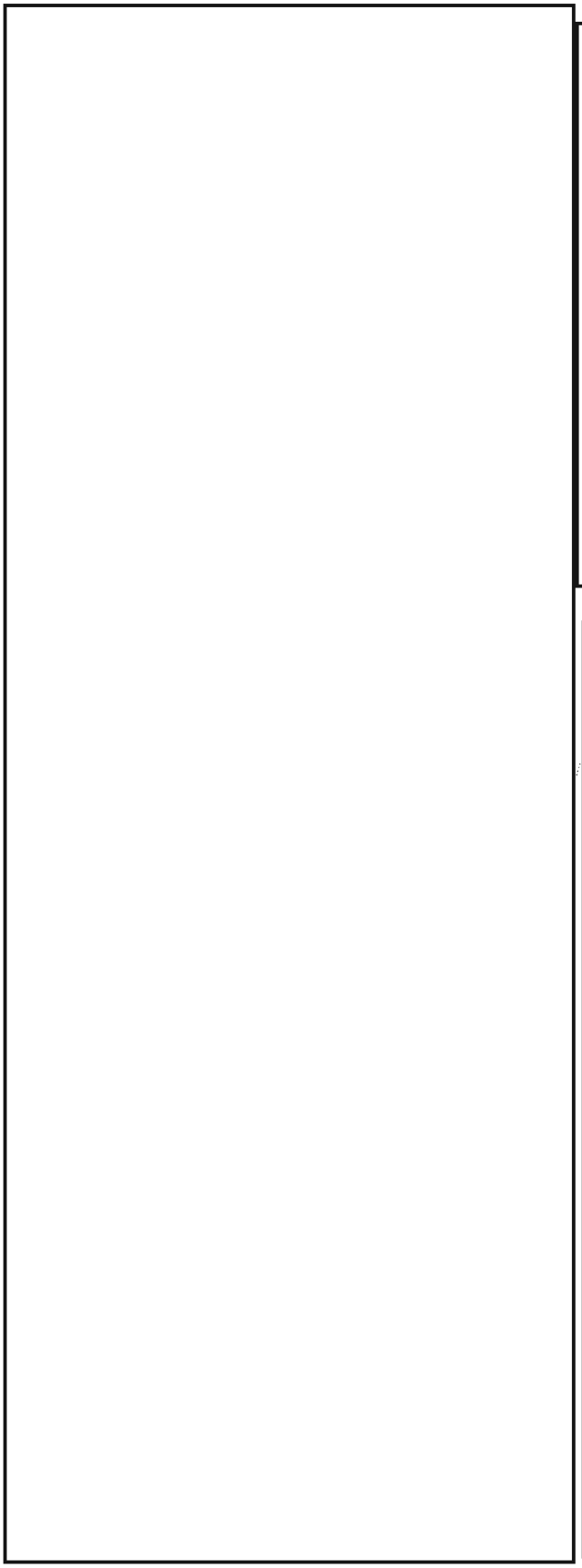
P.L. 86-36

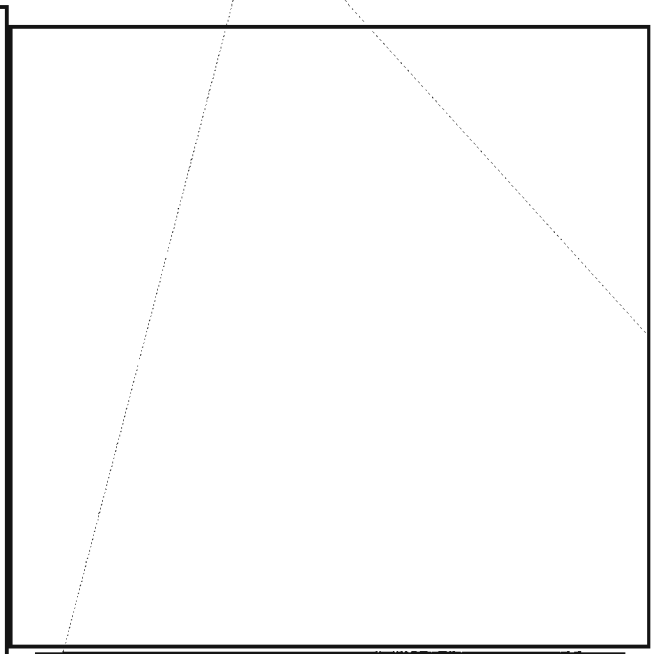
[redacted]

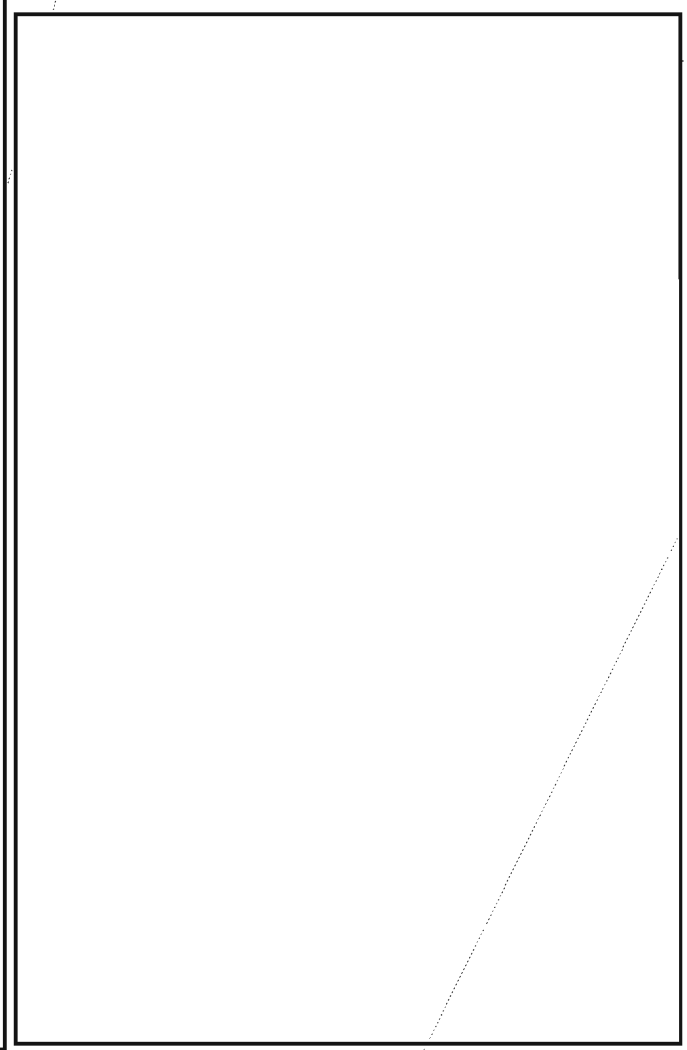
EO 1.4.(c)
P.L. 86-36

~~SECRET~~

EO 1.4.(c)
P.L. 86-36







EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4019691

MORE ON PASSWORDS (U)

by [redacted] P13 P.L. 86-

I have received a number of interesting responses to my comments on this topic in the December 1982 issue of CRYPTOLOG. It is apparent from the thoughtful and detailed comments of Computer Security professionals that they take this issue seriously, and see an urgent need to respond to user needs. But where are the spokesmen for the user side? The folks in Computer Security seem very ready for constructive user input, but they can't operate in a vacuum. Without ideas and, yes, maybe a bit of pressure from users, they will naturally continue to put efficiency and ease of implementation first, and who can blame them? Too many users tend to regard passwords and access restrictions as an act of God, kind of like a bad cold, that just happens to us and that we can't have anything to say about. Yes, we will always have to have some restrictions, but the WAY THEY ARE IMPLEMENTED AND IMPOSED can be influenced by informed and constructive user input.

We have a great variety of systems, and they make use of a number of different methods to protect files and programs from unauthorized access. As you can see in the contributions below from various readers, each applies only to certain limited cases. It seems as if we need to take a closer look at computer systems throughout the Agency and study the kinds of passwords, identity checks, physical access restrictions, etc. that they employ to preserve security, and look particularly at the impact each restriction or class of related restrictions has on the user. Maybe this has been done already; it would make a very good professionalization paper! If any reader knows of a study of this sort (a survey of all or some subset of file protection techniques, and their impact on users), please let me know. How many different sets of rules have we just for composing passwords, for example? I bet there are nearly as many different sets of rules as there are software systems (at least operating systems). How can we find out which of these burden users the least, while still providing the requisite security? Some of the comments below suggest specific changes in the form of passwords (e.g., the use of long phrases instead of single words). Unfortunately, we have no real way to decide whether these changes will, in fact, improve matters for users. Like so much else about human factors, this is an area where we need a lot more hard data. Intuitive guesses on the part of programmers are surprisingly often far off the mark when it comes to imagining what is easy or hard for end-users to do or remember, because programmers have had to (and have chosen to) develop a special cast of mind that sets them apart from non-programmers.

Let's hear from some more users out there! What do YOU think of these ideas the Computer Security people are proposing? Do you have some ideas or experience that can throw some more light on the subject?

HORROR STORY

"I loved your comments on passwords. I will pass along my horror story that resulted from [redacted] suggestions. Being a good, security conscious person, I promptly

P.L. 86-36

changed my password to one more complicated. It was a good one that would baffle any vicious attempt at penetration. All went well until the next time I tried to do some work at the terminal. It was late in the day, and I had to wake up the Delta Data. Every time I tried to login, it refused to recognize me: said my password was not correct and threatened Gestapo action (even called me 'naughty' - that made me mad). To abbreviate this long story, my PWB [Programmers Workbench] system will not accept passwords with numeric or special characters in 'load' mode. So, I went back to my comfortable, vulnerable old alpha style password. The system and I are friends again."

SOME THOUGHTS

"Use of computers may involve two distinct types of security problem:

"A. Protection from legitimate users of the system whose access to certain data is to be restricted.

"B. Protection from illegitimate users of the system who endeavor to gain access to certain data by the use of an identity (sign-on and password) that is not theirs.

"In the case of A, a procedure with which I am familiar calls for a system protection word to be associated with each created file. This word contains four units of four bits each. The four bits of a unit give Delete, Execute, Write, or Read privileges when zero; they deny the same when one. The four units relate to the system, the user (who created the file), the group (a limited number of users), and the world (all legitimate users who are not members of the user's group). In this way, control is maintained over who may do what with the data in any specific file.

"In the case B, to which your article mainly seems to address itself, it is pointed out that an increase of security in the sign-on and passwords procedure seems to require an equal increase in legitimate users' inconvenience. One simple change that would increase security but not inconvenience would be to eliminate the use of initials in sign-on procedures. An illegitimate user (or 'spook') who wanted access to your files would probably sign on as MDI with a good chance of success (at least on [one system]) and only then would have to consider some procedure for generating possible passwords via the computer itself. If the sign-on is ITSELF a password, the recovery of someone else's sign-on could not easily be done, as each sign-on trial would need to be typed in until the spook could find one accepted by the computer. Thus password first, then initials, would be more secure than the present initials plus password process; and password 1, then password 2 would be still better. Indeed, any one could make this change right now (if the system being used has no restrictions on the length of the sign-on or the password). But establishment of a specific policy excluding use of initials would be desirable.

P.L. 86-3

"A sufficiently clever systems programmer could, of course, dig out any information residing in the system, including protection bits and passwords, but measures against such a type of snooping will have to be taken up for discussion at another time. I am limiting myself for the present to the topic raised in your article."

P.L. 86-36 [redacted]

[This comment highlights two of the different points in the user dialog with a system where access restrictions come into play: i.e., 1) login, or sign-on; 2) file access. Additional possibilities are 3) access to data base management or other applications packages; 4) access to operating system or file system mechanisms (e.g., "superuser" passwords on UNIX systems); 5) access to related groups of files (e.g. M204 "file group" passwords). From a human factors point of view, the context within an on-going user dialog with the system is also important: how many steps has the user already had to go through before he must give this password? How complex have previous steps been? How many more steps must he go through, and how complex are they, before he can begin work? How often must he go through all the steps in a working day? How fast or slow is the system response between each step of his login and access to resources? It would be a mistake to look at a single "frame" of the dialog in isolation, and consider only the system's prompt for a password and the user's response, without looking at the surrounding context. -MED]

IT'S MORE FUN WITH PASSCODES
OR: SQUASHING/ENCOURAGING CREATIVITY

I enjoyed your article about passwords, and agree that creative passwords can SOMETIMES be so hard to remember that you have to write them down. Then you have less security than you WOULD have had with a more memorable password.

However, with a bit of creativity, (and a lot of inspiration from your article), I was able to conjure up a password that was at the same time memorable AND a scrambled mess of lowercase, uppercase, numbers and symbols. It was actually FUN to make a clever password!

Now I find that the cftp program (used to transfer data from one machine to another) will not function if a password contains either CAPITAL letters or punctuation marks. Not fun. Rather than remain frustrated, I picked a less clever password again. Isn't it bad psychology to squash a user's efforts like that?

We need to think about some programming standards here ... cftp can probably be modified to accept fancier passwords. For that matter, passwd (the UNIX program for setting a new password) can probably be modified to reject passwords that are all lower case (or all upper case), or to reject passwords that contain NO letters or symbols.

Finally, a weird idea that just MIGHT encourage creation of undecipherable passwords. Try this the next time someone knocks at your front door. Don't open it. Yell out "What's the password?" Chances are, your visitor will try common words ... "apple?","banana?","cranberry?". When your NEXT visitor arrives, cry out "What's the code?" Perk up your ears, 'cause he's going to try things like "murffle-87Z", "78rpm", and "DAH-di-DAH-dit". This should tell us something. Ask a person for a PASSWORD, and you get a WORD. Ask him for a CODE, for a PASSCODE, for an ACCESS CODE, and he stops to think of something unusual (and enjoys doing it). On UNIX, the word "password" would have to be replaced at login, and in the passwd program, and in a few other utilities.

[redacted] P.L. 86-36

UPDATE FROM [redacted] P.L. 86-3
HUMAN FACTORS OF PASSWORDS

"A SAD Dilemma.

"The recent remarks on Good (Pass)Words vs User Friendliness deserve some comment.

"The first full sentence on page 8 says that 'our lives are a lot easier if our password is 1) short, 2) easy to type, and 3) easy to remember". This order should be reversed. The password must be easy to remember. If you cannot remember it, you cannot type it, easily or otherwise.

"The comments about the difficulty of remembering VKJRD and like values are correct. Passwords made up of large alphabets are called for in situations where the password is limited in length. Short passwords are common in computer systems that store unencrypted passwords. If a password is to have any strength it must be of sufficient length or be made up of choices from a big alphabet.

"Currently, work on a new login for UNIX is underway. The specifications are:

"The password will be 8 or more characters; up to a maximum of 40 characters.

"Of all the characters, six or more will be unique.

"These specifications will permit pass phrases such as:

"Low flying bees eat wax beans

"I own cherry trees and crab grass

"If the user can accept using phrases, then sufficient strength can be obtained by using sufficient length for the pass phrases. This scheme does not increase the demand for computer storage if the pass phrase is encrypted and collapsed into 11 bytes regardless of length.

"The user's selection of the pass phrase will be inspected only at time of creating (when passwords are changed) to see that the password is 8 or more characters long with six unique. Because a user could choose abcdefg as a password or could switch back to a previously used password, the old password will be captured. The security officer will review captured passwords to see if a user needs counseling on password choices.

"The central distribution of passwords that are difficult or impossible to pronounce or remember is unacceptable. I agree that the pass phrase should be as usable as possible consistent with the need for protection.

"There is a human factors element to a well designed and properly functioning password system which deserves some comment. The password authenticates the user to the system. It prevents anyone else from masquerading as the user. It protects the work of the user from damage. It prevents anonymous use of the computer. This encourages all users to be responsible citizens in the community of computer use.

"There are alternatives to passwords, but they are worse. Each individual has a unique pattern of blood vessels on the retina visible through the lens of the eye. The pattern could be used as an identifier. But how could the identifier be forwarded over the telephone to a trusted fellow employee? Emergencies do arise.

"If a password is remembered, it is easy to type. I doubt that a non-typist will use a terminal very long. As for passwords should be short; sorry about that, they must be long enough to be secure."

[redacted] (29 December 1982) P.L. 86-36

A RESPONSE FROM THE COMPUTER SECURITY CENTER

GOOD (PASS)WORDS VS HUMAN FRIENDLINESS

"1. Reference your article.

"2. As a regular user of computing systems I share your concern that password systems be user friendly. Wearing my other hat, as Chief of Standards and Commercial Products Evaluation at the DoD Computer Security Evaluation Center, I am quite concerned that passwords be chosen and used in as secure a fashion as possible.

"3. An approach to the dilemma between user friendly passwords and secure passwords is to

P.L. 86-36

stop focusing on the word WORD in PassWORD. There is no real reason why the authentication sequence for a computer log-on could not be a PHRASE - one typed in lower case letters with embedded blanks (if one chooses). This suggestion opens new realms for passphrases which are easy to remember, easy to type, plus long enough to be not practically attackable by simple analysis means. Any source of written material at hand provides candidate passphrases which are far more secure than one's initials, name spelled backwards, license plate number, radio amateur callsign, wife's name, project name, etc. which appear frequently in the set of user chosen passwords in use today. Phrases like 'ordered bifocal glasses', 'simple analysis effort' or 'do we need to depend' all suggest themselves as passphrases from your recent Technical Notes. Real security in passphrases (or passwords) comes from being chosen at random from a large set of possibilities. The phrases such as 'including the electrons', 'larger than a gimlet', 'around which cable' or 'outspoken plain and blunt' were all drawn from the dictionary on my desk.

"4. We who work in computer security realize that the user of the system is the real key to system security. The user's needs must be taken into account when security measures are devised and put into place. There is real room for creative thinking in the area of meeting users' needs and maintaining and improving computer system security. Let's break out of the past shallow thinking (use passphrases instead of passwords) and apply our talents to making things better for everyone."

[redacted] (4 January 1983)

MORE ABOUT PASSWORDS AND...HUMAN FACTORS?

"We have a rebuttal! [redacted] has published a rebuttal to an article about the password compromise that appeared in the October issue of CRYPTOLOG. It seems that Mary thinks that passwords that are: long, use upper and lower case, are selected from a large alphabet, (special characters, punctuation, etc.) are a pain in the human factors... neck? Mary's point of view is that passwords are just one more obstacle between the user and the computer. Mary states that life is a lot easier if our passwords are: 1) short; 2) easy to type; and 3) easy to remember. Hmmmm..seems to be a conflict of interest here. There is no question that we must use passwords that are reasonably secure. Admittedly, however, we cannot ignore the human factors issues while pursuing this goal."

[redacted]

(Excerpted from COMPSECNEWS, January 1983)

CENTRALLY-ASSIGNED PASSWORDS

"Some years ago I identified what I consider a near-perfect trade-off between security and convenience with respect to the assignment of passwords. At that time the CESSO was assigning new passwords to the users of their facility. The principal mechanism was a program which could effortlessly generate 8-character alphanumeric passwords in an approved fashion. The CESSO's plan was to run off a sheet of several hundred passwords, and then arbitrarily assign one to each customer.

"Noting that the password assigned to me was onerous, I asked for a sheet of 1000 passwords from which I could choose a better one. While the CESSO acceded to my wishes for myself and my team members, there was unwillingness to make this a standard practice. There were a number of objections, most of which I could not appreciate, one being that it would be wasteful to run off 1000 passwords and 'waste' 999.

"Nevertheless, each of us found within our own list of 1000 potential passwords some string that was 'personally memorable' and did not need jotting down--despite being random and, for all intents and purposes, meaningless.

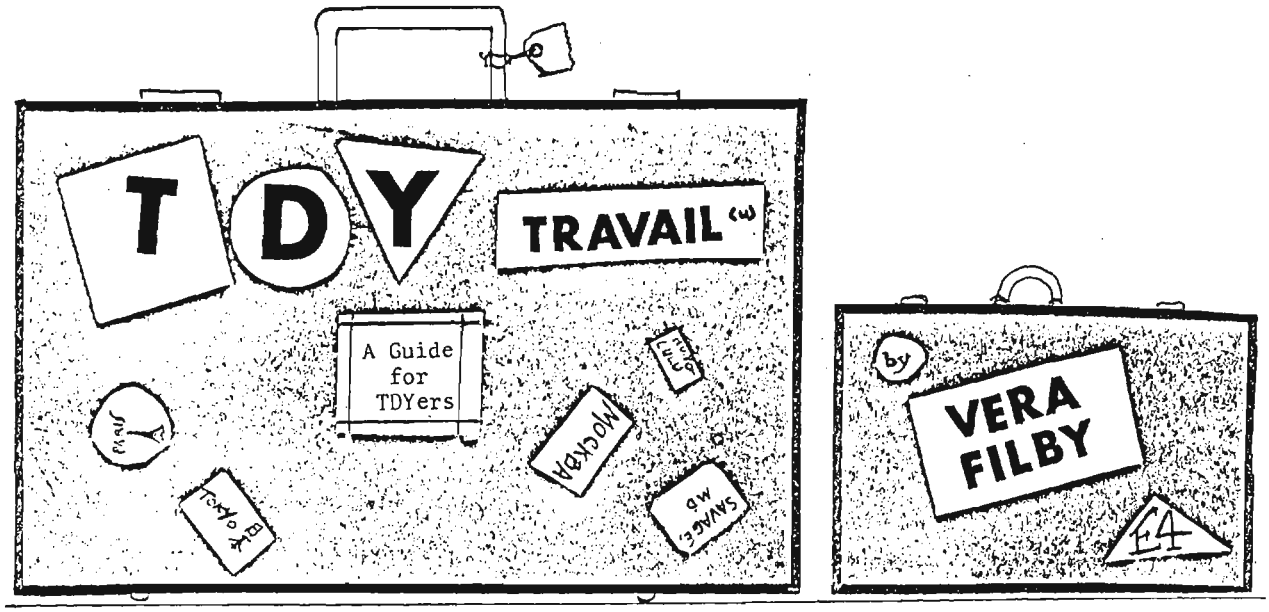
"Passwords are a fact of life, but their burden can be lightened significantly without compromising security.

"My experience--and I suspect yours as well--has taught me that the cost and complexity of user convenience is often less than it first appears; the payoff, whether large or small, is often longlasting."

[redacted] (9 February 1983)

P.L. 86-36

DOCID: 4019691



If you have not traveled on TDY (Temporary DutY) lately, or if you are now contemplating your first TDY assignment, there are many facts that you should know and actions that you should take. Knowing what to do and doing it in time can prevent unpleasant surprises, hassles, snafus, and disappointments. The key factors are time and your personal attention. Do not assume that "Admin" or "Management"--or somebody--will handle everything in good time while you just wait to be told what to do. You may have to do it yourself. Here are things you should know.

Rules and Regulations

You probably have better things to do with your TDY preparation time than to study TDY rules and regulations, but you should know that you can find them in the Personnel Management Manual, NSA/CSSPMM Part VII--Series 700 (Travel Regulations). For general assistance, your key component has a central travel activity, and the Travel Management and Support Branch (M62) will answer all your travel questions. Ask them.

Travel Arrangements

Nothing can happen before M62 receives a copy of your planning message. This is a message prepared according to a prearranged format by your home element announcing your itinerary, schedule, mission, and clearances to the commands and installations you will be visiting. M62 needs at least 30 days, and preferably 45, to do its part; the field activity you are visiting may need as long as 30 days for the paperwork in preparing for your visit. M62 will select the best bookings within the range of allowable options, including, when available, Category Z, which is a class of services quoted by certain airlines for government use. If you have complications, such as traveling with your spouse or taking annual leave in conjunction with TDY, discuss this with your M62 representative so that she can make the most favorable arrangements and suggest how best to take advantage of whatever airline bargain gimmicks may be in force at the time.

Advance Preparations for Arrival

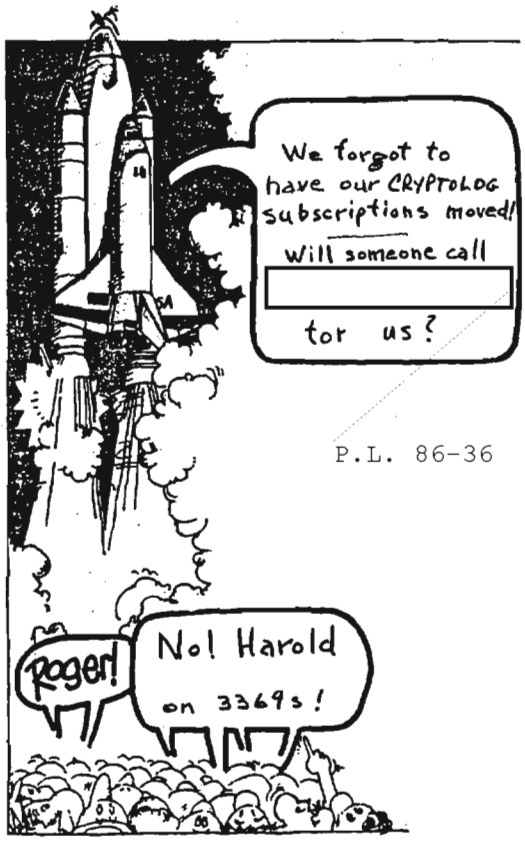
If you are sending equipment, briefing notes, or anything else you will need when you get there, make sure you allow enough time. Check the Armed Forces Courier System (ARFCOS) schedules. Make sure you get back the Receipt for Transmittal, Form A1295, which is attached to packages for shipment.

Keep handy the names and telephone numbers (home and office) of your points of contact. If you are to be met, be sure that your time and place of arrival are known. Messages don't always get through, so make some contact yourself (OPSCOMM, phone call, letter--whatever you can). You may find yourself alone in a foreign country where you don't

speak the language, with a pile of luggage to look after. You must be ready to cope with a situation like this. If you are not to be met, then be sure you know how to get from the airport to your destination, which may be many miles away. What modes of transport are available? Taxi? Limousine? Bus? Train? Some combination of these? If you are arriving at night or on a Sunday, are they running then?

Passport

Probably you already have a passport. This is not good enough. You need an official passport because you will be traveling on government orders. Go to M624 and apply for it as soon as possible. Your passport number should be included in your TDY planning message or a later message. This will assist you in on-base processing at locations where responsibility for security is shared by the United States and the host country. When you return, your official passport will be taken away from you and filed for possible future use. Even though it is not in your possession, don't let your passport lapse.



P.L. 86-36

Shots

For some destinations, shots come in series, so find out how much lead time you will need to have them--and to recover from having them, if shots bother you. You don't want to go chasing around airports with a sore arm. Depending on where you are going, you might assume that you don't need shots--and you might be wrong! You will be traveling on an official passport and additional rules apply. The Medical Center, M7, will know the answers and give you the proper shots.

Travelers' Checks

Buy your travelers checks in good time to avoid being rushed at the last minute. There may be restrictions, depending on where you are going. Ask your travel representative.

Money

When you finally pick up your orders--and this can happen at a panic-stricken last minute!--you will be presented with a large sum of cash. This is your travel advance. This could happen on a holiday, Saturday, or Sunday or in the evening, when you would have no way of safely stashing it in the bank. Be prepared to deal with this possibility in whatever way suits you best. You may have it held for you if you wish.

When you change money from one currency to another, note the exchange rate and copy it down. Rates change from day to day. Be sure to have small change in the foreign currency with you when you arrive. You may need it for tips, snacks, telephone calls, or toilets.

Accommodations

Will you be staying at a hotel? In the BOQ? In base housing? Will transportation be available, or will you have to get to your destination from a distant hotel every day in a hired car? Ask. You need to know. If you know you will be driving a rental car in a foreign country, determine in advance what the restrictions are. You may need a local or international driver's license ($10.00 at AAA offices). And be sure you know which car rental company holds your booking.

Records

When you leave, you will receive your tickets, travel orders (Form DD1610) in multiple copies, and travel voucher (Form DD1351-2) with carbon copies. An examination of the travel voucher form will convince you that you will need to keep records of all your expenses. Do this as you go along. You will have enough to do when traveling just to keep track of today, never mind trying to remember which meals you paid for or what taxi rides you took yesterday.

If you cannot get quarters on a military base, make sure that you get a statement of nonavailability from the base billeting office. Without it, you may have to pay for off-base quarters yourself. Be careful not to lose any tickets, bills, or receipts. If you get a chance, have them copied and send the copies home. When you get back, you will have to turn in your completed forms with all your documentation.

Security Briefing.

For overseas travel you will need a briefing on security. Find out when these briefings are scheduled well enough in advance so that you can attend on a day convenient for you. You will be busy in the days just before you leave, so do what you can ahead of time.

Travelers' Guides

The State Department, the US Customs Service, and other organizations publish brochures and pamphlets with tips for travelers. When you pick these up, take a look at the publication dates. Rules change. Make sure that the advice you are getting is current.

Trip Report

When you get back, you will probably be expected to write a trip report. Find out in advance the type and amount of detail that will be wanted so that you can be thinking about it and making notes.

The Assignment

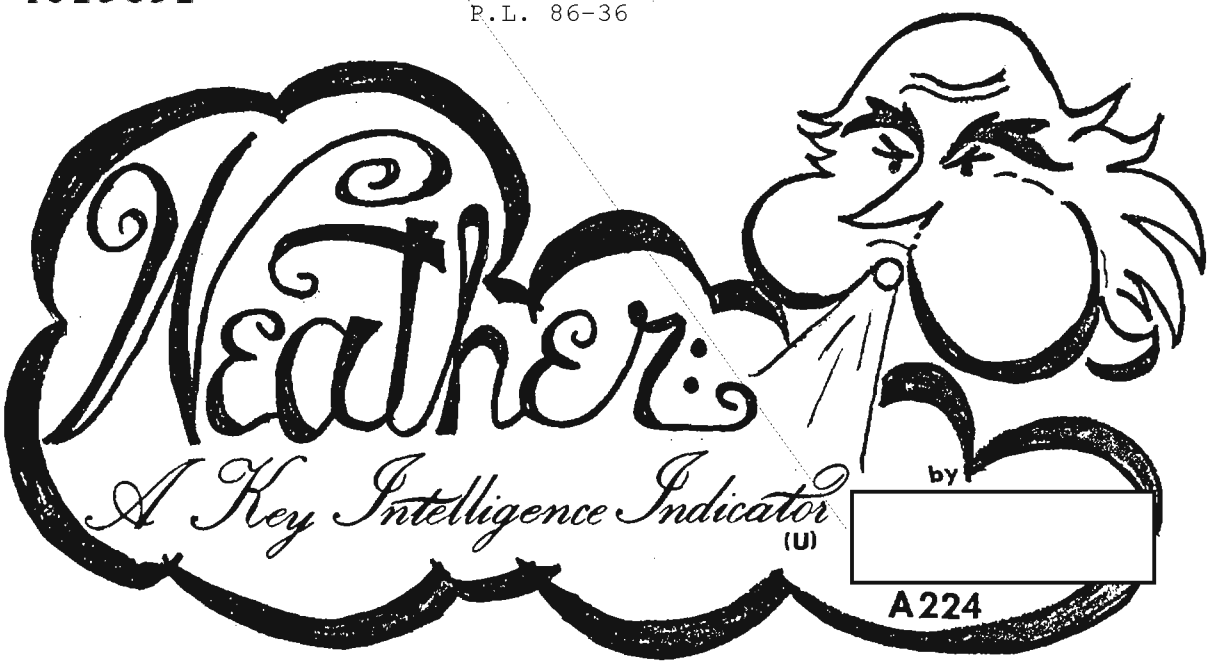
Now with all the preliminaries disposed of, you're off. You will almost certainly find your TDY interesting and rewarding, well worth all the initial (and subsequent) bother, which, with a lot of attention and a little luck, can be held to a tolerable minimum.

Have a good trip!

Author's note: My thanks to [redacted] of M62 for her advice as well as to friends in P1 and my E41 colleagues [redacted] for their suggestions. Brian has a last word: "Take a good book and maintain your sense of humor.")

P.L. 86-36

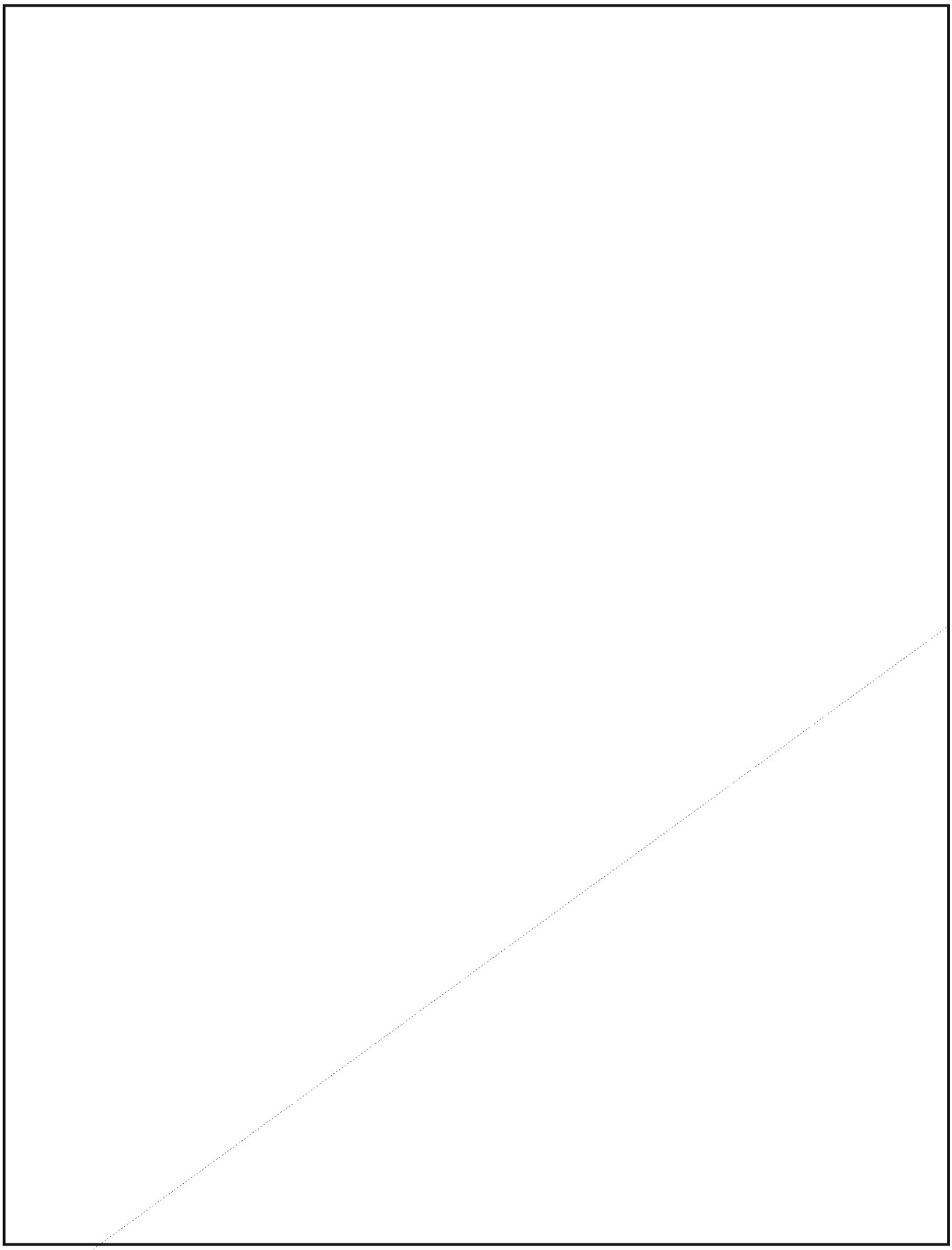
DOCID: 4019691



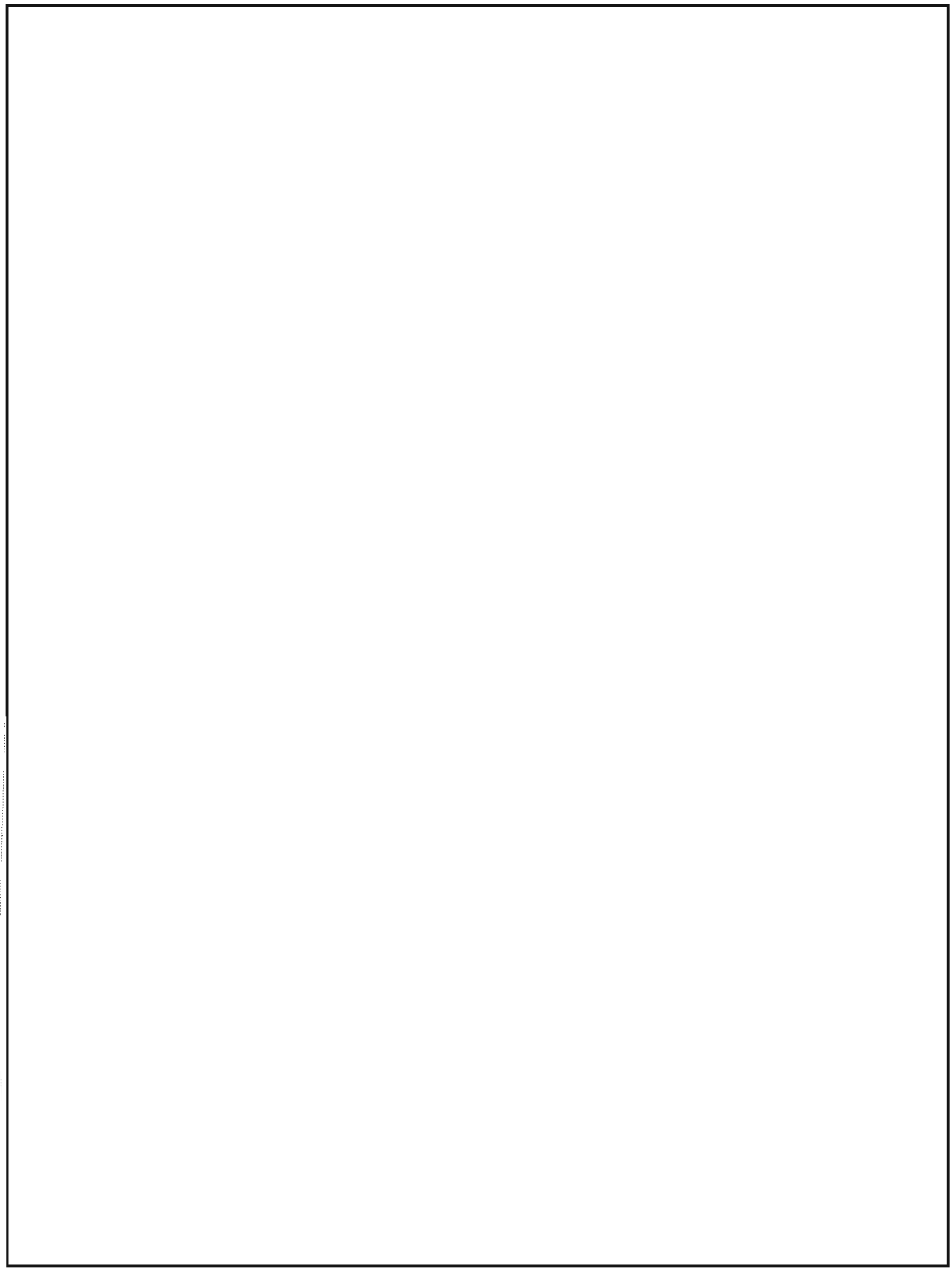
We have all heard the old saying, "Everyone talks about the weather, but no one does anything about it." Yet, hardly a day goes by that each ~~(S)~~ of us does not watch or listen to a weather report on television or radio. Regardless of whether or not we believe the forecast, we all tend to make plans accordingly. Just as weather forecasts tend to influence our personal activities, so the same types of weather information influence military commanders in planning their operations. This dependence on weather support by the armed services can yield unexpected intelligence information and, indeed, is used daily by Agency weather analysts

~~(S)~~ The progress of scientific knowledge and modern technology continues to call attention to the critical need for all-source environmental information from potential enemy nations. This data is required to more accurately assess a nation's success in developing, deploying, and operating new weapons systems and to study the influence of a nation's weather on the capabilities, disposition, and mobility of friendly or unfriendly military forces.

EO 1.4.(c)
P.L. 86-36

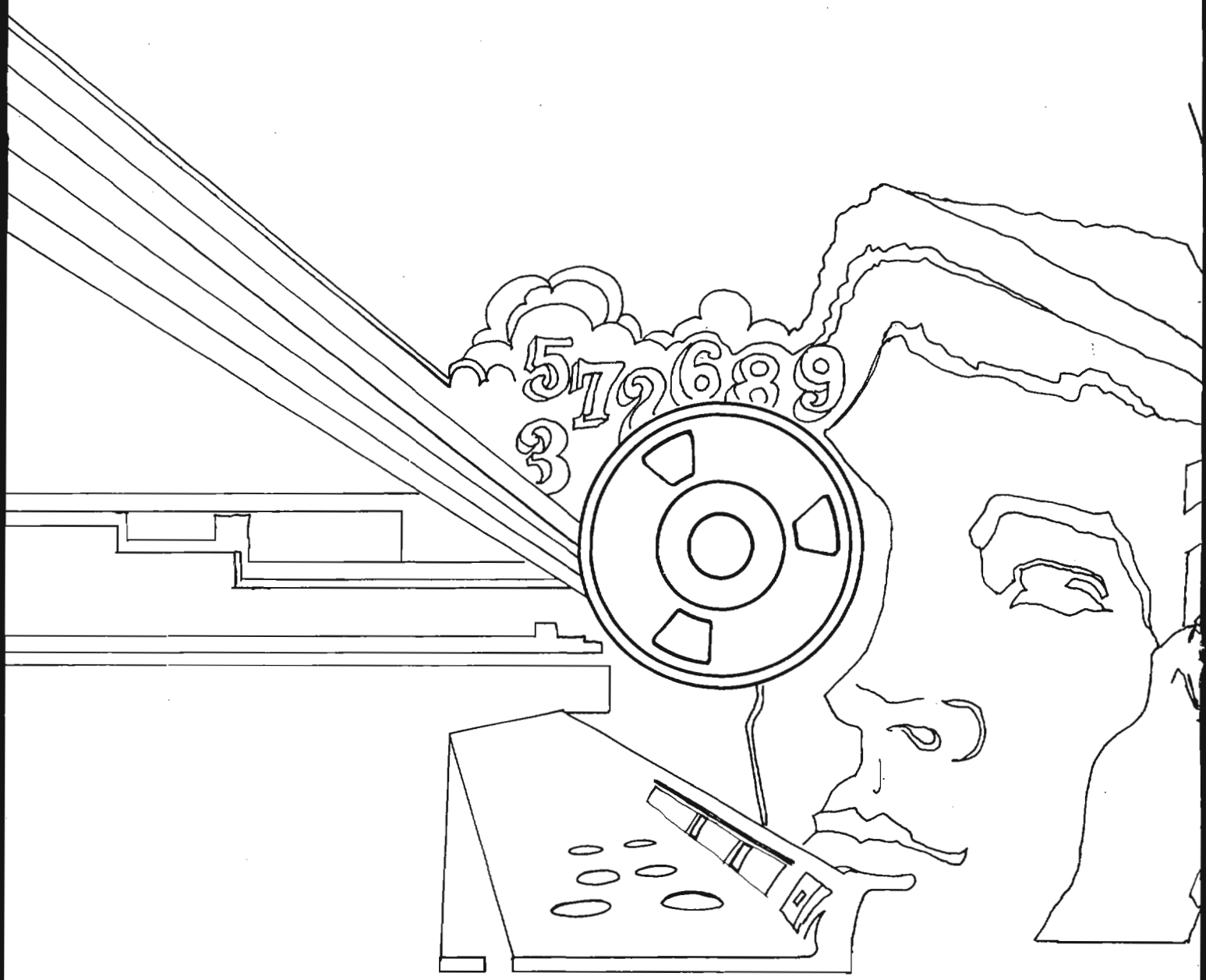


EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

P1-Jul 83-S3-30845


5 7 7 6 8 9
3

DOCID: 4011963

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

January - February 1983

Revd 13 OCT 83

SPECIAL ISSUE

CISI ESSAY CONTEST [U]

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4011963

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. X, No. 1 JANUARY 1983

PUBLISHER [redacted]

BOARD OF EDITORS

Editor..... [redacted] (968-8322s)
Asst. Editor... [redacted] (963-1103s)
Production..... [redacted] (963-3369s)

Collection..... [redacted] (963-3961s)
Cryptanalysis..... [redacted] (963-5311s)
Cryptolinguistics. [redacted] (963-1103s)
Information Science
..... [redacted] (963-5711s)
Language..... [redacted] (968-8716s)
Machine Support [redacted] (963-4681s)
Mathematics..... [redacted] (968-8518s)
Puzzles.....David H. Williams (963-1103s)
Special Research.....Vera R. Filby (968-7119s)
Traffic Analysis.....Don Taurone (963-3573s)

For subscriptions
send name and organization

to: CRYPTOLOG, P1
or call [redacted]3369s

P.L. 86-36

To submit articles or letters
via PLATFORM mail, send to

cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no 'O' in 'log')

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

"Something different" is what we promised for this issue and this is, for CRYPTOLOG, something different--an entire issue devoted to one general field.

Opinions will differ about whether a publication, even a relatively informal one such as this is, should always have "something for everyone." On one level, this question sometimes crops up in the form of "should we have lots of short articles on a variety of subjects, or should we run fewer but longer articles?"

Pragmatically, our approach to the question involves looking at just what articles and items come in for publication. We don't do a lot of recruiting of material for the magazine. The board of editors does some, but they are all busy people and working for the magazine is a sideline for them. Then, we try to keep up with what people are doing and what their current interests are. This means, among other things, that more articles about computers are showing up in these pages at the same time that a general resurgence of interest in computers is evident, both inside and outside the agency. That doesn't mean we aren't still interested in other topics, but it probably means that we aren't getting many submissions about other topics. Art Salemme used to respond to, "Why aren't there more articles about my field?" with "Why don't you write one?" That's a good thought.

Finally, and perhaps most important to us, there is a clear need to develop the expository skills around this place. Those who are particularly good at certain skills have to find a way to tell others about what they know and do. This takes practice, and practice requires a place to publish. CRYPTOLOG is one such place.

ID: 4011963

1982 CISI Essay Awards

In 1982, CISI began an annual CISI Essay Awards competition. The purpose of this competition is to encourage NSA employees to share their expertise and experience in computer and information sciences with the NSA community. The papers submitted were judged in the following three categories:

- Hardware and Software Systems
- Applications, Information Systems, Computing Milieux
- Methodologies and Theory

Each category was refereed and judged separately and monetary prizes of $100 for first place and $75 for second place were awarded in each category. The general criteria for judging were:

- relevance to the fields of computer and information science
- writing style
- organization
- significance to NSA

P.L. 86-36

Two first prizes were awarded, one to [redacted] of L091 for her paper "The Future Brightens for Flat-Panel Displays" and one to [redacted] of E53 for her paper "Menu Selection as a Tool for Human/Machine Interaction."

P.L. 86-36

Three second prizes were awarded. They went to [redacted] of R532 for her paper "Improving Raster Graphics Images by Anti- Aliasing," to [redacted] of T333 for his paper "Managing Our Systems for Performance," and to [redacted] of B62 for her paper "A Tutorial on Color Theory and Human Color Perception the Color Graphics Programmer."

CISI would like to thank the following judges for their time and effort in judging the fifteen papers that were submitted:

[redacted]

[redacted]

[redacted]
CISI Member-at-Large

P.L. 86-36

DOCID: 4011963

Special Issue: CISI Essay Contest

TABLE OF CONTENTS

P.L. 86-36

The Future Brightens for Flat-Panel Displays (U)		3
Improving Raster Graphics Images by Anti-Aliasing (U)		19
Current Local Area Network Status (U)		37
Logic Design Exceeding Boolean Capabilities (U)		42
Ada: Conquering the Tower of Babel (U)		49
Managing Our Systems for Performance (U)		55
Getting Personal (U)		71
Menu Selection as a Tool for Human/Machine Interaction (U)		75
A Tutorial on Color Theory and Human Color Perception for the Color Graphics Programmer (U)		86
Computer Graphics to Enhance Collection Management (U)		95
The NSA High-Level Display File (U)		114
A Survey of Parallel Sorting (U)		133
ADA News (U)		155
Puzzle (U)	D.H.W.	156

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011963

The Future Brightens for FLAT-PANEL Displays (U)

P.L. 86-36

by [redacted]
T Intern

INTRODUCTION

In the United States, more than two million cathode-ray tubes (CRTs) are installed and, despite the recession, market demands continue to grow.[2] Surveys conducted by Booz Allen and others suggest that by 1990, one-quarter of the white-collar clerical and professional employees in the US will have display terminals on their desks.[3] What is important to note is that many of these terminals will not be the traditional CRTs of the past.

> "There's one feature that a CRT cannot have, and the lack of that feature makes it awkward in certain applications...a CRT cannot be flat."[1] Larry Tannas

The major challenge to the cathode-ray tube is coming from flat-panel displays. Although the CRT has been relatively well accepted for many years, numerous limitations have made it a prey for competing technologies. This has encouraged a strong and rapidly expanding interest in the development and production of flat-panel displays, one of the most viable alternatives in overcoming the many disadvantages inherent to the CRT.

This paper will pursue a thorough examination of flat-panel display technology. The first area of investigation includes a detailed explanation of CRT and flat-panel display technology. We will then proceed to take a close look at four major flat-panel displays currently being either researched or developed, to include a discussion of their physical design, operating characteristics, strengths, and weaknesses. The third area will cite the major advantages and disadvantages of CRTs and flat-panel displays. Fourthly, we will briefly summarize some of the current research in flat-panel technology. The final area will examine the present and future markets for flat-panel displays.

CREATING THE DISPLAY IMAGE

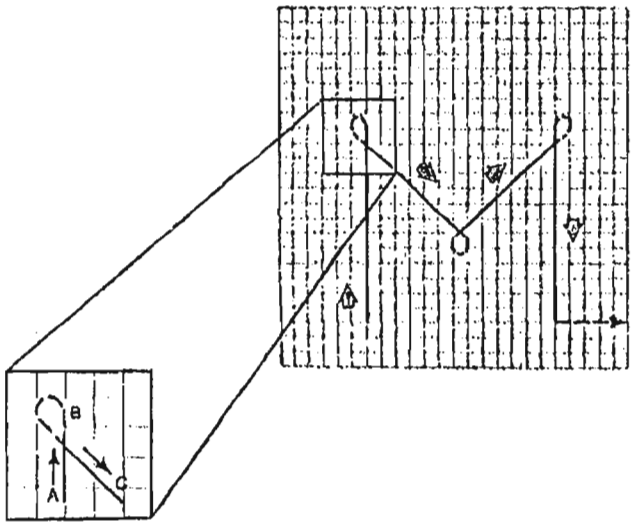
Displays may be classified according to a number of attributes, a significant one being their screen addressing technique. This section of the paper will discuss the methods that both the CRT and flat-panel devices employ to create a display image.

The CRT uses beam addressing, a process which utilizes a deflected focused beam of electrons to trace the display image on the screen. In CRTs, this can be accomplished in generally two ways (Figure I). First, in both calligraphic and direct-view storage displays, the beam is deflected in a random motion across the phosphor-coated tube to create the display image, somewhat analogous to "painting" the image on the screen.[4] In this manner, the electron beam may be deflected in any sequence given by the computer. Raster displays employ a second method, applying a fixed deflection system which forces the electron beam to scan the CRT in a definite sequence, usually from left to right and from top to bottom. As the electron beam is

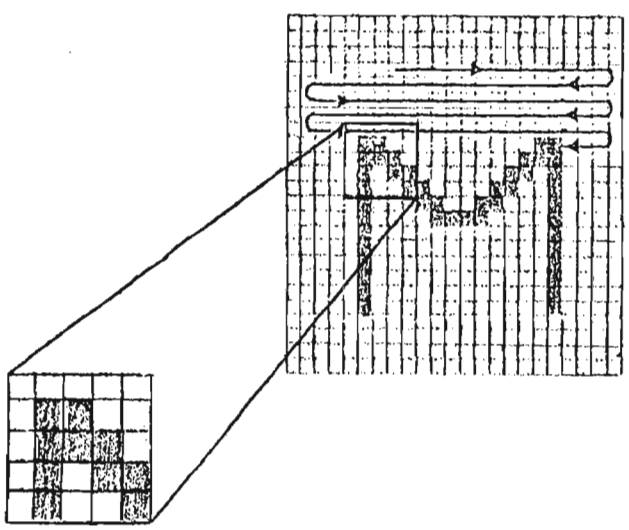
~~FOR OFFICIAL USE ONLY~~

OCID: 4011963

FIGURE I
Display Image Creation



In calligraphic and storage tube displays, vectors are drawn with "strokes" of the beam on the display surface.

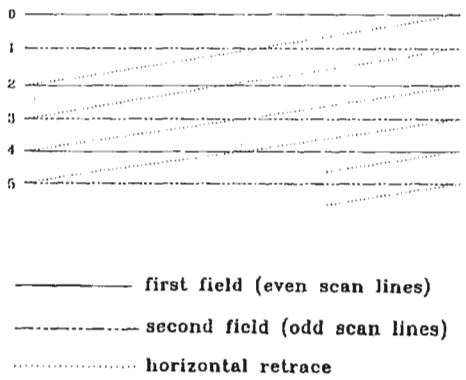


On raster systems, vectors are displayed by turning pixels on and off as the beam moves back and forth down the display surface.

---

deflected line by line, the beam current may be adjusted to cause variations in brightness along the lines. In television applications, this raster-scanning technique usually applies a method called interlace, which produces a more random scan sequence.[5] The effect of interlace is to create the display image as two separate fields, the first field containing the even-numbered scan lines and the second field containing the odd-numbered scan lines. Figure II illustrates the interlace process. This works well with television images, since the pictures they generate do not differ markedly from line to line; this is not always the case in computer graphics; therefore interlace may not always be implemented.[6]

FIGURE II
Interlaced Scan Sequence



Unlike CRTs, flat-panel displays make use of matrix addressing to create a screen image. This technique employs a matrix of horizontal and vertical microelectrodes, the intersections of which are discrete picture elements, known as pixels.[7] To illuminate a point on the screen, the row and column microelectrodes intersecting at that specific location are activated. In practice, as each row is energized, all of the column lines intersecting that row at locations which require illumination are simultaneously activated. That horizontal row is subsequently turned off and the cycle is repeated with all the remaining rows. In this manner, flat-panel display images are created a line at a time, whereas CRT images are traced a dot at a time.[8]

Each addressing scheme places a different requirement on the display element. Beam addressing requires the display element to be capable of responding to extremely short drive pulses, due to the manner in which the electron beam rapidly sweeps across the CRT screen, point by point, to create an image.[9] In contrast, matrix addressing requires each display element to incorporate a threshold function so that the element will not respond to any excitation it may receive when adjacent

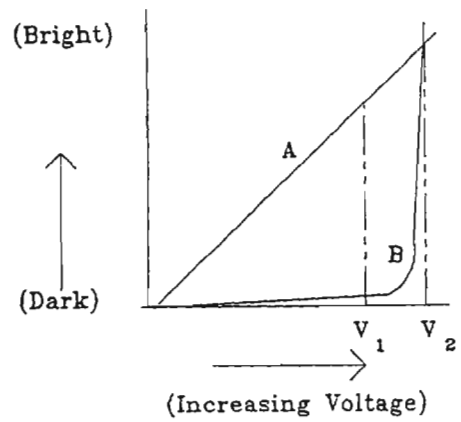
OCID: 4011963

elements are activated.[10] This threshold effect is achieved through the application of a non-linear voltage-versus-light characteristic.[11]

Flat-panel displays all contain some substance which will either glow (emissive) or change the way light is reflected (non-emissive) when a voltage is applied. If such displays employed a linear voltage-versus-light characteristic, as any pixel is selectively excited, all of the pixels along the associated column and row electrodes would glow dimly, activated by a partial voltage.[12] This is inadequate for a satisfactory matrix-addressed display, therefore a non-linear voltage-versus-light characteristic is applied. In this way, as voltage is increased between the horizontal and vertical electrodes, insignificant light emission or reflectance occurs at the selected pixel until a threshold is passed, at which time the light output rises steeply.[13] A pictorial representation of both the linear and non-linear voltage-versus-light characteristic may be found in Figure III.

FIGURE III

Threshold Effect



Threshold effect is needed so a single circuit can drive all pixels along one line. Otherwise, for a linear curve (A), all the other pixels along the selected line would glow when any voltage is applied. But with nonlinear curve (B), they would not glow even when a large voltage V_1 is applied to the row. Combined with a small additional voltage to the column electrodes, the threshold V_2 is passed, creating a bright dot at that crosspoint.

As a result of this non-linear characteristic, a fairly high voltage can be applied to all the elements of a selected row with a single driver. While this voltage is maintained below the threshold level, all the pixels in the selected row will remain dark. When small voltages are applied to selected column drivers, the potential at the crosspoints of these row and column electrodes will rise above the threshold level, causing selected pixels along the activated row to be illuminated. The duration or strength of the voltage can be varied to control the brightness or gray levels of the selected pixels. By repeating this process for each row of the display device, an entire image can be created, line by line, on the viewing surface.[14]

In selecting a display device, an important factor to consider is its particular screen-addressing technique. If the application demands high-resolution moving images with full color and good contrast, a CRT may be the best selection. On the other hand, if full color is not essential, but high precision and good resolution are, a flat-panel display may be the better choice. Whatever the application, understanding the special advantages each screen-addressing technique has will provide assistance in making a selection.

EXPLORING FLAT-PANEL TECHNOLOGY

Among the many flat-panel displays currently being researched and marketed, several esoteric technologies may be identified as being potentially the most viable alternatives to the CRT. In this section of the paper, four flat-panel display implementations will be examined in terms of their design, operating characteristics, strengths, and limitations. These four technologies include gas plasma, electroluminescent, electrophoretic, and liquid-crystal displays.

Gas plasma displays

Of the major flat-panel displays currently available, gas plasma panels appear to be the most prolific. This may not be a function of their technical superiority, but rather a result of being marketed longer.

The notion that light could be produced by an electric discharge through a gas has been known for over 200 years. Scientific interest in this phenomenon was stimulated as early as the mid-1800s, when Geissler fabricated glass tubes with electrodes sealed at opposite ends and filled them with gases such as oxygen, carbon dioxide, and hydrogen under low

pressure.[15] While these tubes had a short operating life, they were of technical interest for the study of radiation spectra of different gases.[16] Following the discovery of neon in the early 1900s, elongated tubes containing this gas came into use for advertising signs.[17] Soon after World War I small neon-filled bulbs became available commercially because of their usefulness as on/off indicators for line voltage.[18] Today, the demand for information displays in digital computer systems and the persistent desire for flat-panel displays has spurred a steady growth in the development of gas plasma displays.

The essential picture element (pixel) in gas plasma displays is an electrical gas discharge that develops between two electrodes when the applied voltage exceeds a threshold level. In a simple display, such as an on/off indicator, there is only a single discharge site. In recently developed high-resolution matrix displays, however, there are over one million discharge sites.[19] If such a high resolution matrix required two million electrodes, the development of such a display would be completely impractical. In matrix displays, electrodes are usually shared by a row or column of discharge sites. One million discharge sites in this configuration would require only 2,000 electrodes, a thousand for each axis. This makes development of such high-resolution matrix displays extremely practical and highly desirable.

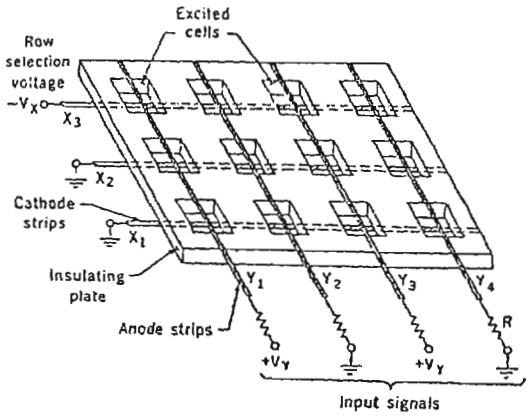
Gas plasma displays can be classified according to a number of attributes. They are usually identified as being either AC or DC displays.

- In AC versions, dielectric surfaces separate the electrodes from the gas.
- In DC versions, the electrodes are immersed in the gas.[20]

Another classification relates to their mode of operation as storage or nonstorage.

- In storage mode, the memory that holds the image information is inherent to the display device.[21]
- In nonstorage or cyclic mode, the memory is external to the display. Unless the image can be represented by a single discharge, the image information is transferred to the device and displayed sequentially, usually one row or column at a time. To avoid flicker, this entire image must be continually refreshed.[22]

FIGURE IV
DC Plasma Panel

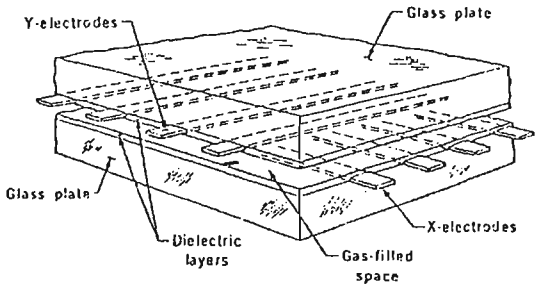


The basic structure for a matrix-addressed DC plasma display is presented in Figure IV. The individual cells in this display type are defined by holes in the insulating plate. In line with the holes is a set of cathode strips on the lower surface of the plate. Running perpendicular to these is a set of anode strips on the opposite surface. While not depicted in this diagram, it must be assumed that this entire structure is contained between a pair of glass plates that are vacuum-sealed at the edges and filled with gas at a low pressure.[23] To operate, a pulse voltage, $-V_x$, is applied to one of the cathode strips while input signals in the form of pulse voltages, $+V_y$, are applied simultaneously to selected anode strips. Since the voltage sum V_x+V_y is assumed to be greater than a threshold voltage, V_t, for initiating a gas discharge, light emission is produced at the excited cells, wherever the two voltages intersect. Since the individual voltages V_x and V_y are assumed to be less than the threshold voltage V_t, no other cells of the matrix will be excited. Similarly, other rows of cells can be repetitively addressed in rapid sequence to produce a flicker-free image.[24]

An alternative gas plasma device in commercial use today is the AC plasma panel, depicted in Figure V. In this display, the X and Y conductors are fabricated on the inner surfaces of two glass plates. These electrodes are then covered with a thin layer of glass so there is no direct contact between the electrodes and the gas contained between the two plates.[25]

CID: 4011963

FIGURE V
AC Plasma Panel



During operation of this plasma display, an AC sustaining voltage is maintained between the sets of X and Y conductors. This voltage alone is insufficient to excite any cells in the off state. If voltage pulses of suitable magnitude are applied to a selected pair of X-Y conductors, a discharge can be initiated. This discharge will quench itself within approximately one millisecond, due to the buildup of charges on the insulating walls resulting from the current flow. Following this, the cell will continue to fire on successive half-cycles, since the voltage built up on the walls during each half-cycle will add to the applied voltage of the next half-cycle. Subsequently, triggering selected cells in sequence, a complete image can be stored.[26]

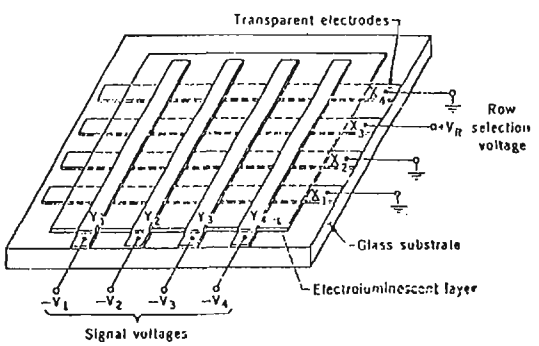
The plasma panel has several advantages and disadvantages. Its ruggedness makes it more appropriate for some military and industrial applications where CRTs would be unacceptable.[27] Its small size makes it suitable in aircraft and certain office environments where space may be a critical consideration. With a diffusing surface on the back or within the panel, optical images can be superimposed on the digitally-generated images.[28] Finally, the plasma panel produces steady and flicker-free images and text that is easy to read and interpret.[29]

The disadvantages of plasma display are its poor resolution and complex addressing and wiring requirements.[30] Its inherent memory may be useful in certain applications, although it is not as flexible as the frame-buffer memory available in CRTs.[31] While gas discharge technology has stimulated efforts to develop color displays, this area remains primarily in the research stage due to the technical problems and costs associated with this enhancement.[32]

Electroluminescent displays

The flat-panel display technology most likely to challenge the characteristics of the CRT is the electroluminescent display--in particular, the thin-film electroluminescent layer display. As early as 1937, G. Destrian showed that light could be obtained from specially prepared zinc sulfide powder layers when an AC electric field was applied.[33] Unfortunately, development of this technology was delayed until 1950, due to a lack of satisfactory transparent electrodes for viewing the phosphor.[34]. In 1950, however, workers at Sylvania, using a similar phosphor powder, were successful in producing cells which employed recently-developed transparent coatings of tin oxide on glass.[35] From that point, research has expanded to include improving electroluminescent phosphors and developing display devices based upon these materials.

FIGURE VI
Electroluminescent-layer Display



In the early 1970s an electroluminescent layer was developed that could be excited with a DC (or pulsed DC) voltage and that exhibited highly desirable characteristics for display applications. These devices are of particular interest for displays containing a large number of pixels, due to their proven high light output obtainable through short DC pulses and sharp threshold voltages.[36] As with gas plasma displays, electroluminescent layer displays employ a matrix addressing scheme to reduce the number of electrodes necessary for the display. The operation of

DOCID: 4011963

this device is highly similar to that of the gas plasma display, and tests have shown that a flicker-free image can be produced by applying the pulse voltage, $+V_r$ to successive rows and cyclically repeating this addressing process.[37] (Figure VI) Panels of this type have been developed for experimental purposes to display both alphanumeric information and television images.[38] Electroluminescent panels, 20 by 27 centimeters in size, containing 224 x 224 elements, have been developed and successfully exhibited images with good gray scale and highlight brightness of 10fl (foot-lamberts), approximately one-tenth the brightness exhibited on commercial television receivers.[39]

Current efforts have been directed more toward developing thin-film electroluminescent displays, as an alternative to powder layer displays. Initially, these attempts resulted in films with poor light output and limited duration.[40] In the period between 1964 and 1970, workers at Sigmatron were successful in developing much improved films. They achieved this by using manganese-activated zinc sulfide powder, applying additional insulating films on one or both sides of the panel, and by coating the rear surface of the phosphor with an additional light-absorbing layer of arsenic selenide, enabling the transparent phosphor to appear black while in its off state.[41] This led to the development of display panels that could be viewed with good contrast even in high ambient light.

Much like the DC powder layers, thin-film phosphors react to a very sharp threshold voltage, also enabling them to be designed in an X-Y matrix-addressing scheme. Thin-film panels of this type have been developed and used to display alphanumeric information and television images.

Thin-film electroluminescent panels may be scanned at video rates, due to the rapid response of their phosphor.[42] When a given pixel is excited, its light output diminishes to approximately half its original brightness in about a millisecond. This persistence level, comparable to that of CRT phosphors designed for video displays, contributes to the panel's average brightness.[43]

Thin-film panels have been developed to display television images with good gray scales, an important attribute for displaying high-quality pictures. In CRTs, displaying video images with gray scale is an analog function of the electron beam. Thin-film electroluminescent panels typically feed the video input through an analog-to-digital converter, which codes it into 16 levels of gray and converts it to a 4-bit digital number. When the signals are transferred to the column drivers, the 4-bit code associated with each column is used to set the column drivers to one of 16 levels of voltage, thereby varying the brightness levels.[44]

Research indicates that arrays of thin-film panels may be successfully used as memory devices if the manganese content of the zinc sulfide is increased (from approximately 1 percent by weight to approximately 5 percent).[45] While this storage mechanism is still in the experimental stage, panels of this type exhibit the potential for displaying stationary images with a large number of pixels, since slow writing speeds may be used to create images totally free of flicker.

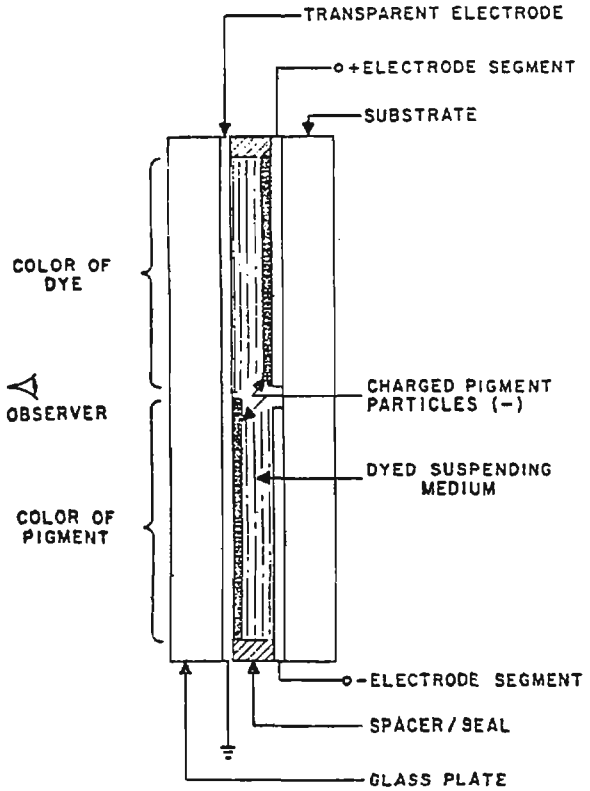
While thin-film electroluminescent panels show promise for a wide range of display applications, several disadvantages are inherent to their design and the elements used to create their displayed images. The high-voltage addressing circuits required to drive these displays are currently a disadvantage of this type of flat-panel device. This problem may be resolved in the near future as suitable low-cost integrated circuits become available.[46] Another problem is the relatively low efficiency of electroluminescent layers resulting in considerable power dissipation in the panel and drive circuits. As a result, electroluminescent layers exhibit only a small percent of the efficiency of the finest electron-bombarded phosphors.[47] Limitations of the materials presently used in constructing X-Y-addressed thin-film panels leads to a maximum obtainable brightness for full television resolution of approximately one-tenth that available from cathode-ray tubes.[48] Researchers have pursued developing phosphors with colors other than the yellow-orange characteristic of the standard thin-film panels, but they tend to exhibit a significant decrease in efficiency.[49]

Electrophoretic displays

Another flat-panel device, the electrophoretic display, is a nonemissive device based upon the principle of electrophoresis--the migration of charged particles in an electric field.[50] This display makes use of a thin layer of dyed fluid in which pigment particles of a highly contrasting color or reflectivity are suspended.

CID: 4011963

FIGURE VII
Electrophoretic Display



Electrophoretic display images are formed by light-colored pigment particles being deposited on a viewing electrode against a dark background of dielectric fluid. By electrostatically driving the pigment to the viewing surface of the display, the pigment color becomes observable at that specific picture element. Conversely, by electrostatically driving the pigment toward the back electrode and thus, away from the viewing surface, the pigment particle is masked from sight by the dark colored fluid.[51] (Figure VII)

The advantages of electrophoretic displays, including high contrast, wide viewing angles, inherent memory, and low power consumption, have encouraged researchers to apply this medium to large-information-content flat-panel devices.[52] Two methods investigated to accomplish this goal include the direct matrix and active matrix approaches.

The direct matrix, containing only the display medium held between the row and column electrodes on their respective cell walls, is relatively easy to build and simple to operate. Not only does this provide for an attractively low overall system cost, but a further advantage is its inherent memory which eliminates flicker, avoids the necessity of refreshing, and allows for high levels of multiplexing.[53]

While the early electrophoretic fluids often lacked the well-defined voltage threshold required for direct matrix addressing, several techniques have been researched which successfully ameliorate this problem. One technique introduces an external threshold by fabricating three sets of electrodes and operating them in a triode mode. This successfully permits matrix addressing and also reduces addressing times.[54] A second technique has proven successful by building an inherent threshold into the electrophoretic suspension. This is accomplished by adjusting the particle-to-particle and particle-to-electron interaction. The voltage threshold is thereby created by either altering the composition of the suspension or the nature of the surfaces.[55]

The active matrix approach, with matrix drivers and local storage capacitors integrated into the display, appears to be the most viable display technique for a high-speed, page-size, interactive electrophoretic display.[56] An experimental 32 x 32 varistor-capacitor array-driven electrophoretic device has been developed which creates images a line at a time without crosstalk, flicker, or refreshing.[57] Future varistor-capacitor array-driven electrophoretic devices should have higher resolution and larger viewing areas for better utility.

Liquid-crystal displays

The final flat-panel device to be discussed is the liquid-crystal display. Like the electrophoretic display, this device is a nonemissive display, since it controls the transmission or reflection of external light.[58] This characteristic makes it especially useful for displays that must be viewed in high ambient light.

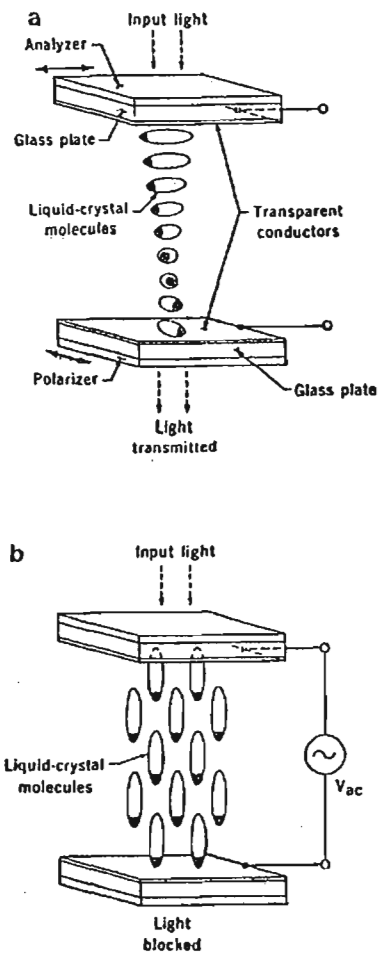
Liquid-crystal materials belong to a class of organic compounds which, under certain temperature constraints, exhibit several optical and electrical properties characteristic of crystalline solids.[59] Interest in liquid-crystal materials for display devices first began in the 1960s when it was demonstrated that an electric field applied across a thin

DOCID: 4011963

layer could produce significant changes in light transmission with very low power consumption.[60] Since that time, following extensive research, liquid-crystal displays have proliferated in the market in watches, pocket calculators, and various other electronic instruments.

Molecules of all liquid-crystal materials are generally elongated in shape, causing variations in the index of refraction depending upon the orientation of the molecules. Most liquid-crystal displays currently available use twisted nematic molecules.[61] The alignment of these nematic liquid crystals is essentially parallel. In addition, if the alignment direction is established at the liquid's boundary, such as at the surface of the glass plates restraining the liquid material, all the molecules tend to assume the same alignment.[62]

FIGURE VIII
Liquid-crystal Display



A twisted nematic display is composed of a layer of nematic material contained between the transparent conductive surfaces of two glass plates. This structure is then placed between two polarizers. Before constructing the panel, the glass plates are specially treated to cause the molecules at the surface to align in a direction nearly parallel to the surface of the plate. Figure VIII(a) shows this configuration, which also represents the appearance of a twisted nematic liquid-crystal cell when no voltage is being applied. In this configuration, light is guided by the helical molecules so that the panel is bright with the voltage off.[63]

When an AC voltage is applied across the cell, nearly all the molecules will align themselves perpendicular to the glass surfaces, as shown in Figure VIII(b). With the molecules aligned vertically between the two plates, light is blocked by the polarizers.[64]

Liquid-crystal displays consume less than 1 microwatt per square centimeter, considerably less power than that required for luminescent displays.[65] This makes them highly practical for portable, battery-operated devices. An important disadvantage of liquid-crystal displays is their relatively slow response, their turn-on and turn-off times both requiring approximately Ø.1 seconds at room temperature.[66]

Considerable effort has been directed toward developing liquid-crystal displays that do not require polarizers. Success has been achieved by dissolving dichroic dyes in the liquid-crystal material. This improves brightness and provides for a wider viewing angle, two significant limitations of the twisted nematic displays. In panels of this type, positive-contrast images (colored images on a colorless background) or the reverse can be produced in a variety of colors depending on the dyes used.[67]

X-Y-addressed arrays with good contrast over an acceptable viewing angle (more than 10 rows) have not yet been developed for liquid-crystal displays. This is largely due to the lack of a sharp threshold function.[68] Attempts to overcome this limitation involve either incorporating a field effect transistor at each pixel to prevent voltage from appearing along unselected elements or utilizing collimated light to exploit other optical effects in liquid crystals whose threshold is much sharper. This second technique should allow display images to be created with several hundred rows.[69]

OCID: 4011963

ADVANTAGES AND DISADVANTAGES OF THE CRT

Despite the competition from flat-panel and other display technologies, the cathode-ray tube remains preeminent in today's market. Its numerous advantages make it a stiff competitor for less researched and developed technologies. The CRT is a high-resolution display, adaptable for both individual and small group viewing.[70] Its method of screen addressing is through the use of a deflected focused beam of electrons. This is especially useful for applications where the information to be displayed is supplied serially.[71] The CRT is the basic component for the direct-view storage tube, calligraphic displays, and raster displays, adding to its continued success.[72] The wide range of phosphors and careful filtering have made it possible to achieve good contrast in extremely bright ambients.[73] Phosphors exist which also exhibit good and predictable lifetime characteristics.[74] CRTs are inexpensive and relatively easy to manufacture.[75] They can produce high-resolution color displays having wide viewing angles without degradation of brightness or contrast.[76] Their phosphors emit light instantaneously and decay quickly, thereby permitting real-time video displays.[77]

While the CRT has proven adaptable to the demands of many applications, numerous disadvantages render it inappropriate or useless in others. CRTs are bulky devices, occupying considerable desk space. This becomes a serious concern in applications where space considerations are paramount. They lack ruggedness, with their thin glass envelopes susceptible to breakage.[78] Their screen surfaces reflect light, a characteristic which can both distract and annoy the user.[79] Limited success has been achieved in developing self-luminous projection CRTs. It appears difficult to produce and collect sufficient light from a self-luminous CRT to provide bright, high-resolution, large-screen displays with adequate cost and lifetime.[80] The CRT is an analog device, making it inadequate for interactive graphic applications where true digital displays are necessary.[81] CRTs nearly always exhibit some distortion because the electron beam must travel different distances to strike all areas of the screen surface, striking it at different angles and with varying spot size and shape.[82] Finally, the CRT is a high-voltage device, a definite disadvantage under low-pressure conditions, such as in aircraft.[83]

BENEFITS AND LIMITATIONS OF FLAT-PANEL DISPLAYS

Functionally, flat-panel displays offer a viable alternative to CRTs, especially in applications where space considerations play an important role in the design of a system. Some of the numerous advantages of flat panels, which make them especially attractive for military and certain industrial applications, include their ruggedness, portability, shock resistance, ability to withstand wide temperature variances, long-life characteristics, and low power consumption requirements.[84] Flat panels are inherently free of geometric distortion and have such "built-in" features as orthogonality, linearity, and resolution.[85]

Economically, flat-panel displays are still too expensive to replace CRTs: a 10-to-1 price ratio currently exists between flat-panels and CRTs.[86] Production costs of AC and DC plasma panels, liquid-crystal displays, and electroluminescent panels are significantly greater than those of CRTs with relatively the same resolution.[87]

Two major factors contributing to the high cost of flat-panel display terminals are their expensive drive electronics and low production volumes. Flat-panel display terminals continue to maintain a high price tag because they are still produced in small quantities, compared to CRTs.[88] Even if production increased dramatically, the cost of drive electronics would have to drop significantly before the market would open for flat-panel displays.[89]

Progress is currently being made in that direction. Texas Instruments (TI) has developed a 32-channel integrated circuit that significantly reduces the display-drive electronics. "Where it once took two diodes and a resistor to drive each line of a 512 x 512 display, it now takes only 32 TI integrated circuits."[90]

Despite the high costs, flat-panel displays should not be dismissed when searching for a display technology that best suits the needs of a specific application. In many situations, flat-panel terminals can be justified due to their size, durability, and low power consumption.

OCID: 4011963

FLAT-PANEL DISPLAY APPLICATIONS

As long as complicated drive circuitry and low-volume production continue to make flat-panel displays expensive, applications for these devices may remain limited to military and highly specialized commercial users.

IBM's flat-panel displays are available with their retail and banking systems and are primarily targeted for high-volume-usage applications.[91] The Q-1 Corp., Hauppauge, N.Y., has incorporated flat-panel terminals into systems for its small business and banking customers, who appreciate the durability and space savings of the displays.[92] Companies such as General Digital Corp., East Hartford, Conn., and Science Applications, Inc., La Jolla, Calif., sell flat-panel display terminals to industrial customers for use in factories and on oil-drilling platforms, applications demanding a rugged display device.[93] A DC plasma display terminal marketed by General Digital Corp., is being used for applications such as an instructor's controller in advanced aircraft simulators, a metal-rolling-mill controller, an automated electronic testing device, an executive desktop information retrieval terminal, and a control and monitoring device in manufacturing and food processing plants. Named the VuePoint, this flat-panel device incorporates a Burroughs display, the Self Scan II, and uses a touch-sensitive screen overlay that eliminates the need for a keyboard.[94]

Until the high cost of flat-panel technology is considerably reduced, many suppliers will have to depend heavily on military contracts to remain in the market. The military is generally able to base purchasing decisions on utility rather than cost, which has enabled them to investigate and purchase flat-panel terminals applicable to their specific needs.[95] Elliot Schlam, Chief of the display division of the US Army's Electronics Research and Development Command (ERADCOM), Fort Monmouth, N.J., says "the Army decided 12 years ago that it had to use automated data-processing equipment on the battlefield rather than rely on antiquated means of communication, such as teletypewriters, walkie-talkies, and hard-copy message deliveries. Flat-panel displays, rather than CRTs, are playing a major role in the military's communication scheme.... A battle unit needs a rugged, portable terminal that can withstand shock, vibration, and a wide range of temperatures, one that will have a long life, and one that will not consume much power. Considering those criteria, CRTs do not match up to flat-panel displays."[96]

Among the many flat-panel display devices being used in military applications is a portable unit that fits into a briefcase, built by Hycom, Irvine, Calif., a subsidiary of Sharp.[97] This particular system is intended for a wide range of functions, to include command and control, intelligence-data relay, radar display, air-traffic control, and ballistic calculations. Other flat-panel devices being built for the military include large-screen displays for use in command centers. One such display is being manufactured by Photonics, Luckey, Ohio, an AC plasma display supplier. It is a large-screen AC plasma device, assembled by Magnavox, measuring 1 meter diagonally and containing 2 million light-emitting pixels.[98] In addition, Photonics and other flat-panel suppliers are producing small displays that can be incorporated into hand-held computers, transparent map-overlay displays, and instrumentation displays for aircraft and submarines.[99]

While plasma displays have primarily been designed into military terminals over the past 10 years, Elliot Schlam says most future contracts under his control will be for electroluminescent displays and states, "In a point-by-point comparison of plasma and electroluminescent displays, electroluminescent models weigh less, consume less power, and are priced lower than plasma displays."[100] In his opinion, electroluminescent technology is clearly the one to pursue.

Hycom has made its first large-scale commercial sale for a portable terminal that will be used for such applications as field service, diagnostics, and electronic mail. Riley Holly, an assistant vice president for the company says, "It will be like an Apple [computer] in a suitcase. The price should be comparable to what a small Apple would cost, but the user will be able to carry the system around with him."[101] He also states that the unit will be battery operated and may use CMOS nonvolatile memory.

CURRENT RESEARCH IN FLAT-PANEL TECHNOLOGY

The CRT has maintained its preeminent position in the field of television and information displays largely as a result of its many outstanding characteristics, including high resolution, wide range of colors, high brightness, good contrast, low cost, and firmly established manufacturing techniques. Its numerous disadvantages, however, have encouraged researchers to actively investigate alternative display technologies. This section of the paper will briefly describe some

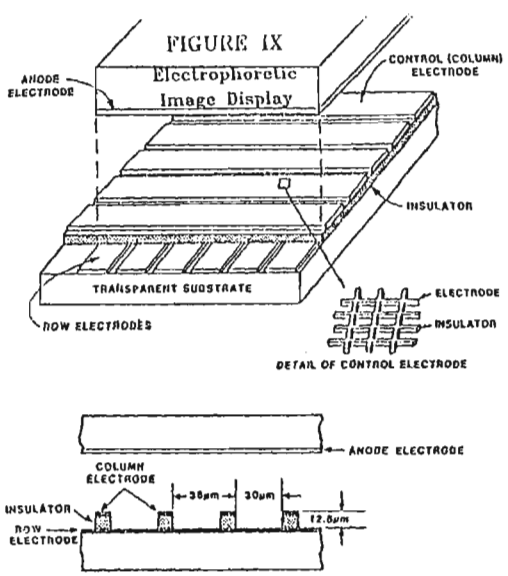
OCID: 4011963

research currently being undertaken in the area of flat-panel technology as attempts to solve these limitations.

The Defense Advanced Research Projects Agency (DARPA) has partially supported the development of a 512-character electrophoretic display by Philips Laboratories, Briarcliff Manor, New York. This matrix-addressed electrophoretic image display, using a control electrode principle, is a non-emissive flat-panel display having 228 columns and 148 rows with pixels 0.25 mm square. Commercially available high-voltage shift registers and microprocessor control have been used in driving this display device.[102]

An important characteristic of this electrophoretic image display is the application of the control electrode principle. This entails creating an electrostatic threshold for switching by introducing a third electrode between the two electrodes of the basic device. This third electrode is in the form of a mesh and is detailed in Figure IX. The significant advantage of this matrix addressing approach is its extremely fast addressing time.[103]

FIGURE IX
Electrophoretic Image Display



Research indicates that the control electrode principle provides a practical and dependable method for the introduction of an electrostatic threshold into an electrophoretic image display. The basic structure is simple and the threshold is not materials dependent, but is controlled by the geometry of the device. It does not require special suspensions and it appears that the size of the display and the number of pixels can vary to include large screen displays with few serious limitations. The developers of this electrophoretic image display believe it will make the use of non-emissive displays in large information content applications highly practical in the near future.[104]

Individuals at IBM's Watson Research Center, Yorktown Heights, New York, have investigated the notion of a storage CRT display using a thin-film electroluminescent faceplate.[105] After summarizing their findings in the areas of selective erasure, attainable levels of brightness, contrast, resolution, and the constraints and concerns associated with the development of such a large thin-film electroluminescent faceplate, they support the concept of developing this storage CRT. It show promise for exhibiting such outstanding display features as high luminance, good contrast, no flicker, high information capacity, and reasonably high rates of interactivity.[106] Technical problems in fabricating a practical device of this type remain, yet the developers do not perceive them to be insurmountable. Solving these problems will most likely yield a highly useful and marketable display device.

James L. Ferguson of American Liquid Xtal Chemical Corp., Kent, Ohio, has investigated the use of birefringence in liquid-crystal displays and has developed what he terms "the fastest mode of drive for a nematic liquid crystal yet available."[107] While many of the characteristics of this device remain to be investigated, Ferguson asserts that a high-performance matrix display can be produced which has the capability of presenting a moving image without tailing or sticking, and attainable multiplexing levels in excess of 30 to 1.[108]

Jacques Robert, partially sponsored by the Centre National d'Etudes des Telecommunications of France, has developed a complex liquid-crystal matrix display to be used as a television screen.[109] The three major components of his experimental video display, developed mainly for videophone applications, include a liquid-crystal cell, driving electronics, and projection optics. It has

OCID: 4011963

128 x 128 display elements, multiplexing capabilities allowing a display of eight shades of gray and an image change rate greater than five times per second. Intermediate results have demonstrated that fairly complex pictures of faces can be produced with the stated system characteristics. Robert suggests this is simply the first stage in the development of a liquid-crystal video display. He asserts that performance can be enhanced by such improvements as increasing the number of display elements to 256 x 256, increasing the levels of gray scale to 16 or 32, and improving the image rate.[110]

A low-threshold-voltage thin-film electroluminescent device has been developed by members of the Faculty of Engineering Science, Osaka University, Osaka, Japan.[111] Although high brightness, long life, and limited color have been achieved for thin-film electroluminescent displays, the problem of high voltage requirements has remained. This has severely hampered the use of commercially available integrated circuits, leading to highly complicated and expensive driving circuits. This voltage requirement has also prevented improvement of the device's reliability. The low-threshold-voltage thin-film electroluminescent has been successfully implemented at 60 volts. This is nearly one-fourth the voltage of most conventional thin-film electroluminescent devices.[112] In addition, it has successfully exhibited brightness levels of 300fl at 60 volts, with a maximum attainable of more than 800fl.[113]

Exxon has been particularly active in flat-panel display research. Kylex, an Exxon subsidiary in Mountain View, Calif., has recently developed a liquid-crystal flat-panel device capable of displaying eight lines of characters. While this appears quite restrictive, there is speculation that Kylex displays will soon be expanding to CRT capacities.[114]

Innovative research is being conducted by a wide variety of groups. Hopefully, their continued efforts will assist in promoting greater interest in the development of all types of flat-panel displays, leading to an enhanced display technology without the identifiable disadvantages characteristic of the CRT.

THE PRICE DIFFERENTIAL

Ken Bosomworth, President of International Resource Development, Inc., Norwalk, Conn., suggests that there is a 10-to-1 price ratio between flat panels and CRTs.[115] A cost comparison of the two technologies easily substantiates this figure. Purchase price estimates for a basic CRT range from $100, for a single-unit purchase, to as low as $60 for volume purchases.[116] In contrast, Electro-Plasma of Millbury, Ohio, manufactures a 256 x 512-pixel AC plasma display which sells for $2,450 in single-unit orders and $1,500 for volume purchases greater than 1,000.[117] In a similar price range, Sharp manufactures a 240 x 320-pixel electroluminescent display that sells for $2,800 in single-unit orders, with no quantity discounts.[118]

Despite these high costs, many terminal manufacturers remain in the market and appear enthusiastic about the future of flat-panel display technology. An example of one such manufacturer is Televideo, Inc., San Jose, Calif. Mel Snyder, Vice President for Marketing and Sales of Televideo, refers to flat-panel terminals as the "products of the future" and adds that his company is particularly interested in the development of electroluminescent technology.[119]

As such optimism continues to grow and pervade the manufacturing community, the research and production of flat-panel technology will undoubtedly surge. Ultimately, this should lead to a significant drop in flat-panel display prices, closing the price gap between CRTs and flat panels, and enabling flat-panel technology to become more economically competitive with the CRT.

CURRENT MANUFACTURERS OF FLAT-PANEL TECHNOLOGY

Despite the limited market and high costs presently associated with the development of flat-panel displays, many companies remain actively involved in the research and production of this technology. Companies as large as IBM, Nippon Electric Company, Burroughs, and Sharp, and as small as Electro-Plasma and Photonics, are highly supportive of advancing the development of flat-panel display products.[120] Manufacturers in the process of developing prototype TV displays using plasma or liquid-crystal devices include Fujitsu, Hitachi, Matsushita, and Seiko Denki Company.[121] Military data terminals utilizing gas plasma panels are currently in production by Magnavox, SAI, Interstate, Singer Librascope, and Norden.[122] Aerojet Electro Systems, Azusa, Calif., and Rockwell Electronics Research, Thousand Oaks, Calif., are developing new thin-film electroluminescent panels with self-contained integrated circuit drivers

DOCID: 4011963

for upcoming enhancements in Army data terminals.[123]

Hycom, a US-based subsidiary of Sharp, is one of the leading manufacturers of flat-panel display technology. Hycom has produced a thin-film electroluminescent panel for use in the Army's Digital-Message Device, a portable battlefield terminal. While manufacturing costs of a comparable CRT would be considerably less, this panel requires much less power and has a longer life. Hycom speculates that high-volume production will bring manufacturing costs down to CRT levels within the next two years.[124] Hycom is nearing delivery of a Tactical Video Display, which has demonstrated the compatibility of a thin-film electroluminescent display with a standard video signal. Company officials claim commercial versions of the Tactical Video Display will sell for less than $500 each for production rates of one thousand or more per month. A special feature of this device is a black layer on the rear surface of the display. This will provide for greater contrast in high ambient light, such as will be found in field operations or in helicopters.[125] Hycom is currently marketing electroluminescent panels with high resolution and picture element density applicable for both graphic and alphanumeric displays.[126] Hycom and GTE's Lamp Division, Salem, Mass. are in the process of developing fully transparent thin-film electroluminescent displays for Army Tactical Data terminals. These displays will be used as overlays on top of field maps.[127] In addition, Hycom is currently developing flat-panel displays for the "electronic desk" of the future, possibly even for the "electronic briefcase."[128]

Rockwell Electronics is nearing completion of a miniature thin-film electroluminescent device that could possibly provide full video capabilities. With a screen size of 1 x 1.4 inches, the device produces a high-quality video display of 512 x 683 lines, aptly demonstrating the high-resolution capabilities of electroluminescent technology. The display's total power consumption is less than five watts, making it highly suitable for such military applications as thermal weapon sights, head-mounted cockpit displays, mortar-locating radar displays, and terminal displays.[129]

CONCLUSIONS

The goal of this paper has been to pursue a thorough examination of flat-panel technology. To achieve this result, the paper has explored contrasting methods of creating display images on both CRT and flat-panel devices, examined in depth four major flat-panel displays currently being researched or developed as viable CRT alternatives, cited major advantages and disadvantages of CRTs and flat-panel displays, and summarized some current research in flat-panel technology.

Despite the distinctive characteristics of each of the flat panels explored within this paper and the different immediate and specific goals of these technologies, it appears they all share a common goal; namely, the achievement of a level of performance comparable or superior to that of the cathode-ray tube. While the present limitations of these technologies may hinder their achieving this goal within the next few years, it is clearly just a matter of time before flat-panel display technology will successfully displace the cathode-ray tube in both military and commercial markets.

FIGURE X

Estimated flat-panel display market*
(US shipments - $million)
1980-1990

Word- and data-processing application	Military	Consumer
1980	15	-
1982	80	-
1985	130	-
1990	320	130

* Displays with more than 200 characters

Figure X presents the International Resource Development's forecast for flat-panel display shipments, based on current technology and pricing trends. The table indicates that by 1985, flat panels will be offering CRTs a serious challenge in military applications and by 1990, they will have made great strides into the consumer market.[130]

Saul Kuchinsky, president of Quantum Systems, a consulting firm that specializes in flat-panel displays, says there are "literally thousands" of applications for flat-panel displays in the commercial market.[131] He comments, however, that the real problem lies not so much with the technology as with conservative management policies. Kuchinsky estimates that within five to 10 years, flat-panel display terminals will account for 25 percent

OCID: 4011963

of the display market.[132] He predicts, "One company, probably a Japanese company, will have success with flat-panel terminals, and all of a sudden everyone will get involved. Cautious companies need proof of someone else's success."[133]

Although low-volume production and high costs currently suppress market demands for flat-panel terminals, innovative research, in both the commercial and private sectors, is expanding at a phenomenal rate, creating a bright future for flat-panel technology.

Footnotes

1. Catalano, Frank. "Exploring Flat-Panel Technology." Mini-Micro Systems, Dec. 1981, p. 126.
2. DeJackmo, Margaret. "Major Challenge to CRTs from Flat-Panel Displays." Mini-Micro Systems, Nov. 1980, p.113.
3. Ibid.
4. Tutorial: Computer Graphics. Proceedings of the Spring Compcon79 on Computer Graphics. 26 Feb.-1 Mar. 1979. Institute of Electrical and Electronics Engineers, Inc.: New York, N.Y., 1979, p. 23.
5. Newman, William M., and Robert F. Sproull. Principles of Interactive Computer Graphics. New York: McGraw-Hill, Inc., 1979, pp. 35-36.
6. Ibid., p. 217.
7. Meyer, Franklin. "Picture Brightens for Flat-Panel Displays." High Technology, March/April 1982, p. 36.
8. Ibid.
9. Anderson, L.K. "The Cathode Ray Tube Display: Why Use Anything Else?" Symposium on Display Materials and Devices, Murray Hill, New Jersey. 3 May 1973, p. 4.
10. Ibid.
11. Meyer, p. 36.
12. Ibid.
13. Ibid.
14. Ibid.
15. Kazan, b. "Material Aspects of Display Devices." Science, Vol. 208, 23 May 1980, p. 931.
16. Ibid.
17. Ibid.
18. Ibid.
19. Tutorial: Computer Graphics, p. 89.
20. Ibid.
21. Ibid.
22. Ibid.
23. Kazan, p. 932.
24. Ibid.
25. Ibid.
26. Ibid.
27. Catalano, p. 125.
28. Tutorial: Computer Graphics, p. 99.
29. Ibid.
30. Kazan, p. 932.
31. Ibid.
32. Ibid., p. 933.
33. Ibid., p. 928.
34. Ibid.
35. Ibid.
36. Ibid., p. 929.
37. Ibid.
38. Ibid.
39. Ibid.
40. Ibid.
41. Ibid.
42. Ibid., p. 930.
43. Meyer, p. 37.
44. Ibid.
45. Kazan, p. 930.
46. Ibid.
47. Ibid.
48. Ibid.
49. Ibid.
50. 1980 Biennial Display Research Conference. Proceedings of a Conference on the Current Research in Information Display. 21-23 October, 1980. Institute of Electrical and Electronics Engineers, Inc.: New York, N.Y., 1980, p. 10.
51. Meyer, p. 38.
52. 1980 Biennial Display Research Conference, p. 10.
53. Ibid.
54. Ibid.
55. Ibid.
56. Ibid.
57. Ibid.
58. Kazan, p. 933.
59. Ibid.
60. Ibid.
61. Ibid.
62. Ibid.
63. Ibid.
64. Ibid., p. 934.
65. Ibid.
66. Ibid.
67. Meyer, p. 38.
68. Kazan, p. 935.
69. Ibid.
70. Anderson, p.3.
71. Ibid.
72. Newman, pp. 33-50.
73. Anderson, p. 10.
74. Ibid.
75. Meyer, p. 36.
76. Ibid.
77. Ibid.
78. DeJackmo, p. 113.
79. Ibid.
80. Anderson, p. 20.
81. Ibid., p. 21.
82. Meyer, p. 33.
83. Anderson, p. 22.
84. Catalano, p. 126.

CID: 4011963

85. Meyer, p. 36.
86. Catalano, p. 125.
87. DeJackmo, p. 114.
88. Catalano, p. 130.
89. Ibid.
90. Ibid.
91. Ibid., p. 125
92. Ibid.
93. Ibid.
94. Ibid.
95. Ibid., p. 126.
96. Ibid.
97. Ibid.
98. Ibid.
99. Ibid.
100. Ibid., p. 128.
101. Ibid., p. 132.
102. 1980 Biennial Display Research Conference, p. 26.
103. Ibid.
104. Ibid.
105. Ibid., p. 154.
106. Ibid.
107. Ibid., p. 178.
108. Ibid.
109. 1978 Biennial Display Research Conference. Proceedings of a Conference on the Current Research in Information Display. 24-26 October, 1978. Institute of Electrical and Electronics Engineers, Inc.: New York, N.Y., 1978, p. 52.
110. Ibid
111. 1980 Biennial Display Research Conference, p. 143.
112. Ibid
113. Ibid
114. DeJackmo, p. 114.
115. Catalano, p. 125.
116. Ibid
117. Ibid
118. Ibid
119. Ibid
120. Ibid
121. DeJackmo, p. 114.
122. Meyer, p. 39.
123. Ibid.
124. DeJackmo, p. 114.
125. Ibid.
126. Ibid.
127. Meyer, p. 39.
128. DeJackmo, p. 114.
129. Meyer, p. 40.
130. Catalano, p, 130.
131. Ibid., p. 132.
132. Ibid.
133. Ibid.

GLOSSARY

AC: Alternating current: an electric current that reverses direction at regular intervals, having a magnitude that varies continuously in a sinusoidal manner.

ambient: completely surrounding; encompassing.

anode: the positively charged electrode, plate, strip, or terminal of a cell, battery, vacuum tube, etc.

birefringence: the separation of a ray of light into two unequally refracted, polarized rays, occurring in crystals in which the velocity of light rays is not the same in all directions.

cathode: the electrode that emits electrons or gives off negative ions and toward which positive ions move or collect; the negative pole of a battery or other source of electric current.

cathode-ray tube: a vacuum tube in which cathode rays, usually in the form of a slender beam, are projected onto a phosphor-coated screen to produce a luminous spot.

CMOS: capacitive metal oxide semiconductor.

collimated light: an optical system that transmits parallel rays of light.

CRT: cathode ray tube.

DARPA: Defense Advanced Research Projects Agency.

DC: direct current: an electric current of constant direction, having a magnitude that does not vary or varies only slightly.

dichroic: exhibiting of essentially different colors by certain solutions in different degrees of dilution or concentration.

dielectric: a nonconducting substance; insulator.

diode: a device, as a two-element electron tube or semiconductor, through which current can pass only in one direction.

electrode: a conductor used to establish electrical contact with a nonmetallic portion of a circuit (as in an electrolytic cell, an electron tube, etc.)

electrophoresis: the migration of charged particles in an electric field.

ERADCOM: Electronics Research and Development Command.

fc: foot-candle; the quantity of light reaching a surface or the illumination as measured in foot-candles (fc = lumens/foot^2).

DOCID: 4011963

fl: foot-lamberts; the quantity of light radiated by a surface per unit area in a given direction, or its luminance as measured in foot-lamberts. The foot-lambert is defined in such a way that a perfect uniformly diffuse reflector (white bond paper is a reasonable approximation of a lambertian surface) illuminated with 1 fc will have a brightness of 1 fl.

flicker: In relation to graphics, flicker may be thought of as an unsteady image resulting from a display device with an inadequate refresh rate (number of times per second a picture is redrawn). The main determinant of the refresh rate is the phosphor's persistence, the time from the removal of excitation to the moment when phosphorescence has decayed to 10% of the initial light output. The longer the persistence, the lower the required refresh rate to produce a flicker-free picture. A picture appears constant or flicker-free to the viewer even though in reality any given point is "off" much longer than it is "on."

frame buffer memory: a large digital memory used to drive raster displays. Modern frame buffer memories generally use random-access integrated memory circuits. Given 8 bits or more of intensity precision, the frame buffer is capable of producing color and monochrome images whose complexity and quality are limited only by the quality of the TV monitor on which they are displayed. The frame buffer offers the only satisfactory display device for applications requiring shading, solid areas of color, high-quality text, or any type of image processing. Disadvantages of the frame buffer include the large amount of memory it requires to represent the display image, thus making it expensive, and the time it takes to fill this memory or change it, thus slowing down interactive response time.

index of refraction: the ratio of the velocity of light or other radiation in the first of two media to its velocity in the second as it passes from one into the other, the first medium usually being taken to be a vacuum.

integrated circuit: an interconnected group of circuit elements, as of resistors and transistors, in a single tiny wafer of semiconductor material.

linearity: the faithfulness with which an output signal of an electronic reproducing system reproduces an input signal; more specifically, the faithfulness with which the shape and arrangement of the elements in a television picture reproduce the shape and arrangement of the original televised image.

multiplexing: In general terms, the word "multiplexing" refers to the use of a single facility to handle simultaneously several similar but separate operations. Most computers, for example, have high-speed multiplexing input/output channels to handle many peripheral devices such as line printers or card readers, all of which may operate simultaneously. The main use of multiplexing, however, is in the field of data communication, where it is used for the transmission of several lower-speed data streams over a single higher-speed line. The primary motivation behind multiplexing is the reduction of costs, although in many cases an increase in reliability is an additional benefit.

nonvolatile memory: a memory that retains its contents even if the power supply is removed.

orthogonality: a system of surfaces consisting of two families whose components are mutually perpendicular where they intersect.

pixel: a picture element.

precision: with respect to graphic display devices, the measure of the programmer's ability to address a point on the screen.

refresh: the repeated passing of an image to the display device.

resistor: a device, the primary purpose of which is to introduce resistance into an electric circuit.

resolution: with respect to graphic display devices, the measure of the user's ability to distinguish points on the screen from one another.

semiconductor: a substance whose electric conductivity at normal temperatures is intermediate between that of a metal and an insulator.

suspension: the state in which the particles of a substance are mixed with a fluid but are undissolved.

transistor: an electronic device made of semiconducting material and equipped with three or more electrodes. It performs functions similar to those of a vacuum tube without requiring current to heat a cathode.

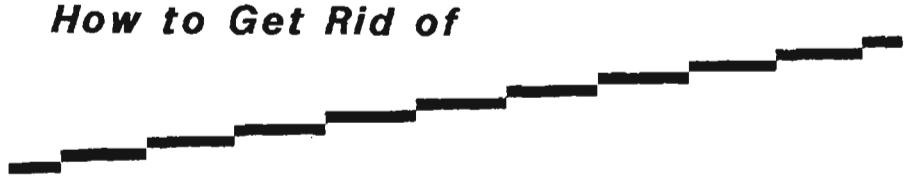
~~FOR OFFICIAL USE ONLY~~

CID: 4011963

Improving Raster Graphics Images by Anti-Aliasing

or

How to Get Rid of



the Jaggies(U)

by [redacted] R53

P.L. 86-36

I. Introduction

A. Graphics Devices

There are two main classes of graphics devices: continuous and discrete. A continuous or random-scan device draws with a beam on the display surface much as a person draws with a pencil on paper, with smooth, continuous strokes. A discrete or raster-scan device divides the display surface into a matrix or raster of picture points (or pixels). The picture is created by lighting up the pixels that it would cover if laid on top of the display surfaces.

Continuous devices, such as the calligraphic and storage tube displays, are excellent for representing line drawings because of their smooth, precisely positioned lines. Calligraphic display devices have the advantages of moving images and selective erasure, since the images must be redrawn 30 times a second, but the complexity of the image is limited. Storage tubes can represent very complex images, but the whole image has to be erased and redrawn every time one part of it has to be erased. In either device, filled-in areas are difficult to represent and there is no broad range of colors available.

Discrete devices can represent any amount of information possible without affecting performance. Areas are filled easily. A raster device can provide a full range of colors or intensities, which makes it possible to represent realistic images. Selected areas can be erased without affecting the rest of the image. However, animation is not very practical, since a lot of computation would be needed for each image and the precision to which objects can be placed in the image is usually not as high as in a continuous device.

B. The Raster Display

Since this paper is concerned with the raster device in particular, a little more information about it is needed. The raster device is very much like a television set controlled by a computer. The image is drawn, line by line, 30 times a second. These lines are called scan lines and the order in which they are drawn is called an interlace pattern. The information about whether or not to turn a pixel on is located in a frame buffer. This frame buffer is read 30 times a second and the values in it are converted to intensity or color information for the beam. Each pixel may have a number of bits of information about it if its intensity can vary. On a color display, the red, green, and blue components of a pixel's color have to be specified separately since three beams are used. Many raster displays use what is known as a color lookup table, which contains a list of the components for a number of specified colors. The number in the frame buffer corresponding to a pixel points into the color lookup table and specifies the color with which to draw the pixel. In this way, a few bits of information per pixel can specify a color from a wider range than they would directly.

One way to draw a picture on a raster display device is to send commands to the device which tell it to choose a color, draw a

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011963

line, fill an area, etc. The device uses line-generating algorithms to figure out which pixels are affected and changes the corresponding locations in the frame buffer to the appropriate value. The next time the frame buffer is read, this new information is displayed on the screen.

There is another way to draw a picture that will be considered in this paper; it is called scan conversion. A geometrical representation of the scene (i.e., a list of lines, polygons, etc.) is examined by testing the image at each pixel point to see if there is anything there. If there is, its color is determined and the value is put into the frame buffer directly. This is called sampling the image.

Because of decreasing memory and processor costs and the proven inexpensive television technology used, raster displays are becoming more popular. Other attractions are the realistic images, color, shading, and the ability to display a substantial amount of information. But the discrete quality of the device and the sampling process, along with low resolution, lead to poor image quality due to the attempt to represent continuous scenes with discrete points. It is important to solve this problem so that complex images, free from any inaccuracies can be presented on a raster device.

This paper will discuss the kinds of image defects that are produced by the discrete quality of a raster device and briefly list the proposed solutions. It will be shown that one of these, area sampling, is the most effective and logical solution. The paper will then explain the theory involved in this solution and present some algorithms used to implement the solution. Finally, there will be a discussion of the advantages, disadvantages, and possible future use of this technique.

II. Manifestations of the Sampling Problem

The defects due to the discrete quality of a raster display occur in a few distinct places: along edges on the silhouette of an object, a crease on a surface, or along a colored patch on a surface; in very small or thin objects; and in areas of complicated detail.[3] There are a few basic types of defects caused that are very apparents to a viewer.

The most obvious problem is that of jagged edges (or "the jaggies"). Since a raster device can only display dots in given positions, lines made of these dots have to follow a regular grid defined by the raster scan. This stair-step effect is most noticeable on edges that are nearly horizontal or nearly vertical (see Figure 1). Also, lines cannot be arbitrarily positioned but must start and end at dot positions.[4, 7]

Test pattern synthesized at a resolution of 256 samples by using techniques similar to those of conventional hidden-surface algorithms.

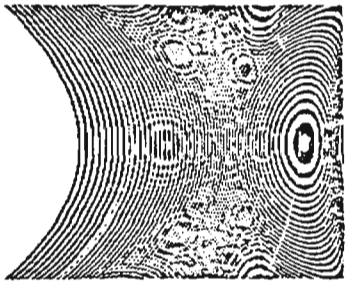


Figure 2: Moire Patterns (from reference [3])

Another general category of defects is the misrepresentation of details that are smaller than the size of a pixel. Small objects can "fall between the dots." This occurs because each dot on the image represents an infinitesimally small point in the scene being depicted. If the object is small enough, it is possible that none of it will fall on a sample point. A small object may disappear entirely; a long, thin object may appear in some places and not in others, looking like a barber pole; a very complicated object may lose some of its detail.[3]

Moiré patterns are produced in periodic images with closely spaced lines. The spaces in thin, broken lines and the jagged places in thicker lines are repeated from line to line with slight variations, causing patterns.[2, 3, 7] Figure 2 shows these patterns appearing in the raster image of closely spaced parabolic arcs.

In animated sequences of images, these problems become much more obvious and some additional problems appear. As slopes change, "armies of ants" appear to be running along the edges of objects as the edge detail changes. Small moving objects appear and disappear in successive frames. When they do appear, they are suddenly represented by a whole pixel, causing a distracting flashing, or scintillation. Slow-moving objects appear to change shape, due to the fact that the edges can only change positions in pixel increments and the edges change at different times. Since the object does not move smoothly, this is called crawling and it occurs only in animated sequences. A horizontal edge which looks fine in a still image will appear to jump from scan line to scan line as it moves vertically.[3, 7]

CID: 4011963

The next section of this paper will discuss proposed solutions to this problem, which are called anti-aliasing techniques for reasons that will be explained later.

III. Area Sampling as the Solution to Aliasing

A. Proposed Solutions

There are three basic techniques for improving the quality of raster display. The one that first comes to mind is to increase the resolution of the CRT. By increasing the number of scan lines and pixels per scan line, finer details can be represented and the "jaggies" are diminished. It can be shown that a "typical CRT" (17-inch diagonal screen screen viewed from 25 inches) would require 3,577 scan lines in order for the human eye to be unable to resolve the dots. Even at this resolution, some defects (such as scintillation) will still be visible unless the input is limited.[4] Today the highest resolution commonly available on a raster display is 1,024 lines, so it will probably take some time to develop a device with at least 3,577 lines. Since the computation time for most images is proportional to the square of the resolution, the cost of producing an image would be high and the picture generation time too long, especially in an interactive environment.[3,7].

The simplest and cheapest technique to get rid of the "jaggies" is to blur the image by actually defocusing the device or applying contour smoothing to the image after it has been computed. Although this does lessen the impact of the jagged edges, it does nothing to restore lost detail. As a matter of fact, the detail and sharpness that other techniques preserve is lost and the amount of information displayable is limited.[3,7]

A technique which is a combination of the first two is the wobbled raster. This is implemented by an addition to the deflection circuitry of the regular raster device. The wobbled raster actually doubles the horizontal and vertical resolution by quadrupling the number of dots per line and wobbling the beam one quarter of a scan-line width above and below the line twice as it scans across what was one pixel. Each scan line produces two consecutive lines simultaneously, offset by half a pixel width. Like the half-toning process used to produce continuous images in printing, the new pixels are aligned at angles, which tends to reduce the visibility of the basic dot structure. If all four new pixels are given the same color, the effect is the same as blurring the image.[9] While the idea of having all pixels the same distance from their neighbors is a good idea, using the wobbled raster as a solution to jagged lines seems contrived and has no advantage over the other two techniques.

The third and best technique is to make each sample point represent a finite area in the scene rather than an infinitesimal point. For example, a very small object would occupy a fraction of the small area that would correspond to a pixel on the output image. The color of that pixel would be computed as the sum of the colors of the object and background, weighted by their respective areas. In the simple black-and-white case, the intensity would just be the fraction of area the object occupies in the pixel.

This approach corresponds closely to what actually takes place in television picture reproduction. The television camera receives light reflected from a finite area to form the color for every dot. While the other techniques mentioned offer somewhat ad hoc solutions to the problem, this technique is based on sound principles and makes sense intuitively.[3] The remainder of this paper will go into more detail about this technique and will refer to it, in general, as area sampling.

B. The Theory of Area Sampling

1. General Introduction

The difference between sampling an image at points and area sampling is qualitative. Area sampling will always produce the same intensities at any translation of the image. In point sampling, the sum of all the intensities will vary as an image is translated. For example, a small object may appear in one scene and not in the next, depending on how it falls on the pixels.[2] A properly adjusted digital raster display consists of regularly spaced dots (the pixels) which overlap by around one half. Ideally, the intensity displayed at each pixel should represent the intensity and size of whatever in the scene is covered by the area of the dot on the screen. Most points in the image would contribute to the intensities of three or four pixels.[4]

A model of the display which is easier to understand and manipulate is what will be referred to as the simple filter. Represent each pixel as a square centered on the pixel center with the side equal to the distance between the centers of two adjacent pixels. This divides the scene into a rectangular grid. The intensity of the pixel is proportional to that area of the pixel which is covered by an object. That is, the intensity

of the the pixel is the average visible intensity of the scene over the square area. If a color display is used, the pixel color is the sum of the colors of all the objects in the square weighted by their areas.[2]

Using this method, one can represent smooth and arbitrarily positioned lines and edges and small objects of any size and in any position. Varying intensity levels create the appearance of details lying between pixel positions (sub-pixel details). To see this, consider a small object the size of a pixel. This spot can be made to appear to be moving smoothly across the screen from pixel to pixel by dimming one pixel while brightening the one next to it. Adjacent pixels at half intensity will give the appearance that the object is lying between them.

Similarly, varying intensity levels allow nearly horizontal or nearly vertical lines to appear smooth instead of jagged. On a raster display, a line of pixel width which is more horizontal than vertical (i.e., the slope is less than 1) will be represented by one pixel per column at full intensity by a regular digital vector generator. Using the simple filter, one can see that the line will actually cross two or three pixels per column. If these pixels are intensified proportionally to the area the line occupies over each of them, the line appears smooth. Figure 3 illustrates the application of the simple filter to a line. While the lines represented this way are thicker and not as sharply defined as their jagged counterparts, their apparent positions are actually more accurate since they are derived implicitly from their environment rather than being set explicitly by the display device.[4]

2. Aliasing and Rastering

Having the value of each pixel represent a finite area instead of a point has the effect of applying a convolutional filter to the scene before it is sampled.[3] For the present, filtering can be thought of as blurring the scene before it is point-sampled.[5] By producing "blurred" images, we have shown that greater precision is possible. This is true only because the sharp images produced by displays without using varying intensities, or gray scale, contain inherent inaccuracies.[4]

In the field of signals processing, it is well known that a signal cannot be faithfully reproduced from digital samples if the sampling frequency is less than twice the highest frequency in the signal. In terms of reproducing a scene on the graphics device, the signal is the mathematical model of the scene to be displayed. A faithful reproduction of that scene on a graphics device is one which contains just as much detail and accuracy as the original scene, without any added information. For us to make a faithful reproduction of a scene, the scene cannot change more frequently than once per sample point. If this is not the case, an image with less detail than the original scene will be produced. This is called an alias of the scene, and aliasing refers to the defects produced. For example, highly periodic scenes, such as a picket fence, may appear as a few broad stripes instead of as many thin lines if these lines occur more than once every two sample points. Convolving a scene with a two-dimensional filter is done to ensure that the high frequencies in the scene do not exceed one-half the sampling rate. Techniques which attempt to reduce the effects of aliasing are methods of anti-aliasing.[3]

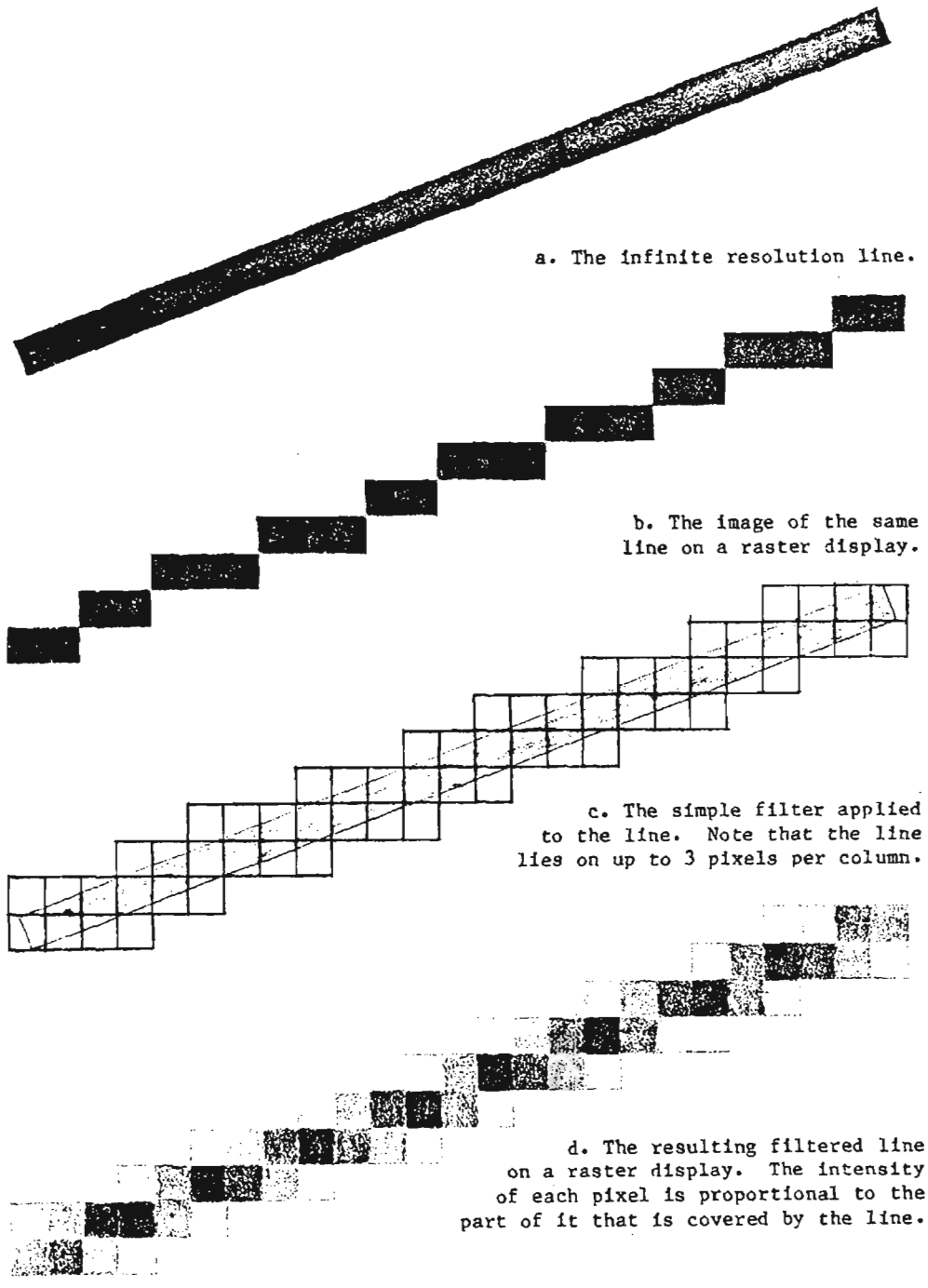
Aliasing is the consequence of improper filtering of a scene before it is sampled. Another term, rastering, is also used to refer to the defects described above, but actually it is a result of improper filtering of the image during reconstruction on the device, rather than at construction. Rastering appears as "ghosts" of the original image, since the pixels are not being displayed as intended. If the beam is not properly focused, the results are due to rastering as are the dark lines that may appear between scan lines. If aliasing can be thought of as getting less information than intended, rastering can be thought of as getting extraneous information that did not exist in the original scene.[3, 7]

3. Filtering

It has been said that aliasing is caused by neglecting to filter a scene before sampling it and that the cure, making each sample represent a finite area, has the effect of applying a filter to the scene. Now a more detailed definition of filtering is needed.

Filtering is an averaging process; the intensity of a pixel is determined by the scene within a small distance of the pixel center, not at a single point. This averaging is what eliminates the "high frequencies" that cause aliasing. Filtering is controlled by a filtering function, which supplies a weighting function for the averaging process. Convolution by a function just refers to this weighting process. The filter function describes the distribution of light emitted by a pixel on the display. Typically, a pixel is brightest at the center and decreases in intensity rapidly in all directions away from the center. Filter functions do not have to match

CID: 4011963



a. The infinite resolution line.

b. The image of the same line on a raster display.

c. The simple filter applied to the line. Note that the line lies on up to 3 pixels per column.

d. The resulting filtered line on a raster display. The intensity of each pixel is proportional to the part of it that is covered by the line.

Figure 3: Applying the Simple Filter to a Line

DOCID: 4011963

the light emission properties of a display device exactly. Usually functions are chosen that are easy to manipulate, and their parameters are varied until the image looks good.[6]

While the difference between area sampling and point sampling is qualitative, the difference between the simple filter and better, more complex ones is quantitative. Most good filters will integrate the intensities in a small area around the pixel center; as resolution increases, all filters produce the same image.[2] The filter function is usually only non-zero in a small area around the pixel. The width of the filter corresponds to the diameter of the area to be sampled. Wider filters are lower-pass filters, which sample a larger area and tend to blur the image. Narrow filters sample a small area and tend to undersample. Point sampling can be thought of as an infinitesimally narrow filter.

The shape of a filter determines the relative weights assigned to various points in the small area. Flat filters, such as the simple filter described above, weight all points in the area equally and are lower-pass filters. Most good filters are circularly symmetrical, weighted more heavily at the center and falling to zero at the perimeter. These filters approximate the pixel's intensity distribution. Filters that are weighted very heavily in the center and fall off rapidly will cancel the blurring effect of a wide filter. As long as filters have the same width and the same general shape, the results are not noticeably different.[10]

The simple filter is equivalent to convolving the scene with a "box" function; it is a flat filter with a width equal to the distance between pixels but is not circularly symmetrical.[2] The most popular filters are the simple filter (used for its simple representatin of pixels) and a roughly conical filter about one-and-a-half to two times as wide as the distance between pixels (used to more accurately approximate the pixel's properties and to take advantage of circular symmetry).

4. An Added Benefit: Increased Resolution

There is an interesting result of the anti-aliasing technnique of using gray scale levels to represent a scene. Not only does it achieve its goal of eliminating the effects of aliasing, it also results in a noticeable gain in resolution. This also occurs in the half-toning process, which is just the opposite of the anti-aliasing method described above. While anti-aliasing converts size into various intensities, half-toning converts intensities into different sizes of dots. In newspapers these dots are all printed in black, but the image produced appears to be continuous and to possess gray scale. This is because the dots are small enough to be point sources.

When looking at a point source, the human eye does not distinguish between the dot's size and its intensity, even though one could resolve the dots by looking more closely. This means that the resolution at which dots become point sources is less (i.e., fewer dots per inch) than the resolving power of the eye. For good-quality half-toning, that resolution is between 85 and 133 dots per inch. A picture with 100 dots per inch held at distance of one foot corresponds to 480 scan lines on our "typical CRT." Experiments have shown that for this screen size at average brightness, 440 lines is the minimum resolution for which size and intensity of dots are interchangeable. This figure agrees well with one derived from the half-toning analogy.

Since in a point, source intensity and size are equivalent, subpixel details can be represented using varying intensities. Therefore, the "effective" resolution of a display using anti-aliasing will be greater than the pixel resolution. For example, consider a large object with its left edge overlapping a column of pixels by one half. The pixels in that column will be calculated at one-half full intensity, while the ones to the left of the column will be at zero intensity and those to the right at full intensity. Studies have shown that the brain reacts to this image the same as it does to an infinite-resolution picture of the same edge. Therefore subpixel positioning of the edge can be represented by using varying intensities. Furthermore, changing the intensity of the intermediate column of pixels is interpreted as a corresponding movement of the edge.

The effective resolution of a display is determined not only by the number of pixels but also by the number of the differentiable intensity levels the device is capable of producing. Factors such as room lighting, phosphor characteristics, spot size, and screen reflectivity all determine the eye's ability to distinguish one intensity from another. The device itself may be limited in the number and range of intensities it can display. The ratio of the brightest to the dimmest intensities displayable on our "typical CRT" is about 25 to 1. Using this figure and the fact that on the same CRT the eye can distinguish a 4% difference in the intensities for single spots, the number of levels needed is 83. These levels are on an exponential scale, each intensity a 4% increase over the previous one.[7] When looking at large areas of varying intensity, though, the eye is able to distinguish a 2% difference, which implies 162 levels, also on an exponential scale. But in

CID: 4011963

order to properly represent spot positions, for example, two spots at half intensity should have the same brightness as one at full intensity. In this case a linear scale, in which each intensity differs from the previous one by a fixed amount, would be more useful. Since this concern is more important than distinguishable levels, the linear scale is the most common kind.[4] The 83 exponential levels would translate into 628 linear levels. Studies have shown, however, that 256 levels are sufficient with only a little roughness in variation noticeable in the low intensities.[7]

One way to look at these 256 levels is as follows: Divide each pixel into a 16-by-16 grid, forming 256 "subpixels." Then, using the 256 intensities to represent lighting from none to all of these subpixels results in a factor of 16 increase in the "effective" resolution of the device. A 512-line CRT would have an effective resolution of 8,192 lines, but since only around 3,600 can be resolved, less than half of that would be "usable." Of course this is not real resolution, but it is perceptually equivalent. Objects as small as one-256th the size of a pixel can be represented, and objects can be positioned to one-sixteenth pixel precision. It should be noted that the 256 intensity levels require eight bits of memory per pixel, and for a full-color display one would need three times this much.[7] Some successful anti-aliasing schemes use only 16 intensity levels, but even with this amount, 12 bits are needed per pixel. All combinations of the colors available are needed to accurately render any pixel, so it appears that using anti-aliasing on a device which uses a color lookup table would be difficult. Most of the colors needed for the table would be implicitly determined by a few explicitly chosen colors. (See Section IV.C).

We have shown that the anti-aliasing technique of area sampling an image eliminates the effects of aliasing and also allows,to some extent, the representation of detail finer than the resolution of the display and a corresponding increase imprecision. The next section of this paper will show how this theory is applied to a general scene and then how problems in specific areas can be eliminated with simpler, but perhaps not as accurate, techniques.

IV. Applications of Anti-Aliasing

A. The General Case

The general case that anti-aliasing will be applied to is that of a fully described, or modeled, three-dimensional scene of solid objects. Each object is modeled as a polyhedron, each face of which is a polygon. By increasing the number of faces, a polyhedron can be constructed to approximate any solid object. Since a polyhedron is described by a relatively small number of vertices, it is easy to represent and manipulate mathematically. In translation, rotattion and scaling, the primary parts of a polyhedron (points, lines, and planes) all retain their properties. Any scene to be depicted is thus a list of these geometric objects with information about their positions and colors.[8]

Techniques for achieving realism in three-dimensional raster graphics are mostly concerned with how to restore the information about the third dimension to the images. These include projections, shading, and hidden surface removal (removal of hidden parts from images of solid objects). In recent years, these techniques, especially hidden surface removal, have improved dramatically. Recently developed hardware processors for hidden surface removal can create images at 30 frames per second, fast enough for real-time applications. Unfortunately, anti-aliasing techniques have not progressed as rapidly. Most techniques are "ad hoc" ones to remove the most obvious effects of aliasing, such as

A computer-generated image of a teapot with simulated specular reflections of light entering through a window. *Courtesy University of Utah.*

Figure 4: Shaded Image with Jagged Edges (from reference [8])

jagged lines.[2, 8] How realistic is an image of a shaded object that has a smoothly curved and shaded surface, if the edges appear jagged? For an example of this contrast, see Figure 4 (which originally appeared in reference [8]).

1. Hidden Surface Removal

To properly solve the aliasing problem in the general case, one must find solutions to both the hidden-surface problem and the filtering problem. That is, for each pixel one must implement a hidden-surface algorithm to find out what is visible in that pixel and

DOCID: 4011963

then use the filter function to determine the resulting intensity. A "simple-minded" anti-aliasing algorithm would not properly take into account what is visible. For example, if it just summed the intensities of all the objects falling on a pixel, a completely hidden color might contribute significantly to a pixel. Errors like these are quite visible, even though they may occur in an area one-millionth of the screen area.[2]

When implementing hidden-surface algorithms with anti-aliasing, it saves time to find the places where aliasing is likely to occur, such as polygon edges, silhouettes, and creases and to restrict the time-consuming filtering process to these places. When approximating a curved surface with a polyhedron, the shading techniques used to give the polyhedron the appearance of a smooth surface make anti-aliasing unnecessary at the polygon boundaries on these surfaces.[3]

Most hidden-surface algorithms are applied after a scene is transformed into a two-dimensional image. This image is a list of overlapping polygons with a certain depth or priority associated with them.[8] The algorithms are separated into two basic types: depth algorithms and scanning algorithms. Depth algorithms process each polygon separately and determine the color of a pixel by the color of the closest polygon falling on that pixel. Scanning algorithms generate the image scan line by scan line by keeping a list of all polygons falling on that line. Scanning algorithms are the most usable ones with anti-aliasing, since all the information needed is available; i.e., all visible surfaces in the neighborhood of a sample point. The depth algorithms do not recognize or keep track of any relationships between polygons. Using this kind of algorithm would require pointers to neighboring polygons and keeping track of the edges and their amount of contribution to a sample point.[3]

2. Algorithms

This section gives two different examples of algorithms for hidden-surface removal with anti-aliasing. In both cases, the input to the algorithm is a list of two-dimensional polygons with their associated priorities and colors.

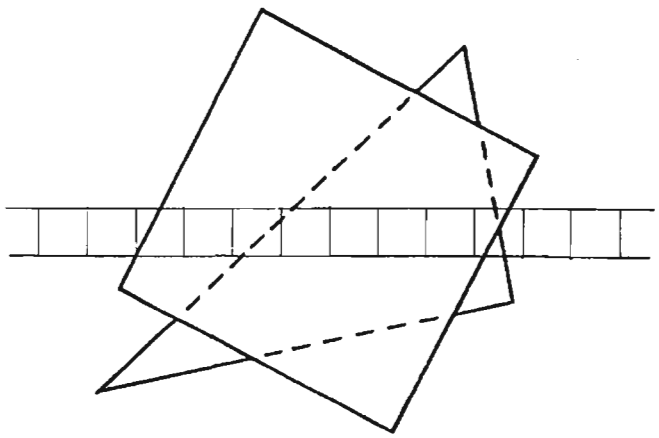
a. Example 1: Scanning Hidden-Surface Algorithm

The first algorithm is described by Catmull.[2] It uses the simple filter and a scanning hidden-surface algorithm. Basically, it performs a hidden-surface algorithm at every pixel and then integrates the intensities. Everything needed for anti-aliasing is provided to much more precision than is available to the display. This precision is only limited by the computer running the algorithm. Finding which pieces of polygons are visible is like the original hidden-surface algorithm, except that there are two simplifications. First, we are interested only in the sum of the intensities of each piece weighted by its area, and not in the exact coordinates of the vertices. Second, much of the work in sorting the polygons has already been done in the higher-level hidden-surface algorithm.

The basic algorithm follows, and a simple illustration is given in Figure 5. A more detailed description can be found in reference [2]. There is an active polygon list which is a list of all polygons in the current scan line. Polygons are added to and deleted from this list as necessary as each scan line is processed. For each scan line, set the pixels to background color. Each pixel has a "bucket," which is a list of all polygon pieces which fall on it. Clip each polygon in the active polygon list to the part which falls on the scan line. What is left is a list of very narrow polygons. For efficiency, clip these polygons into three sections: a piece in the center, which is all solid pixels, and the two irregularly shaped pieces on either side of it. Sort these pieces into the buckets by the X coordinate of the leftmost pixel in the piece. For every pixel in the scan line, sort the pieces in the bucket by priority, putting a solid piece of background color last. If the first piece is a solid piece, put its color into the pixel. If it is an irregular piece in front of a solid piece, find its area and use it to weight the two colors. In any other case, the first two pieces are irregular and a special hidden-surface algorithm, called the pixel integrator, is used.

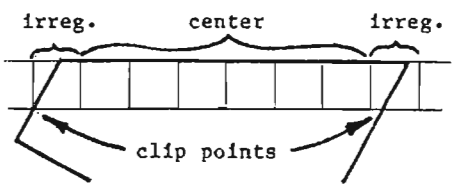
The pixel integrator is like the polygon subdivision algorithm, which will be discussed in the next example. This algorithm is entered with a list of polygons in sorted order. An edge of the first polygon is selected as a dividing edge, and every polygon in the list is clipped against that edge. Two lists are formed, one for the polygon pieces lying to one side of the edge and another for the other side. If the algorithm is recursively applied to both of the resulting lists, then very shortly the first polygon in each list will cover all the ones behind it since everything else has been clipped away and is in another list. The area of this polygon can be found, the color of the polygon is weighted by it, and the result is returned. The sum of these weighted intensities from all the lists (one for each visible polygon) gives the final average intensity for the pixel.

CID: 4011963

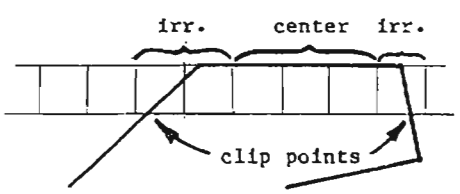


The scene is a red square on top of a green triangle.
The current scan line is superimposed over the scene.

Red Polygon



Green Polygon



Clipping the polygons to the scan line
and dividing them into irregular and center pieces

For the first pixel, an irregular piece is in front of a solid pixel, so the pixel's area is used to weight red with the background color.
For the middle pixels, the first piece is a solid piece, so the pixels' colors are all red.
For the last pixel, the first two pixels are irregular pieces, so call the pixel integrator to return the pixel's color, which will be a weighted sum of red, green, and the background color.

Figure 5: Scanning Hidden-Surface Algorithm with Anti-Aliasing

DOCID: 4011963

b. Example 2: Polygon Area Sorting Algorithm

The second algorithm is described by Feibush, Levoy, and Cook.[5] It uses a newly developed hidden-surface algorithm called the polygon area sorting algorithm, which is based on the polygon subdivision algorithm. The polygon subdivision algorithm clips all polygons against the ones in front of them and discards the covered parts, so that the final output of the algorithm is a list of polygons which do not overlap, somewhat like a jigsaw puzzle representation of the scene.[8] The pixel integrator described above is similar to this, but is just concerned with the polygons' areas and not with their vertices. Figure 6 illustrates an example of the algorithm in the particular case of the pixel integrator.

The basic hidden-surface algorithm is as follows: Polygons are a list of vertices, with the edges between them marked as "clipped" or "unclipped." Find the first unclipped edge in the closest polygon in the list. If there is only one polygon in the list, or if there is no unclipped edge, return the polygon as is. Otherwise, clip all polygons in the list against that edge and put them into two lists, one for parts on each side of the edge. Set the clip flag for the clipped edge to "clipped." Reenter the algorithm for each of these two lists, combine the two resultant lists of polygons, and return this list. The final result will be a list of all visible parts of polygons.[2]

After this list is constructed, it is a relatively straightforward, but involved, matter to do the anti-aliasing. This algorithm uses a conical filter and keeps a lookup table to store the volumes above selected right triangles in the sample area, one vertex of which is the pixel center. A complicated computation finally results in the volume above any of the polygon pieces in a sample area, which is the weight for the color. The results from each polygon in a sample area are added together to get the final result. An advantage of using lookup tables is that the filter function can be changed easily by just changing the values in the table.

The same paper gives a method for anti-aliased texturing of the interiors of polygons. Texture is defined as a rectangular array of points with varying intensities. These points give the appearance of roughness or patterning to a polygon. For any visible polygon to be textured, all pixels that it falls on are mapped onto the texture definition. All texture points in the pixels are translated back to the image, and the value of each pixel is determined by weighting the points with the same filter used in the rest of the algorithm.

B. Algorithms for Specific Cases

The algorithms above are used to solve the aliasing problem in the general case, which is any scene (no matter how complicated) that has been completely described before the algorithm is applied. These algorithms just send the image to the device as a list of colors, one for each pixel. This is very useful for real-time applications, such as flight simulation, where the entire scene is known beforehand. But this is not always the case. The graphics device is commonly used as an interactive device, with the user adding, changing, and deleting objects to create the final image. He is really drawing on the screen, and each new piece being drawn is considered to be independent from what is already on the screen.

In these cases, there probably is neither the need nor the money available for a system that keeps track of everything drawn and which essentially recomputes the image every time the screeen is redrawn. (This technique is called real-time conversion and is similar to what happens in calligraphic devices.) What is needed is a set of anti-aliasing algorithms that are specific to the elementary pieces that make up a scene, such as lines, polygons, and text. While these algorithms will be simpler and faster than the general-case ones, they will also be less accurate, especially when two or more pieces interact, since the relationships between pieces is not known. They have been described as "ad hoc" techniques, but sometimes they are the most feasible ones and their results are acceptable for most real-life applications. These applications are probably not concerned with shading, texturing, shadows, and reflections. They deal with simple objects and need fast responses.

This section will describe a few algorithms that are designed specifically to treat aliasing problems in these elementary pieces. The effectiveness of these algorithms can be seen in the illustrations in the articles mentioned. A few of these illustrations have been included in this paper, but because of the various reproduction processes used, their quality is not representative of the results seen directly on the displays.

1. Lines, Curves, and Polygons

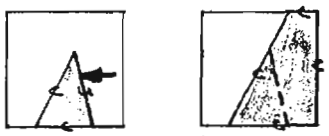
Lines, curves, and polygon edges will all be treated as the same case. In most graphics applications, curves are approximated by a set of points connected by short line segments. Polygon edges will be seen as an extension of the case for lines. A faster algorithm specifically for drawing anti-aliased lines

CID: 4011963

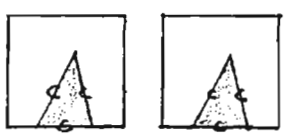
The list of polygons, the topmost on the left, which is the input to the first level of the algorithm. The edges are marked "u" or "c" for unclipped or clipped. The arrow points to the chosen unclipped edge.

Polygons lying to the left of the clipping edge. Input to a second level of the algorithm.

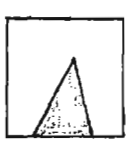
There are no unclipped edges in the first polygon, so it or its color value is returned to the main level of the algorithm.



Polygons lying to the right of the clipping edge. Input to a second level of the algorithm.



Polygons lying to the left of the edge. Input to third level.



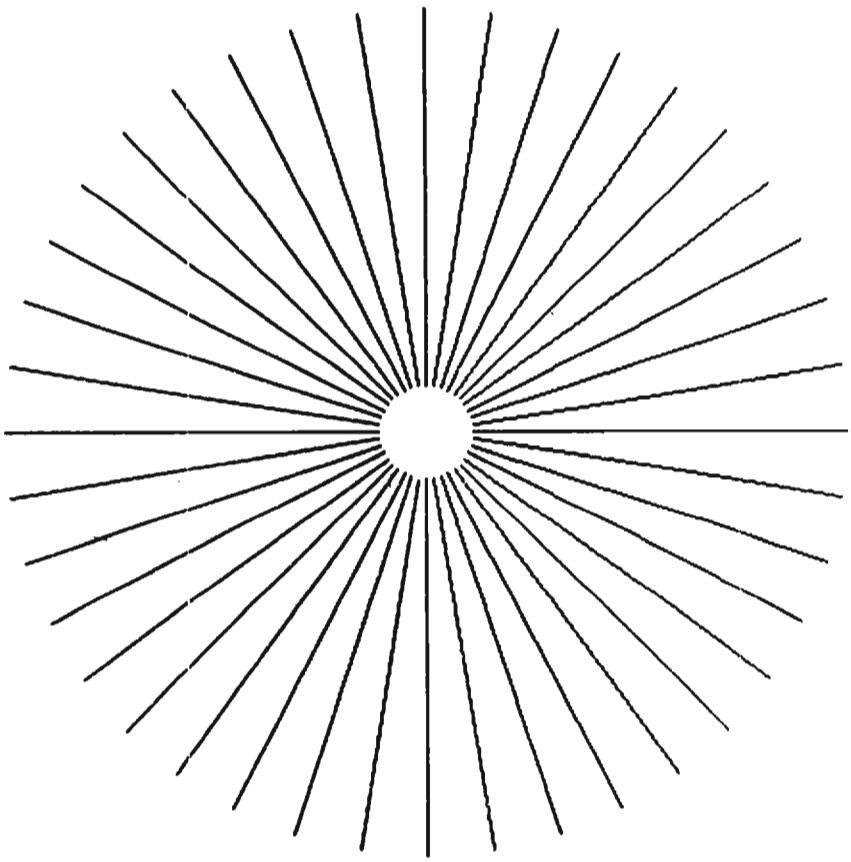
Same for the right side.

There are no unclipped edges in either list, so these polygons or their color values are returned to the second level, which combines them and returns the result to the main level of the algorithm.

The main level of the algorithm combines the results from the two second level algorithms and returns the final list of non-overlapping polygons, or a color value which is the sum of the colors of the polygons weighted by area.

Figure 6: Pixel Integrator (or Polygon Subdivision Algorithm)

DOCID: 4011963



The lines on the right are normal.
The lines on the left are anti-aliased.

Figure 7: Comparison of Jagged and Anti-Aliased Lines

OCID: 4011963

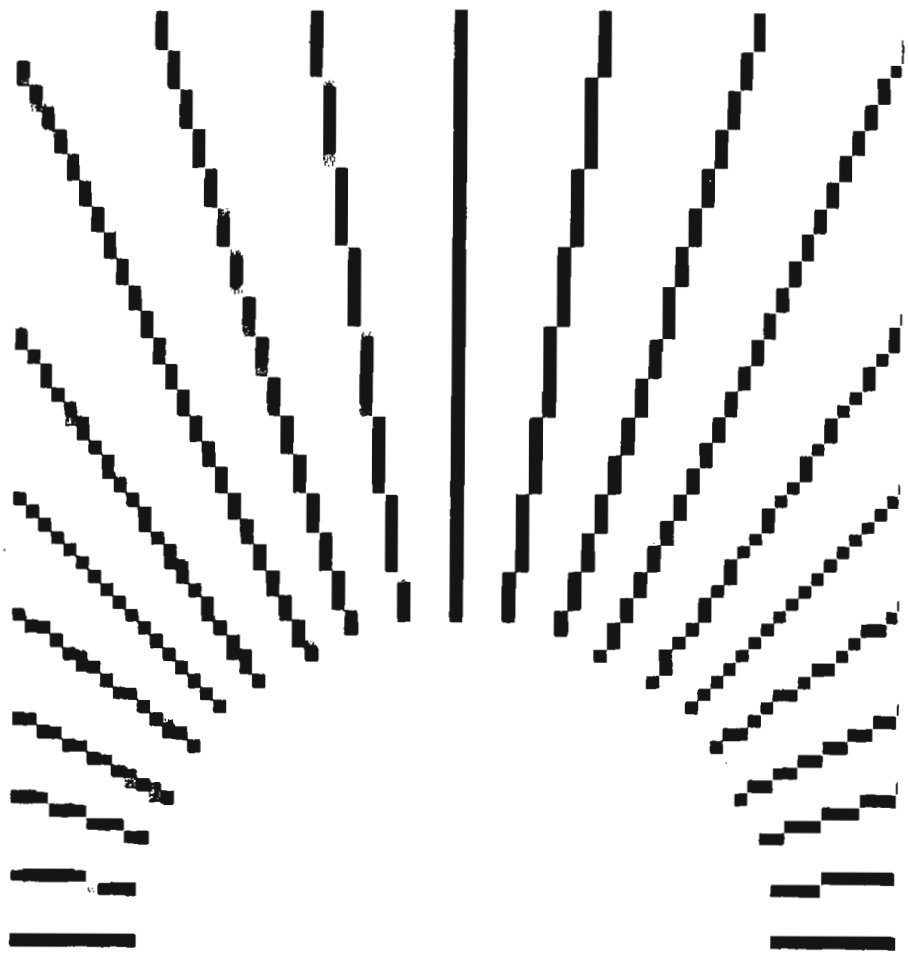


Figure 8: Enlargement of Figure 7 to Show Pixel Intensities

OCID: 4011963

takes advantage of the "spatial coherence" of lines. That is, given a small part of a line, the remainder of it can be easily extrapolated. If the representation of a line on one scan line is known, changing it incrementally will provide its representation on the next scan line.[4]

a. Example 1: Bresenham's Algorithm with Anti-Aliasing

The following algorithms for drawing anti-aliased lines can be used to draw them directly onto the screen (or actually into the frame buffer) and is an extension of Bresenham's algorithm, a commonly used technique for drawing lines on raster devices. It is described in full detail by Gupta and Sproull.[6] This algorithm uses table lookup to reduce the computation of intensity levels, and variations can be used to draw lines of varying thicknesses and to smooth the edges of polygons. Figure 7 compares the lines drawn with an implementation of this algorithm to jagged lines and Figure 8 is an enlargement of the same image showing the different intensities.

The basic idea of the algorithm follows: The filter used is a conical function which has its maximum value at the center of the pixel and decreases linearly to zero at a distance of one, in units of pixel-to-pixel distance, from the pixel center. The function is such that the volume of the cone is also 1. When a line passes through a pixel, the pixel's intensity should be proprotional to the volume of the cone intersected by the line. Because the cone is circularly symmetrical, this depends only on the line's width and the perpendicular distance from the pixel to the line. Lookup tables, which have these volumes listed for certain distances from point to line, can be constructed for any line width. The precision of these tables depends on how many intensity levels are desired.

The discussion of the algorithm is restricted to lines of unit thickness in the first octant (i.e., the slope is positive but no greater than 1). These lines intersect two or three pixels in each column of pixels. The algorithm keeps track of the location of the pixel that the center of the line passes through, the center pixel, and the perpendicular distance from the center of that pixel to the line. At each column the center pixel and the pixels above and below it are shaded according to their perpendicular distances from the line, which are easily calculated from the that of the center pixel. These distances point to intensity values in a lookup table. Then the center pixel for the next column is found and the new perpendicular distance is calculated.

Endpoints have to be treated differently. A separate lookup table has intensities for the six pixels that are affected by an endpoint, the three in the endpoint's column and the three adjacent to them. Since these values vary with the line's slope, the slope is the index into this table. Extending this algorithm to lines of all slopes is just a matter of switching the roles of the X and Y coordinates for slopes greater than 1, and of replacing the Y coordinate with its negative for negative slopes.

The variations on this algorithm make it a very useful one. Lines of different thicknesses can be produced by calculating separate lookup tables for various thicknesses and choosing the appropriate one. The algorithm may have to be modified so that it intensifies more than three pixels per column. Similarly, the endpoint table for each thickness will have to have more than six pixels per endpoint. Different endpoint shapes, such as rounded or beveled instead of squared-off, can be accommodated with different endpoint tables. Polygon edges can be produced with a table which contains intensities based on how much of a pixel is covered by an edge.

Different filters, needed for different output devices, can be accommodated by lookup tables. As in the case of thicker lines, the algorithm may have to intensify more than three pixels per column. If these filters are not circularly symmetrical, though, a second parameter, slope, is needed to select the correct lookup table.

Any background shade and any line shade can be used by mixing the intensities. The same applies to colors; the red, green, and blue components are mixed independently.

Endpoints need not be at pixel centers. Precise endpoints are needed to avoid problems in repetitive patterns where the endpoints should appear to be aligned.[4] They are also needed to allow smooth motion in moving lines. Subpixel precision endpoints are a problem because their accurate rendering requires either many lookup tables or a lot of computation.

b. Example 2: Filtering Tiler

Crow [3] describes a tiler with anti-aliasing. A tiler is a procedure which generates the individual pixels which form a solid polygon from a list of the polygon's vertices. This tiler has no hidden-surface removal; it just draws a convex polygon with anti-aliased edges. This kind of tiler is needed because if the polygon's border were drawn first as anti-aliased lines, a hardware fill of the area would not work. Hardly any

CID: 4011963

of the pixels making up the border would be the same color as the polygon interior so the tiler wouldn't know when to stop, unless it were "smart" enough to recognize different intensities of the same color.

A filtering tiler differs from a conventional one in that it must keep track of the edges that fall on a given scan line, and edges that are very short or nearly vertical cannot be ignored. The algorithm is straightforward and uses the simple filter. Lists are kept, one of the edges on the left side of the polygon that intersect the current scan line and another for those on the right side. Starting at the top vertex, the polygon is created, scan line by scan line, until the bottom vertex is reached. At each scan line the edge lists are updated. Starting at the left side, the intensities of the pixels that hold irregular pieces are calculated by going through the list of the left edges and adding the weighted area on the right of that edge to the corresponding pixels it intersects. It does the same for the right side, but subtracts the weighted area to the right, to correctly render objects thinner than a pixel. It then fills in the middle of the scan line. Crow notes that this algorithm takes from two to five times longer than an ordinary tiler, depending on the number of edges.

c. Intersections

In a typical drawing, lines and polygons are not isolated. They meet, intersect, and overlap. When two objects affect the same pixel, a rule is needed to determine the ruling intensity. The simplest method is to just overwrite the old intensity. However, this will cause gaps in earlier objects where they are overwritten by dimmer pixels from later objects. Ideally, the intensity should be based on the areas occupied by the two objects. But this is not practical, since it would require information about the relationship between the objects, such as whether or not they overlap. A compromise is to sum the intensities, making sure that the sum does not exceed the maximum possible intensity. This can lead to the problems of colors showing through solid objects and of two dim lines intersecting in a bright spot, which happens on a calligraphic display. If the frame buffer does not have have a readback capability, these methods are not even possible. That is, if the previous intensity of the pixel cannot be found out, no sum or comparison can be made.[4]

2. Characters

Another important part of graphics image is text. Dot matrix characters look fine rotated in increments of 90°, and scaled or translated at pixel increments, but otherwise the results are terrible.[4] Other techniques for representing characters, such as high-resolution bitmaps (similar to dot matrices), or as curved outlines which are treated as filled polygons, or as a set of "strokes" (lines), work fine on high-resolution devices. But at low resolutions the characters are bad representations because they are undersampled. Usually the low-resolution matrices have to be constructed by hand.[10]

Warnock has addressed this problem.[10] The motivation for developing his technique was a need to represent high-quality text for a graphics application used to design page layouts. A technical article may have as many as 30 different fonts. The page layout must accurately represent the styles and shapes of the fonts that will appear on the final copy. The spacing, layout, and appearance are all very important. The requirements for character sets for use with a low-resolution raster display are:

- [] they must be faithful to the masters, even at low resolution;
- [] they must be free of aliasing, that is, no holes, dark spots, or blurring;
- [] they should look properly spaced regardless of the display's resolution.

The method is to make a high-resolution black-and-white representation, or bitmap, of the character and to sample areas of it for each pixel. The area sampled depends on the size of the character to be drawn and the width of the filter. The bits that are turned on in the sampling area are weighted by a filter matrix, which has values in it corresponding to the values of the filter function at these points. The sum of these is the intensity for that pixel. Like the line-drawing algorithm, the filter can be changed by changing the matrix values. When two characters affect the same pixel, the intensities are added, since the characters are known to overlap.

Using only 16 intensity levels and filter similar to the one in the line-drawing algorithm, the results are very impressive. Text of only five pixels high was readable by content, six pitch was sufficient to recognize letters, and at seven pixels the text was perfectly readable. The characters produced are more faithful to their masters than directly sampled ones, there are many fonts available, and the characters can be rotated and placed to subpixel precision. Very small fonts can be used for thumbnail layouts to get the feel of the page, even though the text may not be readable. Figure 9 contains some of the illustrations from the paper, showing a comparison of non-filtered and filtered

DOCID: 4011963

characters, rotated characters in various fonts, and an enlargement of a character.

C. Hardware with Anti-Aliasing Features

Several algorithms have been devised to eliminate the effects of aliasing in specific areas. The ones mentioned above are just a few examples of them. They have been written to coincide with the hardware implementations of their ordinary counterparts. This section will look at a commercially produced display device, the AED767, which has some anti-aliasing features. The only information available about this device is a product review from August, 1981 [1] so this discussion is not very complete or up-to-date, but it will give something of an idea of what the situation is currently. The review says that this device is the first raster graphics device produced that has "anti-aliased vector generation in the terminal hardware/firmware."

The AED is an enlargement of the AED512, an earlier color raster device. It has a resolution of 575 lines, with 768 pixels per line. There are a maximum of eight bits of information per pixel, which point into a color lookup table which holds 256 entries. The anti-aliasing feature can be turned on or off. When it is turned on, vectors can be drawn in 16 programmable base colors, each of which has 16 intensities. The algorithm used is probably much like the one described in this paper. The 16 intensities correspond to a quadrupling in effective resolution to 2,300 lines, which may be enough for effective anti-aliasing, since the screen size is smaller than our "typical CRTs."

The review states that "intersecting vectors [are] accurately rendered by a proprietary technique." The device has a readback capability from the color lookup table, which implies that the proprietary technique probably consists of choosing the maximum of the two values. In order to represent every possible mixing of any two base colors, many more colors than the 256 available (29,056 to be exact) would be required. It is doubtful that they are using a technique which somehow represents each pixel by a list of color lookup table entries which it sums upon scanning to compute the beam intensities.

The review does not mention filled polygon edges, so it is assumed that they will still have jagged edges. (See Section IV.B.1.b above about the problems with hardware fills to anti-aliased edges.) The contrast between jagged polygon edges and smooth lines may be distracting. The limitation the color lookup table poses on the accurate rendering of intersections is unfortunate. The lines can still only strart and end at pixel precision. All of these facts lead one to question the benefit derived from using a device that only does the job half-way.

V. The Costs and Future Use of Anti-Aliasing

It has been shown that using area sampling to generate gray-scale images is an effective technique for eliminating the effects of aliasing on raster display devices. It also has the added benefit of increasing the effective resolution of the display device. To balance these advantages, there are some problems with the technique which will be described below, along with the solutions to them.

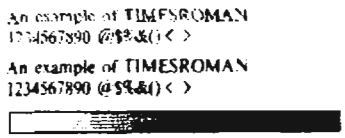
One problem is that a loss of acuity is apparent. A field of small objects appears as a solid gray mass instead of individual objects. Actually, in this case the eye would not be able to resolve the objects either, and that is how it would appear to the eye also.[7] The only problem would arise if the viewer got closer to the screen and expected to see more detail.

Another problem is non-linearity. Two pixels at half intensity should have the same total brightness as one pixel at full intensity. Non-linearity in the phosphor, digital-to-analaog converters, or any other transformation the calculated intensities go through before they are displayed may contribute to the problem, which makes lines look "barber-poled." Techniques which involve getting new intensities from compensation tables have been developed to compensate for the non-linearities.[7, 10]

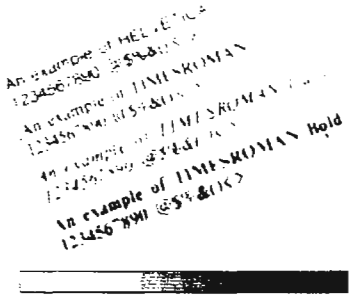
Rastering is still a problem. Unless the display is properly adjusted, the dark lines between scan lines will be easily visible. Hardware techniques, such as the wobbled raster or more complicated interlacing schemes are used to reduce the line structure. In color CRTs the effect is not as bad since each pixel is represented by three spots instead of one.[7]

The most serious problem with anti-aliasing techniques is that they are time-consuming. The hidden-surface algorithm with anti-aliasing runs three times slower than a regular hidden-surface algorithm.[2] Even in the case of the line-drawing algorithm, three times as many pixels per column are intensified, and the computation for each pixel is more complicated. There is also the higher cost of the hardware needed to implement varying intensities and the cost of the memory to store several bits of information per pixel.[4]

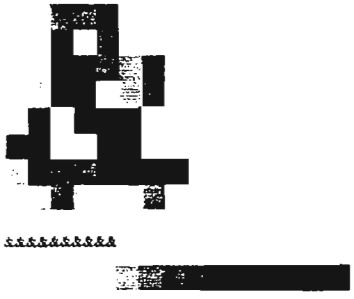
CID: 4011963



Comparison of directly sampled black and white text and filtered gray scale text. The font is 8 pixels high.



Examples of rotated text in various fonts, 8 pixels high.



An enlarged "&" showing grayscale values, and a row of the same character as it appears on the screen.

Figure 9: Anti-Aliased Characters (from reference [10])

DOCID: 4011963

~~FOR OFFICIAL USE ONLY~~

One way to reduce the time factor is to put the anti-aliasing capability under user control. A rough sketch of the image can be constructed without using anti-aliasing, since the preliminary sketching is probably the longest part of the job. Once the final image is constructed, the anti-aliasing can be turned on and a high-quality image can be produced. The algorithms which use lookup tables avoid the complex filtering computations and reduce time considerably. Also, the techniques for specific cases are less time-consuming because information about the structure of the object is used.

As more display terminals contain their own micro-processors instead of hardwired logic, it seems reasonable that the complexity of the operations performed in the terminal itself will increase. An implementation of these specific algorithms in a processor would not be very expensive. With the advances being made in the speed and computing power of these processors, there is every reason to think that anti-aliasing will soon be a "universally available" feature in raster display terminals.[4]

The VLSI (Very Large Scale Integration) technology has already been used in a computer graphics design and the result is an increase in speed of image generation by a factor of 1,000. This is because many operations are performed at the same time, instead of sequentially. Currently raster graphics systems which produce full-color shaded images in real time have a smaller capacity for manipulating images with many edges than a calligraphic system and cost much more. A system has already been devised, using the VLSI technology, for producing real-time anti-aliased movement in two dimensions. Soon it may be possible to produce completely anti-aliased real-time raster images with as much detail as a calligraphic system, with the added benefits of color and shading.[11]

VI. Conclusions

In view of the technology that is commonly available today, the main factors governing the decision of whether or not to use anti-aliasing are the higher cost of hardware and the slower image generation time versus the low quality of raster images due to misrepresentation of detail. But anti-aliasing need not be as time-consuming as it is thought to be. A good realistic setup for a raster graphics system would include a set of specific anti-aliasing techniques, which would be available at user discretion. For good-quality hardcopy from a low- to medium-resolution display device, the results are definitely worth the time involved. The method is much cheaper than getting a device with the comparable actual resolution. A more costly and time-consuming system for producing high-quality final images would include a scan-convedrting algorithm with anti-aliasing.

Aliasing effects will occur at any resolution, so this technique will have to be used if accurate images are desired. It need not be a time-consuming process, and the results will be worth the effort.

References

[1] -----, Product Review for AED767, Advanced Electronics Design, Inc., August, 1981 (distributed at SIGGRAPH 1981).

[2] Catmull, Edwin, "A Hidden-Surface Algorithm with Anti-Aliasing," Computer Graphics, Vol. 12, No. 3, pp. 6-11, August, 1978 (Proceedings of SIGGRAPH 1978).

[3] Crow, Franklin C., "The Aliasing Problem in Computer-Generated Shaded Images," Communications of the Association for Computing Machinery, Vol. 20, No. 11. pp. 799-805, November 1977.

[4] Crow, Franklin C., "The Use of Grayscale for Improved Raster Display of Vectors and Characters," Computer Graphics, Vol. 12, No. 3, pp. 1-5, August, 1978 (Proceedings of SIGGRAPH 1978).

[5] Feibush, Eliot A., Marc Levoy, and Robert L. Cook, "Synthetic Texturing Using Digital Filters," Computer Graphics, Vol. 14, No. 3, pp.294-301, July 1980 (Proceedings of SIGGRAPH 1980).

[6] Gupta, Satish, and Robert F. Sproull, "Filtering Edges for Gray-Scale Display," Computer Graphics, Vol. 15, No. 3, pp. 1-5, August, 1981 (Proceedings of SIGGRAPH 1981).

[7] Leler, William J., "Human Vision, Anti-Aliasing, and the Cheap 4000 Line Display," Computer Graphics, Vol. 14, No. 3, pp. 308-313, July 1980 (Proceedings of SIGGRAPH 1980).

[8] Newman, William M., and Robert F. Sproull, Principles of Interactive Computer Graphics, Second Edition, McGraw-Hill, New York, 1979.

[9] Ward, John E., "Wobbled-Raster High-Resolution Display," Electronic Systems Laboratory, MAC-MEMO-431, March, 1974.

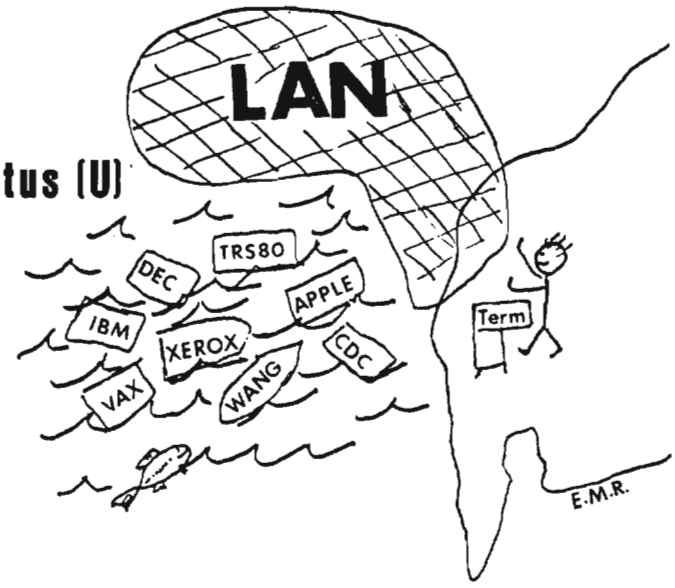
[10] Warnock, John E., The Display of Characters Using Gray Level Sample Arrays," Computer Graphics, Vol. 14, No. 3, pp. 302-307, July, 1980 (Proceedings of SIGGRAPH 1980).

[11] Weiman, Carl F. R., "Continuous Anti-Aliased Rotation and Zoom of Raster Images," Computer Graphics, Vol. 14, No. 3, pp. 286-293, July, 1980 (Proceedings of SIGGRAPH 1980).

~~FOR OFFICIAL USE ONLY~~

CID: 4011963

1982 Local Area Network Status (U)



by [redacted] T44

P.L. 86-36

OVERVIEW

The purpose of this paper is to describe the current status of Local Area Networks (LANs). LAN technology is one of the fastest growing areas of computer communications. Early systems have been operational since 1977. In the past two years there has been an increased interest by vendors and the business community to utilize new technology and reduce computer processing costs. In this paper it is assumed that the reader has a basic knowledge of networking concepts and that there is interest in the basic components of LAN architectures. This paper is not intended to cover extensive long-range developments or to get into technical details below what is necessary to explain current LAN architecture. Future LAN objectives will be mentioned with the purpose of expanding the knowledge of NSA/DOD standards, requirements, and applications.

The demand of the business community to consolidate data storage and computer processing while reducing operating costs is one of the motivating factors of LAN development. Technical advances in computers and communications have brought both entities closer together. Many computers are beginning to rely on LANs to perform communication functions external to them. For example, LANs are utilized to move data from a computer to a central storage area for future access. Magnetic tape and printer functions can be centralized by using LAN technology thus minimizing computer workloads and processing time. Data can be moved on the LAN at speeds ranging from 9.6 Kbps up to 50 Mbps. The data can be moved error-free, to the users' eyes and be structured in a form to meet vendors' computer requirements.

Basic LAN Structure

Local Area Networks function as community interconnection media within broader network architectures to allow rapid communications among members of user groups within limited physical areas at relatively low costs. LANs are frequently used to provide for connectivity, office automation, data transfers within distributed processing systems, and for terminal-to-host computer connections. The basic components of a LAN are its host systems, communication medium (twisted pair, CATV cables, microwave, fiber optics), hardware that interfaces hosts to the communication medium (generally called bus interface units or BIUs), and protocols (generally implemented in software). A particular LAN implementation depends on the user's requirements, the available technology, physical constraints, and relevant network standards. Anticipated developments within communications and computer technology dictate that LANs be flexible in order to accommodate different types of processing equipment and to provide for BIU upgrade without requiring protocol changes.

Basic Network Structure

DOCID: 4011963

LAN Communication Media

Communication technology advancements are minimizing the costs of LANs while providing for rapid delivery of data over short distances. The most commonly used transmission technologies are twisted pair, microwave, fiber optics, and coaxial cable (CATV).

Twisted pair have a high bandwidth which makes them reliable for high-speed data transmissions. By twisting the wires, requirements for shielding are reduced, but they are still very susceptible to external interference. The twisted pair are easy to install for a point-to-point connection. Some vendors, such as IBM and the telephone company, use twisted pair in their network structures.

Microwave transmissions are the most expensive LAN systems to install, mainly because they require special transmitters and receivers to move the data through the air. This is used where a line-of-sight transmission is possible and a physical connection is too expensive or not possible. An example of such a situation is where LAN hosts are in two different buildings with a main road between them. In this case it may be less expensive to install microwave equipment than attempt a physical connection.

Fiber optic lines transmit data at speeds in the Gigahertz range with a very low bit error rate. It transmits data in one direction only which means two cables would be required for a LAN installation. Current fiber optic technology can only be used in point-to-point connections because cable splicing has not been perfected. Fiber optic lines are relativity free from line interference and are the most secure for a DOD mode of operation. Fiber optics will be the transmission medium of the future when the technical problems are solved and the costs come down.

Coaxial cable (CATV) is currently the most widely used transmission medium. It combines a very low data loss with high bandwidth transmission. The CATV (75-ohm) has been used in television and antenna connections for many years and is very reliable. This means it is a commercially produced product with connection methods and installation techniques being readily available at a low cost (approximately 31 cents per foot). The two most mentioned CATV transmission media are baseband and broadband. Baseband is simple to use, but it uses the entire transmission bandwidth to move the data from one host to another. You may have to use two lines if the volume of transmissions is large. The baseband system is used by XEROX ETHERnet and Ungermann & Bass LANs, to name a few. Baseband on a bus topology is a very reliable and fast communication medium. Broadband, which is the other type of bus transmission, employs up to 41 separate channels (frequency ranges) on one cable. Each cable functions independently and is monitored by the BIU. The BIU must be tuned to the frequency or frequencies required. A channel on the broadband system can transmit analog, digital, voice, and video data on different channels at the same time. A host connected to the BIU can be a dumb terminal, intelligent terminal, large computer, telephone, or a TV camera. Broadband is fast and has to be developed more but it has great potential, especially for Agency field site and in-house use. Currently, baseband and broadband cannot communicate with each other. This is where gateway technology, which will be mentioned later, fits into the LAN picture.

Access Methods

An access method on the LAN communication lines is but one of the items necessary for rapid data movement. Some of the basic access methods are circuit switching, token passing, slotted ring, and bus contention transmissions (baseband and broadband). The type of access method is usually determined by the vendor and LAN topology selected to meet the requirement.

Private Automatic Branch eXchange (PABX) is a circuit-switched system with dedicated line transmission that has been in service since 1977. The ROLM CBX corporation has produced over 6000 systems which are in use today. Early PABX systems used analog switching but the newer systems are digitized. Voice data is first digitized and then sent over the network. The architecture of today's telephone system uses the PABX technology and has been in use for several years. INTERCOM IBX, a subsidiary of EXXON Corporation, has one large PABX system installed with approximately 20 more systems on order. The EXXON system is too new for comments.

Token passing is an access method used on ring and loop LAN topologies. It is very fast (1-10 Mbps) with high reliability. A special token character configuration is sent around the ring or loop when there is no data to be transmitted. When a host wants to send data on the network the token must be identified before the host can transmit. This eliminates the possibility of data collisions on the network.

Slotted ring is also an access method used on ring and loop LAN topologies. It is very fast (1-10 Mbps) with high reliability. The slotted ring consists of empty slots moving around the ring of a fixed slot size. Each slot size must be predefined to match the block size of data to be transferred. When

DOCID: 4011963

the host wants to transmit data, it finds the first empty slot and moves a block of data.

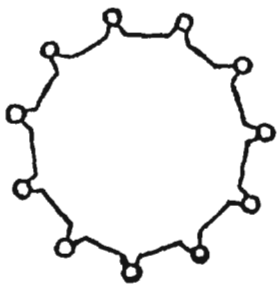
Bus contention transmission is a random procedure with no preestablished time slots or order of transmission. Usually Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is the mode of transmission. A host will listen for activity on the network before it attempts to transmit the data. There is a possibility that two hosts could sense a clear network and begin transmitting at the same time. Most well-defined vendor networks have algorithms that sense the collision and retransmit the data again without the user's knowledge.

LAN Topology

LANs have architectures that follow basic topologies like ring, loop, star, tree, and bus. To aid in understanding how these LAN topologies function each will be described below. LAN topologies are usually designed to meet a specific requirement. Some requirements dictate that two or more topologies be combined to serve the users needs within the LAN.

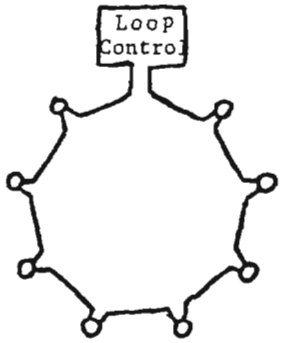
LAN TOPOLOGIES

Ring



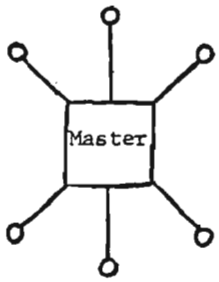
A ring topology is a single closed path between any two users. Communication is usually over a one-way path and very fast (about 10 Mbps) As the data passes by a connecting node on the communication line the node tests the data address to see if the data belongs to it. If the data belongs to that node it will be extracted from the ring and sent to that host. If the data does not belong to the node, it just passes the data to the next node in the ring.

Loop



Loop topology is basically the same as the ring except there is a controlling node in the ring. This node can monitor and control the data as it passes around the ring.

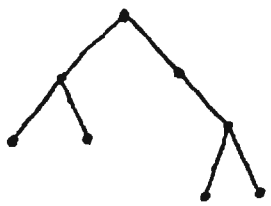
Star



Star topology is a master/slave type LAN architecture with the master host being the hub of the network and all network functions passing through it. The slave hosts are attached directly to the master host. In this topology the master node has full control of the network. The star topology has the capability to control such things as priority type transmissions and large data base files for the slave hosts. A disadvantage of this architecture is that if the master host ever goes down the entire LAN will not function.

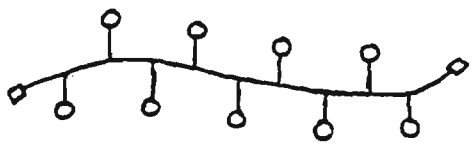
DOCID: 4011963

Tree



A tree topology provides a single non-closed path between users. It supports two-way communications after the connections are made. PABX circuit switching is the access media on most of the tree architectures. For the connection to be made, all nodes switch to make the path on which the data will flow. Data must pass through all nodes in the circuit to reach its destination. Telephone company network systems utilize the tree architecture for voice communications.

Bus



The bus topology is a single non-closed path between users. Bus networks are broadcast-type communications with mostly CSMA/CD as the transporting protocol. The bus topology is the most talked-about LAN architecture today. One of the more controversial subjects of bus architectures is the type of communication media (CATV or fiber optics and baseband or broadband). Each has advantages and the LAN architecture based on the requirements would dictate what is used.

Commercial Status

There has been little cooperation among vendors to establish a unified approach to developing hardware and software for LANs. Rapid advances in communication technology have inspired many old and new vendors to develop their own LANs independently. Most suppliers are still developing their own components and few have working hardware in production. Some vendors have developed solutions to specific technical problems but have not produced the algorithms or appropriate hardware to implement them. For example, Ungermann & Bass has proposed a solution to provide communication between baseband and broadband network systems and has just started production. Another example is SYTEK Corporation which advertises gateways to handle inter-network communications. This is not yet in production either. SYTEK is over a year late delivering an operable System 40 (host-to-host) BIU line of hardware. Still another example is IBM, which has started support of X.25 but has not released any product specifications. These are only a few examples of products which are advertised but are not yet in production. Most vendors have directed their technology towards capturing a specific part of the LAN market. Some developers (such as SYTEK and MITRE) are addressing general LAN applications that exist now, as well as those expected in the future.

Government agencies and private industries which require LANs now are forced to buy the ones which come closest to meeting their requirements, realizing they may have to change their LANs in the future to meet requirements for inter-network communications. The cost of such an upgrade would be diminished if a set of host interface standards were adopted.

Protocols

In addition to the diversity of hardware, there are presently no accepted standards for LAN protocols. Protocol development is a costly part of building a LAN. In general the BIU hardware and vendor architecture dictate which protocols are implemented in the BIU or which are required to be written by the host's software group. Vendors such as SYTEK propose to supply a large quantity of protocol software within the bus interface unit (BIU) itself. The cost of procuring this type of BIU will be higher than for a less robust BIU, but protocol development in the host will be reduced.

Every vendor develops its own version of a protocol to meet its own product requirements, both within the network itself and for host access to the network. Protocol standards for LANs are currently being considered by the Institute of Electrical and Electronics Engineers (IEEE), National Bureau of Standards (NBS), and other standards organizations. Once such protocol standards become a reality they are more prone to be implemented in firmware. This would allow vendors to concentrate on simpler uniform host interfaces.

CID: 4011963

However, it must be realized that user requirements may dictate exceptions to the protocol standards. At least there will be protocol standards from which to begin.

LAN Security

The security aspects of protecting data from compromise has been addressed by very few LAN vendors. None has yet produced a totally secure system. There are two types of LAN security of concern for our mode of operation, namely TEMPEST and transmission security. The TEMPEST problem involves electronic radiation from the BIU, communication media, and line connectors. Vendors have not addressed this problem at all. A commercial LAN would need to be TEMPESTed by the purchaser unless the vendor agrees to do it at additional cost.

Transmission security is the encryption of data being sent over the communication lines. Several vendors are addressing transmission security by putting an encryption algorithm in the BIUs. There are no such off-the-shelf units available to date. Network Systems Corporation and SYTEK corporation are two vendors that are addressing data encryption. The only other approach to transmission security is one in which the host provides the software to encrypt and decrypt the data itself.

LAN In-House Activities

NSA has had working packet switching and local area networks in operation for several years. The experience and knowledge gained through these efforts will prove invaluable in the development and integration of LAN technology to meet agency needs.

T443 will be evaluating LAN technology for office automation through the use of the XEROX ETHERnet. This allows office clericals, professionals, and managers using workstations to interact with other users on the same LAN. Office memoranda, inter office mail, and data files can be shared with every connected LAN user. A prototype system will be used to evaluate LAN data flows between users. Basic XEROX hardware is being tested to attain maximum network operational efficiency. Functional procedures are being generated to create an operational test package. Upon completion of the prototype, test evaluations will be coordinated in T443 for the planned implementation of the full operational office automation network.

Since 1976, T41 has been developing a local network using Network System Corporation's HYPERCHANNEL adapters. The HYPERCHANNEL hardware has proved very reliable with a 6000-hour Mean Time Between Failures (MTBF). These adapters are employed in three major processing centers where extremely high data transmission rates are required. The cost for this type of network is 40 to 50thousand dollars for each host connection permitting an advertised data rate of 50 Megabits per second.

R81 has been actively involved in network technology for several years. They have studied different vendors' hardware and software and are currently contributing to the development of MITREBUS technology for general applications. They intend to model and test baseband and broadband technologies on LSI-11/Z8000 and Motorola 68000 hardware. T44 has been directing many of its LAN inquires to R81.

R63 is developing a fully TEMPESTed LAN for field site use, also based on MITREBUS technology. Their efforts in LAN technology are of interest to T44 since it appears that the requirements driving the development of field site LANs are similar to those we may have in-house. T44 is currently evaluating the R63 requirement in order to assess the level of compatibility with both LAN architectures.

Gateways will be required for inter-network communications with LANs and other networks. R63 and T44 are currently studying one such gateway problem. This gateway will permit a field site LAN to be connected to PLATFORM.

Future LAN Plans

With the rapid development of communications and computer technology the cost of LANs is expected to come down within a few years. Technical advances will no doubt stabilize the technology to allow mass production of more reliable LANs. This should solve the majority of user requirements for communicating locally. The next significant development will come when the LANs need to be connected to other networks. Worldwide communication on digital packet switched networks is now becoming a reality. LAN technology and the development of gateways will make it possible for the local user to achieve local and global communications. Current LAN architectures must consider the global communication requirements of the future, whenever possible, in order to meet the ever expanding Agency commitments.

Conclusion

This brief overview of LAN topologies and access methods depicts that current commercial status and Agency development is progressing. Within two years LAN concepts will be stabilized and a user will be able to select a well defined LAN to meet the requirements of his application.

DOCID: 4011963

LOGIC DESIGN EXCEEDING BOOLEAN CAPABILITIES

P.L. 86-36

by [redacted] R53

BACKGROUND

Contemporary digital computer programming makes use of "languages" which have progressed from the entirely machine-dependent, tedious, "assembly" stage to a nearly machine-independent, expedient, "high-level" stage. High-level language efforts continue to push towards even higher levels (e.g., Ada). The equivalent of a few statements in a latest high-level language could require hundreds of assembly language statements.

A hardware counterpart, digital logic design, makes use of methods which have "progressed" from 2-valued Boolean algebra, truth tables, and Karnaugh maps, to those in combination with hardware design languages, system development hardware, etc. These additional means for logic design include art forms and various algorithms developed since Karnaugh maps.

There is at least one difference between the progress made in programming and that in digital logic design. Programmers, having advanced from the assembly language environment, now create almost entirely with expedient, yet efficient, high-level languages. Logic design practitioners (in contrast to theorists or researchers) still rely heavily on a tedious 2-valued Boolean algebra when not engaged in design art. An expedient, acceptable "high-level" version of 2-valued Boolean algebra has not evolved.

PROBLEMS

A problem with today's use of 2-valued Boolean algebra, the "assembly language" of digital logic design, is that it forces the algebra into service where it really does not apply. Two-valued Boolean algebra applied quite well (transitions between values aside) back in the days when SSI (small scale integration) circuits dominated. In fact, SSI is an attempt to realize 2-valued Boolean algebra.

Besides using 2-valued Boolean algebra, logic design practitioners now "fiddle around" (an art form) with bits, forcing them into devices which, for the most part, do not really operate on bits. Those devices mostly operate on buses of bits--inputs having more than two values--in other words, multivalued inputs!

THE STATUS QUO

One might argue that the logic design methods used today, however described, must be working. After all, technology is nearly at the point where microprocessors could be sold by the pound from a barrel like dried beans.

Logic circuits today are designed using a combination of art and science, and they may always be. A problem with that is balance. Given that logic design is much more an art, then if person A is born with artistic talent, only A may be able to produce "good" designs. Artistic methods cannot be reproduced without

DOCID: 4011963

interpretation. Scientific methods can, but can also be tedious and even encumber innovation (an art) when the basis of such methods has been overwhelmed by progress. Such appears to be true for today's logic design methods when they present the designer with 2-valued Boolean algebra as a principal tool.

But who cares? One must admit, microprocessors by the pound is by no means a small achievement.

"Microprocessors by the pound" was fueled with money. Business and government invested and still plan to invest "megabucks" (millions of dollars) in complex systems and commit for long term amortizations in order to produce today's technology. A problem with the megabucks approach applied to processes which include outdated components is that the massiveness of the approach tends to perpetuate the included obsolescence.

CHANGE

At some point a new decision regarding continuation of the present megabucks method is needed. Technology is near the limits of speed and "real estate" (room) on IC (integrated circuit) substrates. Gross parallelism and concurrency, both candidates for megabucks support, are brute force solutions to the limits problem. But is that where the money really should be spent?

One wonders, is the technology at hand being used anywhere near its capacity? Fearfully, the suspicion is that it is not. How about the designs placed on substrates--are they known to be minimized? No. Can some justification for the status quo be made on the basis of expediency? In the megabucks environment, yes, but technological limits are eroding the validity of this argument.

One component of a "smarter" approach to future logic design is to provide a better logic design mathematics. Such a "math" would allow logic design to become less of an art. Even if incapable of producing minimized results under all criteria for minimization, a new design math equipped to be compatible with current and future technologies, yet of itself costing nothing in hardware and software monies, might yield optimal mixes of expediency and efficiency.

This idea is far from new. Algebras and other calculi that could be used in logic design proliferate. Multivalued logics have been around for quite some time, and attempts have been made to convince industry to use them. But two problems with multivalued logics are their complexity and diversity. Add to that their implied required technology changes, and rejection results. The required technology changes are fearsome. Recall all the megabucks of industrial investments and long term amortizations. Add to that another fear on the part of industry's customers that all their products could quickly be made obsolete.

How can the stalemate be broken? Altruistically, perhaps the federal government could help by attraction: introduce and use a design math that eliminates at least the scary problems discussed. But remaining even with that idea is human resistance to change. Logic design practitioners may fear that the algebra which they have known all their lives will be taken away. Given the math discussed in the next section, nothing is taken away. More is added.

A FIRST RESULT FROM RESEARCH

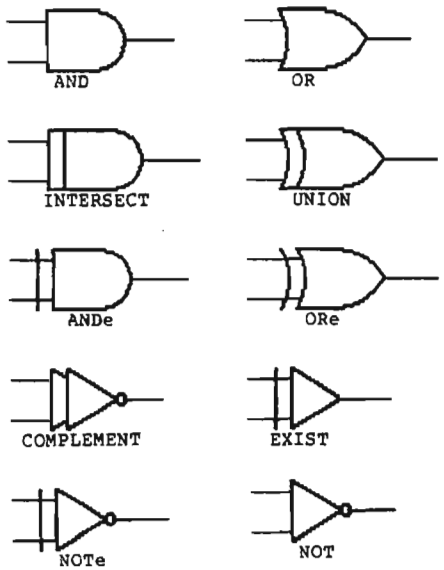
A "mix-valued" algebra denoted by "Mx" (which we pronounce, "mix") was first reported on [1] while it was in the throes of pre-result research. Mx has since grown to a first level of usable maturity. Now, as a first result of research from R53 [2,3], Mx may be a step in the direction of a math suitable for future logic design.

As proposed, instead of having only AND, OR, and NOT gates, Mx has seven others. Possibly, the additional primitives will enhance designer creativity. (However, one may use Mx as a 2-valued Boolean algebra only.) Each of Mx's ten gates is capable of accepting a whole bus at each of its inputs and can deliver a whole bus as a single output (this includes bus width=1). These bus-handling attributes may help to reduce logic design complexities. Instead of being constrained to the value universe {0,1}, Mx allows one to redefine it for every use of any gate. Such a freedom may enable whole design outlooks to change to the point of inspiration. Each of Mx's ten gates can also operate on combinations of buses of any radix and multivalued signals, without concern for technology. This independence may help Mx to be resistant to obsolescence. Possibilities for compounds of the proposed Mx-gates, analogous to the NAND and NOR gates developed from 2-valued Boolean algebra's three operators, can be imagined. Clearly, there should also be use for the fact that the proposed Mx-gates can be arranged to form sequential and memory circuits.

Although not as mature as 2-valued Boolean algebra, meaning it remains fertile in many ways, Mx has been used successfully in modest, practical logic design experiments. A review of 2-input instances of Mx's proposed gates, some of which were used in those experiments, are pictured below. (Yes, Mx's NOT gate can

CID: 4011963

have more than one input.)



ANDe, ORe, and NOTe are pronounced, respectively, "existential AND," "existential OR," and "existential NOT."

Each Mx-gate has an associated connective symbol. The following table shows them used with output z and inputs $x_1,x_2,\ldots,x_n$.

gate	usage
AND	$z=x_1x_2\ldots x_n$
OR	$z=x_1+x_2+\ldots+x_n$
NOT	$z=x_1\hat{}x_2\hat{}\ldots\hat{}x_n$
INTERSECT	$z=x_1\bigwedge x_2\bigwedge\ldots\bigwedge x_n$
UNION	$z=x_1\bigvee x_2\bigvee\ldots\bigvee x_n$
COMPLEMENT	$z=x_1"x_2"\ldots"x_n$
ANDe	$z=x_1\&x_2\&\ldots\&x_n$
ORe	$z=x_1\Subset x_2\Subset\ldots\Subset x_n$
NOTe	$z=x_1\nexists x_2\nexists\ldots\nexists x_n$
EXIST	$z=x_1\exists x_2\exists\ldots\exists x_n$

Concatenation in the expression for AND may be replaced with dots, resulting in

$$x_1x_2\ldots x_n = x_1\cdot x_2\cdot\ldots\cdot x_n.$$

"^" may be replaced with "′" in expressions where the NOT gate is to operate entirely within 2-valued Boolean constraints, that is, when the gate's value universe is {0,1} and n=1. $x_1'x_2'\ldots'x_n$ is undefined for n>1 because 2-valued Boolean NOT is unary. Notice that $x' \neq x\hat{}$.

Each Mx-gate instance g operates with respect to its own value-universe, called a "reference set," denoted by the variable, "r_g." A reference set instance may be ordered or not, as needed. Since r_g is a variable, a gate's reference set may be changed as often as desired. There are no limitations on r_g contents for any Mx-gate. However, the "reference set" for every 2-valued Boolean gate instance is the constant, {0,1}, and is ordered, 0<1. (This is why designers can use Mx yet not do anything different than when using 2-valued Boolean algebra--2-valued Boolean algebra is a subalgebra of Mx!) When a Mx-gate's inputs contain an element not in r_g, the gate will produce the null, "ϕ" [2,3]. ϕ can also be the valid result of a Mx-gate's operation.

ϕ can have one of two effects at Mx-gate inputs:

a. The ϕ-bearing input effectively vanishes, needing no consideration in the gate output determination.

b. The ϕ-bearing input appears to have no value.

With (b), a gate can be made to wait for a non-ϕ on all, none, or exactly one of the inputs before generating an output.

ϕ-generation results in a situation which may be unfamiliar to many: the usual algebraic properties of association and distributivity involving any gate receiving a ϕ are disallowed. As an example regarding associativity, let two AND Mx-gates be connected in series, the first having inputs a, b, and c, and the other having the additional inputs d, e, and f. The expression for their output z cannot be correctly written as, z = abcdef. Instead, the correct expression is z = (abc)def, where (abc) must be evaluated first.

Definitions of the operations of the proposed Mx-gates first requires definition of the "atomizer function." Specifically, the atomizer function A on a set X of n inputs, i.e., A(X), where $X = \{x_1,x_2,\ldots,x_n\}$, decomposes the sets ranged over by all its member input variables x_i, $i\in\{1,2,\ldots,n\}$, so that no member of the result set is itself a set. For example,

if $X = \{x_1,x_2\}$, $x_1 \in \{3,4,\{7,13\},6\}$,

and $x_2 \in \{2,4,\{6,13\},25\}$,

then A(X) ={2,3,4,6,7,13,25}.

DOCID: 4011963

Definitions of the operations of the proposed Mx-gates follow and are different from those originally reported [1]. Except where stated otherwise, ordering of r_g members is not needed in those definitions. Notice that for $r_g=\{0,1\}$ and $x_i \in \{0,1\}$, the AND, OR, and NOT Mx-operations produce results identical to those same-named operations in 2-valued Boolean algebra.

$$\text{AND}(X) \equiv \begin{cases} \min(A(X)) \text{ if } \forall x_i \in X,\ x_i \subseteq r_g \\ \emptyset \text{ otherwise} \end{cases}$$

$$\text{OR}(X) \equiv \begin{cases} \max(A(X)) \text{ if } \forall x_i \in X,\ x_i \subseteq r_g \\ \emptyset \text{ otherwise} \end{cases}$$

$$\text{ORe}(X) \equiv \begin{cases} x_1 \text{ if } x_1 \neq \emptyset,\ x_2 = x_3 = x_4 = \ldots = \emptyset \text{ and } x_1 \subseteq r_g \\ x_2 \text{ if } x_2 \neq \emptyset,\ x_1 = x_3 = x_4 = \ldots = \emptyset \text{ and } x_2 \subseteq r_g, \\ \quad \vdots \\ x_n \text{ if } x_n \neq \emptyset,\ x_{n-1} = x_{n-2} = \ldots \\ \qquad = x_{n+1} = x_{n+2} = \ldots = \emptyset, \text{ and } x_n \subseteq r_g \\ \emptyset \text{ otherwise} \end{cases}$$

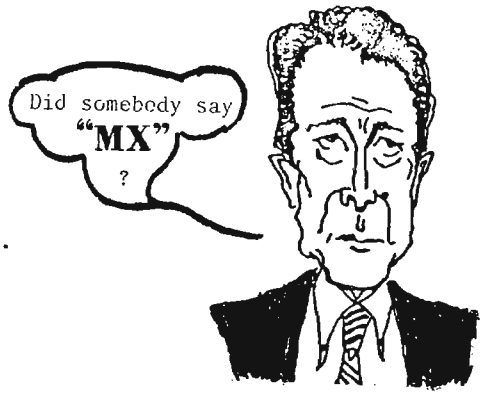
Total ordering of r_g members is needed for the following NOT(X) definition. Also, the least valued member or its r_g must behave like a zero, the next higher must behave like a one, the next higher like a two, etc.

$$\text{NOT}(X) \equiv \begin{cases} \max(r_g) - A(X) \text{ if } \forall x_i \in X,\ x_i \subseteq r_g \\ \emptyset \text{ otherwise} \end{cases}$$

$$\text{EXIST}(X) \equiv \begin{cases} \max(r_g) \text{ if } \forall x_i \in X,\ x_i \subseteq r_g \text{ and } x_i \neq \emptyset \\ \emptyset \text{ otherwise} \end{cases}$$

$$\text{UNION}(X) \equiv \begin{cases} \text{union}(\{A(x_1)\},\{A(x_2)\},\ldots,\{A(x_n)\}) \text{ if } \forall x_i \in X,\ x_i \subseteq r_g \\ \emptyset \text{ otherwise} \end{cases}$$

$$\text{INTERSECT}(X) \equiv \begin{cases} \text{intersection}(\{A(x_1)\},\{A(x_2)\},\ldots,\{A(x_n)\}) \\ \quad \text{if } \forall x_i \in X,\ x_i \subseteq r_g \\ \emptyset \text{ otherwise} \end{cases}$$



"-" is set subtraction in the following COMPLEMENT definition.

$$\text{COMPLEMENT}(X) \equiv \begin{cases} [r_g - \text{union}(\{A(x_1)\},\{A(x_2)\},\ldots,\{A(x_n)\})] \\ \quad \text{if } \forall x_i \in X,\ x_i \subseteq r_g \\ \emptyset \text{ otherwise} \end{cases}$$

$$\text{ANDe}(X) \equiv \begin{cases} X \text{ if } \forall x_i \in X,\ x_i \subseteq r_g, \text{ and } x_i \neq \emptyset \\ \emptyset \text{ otherwise} \end{cases}$$

$$\text{NOTe}(X) \equiv \begin{cases} r_g \text{ if } x_1 = x_2 = \ldots x_n = \emptyset \\ \emptyset \text{ otherwise} \end{cases}$$

DOCID: 4011963

USING THE FIRST RESEARCH RESULT

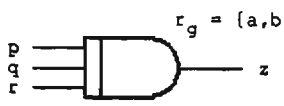
Step-by-step Mx-designs of five combinatorial memoryless circuits, ranging from very simple to not-so-simple, have been reported [2], making use of a "First-Order Logic Design" procedure. [2] An improved statement of the Procedure has also been reported [3].

A listing of specifications and results of the five Mx-designs referred to in the preceding paragraph, follows. When compared to bused I/O (input or output or both) versions designed using 2-valued Boolean algebra, those Mx-design results are obviously significantly simpler. Such simplicity will have more value once direct realization ICs for the Mx-gates exist. (A direct realization effort is under way, and a patent has been applied for.)

DESIGN #1

Specification: Transmit to an output z any value from the set {a,b,c} common to input buses p, q, and r.

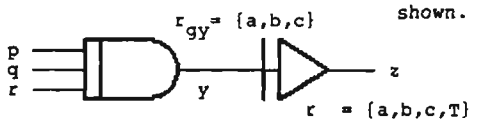
Result: $z = p \wedge q \wedge r$, with the reference set shown.



DESIGN #2

Specification: Same as for Design #1 except instead of transmitting to the output the identical value from the set {a,b,c}, send only one signal to indicate that all three inputs are one of a, b, or c.

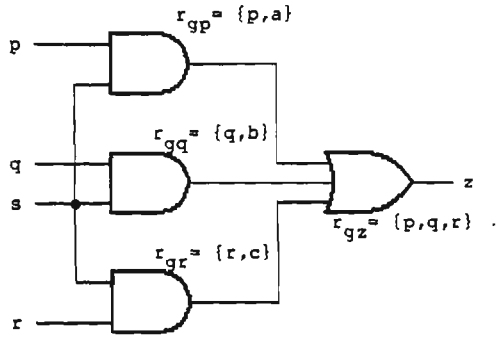
Result: $z = \exists(p \wedge q \wedge r)$, with the reference sets shown.



DESIGN #3

Specification: Design a multiplexer having bus output variable z, data bus input variables p, q, and r, and a "select" bus input variable s, so that via s, value "a" selects p, value "b" selects q, and value "c" selects r.

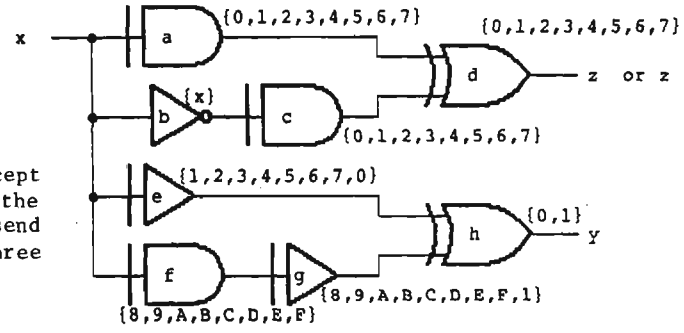
Result: z = ps + qs + rs, with the reference sets shown and where a>p, b>q, and c>r. (Notice that associativity cannot be applied to the result expression.)



DESIGN #4

Specification: Convert a single binary bus input x of hexadecimal code to octal, delivering the results to binary bus outputs y and z.

Result: $y = (\exists x) \Leftrightarrow (\exists (\&x))$ and $z = (\&x) \Leftrightarrow (\&x\hat{})$, with the reference sets shown.

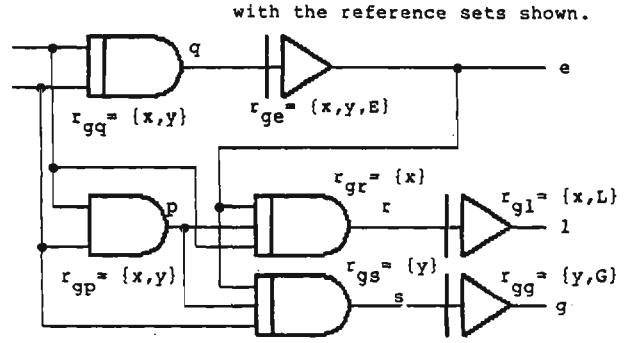


DESIGN #5

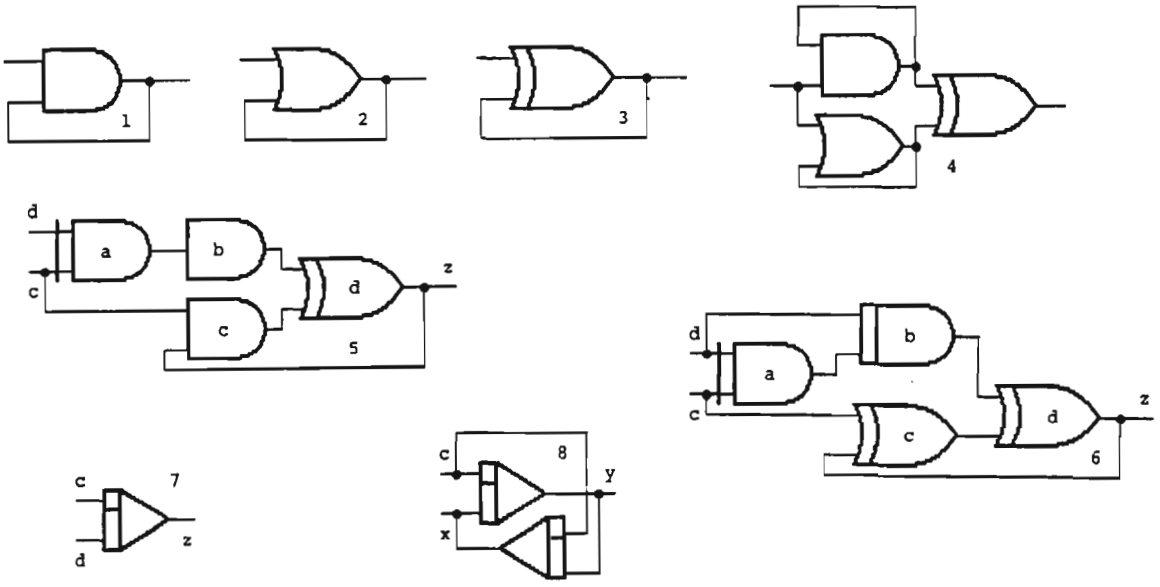
Specification: Design a comparator which will indicate at one of its outputs g, e, or l (lower case L), that at its inputs x and y, x>y, x=y, or x<y, respectively.

Result: $g = \exists(\exists(x \wedge y) \wedge (xy) \wedge y))$,

$e = \exists(x \wedge y)$, and $l = \exists(\exists(x \wedge y) \wedge (xy) \wedge x))$, with the reference sets shown.



DOCID: 4011963



ITEMS STILL IN RESEARCH

The above figures (an assortment of heretofore unpublished memory circuits for the reader to ponder) use only the proposed Mx-operators.

1. A "min" latch. The output will hold the minimum of all values it has received since being activated. Resets to ϕ upon introduction of a value not in the reference set.

2. A "max" latch. The output will hold the maximum of all values it has received since being activated. Resets to ϕ upon introduction of a value not in reference set.

3. An accumulating data latch. The output will hold all inputs. Resets to ϕ upon introduction of a value not in the reference set.

4. A min-max latch (could be used as a "truest and most false" value finder). The output holds the least and greatest values received since being activated. The min or max value is reset to ϕ upon introduction of a value not in the AND or OR gate reference set, respectively. Both the min and max values are reset to ϕ upon introduction of a value not in either reference set.

5. An arbitrary-value, one-level memory. $c \in \{\phi, C\}$, $C > d$, $d \equiv$ data, $r_{ga} = r_{gb} = \{C,d\}$, $r_{gc} = r_{gd} = \{d\}$. A new value of d is loaded in memory whenever c=C. (When c is a clock signal, C is a high potential, and ϕ is a low potential, this circuit also describes the single-direction behavior of the nMOS pass transistor used in IC chip design.)

6. An arbitrary-signal, one-level memory. $c \in \{\phi, C\}$, $d \equiv$ data, $r_{ga} = r_{gb} = \{C,d\}$, $r_{gc} = r_{gd} = \{d\}$. A new instance of d is loaded in memory whenever c=C. This is a generalized version of circuit 5; d may be other than a value (e.g., a set). Therefore, under the same assignments of potential values for C and ϕ as described for circuit 5, this circuit also describes the single-direction behavior of the nMOS pass transistor.

7. A polarized, single symbol used to represent circuit 6, i.e., a gated single-level memory.

8. A connection of two circuits (7). This configuration accounts for the bidirectional behavior of the nMOS pass transistor. When allowed to represent a connection of two circuits (6), this configuration more specifically accounts for the bidirectional behavior of the nMOS pass transistor. Input c still represents a clock signal, but the remaining terminals are now each I/O terminals. Hence, the remaining terminals are relabeled impartially, "x" and "y." This configuration additionally requires an additive "Logic Current Law," analogous to Kirchoff's Current Law, for complete operation description. The Logic Current Law is beyond the scope of this paper.

DOCID: 4011963

CONCLUSIONS AND SUGGESTIONS

Although at a usable level, Mx is still immature. It needs enhancements born of feedback from users and researchers (who may even find fatal problems with it). But potential users may find little immediate incentive to try Mx. Having a variety and abundance of "building block" ICs, those users may not want to learn a new design algebra, no matter how good it may be. Logic design today is largely a matter of "putting together" (an art form) large, IC-realized, functional modules. Having to work a little harder every now and then, designing-in some SSI "glue chips" by means of a "tedious" 2-valued Boolean algebra, may be acceptable. And, having even greater capability yet with the same size building block ICs, possibly resulting from use of an updated design math, may have little importance to them.

Yet among them may be those who would like to see logic design done more expediently and methodically, with the possibility of mathematical verification, and at the same time would like to try Mx. For them, beginning suggestions follow: First, throw away nothing currently used in design, i.e., methods, ICs, systems, etc. Next, while designing in the manner accustomed to, try to identify logic design tasks which seem tedious. Try some of the Mx design methods known [2,3] and possibly add some of your own. Note how those methods may or may not have applied; then with that experience, look for other areas in your design that could use improvement. (These steps should help to increase one's ability to think in terms of Mx-gates and properties.)

When sufficiently brave, try a small design from scratch using Mx. If there are parts of the design for which no Mx method is known, patch in what has worked in the past. When done, one can either put the resultant logic design away until the day when direct-realization chips for Mx exist or try to create realizations.

Realizations can be created by:

a. building them from non-programmable "catalog" parts,

b. building them from programmable "catalog" parts, and

c. making custom ICs.

Method (a), although expedient, may not result in the best solution in terms of space, speed, and power consumption. Method (b), using PLAs (programmable logic arrays) or variations on ROMs (read-only memories), may be slightly less expedient and possibly result in slower operation than (a). But for modest-size reference set and input cardinality combinations, (b) probably uses much less space and power than (a). Method (c), if one can monetarily afford it, may be the most efficient from the standpoint of circuit performance but may also have the longest period from design to realized circuit (bad for "breadboarding" expedience). Using a table-lookup approach (suggested by Dr. Richard K. Kunze, R53, 24 August 1982, and also used in method (b)), PLA or ROM versions of Mx circuits have regularity, readily lending themselves to "very large scale" IC implementation. Physical circuit compaction beyond that possible by using Mx alone may be available through electrical and physics "tricks" and sharing of on-chip resources. (Such an extra-method of compaction is analogous to the greater compactions in assembly language achievable when human intelligence is applied to the object code produce by a software compiler.)

Has the time come to move towards a logic design mathematics compatible with today's and future technologies?

References

P.L. 86-36

CID: 4011963

Ada:

Conquering the TOWER OF BABEL©

P.L. 86-36

Ada Augusta, Countess of Lovelace, the daughter of Lord Byron and a gifted mathematician who worked with Charles Babbage, a computer pioneer. She is the person after whom the Ada language is named.

by [redacted]

INTRODUCTION

In an effort to implement standards, to stay steadily increasing software costs, and to create a universal language for embedded computer systems, a long-term research effort began at the Department of Defense (DoD). The result of this effort is Ada, a new programming language.

This paper will explore the development and capabilities of Ada. In the process, it will illustrate to the reader that several factors have to be considered when examining the performance of a programming language. It is not enough to look at only the characteristics of the language. The language must be studied within the context of its intended purpose.

The following sections will examine the Ada language. Ada's history will be presented as will some features which are not common to higher-level languages. Factors which will be important to the long-term success of Ada will be presented in the "Conclusion." It will be apparent that Ada is still in an evolutionary process and its success is not assured.

GENERAL OVERVIEW

The influx into the marketplace of a variety of programming languages and resultant software began with the commercial acceptance of computers. The user, who was originally a participant in the creation process, was replaced by specialists who provided languages and software which did not necessarily meet the user's specific needs.[1] Changing technology and demands for increased capabilities aggravated this problem. Many approaches were initiated to alleviate the resultant software crunch. This paper will focus on Ada, one Department of Defense (DoD) solution to software problems. Here, the pendulum has swung back again and the user, in conjuction with the specialists, is a participant in the process.

A programming language cannot be created in a sterile environment. It must be designed with the same care an architect would take in designing a house. The architect must be aware of the customer's needs and objectives before initiating design plans. He must also be aware of other factors which will interact with the house. These will include, but are not limited to, public utilities, the neighborhood, and the customer's lifestyle. Once the architect has developed a clear understanding of his objective, he can begin to draft a design fitting the customer's desires and relating them to the physical environment. The architect's interaction with the customer, the zoning commissioners, and others should not end here if the plans are to be acceptable to all involved. To ensure that the final product meets the requirements, the design must be reviewed at intermediate stages, preferably with those involved, to ensure that the original objectives have not been lost.[2]

The creation of a programming language should proceed in the same manner. The creator must determine what the objectives of the language are to be, and with what it will interact. Upon determination of what the programming language should contain, design plans should allow for adequate reviews throughout the process. The final product should be a programming language which meets the needs of the user and can interact well with the user's environment.

All languages which have been created to date have been created to perform certain functions. FORTRAN (FORmula TRANslation) is a mathematically based language intended for use by both scientists and engineers. It is well-suited for the handling of complex mathematical problems but is not well-suited for handling large amounts of input and output (I/O). COBOL (COmmon Business Oriented Language) was designed for business-oriented problems which may involve a large amount of file processing and I/O, but only involve simple mathematical functions. Because of its business orientation, the language was designed to closely resemble English, thus being made easy to code and read as well as self-documenting. Unlike FORTRAN, it has

Also see page 155.

* Ada is a trademark of DOD Ada Joint Program Office

DOCID: 4011963

special provisions to make it easier to manipulate and process alphanumeric data. PL/1 (Programming Language 1) combines the advantages of COBOL and FORTRAN, i.e., the file processing, I/O, and mathematical capabilities. It is a multi-purpose language which can efficiently handle either scientific or commercial problems as well as combinations of the two. These examples illustrate the diversity of programming languages. It should be evident that to date there is no language which can perform all functions optimally. Tradeoffs have to be made when deciding which programming language to use.

The programmer thus has to consider several factors when choosing a programming language. Among them are:

[] Language availability,
[] Language familiarity of programmers,
[] Ease of program maintenance,
[] Cost of programming,
[] Time needed to write the program,
[] Time needed to execute the program, and
[] Characteristics of the problem.[3]

Whether a language is or can be supported by his system must also be considered. These are factors which help to determine which language will be chosen for a particular application. They are also factors which will be included in the determination of whether Ada will become the standard Department of Defense language.

EVOLUTION OF ADA

The creation of a new programming language was not originally considered as a solution when it was discovered through several studies in the early 1970s that a major problem at the Department of Defense (DoD) was language proliferation. Instead, the DoD high-order-language standardization program was initiated. This program considered standardizing seven already established programming languages in order to alleviate the problem. Feedback from the users, however, indicated that seven languages would still be too many languages to simplify the problem notably. More studies were initiated to determine what the requirements of the language would be. It was discovered that there were no significant differences in the tri-service (Army, Navy, Air Force) requirements. Furthermore, $100 million per year would be saved by converting to a simple common language. The decision was made to consider a single programming language.[4]

The first definition of requirements for a single common language was presented in 1975 by the High-Order Language Working Group (HOLWG) which had been created to identify and recommend solutions. Existing programming languages were reviewed to see if any could fulfill all the requirements. None could satisfy more than 75% of them. Factors which led to the decision to create a new programming language included the inability of current languages to handle easily and efficiently such functions as parallel processing, real-time input and output (I/O), and exception handling. It was also noted that in many projects at DoD it was necessary to modify existing languages in order to provide for needed enhanced capabilities. Once the decision was made that a language needed to be created, competitive bids for a language design that met the requirements were requested. The design was to use one of three languages for its base: ALGOL 68, PASCAL, or PL/1. Of the three, PASCAL was the most popular.[5] In 1977 the field of competitors was cut from four to two, and in early 1978, CII HONEYWELL BULL's language design was accepted as the preliminary definition of Ada.[6]

It is important to note that there was a great deal of input from many sources about the requirements of the language. As was stated in the Foreword of the Reference Manual for the Ada Programming Language:

> "The reviews and comments, the numerous evaluation reports received at the end of the first and second phases, the more than 900 language issue reports, comments, and test and evaluation reports received from 15 different countries during the third phase of the project, and the on-going work of the IFIP Working Group 2.4 on system implementation languages and that of the LTPL-E or Purdue Europe all had substantial influence on the final definition of Ada."[7]

The requirements documents, all of which were circulated for comments, went through five revisions. The culmination of this effort was the STEELMAN Report published in June 1978, which set forth the final requirements of the language.[8] Because the importance of the support environment is realized, the same approach used to develop the STEELMAN requirements was used to develop the requirements for a support environment.[9]

Both the Army and Air Force have awarded contracts to build the Ada compiler and develop a program development environment.[10] In their contract, the Army specified that the compiler be capable of running on four systems: the VAX-11/780, the PDP-11/70, the AN/GYK-12, and the Litton L3050.[11] The initial compiler will be designed to run on the VAX-11/780 and will generate code for various target machine environments. The completion of this compiler is slated for early 1983.[12]

CID: 4011963

The Air Force contract initially specifies a compiler to run on the IBM 370 series with future systems including the Perkin-Elmer Corp. model 8/32, the Dec system 10, and the CDC 6600. The completion date is slated for mid-1983.[13] Because some universities and hardware manufacturers have also begun compiler development projects, it is considered likely that there will be a workable full Ada compiler by the end of 1983.[14]

The Ada programming language was completed in July 1980. By December 1980, it was designated Military Standard 1815 [15] with the intent of using the language to create software which will "implement such applications as command, control and communications, fire systems, storage and retrieval, and tactical systems."[16] Ada was submitted by the Department of Defense in April 1981 for approval by the American National Standards Institute (ANSI) and will be submitted by ANSI to the International Standards Organization (ISO) for approval as an international standard.[17] While Ada has been designed to act as common language for embedded computer systems, indications are that it might also act as a standard language for general application computer systems.

AN ANALYSIS OF FEATURES OF ADA

The structure of the Ada language is not unique in itself as Peter Wegner illustrates in the following overview of the levels of Ada's program structure:

- [] Characters, which are the lowest-level atomic constituents of a program;
- [] Lexical units, which are the atomic units of meaning (semantic units);
- [] Expressions, which specify a computation that computes a "value";
- [] Assignment statements, which assign the value computed by an expression to a variable:
- [] Control structures, which can control the sequence in which assignment statements and other statements of the program are executed;
- [] Declarations, which define the attributes of identifiers used in the statements of a program;
- [] Program Units, which associate declarations defining the attributes of identifiers with statements which use them;
- [] Compilation Units, which are the units of structure for program development and separate compilation.[18]

The majority of these features are common to all higher-level programming languages. What makes Ada unique is the versatility of the compilation units. These include procedures and functions, as well as two newer concepts, packages and tasks. Each unit is separately compiled and subsequently placed in a program library. The compiler can then check for syntax errors and error of type compatibility of calls throughout its compilation process. Types will be discussed later.

The Ada Package is considered one of Ada's most significant features. It is defined in the Reference Manual as a "unit specifying a collection of related entities such as constants, variables, types, and subprograms."[19] By grouping these together, it facilitates a logical view of the unit as well as allowing the modularity sought in top-down design. It is a flexible construct which can be used for a variety of functions. One is to create a package which allows the sharing of information in a common area apart from any one program. This is similar to the FORTRAN COMMON block. The difference lies in the fact that data types may also be provided via the package. Another use, which deals with the information hiding feature to be discussed later, is grouping related subroutines. This allows the grouped subroutines to share the same variables while inhibiting access by modules outside the package.[20]

It is the structure of the package which allows information to be hidden from the user of the package. The package is partitioned into two sections. These are the package specification and the package body. The package specification is basically a sequence of declarations. It is divided into a visible part and a private part. Within the visible part are those entities which may be used by units outside the package. The private part contains that which is necessary for the compiler but not for the user of the program. In the package body is contained the code necessary to implement those resources specified in the visible part of the program specification. Neither the declarations nor the code in this section is accessible to the user. An example of a package and its call follows.

```
package RATIONAL_NUMBERS is
  type RATIONAL is private; --hides
                             representation
                             from users
  function EQ (X,Y:RATIONAL)return BOOLEAN;
  function "+"(X,Y:RATIONAL)return RATIONAL;
  function "*"(X,Y:RATIONAL)return RATIONAL;
  function "/"(M,N:RATIONAL)return RATIONAL;
private
  type RATIONAL is
    record
      NUMERATOR:INTEGER;
      DENOMINATOR:INTEGER
                  range 1..INTEGER'LAST
    end record
end RATIONAL_NUMBERS; --end of package
                        specification
```

DOCID: 4011963

```
package body RATIONAL_NUMBERS is
  procedure SAME_DENOMINATOR
            (X,Y:in our RATIONAL)is
  begin
    --reduces X and Y to the same denominator
  end;
  function EQ(S,Y;RATIONAL)return BOOLEAN is
    U,V:RATIONAL          --body of EQ
  begin
    U:=X;
    V:=Y;
    SAME_DENOMINATOR(U,V);
    return(U,NUMERATOR=V,NUMERATOR)
  end EQ;
  function "+"(X,Y:RATIONAL)return RATIONAL
                    is ...end"+";
  function "*"(X,Y:RATIONAL)return RATIONAL
                    is ...end"*";
  function "/"(M<N:RATIONAL)return RATIONAL
                    is ...end"/";
end RATIONAL_NUMBERS:
```

To use the Rational Numbers Package:

```
with RATIONAL_NUMBERS; --make compilation
                         unit visible
procedure USE_RATIONAL is
  use RATIONAL_NUMBERS; --allow unqualified
                        use of +,*,EQ,/,RATIONAL
  X,Y,Z:RATIONAL;         --declare three
                          RATIONAL objects
begin
  X:=3/4;           --rational number creation
                      and assignment
  Y:=6/8;
  if EQ(X,Y)then    --rational number equality
                      testing
    Z:=X*Y;         --rational no multiplication
                      and assignment
  else
    Z:=X+Y;         --rational number addition
                      and assignment
  end if;
end [21]
```

The Ada Task is defined by the Reference Manual as a routine that may operate in parallel with other routines.[22] In essence, what occurs is a simulation of a multi-processing system. Through the use of keywords, execution of task routines can be interleaved. While this is common to assembly level languages, it is not common to higher level languages. Benefits include increased efficiency and "aid in conceptualizing certain applications."[23]

The construct of the task is the same as the package. Consequently, the same information hiding feature is present. The difference is that the body part of a task contains a routine that can be run in parallel with other tasks.

Another prominent feature of Ada is strong typing. The data type determines which set of values and corresponding operations are applicable for a given identifier that has been declared. Strong typing restricts the value and operations of the declared variable to only those that are applicable to the declared type. The type of every variable and expression can be determined at compile time, thereby reducing run-time errors. The attention the programmer needs to give to typing of variables also reduces errors during the writing of the program. The user is given some flexibility in that there are four classes of types. These are scalar types, composite types, access types, and private types. Furthermore, Ada has powerful type-definition capabilities which allow for the defining of new types by the user.

The first class of types to be addressed is scalar, which is subdivided into discrete and numeric subtypes. Discrete, in turn, includes enumeration and integer types. Scalar types can be used for indexing, loop iteration, and choices in case statements and record variants. The enumeration type explicitly declares its values in the type definition. It is useful because it can be used to define finite sets of objects such as colors, weekdays, or directions. The predefined types 'character' and 'boolean' are enumeration types. Numeric types provide the means for performing numerical computations. It can be viewed as being subdivided into integer and real types. The integer type is predefined and consists of a set of consecutive integers. While it has an implicit set of values, a range of values can be explicitly set by establishing a range constraint in the type definition. Approximate computations can be accomplished through real types which are subdivided into floating point types and fixed point types.

Composite types describe arrays and records. An array is an aggregate of identically typed elements which are identified by indices. A record can be viewed as a structured object consisting of named elements of possibly different types. The elements are selected through their identifiers. Composite typing allows a good deal of flexibility to the programmer. The elements in both arrays and records can be manipulated individually, treated as aggregates and/or be directly assigned to compatible structures. The bounds of an array need not be specified until object declaration time. Thus it is possible to define an array with unspecified bounds and allow other arrays to be defined within a specified range. For example:

DOCID: 4011963

```
type INDEX is
  range 1..1000;  --type INDEX is
                    used to define
type VECTOR is
  array(INDEX) of INTEGER;  --array type
                              VECTOR with
                            unspecified bounds
U,V:VECTOR(1..20):  --20 elem vector objects
W:VECTOR(1..10);    --10 elem vector objects
```
[27]

Also permitted by Ada, are records having elements of varying size or type. They may also be defined dynamically, however, the size must be specified at record allocation time.

The last two types to be reviewed are access and private types. The access type is required in order to define a group of dynamic variables. The variables are generated internally and assigned internal names. Because these are not static variables, their existence begins at execution time and ends at the termination of the program.[29] The private type exists as a function of the information hiding feature of Ada. It allows only the name of the type to be accessible to the user. Only internal modules have knowledge of its properties. This is another way to ensure that external programs cannot corrupt local entities.[26]

CONCLUSION

The scope of this paper only allows a cursory look at some of the features of Ada which distinguish it from other higher-level languages. It is a complex language which is capable of a variety of applications. The fulfillment of the STEELMAN requirements appear to have created a language which will satisfy the broad spectrum of applications that exist at the Department of Defense.

The success of Ada relies ultimately on its acceptance by the programming community. The Department of Defense has expended a great deal of time and money in an effort to create a language that will meet its needs. In doing so, they have utilized worldwide resources throughout the computer industry. Participants have included, but were not limited to, universities, private industry, and US government, as well as foreign contributors. Private industry has been encouraged to participate in the process, since it will continue to be a major source of software. Currently, Zilog, Inc. and Litton Systems, Inc. are working on a program which will allow the Ada language to run on Zilog's 16-bit System 8000 and generate code for the 28000 microprocessor family.[27] As an indication of possible international acceptance, both the West German and British Ministries of Defense are developing Ada systems.

The fanfare with which Ada is being presented can be deceiving. Experience has shown that major changes are not quickly accepted. It is important to note, for instance, that the Department of Navy is not an enthusiastic supporter of Ada. One reason for this is that they have already committed themselves to another single language which meets their needs. In this case, the cost-effectiveness of any changes has to be fully considered before they will take place. This illustrates that Ada will not necessarily be accepted with open arms by all. Personal prejudices will have to be overcome.

Efforts are being made by the Department of Defense to combat these barriers. The importance of the Ada Support Environment has been recognized and the same amount of time and energy which has been poured into the language is being placed into its environment. The Department of Defense has realized that if the overall system is not compatible with the user, then the chance of success for the language is limited. In addition, a compiler validation program is being created in order to ensure that all compilers meet the rigid requirements. All proposed Ada compilers must pass this validation test before they will be accepted.

The language uses many software-engineering principles. The textual layout of the program units encourage modularity and top down design. They may be developed independently and then separately compiled. This is particularly useful in a team programming effort. After a common interface has been agreed upon, each programmer may develop, code, and compile his unit. The result would be an interacting program. The ability to hide information within a program unit is another important feature. The control over the access of a program's local variables and the implementation features for that control prevent both corruption of the variables and changes to the body of the program by external programs. Security of a program is also enhanced by the denial of access.

The language is problem-oriented. Various factors work together to shorten the distance between a program's conception and its implementation. This is especially true of the strong typing feature. A programmer must be aware of a variable's type at all times, because the compiler will flag type compatibility errors. Run-time errors may also be flagged because of the ability to place range constraints on variables. For example, if a number should fall out of bounds, the compiler will flag it.

Ada is a powerful language with the ability to perform complex mathematical functions. Current software-engineering principles have been utilized. Efficiency, readability, and maintainability of programs has been stressed. It is able to perform real-time and time-critical operations. Its abstraction facilities encourage the portability of programs. In essence, it fulfills the functional requirements of STEELMAN.

Ada's success, however, will be dependent upon the support environment. The beginning of this paper pointed out that various factors are considered when choosing a language. Most of them were related in some way to the training of the programmer. At present there is not a well-defined training program. The Ada Reference Manual is not adequate as a tutorial. It has been indicated that the Department of Defense is relying on the universities and private software firms to initiate teaching procedures. It is doubtful that this will be adequate.

The complexity of the Ada language is not the only thing working against it. Cost-effectiveness is an important factor. As was noted, the Navy is already firmly committed to its own standardized language. It has to be proved that Ada will be more effective for its purposes before any full commitment will be made. Another question arises when determining what costs are involved in implementing Ada and rewriting current software. The implementation schedule of Ada will affect how well Ada is received. A gradual introduction of Ada into the working environment may, in the long run, be more successful.

While Ada is a powerful language, it was written especially for embedded computer systems and is not all-encompassing. There will be instances where Ada will not be the best language for a given application. Judgments will still have to be made as to which language should be used. If the Ada language is successfully implemented, however, it will cut down on the proliferation of languages in the Department of Defense and, subsequently, cut down software costs.

Footnotes

1. Welke, Larry. "The Origins of Software." Datamation, Vol. 26, No. 12, December 1980. pp. 127-130.
2. Osterweil, Leon J. and Richard N. Taylor. "Notes on Software Engineering." (Lecture). Dept of Computer Science, University of Colorado, Boulder, Colorado.
3. Edwards, Perry and Bruce Broadwell. Computers in Action: Data Processing. California: Wadsworth. 1979.
4. Carlson, William E. "Ada: A Promising Beginning." Computer, Vol. 14, No. 6, June 1981, pp. 13-14.
5. Carlson, p. 14.
6. Buxton, John N. and Larry E. Druffel. "Requirments for an Ada Programming Support Environment: Rationale for STONEMAN." The IEEE Computer Society's 4th Annual International Computer Software and Applications Conference, 1980, p. 66.
7. Reference Manual for the Ada Programming Language. United States Department of Defense. July 1980.
8. Cohen, Paul M. "Ada: A Language and a Concept." 20th Annual Technical Symposium of the Washington, D.C. Chapter of the ACM Proceedings, June 1981, p. 59.
9. Hurwitz, Judith and Paul Kinnucan. "Ada Compiler Programs Get Under Way at Pentagon." MiniMicro Systems, Vol. 12, No. 12, December 1979, p. 35.
10. Cohen, p. 59.
11. Hurwitz, p. 35.
12. Cohen, p. 59.
13. Ibid.
14. Hurwitz, p. 35.
15. Cohen, p. 59.
16. Ibid.
17. Reference Manual.
18. Wegner, Peter. "Programming with Ada: An Introduction by Means of Graduated Examples." SIGPLAN Notices, Vol. 14, No. 12, December 1979, p. 15.
19. Reference Manual, p. D-2.
20. Reference Manual;
    Wegner, Peter. "A Self-Assessment Procedure Dealing with the Programming Language Ada." Communications of the ACM, Vol. 24, No. 10, October, pp. 647-677;
    _____, Programming with Ada, pp. 1-46.
21. Wegner, A Self-Assessment Procedure, pp. 670-671.
22. Reference Manual, p. D-3.
23. Evantoff, William, Gary Anderson, Ronald Price, and Irving Rabinowitz. "Ada: A Significant Software-engineering Tool." Mini-Micro Systems, Vol. 14, No. 4, April 1981, p. 224.
24. Wegner, Programming with Ada, p. 11.
25. Ichbian, J.D., J.C. Heliard, D. Roubine, J.G.P. Barnes, B. Krieg-Brueckner, and B.A. Wichmann. "Rationale for the Design of the Ada Programming Language." ACM Sigplan Notices, Vol. 14, No. 6, June 1979, pp. 6-1 - 6-10.
26. Reference Manual;
    Wegner, A Self Assessment Procedure, pp. 647-677.
    Wegner, Programming with Ada, pp. 1-46.

DOCID: 4011963

MANAGING OUR SYSTEMS FOR PERFORMANCE:

ARE WE GETTING WHAT WE DESERVE? (U)

by [redacted] T3

P.L. 86-36

Psychologists tell us that students who are graded perform better than students who are not graded. While it is not generally realized, the same holds true for computer systems: measuring and reporting their performance induces better performance--not because computers are somehow people-like, but because their managers are.

Yet over the years, the benefits of grading computers--of formulating relevant processing objectives and then scoring system performance against these objectives--have been largely overlooked.

In an attempt to promote objective-oriented performance management practices across our large installations and subsystems, this paper takes a twofold approach:

[] A strong case is presented for the implementation of installation and subsystem performance reporting which is effective, reporting which accurately portrays the ability of the installation to satisfy customer needs and which is sufficiently comprehensive to aid in the ongoing management and administration of the installation.

[] Within the framework of a large, general-purpose Agency installation, the mechanics and pragmatics of implementation are discussed and demonstrated.

Over and above informing and explaining, this paper seeks to move Agency thinking--to persuade and convince Agency managers and implementors that performance reporting can provide a sizable payoff and that the obstacles to reporting performance within a complex processing environment can be surmounted.

MEASURES OF PERFORMANCE

Any serious attempt to report or even discuss system performance requires that the basic components of performance be separated out into measurable dimensions.

[] Availability is normally expressed as percent of a specified time period during which the system was available to the customer. Since the "system" may actually represent the intersection of several subsystems, the determining and reporting of availability in a way that is relevant to the customer is essential.

[] Responsiveness, the time taken by the system to perform a service, is best measured over groupings of like transactions. Typical metrics of responsiveness include:

- average response time per Class Z transaction,
- percent of Class A jobs completed within Z minutes.

[] This writer has found it exceedingly useful to report on a hybrid performance dimension, dependability, representing the intersection of availability and responsiveness: percent of time during which the system was up and reasonably responsive.

[] Productivity describes the amount of product processed through the system over a time period of interest and is normally expressed in terms such as:

- ★ transactions per hour,
- ★ jobs per shift.

[] Reporting the utilization of installation resources and devices fulfills dual purposes:

- Breaking down all work transactions performed by the system into meaningful work categories or "workloads," and then describing the consumption of

OCID: 4011963

installation resources in terms of these workloads, enables the allocation of resources and the relative cost of each workload to be reviewed.

- The aggregate utilization of installation resources across all workloads gives an indication of reserve capacity to support crisis loads in the present and expanded services in the future.

ENSURING PERFORMANCE REPORTS WHICH ARE RELEVANT

Most assuredly, the concept of reporting performance is not a new one. But a survey of our large installations and subsystems would reveal that in many cases, performance reports are conscientiously generated but routinely ignored--because management finds them irrelevant. For other installations, performance reporting is just not practiced, perhaps because a past history of irrelevant performance reporting has cast the concept into benign neglect, or even disrepute. Performance reports fail to be relevant when they are inconsistent with customer perceptions; those which fail to explain or account for irate customers are just not worth the bother of reading. Performance reports achieve relevance when they:

[] focus on meaningful customer objectives; and

[] report on the system's degree of success in attaining them.

Customer objectives may be estimated or negotiated; but no matter how they are arrived at, they should represent real and perceived customer needs. Specifically, customer objectives:

should address activities and services of concern to a large cross section of customers...

over time periods deemed critical by the customer (for example, the prime shift)...

in terms of those performance dimensions which the customer deems critical.

EXAMPLES

System Availability over Prime Shift > 95%
Average Response Time of Transaction < 5 sec.
Percent Class A Jobs Completed in 10 min > 80%

The successful identification of customer objectives virtually guarantees relevant reporting--reporting which documents user satisfactions and dissatisfactions, suggesting the cause of the latter or at least hinting at its origins.

ENSURING RELEVANT REPORTS GET READ

As a rookie journalist quickly learns, an interesting and relevant story is apt to go unread unless it has been headlined and organized to attract and retain the attention of the reader. For just this reason, the daily performance report should resemble stylistically a newspaper article, telescoping the data from most important to least important, from summarizations to specifics.

Analogous to the headline is an executive shift summary, scoring total installation performance against objectives and rendering a rapid determination as to whether and where attention (and further reading) is required.

Intermediate level report segments should break down shift productivity and utilization into categories that are meaningful to management. Lower level report segments should refine problem areas both in detail and by time slice, hinting at suspected problem areas.

Processing exceptions should conclude the report, with inordinate wait times noted and inordinate resource consumption--sometimes the cause of systemwide degradation--attributed.

BENEFITS OF EFFECTIVE PERFORMANCE REPORTING

Routine performance reporting which is:

[] directed at relevant processing objectives,

[] sufficiently comprehensive to support troubleshooting, and

[] organized so as to attract and not deter the reader,

offers many benefits to installation management, tuners, planners, and operators. Yes, operators!

The degree to which an installation is fulfilling quantifiable processing objectives becomes a source of pride, or concern, to its staff. Concern leads to concerted action. But pride or concern, when commonly shared, enhances the esprit de corps of an organization.

Performance reporting exposes the existence of performance bottlenecks which, once uncovered, are not apt to be ignored.

Performance reporting suggests focal points for system tuning, and ultimately enables systems personnel to determine if their tuning efforts have improved (or worsened) the performance of the system.

DOCID: 4011963

The reporting of performance exceptions enables installation personnel to spot resource consumption "hogs" and to take appropriate action. (An offending user is often unaware of his culpability and grateful to learn what he can do to improve his service.)

Performance reporting enables management to determine if the allocation of installation resources among the different work classes is as intended and to determine if priority service is being accorded to priority work classes.

Over the long run, a continuing history of performance reporting enables installation managers and planners to track growth by workload and to anticipate future capacity needs on the basis of continuing trends.

In summary, performance reporting enables management at all levels to accurately assess the quality and quantity of service being delivered, to determine if processing objectives are being met, to evaluate the results of intended corrective action, and to continually gauge reserve capacity with an eye to the future.

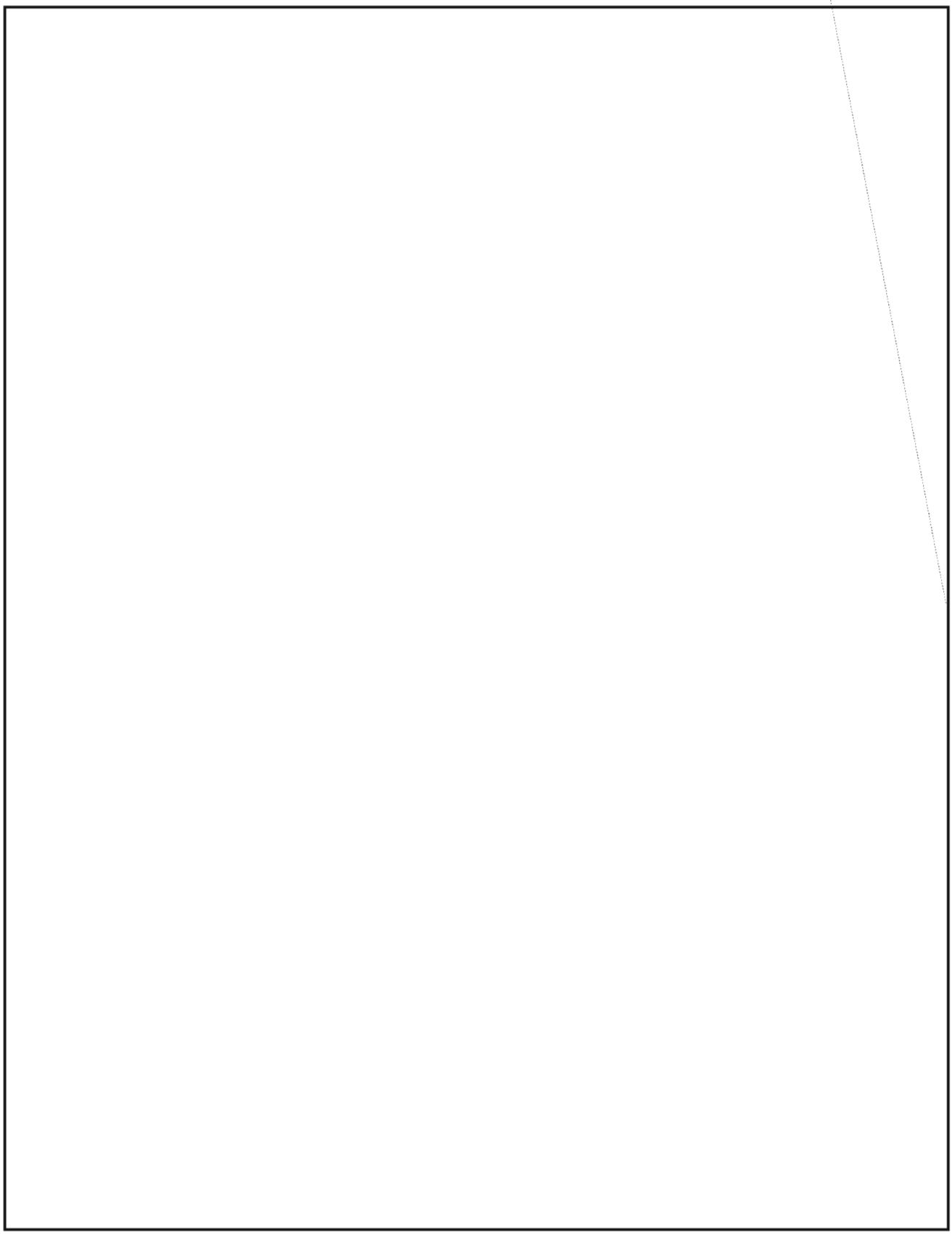
A CASE IN POINT: CARILLON

High-sounding and idyllic as they may sound, these concepts can be put into practice, even in a very complex environment. As a case in point, we will focus upon CARILLON, an Agency installation whose size and complexity ambivalently discourage and demand the management control which only effective performance reporting can provide.

P.L. 86-36

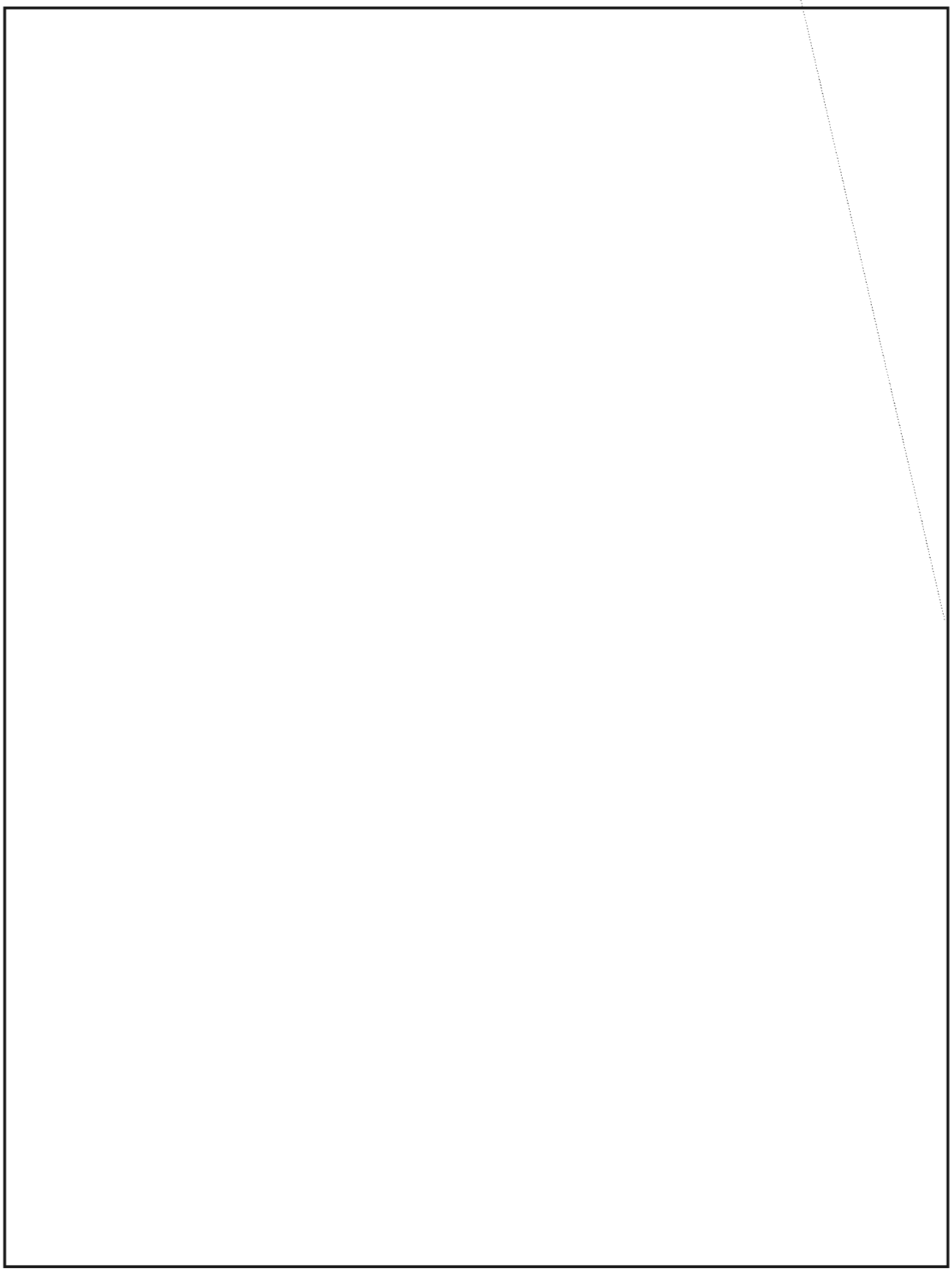
DOCID: 4011963

P.L. 86-36

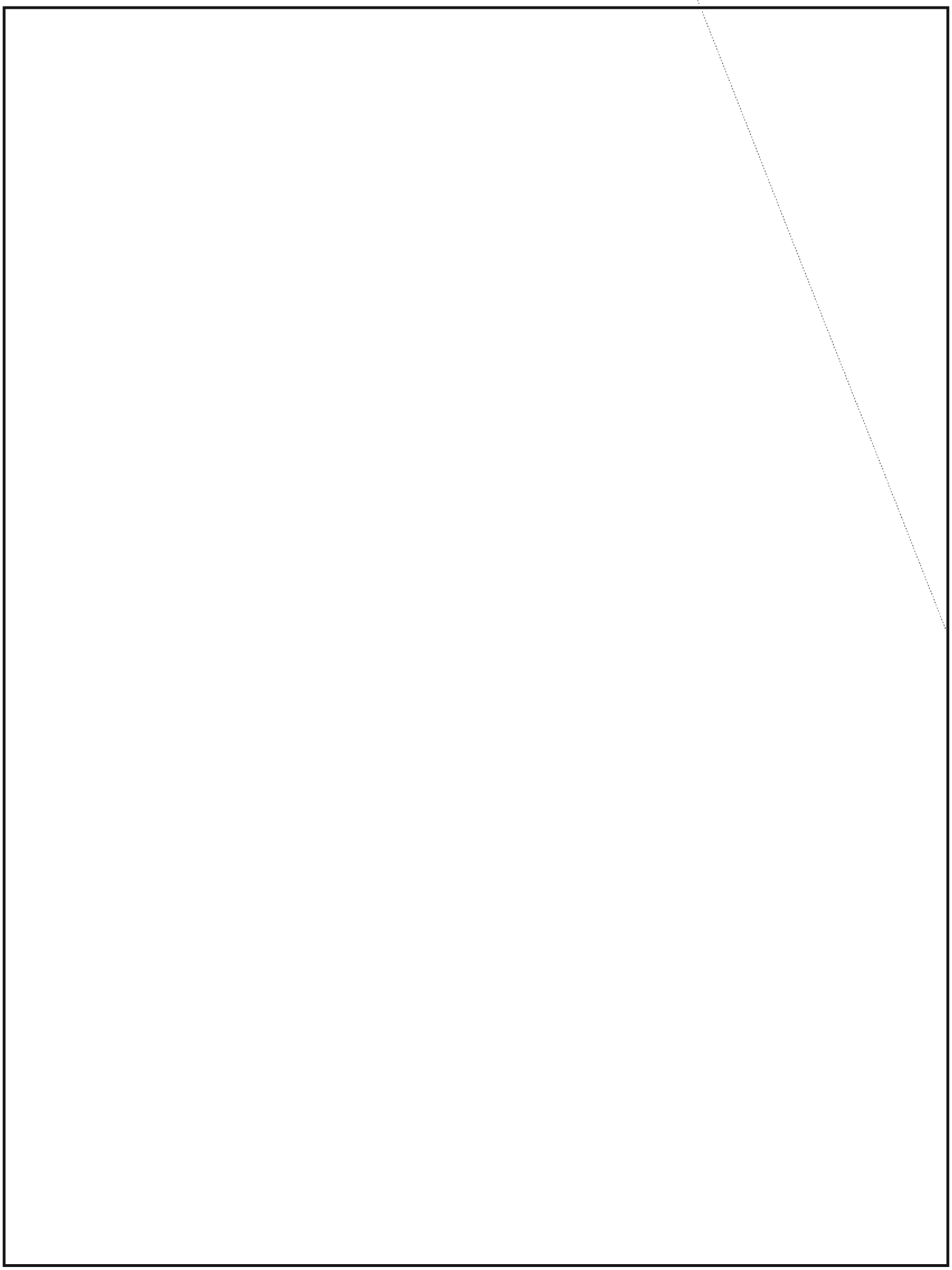


OCID: 4011963

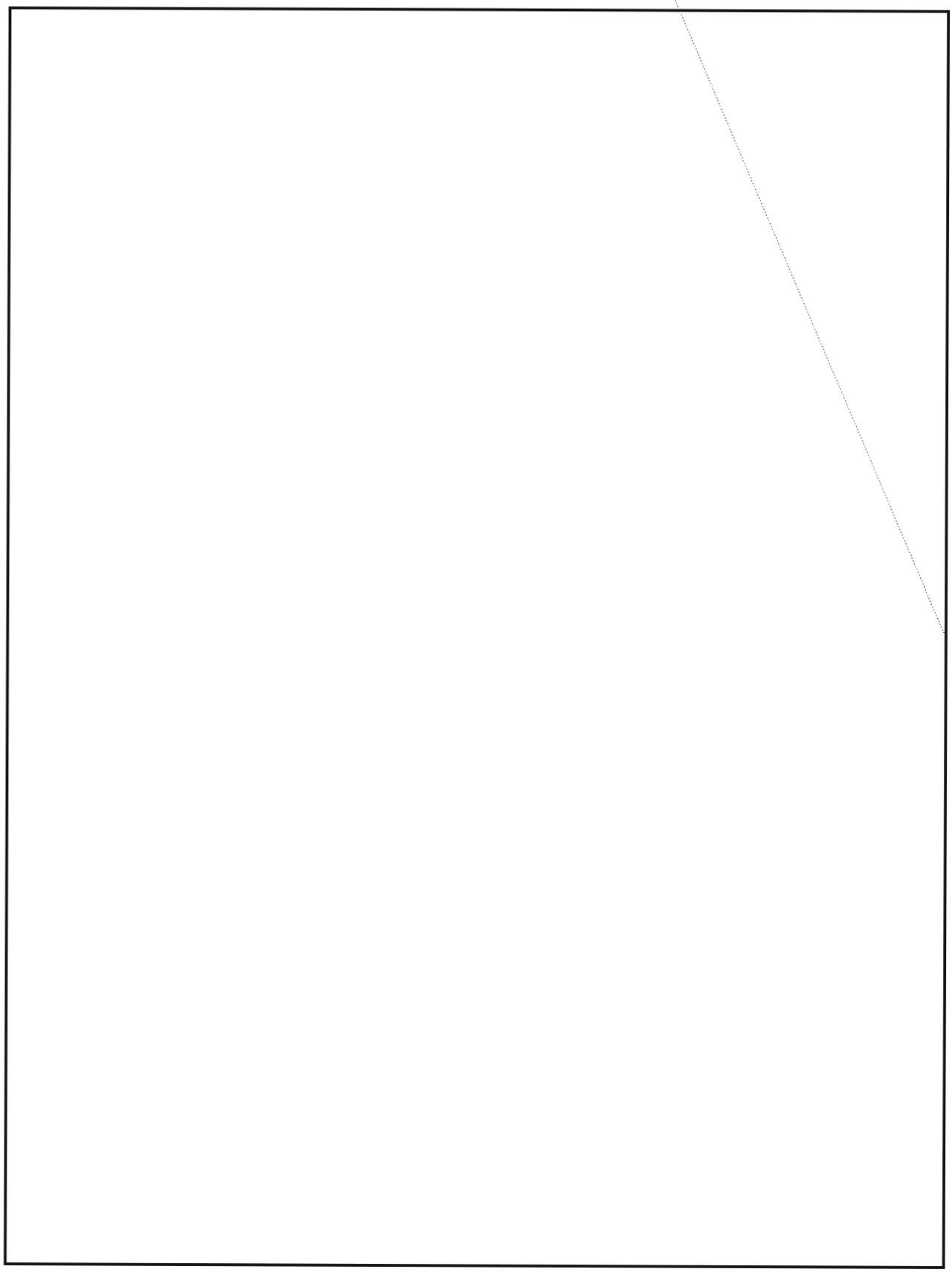
P.L. 86-36

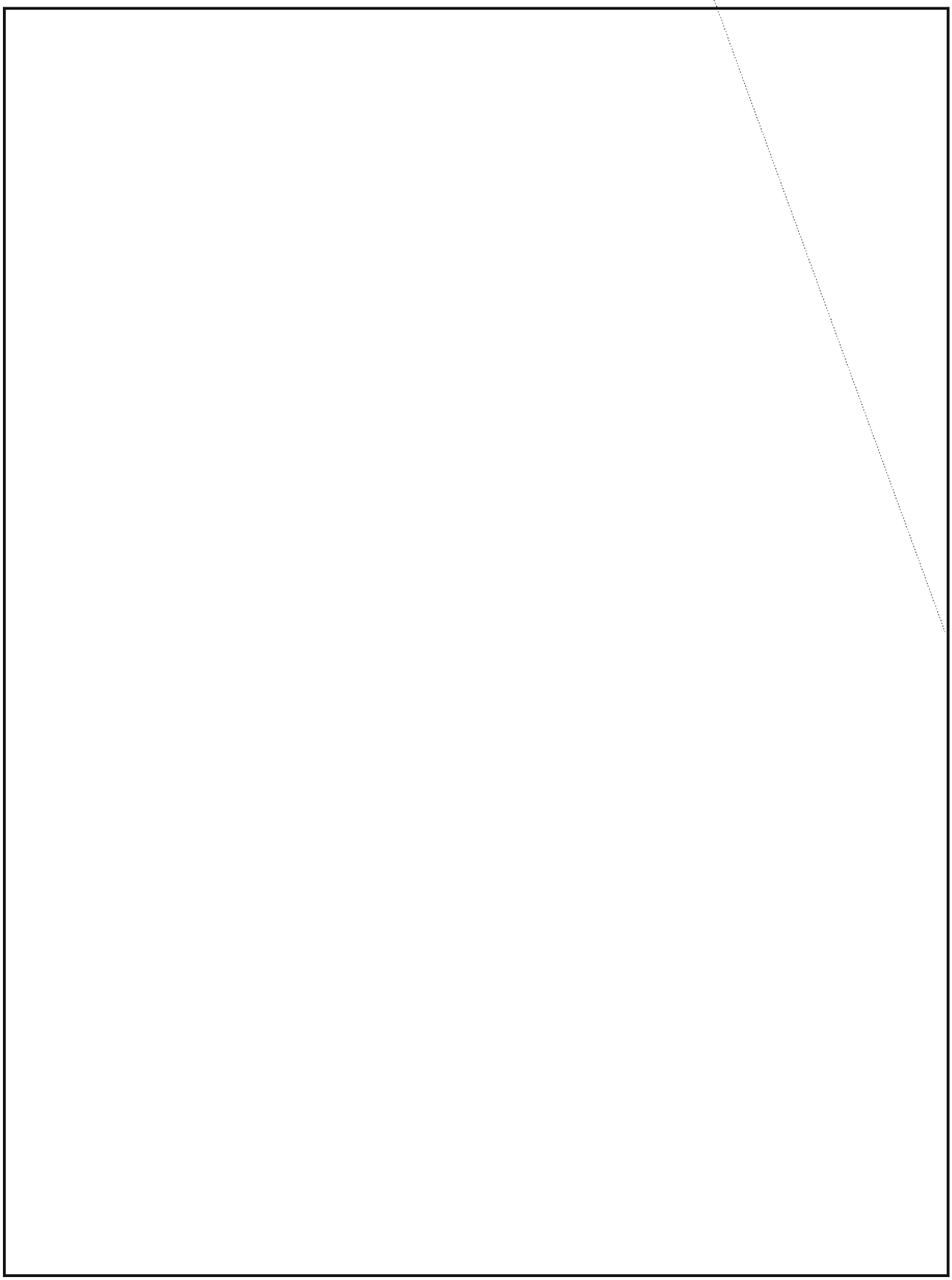


DOCID: 4011963

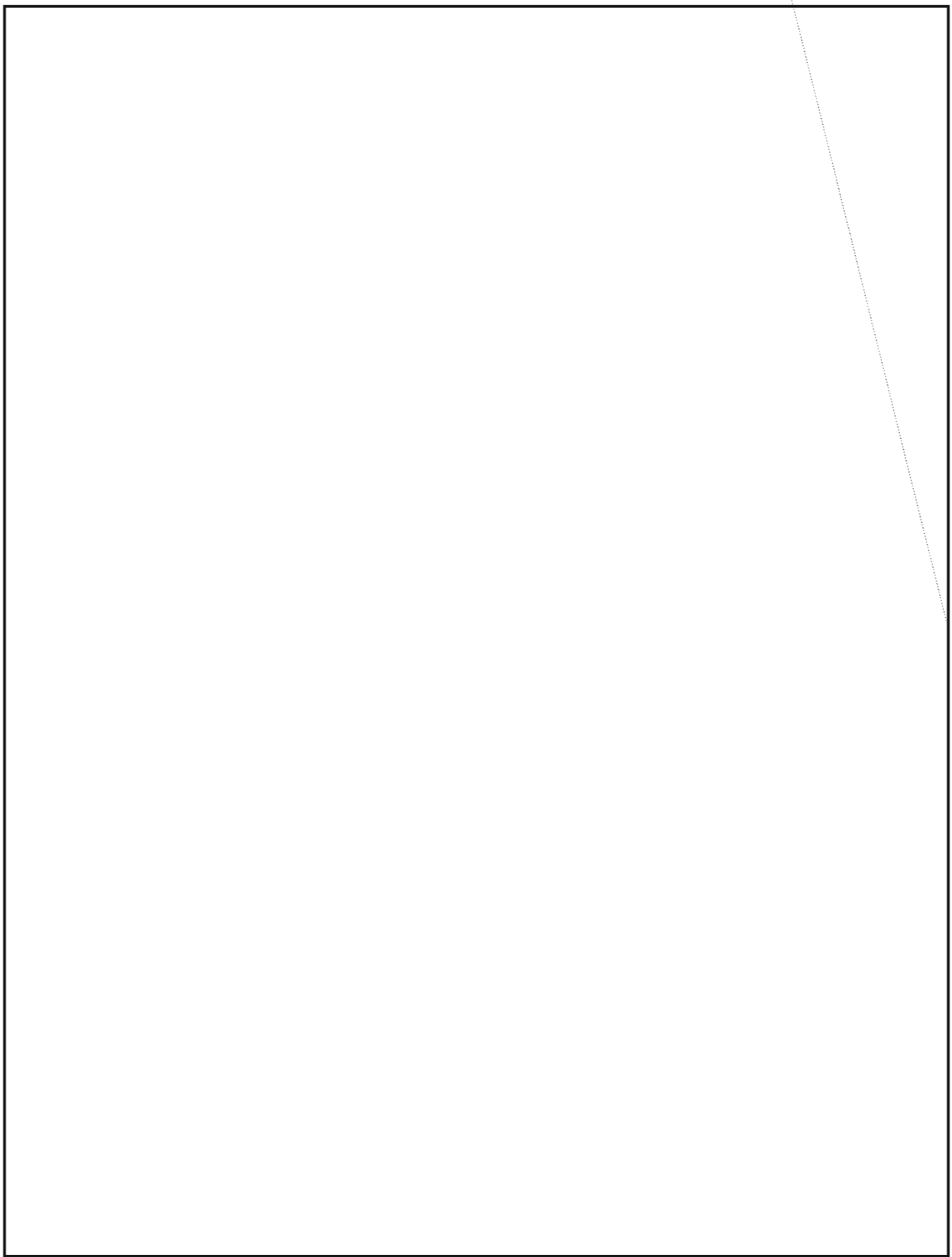


DOCID: 4011963

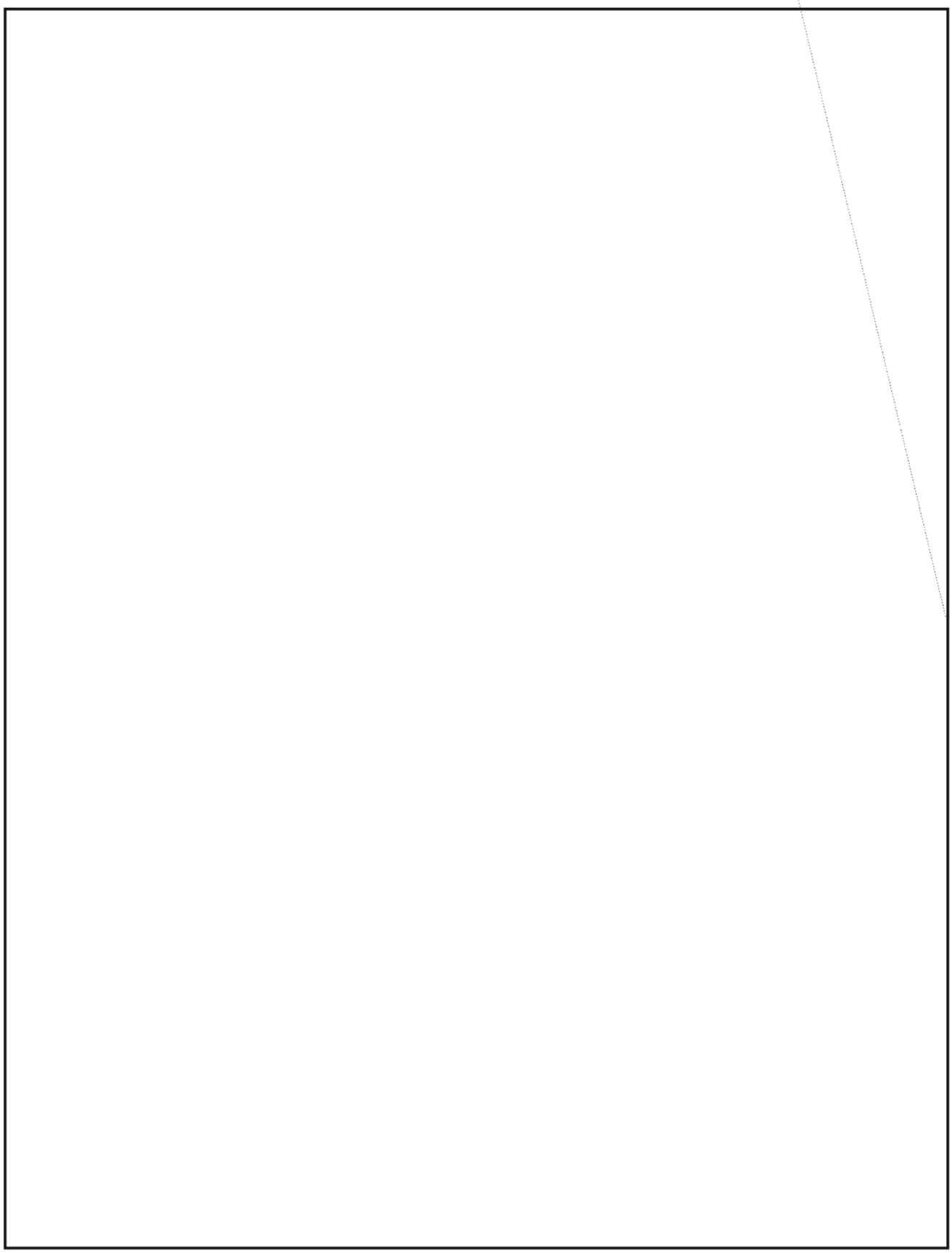




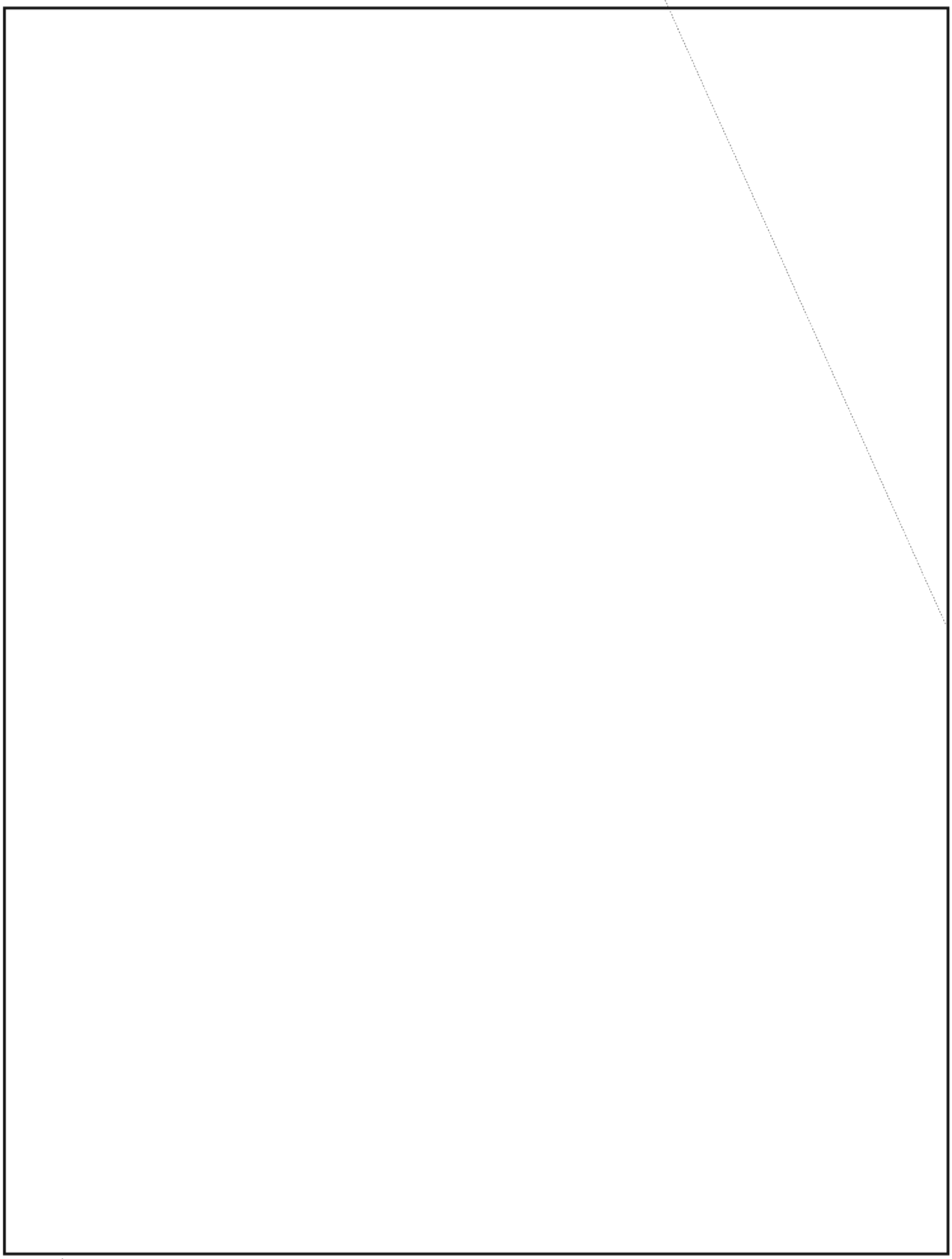
DOCID: 4011963

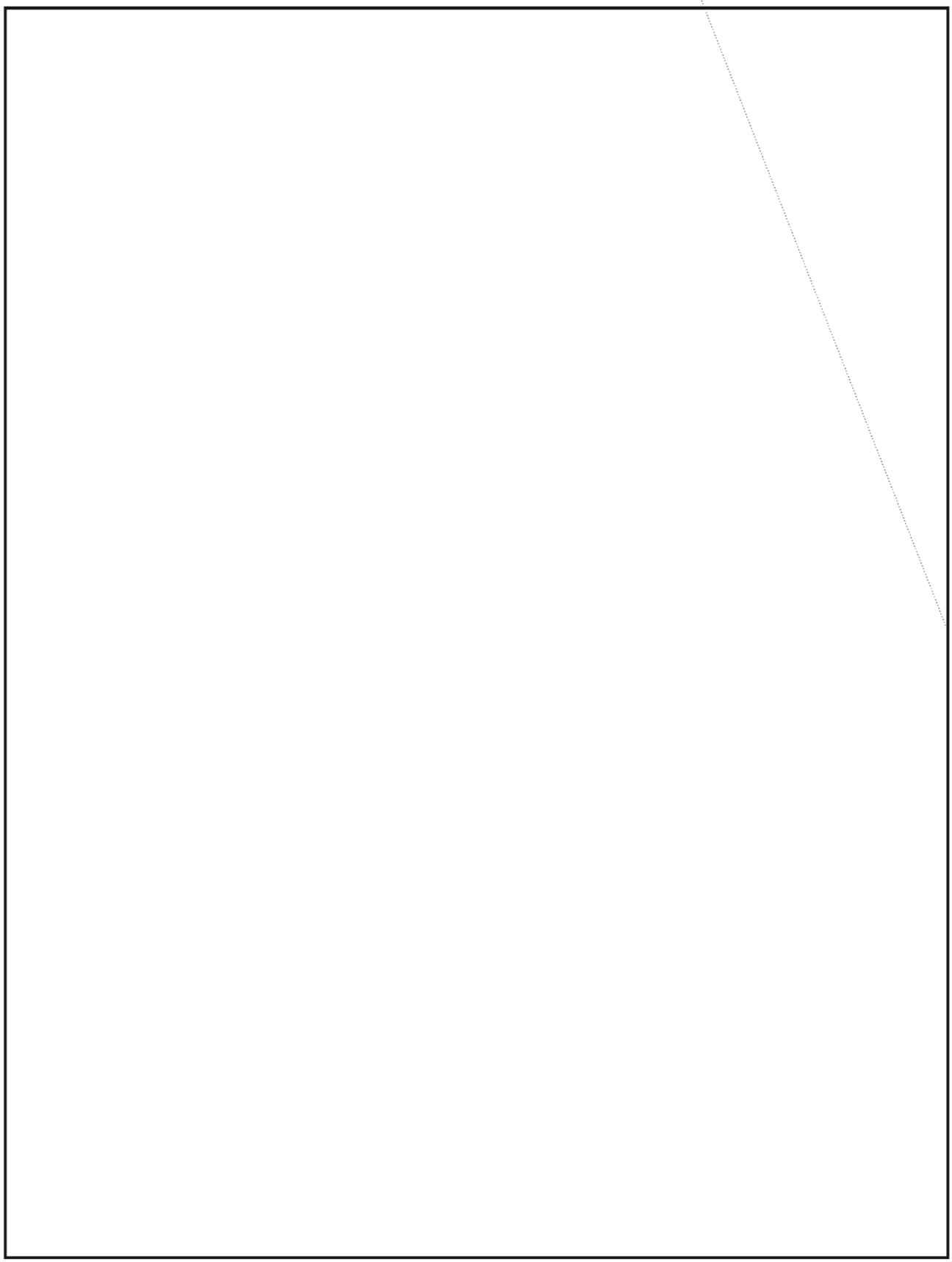


DOCID: 4011963

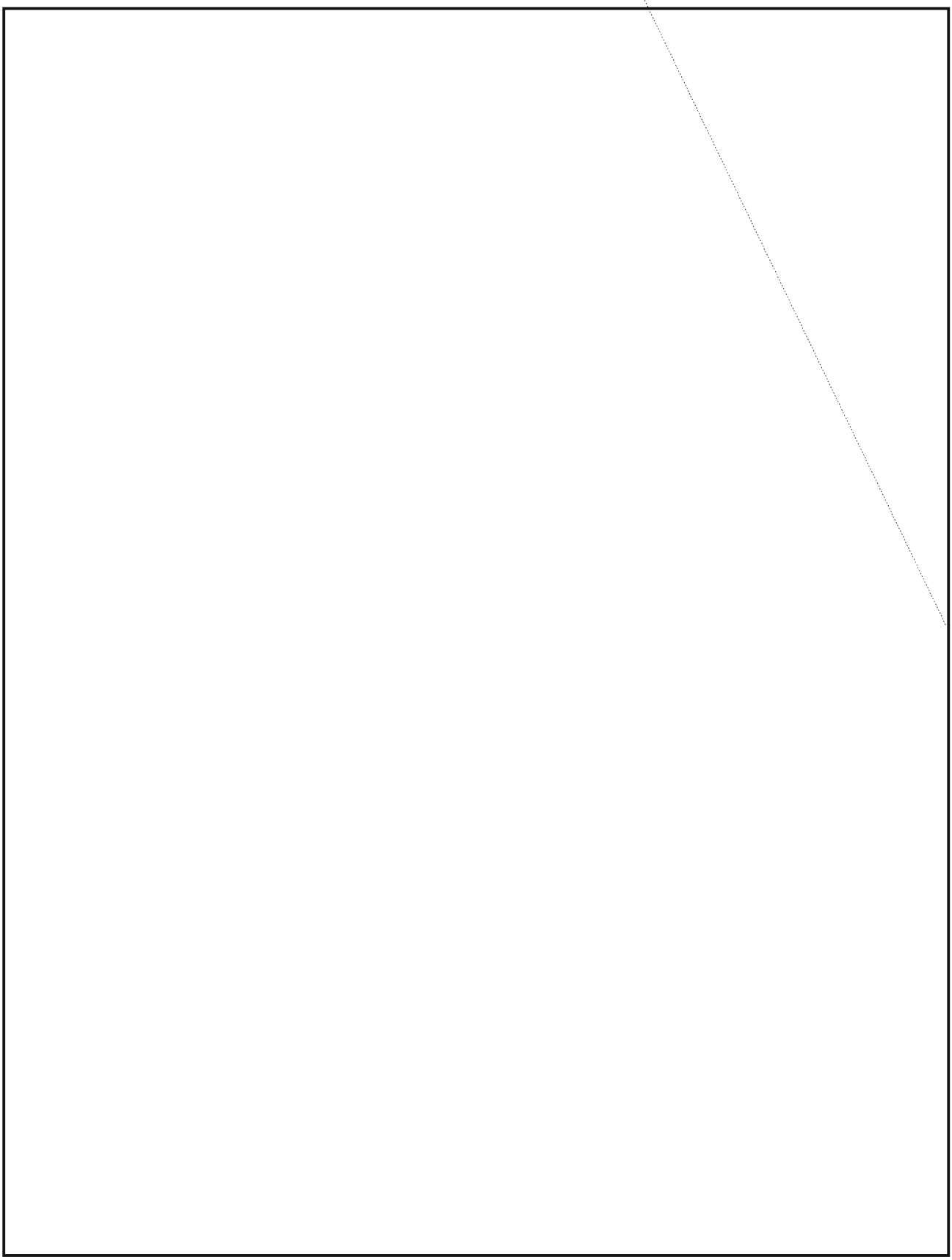


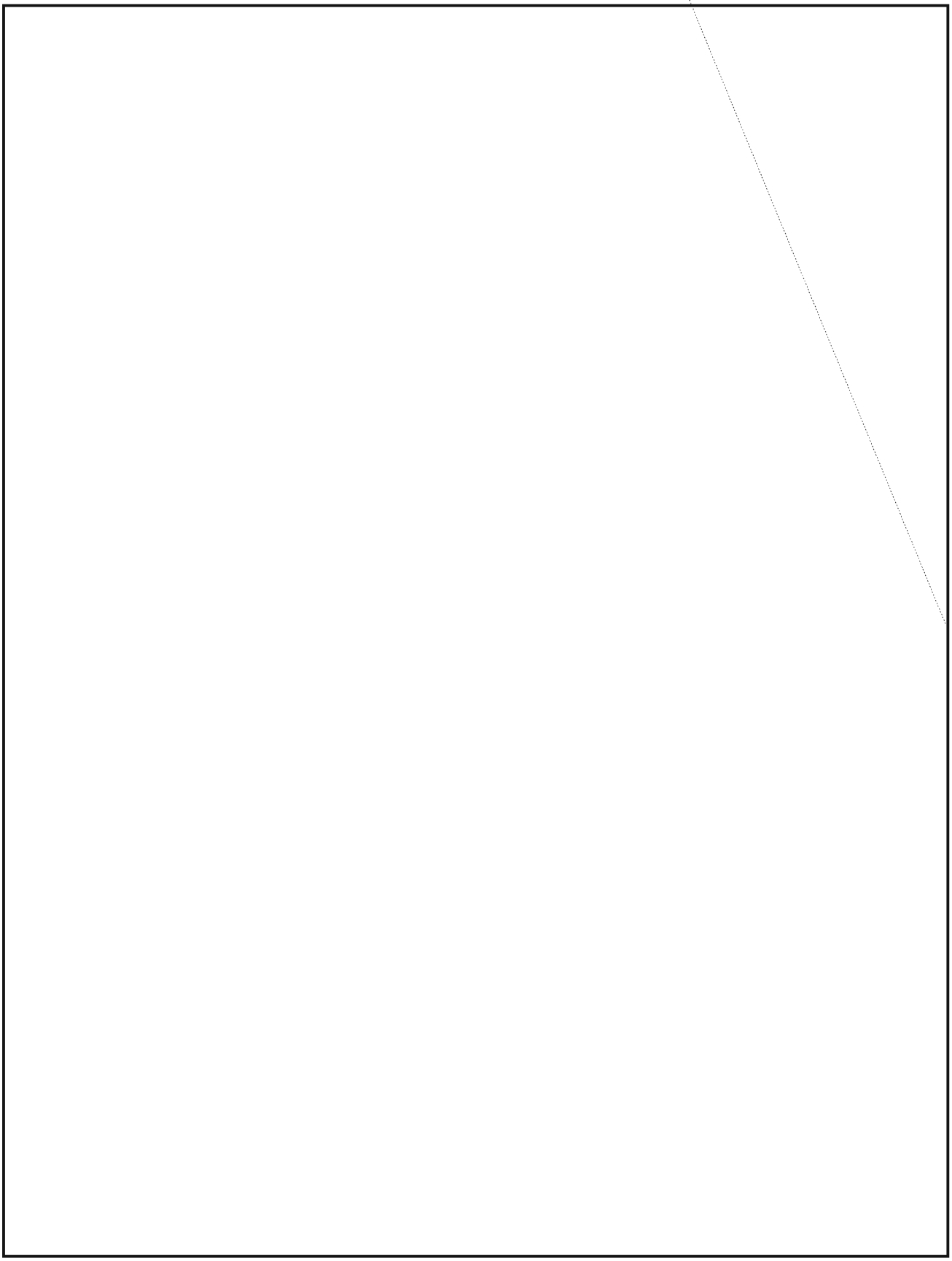
OCID: 4011963

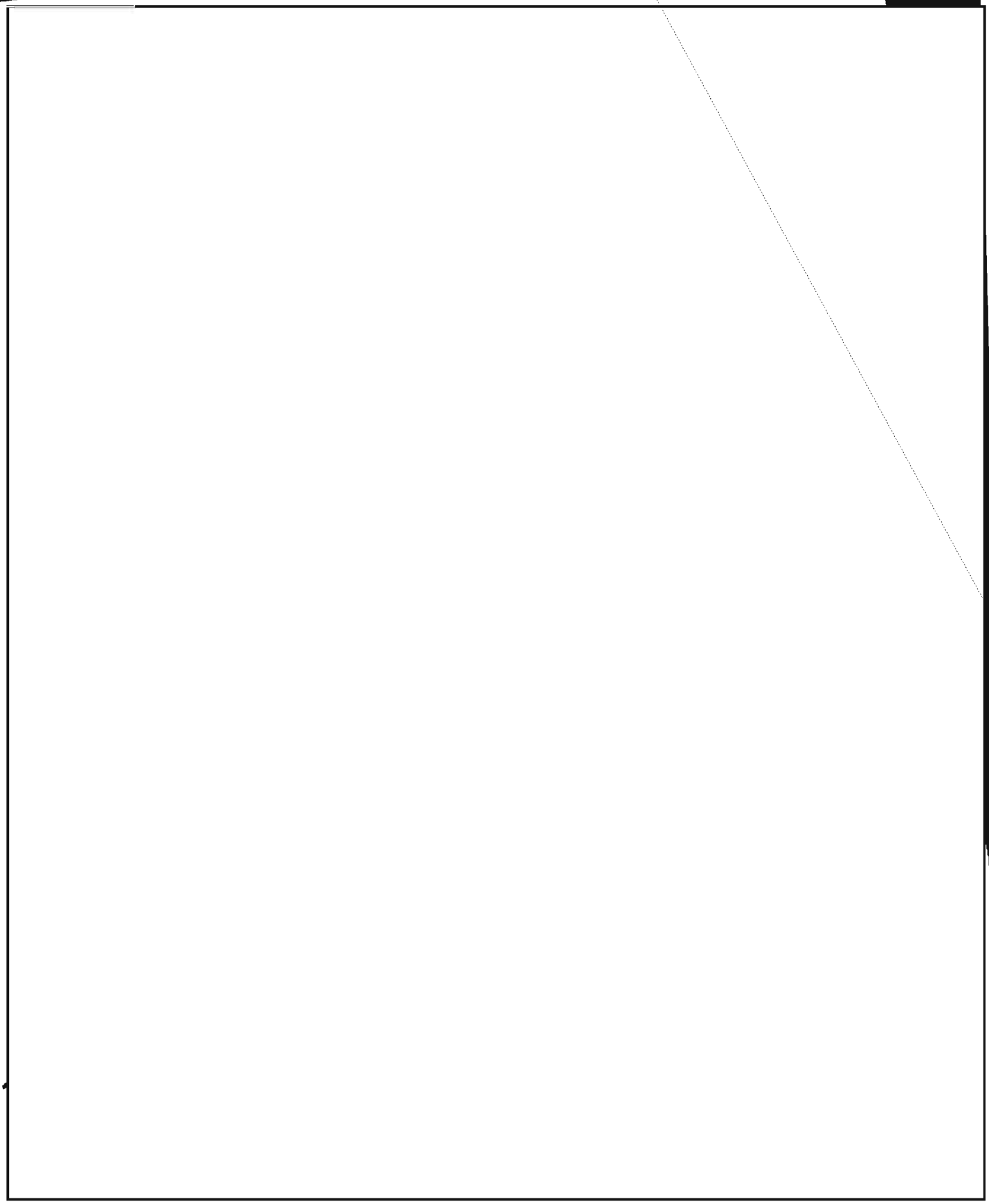




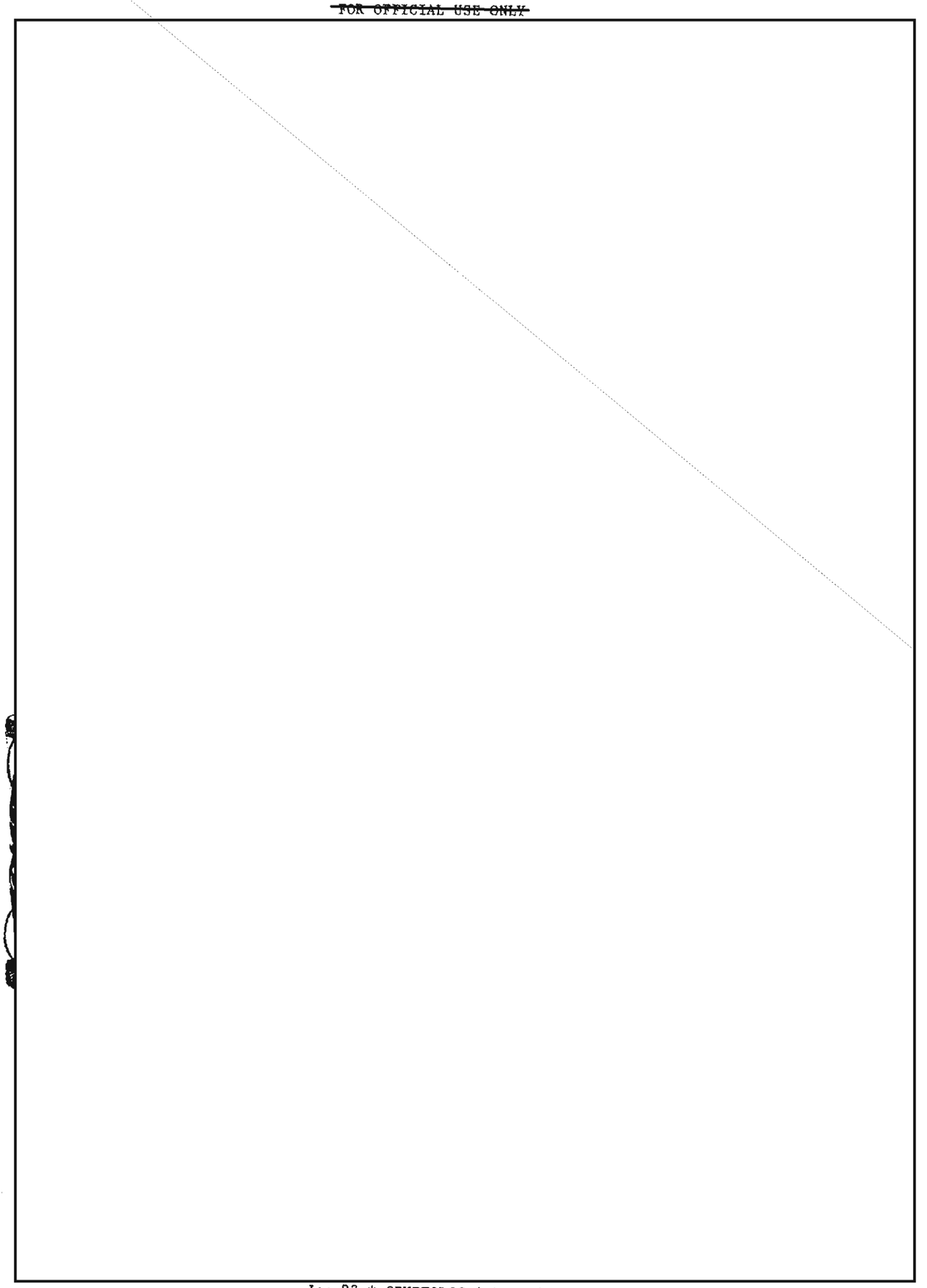
OCID: 4011963





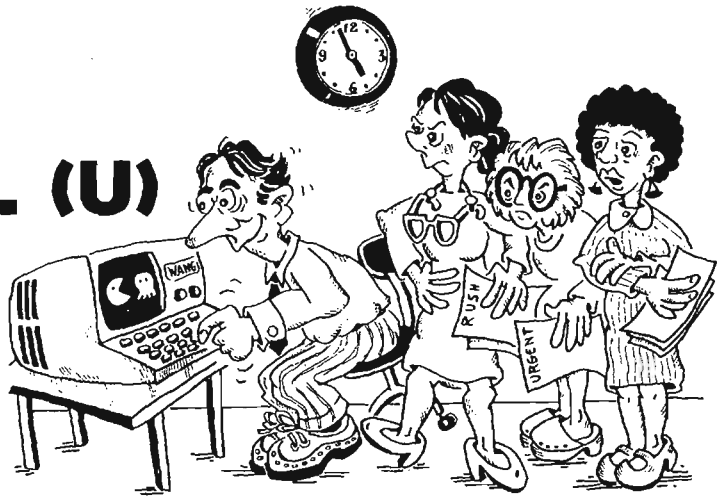


DOCID: 4011963 P.L. 86-36



CID: 4011963

GETTING PERSONAL (U)



P.L. 86-36

by [redacted] T52

Today, with the information explosion fully underway, information managers around the world find themselves trying to cope. NSA is no exception. (U) And as technology marches on, NSA analysts (or "users," as we call them) cannot always keep pace. While discussing how new technology can help NSA manage its information resources, this paper will also examine the human factor: how people fit into the automated information systems picture.

~~(FOUO)~~ Information--its acquisition, processing, dissemination, storage, and retrieval --permeates every phase of NSA operations. The majority of information handling, including research, takes place in the Agency's T5 (Information Resources Management) organization. Here, the battle with the information glut is waged daily.

~~(FOUO)~~ As the need for fast, precise, and complete information has increased, T5 has begun to rely more and more on the speed and accuracy of commercially available information services. Designed for every phase of the information process, (from acquisitions and cataloging to electronic mail and report generation), the automated information system is billed as this era's panacea. The most popularly subscribed-to elixir today is the on-line information data base. Again, NSA is no exception.

~~(FOUO)~~ In its role as Agency information manager, T5 maintains contracts with a myriad of these corporations. Central Research (T5211) alone, where the majority of NSA's on-line information searching takes place, subscribes to five commercial data bases: Lockheed's DIALOG, System Development Corporation's (SDC) ORBIT, the subsystems of the New York Times Information System (NYTIS), the Bibliographic Retrieval Service (BRS), and Mead Data's NEXIS.

(U) Simply stated, the hosts for these multi-file information systems are accessed through leased hardware (terminal/printers), via commercial nonsecure telecommunications networks. Search results are retrieved by keyword and field strings in the appropriate query language, connected with Boolean operators. Results, most often in the form of bibliographic citations and/or abstracts, can be scanned and printed on-line at 1,200-baud rates, or can be ordered off-line for receipt by mail in 10-12 days. Beyond start-up and yearly contract fees, costs include per-hour connect rates for the telecommunications networks and the files, and range from $15.00 to $450.00 per hour, depending on the file accessed.

(U) At first glance these costs may seem high, but when balanced against the savings in person-hours for processing and scanning, storage space, and subscription fees, the commercial systems are actually cost-efficient. DIALOG, with its more than 170 separate information files, is a good example of this efficiency. Why subscribe to, process, store, and scan through the more than 750,000 sources that DIALOG indexes when you can pay a reasonable fee to access just what you need when you need it?

DOCID: 4011963

(U) But these systems are already "old hat." New technology can make what once seemed a revolutionary way of coping with the information explosion seem passe. Applying microcomputers (also referred to as personal computers) to these commercial information systems can greatly increase the speed, accuracy, and usefulness of their services.

(U) The most common application of a microcomputer to the commercial data bases is for reducing a four-minute or more, six-line log-on procedure to a one-keystroke stored operation. This can prevent the personal frustration that often develops when a seemingly simple log-on process turns into an aggravating 20-minute tug-of-war with the system. (That makes the research to follow begin with an already annoyed researcher: a volatile and often disastrous combination!) Since the searcher is already connected to the communications network when he/she is attempting to log on, the time spent is costing money. With the attachment of a personal computer to speed and ease the log-on process, cost efficiency results and mental stability is preserved.

(U) Another practical use for the personal computer attached to the commercial data bases is for storing frequently-run queries. Although the systems already have a query-saving (by number) capability available for a small monthly fee, there is no provision for cross-saving a search from one system to another. The query would have to be saved under a different number in each system checked. The personal computer could "can" the query and dump it into a file that could be consulted quickly before a query is run to make sure it hasn't already been searched on the systems. With some sophisticated programming, the personal computer could translate a query saved in the language of one system into that of the others and run the search against them as well. It could even be instructed to "weed out" the duplicate citations after they are retrieved.

~~(FOUO)~~ Saving an NSA item of interest in our own terminal instead of the system sponsor's also seems a bit more private. Although all information on these commercial data bases is unclassified, it is wise not to call undue attention to our topics of interest by storing them out in plain view, under our sponsor-provided password.

~~(FOUO)~~ The personal computer could also be programmed to remind the analyst when an update of a saved search should be run, to whom it should be sent when completed, etc. When electronic mail becomes a more widespread reality at NSA, the personal computer could be networked to other microcomputers in other organizations. Search results could be delivered without hardcopy printing ever taking place.

(U) Most microcomputers on the market today can be programmed in a variety of languages, including BASIC, POGOL, PASCAL, PILOT, and LOGO. Many come with basic programs preset on floppy disks or offer "how-to" floppy diskettes (also called "floppies") that instruct the user in programming his/her own personal computer.

(U) The microcomputer can offer the professional information manager/searcher the opportunity to somewhat "polish" the product before supplying the retrieved information to the client. Headers and comments could be added, duplicates or "false drops" could be removed, typos corrected. In striving to fulfill a mission of providing the most accurate information available in a reasonable period of time and in its most usable form, editing capabilities like these could aid the information analyst.

(U) The hottest use yet, however, for microcomputers attached to commercial information data bases, is data downloading. "Downloading" is a process by which information being retrieved from one system is written onto a medium (most likely diskettes) of an attached microcomputer for future retrieval, editing, or storage. Once this data is written onto the disks, there is really no need to ever pay for retrieving that same information again. When a similar request is received later, the information is provided to the requestor without the costs incurred by rerunning a search.

(U) The diskette can be labeled and filed, or be indexed in a directory on the personal computer for future use. Floppies can be written over when their content has served its purpose. They have a long life, when stored properly, but their file integrity is somewhat susceptible to physical maladies such as scratches.

(U) Requestors could begin to scan their own search results instead of having the knowledgeable, but not omniscient, information specialist determine which retrieved items are pertinent and which are not. The client can determine which items he/she would like to have and print them out, or in the day of

DOCID: 4011963

electronic mail, receive, scan, and store the pertinent information in soft form at his/her own desktop terminal.

~~(FOUO)~~ Audit and security trails are always of interest in our line of work. The microcomputer can record the various use and performance statistics monitored for these on-line data bases. Central Researchers currently record manually their on-line time and charges, summaries of requests, communications network accessed, and results on a systems logsheet. The microcomputer could easily monitor all this information automatically and also provide monthly statistical summaries, including audit trails and user performance charts. On some models, packages for producing color-coded graphics for this type of information are available. These statistics could then be employed in identifying problem areas, searchers who may need extra training, billing irregularities, and the general effectiveness of the information tool.

~~(FOUO)~~ The microcomputer could contain the on-line tutorials crucial to properly accessing these systems with a minimum of aggravation. With more than 10 query languages to learn and employ in Central Research, the simplest of procedures can often become confusing! The microcomputer could provide logically organized menu screens and step-by-step instructions for the various systems. The searcher could refer to these instructions as he/she performed the search on-line. On-line time spent floundering around in "trial-and-error-land" is expensive and could be alleviated with this capability. No new technology is really helpful unless people can use it.

(U) The human factor--how people fit into this picture of automated information management--is and should remain a concern of systems designers and consumers. With much of the work force still experiencing "Technofear" (also known as "Technophobia," fear of technology), "Technomaniacs" must beware of so complicating an information specialist's tools that the information research process becomes the search for the Holy Grail!

(U) The increasingly frequent appearance of on-line tutorials, "help" screens, and logically layered menu screens indicates that some designers are already paying attention to the human needs of their consumers. The demands of executives, who do more and more of their own research and on-line report generation, were for easier-to-use working aids. In response, designers are moving away from voluminous technical hardcopy "how-to" system manuals full of coded fields and technical lingo to "English-y" user-oriented on-line instructions and brightly-colored, almost tempting, keyboards.

(U) The "user-friendly" concept, an integral aspect of any attempt towards creating a healthy person-machine relationship, is well worth the effort devoted to countless studies on the subject. These studies show people much more inclined to use (and, as studies prove, use correctly) a system that talks to them, as if in conversation. The concept of on-line (usually an interactive session, like volleying in a tennis game) means that both participants (the user and the host computer) must do their part. Chances are that if a user is uncomfortable with a language or terminal, an input error will occur, and the host computer (sympathetic, but without human compassion) will reject the input. The result: user frustration and incomplete research. On-line tutorials and working aids provide the user with a convenient, quick place to look for the proper formats and phrases. Since logging off to look for instruction in some manual is impractical and rarely done, the on-line aid can solve many problems before they have the chance to develop.

(U) A correctly chosen personal computer can become almost a friend or interpreter to the on-line searcher. The importance of the proper training in how to use the microcomputer and concentration on what it can do to help (not usurp) the role of the information specialist should be emphasized when introducing users to new technology. Personal computers should be chosen with a number of things in mind, including: design and capabilities, naturally; compatibility with other systems; the selection and functions of its peripherals; "creature comforts"; and costs. Will information managers be inclined to sit at this terminal and use it for that purpose for which it was purchased? Or will they be so intimidated by the looks of it alone that they will avoid it like the plague or pray for an early retirement? Is it of a comfortable height? Is there ample legroom? Is the keyboard well-labeled? Is the color-type contrasted comfortably with the background screen? Is the screen designed to tilt at a natural reading angle? Is it noisy? Are the diskettes easy to load and remove? Is there room for growth? Will it still be cost-efficient in five years? Are there peripherals that can be purchased later to expand existing functions? These questions and many more must be asked before choosing a personal computer that many different people, including Technophobics, will have to access daily.

DOCID: 4011963

(U) Unfortunately, one of the reasons these human factors are often overlooked is because those who determine which equipment to procure are most likely neither Technomaniacs nor Technophobics--they are most often Bureaucrats. But a personal computer, or any technological device, chosen at least partially with its users in mind, can aid the employee in accomplishing his/her tasks, increasing productivity and success, and developing a healthy person-machine relationship.

(U) This paper has stressed both cost efficiency and the human factor in applying personal computers to the commercial data bases at NSA. Perhaps we should also take a look at the initial financial investment required to obtain and implement these ideas.

(U) Costs for the average microcomputer (see charts below) ranges from $600.00 to well over $5,000.00, depending on the capabilities desired in both the software and the hardware. With each personal computer marketed, compatible software packages are also sold at additional costs. Peripherals like CRT's, printers, modems, disk drives, and Tempest packages also add up. Adequate supplies of floppies for stored data and preprogrammed disks are reasonably inexpensive, but they are still an additional cost. It is safe to say, however, that with the proper forethought and investigation (including observing how these microcomputers perform in actual workcenter settings), and by considering the uses for and the users of the proposed microcomputer, the initial investment could easily repay itself within a 1-to-3-year period. Applying carefully selected and well designed technology to prevent waste, increase productivity, and improve morale is almost always cost-efficient.

FEATURES	COMMODORE 64	APPLE II+*	IBM® PC	TANDY TRS-80® III	ATARI 800®
Base Price*	$595	$1530	$1565	$999	$899
Advanced Personal Computer Features					
Built-in User Memory	64K	48K	16K	16K	16K
Programmable	YES	YES	YES	YES	YES
Real Typewriter Keyboard	YES (66 keys)	YES (52 keys)	YES (83 keys)	YES (65 keys)	YES (61 keys)
Graphics Characters (from Keyboard)	YES	NO	NO	NO	YES
Upper and Lower Case Letters	YES	Upper Only	YES	YES	YES
5¼" Disk Capacity Per Drive	170K	143K	160K	178K	96K
Audio Features					
Sound Generator	YES	YES	YES	NO	YES
Music Synthesizer	YES	NO	NO	NO	NO
Hi-Fi Output	YES	NO	NO	NO	YES
Video Features					
TV Output	YES	EXTRA	EXTRA	NO	YES
Input/Output Features					
"Smart" Peripherals	YES	NO	NO	NO	YES
Software Features					
CP/M® Option (Over 1,000 Packages)	YES	YES	YES	YES	NO

MAKE & MODEL	Victor 9000	IBM PC	Xerox 820	Apple III	Radio Shack TRS80 Model II
Processor Type	8088	8088	Z80A	6502	Z80A
Word Length	16 bits	16 bits	8 bits	8 bits	8 bits
Memory Size (Internal)	128-896KB	16-256KB	64KB	96-256KB	32-64KB
Storage Capacity on 2 Floppies	2400KB (5¼")	640KB (5¼")	160KB (5¼")	280KB (5¼")	960KB (8")
CRT Display Standard Format	80 x 25	80 x 25	80 x 24	80 x 24	80 x 24
Alternate Format	132 x 50	None	None	None	None
Graphics Resolution	800 x 400	640 x 200	None	560 x 192	None
Communications Built-in Serial Ports at no extra cost	2	0	2	1	2
Built-in Parallel Ports at no extra cost	1	0	2	0	1
Human Factors Keys on Keyboards	94-104	83	96	74	76
Detached Keyboard mechanism	Yes	Yes	Yes	No	Yes
Tilting Display mechanism	Yes	No	No	No	No
Swiveling Display	Yes	No	No	No	No
Desk Area Required (Approx. Square In. with 2 floppy disks)	310	420	470	381	500
Operating System Supplied Standard	CP/M-86* MS-DOS	None	None	Apple DOS	TRS DOS

NOTE: Chart based on manufacturer's information available as of April 4, 1982.
*CP/M is a registered trademark of Digital Research, Inc.

DOCID: 4011963

Menu Selection as a Tool for Human/Machine Interaction (U)

P.L. 86-36

by [redacted] E53

(U) During the past decade, system designers and applications programmers have come to realize that the most unpredictable component of an interactive program in terms of performance is the user interface. By its very nature, an interactive program must deal with many factors that need not be considered when developing a conventional non-interactive program. Primarily, the applications programmer must consider the "human factors" aspects of the program-user interaction, since the success or failure of an interactive program depends mainly on its ease of use [1]. Because the user interface design has such a strong impact on program acceptability and usefulness, it becomes very important to design good interactive user interfaces. One technique being used more frequently to promote good human/machine communications is menu selection.

(U) A menu consists of a list of items, usually displayed along the screen border, from which a user makes a selection. These items can be represented numerically, graphically, or by text. In each case, the user can choose an item using one of several techniques, e.g., pushing a numbered key corresponding to the number of the choice or positioning a light pen over the choice as displayed. There are other ways of interacting with a computer display: command languages, function buttons, and transaction codes. However, these methods do not provide an interactive interface for the naive user which is as user-friendly as menu selection. By definition, a naive or casual user is a person who has little, if any, training in computer science and is unfamiliar with the internal workings of the computer. This person's job description does not mandate the use of the computer. However, if the computer can get the job done better and faster, without losing data and can be operated without extensive training, the casual user will be more likely to utilize this resource [2].

(U) A well-written menu utility is the perfect interactive tool for both the naive and sophisticated user. With a menu, the user does not have to remember commands or syntax and is less likely to make errors with all the valid choices displayed. Since making a selection can be as simple as pushing a button, the amount of time spent typing commands and studying documentation is reduced. In addition, a selection menu provides more flexibility than fixed keys when changing or updating functions. Although a well-written menu utility provides both types of users with a good interface to the computer, a poorly designed utility can have the opposite effect. A poorly designed menu utility could force the user to page through a large number of levels to perform an operation. This is annoying, especially when the response time between selections is very slow. A system which provides no feedback to the user that selections are being received and processed is another example of poor design. The next section of this paper will focus on the features necessary to design and implement a menu utility which provides a good user interface.

MENU SELECTION IMPLEMENTATIONS

(U) A well-written menu utility offers both the sophisticated and naive user a good way to interface with an interactive graphics system. Menus usually consist of a number of choices listed for the user from which he or she may choose an operation or command to be performed. This type of selection may be implemented very simply by typing the desired

OCID: 4011963

response on a keyboard or by selecting the desired option via touch panel, light pen, mouse, or any other interactive input device. The options may be presented in a list across the bottom of the screen or along one side, or they may be represented graphically as icons. (An icon is a pictorial symbol used to represent an idea or entity.) The menu may only be displayed at the user's request, in which case a movable menu could appear close to the cursor to minimize movement.

(U) In more advanced systems, such as SMALLTALK [3], the screen may be divided into several windows, each with its own menu. Only one window at a time can be interacted with; it is indicated as active and in the foreground. A different window can come into the foreground by activating its menu. Thus, by designing a system which simulates how someone might work at a desk with various papers spread out on top of it, an interface is created which is close to the actual working conditions of the user. By choosing from different menus, the user can manage several simultaneous tasks and contexts, alternating between them at his or her convenience. Though menu selection may be implemented using many different methods and formats, the advantages offered by a menu utility are similar from one implementation to another.

MENU SELECTION: ADVANTAGES

(U) Although a good menu utility offers many advantages as a user interface, perhaps the most important is that little training is required of the user. In all of the graphic systems investigated and reported in a later section of this paper, the user was found to be a professional in a non-computer-related career field. A menu utility could save the casual user from extensive training time by presenting a range of alternatives from which to choose. Since only valid choices are included in the menu, the user is protected from making an invalid selection. This may also serve as a security feature if the user is shown only the names of operations he or she is authorized to access.

(U) Because the user is prompted with a repertoire of commands, he or she is relieved of the burden of remembering command names. By giving the user the ability to point to material currently displayed, this material can be treated as input, drastically reducing the amount of typing to be done, saving time and preventing errors [4]. There are only a limited number of choices in a menu, so that designing effective user aids such as a "HELP" key should be easier than when the user has an unlimited number of options. The programmer should have less complicated error handling and documentation to write than with a system which requires the user to know what each command does and when to type it [5]. A menu utility is generally more flexible with changes in the application or requirements, since it is easier to change or add menu items than it is to change or add new function keys. For the many reasons cited above, menu selection is becoming a popular tool for those tasked with designing interactive systems.

MENU SELECTION: FEATURES

(U) Once the decision has been made to write a menu utility, the designer must be aware of the many features it should include to be a successful tool. While some of these features were promoted by most of the listed references, the usefulness of others may be more dependent on the particular application. Generally it was felt that menus should always be numbered starting with one instead of zero, since that is how people begin to count. The menu should be kept short using submenus if necessary. However, these submenus should not be nested more than three or four levels deep. An option for longer menus that cannot fit on one screen is a scrolling mechanism to allow the user to browse through the menu which has choices listed alphabetically.

(U) A very important feature is the use of feedback to provide reassurance to the user that the selected operation is acceptable and is being processed. The user should be able to respond as soon as the choice appears and should be informed if the system is slow and the process will take a long time. According to Miller [6], both experienced and novice users may tend to become bored and frustrated if an interactive system takes more than 15 seconds to respond to their query or command. Schneiderman agrees that long delays are usually disruptive and disturbing, but he says that "the variance of response time may be as critical as the mean response time." [7] He suggests that performance and satisfaction may improve if responses are delayed to minimize variance and also suggests informing users of the estimated waiting time as another tactic. Another way of giving feedback to the user is by highlighting or increasing the brightness of the menu item chosen [8]. Feedback could further be provided by blinking the item on and off, drawing a box around it, or changing colors to indicate an "ON" state [9].

OCID: 4011963

(U) Another important feature of a menu utility is the provision of special keys or functions to aid the user. Martin says that a "help" key or option can be a psychologically valuable device to minimize the potential confusion and hostility of the unskilled operator [10]. Once the user chooses the "HELP" option, a "HELP" conversation could begin with a menu screen giving possible categories where help is provided. After being helped, the user must have access to a "CONTINUE" key or function to return the system to its point of interruption. The casual user may feel less intimidated in using the system if a key is provided which will "undo" any operation he or she has already started. Having a "modify" feature to correct any mistakes in building a picture might also be convenient for the user. In a system described by Teitelman at the Xerox Palo Alto Research Center, if the interactive input device button on the mouse is held down instead of lightly pressed, the system is instructed to tell the user what it "would" do if the chosen operation were actually performed [11]. Being able to see the result of an operation before it is actually performed would save the user time in correcting errors and in redoing the operation.

(U) The user should always be provided with the opportunity to exit the menu sequence at any point and return to previous menus. Being able to continue a computation following an error would be useful when the error occurs following a significant amount of computation. This facility would be essential for good interactive debugging, although not all graphics applications would require a tremendous amount of computation. In designing any features for the users' convenience, it is important for the designer to remember that there should be consistency of choices to minimize the users' difficulty in learning to operate the system. A "HELP" option, for example, should work at any level of the menu, and any operation should produce the same result whenever or in whatever context it is performed.

(U) In an interactive system using a menu generator developed by Logicon [12], the designers' rationale was that the users would not use the system if they did not like it, and one reason they would dislike a system would be because of the unfriendly environment it provides. To keep the novice user from becoming anxious and the experienced user from becoming bored at the terminal, their command menu interpreter writes a joke or witticism on the bottom of each menu or command page. They provided two different environments, a verbose and a terse mode, to provide more explanation for new users and to reduce this information after they have had a chance to become more experienced. Other researchers suggest tailoring the menu to the user, which might be helpful if there are different applications on a given system [13]. Lastly, a profile might be saved for each user so that when he or she logs into the system, he or she will be provided with the appropriate menu or can continue with a process. Use of these techniques should enable any designer to create a well-written menu utility for an application using interactive graphics. In the following section, some NSA graphics systems will be investigated to show the versatility of menu utilities as they are implemented in different applications.

EXISTING NSA SYSTEMS USING MENU UTILITIES

(U) In the following pages, several NSA graphics systems are described which have implemented menu selection in some form to improve their human/machine interface. Although the systems surveyed do not include all NSA graphics systems which have menu utilities, all three types of display technologies (raster, calligraphic, and storage tube) are represented. These systems are then compared, not by the type of graphics display, but on the basis of the characteristics of the menu utility implemented on each system.

CALMA GDS2

(U) The CALMA GDS2 of S27 is a medium-resolution color graphics system used for designing chips, pattern generation, design rule checks, and plotting. The cost of the system was about $500,000, with $100,000 of special software. It consists of an Eclipse computer with 256K of memory (i.e., 262,144 bytes), disks and tape drives, a color display controller, a Lexidata color monitor, and a black-and-white Hazeltine terminal. There are two workstations which consist of a graphics terminal and an alphanumeric terminal mounted in a movable hood with a keyboard and tablet on a desk below. As the user moves a pen across the tablet, a cursor is moved across the screen.

(U) A menu is displayed on this system as a series of small rectangular boxes, four rows across the top and four columns down the side of the screen in an "L" shape. Each box has a symbol or word which denotes the operation it performs. The user makes a selection by moving the pen on the tablet until the cursor is over the box he or she wants to select and then presses the pen down on the tablet to

OCID: 4011963

make the actual choice. The software allows for up to four different levels of menus with up to 300 different commands in ten categories, but only two levels of options are presently available. Selections made from the menu are reflected on the black-and-white monitor so the user can review previous selections he or she has made.

(U) This particular menu utility has many of the advantageous features mentioned in the previous section. For example, it has an option to highlight changes to be made before they become permanent and has a "wipe-out" key to undo the latest changes. The user can be working on ten different scratch areas of the screen at once and can get a summary of the characteristics of each area by typing a command. The menu has four different options for filling figures, along with a scale that pops up to measure distances. Although there are up to 64 layers on a chip that can be made selectable for viewing, there is never a delay of more than a few seconds before a chip is displayed or a command is given a response by the system.

(U) The users, who are engineers, can take a two-week training seminar to learn the different commands and how to run jobs and seem to be quite satisfied with the system. In general, the menu utility provides a very good user interface because it simplifies what could have been a complicated system to learn.

QUICKER

(U) The QUICKER system in R812 is a high-resolution graphics system used for designing circuit boards, floor plans, mechanical drawings, and software flowcharts. Each of the four workstations costs about $50,000 and consists of a Tektronix 4014 graphics device, driven by Computer Vision software, a separate alphanumeric terminal with a keyboard, and a tablet with a pen for selection. Special hardware and software purchased from Computer Vision makes this storage tube draw images more quickly than conventional storage tube technology.

(U) The menu utility on this system is implemented by overlaying on the tablet a sheet of paper containing several rows of rectangular boxes with symbols or words designating the operations to be performed. This menu is unusual in that it is not displayed on the graphics screen at all. The user can point to a box with the pen and to a part of the circuit board displayed to delete or insert portions of the drawing. Different sheets with different menu items can be overlayed for other applications. Since the menu software was not built into the system, R812 can change or add new functions to the 200 options already available.

(U) Although this system has the advantage that no space on the screen is used up by a menu, this can be a disadvantage since the user must constantly move his or her eyes from the screen to the tablet to make selections. With the CALMA system mentioned above, the user can focus his or her entire attention on the screen while making menu choices. Despite the fact that the QUICKER system is faster than most storage tubes, it might be uncomfortable for the user to have menu selection from the screen since the entire picture would have to be redrawn each time the menu level changed and a new one appeared. Some of the most useful features of a menu utility (highlighting, special keys, etc.) are impractical to implement on QUICKER because of the bright flash which occurs when the screen is cleared. Though the QUICKER system's users seem fairly satisfied with their system in general, a better technology to use for interactive user interfaces would be raster or calligraphic.

(U) R812 is now developing a new graphics system by Megatek which uses medium-resolution raster technology and costs $50,000 per device. This system receives input from a keyboard with twelve function buttons, a tablet with a pen, and a joystick with a button. A menu resembling the twelve function buttons is displayed on the screen and the user can use any of the named input devices to make a selection. The menu can be moved to different parts of the screen or made invisible, and the user can push one of the function buttons to move to different menu levels. Although only 512 by 512 pixels are displayed, this represents only one out of eight pixels which are stored so that as raster technology improves, a higher resolution may be obtained. In the meantime, added detail is gained by using a zooming feature. The Megatek contains fifteen microprocessors to do hardware fill and transformations and will eventually be connected to a mini-computer enabling parallel transmission.

[redacted] P.L. 86-36

[redacted]

P.L. 86-36
EO 1.4.(c)

CID: 4011963

[redacted]

[redacted]

(U) Since [redacted] is a fairly old system using electrostatic deflection, each display station is about the size of a 5 foot cube. Only 2,500 to 3,000 vectors and place-names can be displayed and images are blurred around the edges of the screen. [redacted] menu utility is very rudimentary because of its age and lacks most of the features implemented in the newer systems such as the CALMA. A2 will eventually change its display stations to [redacted] calligraphic devices to handle a mixture of signals at once with a 65K microprocessor, instead of the 4K of storage available from the current system. The menu utility could be updated to provide a better user interface with this newer, more powerful graphics system. P.L. 86-36

A21 REPORTING PROTOTYPE

~~(C-CCO)~~ A new high-resolution raster system with keyboard and an interactive device proposed by A21 will aid the analyst whose function is reporting. Instead of using wall-sized maps and slide presentations, the analyst will be able to view maps with special symbols and place-names, timelines, and business/management data on a graphics device. Hardcopies can be made of the display file for in-house presentations or the time-sensitive displayed data may be transmitted to other agencies. The user will interact with the system through displayed menus. There will be menus offering options of geometric shapes and military symbology to superimpose on maps created from World Data Bank II data, as well as menus for adding, deleting, editing, or moving text. A scroll feature will be provided for all those flags or designs which cannot fit into the menu area at once. In addition, a "modify" feature is proposed for the analyst to correct mistakes made in constructing his or her symbol. Planning the user interface in the design phases of the system, instead of adding features as an afterthought, should make the A21 prototype system a good model for those planning to develop interactive graphic systems in the future.

P.L. 86-36

[redacted]

[redacted]

P.L. 86-36
EO 1.4.(c)

DOCID: 4011963

COMPARISON

P.L. 86-36

(U) As new interactive graphic systems are being developed (like the CALMA GDS2 raster system for engineers and the A21 reporting prototype), more emphasis is being placed on developing a good user interface to make these systems better tools for the casual user. Both older systems surveyed, [redacted] have added menu software to improve the user interface. Yet the original design makes the system more complicated for the analyst to learn. Besides deciding on the appropriate choice from the older systems' menus, the user must learn numerous function buttons and other input devices like the trackball and light pen in order to effectively complete an operation.

P.L. 86-36

(U) [redacted] menu utility shows no indication of the particular level the user is at and he or she may become easily trapped in a mode or level. Although the [redacted] system's menu levels are not confusing, there is no legend to remind the user what the symbols or linestyles he or she has chosen represent, and no help in prompting the user for fill-in-the-blank responses. Neither system has a method for the user to wipe out previous choices and begin again, whereas the newer CALMA system has such an option to enable the user to make a mistake without the fear that the system may crash. In addition, the CALMA system highlights the user's creation or change of a design enabling the user to study the update before making it permanent.

(U) Although the QUICKER and CALMA systems physically implement menu selection differently, the former having a menu overlay sheet on a tablet and the latter with menus on the screen, both utilities are designed with the flexibility to add new menu items. Whereas the QUICKER system has a much higher resolution for electronic details than the CALMA, the CALMA system utilizes color to distinguish between layers of a design. Viewing the menu and drawings in color should not only be more pleasing to the user's eye, but also should keep the user interested longer than when watching a black-and-white display. Both the CALMA and [redacted] systems allow the user to point to an item on the screen and receive more detailed information about the item. Additionally, the CALMA system is sophisticated enough to allow the user to type a query on the monitor to show the status of the 10 different scratch areas of the screen he or she can be working on simultaneously.

P.L. 86-36

(U) As newer systems are being developed, like the CALMA GDS2, the user interface to the computer continues to improve over older models because human factors are being considered when designing a system, instead of being implemented as an afterthought.

MENU SELECTION TECHNIQUES
USED BY R53 IN THE IOMS SYSTEM

(U) In this section the IOMS interactive graphics system, developed by R53 in conjunction with T333 and A512, will be described. This system is concerned with the user interface from the design stages and, in addition, is using a graphics standard to develop device- and machine-independent menu software.

(U) An R53 technical report published by David Nation in April 1980 [14] found that there is an unexpectedly large requirement for geographical computer graphics across many DDO organizations. Based on Nation's survey and given that similar geographical display capabilities are required by many NSA organizations, it was evident that development costs of geographical display systems could be reduced by designs which take advantage of a set of reusable geographical display software. In order to write reusable geographical display software, a standard graphics software package was needed. R531 had been interested in using a commercial implementation of the ACM SIGGRAPH CORE System, which is a proposed standard developed by the ACM/SIGGRAPH Graphics Standards Planning Committee to promote application program portability and device-independence [15]. R531 has installed one such system, DI-3000, on the MYCROFT PDP 11/70.

~~(S-CCO)~~ In order to test the theory that graphics software developed on one system could be easily implemented on another by using a CORE graphics package, a prototype had to be chosen which would meet a real Agency requirement and at the same time illustrate the usefulness of the CORE System. R531 worked with the Graphics Investigation Group (GIG) in selecting a prototype application [16]. The Initial Operations Management System (IOMS) in A512 was chosen to be the prototype graphics application. [redacted]

EO 1.4.(c)
P.L. 86-36

OCID: 4011963

IOMS GS general screen format

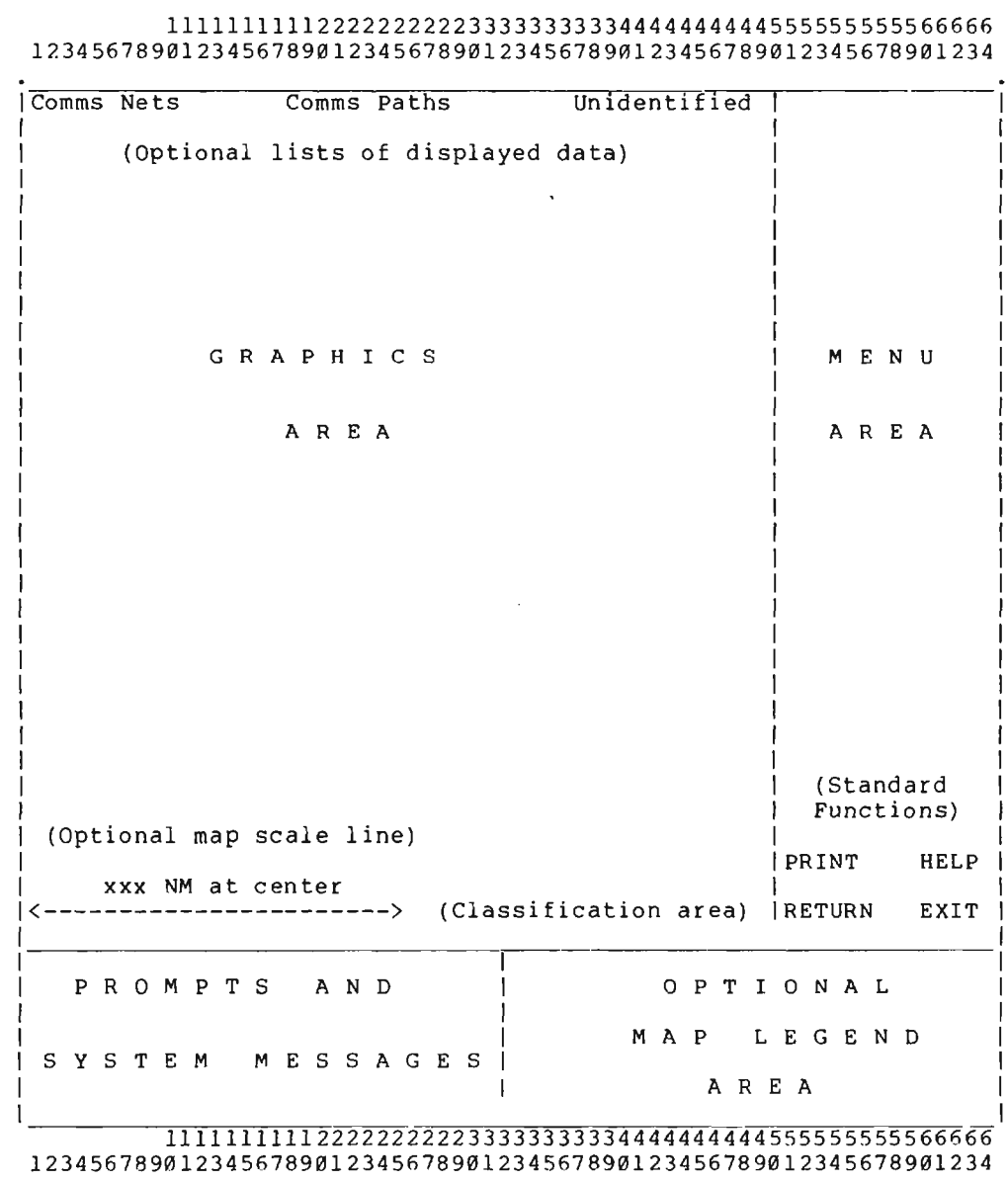


Figure 1: Mock-up of a Typical Display Screen

DOCID: 4011963

~~SECRET~~ EO 1.4.(c)
P.L. 86-36

(C) In order to design a system which would met the requirements of the A512 analysts and have a good interface for users in a non-computer-related profession, R531 had to learn A512's terminology and understand the types of data from which they derived information about collection targets. Mock-ups illustrating various scenarios, similar in format to the one shown in Figure 1, were used to aid the user in knowing what could be expected from the graphics software. A menu generator was designed to communicate with the user in the simplest manner with a limited amount of computer training required (see Figure 2). Figure 3 shows a hierarchical breakdown of the different menu levels.

(U) The graphics process is initiated at a Delta Data alphanumeric terminal. Thereafter, the user makes all responses to menu queries using the keyboard of the graphics display for input. The user is prompted in the message box of the display when it is time to make a selection from the menu and receives feedback in the form of a message indicating that his or her request is being processed. Figure 4 shows an example which begins with the highest menu level and continues to three lower levels as the user presses the number of the menu option on the keyboard.

(U) Each menu has been designed to indicate if submenus exist for a given choice by having a dash placed after the selection number (see Figure 4). The user may return to previous menus by typing an R for return or may exit the process at any level by typing an E. Other special features planned, but not yet implemented, include a "HELP" key to display documentation on the Delta Data and an "ESCAPE" key to take the user back more than one menu at a time. To further increase the flexibility of the utility, the user will have the option of picking a displayed data item with the joystick and receiving more detailed information about the item. Currently, the user has the option of replaying one or more sessions, redisplaying data already processed without requerying the data base. The user has a "CLEAR" option if he or she does not want to save the data displayed and a full screen feature to expand the map display and erase menu areas. The user may also type text onto the map to provide annotated hardcopy for analytic use or presentations.

~~(S-CCO)~~ The colors of the menu selections match the color of the item as it is drawn. If a river is shown in blue on the menu area, it is drawn in blue on the map. Likewise, when communications networks are displayed, the links between cities are shown in the same color as the signal types they represent in the legend area. As additional feedback to the user, menu items are brightened from gray to white to indicate that these features are "on." Eventually, a command mode feature will be added to allow the more experienced user to type in options like "projection = Mercator" without having to browse through several menu levels to the menu which sets projections. One of the most useful menu features is a file that is created at the end of each session which saves all the parameters the user has set, such as environment, map scale and coordinates, map details, type of projection, etc. Given this parameter file, the user does not have to reset these options anew each time a new session begins.

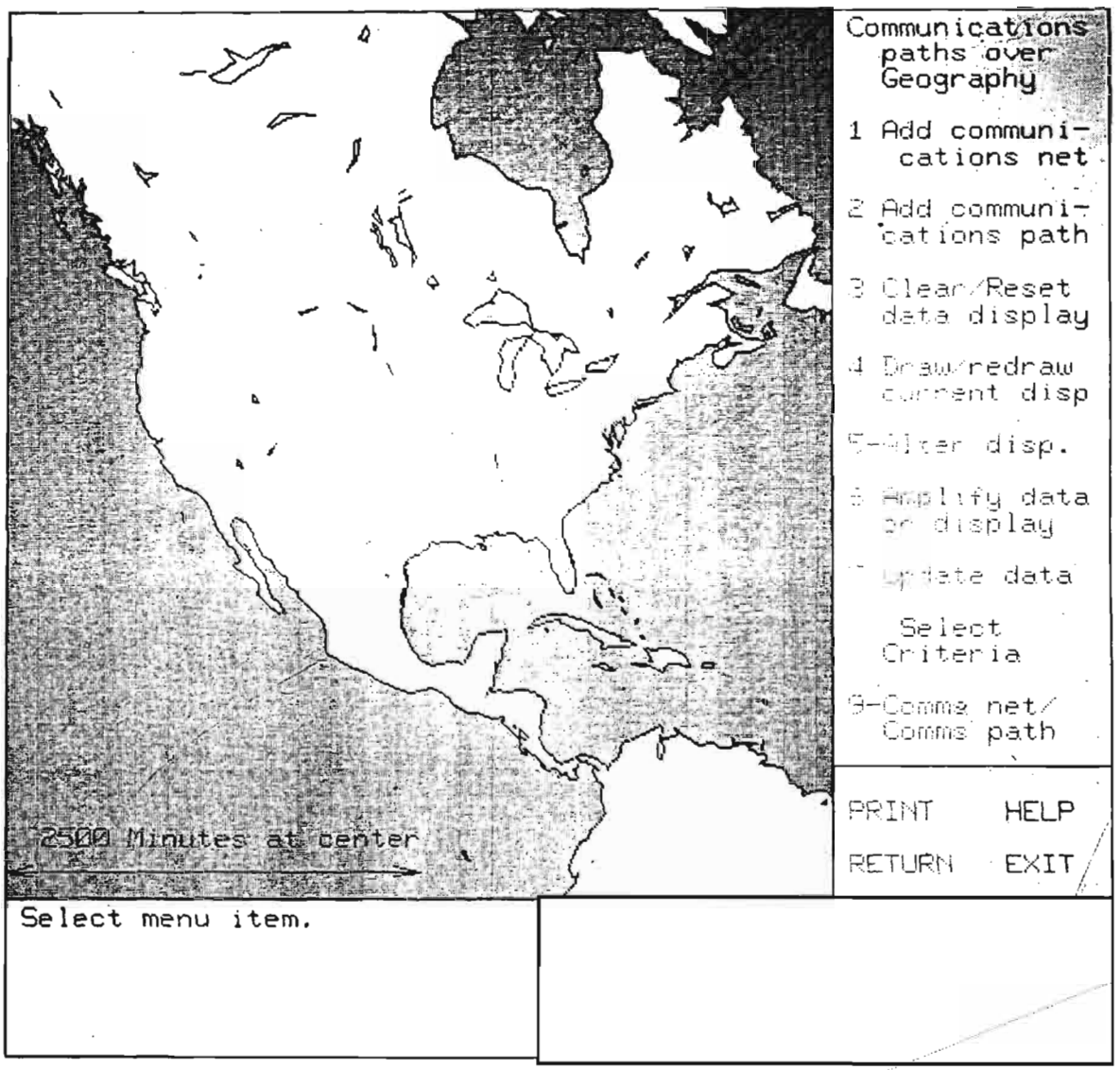
(U) The IOMS graphics subsystem was developed and tested on the R53 MYCROFT PDP 11/70. Delta Data 7000 alphanumeric terminals and AED 512 color raster displays are used for display and interaction. The software was written using the DI-3000 implementation of the CORE System (DI-3000 is a product of Precision Visuals, Inc.). R53 has transferred the IOMS graphics subsystem to A512's system with little difficulty, except in synchronizing operating systems. There are now plans to transfer the software from the PDP 11/70 to a VAX system to document the effort and the number of code changes needed for the software to run on a different host system. Since a different computer and different graphics devices will be used, this effort will be an even better test of the CORE System's transportability feature. Another future test being considered is to use the same basic menu generator, altered somewhat to meet a related but different application. This would be done on a third type of host system.

CONCLUSIONS

~~(S-CCO)~~ The purpose of this paper was to show that a well-written menu generator makes a good user interface for interactive graphic applications because of the many advantages it offers the casual user. The most important advantages are feedback, the need for little training, ease of use, choice of alternatives, and special help keys. After the features and advantages of menu selection were discussed, several case studies involving NSA graphics applications which utilized menu tools were presented to illustrate the various ways menu utilities have been implemented. Finally, R53's implementation of menu selection using

~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4011963



EO 1.4.(c)
P.L. 86-36

the CORE System [redacted] was presented, not only to show the use of a menu utility as a good user interface in a geographical application, but to illustrate the concept that properly designed software can be transportable to other future systems with related applications by using a graphics standard such as the CORE System.

(U) Although there are still a few refinements to be made to the IOMS graphics software, the reaction of A512 analysts using the graphics subsystem has been very favorable. R53 has been successful in developing menu software for an interactive graphics application that is both convenient and user-friendly. This is due in part to the large effort made by the design team to consider what the user wanted from the system and how he or she would interface with it before any coding ever began. Even after the first implementation of the graphics software, the R53 team continued working closely with the users to determine how the menu utility could be further upgraded or changed to aid the analysts. R53's success can also be credited to the fact that many of the features mentioned above as being desirable in a menu utility were implemented in the menu utility designed for IOMS. From the IOMS project, R53 has demonstrated that menu selection is an invaluable tool for creating a good user interface in an interactive graphics environment. Further research and future projects should show that by using a graphics standard such as the CORE, the success of R53 can be replicated in other applications without having to replicate the entire programming effort.

REFERENCES

[1] Bergerson, Bono, and Foley, "Graphics Programming Using the CORE System," ACM Computing Surveys, (10)4 Dec,1978 p.400-425.

[2] Lecture notes from Computer Graphics MP-413 class, Oct-Dec, 1981.

[3] Tesler, Larry, "The SMALLTALK Environment," BYTE Publications, Inc. August, 1981 pp.90-147.

[4] Tesler, Larry, "The SMALLTALK Environment," BYTE Publications, Inc. August, 1981 pp.90-147.

[5] Schneiderman, Ben, "Software Psychology,," Winthrop Publishing Company, Cambridge, Mass., (1980).

[6] Miller, Robert, "Response Time in Man-Computer Conversational Transactions," Fall Joint Computer Conferences 1968, p.267-277.

[7] Shneiderman, Ben, "Improving the Human Factors Aspect of Database Interactions," ACM Transactions on Database Systems, Vol.3,No.4, December 1978, p.417-439.

[8] Ellis, T., "Interactive Man-Machine Communications," The RAND Corporation, DAHC15-67-C-0141-Arpa, January,1971.

[9] Newman and Sproll, "Pinciples of Interactive Computer Graphics," McGraw-Hill,Inc., (1979).

[10] Martin, James, "Design of Man-Machine Dialogues," (1973).

[11] Teitelman, Warren, "A Display Oriented Programmer's Assistant," Int J. Man-Machine Studies (1979)11, p.157-187.

[12] Logicon Inc., "Design Considerations for the Man-Machine Relations User Interface," San Diego, Calif. July, 1979.

[13] Mehlman, Marilyn, "When People Use Computers," Prentice-Hall, Inc., Englewood Cliffs, New Jersey. (1981).

[14] Nation, David A., "Survey of NSA/CSS Computer Systems Using Graphics," TR-R53-02-81, August 15, 1981.

[15] Newman and Van Dam, "Recent Efforts Towards Graphics Standardization," Computing Surveys, (10)4, Dec 1978 p.365-379.

[16] Graphics Investigation Group, "Interim Report," September,1980.

DOCID: 4011963

IOMS Graphics System

Menu Hierarchy
State transition diagram

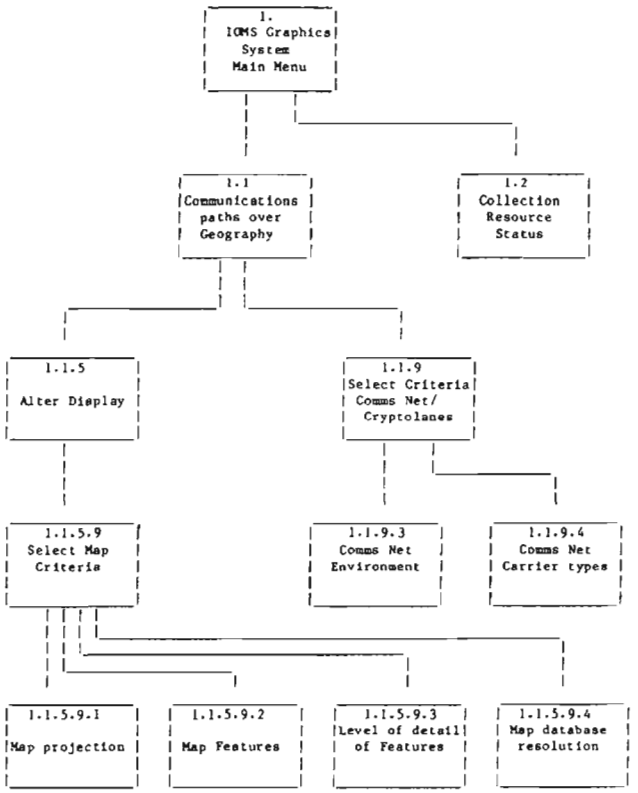


Figure 3: A hierarchical breakdown of the IOMS system

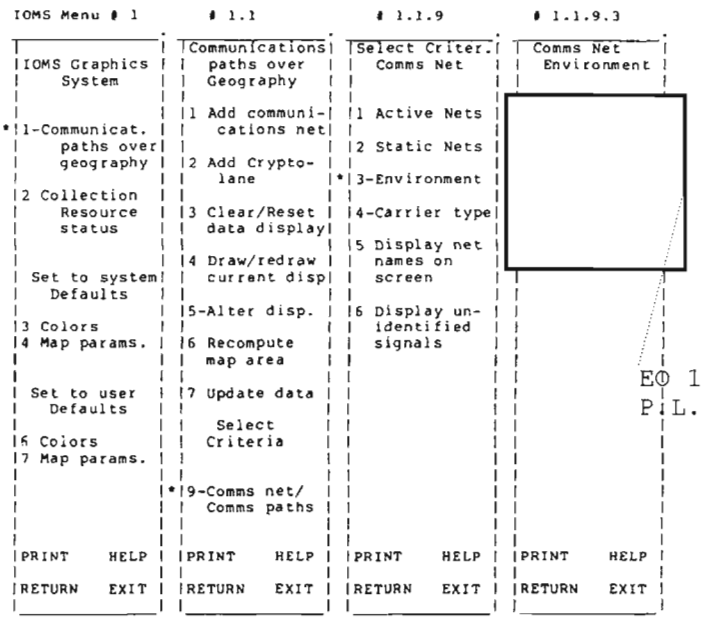
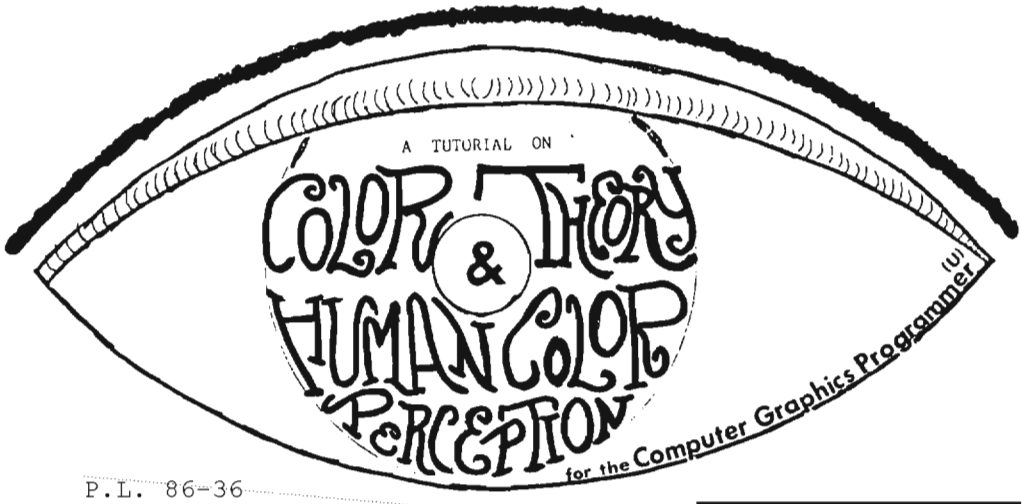


Figure 4: A logical menu sequence with selected options (*)

E0 1.4.(c)
P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011963



P.L. 86-36

by [redacted] B62

INTRODUCTION

Psychological studies have found that color graphic systems (compared to monochrome displays) significantly improve the presentation of complex data: data are easier to recognize, exceptions and errors are easier to detect, and user satisfaction is increased.* The purpose of this paper is neither to support nor to dispute these views. Color graphics does indeed represent the computer state of the art more than any other single machine discipline.

A user receives hundreds of times more information from his eyes than from all his other senses; moreover, a user thinks graphically. The user sees signs or pictures instead of spots of light; he reacts to patterns of stimuli, usually with little awareness of the parts composing the pattern. Given a black and white photograph, the human eye can only distinguish the difference between thirteen levels of gray from black to white. Under carefully controlled conditions, adults with normal color vision can discriminate from 120 to 150 color differences across the visible spectrum. If saturation and brightness are added, the number reaches into the millions[2]. Consequently, color extends the amount of perceptable information that can be injected into, or extracted from a visual image. The intrinsic nature of color adds a new dimension to computer graphics techniques. The varied character of color provides the potential for creating unlimited effects with color that can accurately delineate various aspects of a visual image.

The challenge, then, is to create displays which are not just aesthetically pleasing. The graphics programmer must start with what, when viewed closely, appears to be a meaningless collection of colored dots to create a total impression with predictable properties from organized stimuli. In order to effectively utilize color in the visualization of ideas, information, or concepts, the aspects of human color perception as well as basic color theory will be explored in detail. The conclusions presented following this discussion are intended to be used as a guideline

* In one such study[18], four different types of CRT display formats were evaluated in the context of a computer-based telephone line testing system (see figures 1[18] and 2[18]). The subjects, eight Bell System employees (ages 25-50, all high school graduates, one college graduate) had normal visual acuity and color vision. The formats considered were narrative, which used complete words and phrases; structured, which used a tabular format; black and white graphics, which used a schematic of the telephone line; and color graphics, which also used a schematic but added color coding. The evaluation measured speed and accuracy of the subjects' interpretation of the displays of the test results. Accuracy did not significantly vary with format, but speed did. Response times for both graphic formats were consistently shorter than those for the narrative format. With additional practice, however, response times for the structured format were just as short. These findings are in agreement with earlier studies by Richard Christ and his associates [18] who concluded that while color is often an effective code, it neither improves nor detracts from human performance when compared to achromatic schemes.

~~FOR OFFICIAL USE ONLY~~

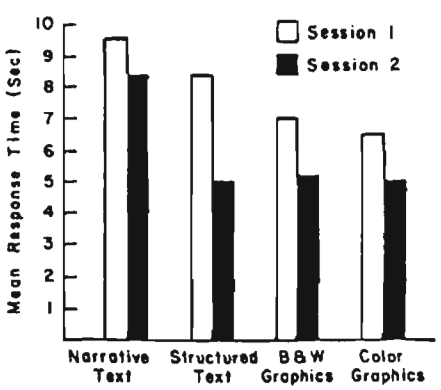
DOCID: 4011963

Figure 1

Advantages and Disadvantages of Test Results Formats as Stated on Questionnaire

Format	*Advantages*	*Disadvantages*
Narrative	"You get a lot of information on the screen."	"A bit difficult to read." "Not as clear for a person with (little) experience." "Too much initial concentration." "Not as easy to read—time consuming." "In a busy office . . . could become tedious." "Recognition factor slower than graphics." "Time needed to read the test results." "Difficult to read and use."
Structured	"Summary stands out." "Information is simpler to absorb initially, strictly from the way it is . . . segmented in contrast to the narrative system." "Very good—are familiar with all areas of failures." "A blend of the qualities needed."	". . . would rather have all categories of data in one row." "In a busy office . . . could become tedious."
Black-and-white graphics	"Easy to read. More accurate, less time consuming" "Time saver" "Summary stands out." "Quick recognition of trouble and location." "Fast to use during busy days." "Clear—easy to read."	"Could be hard on the eyes if used constantly—unless toned down." "Broken lines tend to confuse at times."
Color graphics	"Pleasant, accurate. Good color selection, faster trouble decision." "Summary stands out." "Color adds to what might otherwise be a boring task." "Quick recognition of trouble and location." "Clearest for person with no mechanical background." "Color highlights important parts. High speed and very clear."	"Color could be hard on the eyes."

Figure 2



Mean response times to test questions for the four formats, by session.

CID: 4011963

for the graphics programmer to enhance graphics displays (when it has been determined that color applications will accomplish a particular job more effectively) without overstimulating the viewer.

COLOR THEORY

The vast diversities found in color result from the fact that colors vary on three dimensions--hue, brightness, and saturation. No matter how an image is created, be it electronic, photographic, or otherwise, it is perceived by a human observer only according to these three visual perception parameters[3].

Hue, which is determined by the length of the light wave, is defined as the perceived "color". Hue refers to the specific color family such as red, blue, green, or yellow. Brightness (value) corresponds to the perceived intensity of the light and varies with the amount of energy in it. Saturation (chroma) refers to the amount of color and is dependent upon the degree to which the wavelength is diluted by white light.

Further discussion of hue, brightness, and saturation is dependent upon a basic understanding of the relationships among and between the colors found on the color wheel. Sir Isaac Newton discovered that the spectral colors can be wrapped around in their natural order about the circumference of a circle (see figure 3[7]), allowing room between the red and violet ends of the spectrum for the purples not found on the spectrum[5]. If properly spaced, colors opposite each other on the circle will be complementary; that is, if the lights of these colors are mixed in proper proportions, they disappear to a neutral gray (see figure 4[5]). Some colors appear to be more elementary than others; they appear to be composed of a single hue. These elementary colors are called psychological primaries--red, yellow, green, and blue. Between them are secondary colors in which the components are still identifiable--orange between red and yellow, the yellow-greens between yellow and green, the blue-greens between blue and green, and the purples and violets between blue and red.* Another set of primaries is called the color-mixture primaries. Any three widely spaced colors on the spectrum can be used to provide all the other colors by additive mixture (see figure 4[5]); the three usually chosen are red, green, and blue.

Using the color wheel as a reference, colors can be chosen for their varying degrees of similarities or differences to meet the needs of the image. Warm colors, reds and oranges, tend to advance in space and take a frontal position in a composition. On the other hand, cool colors, blues and greens, tend to recede in space and take a background position. Spatial effects can be created with warm/cool contrasts (forms may appear larger when they are colored red as opposed to green or blue). Bright reds and oranges seem to radiate warmth and light and are thus appropriate colors for depicting light, warm spaces or objects. Blues and greens project a sense of coolness or a cool temperature. These cool colors are passive and seem to imply a comfortable stability. Reds and oranges are very dynamic, active colors and seem to energize spaces and objects.

As one continues to explore the similarities and differences of chosen colors, it becomes increasingly apparent that hue, brightness, and saturation can be used to clarify elements in a composition as well as to provide more detailed information. Gradual changes in hue create a subtle blending in which boundaries are obscured; depending on the degree of similarity or difference between the hues, three-dimensional spatial effects can be created. Brightness, a matter of appearance (whatever the composition of the color may be), can be reduced by mixing gray with a hue or by increasing (or decreasing) the value of a pure color. Brightness contrasts can be used to create spatial effects (light areas in a composition imply a source of light or lightness while dark areas create a sense of depth or weight). Saturation can be reduced by adding a gray of the same

---

* This set of color categories is generally recognized by Western peoples. Other culture groups see colors in ways that seem curious to a Westerner. The Hanunoo, a Stone Age People, for example, describe four basic classes of colors: dark colors such as black; light colors such as white; "dry" colors including red, orange, and yellow; and "wet" colors including light green, green-yellow, and brown. To the Hanunoo, these categories make sense because they help to describe the vegetation that supplies their food.

Regardless of the terms used to describe colors, all people appear to perceive the divisions in the spectrum in about the same way. Despite differences in the words used by various languages to describe colors, people generally agree on what colors are the best examples of focal colors (what adults identify as the purest example of each color category, such as "blue" or "red"): black, white, red, yellow, green, blue, and so on. Similarly, people say nonfocal colors (for example, blue-green or red-orange) are like focal colors rather than focal colors are like nonfocal ones (i.e., pink is almost red, but not that red is almost pink)[2].

CID: 4011963

brightness creating a very drab color or by adding a complementary color of similar value. The latter method is preferred since a richer color is maintained as the saturation is reduced. Variations in saturation can be used to differentiate elements as well as to create three-dimensional figures in space.

Harmony is a sense of continuity that is created by establishing a relationship between the compositional elements. In choosing harmonious color sets, colors should relate to one another in a given manner. Two techniques for choosing harmonious color sets are:

1. the use of a series of adjacent colors on the color wheel, and

2. the use of a pair of opposite (complementary) colors.

Adjacent or neighboring colors, such as red and orange, have close similarities, while complementary colors, such as blue and orange, exhibit a high degree of contrast in hue. Another technique for choosing harmonious color sets is the selection of colors that are found at equal intervals on the color wheel. Harmony can also be achieved within a set of colors by maintaining equal brightness and/or saturation levels.

If a person stares at a red circle and then looks at a plain gray rectangle, he is likely to see a green circle on it. The viewer experiences a negative afterimage--negative because green is the complementary color of red (see figure 5[5]). Seeing the complementary color is common, but not always the case. After staring at a very bright light, one would probably see a whole succession of colors rather than the predicted complementary color. Still another exception is worth noting: usually, dark surroundings make a light area seem lighter, and light surroundings make the enclosed area seem darker. Under some conditions, there is what is called a spreading effect so that dark areas make neighboring portions appear darker, and light areas make neighboring portions appear lighter[5] (see figure 7[5]).

THE TRANSITION FROM COLOR THEORY TO HUMAN COLOR PERCEPTION

Light is a continuous mixture of all the wavelengths across part or all of the visible spectrum. The normal human visual system is sensitive to visible light from violet with a wavelength of 400 nanometers to deep red with a wavelength of 700 nanometers.* Two kinds of light-sensitive bodies in the retina, rods and cones, catch the photons of visible light and in effect count them, thereby triggering a complex series of chemical and neural events[10]. The rods function mostly in very dim light to which the cones are insensitive. At normal light levels, virtually all visual information is provided by the cones. (In reality, individual cone cells distinguish color no better than rod cells; additional neural "wiring" is required before discrimination can be made solely on the basis of color[10].) Three types of these receptors, each sensitive to different wavelengths, together are responsible for color discrimination. Although the sensitivities of the three receptors overlap, one is sensitive particularly in the blue area of the spectrum, one in the green, and one in the red.

Any three wavelengths of light can be mixed in varying proportions to create many different colors, but the particular characteristics of the three human receptor systems make it impossible to duplicate all colors. The three primaries which can be mixed to produce the greatest number of colors are particular wavelengths of red, green and blue. For this reason, most color display systems are based on three light sources which are as close to an rgb component system as possible[8].

---

* There are two curious aspects as to how the progression across the visible spectrum is perceived. First, there is a simple, continuous change in a single quantitative property of light--the length of the light wave. This change in a physical quantity leads to a changing perceptual quality, namely hue. Reds do not look longer than yellows, greens do not look longer than blues. Instead, they all look different.

Second, though one can change the physical wavelength of light in a continuous fashion, from short to long, the changes in color are themselves rather discontinuous, and the colors seem to group themselves into sets or categories. Blue, green, yellow, and red have for many people a unique appearance, and seem to characterize rather stable portions of the spectrum. A physical change in wavelength entirely within the blue or green region may be hardly noticeable, or may seem to be a change from one kind of blue or green to another. The same physical change in wavelength between categories (a change across the blue-green boundary, for example) can be striking, appearing to be a change from mostly blue to mostly green. It may be that humans have a built-in mechanism that partitions the continuous physical spectrum into a small set of color categories[2].

DOCID: 4011963

HUMAN COLOR PERCEPTION

All experiences of objects and events take place within a framework of space and time. Vision, being the user's preferred spatial sense, provides some of the most complex patterns of these perceptual experiences.

During the last century, two major theories of color vision vied for supremacy. The physicist Herman von Helmholtz proposed that there were three color receptors in the eye, each giving its own color sensation--violet, green, and red. According to von Helmholtz, these primitive sensations combine to form the entire gambit of color experiences--for instance, sensations of red and green together produce the color yellow.

The other theory was that of the physiologist Ewald Hering, who argued that there were three pairs of colored processes--a black-white process, a red-green process, and a yellow-blue process. Hering's view was an "opponent-process" theory, in that the two elements in each pair are antagonistic to each other--a color can have some yellow or some blue, for example, but cannot be both yellow and blue in the same place at the same time.

Recent studies strongly support Hering's view. Work by Dorothea Jameson and Leo Hurvich of the University of Pennsylvania [2] have extablished that although it is true that the eye contains three color receptors, these receptors do not give sensations directly. Instead, in a complex fashion, the three receptors feed into a set of nerve cells that work by opponent processes. It is the pattern of activity of these opponent cells that appear to underlie the experiences of color.

Russel DeValois and his associates at Berkeley have identified three main classes of nerve cells that are specifically sensitive to variations in light wavelengths[2]. Generally, it is possible to identify these three kinds of cells as the embodiments of white-black, red-green, and yellow-blue opponent processes.

The above mentioned color categories match up quite well with the action of these three main classes of color-sensitive cells in the brain. For example, when a person sees yellow, opponent cells that become more active in response to yellow, and less active in response to blue, are excited. When one sees green-yellow, both green (in a green-red cell) and yellow (in a yellow-blue cell) are excited simultaneously. The existence of color cells that can give sensations of black (versus white) presumably makes it possible for a person to see surfaces with dark colors, such as navy (black plus blue), maroon (black plus red), and brown (black plus orange).

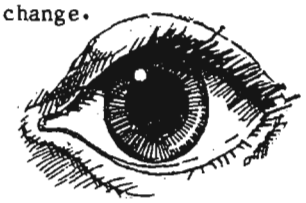
INTEGRATING COLOR INTO THE VISUAL IMAGING PROCESS

In the natural world, color comes free; in the graphics world, the advantages of color must be great enough to offset the greater cost, lesser resolution, or other disadvantages[15].* Use of color, therefore, is recommended as a coding agent (to indicate to a user the category into which data being displayed falls) and as a formatting aid (whereby color helps the user in understanding the logical structure of the data on the screen). Unfortunately, computer programmers often have a low A.Q. The conclusions which follow should be useful to computer graphics programmers who are now designing screen displays for the application of color graphics in today's world.

CONCLUSIONS

The appearance of color is relative and is dependent upon the background color which can influence the appearance of foreground color(s) in various ways (see figure 6[5]). The most obvious change in the character of a color occurs with the hue. If the foreground colors are opposite one another on the color wheel, they take on characteristics of the complement of the background. The brightness of the background color can also have an effect on the appearance of foreground color. Blue lines on a black background are hard to distinguish and will tend to deemphasize data fields whereas white, with the opposite effect against the dullness of the screen, can be used for emphasis. Yellow lines are hard to distinguish on a white background. Neutral backgrounds help set off full color. A dark background makes a color tend to appear lighter than it really is and a light background makes a color appear darker. In order

* Much has been written or said about the number of "colors" a system is capable of displaying[3]. Some manufacturers claim the ability to create and display several million color combinations. In an additive color system with three 8-bit digital to analog converters, the number of possible combinations is 16,777,216. The vast majority of the combinations are redundant and cannot be perceived. It is of no use for the range of values displayed to exceed the limits of visual perception; the observer wants only to be able to discern each independent gradation of intensity, hue, or saturation as a minimally detectable change.



CID: 4011963

for these color changes to occur, the background area must be considerably larger than the foreground figure. Generally, a small area of intense color is balanced by a larger area of less intense color. Also, a smaller proportion of a light color, such as yellow, is balanced by a larger area of dark color, such as purple.

Patches of light colors will seem to be larger than those of dark colors. This is because brightness is more stimulating than darkness. Bright colors appear brighter on a dark background, and dark colors appear still darker on a bright background. In other words, predominant components of an image can be given visual dominance by displaying them in a bright intense color on a duller, less bright background. For example, a gray arrow shown on a white background looks darker than a gray arrow exactly like it shown on a black background (see figure 8[7]).

When blue rays of light enter the user's eye, they bend sharply and are focused at a point in front of the retina. Red colors are bent less, and focus at a point behind the blue rays. Therefore, the human eye cannot focus red and blue at the same time to form one image. Looking at alternate red and blue bands, or lines, will tend to "hurt" the user's eyes and make the colors glisten and vibrate (see figure 9[7]).

Color harmony is created with opposite colors since the mixing of complementary colors intensifies each other (blue or violet flowers often have orange or yellow centers). Each pure color physiologically demands its complement. If the opposite color is not present, the eye simultaneously produces the complementary color.

The colors on the right side of the color wheel, from yellow to red-violet are generally called warm colors. They suggest sunlight and the flames of fire. The colors on the left side of the wheel, from yellow-green to violet, are cool colors as seen in nature, the sky, and water. Greatest cool/warm contrasts are achieved using orange-red and blue-green. All other colors appear cool or warm depending upon their placement with warmer or cooler values. Red and red-orange are seen by most persons as the colors of greatest excitement. Blue and blue-violet are colors that seem peaceful and subdued. Green and yellow-green are the most neutral and tranquil. Yellow is the most cheerful.

High contrasts clearly delineate shapes by creating sharp, clearly discernable boundaries (see figure 10[7]). High contrasts imply a difference between elements. In situations where false coloring is used to differentiate previously unclear gradation, the technique of using high contrast is successful. Low contrast in colors is used in continuity. Spatial effects can be created by employing different levels of contrast.

With similar objects of unknown but equal size, the brighter appears to be closer. If two objects at indeterminate distance are changed in both size and brightness, apparent motion toward or away from the subject will be enhanced if the cues cooperate.

Color edging enhances polygons (in general, any border pulls a graphics display together).

Other general rules will be found by studying the Birren color triangle (see figure 11[7]). Colors naturally fall into tints, shades, and tones. Tinted colors look well together and are the chief colors of spring. When colors are viewed under tinted light, the dominant tint tends to draw a group of colors together by introducing a mellow tone. Pure hues are the colors of midsummer. Shades are the colors of fall. Grayed tones are the colors of winter. On the triangle, any colors connected by a straight line also go well together. A hue may be safely harmonized with various values and chromas of itself; pure hues harmonize with tints and white; pure hues also are pleasing with shades and black, or with tones and gray. Other harmonies are found with combinations of tint, tone, and black, as well as of shade, tone, and white.

The above list is neither exhaustive nor applicable to every situation. The graphics display programmer is faced with the choice of:

1. using only colors and techniques that he knows are pleasing as well as effective,

2. using only the colors and design specifications indicated by the user, or

3. creating a subtle and harmonious blending of the first two options.

The last alternative is probably the most successful and certainly the most difficult solution. Therefore, when any doubt remains, the programmer should keep in mind the following two considerations:

> Most people like blue best, then other colors in the following order: red, green, violet, orange, and yellow[2]. Appreciation, by the user, of nonfocal colors such as turquoise, rose, chartreuse, beige, and tan, requires many years of familiarity with color[7].
>
> Above all, one should avoid using too

DOCID: 4011963

much color; overstatement or "business" will only confuse the user.

SUMMARY

Because of the benefits offered by the visual image, the projection by experts in the computer industry that computer technology in the '80's will emphasize graphics in addition to alphanumeric displays is already being realized. Computer graphics is fast becoming the medium of visual communication between man and machine, allowing improved data interpretation, higher productivity, and complex problem solution. A properly designed and used graphics display can transfer many types of information from machine to user much more rapidly and efficiently than can a verbal or numerical description. In a black and white picture, distinctions are made between elements according to the visual cues of size, shape, position, orientation and gray value. These visual cues allow the viewer to organize and comprehend the image. Carefully used, the addition of color adds an entirely new dimension to a composition and provides information beyond that encoded in the normal visual cues. Color expands the capability of the visual composition in communicating ideas by providing more detailed information.

It is essential that the choice of color and its application to various areas be used effectively in order to present clear, accurate and well organized information in a visually pleasing manner. An awareness of the behavior of color in composition and the impact it has on the aesthetics of an image combined with a firm understanding of how humans perceive and interact with color (in other words, a high A.Q.) will clearly benefit the programmer to effectively and sensitively develop and enhance color graphics displays.

BIBLIOGRAPHY

[1] Baeverstad, Jr., Harold and Bruderer, Clark C. "Display System Designed for Color Graphics." HEWLETT PACKARD JOURNAL, Vol. 31, No. 12, December 1980, pp. 25 - 31.

[2] Bornstein, Marc H. and Marks, Lawrence E. "Color Revisionism." PSYCHOLOGY TODAY, Vol. 16, No. 1, January 1982, pp. 64 - 73.

[3] Buchanan, Michael D. and Pendergrass, Richard. "Digital Image Processing." EOSD ELECTRO-OPTICAL SYSTEMS DESIGN, March 1980.

[4] Calew, Fred. "Enhancing Comprehension with Color." MINI-MICRO SYSTEMS, Vol. XIV, No. 8, August 1981, p. 139.

[5] Hilgard, Ernest R. INTRODUCTION TO PSYCHOLOGY. New York, New York: Harcourt, Brace, and World, Inc., 1962, pp. 186 - 193, 207 - 208, 228 - 232.

[6] Itten, Johannes. DESIGN AND FORM THE BASIC COURSE AT THE BAUHAUS. New York, New York: Reingold Publishing Company, 1963, pp. 42 - 43.

[7] Itten, Johannes. WORLD BOOK ENCYCLOPEDIA. Chicago, Illinois: Field Enterprises Educational Corporation, 1960, pp. 658 - 667.

[8] Joblove, George H. and Greenburg, Donald. "Color Spaces for Computer Graphics." COMPUTER GRAPHICS, Vol. 12, No. 3, August 1978, pp. 20 - 25.

[9] Kaplan, Alan R. "Special Report." MINI-MICRO SYSTEMS, Vol. XIII, No. 12, December 1980, pp. 68 - 69.

[10] Levine, Joseph S. and MacNichol, Edward F. "Color Vision in Fishes." SCIENTIFIC AMERICAN, Vol. 246, No. 3, February 1982, pp. 140 - 149.

[11] Meyers, Ware. "Computer Graphics: The Need for Graphics Design--Part One." COMPUTER, Vol. 14, No. 6, June 1981, pp. 82 - 92.

[12] Meyers, Ware. "The Need for Computer Design - Part Two." COMPUTER, Vol. 14, No. 7, July 1981, pp. 82 - 88.

[13] Pratt, Warren C. "A Precision Color Raster-Scan Display for Graphics Application." HEWLETT PACKARD JOURNAL, Vol. 31, No. 12, December 1980, pp. 19 - 24.

[14] Rossiter, Frank. "A Close Look at IBM's Color Graphic Offerings." MINI-MICRO SYSTEMS, Vol. XIII, No. 12, December 1980, pp. 116 - 128.

[15] Sorenson, Keith. "Making Color Affordable." HEWLETT PACKARD JOURNAL, Vol. 31, No. 12, December 1980, p. 152.

[16] Tektronix, Inc. TEKTRONIX 4027 OPERATORS MANUAL, pp A-1 - A-3.

[17] Truckenbrod, Joan. "Effective Use of Color in Computer Graphics." COMPUTER GRAPHICS, Vol. 15, No. 3. Siggraph 1981 Conference Proceedings, August 1981, pp. 83 - 90.

[18] Tullis, Thomas. "An Evaluation of Alphanumeric, Graphic, and Color Information Displays." HUMAN FACTORS, Vol. 23, No. 5, October 1981, pp. 541 - 550.

[19] _____. "User's Report: Terminal Turns Executive into Color." INFO SYSTEMS, Vol. 27, No. 11, November 1980, p. 93.

FOR OFFICIAL USE ONLY

DOCID: 4011963

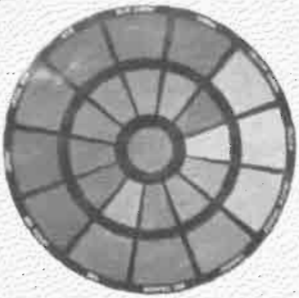


Figure 3

The Color Wheel

All major colors are shown in the outer circle. The grayed colors in the inner circle are made by mixing colors that are directly opposite each other in the outer circle.

Figure 4

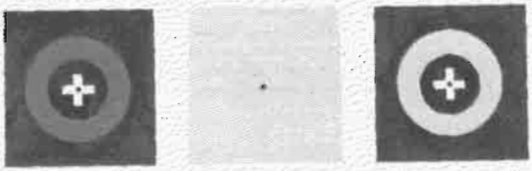


Figure 5

Negative afterimages

Look steadily for about 20 seconds at the dot inside the blue circle; then transfer your gaze to the dot inside the gray rectangle. Now do the same with the dot inside the yellow circle. What do you see?

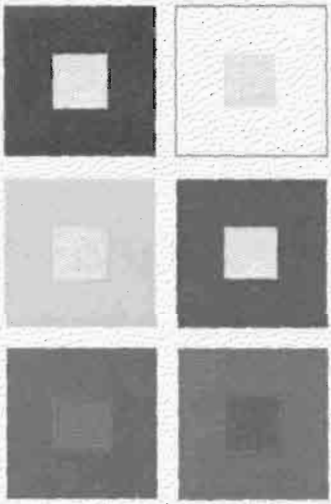


Figure 6

Simultaneous contrast

Note the darkening effect on the gray patch when it is against white; the same patch of gray against black looks much lighter. A gray patch against a colored background tends to take on the complementary hue. With colors that are approximately complementary (as in the red and green patches), there is an enhancement through contrast.

FOR OFFICIAL USE ONLY

DOCID: 4011963

Figure 7

The spreading effect
The same red is used throughout the strip, but the red with black looks darker than the red with white.

Figure 8

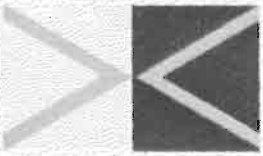


Figure 9

Background Makes a Difference
in the appearance of color. The two arrows shown below are the same tone of gray, but the one on black seems to be lighter than the one on white.

Figure 10

Legibility of Color
The letters on the left are easy to read, because of the color contrast. The letters in the center panel are not so easy to read because the colors clash. The edges of the letters seem to vibrate when we look at them closely. The panel on the right is not as legible as the one on the left because there is not enough color contrast.

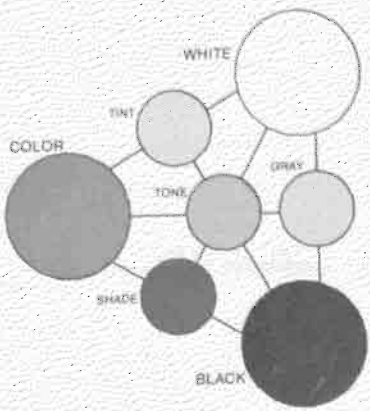
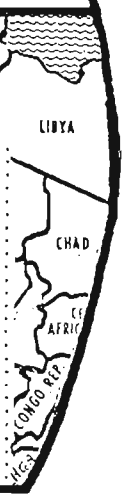


Figure 11

Color Triangle
designed by Faber Birren classifies all color sensations in seven forms. Mix pure color with white to get a tint; mix it with black and get a shade. Black and white make gray; black, white, and color produce a tone.

DOCID: 4011963
E.O. 1.4.(c)
P.L. 86-36

Computer Graphics to Enhance Collection Management (U)



by [redacted] R53
and [redacted] R53

P.L. 86-36

INTRODUCTION

(U) The declining cost of hardware is making small interactive computer systems with graphic capabilities practical for small groups and individuals. Although "turn-key" systems are available in areas such as CAD/CAM and management graphics, many applications do not lend themselves to a standard solution. Individually tailored software to drive these systems is not generally obtainable without considerable investment in software development.

(U) There can be much similarity between systems having related applications. What often happens during normal system development is the "reinvention" of basic functions for each one. Software and data exchange are often difficult because of differences in hardware or software implementation.

(U) This paper will show that software designed using a standard set of graphics functions can be moved between mainframe systems or graphics devices and applied to similar applications.

(U) It was demonstrated that a working version of an interactive system could be developed in a short period of time. The first version was running on the target system three months after software design began. An additional three months was spent working closely with the users in the refinement of the interactive approach and in the incremental addition of functions.

~~(C)~~ A recent survey of computer systems using graphics at NSA revealed numerous different computer and graphics device technologies. On closer examination of the graphics applications, many similarities were discovered. Most systems had charting and graphing applications, many had applications involving the creation of graphic pictures by the operator, and a significant number involved the display of geography and the overlay of various kinds of data on geography.

(U) A subsequent study was made of requirements for applications involving geographics and management graphics. Many of the geographically related requirements were the same. Typically a map was needed with geographic features (e.g. coastlines, political boundaries) shown as line segments. Various scales and projections were appropriate for each application. The primary differences between the requirements were the types of overlay data and the method of storing or creating these data.

OVERALL OBJECTIVES

(U) A new approach was needed in the development of interactive graphics software. It was apparent from the survey that most systems were developed "from scratch" even though existing systems had similar requirements. This happened for a variety of reasons. Early systems were written in assembly language and were not portable. Other systems were based on software packages that support a specific

DOCID: 4011963

graphics device. Changes in the graphics device or other hardware required software modifications to maintain equivalent functionality.

(U) The overall objectives in the development of software to improve this situation were:

1. Portability,

2. Rapid prototyping,

3. User friendly systems, and

4. Reusable software.

(U) Portability is concerned with the transfer of items between two or more environments. In this context, portability was applicable in three areas. First was the transfer of software between environments without extensive modifications and without compromising functionality. Currently it is difficult to use improvements in hardware technology, such as new host computers or graphics equipment, because of the software conversion expense.

(U) Secondly, the geographic reference data needed to be flexible to conform to specific application requirements and environmental constraints. Different systems had similar geographic data requirements with emphasis on specific areas of the world, and different environments would not accommodate the same size data sets. There was a need to dynamically "customize" data for each new system, based on the requirements and system configuration, from a centralized source.

(U) Finally, the finished graphic picture needed to be portable to permit recreation in another environment. Because of differences in system configurations, the method to accomplish picture portability required efficient storage utilization. It was impractical to retain every vector to draw a map with data overlays. It was feasible to retain the logical map specification and overlay data coordinates that were necessary to recreate the picture.

(U) A problem existed in the specification of requirements for new systems. It was often difficult for potential graphics users to adequately communicate their requirements for an interactive system. Problems in specification were encountered when some of the capabilities offered by the new system did not exist in the non-automated system. A need was recognized for the capability to quickly demonstrate the behavior of a proposed system during requirement definition, or "rapid prototyping." The appearance of the graphics produced and the means of interaction would be clear to the end user and to the designer before implementation. This method reduced risk of major revisions late in development when the cost of such changes is much higher.

(U) A primary objective of the prototype development was to make the system appear friendly to the new user. It was considered essential for the success of this effort to provide for a user totally inexperienced in programming or the operation of interactive systems. Features oriented to experienced users will be included later in the development process.

(U) The concept of reusable software was important for subsequent system developments. Reusable functions were specified as autonomous subroutines that could be called with a minimum number of parameters. Hidden values, such as those sometimes found in FORTRAN common blocks, were avoided in the specification of parameters. The product was a subroutine or set of subroutines that could be used without alteration for similar applications with minimal knowledge of the software environment.

APPROACH

(U) The following approach was taken to satisfy these objectives:

1. Use a graphics lab with a variety of computer systems and graphics equipment,

2. Use a detailed worldwide geographic database,

3. Use a standard graphics interface,

4. Build additional layers of software to implement common functions,

5. Develop a High Level Display File format for exchange of pictures,

6. Develop one or more prototypes for real applications,

7. Develop a quick look capability to experiment with new applications, and

8. Build future interactive graphics systems using software components from prototypes.

(U) It was essential to have several different computer systems with varying capabilities to demonstrate the portability of the software and data. Graphic output devices representing various technologies made it possible to compare the appearance of the same picture.

DOCID: 4011963

(U) The primary geographic database chosen was the World Data Bank II (WDBII) [1] because of its high level of detail on a worldwide basis. It represents geographic features such as coastlines or railroads as line segments. Each line segment is composed of a set of geographic locations defined in terms of latitude and longitude. The WDBII consists of approximately 47,000 line segments with over eight million of these latitude/longitude pairs. The capability exists to extract data from the WDBII with specified characteristics for individual user's needs.

(U) The CORE system [2] was the primary basis for portability and reusability of the basic graphics software. It consists of a set of subroutines the functionality of which was defined by a committee of the Special Interest Group on Graphics of the Association for Computing Machinery (SIGGRAPH-ACM). The CORE system has been proposed as the basis for a national standard for graphics programming. The functions defined are independent of the particular graphics device being used, the host computer or the language used to implement the software. Software developed on this basis may be used with little or no modification on a variety of graphics devices and computer systems. Additional functions were added using CORE primitives that would expand the utility of the CORE software for common graphics requirements.

P.L. 86-36

(U) The development of the prototype is detailed below. We considered the implementation of a set of requirements as an appropriate approach to the demonstration of these techniques. Another prototype is currently being designed. It will utilize software implemented for the first one, and add new functional capabilities for future software developments.

(U) A High Level Display File (HLDF) format is being developed to facilitate the exchange of pictures. Typical functions to be performed include drawing a map with certain characteristics, drawing a bar graph or using one of a standard set of graphic markers or "icons" to indicate the location of data.

(U) Software components developed for the prototype are intended to be used for experimentation in interactive techniques and to aid in the specification of requirements for proposed systems. The software itself is intended to be used as the foundation for new systems.

P.L. 86-36
EO 1.4.(c)

THE PROTOTYPE SYSTEM

Application

~~(C-CCO)~~ [redacted] is designed to convert [redacted] records, received from [redacted] over the PLATFORM network, into significant information for the System Operations Manager (SOM). The SOM has interactive tools that provide access to several online databases (kept current by background processing of the [redacted] records), automatic notification of special conditions as they occur and interactive color graphics to enhance the analysis of collection activities.

Environment

(U) The prototype was developed using a PDP 11/70 running the UNIX\PWB operating system (version 6). The display device was the AED512 raster color terminal with 8 memory planes and joystick. The target system was not available for the initial prototype development; consequently all software was completed on a second homogeneous (same architecture and configuration) system. This second system had been used for previous graphics research and was able to support the significant development effort required. When the initial system was completed it was transferred to the target system and installed with minimal effort. Enhancements were installed on the development system and periodically moved to the operational system reducing the impact on the operational system.

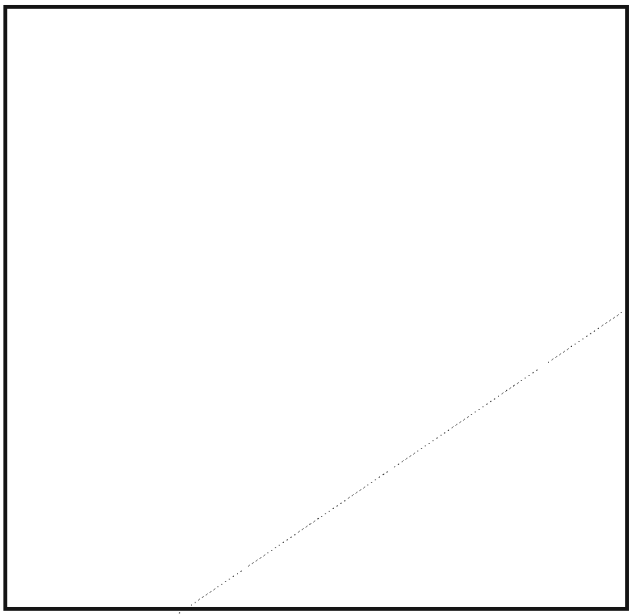
DOCID: 4011963

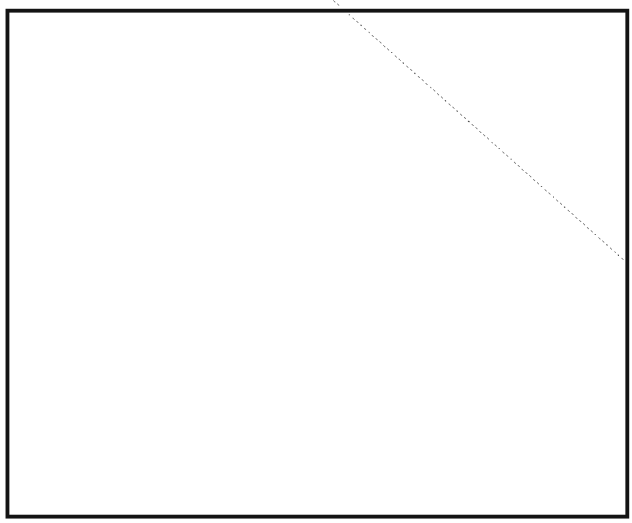
EO 1.4.(c)
P.L. 86-36

(U) A third heterogeneous system was available to enable the testing of software portability and device independence. This system was a VAX-11/780 with the VMS operating system. In addition to the AED512 graphics terminal, the VAX had a RAMTEK 9400 color raster system with 9 memory planes and a MEGATEK vector system.

(U) The graphics applications software was written using a FORTRAN 77 compiler developed and implemented under UNIX at Bell Labs. The Precision Visuals Inc. DI-3000 CORE graphics software package was used to generate all graphics displays. The installation of DI-3000 on the UNIX operating system and the PDP 11/70 was performed in-house and is not directly supported by Precision Visuals Inc. However, this installation does not affect the graphics software and therefore did not affect software portability. Certain application dependent and environmental constraints required the implementation of functions in the C programming language. These segments did not affect the portability of the major graphics components to a heterogeneous environment.

(U) Several databases were developed to support the dynamic map generation features and the application requirements. The map data was obtained from WDBII. Two additional map related files were also used. The first permits map selection by area name (e.g., country names) and the second allows the water areas of a map, such as oceans, to be differentiated from land areas and consequently permits "filling in" these areas on the display. The ocean fill data were created interactively using a modified version of the software described.





Software structure

(U) The extent of the prototype and the size of the commercial graphics software package exceeded the available program space on the 16-bit PDP 11/70. A multiprocess environment was established with UNIX "pipes" invoked to enable interprocess communication. The "pipes" were were used to pass data between processes and to synchronize the sequencing of operations.

(U) There are eight processes which comprise the current software structure: three to support DI-3000 and five to support the application (see figure 1). The The processes are organized by function with the interprocess communication kept to a minimum for performance reasons. The main process (main FORTRAN program) is responsible for initiating the other non-DI-3000 processes, and for controlling the interaction between the software and end-user. All menu generation and processing, all data input and database query generation and all parameter file input and output is coordinated by the main process. The main process "spawns" several other processes: the Database Query Process(DQP), the High Level graphics Display Process (HLDP) and the FFIX process. The DQP generates query strings based on the SOM input values, performs the database query and interprets the results. Successful queries require interpretation and secondary queries to obtain all data required to display the network(s) or paths. It also starts the Database Display Process (DDP). The DDP is notified of the query results and displays the application dependent graphics overlays. It does this by sending graphics commands to the HLDP. Query statistics and overlay display data are returned to the main program from the DDP.

EO 1.4.(c)
P.L. 86-36

DOCID: 4011963

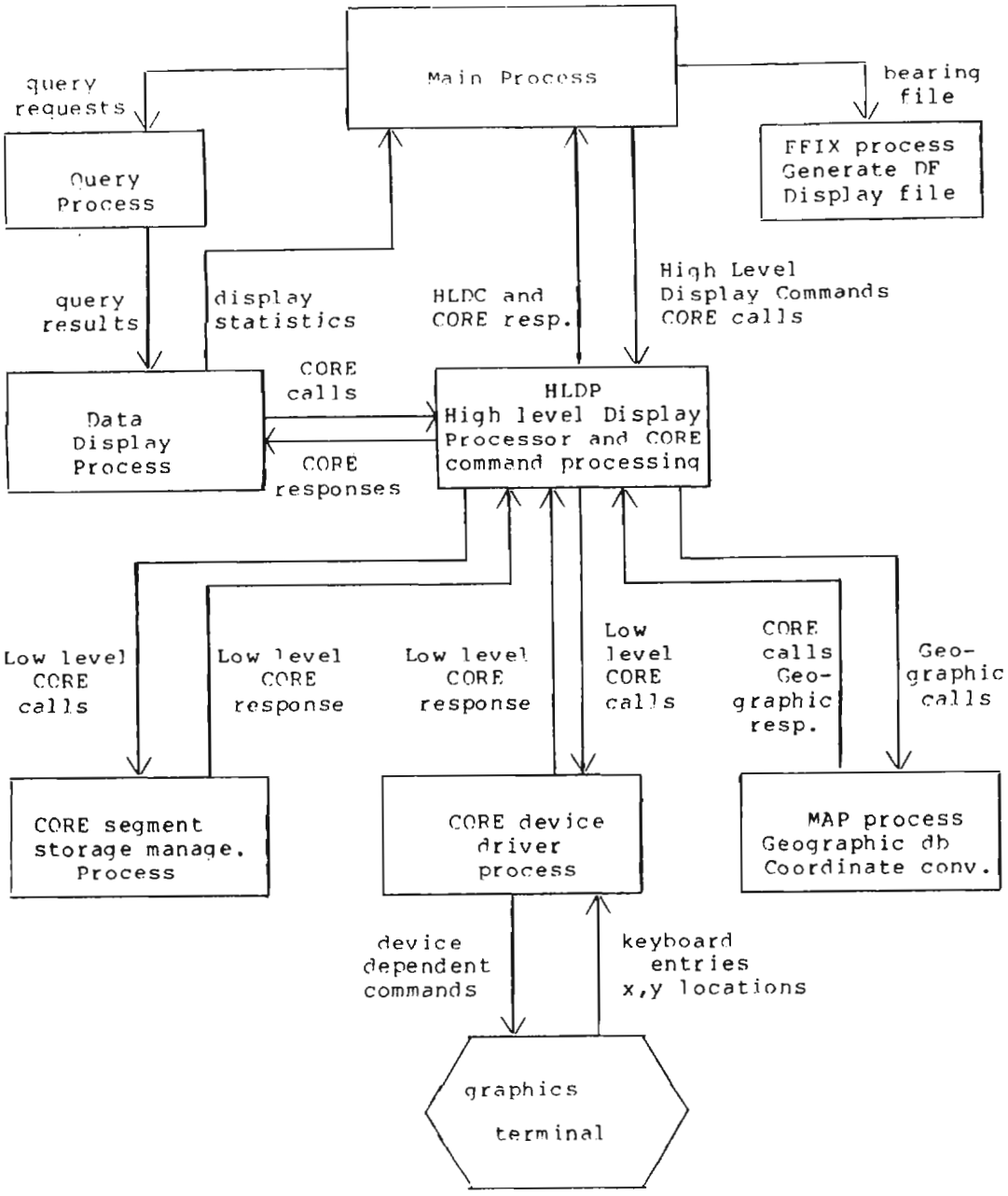


Figure 1.

~~(C CCO)~~ Geographic Process Interaction Diagram

OCID: 4011963

(U) The HLDP is the focal point for all graphics operations. It provides the interface between the application program and the graphics software. This process receives commands from the pipe which it translates to specific DI-3000 subroutine calls or to other high level graphics commands, such as the map generation command. When necessary it will initiate additional processes to do certain functions.

(U) The map generation process is initiated by the HLDP whenever geography based displays are requested. This process performs all access to the geographic data files, converts data to graphics oriented coordinates, and generates commands to the HLDP to invoke the necessary DI-3000 graphics subroutines. It receives parameters which determine what features are to be displayed, the geographic extent of the display and the projection to be used in the conversion process.

(U) The FFIX process [3] is initiated only when needed to generate a Best Point Estimate (BPE) and 95% confidence ellipse from a set of bearings or "flash." This process reads a file containing a set of digraphs and angles. The digraphs represent Direction Finding (DF) sites whose locations are stored in a separate file. The FFIX process creates an intermediate file containing information necessary to display the BPE, ellipse, and lines of bearing on a map. This file is used by the Map process to display the current DF data if that option is active on any map that is drawn.

(U) The remaining two processes, the CORE device driver and segment storage process, are part of the DI-3000 installation on the PDP 11/70. Each is initiated by the DI-3000 software when required, with the device driver designed to perform the device dependent functions and the segment storage process designed to manage retained segment usage.

(U) The collection resource utilization program requires one process to manage the user interaction and a second process whenever the collection resource database is queried (see figure 2). It also uses the HLDP and AED512 device driver for all graphics output.

(U) The multiprocess environment was necessitated by the small address space of the PDP 11/70. The implementation of the software structure was performed transparent to the user and in most cases to the application programmer. The interprocess structure can be collapsed without modifying the application software by linking the program with a different library. This makes the majority of the software portable to larger machine environments.

User Interface

(U) The prototype was implemented for inexperienced computer graphics users. The user interface had to be easy to use and "friendly" to avoid user alienation. It also required minimal user interaction to produce useful displays. There are two components to the effective user interface; the graphics screen layout, and the interaction required to produce displays.

(U) The screen was divided into five functional viewports: graphics, menu, legend, system message area, and access time (see figure 3). The intention was to provide the necessary information on the screen to enable the user to perform a task without extensive hardcopy documentation. The arrangement of the viewports is different for the collection resource display and the communications network displays. This was necessitated by the type of data contained in each display. In each case, the largest area is reserved for the user's data. The menu area provides the options available to the user. The menu options are specified in user terminology to enhance the ease of use. Items are preceded by a digit from 0 - 9 indicating the button which will initiate the function. A special menu area is defined to permit certain functions at any processing level. These functions include an online Help facility, a hardcopy Print facility, a Return function and a system Exit function. The collection resource display has an Update function which will requery the collection resources database to obtain the current collection status.

[] The Help facility provides documentation on how the graphics functions work;

[] the Print facility enables users to obtain a hardcopy print of the current display on a TRILOG color printer;

[] the Return function displays the previous menu; and

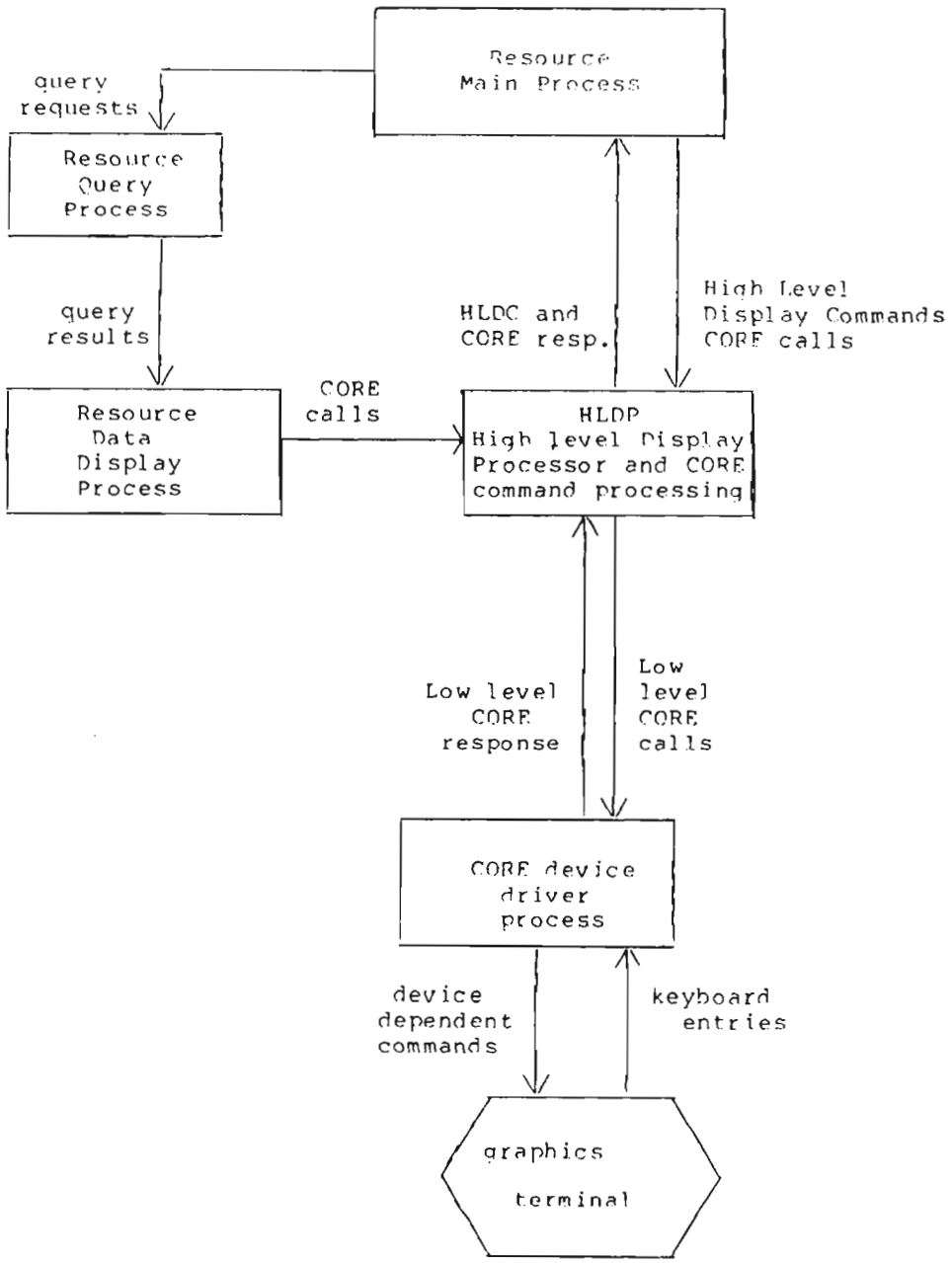
[] the Exit function terminates graphics mode after verification.

Each of these operations is invoked by pressing the key with the first letter of the function. The optional legend area permits user symbols to be defined to aid in interpreting the display.

[] The communications network displays use the legend to color code signal types and define line styles as environments.

[] The collection resource displays use the legend to show the color definitions for the collection data. It has relevance

DOCID: 4011963



~~(C GCO)~~ Resource Status Process Interaction Diagram

Figure 2

DOCID: 4011963

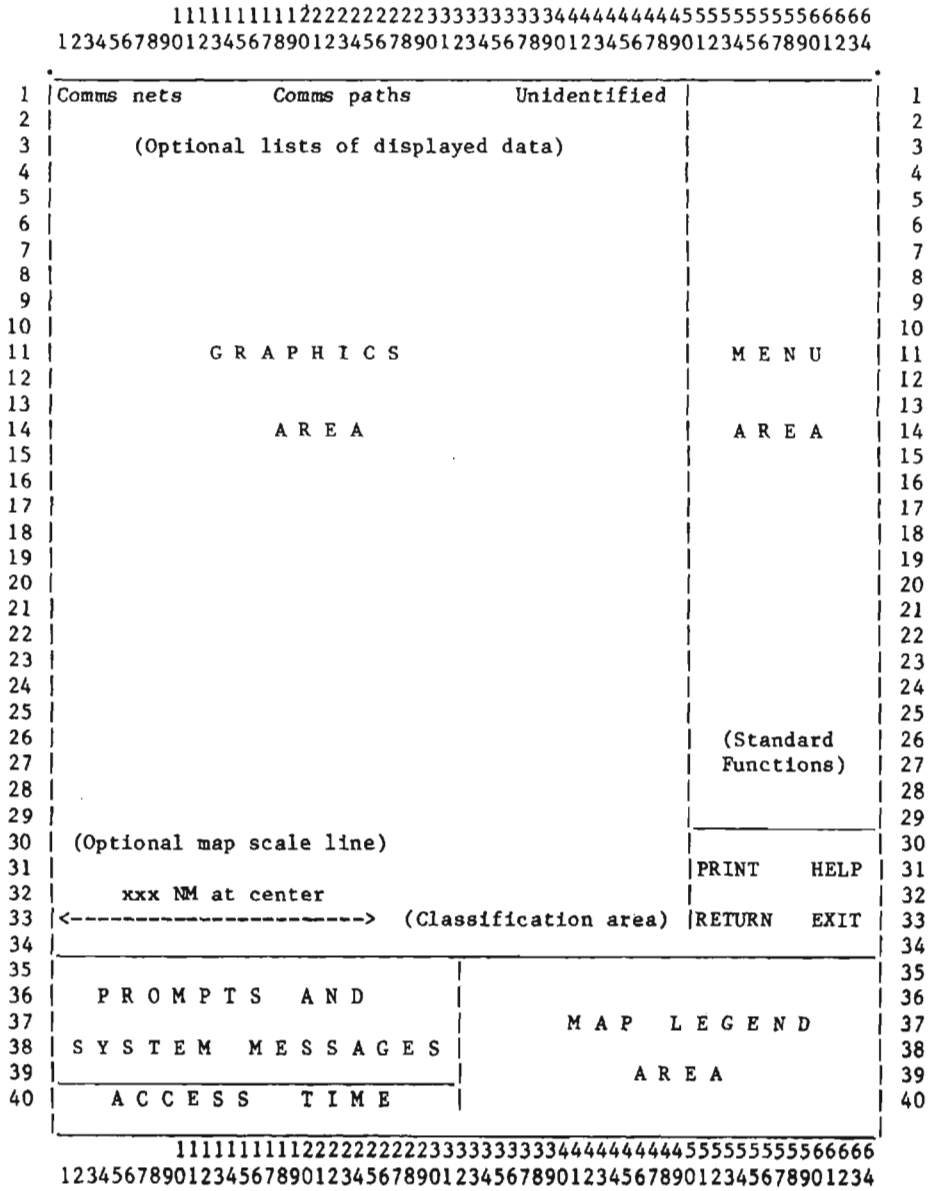


Figure 3

~~(C-CCO)~~ OMSGS general screen format

DOCID: 4011963

only in the communications network display where there is more user interaction with the software. The user is always aware of the current system status by the message displayed in this area.

[] The time area reflects the date and time that the database was accessed to produce the current display. The SOM can determine how old the current display is by examining this field.

(U) The user workstation consists of one alphanumeric terminal for data entry and display (Delta Data 7000), and one AED512 graphics terminal for all graphics displays. The user selects either Collection Resource Display or Communications Network Display from a menu on the alphanumeric terminal. This action will bring the initial graphics display to the AED512 and request input from the user. All graphics interaction is provided through the graphics terminal. The alphanumeric terminal is available to perform other tasks.

(U) The user selects a function from the on-screen menu by pressing the key corresponding to the number beside the menu option. The function selected will either result in a new menu being displayed, a request for additional user input, the change in color of a menu option (turning the parameter on or off), or a change to the main display area. Figures 4 - 8 illustrate a typical sequence of interactions and the resulting displays for communications networks. The system message area will always reflect the current system state to keep the user informed. Invalid selections are trapped and the user is informed of the extraneous input before requesting the next selection.

(U) The collection resource program initiates a database query when the menu item is selected and when the SOM requests an updated status while examining an existing set of resource data. Figure 9 gives an example of a collection resource display.

(U) The user interface has several additional benefits. First, the screen image remains stable at all times. Whenever a state change requires a display alteration, such as displaying a new menu, only the affected viewport is redrawn. The remaining viewports are not affected and the user can page through menus without affecting the legend or main display area. Second, the use of color is effective in showing "on/off" states for system parameters in the menu area. The user can easily recognize the current status of certain parameters by the color in which they appear. The prototype employed yellow for "on" states and gray for "off". The parameter change is reflected immediately in the menu display. Third, the user may request to have the main graphics area redrawn using the full screen area by pressing the 'F' key. This is particularly useful when a hardcopy print of a display without the other four viewports is desired. This full screen mode is available at any level of processing. (You need not be at a specific menu to invoke full screen mode.)

(U) The user has several local files that can optionally be created to save display parameters and overlay data, to alter the color scheme, and to alter the arrangement of the viewports on the display. These files are stored in ASCII format that individuals may alter using any file editor. The files are transportable between homogeneous and heterogeneous systems which enhances their usefulness. The prototype provides the mechanism for users to dynamically override the system default definitions by specifying an alternate filename. The color table specifications are defined by hue, lightness and saturation, and can be easily modified to user desires. The prototype provides a means for users to save display parameters in named files which are then used to regenerate the same display at a different time. The display is regenerated from the user specified filename. The system always saves the current system parameters on exit so a user may resume processing when reentering graphics mode.

(U) The final user interface feature is an online help facility. The user may request documentation on the currently displayed menu options by pressing the 'H' key. The system will display the document on the user's alphanumeric terminal. The user may browse through the document using the alphanumeric keyboard buttons to do paging and scrolling operations.

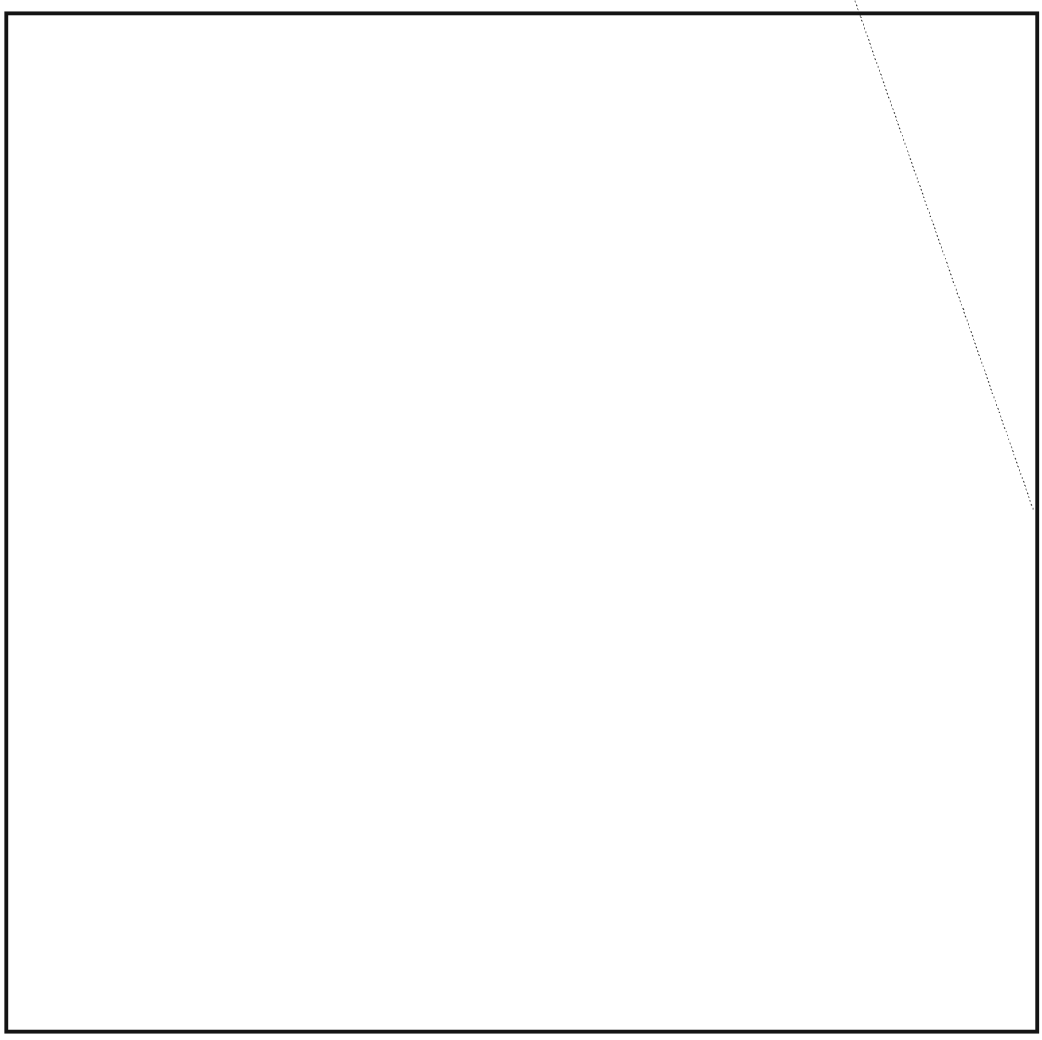
(U) The prototype provides a simple, easy to understand, and flexible user interface. It attempts to encourage inexperienced users without alienating them and at the same time it has the flexibility to enable experienced users to adapt the system to best fit individual needs. Despite the multiprocess configuration, the graphics software is reasonably efficient in processing and response time. Users are always aware of the current processing state and may alter system parameters through menus or files.

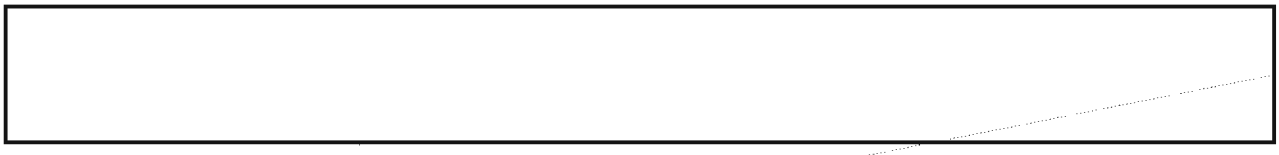
Geographic Software

(U) One objective of the prototype was to provide common geographically oriented displays. This requirement resulted in a map software package that is easy to use and adaptable to general purpose mapping

DOCID: 4011963

EO 1.4.(c)
P.L. 86-36

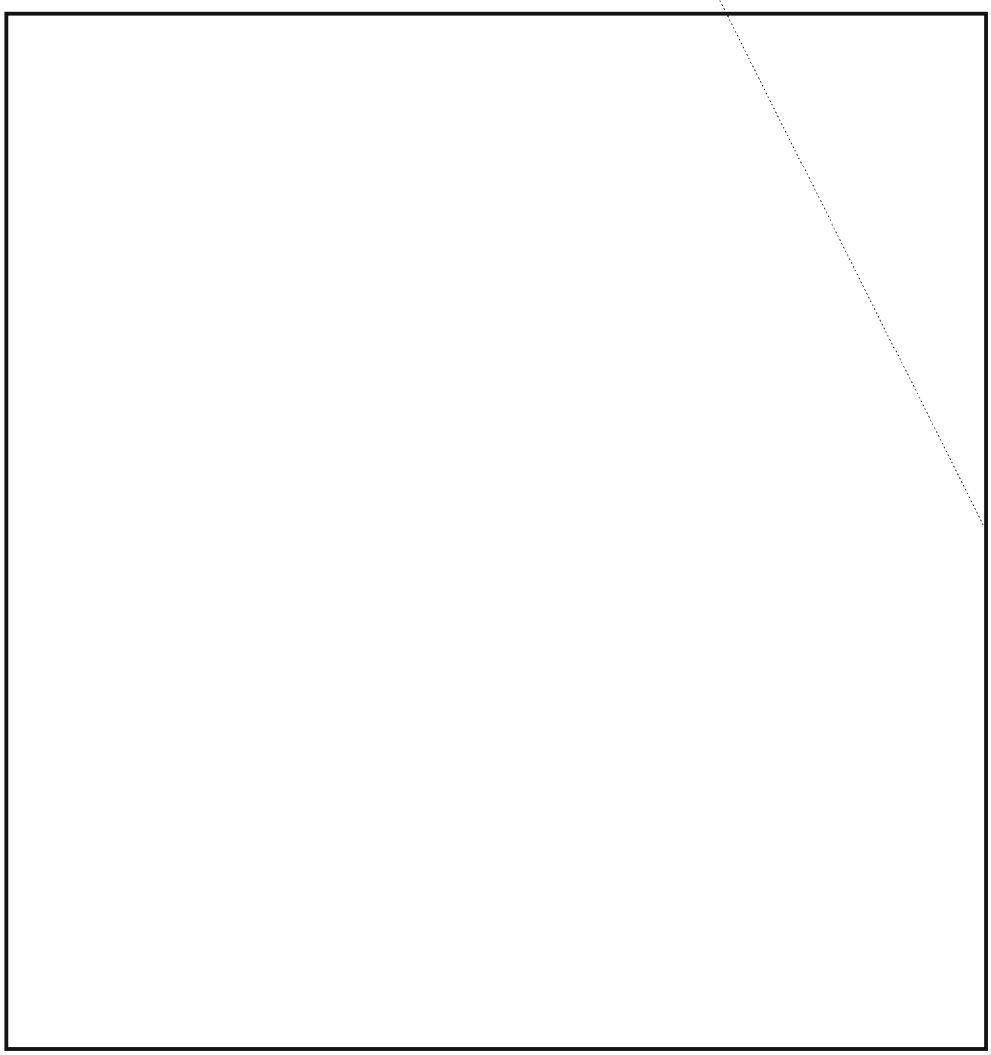


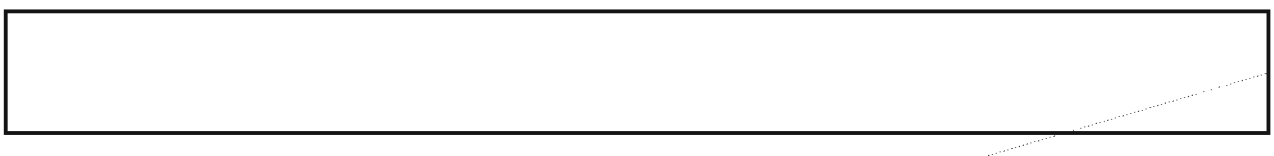


EO 1.4.(c)
P.L. 86-36

DOCID: 4011963

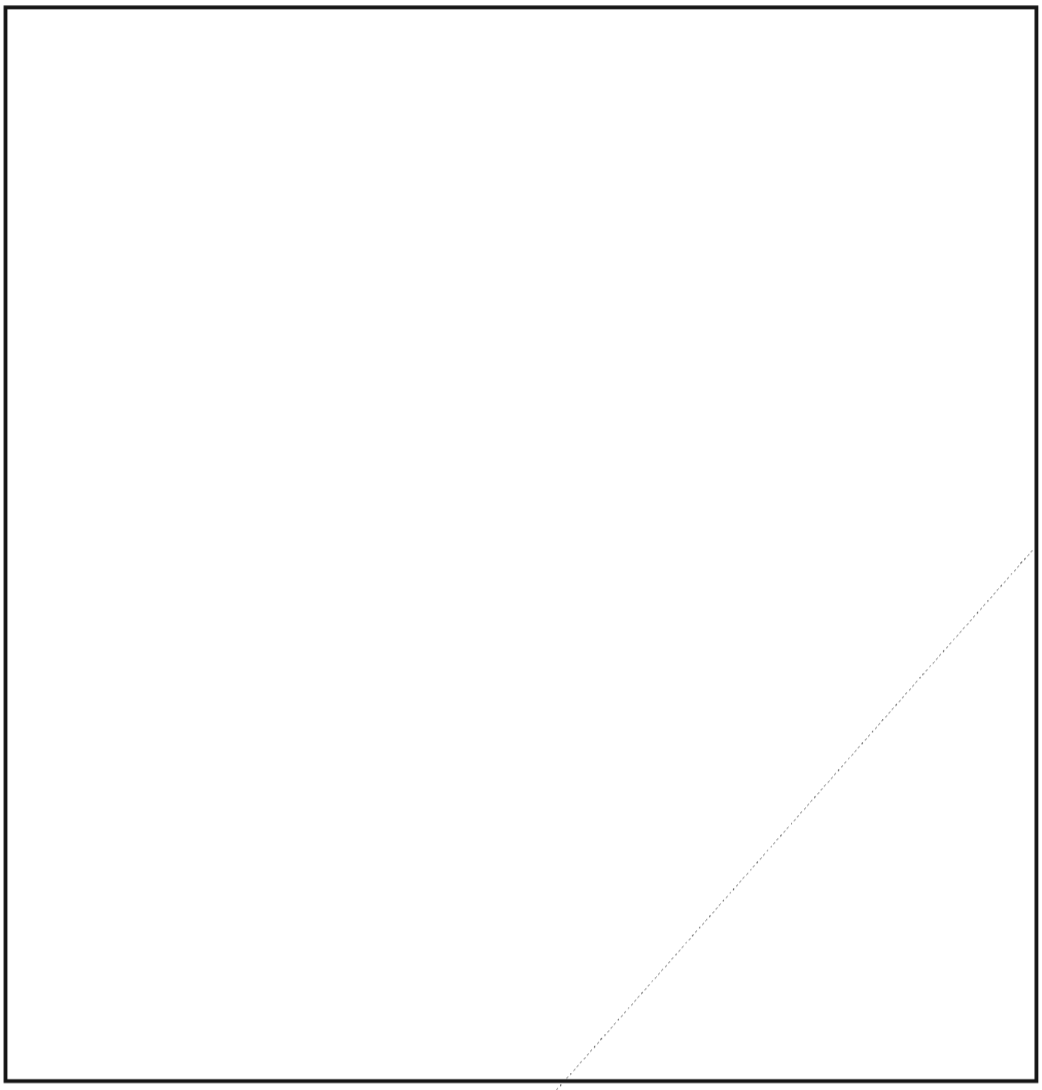
EO 1.4.(c)
P.L. 86-36





EO 1.4.(c)
P.L. 86-36

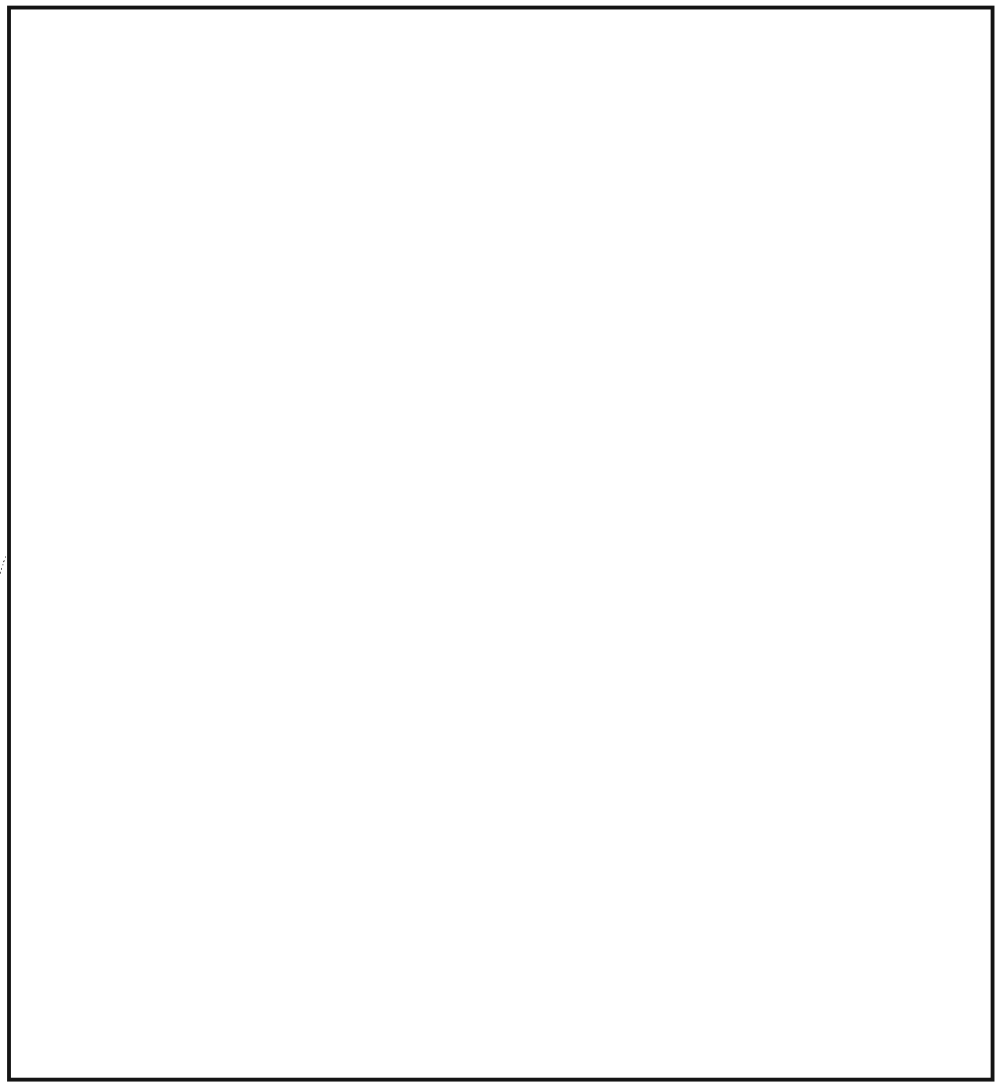
DOCID: 4011963



(U) The "Drawing map ..." message is displayed in the system message area while the map is being drawn.

EO 1.4.(c)
P.L. 86-36

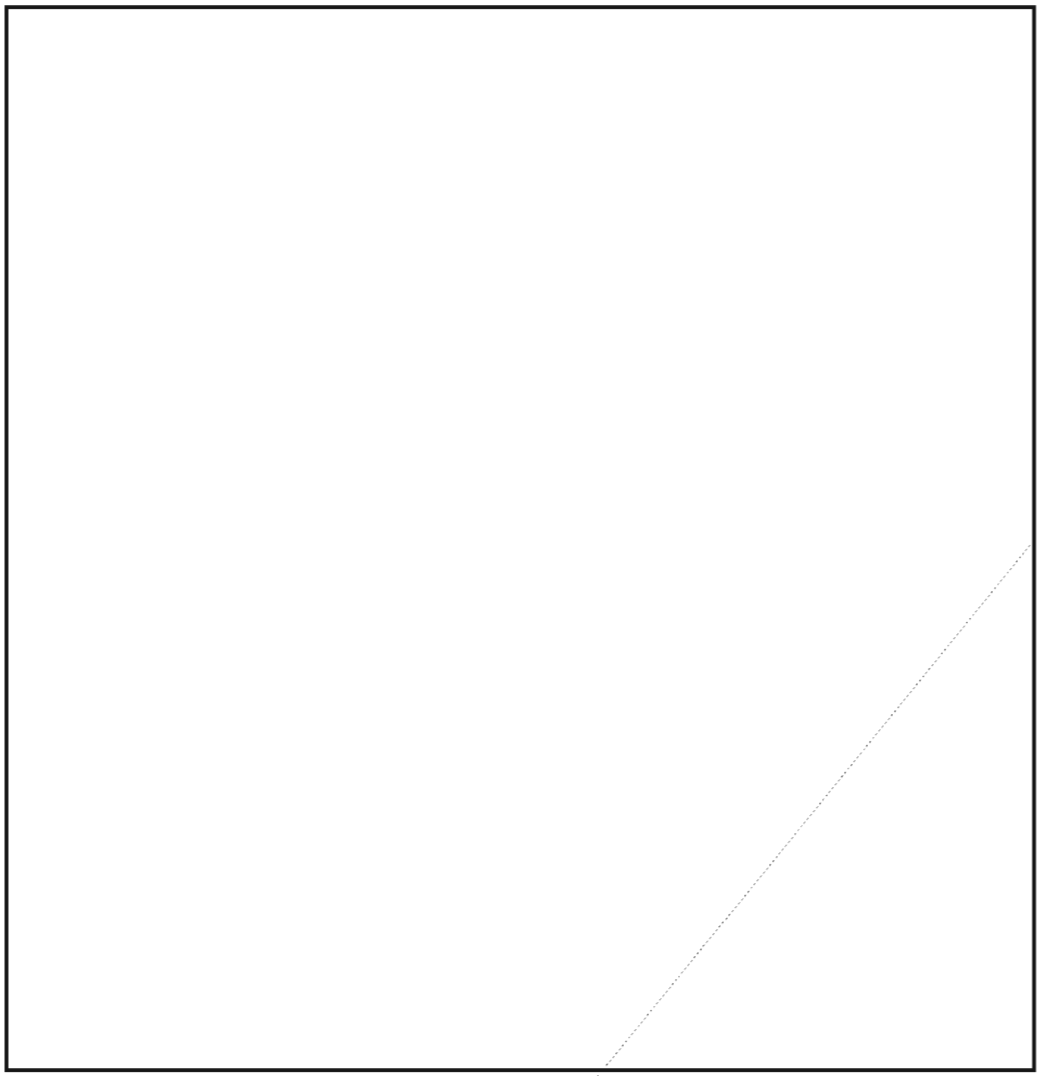
DOCID: 4011963



EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

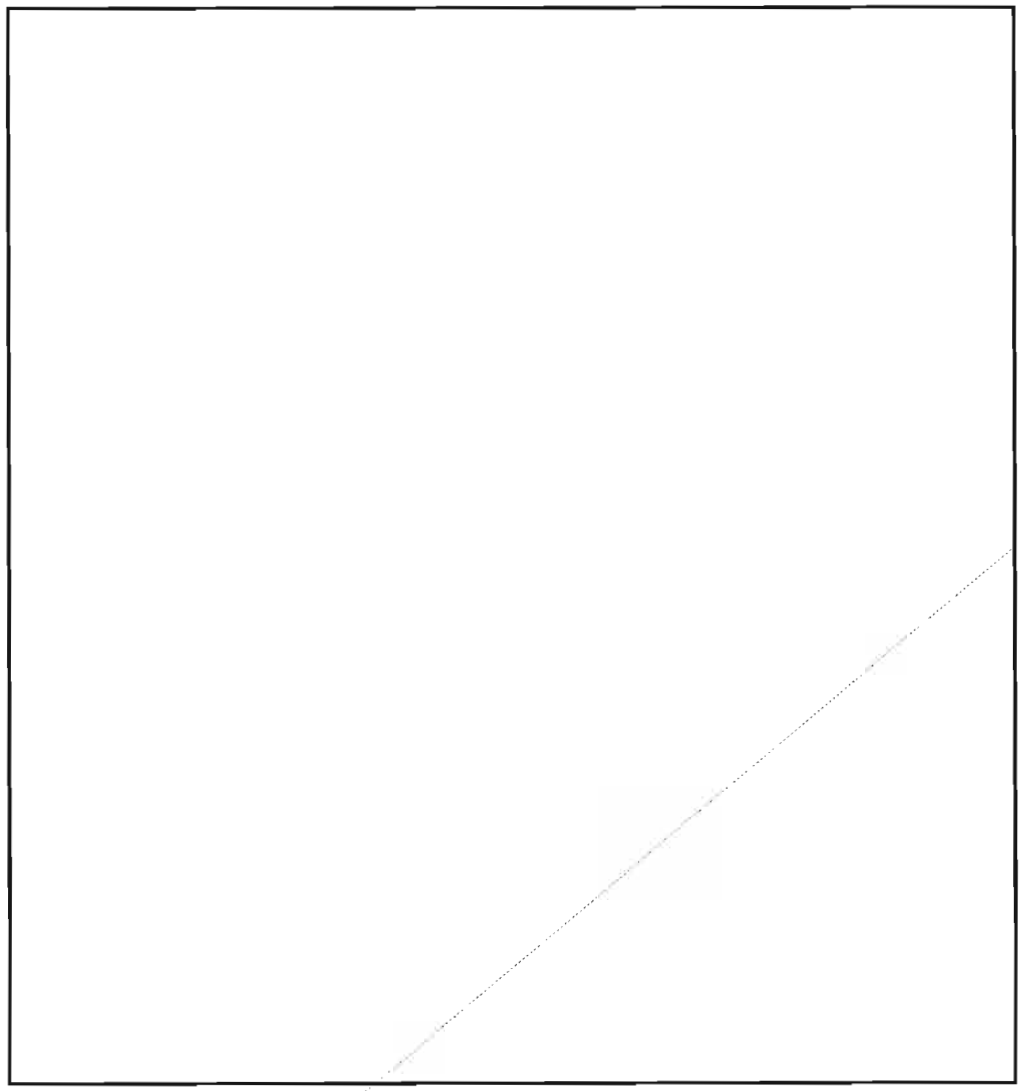
OCID: 4011963



~~(C-CCO)~~ The communications net can be drawn in proper geographic position without the presence of a map. All map features can be "turned off" using the "map features" menu. Subsequent net diagrams will appear more quickly due to the absence of the geographic database access. Map features can then be added when appropriate.

EO 1.4.(c)
P.L. 86-36

DOCID: 4011963

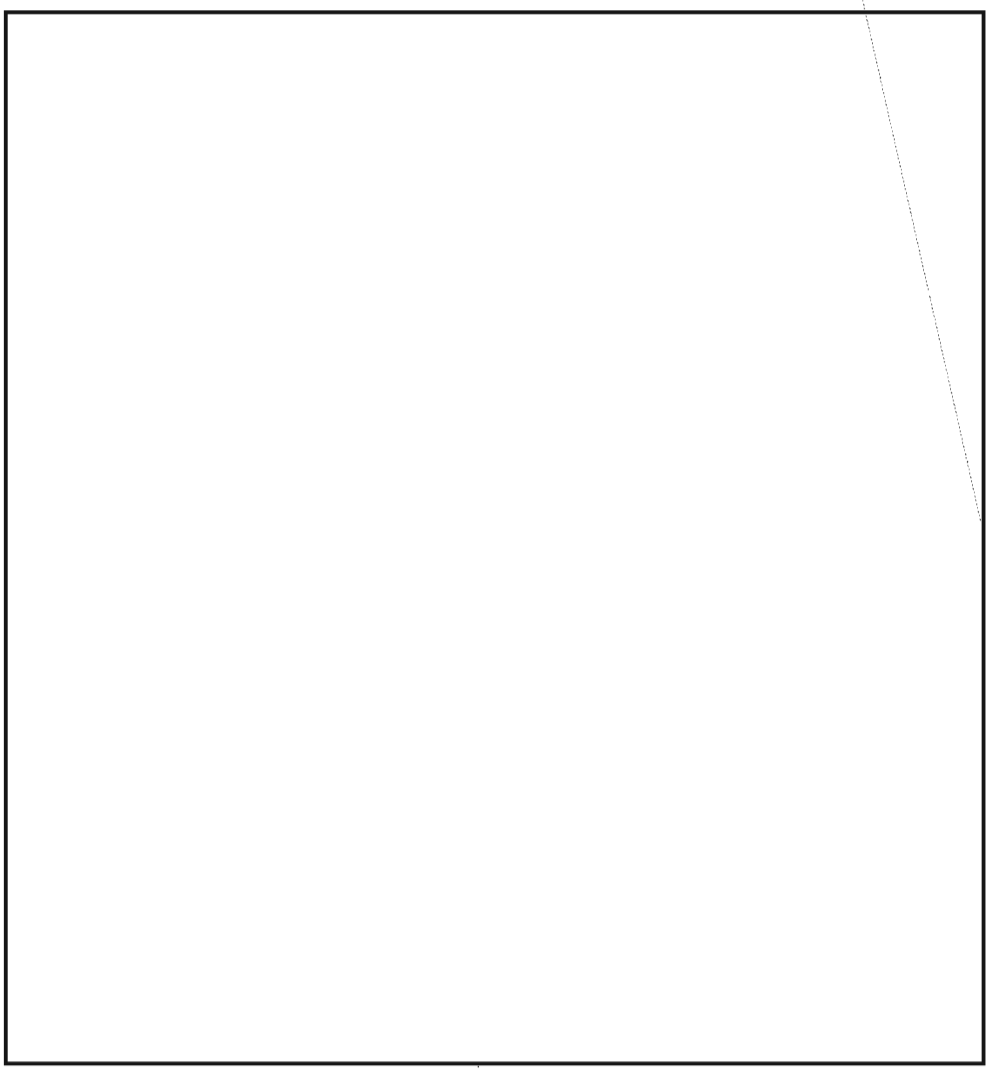


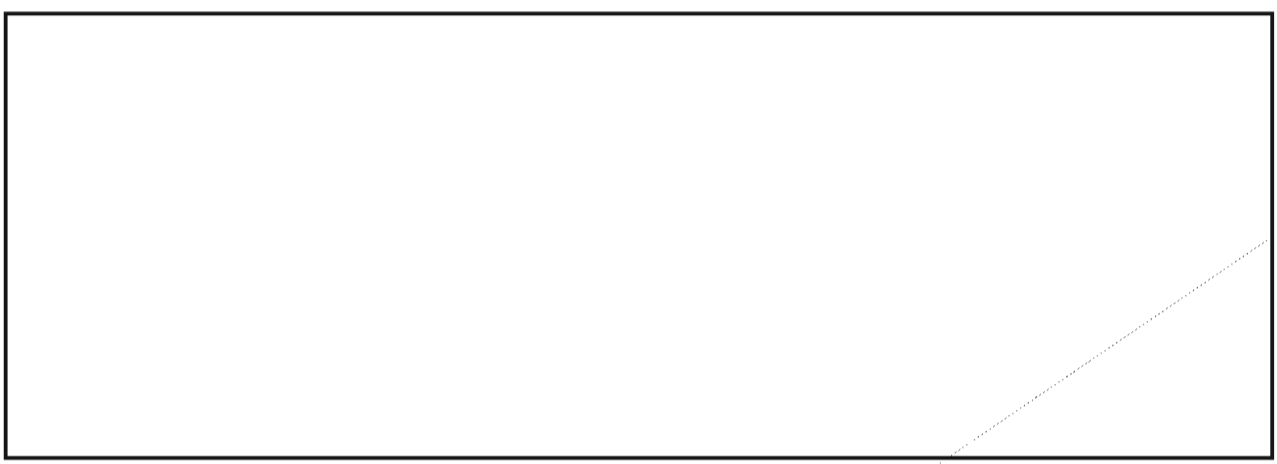
(U) This is an example of the screen used to display collection resource status information. The legend area has been relocated to the lower left and the menu is in the lower right.

EO 1.4.(c)
P.L. 86-36

DOCID: 4011963

EO 1.4.(c)
P.L. 86-36





EO 1.4.(c)
P.L. 86-36

DOCID: 4011963

applications. The programmer draws a map by invoking one subroutine which has a series of arguments to define the map characteristics. The arguments can be set via assignment statements in the program or by end users through the menu interface.

~~(C)~~ The options include:

a. seven projections;

   [] mercator,

   [] gnomonic,

   [] perspective,

   [] orthographic equatorial,

   [] orthographic polar,

   [] orthographic,

   [] equirectangular,

b. four (or more) geographic database resolutions;

c. twelve (or more) geographic feature options;

   [] coastlines, islands, lakes,

   [] political boundaries,

   [] internal political boundaries,

   [] rivers,

   [] railroads,

   [] roads (S.E. Asia),

   [] military district boundaries,

   [] DF data,

   [] latitude/longitude grid lines,

   [] earth outline (orthographic projections),

   [] water fill,

   [] world area names,

d. specification of colors for graphic features;

e. center point of map;

f. map scale (scale indicated by distance across viewport);

EO 1.4.(c)
P.L. 86-36

(U) The map displays are generated from a standard geographic database, the WDBII. Special access techniques are employed to directly address subsets of the data and reduce data access time for arbitrary area maps. One of four versions of the WDBII data is chosen automatically based on the scale of the map being drawn. These subsets were created by selecting "1 out of N" points from the original data. This method reduces the amount of data that is read and processed when minimal detail is sufficient. The most detailed version of the map data on the operational system uses 1 out of 32 points.

(U) There are several additional features the geographic software provides. First, the selection of the map area can be dynamically determined based on the user overlay data. The user may select the data to be displayed and the software will provide the correct map based on the area covered by the data. The burden of producing the proper geographic region is not on the user. Second, the user may select a geographic area or country by name and the map software will select the map center and scale. Finally, the geographic software provides calculations to compute distances between two user specified points, azimuth calculations, and inverse projections. The current geographic parameters are preserved at the end of a user session to enable continuation in the next session.

EO 1.4.(c)
P.L. 86-36

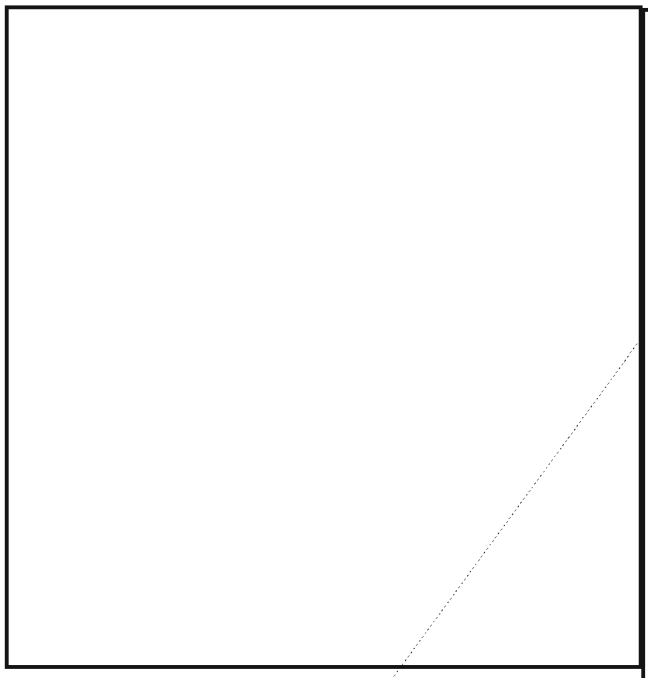
[redacted]

P.L. 86-36

[redacted] Software: Collection Resource Status

[redacted]

DOCID: 4011963

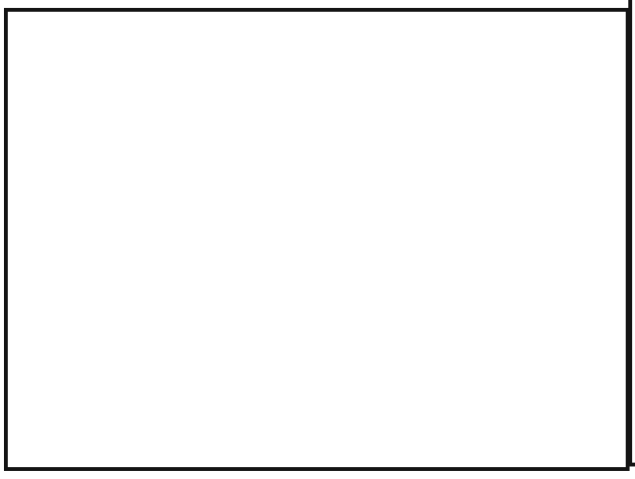


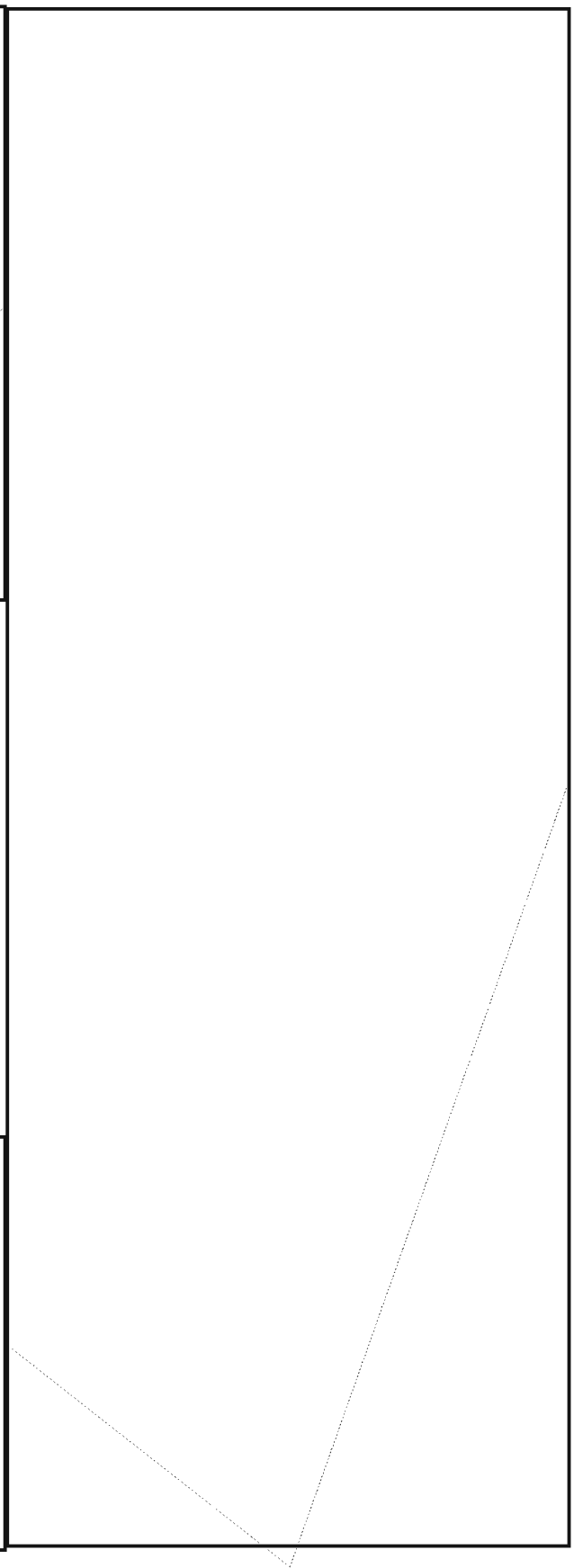
(U) The SOM can manipulate the display by scrolling up or down, paging up or down, proceeding directly to the beginning or end of the display, or requerying the file to obtain the latest information. These are invoked by pressing the corresponding key number next to the option or a 'U' for the update. The last page of data contains statistics on information being collected but not forwarded and counts of the receivers used for the collection.

P.L. 86-36
EO 1.4.(c)

~~(C-CCO)~~ Future considerations include selective query for either GOOTEE 1 or GOOTEE 2 lines and options for displaying partial records and summaries.

IOMS Software: Communications Network Displays





P.L. 86-36
EO 1.4.(c)

DOCID: 4011963

EO 1.4.(c)
P.L. 86-36

(U) Not all information contained in the network data records can be conveyed using the techniques described above. A menu option was provided to enable the SOM to enter "amplify mode." This feature permits the SOM to position the cursor (using a joystick) over a marker, PNAB or line segment, press any key and have the data record(s) corresponding to that item displayed in an enlarged system message area. This is especially useful to investigate display conflicts.

CONCLUSION

(U) The prototype was a significant step toward a coherent approach to the development of new graphics software at NSA.

(U) The value of color graphics was demonstrated in an operational environment on important Agency concerns. Color graphics provides an effective, dynamic method of conveying information to an analyst to affect near-real-time decision making. It proved effective in reducing or eliminating:

- [] time examining black and white alphanumeric listings to isolate events requiring analysis,
- [] volumes of multiple hardcopy alphanumeric listings required to present the same "picture" to an analyst, and
- [] the documentation in comparison to written summary detailing the collection management events.

(U) Portability was demonstrated in the transfer of software between 16- and 32-bit machines, and the use of several graphics output devices without significant change in the application software. The WDBII and other geographic data files were also transferred without change. The named map parameter and data files provided an initial version of the capability to store and transfer finished pictures.

(U) The quickly developed initial capability and subsequent evolutionary growth were valuable in keeping the system visible to the users. There were no major surprises, and the feedback from the users helped in "fine tuning" the system to meet their needs.

(U) New users considered it easy to learn. Additional features for the experienced user are planned including a command mode consisting of short English sentences to allow direct control of the system without menu interaction.

(U) Many of the geographic and menu functions are applicable to other systems without change. The technique developed to transfer CORE commands between processes on the 16-bit machine has already been used to transfer commands between two other computer systems.

(U) CORE as a basis for the development of interactive graphics software has been shown to be effective. The addition of modular graphics functions using CORE primitives was important in enhancing the value of the CORE system for the development of applications software with similar requirements.

BIBLIOGRAPHY

[1] Delmar E. Anderson, James L. Angel and Alexander J. Gorny, "World Data Bank II: Content, Structure and Application", Harvard Papers on Geographic Information Systems, Vol 2, 1978.

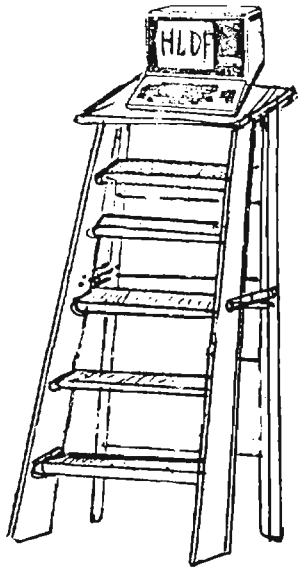
[2] "Status Report of the Graphic Standards Planning Committee", Computer Graphics 13(3), August 1979.

[3] W. Jones, A. Hockenbery, P. Peters, C. Lempke, "Standardized DF Algorithm for Target Location using Bearing Information", NSA/CSS paper, 1 March 1976.

DOCID: 4011963

THE NSA HIGH-LEVEL DISPLAY FILE

Requirements and Basic Design (U)



P.L. 86-36

by [redacted] R53

Introduction

(U) The NSA High-Level Display File (HLDF) is a high-level applications data structure to be used in the modern NSA graphics system. The fundamental idea behind the HLDF is to unambiguously describe the graphics used both in the analytic processes at NSA and in NSA end product. While a simple file format for such a graphic (and a conceptually adequate one) would include only primitive geometric constructs such as lines, polygons, markers, etc. (in the manner of the Core System metafile [1], the GKS metafile [2], and the Tektronix Graphic Model Exchange Format [3], and others [4, 5, 6]), the HLDF is an application data structure that contains not only these primitives but also contains high-level application-specific constructs. The particular high-level constructs included in the HLDF have been especially chosen to reflect NSA's peculiar graphics needs and include entities such as maps, timelines, pie charts, etc. The set of constructs and primitives chosen for the HLDF is certainly not logically minimal (because a map, for instance, can be expressed as a sequence of line primitives) but it is a logically complete set because of the inclusion of the more primitive geometric constructs. These primitive constructs provide a "safety net" ensuring that any graphics image can be encoded in an HLDF. The design of the HLDF is also constructed so that the set of HLDF primitives and constructs can easily be extended to include, at an equally high level, other graphic formats should they become desired.

(U) One use of the extensibility feature of the HLDF can be seen in the inclusion of what is traditionally not considered to be a part of graphics: digital images. This "other side of the coin" of displayed pictures is included in the HLDF in a logically consistent manner with that of traditional graphics, and its inclusion represents a possible future trend for analytic graphics at NSA.

ACKNOWLEDGEMENTS

The need for an HLDF was recognized as a result of informal discussions held by the Graphics Investigation Group (GIG), a cooperative effort between T4, R5, and T3, as part of the GIG's proposals for a coherent Agencywide approach to computer graphics. All of the individuals involved in the GIG provided the author with numerous ideas, read and critiqued the early versions of this paper, and in general provided the enthusiasm and camaraderie that is needed to strike out on such a novel path. Especially noteworthy in this regard were the contributions of [redacted] the chairman of the GIG. P.L. 86-36

The HLDF idea also matured as a result of presentations before two groups. A presentation was made before the R53 Technical Forum in July 1981 that provided for an early examination of the HLDF goals and basic proposals--an examination that had a noticable effect on the resulting proposal. The students of the National Cryptologic School course on computer graphics (MP-413) read the final draft of this paper and their questions and observations forced me to improve the overall clarity and consistency of the document.

My thanks to all for their contributions. Any errors still present remain, of course, the responsibility of the author. K.J.S.

OCID: 4011963

Ed note:
Only Appendix I of this paper has been included. All the other appendices are available in the full report (TR-R53-11-82, S-224-904).

(U) The HLDF is NSA specific but it is not a repeat of the NSA designed and developed programming languages such as BETA [7], GOTS, or POGOL with their corresponding support, acceptance, and transportability difficulties but rather is a data structure, and more specifically, a file format. Such an NSA specific format definition would be needed if, among other things, NSA product is to be shipped electronically to NSA customers. The need for such a specific format and its precise definition is independent of the particular programming language chosen for the various applications programs. There are commercially available graphics file formats ([1, 2, 3]), but these include only the most primitive graphics entities that would be common across the myriad commercial applications of graphics. The encoding of a map, for example, using these schemes would be voluminous and would not allow later manipulation at the logical level--for example changing the map projection. For this reason the design of an NSA HLDF was undertaken.

Design Goals

(U) The design goals of the High Level Display File are:

- to contain all the information necessary to reconstruct a given display;
- to provide for the "logical" manipulation of a display generated from an HLDF (the so-called "Out to Lunch" problem; i.e., the problem of the construction of a complex graphic by a computer-naive analyst with interruptions of several hours or several days);
- to be machine- and graphics device-independent;
- to be unseen and transparent to the end user;
- to serve as an NSAwide (and perhaps Communitywide) graphics metafile for picture storage, transmission, and regeneration;
- to be easily interpreted; and
- to be as compact and space-efficient as possible for most of NSA's graphics needs, without conflicting with the other design goals.

(U) Peripherally, it is also desired that this data structure promote a modular design of the graphics system using it. This goal can be achieved by a system in which the HLDF is:

- constructed by one routine of the system, thus localizing the need to understand the details of the HLDF structure; and
- "executed" by another routine, whose lower level routines implement the actual graphics algorithms that construct the displays encoded by the HLDF.

(U) These goals imply that the current HLDF (i.e., the HLDF corresponding to the current display):

- store the structure of the current display (e.g., at the level of map, circle, text, histogram, etc.) and not just store separate and logically "disconnected" line segments or pixels;
- be updated (i.e., by the addition, the modification, or the deletion of an entry) with each and every modification to the graphics portion of a display; and
- explicitly store all possible parameters, e.g., line color and style, text font, map projection, scale, etc. Thus, the HLDF itself must not rely on any system defaults since they can be different not only from system to system within the Agency, but also from user to user within any system.

(U) Also the design of the HLDF:

- will resolve conflicts between space-efficiency and ease of use (in construction, execution, and debugging) in favor of ease of use:
- will not enable the end user to differentiate between a display built "from scratch" from one recalled from secondary storage. Thus any operation possible at any point in a graphics system must be equally possible for a restored display (created in a previous session on that system) and a display built entirely at that session;
- will guarantee that a transmitted picture will be redisplayed exactly as it was created (e.g., same colors, line styles, marker positions, etc.), though the receiver will be able to modify the display at the logical level (e.g., change

DOCID: 4011963

the color of some entity or the background, move a marker or icon, add additional lines, text, or markers, redesign legends, use a different map projection, add or remove inserts, etc.);

- is the "glue" that holds together many of the modules in the modern NSA graphics system. It compactly represents the display at any point during the user's session with the system. It must efficiently encode displays associated with geographics, management graphics, briefing slides, and dependency charts, but must also be capable of use in other application areas such as signals analysis, VLSI design, ideographic language processing, etc.

(U) The use of this HLDF for the transmission of graphics is not dependent upon the particular CPU of the receiver, the graphics hardware, or even the graphics systems software of the receiving system. The receiving system need only possess software which can interpret the HLDF format. In addition, the receiving system must have appropriate geographic data [redacted] the NSA Icon file (a file now being designed which will store frequently used icons, e.g., missile outlines, military unit designators, mushroom clouds, etc.), and the font data for the various character sets to be used.

Proposed Design

(U) The following is a design for an HLDF that purports to satisfy all of the above design goals. In the course of constructing this design, two major implementation decisions were made--decisions whose impact and effect on the HLDF design are second only to the major design goals enumerated above. The first of these implementation decisions is that this HLDF design does not allow for the direct encoding of three-dimensional data, but only for data in two dimensions. This decision is motivated by two concerns:

- the extremely small use of three-dimensional graphics in graphics applications in the Agency and
- the great increase in complexity that would be incurred in designing and implementing a three-dimensional HLDF as opposed to a two-dimensional one.

There is little to be gained in delaying the use of a two-dimensional HLDF for the amount of time that it would take to design and implement a complete three-dimensional HLDF. For those few applications that may require a three-dimensional HLDF, such an HLDF could be designed at a later date and equipped with a three-to-two-dimensional HLDF translator. A three-dimensional HLDF-based system equipped with such a translator would allow a three-dimensional display to be stored locally with the ability for later logical manipulation of three-dimensional entities and for the transmission of such a display in a manner that would allow redisplay by anyone capable of processing a two-dimensional HLDF. The receiver of such a transmission would not, however, be able to modify this transmitted display at the logical level, since the three-dimensional entities that make up this display are not directly represented in the translated and transmitted HLDF; they are represented by their two-dimensional projections and thus the modification process would not be possible at the logical level.

(U) The second major implementation decision for the proposed design which follows is in the choice of coordinate systems. In this proposed design, an HLDF can contain data expressed in either one of only two coordinate systems: the traditional latitude/longitude coordinates for geographic plots and an integer Cartesian coordinate system with a range from 0 to $2^{16} - 1$ for each dimension (hereafter referred to as the integer virtual coordinate system). Systems that use any other type of coordinate system (e.g. polar coordinates, normalized device coordinates, etc.) are responsible for transforming that data into one of these coordinate systems for inclusion into an HLDF. These two coordinate systems are meant to be used exclusively for any given HLDF, though with some disclaimers concerning the results of subsequent zooming operations. These two coordinate systems can be used in one HLDF.

(U) Given these two implementation decisions, there are at least two different approaches to the design of this format. One approach is that of a generative grammar (used, for example in the Caltech graphics metafile for VLSI circuits [8]) and another is an assembly language model with op-codes and arguments. Because the graphics used in NSA product typically do not have the intricate internal structure found in circuit layouts and thus cannnot easily avail themselves of the expressive power of a generative grammar, the assembly language model was chosen as the basis for the HLDF design. At the highest level, a general format of an HLDF which will satisfy the stated design goals is:

OCID: 4011963

```
OP_CODE[1]      ARGUMENT_LIST[1]
OP_CODE[2]      ARGUMENT_LIST[2]
   .
   .
   .

OP_CODE[n]      ARGUMENT_LIST[n]
```

where each ARGUMENT_LIST is of variable length. However, since on some systems (i.e., machines and/or operating systems) this variable-length structure is difficult (if not impossible) to construct and process, this format may be further specified as

```
BEGIN_HLDF_TOKEN

     OP_CODE[1]      BEGIN_ARG_LIST_TOKEN

                     ARGUMENT[1],

                     ARGUMENT[2],

                     ARGUMENT[3],

                     .
                     .
                     .

                     ARGUMENT[n]

                     END_ARG_LIST_TOKEN

     OP_CODE[2]

        .
        .
        .

END_HLDF_TOKEN
```

giving it fixed-length records. This second approach of using an assembly language model for the design of the format of the HLDF itself has two alternatives:

- the op-codes can be fixed length encodings, e.g., a three-long character string; or
- they could be encoded using a Huffman-like encoding giving the more frequently-used op-codes shorter encodings and the less frequently used op-codes longer encodings.

A Huffman scheme can significantly reduce the size of the data set to be transmitted, but for our purposes here it is felt to be an unnecessary complication to the basic design. Accordingly, the proposed encoding for the op-codes will be fixed length. Note that this does NOT prevent any particular installation from using such a Huffman scheme for transmission, nor does it prevent a later modification to the detailed design for the HLDF from using such a scheme.

(U) The op-code is a three-long character string representing the graphics entity being constructed or some information necessary for the reconstruction of the display. The elements of the ARGUMENT_LIST are separated by commas and not all arguments are mandatory.

(In the detailed description of the individual op-codes that follows, optional arguments are surrounded by square braces. The only other use of braces in that description is for array indices. Context easily distinguishes these two uses.)

The order of the op-codes in an HLDF is important to the structure of the display it represents in two ways:

- the overlaid structure of the display may depend on the order in which particular entities are displayed (the so-called "two-and-one-half" dimension hidden surface processing which allows pseudo-three-dimensional pictures to be constructed by judiciously choosing the order in which two-dimensional objects overlap and are displayed); and
- some control information necessary for the display of some entities is contained in op-code entries that precede the actual definition of the entity.

(U) The op-codes that have been defined to date are given below, separated into the logical categories of General Control, Geographics, Management, and Basic Graphics. Following these lists are detailed explanations of the individual op-codes.

- General Control
  - [] Begin
  - [] End
  - [] Comment
  - [] Viewport
  - [] Plot Size
  - [] Classification
- Geographics
  - [] Map Controls
  - [] Map

OCID: 4011963

- [] Geo_Marker
- [] Geo_Line
- [] Geo_Conic
- [] Geo_Text
- [] Geo_Polyline
- [] Geo_Polygon
- [] Geo_Military Symbol

● Management

- [] Histogram
- [] Pie Chart
- [] Bar Chart
- [] Timeline
- [] Line Graph

● Basic Graphics

- [] Text
- [] Rectangle
- [] Line
- [] Marker
- [] Polygon
- [] Fill
- [] Axes
- [] Polyline
- [] Circle
- [] Arc
- [] Image
- [] Military Symbol

General Control Op-Codes

Op_Code: BEG (Begin Segment)

Argument List: [Label, Line_Color, Line_Style, Line_Width, Character Attributes (Font, Text_Color, Character_Direction (x,y), Character_Path, Character_Size, Position_Precision)]

(U) Comments: The op-code 'BEG' allows for an Algol-like block structure to be imposed on the HLDF. Within the scope of a particular block (named with the 'Label' argument), one can set values for the current color, current line style, current line width, current character attributes, etc. These values will be used unless specifically overridden by different values in one of the op-codes within the block, and then these new values will be used only for that particular op-code. The initial 'BEG' of an HLDF, i.e., the 'BEG' of the outermost block must contain values for all the optional arguments in order to set the initial default values for this HLDF, since one of the design goals was that the interpretation of an HLDF not depend on the defaults for a particular system or user. Subsequent 'BEG' op-codes may contain only those arguments that are desired.

(U) Note: 'BEG' must be matched with the next most closely nested 'END'.

(U) The possible values for the various parameters are:

Label	Any text string
Line_Color	An HLS triple PLUS a Line, Style value. The Line Style value included here will be used *ONLY IF* the displaying system does not support color and, in this case, this Line Style overrides the normal Line Style. (See Appendix III or original report.)
Line_Style	{Solid, Dashed, Dotted, Dot-Dash}
Line_Width	An integer from 1 to 99. 1 corresponds to the narrowest line and 99 to the widest.
Character Attributes	The display attributes of any text string. (See Appendix IV of original report for details. This parameter has a number of possible subparameters explained below.
Font	{Roman, Italics, Roman Bold}
Text_Color	An HLS triple
Character_Direction	The direction vector for the writing direction of the text. Both X and Y must be integers from 0 to $2^{16} - 1$. Note that a

DOCID: 4011963

	character direction of (0, 0) is not valid, since this vector has no direction.
Character_Path	{Right, Left, Up, Down} (See Appendix IV of original report for a description of how the character attributes work.)
Character_Size	An integer from 1 to $2^{16} - 1$ where $2^{16} - 1$ corresponds to a character filling the entire current viewport.
Position-Precision	{High, Medium, Low}

(U) Note: From this point on in the HLDF proposal, none of the individual character attributes will be explicitly named in the op-code description. These parameters will be referred to by the group name "Character Attributes". See appendix IV for further details.

Op_Code: END (End Segment)

Argument List: [Label, Checksum]

(U) Comments : This op-code delineates the extent of a picture block. The optional, though strongly encouraged, argument must match the 'Label' of the corresponding 'BEG' op-code.

(U) The 'Checksum' argument provides a further level of redundancy and error detection for an HLDF file than is normally given to any other alphanumeric file by the system. If present, this argument should contain a checksum of the bytes in the concluded HLDF. If the receiving system finds a discrepancy between this count and the count of the received block, then that HLDF should be marked as defective and the transmitter should be notified to retransmit.

(U) It is possible that there would arise a situation where an HLDF would be constructed on one graphics system and then transferred via magnetic tape to another system (possibly with a different CPU and/or operating system) for transmission. This situation is important because in the writing to magnetic tape the HLDF may undergo some seemingly trivial modifications, such as replacing EOLs or <CR>s by <CR><LF>s, addition or deletion of nulls and of trailing spaces, conversion of TABs into spaces, addition of spaces/CRs at either end of the HLDF, and the like. It is desired that any checksum algorithm proposed for use with the HLDF for the computation of the 'Checksum' argument be invariant under such transformations.

(U) This checksum provides only an additional level of error detection not error correction. It is modeled after (more properly, stolen from) the checksum proposed for the Caltech Intermediate Form (CIF) format for the transmission of VLSI designs over the ARPAnet.[9] The computational method proposed there may even be useful for the HLDF checksum and this checksum algorithm is presented in Appendix II of original report.

Op_Code: COM (Operator Comment)

Argument List: String

(U) Comments : This non-graphic, non-executable op-code allows the originator of the HLDF to communicate a small amount of alphanumeric information to the displayer of the HLDF. This text string could contain such information as the originator's name, the classification (admittedly redundant, but not a bad idea anyway; see CLA below), etc. The displaying program may, for example, merely echo the 'String' to the associated alphanumeric "device" when the HLDF is processed.

(U) Note that there is no theoretically imposed or a priori limit on the size of the 'String' argument, but a limit of 100 characters seems consistent with the intent of this op-code.

Op_Code: VPT (Screen Viewport)

Argument List: Lower_Left_Corner (x,y), Upper_Right_Corner (x,y) (in the integer virtual coordinate system)

(U) Comments : This defines the portion of the display surface in which the picture corresponding to this HLDF is to be displayed. The default (that is, the value if this op-code is not present) is for a full-screen viewport. This op-code, if present, governs the display of all entities in its block. Accordingly, it must preceed all op-codes which construct graphic entities.

(U) This use of a 'VPT' op-code allows one HLDF to contain more than one viewport and allows the user to logically manipulate this image in terms of these viewports. The user could, for example, make only one of several viewports appear on the screen or could even change the viewport extent.

(U) This control op-code allows the user both to place several non-overlapping pictures

on one screen, as well as to specify a portion of the display for an inset (i.e, overlapping pictures). Because of this, the virtual coordinate system used in this block (with the exception of the 'VPT' op-code) is the full coordinate system, not a subset, and is such that its full extent is displayable in the viewport window. That is, the coordinate system inside any viewport is the same. A viewport using the integer virtual coordinate system uses the entire coordinate system regardless of the size of the viewport or its aspect ratio. This will allow for subsequent zoom opertations to be accurately displayed.

(U) The VPT op-code will be used for, among other things, legend boxes and small map inserts displayed at a different scale than the main map.

(U) Note that such an inset viewport may "lie on top of" a larger picture and the end user will be able to "look under" the inset by removing it. The picture underneath will not be affected by this use of a viewport.

Op_Code: SIZ (Plot Size)

Argument List: X_Extent (in hundredths of an inch), Y_Extent (in hundredths of an inch), String

(U) Comments: This op-code allows the originator of an HLDF to request a certain plot size when hardcopies are made. An 8.5" x 11" plot, for example, would be requested with the arguments (850, 1100). The 'String' argument allows for the passing of a small amount of alphanumeric information from the originator to the plotter operator.

Op_Code: CLA (Classification)

Argument List: Major_Classification, [Position, Character Attributes], [Codewords (Codeword[1], Codeword[2], ... , Codeword[n]), Caveats (Caveat[1], Position[1], Caveat[2], Position[2], ... , Caveat[n], Position[n], Character Attributes)]

(U) Comments: The classification for use by the receiver of the HLDF, for hardcopies, etc. The classification is set in this op-code in order to make it easily accessible by the receiving system. Some have suggested that the system not allow a graphic hardcopy to be made of any HLDF file that does not possess a CLA op-code somewhere in its structure.

(U) The possible values for the various parameters are:

Major Classification	{None, Unclassified, Secret, Top Secret}. Note that 'None' is the null classification; i.e, it will not appear on the graphic when the HLDF is interpreted.
Position	(x,y) in the integer virtual coordinate system or a lat/long value.
Character Attributes	(See 'BEG' op-code and/or Appendix IV of the original report.) (For Major Classification and Codewords only.)
Codewords	String. These strings will be appended to the Major Classification and will appear on the same line with it.
Caveats	String. These strings will be diplayed at their individually specified positions, typically on separate lines. One example of a caveat is "EYES ONLY DIRNSA". No maximum size is given for these caveats, but 50 seems reasonable.
Character Attributes	(See 'BEG' op-code and/or Appendix IV of the original report.) (For Caveats only.)

Geographic Op-Codes

Op_Code: MPC (Map Controls)

Argument List: Center (lat/long), Radius (nautical miles), Projection, Grid_Switch, [Grid_Height, Grid_Width,] Map_Line_Resolution, Altitude_Viewpoint

(U) Comments: This op-code must precede any of the geographic op-codes, and its parameters govern the display invoked by all subsequent geographic op-codes. At most one MPC op-code may be present within the scope of a single viewport (VPT), regardless of whether the VPT op-code is explicitly present or if it is implied for an entire HLDF by its absence. The 'Projection' argument takes its values from the set of cartographic projections, a set which currently includes Mercator, Gnomonic, Orthographic, Polar, Perspective, etc. The 'Grid_Switch' argument determines

OCID: 4011963

whether or not a lat/long grid is to be displayed, and 'Grid_Height' and is displayed, in degrees (in DDDMMSS format). The 'Map_Line_Resolution' parameter gives the user some control over the precision of the map background. This parameter takes its values from {rough, medium, detailed}, with 'detailed' providing the largest amount of map detail. The value of 'detailed' for this parameter may be appropriate for very detailed maps of a small region or for the final high-quality plotting of maps for inclusion in product. The 'rough' value would be appropriate for a schematic of a large area or for a "quick and dirty" map for some types of preliminary analytic work. It is anticipated that the user-perceived response time for a graphics system to draw a detailed map will be significantly larger than for a rough map. The 'Altitude_Viewpoint' is a measure in nautical miles of the altitude of the viewpoint used in perspective cartographic projections.

Op_Code : MAP

Argument List : Feature_Level_of_Detail,
(Feature_Name[1], Color[1]),
(Feature_Name[2], Color[2]), ...,
(Feature_Name[n], Color[n]),

(U) Comments : This op-code is the encoding for the map background data. The feature names are present only if they are to be displayed and are chosen from the following set : {International Boundaries; Coastlines, Islands, and Lakes; Rivers; Internal Boundaries; Military Districts; Air Corridors; Railroads; etc.} Any given feature name can be present in the argument list at most once. The 'Color' subparameters are chosen in accordance with the usual HLDF color encoding. (See the 'BEG' op-code and/or Appendix III of the original report.) and a particular "color" may be present in the argument list more than once. The 'Feature_Level_of_Detail' subparameter takes its values from the set {major, intermediate, all} with the value 'major' providing only the most prominent features and the value of 'all' providing all of that feature present in the map data base.

Op_Code : GMK (Geographically_based Marker)

Argument List : Position (lat/long),
Marker_Number (in the NSA Icon File),
Scale, Orientation (as measured in degrees from the equator), [Mirror_Image_Flag,
Text_String[1], Text_String_Position[1] (x,y), Character Attributes[1],
Text_String[2], Text_String_Position[2] (x,y), Character Attributes[2], ... ,
Text_String[n], Text_String_Position[n] (x,y), Character Attributes[n]]

(U) Comments : This op-code allows for the placement of marker symbols (e.g., circles, triangles, military unit symbols, icons of antennas or missiles, etc.) on a map. The 'Mirror_Image_Flag' takes its values from {on, off} and when 'on' causes the icon displayed to be a mirror image of the stored icon image. Since some of the symbols have a varying textual component, the 'Text_String' allows a user to associate this string with the marker. The position of the text string is expressed in the integer virtual coordinate system but with respect to the position of the marker. That is, the position of the text string is relative to that of the marker. Its character attributes are determined by the optional parameters, if present, or the current character attributes otherwise. Note that the Character_Direction is with respect to the coordinate system of the marker; i.e., if the icon is turned 5 degrees with respect to the equator, then the Text_String will be too if the horizontal Character Direction is used. The horizontal Character_Direction is (1, 0).) To angle just the Text_String with respect to the marker the Character_Direction parameter should be changed accordingly. The 'Scale' parameter controls the size of the displayed icon relative to its definition size. The values for this parameter range from 0 to 99, with the scale of the icons as stored in the NSA Icon file defined to be size 30. Some samples depicting the effect of these various parameters on the display of icons are shown in Figure 1.

(U) Note that (1) the application programs that change the size of a marker will probably also want to change the size of any attached text, but that this function is outside of the HLDF itself; (2) the display of any associated text string is not affected by the value of the 'Mirror_Image_Flag'; and (3) there is no 'Color' parameter to this op-code since the Icon file itself is assumed to store multicolored icons.

Op_Code : GLN (Geographically-based Line)

Argument List : Endpoint[1], Endpoint[2], (Both expressed in lat/long), Direction_Flag, [Line_Style, Color, Width]

(U) Comments : This op-code allows for the placement of geographically-based lines. The 'Direction_Flag' is set to TRUE if the line direction (from Endpoint[1] to Endpoint[2]) is to be indicated (e.g., with arrowheads). Other optional arguments allow for the temporary override of the current color, line style, and width. Note that this line will not, in general, be a straight line on the display; but rather will be seen by the viewer as the result of a cartographic projection of

OCID: 4011963

a "straight" line onto the Earth's surface.

Op_Code: GCO (Geographically-based Conic)

Argument List: Type, Center (lat/long), Semi_Major_Axis, Semi_Minor_Axis (in nautical miles), Orientation (as measured in degrees from the Equator)

(U) Comments: This op-code allows for the placement of a conic against a geographic background. The 'Type' argument takes values from the following set: {ellipse, circle, hyperbola, parabola}. Note that the conic is on the Earth's surface; the displayed figure will exhibit the distortions typical of cartographic projections.

Op_Code: GTX (Geographically-based Text)

Argument List: String, Position (lat/long), [Character Attributes]

(U) Comments: There are a number of possible relationships between the position value and the exact string placement. For example, the position value could be the left bottom corner of the string. It could be the bottom center, top center, center center, etc. For the HLDF encoding, the left bottom corner will be used. Note that this does not affect the manner in which the end user perceives his text placement functions, but rather only the manner in which the applications programmer must provide the information to an HLDF routine--two entirely different operations!

Op_Code: GPL (Geographically-based Polyline)

Argument List: Number_of_Points, Point[1] (lat/long), Point[2], ..., Point[Number_of_Points], [Line_Style, Width, Color]

(U) Comments: Self-explanatory extension of the geographically-based line (GLN). This GPL op-code is included in the HLDF definition for the same reason it is included in other graphic file formats; i.e., for efficiency in implementation.

Op_Code: GPG (Geographically-based Polygon)

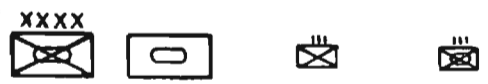
Argument List: Number_of_Points, Point[1] (lat/long), Point[2], ..., Point[Number_of_points], Fill_Pattern (Interior = Color, Edges = Color, Vertices = Color)

(U) Comments: The argument 'Point[1]' is both the starting and ending point of the polygon. The values for the subparameter 'Color' are the same as those in MAP.

Op_Code: GMS (Geographically-based Military Symbol)

Argument List: Position (lat/long), Flag, Symbol_Size, [Primary_Duty, Secondary_Duty, Staff, Base, Associated Text (Text_String[1], Text_String_Position[1], Character Attributes[1], Text_String[2], Text_String_Position[2], Character Attributes[2], ... , Text_String[n], Text_String_Position[n], Character Attributes[n]), Size, Color, Interior_Color]

(U) Comments: These entities denote the positions of particular types of military units. They are derived from the "standard" military symbols such as:



For further details, see Appendix V of the original report.

Management Graphics Op-Codes

(U) NOTE: The HLDF encodings presented here for management graphics are not final. See the section on Unresolved Questions for a discussion of the alternate path that may be taken for this encoding.

Op_Code: HST (Histogram)

Argument List: X_Axis_Label, Y_Axis_Label, Percentage[1], Percentage[2], Percentage[3], ... , Percentage[n], Color, Number_of_Title_Lines, Title[1], Title[2], ..., Title[Number_of_Title_Lines], X_Axis_Ticks, Y_Axis_Ticks, X_Axis_Labels[1], X_Axis_Label[2], ... X_Axis_Label[n], Y_Axis_Labels[1], Y_Axis_Label[2], ... Y_Axis_Label[m],

(U) Comments: An encoding of a histogram. The possible parameter values are:

X_Axis_Label, Y_Axis_Label	Character string
Percentage[1:n]	[0 .. 100]
Color	An HLS value PLUS a line pattern. See

OCID: 4011963

Appendix III of the original report for details.

Number_of_Title_Lines	[0 .. 4]
Title[1:Number_of]	Character string
X_Axis_Ticks, Y_Axis_Ticks	[0 .. (2^{16})]
X_Axis_Label[1:n], Y_Axis_Label[1:n]	Character string

(U) Note that the actual data from which the histogram was constructed is not stored in the HLDF, but rather only the data necessary to reconstruct the display.

Op_Code: PIE (Pie Chart)

Argument List: Number_of_Sectors, Percentage[1], Percentage[2], ..., Percentage[Number_of_Sectors], Label[1], Label[2], ..., Label[Number_of_Sectors], Label_Position[1], Label_Position[2], ... , Label[Number_of_Sectors], Explode((Sector[1], Distance[1]), (Sector[2], Distance[2]), ... , (Sector[m], Distance[m])), Percentage_Label_Position[1], Percentage_Label_Position[2], ... , Percentage_Label_Position[Number_of_Sectors], Radius, Color[1], Color[2], Color[3], ... , Color[Number_of_Sectors], Pattern[1], Pattern[2], Pattern[3], ... , Pattern[Number_of_Sectors], Starting_Angle, Edge_Style

(U) Comments: An encoding of a standard pie chart allowing for exploded sectors and two types of labels. The "Starting Angle" parameter is the angle from the horizontal for the start of sector 1. This is required in order to insure that the pie chart will be displayed in exactly the same orientation on different systems. All other parameters are self-explanatory.

Op_Code: BAR (Bar Chart)

Argument List: Style, X_Axis_Label, Y_Axis_Label, Number_of Families, Number_of_Bars, Amount1[1], Amount1[2], ... , Amount1[Number_of_Bars], [Amount2[1], Amount2[2], ... , Amount2[Number_of_Bars], Amount3[1], Amount3[2], ... , Amount3[Number_of_Bars]], Color[1], Size (Left_Top_Corner, Right_Bottom_Corner), [Color[2], Color[3], Color[4], Number_of_Title_Lines, Title_Line[1], [Title_Line[2], Title_Line[3]], Legend_Position, Legend_Name[1], [Legend_Name[2], Legend_Name[Number_of_Title_Lines]], Legend_Style, X_Axis_Tic_Mark_Labels[1:n], X_Label_Position, Y_Axis_Tic_Mark_Labels[1:n], Y_Label_Position

(U) Comments: (To be determined)

Op_Code: TML (Timeline)

Argument List: (To be determined)

(U) Comments: (To be determined)

Op_Code:LNG (Line Graph)

Argument List: Number_of_Families, X_Axis_Label, Y_Axis_Label, X_Range (X_High, X_Low), Y_Range (Y_High, Y_Low), Family[1] (Number_of_Line_Segments, (X[1], Y[1]), (X[2], Y[2]), ... , (X[Number_of_Line_Segments], Y[Number_of_line_Segments])), [Family[2] (Number_of_Line_Segments, (X[1], Y[1]), (X[2], Y[2]), ... , (X[Number_of_Line_Segments], Y[Number_of_line_Segments])), ... , Family[Number_of_Families] (Number_of_Line_Segments, (X[1], Y[1]), (X[2], Y[2]), ... , (X[Number_of_Line_Segments], Y[Number_of_line_Segments])),] Color[1], [Color[2], ... , Color[Number_of_Families],] Number_of_Title_Lines, Title_Line[1], [Title_Line[2], Title_Line[3],] X_Axis_Tic_Mark_Labels[1:n], X_Tic_Mark_Interval, Y_Axis_Tic_Mark_Labels[1:n], Y_Tic_Mark_Interval

(U) Comments:(To be determined)

Basic Graphics Op-Codes

Op_Code: TXT (Text)

Argument List: String, Position, [Character Attributes]

(U) Comments:(None. See Appendix IV of the original report for details.)

Op_Code: RCT (Rectangle)

Argument List: Lower_Left_Corner, Upper_Right_Corner, [Fill_Color, Fill_Pattern, Orientation]

DOCID: 4011963

(U) Comments: "Orientation" is measured in degrees from the X-axis direction. Possible "Fill Pattern" values are shown in Figure 6 of Appendix IV (in the original report).

Op_Code: LIN (Line)

Argument List: Endpoint[1], Endpoint[2], [Width, Line_Style, Color]

(U) Comments: (None)

Op_Code: MRK (Marker)

Argument List: Position (x, y), Marker_Number, Scale, Orientation (as measured in degrees from the X axis), [Mirror_Image_Flag, Text_String[1], Text_String_Position[1] (x,y), Character Attributes[1], Text_String[2], Text_String_Position[2] (x,y), Character Attributes[2], ... , Text_String[n], Text_String_Position[n] (x,y), Character Attributes[n]]

(U) Comments: (Same as Geographically based Marker, GMK.)

Op_Code: PLG (Polygon)

Argument List: Number_of_Points, Point[1] Point[2], ..., Point[Number_of_points], Attributes (Interior_Style, Interior_Color, Edge_Color, Edge_Style, Edge_Width, Vertex_Color, Vertex_Size)

(U) Comments: Point[1] is both the starting and ending point of the polygon. 'Vertex_Size' is the size of the dot used for the vertex. The meaning of the other arguments is self-explanatory. The values for the Attribute subparameters are:

Interior_Style	(To be determined)
Interior_Color	HLS value PLUS Fill Pattern
Edge_Color,	HLS value PLUS Line Style
Vertex_Color	HLS value
Edge_Style	(Solid, Dashed, Dotted, Dot-Dash}
Edge_Width	{Narrow, Normal, Wide}
Vertex_Size	[0 .. 99]

Op_Code: FIL (Fill)

Argument List: Interior_Point (x,y), Fill_Color, Fill_Pattern

(U) Comments: This command will be used to fill an area of the screen not defined as a polygon (using the PLG command above), such as the region bounded by three mutually intersecting lines. Fill_Color is an HLS value PLUS a Fill Pattern. See Appendix III of original report.

Op_Code: AXS (Axes)

Argument List: X_Lower_Bound, X_Upper_Bound, Y_Lower_Bound, Y_Upper_Bound, [X_Axis_Tick_Mark_Labels[1:n], X_Tick_Mark_Interval, Y_Axis_Tick_Mark_Labels[1:n], Y_Tick_Mark_Interval, Line_Style, Width, Color]

(U) Comments: (To be determined)

Op_Code: PLN (Polyline)

Argument List: Number_of_Points, Point[1] (X, Y), Point[2], ..., Point[Number_of_Points], [Line_Style, Width, Color]

(U) Comments: (None)

Op_Code: CIR (Circle)

Argument List: Center (X, Y), Radius, [Fill_Style, Fill_Color], Border_Style, Border_Color]

(U) Comments: (None)

Op_Code: ARC (Arc)

Argument List: Center (X, Y), Radius, Start_Angle, Stop_Angle, [Fill_Style, Fill_Color], Border_Style, Border_Color]

(U) Comments: The parameters 'Start_Angle' and 'Stop_Angle' are measured in degrees from the horizontal.

Op_Code: MIS (Military Symbol)

Argument List: Position (x, y), Flag, Symbol_Size, [Primary_Duty, Secondary_Duty, Staff, Base, Associated Text (Text_String[1], Text_String_Position[1], Character Attributes[1], Text_String[2], Text_String_Position[2], Character Attributes[2], ... , Text_String[n], Text_String_Position[n], Character Attributes[n]), Size, Color, Interior_Color]

OCID: 4011963

(U) Comments: These entities denote the positions of particular types of military units. They are derived from the "standard" military symbols. For further details, see Appendix V of original report.

Op_Code: IMG (Image)

Argument List: (To be determined)

(U) Comments: A pixel array that is to be placed within a certain portion of the current viewport. It is through this image op-code that digital images can be placed in the background of an HLDF with the possibility of adding additional graphics "on top of" the digital image.

Operations involving an HLDF

(U) The operations which are to be performed on a data structure (and the frequency with which they will be performed) can be used to guide the decisions in its implementation. The operations which will be performed on the HLDF are (roughly in order of frequency):

- Execute (i.e., construct the display represented by some HLDF, thus making that HLDF the current HLDF.) The HLDF to be executed will usually be stored on disk.
- Add a new graphics entity.
- Store (on disk).
- Transmit (over PLATFORM).
- Search for some entity by op-code and some parameters.
- Modify some entity (e.g., change color, edit text).
- Search for some entity based on the values of some parameters (no op-code).
- Delete some entity.
- Overlay the display represented by a given HLDF on the current display, thus concatenating the given HLDF to the current HLDF.

??? UNRESOLVED QUESTIONS ???

(U) There are two approaches to the inclusion of management graphics in the HLDF design. One is to try to parameterize the seemingly infinite varieties of such charts (e.g., the MANY possible styles of line graphs). This is the approach that was taken, with perhaps some success. This approach can be termed the "All things to all people" approach. The other approach is to standardize a couple of line graph formats, a couple of bar chart formats, etc. These would then be the ones compactly encoded by an HLDF. If an end user had to have a different format, it could still be encoded using the basic graphics safety net, albeit with some loss of later functionality with regard to later modifications of that HLDF. In this second approach, there would be a FAMILY of op-codes for, say, line graphs: LGA, LGB, LGC, ... Implementation would probably be simplified. This approach can be called the "Family of Fixed Formats" approach. Which approach is better in the long run for the HLDF?

Appendix I: HLDF Examples

(U) Following are some sample HLDF encodings. Each has been done "by hand" from a given display in order to simulate the HLDF that would be output, so the reader should not be concerned about the third or fourth decimal place for the numerical values, but rather the overall structure. All examples closely resemble Agency product but all are taken from unclassified open-source material. In order to increase the readability of these examples, the format used will be "Variable = VALUE" where the "Variable" is some argument name and "VALUE" is the value for that argument. Most probably this will not be the format employed for an actual HLDF implementation and, accordingly, the values given for the sizes of these example HLDFs will be character counts for the VALUEs only.

(U) Unless otherwise indicated, all the figures in this section are from [10].

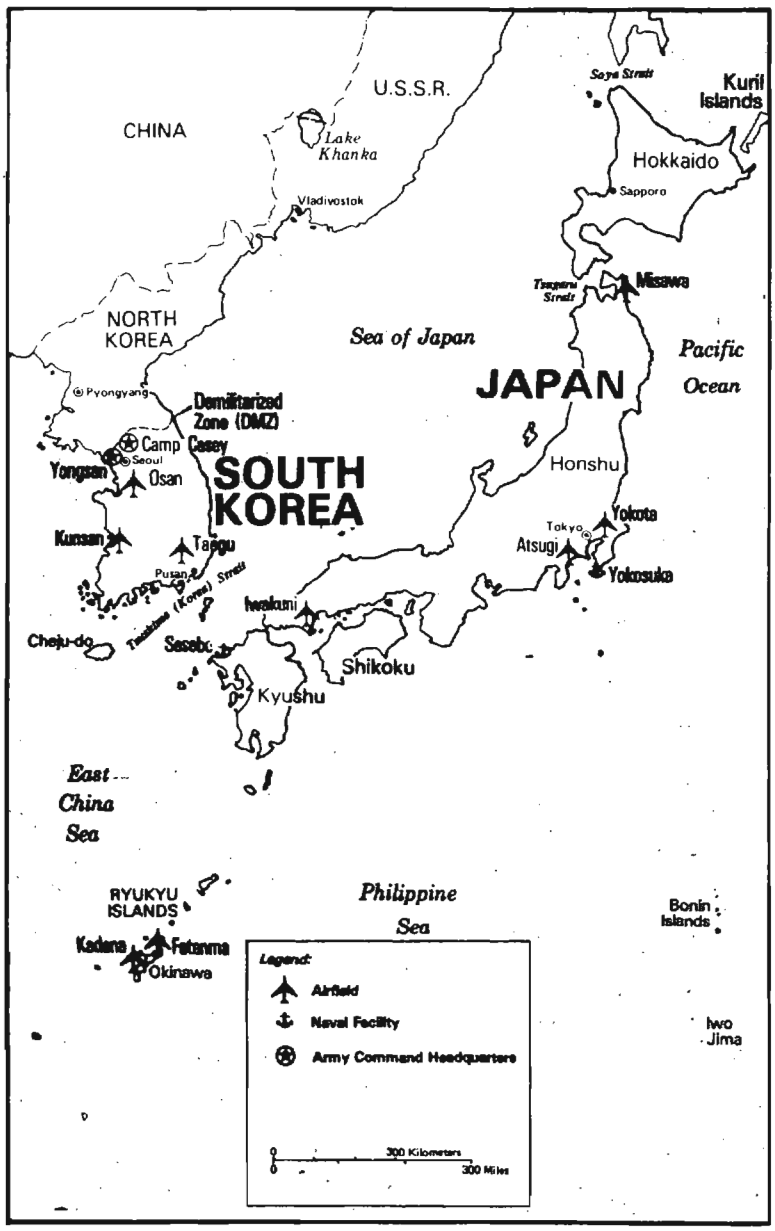
Example 1: Geographic HLDF with Icons and Inset (Shown in Figure 1)

(Size of this HLDF is 4,152 characters)

```
OP_CODE      ARGUMENT LIST

  BEG        Label = EXAMPLE1, Line-Width = 1,
             Character Attributes (Font = ROMAN,
             Text_Color = (0, 0, 0),
             Character_Direction = (1,0),
             Character_Path = RIGHT,
             Character_Size = 500,
             Position_Precision = HIGH.

  COM        String = "BLACK AND WHITE GRAPHIC,
             HIGH PRECISION. UNCLASSIFIED"

  CLA        Major_Classification = NONE
```

DOCID: 4011963

Figure 1: Geography with Icons and Legend



OCID: 4011963

MPC Center = (354000N,1341200E), Radius = 893, Projection = MERCATOR, Grid_Switch = OFF, Level_of_Detail = DETAILED, Altitude_Viewpoint = 1000

MAP (COASTLINES, SOLID), (INTERNATIONAL BOUNDARIES, DOT-DASH), (MAJOR ISLANDS, SOLID), (MINOR ISLANDS, SOLID), (MAJOR LAKES, SOLID)

GMK Position = (410000N, 1412000E), Marker_Number = 122, Scale = 30, Orientation = -5, Text_String = "Misawa," Character Attributes (Font = ROMAN BOLD, Position = (600, 100), Character_Size = 700)

GMK Position = (434000N, 1404200E), Marker_Number = 3, Scale = 30, Orientation = 0, Text_String = "Sapporo," Character Attributes (Position = (300, 0), Character_Size = 200)

GMK Position = (424200N, 1321000E), Marker_Number = 3, Scale = 30, Orientation = 0, Text_String = "Vladivostok," Character Attributes (Position = (100, 300), Character_Size = 200)

GMK Position = (372000N, 1265200E), Marker_Number = 62, Scale = 30, Orientation = 0, Text_String = "Pyongyang," Character Attributes (Position = (300, 0), Character_Size = 200)

GMK Position = (365200N, 1271000E), Marker_Number = 39, Scale = 30, Orientation = -5, Text_String = "Camp Casey," Character Attributes (Font = ROMAN BOLD, Position = (400, 0), Character_Size = 700)

GMK Position = (364100N, 1263200E), Marker_Number = 39, Scale = 30, Orientation = -5, Text_String = "Yongsan," Character Attributes (Font = ROMAN BOLD, Position = (-2048, -300), Character_Size = 700)

GMK Position = (363700N, 1265200E), Marker_Number = 62, Scale = 30, Orientation = 0, Text_String = "Seoul," Character Attributes (Position = (200,50), Character_Size = 700)

GMK Position = (360200N, 1273300E), Marker_Number = 122, Scale = 30, Orientation = -5, Text_String = "Osan," Character Attributes (Position = (300, 50), Character_Size = 700)

GMK Position = (354200N, 1264600E), Marker_Number = 122, Scale = 30, Orientation = -5, Text_String = "Kunsan," Character Attributes (Font = ROMAN BOLD, Position = (-2000, 0), Character_Size = 700)

GMK Position = (353841N, 1285500E), Marker_Number = 122, Scale = 30, Orientation = -5, Text_String = "Taegu," Character Attributes (Font= ROMAN BOLD, Position = (200, 50), Character_Size = 700)

GMK Position = (354000N, 1400000E), Marker_Number = 62, Scale = 30, Orientation = 0, Text_String = "Tokyo," Character Attributes (Position = (-1024, 200), Character_Size = 200)

GMK Position = (353000N, 1382216E), Marker_Number = 122, Scale = 30, Orientation = -5, Text_String = "Atsugi," Character Attributes (Font = ROMAN BOLD, Position = (-2000, 100), Character_Size = 700)

GMK Position = (344225N, 1413000E), Marker_Number = 164, Scale = 30, Orientation = -5, Text_String = "Yokosuka," Character Attributes (Font = ROMAN BOLD, Position = (300, -75), Character_Size = 700)

GMK Position = (344016N, 1293511E), Marker_Number = 3, Scale = 30, Orientation = 0, Text_String = "Pusan," Character Attributes (Position = (-100, -40), Character_Size = 200)

GMK Position = (335750N, 1321047E), Marker_Number = 122, Scale = 30, Orientation = -5, Text_String = "Iwakuni," Character Attributes (Font = ROMAN BOLD, Position = (-2500, 100), Character_Size = 700)

GMK Position = (332712N, 1295842E), Marker_Number = 164, Scale = 30, Orientation = -5, Text_String = "Sasebo," Character Attributes (Font = ROMAN BOLD, Position = (-1500, 100), Character_Size = 700)

GMK Position = (290502N, 1281116E), Marker_Number = 122, Scale = 30, Orientation = -5, Text_String = "Fatanma," Character Attributes (Font = ROMAN BOLD, Position = (175, 0), Character_Size = 700)

OCID: 4011963

GMK Position = (281942N, 1273000E), Marker_Number = 122, Scale = 30, Orientation = -5, Text_String = "Kadena," Character Attributes (Font = ROMAN BOLD, Position = (-900, 300), Character_Size = 700)

GMK Position = (360103N, 1402213E), Marker_Number = 122, Scale = 30, Orientation = -5, Text_String = "Yokota," Character Attributes (Font = ROMAN BOLD, Position = (600, 100), Character_Size = 700)

GTX String = "Soya Strait," Position = (442020N, 1395216E), Character Attributes (Font = ITALICS, Character_Size = 200)

GTX String = "Kuril," Position = (450311N, 1452011E), Character Attributes (Character_Size = 800)

GTX String = "Islands," Position = (451016N, 1441022E), Character Attributes (Character_Size = 800)

GTX String = "U.S.S.R.," Position = (444517N, 1332037E), Character Attributes (Character_Size = 800)

GTX String = "CHINA," Position = (442002N, 1264712E), Character Attributes (Character_Size = 800)

GTX String = "Lake," Position = (441001N, 1323000E), Character Attributes (Font = ITALICS, Character_Size = 500)

GTX String = "Khanka," Position = (435716N, 1322511E), Character Attributes (Font = ITALICS, Character_Size = 500)

GTX String = "Hokkaido," Position = (434123N, 1403719E), Character Attributes (Character_Size = 800)

GTX String = "Tsugaru," Position = (413000N, 1382051E), Character Attributes (Font = ITALICS, Character_Size = 200)

GTX String = "Strait," Position = (411000N, 1383116E), Character Attributes (Font = ITALICS, Character_Size = 200)

GTX String = "Sea of Japan," Position = (400000N, 1331627E), Character Attributes (Font = ITALICS, Character_Size = 800)

GTX String = "NORTH," Position = (402632N, 1263023E), Character Attributes (Character_Size = 800)

GTX String = "KOREA," Position = (392518N, 1263023E), Character Attributes (Character_Size = 800)

GTX String = "Pacific," Position = (395756N, 1420106E), Character Attributes (Font = ITALICS, Character_Size = 800)

GTX String = "Ocean," Position = (384016N, 1370000E), Character Attributes (Font = ITALICS, Character_Size = 800)

GTX String = "JAPAN," Position = (384016N, 1370000E), Character Attributes (Font = ROMAN BOLD, Character_Size = 1200)

GTX String = "Demilitarized," Position = (383012N, 1290037E), Character Attributes (Font = ROMAN BOLD, Character_Size = 700)

GTX String = "Zone (DMZ)," Position = (380217N, 1290037E), Character Attributes (Font = ROMAN BOLD, Character_Size = 700)

GLN Endpoint[1] = (383012N, 1290000E), Endpoint[2] = (381612N, 1283000E), Width = 50

GTX String = "SOUTH," Position = (371024N, 1294500E), Character Attributes (Font = ROMAN BOLD, Character_Size = 1200)

GTX String = "KOREA," Position = (371024N, 1294500E), Character Attributes (Font = ROMAN BOLD, Character_Size = 1200)

GTX String = "Honshu, Position = (373012N, 1383026E), Character Attributes (Character_Size = 800)

GTX String = "Tsushima (Korea) Strait," Position = (333243N, 1262247E), Character Attributes (Font = ITALICS, Character_Size = 200, Character_Direction = (1, 1))

GTX String = "Cheju-do," Position = (244019N, 1335247E), Character Attributes (Character_Size = 700)

GTX String = "Shikoku," Position = (332143N, 1324237E), Character Attributes (Character_Size = 800)

GTX String = "Kyushu," Position =

OCID: 4011963

```
        (325947N, 1303017E), Character
        Attributes (Character_Size = 800)

GTX      String = "East," Position =
        (320627N, 1252742E), Character
        Attributes (Font = ITALICS,
        Character_Size = 800)

GTX      String = "China," Position =
        (313000N, 1251000E), Character
        Attributes (Font = ITALICS,
        Character_Size = 800)

GTX      String = "Sea," Position =
        (310941N, 1251000E), Character
        Attributes (Font = ITALICS,
        Character_Size = 800)

GTX      String = "RYUKYU," Position =
        (300000N, 1263047E), Character
        Attributes (Character_Size = 750)

GTX      String = "ISLANDS," Position =
        (294738N, 1263000E), Character
        Attributes (Character_Size = 750)

GTX      String = "Philippine," Position =
        (300000N, 1330000E), Character
        Attributes (Font = ITALICS,
        Character_Size = 800)

GTX      String = "Sea," Position =
        (293041N, 1341258E), Character
        Attributes (Font = ITALICS,
        Character_Size = 800)

GTX      String = "Bonin," Position =
        (295907N, 1413137E), Character
        Attributes (Character_Size = 700)

GTX      String = "Islands," Position =
        (294251N, 1410939E), Character
        Attributes (Character_Size = 700)

GTX      String = "Iwo," Position =
        (280944N, 1421033E), Character
        Attributes (Character_Size = 700)

GTX      String = "Jima," Position =
        (280000N, 1421033E), Character
        Attributes (Character_Size = 700)

BEG      Label = INSET1, Character Attri-
        butes (Font = ROMAN BOLD,
        Character_Size = 500)

VPT      Lower_left_Corner = (12739, 1024),
        Upper_right_Corner = (28221, 14327)

GTX      String = "Legend:," Position =
        (4096, 61440) Character Attributes
        (Font = ITALICS, Character_Size =
        300)

MRK      Position = (8192, 50462),
        Marker_Number = 122, Scale = 30,
        Orientation = 0, Text_String =
        "Airfield," Character Attributes
        (Position = (8000, 0))

MRK      Position = (8192, 43253),
        Marker_Number = 164, Scale = 30,
        Orientation = 0, Text_String =
        "Naval Facility," Character Attri-
        butes (Position = (8000, 0))

MRK      Position = (8192, 35389),
        Marker_Number = 39, Scale = 30,
        Orientation = 0, Text_String =
        "Army Command Headquarters," Char-
        acter Attributes (Position = (8000,
        0))

LIN      Endpoint[1] = (6000, 5400), End-
        point[2] = (50000, 5400)

TXT      String = "0," Position = (6000,
        6100), Character Attributes (Font =
        ROMAN, Character_Size = 175)

TXT      String = "0," Position = (6000,
        4800), Character Attributes (Font =
        ROMAN, Character_Size = 175)

TXT      String = "300 Kilometers," Posi-
        tion = (32768, 6100), Character
        Attributes (Font = ROMAN,
        Character_Size = 175)

TXT      String = "300 Miles," Position =
        (49000, 4700), Character Attributes
        (Font = ROMAN, Character_Size =
        175)

END      Label = INSET1

END      Label = EXAMPLE1, Checksum = ****
```

Example 2: Geographic HLDF with Arrows as Geo-Polygons (Shown in Figure 2)

(Size of this HLDF is 2,847 characters)

```
OP_CODE     ARGUMENT LIST

BEG      Label = EXAMPLE2, Line_Color =
        ((0, 0, 0), SOLID), Line_Style =
        SOLID, Line-Width = 50, Character
        Attributes (Font = ROMAN,
        Text_Color = (0, 0, 0),
        Character_Direction = (1,0),
        Character_Path = RIGHT,
        Character_Size = 700,
        Position_Precision = HIGH.
```

DOCID: 4011963

COM String = "BLACK AND WHITE GRAPHIC, HIGH PRECISION. UNCLASSIFIED"

CLA Major_Classification = NONE

VPT Lower_Left_Corner = (4000, 4000), Upper_Right_Corner = (61000, 44500)

MPC Center = (504900N,0100000E), Radius = 310, Projection = ORTHOGRAPHIC, Grid_Switch = OFF, Level_of_Detail = ROUGH, Altitude_Viewpoint = 1000

MAP (COASTLINES, SOLID), (INTERNATIONAL BOUNDARIES, DOT-DASH), (MAJOR ISLANDS, SOLID)

GTX String = "SCHLESWIG-," Position = (544026N, 0084512E)

GTX String = "HOLSTEIN," Position = (542216N, 0092000E)

GTX String = "EAST," Position = (534500N, 0123000E), Character Attributes (Character_Size = 1000)

Figure 2: Geography with Arrows

OCID: 4011963

GTX String = "GERMANY," Position = (533000N, 0104000E), Character Attributes (Character_Size = 1000)

GTX String = "WEST," Position = (484848N, 0104101E), Character Attributes (Character_Size = 1000)

GTX String = "GERMANY," Position = (482701N, 0091216E), Character Attributes (Character_Size = 1000)

GTX String = "NETHERLANDS," Position = (514200N, 0055500E), Character Attributes (Character_Direction = (1,2))

GTX String = "(NORTHAG)," Position = (511000N, 0064200E), Character Attributes (Character_Size = 1100)

GTX String = "(CENTAG)," Position = (492302N, 0072847E), Character Attributes (Character_Size = 1100)

GTX String = "BEL.," Position = (501500N, 0053616E), Character Attributes (Character_Direction = (3, 1))

GTX String = "LUX.," Position = (494218N, 0055732E)

GTX String = "CZECHOSLOVAKIA," Position = (493912N, 0120246E), Character Attributes (Character_Direction = (3, 1))

GTX String = "FRANCE," Position = (483606N, 0054232E), Character Attributes (Character_Direction = (2, 1))

GTX String = "SWITZERLAND," Position = (470319N, 0064500E)

GTX String = "AUSTRIA," Position = (470330N, 0105739E) Character Attributes (Character_Direction = (4, 1))

GMK Position = (534016N, 0083127E), Marker_Number = 16, Scale = 20, Orientation = 0, Text_String = "Bremerhaven," Character Attributes (Font = ITALICS, Position = (500, 0), Character_Size = 400)

GMK Position = (494201N, 0093522E), Marker_Number = 16, Scale = 20, Orientation = 0, Text_String = "Wurzburg," Character Attributes (Font = ITALICS, Position = (-5000, 100), Character_Size = 400)

GMK Position = (485226N, 0085814E), Marker_Number = 16, Scale = 20, Orientation = 0, Text_String = "Stuttgart," Character Attributes (Font = ITALICS, Position = (500, 0), Character_Size = 400)

GMK Position = (500214N, 0082237E), Marker_Number = 16, Scale = 20, Orientation = 0, Text_String = "Frankfurt," Character Attributes (Font = ITALICS, Position = (-5000, 0), Character_Size = 400)

GPL Number_of_Points = 9, Point[1] = (534016N, 0083127E), Point[2] = (533022N, 0083923E), Point[3] = (523000N, 0093410E), Point[4] = (515000N, 0093520E), Point[5] = (510400N, 0092214E), Point[6] = (513516N, 0092400E), Point[7] = (494201N, 0093522E), Point[8] = (492314N, 0090416E), Point[9] = (485226N, 0085814E), Line_Style = DOT-DASH, Width = 50

GTX String = "MAJOR LINE OF," Position = (533314N, 0083127E), Character Attributes (Character_Direction = (1, -1))

GTX String = "COMMUNICATION," Position = (532742N, 0082214E), Character Attributes (Character_Direction = (1, -1))

GMK Position = (524000N, 0123316E), Marker_Number = 23, Scale = 20, Orientation = 0, Text_String = "Berlin," Character Attributes (Font = ITALICS, Position = (500, 0), Character_Size = 400)

GMK Position = (504227N, 0070123E), Marker_Number = 23, Scale = 20, Orientation = 0, Text_String = "Bonn," Character Attributes (Font = ITALICS, Position = (300, 200), Character_Size = 400)

GTX String = "XXXX," Position = (520000N, 0081000E) Character Attributes (Character_Direction = (1, 1), Character_Size = 600)

GPL Number_of_Points = 7, Point[1] = (515842N, 0105847E), Point[2] = (512036N, 0090415E), Point[3] = (511627N, 0083057E), Point[4] = (510243N, 0081057E), Point[5] = (504000N, 0073000E), Point[6] = (503229N, 0070000E), Point[7] = (502234N, 0061000E), Width = 50

GPG Number_of_Points = 24, Point[1] =

DOCID: 4011963

```
(533742N, 0115103E), Point[2] =
(523758N, 0113000E), Point[3] =
(522903N, 0113000E), Point[4] =
(522000N, 0075537E), Point[5] =
(522600N, 0075426E), Point[6] =
(521000N, 0072800E), Point[7] =
(515800N, 0075530E), Point[8] =
(520008N, 0075530E), Point[9] =
(520900N, 0113428E), Point[10] =
(514000N, 0120000E), Point[11] =
(504216N, 0080937E), Point[12] =
(504937N, 0080812E), Point[13] =
(503000N, 0075116E), Point[14] =
(502616N, 0081422E), Point[15] =
(502811N, 0081152E), Point[16] =
(511923N, 0115211E), Point[17] =
(492437N, 0095723E), Point[18] =
(492540N, 0095103E), Point[19] =
(490023N, 0094728E), Point[20] =
(491316N, 0102347E), Point[21] =
(491522N, 0101833E), Point[22] =
(512000N, 0122116E), Point[23] =
(511826N, 0123142E), Point[24] =
(512631N, 0124106E), Width = 70

GTX     String = "NORTH GERMAN PLAIN,"
        Position = (520101N, 0075916E),
        Character Attributes
        (Character_Direction = (15,1), Font
        = ROMAN BOLD, Character_Size =
        1000)

GTX     String = "FULDA GAP," Position =
        (504223N, 0090400E), Character
        Attributes (Character_Direction =
        (4,1), Font = ROMAN BOLD,
        Character_Size = 1000)

GTX     String = "HOF CORRIDOR," Position
        = (493316N, 0103000E), Character
        Attributes (Character_Direction =
        (1,2), Font = ROMAN BOLD,
        Character_Size = 1000)

END     Label = EXAMPLE2, Checksum = ****
```

References

[1] Graphic Standards Planning Committee, "Status Report of the Graphic Standards Planning Committee," Computer Graphics, Volume 13, Number 3, August 1979 (Special Issue).

[2] International Standards Organization, Information Processing Graphics Kernel System (GKS), Draft International Standards Organization Standard (ISO/DIS) (ISO TC97/SC5/WG2 N117) (ANSI X3H3/82-10), 14 January 1982.

[3] Tektronix, Graphic Model Exchange Format Functional Description, GCS Software Standard, 5 November 1980.

[4] Enderle, G., I. Giese, M. Krause, and H. P. Meinzer, "The AGF Plotfile towards a Standardization for Storage and Transportation of Graphics Information," Computer Graphics, Volume 12, Number 4, (December 1978), pp. 92-113.

[5] Warner, Jim, "Device-Independent Intermediate Display Files," Computer Graphics, Volume 13, Number 1, (March 1979), pp. 78-109.

[6] Teus Hagen, Paul J. W. Ten Hagen, Paul Klint, and Hans Noot, "The Intermediate Language for Pictures," Information Processing 77, (B. Gilchrist, Ed.) International Federation for Information Processing and North-Holland Publishing Company, The Hague, (1977), pp. 173-178.

[7] National Security Agency, BETA--A Cryptologically Oriented Advanced Programming Language, May 1970, S-196,383.

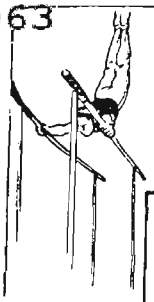
[8] Mead, Carver, and Lynn Conway, Introduction to VLSI Systems, Addison-Wesley, New York, 1980, pp. 115-127.

[9] Cohen, Danny, A Proposed End/End Check-Sum Option for CIF Files, USC/ISI Unpublished manuscript, 28 April 1978

[10] Collins, John M., U.S.--Soviet Military Balance--Concepts and Capabilities 1960-1980, (New York: McGraw-Hill, 1980).

[11] American National Standards Institute Committee on Computer Graphics Languages (ANSI X3H3), American National Standard Functional Specification of the Programmers's Minimal Interface to Graphics, Working Document ANSI X3H3 / 82-15, 19 February 1982.

OCID: 4011963



A SURVEY OF PARALLEL SORTING (U)

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

by [redacted] E4

Donald Knuth [6] says that computer manufacturers estimate that over 25 percent of the running time on their computers is devoted to sorting when all customers are taken into account. No one in the Agency is as willing to estimate the amount of sorting that we do, though informal estimates put our sorting use at about five percent. This paper will review several parallel sorting algorithms, particularly in the context of sorting very large files.

~~(C)~~
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

[redacted]

(U) Thus our file of tapes functions as a massive random access memory. To locate a data item, we first must determine the tape it is in, and then run through the tape to the desired word. Even with the efficiency gained by sorting the tapes, access in this data base is a lengthy process. The access time includes the mounting of the tape and the time to run through (on the average) half of the tape--about two minutes total.

[redacted]

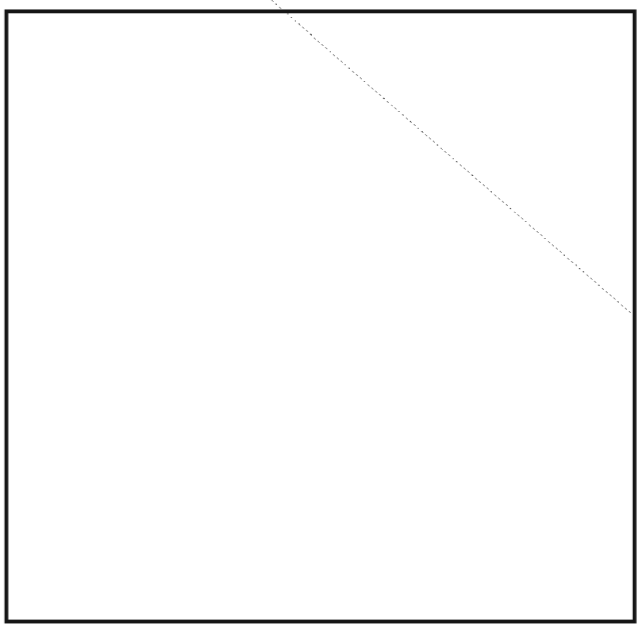
[redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~

DOCID: 4011963 EO 1.4.(c) P.L. 86-36



~~(S-CCO)~~ Some cryptanalytic programs on our various computer systems are limited as to the amount of data they can handle. By presorting the data into pockets, we can produce small data sets that can be handled by the programs. The remaining data can then be used for secondary testing.

(U) Generally speaking, sorting N words requires O(N log N) word comparisons. On a standard serial computer, log N passes over the N data items usually produces a sorted list. Parallel processing enables us to make some comparisons simultaneously. The parallel algorithms discussed below can decrease the running time from about N log N to $\log^2 N$ or log N, but at the expense of making a larger total number of comparisons.

(U) Note that throughout this paper we use log N to stand for the base 2 logarithm of N. Thus log 32 = 5.

PARALLEL ALGORITHMS

(U) The acronym SIMD stands for single instruction stream multiple data stream. An SIMD array processor is well suited to take advantage of parallelism in many algorithms. Both ILLIAC IV and Staran are SIMD machines and this is the type of parallel processor most seriously considered for construction. If array processors become commercially available, they will probably be of the SIMD design. For this reason, it is important to study and understand algorithms for various interconnection networks in SIMD array processors.

(U) An SIMD machine usually has a central controller, N processors, N memories, and an interconnection network. The central controller issues a single instruction to all processors which in turn operate on their memories (multiple data) as required. A mask register permits certain processors to be inactive during an instruction, but only one operation is performed at one time by each active processor. The interconnection network allows the processors to communicate with each other. In general, each processor is connected to between O(1) and O(log N) other processors.

HIRSHBERG'S BUCKET SORT ALGORITHM

(U) D.S. Hirshberg of Rice University has developed a parallel sorting algorithm for SIMD machines [4] which requires time O(log N). His SIMD model assumes that there is a common memory which can be accessed by all processors. Simultaneous access to a memory location is not allowed for stores, but may be allowed for fetches.

(U) Hirshberg's algorithm is a parallel version of the "bucket sort."[7] Assume that the numbers to be sorted C_i, are from 0, ..., M-1 where $M \leq N$. In the common memory there is a "bucket" devoted to each processor. If there are no repetitions among the C_i, and if each processor p_i (which has been temporarily assigned to C_i, the ith number to be sorted) places the value i in bucket B_j, where $j = C_i$, then bucket i contains the address of the jth sorted word. An example of this for N = 8 is given in Figure 1.

i	C_i	B_i
0	3	1
1	0	5
2	6	3
3	2	0
4	7	7
5	1	6
6	5	2
7	4	4

Figure 1

(U) In general, there may be repetitions in the C_i's, and this could cause store conflicts if more than one processor tried to write to its address in a bucket. We can avoid this by assigning N locations per bucket so that each processor has a unique place in each bucket to make conflict-free marks (only a mark, not the processor number i, is now written.) An example of this is shown in figure 2, where N = 16 and $0 \leq C_i \leq 11$. Consider specifically the case of bucket 1. Processors 5, 8, 9, and 15

~~SECRET SPOKE~~

DOCID: 4011963

have made their marks in their respective portions of the bucket.

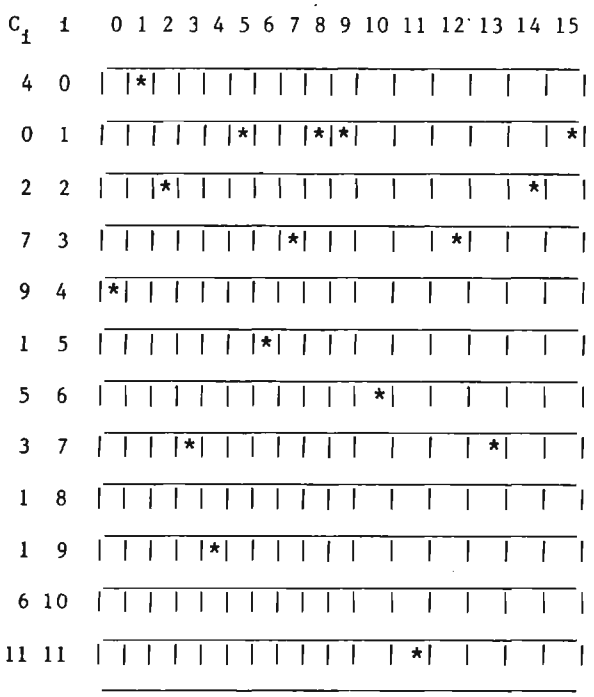
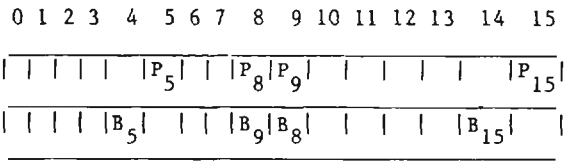


Figure 2

(U) If each bucket comprises one memory location, we must avoid multiple accesses to a bucket. We need a technique to allow processors to "sense" the presence of other processors in the bucket and deactivate themselves if necessary, leaving one active processor in each bucket.

(U) We will use the "buddy system," analogous to the buddy system for dynamic memory allocation.[6] If $\oplus$ represents bit-by-bit mod 2 addition, and processor i is marking location j, then the kth buddy of processor i is $j \oplus 2^k$. Each processor determines whether its buddy is active within the same location. If so, then the processor with higher rank (numerical value) will deactivate. If the buddy is not active, or if the buddy is of higher rank than the location the processor is marking, the processor continues. The processor shifts its mark to the smaller of its mark and that of its buddy. After log N iterations, only one processor remains active in each bucket. This process is illustrated below.

Bucket 1

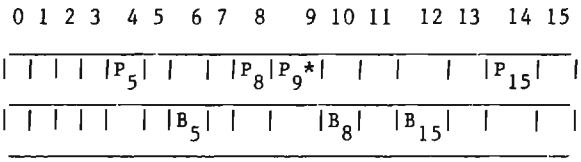


k = 0

Figure 3

(U) Figure 3 shows bucket 1 and the locations marked by the active processors (all four are active initially). The locations of each processor's 0th buddy is also marked. Processors 5 and 15 check the location of their buddies, and find no processor has that location marked. Because their buddies are smaller than the locations they are marking, they will move their marks to their buddies' locations. Processors 8 and 9 check their buddies' locations and simultaneously discover that they are both active. Processor 9, being of higher rank than processor 8, will deactivate. Because the 0th buddy of processor 8 is larger than the location marked by processor 8, processor 8 will not move its marker.

Bucket 1



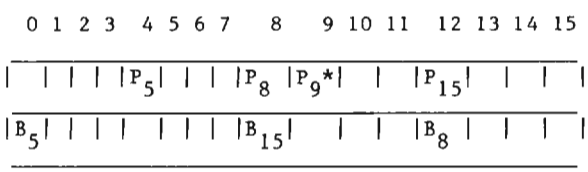
k = 1

Figure 4

(U) Figure 4 shows processor 9 deactivated (though it continues to mark its last active location) and the markers of processors 5 and 15 moved to their new, lower locations. Each remaining active processor finds no mark in the location of its first buddy, so each remains active. Processors 5 and 8 do not move their markers because their buddies are at locations higher than their markers. Processor 15 moves its marker because its first buddy is in a location lower than its marker.

OCID: 4011963

Bucket 1

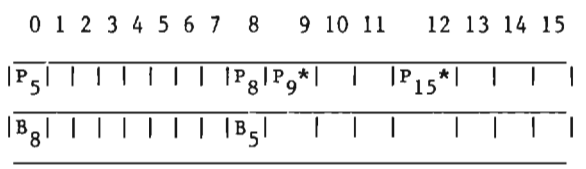


k = 2

Figure 5

(U) Figure 5 shows the locations of the second buddies. Processors 8 and 15 detect each other's presence simultaneously, and processor 15 deactivates. Processor 5 moves its marker to the location of its second buddy.

Bucket 1



k = 3

Figure 6

(U) Finally, in Figure 6, the third buddies of processors 5 and 8 detect each other, processor 8 deactivates and processor 5 is left as the only active processor in bucket 1 with its marker in location 0. In general, the lowest ranked processor will remain active in each occupied bucket, with its marker at location 0.

(U) This algorithm sorts the list in O(log N) steps, but discards duplicates from the list. A modification of this algorithm will enable us to sort in O(log N) and keep the duplicates. Each processor keeps a running count of the number of processors greater than or equal to itself that are active in the bucket. Figure 7 illustrates this procedure within bucket 1, using a modified buddy system.

(U) The modified buddy system is much like the system described earlier. Whenever a processor's buddy detects an active processor of lower rank, the higher ranked processor deactivates (that is, it does not move its mark). However, its buddy assumes the value of the lower ranked processor's buddy, and the value of the buddy of any lower ranked processor it subsequently detects. Whenever a processor's buddy detects a processor of higher rank, it adds that processor's count to its count. Note that a processor can be detected by several processors simultaneously because we allow multiple fetches.

(U) At the end of log n steps, location 0 of each bucket contains the marker of the lowest ranked processor active in that bucket. The market will be equal to the number of processors in the bucket. Also in the bucket, at various locations, will be the markers of the other processors, each equal to the number of processors ranked greater than or equal to the processor.

(U) Algorithm 1.1 formally expresses these ideas. In the algorithm, we use the notation that x<k> is the kth binary digit of x (note that we have digits 0 through $\log_2 N-1$), $\oplus$ represents bit by bit mod 2 addition, and e_k is the $\log_2 N$ digit number with a single 1 in the kth place.

Algorithm 1.1 - Parallel Bucket Sort

(N numbers, range $M \leq N$)

Input: $A[j,i] = 0$ $\quad 0 \leq i \leq N-1$, $0 \leq j \leq M-1$

C_i $\quad 0 \leq C_i \leq M-1$

(the numbers to be sorted)

```
Concurrently for all i do
  mark_i <- i
  point_i <- i
  A[C_i, mark_i] <- i
  flag_i <- 1
for k <- 0 step 1 until (log2N-1) do
  buddy_i <- point_i ⊕ e_k
  if point_i<k> = 0 then
    A[C_i,mark_i] <- A[C_i,mark_i] + A[C_i,buddy_i]
  else if point_i<k> = 1 then
    point_i <- buddy_i
    if A[C_i,buddy_i] = 0 then
      if flag_i = 1 then
        A[C_i, buddy_i] <- A[C_i, mark_i]
        A[C_i, mark_i] <- 0
        mark_i <- buddy_i
      end (if flag_i = 1)
    else if A[C_i, buddy_i] ≠ 0 then
      flag_i <- 0
    end (if A[C_i, buddy_i] ≠ 0)
    end (else point_i<k> = 1)
end (for k loop)
end (Algorithm 1.1)
```

(U) We now have completed the first part of our algorithm and know how many elements are in each bucket. We next want a cumulative total so that bucket i contains the number of terms less than or equal to i. This is accomplished by transferring the data in A[j,0] to B[j] and totaling B[j]. Then with D[i] <- $B[C_i]$ - $A[C_i, mark_i]$, D[i] has the location

CID: 4011963

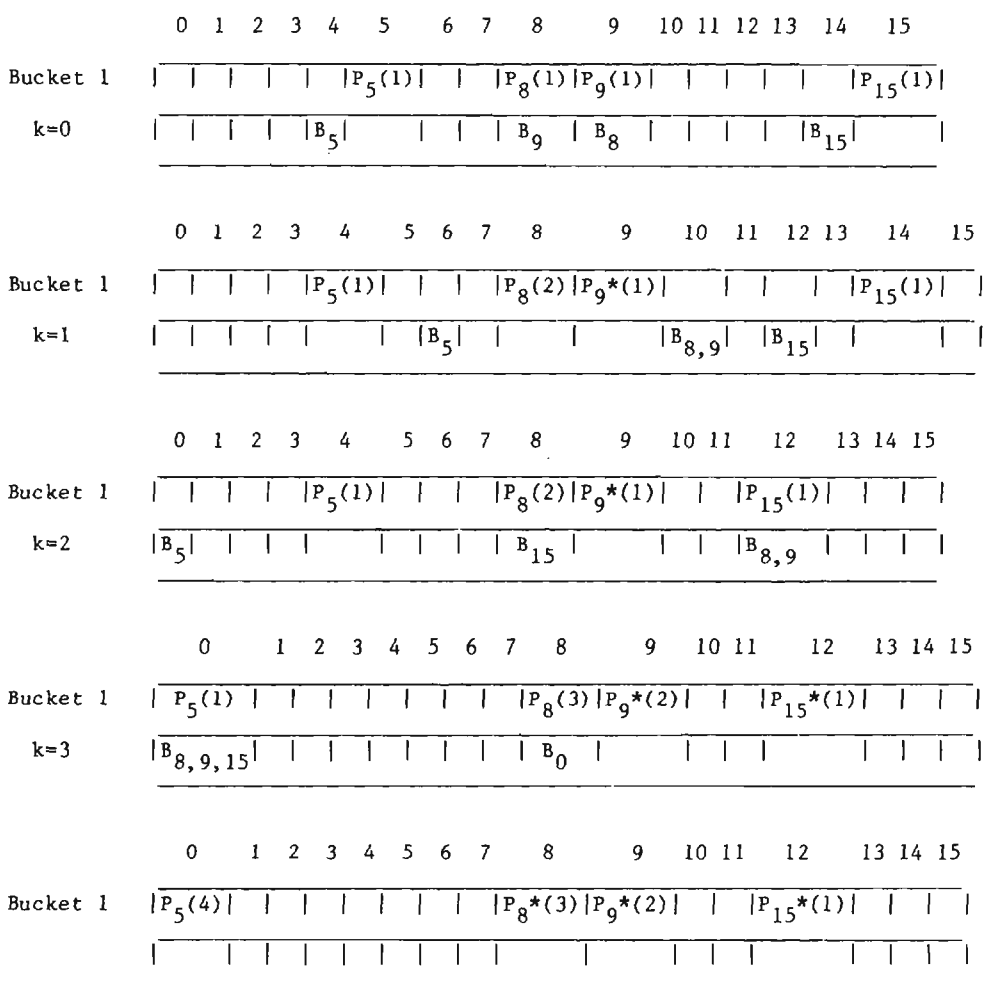


Figure 7

DOCID: 4011963

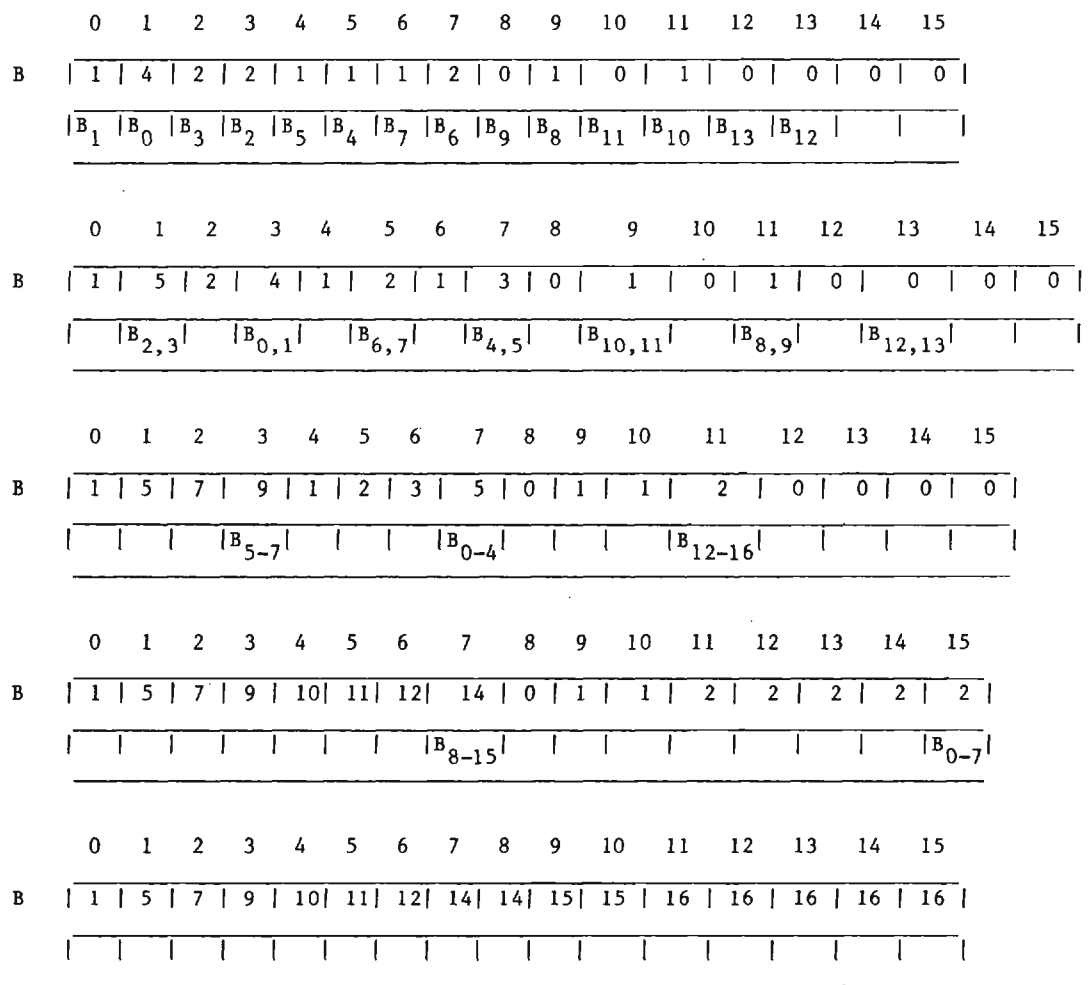


Figure 8

OCID: 4011963

(in an N-long sorted list) which contains the first value i.

(U) Figure 8 shows the various steps of producing the cumulative total. Note again that we allow multiple fetches from the same memory location. The cells in Figure 8 represent B[0] through B[15], and are a continuation of the example begun in Figure 7.

(U) To conclude this algorithm, note what happens in bucket 1. Processors 5, 8, 9, and 15 have totals of 4, 3, 2, and 1 respectively. With only one element in bucket 0, C_5, which equals 1 and is assigned to processor 5, has final position $B[C_5] - A[C_5, mark_5] = B[1] - A[1,0] = 5 - 4 = 1$. Similarly, C_8, C_9, and C_5 have final positions 2, 3, and 4.

(U) Algorithm 1.2 concludes Hirshberg's parallel bucket sort.

```
Algorithm 1.2 - Parallel Bucket Sort
Input: from Algorithm 1.1
  B[i] = 0        0 ≤ i ≤ N-1
  D[i] = 0        0 ≤ i ≤ N-1

Concurrently for all i do
  B[i] <- A[i,0],   0 ≤ i ≤ M-1
  point_i <- i
  for k <- 1 step 1 until log N do
    buddy_i <- point_i ⊕ e_k
    If point_i <k> = 0 then
      point_i <- buddy_i
    else point_i <k> = 1 then
      B[i] <- B[i] + B[buddy_i]
    end (if point_i <k> = 1)
  end (for k loop)
  D[C_i] <- B[C_i] - A[C_i, mark_i]
end (Algorithm 1.2)
```

(U) The algorithm produces D = (0, 1, 5, 7, 9, 10, 11, 12, 0, 14, 0, 15, 0, 0, 0, 0) from the initial data C = (4, 0, 2, 7, 9, 1, 5, 3, 1, 1, 6, 11, 3, 7, 2, 1), M = 12, N = 16.

VALIANT'S FAST MERGING ALGORITHM

(U) Leslie Valiant at the University of Leeds has developed a fast merging algorithm for SIMD machines [2] which in turn leads to a fast sorting algorithm. The merging algorithm is somewhat dissatisfying because of the vagueness of the data rearrangement techniques. To merge two lists of length M and $N \leq M$, Valiant requires $\sqrt{NM}$ processors and O(log log N) time and to sort he requires O(log N · log log n) time. His SIMD model requires either that each processor has access to a common memory or that the processors have a sufficiently robust interconnection to permit necessary data routing.

(U) To see that Valiant's merging algorithm requires time O(log log N), we shall proceed recursively. We will reduce the problem of merging two lists of length N and M to that of merging $\sqrt{N}$ lists of length $\sqrt{N}$ and, at most, $2\sqrt{M}$.

(U) Let $X = (x_1, x_2, \ldots, x_N)$ and $Y = (y_1, y_2, \ldots, y_M)$ be the two sorted lists we want to merge with $1 \leq N \leq M$. First, mark the elements of X that are subscripted by $i\sqrt{N}$ and those of Y that are subscripted by $i\sqrt{M}$, for $i = 1, 2, \ldots$.

(U) Then compare each marked element of X with each marked element of Y. This will require at most $\sqrt{MN}$ comparisons, and can be done in unit time with $\sqrt{MN}$ processors. We now can pinpoint the segment between marked elements of Y into which each marked element of X must be inserted. Now, compare each marked element of X with every element in the segment Y into which it must be inserted. As each segment of Y has $\sqrt{M}$ elements, at most $\sqrt{MN}$ comparisons are needed, and these can be done in unit time.

(U) After these comparisons, we know exactly where each marked element of X should be inserted into Y. X is subdivided into $\sqrt{N}$ segments of length $\sqrt{N}$, X_i, between the marked elements of X; and Y is subdivided into $\sqrt{N}$ segments, Y_i, between the $\sqrt{N}$ inserted elements of X. Further, we know which segments of X and Y must be merged.

(U) Before we can recursively use our algorithm to merge the disjoint segments $|X_i|$ and $|Y_i|$ we must determine if we have enough processors. We will need $\sqrt{|X_i|+|Y_i|}$ processors to merge each pair (X_i, Y_i). Now, we clearly have $\Sigma|X_i| \leq N$ and $\Sigma|Y_i| \leq M$, so by Cauchy's inequality,

$$\Sigma \sqrt{|X_i| \times |Y_i|} \leq \Sigma \sqrt{|X_i| \cdot |Y_i|} \leq \sqrt{MN}.$$

Thus we have enough processors to handle merging each pair of disjoint segments.

(U) In two time units we have reduced the problem from merging two lists of size M and N to that of merging several pairs of size $\sqrt{N}$ and at most $2\sqrt{M}$. Our cutdown varies on the larger of the two lists but is quite regular on the smaller: from $2^{\log N}$ to $2^{(\log N)/2}$ to $2^{(\log N)/4}$ and so on. The merging is finished when we have reduced the problem to merging several lists of length 1 with other larger

OCID: 4011963

lists, and this requires about 2 log log N = O(log log N) time units.

(U) A few comments on Valiant's merging algorithm are in order here before proceeding. Our estimations of timing have allowed for one comparison to be made per unit time. We have not directly addressed the time needed to determine the insertion location nor the time needed for assigning data to processors. While both of these operations may be able to be done in a constant amount of time, the time required could still be overwhelming. Further, the requirement of $\sqrt{MN}$ processors is itself somewhat staggering. Finally, each processor must have some sort of broadcast capabilities to allow a word to be simultaneously compared with several other words (which might be handled by memory access capability). However, Valiant's techniques are nevertheless worth considering, if only for their elegance.

(U) This merging technique can easily be adapted to a sorting algorithm. Consider the problem of sorting $N = 2^n$ words with 2^{n-1} processors. At time i we have 2^{n-1} sorted lists of length 2^i. We can merge 2^{n-i-1} pairs of these lists by assigning 2^i processors to each pair. At stage i, the time for merging is about 2 log log 2^i = 2 log i. Thus the total time for sorting the N words is about

$$\sum_{i=1}^{\log N} 2 \log i \le \sum_{i=1}^{\log N} 2 \log \log N = 2 \log N \cdot \log \log N = O(\log N \cdot \log \log N).$$

PREPARATA'S ALGORITHM

(U) Franco Preparata at the University of Illinois used Valiant's fast merging to design a parallel sorting algorithm for SIMD machines.[14] Recall that Valiant required 2^{n-1} processors to sort $N = s^n$ words in O(log N · log log N) time. Preparata uses N log N processors to sort in O(log n) time. Note that with $\sqrt{N}$·log n times more processors, he was able to reduce the time by a factor of only log log n.

(U) Preparata's algorithm, as well as Hirshberg's, are examples of what Knuth [7] terms "enumeration sorting." In these methods, each word is compared with all others, and the number of smaller keys determines the word's final position. In this instance, we will merge two sorted lists to count the number of terms less than a given word. As an example, consider two sorted lists, X and Y, and consider the word in X in position i, x. After merging X and Y with a stable merge algorithm to produce Z, X is now in position q; that is, $z_q = x$. This means that there must be q - i words in Y that are less than or equal to x.

(U) Preparata's algorithm proceeds as follows: Let $N = 2^n$ and let $A = \{a_i | i=0,\ldots,N-1\}$ be our list to be sorted. We assume that for fewer than N words, at most $N \log^2 N = n2^n$ processors are needed to implement the sort, and we will use induction to prove it for N. Divide A into n subarrays, each of size N/n, $A_0, A_1, \ldots, A_{n-1}$, and recursively call on the sort algorithm to sort the subarray. By the inductive hypothesis, each subarray requires at most (N/n) log (N/n) processors to be sorted. With n subarrays, the total number of processors needed to sort the subarrays is

$$\begin{aligned} n(N/n) \log (N/n) &= N \log (N/n) \\ &= N \log N - N \log \log N \\ &\le N \log N . \end{aligned}$$

If it requires T(k) time to sort K words, then this step requires T(N/n) time. Associated with the lth word of the sorted subarray A_i is the label (i,l).

(U) Next, we copy our sorted subarrays A_i into longer arrays: $S_{i,j} = A_i, A_j$ for i<j. Note that there are (n/2)(n-1) arrays $S_{i,j}$ and each requires 2N/n words (including their labels). If we assign one processor to each word to be written into $S_{i,j}$, we will need $(n/2)(n-1)(2N/n) < N \log_2 N$ processors. This copying can be done in one time unit and will require simultaneous fetches of some words (for example, A_i is copied into N - 1 arrays).

(U) We now use Valiant's technique to merge each $S_{i,j}$. This will require $\sqrt{N/n \cdot N/n} = N/n$ processors for the $(n/2)(n-1)S_{i,j}$, or a total of $(n/2)(n-1)(N/n) < N \log_2 N$ processors. The time required is O(log log (N/n))

(U) An array R[i;j;k] $0 \le i,j < n$, $0 \le k$ N/n is set up to hold the count information of each word, prior to the final rank computation. R[i;j;k] will equal the number of words in A_j that are less than or equal to the kth word of A_i.

(U) The R[i;j;k] are determined as follows. Let (x,ℓ) be the label associated with the word in the qth position of $S_{i,j}$, $S_{i,j}[q]$. (Recall that (x,ℓ) is associated with the ℓth word of A_x, so x = i or x = j.) If x = i, then $R[i;j;\ell] = q - \ell$ or if x = j, then $R[j;i;\ell] = q - \ell$, and $R[x;x;\ell] = \ell$. There are

OCID: 4011963

$n \cdot n \cdot N/n = N \log_2 N$ words to be copied into R, and, as before, we use one processor per word to accomplish the copying in one time unit.

(U) Now to determine final rank of $A_i[\ell]$, we must sum up the number of words less than or equal to $A_i[\ell]$ in all other subarrays.

Thus,

$$\text{rank}\,(A_i[\ell]) = \sum_{j=0}^{n} R[i;j;\ell],$$

and this computation requires n/2 processors for each $A_i[\ell]$ (compare this with the buddy method in Hirshberg's Parallel Bucket Sort) and log log n time. The total number of processors used here is N log N. Finally, we complete our work by

$$A[\text{rank}(A_i[\ell])] = A_i[\ell].$$

(U) To conclude our analysis, note that none of the steps used more than N log N processors. The time required to sort N words, T(N), is: T(N/log N) to sort the subarrays A_i; one time unit to copy A_i and A_j into $S_{1,j}$; O(log log (N/n)) < O(log log n) time for merging the $S_{i,j}$; one time unit to copy partial data into R; log log N time to compute rank $(A_i[1])$; and one time unit to make the final rearrangement. Thus

$$T(N) \cong T(N/\log N) + C_1 \log\log N + C_2,$$

and solving this recurrence, we have

$$T(N) = O(\log N).$$

Thus, Preparata using an SIMD model similar to Valiant's model is able to sort in time O(log N) as compared to O(log N log log N). However this faster method uses N log N processors, and it also requires a considerable amount (2 N log N) of extra storage to keep up with the various arrays.

(U) Preparata in [14] also presents a generalized version of the preceding algorithm. This generalized algorithm avoids memory fetch conflicts, and uses $N^{1+\alpha}$ processors to sort in time $(1/\alpha)$ C log N + O(log N), for $0 < \alpha \leq 1$ and C a constant. However, as elegant as this result may be, or that of Hirshberg or Valiant, they all presuppose a multiple-access memory, and this is not a likely or sound basis for design. Even with the elimination of fetch conflicts, this memory design is not likely to be seen in the near future. These three algorithms fall in the class of the theoretically important but practically unworkable.

MESH-CONNECTED COMPUTERS

(U) A more practical avenue of research is to consider an SIMD model where each processor has its own memory and can communicate directly with other processors with which it is connected. This fixed interconnection network in turn becomes the dominant factor to be considered in the design of efficient algorithms.

THOMPSON AND KUNG'S ALGORITHM

(U) Thompson and Kung [21], and after them Nassimi and Sahni [12], have produced algorithms for a mesh-connected computer. The ILLIAC IV computer is an 8 x 8 example of this type of architecture. Figure 9 shows the two-dimensional array of processors, each denoted by P, and their interconnections. The processors are placed in a square array and each one is connected to all of its neighbors. Processors at the perimeter have two or three rather than four neighbors--there are no "wrap-around" connections, as found on the ILLIAC IV.

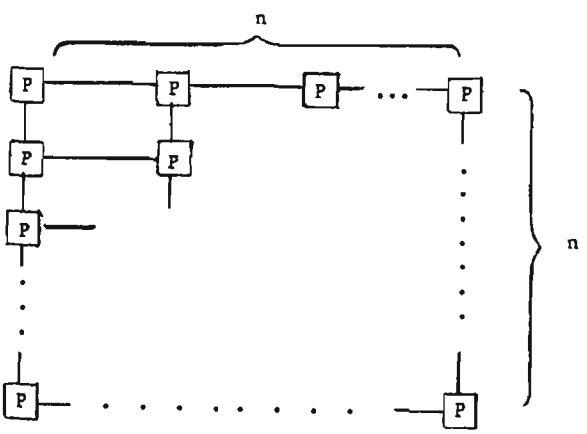


Figure 9.

(U) Before describing the algorithm, it will be necessary to decide upon an indexing scheme. Such a scheme is dependent upon how the sorted words will be used and upon the algorithm chosen. Figure 10 shows two indexing methods: row-major and snake-like row major. While in general in an SIMD machine every processor executes the same instruction or transmits data in the same direction, it would not be difficult to allow one special

DOCID: 4011963

0 1 2 3	0 1 2 3
4 5 6 7	7 6 5 4
8 9 10 11	8 9 10 11
12 13 14 15	15 14 13 12
Row-major indexing	Snake-like row-major indexing

Figure 10

instruction that permits data to be transmitted along some fixed path, such as the snake-like row-major indexing. Thompson and Kung use the snake-like row-major indexing for their sort and Nassimi and Sahni use row-major indexing for their scheme.

(U) In our mesh-connected SIMD model, we shall define t_r to be the time required to route data one unit distance in any direction, and t_c to be the time to perform the comparison of two words within one processor. Any number of simultaneous data moves can be made in any one direction at one time, and any number of simultaneous comparisons can be made at one time. Thus a comparison-exchange step between two items in horizontally adjacent processors can be done in time $2t_r + t_c$ (route left, compare, route right).

(U) Regardless of the algorithm selected for our model, it is possible to get an absolute lower bound on the time. For any indexing scheme, there are situations where it will be necessary to exchange the words in opposite corners of the processor array. For this movement, shown in Figure 11, 2(n-1) routing steps are needed to move a up and to the right, and 2(n-1) routing steps are needed to move b down and to the left. Thus, at least 4(n-1) routing steps are needed. For this model then, no algorithm can sort n^2 words in time less than O(n).

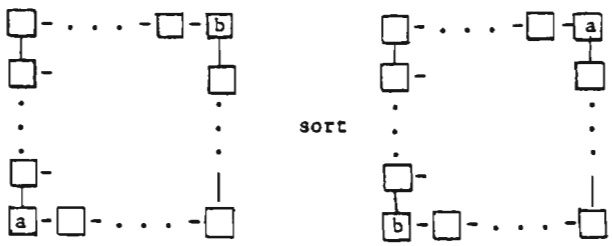


Figure 11.

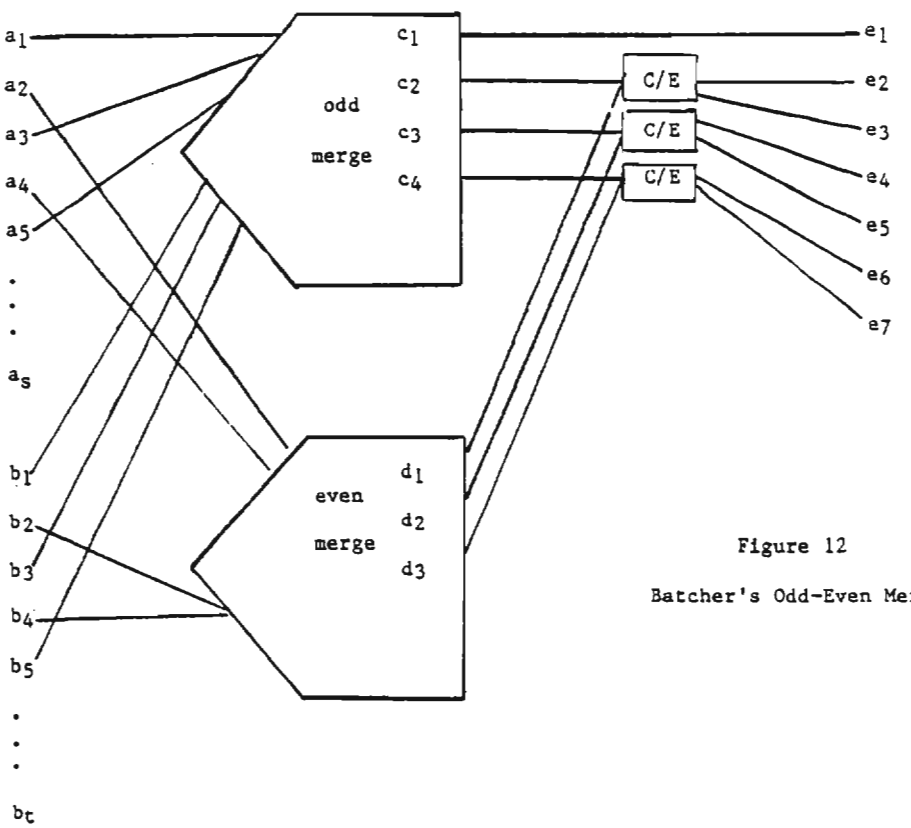


Figure 12

Batcher's Odd-Even Merge

DOCID: 4011963

ODD-EVEN TRANSPOSITION SORT

(U) Before proceeding with a description of the Thompson-Kung algorithm, we must discuss two other algorithms: the odd-even transposition sort and the Batcher odd-even merge. The odd-even transposition sort is described in Knuth [7] and is a straightforward, if slow, sort. To sort N words, the first step is to compare words 2i, and 2i+1, for $0 \leq i \leq N/2$, and exchange (or transpose) them if needed so that the larger is now in position 2i+1. Then for the second step, compare 2i-1 and 2i and exchange them so that the larger is in position 2i. After alternating N/2 of step 1 with N/2 of step 2, the words will be sorted, with the smallest in position 0.

(U) With this algorithm, it does not matter if we start with step 1 or step 2, as long as they alternate. When N is odd the beginning step will be executed once more than the second step. The algorithm requires $N^2/2$ comparison exchanges. Because both steps 1 and 2 compare disjoint pairs of elements, N/2 processors in parallel could execute the algorithm in O(N) time.

BATCHER'S ODD-EVEN MERGE

(U) The Batcher odd-even merge [1, 7] is a technique for merging two sorted lists (of possibly different lengths). The two lists are "unshuffled" so that all the odd terms are together, as are the even terms. The odd terms and the even terms are merged (by a recursive call to the odd-even merge), the two merged lists are shuffled together, and a final step of N/2 - 1 comparison-exchanges completes the merge. Figure 12 illustrates Batcher's merge.

(U) The Thompson-Kung algorithm [21] assumes that for our N x N mesh-connected computer, N is a power of 2. We first consider an odd-even transposition sort on a j x k subarray, were both j and k are powers of 2, and the processors are indexed by a snake-like row-major order. As discussed earlier, the time required for a comparison-exchange on a pair of words (or several similarly oriented pairs) is $2t_r + t_c$.

(U) Let $T_{oe}(j.k)$ be the time required for an odd-even transposition sort on a j x k subarray. If j = 1 or k = 1, then our model reduces to a linearly connected SIMD machine and $T_{oe}(j,k) = jk(2t_r + t_c)$. If k = 2, the step 1 comparison-exchanges are all made horizontally and the step 2 comparison-exchanges are all made vertically, and $T_{oe}(j,k) = jk(2t_r + t_c)$. These cases are illustrated in Figure 13, with an arrow indicating a comparison-exchange.

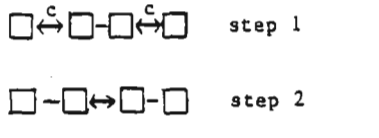
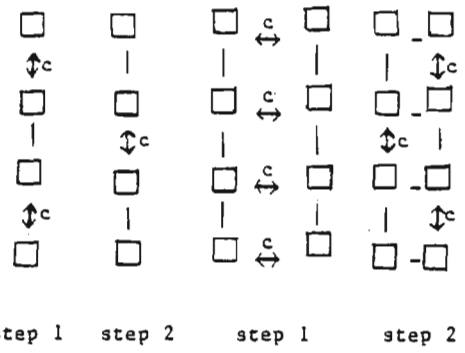


Figure 13



(U) In the case where j > 1 and k > 2 the times for steps 1 and 2 become different. Step 1 still requires $2t_r + t_c$ time because all of its comparison-exchanges are made horizontally; however, step 2 now requires $4t_r + t_c$ time, because some of its comparison-exchanges are made horizontally and some vertically. (Recall that data movements must all be in the same directions. Thus, for step 2 we perform: route left, route up, compare, route right, route down.) Thus for j > 1, k > 2

$$T_{oe}(j,k)=1/2jk[(2t_r+t_c)+(4t_r+t_c)]=jk(3t_r+t_c).$$

This is illustrated in Figure 14 for j = k = 4.

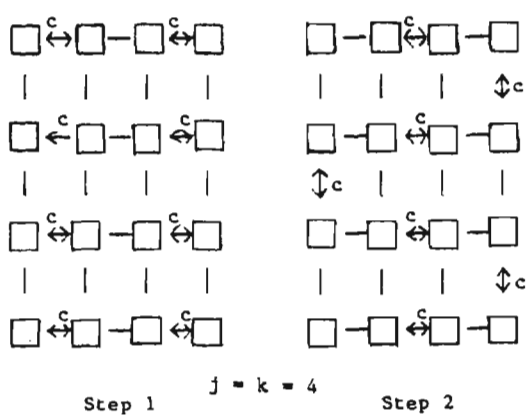


Figure 14

DOCID: 4011963

(U) By these timing arguments, our initial array of $N = n^2$ words could be sorted with N processors by the odd-even transposition sort in time $N(3t_r + t_c)$. We will now describe a variation of Batcher's odd-even algorithm for merging two j x k/2 sorted arrays to produce a j x k sorted array. This will lead to a divide-sort-merge strategy that will sort in $O(\sqrt{N} \log \sqrt{N})$ rather than $O(N)$. First note that the two halves of a 1 x k can be shuffled (or unshuffled) in time $(k-2)t_r$. This is illustrated in Figure 15. The case for merging two j x 1 lists will be treated separately.

a - a - a - a<->b - b - b - b

a - a - a<->b - a<->b - b - b

a - a<->b - a<->b - a<->b - b

a - b - a - b - a - b - a - b

Figure 15

Algorithm 2.1: Thompson-Kung j x 1 Parallel Merge (M(j,2))

Input: Two adjacent j x 1 sorted arrays in a mesh-connected computer

M_1 - Move all even terms from the right column to the left column, and all odd terms from the left column to the right column. (This "unshuffles" the terms.)
Time: $2t_r$

M_2 - Sort each column with an odd-even transposition sort.
Time: $j(2t_r + t_c)$

M_3 - Interchange on odd rows. (This "shuffles" the terms back together.)
Time: $2t_r$

M_4 - Compare-exchange words 2i - 1 and 2i of the j x 2 array.
Time: $2t_r + t_c$.

Figure 16 illustrates M(4,2). The merge M(j,2) takes time $T(j,2) = (2j + 6)t_r + (j + 1)t_c$.

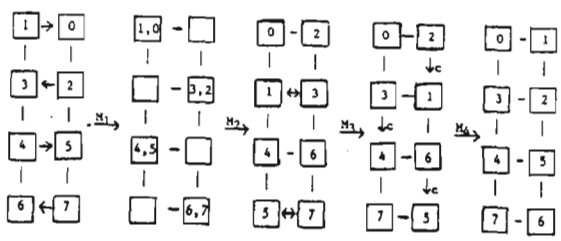


Figure 16.

Algorithm 2.2: Thompson-Kung j x k Parallel Merge (M(j,k))

Input: Two adjacent j x k/2 arrays in a mesh-connected computer, each sorted in snake-like row-major order.

M_1 - Interchange words 2i and 2i+1 on odd rows so that each column contains either all evens or all odds.
Time: $2t_r$

M_2 - Unshuffle each row so that the first quarter of the columns are now the odd columns from the first half of the columns.
Time: $(k-2)t_r$

M_3 - Merge each half with M(j,k/2).
Time: T(j,k/2)

M_4 - Shuffle each row.
Time: $(k-2)t_r$

M_5 - Interchange words 2i and 2i+1 on odd rows.
Time: $2t_r$

M_6 - Compare-exchange words 2i+1 and 2i.
Time: $4t_r+t_c$.

Figure 17 illustrates M(4,4).

```
 2 -  4 -  0 -  1
 |    |    |    |
 8<-> 5 -  6<-> 3   M1
 |    |    |    |
10 - 13 -  7 -  9
 |    |    |    |
15<->14 - 12<->11
```

```
 2 -  4<-> 0 -  1
 |    |    |    |
 5 -  8<-> 3 -  6   M2
 |    |    |    |
10 - 13<-> 7 -  9
 |    |    |    |
14 - 15<->11 - 12
```

```
 2 -  0 -  4 -  1
 |    |    |    |
 5 -  3 -  8 -  6   M3
 |    |    |    |
10 -  7 - 13 -  9
 |    |    |    |
14 - 11 - 15 - 12
```

OCID: 4011963

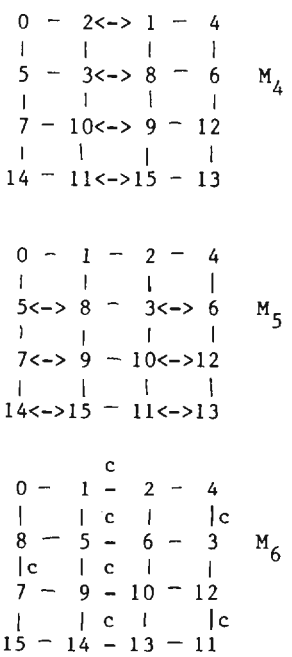


Figure 10

(U) The time required to perform M(j,k) is given by

$$T(j,k) = (2k + 4)t_r + t_c + T(j,k/2),$$

and we can find that

$$T(j,k) \leq (2j + 4k + 4\log k)t_r + (j + \log k)t_c.$$

In particular, $T(n,n/2^i) = O(n)$. Now to obtain our sorting algorithm, we first sort each column in time $T_{oe}(n,1) = n(2t_r + t_c)$ and then successively call on M(n,2), M(n,4), ..., M(n,n). The total time required for the sort, S(n,n), is then

$$S(n,n) = T_{oe}(n,1) + \sum_{i=1}^{\log n} T(n,2^i) = O(n \log n).$$

Thus we can sort $N = n^2$ in time $O(\sqrt{N} \log \sqrt{N})$.

(U) One further refinement of the algorithm will give us an improvement in the time to sort N words from $O(\sqrt{N} \log \sqrt{N})$ to $O(\sqrt{N})$. Rather than merge sorted columns of length n horizontally, we shall merge columns of length $n/2^i$ both horizontally and vertically. The algorithm M(j,k) merges two horizontally adjacent subarrays of size j x k/2. The same steps allow us to merge vertically adjacent subarrays of size k x j/2 in exactly the same time.

(U) Thus if M'(j,k) is an algorithm that merges four square adjacent subarrays of size j/2 x k/2, then

$$T'(j,k) = T(j/2,k) + T(j,k).$$

The case of particular interest to us yields

$$T'(j,j) \leq (11j + 8 \log j)t_r + (3j/2 + 2 \log j)t_c.$$

This means that we can sort an n x n array by M'(2,2), M'(4,4),...,M'(n,n); that is, we first merge 4 square adjacent 1 x 1 arrays, then 4 square adjacent 2 x 2 arrays, and so on. The total time for our sort, S'(n,n), is then given by

$$S'(n,n) = \sum_{i=1}^{\log n} T'(2^i,2^i)$$

$$\leq \sum_{i=1}^{\log n} (11j + 8 \log j)t_r + (3j/2 + 2 \log j)t_c$$

$$\leq (22n + 8 \log^2 n)t_r + (3n + 2 \log^2 n)t_c$$

$$= O(n).$$

That is, we can sort $N = n^2$ in time $O(\sqrt{N})$.

(U) Thompson and Kung use a slightly different square adjacent merge that has a time of about one-half that of ours. They also have an s x s square adjacent merge whose linear term is 6N, which is quite close to the optimal time of 4N. However, all of these algorithms are O(N), regardless of the value of the linear term.

(U) In the same paper [21], Thompson and Kung present an algorithm for performing a bitonic sort (discussed later) on a mesh-connected computer. They again require the data to be in snake-like row-major order and the sort time is O(N). In particular, the linear term is 14N for the bitonic sort versus 6N for the s x s merge sort. However, for small values of N, $N \leq 2^{18}$, the bitonic sort is faster, under the assumption that $t_c \leq 2t_r$. Nassimi and Sahni [11] present a bitonic sort algorithm for a mesh-connected computer that runs in about the same time as Thompson and Kung's algorithm, but it sorts in row-major order, rather than snake-like row-major. Finally, Thompson and Kung state that for a j-dimensionally mesh-connected computer, a bitonic sort on N words can be done in time $O(N^{1/j})$.

RING-CONNECTED COMPUTER

(U) An important factor to be considered in choosing an algorithm for an SIMD machine is a good match of the machine's interconnection network with the data routing of the

DOCID: 4011963

algorithm. For example, the odd-even transposition sort requires comparison-exchanges between adjacent words, so a mesh-like connection seems naturally suited for this algorithm. After discussing some sorting networks later, we will discuss further SIMD networks that are well suited for sorting. Figure 18 shows a ring connection and how an odd-even transposition sort "naturally" fits the network.

(U) A good measure of the effectiveness of a parallel sorting algorithm is the ratio of time to the number of processors. It is well known that for a serial processor, this ratio is asymptotically N log N. With k processors, the best speed that we can hope for is (N log N)/k. This is so, because otherwise we could make a serial machine run k times faster and then beat N log N time.

SORTING NETWORKS

(U) The several algorithms previously discussed have been designed for various models of SIMD machines. These involved several memories and processors with the capability of choosing among interconnection paths, and a master control unit. If our primary use for this configuration is sorting, then we have much more hardware than necessary. We will now develop a series of processors whose only purpose is to sort and which achieve a more efficient use of their component parts.

(U) Figure 19 shows the basic processor unit that we will use: a 2-sorter (or a comparison-exchange module or a comparator). The 2-sorter accepts two words, one on each of its input lines A and B, compares them and, if necessary, exchanges them so that the larger exits on the line marked "high" and the smaller on the line marked "low." The comparator would probably be built to accept words in bit serial order, most significant bit first. This would require the least amount of hardware, though a parallel design is feasible.

(U) To sort more than two words, we will seek some connection of comparators that will produce the desired result. Figure 20 shows a 3-sorter and a 4-sorter. In general, it is difficult to determine if such a network sorts. Knuth [7] has shown that if a network sorts all 0 - 1 sequences, then it will sort any sequence. Clearly testing 2^N sequences is easier than N!, but it is practical for small N. The solution is to find a recursive construction which guarantees a network that sorts, at perhaps the expense of less than an optimal design.

(U) If we have a technique for sorting N words, it is quite easy to extend it to an (N + 1)-sorter. Figure 21 shows the technique of insertion. After sorting the N words, the $n + 1^{st}$ word is compared with the smallest of the sorted list and exchanged if necessary. The larger of these two is compared with the next word, and so on. The $n + 1^{st}$ word "bubbles" up to its final position.

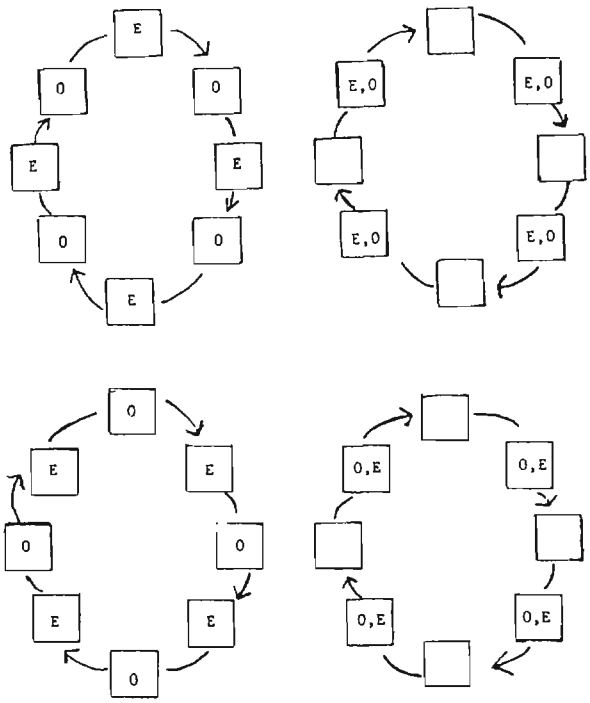


Figure 18.

(U) The repeated application of this insertion principle produces the network shown in Figure 22. To sort N words, this algorithm requires (N - 1)N/2 comparators and a delay of 2N - 3. The product of time and processors here is $O(N^3)$, and this seems decidedly nonoptimal. One apparent inefficiency of the network in Figure 22 is that line E is only involved with one comparison. We shall soon present elegant constructions that exceed this naive approach.

BATCHER'S BITONIC NETWORK

(U) Before continuing, it is necessary to define what Kenneth Batcher [1] calls a bitonic sequence, and then state his basic theorem about bitonic sorting.

CID: 4011963

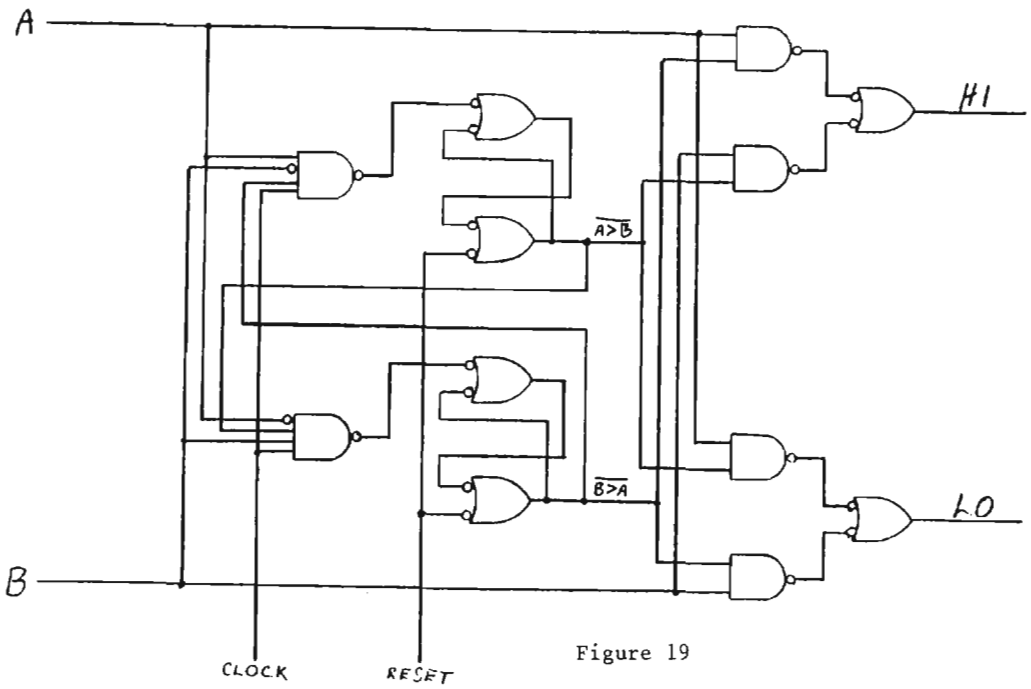


Figure 19

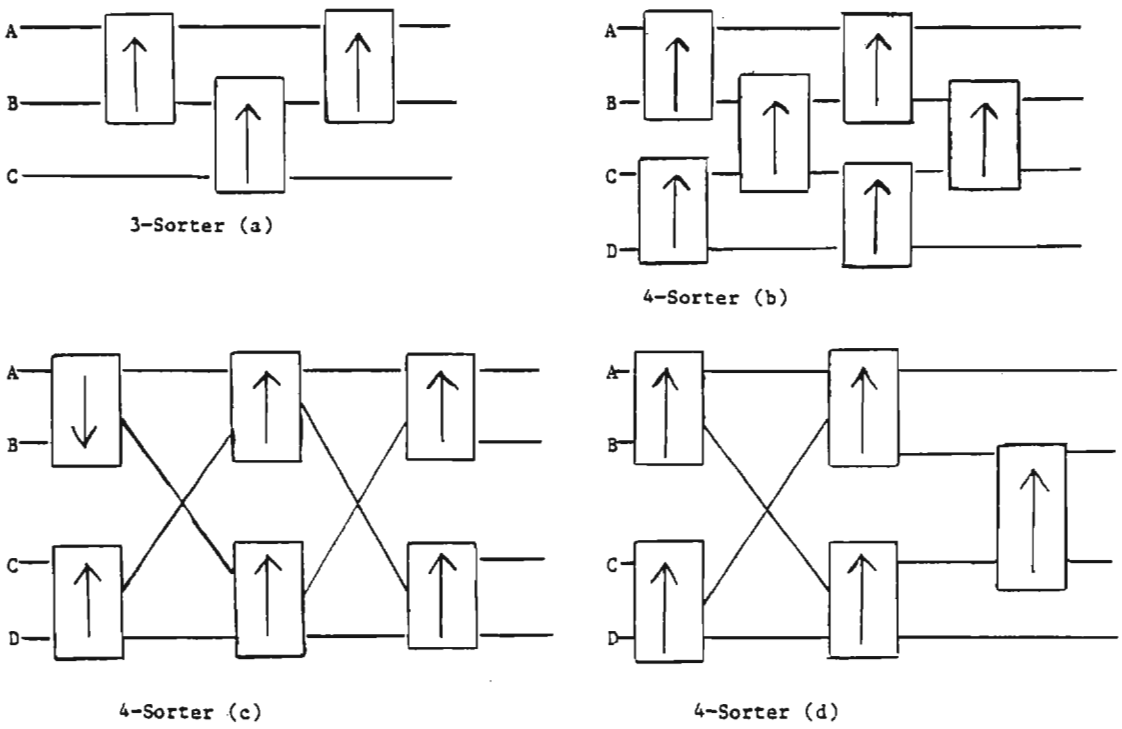


Figure 20.

OCID: 4011963

Definition: A sequence of numbers $\{a_i | i=1,N\}$ is said to be bitonic if either

1) there is a j, such that $a_i \leq a_j$, if $i \leq j$ and $a_i \geq a_j$, if $i \geq j$, or

2) the sequence is an end-around shift of a sequence satisfying 1).

Theorem: let $a_i | i = 1,\ldots,N$ be bitonic, and define

$$b_i = \max(a_i, a_{i+N/2}),\ i = 1,\ldots,N/2$$

and

$$c_i = \min(a_i, a_{i+N/2}),\ i = 1,\ldots,N/2.$$

Then $\{b_i | i = 1,\ldots,N/2\}$ and $\{c_i | i = 1,\ldots,N/2\}$ are both bitonic, and $b_i \leq c_j$ for all i and j.

(U) The importance of Batcher's Theorem is that it enables us to take a bitonic list of length N, and with N/2 simultaneous comparison-exchanges divide the list into the smallest and largest elements, with each of these two sublists itself bitonic. It is easy to see that log N of these subdivisions will sort the initial bitonic list of length N.

(U) The initial list is obtained in a recursive manner. First, two words are sorted with one comparator and combined with another sorted 2-list to form a bitonic 4-list. The 4-list is then sorted by using Batcher's Theorem, and then paired with another sorted 4-list to make a bitonic 8-list, and so on. This procedure is illustrated in Figure 23.

(U) A few calculations will show that the delay for sorting N words is $1/2 \log_2 N(\log N + 1)$ and the number of comparators needed is $1/4\ N \log N(\log N + 1)$. As clever as Batcher's recursive construction is, it does not produce the network with the least delay or the smallest number of comparators. For example, an 8-bitonic sorter requires 24 comparators and 6 delays (see Figure 23(d)), while the network in Figure 24 needs only 19 comparators, though still 6 delays (which is minimal in time and comparators). Networks in general and the Batcher network in particular (as illustrated in Figure 23) have certain drawbacks: a small number of comparison-exchanges are made at each stage, but the interconnection varies from stage to stage. Further, once built, the network can only be used to sort a fixed size list. We will present techniques that overcome both of these disadvantages.

STONE-BATCHER NETWORK

(U) Harold Stone [19] first observed that the perfect shuffle interconnection could be use as a fixed interconnection. He noted that Batcher's bitonic sorter for $N = 2^n$ first compared words that differed in the 1's digit; then the 2's digit and the 1's digit; then the 4's digit, the 2's digit, and the 1's digit; and so on. The perfect shuffle permutation on $N = 2^n$ elements has $i \rightarrow 2i \pmod{2^n - 1}$. It can be visualized as the rearrangement caused by "cutting" the elements into halves, like a deck of cards, and "shuffling" them together. The permutation has the property of bringing together words that differ first in their most significant digit, then the next most significant, and so on.

(U) A sorting network that utilizes this fixed interconnection between stages is shown in Figure 25(a). Note that some of the comparators are inactive and simply allow data to pass through. By utilizing a three-state comparator (sort up, sort down, and pass through), it is possible to reduce a bitonic sorter to a single stage of comparators with a feed-around interconnection, as shown in Figure 25(b).

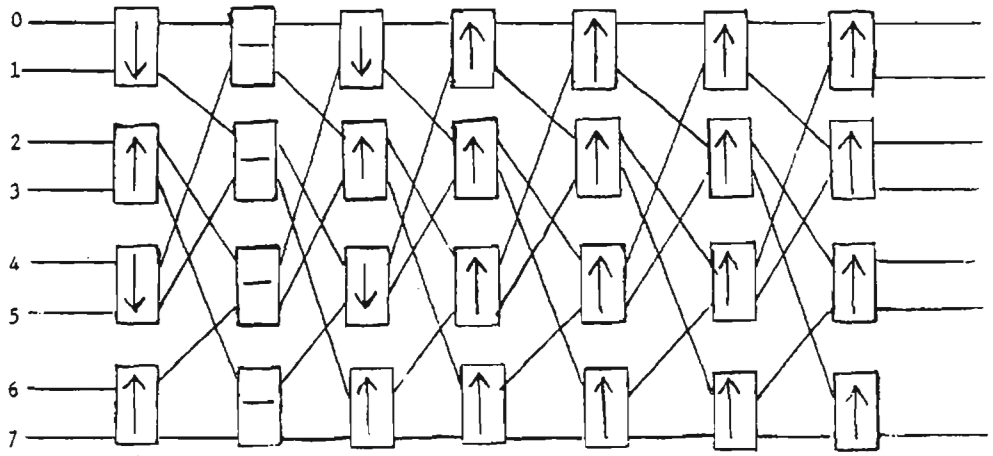
(U) The Stone-Batcher sorter requires only N/2 comparators as compared to about $1/2\ N \log^2 N$ for a bitonic sorter, though its time is about twice as slow: $\log^2 N - \log N + 1$ versus $1/2\ (\log^2 N + \log N)$. While Stone's configuration does dramatically decrease the hardware needed at only a slight increase in time, it will not allow data to be pipelined through it. If it is necessary to sort several lists of length N, the Stone-Batcher network requires that each list be sorted before the next one can be processed. A full network, on the other hand, can begin processing a new list as soon as the first stage of comparison-exchanges of the first list is completed.

(U) Another problem with sorting networks is that, once built, they cannot handle lists of a larger size, and they can only handle lists of a smaller size by "padding" them with $+\infty$ or $-\infty$. This can be overcome by expanding on the Stone-Batcher configuration shown in Figure 25(b) by replacing the storage register with first-in-first-out memories. These could be realized with disks, tapes, or similar media.

FASB SORTER

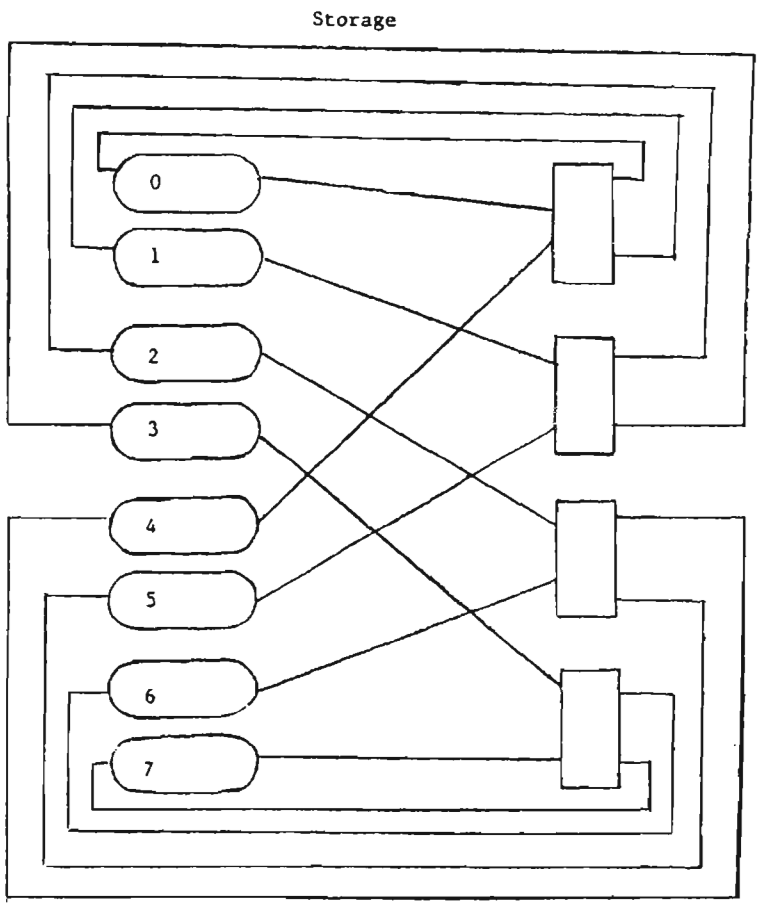
(U) Morris [10] first considered this design and called it the FASB Sorter, which is shown in Figure 26. Each box labeled M_i is a

OCID: 4011963



(a)

Figure 25.



(b.)

DOCID: 4011963

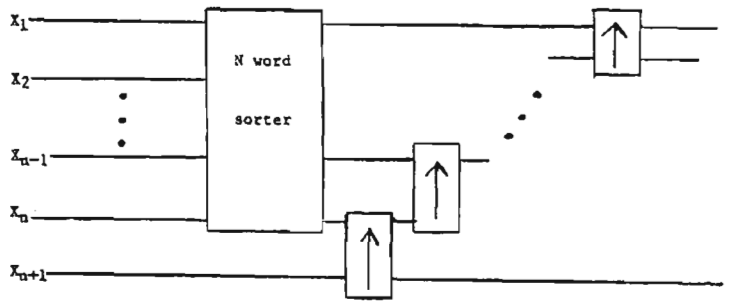
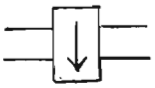
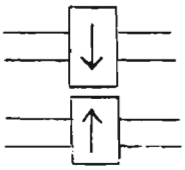


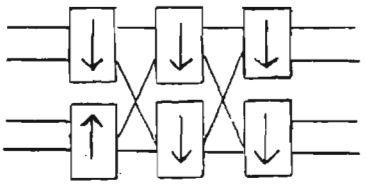
Figure 21.



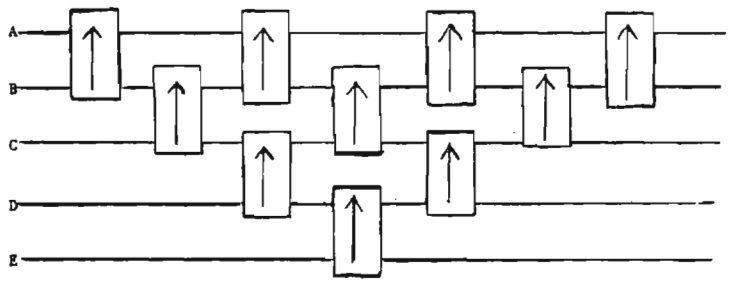
Sorted 2-list
(a)



bitonic 4-list
(b)

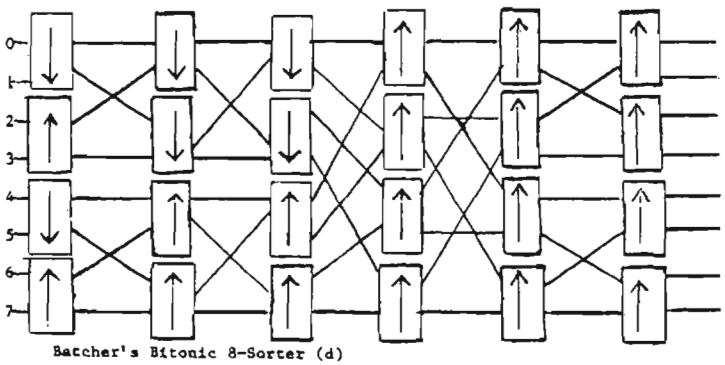


Sorted 4-list
(c)



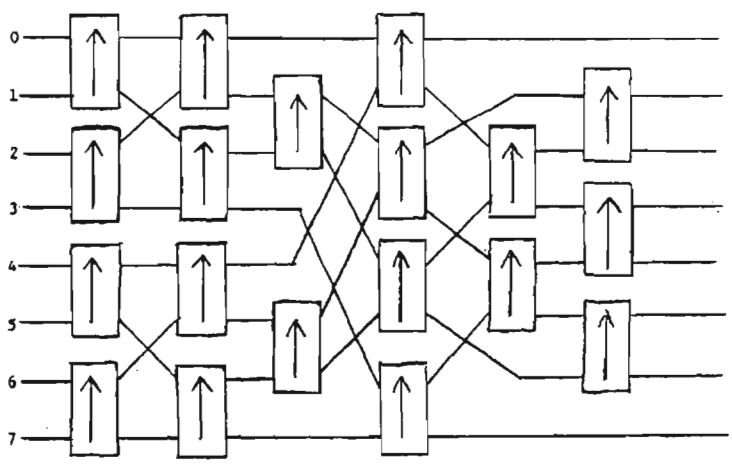
5-Sorter

Figure 22



Batcher's Bitonic 8-Sorter (d)

Figure 23.

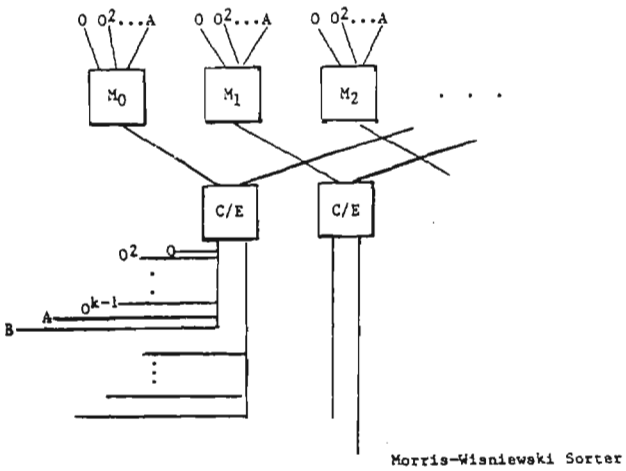


8-Sorter

Figure 24

OCID: 4011963

serial memory and each box labeled C/E is a three-state comparator. Note that we have a special switch for each even-odd pair of memories that allows two words to be written simultaneously into one memory or another. Because one word is written out while two are written in, the memories must effectively work at half-speed (unless radically redesigned).



Morris-Wisniewski Sorter

Figure 27.

MORRIS-WISNIEWSKI SORTER

(U) An improvement was made in this design by Morris and Wisniewski [11]. Rather than have three-state comparators that were idle nearly half of the time, they substituted a multiple interconnection scheme--in effect trading more wires for less time. The interconnections needed are all nontrivial powers of the perfect shuffle; 0, 0^2, 0^3, ..., and two permutations called A and B. Permutation A takes the outputs of the comparators and routes them in pairs to the first half of the memories and B routes the outputs in pairs to the second half of the memories. For 2^k elements, 0^k = id, thus for 2^k memories, k - 1 + 2 = k + 1 interconnections are needed, rather than 1. Figure 27 shows a Morris-Wisniewski sorter.

(U) The Morris-Wisniewski sorter requires a more complicated control mechanism than the FASB or the Stone-Batcher because of the k + 1 data paths to choose from. However, for a configuration with 2^k memory modules, it can sort $N = 2^n$ words in time $2^{n-k-1} \log N(\log N + 1)$, about one half the time of a Stone-batcher sorter if k = m. The Morris-Wisniewski sorter can be expanded to handle any lists up to memory capacity.

SINGLE LADDER ODD-EVEN TRANSPOSITION SORTER

(U) The last two sorting machines are highly specialized processors and would be useful only when considering the sorting of massive files. If, for example, it was necessary to serially read the data out before it could be used, then the I/O would dominate our considerations. For the latter situation, IBM [3] has proposed a special-purpose sorting processor that would be attached to a serial computer. Most of the sorting time would be hidden by the I/O time.

(U) The device is called a single ladder odd-even transposition sort (SLOETS). It consists of a series of comparators that can be set to allow straight-through or exchange data flow. The modules are linked by loops into a "ladder." Figure 28 shows a four-stage ladder in operation. The words are routed in serially so that each loop is filled with one word. Then as the words circulate through the loops, alternately odd-even and even-odd pairs are brought together in the comparators. As the data is routed in, some comparisons can be made before the ladder is full and data can be routed out before the sort is entirely finished. The net result is that all but about 20% of the sorting time is overlapped with I/O.

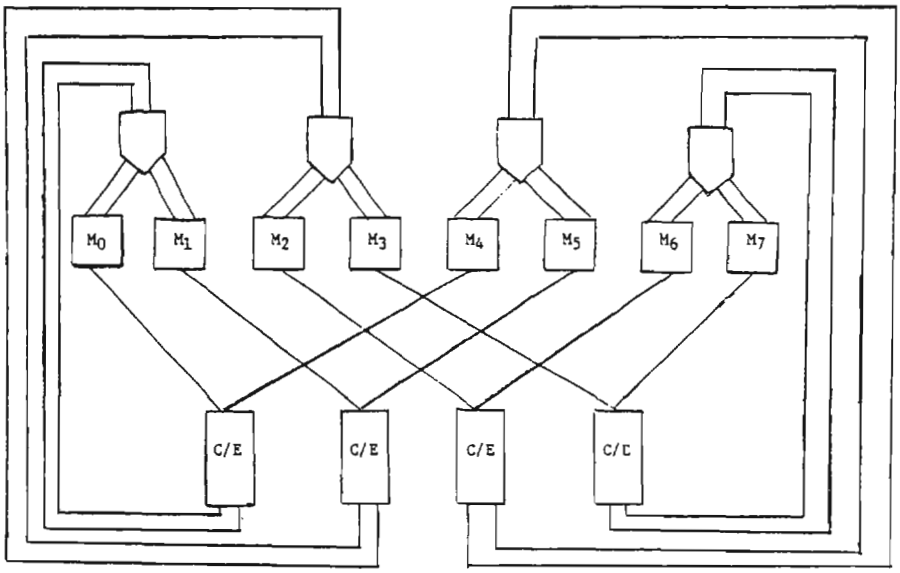
(U) By having two ladders, with the first sorting while the second is being filled, it is possible to overlap all but 6% of the sorting time with I/O. After sorting the two separate lists, they are merged as they are read out. With three or four ladders, the non-overlapped sorting time is negligible.

SORTING MASSIVE FILES

(U) During the editing of this paper, a paper appeared containing an analysis of merge and bitonic sorting in the context of massive files. The paper, "A Comparison of Merge and Bitonic Sorting," R51/MATH/05/81, shows that when the distribution of data is known and uniform on all subsets of tapes then merge sorting is superior.

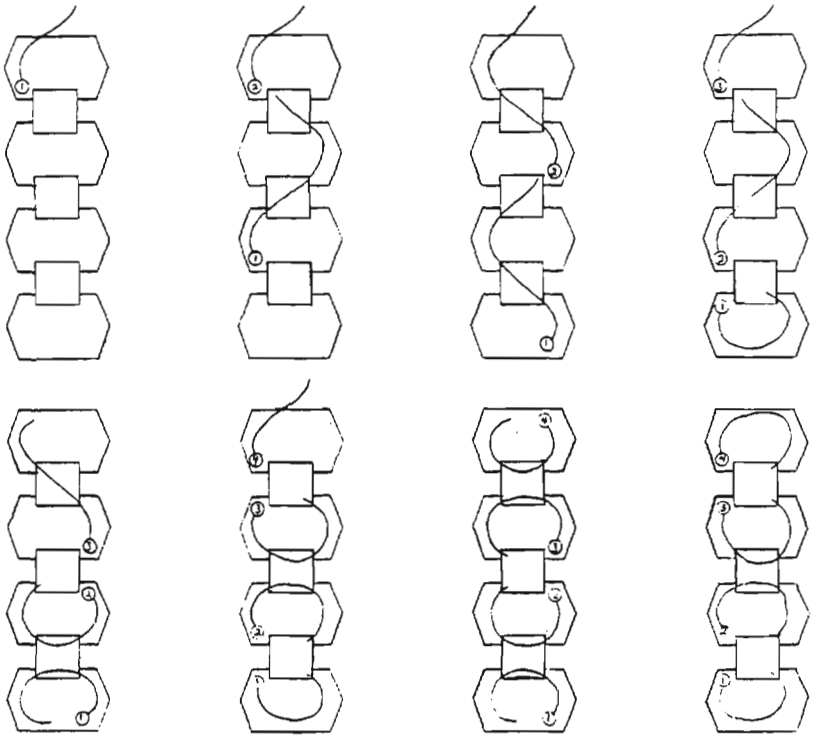
EO 1.4.(c)
P.L. 86-36

OCID: 4011963



FASB Sorter

Figure 26.



Single Ladder Odd-Even
Transposition Sort

Figure 28.

DOCID: 4011963
EO 1.4.(c)
P.L. 86-36

(U) A standard tape reel has 2,400 feet of usable tape. Current high-density tape has 6,250 bits per inch and eight tracks (plus a ninth track for parity). Thus, one reel can hold about 2.25×10^7 64-bit words. If we allow for record gaps, we have perhaps 2×10^7 64-bit words. One of these tape reels can be sorted on a computer with sufficient disk storage in 20 minutes. Two sorted tapes can be merged at essentially the rate at which the data can be written out, about eight minutes per merge.

[redacted]

[redacted]

[redacted]

(U) One final note on sorting networks should be made. Batcher's bitonic sort of $N = 2^n$ elements in time $1/2\ n^2 + 1/2\ n$ is not the fastest known network. David van Voorhis [23] has developed a recursive construction that sorts in about time $1/2\ n^2 + 1/4\ n$, and the van Voorhis construction requires about $1/4\ n^2 2^n - .37n2^n$ comparators versus $1/4\ n^2 2^n + 1/2\ n2^n$ for a bitonic sort. However, the van Voorhis network is not as easy to analyze as is Batcher's network. For example, it is a simple task to determine which elements are being compared at any stage of a bitonic sort while the same cannot be done for an van Voorhis network. This means that for actual construction of a small-size network, van Voorhis' techniques would be used, though Batcher's networks will continue to be used to obtain performance estimates.

(U) The very pertinent question, "What is the best way to sort in parallel?" can best be answered: "It depends!" For a truly massive sort, some type of merging technique using tapes and many processors seems best. A parallel processor, though, is another matter. The instruction set, timing, and individual quirks are probably more important than the theoretical complexity of any algorithm. The best strategy, in advance of knowing the particular machine and its peculiarities, is to have a broad knowledge of the available algorithms.

EO 1.4.(c)
P.L. 86-36

APPENDIX

A Comparison of Some Algorithms in this Paper

Hirshberg's Bucket Sort:

Words: N
Processors: N
Interconnections: Each processor is connected to a common memory.
Time: O(log N)

Valiant's Fast Merge:

Two Lists: N M
Processors: $\sqrt{NM}$
Interconnections: Each processor is connected to a common memory, or the connections are "sufficiently robust."
Time: O(log log N)

EO 1.4.(c)
P.L. 86-36

Preparata's Sort:

Words: $N = 2^n$
Processors: 2^{n-1}
Interconnections: Each processor is connected to a common memory.
Time: O(log N)

Thompson and Kung's Sort:

Words: $N = n^2$
Processors: N
Interconnections: Mesh-connected, without end-around paths.
Time: $O(\sqrt{N})$

Batcher's Bitonic Sorter:

Words: $N = 2^n$
Processors: $N \log^2 N = n^2 2^n$
Interconnections: As required by the algorithm.
Time: $\log^2 N = n^2$

Stone-Batcher Sorter:

Words: $N = 2^n$
Processors: $N = 2^{n-1}$
Interconnections: Perfect Shuffle
Time: $\log_2 N = n^2$

Morris-Wisniewski Sorter:

Words: $N = 2^n$ in 2^k memories
Processors: 1 2^{k-1} 2^{n-1}
Interconnections: Multiple perfect shuffles
Time: $2^{n-k-1} \log^2 N = 2^{n-k-1} n^2$

BIBLIOGRAPHY

1. Batcher, Kenneth E., "Sorting Networks and Their Applications," Proc. AFIPS Spring Joint Comp. Conf. Vol 32, 1968, pp. 307-314.
2. Baudet, Gerard, and David Stevenson, "Optimal Sorting Algorithms for Parallel Computers," IEEE Trans. Comp. Vol. C-27, No. 1, January 1978, pp. 84-87.
3. Chen, T. C., K. P. Eswaran, V. Y. Lum, and C. Tung, "Simplified Odd-Even Sort Using Multiple Shift-Register Loops," Internat. J. Comput. and Inform. Sci., Vol. 7, No. 3, 1978, pp. 295-314.
4. Hirshberg, D. S., "Fast Parallel Sorting Algorithms," Com. ACM, Vol. 21, No. 8, August 1978, pp. 657-661.
5. [redacted] "A Merging Sort Machine," SCAMP Working Paper No. 18/78, IDA, September 1978.
P.L. 86-36
6. Knuth, Donald E., The Art of Computer Programming, Vol. 1, Fundamental Algorithms, Reading, MA: Addison Wesley, 1973.
7. -----, The Art of Computer Programming, Vol. 3, Sorting and Searching, Reading, MA: Addison Wesley, 1973.
8. Martin, William S., "Sorting," Comput. Surveys, Vol. 3, No. 4, December 1971, pp. 147-174.
9. [redacted] "Costing Massive Sorts," R51/MEMO/06/80, 13 February 1980.
10. -----, "The FASB Sorter," S61 Informal Note No. 381, February 1976, S-218,292.
11. [redacted] "A Fast Parallel Sorting Processor," R51/MATH/17/78, S-216,947.
P.L. 86-36
12. Nassimi, David, and Santaj Sahni, "Bitonic Sort on a Mesh-Connected Parallel Computer," IEEE Trans. Comp., Vol. C-27, No. 1, 1 January 1979, pp.2-7.
13. -----, "Parallel Permutation and Sorting Algorithms and a New Generalized Connection-Network," Technical Report 79-8, April 1979, University of Minnesota, (to appear in JACM).
14. Orcutt, Samuel Ellis, Jr., "Computer Organization and Algorithms for Very High Speed Computations," Ph.D. dissertation, Stanford University, September 1974.
15. Preparata, Franco R., "New Parallel-Sorting Schemes," IEEE Trans. Comp. Vol. C-27, No. 7, July 1978, pp. 669-673.
16. Schwartz, J. T., "Ultracompilers," Comp. Sci. Dept., New York University, 1979.
17. [redacted] "Shuffle Sorting with the Odd-Even Merge," SCAMP Working Paper No. 13/78, IDA, October 1978.
P.L. 86-36
18. Smith, Burton J., "An Analysis of Sorting Networks," Sc.D. thesis, Dept. of E.E., M.I.T., August 1972.
19. Stone, Harold S., "Parallel Processing with the Perfect Shuffle," IEEE Trans. Comp., Vol C-20, No. 2, February 1971, pp. 153-161.
20. -----, "Sorting on STAR," IEEE Software Eng., Vol SE-4, No. 25, March 1978, pp. 138-146.
21. Valiant, Leslie G., "Parallelism in Comparison Problems," SIAM J. Comput. Vol. 4, No. 3, September 1975, pp. 348-354.
22. Van Voorhis, David C., "An Economical Construction for Sorting Networks," Proc. AFIPS Nat. Comp. Conf., 1974, pp. 921-927.
23. -----, "Efficient Sorting Networks," Ph.D. dissertation, Comp. Sci., Stanford University, December 1971.

CID: 4011963

ADA NEWS(U)

DIRNSA has designated T303 as the Office of Primary Responsibility for Ada planning and transition activities at NSA. For information on the Agency's current and planned Ada technology utilization, contact [redacted] or [redacted] on 923-3227 or your local Cadre member.

The Ada Cadre is intended to serve as points of contact for the dissemination of information concerning Ada in addition to advising and assisting T303 as to Ada planning and requirements.

P.L. 86-36

Current Cadre members are:

[redacted]

A043	963-3177
B62	963-4398
C31	968-7155
E09	968-8953
G33	963-4301
P309	963-5621
P372	963-4604
P5	963-3043
R09	968-7381
R623	968-8485
S352	972-2346
T303	963-3227
T303	963-3227
W09	963-3401

WE ARE ALWAYS LOOKING FOR

ARTICLES, COMMENTS, NOTES, LETTERS,

THAT WOULD BE OF INTEREST TO OUR READERS

SOLUTION TO NSA-Crostic No. 45

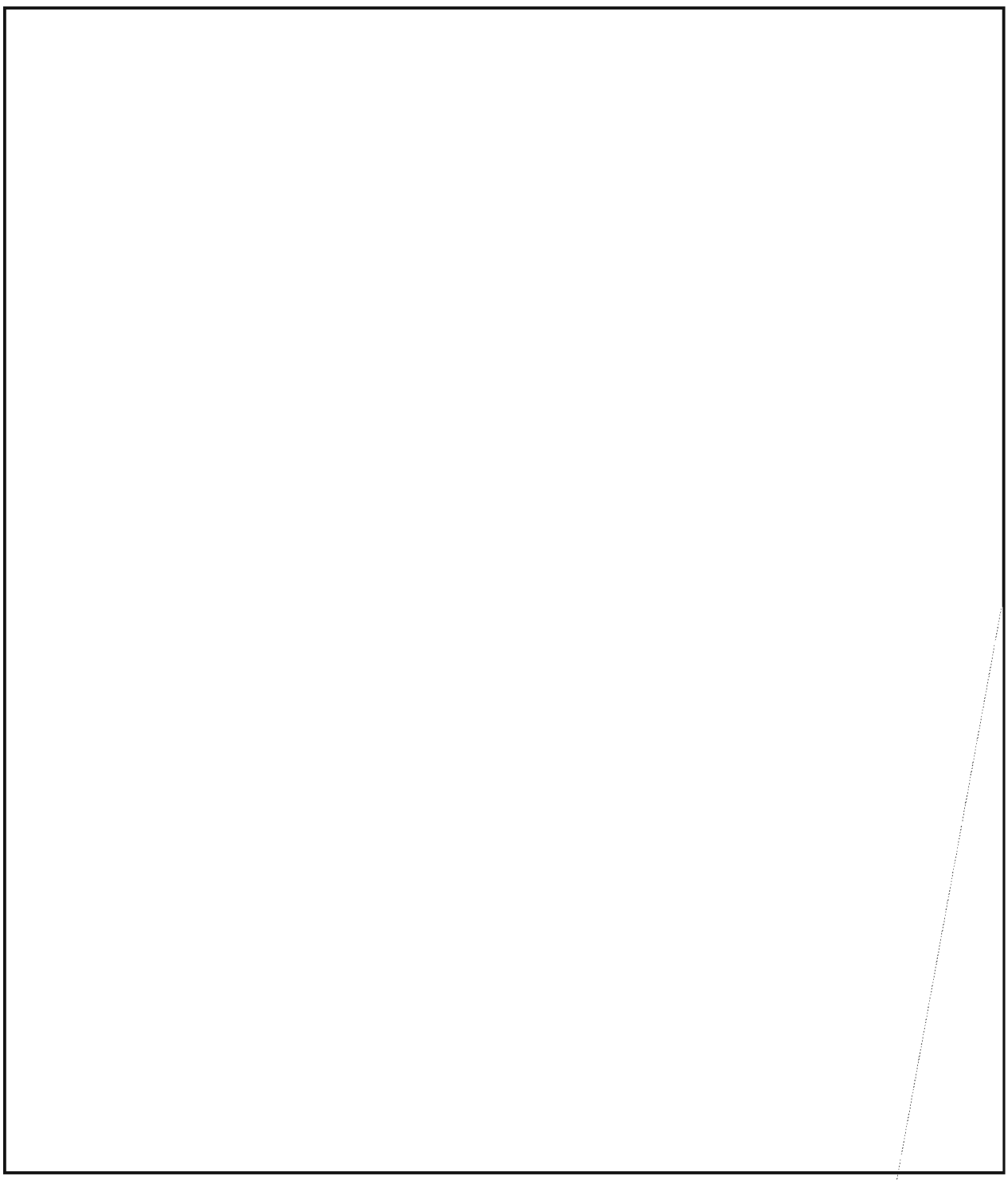
A. J. Salemme, "I Remember SPELLMAN," CRYPTOLOG, Jul-Aug 1978

[redacted]

EO 1.4.(c)
P.L. 86-36

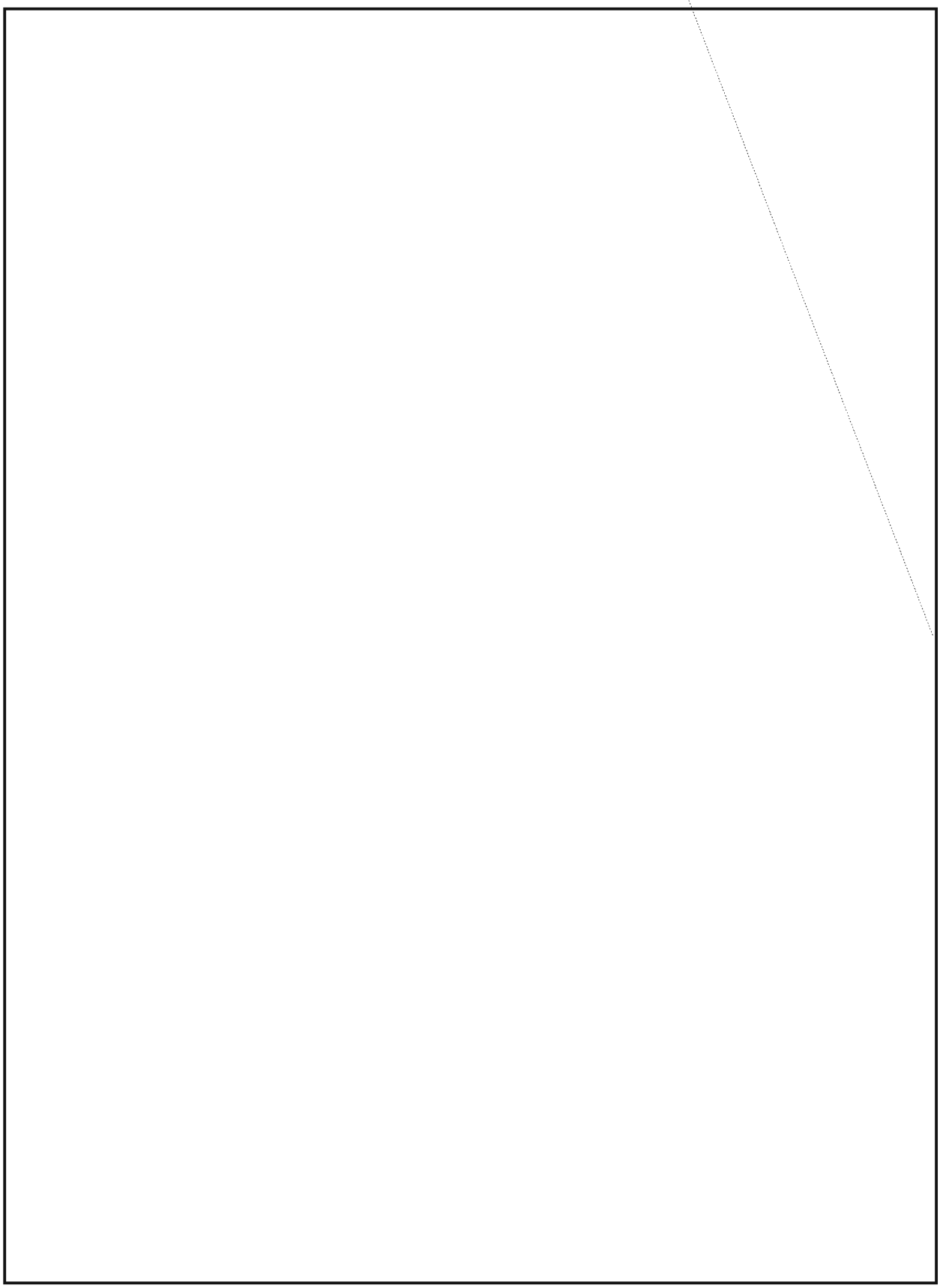
DOCID: 4011963

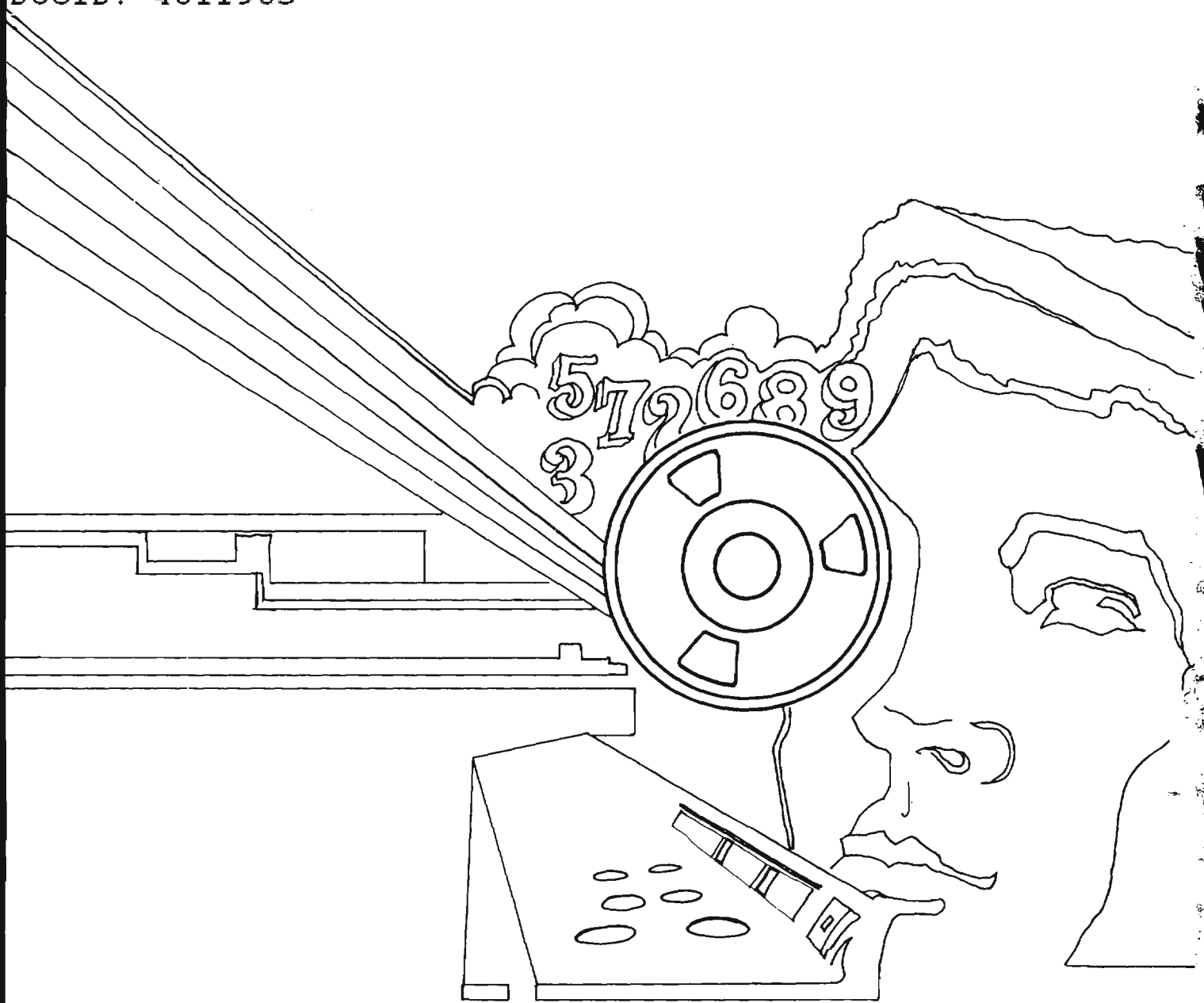
NSA - CROSTIC No. 46



P.L. 86-36

OCID: 4011963




5726893

DOCID: 4009856

P.L. 86-36

~~TOP SECRET~~

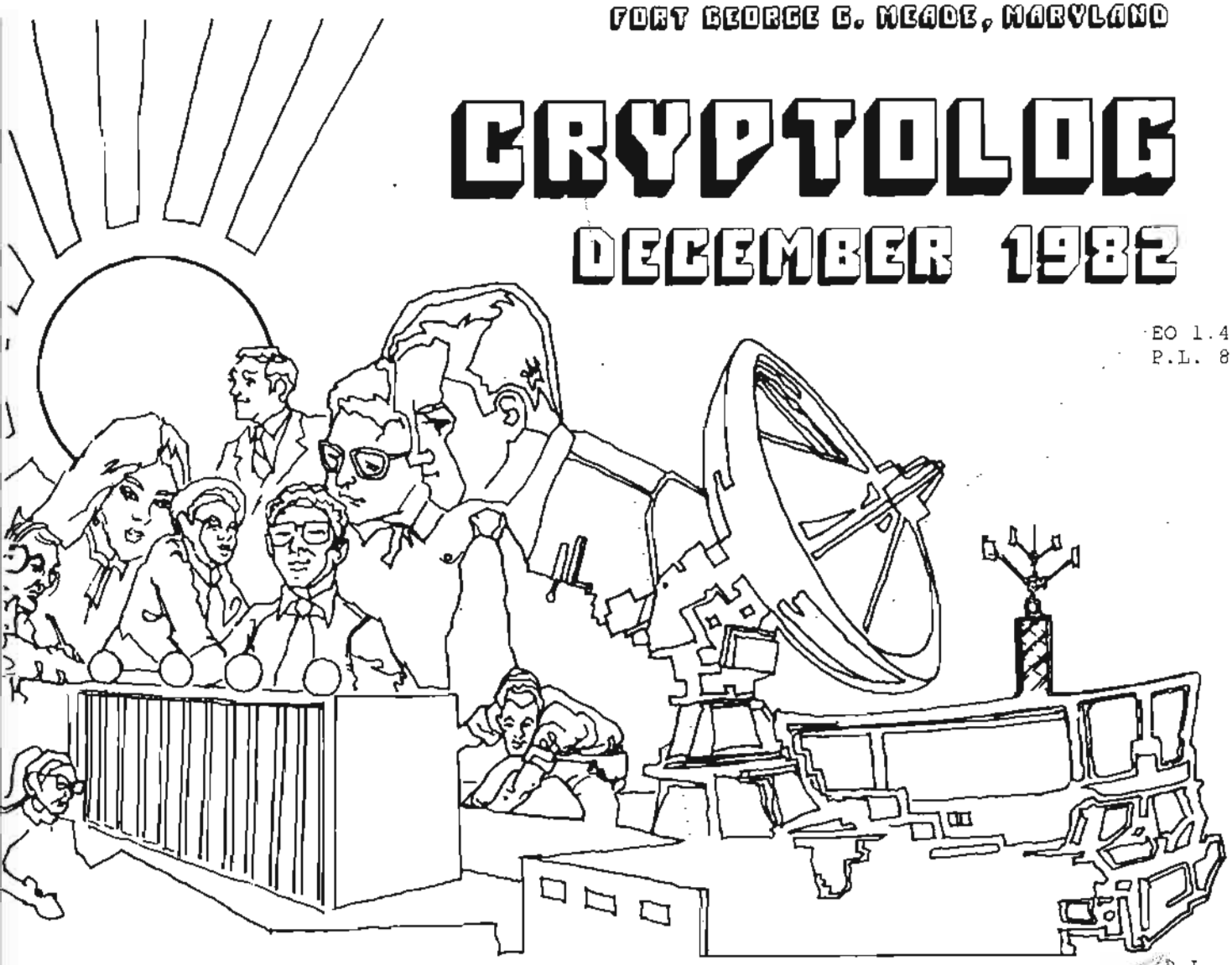
I423 [redacted]

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

DECEMBER 1982

EO 1.4.(c)
P.L. 86-36



P.L. 86-36

[redacted] ..... [redacted] 1
DEVELOPMENT AND CORRELATION OF INDICATORS (U) ... [redacted] 6
DOES ANYBODY HERE REMEMBER PURPLE? (U) ..... [redacted] 8
GOING ON-LINE WITH INFORMATION AIDS (U) ..... Jack Gurin 10
QUESTIONS IN SEARCH OF A PQE (U) ..... [redacted] 13
SHELL GAME: COUNTER (U) ..... W.E.S. 14
AJSQUE (U) ..... [redacted] 15
PWB WHEN (U) ..... [redacted] 16
KRYPTOS NEWS (U) ..... [redacted] 17
PASSWORDS (U) ..... [redacted] 18
NSA-CROSTIC (U) ..... David H. Williams 20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~
US/UK/CAN/AUS/NZ EYES ONLY

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

~~FOR SECRET~~

DOCID: 4009856

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. IX, No. 12 DECEMBER 1982

PUBLISHER [redacted]

BOARD OF EDITORS

Editor.....[redacted](8322s)
Asst. Editor.....[redacted](1103s)
Production.....[redacted](3369s)

Collection.....[redacted](3961s)
Cryptanalysis.....[redacted](5311s)
Cryptolinguistics.....[redacted](1103s)
Information Science.[redacted](5711s)
Language.....[redacted](8161s)
Machine Support.[redacted](4681s)
Mathematics.....[redacted](8518s)
Puzzles.....David H. Williams (1103s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Don Taurone (3573s)

For subscriptions
send name and organization

to: CRYPTOLOG, P1
or call [redacted]3369s

P.L. 86-36

To submit articles or letters
via PLATFORM mail, send to

cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no '0' in 'log')

Contents of Cryptolog should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

It is undoubtedly a coincidence, but just three weeks after our editorial appeared about moving, we were notified that WE were moving. There is something about moving that is, frankly, unsettling.

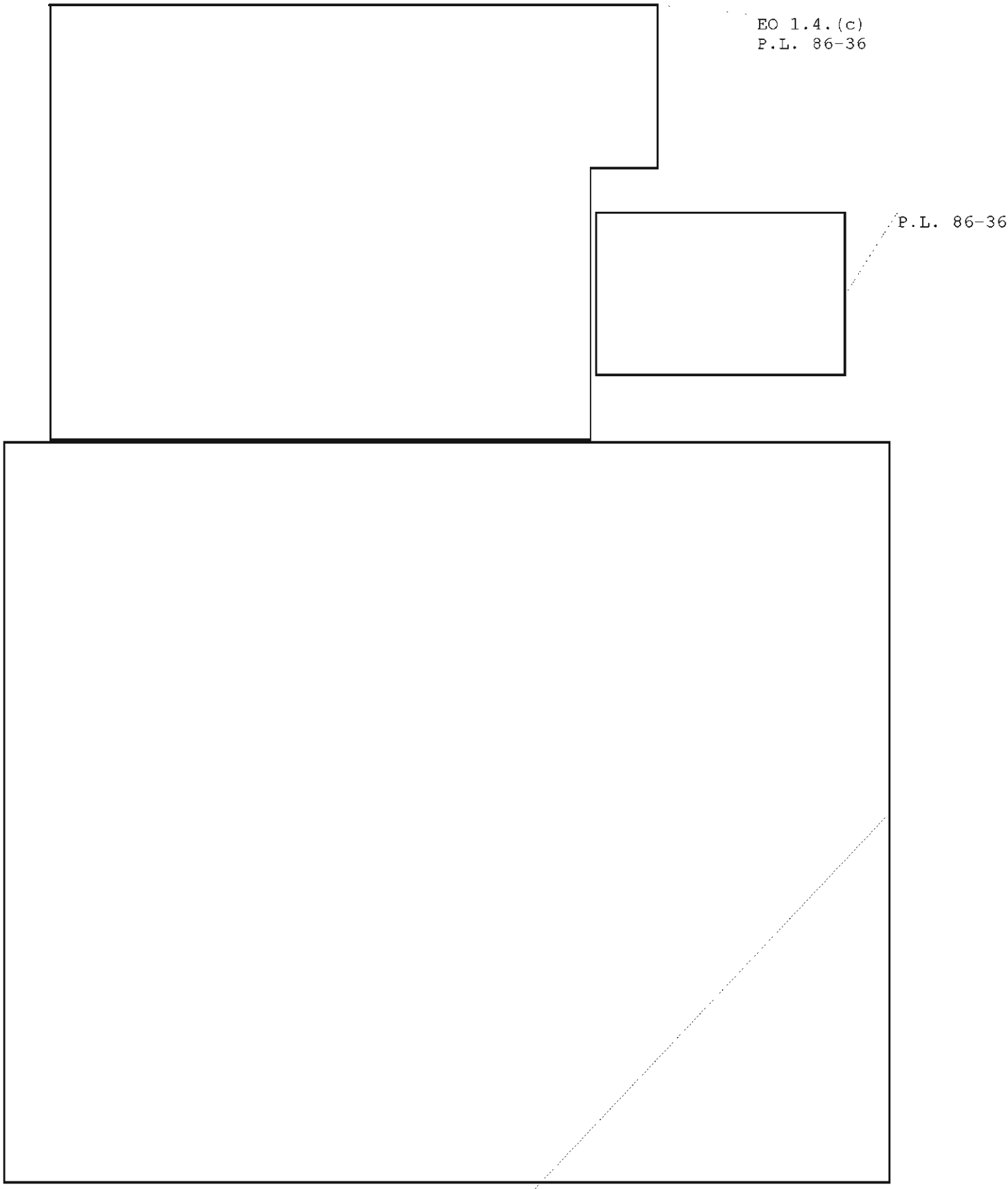
It must be said that the people one encounters when moving are quite friendly and helpful. The telephone people, for instance, must spend much of their time having to deal with people who are unhappy about having to move, yet they were sunny in disposition (more so than I would be if my job required me to deal continually with displaced persons). And so, in fact, were all of the other folks we met along the trek.

Moving can be an adventure. I have fond memories of long columns of desks, moving slowly at the command of column coordinators with walkie-talkies. And there are advantages to moving: it is a good time to throw away some of that accretion of stuff that I keep accumulating.

Besides, if [redacted] is right (CRYPTOLOG, June-July 1982, p25), then somebody has to move! So as long as whoever keeps the roster does it fairly, my turn will only come up every so often. Of course, if I could figure out how that roster works, maybe by getting myself transfered at just the right time, I could stay in one place and let the new organization move in around me!

Next month, something different...

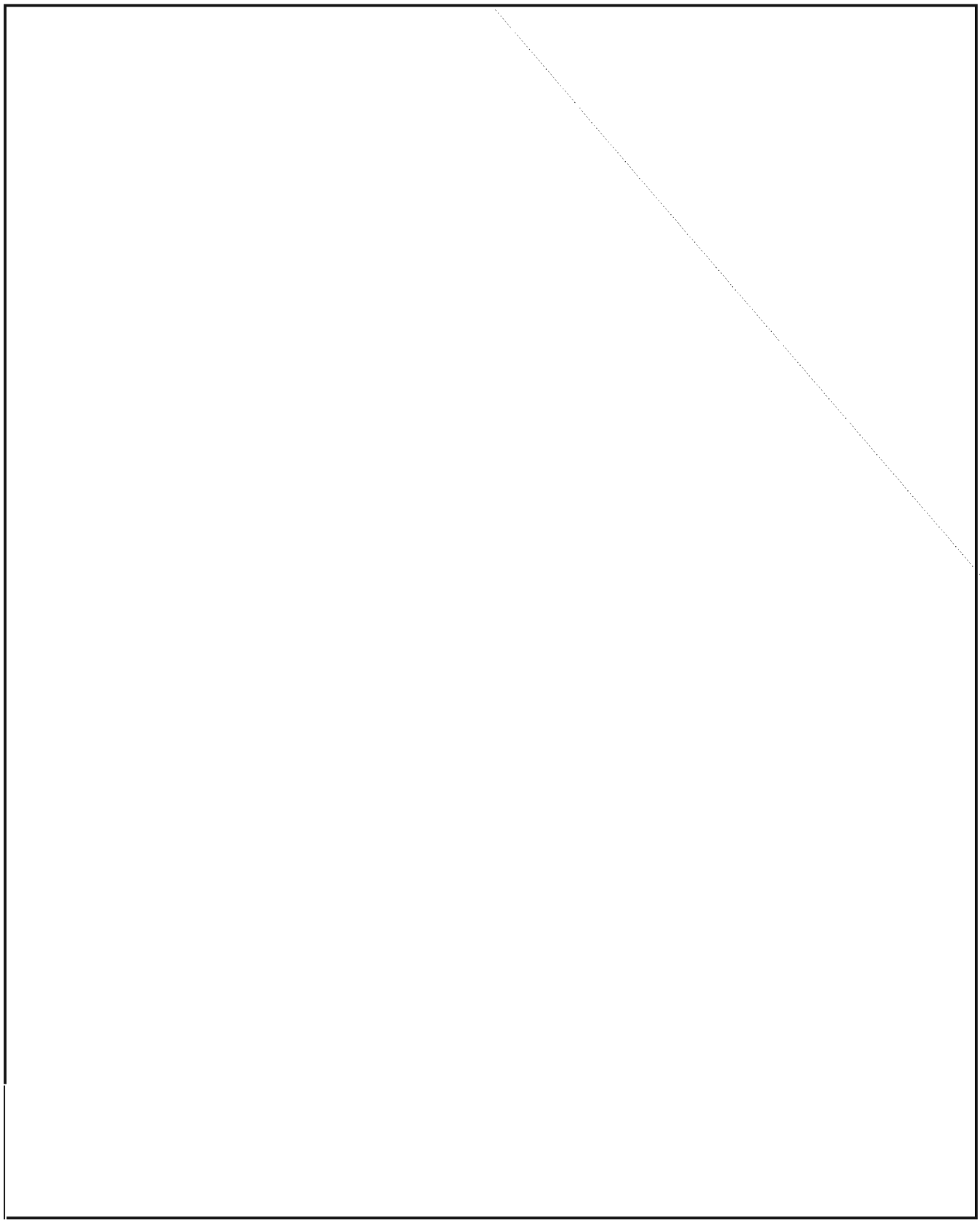
~~FOR OFFICIAL USE ONLY~~



EO 1.4.(c)
P.L. 86-36

P.L. 86-36

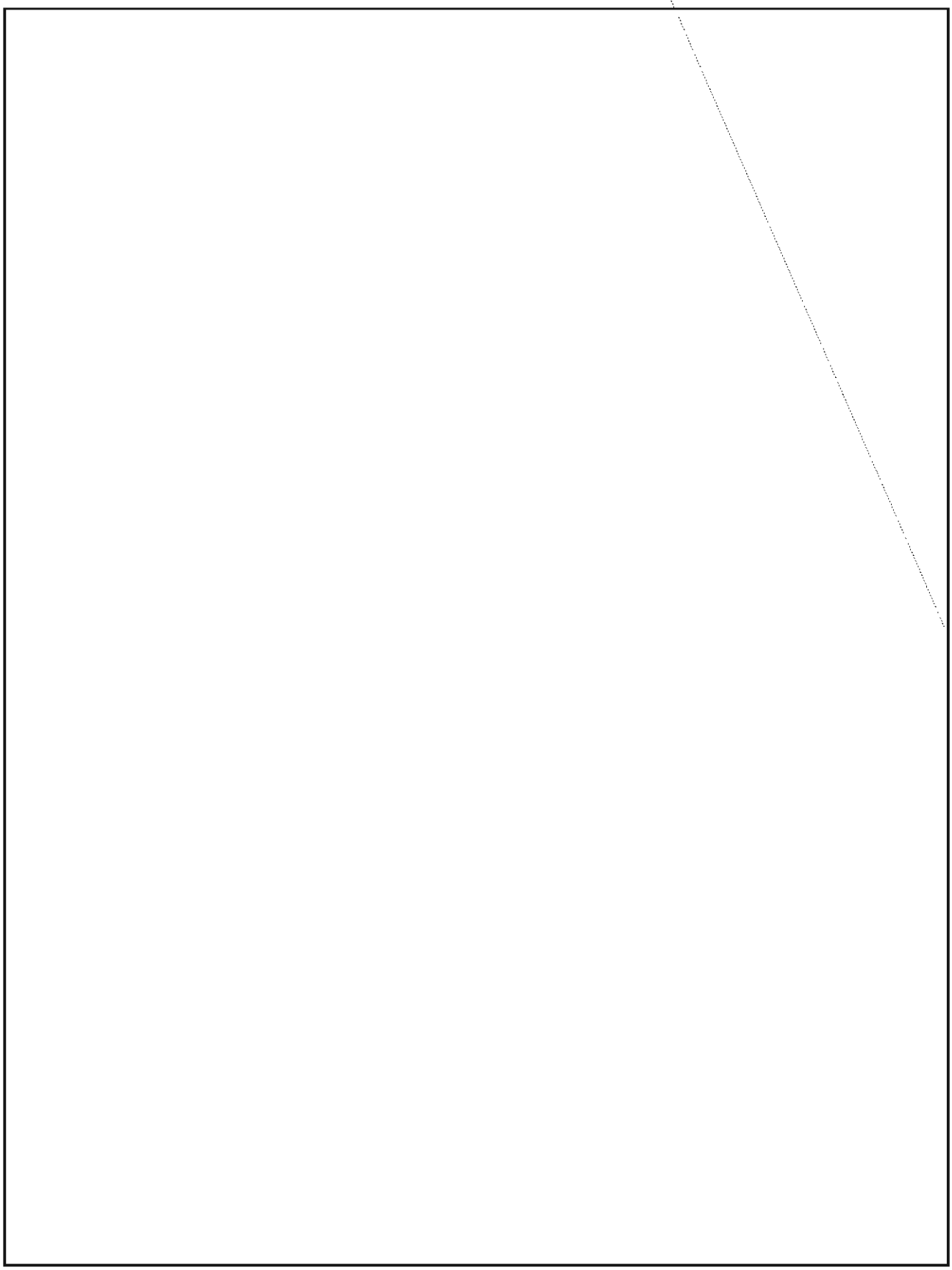
EO 1.4.(c)
P.L. 86-36

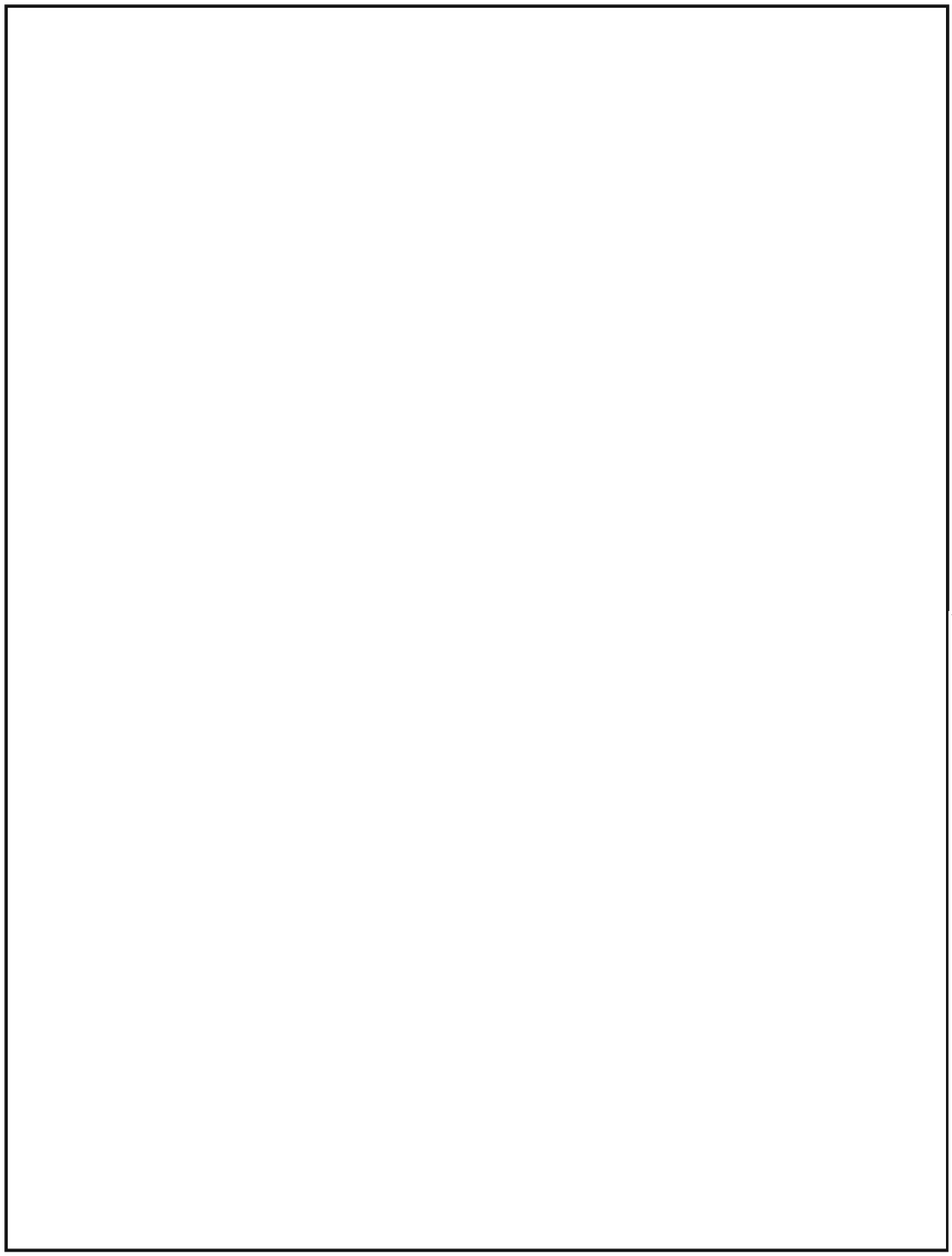


EO 1.4.(c)
P.L. 86-36

DOCID: 4009856

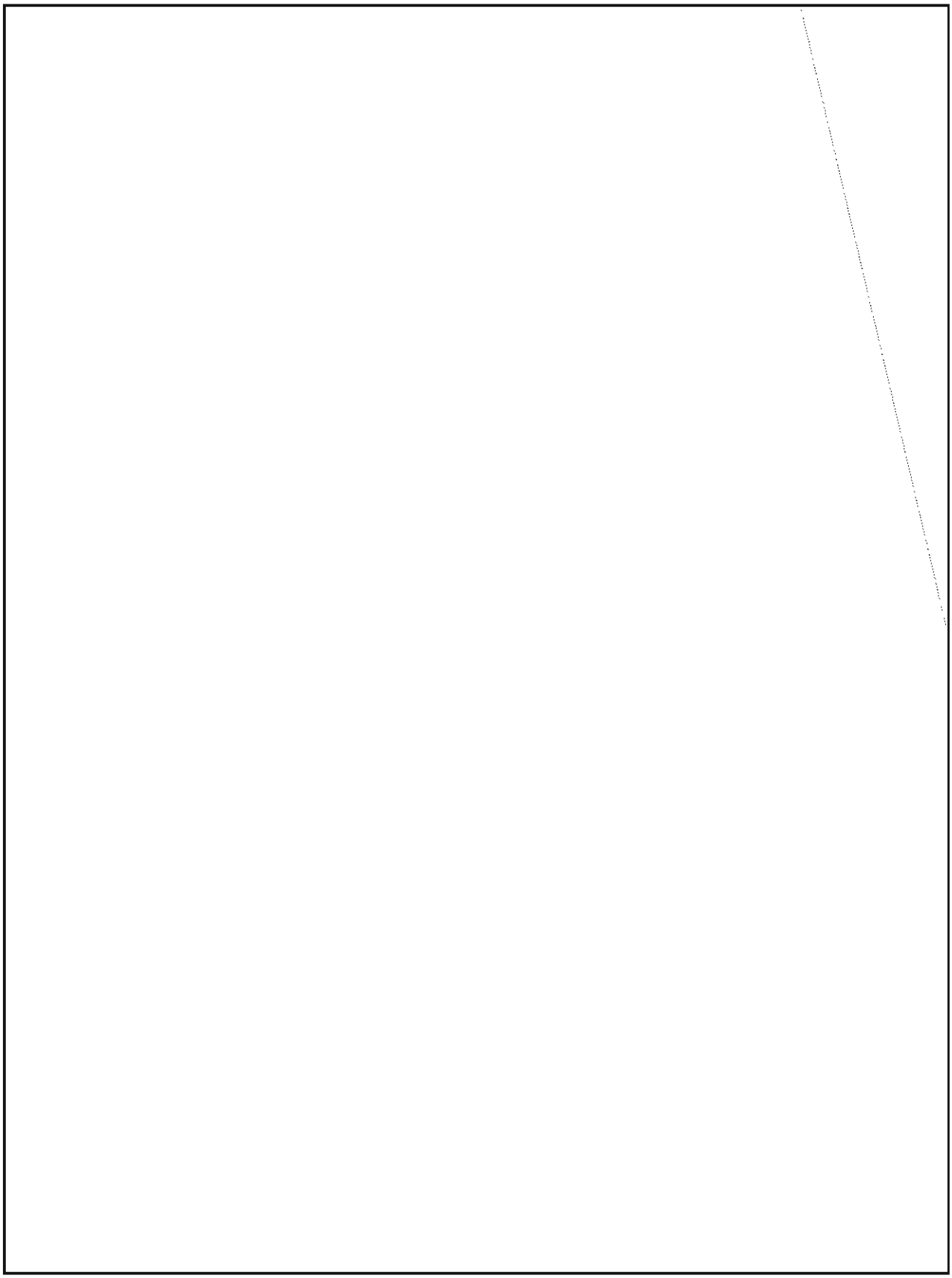
EO 1.4.(c)
P.L. 86-36





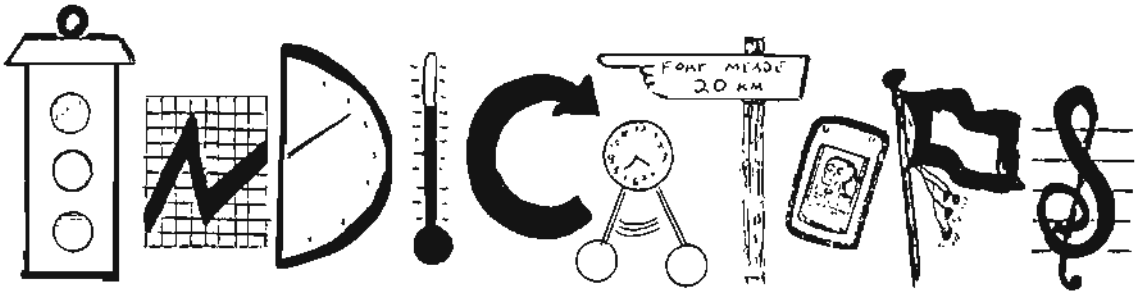
EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



DOCID: 4009856

The Development and Correlation of



by [redacted] S24

P.L. 86-36

Warning indicators postulate specific actions that a foreign power may take prior to the initiation of hostilities. Indicators are ~~(C)~~ developed from collected intelligence, historical data, and the political and military doctrine of a foreign power.

~~(S)~~ Indicator lists are formed by correlating indicators under specific categories; they are used by indications and warning (I&W) analysts as a tool to determine if a possible strategic warning environment is developing. These lists denote the capabilities of specific targets. Those capabilities include known and suspected economic, technical, physical, and military abilities. [redacted]

[redacted]

~~(C)~~ With the indicator list being a tool for warning, the scale for warning is the norm, the target's normal level of activity. I&W analysts use indicator lists to determine if current activities in their area of concern deviate significant from the normal level of activities. [redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~(S-CCO)~~ To develop indicators from historical data, I&W analysts study the involvement of specific targets in military action.

Indicators based on normal activity are developed from the actions that lead up to the preparations for deployment of forces for an invasion or exercises, as well as from the actions observed during those events.

~~(S-CCO)~~ Developing indicators from a target's political or military doctrine tells I&W analysts what the target may do to prepare for hostilities.

~~(S-CCO)~~ Sources for indicators include all the major intelligence collectors and sensors employed by the US.

~~(C)~~ The development and correlation of indicators is very important to warning. Indicator lists are developed from collected intelligence and the analysis of a foreign power's actions and doctrine. The sources of indicators are the intelligence collectors and sensors that the US employs in its defense. Indicator lists air I&W analysts in determining the status of a foreign power's military capability that decision-makers need to know in order to make the necessary decisions to protect US interests.

DOCID: 4009856

A Cry for HELP or Does Anyone Here Remember PURPLE?

by [redacted] P.L. 86-36

(U) During the course "Japanese Cipher Devices Through World War II," which was a part of SPICE (the Summer Program in Intensive Cryptologic Education), some questions arose which neither the teacher nor students could answer. Two of those questions will be posed in this article, with the promise of future articles with additional questions and explanations of the systems involved.

~~(C)~~ There were two goals in the course. The first was to study the history and solution of Japanese cipher systems before and during World War II. The second was to try to solve the Japanese systems with our modern techniques.

~~(S)~~ The students accepted the challenge to treat a set of World War II messages as unknown cipher. The results of the statistical tests were not what the teacher (the author of this piece) had expected to see, based on her research of how the systems worked. The problem was that the messages which she had pulled from the Cryptologic Collection and typed onto the system did not all possess the properties that had originally made solution of the systems possible. It was necessary to tell the students what was supposed to have happened and then try to figure out why the runs had come out as they did.

(U) The class watched the tapes of Frank Rowlett's talk on the solution of RED and

PURPLE, and of Frank Raven's recent talk in the Friedman Auditorium. These analysts imparted the excitement in achieving the original solution, but students and teacher felt that both men underemphasized the difficulty of this achievement.

~~(C)~~ The material in the Cryptologic Collection on RED was understandable and the students were able to solve the messages, given how the systems worked. It was not clear how the original analysts constructed the device from the cipher solution but one student wrote a program simulating RED motion.

~~(S)~~ The material on PURPLE was difficult and the explanations of the system's solution left certain questions unanswered. The first concerned the initial analysis of the system. The World War II analysts had the plain text for parts of 15 messages. In an intensive cryptanalytic study of these messages they found that the number of repetitions was much smaller than would be expected at random. Repetitions of three or four letters never represented the same plaintext letters. Conversely, two identical plaintext letters in sequence could never be represented by two identical ciphertext letter. Friedman writes, "This phenomenon turns out to be the undoing of the machine." [1] However, he does not explain how the lack of repetitions was exploited.

~~(S)~~ The second question concerns the solution of the system. The original analysts felt that they needed 20 to 25 messages with the same indicator on the same day to solve the system. They never found more than two messages that satisfied these conditions. Another idea was to convert messages with the same indicator, but on different days, to a common base. Out of a thousand messages, six were located with the indicator 59173. When reduced to a common base, these six messages became the key to the breaking of PURPLE. Friedman describes the process as "too difficult to explain here." [2]

~~(S)~~ The two unanswered questions are:

1. How did the analysts use the repression of repetitions in solving PURPLE? and

2. How were the messages with the same indicators, but on different days, reduced to a common base?

~~(S)~~ Further questions can be posed in an article which describes the system. In addition, there is a course in the Cryptologic Collection on PURPLE with explanations and assignments. Though most of the explanations were understandable and the answers to the problems in the assignments were provided, something was lacking because the problems did not seem solvable.

~~(C)~~ Is there anyone at the Agency who worked with PURPLE or who once studied the PURPLE course material? Would anyone like to help resolve these puzzles? Could modern techniques solve the systems today? Please contact [redacted] B63, on extension 4871s. P.L. 86-36

1. Friedman, William, "Preliminary History of the Solution of the B Machine," p. 4.

2. Ibid., p. 5.

WE ARE ALWAYS LOOKING FOR

ARTICLES, COMMENTS, NOTES, LETTERS,

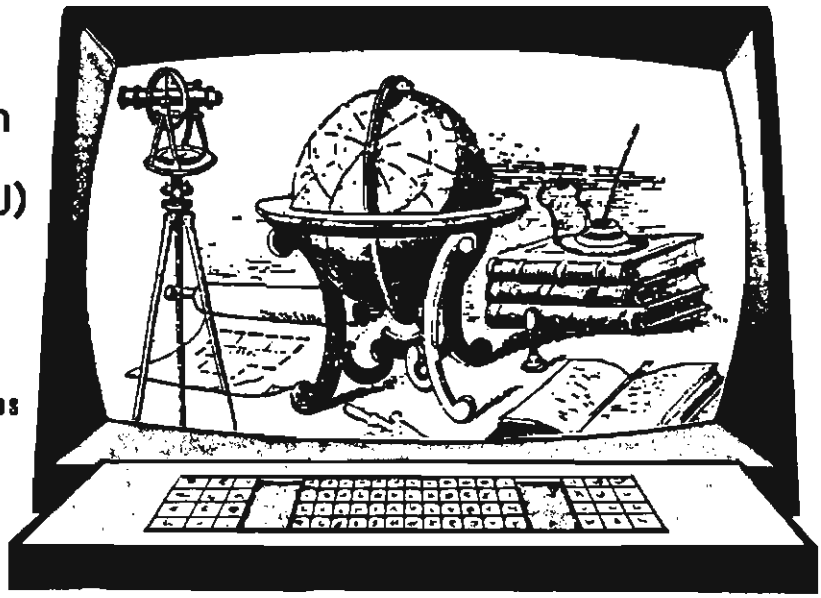
THAT WOULD BE OF INTEREST TO OUR READERS

DOCID: 4009856

Going *On-Line* With Information Aids (U)

by Jack Gurin, (R831)

Systems Research Labs



That we are in the information age is no longer debatable. For some years now we have been aware of the impressive advances being made in the business of acquiring, storing, retrieving, and displaying information. We are also assured that there is much more to come--smaller, better, faster--and we have no reason to question that claim. It is exciting to contemplate the possibilities, and not a little scary. Even if we wished to slow down or stop the process, there would be no way to do it, and so we speed along with the current.

Of course it is the computer that is in the middle of the information explosion, and it is the computer that enables us to sit at home or in an office and be the recipient of all sorts of facts and figures, provided that we have subscribed to the appropriate service. If we really wanted to, we could see the entire daily New York Times on our screen by 0800 each morning, but there are better ways to read the paper. On-line information services crisscross the country and there seems to be no limit in the kinds of information that may be provided. Too busy to read all the magazines and journals affecting your area of interest? You can subscribe to a service that summarizes all the information for you. Reluctant to plow through all the stock market information in the papers to see how your investments are doing? You can be served precisely the information you need on a regular basis. The on-line services cater primarily to businesses, as one would expect, but the range of information available in all fields is impressive and it is growing all the time.

It is in the cards that the computer will be asked to provide more and more answers to questions asked in the course of SIGINT analysis, and yet there remain many questions regarding the advantages of on-line versus off-line information support. It isn't easy to visualize a familiar operation like looking up a word, a person's name, a place name or an abbreviation without the comforting reassurance of dictionaries, working aids, gazetteers, and other friendly reference works. It will take heavy-duty convincing to get some people to agree to give away their books and rely instead on the flickering images of that close relative of the medium that brings us "Charlie's Angels."

We need to discover just how valuable on-line information would be for SIGINT analytic processes. Speculation will take us only so far, and we need to know for sure how useful it would be to have answers to our questions provided on the screen. Would it take less time? Would the answers be more accurate and complete than if one proceeded in the traditional way? What would this do for SIGINT productivity? Output quality? How would the individual transcriber or analyst react? How valuable would it be for the linguist to be able to look up a the meaning of a word when he does not know either the beginning or the ending? What about place-names and maps being displayed on the screen? Or charts and diagrams? In our planning for large-scale systems of the future, what should our requirements be for on-line information support? What will it do for (or to) the individual sitting in the middle of the system?

DOCID: 4009856

The answers to these and related questions are being sought by KEPLER, the laboratory in R83 that is working on a design for the ideal transcriber work station. In April and May of 1982 a test was conducted in operational spaces, employing two transcriber teams in A67 who continued to work on their regular traffic. A group of six information aids, some of them the most frequently used by transcribers, were made available in computer-retrievable form to the transcription teams. Experimental equipment was brought in to display answers to their queries on-line, and while one team used the experimental positions, the other operated in normal fashion. Periodically the teams reversed roles and all the while trained observers were watching the operation and collecting data to permit an evaluation of on-line aids in the transcription process.

It became apparent almost from the outset that the experimental on-line information aid system, nicknamed WALDO, would quickly become a favorite reference device for most of the transcribers participating in the test. WALDO, to the transcriber, was a second DD7000T screen that was controlled by the same keyboard that was used for creating transcripts. It was connected to a minicomputer that contained the information aids. The transcriber could and did ignore all of the experimental equipment but the second screen. The retrieval system was designed to be attractive and easy to use, and that WALDO was a most welcome tool is evident from comments made by the transcribers in their End-of-Test Questionnaires:

√ "Easier and faster than paging through hardcopy."

√ "String-search allows scribe to look up words even when portions are unknown--a big help."

√ "Fun to use."

√ "Caused scribe to look up more entries, thereby improving quality of work."

√ "Dread going back to STEPSTONE alone."

√ "Makes STEPSTONE look primitive in comparison."

√ "It would be great if we could incorporate WALDO/KEPLER into our permanent operations for the whole branch."

√ "I hope this helps get us all on-line working aids because I feel the time we save using these aids is time we can use to concentrate on our ever-increasing workload. I know I've said this before, but I just can't get over how convenient and easy this on-line system is. If all the working aids that we use with any frequency are put in WALDO, then we'd have that much more space in our desk."

√ "With the ORTHO on-line, I find myself using it at least 10 times more than if I had to drag out that book for every jumble of sounds I heard. It is easier with WALDO to try the various configurations of letters to see if a legit word turns up. Paging through the orthographic hardcopy was something I unfortunately avoided, which left blanks in my transcripts. But I find myself now filling in more blanks because it's easier to do with the orthographic on-line. I think my work has definitely improved!"

The observers who noted how aids were used during the test found in general that, when an information aid was available on-line in the experimental mode, it was used more frequently than its hardcopy equivalents in the control mode. Also significant was the finding that the average durations of aid use by transcribers tended to be shorter for on-line than for off-line aids. It should be noted that these savings were in worktime per individual query and did not necessarily result in a savings in tape processing time. It is likely that, because it is so much easier and quicker to find answers in on-line aids, many more queries will be made than when only off-line aids are available. This would probably offset some of the savings in time but might do wonders for the quality of the product.

In addition to determining that on-line aids were used more frequently and took less time per query, it was also found that the subject transcribers were unanimous in preferring the on-line version of most WALDO aids to any alternative form.

While the results were far from conclusive in the calculations of the transcription work

factor, there were strong indications that working with on-line aids had reduced transcription time as much as 18 or 19%. In view of the limitations of subject population, targets, and time, however, it is difficult to predict the probable impact of on-line aids on the transcription work factor in other target areas.

In a related but separate subtest, 150 terms were selected randomly to determine how quickly one could look them up using WALDO versus using equivalent hardcopy or microfiche aids. Simulating operational conditions, both experimental and control, the tester kept track of the times it took to look up each of the terms on WALDO and on six off-line aids. He found that on-line retrieval times were generally faster than other times. This finding came as no surprise for those aids that are located away from the work area, in which case the on-line answer could be provided in as little as one seventh of the time. The unique characteristic of on-line files, that of providing the opportunity to look for terms without knowing how they begin and end, was not tested because there was nothing in hardcopy or microfiche with which to compare it.

What happens next? There is little doubt now that on-line information aids are a GOOD THING and should become a standard feature of all workstations. It also seems that the effort and cost involved in preparing aids for on-line retrieval would be, in many cases, quite modest since a surprisingly large proportion of all hardcopy aids are produced through computer word-processing and therefore exist in digitized form. But it will take a commitment on the part of systems planners and managers not only to bring in on-line aids but to follow through, for many of the aids require updating and new ones are waiting to be created. Perhaps what is needed is more evidence that on-line aids pay off handsomely in raising both the quantity and quality of the end product, and proof that transcribers, translators, and analysts would find their work so much more rewarding with on-line information aids that they would be reluctant to leave for other types of employment.

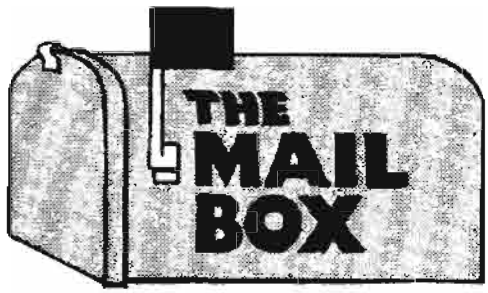
The KEPLER experiment and test was directed toward the needs of transcribers, but the principles and techniques are capable of much broader application. It is characteristic of almost any analytic activity that the practitioner consult reference materials. It also seems reasonable to assume that it would be highly desirable to make the retrieval of the information easier, faster, more timely, and more complete, all likely results from an effective on-line information system.

How did they ever make reservations on the airlines before computers?

SOLUTION TO NSA-CROSTIC No. 44

[redacted] "Language [in the News], CRYPTOLOG, September 1974. P.L. 86-36

"When Archbishop Casaroli, Vatican Secretary of State, came to Warsaw to consult with the Polish Foreign Minister, [he] spoke some Polish...'Let God guard Poland and lead it to great and happy goals,' he said, adding, 'Niech zyje Polska!' ('Long live Poland!')"



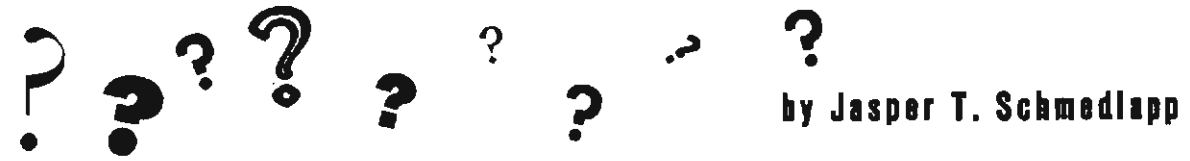
From: djh at ERMELIN
Subject: Cryptolog subscription
To: cryptolg at barlc05
cc: djh

I'm tired of borrowing copies of Cryptolog and would appreciate receiving my own copy. Thanks.

[redacted] P.L. 86-36
R722

DOCID: 4009856

QUESTIONS IN SEARCH OF A PQE (U)



by Jasper T. Schmedlapp

Here are the five questions submitted by the author for the Computer System Analyst certification exam that never saw the light of day at the end of the tunnel. Choose the best answer, break your #2 pencil when done, and then look up.

1. What are the chances of project success, in a matrix management environment?

   a. Slim and none.

   b. It's fine for small projects.

   c. It's fine for large projects.

   d. Actually, it's the individuals assigned that make the difference.

   e. Good, if you stick like glue to 81-2 and 81-3 is your apogee.

2. According to a current book about the agency, how many computers are there in the basement?

   a. Not too many, since the roadway is 100 yards wide.

   b. Enough to decrypt the boss's handwriting.

   c. It's classified, but the main ones are CARRILLON, STARFIRE, LOADSTONE, and WINDHILL.

   d. Just as many as they can possibly fit in, and then some.

   e. One for every man, woman, and child in (pick a county in the state of Maryland).

3. Just what is Computer Programming anyway? It's...

   a. All just 1's and 0's.

   b. An arcane art that Macbeth's witches would have enjoyed.

   c. A way to make a living.

   d. Where a man belongs.

   e. A hell of a lot of fun when we do it, instead of everything else involved.

4. If the program doesn't work, what to do?

   a. Run it again, just to be sure.

   b. Ask the gang in the carpool.

   c. Hope that that case never comes up.

   d. Consider using "GO TOs".

   e. Come back to it tomorrow with a fresh mind.

5. In 1's complement arithmetic, +0 = -1; are the operations "minus" and "nonplused" also equivalent?

   a. Only on the CDC peripheral processor, which has 4000 words of memory.

   b. Yes; but in Burroughs ALGOL, it's much more elegant.

   c. The C language doesn't make this distinction and many others.

   d. Why not try it and see? After all, life is an open-book exam.

   e. No, but be careful for it in your local TELNET command language.

To find the answers, look deep within your heart and pick the first things that float to the top of your head.

DOCID: 4009856

SHELL GAME:

COUNTER by W.E.S.

AJSQUE by [redacted] P14

P.L. 86-36

PWB WHEN by [redacted]

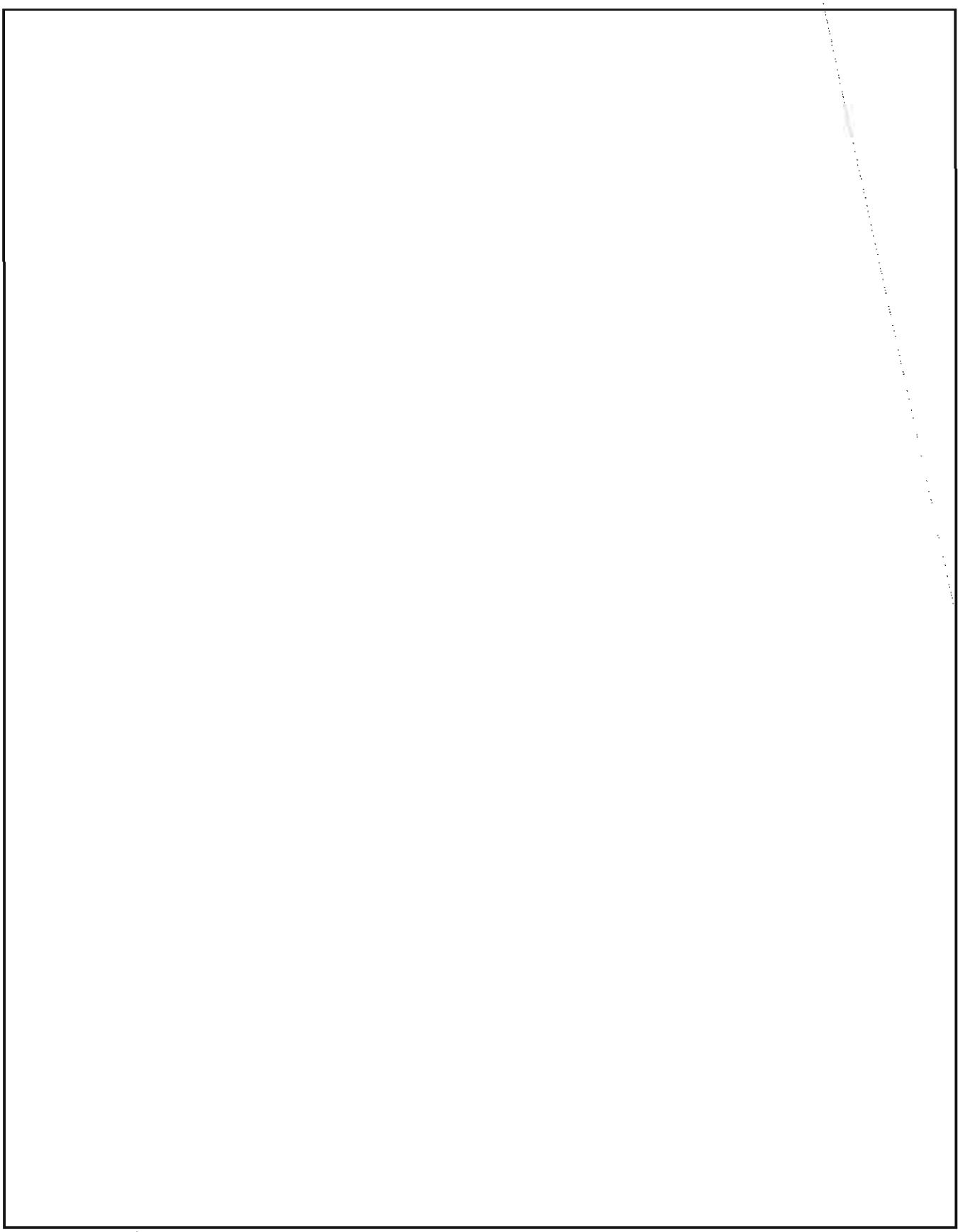
P.L. 86-36
EO 1.4.(c)

(S-CCO) UNIX is not known as a good command language for arithmetic operations. Most sophisticated calculations probably ought to be done by some other means. That doesn't mean, however, that nothing arithmetic can be done in UNIX.

~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36

~~SECRET~~



DOCID: 4009856
EO 1.4.(c)

P.L. 86-36

~~(C-CCO)~~ Reminder:

if you have any old codes or code materials, such as runs or tapes or cards or write-ups, and you're looking for a good home for them, I'll be happy to take them in. [redacted] also accepts such material. His address is T54, SAB 2 Door 3, and he can be reached on x2268s.

[redacted]
P16, x1103s
Bookbreaking and Cryptolinguistics Coordinator

To: Editor, CRYPTOLOG

Dear Ed:

Kudos to [redacted] for his perceptive, albeit scary, series on "SIGINT: 1990." He graphically lays out the challenges facing the SIGINT folks of that era, which is rapidly becoming more and more imminent. The table in the November article displaying the 64 teleservices envisaged by the French CNET study for the year 2000 can set one's mind adrift on a sea of imaginings in the sphere of social relationships, too. For example, a young bachelor of that day might embark on TELESURVEILLANCE to check out the field; or if that fails, there are TELEWANT ADS or TELESHOPPING as prelims to his TELECOUPLE adventure, followed perhaps by TELEGAMES together--and then, sadly, by TELESWAP (if ardor cools)... The TELEpossibilities boggle the mind.

[redacted] P13

P.L. 86-36

DOCID: 4009856

KRYPTOS Society:

Distinguished Members

and New Seal(U)

P.L. 86-36

by [redacted] S14

At the 14 September 1982 meeting of the KRYPTOS Society, President [redacted] announced the names of the first 14 Distinguished Members of the Society. The initial group was selected from a list of over 100 candidates. Selection criteria were based solely on cryptanalytic skills and achievements. To be eligible for consideration, a candidate must have retired since 1935 from the "official cryptanalytic community" in the United States, Great Britain, Australia, Canada, and New Zealand. The following were selected:

~~(S-CCO)~~

[redacted]
William Blankinship
[redacted]
Prescott Currier
[redacted]
William F. Friedman
Hugh Gingerich
Solomon Kullback
Francis ("Ted") Leahy
[redacted]
William Lutwiniak
Francis Raven
Abraham Sinkov
John Tiltman
[redacted]

P.L. 86-36

(U) In the future the KRYPTOS Society will publish a paper describing the achievements of these Distinguished Members.

(U) At the same meeting [redacted] Chairman of the Logo and Seal Committee, presented the seal of the Society, which is based on the Gordian Knot. The following is Joe's version of the story:

(U) Once upon a time in the ancient kingdom of Phrygia, the government had many problems, the most immediate of which was to choose a new king. So the high officials went to consult the leading local oracle for advice on whom they should select for their king. The oracle gave them the following astonishing advice: "Choose the very next person who approaches the Temple of Zeus in a wagon. Then all will go well for Phrygia." (History does not record how much the oracle was paid for this advice.)

(U) Along come a country farmer named Gordius and his wife, driving their oxcart into town and they pull up in front of the Temple. You can imagine Gordius' surprise when he is surrounded by government officials and other well-wishers heralding him as king. Well, Gordius was quite thrilled, to say the least, and to show his gratitude he tied his oxen to the Temple with a beautiful and intricate knot. In fact, the knot was so intricate that no one could untie it. Years went by, and still no one was able to untie it. Centuries went by, and still no one could untie it, so that the legend grew that that the knot could be unraveled only by the one who was to be the conqueror of Asia. According to the story, when Alexander the Great invaded Phrygia he was shown the Gordian Knot. He took out his sword and--in true, pragmatic, cryptanalytic fashion--slashed it apart.

(U) [redacted] was the one who suggested the Gordian Knot as the theme for the Kryptos Society seal. He also suggested that it could be portrayed in the form of a shield with three important elements depicted on it: the knot, a sword, and a helmet. The knot depicts the cryptanalytic problem; the sword depicts the tools of the cryptanalyst; and the helmet symbolizes the cryptanalyst--the helmet being a symbol of anonymity. The seal that we see today incorporates those three elements and adds the word KRYPTOS (Greek for "hidden" or "secret") across the top in Greek letters. The shield was designed in its present form by [redacted] of L23 and professionally rendered by [redacted] of L2.

P.L. 86-36

DOCID: 4009856

m#4Jb:A7wkSEs ???

XeH8|5gP2:K% ???

6I|mUDu&s-40 ???

PASSWORDS(U)

by [redacted] P13

P.L. 86-36

While reading [redacted] excellent article in the October issue of CRYPTOLOG (p. 6), I could not help becoming more and more unhappy under my "human factors hat." The article describes a recent compromise of a password file in one of our computer systems. It shows that the passwords, even though encrypted in the file, could easily be recovered by guesswork. It advises users to cooperate with the intent of protecting passwords by choosing passwords that "will not fall out through a simple analysis effort." In order to make passwords harder to guess, [redacted] offers advice I will paraphrase as follows:

- the longer the passwords are, the better;
- increase the alphabet size, for example, by mixing upper and lower case characters, numbers, and punctuation.

This is all good advice, when we are maximizing only one value: that of making passwords as secure as possible. Unfortunately, the average computer user has multiple goals in his use of a computer system, only one of which is prevention of unauthorized access. All of us at NSA are all too aware of the crucial importance of security. Passwords are still a pain in the neck to most of us, constituting one more obstacle between us and our work at the terminal. We know they are necessary, but we also know that our lives are a lot easier if our password is

- short,
- easy to type, and
- easy to remember.

P.L. 86-36

Alas, we see that [redacted] good advice flies directly in the face of normal human factors design guidelines: to make passwords hard for potential trespassers to guess, we must make them even harder for ourselves to remember and type correctly! [redacted] notes rather plaintively that "there is not a single upper case character" in the 107 passwords recovered from the compromised list by guessing. There are good reasons for that absence of upper case characters, from the user's point of view:

The author's address for PLATFORM mail is mary at mycroft.

first, it's hard to recall which letter or letters were upper, and which were lower case, especially in the meaningless nonsense-words (e.g., "vkjrd") that are recommended as the best passwords;

second, the shift key is a great error-maker in all typing, since it forces you to use two keys where one would do. All this guarantees that, if you create a password like "vKJ.r-dX", you will probably have to type it over several times before you get it right.

Computer Security folks may be saying "tough!" with little sympathy, since they are interested only in security. I can't quite look at it that way. I think we have to remember that productivity, efficient accomplishment of our jobs, and good morale are also important values we need to maximize.

I don't know what we can do about this conflict of interest between computer security requirements and user friendliness. I can't help wondering why user identifications (initials, organization) couldn't be enough to establish the necessary access restrictions and permissions when tied to user profiles or tables stored in the system software. Why do we need to depend on passwords at all? Might there not be other ways to enforce security at less cost to users?

I suspect that this is only one of many similar conflicts in our software, some far more expensive to users than unlearnable, untypable passwords. My intention here is just to point out the conflict. I am sure some of you could report similar situations, where file security, access restrictions, etc., create real problems for users in the way they are implemented. Those readers in the Computer Security business will doubtless have plenty to say on the other side of the issue. At any rate, I invite readers to send in their ideas on the topic of User Friendliness and (or versus, if you prefer) Computer Security to me [redacted] for inclusion in a future issue of the SIG/Human Factors Technical Notes and/or CRYPTOLOG. (Ed Note: what about using two passwords and letting the system combine them in some periodically changing way?)

P.L. 86-36

HUMAN FACTORS TECHNICAL NOTES

The Computer and Information Sciences Institute's Special Interest Group on Human Factors, chaired by [redacted] publishes a series of technical notes covering a wide range of topics of interest to anyone who wants to keep up with the growing field of human factors. The editor of the notes is [redacted] whose name and articles you have been seeing on these pages.

P.L. 86-36

Some of the articles in the Human Factors Technical Notes have been republished here in CRYPTOLOG, but if you want to keep up with the latest news, you should call Mary on x8845s (or send her a note via PLATFORM using the address 'mary at mycroft') and have your name placed on her mailing list.

The most recent issue contains reviews and comments about recent articles and papers, including:

- Ergonomics of Visual Display Terminals
- Human Factors Standards for Terminals
- Workplace Design
- Windowing vs. Scrolling on a Display Terminal
- Experiments with Terminals and Eyestrain
- Why Alphabetic Keyboards are not easy to use
- Furniture and Posture Problems
- Modelling Computer Data Entry
- Structured Menus

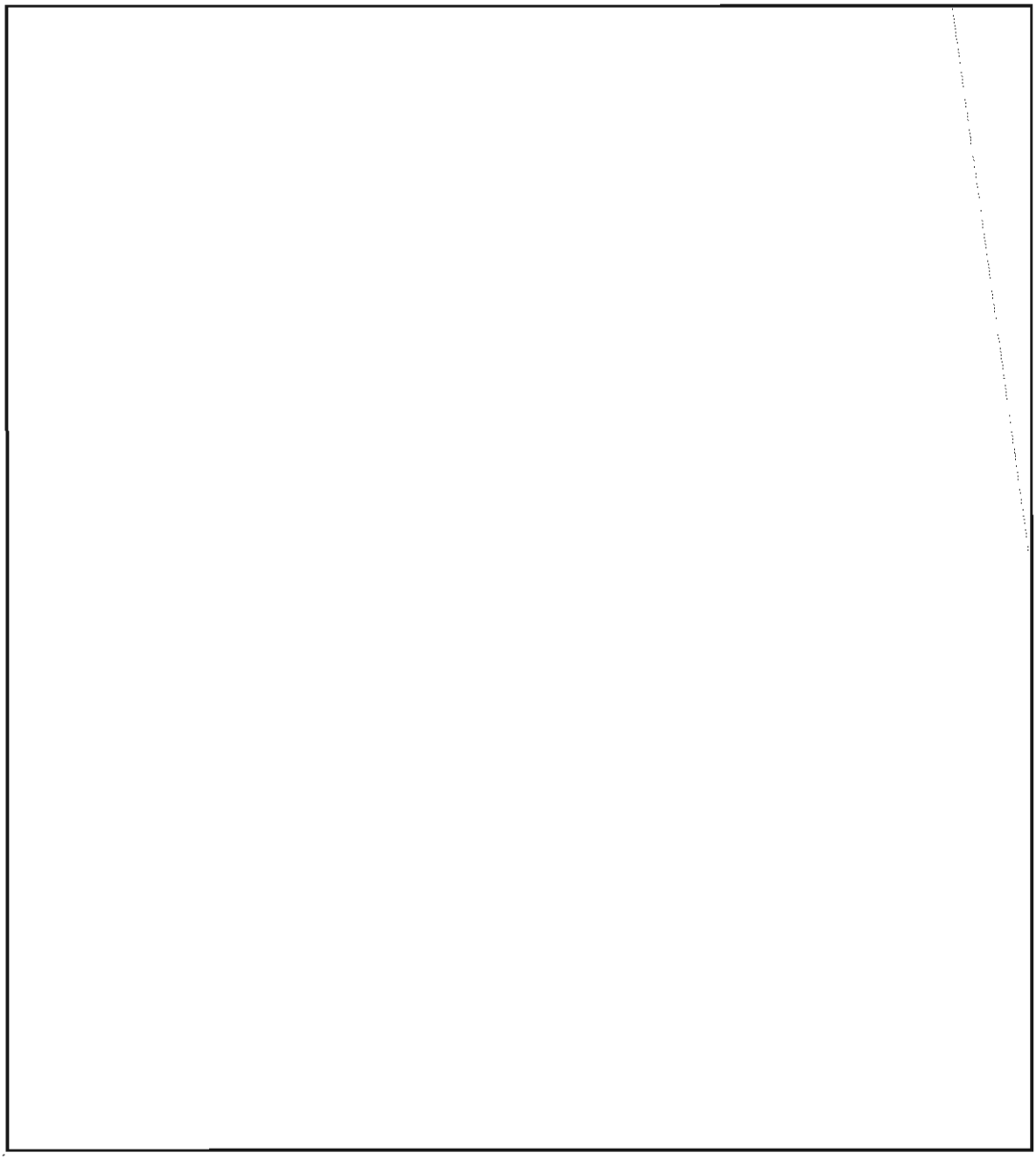
~~CONFIDENTIAL~~

EO 1.4.(c)
P.L. 86-36

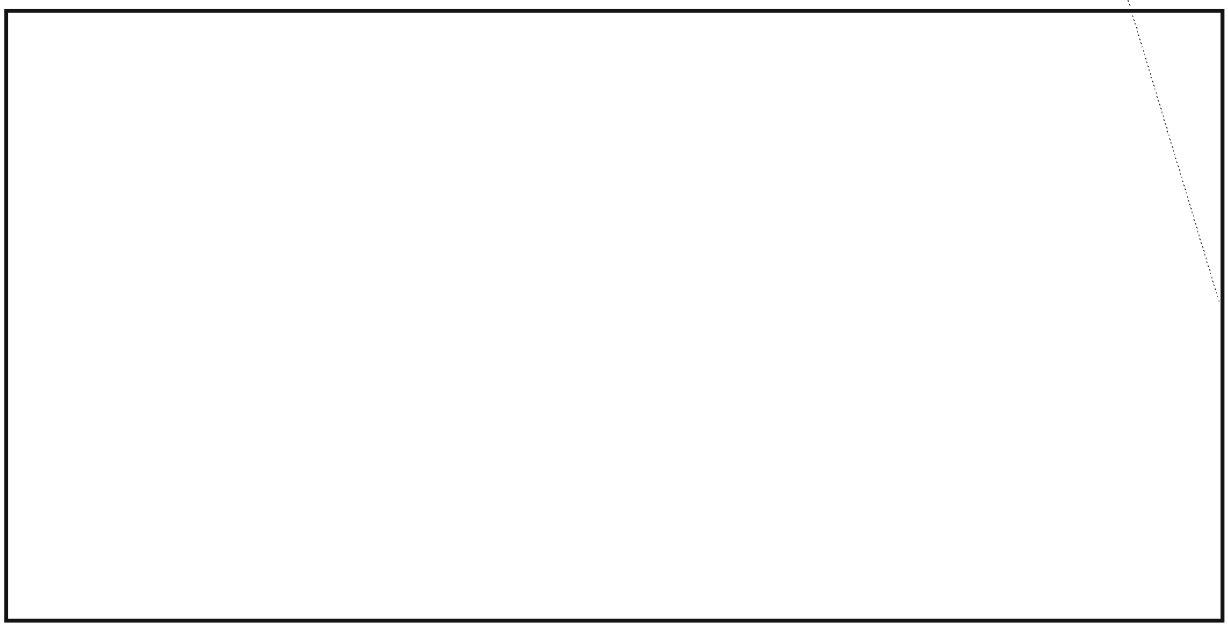
NSA·CROSTIC No. 45

BY REED DAWSON (Retired)

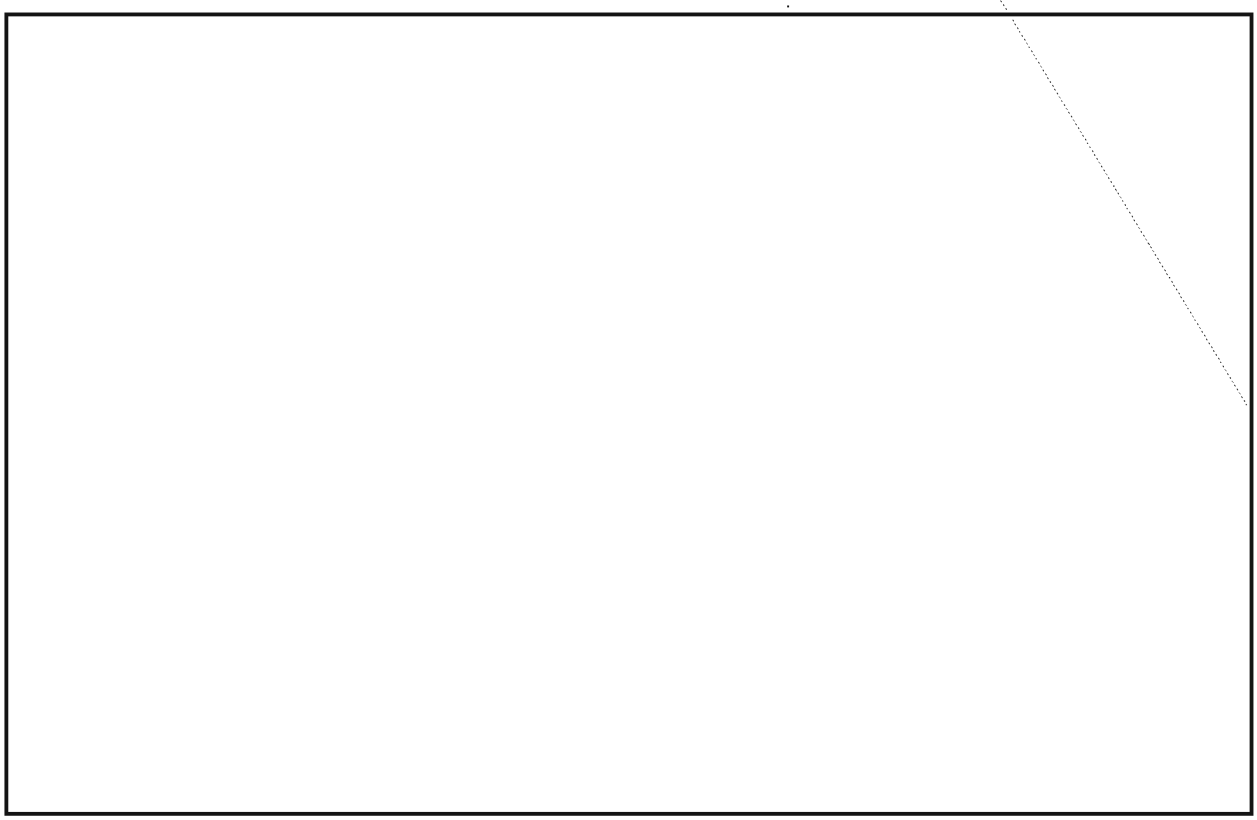
NOTE: The text of the quotation is classified CONFIDENTIAL - HVCCO.



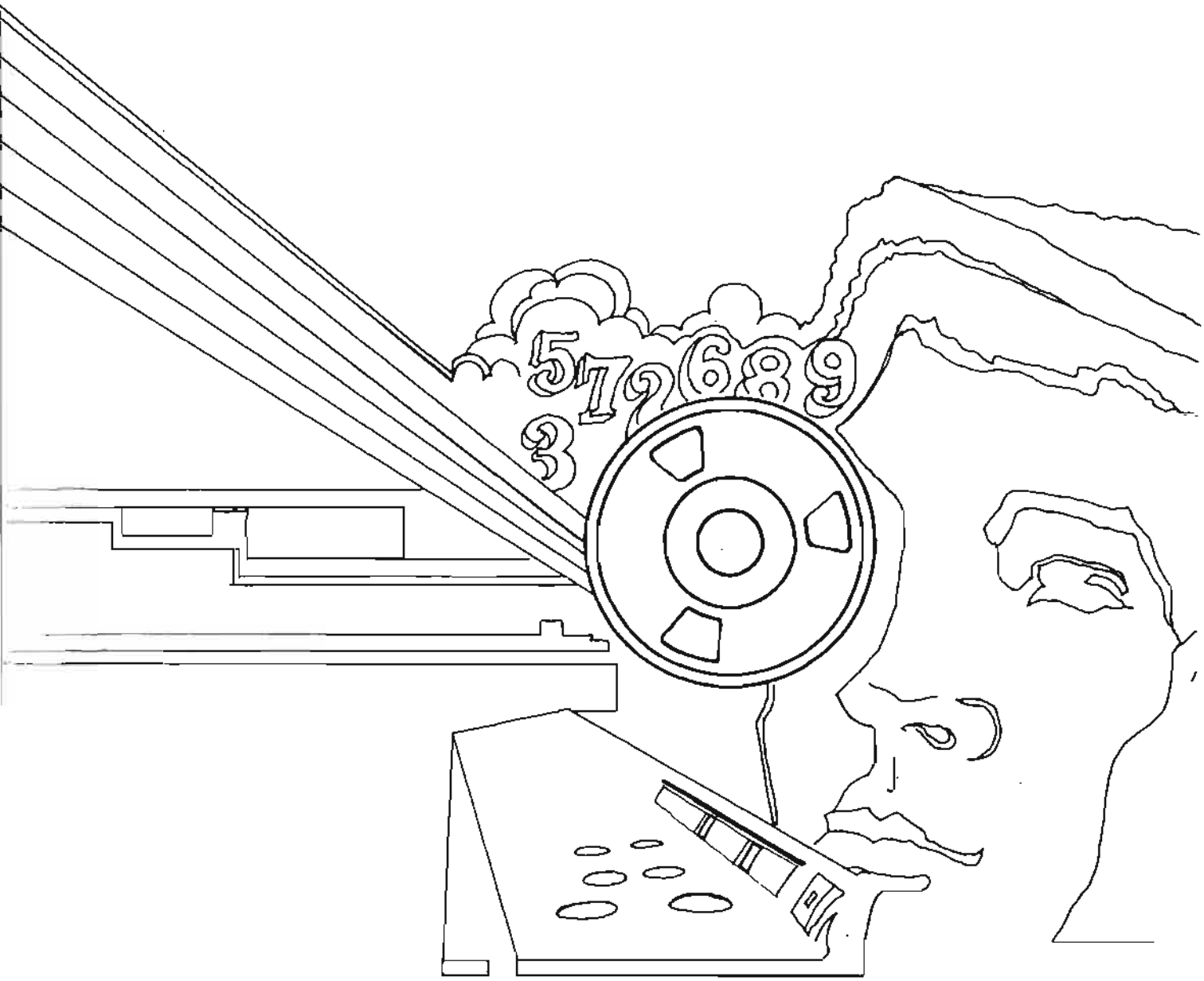
EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36



~~TOP SECRET~~



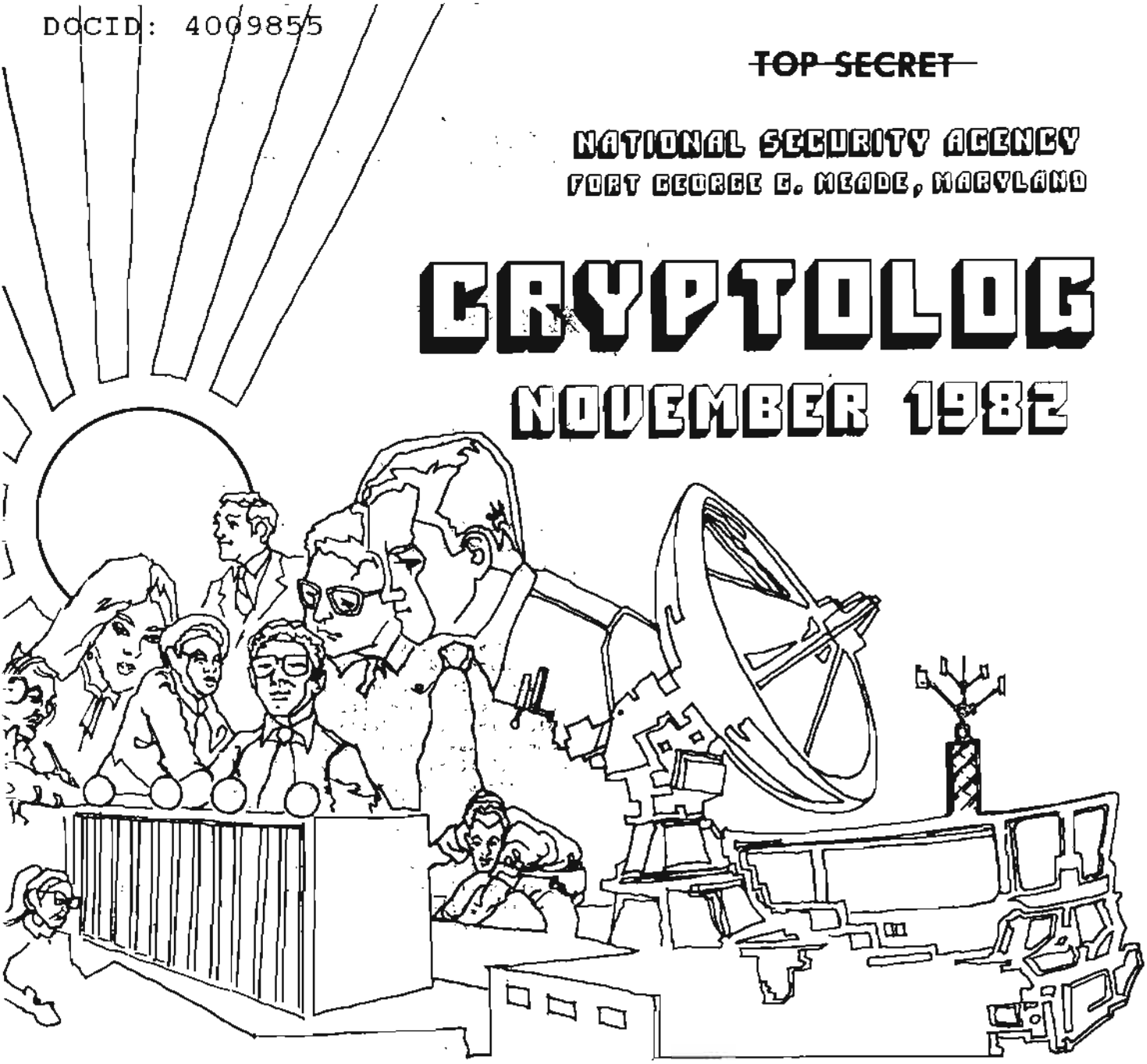
DOCID: 4009855

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

NOVEMBER 1982



P.L. 86-36

CENTRAL RESEARCH AND THE PAPER BLOB (U)..... [redacted] 1
HOW DO PEOPLE ORGANIZE COOPERATIVE WORK? (U)... [redacted] 4
COMSEC CHALLENGES (U)..... [redacted] 7
NSA-CROSTIC (U).....David H. Williams.....12
THE COSTS OF MUDDLING THROUGH (U).....Robert E. Gould.....14
AN OLD TIMER IS ONE WHO...(U).....W.P. Meyer.....17
SIGINT: 1990, Part Three (U)..... [redacted] 18
MAIL BOX (U).....28

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Not Releasable to Contractors~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009855

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. IX, No. 11 NOVEMBER 1982

PUBLISHER [redacted]

BOARD OF EDITORS

Editor..... [redacted] (8322s)
Asst. Editor..... [redacted] (1103s)
Production..... [redacted] (3369s)

Collection..... [redacted] (8555s)
Cryptanalysis..... [redacted] (5311s)
Cryptolinguistics... [redacted] (1103s)
Information Science. [redacted] (5711s)
Language..... [redacted] (8161s)
Machine Support. [redacted] (4681s)
Mathematics..... [redacted] (8518s)
Puzzles.....David H. Williams (1103s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Don Taurone (3573s)

For subscriptions
send name and organization

to: CRYPTOLOG, P1
or call [redacted] 3369s

To submit articles or letters
via PLATFORM mail, send to

cryptolg at barlc05
(bar-one-c-zero-five)
(note: no '0' in 'log')

Contents of Cryptolog should not be reproduced or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

Editorial

Some of the skill areas in the agency have no obvious counterparts in the outside world. For example, traffic analysis is not really very similar to any organized skill group in the business or academic world. (One of the old timers used to claim that traffic analysis was, in fact, quite similar to archaeology--both in techniques and age of material under study.)

Other skill areas, such as language and mathematics, do have obvious parallels in the outside world. Over the years, people in these fields have been at some pains to explain that cryptologic linguistic work, for example, was really not the same as other "outside" linguistic work. Their arguments have been persistent and persuasive.

P.L. 86-36

So it is rather remarkable that one of our larger skill areas, computer science, seems relatively silent on this point. At least, we do not hear the point made very often that there is anything unique about a "cryptologic computer scientist."

Perhaps the computer science people in the agency do not perceive themselves as distinct from their brethren in the outside world. Or perhaps we have not been listening to the right people.

CENTRAL RESEARCH AND THE PAPER BLOB (U)

by [redacted] T5

P.L. 86-36

(U) You've all seen it: the TV commercial in which a giant wad of paper rolls along the hallowed halls of a large company, cornering busy executives in their offices, burying them and their desks under mounds of seemingly important documents. Although this is only an advertisement, there are many at NSA who can readily identify with the situation, perhaps none more easily than those who grapple daily with the processing of this paper blob in T5, Information Resources Management.

MYTHS AND FUNCTIONS

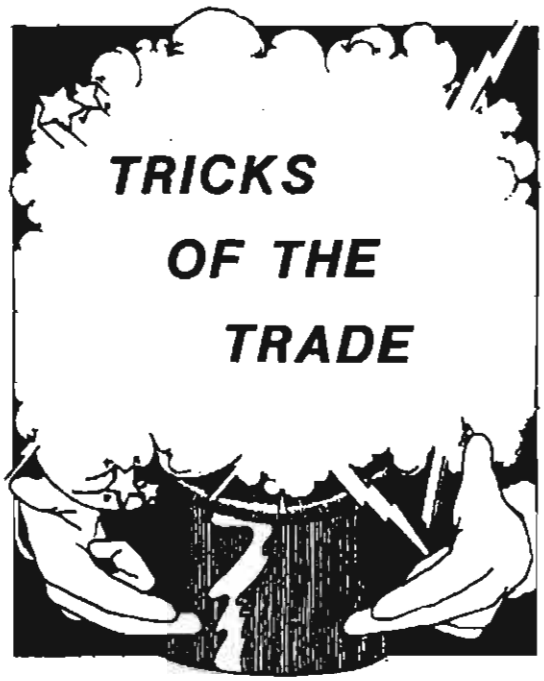
~~(POUO)~~ In particular, Central Research (T5211) is responsible for maintaining and consulting a plethora of information to ensure that the proper people somehow receive the correct information at the right moment and within a reasonable period of time. Central Research is tasked with using whatever sources are available to respond to requests from any person in any element in the Agency (and sometimes beyond) as quickly as possible. T5211 receives approximately 50 to 75 questions per day, handled by 11 full-time researchers. Queries range from the specific to the ultra-vague, from the sublime to the ridiculous. So, when some refer to Central Research as "the place where they find needles in haystacks," they couldn't be more correct.

(U) The team of experienced researchers who comprise Central Research (the old "C-Ref") are not, contrary to popular belief, "little old ladies in tennis shoes." Neither are these researchers part of the T51 Main Library, although physically located adjacent to its special book collection to share resources.

(U) The T5211 branch, besides performing research, also processes all-source (classified and unclassified, controlled and open-source) information for inclusion in automated and hardcopy information files. These 15 information specialists include analysts, technicians, and analytic aides. Most have earned college degrees, some offer foreign-language proficiencies or even translating experience, others are data base experts, two are graduates of the Information Science Intern program, and many provide invaluable knowledge acquired only through years of experience.

THE OTHER GLUT

(U) As the information explosion (or "information glut," as some prefer to call it) continues to grow, so does the rate at which new tools are designed to manage this information. It is the responsibility of Central Research and its staff to keep pace with the technology that attempts to keep pace with the information glut. This includes periodic evaluation and reevaluation of hardcopy files for possible transformation or incorporation into machine files, acquiring the relative skills necessary to effectively employ commercial and traditional search tools, and undertaking the training needed to perform as information professionals in a rapidly-changing environment.



~~(C)~~ Among the tools employed by Central Researchers in their quest for "the needle in a haystack" are:

- the reference books of the Main Library's special collection,
- government manuals and working aids,
- hardcopy files of worldwide diplomatic information,
- hardcopy collections of international organization documentation (especially the United Nations),
- worldwide treaties and conferences files,
- press clippings of current events,
- the SOLIS (SIGINT On-Line Information System) and WEEDER (State Department Cables) automated systems,
- [redacted]
- The T5 Calendar of Worldwide Holidays and Observances (prepared by T5211 and maintained on T5's UNIX-based [redacted] system),
- [redacted]
- liaison officers at other government agencies and departments,

[redacted]

This variety of sources (a Paper Blob in itself), when employed in the proper combination by those familiar with the structure and capabilities of each source, usually lead the Central Researcher to that crucial bit of information that can make or break the value of an intelligence report.

MACHINE MANIA

(U) Among all the sources listed above, the commercial data bases are probably the most talked-about and the least known-about of Central Research's tools. While some mistakenly think of them as "answer-alls," they are not. Unmistakably valuable they are. Four of these leased systems: Lockheed's DIALOG, System Development Corporation's ORBIT, Bibliographic Retrieval Service (BRS), and the New York Times Information System (NYTIS) are accessed on-line over non-secure telephone connections via commercial networks (TELENET, TYMNET, and UNINET) through a Texas Instrument (TI) 1200 baud terminal/printer.

(U) The DIALOG system alone, with its more than 150 separate files covering almost any subject imaginable, offers NSA access to more than 750,000 sources (including books, magazine articles, journals, conference papers, and non-print material). Although these files range in access fees from $10-$300 per connect-hour depending on the file, they are determined to be cost-efficient when compared with the exorbitant costs involved in scanning, processing, storing, and consulting information from those 750,000 sources.

(U) The BRS and ORBIT systems complement the DIALOG system, offering some unique files, some duplicates, and some gap-filling date ranges. These three systems provide the searcher with bibliographic information and usually an abstract (summary) of the entire article or paper. (The full text of the article or paper can then be acquired by the client through the Main Library). P.L. 86-36

(U) NYTIS, with its eight separate data bases/files, provides mostly items of news interest, especially through the Information Banks I and II and the full-text New York Times On-Line (NYTOL). Except for NYTOL, the searcher retrieves bibliographic citations to major sources. (The client can then access the full text of the article with the aid of the Main Library's personnel.) P.L. 86-36 EO 1.4.(c)

DOCID: 4009855

THE NEXIS CONNECTION

(U) The fifth of Central Research's commercial information data bases is produced by Mead Data Central of Ohio. Also accessed via a non-secure (but dedicated) telephone connection, NEXIS provides access to the full text of major foreign and domestic newspapers, magazines, press wires, and newsletters. Originally designed for busy executives, the system offers logical source hierarchy and can be called "user-friendly," judging by the tone of its on-line tutorials, step-by-step instructions, and brightly-colored keyboard. Beyond its full-text capabilities, NEXIS also offers KWIC (keyword-in-context) scanning, segment searches (including references to graphics), and bibliographic citations displayed on the attached CRT (cathode ray tube) screen or printed off at a 2400-baud rate.

(U) The most expensive of the five systems, NEXIS is worth its weight in gold. As Mead Data continues to add new sources to NEXIS (including APOLIT, a new Associated Press Political Service), and expand cumulative date ranges (already seven years of full text on-line for Aviation Week and Space Technology and five years of the Washington Post), the cost savings on subscriptions, time delays, processing, scanning, storing, and searching are inestimable.

OVER THE RAINBOW

(U) While Central Research and the information world expand their horizons, new applications of today's technology are considered and evaluated. Although seemingly costly at the outset, (contracts, studies, equipment, training, etc.), the long-range benefits of these new approaches to information management are actually cost-efficient and long-term. Many of these innovations can be applied directly to the commercial data bases or other automated information systems. They range from simple peripherals like CRT's, faster printers, and improved telephone communications to more complicated concepts like data downloading, on-line data base management systems (DBMS), and universal query language translators. (The typical Central Researcher today is fluent in more than 10 separate query languages!)

(U) Attaching a personal computer to the commercial data base terminals could become a reality in the near future. Many government agencies and most research organizations in the private sector already employ such technology. The implications of this advancement are many. For example, the ability to translate a multi-step logon/logoff procedure into a single keystroke on the attached personal computer saves money and alleviates analyst frustration with what can become an aggravating and time-consuming step. The ability to store queries and profiles of major interest to Agency elements and run them periodically without the usual charges incurred would also be well-worth the initial investment.

(U) Probably the single most important feature involves data downloading, or writing off search results onto an output medium of the personal computer (most likely diskettes), for storage, retrieval, and scanning later. In Central Research this could be most beneficial, as the current practice has researchers determining the usefulness of retrieved information based on their own possibly limited knowledge of a particular subject. The future sees a requestor scanning his or her own search results to determine their worth or relevance and to discover related topics.

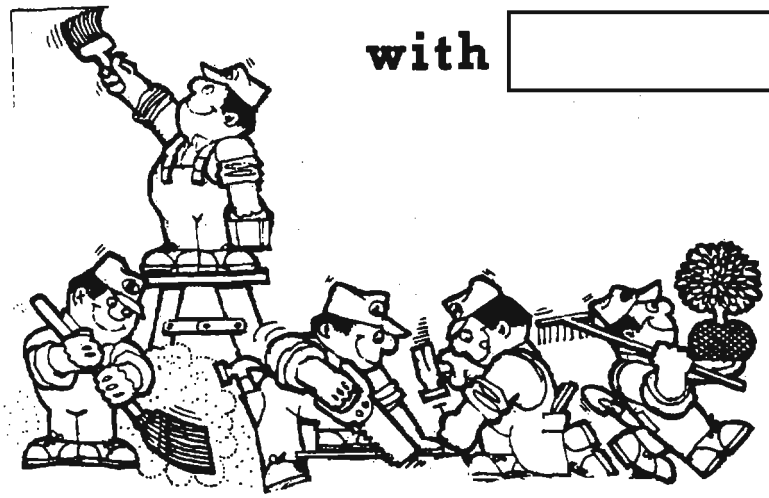
AND THE BEAT GOES ON...

(U) The list of applicable technology goes on and on. It is impossible to keep pace with all of the daily developments in this field, and unrealistic to try to "catch up" with what has already passed NSA by in the world of information management. The much-needed trend is to develop a staff of highly skilled professionals flexible enough to adjust to today's changing technology, as they take their place in a world increasingly dependent on information.

(U) In tapping all the above-mentioned resources (automated, hardcopy, and human) and by applying new technology with flexibility, Central Research can combat the Paper Blob--and win.

HUMAN FACTORS

with [redacted] **P13**



P.L. 86-36

How Do People Organize Work? (U)

We must clearly face the fact that, when we introduce a fully automated system into a set of totally manual or only partially computerized procedures, we are redesigning a large piece of people's behavior. Work takes place within an existing social grouping with a complex set of interactions, customs, and ways of relating to other people and to the jobs at hand. A whole new set of truly fascinating questions is raised for study: questions we need to know a lot more about, and which have rarely, if ever, been clearly addressed in the past. We need to go into the offices whose procedures we propose to automate and really look with open minds and eyes until we understand what the people are doing, how they coordinate and sequence their work, the way they see themselves and their jobs, and where the weak spots and strong spots are in their present procedures. The potential system users and their line managers must be involved from start to finish, and must have a decisive voice in design of the new procedures and workstations. When this approach is followed, the new system becomes "my terminal," rather than an unwelcome affliction imposed on me by the "people upstairs."

For illustrative purposes, think about your own work center in our Agency. Ask yourself the following questions, as if you were a visitor from Mars coming into the office to study the way work is done:

- When you come in in the morning, how do you know what needs to be done?
- If more than one thing needs to be done, how do you decide (or remember) which to do first?
- What about when you come back from lunch?
- What about after a two-week vacation?
- How does your boss (or how do you, if you are the boss) assign work to those on the team?
- Is it easy or hard to communicate information, advice, instructions?
- How do you go about getting information or instructions or tasking, and from whom?

Chances are that most of the answers to these kinds of questions are focused around two prominent classes of events: social (who talks to whom) and physical (presence of logs or papers or formats, location of materials in cabinets or on tables, in racks or folders or drawers or stacks, movement of materials from one location to another in a prearranged sequence). Without these procedures, there would be chaos. One of the crucial questions in office automation concerns our understanding these organizing mechanisms as they

DOCID: 4009855

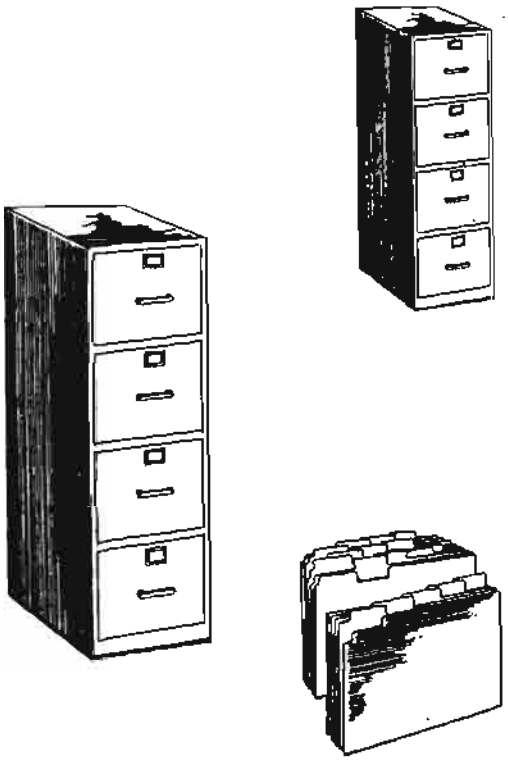
operate in a manual or partially computerized office, and translating them sensitively and intelligently into new but functionally equivalent forms in the totally automated office.

I will use myself as an example to illustrate some of the above ideas. When I come to my work area at the start of the day, the first thing I do is to turn on my terminal. Then I get a cup of coffee and remove the black cloth from my desk, revealing a stack of folders and machine printouts I was working on the day before. They look very messy, but in fact I put them away pretty much in priority order. I usually have about three completely unconnected projects going at once. I pick up the uppermost batch of papers in the stack, look at it, and recognize it by a familiar set of scribbles, smudges, or dog-ears: "Oh, yes! That's Project X; I want to work on that this morning." I set it right beside my terminal. The second and third batches are similarly unpacked from the "mess" and positioned at slightly removed places on my terminal table: Project Y, second priority, at the rear of my table; Project Z, to be done if I have time left over, on top of my terminal. I sit down, log on, and look at my system mail if I have any. Then I call up a file whose name I remember because I assigned it mnemonically to remind me that it pertains to Project X. If I haven't worked on X for a while, and can't remember what I was doing, I may call up "XLOG", which is a journal record of my work on X for each previous day. (I keep a running log of each major project, and its name is always something starting with a mnemonic tag I assign to all files for that project and ending in "log.") Looking at the last paragraph I wrote into the file I am currently writing for Project Y reminds me of what I want to do next, and I begin keying away into my text editor window, calling up other files on a split screen from time to time as needed. SEEING WHAT I WROTE BEFORE, or SEEING A HARD COPY REFERENCE is what triggers my ideas in continuing the project, and determines my next step. In fact, I fear that I would be set back severely if my current file or log were clobbered by the system, or if my pile of papers and folders got burned up in a fire overnight!

Here is another example, drawn from a study I am making of the Agency's Payroll procedures in N41. The two-week payroll cycle is divided up into two different kinds of work: the first week is "Process Week," when time cards are collected and processed, the payrolls are balanced, and checks are issued; the second is "Variation Week," when changes are entered into the payroll records. During "Process Week" all the action is focused on the Time and Attendance Cards. They are gathered, sorted, checked against the records in the the CARILLON system, carefully scrutinized and corrected, and filed away for future reference. Since the physical time card is a legal record of employee attendance, this punched card must remain at the heart of all procedures. Procedures in the Payroll office are highly dependent on close teamwork, meticulous attention to detail, and dedicated care. Batching of the punched cards in separate piles each to be processed in a specific way is a very important part of the procedure. A large table at the front of the office serves as a work staging area, with cards and machine listings laid out in an orderly arrangement.

During "Variation Week" the focus changes to a set of documents which each payroll clerk has collected in a folder. These are official requests and notifications for changes to the employee payroll records. The clerks examine each of these documents, check the requested change against files of machine runs and previous time cards, and make changes using M204 update and retrieval segments on CARILLON. Some of the records, procedures, and determinations they must make are of astonishing complexity and require extensive research, dedicated care, and meticulous documentation. In summarizing my impression of the way the Payroll office works, I would say that everything depends on documents and cards being totally accurate and complete, and being placed in the right location (batch, folder, notebook, file drawer) at the right time.

Let's look at a third example from a very different kind of office: a transcription shop. The transcriber gets tapes to be worked on from a cabinet or drawer where they have been placed, in priority and target order, by a technician or supervisor. He logs the tapes in and out with his initials in a tape log maintained on-line in his STEPSTONE computer system. Once he has a tape, he mounts it on his recorder/reproducer, and works his way through it with the aid of a machine printout that lists the contents and may be annotated by a prescanner to indicate which segments should be transcribed and how detailed the transcript should be. His record of what he is doing consists of the tape reels he has mounted or stored in his desk, with the data about them on the jackets and accompanying printouts, notes he makes on the printouts, and the transcripts he has entered into STEPSTONE. If he stops work in the middle of a tape track, he may dismount the tape just as it is, half on one reel and half on the other, and store the reels in his desk with their rims interlocked; then he can mount them again right where he left off. The supervisor can find out who is doing what by looking at the on-line tape log. As tapes are completed, they are logged out and placed in a specific



file drawer and after they are checked they are placed in another cabinet. In this partially automated office, we can see that physical locations are still quite important. It is interesting, however, to consider what will happen if analog tapes are no longer the form in which work comes to the transcriber, and he gets his work in digital form, stored in computer files. How, then, can we help him and his supervisor keep track of where he is, and of who is doing what?

I suspect that one good way to understand what is going on in an office is to ask this question: What are the key OBJECTS around which the action seems to take place, and where do the workers go to get them?

They may be computer files, and workers may access them at CRT terminals or through listings. They may be hardcopy documents, stored in folders or drawers. They may be punched cards (as in the Payroll process) or magnetic tape reels (as in the transcription shop). In almost every office, however, we can make sense out of the seeming complexity by looking for the small set of basic kinds of OBJECTS that lie at the center of everyone's work.

Another key question is "How does work get organized?" How do workers find out about and keep track of what is next on the agenda?

A third key question is "How do workers coordinate their efforts?" The answers to these last two questions often also involve OBJECTS and LOCATIONS--logs, folders, counters, tables, piles, duty rosters, etc.--as well as meetings, discussions, and other less formal mechanisms. When we attempt to automate a manual or partially automated procedure, we must be certain that we fully understand the objects and locations that are central to the work as the workers see it. If we do not preserve the essentials of these objects, locations, and relationships in the new system, the job will cease to make sense to the workers in the office, and accuracy and productivity will suffer.

I don't want any reader to think I am arguing that office procedures should stay the same, or that the specific ways the work of an office is NOW organized must be preserved in every detail after automation. What I am urging is that we understand how the present system really works so that we can ensure that the new system includes provisions for the coordination, data flow, recordkeeping, and teamwork that the present system depends on. In fact, we should understand the present workings of our office so well that we can design a new system which will IMPROVE on the existing objects and locations that keep the office ticking. If we don't understand the present system, how can we expect to improve on it?

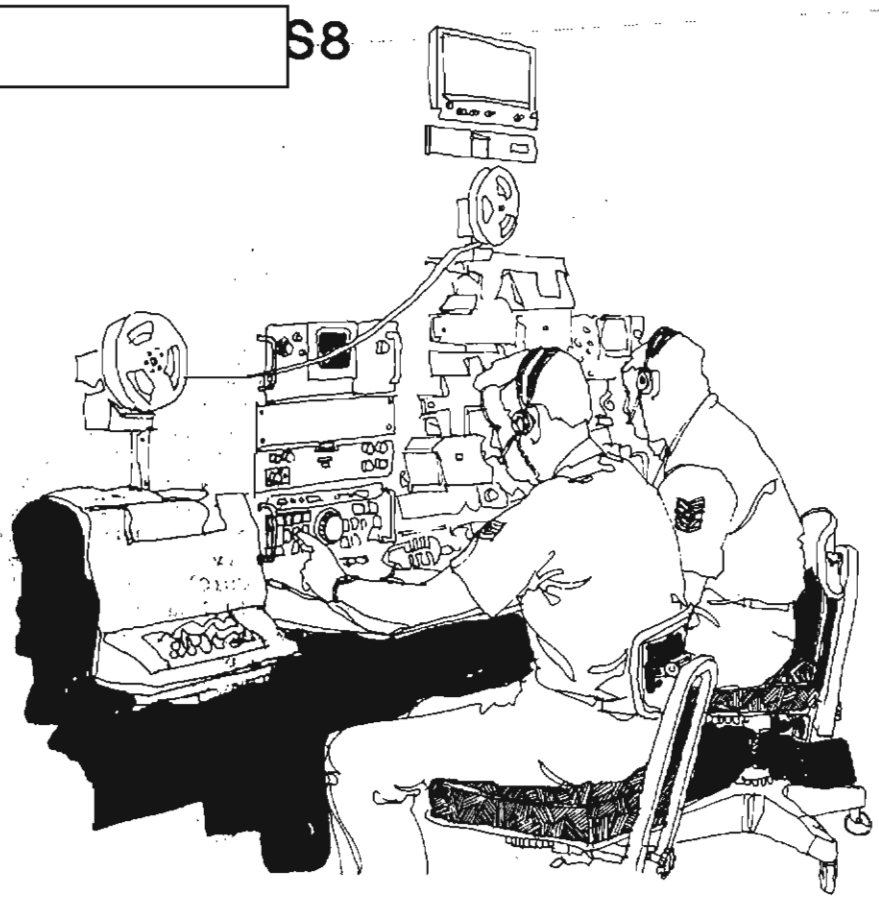
Up until recently, we have never really tried to automate all or most of what goes on in an office. Automation has usually consisted in running a computer program or using machine procedures to carry out scattered tasks at various points in the day's or week's work of the office. If we did a poor job of software design from a human factors point of view, it may have inconvenienced a limited set of users and degraded the performance of one set of tasks. Everything else in the office could still get done, thanks to the routine human context (procedures, habits, conventions regarding familiar OBJECTS and LOCATIONS) that we took for granted as a background to the machine procedures, and independent of them. Now, however, we are considering automating much, if not all, of what everyone in the office does, every day, week in and week out. That will involve changing the informal ways of doing things, and replacing them with automated procedures which we must design. Mistakes in human factors design will now have the potential of seriously disrupting the communication, accountability, and teamwork throughout all the work in an office. We can no longer afford to take for granted or ignore any of the activities that go on in the office and keep things running smoothly.

DOCID: 4009855

COMSEC CHALLENGES (U)

by [redacted] S8

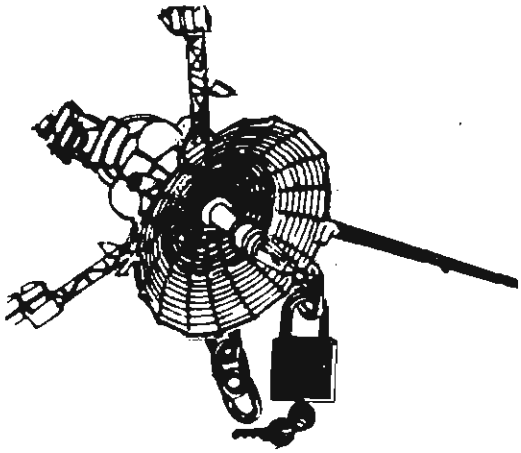
P.L. 86-36



(U) Technology is creating new challenges to COMSEC. Microcomputers, packet-switching, growth in data terminals, etc., are stimulating new requirements and applications for which the line between communications and COMSEC is virtually nonexistent. Traditionally, COMSEC equipment has been viewed by communicators as an individual component--separate from the communications system for which it is intended to provide security. This view is changing--given today's technology. This paper provides an overview of selected technological advances within the past decade that are having a definitive impact on the way COMSEC hardware and software are designed, produced, and implemented into a data communications system.

(C) The single, most significant, recent advance in technology has unquestionably been the introduction of integrated semiconductor devices. It took several decades--through the 1950's--to optimize vacuum tube technology. At about the time that miniature vacuum tube technology was being optimized, the transistor was commercially introduced. Transistor technology was a breakthrough, but there was a lot of skepticism about the transistor's ability to replace the vacuum tube. The skeptics were proved wrong by the rapid growth and application of transistor technology. The tremendous success of the transistor seems to have led to its own self-demise; the transistor stimulated new research which, by the early 1970's, led to the commercial availability of the semiconductor "chip." The chip demonstrated that

DOCID: 4009855



several transistors can be simultaneously produced--each with practically identical characteristics--on a common slab of silicon about one square centimeter in size. During the 1970's the chip's silicon real estate became priceless. New manufacturing processes permitted the production of chips with the equivalent of hundreds of transistors. This large scale integrated (LSI) technology evolved into very large scale integrated (VLSI) technology (10,000 transistors) and we will soon see chips with the equivalent of 100,000 transistors.

(C) Because of their high reliability, low power consumption, and low cost, integrated circuits (ICs) have become readily available and have resulted in a phenomenal growth in data communications while creating numerous challenges for the COMSEC community. Following is a discussion of some specific and very direct results that the chip and its impact on communications technology are having on COMSEC.

(C) Many government agencies provide a data communications service that includes a variety of remote terminals in various locations that are engaged in interactive time-shared dialogues with a host computer. In certain facilities, a remote terminal on which classified work is to be performed must be located within a vaulted room. Such installations are very expensive, entail a lead time on the order of years, and require an allocation of substantial floorspace for the purpose. The electrical connections between many classified terminals and hosts is achieved via protected wireline distribution systems (PWDS); these are very costly and often difficult to implement. The above problems, currently tolerated in many government agencies, are being further aggravated by the continued growth and use of data terminals. The proliferation of data terminals, a spin-off effect of the IC, will place an increasing demand on the need for COMSEC equipment that is office-oriented. The use of COMSEC in a moderately secure office environment (as opposed to a security vault) will motivate novel approaches to the development of COMSEC; the equipment will essentially be tamperproof; it must be simple and human-engineered to facilitate its use by administrative personnel; perhaps for the first time, the physical appearance (i.e., color, size, shape) of the device will be the determining factor in its acceptance by the user.

(C) The proliferation of data communications and computer technology has resulted in telecommunications systems with many different hosts and a spectrum of terminal equipments operating at various speeds, line disciplines, interfaces, and protocols. Many of these terminals use American Standard Code for Information Exchange (ASCII); many use Extended Binary Coded Decimal Interchange Code (EBCDIC); operational speeds vary from 75 bps to 19.2 Kbps. Compounding this problem is the wide spectrum of network architectures that are used to connect terminals and hosts. For example:

- IBM's System Network Architecture (SNA) uses the character-oriented Binary Synchronous Communications (BSC) protocol;
- Digital Equipment Corporation (DEC) uses its Digital Data Communications Message Protocol (DDCMP) for all network link control;
- Advanced Data Communications Control Procedures (ADCCP) has been mandated by Federal Standard 1003 for use on government purchases of synchronous data communications equipment;
- CCITT recommendation X.25 identifies the high-level data link control (HDLC) protocol as a standard for use between a terminal and a host.

Many more examples can be cited. All of this has resulted in a COMSEC requirement to provide crypto-equipment with a high degree of flexibility so a variety of terminals can exchange data over different types of communications channels and operate with different line protocols.

DOCID: 4009855

(S) Currently, end-to-end security is achieved via link encryption along the transmission path and the manual processing of plaintext by cleared personnel at intermediate switching/communications centers. This concept is costly in terms of providing the intermediate personnel with system-high clearances and has the disadvantage of exposing all traffic to personnel without a "need to know." The latter has been expressed by many communicators as a serious concern with the potential for compromise and/or mishandling of classified traffic. The military departments have expressed a similar concern regarding the cost and time required to grant system-high clearances to such a large number of maintenance and operational personnel. The problem can be expected to become more critical as the need for and use of long-haul communications continues to increase. The only practical way to resolve these problems is through the implementation of end-to-end encryption. Thus, a COMSEC objective is to provide the capability to encrypt data at its source and decrypt it at the intended destination. This is a significant departure from the current use of bulk encryption on a link-by-link basis.

(S) Current and projected growth in the use of telecommunications services and equipment is creating a comparable growth in the need of COMSEC equipment. Each piece of crypto-equipment that is fielded requires the essential key management support: key generation, key distribution, and key implementation. Existing key management concepts are very manpower-intensive and depend upon a trusted distribution system as well as highly skilled personnel for implementation. Thus, existing concepts are not adequate to meet the increasing demand for key distribution and implementation. This problem is compounded when one considers end-to-end encryption in a common-user network. The latter requires a unique key between each source and destination--a nearly impossible situation with current concepts. A COMSEC objective is to provide a means to achieve automatic remote key generation, distribution, and implementation; complementary objectives are personal authentication and access control.

(S) The growth of packet-switching technology has resulted in numerous communications networks using this technology. The many advantages of packet-switching networks (speed, flexibility, economy) over classical store and forward networks clearly forecast a continuing trend toward use of packet-switching technology. Packet switching will add further impetus to the requirement for end-to-end encryption and will likely result in the need for a communications network supporting multilevel user access--two concepts that are not readily achievable with NSA's existing inventory or COMSEC equipment. In addition, packet-switching has introduced new transmission and terminal-oriented communication protocols. These protocols--Transmission Control Protocol (TCP), Internet Protocol (IP), and Terminal Handling Protocol (THP)--will become the DoD standards for packet-switched networks. There is a need to provide communications security on an end-to-end basis for packet-switched networks; a COMSEC objective is to ensure compatibility with the new DoD standard protocols for packet-switching. This is not an easy task since the standards are still evolving and, furthermore, the DoD protocols are not totally compatible with the International Standards Organization (ISO) scheme for protocol layering. This is noteworthy since, if present trends continue, the DoD standards will be at variance with the widely accepted ISO standards. The latter presents a real dilemma to the COMSEC planner and designer. Related issues are determining what levels in a hierarchical protocol scheme are optimal for performing COMSEC functions (e.g., encryption, key distribution, authentication) and to what extent the latter is considered to be classified information.

(S) In practice, most applications entail multichannel networks wherein a central computer exchanges messages and data with some number of remotely located terminals. In such configurations, with N remote terminals in operation, 2N key generators are required (one at each end of each link). This situation results in a large number of key generators at the host computer location with a corresponding increase in the probability of failure, high cost, more power consumption, floorspace, etc. The situation will worsen as the demand for data communications services increases. There is a COMSEC requirement to provide time-division multiplexing of the COMSEC functions over N input/output channels such that N remote terminals can securely interact with a central computer, thereby requiring only N+1 key generators. The cryptoconcentrator must be capable of providing link or end-to-end encryption and must be compatible with packet-switched networks.

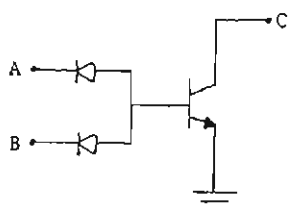
(S) The use of microprocessors and microcomputers in crypto-equipment is becoming pervasive. In addition to control and I/O functions, microcomputers are now being implemented in crypto-equipments to perform the actual data encryption. This use of microcomputers is referred to as "software encryption." Software encryption is vastly easier to implement than classical hardware encryption. Although slower in throughput speed, it

is also vastly cheaper. A typical eight-bit microcomputer can be purchased, in quantities, for less than $5.00 each. A computer programmer can program the PHALANX algorithm in a few hours. It would be impossible to accomplish the same in hardware using discrete components. There are definite benefits to software encryption; however, there is also the potential for serious risk. Consider the following software-versus-hardware approaches to achieving a simple, logical "OR" function.

- The hardware approach consists of discrete components--two diodes and a transistor--that are tangible.

- The software approach consists of some lines of code written by a programmer and executed by the microcomputer to achieve the same end result.

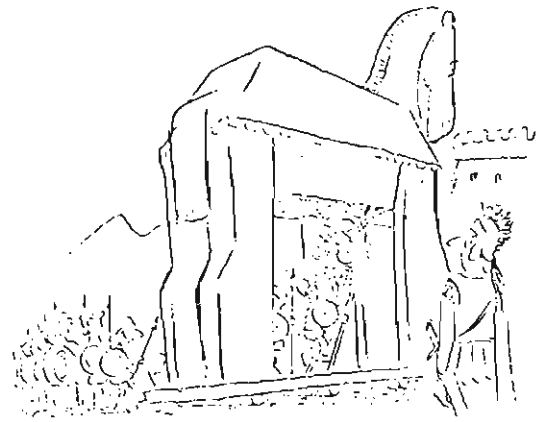
Logical OR Operation
C=A+B



(a) hardware implementation

```
L  R1,  A
L  R2,  B

OR R1, R2
ST R1,  C
```

(b) software implementation



~~(S)~~ The hardware "OR" is physically real and hence easily evaluated; the software "OR", although functionally identical to the hardware "OR", cannot be empirically evaluated--at least not on a component basis as the hardware "OR" can. This situation has created serious concern (in particular, the Trojan horse attack) and is changing the way COMSEC is being evaluated. The duplication of all crypto "chip" hardware and software is often required as a means to detect failures and programming errors; to alleviate the probability of a Trojan horse, it has been recommended that COMSEC contractors be selectively required to submit to polygraph testing.

~~(S)~~ As stated above, the use of micros in crypto-equipment extends beyond the encryption function. The I/O features of a key generator are greatly enhanced through the application of microprocessors. Microprocessors and/or microcomputers may be used in a key generator to accomplish a multitude of communications functions:

- TDM multiplexing;
- protocol conversion;
- peripheral interfacing;
- modulation/demodulation;
- speed conversion, etc.

As a result of their availability, low cost, and ease of implementation, there is a growing tendency to employ microcomputers to couple many communications requirements with COMSEC requirements. This concept is received quite favorably by COMSEC users although it raises an institutional question within NSA: How far

does NSA go (i.e., where is the line drawn between communications and COMSEC)? Two things seem clear; first, the concept of coupling selected communications functions with COMSEC is beneficial, from a system engineering standpoint, to the COMSEC user as well as to NSA; second, NSA will inevitably be satisfying more communications functions than in the past.

(S) Cryptography in the user's terminal is an area that will receive close scrutiny in the near future. As the cost of data terminals decreases, new applications will continue to surface. The low cost, convenience, and operational efficiencies associated with the use of data terminals will bear similar demands on the COMSEC required to secure these terminals. Future COMSEC will be subject to the constraints of the office environment and, hence, there will be a natural tendency to make the COMSEC transparent to both the user and his environment. The concept of an integrated cryptomodule (CM) is operationally attractive; however, it poses numerous challenges to the COMSEC designer and evaluator. Application of an integrated CM is sure to extend beyond data terminals. Requirements have already been identified for implementing a CM in a bus interface unit (BIU) used in local area networks.

(S) The doctrine required to support the use of COMSEC in an office environment will be critical. The wide variance in applications will make it difficult to assess the threats and vulnerabilities of each application. The extent to which tamper detection measures (e.g., QUADRANT [2]) alleviate physical security concerns has yet to be determined. In any event, COMSEC doctrine will be relied on--more in the future than in the past--to fill any uncertainty voids inherent in COMSEC hardware. Established doctrine and policy with regard to handling and use of cryptomaterial will have to be revised since electronic key generation and distribution will introduce new operational concepts and procedures. Because of the retentivity charactaristics of EPROMs (Erasable Programmable Read Only Memory), their very use in COMSEC applications has already caused serious concerns. The advent of end-to-end encryption in a common-user network will necessitate new doctrine and standards to minimize vulnerabilities associated with user authentication, access control, and trusted systems. The use of electronic ignition key devices and/or personal passwords will become standard features for future crypto-equipment. Among the most interesting challenges in the area of threat assessment is the use of public encryption. DES, now available to the casual buyer on a single chip, presents an economically attractive means of achieving communications "privacy" and compartmentation. New policies and supporting doctrine are required to define the extent to which DES may be used for privacy protection in a secure communications environment.

(S) COMSEC standards and evaluations will become increasingly oriented toward communications functions. The use of microprocessors and microcomputers in cryptosystems will necessitate new evaluation techniques. The use of software encryption is among the most significant challenges to the evaluators since the circuitry within a micro (and hence, the evaluation of that circuitry) is not accessible. The need to verify and validate software will become critical. Added emphasis will be placed on software evaluation. COMSEC will have to be evaluated not only as a cryptosystem, but to a much larger extent than at present, as an element within a communications network.

(S) The area of COMSEC applications will present major new challenges. The job of defining and interpreting user's requirements--with a wide spectrum of communications applications--will be formidable. The COMSEC user is demanding. He wants a secure device that is operationally transparent, has a multitude of communications features, a highly flexible interface capability and, as usual, low cost. These demands will have to be pursued with some sense of urgency so as to dampen any user tendency to seek "interim" solutions (e.g., DES) in lieu of high-grade cryptography. The broader task at hand is one of grasping the scope of the user's changing requirements and to coalesce these requirements with evolving COMSEC doctrine and standards. The user's acceptance criteria (operationally oriented) are different from (although not usually inconsistent with) the acceptance criteria defined by NSA which are naturally security-oriented. Both sets of criteria have to be addressed with little room for trade-offs in some cases. In the final analysis, however, it is the COMSEC user who determines the extent to which a cryptosystem will be categorized as successful.

---

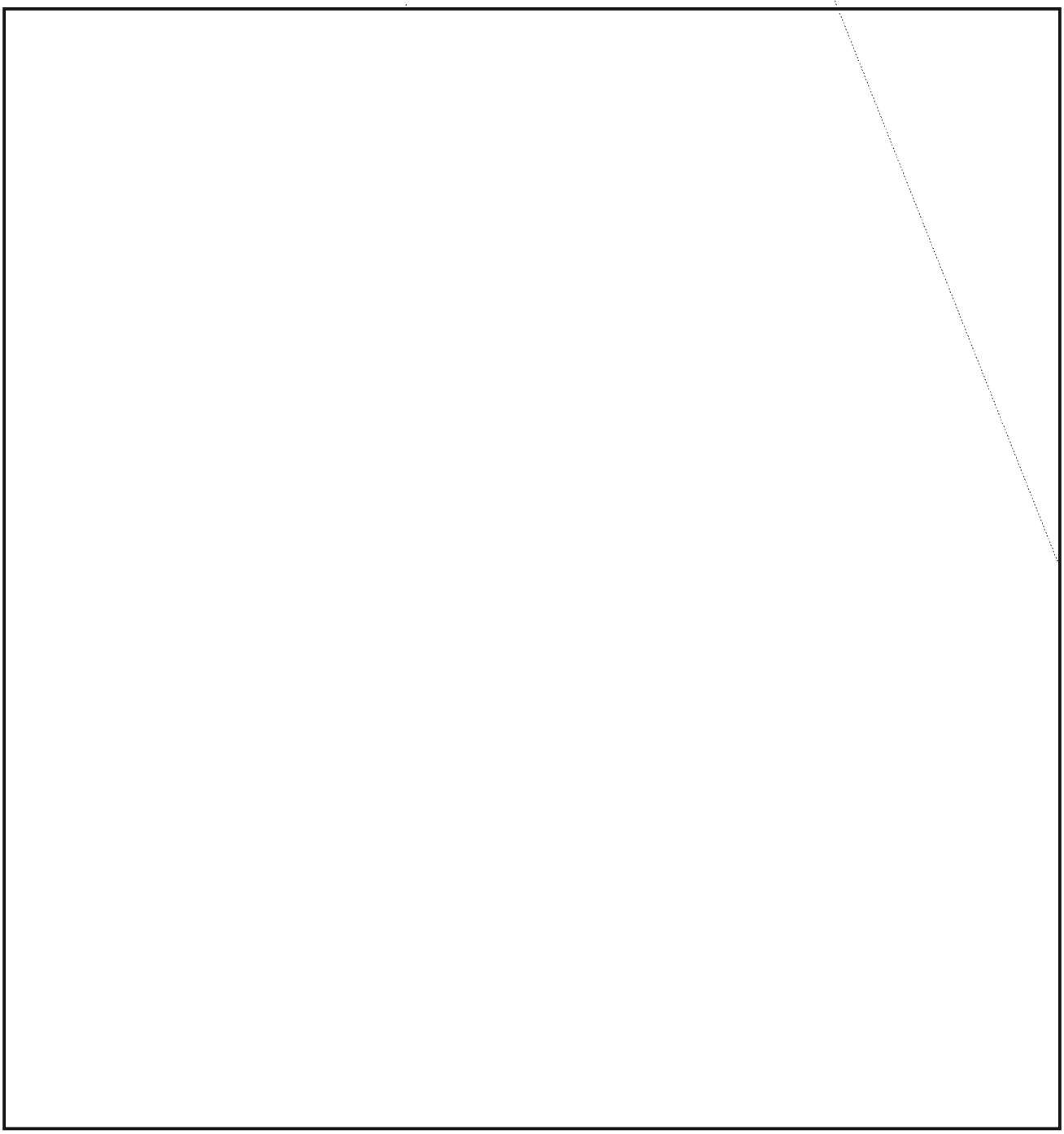
1. "Trojan horse" refers to a ploy whereby a programmer hides within a legitimate, often-used program some additional code completely unrelated to the documented function of that program. That code, for instance, might search the storage system for data to which the programmer has no access.

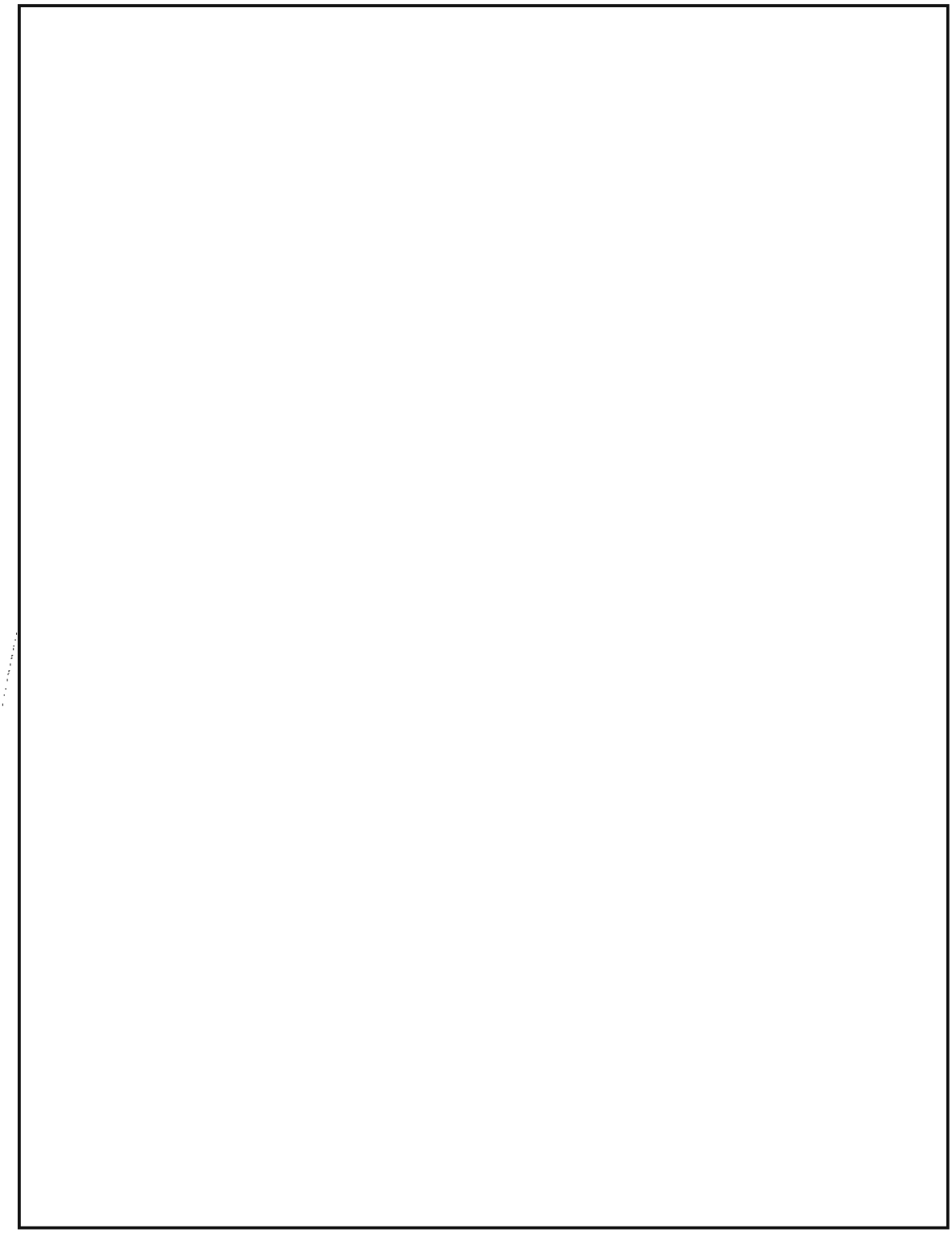
2. "QUADRANT" refers to a variety of hardware and software techniques used to detect the unauthorized tampering with a crypto-equipment.

P.L. 86-36

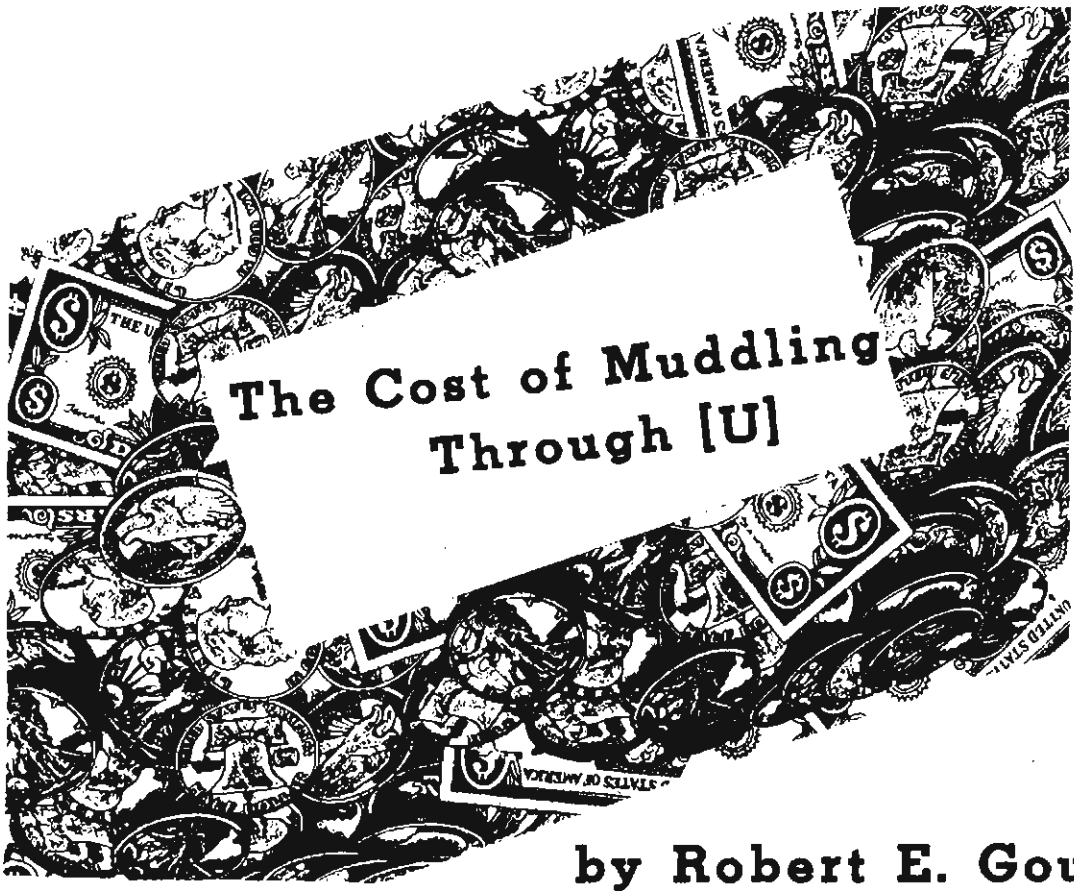
NSA-Crostic No. 44

By D.H.W.





DOCID: 4009855



The Cost of Muddling Through [U]

by Robert E. Gould

(U) In beginning this paper, I must state for the sake of clarity that I am not concerned with individual linguists so much as I am with the career of languages. The field of languages is not static but is susceptible to progress or regression. Whether or not it does progress depends upon the relatively few who can provide it leadership. It is my conviction that as it is presently constituted, the language field does tend to lose a significant number of its potentially most valuable members and does not make full use of those who remain in the field.

(U) In considering a career field or profession, attention should be given to all the factors that make up a career. When given a choice, people normally select and remain in those fields that offer money, security, prestige, individual recognition, variety of experience, and opportunity for personal growth.

(U) So far as money goes, NSA pays its linguists very well in comparison with salaries offered translators, interpreters, and teachers by other national and international organizations. Statistically it also offers a fair salary for linguists in comparison to that offered other technical fields in NSA. Job security has rarely been a factor with us.

(U) It might be stated at this point that if NSA's language needs could be met simply by producing translators, transcribers, and cryptolinguists, we probably would need to do no more than we are doing now. I don't think that our needs can be met by producing just

~~(C)~~ This article is reprinted from the November 1972 issue of the Quarterly Review for Linguists (QRL). The author was a highly respected linguist, bookbreaker, supervisor, and staff member in G Group and its predecessors. He also served as President of the Crypto-Linguistic Association (CLA) and as the founder and editor of Keyword during his Agency career, which ended with his retirement in 1973. He is now living in Tucson, Arizona, where he is doing biblical research.

DOCID: 4009855

the technicians described and if we want to get enough of the right kinds of people to stay in the field, one way to do it is to recognize where we have to offer more, as I shall discuss later.

(U) Prestige is a far less concrete matter than money, but generally it can be estimated by the hierarchical level at which a person's counsel is sought and by the frequency with which it is requested. In estimating the prestige that accrues to linguists, the following questions might be helpful. Do practitioners in the field participate in planning or decision making at branch, division, or office level? Are they kept aware of operational plans and programs? Are they consulted by their managers on decisions regarding their particular field or production in general? Are their professional opinions regarded as authoritative? In my experience, the answer to these questions is frequently, and within certain areas, generally negative.

(U) One reason for this situation is that a number of linguists have narrowed their view of intelligence production to the problems of language and have failed to see the relationship between their field and the rest of the Agency or to accord other operations their proper importance. In addition, only a few have ever phrased the problems of language processing in objective language that would make them accessible to nonlinguists.

(U) These comments are not made to belittle the specialist or his contribution, but to point out the result, that the nonlinguist manager may often regard linguists as narrow, impractical people and feel that even in the management of language problems, he can more safely rely on the advice of common-sense people outside the field. What is often hardest for the linguist to bear is that the intelligence analyst, too, may come to feel that in substantive questions, his opinion on the meanings of a text is more likely to be correct than is that of the person who translated it.

(U) There is no quick way of insuring the field prestige, but it can acquire it if the practitioners develop a wider view of their work, its place in SIGINT, and apply their knowledge. Specifically I would suggest the following:

- As intelligence producers, linguists should have a professional's knowledge of the intelligence field as it affects them; i.e., who their customers are, how their product is used, what requirements are, and how they are used and generated.

- They should have a thorough understanding of the support functions that linguists must perform for traffic analysts, cryptanalysts, collection, and ELINT. To be able to function properly as professionals, they must also acquire a fairly detailled understanding of various aspect of communications and cryptography.

- Linguists should also have a professional view of their own field--the linguist's various functions in production; research needs; training problems; the problems of field reporting; requirements of the Service Cryptologic Agencies' linguists.

(U) This knowledge is not something that can be instilled all at once into any given linguist, but it represents a basis for training of the professional.

~~(C)~~ For most linguists coming into production, a career seems to consist of ten years translating and ten-plus working at the checker's desk. The field does, in fact, contain a variety of jobs, but they are poorly publicized. About two thirds of the senior linguists in G Group have worked in two or more languages. Almost all have worked on a variety of problems: translation, reporting, cryptolinguistics, and others. There are, outside of production, jobs in teaching, as well as linguistic and cryptolinguistic research to which some linguists should be able to aspire. There are language staff groups in two of the G offices. Opportunities for overseas assignments exist in some areas.

~~(C)~~ The varieties of work should be made known to all beginning linguists. It would be desirable also to state the qualifications for the jobs in order to try to inspire some competition for them. Because there is no clearly enunciated public statement of the training and experience required for various positions, there is not much that an individual can do to direct his own career.

(U) The possibility of making a recognizable personal contribution seems denied the linguist to a rather considerable degree, since by the nature of much of his work, the quantity and quality of his achievements are visible only to his immediate supervisor. The room for personal contributions, however, is much greater than is at first apparent. The problem is that because of the peculiar isolation in which they have often worked, the linguists have rarely been led to think in terms of the needs of their field, where the contributions are needed.[1] Another difficulty was posed by the fact that until recently there were few means for acquainting the rank and file with developments in the field, so that they might become aware of the needs, themselves.

(U) If a profession or career field is to advance, it must afford opportunity for innovative and exploring intellects. One of the reasons we lose linguists to management is not only that certain linguists want to get out of the field, but that their superiors see a more productive used of their talents in administration than in languages. A given linguist may be able to improve his skills so that he can do as much as two or three other employees, but his division chief may recognize that he has the vision to improve the output of the whole organization. Unless the field of languages can offer such people room for action of comparable scope in the profession, it will lose them and the progress they might bring to the field.

~~(C)~~ The cost of not providing opportunities for the creative linguist employee in his field is easy to delineate. It was long recognized that relying on experience as a teacher, we needed years to produce a good COMINT linguist, even in a well-known language such as Spanish, but an on-the-job course prepared by an expert was not developed until the mid-60's. It was also well known that continuing effort was required to keep up with contemporary language, but no serious work was undertaken until the introduction of the CAMINO Spanish Language File in 1966.

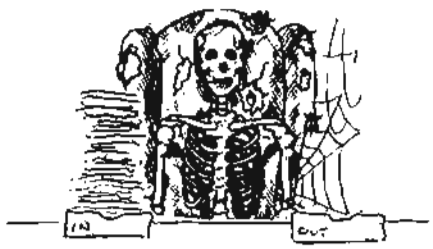
(U) The significant point of those advances is that they were made by linguists of unusual talent who had created their own jobs. If we are content to wait another twenty years for some of our other language problems to be solved, we can proceed in the accustomed manner, directing all efforts to producing desk linguists and relying on some few of them to work themselves loose at some uncertain date for work of a broader scope.

(U) The more direct approach is to recognize that we have a continuing need for inventive, practical, and broadly experienced linguists for developmental work and not only create places for them, but insure that these places offer sufficient rewards to draw the right people and keep the places filled, also with the right people.

---

1. Some specific examples recently uncovered are:

* a good, existing reference grammar requires indexing before it can be used effectively;
* specially prepared training tapes are needed for new transcribers;
* more effective means of training service transcribers may be possible by proper application of phonetic theory;
* grammars of COMINT language and usage need to be prepared in several languages;
* advanced on-the-job instruction needs to be developed in the absence of formal courses;
* more and new material needs to be assembled to expedite training of new linguists.



DOCID: 4009855

AN *OLD TIMER* IS ONE WHO... (U)

by W. P. Meyer, T5

Remembers when there were two Marine guards at the escalator in the middle of the Operations Building, one at the bottom of the stairs and one at the top of the second floor.

Remembers when the Headquarters Building was being built and the rumors said it was going to be reserved for all of the M organizations.

Remembers the rumor that NSA was going to be split in half, one part moving to California and the other to North Carolina, i.e., NSA East, and NSA West.

Remembers when there were so many rumors concerning anything and everything at NSA that someone said they were going to build a hotel on the Baltimore-Washington Parkway to house the "roomers," and so they built Colony 7.

Remembers when the copying machines used tulip-imprinted paper so you could tell the reproduction sheet from the original copy.

Remembers that when the IRC (Information Research Center) Building was built it was not meant for human occupancy. It was originally called the "SMSB" (Sensitive Material Storage Building). When the heat and humidity reached a certain point, everyone was excused to leave. Of course, if you were in a carpool with people from the Operations Building, you couldn't leave to go home anyway.

Remembers when a bored Marine climbed the microwave tower in front of the IRC Building one night and put up a Nazi flag, and it took the Post Engineers a week to bring it down.

Remembers when the old CREF (Central Reference) moved to the IRC Building, and no one used the library again. Every office began to build up its own collection of books. Information is so fragmented now that no one knows where anything is anymore.

Remembers when R wanted to build their own building near College Park and establish their own collection of books; here it is 20 years later and they have their own buildings, only they are called FANX-II and FANX-III, and their library is the FANX Library.

Remembers when NSA had no flagpole in front of the Operations Building. When Admiral Frost arrived, he stated that NSA was a ship and he needed to fly his personal flag so that the public would know that he was aboard.

I am not "really" an old timer. I did attend the U.S. Army Signal Corps School at Fort Monmouth, New Jersey: I did have an MOS 805 (Cryptographic Technician) but I did not start to work at NSA until 1958. A "real" old timer is one who was at NSS (Naval Security Station) or at AHS (Arlington Hall Station), or even the old Munitions Building. You should hear the stories they can tell--and I hope they will.

SIGINT: 1990 (U)
PART 3

by [redacted] P13

P.L. 86-36

COMPUTER COMMUNICATIONS SYSTEMS

~~(S-CCO)~~ As computers become more tightly integrated into telecom nets, the central problems facing SIGINT will become what to target and how. The most useful data, from an intelligence or a SIGINT viewpoint, may be resident in the system in a computer memory, rather than passing over a communication channel. SIGINT, instead of waiting for data to be transmitted and then passively collecting and exploiting them, will have to penetrate into the nets, find what is there, and extract it.

~~(S-CCO)~~ Several points, which are obvious truisms, must be borne in mind. It is fairly easy and cheap nowadays to make a link secure. This is the COMSEC function, now virtually solved. On the other hand, it is very hard to secure a whole network against every possible attack. This is the NETSEC problem, and part of the NETSEC, viz., computer security, is actually operating as a separate organization inside NSA because it is a different problem.

~~(S-CCO)~~ Although the security role of NSA is extending from protecting channels to protecting nets, the analytic role still seems trapped in the passive posture of intercepting links rather than penetrating nets. By 1990 this will not be a viable SIGINT position.

What new problems will SIGINT have to face by 1990? What do the new trends in technology tell us about the not-so-distant future? The author has adapted this article, presented here in the third of several monthly installments, from his presentation at a January 1982 session of CA-305.

This is one of the choices that must be faced and acted on.

[redacted]

P.L. 86-36
EO 1.4.(c)

~~(S-CCO)~~ The two major effects of having computers integrated into the telecom nets are logic and storage. The computers can provide services which are logically complicated, compared with old-fashioned manned message centers which were fully burdened just to receive and pass on messages. The modern storage systems can provide economical central repositories of data. Because of economics it is still not feasible to provide immense storage capacity at the subscriber outstation, because big memories cost far more than telephones. The effect of centralizing on-line memories around computer systems leads to a lot of man-machine and machine-machine data transfers. The total amount of storage capacity that is coming into the networks as on-line memory is quite significant, and currently sums to about 1 quadrillion bytes of data which can be automatically accessed by remote requests. By 1990 over 100 quadrillion bytes of online storage are expected worldwide, under various access controls. The SIGINT task is to penetrate into this on-line storage, find out what is accessible, and extract the useful data.

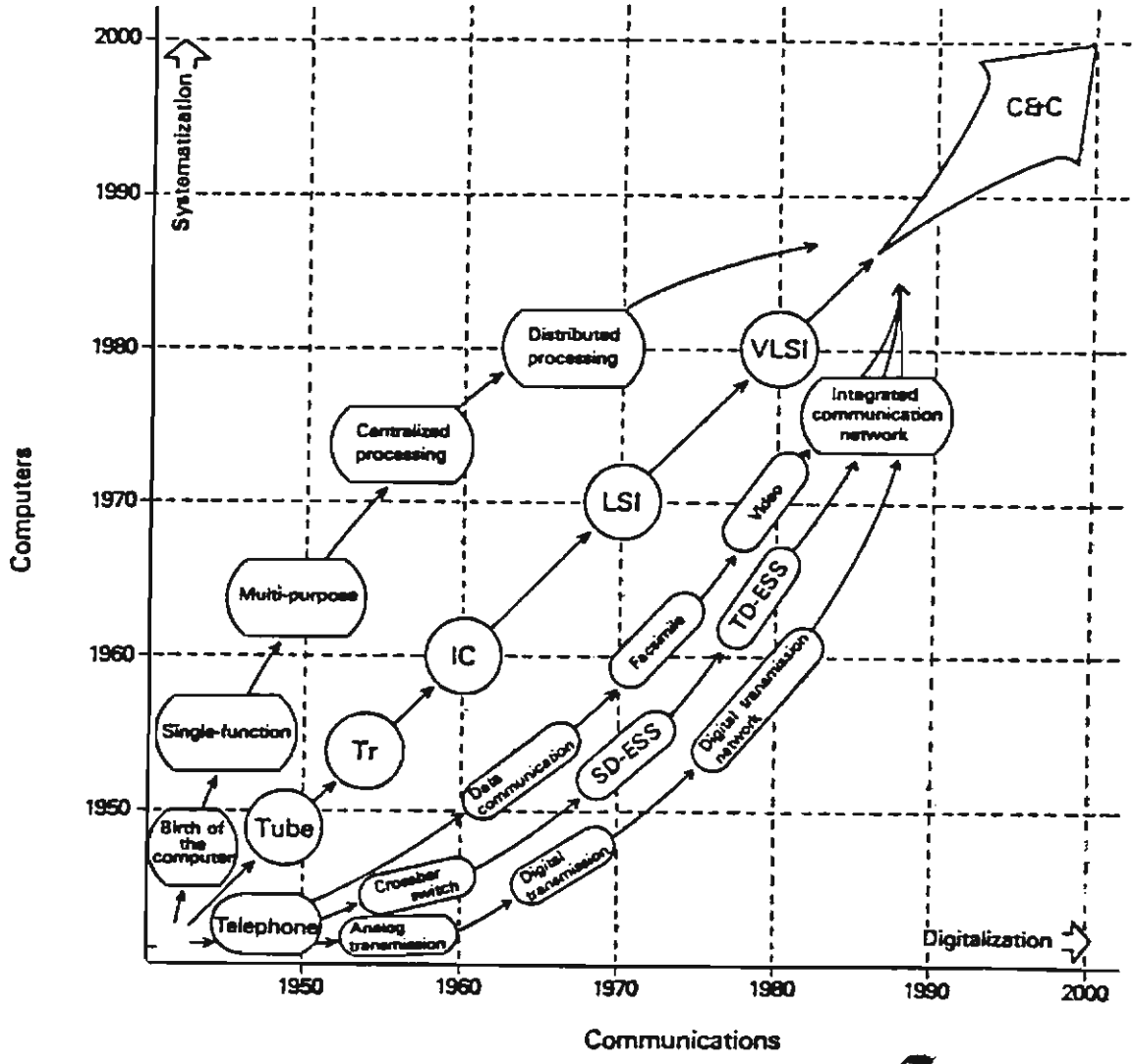
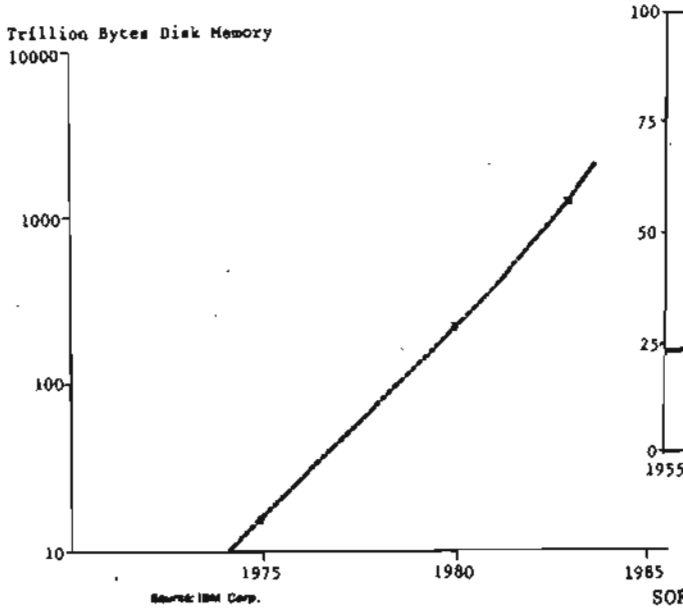


Fig. 32

PERSPECTIVE OF "C & C"

DOCID: 4009855



WORLDWIDE GROWTH OF
ONLINE COMPUTER STORAGE (Fig 33)

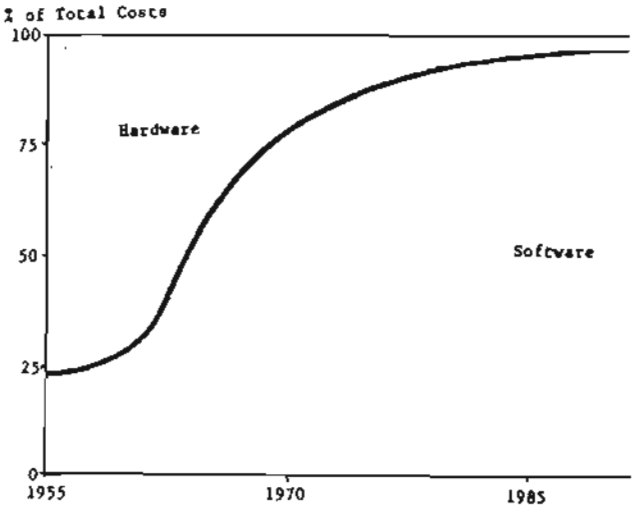
(U) Two unavoidable consequences of all this storage capacity are that:

[] first, information flow (not mere traffic flow) through the networks becomes very complicated, because data files may be located at dozens of different points as identical or slightly altered sets, and

[] second, the users are forced to think about and rely on the storage and the stored data.

(U) While a user can interact with a memoryless telecom system, e.g., a telephone net, through a mechanical terminal (telephone, teletype, facsimile), once the network has memory, especially on-line storage, the user needs elaborate protocols, embodied in software or firmware, to interpret what he wants to do into command sequences that the network can execute.

(U) The result is that in a C&C net the bulk of the investment shifts from the central switch and outside plant, which connects $10 telephones, to a huge investment in software and "intelligent" terminals which perform many different functions for the network users. Typically, 90 percent of the customer's investment is in the terminal, and the aggregate cost of producing software or firmware that the customers will purchase becomes the dominant factor in system cost and success.



SOFTWARE COSTS FOR SYSTEM DEVELOPERS (Fig 34)

(U) The performance requirements for the terminal software are not all trivial, because banking and financial services will be supplied more and more through terminals which not only give access to cash, but to many other banking services, from private or public locations. The software, firmware, and cryptography needed to assure reliable functioning will be critical.

(U) As an example, the major U.S. banks will soon be offering interstate banking services via terminals, and extension to international services is only a matter of time. Hence, critical economic information, generated by network terminals, will flow through public C&C networks, replacing much of the mail and conventional financial, shopping, and business activities.

~~(S-CCO)~~ As circuit technology has improved, software development has become the dominant factor in system cost and delivery (and performance). This software development burden will have the effect of "freezing" the network services to a considerable degree, even if the hardware is easily replaced, because of the "learning cost" that the users have to pay to get access to the system. At the same time, the burden of producing software will tend to freeze SIGINT methods, for the same reasons.

L. 86-36
1.4.(c)

[redacted]

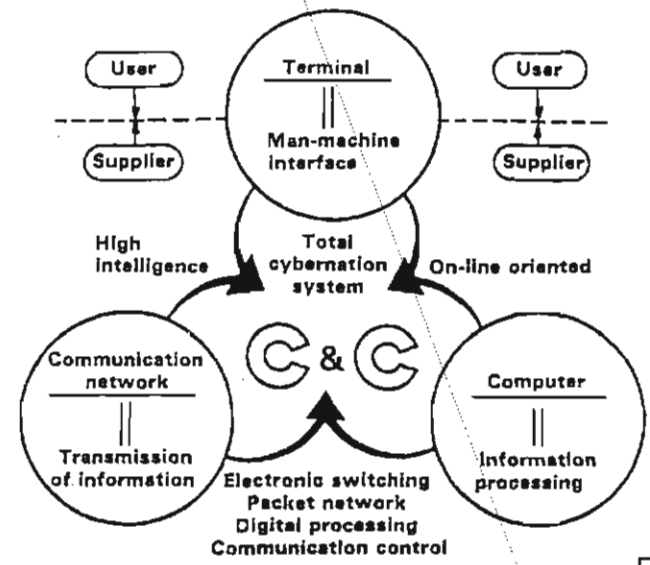


IMAGE OF C&C INTERACTION (Fig 35)

(U) A C&C network consists of a number of components, viz., computers, on-line storage, telecom circuits, switching, software, data bases, terminals, users, and projects or activities that use the C&C net.

[redacted]

(U) Over the next ten years the main effort in the industrial nations will be to establish the IDN (integrated digital network) as an operating entity. The object of IDN is digitalization of the local network and terminals in the form of a 4-wire digital circuit. When this is achieved, many new services can be provided, leading to the ISDN (Integrated Services Digital Network) based on 64-Kbps circuits all through the network. This will allow the C&C terminals to provide point-to-point switched encrypted voice, data, and facsimile with many data base services, and interface into other message services, such as Telex, Teletex, etc.

~~(TS-CCO)~~ The deliberate deregulation of the U.S. telecom market and the increasing role of computers and software and microprocessor terminals will tend to force experimentation and innovation onto the PTT's in both industrial and Third World countries, as powerful customers demand the procurement and introduction of useful and sophisticated new services, such as domsats, POS terminals, E-Mail, electronic banking, etc. A major advantage that U.S. suppliers have in C&C competition is the highly knowledgeable customer base that demands everything the technology can supply. The increasing internationalization of U.S. business will inevitably hurry the spread and export of the advanced C&C services and technology into all areas of the world where those companies operate. Many sophisticated foreign business C&C nets will be SIGINT targets, wherever they extend, and therefore the current backward state of a poor country's telecom plant is not a guarantee that they will not superimpose the most advanced C&C nets on top of the local plant, in the same way that inefficient subsidized jet airlines are superimposed as status symbols over oxcart economies.

[redacted]

DOCID: 4009855

COMPLEXITY OF TELECOMMUNICATIONS

(U) A century ago telecommunications consisted of Morse telegraphy. In the latter part of the 19th century telephony was added, after some initial resistance by the Post and Telegraph authorities. At the turn of the century coastal radio telegraphy was introduced and gradually brought into the network of services, although for some years the British Post Office, for example, would not allow the Marconi stations to have telephone or telegraph lines, since radio threatened their monopoly.

(U) Gradually new services were added, many based on radio, to take care of special needs such as safety services, mobile radio, marine and aircraft traffic, air traffic control, amateur, radar, broadcasting, TV transmission, facsimile, and so on.

(U) Now the capabilities of digital networks, with computers to carry out the details of providing user interface and networks access, have encouraged many new notions about what telecommunications are, and what role they should play in a modern nation.

(U) The French CNET study for the year 2000 has formulated a large number of new services which can be integrated into the future networks. A table of 64 new services has been published in the study.

Telecommunications by 2000 — Some services for the year 2000

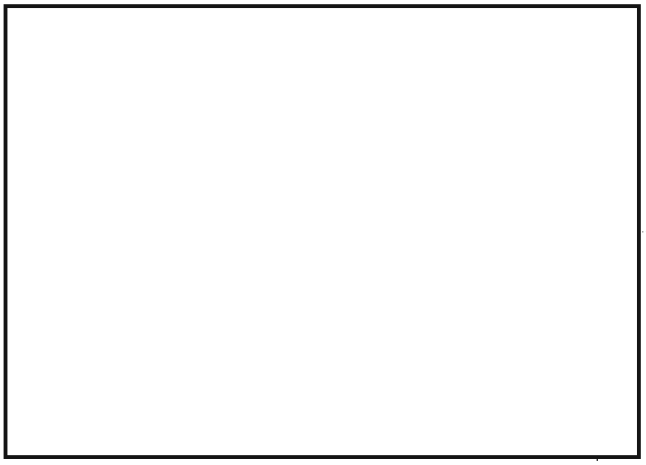
Fig. 36 - 64 additional new services

TELE-ENERGY Monitoring & control of energy consumption	EUROPHONE Handset H/T on a Europe-wide level	UNIVERSAL IDENT BADGE An electronic passkey (also see below)	TELEFINGERPRINT Enter without knocking, thanks to voice recognition	TELEWORK Shiftwork in your home (Cf. HOUSEWORK)	TELELIBRARY Look at books, documents, newspapers, etc.	TELECONFERENCE Color, hi-fi, graphics, on a Europewide level	TELEMAIL Telecopying of the future
2-1/2D IMAGES For those who want to change their point of view	TELEHELP Pinpointing of dangerous situations	TELECONTROL Location of individuals	TELEDESIGN The Office of R&D in era of TV automation	"SLY BISON" Videotex version that can be used in a car	WEATHERCULTURE Weather forecasting in the service of agriculture	TELEFILLING To save paper ...& space. (Cf. TELELIBRARY)	TELECHECKING Electronic pay cards
TELEANALYSIS Detection of pollution & toxic products	VOICE PLACEMENT OF ORDERS No more dialing; forget the keyboard!	TELEDIAGNOSTIC In case the electronic housekeeper breaks down	TELESIMULTANEOUS TRANSLATION For better understanding between people	HOUSEWORK With videomatic assistance (Cf. TELEWORK)	TELEHEALTH Computerized preventive medicine	TELESURVEILLANCE Videosurveillance for various purposes: family, social, business ...	TELEWARNING National net for detecting & warning about disasters
3D TELEMOLDING 3-dimensional facsimile	TELEANIMATION A companion, a babysitter, the life of the party	QUICK CALLS A guarantee of short duration	TELECOMPUTERS All the computers in the world want to lend you a hand	TELEVILLAGE A real estate office	IGB or IMB Individual Genetic (or Medical) Badge	TELEINFORMATION TELEADVICE Starting with data banks or a group of experts	TELETEACHING Education marches on
TELECLEANING Automatic housecleaning w/centralized supervision	TELESEARCH For doing research & paging people	TELEJUKEBOX Songs & music on the phone, w/a TELE/HI-FI version	TELESCRIPTING For the handicapped, converts the written word to Braille	TELETAXI Automated location of vehicles	TELEWEATHER A real-time service	AUTOMATIC RECALL There's this phone number that you've called (over & over)	AUTOMATIC FILTERING Freedom from the telephone
TELEDECORATING A new kinetic & musical art in your home	TELEMAINTENANCE Remote repairs. System connected to TELEDIAGNOSTIC	TELEVOTING Electronic democracy	TELEAVAILABILITY To be called or recalled when wanted	TELESTOCKMARKET Automated trading & data (Cf. TELEWANT ADS & TELESWAP)	TELEPROGRAMS Bidding on TV programs	TELEWANT ADS Videotex want ads (Cf. TELESTOCKMARKET & TELESWAP)	TELERESERVATION For shows, hotels, travel, w/automatic payment
TELECOUPLE Marriage by TV technology. A form of Computer-Assisted Design	TELEOPTIMIZING It will solve all your problems	TELEPOLLING See the box above	TELESOFTWARE To plug your pocket calculator into the network	TELEPRICE LIST for HCRPS Wholesalers National Computerized Retail Price Service	TELEFORUM Meetings & debates over the phone	TELESWAP A second-hand store in connection with TELEWANT ADS	TEACHING TERMINAL You'll learn how to use all the other terminals
TELEGAMES Interactive video games for one or more persons	TELECOMMAND A generalization of the automatic wake-up call	INTERNETWORK Don't send anything but flowers...	TELEFLEA MARKET A teleautomated second-hand shop, employment agency, etc.	TOM-TOM Your dialing time shortened, using a card	AUTOMATIC PCV Just what its name says (PCV = Reverse the charges)	TELESHOPPING Videodiscatalogue & automatic shopping by phone	TELEAUTOMAT Away from all those fareway counters

DOCID: 4009855

CNET: NEW TELECOMMUNICATIONS SERVICES IN 2000 (Fig 36)

(U) This tabulation expresses the significant increase in the complexity of future telecommunications. Even marriage by telecommunications (see TELECOUPLE) is included in the plan. There is so far no mention of telenuptials. The different services interact to some extent. Some teleservices will be forced onto the user, e.g., by the banks eliminating paper checks, or by the existing French plan to eliminate the telephone books throughout France in favor of small text terminals which a telephone subscriber will use to request directory service. As the teleservices extend farther through the society and economy, the PTT's will have a much greater policy role in determining what transactions will occur in a nation. The recent telephone cutoff in Poland and in the USSR, to enforce government control, illustrates the importance attached to controlling teleservices.



~~(C-CCO)~~ SIGINT is familiar with the conventional point-to-point communications and with point-to-mass (broadcast) nets, but computers now make mass-to-point nets feasible, which collect data or serve a star net of subscribers.

(U) Different parts of the networks will grow at different rates; e.g., in Japan computer production has grown at 20 percent, while video tape recorder and robot production have grown at almost 50 percent. Facsimile, word processing and other office information equipment have grown at 40 percent.

(U) Both government and business, through teleservices, will be able to reach out through the telecom nets and extend an interactive environment over time and distance. The teleservices may extend from the exercise of police or taxing power to the marketing of luxuries. Ownership of the teleservices will be important, just as ownership of the telecom plant also confers power. As competitive nets, offering similar teleservices, extend further, there will be greater emphasis on controlling the flow of information within and between nets. Encryption will be only one of the means used to control or regulate access and flow.

(U) Although the French model projects the future in terms of different services, a rather different view of current telecommunications and media was presented in recent Congressional hearings about competition in the communications industry.

THE MEDIA BUSINESS, 1981 (Fig 37)

(U) The tabulation in the hearing record, which was adapted from a Harvard study, roughly segregated the broadcast services from the various means of delivering information. The resulting somewhat crowded and inscrutable chart is a testament to the difficulty of describing the conglomerate of products, services, channels and content that constitute modern communications.

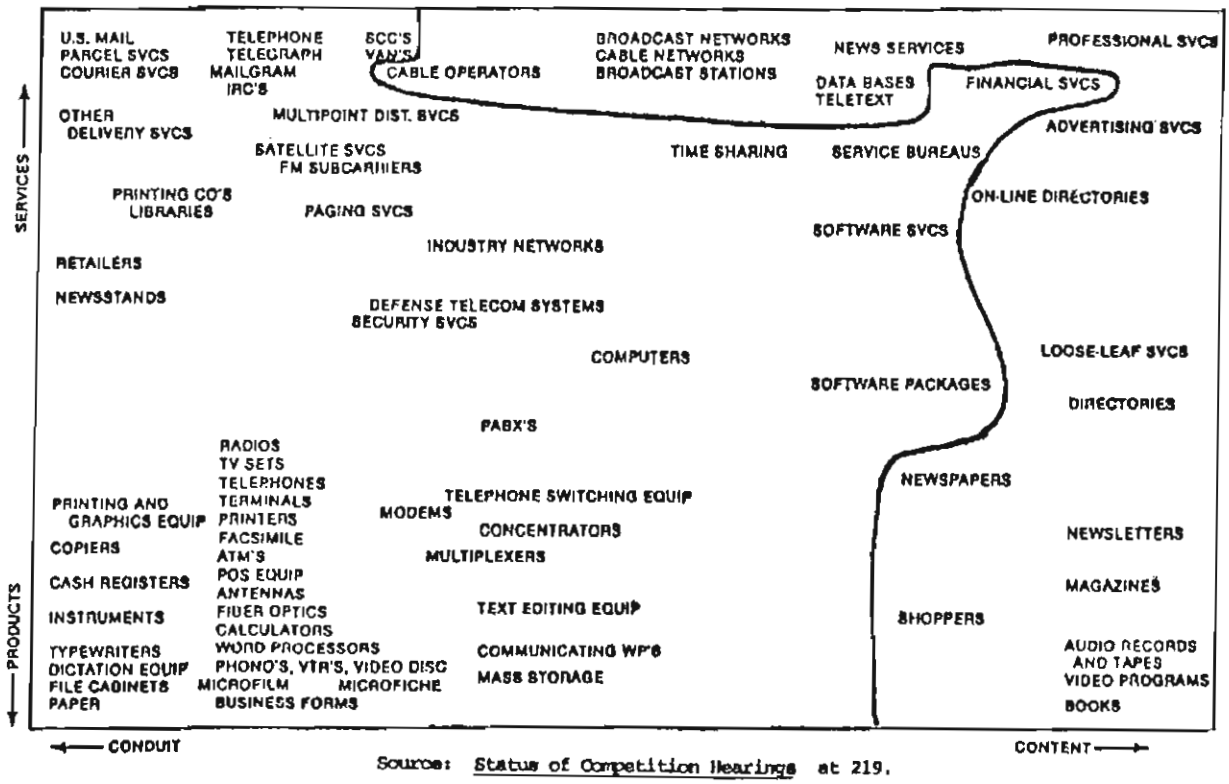
~~(S-CCO)~~ This variety and complexity would not matter directly to SIGINT were it not for the fact that as the new networks become more efficient, it will become a matter of economic necessity to supply the products and services by electronic means. The development of E-Mail, to compensate for the cost and delay of postal services, and the corresponding development of robots to answer phone calls, place calls, and telemeter building conditions--because of high labor costs, lack of servants, and a consumer market for such "personal" services--is a further illustration of the increasing use of electronics and telecoms to perform social and economic functions.

P.L. 86-36
EO 1.4.(c)

~~(S-CCO)~~ The "mining" of some of the teleservice transactions would be comparable to the vast diamond recovery operations off the coast of South Africa, where a bulldozers continuously work to push a sand dike farther out to sea, while huge machines dig up the exposed seafloor and screen alluvial diamonds.

DOCID: 4009855

THE MEDIA BUSINESSES, 1981 Fig. 37



Source: Status of Competition Hearings at 219.

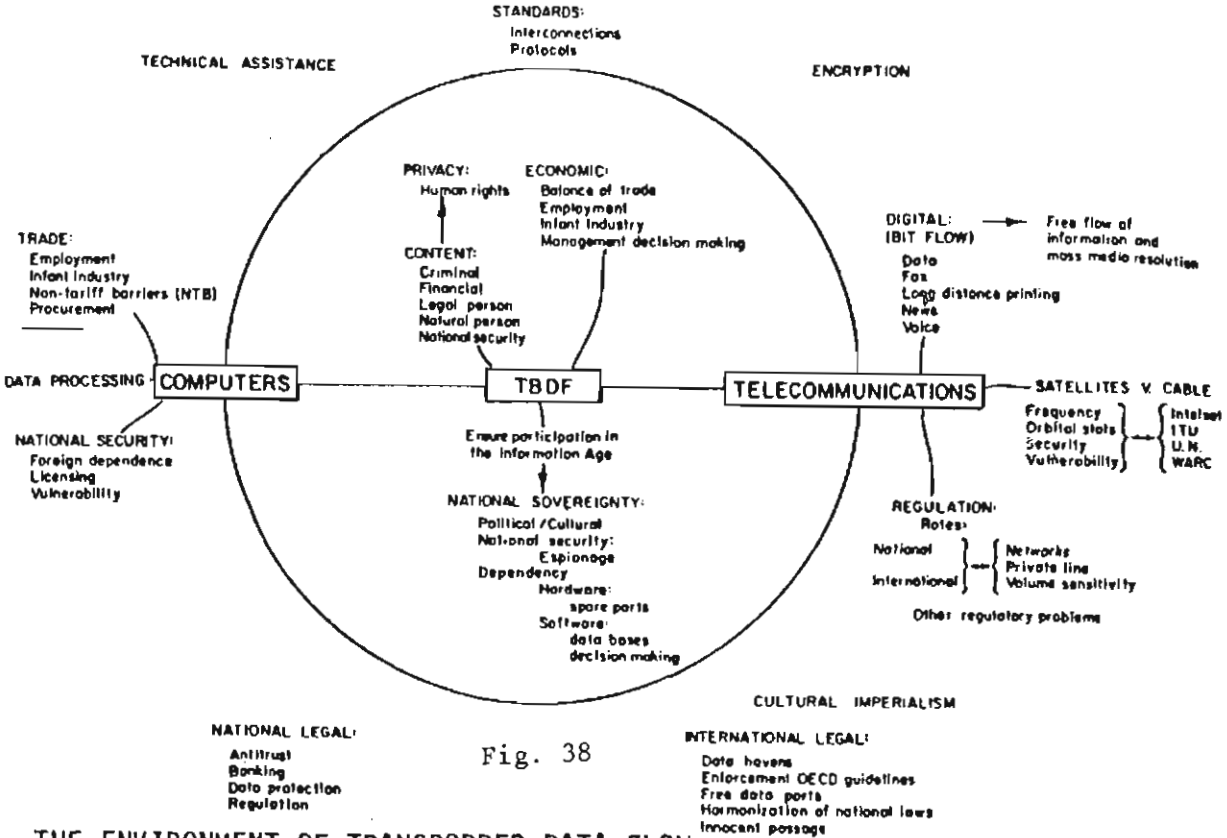


Fig. 38

THE ENVIRONMENT OF TRANSBORDER DATA FLOW

DOCID: 4009855

The ratio of sand moved to diamonds extracted is about 130 million to one. While some SIGINT will continue to operate against high grade teleservices such as dedicated military and diplomatic cipher links, other SIGINT will have to work the huge mass of low grade transactions, which may be coded or encrypted in a way that conceals their lack of value.

~~(C)~~ Put in different words, the teleservices will represent the actual policies of a nation, just as transactions and teleservices within a small computer net embody the net policies. In the course of analyzing the complex networks and teleservice repertoires, SIGINT will inevitably discover just what the social, economic and, in many cases, security policies of the target nation are. As policies change, teleservices will change with them, just as the U.S. imposed peacetime censorship on international radio and cable services in 1914, and many countries impose such censorship on various internal and transborder telecom services and transactions during wars and crises nowadays.

~~(C)~~ One elementary example of the significance of teleservices and transactions in defining policy and status is the power currently possessed by computer network managers to access and change passwords, access and rename and move files, change access codes, and monitor or alter the actual usage of network facilities, and even to take the network down or change the operating systems gradually or totally without much reference to the users or even to the owners of the nets. Their "privileged" terminals, plus far-reaching power to change and tamper and inspect, and to deny access or shut down, shows how teleservices define policy and power. In future, the power of the network managers will be a key index of where actual power in a target system is concentrated--always an interesting fact.

~~(S-CCO)~~ In capsule form, teleservices are the image of policy. Teletraffic is the image of operations defined by policy. SIGINT is the insight channel.

~~(S-CCO)~~ One of the most vivid illustrations of the complex intertwining of telecommunications and social policy is the issue of transborder data flow.

ENVIRONMENT OF TRANSBORDER DATA FLOW (Fig 38)

~~(S-CCO)~~ A Harvard study represented the TBDF (transborder data flow) problem in a semi-inscrutable diagram, with "encryption" apparently floating freely as an environmental factor. In fact, encryption will be one of the major issues in TBDF.

~~(S-CCO)~~ TBDF began as an endeavor in Europe to protect certain personal data which in several countries is protected by law from exploitation in bordering nations. This privacy interest gave it political power, and the discussion soon turned to the more interesting matter of controlling the power of foreign e.g., U.S., corporations by limiting the kinds of files and data they could send across borders by telecommunications. In France a small tax is levied on many kinds of data exports, not for revenue purposes, but to keep records on what is passing. The principal method for moving sensitive business files across borders has long been to fly them by courier as magnetic tape files, because this is much cheaper and more accurate for subsequent processing on U.S.-based computers. However, the European nations have begun to draft regional legislation to control all kinds of files to establish non-tariff trade barriers and other limitations on foreign companies. The Canadians have also taken a view that TBDF represents a loss of jobs in Canada.

~~(S-CCO)~~ U.S. business interests not only want "free flow of information," but also claim a "right" to operate cryptographic devices over transborder data channels. Most transborder telephone lines to and from the U.S. are leased and are used by corporations for their internal communications.

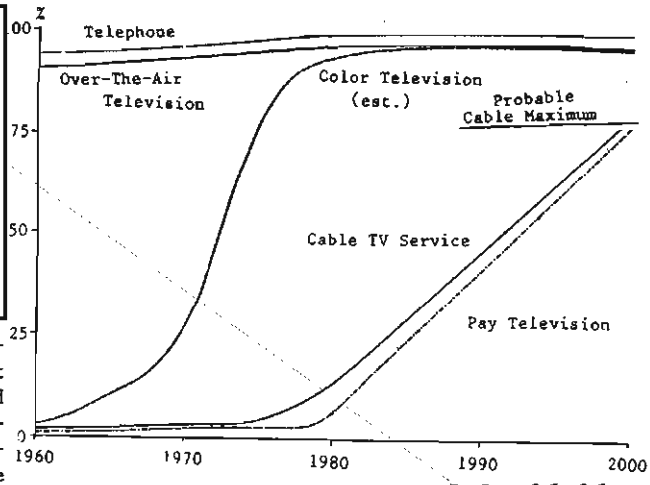
~~(S-CCO)~~ For the foreign governments to impose their TBDF policies, they must have access to the contents of the traffic passing over their borders. Under international law (The International Telecommunications Convention) they have the legal power to examine any non-government traffic that terminates in their territory. Encryption would thwart the power of the state. Therefore, encryption will be a central issue in TBDF.

~~(C)~~ Because there are many subtle ways to send traffic across borders (e.g., indirect transmission to an undeclared recipient, etc.), the PTT's and security services will have to use their own SIGINT and intelligence services to verify that the actual TBDF corresponds to their laws and policies. The U.S. is one of the most important players in the TBDF controversy, because quite a lot of technology transfer occurs from U.S. data bases to foreign subscribers, and U.S.

transnational corporations are major users of advanced data services.

[redacted]

Percent Penetration in U.S. Homes



P.L. 86-36
EO 1.4.(c)

(U) One of the driving factors in telecommunications and teleservices which is not under the control of the telecom planners and managers, is the market penetration of consumer communications devices, such as telephones, TV sets, radios, stereos, mobile radios, home computers, etc.

(U) As the public acquires these communication devices, the PTT's and manufacturers and network designers have to develop supporting services to correspond to the consumer needs. Thus, for example, microwave radio relay stations and trunk routes spread throughout the U.S., Europe, and the rest of the world at a very high rate after World War II to provide a cheap wideband channel for distribution of TV programs. The programs were expensive to produce, compared to radio programs, and, before video tapes existed, had to be distributed from central studios. There was no security problem, so radio relay was acceptable. After the microwave trunks were installed and functioning, additional equipment was developed to carry telephone traffic. The driving factor was the success of the TV receiver in the market, which created a demand for the wideband network.

(U) Even consumer communications reflect commercial or governmental policies. In Israel only black and white programs are broadcast, to thwart sales of imported color TV sets, because the Israeli economy cannot stand the outflow of hard currency. At the same time, TV sets in Israel are only allowed to receive UHF so that the powerful Arab VHF programs cannot be heard. In the U.S. the broadcasters with good VHF frequencies have been influential in retarding the use of UHF and cable as a competing medium.

MARKET PENETRATION OF CONSUMER ELECTRONICS (Fig 39)

[redacted]

(U) A very different implication comes from the growth of pay-TV. This has been shown to be a profitable way of selling certain kinds of entertainment because the revenues are directly connected to market success of specific entertainment products. In order to keep non-paying viewers out, TV encryption systems have come into use. At present most of them are very weak and can be circumvented, but much better systems are under development. In the U.S. the pay-TV distribution consists of two parts, viz., the distribution of program material from a central point to local CATV companies, and the further distribution by local broadcasting. There is also a background of TVRO small earth stations which intercept both pay-TV and ordinary TV satellite relay transmissions.

(U) As pay-TV gains in success and is able to sell better programs, the economic value of TV encryption will increase. On the satellite links it is worth while to provide fairly secure encryption, but the emphasis is on program quality after decoding. In general the voice channel will be secured by something equivalent to DES. At the local level, quality is less important to the supplier than being able to defeat piracy and assuring that all customers pay their bills. The emphasis in encryption is on the command channel that shuts sets off if they are stolen or delinquent in payment.

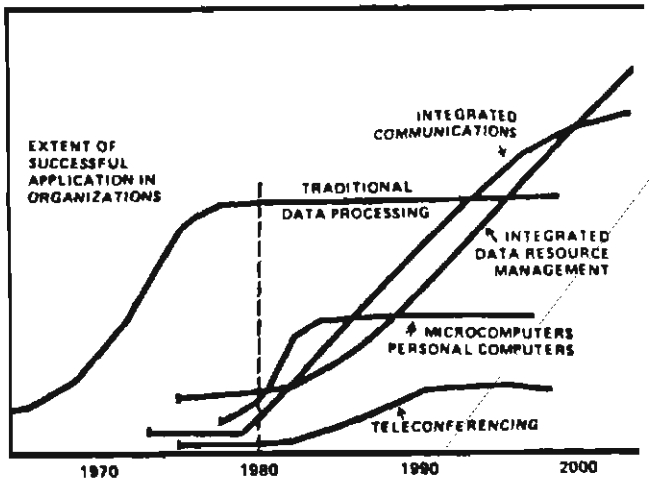
(U) The growth of many specialized TV services, including pay-TV, has made U.S. domsats (domestic satellites) a profitable industry over the past two years, and three quarters of the domsat transponders are used for TV relay.

~~(C)~~ As these new TV services, especially pay-TV, spread to foreign countries as ways of making money or raising PTT revenues, the encryption schemes will spread with them. The result will be that most of the foreign domsats will be carrying encrypted wideband traffic. The U.S. market study shows pay-TV at a 40-percent penetration level by 1990. The penetration will probably lag in most foreign countries, but the use of wideband encryption on TV satellite relays may spread faster than local TV encryption to thwart interception or copying of national programs.

~~(S-CCO)~~

(U) All of this will add to the burden on SIGINT to know what is passing through the networks, and what services are being offered, on channels which in the past have been of no interest at all.

(U) An additional implication is that the development and deployment of wideband encrypted broadcast trunks, in the U.S. or elsewhere, will have a significant strategic impact because of the difficulty of knowing the true purpose of the broadcast facilities. At the very least, it will create more international tension and suspicion unless special arrangements are made for exchange of keys on benign entertainment links. But any such exchange of keys would defeat the marketability of conference services, so that commercial interests may be directly contrary to strategic interests.



Concurrent learning curves for new technologies.

P.L. 86-36
EO 1.4.(c)

LEARNING CURVES FOR USERS (Fig 40)

(U) When a new technology or service is introduced, it does not usually reach its full development at that point. There is an S-shaped learning curve, and at the beginning progress may be quite slow. At some point the utility levels off.

(U) In service industries there are usually diseconomies of scale because internal coordination and administration increase faster than the size of the organization. One of the schemes for reducing these inefficiencies is for the high-level people, both technical and managerial, to use automatic systems, viz., terminal systems, to get their work done, without having to expend energy in human coordination and administration. Even this kind of scheme implies a long learning time, for individuals or organizations.

~~(C-CCO)~~ The implication to SIGINT is twofold. In the first place, no matter how quickly new technologies and services are introduced into target networks, it will take the target users some time to learn how to use them efficiently, or even to use them at all. Security or political limitations may slow down this learning even more. This creates a theoretical opportunity for SIGINT to pick up the target usage at an early stage, and follow

it as the users become more proficient and extend the usage. However, this creates a requirement for continuity and for slack capacity within the SIGINT system so that some response to new events is possible without tearing up all the existing operations.

[redacted]

~~(C-CCO)~~ In any service activity, the diseconomies of scale are always a peril to competitive survival. SIGINT faces the special hazards that the target telecom nets are expanding inexorably in a way that will defeat any small analytic and processing effort, while at the same time the combination of secret and unknown information, and technical complexity, will force more and more internal coordination--through the "unified integrated" centralized analytic centers. With this combination of an increasing volume of data and greater coordination and decision cost per datum, any mathematical model of the process would explode.

MAIL BOX

From: rcg at BROWN2
Subject: shell game
To: cryptolg at barlc05

Hi,

~~(S)~~ We just received a copy of the August 1982 CRYPTOLOG here at Menwith Hill Station (association with NSA is CONFIDENTIAL). I read with interest the SHELL GAME article. By the way, I think it is a good idea to maintain this kind of interchange.

P.L. 86-36

(U) I have some comments on the shell written by [redacted] to transfer files using cftp. I believe it a good idea to begin using programs which request the user account name and password when connecting to other systems. We all have too many shell files which place the login line complete with password right in the file. The newer version of UNIX (PWB), in addition to including the 'gather' program, provides some new features which may accomplish the same purpose. Specifically, the shell process now allows one to easily read input direct from the terminal. The 'pump' command, implemented within the shell, allows the user to place input parameters into command lines of a called process (like cftp), where normal shell arguments ($1,...) do not work.

P.L. 86-36
EO 1.4.(c)

(U) Also I might note the writer's problem with the line 'stty -echo > /dev/ttyX'. On any Agency UNIX system, the generic device name '/dev/tty' may always be used to specify the current terminal which is being used. Thus there is no need to worry about finding one's terminal ID to put into a shell.

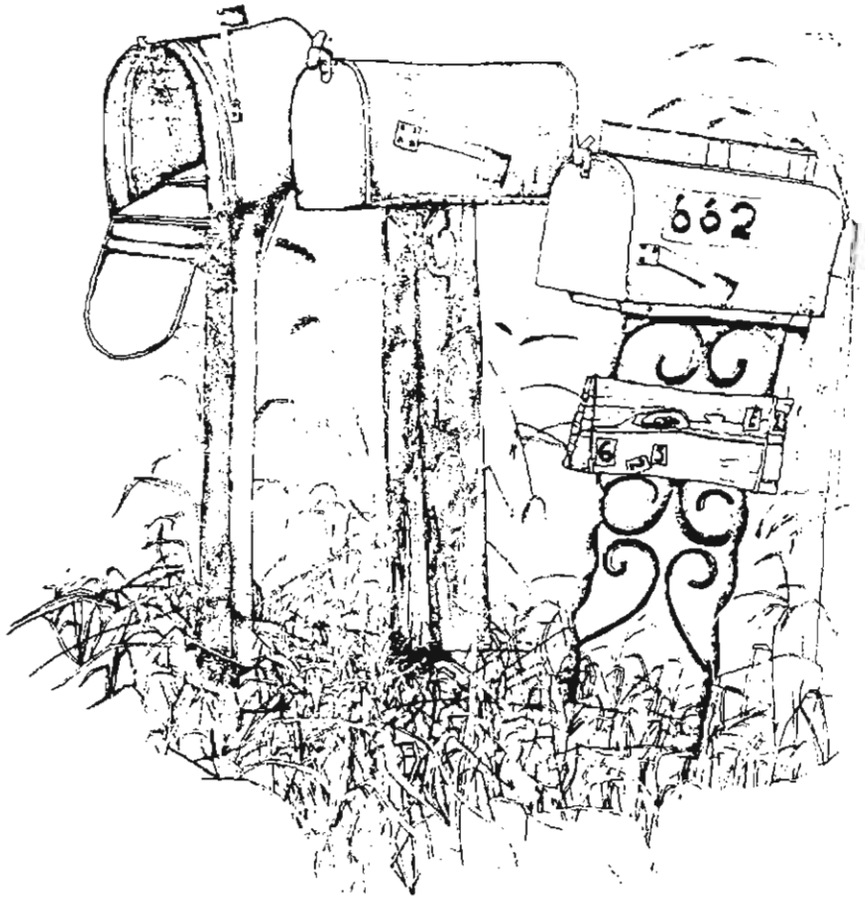
[redacted]

P.L. 86-36

SOLUTION TO NSA-CROSTIC No. 43

"[The] Uses of Elegant English," [redacted] CRYPTOLOG, November, 1976.

"It was Engelbert Humperdinck, I think, who sang a song recently, whose lyrics are the epitome of originality and poetic imagery of which today's songwriters can be so proud. 'I'm yours,' sang Mr. Humperdinck, 'till the stars fall from the sky, for you and I.'"



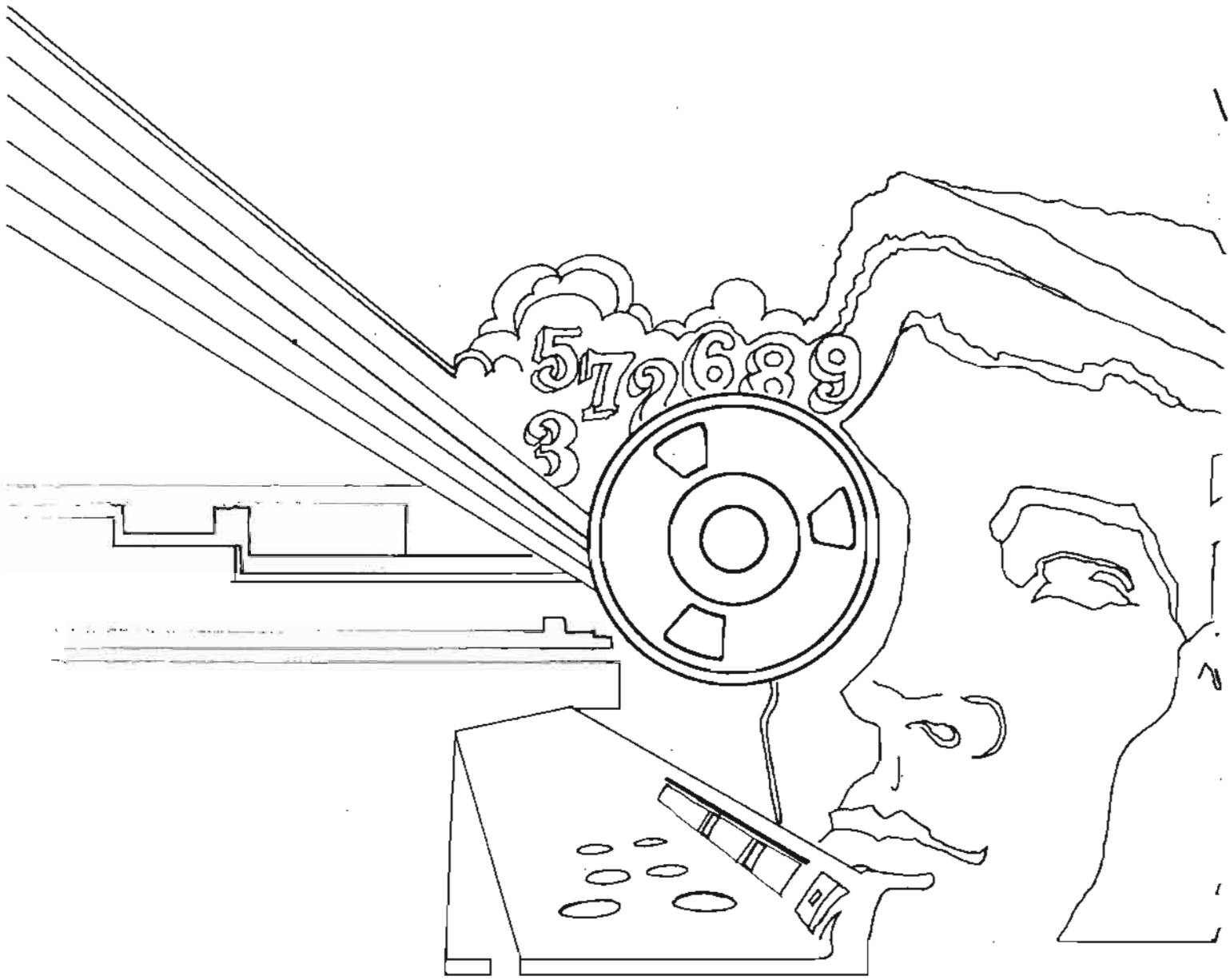
If you would like to have

CRYPTOLOG sent directly to you...

Call

[ ] ***on x3369s.***

P.L. 86-36


5726893

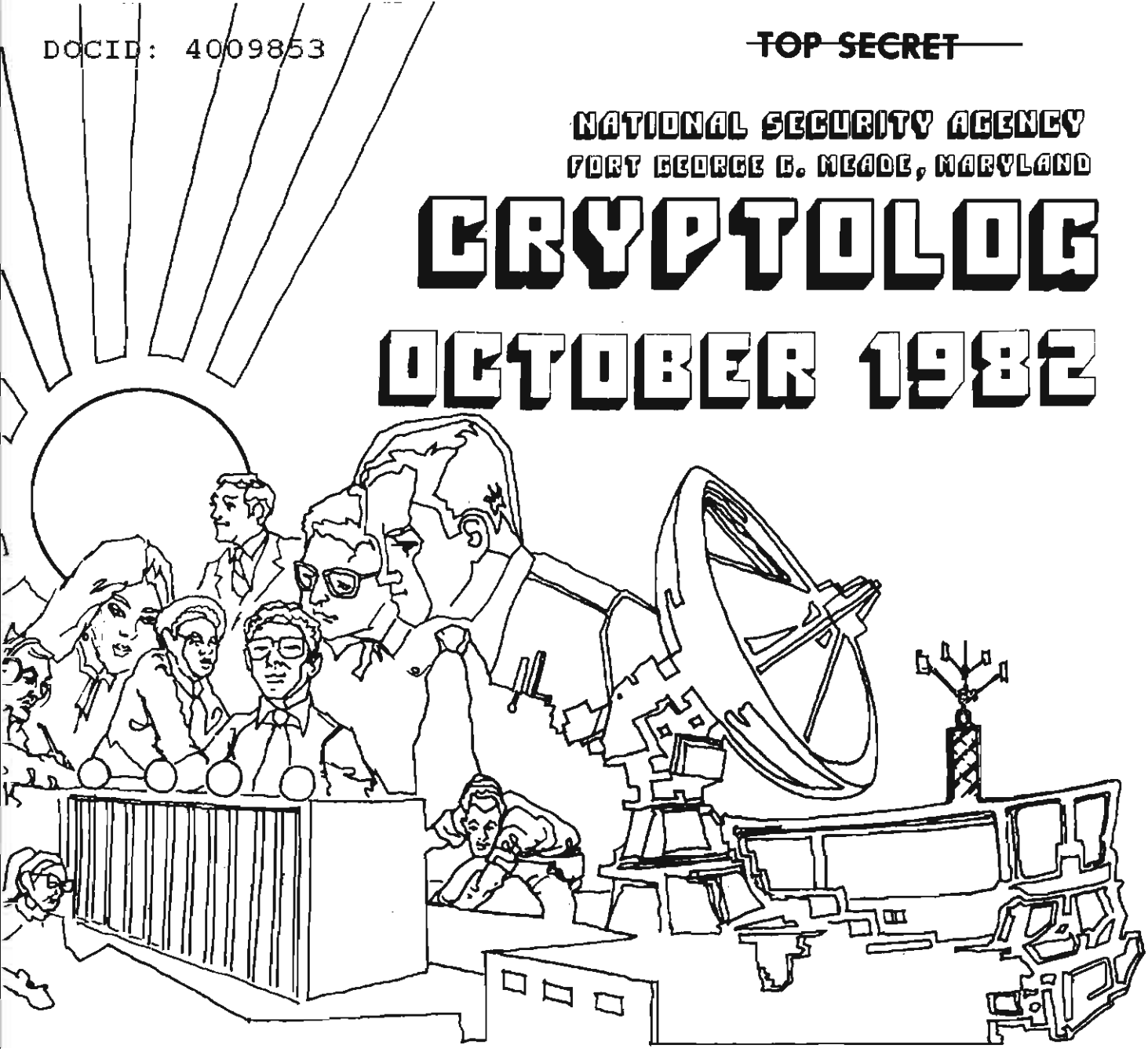
DOCID: 4009853

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

OCTOBER 1982



P.L. 86-36

LEADERSHIP: A PERSONAL PHILOSOPHY (U)..... [redacted] 1
WHAT'S THE GOOD (PASS)WORD? (U)..... [redacted] 6
HUMAN FACTORS: TEXT EDITORS (U)..... [redacted] 9
THE REALITY OF COMMUNICATIONS CHANGES (U)..... [redacted] 12
PUZZLE (U).....14
SIGINT: 1990, Part Two (U)..... [redacted] 16
ANSWER: AN OLD PROBLEM (U).....29
NOT SECRET ANYMORE..... [redacted] 29

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009853

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. IX, No. 10 OCTOBER 1982

PUBLISHER [redacted]

BOARD OF EDITORS

Editor.....[redacted](8322/7119s)
Asst. Editor.....[redacted](1103s)
Production.....[redacted](3369s)

Collection.....[redacted](8555s)
Cryptanalysis.....[redacted](5311s)
Cryptolinguistics.....[redacted](1103s)
Information Science.[redacted](5711s)
Language.....[redacted](8161s)
Machine Support.[redacted](4681s)
Mathematics.....[redacted](8518s)
Puzzles.....David H. Williams (1103s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Don Taurone (3573s)

For subscriptions
send name and organization

to: CRYPTOLOG, P1
or call [redacted]3369s

P.L. 86-36

To submit articles or letters
via PLATFORM mail, send to

cryptolg at barlc@5
(bar-one-c-zero-five)
(note: no '0' in 'log')

NOTE:

The front cover of the September 1982 issue should carry the caveat:

Not Releasable To Contractors

Editorial

"Can two walk together unless they are agreed?" And can they agree unless they communicate? Many of the tasks we find ourselves confronted with these days require a multi-skilled approach. From the manager's point of view, it would be nice to have a lot of multi-skilled people around, so that when a problem came up, one could decide just what mix of skills were needed and then order the proper multi-skilled person(s) to go in and solve the problem. We might even set up a data base and query the computer....

Although managers continue to ask for multi-skilled people to do these tasks, it seems clear that most people learn only one skill at a time. Therefore, most of these tasks requiring a multi-skilled approach must be attacked by using two or more people, each with different skills.

Supervising a group of people with similar skills and perspectives is hard enough, but trying to manage a group of people with various skills and viewpoints is often much harder, especially if the supervisor doesn't have all of those skills. That is probably why managers keep asking for multi-skilled people.

Part of the problem lies in communications. When we talk with people in other skill fields, we may think we use the same language. Mostly, we use the same words--with different meanings. Each skill area develops its own working dialect, borrowing words and changing their meaning to fit the skill area. The answer probably lies in listening to one another.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009853

FOR OFFICIAL USE ONLY

LEADERSHIP: A Personal Philosophy (U)

by [redacted] G12

P.L. 86-36

Each member of the Class of 1982, Army War College, was required to prepare a paper setting forth a personal philosophy of leadership which best met the challenge of a senior leadership position in his organization or agency. This paper was selected by the faculty for publication and is reprinted here by permission of the author.

Leadership has received much attention in recent years from various writers and research groups. The question of how we get people to cooperate on a common task for the purpose of achieving a shared goal has always been a major problem for mankind. Concern with this question has mounted as the complexity of tasks in our world has increased to the point where relatively few jobs can be accomplished by an individual working alone.

Leadership has been defined in several ways by those who have worked in this area:

> "Leadership is the exercise of authority and the making of decisions." (Dubin, 1951)
>
> "The leader is the person who creates the most effective change in group performance." (Cattell, 1951)
>
> "The leader is one who succeeds in getting others to follow him." (Cowley, 1928)
>
> "Leadership is the process of influencing group activities toward goal setting and goal achievement." (Stogdill, 1948)

Two important threads run through all of the above definitions. The first is that leadership is a relationship between people in which influence and power are unevenly distributed. The second observation is that there can be no leaders in isolation. If you want to know whether you are a leader, see if there is someone following you. The difference that makes the difference between successful and unsuccessful leaders is of great importance to me, and I'm sure to the other students here at the War College, as we move towards higher-level civilian and military positions.

THEORETICAL CONSIDERATIONS OF LEADERSHIP

Leadership is always a relative process. To be effective and to communicate as intended, a leader must always adapt his behavior to take into account the expectations, values, and interpersonal skills of those with whom he is interacting. There can be no specific rules of leadership which will work well in all situations. Broad principles can be applied in the process of leadership and furnish valuable guides to behavior. These principles, however, must be applied always in a manner that takes fully into account the characteristics of the specific situation and of the people involved.

FOR OFFICIAL USE ONLY

DOCID: 4009853

It is possible to state principles of leadership in such a way that they are incapable of empirical refutation and appear equally consistent with quite different forms of leader behavior. To say that a leader should manage in such a way that personnel at all levels feel real responsibility for the attainment of the organization's goals (Likert, 1967) or alternatively, that he should exhibit concern for both production and people (Blake and Mouton, 1964), is not saying a great deal about what he should do in the concrete situations that he faces daily.

The increasing tempo of our social evolution requires improved human relations techniques and increased knowledge of the social sciences in contrast to the greater emphasis on mechanical techniques and the natural sciences in the past. To cope effectively with these shifting demands, the successful leader must have a keen sense of timing and adaptation. He must learn to "roll with the punch" and yet maintain a gyroscopic guidance for the organization, keeping it within the confines of fundamental principles and headed toward a sound objective.

Over the past three decades, research has been conducted into the relationships between the four styles of leadership

- high-initiating-structure, low-consideration;
- high-initiating-structure, high-consideration;
- low-initiating-structure, high-consideration;
- low-initiating-structure, low-consideration,

productivity, and employee satisfaction. The findings were neither consistent nor definitive. The major conclusion that can be drawn from these studies is that, as previously stated, there is no one best style that is appropriate for all situations.

HOW WE CAN GET THERE FROM HERE OR HOW I WOULD RUN (MANAGE) MY AGENCY

My initial thoughts on how I would run such a massive intelligence organization as the National Security Agency coincided, to a large degree, with those functions of an executive as delineated in numerous writings on administration. These leadership duties essentially are as follows:

1. Planning: determining what should be done--including clarification of objectives, establishment of policies, mapping of programs, and determining methods and procedures.

2. Organizing: grouping the activities necessary to carry out the plans into administrative units, and defining the relationships among the executives and workers in such units.

3. Assembling resources: obtaining the personnel, capital, facilities, and other things needed to execute the plans.

4. Directing (issuing instructions): Indicating plans to those who are responsible for carrying them out, and stressing personal relationships between the "boss" and his subordinates.

5. Controlling: seeing that operating results conform as nearly as possible to the plans--the establishment of standards, motivation of people to achieve these standards, comparison of actual results against the standard, and necessary corrective action where performance deviates from the plan.

DOCID: 4009853

However, after some intensive reflection on this subject, other salient aspects began to emerge which embrace, if you will, my personal philosophy of leadership. Firstly, I believe that leadership is the process of influencing a group or getting others to accomplish things. A leader doesn't necessarily have to solve problems; rather, his job is to get problems solved. TO MAKE POLICY IS EASY; TO MAKE IT HAPPEN IS DIFFICULT. During my twenty years as an analyst at NSA, I have been exposed to a variety of managers, some good and some not so good. The manager I have the greatest respect for is an individual who:

(a) delegated responsibility to me without hesitation;

(b) trusted me fully;

(c) listened intently to problems and recommended solutions; and

(d) supported me completely.

If I occupied the top position at NSA, I would make every effort to emulate my favorite manager's leadership style to the maximum extent possible. One of the most important things that I learned from him was that the higher your position is, the more (no less) dependent you become on others.

Secondly, I believe that a leader must be courageous and possess the ability to make rapid but sound decisions. As you are aware, intelligence information come from a variety of sources and is often fragmented and incomplete. Even in the absence of complete and vital data, I would not hesitate in making the critical decision required. Remember, the moment of absolute certainty never arrives. One can never be 100 percent sure of anything.

Thirdly, I can not overemphasize my feeling that leadership style must rise above day-to-day activities. I strongly believe that a leader must have the mental agility and the creative vision to conceptualize how "things come together." As the Director, NSA, I would make a concerted effort to instill in my subordinates that in order to become effective leaders, they must possess the courage to dream, the ability to organize, and the strength to execute. My first step would be to host an informal gathering of my top-level executives (Office Chiefs for Planning, Operations, Budgeting, Research and Development, COMSEC, etc.) at some secluded location that was conducive to relaxation and reflective thinking. To set the tone for this session, I would cite some inspirational remarks made by the following outstanding leaders who were truly men of vision:

"Ask not what your country can do for you, but what you can do for your country."

John F. Kennedy

"I have a dream...."

Martin Luther King

"Some men see things as they are and say why. I dream things that never were and say why not."

Robert F. Kennedy

I would then ask my executives to provide a frank assessment of their individual leadership skills, style, and effectiveness, with particular emphasis on the following general areas:

(a) Working with people;

(b) Personality and character traits;

(c) Making decisions;

(d) Developing and selling ideas;

(e) Delegating responsibility.

The next step would be to compare their evaluations with the following criteria that I have personally established for these general areas.

DOCID: 4009853

Working with people

Working with your superior: Dependability and follow-through constitute two of the strongest measures of effectiveness in working with your superior. Initiative and doing more than expected make the best sales approach for a subordinate in building himself up in the eyes of his superior. It is always constructive to help the superior by supplementing his weaknesses, particularly when this can be handled with a reasonable degree of finesse and understanding.

Working with your associates: Make yourself easy to get acquainted with and to work with--loosen up--be adaptable. Be alert to your associates' attitudes--develop sensitivity. Learn how they react and what motivates them--develop objectivity. Show interest in your associates; seek advice from them, and go out of your way to help them.

Working with your subordinates: In working with subordinates, the necessary respect, prestige, and confidence to warrant acceptance as a leader must be earned. Such acceptance results from a consistent application of high personal standards and sound principles and from a good quality of decisions and ideas. A leader should seek the advice of his subordinates on problems and keep them posted on new policies and programs. He should help them to start new projects and carefully evaluate results of completed work. He should also outline their duties and responsibilities, preferably in writing, in terms which the subordinates can understand. Planning the work and having a program are great assets in effective leadership.

A leader should learn to inspire confidence and develop enthusiasm in subordinates. He should be a good listener, show a sympathetic understanding, and try to see the other fellow's viewpoint. He should keep the group "looking ahead" with a well worked out program. He should take an optimistic view whenever it is feasible and make subordinates comfortable when the "going is tough." He should show confidence by expecting much and letting subordinates know that he does expect much. He should compliment people when it can be done appropriately and sincerely, and he should, in fact, look for opportunities to do so.

Personality and Character Traits

I consider purposeful energy, progressiveness, intensity, and health as being particularly necessary to the successful leader.

Purposeful energy is commonly reflected in enthusiasm, initiative, and optimism.

Progressiveness is often reflected in the ease of generating and accepting new ideas.

Intensity and drive are characteristics of the outstanding executive which make him and his job almost one. A real leader reflects his job, and the job reflects his personality.

Health is a factor of growing importance. The requirements of leadership are becoming more exacting and complex, and the tempo continues to rise. The increasing frequency of hypertension, heart ailments, and stomach ulcers among executives, particularly those of middle age, should be viewed with alarm. More real relaxation, better planned vacations, and greater hobby interests are certainly desirable.

DOCID: 4009853

Making Decisions

Sound decisions are generally based on a combination of background knowledge, available facts, and exercise of judgment.

The knowledge element in decision-making is primarily derived from theories, principles, and practical experience. Good executives will coordinate, group, and use other people's knowledge for their mutual benefit.

The facts element is highly important in arriving at correct decisions. The ability to recognize facts, to know what facts are available in connection with each particular problem, to be able to assemble them, and then to analyze and interpret them, is fundamental to good leadership.

The judgment element includes drawing sound conclusions based on knowledge and facts. It involves thinking effectively--sifting the important elements of the problem from the superficial and exercising perspective.

Developing and Selling Ideas

A leader must get ideas easily. Hence he should try to develop his imagination. Ideas must first be obtained, then tested and timed for presentation, and finally sold to others for application.

Ideas usually originate from knowledge or research. I believe that every important office in my agency should continually apportion some of its time to research for new solutions and new ideas.

A leader must learn to sell ideas--to get his thinking across to others. One approach is to learn to write well organized, clear, convincing, and short memorandums. Another is to learn to conduct himself well in a conference, to go to a conference with a plan of attack, with suggestions and not just to sit in. And still another is to learn to speak to small and large groups; this not only builds personal prestige but is virtually a "must" for present and future leaders.

One should feel and express conviction in selling ideas. The old saying, "be sure you're right--then go ahead," certainly applies. At the same time, to avoid creating negative resistance, the degree of aggressiveness must be moderated by the proper amount of tact, finesse, and understanding.

Delegating Responsibility

A leader must be willing to delegate responsibility and to decentralize authority. You have to trust your people to do the job required. In working with subordinates, a leader should remember that one of the greatest human desires is to create or produce something, and to feel essential. Furthermore, as I previously stated, the higher your position is, the more dependent you become on others.

I truly believe that from the discussions generated in the "exercise" described above, leadership strengths and weaknesses can be identified and corrective actions can be taken to facilitate/promote effective leadership at my agency. If a leader develops his executives, he will in turn be even stronger. You can handle people more successfully "by enlisting their feelings than by convincing their reason."

~~FOR OFFICIAL USE ONLY~~

WHAT'S THE GOOD (PASS)WORD?(U)

by [redacted] T4

DDT Senior Computer Security Coordinator

P.L. 86-36

A computer security compromise was recently discovered here at NSA, by an evaluation team from C1, the Computer Security Evaluation Center. The team was evaluating the computer at the request of DDT.

The compromise was the result of an administrative error. The system administrator had made a copy of the password file, which included the identifier and the encrypted password of all users of the system. However, the protection bits for the file were improperly set and the file could therefore be read by anyone on the system.

The evaluation team attempted to see how many passwords could be discovered from this file. They tried guessing passwords, sending them through the password encryption process to see if they matched: they recovered some passwords. The team then sent a dictionary of common words through the encryption process and compared the results: still more passwords recovered. Then the team tried all five letter values from aaaaa to zzzzz: in three days, they recovered a total of 107 of the 255 passwords in the file.

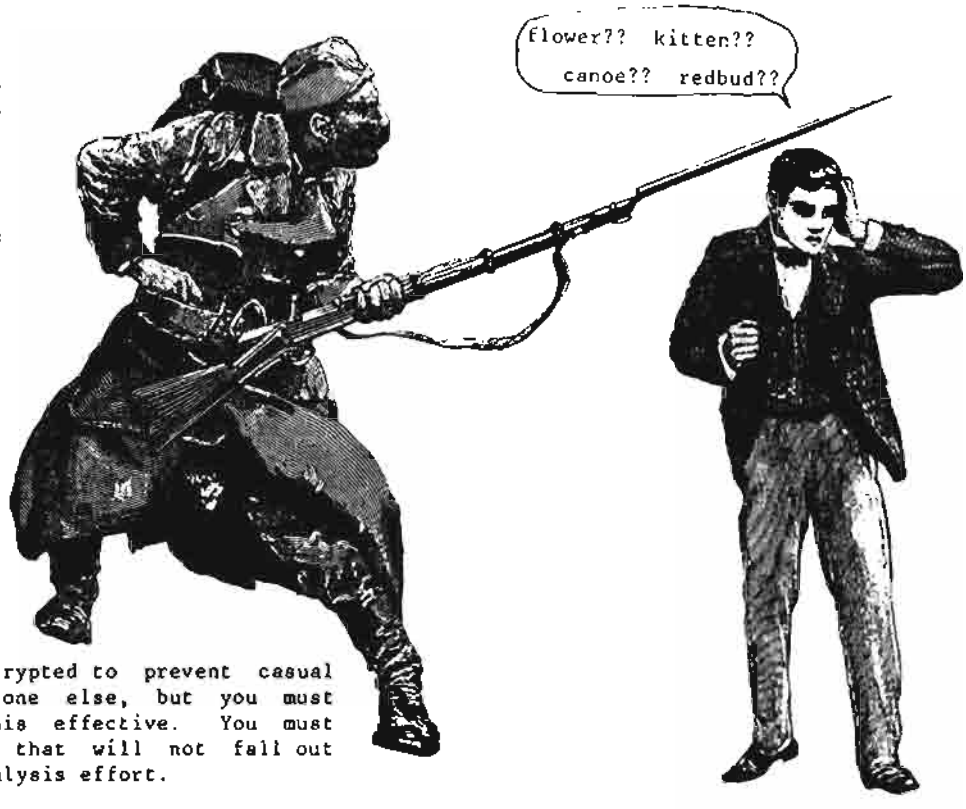
All users of the system have been directed to change their passwords, and the system administrator will be more careful about protecting the file in the future. In order to give the general user some idea of the kind of password that is easily guessed or discovered, the following is the list of passwords recovered by the team.

LIST OF RECOVERED PASSWORDS

abyss	escort
aesir	eyeball
again	fairway
apple	fishs
april	flower
backward	freedom
bandit	funny
barba	geisha
baseball	genie
beaver	golden
beetle	green
bible	happy
bingo	hawthorn
bluetop	holiday
brogue	horse
bushed	intel
candy	ironside
canoe	joewood
chance	kelly
check	kingfish
cjunk	kitten
confused	lambda
converse	landing
copper	lemon
crazy	locked
design	logic
digital	login
dogwood	lumpy
donna	major
drifter	michael
dumbo	mikey
eagle	mouth
elephant	muffin
empire	murphy

~~FOR OFFICIAL USE ONLY~~

nroha	snowball
omega	softball
panel	ssret
panelist	stage
perch	striper
permit	summer
pmrmd	sunshine
poets	susan
popcorn	tacos
puissant	testing
rabbit	tracing
radec	update
redbud	vision
romance	vkjrd
sailing	westward
scooter	wicks
scrabble	wildlife
security	window
shari	wizard
silver	



Passwords are encrypted to prevent casual recovery by someone else, but you must cooperate to make this effective. You must choose a password that will not fall out through a simple analysis effort.

The simplest factor you control is the length of the password. The longer the password, the better. If the password vkjrd in the list above had been one character longer, it would have taken about 26 x 2 1/2 days, or 65 days, to recover it.

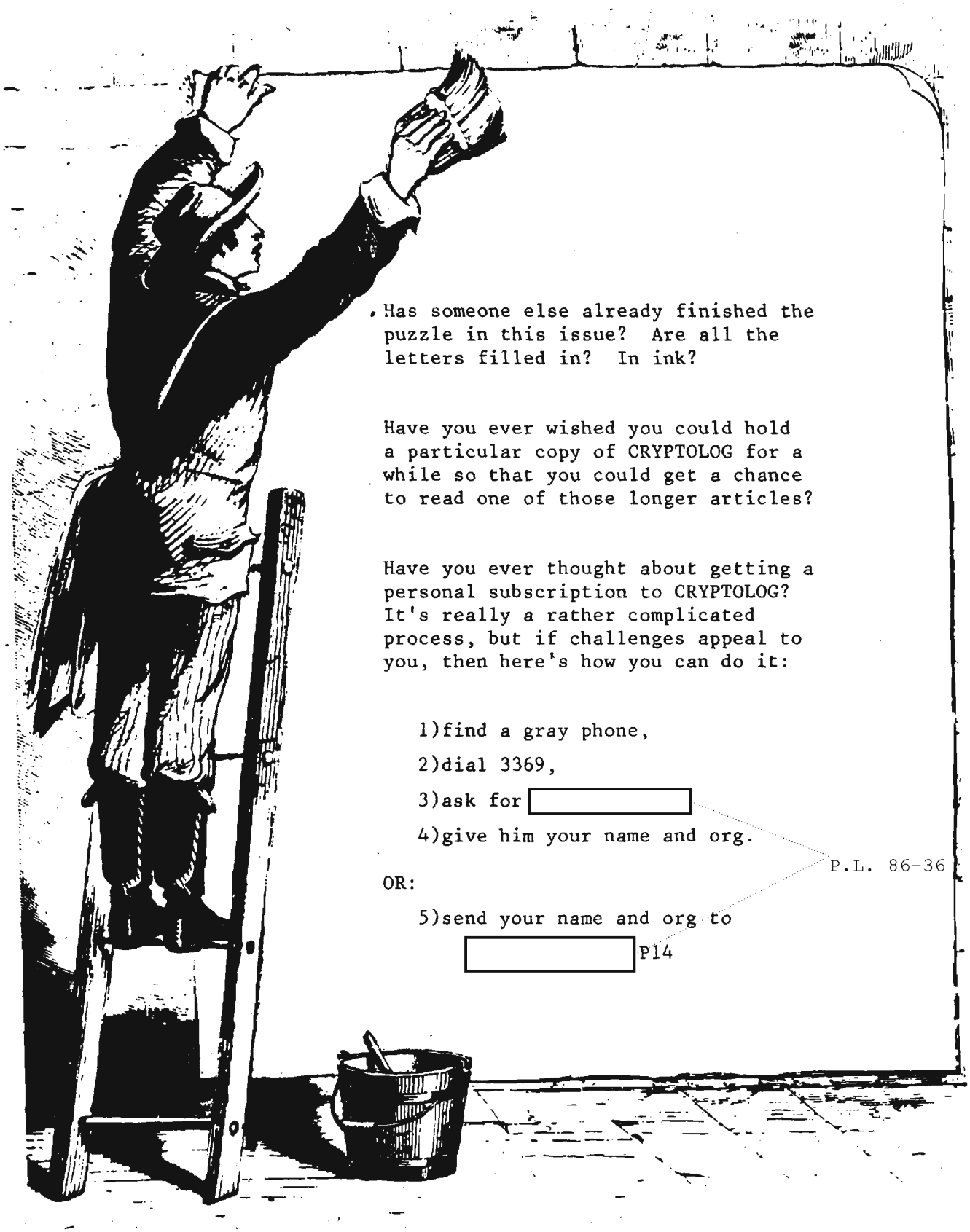
The table tells you that, if you use only a single lower case letter as a password, it can be recovered in, at most, 26 tries. If you use eight characters of lower case, upper case, numerics, and punctuation, then it could require 1,000,000,000,000,000 tries to recover your password.

A second factor that you control is the alphabet size. If you mix in both upper case letters and numbers, you increase the number of tries needed by the exhaustive method (i.e., trying every possibility). Note that there is not a single upper case character in the above list of recovered passwords.

A good password is eight or more characters in length. At least six different characters should be included. You should select uncommon words. Mixing in some upper case characters, along with numbers and punctuation characters, helps defeat discovery through exhaustive search.

EXHAUSTIVE TRIES NEEDED

	Alphabet Size	Password Length 1	2	4	6	8
Lower Case Letters	26	26	676	456,976	3.08×10^{8}	2.08×10^{11}.
Upper and Lower Case	52	52	2704	7.3×10^{6}	1.9×10^{10}	5.3×10^{13}.
UC, LC and Numbers	62	62	3844	1.4×10^{7}	5.6×10^{10}	2.1×10^{14}.
UC, LC, NR, Punctuation	75	75	5625	3.1×10^{7}	1.7×10^{11}	1.0×10^{15}.



Has someone else already finished the puzzle in this issue? Are all the letters filled in? In ink?

Have you ever wished you could hold a particular copy of CRYPTOLOG for a while so that you could get a chance to read one of those longer articles?

Have you ever thought about getting a personal subscription to CRYPTOLOG? It's really a rather complicated process, but if challenges appeal to you, then here's how you can do it:

1)find a gray phone,

2)dial 3369,

3)ask for [redacted]

4)give him your name and org.

P.L. 86-36

OR:

5)send your name and org to

[redacted] P14

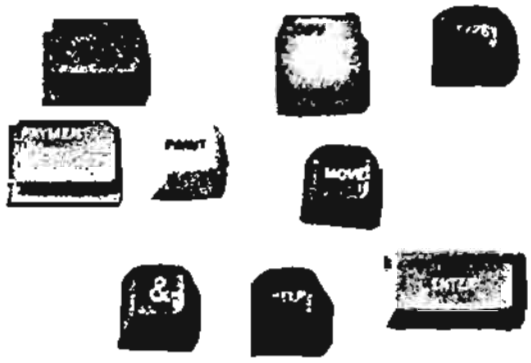
DOCID: 4009853

~~FOR OFFICIAL USE ONLY~~

HUMAN FACTORS:
Text Editors (U)

by [redacted] P13

P.L. 86-36



REVIEW: HOW DO PEOPLE REALLY USE TEXT EDITORS?, J. Whiteside, et al, Proceedings of SIGOA Conference, Philadelphia, 21-23 June, 1982.

This study, carried out by five researchers at DEC (Digital Equipment Corp.), compared knowledge workers and secretaries performing their normal work with two different text editors. Keystroke statistics were gathered during normal usage of the editors. Both of the editors were screen editors. One, called EPT (Editor Prototyping Tool), was an experimental editor which contained a built-in keystroke logging facility. It permitted a simple set of editing functions, including cursor movement anywhere on the screen, search, text relocation, and text deletion. Text could be inserted or overprinted in modes activated by a function key. It did not offer the formatting functions included in most word processors, but it did provide automatic word wrapping. The other editor, WPS, was DEC's 200-Series commercial word processor. It was a character-oriented, screen editor in which editing was done on the bottom line of the screen. The cursor could be moved anywhere within the boundaries of existing text. It had logical equivalents for all EPT functions, but also offered many more functions, including sophisticated text-formatting.

Six knowledge workers were studied as they used EPT to create and revise their own reports and memos; they had at least three weeks experience with EPT before the test began. Eight secretaries provided the sample of WPS usage as they carried out their regular secretarial and administrative duties in a DEC R&D department. Their experience with WPS varied from one month self-taught to two years and three training courses. EPT keystrokes were logged by a built-in facility, while WPS keystrokes were captured by a PDP 11/34 computer. For both editors, the logging of keystrokes was accomplished in such a way that editor performance was not affected. Each keystroke was logged along with the time of occurrence.

The results of the study are highly interesting, and I believe they are directly relevant to our work situations. Neither EPT nor WPS is probably directly comparable to the text editors we use; EPT may be somewhat similar to the UNIX Rand Editor. Still, it seems probable that the essential editing functions (printing characters, cursor movement) are comparable across different editors. The methodology of the study has even more to offer than the results, in my opinion; I would very much like to see analyses of this kind carried out on many of our interactive systems, text editors and otherwise.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009853

The data was first studied at the level of individual keys: What proportion of total keystrokes for all users was taken up by pressing each key? What proportion of the total time was used pressing each key? What was the average time per keystroke?

Transition probabilities were computed for pairs of keys: How likely is it that a user will press key B after pressing key A? The degree of randomness or organization in the pair transitions, and the degree of predictability in longer strings of keystrokes were studied in various ways. Finally, keystrokes were grouped into larger classes to provide a more global analysis in terms of "states," making it easier to compare results with different editors in terms of basic functionality for the user.

Here are some highlights of the results, adapted and simplified from the author's tables:

"Inactive" time was logged whenever no keystrokes occurred for a period of more than 150 seconds. The secretaries usually turned on their machines as soon as they came in in the morning and left them turned on all day, while the knowledge workers were using EPT on a time-sharing system and were less likely to leave the editor running when they weren't actually using it. The actual work hours and total keystrokes are quite comparable in the two samples; in fact, the six EPT users generated a few more keystrokes within slightly fewer work hours than the 8 secretaries. This seems highly interesting in itself. I would like to know more about this unexpected showing, in which six people who were not (presumably) trained typists but professionals doing their own documentation turned out more keystrokes in a shorter time than eight people whose primary task was skilled typing! Unfortunately, the paper does not address this point, so we are left in the dark about it. It may have been related to the text editors, in that WPS may have provided more power with special functions, so that the secretaries could accomplish more with fewer keystrokes. It raises a question about assessments of productivity based on keystrokes per person/hour, in any case.

CHARACTERISTICS OF USERS AND WORK SAMPLES

	EPT	WPS
Type of Editor	Simple Screen Editor	Sophisticated Commercial Word Processor
Users	6 Knowledge Workers	8 Secretaries
Total Person-Hours	212	482
Inactive Hours	127	390
Active Work Hours	86	92
Total Keystrokes	510,513	406,102

DOCID: 4009853

INDIVIDUAL KEYSTROKES IN EPT AND WPS

EPT		
KEY	% OF STROKES	% OF TIME
Print Char.	53.58	46.84
Left-Arrow	12.90	5.08
Right-Arrow	12.52	5.49
Delete	7.35	7.38
Down-Arrow	5.67	9.89
Up-Arrow	3.15	5.89
Return	1.38	4.38
Tab	1.01	1.66
Word	.34	.39
All Other	2.10	13.00

WPS		
KEY	% OF STROKES	% OF TIME
Print Char.	54.81	47.48
Advance	15.48	11.91
Line	10.30	6.27
Backup	6.59	7.41
Rub Char.	3.33	3.35
Return	2.83	8.08
Tab	1.52	1.79
Word	1.24	.65
Delete Char.	1.11	.90
All Other	2.79	12.16

Typing in characters accounted for a little more than half of all keystrokes, and nearly half of all time, in both editors. "Arrow" cursor movements in EPT accounted for about a third of keystrokes and a quarter of user time, while "Advance", "Line", and "Backup" (cursor-movement keys in WPS) accounted for very similar portions of keystrokes and time. Nine key types out of a total of 29 in EPT accounted for 98% of keystrokes and 87% of time, while nine key types out of a total of 64 in WPS accounted for 97% of keystrokes and 88% of time. Thus, even at the level of individual keystrokes, these two apparently quite different editors were used in a very similar way by two highly different sets of users. The authors of this paper summarize these results as follows: "A rough rule of thumb that emerges from our data is that free usage text editing consists of about 1/2 typing, about 1/4 cursor movement, about 1/8 deletion, and 1/8 all other functions put together. This rule has been shown to apply in two different situations: knowledge workers creating documents with an experimental text editor, and secretaries transcribing and updating documents on a commercial word processing system." (p. 37)

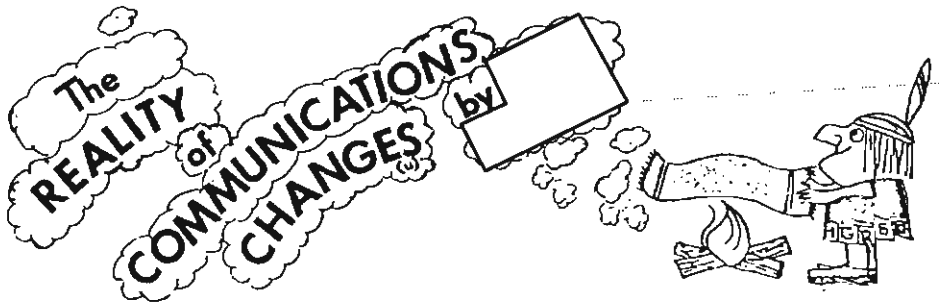
The grouping of keystrokes into states produces results that modify these proportions somewhat, as the table above shows. Typing uses up a bit more than half and cursor movement more than a third of the keystrokes. "Erasing" accounts four four times as many keystrokes as the "all other" category in both editors. It is interesting to note that the knowledge workers gave twice as much weight to "erasing" than the secretaries did. No explanation is offered for this difference in the paper. Perhaps the secretaries made fewer typing errors; on the other hand, the difference may be related to creation of documents by the knowledge workers. Composing an original document might be expected to call for more erasures than transcribing or updating a document originated by someone else.

I recommend this paper to all readers interested in human factors in our Agency. In my opinion, it represents the kind of well-designed, practical study we should be doing to obtain more hard data about user/system interactions in our offices.

STATES IN EPT AND WPS

	PERCENT OF KEYSTROKES	
STATE	EPT	WPS
Type	55.97	59.16
Cursor	34.39	34.45
Erase	8.27	4.44
All other	1.37	1.95

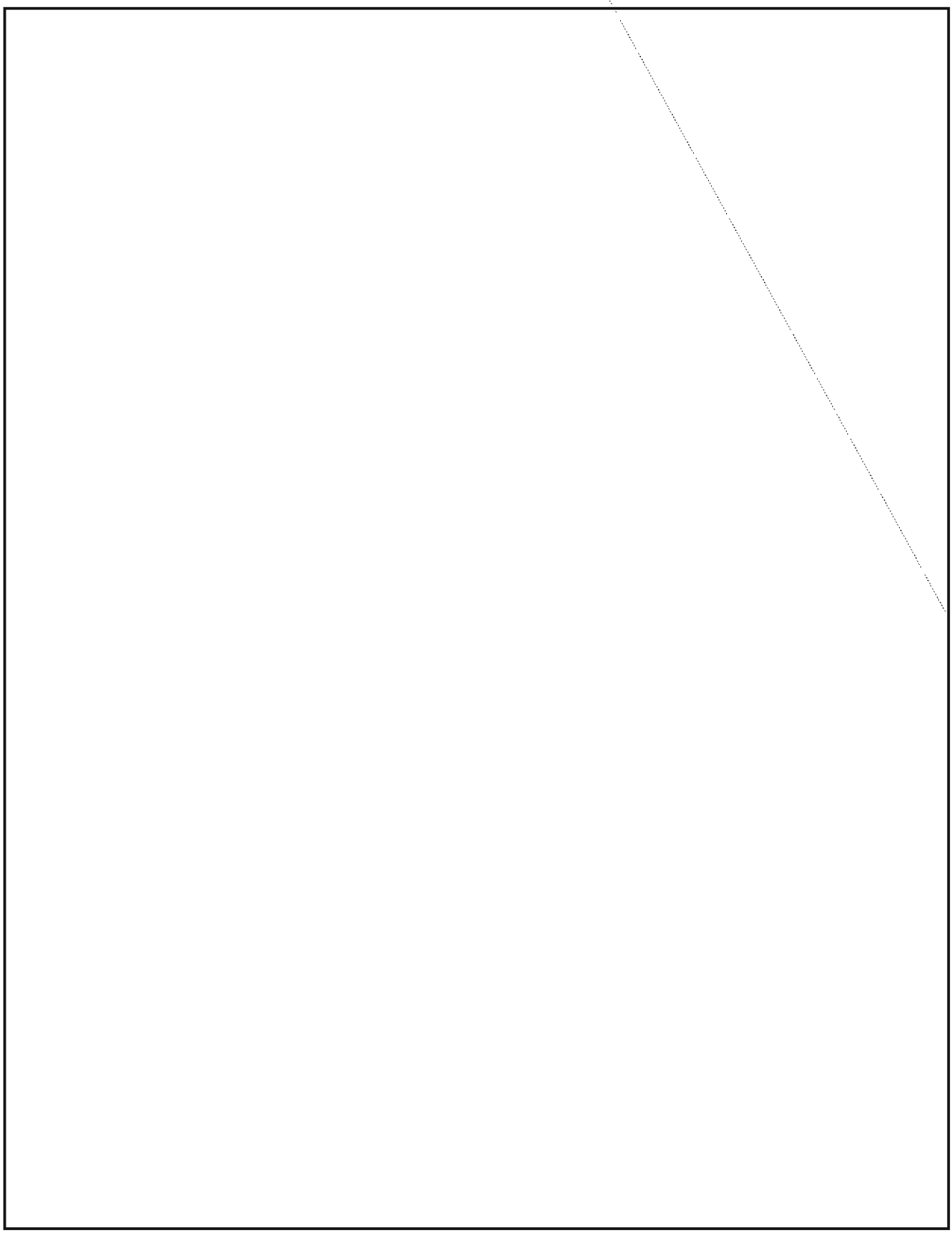
GOLDEN GLOW



P.L. 86-36

Reprint from DRAGON SEEDS, June 1972

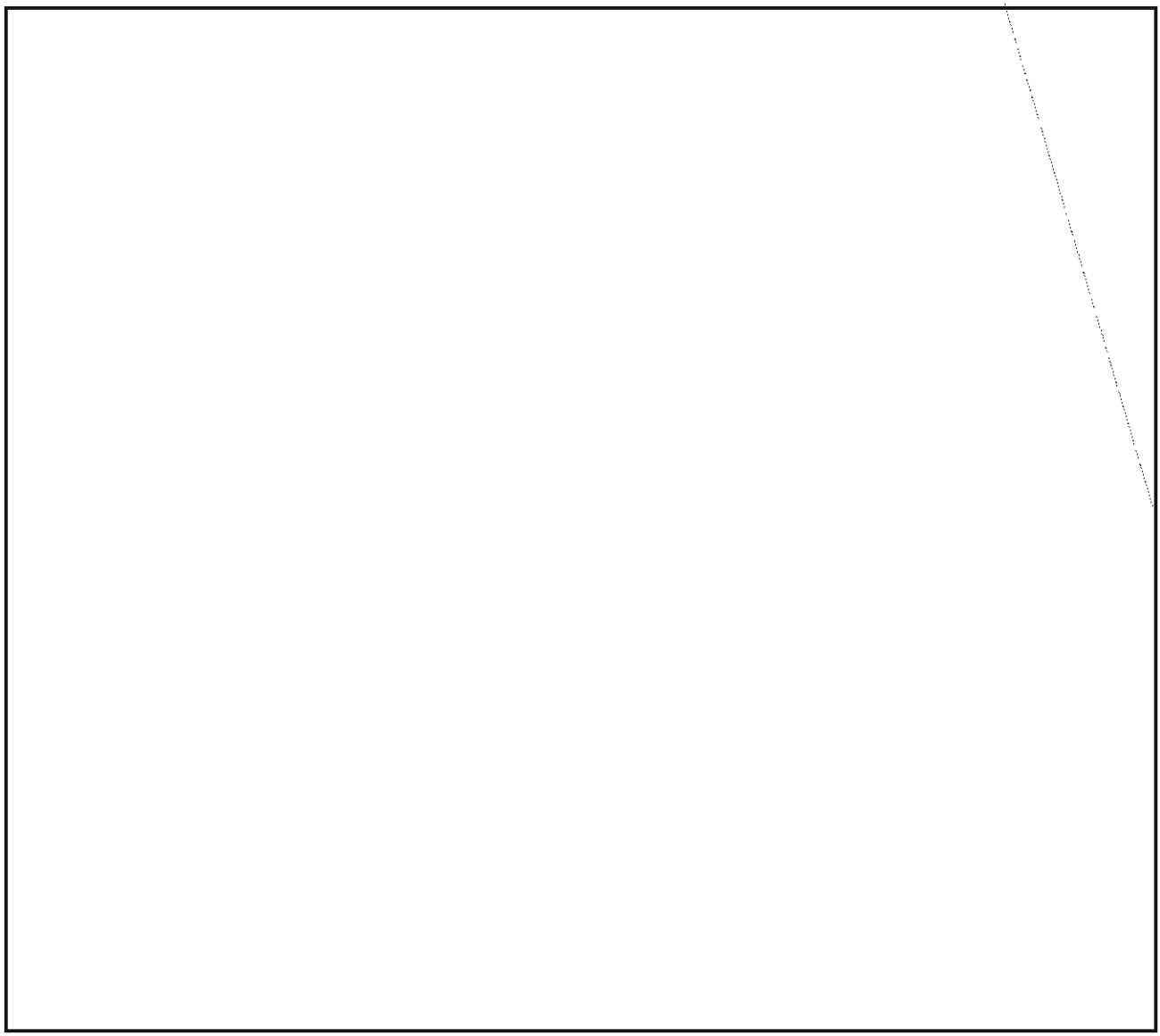
EO 1.4.(c)
P.L. 86-36

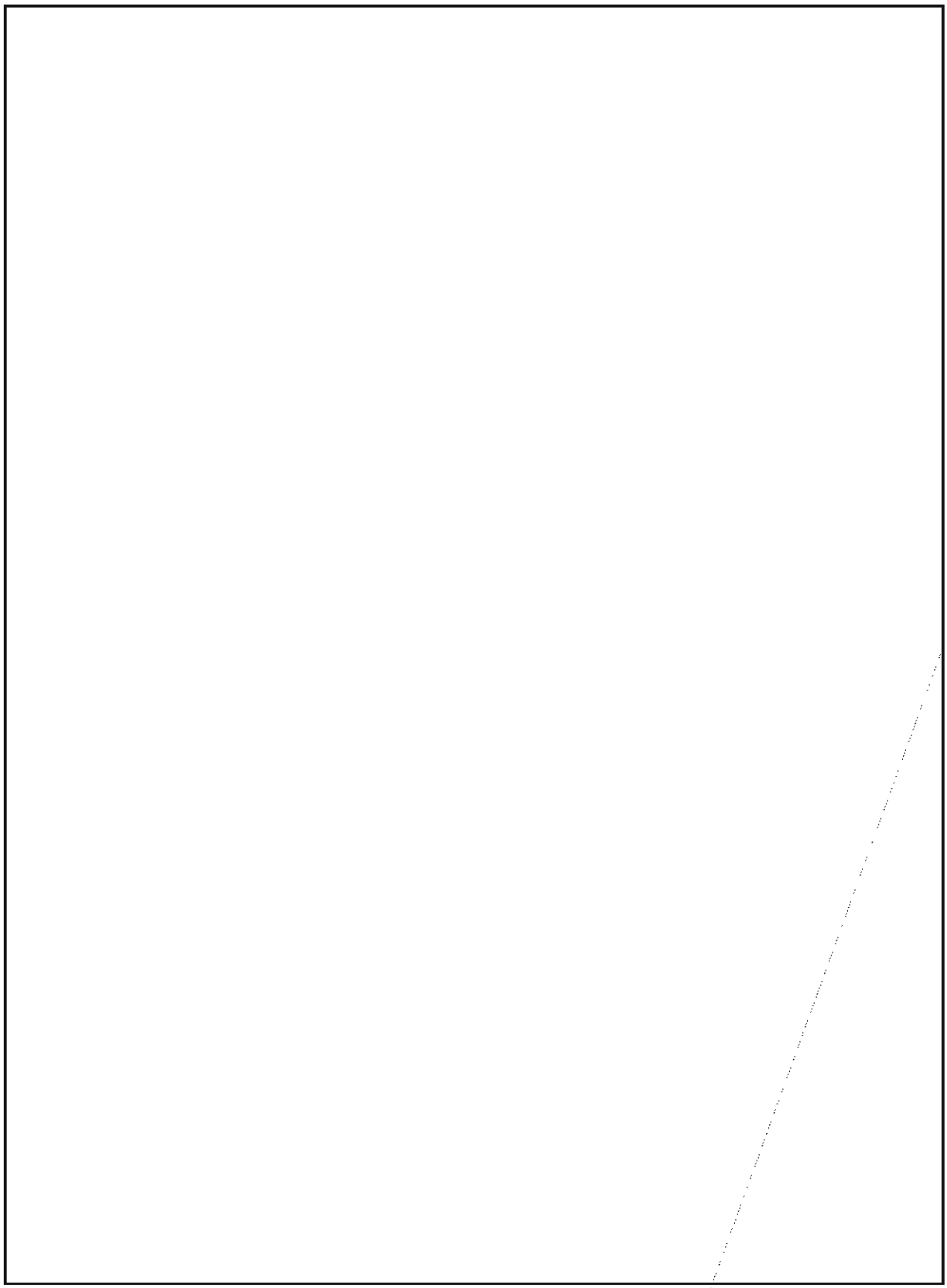


DOCID: 4009853

P.L. 86-36

NSA~Crostic No. 43





P.L. 86-36

EO 1.4.(c)
P.L. 86-36

SIGINT: 1990 (U)

P.L. 86-36

Part 2

by [redacted] P13

OPTICAL FIBER

[redacted]

OPTICAL FIBER COMMUNICATIONS (NEC)

What new problems will SIGINT have to face by 1990? What do the new trends in technology tell us about the not-so-distant future? The author has adapted this article, presented here in the second of several monthly installments, from his presentation at a January 1982 session of CA-305.

(U) Initial applications of optical fiber were for specialized applications, such as the communications circuits (see figure 21) that were installed with buried power cables. The fibers were unaffected by the powerful electrical fields, and gave reliable wideband circuits. Other specialized applications used the resistance to electrical noise and interference for shipboard and military applications, despite the fact that neither the glass nor the electro-optical components were very good.

(U) Rapid advances in glass technology and in laser and LED (light-emitting diode) and detector technology have occurred during the past ten years. These improvements have made short-distance circuits, e.g., within computer nets, economically feasible, and the telecommunication operators are beginning to install short-distance and medium-distance (up to a few kilometers). circuits in parts of the existing networks.

(U) By 1990 better glass and more reliable electro-optical components will make long distance trunks economical, and by the mid 1990's optical fiber loops will be introduced from the local switches to subscribers' premises. By 1982 the various Bell System companies had already installed over 25,000 miles of optical fiber trunk. A typical application will be the Northeast Corridor, a 400-mile trunk from Washington to Boston, using 3C digital transmission at 90 Mbps/fiber. Some fiber systems will use three separate light wavelengths at once, to give 270 Mbps/fiber. Typically an installed fiber system will have 12 fibers, with repeater spacing at 35 kilometers. Since coaxial cable repeater spacing is

DOCID: 4009853

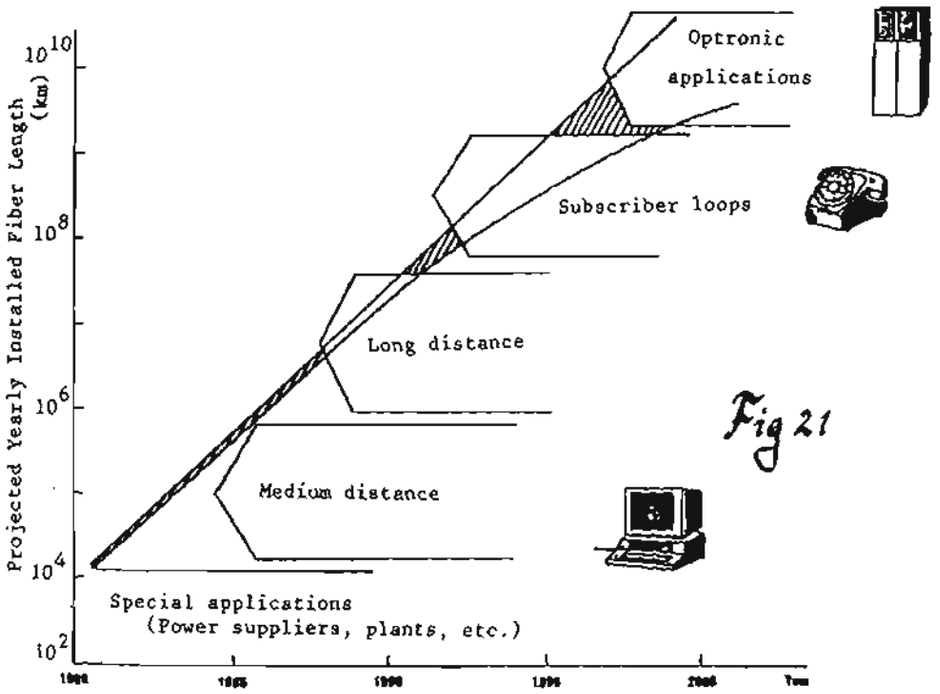
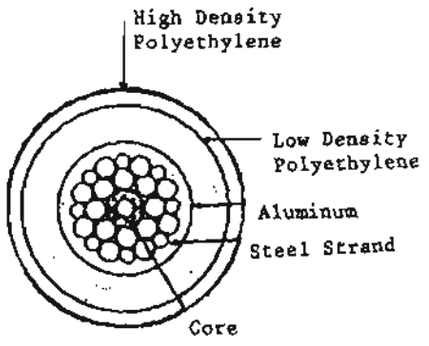
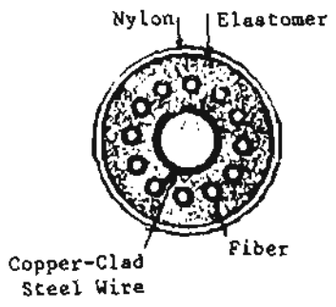


Fig 21

OPTICAL FIBER COMMUNICATIONS



CABLE



CORE DETAIL

Fig 22 UNDERSEA FIBERGUIDE CABLE

about 4 km, the optical fiber offers big improvements in system design, maintenance, and cost.

(U) NEC predicts a million kilometers of installed fiber by 1985 and 100 million kilometers by 1990. Since the Japanese are among the world leaders in both the technology and the marketing, they are in a position to make this prophecy materialize.

UNDERSEA OPTICAL FIBER CABLE

(U) One of the most dramatic illustrations of the advances in optical fiber is the development of a transatlantic optical fiber cable (fig 22), to be operational by 1988, which will carry 72,000 two way voice channels between the U.S. and three foreign countries over a 6500-km undersea cable. Transmission bit rate will be 375 Mbps per fiber, and a TASI (Time-Available Speech Interpolation) will be used to triple the traffic capacity.

(U) Power will be supplied over a copper-clad central steel cable, and a dozen single-mode fibers will surround the core. SG cable repeaters will be used, with a regenerator for each fiber, spaced at 35 km. The system is expected to have a 25-year life. The first cable will probably be the start of a revolution in transoceanic communications, just as the first transoceanic coaxial cable began the explosion of transatlantic telephony.

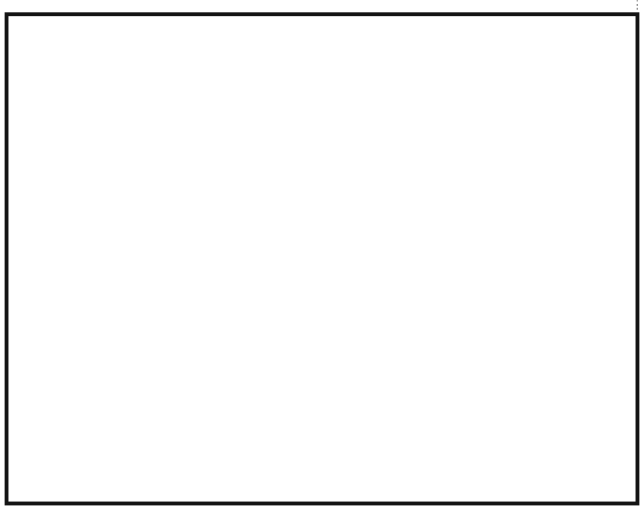
(U) While the AT&T undersea fiber trunk will use digital regenerators, the Japanese are now proposing a 5000-km undersea optical fiber cable with no regenerators, which will use linear optical amplifiers along the fiber. This will allow changes to the digital technology at the cable ends as technology improves. Experiments have already shown that power can be sent along light fibers to operate remote devices, so a completely optical system, with no electrical power or copper wire, should be feasible.

COST COMPARISON FOR UNDERSEA SYSTEMS

(U) Analysis by BTL has shown that, compared to the older 30MHz coaxial cable systems, the 274 Mbps optical fiber cable will give a 5-to-1 improvement in circuit costs. The very high bit rate will make special services such as video, video conferences, and data services feasible.

(U) While satellite technology will improve over the same time period, satellites are a stable technology, while optical fiber is still going through explosive growth in performance. The critical choke point in satellite communications is at the midocean points, where demand for spectrum and services is growing, while orbital and spectrum resources are fixed. The development of intersatellite links will relieve this problem to some extent, but in the long term the transoceanic capacity of optical fiber submarine cable--and its resistance to antisatellite weapons and electronic warfare--will make fiber the primary transoceanic medium. P.L. 86-36 EO 1.4.(c)

~~(S)~~ The impact on SIGINT of the development of transoceanic and overland optical fiber trunks is that traffic which now must go primarily by satellite will disappear onto fiber. The extreme publicity given to SIGINT over the past eight years by the revelations of World War II COMINT and by the excoriations of U.S. and British SIGINT agencies by governmental bodies, by journalists, by former employees, and by COMSEC and "communication protection" advocates, has made the telecommunication authorities highly conscious of satellite interception and microwave interception. Optical fiber will be a preferred transmission medium because it is so difficult to intercept.



DOCID: 4009853

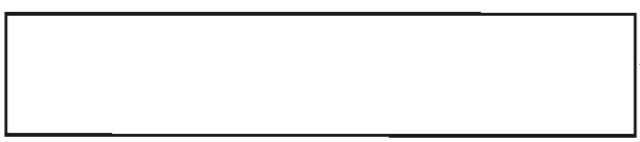
P.L. 86-36
EO 1.4.(c)

BIGFON: OPTICAL FIBER LOCAL LOOP

(U) A number of European countries are now experimenting with applications of optical fiber to the local network. The BIGFON network (see figure 23) will be tested in several German towns over the next few years, to determine how various subscriber services are used. An optical fiber pair with a capacity of hundreds of millions of bits will run from the local switch to the subscriber premises, and will carry various two-way services, including telephony, television, facsimile, data communication, telex/teletex, and stereo reception. At the local switch, selected channels of video, stereo, etc., will be connected to the individual loop. Current estimates are that a fiber pair can carry three TV signals and a variety of other services.

(U) Glass quality and cost are important considerations, since the total amount of glass fiber will be large, replacing the copper wire loops of current local nets. Optical fiber glass is made primarily by two processes, viz: the crucible method which gives a cheap and stable method of producing low-quality glass (10 dB attenuation/km), and the MCVD (multiple chemical vapor deposit) method which gives a very flexible technique for producing high quality but expensive glass (0.2 dB/km loss). Expert opinion (Midwinter) expects industrial techniques to produce a stable low-cost glass at about 1 dB/km which will allow fairly long local loops. The better glass would also allow economical higher bit rates.

~~(C)~~ The effect of low-cost optical fiber local networks would be twofold, viz., a much wider range of services, including videophone and conference nets with high grade voice security at 64 Kbps, would be available in the local nets, and the plant would be cheaper and more reliable than the conventional copper wire networks, leading to expansion of local (urban) telecommunications services in less affluent countries.



(U) One of the main attractions of optical fiber local nets from the point of view of the PTT's is that over the air broadcasting could be almost eliminated, and this would put all information flow completely under the control of the PTT's.

GLASS PURITY

(U) The driving factor in the development of optical fiber communications has been the improvements in glass purity. In 1966 the first article proposing monomode waveguide operation of glass fiber was published, but the glasses available at that time made the proposal appear absurd because the attenuation was too high for any useful system. However blocks of pure silica were found commercially available with losses as low as 10 dB/km, and this spurred enormous progress in glass chemistry.

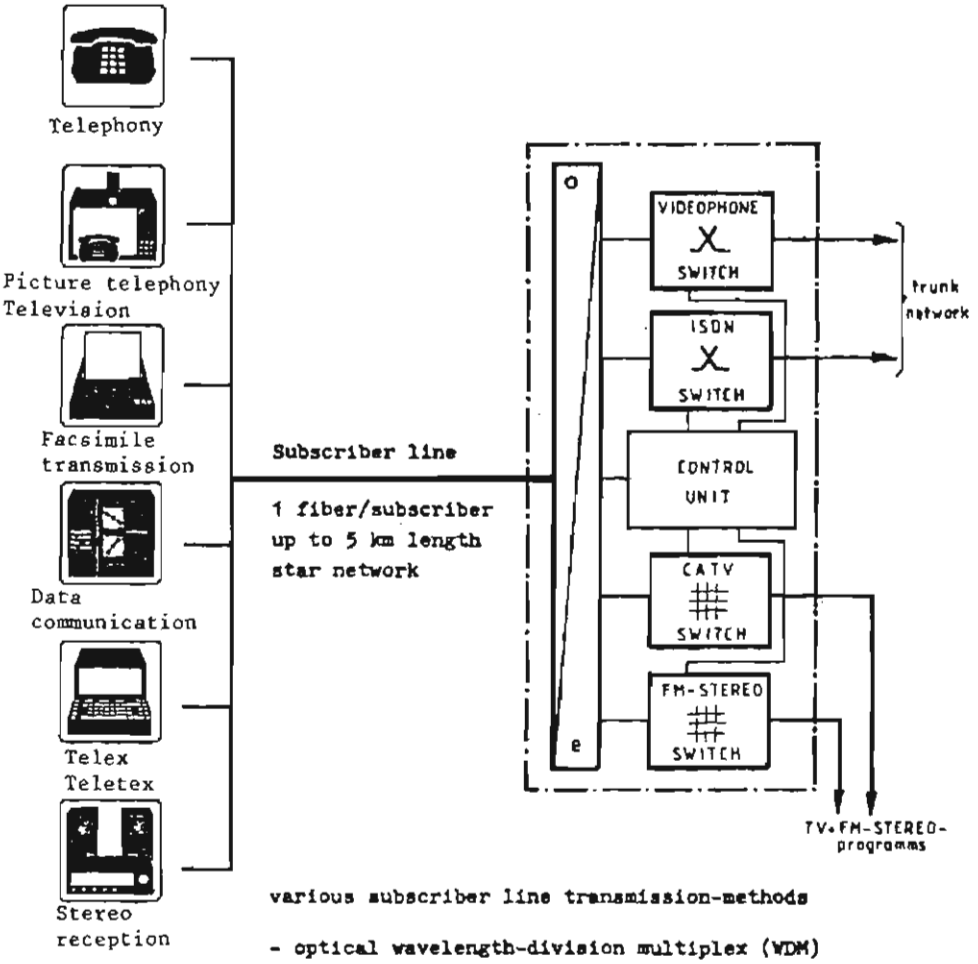
(U) The crude glasses of Egyptian times (3000 B.C.) had attenuation losses of 10 million dB/km, and over more than four millenia glass purity was gradually improved to the quality of Venetian glass of 1500 A.D. with losses of 10,000 dB. This represented a significant decline. Over the next 450 years, through the development of modern chemistry and industrial quality control, a further improvement was made to give the optical top quality glasses of 1970 with losses of 1000 dB per km. Then suddenly, in a decade of explosive development, completely new methods of purifying glass and drawing it into fibers were invented, with the result that a 10,000-dB improvement in glass attenuation was made in only ten years.

(U) The ratio of 10,000 dB corresponds to the number 10 raised to the power 1000, or a 1 followed by 1000 zeros, a truly phenomenal improvement.

(U) To visualize the effect of this improvement on optical communications, if all the power generating stations in the world converted all their power into light with perfect efficiency, and these many gigawatts of light were transmitted into a glass fiber with 1000 dB/km attenuation, then an observer one kilometer away would have to wait over a trillion years for the first photon to emerge. The glass fiber of course would be vaporized in an instant by the light absorption. By contrast, modern glass, at 0.2 dB/km loss, can transmit a few milliwatts of light 100 km without a repeater, at high bit rates over 100 Mbps.

BIGFON

broadband integrated optical fibre local telecommunications network



various subscriber line transmission-methods

- optical wavelength-division multiplex (WDM)
- time-division multiplex (TDM)
- frequency-division multiplex (FDM)
- space-division multiplex (SDM)

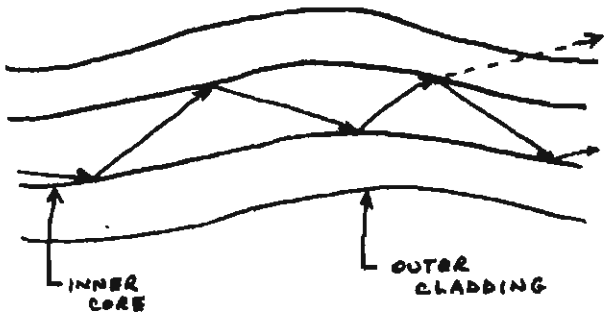
Fig 23

ISS' 81 CIC Montréal 21-25 sept. 1981

~~NOT RELEASABLE TO CONTRACTORS~~ ~~TOP SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

(U) At the same time that the glass has been improved, the light transmitters and detectors have also been improved, especially in matters of lifetime and reliability. A few years ago the lasers and light emitting diodes had lifetimes measured in a few hours, but this has been improved to 100,000 hours, with further improvements to more than a million hours expected. Efficiency has also been improved so that very low power consumption will keep a long series of repeaters operating. This is important to submarine cables, where the repeaters are inaccessible.

(U) A comment about fiber manufacturing is in order because it implies certain limitations on SIGINT operations against different fibers. The manufacture of high-quality optical fiber is done primarily by two processes, viz., Modified Chemical Vapor Deposition (MCVD) and Vapor-phase Axial Deposition (VAD). Both MCVD and VAD produce a large glass rod that is subsequently drawn into very long fibers in a high-temperature furnace. A subtle chemical process known as thermopheresis is used to allow various chemical gases to penetrate into the hot glass while it is a tubular form turning on the lathe, and this process captures unwanted molecules and also deposits desired chemicals in a systematic way. The glass tube is then collapsed into a rod and drawn into a fiber. The lower-quality optical fiber is produced by a "double crucible" process in which a mixture of chemicals is put into two crucibles and melted, giving two kinds of glass of uniform composition but not as pure as MCVD yields. Glass from one crucible is allowed to gravity-feed into a thin fiber, and this is drawn through a gravity-formed tube of an outer glass, still in molten condition, to form coaxial fiber. The light travels in the inner fiber, and is reflected by the outer cladding.



24. MICROBENDING

(U) Because of the very high purity of the best glasses, the losses of light energy in propagation have been greatly reduced, but some losses still occur from a phenomenon known as "microbending," in which the light rays hit the interface between the inner and outer glass at a high enough angle so that some energy is transmitted into the outer cladding and escapes. The fibers are currently stored inside small-diameter plastic tubes so that they are not bent too sharply as the cables are laid around curves. The critical angle seems to be about six degrees. At higher angles of incidence microbending losses occur. In the design of the transmission systems, an allowance for such microbending losses is provided. The geometry of light propagation down a coaxial fiber is very complicated because of coupling between different propagation modes, so that the exact light path is unknown. In the graded-index fibers produced by the MCVD process, an axial focusing and defocusing of light takes place, but even that propagation is very difficult to describe. The result is that, in general, light energy is launched into one end of a lightguide and some of it emerges at the other, with random losses due to absorption, escape, etc.

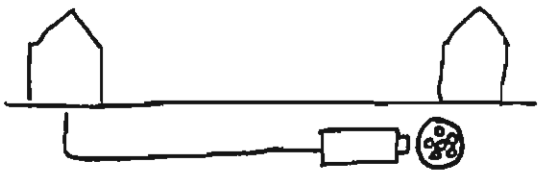
P.L. 86-36
EO 1.4.(c)

[redacted]

[redacted]

~~(S)~~ The central aim of optical-fiber SIGINT would be the concept of "proven reserves," derived from the petroleum and mining industries, rather than the current journalistic concept of hand to mouth immediate exploitation of whatever is easiest to get or fits current consumer requirements.

P.L. 86-36
EO 1.4.(c)



25. MOLE

[redacted]

[redacted]

[redacted]

systems, this after the fact access is not a workable scheme. If it took several years to get access to several fiber cables in an urban area, a crisis could come and go before any traffic could be collected.

~~(S)~~ The "proven reserve" concept does not only apply to interception, but to analytic and exploitation capabilities as well, so that the resources to attack and exploit systems should be developed and proved before there is a desperate need. Arguments that this is unaffordable should be evaluated by looking at the enormous success and wealth of the oil and mining companies, who do find this system affordable.

affects the entire SIGINT activity, rather than just hardening one problem at a time.

~~(S-CCO)~~ There is a historical precedent for this, in the World War II context, where the German traffic security, which at first thwarted Allied efforts at efficient collection, was solved for most of the war, and then at the end of 1944 became so secure that high-level cryptanalysis on the ENIGMA problem almost came to a halt because the traffic networks could no longer be identified or analyzed.

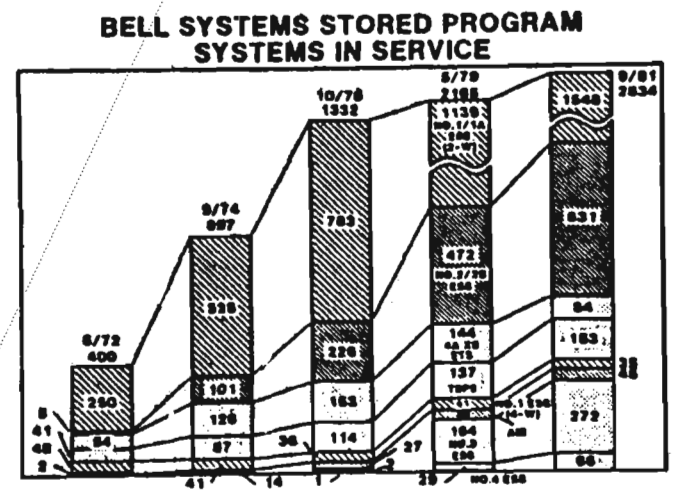
P.L. 86-36
EO 1.4.(c)

EVOLUTION OF EUROPEAN SWITCHING

(U) In the keynote papers at the International Switching Symposium in Montreal in 1981 (ISS 81), the rapid shift of the telecommunications plants of the Western nations from hard wired electromechanical switches to digital electronic switches was described. Although the old fashioned switches had been designed for a 30- to 50-year amortization, there is a growing trend to earlier replacement because the new switches are cheaper to operate and make more efficient use of the network. As a result, some 35 percent of subscriber loops will be connected to digital electronic switches by 1990, and 65 percent will be tied into the digital electronic switches by 2000.

~~(S)~~ As the new switches replace the old, the impact on SIGINT will be that the networks will become more flexible and efficient, and less rigid in the way traffic flows and in the services they provide. Some of the digital services, including those that use end-to-end encryption, will also have an impact on SIGINT.

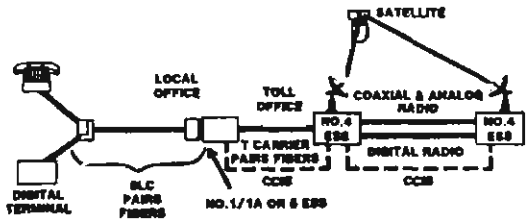
SWITCHING



26. BELL STORED PROGRAM CONTROL (SPC) SYSTEMS IN SERVICE

(U) In the U.S., the Bell System has also been very active in building and installing computer-controlled switches. Currently 47 percent of the local subscriber lines are covered by SPC switches, and the coverage in the Bell System by the early 1990's is expected to be 100 percent. There are now 2800 SPC systems in service.

(U) The SPC switches allow the network to provide new services, and also allow more efficient flow of traffic between switches.



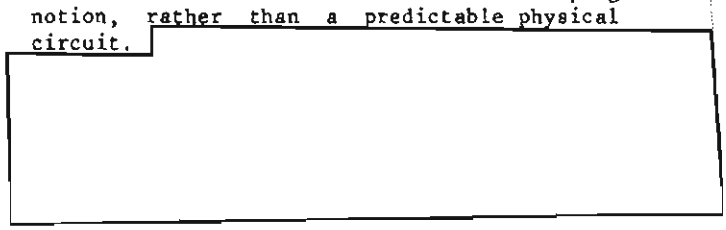
27. SWITCHED DIGITAL CAPABILITY

~~(S)~~ One of the significant changes in local services which the new switches will provide is high bit rate traffic over the subscriber loops. These high bit rates are made possible by the improvements in channel equalization and by sophisticated modems that can be implemented cheaply with the high density microelectronics. Some of the European nets are experimenting with 80 Kbps and 140 Kbps links, and the Bell System will offer 56,000 and 64,000 bps between the subscriber station and the local switch. Encrypted voice as well as facsimile and other data services will be available throughout the network where 1A ESS or No. 5 ESS switches are used. The Switched Digital Capability (SDC) will be introduced in 1984. For some subscribers, optical fiber will be used in the local loop. The 56,000 bps service will be end-to-end and will obviously provide high quality encrypted voice without the distortions that speech coders generate. This should lead to a rapid growth in encrypted voice for business traffic, with DES and Public Key interconnection between subscribers.

(U) Between the local switch and the toll switch, wireline or optical fibers will be used, under control of Common Channel Interoffice Signalling (CCIS). Coaxial cable, analog radio, digital radio, and satellite links will be used at the toll switches (No. 4 ESS), and CCIS signaling will be used where it is available. The CCIS information may flow over coaxial cable where the traffic itself flows over analog radio, digital radio, or satellite circuits.

~~(S)~~ The new Switched Digital Capability is an example of the new kinds of services which the digital electronic SPC switches will provide. In addition to the encrypted voice, encrypted high-speed (facsimile and electronic) mail and encrypted data services will flourish. Because the CCIS or other Common Channel Signalling will separate traffic addresses and routing from the traffic itself, the wideband transmission systems can be efficiently filled to capacity with a continuous stream of bits, or (in the case of analog radio links) successive talkspurts, without any indication of who the sender or recipient are. The toll switches are also capable of instantaneous automatic rerouting of traffic without any break in service, so that a given message or session may flow over various different channels. The effect is that the switches tend to act as transposition scramblers on relatively featureless and unidentifiable analog and digital traffic. The "dedicated" or leased channel will be a bookkeeping notion, rather than a predictable physical circuit.

P.L. 86-36
EO 1.4.(c)



Digital Switching
No.4 ESS

INTRODUCTION 1/16/76
• 67 offices now in service

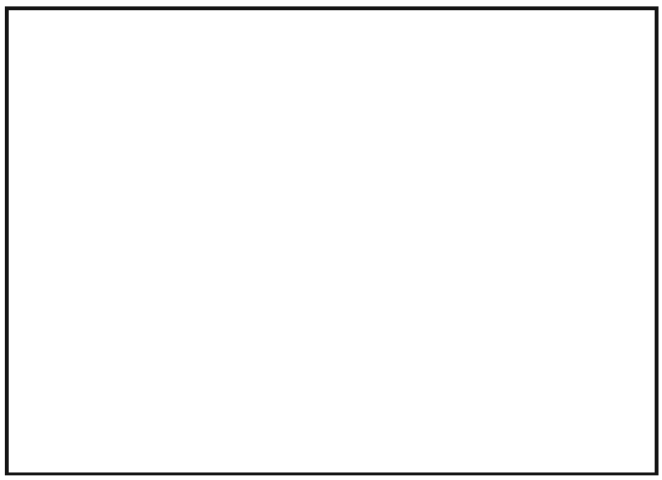
- **Characteristics**
  - **Time division switching network**
  - **Powerful central processor**
  - **New technology**
  - **Full duplication**
  - **Disciplined software methodology**
- **Features**
  - **Large capacity**
  - **Wide range of SPC network features**
  - **Extensive O.A. & M. features**

28. No. 4 ESS TECHNOLOGY

(U) At ISS 72, the No. 4 ESS created a sensation as a novel and ambitious functional and technological development. It was introduced into service in 1976 and 67 offices are now operating. However, the hardware technology of the switch has been completely replaced because of the technical superiority of newer microcircuits. No. 4 ESS uses time-division

switching in its internal logic, to give it very high resistance to "blocking" i.e., refusing a connection where a path actually exists in the switch.

(U) After the first shocking experience with switch software in the No. 1 ESS, the Bell System turned to disciplined software methodology, and now they can produce software which does not cause frequent switch outages. In spite of this, a new switch software product must "run in" for several hundred switch years before all the bugs are removed.



(U) The No. 5 ESS is a new local switch, designed to handle up to 100,000 lines, and designed to be used in rural areas. This switch applies time division switching to local nets. In contrast to the No. 4 ESS which is based on a powerful central processor, the No. 5 ESS architecture is based on distributed control. Powerful microprocessors are used in all of the peripheral modules, while the central processor performs more global control functions as well as overall administration and maintenance of the system.

(U) No. 5 uses modern software concepts, and all elements common to 512 lines are duplicated for reliability. An evolutionary plan has been set to provide a size range from very small to large offices of at least 100,000 lines with a large complement of customer, network, and administrative and maintenance features.

(U) The flexibility of the No. 5 ESS, and its production in various size ranges, is typical of the new developments in switching. The main producers of electronic switches are the French, Japanese, and L.M. Ericsson. The Swedish company produced a modularized AXE switch in the early 1970's, which in its original form routed signals in analog form, but was converted block by block to all digital operation. The first AXE switch was installed in Sweden in 1978, but has sold well abroad. Outside America there are only about 100 PTT customers for switches. The attraction of the AXE was that an analog network could be gradually converted to digital, and this technical lead enabled L.M. Ericsson to win the biggest telecom contract ever awarded, for a $5-billion Saudi telephone system. The conversion of existing analog networks over to digital operation, which involves the integrating of new switches into mixed analog and digital networks, is one of the most demanding problems in switch and network design.

P.L. 86-36
EO 1.4.(c)

ADVANCES IN TECHNOLOGY FOR ESS

- ■ VLSI
  - [] Microprocessors
  - [] Memory
  - [] Custom logic
- ■ Other Hardware
  - [] Optical fibers
  - [] High-voltage semiconductors
  - [] Display technology
- ■ Software
  - [] Architecture
  - [] Operating systems
  - [] High-level language
- ■ Development methodology
  - [] CAD
  - [] Program development support
  - [] Automated testing

(U) The switch designers have found it necessary to move into the forefront in development, manufacture, and application of the most modern hardware, design, and software technology. The network functions call for very complex logic, represented in VLSI hardware and software. Now the switch designers are converting software functions into "firmware" where the critical algorithms are designed in silicon from the start.

(U) Because of the high speed of modern

computers, various real-time telecommunications functions can be codified in higher level languages. Software has become a major part of switch and telecom plant production. At Bell Telephone Laboratories in 1950 no software was produced. Now half the staff works at software production. The advanced programming techniques enable software production at 100 times the rate of 15 years ago. The testing and debugging, and particularly the reliability of modern telecom software is a major technical factor. The other side of this coin is that once the software is designed and tested, it is very hard to change, because hundreds or even thousands of switches and transmission systems are made interdependent and interconnected by the software. Hence, even if the hardware is replaced, and parts of the software are codified into "firmware," the basic software system will probably have a long operational life. The software programs are often very large, running into hundreds of thousands of lines of code, and the developers are frequently protective of their "source level" program scripts.

[redacted]

[redacted]

[redacted]

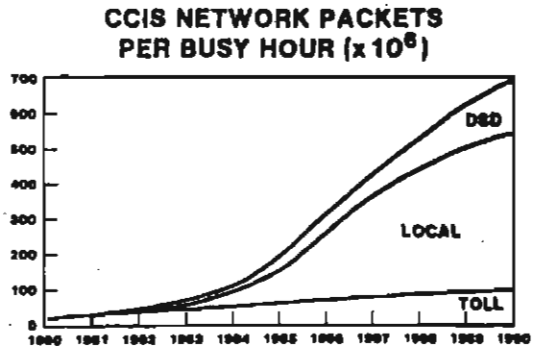
COMMON CHANNEL SIGNALLING

P.L. 86-36
EO 1.4.(c)

(U) In Common Channel Signalling the addressing information used to specify the call and the routing is not sent as a prefix on an idle channel. Instead, a separate dedicated channel is used to carry all the addressing and routing and signaling data. The result is that the transmission facilities are used more efficiently because idle channels do not have to be held open for some minutes while successive channels are found, and then until a called party finally picks up the telephone. On long distance calls, signaling and call setup used to take about half the channel time. The application of common channel signaling allows network efficiency to be practically doubled without building new plant.

(U) Three major systems are No. 6 CCITT, No. 7 CCITT and the Bell System CCIS Common Channel Interoffice Signalling.

[redacted]

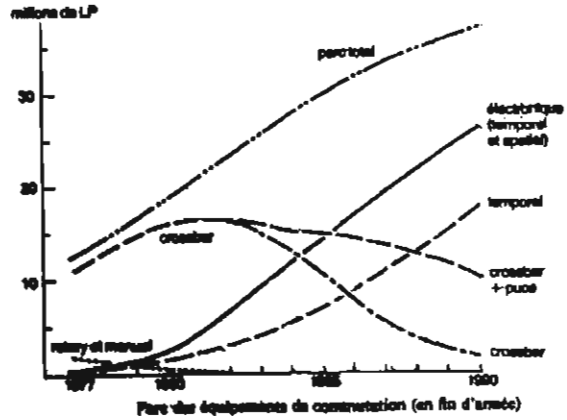


30. CCIS NETWORK PACKET TRAFFIC FORECAST

(U) In the Bell System, Common Channel Signalling is already in use between some switches and a packet network is employed to transmit the switching data. Currently some 20 million packets are sent during a peak hour. By 1990 the packet traffic rate for CCIS will rise to 700 million packets per hour. The dedicated CCIS packet network operates to set up the circuits switched network that will actually carry the traffic.

(U) While the new digital switches can be designed to implement common channel signaling, the older electromechanical switches, e.g., crossbar, are designed around a control system that uses in-channel prefix signaling. The French have developed an innovation for this problem called PUCE, which will retrofit an SPC computer into existing crossbar switches so that the crossbars can be controlled by common channel signaling. This will enable the entire French switched network to be operated by common channel signaling. The PUCE retrofit will allow the existing switches and transmission facilities to be operated more efficiently, without the expense of replacing the existing large investment in electromechanical equipment. This will also prolong the life of the crossbar plant. A plan published by CNET shows the effect of PUCE in extending the life of crossbar switches.

P.L. 86-36
EO 1.4.(c)



31. FRENCH SWITCHING EQUIPMENT ASSETS

(U) The major growth will be in time-division electronic switches (temporel), with rotary and manual phaseout by 1983, and ordinary crossbar dwindling after 1984. The crossbar with the PUCE retrofit will remain at a fairly steady level up to 1990, presumably as a result of converting the ordinary crossbars.

(U) Summing up the switching trends, time-division has the greatest growth potential, and the wide use of time-division digital switches will reduce switching from 50 percent to 20 percent of total plant value, but many

years will pass before most countries can afford this. On the other hand, the low cost and high reliability of microprocessors and computers will make it increasingly attractive for PTT's to seek cheap retrofits and hybrid systems which will give more efficient operation and more or newer services, without the expense of replacing still serviceable equipment.

(U) In most poor countries, the problems of maintaining outside plant will be as significant a factor as shortage of money in retarding the successful introduction of digital electronic switches; defects and noise in the outside plant (subscriber loops and trunk transmission) cause errors that can disable the more critical digital technology. Another key factor in the introduction of digital switches in any country is the distribution of timing standards, because close synchronization through the networks is needed. This is already a problem in the U.S. where different suppliers provide equipment to hundreds of "independent" operating companies. Once a small country starts to introduce digital switches, the difficulties of time distribution and digital interface will cause special problems for any rival manufacturer who wants to sell in that market.

P.L. 86-36
EO 1.4.(c)

~~SECRET SPOKE~~

ANSWER: An Old Problem (U)
(CRYPTOLOG, August 1982)

When you finish, send up a flare!

Not
Secret
Anymore

P.L. 86-36

(U) May I add a few words to [redacted] reminiscences in the August 1982 Cryptolog, especially to his comments about the initials NSA standing for "Not Secret Anymore"? Like Brother [redacted] I recall those days of "M&M" (as we lovingly called Martin & Mitchell) and I also remember figuring out that expansion for myself, but I doubt if I was the only employee to come up with the clever meaning for "NSA."

(U) I remember including a cartoon in my book NonseNSA, showing President Eisenhower denying everything that M&M had said, ending up with, "and there is no such agency as NSA at Fort Meade, Maryland. In fact, there is no such place as Fort Meade, Maryland!" and scribbling on the bottom of the page "NSA now stands for 'Not Secret Anymore!'" Unfortunately, I loaned NonseNSA to [redacted] who used 2 or 3 cartoons from it in early issues of Cryptologic Spectrum and then retired without returning it to me, so I don't know if the book is still in existence.

(U) But at least I'm glad to see that somebody else used "Not Secret Anymore" since my other great discovery about what an agency's initials meant seems to have been restricted to me alone. When President Reagan appointed William J. Casey to be the head of CIA and then got our Admiral Inman to be his deputy, I remarked on several occasions that the CIA was "the Casey-Inman Agency" (which I thought was pretty clever--in fact, I was tempted to send it in to "The Ear" at The Washington Star--but to date I've never heard or seen it used by anyone but little ol' me...and now that Admiral Inman has left, I doubt if I ever will).

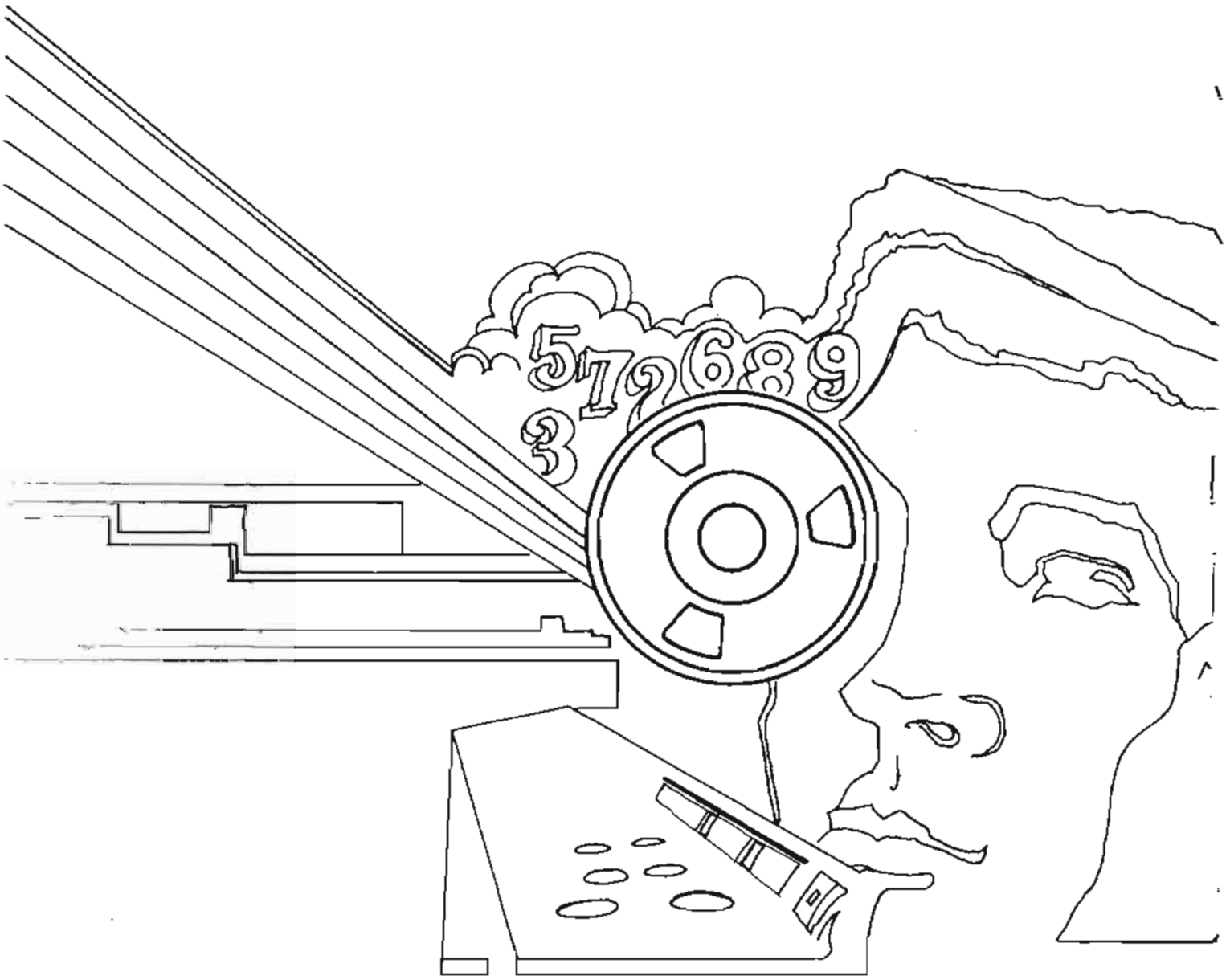
[redacted] P16

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~

P1-Oct 82-SJ-21537


5726893

DOCID: 4011953

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

SEPTEMBER 1982

P.L. 86-36

NORMANDY: 1944 (U)..... [redacted] 1

TSS REVOLUTION (U)..... [redacted] 8

SIGINT: 1990, Part One (U)..... [redacted] 13

LETTERS (U).....29

MORE FREE GOODIES (U).....29

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by NSA/CSSM 123-2
Declassify on: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526.
MDR Case # 54778

DOCID: 4011953

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. IX, No. 9 SEPTEMBER 1982

PUBLISHER [redacted]

BOARD OF EDITORS

Editor-in-Chief. [redacted] (8322/7119s)
Asst. Editor..... [redacted] (1103s)
Production..... [redacted] (3369s)

Collection..... [redacted] (8555s)
Cryptanalysis..... [redacted] (5311s)
Cryptolinguistics..... [redacted] (1103s)
Information Science. [redacted] (5711s)
Language..... [redacted] (8161s)
Machine Support.. [redacted] (4681s)
Mathematics..... [redacted] (8518s)
Puzzles.....David H. Williams (1103s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Don Taurone (3573s)

For subscriptions
send name and organization

to: CRYPTOLOG, P1
or call [redacted]3369s

To submit articles or letters
via PLATFORM mail, send to

cryptolg at barlc05
(bar-one-c-zero-five)
(note: no '0' in 'log')

Editorial

At the end of the first year as editor, I ought to have some profound thoughts, but I don't. The magazine is coming out more or less regularly each month, and that was our first goal. Some of the other goals have been met, including the matching of the distribution against the locator file. Some goals remain to be met.

The purpose of CRYPTOLOG is to help you to do your tasks. Our emphasis is primarily technical, but we don't always limit ourselves to the purely technical. Helping you do you job might be achieved by showing you how to do something, or by letting you know that someone else has worked on something similar. It may also be done by making you more aware of what is going on around you, both in space (at the other end of the building) and in time (last year on a related problem), because many of the best technical people are basically curious people.

For some of you, CRYPTOLOG offers an opportunity to stretch yourselves by writing; you might be surprised at how few readable writers there are in certain fields, whose output is intelligible to readers outside their own territory. Developing a reputation as a writer could give your career a boost. If you are thinking about writing something and are waiting to be asked, call me and I'll ask you.

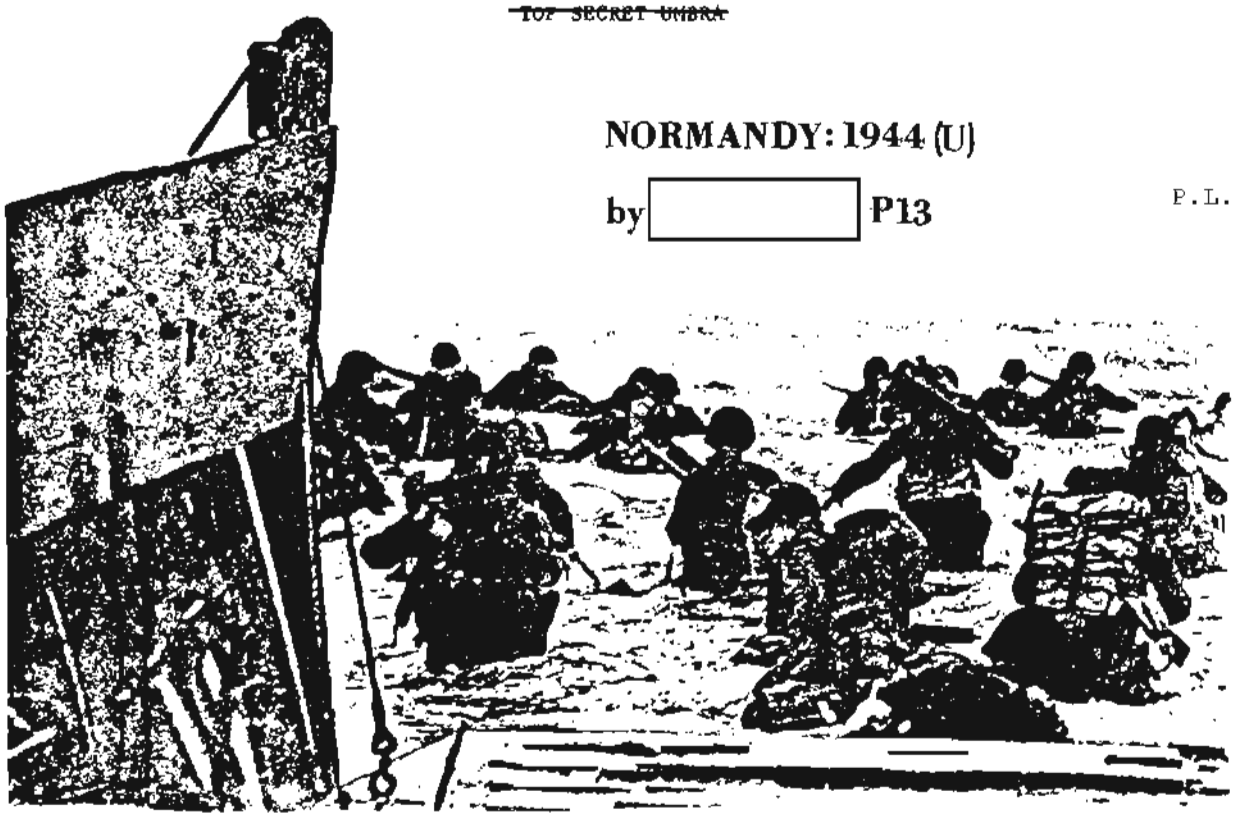
P.L. 86-36

In years past, CRYPTOLOG often skipped a month in the summer. However, as an experiment, we are offering instead an issue containing three somewhat longer articles. Their subjects, interestingly enough, are the past, the present, and the future.

WES

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011953



NORMANDY: 1944 (U)

by [redacted] P13

P.L. 86-36

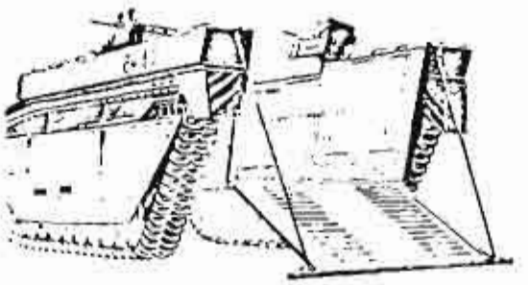
REVIEW: Six Armies in Normandy, by John Keegan, Viking, 1982, NY.

(U) American, English, Scottish, Polish, French, and German armies clashed in a decisive land battle in Normandy from June till September 1944, in one of the major campaigns of modern history. Half a million German troops were lost, most of them killed; their 50 infantry divisions and 12 panzer divisons had been reduced to 24 infantry divisions at quarter strength, and 11 panzer divisions had shrunk from 150 to 10 tanks each. Even the destruction of the Army Group Center in June and July 1944 by 140 Soviet rifle and tank divisions, which had cost 300,000 German soldiers, was a lesser defeat. The Western Allies had committed only 34 divisions to the battle against the 62 German divisions. When the Germans finally lost in Normandy, they lost all of France and fled in disorder to the Dutch frontier.

(U) John Keegan, a lecturer at Sandhurst whose previous book The Face of Battle became a minor classic, has written synoptic accounts of six different divisions in their most critical battles in Normandy, to illustrate not only the key events in the battle seen from battalion down to squad level, but also to illustrate something of the national character of the different armies. Where did the troops and weapons come from? Why did they fight? How did they fight? How did they react to the stress of 1944 warfare?

~~(S)~~ The salient advantages the Western allies had in the land battle were seapower, airpower, plentiful supplies, and COMINT. As a result, the Germans had to defend everywhere, and this left them too weak at many points, and unable to move forces to the battlefield. When they did try to move, the radio communications were deciphered in time to paralyze the movements and prepare defenses. The cardinal contribution of COMINT was that it allowed the Allied armies to defeat the German Schwerpunkt tactics by giving prior knowledge of intentions. (6) In general, the Allied armies were no match, tank for tank or battalion for battalion, with the first-line German divisions. General Alan Brooke, British Chief of Staff, considered the Germans the best soldiers in the world and tried to keep the British forces away from them by a "peripheral" strategy, while the Americans sought a direct cross-Channel attack to destroy the German Armies in the field. Normandy was the result of this prolonged dissent on Allied strategy.

(U) The British had sound reasons for regarding the German Army with caution. In World War I the German Army was the only one in Europe that did not have mutinies. It marched out of the Rhineland in 1919 in perfect order, still willing to fight. In World War II the German soldiers fought until the last few days of the war and Germany had to be invaded and crushed; they would not surrender as long as they could still fight. At Dieppe in 1942 an invading force of 5000 Canadian



soldiers attacked a coastal town defended by a garrison of 400 German soldiers and nearly all were killed in spite of 12-to-1 odds. The German Soldiers in 1942 were in France training for or rehabilitating from the Russian campaign. In 1944 many of the defending divisions at Normandy were bodenstaendige divisions, equipped with captured foreign weapons or other inferior equipment, without transport, and the soldiers were old or unfit. Thanks to the excellent Allied intelligence, most of it from COMINT (although Keegan does not mention this), the initial landings were aimed at these relative weak spots.

(U) The German command system was able to react very quickly by converting spare personnel into infantry formations and putting weak units in front of SS regiments to stiffen their will to fight. German officers did not wait for orders from above, but put their forces into battle very skillfully in anticipation of orders from above. Orders gave objectives, rather than detailed directions, so that German reactions were tailored to the battle situation--rather than premeditated. The troops obeyed orders to the end because they had confidence in the Officers. [13] The German Army ended the war with only half its billetted officer strength because officer casualty rates were much higher than enlisted casualty rate, and the Germans would not commission unsuitable people because it would have destroyed confidence in the Officer Corps as a whole. [4]

(U) At the end of June, the Panzer divisions were committed to the battle and the 9th and 10th SS Panzers, who later destroyed the British and Polish parachutists at Arnhem [3], were taken from the Russian front and moved to Caen, where they smashed into the 2nd Argyll and Sutherland Highlanders in the "Scottish Corridor" west of Caen. An ULTRA decrypt revealed the assembly area of the German attacking force and naval gunnery destroyed the German armor before it could mount its attack in force. This COMINT assist was helpful, for the Scots had no tanks and only six-pounder guns and PIAT antitank weapons for their inexperienced infantry, in their first battle, to fight SS Panzer soldiers who began their war in Poland and had spent several years in armored warfare in Russia.

(U) Because the Germans had no navy left, except U-Boats, and no effective air force, they were unable to drive off the supporting task force, which fired on coastal targets for weeks with long-range indirect fire. These Allied assets were not always well used however, for the helpless city of Caen was reduced to rubble by naval gunfire and then further devastated by a massive strategic bombing operation because Montgomery did not want to expose his troops to heavy losses by the Germans. The Germans were not in Caen, so there was no military result. The French, trying to survive in cellars, were buried under more rubble. An insane asylum, used as a refuge and hospital in the outskirts of Caen, was devastated by Allied bombing. The Germans, however, had to keep huge formations tied up defending coasts from Norway to Italy because they could not match Allied mobility and force at sea or in the air. As soon as they tried to move forces, COMINT read their orders and the transportation facilities were wrecked. Hence Normandy was as much a war of interdiction as it was a war of attrition or maneuver.

(U) For a representative American division, Keegan chose the 101st Airborne Division, which landed by parachute and glider before the invasion to protect certain bridges so that the troops at Utah beach could get inland. The aircraft navigation and the formations were thrown off by clouds, so that the troops were scattered all over the Cotenin peninsula and some were dropped in the sea. With typical staff planning, the communication equipment--essential to coordinate and regroup the scattered airborne troops--was dropped separately from the troops, and virtually all lost. As a result, almost all the operations were impromptu little clashes by tiny packets of troops. Ad hoc formations and chains of command were set up, as circumstances

DOCID: 4011953

dictated, and sometimes several different elements attacked the same target at the same time without knowing who the others were. Runners were used to find higher and lower units and deliver messages. Small groups of paratroops were adrift for weeks, out of touch with everyone. Many units vanished, presumably exterminated by the Germans. Virtually no one spoke French, and the local population was reluctant to get involved in the combat. The resulting disorder apparently confused the German command, who could not decide where the point of the attack was. The results were bloody but successful, with very few prisoners. Keegan compared the American airborne troops to pioneers, ignorant of the language, landmarks, or dangers around them, who simply relied on their own weapons and skills. The metaphor is apt, for the American troops frequently outfought the German troops in the light infantry battles and never waited for orders or refined intelligence. General Maxwell Taylor was cut off from his command and from the invading force until after the invasion forces had gotten inland, but the lower level elements achieved their objectives anyway.

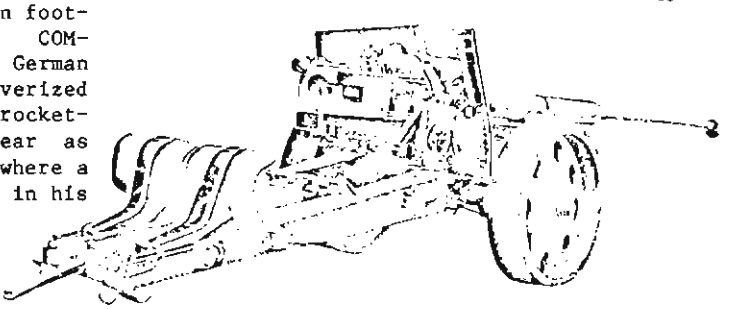
(U) (It has since been said that Germans could never understand why they lost a battle to the Americans at any point in World War II, because they tended to perceive American attacks as disorganized and confused.)

~~(TSC)~~ American military operations are mentioned elsewhere in the book, from the preinvasion buildup in England (where Keegan as a schoolboy was impressed by the wonderful "cornucopia" of vehicles and equipment the "Yanks" brought with them), to the breakout at Avranches and the sweep across France. The Americans were much more willing to take casualties than the British because they had not felt the devastating effects of the trench warfare of the First World War. By 10 July, the Americans had suffered 40,000 casualties, still short of St. Lo. Then they lost 11,000 men in 5 days taking St. Lo. On the third try, carpet bombing was used to break the thin crust of German defenses, infantry crashed through the stunned defenders, and armor poured south into Brittany. American footballers would call this a "power play." COMINT revealed the exact details of the German response and the American defenses pulverized the counterattack. Then masses of rocket-firing P-51's kept Patton's flanks clear as his armor swept eastward toward Metz (where a tiny German defending force stopped him in his tracks). [16, 18] The Americans also did well on logistics. The British favored complicated gadgets such as the Mulberry harbors, two years in construction, which were wrecked in one night by a storm, after which the Americans unloaded massive quantities directly onto the beaches and did far better than the British achieved with their rebuilt Mulberry harbor. [18]

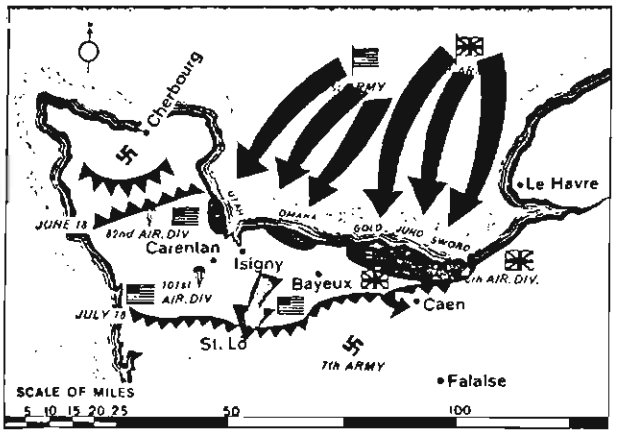
(U) German defense was frequently very tenacious. At Carpiquet on 4 July 1944, two Canadian regiments fought all day to take an airfield from 50 young soldiers of 12th SS Division. In Operation Goodwood in mid-July, a massed formation of British "Guards" armored divisions attempted to break out from Caen, following a raid by 1000 bombers. Battle Group von Luck of the 21st Panzer division threw the attack offstride by hitting its flank, without any orders from above, and then half a dozen Tiger tanks blocked the advance of a Guards Armored Division. Soon the First SS Panzer Division (Liebstandarte Adolf Hitler), which had been in combat since Poland, brought the British attack to a halt. Montgomery was severely discredited by this defeat. The British "Guards" divisions were actually Horse Guard regiments from the yeomanry and gentry of England, who reluctantly gave up their horses and switched to tanks as World War II become imminent. British tanks were unreliable and no match for the 1930's-era German tanks, but the British fitted a new gun and turret to the American Sherman tank and the result was a fairly good tank. However, it could not defeat the Tiger tank, which the Germans used defensively in Normandy. The Guards regiments had experience in desert fighting, but in the terrain of Normandy, the German tactics of using 88-mm antitank guns in conjunction with tanks that fired from cover proved superior. At the same time, the policy of fighting on a rigid line, as ordered by Hitler (and required by the Allied interdiction of the German rear area), left the Germans vulnerable to the breakthrough and encircling operation that occurred in late July and August.

German 88 mm L/70

Weight:	4 tons
Muzzle velocity:	3,700 fps
Length (calibres):	71
Weight of shot:	22.2 lbs



DOCID: 4011953



(U) Keegan chose the landing of the North Shore regiment of the Canadian 3rd Division at Juno Beach on D-Day and contrasted it with the slaughter of the Canadian 2nd Division two years earlier at Dieppe. The Canadians generally played an unsung part in the war. Their battle doctrine was British, but much of their equipment and logistics were American, particularly the indispensable tanks and trucks. Canadian regiments trained for four years before they fought in Normandy, and had to compete to be selected for overseas service. [12] Because of the long training and association in the same battalions and regiments, the Canadian forces were able to withstand the savage battles with the SS Panzer Divisions from Caen to the Rhine. (By contrast the U.S. stripped 60,000 cadets out of flight school in Summer 1944, and 75,000 from advanced training programs, and shipped them to France for immediate combat duty as infantrymen. [15]) Canadian losses were high; a single 2nd Division Regiment (the Algonquins) suffered 1300 casualties, about one third of its strength, from August 1944 to May 1945. [12] Similarly, the U.S. 35th Infantry Division lost 3000 men in a few days in the St. Lo breakout. [17]

(U) In an effort to trap the Germans in the Falaise pocket, the First Polish Armored Division got onto a hill near Chambois and fought off repeated German attacks, although it was itself cut off. At this point the Polish Home Army in Warsaw was facing annihilation by the Germans, while the Russian Army paused not far from the city. The Polish parachute brigade went on a hunger strike because the Western Allies would do nothing to help the Home Army in Warsaw. The First Polish Armored Division had risen from the ashes of successive defeats. After the invasion of Poland in 1939, 100,000 refugees got to France, and an army in exile was formed in France. Only 17,000 got to England, with no equipment, after the fall of France in 1940. They recruited Poles from around the world and manipulated American Lend-Lease to equip and train an armored division. An Austro-Hungarian officer, Maczek, was put in command. This re-formed army kept the titles and colors of various Polish regiments, long since destroyed. It formed part of the Army of the Republic of Poland, rather than being merely a division in the British Army. The Poles were notoriously disdainful of danger and, when given an order to close the Falaise gap, set off without waiting for resupply of fuel and ammunition. They took the wrong road and wound up in an excellent military position on high ground, ready to block the German retreat, but cut off. Twenty German divisions were trying to break out past them. On the same night that the Home Army retreated through the sewers of Warsaw, the Germans began to fight for control of the hill at Chambois. The Poles' resupply was airdropped five miles away. They fought without supplies or support for three days against massed German infantry, tanks, and antitank guns. They also had to guard 800 German prisoners. Seventy percent of the survivors of the Westheer who had tried to escape at Falaise had been stopped by the Poles and taken out of the war. In Warsaw the survivors of the Home Army had to surrender to the Germans. After the war most of the surviving Poles from the First Armored Division stayed in England; their battle to free their homeland had been in vain.

(U) The French Army was commanded by General LeClerc, a nom de guerre for Vicomte Jacques-Phillipe de Hautecloque. LeClerc was actually much higher up in French society and military life than DeGaulle, his nominal superior. His 2nd Armored Division, which fought its way into Paris after the Normandy breakout, actually began its existence in Southern Chad in 1940. The cadre consisted of black Senegalese soldiers and outcast French officers from Fort Lamy. This swashbuckling crew of officers and bloodthirsty soldiers soon made a trek 1000 miles north across the Sahel to the Sahara, where they fell upon the Italians in Southern Libya. In 1942 they made further attacks, in collaboration with the British Long-Range Desert Group, and then left the base in Chad to move into Tunisia. They joined with some Foreign Legionnaires and Levantine soldiers serving under Koenig. They

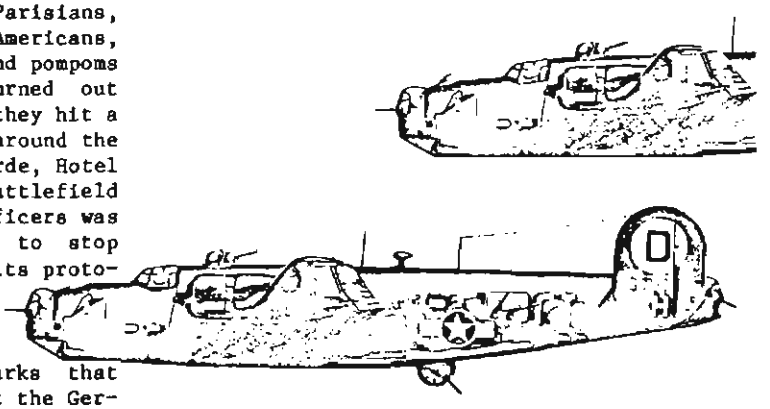
~~TOP SECRET UMBRA~~

filled out the cadres with Algerian and Moroccan mercenaries, and it was these Berber mountain troops who broke the defenses at Monte Cassino in Italy. The Moroccan troops, by some accounts, were paid three centimes for bringing back trophies cut from the enemy corpses. For political reasons it was important to recruit native Frenchmen to fight in the reconquest of France itself. The Americans promised equipment for a full armored division. Former Vichy troops and officers in Africa were permitted to join, on probation. The Senegalese were not regarded as suitable liberators of the white French nation, and were sent back to Chad over their protests. Christian Arabs from North Africa replaced some of the Senegalese. The officers were largely St. Cyr graduates, all known to each other. LeClerc himself, an aristocratic hereditary leader, indifferent to danger, was the central element in healing the divisions between the Vichy and anti-Vichy officers and men. French military pride had been deeply wounded by the ease with which the German Panzers brushed their armored units aside in 1940, so they worked diligently to be up to battle standard by D-Day. They went to France on 1 Aug 1944 under Patton's command.

(U) The battle for Paris was fought for domestic political reasons, rather than for military reasons. Eisenhower wanted to bypass the city, but the underground, Communist and maquis, was too strong politically, so it had to be liberated by the Free French in order to establish DeGaulle as a force in the French government. The German commander, Choltitz, had been ordered to destroy Paris and intended to give an episode of resistance in order to salvage German honor before surrendering the city. The French ran armored columns through the streets of Paris in three columns to reach certain politically important objectives. Their aim was to establish DeGaulle's appointees as the heads of key ministries by fait accompli. They did not want to destroy Paris and were criticized by the Americans for "advancing on a one-tank front." Within a day they achieved their purpose. The Parisians, expecting to be liberated by the Americans, were thrilled to see the insignia and pompoms of French regiments. A huge crowd turned out to rush along with them, just as they hit a German strong point. Battles raged around the Arc de Triomphe, Place de la Concorde, Hotel Meurice, and other parts of a battlefield deluxe. After the honor of the officers was satisfied, the troops were ordered to stop fighting. A European civil war has its protocol.

(U) In his epilogue, Keegan remarks that military analysts are now looking at the German defense in Normandy as a model for how NATO might fight a conventional war where the rear area was disrupted, no territory could be given up, supplies were scarce, and air superiority was held by the enemy. He does not think much of the idea, for the Allies were able to use seapower to attack a coastal point without warning, while a Soviet advance would have to follow some obvious land route. However, there are several factors in the Normandy battle that are worth considering, even if the particular tactics are no longer pertinent. The Allies, with only 34 divisions, defeated some 62 German divisions, destroying half of them. By the book, it should have taken 180 Allied divisions to push the Germans out of France. Despite the inexperience of the Allied divisions and the great tactical ability and experience of the German divisons such as Panzerlehr, etc., the Allied casualties were comparatively low. Airpower was critical, especially in interdiction and in protecting the Allied logistic flow, but one key factor was the Allied ability to avoid slaughters.

(U) Keegan mentions COMINT, citing Bennett's book Ultra in the West, but his treatment is fairly sketchy. ULTRA COMINT was generally of only limited tactical use because it was either too late, or the Germans did not send detailed tactical orders over ENIGMA. There were some exceptions, especially when Hitler sent tactical plans directly, such as the counterattack at Mortain after the Avranches breakout. Many of the read ENIGMA messages were unusable because the British General Staff had thrown away the only copy of the French military map that the German Army was using, which gave the names of many little towns. [5] Reconnaissance, patrolling, prisoners, and captured documents gave most of the timely tactical intelligence. [14] The French, Poles, and Canadians were not direct ULTRA recipients.



~~(TSC)~~ ULTRA did not set the strategy. That resulted from a long conflict between the British and Americans over the "second front," described by Keegan in a chapter. The plan to fight the German Army after a cross-Channel invasion set the conditions for COMINT, which then had to work on the Army keys and other ciphers pertinent to the German defenses. [10] ULTRA from many sources gave an incomparable picture of the German dispositions, fortifications, and preparations for the invasion. It also showed in 1943 that the Foreign Armies West Intelligence was "channel blind" and thus vulnerable to the strategic deception that tied major forces in the Calais area. [8] COMINT on German SIGINT and Intelligence and Agent systems showed that strategic deception was working, and spared the Allies from a devastating surprise in the landing. [9] After that, COMINT continued for several months to give a lot of operational intelligence about major ground and air movements, and high-level reports, so that the Normandy breakout and the sweep across France could be pursued without fear of strategic surprise.

~~(TSC)~~ Although strategic deception worked well, COMINT showed that tactical deception schemes were virtually always penetrated by the Germans. [5] Someone always gave the game away. Knowing that deception was NOT working was probably very valuable in holding down the "butcher's bill" in Allied attacks.

~~(TSC)~~ Some of the main points of the COMINT effort are interesting. No German Army Enigma keys were read from mid-1940 until the spring of 1944. The solution of the cipher teleprinter TUNNY in May 1944 was the biggest success of the year in giving German strength, dispositions, plans, and appreciations in the West. Before D-Day, and for three months afterwards, COMINT was the primary or only source of a vast amount of information about German dispositions, preparations, etc. Almost all of this COMINT was obtained from German military traffic. COMINT gave routine intelligence about the German forces and actions up to the American breakout at St. Lo, after which it became spectacular. In the counterattack at Mortain, messages from the XLVII Panzer Corps and from C-in-C, West were read within hours, giving intentions which had been decided by Hitler. The messages were out of date before they could be acted on because of Allied actions. German intelligence on Allied intentions at Falaise was known from decrypts. German fears of encirclement and Hitler's refusal to permit a withdrawal were known from COMINT. German confusion was reflected in the decrypts, which were often translated and sent to the users within a few hours. When von Kluge vanished on the battlefield at Falaise, Hitler personally ordered a counterattack which was successful, but the message was not read for ten days. The order to withdraw behind the Orne River given on 16 August was read and forwarded in five hours. During the retreat after 18 Aug 1944, most of the decrypts were too late to keep up with the fluid battle situation. Decrypts showed a temporary lapse in German discipline and morale. [7] (Entire paragraph)

~~(TSC)~~ Allied use of COMINT changed radically after the crossing of the Seine River, because only events in the North were covered by the arrangements between GC&CS (Govenment Code and Cipher School) and 21st Army Group. The American forces in France handled ULTRA COMINT differently from all other intelligence. Despite security rules, ULTRA was discussed at all time on the Signal Corps telephone circuits in France. [6] (Entire paragraph)

~~(TSC)~~ Only a small fraction of the decrypts produced were used actively to conduct operations. Most COMINT was used passively to confirm other intelligence, or for information. COMINT was found of less use to the attacker, who had the initiative, than to the defender. One common active use of COMINT was to direct reconnaissance at specific targets. This confirmed and covered the COMINT. In general, active use of COMINT required much more than timely decrypts, but the results were significant. [6] (Entire paragraph)

~~(TSC)~~ By September, as their Army was retreating, German COMINT became very good, while their COMSEC tightened and Allied COMINT quickly fell off [10]. German SIGINT gave 90 percent of their Intelligence about Allied O.B. [8] The Allied advance came to a halt at about the same rate that Allied COMINT dried up. After another six-month buildup and several major calamities, such as Arnhem and the Battle of the Bulge, the Allies were finally able to penetrate Germany and occupy it, but the Intelligence situation was generally very poor and COMINT had serious outages for months.[8] The German Army fell back onto landlines inside Germany, and the gradual spread of Reflector D on Luftwaffe Enigma circuits cut down on decrypts. [7] Three German Army keys were heavily read for the last three months of the war but Tunny was the main source, although it took longer to decrypt and therefore was not as timely. [7,10] At Remagen COMINT gave the German plan to bomb the bridge. [7] Allied aircraft bombed the German airfields, and COMINT also gave damage assesement from the raid.[7] This protected the bridgehead. After the Allied armies broke into Germany, knowledge of German Order of Battle and capabilities was critical to the speed at which the Allied forces moved East. [7] Revelations of German intentions were confused by the disparity between orders given and actions taken. [7]

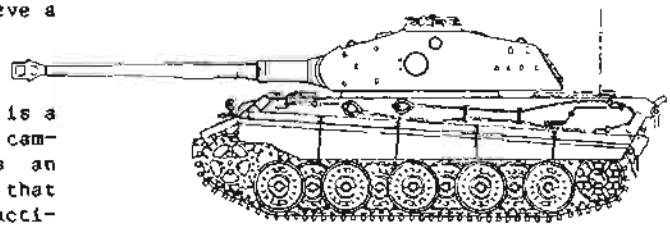
~~(TSC)~~ Although COMINT fell off after September 1944, because the Allies had extraordinarily good COMINT during the critical months before and after the invasion, they were able to apply their local superiority in airpower and seapower to hold down casualties and keep the German ground forces from splitting their armies apart or driving them back to the sea. COMINT gave an unparalleled insight, at the operational level, to what the Germans were doing, and even though the beachhead expanded much more slowly than the planning called for, the Allies avoided disaster until they were strong enough to achieve a breakout.

(U) Summing up, Six Armies in Normandy is a very readable and interesting review of a campaign that, in hindsight, can be seen as an outstanding military success for the side that had the best COMINT and COMSEC. German tactical effectiveness generally offset Allied material advantages. The small size of the Allied force, and the low casualties, compared to the German losses and collapse, suggests that COMINT and COMSEC combined had a much higher tactical value than is generally recognized.

References

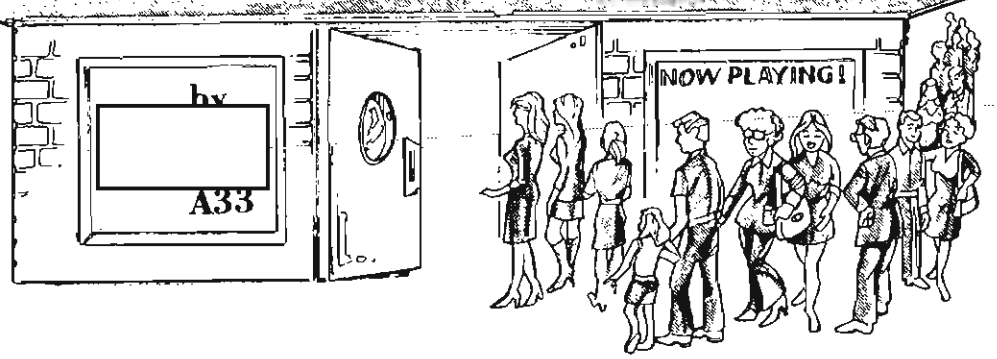
[1] Keegan, John, Six Armies in Normandy, New York: Viking, 1982.
[2] Bennett, Ralph, Ultra in the West, New York: Scribners, 1980.
[3] Bauer, Cornelius, The Battle of Arnhem, Kensington, N.Y. 1979
[4] Gabriel, Richard and Savage, Paul, Crisis in Command, New York: Hill and Wang, 1978.
[5] G.C.&C.S. Army and Air Force Sigint, Vol. XIII, p.196, 228-30, 1952. (TSC)
[6] G.C.&C.S. Army and Air Force Sigint, Vol. XVIII, p.193. (TSC)
[7] G.C.&C.S. Air & Military History, Vol. VIII, Ch. 1,V, 1952 (TSC)
[8] G.C.&C.S. Air & Military History, Vol. XI, pp.220-5. (TSC)
[9] G.C.&C.S. Army and Air Force Sigint, Vol. XVIII, pp.125-7. (TSC)
[10] [redacted] History Lesson, Cryptolog, May 1982.
[11] [redacted] Der Fall Wicher, NSA Technical Journal, Vol XX, No. 2, Spring, 1975. (TSC)
[12] Cassidy, G.L., Warpath, Toronto: Ryerson, 1948.
[13] Shulman, Milton, Defeat in the West, Secker & Warburg, 1948.
[14] G.C.&C.S., Army and Air Force Sigint, Vol. XIII, pp. 14, 20. (TSC)
[15] U.S. Army in WW II, Army Ground Forces, Procurement and Training of Ground Combat Troops. GPO, 1948, pp 72-85.
[16] U.S. Army in WW II, Breakout and Pursuit, GPO, 1950, pp. 692ff.
[17] U.S. Army in WW II, Lorraine Campaign, GPO, 1950, p. 1.
[18] Mallory, K. and Ottar, A., The Architecture of War, Pantheon, 1973. p. 123, Ch. 10.

P.L. 86-36



DOCID: 4011953

TSS REVOLUTION (U)



P.L. 86-36

This paper will convey some of the lessons that have been learned about the effect that Terminal Sub Systems (TSSs) have had on NSA.

(U)

This paper was presented at the CISI Conference, 25 May 1982.

TSS REVOLUTION

~~(C)~~ I can sum up the major effect that TSS has had on the Agency in one word: REVOLUTION (sudden, complete change). The technology is revolutionary because:

- it is a friendly (but not lovable) machine/human interface;
- the PLATFORM network provides access to remote data; and
- the software facilitates a flexible, adaptable system that can satisfy many active analytic requirements.

The *TSSs have* brought about cultural changes that are revolutionary for those analysts, software developers, and Agency managers who have access to or deal with the TSSs.

~~(C)~~ Therefore, I will speak about the technical cultural revolution that has been going on in the Agency for the last five or six years. I believe that we now stand on the brink of yet another revolution at this agency: that of the powerful personal computers, local area networks, and true distributed processing. Some of the lessons we learned during the TSS Revolution can give us insight into the next revolution that lies ahead.

TECHNICAL REVOLUTION

~~(C CCO)~~ First, what's revolutionary about the TSS technology? The PDP11 and UNIX version 6 are mid-70s technology--certainly not state-of-the-art in 1982! But if you step back and consider what a TSS gives you, it might be viewed in a different light. It's a mini-computer that is not overly powerful in terms of performance, but quite powerful in terms of:

★ software;

★ the connection with PLATFORM that provides access to analytic systems and data all over the building and in spots around the world; and

★ the tempested smart terminal that can be loaded with several different software packages.

(U) What's so great, you ask, about the software? After all, it gives you the ability to sort, edit, compile and execute programs, and do the normal things that most systems do. Well, UNIX has some features that set it apart from traditional operating systems, especially in the interactive analytic environment.

SIGINT as an Art

~~(C-CCO)~~ One point we must realize is that SIGINT analysis, like programming, is an art. Individual analysts perform similar jobs in different ways, reflecting their individual styles and approaches to problems. For example:

- one analyst may have a collection of message traffic that he scans in several passes, first very quickly to get an idea of the content, then in several additional passes extracting relevant information from which he is generating his report;
- The next analyst might make only one pass, extracting all the information needed by carefully going through each message only once;
- The next person may extract data and reformat it with, say, a permuted index or a matrix to present the data in a form which he can analyze.

Each is doing the same job, but doing it in a different way. In this dynamic, multi-faceted Agency environment, a system that forces an analyst to conform to the way the system wants him to work and that does not adapt to individual analytic approaches will not achieve widescale acceptance.

Flexibility and Adaptability

(U) The key to the acceptance of UNIX by analysts has been its flexibility and adaptability. The I/O is set up so that, instead of writing a special program that does all the functions you want, you have a large set of programs that perform specialized functions and chain them together in the sequence you need to do the work. The output of one program goes into the input of the next program, until the series of functions is complete. This gives a tremendous amount of flexibility in the sequencing of functions an analyst might need to perform a job.

(U) Add to this feature the ability to create INTELLIGENT command files--shells--and you have a powerful set of functions that can be configured easily into a tailored human interface that is analyst-friendly.

P.L. 86-36

~~(C)~~ Add to this the ability to acquire data electronically from [redacted] and other major and minor computer systems via PLATFORM, and you have an Analyst Support system that helps an analyst:

- ☐ get the data he needs;
- ☐ format it they way he wants it;
- ☐ manipulate it for various types of analysis;
- ☐ store and accumulate data to monitor trends;
- ☐ update data bases on major hosts, if appropriate;
- ☐ access word processing functions to generate reports;
- ☐ forward it electronically for release through [redacted] (soon); and P.L. 86-36
- ☐ interact with analysts on other systems using electronic mail and OPSCOMM-like functions.

(U) So, even though TSS technology is mid-70s, and not state-of-the-art, it does represent what I call a technical revolution at NSA.

CULTURAL REVOLUTION

(U) Now, what about the cultural revolution? I spoke earlier about the cultural effect that TSSs are having on analysts, software developers, and managers. I would like to briefly describe these effects.

Analysts

~~(C)~~ I think you can imagine the effect that TSS has had on the end-user from my previous description of how the system might be adapted to different analysts and analytic approaches. The flexibility that I described not only permits each analyst to do a specific job in his own way; it also provides a wide range of functions that allow each analyst to do many different types of jobs. UNIX supports a wide range of cryptologic functions: collection, CA, TA, linguistics, reporting, data processing, management, and others. It is thus a powerful tool.

~~(POUO)~~ Yet, there are frustrations. It has been estimated that less than five percent of the analysts in the Agency have access to TSSs. People in A3 are literally lining up to use the terminals. So, in a sense, we have not kept pace with the success of TSS in making the system available to analysts on a large scale. Also, the performance and reliability can be trying at times--hardware, software, and communications problems can interfere with the consistency of use that analysts should receive.

~~(POUO)~~ Some systems are overloaded to the point that performance has degraded to a serious degree. I believe [redacted] T44, coined the term "Tyranny of Success" to describe a system that was so successful that it quickly bogged down because it was so popular. Tyranny of success is what we're experiencing on many of our TSS systems. These problems are being addressed, but they do have a cultural effect on end-users.

Software Developers

(U) The TSS revolution has had a significant effect on software development. We learned through experience which approach to software development seems best for this type of system.

Turn-Key Approach

~~(POUO)~~ The first applications project that we tried to develop was a TSS-based transcription system. Since this was a formal system acquisition, we did a lot of work on requirements analysis and came up with a design which was given a formal review. The review determined that the UNIX software which existed at the time would not produce the desired result, so a UNIX-based development was not started and an alternate approach was taken. This project is still in development and hasn't been operationally used by an analyst.

Evolutionary Approach

(U) In our next few projects, we felt that it was necessary to take a less formal approach to development, especially since we didn't really understand exactly what the analyst wanted and the analyst didn't really understand what the system could do. So we prototyped--we experimented. Our psychology changed from delivering a turn-key system to that of evolving into a system through iterations--build what we best understand is needed, try it out in an analytic environment, make changes, try it out, etc. THIS APPROACH WORKED!

~~(C)~~ This brought about many cultural changes. Software developers actually talked with SIGINT analysts. They actually learned about some of the functions that SIGINT analysts performed. They built small systems (and some not so small) that allowed the analyst to do a job. This was a good motivator for the developers and the analysts. REAL users were using the software that was developed on real targets (some of them very high priority). This stimulated and challenged the software developers. Analysts were getting prompt attention to their needs (on a small scale) and getting a growing set of functions that helped them do their jobs. Also, their advice and guidance was being sought--they had great influence over the software functions that were developed.

P.L. 86-36

(U) The people developing the TSS utilities, like Data Base Management Systems, forms packages, intelligent terminal software, etc., had some feedback on how useful the tools they built were, and what other functions might be needed--and this was very important. It caused an impressive set of utility functions to be built and made available, based on feedback from REAL users and applications software developers.

Analytic Approach to Evaluation

~~(S-CCO)~~ The analysts we worked with had two basic approaches to deciding what they needed. One approach was to get onto a UNIX host, go through all the programs available, and try to do their job. If they ran into a situation where there wasn't an existing function to do what they needed, they would ask us to build one. A good example of this is the sort routine. It did most of what was required.

The ASCII codes for characters didn't give the proper sort sequence, so P1 requested a version of 'sort' that could handle non-standard alphabets--and it was provided.

~~(C)~~ The other approach used by analysts to decide what they needed was to write a specification of some type--a concept of operations (CONOP), a requirements specification, or some similar document--and we would develop the capability in an iterative fashion. This approach worked well for the larger, more comprehensive projects like

This was different from the transcription system experience I mentioned earlier because we understood from the beginning that it would be an evolutionary development rather than turn-key. Users were generally pleased with this approach because they would get the opportunity to evaluate the development while it was going on and give feedback to the developers on changes they might need. In some senses, it was a rapid prototype environment.

(U) After this had gone on for a while, we looked around and discovered that a significant stockpile of basic software components existed for various types of analytic work. We basically had a box of analytic tools that had been developed and tested in operational areas on real problems.

Generalized Software

~~(S-CCO)~~ An important lesson that was learned during this development period was that the software could be generalized quite nicely in many cases, so that the same program, properly parameterized, could be used on various targets, by different organizations, on a variety of projects.

There are many instances where this generalizing, if designed into the project from the beginning and developed iteratively, has worked better than we had thought possible.

EO 1.4.(c)
P.L. 86-36

Graphics Experience

~~(FOUO)~~ An important example of this is the work the Graphics Investigation Group (T4, T3, R53) did on computer graphics, which resulted in a highly generalized graphics capability available to any TSS. In 1980 and 1981, the GIG sampled analytic organizations to find out what the general requirement for graphics was at the Agency. We concluded that most of the organizations had similar graphics requirements: mostly overlays on geography and management displays (charts, graphs, etc.). The similarity of functions at the software level told us that we could satisfy a wide range of requirements with a comparatively small software effort, by means of generalized graphics software.

P.L. 86-36

(U) To make a long story short, a generalized graphics package was developed (partly commercial, partly in-house) and installed on a TSS. This gave us a powerful, adaptable graphics software capability that operated on a TSS and could interface with the existing "alphanumeric" graphics programs.

~~(S-CCO)~~ More and more TSS systems were deployed, and more and more people learned about the ability of TSSs to assist them with their work; we began to get a lot of requests for software systems.

The system required some sophisticated alphanumerics, graphics, and transaction processing that challenged us to deploy what is probably the most sophisticated software system I know of on a TSS today. The development effort was successful: the system is in operation today. I would like to acknowledge the substantial software effort put forth by R53 in developing nearly all of the graphics software for OMS.

Management

~~(FOUO)~~ As you might suspect, with approximately 50 TSS systems in existence, the management problems in dealing with the many aspects of these systems are quite significant. This is an entire revolution in itself; we certainly don't have time here to even scratch the surface, but I do want to emphasize one point: there is a significant management problem throughout the Agency in dealing with this many systems.

~~(FOUO)~~ The TSS Configuration Control Board was established last year to gain control over TSS management. They are currently dealing with many management issues that affect current operations and future architectures and policies. The need to provide more direct customer support for a large number of interactive users and software support organizations may require significant changes in DDT and DDO organizations.

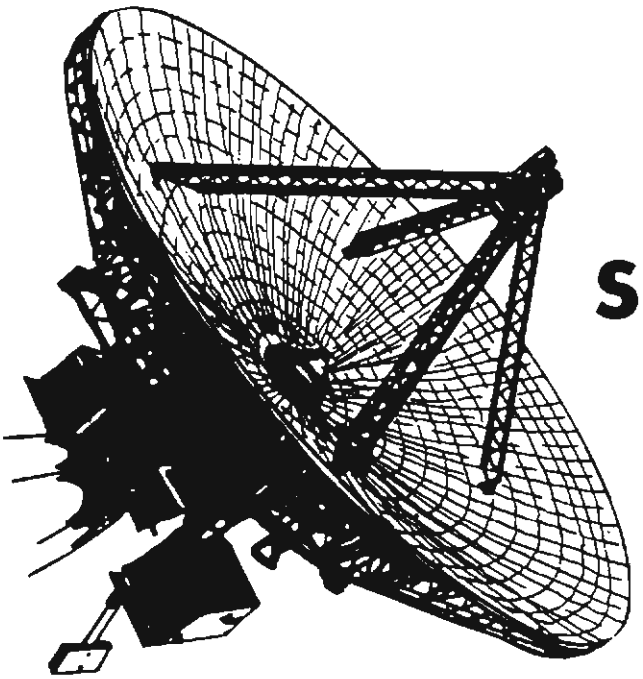
(U) The lessons we have learned from the current TSS Revolution--mixing operational prototyping, experimental development, evolutionary development, generalized software, etc., may, and SHOULD, have an effect on the acquisition of interactive systems. We can't afford on a corporate basis to get too informal, yet the more formal route has been shown to be not very successful.

REQUIREMENTS

~~(FOUO)~~ One final note. There is one substantial weakness in the software development process, whether on TSSs or other systems, that I feel is the cause of many failures and problems in system acquisition: REQUIREMENTS SPECIFICATION. Based on my experience, we don't do it well. It is a very difficult task. It's the most critical stage in the development of a project, yet it has the weakest set of tools of any phase of software development. I feel very strongly that if we had an automated method that would generate the requirements documents--or a functional prototype that both users and technical people could understand and work with--it would dramatically increase the Agency's ability to develop systems that really satisfy user requirements.

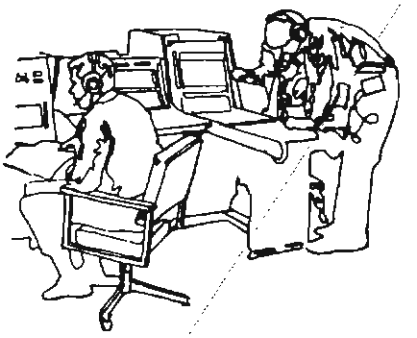
(U) I've tried to give you some of my thoughts and observations on what I call the TSS Revolution at NSA. Even though I've only touched on a small number of the issues involved with a technological and cultural revolution, we must remember that we are now on the verge of a new revolution. They are going to start coming more frequently now because of the rapid advances being made in technology. We have to learn how to deal with them with as little negative effect and as much positive effect on the Agency's mission as possible. We're learning!!

DOCID: 4011953



SIGINT: 1990 (U)

P.L. 86-36
EO 1.4.(c)



by Joseph Meyer, P13

(U) Major developments in telecommunications technology and systems during the 1980's will have a profound effect on SIGINT by 1990. The main threads of this development are new satellite systems, optical fiber cable, electronic switching, the coalescence of computers and communication nets, and the increasing complexity of telecommunications.

What new problems will SIGINT have to face by 1990? What do the new trends in technology tell us about the not-so-distant future? The author has adapted this article, presented here in several monthly installments, from his presentation at a January 1982 session of CA-305. The overall classification of the series will be TOP SECRET UMBRA.

(U) In order to see what the communications environment of 1990 will be like, and to analyze the impact on SIGINT, we will begin by looking at current trends in technology, networks and traffic growth, costs, and specific systems.

SIGINT 90: TRENDS, IMPACT, CHOICES

(U) In order to respond to the changes in the telecommunications environment, it is necessary to make some choices and to consider some specific actions, policies, and projects that will be needed. Most of these will be dealt with later in the paper; however, a fundamental choice is to begin with a suitable definition of SIGINT, viz.

SIGINT is the process of obtaining secret or unknown information from communication systems or signals.

(U) In this definition, it is the process, not the product, that is important. Also, the desired information, which may be intentionally kept secret or merely unknown to us, is to be obtained from "communications systems," not merely from "communications." The "system" includes all the traffic, but also includes things such as computer memories, circuits, switches, software, documents, etc. Any method of getting secret or unknown information from the "communication systems" or from "signals" falls under the authority of SIGINT.

(U) The importance of getting the definition of SIGINT right is that the classical "passive" model of SIGINT sitting back waiting for signals to reach it is no longer appropriate for the problems of 1990. The attacks against computer-communication nets, and against systems such as optical fiber, require operations based on physical and electronic penetration of the target links and nets, tightly coordinated with monitoring and analysis, to gauge how well the penetration is doing. This cannot be handled by multiple agencies trying to "coordinate" a mission; the authority and operations must be unified into SIGINT.

[redacted]

(U) There is little basis at present for optimism about the future if SIGINT continues to operate in its present framework, yet unoptimistic forecasts are rarely welcomed. As a paper "Why Pollyanas Prosper," at the January 1982 AAAS meeting noted, the meliorists discount the future at an extremely high rate in favor of confidence about the present. Thus, all the forecasts are rosy up to the very end.

THE TECHNOLOGY BASIS FOR TELECOMMUNICATIONS

(U) Many of the major advances in telecommunications have stemmed from advances in materials science.

MATERIALS SCIENCE IN TELECOMMUNICATIONS

Material	Application
Copper	Telegraph lines
Carbon Microphone	Telephony
Gutta Percha	Ocean Cables
Tungsten	Vacuum Tubes
Crystal Growing	Stable Frequencies
Semiconductors, Transistors	Computers
Magnetic Oxide	Core Memories, Disks, Tapes
Cryogenics	Space Communications
Solar Cells	Space Communications
Glass	Optical Fibers

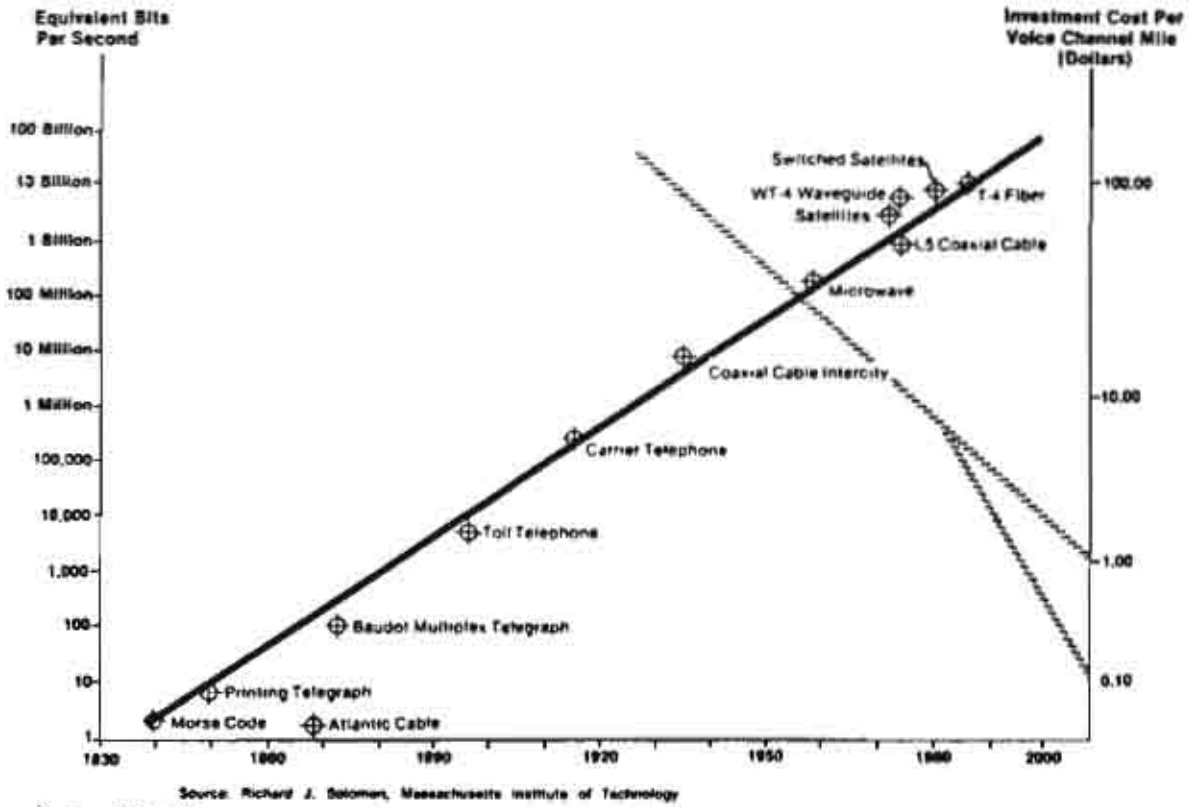
(U) The list above, although not exhaustive, indicates the importance of improvements in materials in the growth of telecommunications. The purification of copper was a fundamental step, for it made possible electrical engineering of all kinds, and electrochemistry has been a basic technique for purification of other materials. The advances in glass technology are currently bringing about a revolution in telecommunications by making landline cheaper than radio relay or satellites.

[redacted] P.L. 86-36 EO 1.4.(c)

(U) The effect of applying materials advances and various other inventions to telecommunications has been a steady improvement in technology, so that much more information can be sent at a much lower cost.

~~NOT RELEASABLE TO CONTRACTORS~~ ~~TOP SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

The Sequence of Inventions in Telecommunications, 1840-2000



P.L. 86-36
EO 1.4.(c)

1. SEQUENCE OF INVENTIONS IN TELECOMMUNICATIONS

(U) From the primitive 10 words-per-minute (wpm) transmissions of landline Morse telegraph to the gigabaud satellites and optical fibers of the late 1980's, there has been a steady advance in transmission capacity amounting to a tenfold capacity increase every 20 years since the invention of the electric telegraph. At the same time the average capital cost of building these systems has dropped tenfold in the last 50 years.

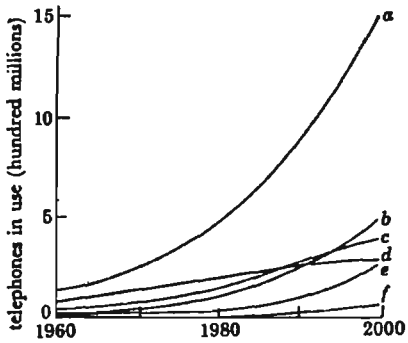
[redacted]

[redacted]

VOLUME FORECASTS

(U) Both traffic and equipment have increased in volume, so that the 400-million telephone plant of 1977 is expected to grow to a 1500-million subscriber plant by 2000.

DOCID: 4011953



Forecast growth in the number of telephones in use: (*a*) the world; (*b*) Asia and Oceania; (*c*) Europe; (*d*) North America; (*e*) Central and South America; (*f*) Africa.

2. FORECAST OF NUMBER OF TELEPHONES

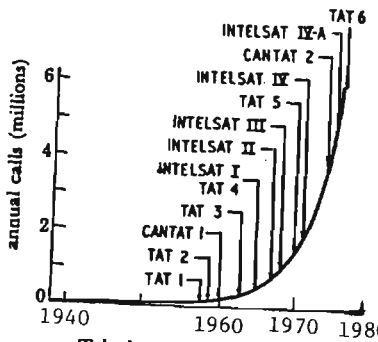
(U) The total "book value" of the world telephone plant at present is about $300 billion. An A.D. Little study predicts that $640 billion will be spent over the next 10 years for a new telecommunications plant, with expenditures rising to about $80 billion by 1990. This will be for a predominantly civil telecommunications plant.

(U) In the developed world the growth of telephone stations has slowed, as shown in curve (d) above, but in Europe and Asia the growth is faster, as high as 10-12%. In Africa the telephone density is not only low, but will remain low because of lack of money to install the plant.

(U) The cost of adding a telephone station to a network is about $2000, which covers the cost of the subscriber loop, local switch, and long-distance transmission facilities. Hence, the expected cost of telephone plants from 400 to 900 million phones by 1990 will require an outlay of about $1000 billion (reduced somewhat by more economical switching and transmission plants).

~~(S-CCO)~~ The impact of this growth in telecommunications plants, which will carry many services in addition to POTS (plain old telephone service) is that more and more of the political, economic, and military activities of the world will pass over telecommunications circuits and will be dependent upon those communications. This means that the potential returns from SIGINT will increase at least as rapidly as the telecommunications traffic, which is already growing at 20% annually. However, the vast physical plant, along with many of the technical improvements in switching, transmission, and security, will make it harder for SIGINT to find and exploit the specific traffic that is worth working on. To quantify this, the U.S., with about 40% of the world's telephones, generates about 170 billion calls per year, of which about 20 billion are toll calls. Non-U.S. toll traffic is about 20 billion calls, each about 10 minutes long. No agency can look at all of this traffic. The problem of selection is paramount and selection will become much harder.

~~(S-CCO)~~ A second impact of the growth of plants is that the turnover time for equipment will decrease. At present transmission systems have a cycle of about 15 years, after which it becomes economical to introduce new transmission technology, e.g., analog satellites of 1965 are being replaced by digital satellites of 1980. Switches have had 30 year cycles, even though old switches often are operated for 50 years. But these long service lives are no longer economical, and equipment will be replaced at a hastier rate by more capable equipment. This means that the lifespan of certain kinds of SIGINT systems and techniques will also be shortened, and new SIGINT plants and methods will be needed to keep up with the target changes.



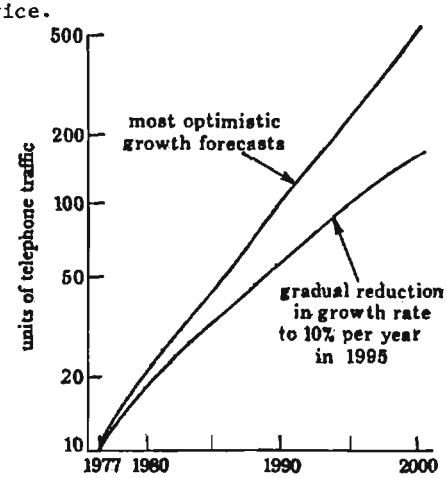
Telephone calls between the U.K. and North America, and the introduction of cables and satellites.

3. PHONE CALLS U.S./U.K.

(U) One of the most dramatic effects of telecommunications advances has been the increase in intercontinental traffic, as cheaper and better systems have allowed economic and governmental activities to operate on a global scale. In 1927 transoceanic telephony was initiated, with calls averaging 2000 per year. The first submarine telephone cable in 1956 brought about rapid growth in traffic, which continued to grow at 20% annually. The development of higher

capacity satellites and cables has given a transoceanic capacity of about 12,000 circuits. During the late 1980's this trans-Atlantic capacity will be more than quadrupled (see undersea cables, discussed below).

(U) In 1927, when there were only 2000 trans-Atlantic phone calls, each of those calls cost about $400, but today, with the increased volume and improved equipment, a trans-Atlantic call costs only a few dollars. The introduction of cable in 1956 improved call quality so much that it uncovered a demand which has justified expanding the capacity to the 12,000 two-way channels now in service.



Intercontinental traffic forecasts: telephone calls from the U.K.

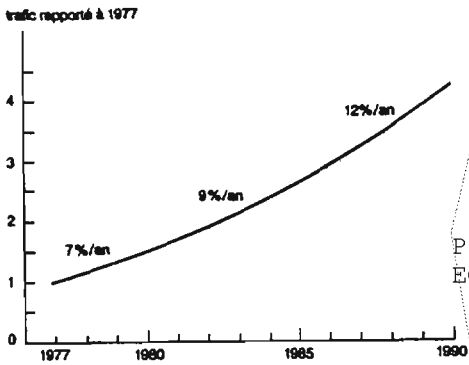
4. INTERCONTINENTAL TRAFFIC FORECASTS

(U) Various authorities, including Intelsat, have estimated intercontinental traffic growth at 22% annually, but more conservative estimates expect growth to taper down to 10% after 1990. The growth of telephony however does not express total traffic growth because, owing to time differences, the calls are generally placed in a short time window when people on both sides of an ocean are at their desks. Thus, late afternoon in Europe connects to early morning in the U.S.

(U) The transoceanic networks are designed to pass this peak load traffic, but so far have been comparatively idle during off hours, with traffic dropping to 20% of trunk capacity outside the peak four-hour period. The development of new kinds of traffic for international circuits, particularly digital facsimile, electronic mail, and computer data traffic, will tend to fill up the slack hours of the nets, so that total traffic flow will grow much faster than 20%. By 1990, the major telephone operating authorities expect digital facsimile to be the next major traffic after voice.

[redacted]

Télécommunications, objectif 2000



Évolution du trafic téléphonique total

5. 6% to 12% INCREASING TRAFFIC GROWTH

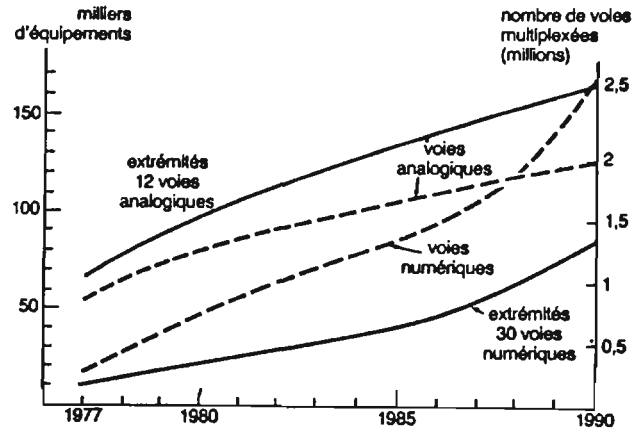
(U) CNET (Centre National d'Etudes des Telecommunications) has projected increasing growth rates for French traffic from 7% in 1977 to 12% in 1990. The projection is apparently due to expected improvements in speed, reliability, and cost of the services, as it becomes easier to use the network. Penetration of the telephone into new user areas is also a factor, for as more people are brought into the network, telephony replaces mail and travel.

P.L. 86-36
EO 1.4.(c)

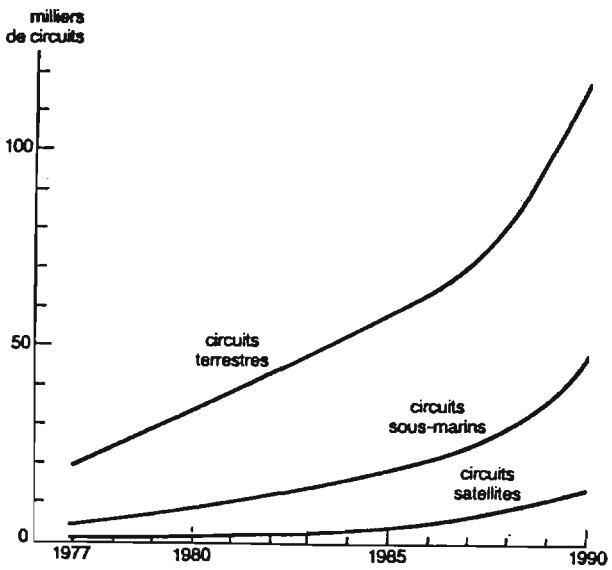
[redacted]

will be almost no aspect of the economic, political, social, or security activities in any country that does not use and depend upon the telecommunications systems. Hence SIGINT will have the highest potential growth rate of any intelligence service, and will be capable of the deepest and most extensive penetration into the activities of any target country--providing it can be done successfully and is adequately funded.

Télécommunications, objectif 2000



Équipements d'extrémité



Circuits internationaux

6. CNET: INTERNATIONAL CIRCUITS

(U) The French forecasts of international circuits up to 1990 show several interesting characteristics. Total circuit growth will be about sevenfold, but satellite circuits will only be a small part of the total, in spite of the fact that the French have been developing Telecom satellites. The main growth will be terrestial circuits, which is logical since France has substantial business with neighbors. The hidden element is that the French, as well as the other Europeans, intend to stay away from satellite circuits in favor of optical fiber interurban and international trunks. Satellites will be used for mobile services, and for backup and to establish new services temporarily until landline or optical cable can be installed.

~~(TS-CCO)~~ The impact on SIGINT of the European preference for optical fiber cable over satellite is that their international traffic will be harder to intercept. If the relations between the U.S. and Europe change during the 1990's (e.g., by the dissolution of NATO or by a political shift toward the Soviet Bloc or to Eurocommunism) those countries may become active targets, but access to their traffic will be harder. This access will be even harder if the U.S. presence is greatly reduced, e.g., by withdrawal of U.S. military and governmental organizations from Europe.

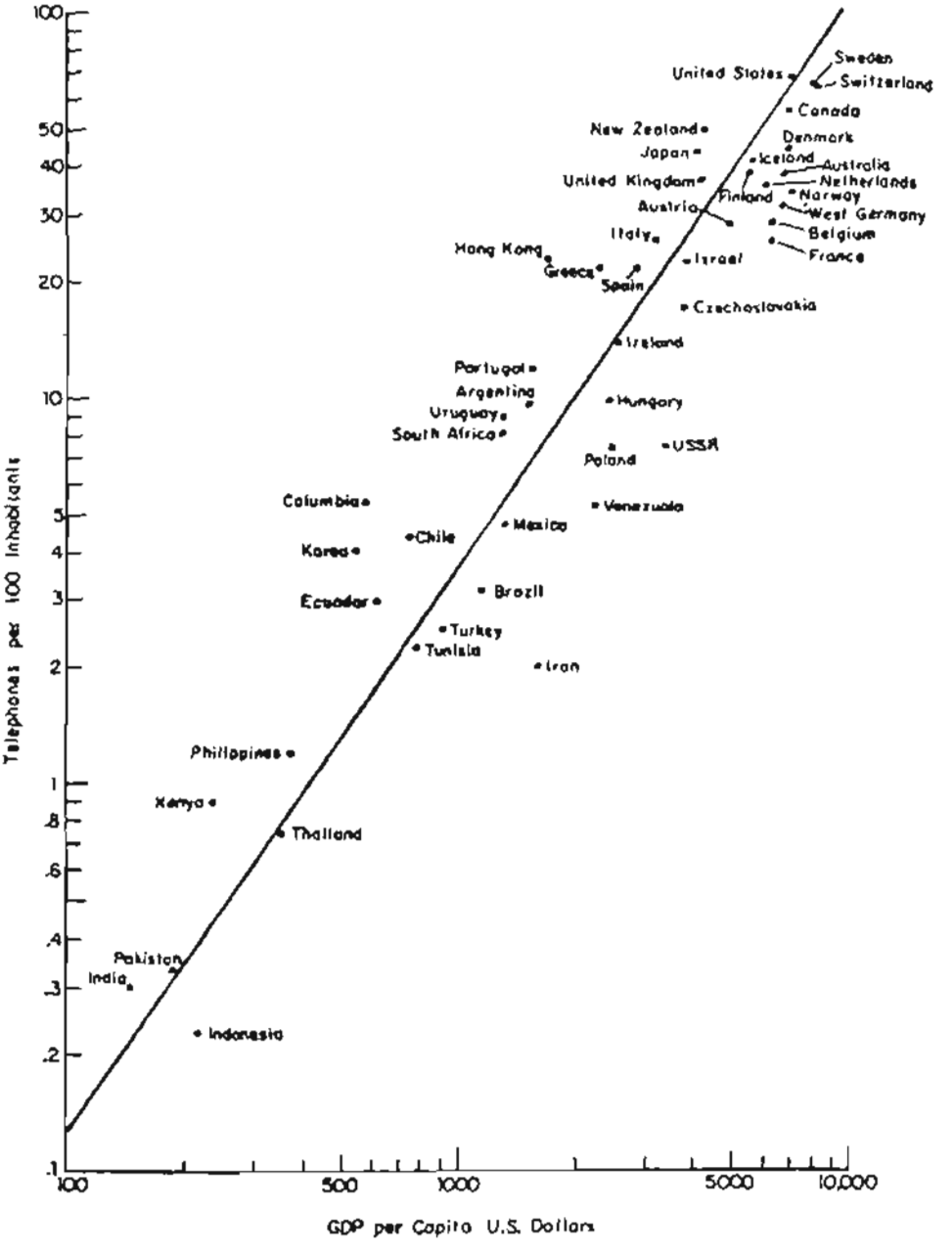
PHONE DENSITY/GNP RATIO

(U) The correlation between national wealth and telephone density is well established (see page opposite). The rich industrial countries have a high telephone density, as many as 70 phones per capita, while poor nations such as India have only about 3 telephones per 1000 inhabitants. In Africa the telephone plant is so undeveloped, that only Kenya appears on the graph at all.

(U) In spite of the lack of civil telephone facilities, the governmental telecommunications plants are often more advanced, with satellite and microwave and long-distance shortwave nets. The U.S.S.R. is a case of special interest because its telephone density is quite low, yet it has a highly developed governmental telecommunications network.

(U) One of the striking features of civil telecommunications in Africa and Asia and other low-income areas is that there are practically no rural telephone plants at all. At INTELCON 80, the Communications Minister of Nigeria asked his fellow Ministers of other African countries if any of them could name a single case of a rural telephone system, and there was no reply. The World Bank has been pursuing projects to introduce public telephone service into the rural areas of the

THE RELATIONSHIP OF NUMBER OF TELEPHONES TO
GROSS DOMESTIC PRODUCT IN VARIOUS COUNTRIES



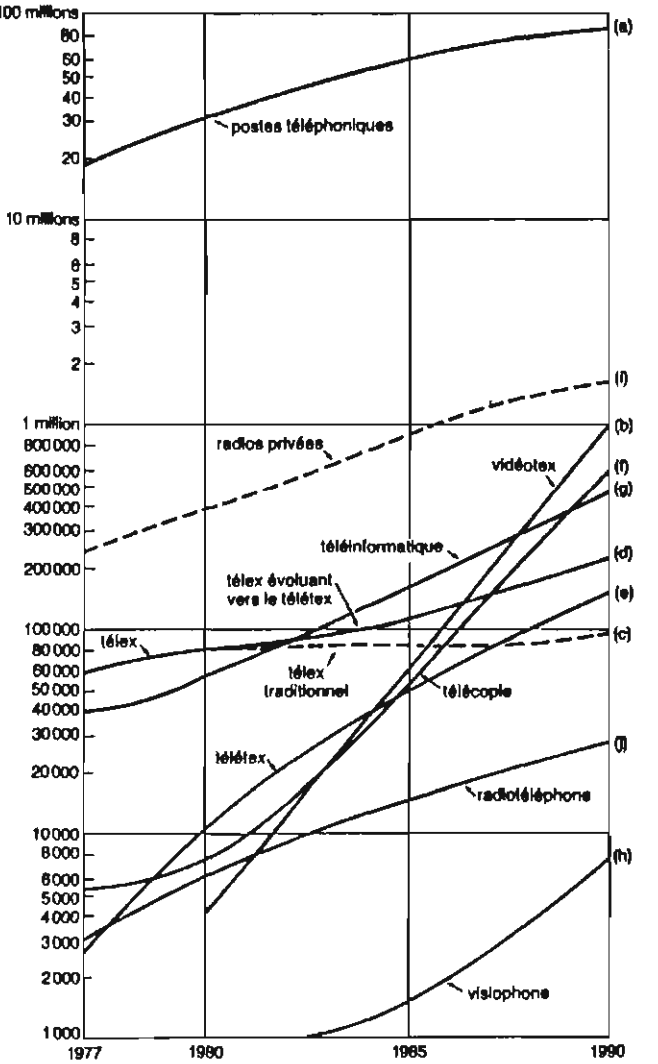
Source: INTELTRADE

Fig. 7

~~NOT RELEASABLE TO CONTRACTORS~~ ~~TOP SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

Third World, on the economic argument that the phone service will pay for itself, but progress is slow. The basic problem is cost, coupled with problems of equipment reliability. Satellite communications are not seen as an answer to Third World telecommunications in general, because the population is too sparse and the economic margins too slender to make two-way earth stations feasible even at the town level. Even when nations get some cash flow, e.g., from mineral exploitation, the money tends to stay in the cities where the rate of return is highest.

~~(S-CCO)~~ The impact of this telephone/GNP correlation on SIGINT is that for the rest of the century the spread of telecommunications services and the flow of traffic in the undeveloped countries will be tied to the cities and to economic and governmental activities, with the exception of broadcasting. The demand of the Third World countries for robust long distance communications created a problem at WARC 79 over HF allocations and assignments. The Third World nations will probably crowd into the HF spectrum as fast as they can buy equipment, but there is not nearly enough HF spectrum to accommodate them. The best alternative communications for remote area communications will be low-cost over-the-horizon systems such as meteor burst (cited below), thin route tropospheric scatter, and low bandwidth mobile satellite services, using high-powered satellites with big antennas. At the same time, the main telecommunications trunks serving cities and the industrialized countries will carry traffic that penetrates to every business, household, and government function. In brief, economic status will be the primary selector of telecommunications plant and traffic. The higher the relative cost of a message (or an enciphered message) in a country, the greater its expected information value.



Impact quantitatif des services de télécommunication (parc de terminaux)

(1) En dehors du terminal annuaire.

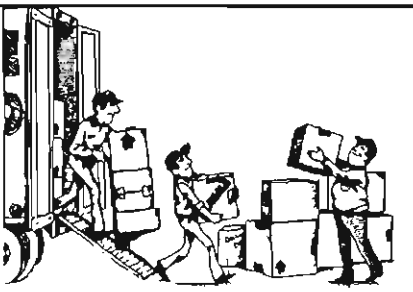
8. CNET: QUANTITATIVE GROWTH OF VARIOUS TELECOMMUNICATION SERVICES

~~(S-CCO)~~ The SIGINT systems will cover increasing masses of traffic in which the expected value of any message continually decreases, even though the total value of the information in the networks will continue to grow at least as fast as the GNP. One of the most interesting SIGINT factors is that the third world nations, being poor, are still largely open markets for well designed, heavily subsidized basic telecommunications plants which could, with enough ingenuity, create interesting SIGINT opportunities.

(U) While overall growth of POTS (plain old telephone service) will increase at about 6% annually, a number of specialized and new services will grow at higher or lower rates. The CNET graph above shows projections till 1990 for French services. Traditional Telex, which is already a saturated market, will grow very slowly, while new services such as private radio, videotex, teletex, and telecopier will grow at much higher rates. Private radio has been resisted by European PTT's, but CNET shows an expected fivefold growth over the next ten years. Teletex, at 2400 bps, is expected to have fifteenfold growth from 1980 to 1990, and more significantly is expected to become the "lingua franca" between various

information systems such as telex, videotex, computer data, etc.

(U) The growth potential of new specialized services is sometimes misleading, as the case of SBS (Satellite Business Systems) shows. Originally developed to sell high-speed data services to the top Fortune 100 companies, it has only managed to attract about 25 major companies, and they want POTS, viz. corporate voice traffic services. Long-term growth potential of network computing services is expected to be good, but over the short term the system and software costs may eliminate all but the richest companies. L.M. Ericsson has bought up Datasaab, to position itself in computer networks, AT&T is trying to develop a computer net service, and IBM is looking to extend its computing capabilities to overseas markets by international operation of a domestic satellite SBS system. Other domestic satellite (Domsat) operators are also looking for overseas outlets for their services. Even the German telecommunications giant Siemens is struggling to develop and incorporate successful computer services, even though its microelectronics VLSI technology is as good as that of the U.S. leader Intel Corp. (Business Week, 1 Feb 82, p. 87). The French government has undertaken a high technology program in telecommunications, aimed at export markets, and French industry is in a leading position in electronic switches and terminal equipment. For the modern telecommunication services, software development is a critical element, and only the Japanese are in a position to challenge the U.S. seriously.



FACTORY SHIPMENTS OF ELECTRONICS

(U) The steady growth of electronic sales (see figure 9) in all categories shows a tripling in dollar value. Electronics for information processing is the largest segment of the electronics industry, but the demand for communications common carriers has been growing the fastest in the last half-decade. Common carrier growth may be accelerated even more by future demands from "home information" systems.

P.L. 86-36
EO 1.4.(c)

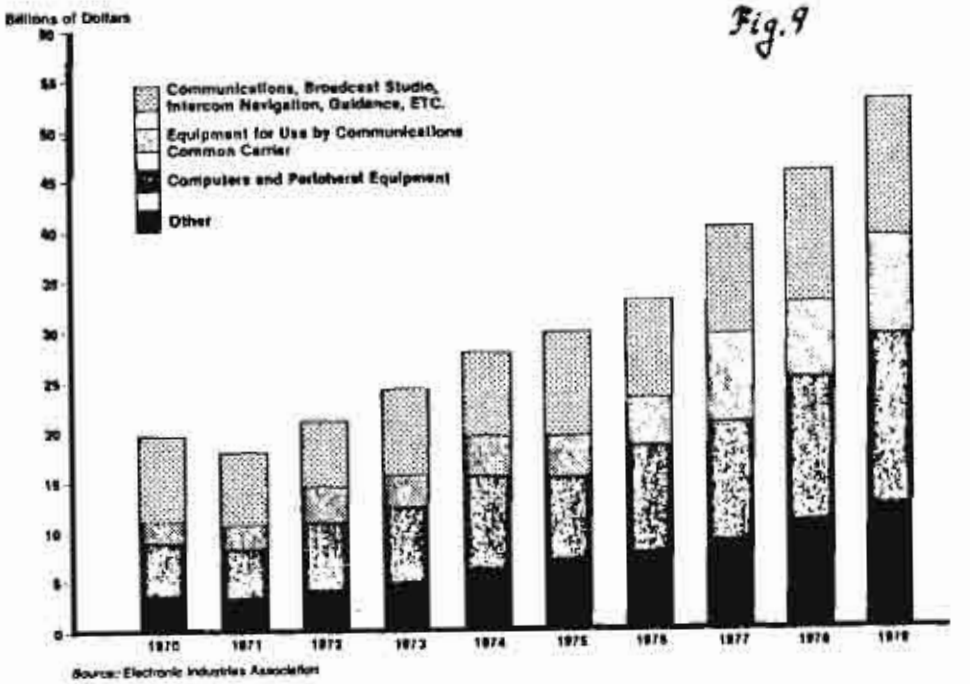
U.S. TRADE IN COMPUTERS

(U) The continuing growth in computer sales, and particularly the growth in imports, is a manifestation of the spread of computer manufacturing technology. The coalescence of computers and communications, examined below, will make this computer base a major factor in telecommunications. The strength of the foreign technology, especially the Japanese, is manifested in the imports. Another factor of some importance is that the U.S. market for telecommunications equipment is now virtually unrestrained for foreign competitors, who can subsidize sales to the U.S. to force an entry into the U.S. market. As the U.S. telecommunications industry is fragmented in the name of competition, more foreign computers, communication equipment, and services will take over parts of the U.S. market, e.g., for PBX's, interconnections, satellite links, data terminals, and even basic transmission and switches.

DOCID: 4011953

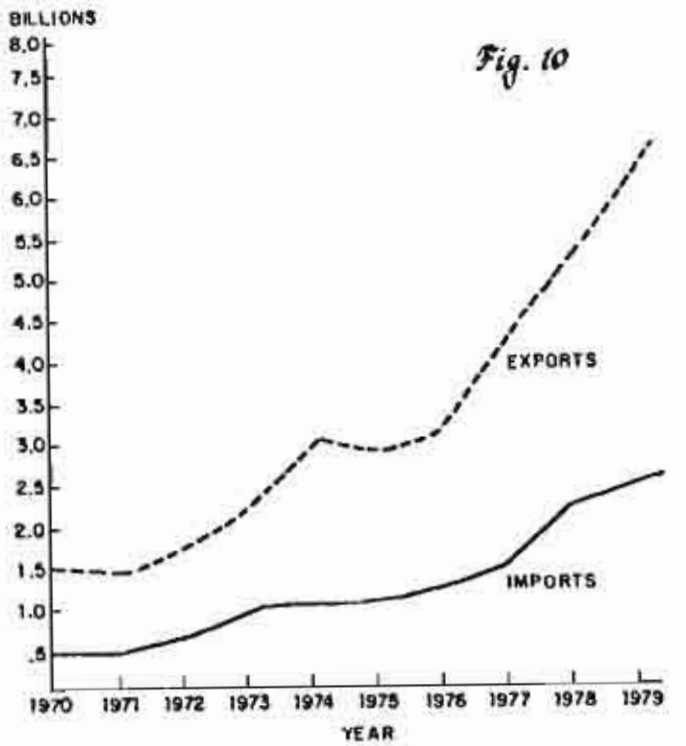
Annual Factory Shipments: Communications and Electronic Equipment by Type, U.S., 1970-1979

Fig. 9



U.S. TRADE IN COMPUTERS AND RELATED EQUIPMENT

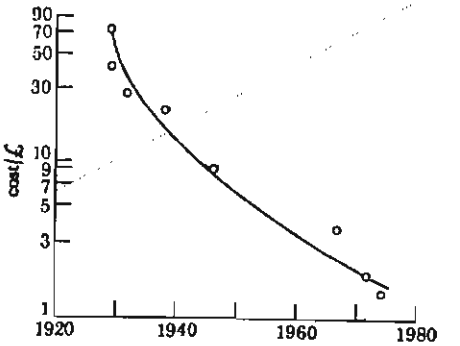
Fig. 10



Source: CBEMA

~~NOT RELEASABLE TO CONTRACTORS~~ ~~TOP SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

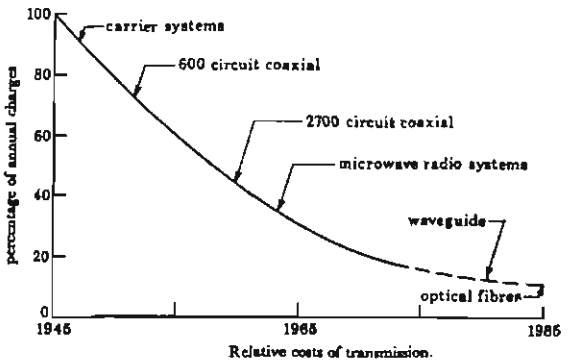
P.L. 86-36
EO 1.4.(c)



11. NY-LONDON PHONE CALL

(U) In 1927, when there were only 2000 calls per year, each of those calls cost about $400, but today such calls cost only a few dollars. The introduction of cable in 1956 improved call quality so much that it uncovered a demand which has justified expansion in capacity to the 12,000 two-way channels in service now.

P.L. 86-36
EO 1.4.(c)



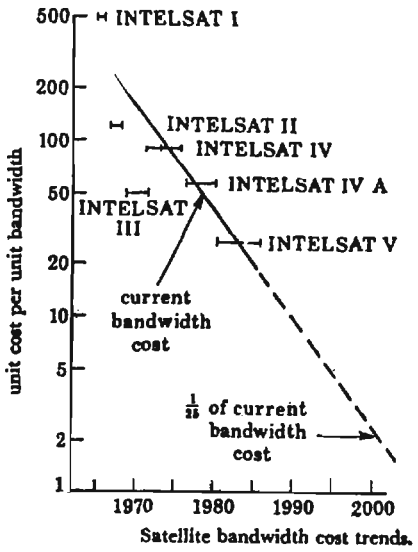
12. TRANSMISSION COSTS FOR DIFFERENT MEDIA

COSTS

(U) At the same time that the civil telecommunications plant has greatly increased in size and traffic capacity, the cost of services and equipment has gone down drastically. This has encouraged greater usage by a wider public, giving a larger revenue base which in turn leads to faster expansion and greater cost reductions.

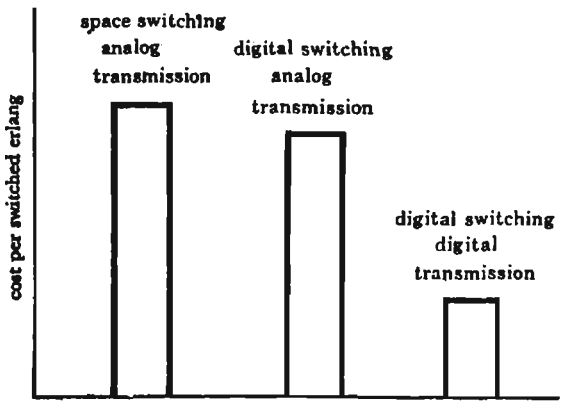
(U) To some extent the economies in technology in the civil nets have been applied to governmental and military dedicated nets, but at the same time the military nets have been given more difficult requirements, e.g., anti-jam, security, transportability, survivability, etc., so that the unit cost of military communications has not fallen much, and the demand for much greater capability and higher information rates has made military telecommunications more expensive for the same mission.

(U) Technological advances in transmission have greatly reduced the costs of moving traffic. For many years microwave radio relay was unsurpassed as the cheapest medium for trunk traffic. Efforts to develop radio waveguide transmission were unpromising, but optical fiber waveguide has developed so rapidly in the past ten years that even the major manufacturing companies have been surprised. Over the next ten years optical fiber will be substituted for existing or new cable and radio relay on many thousands of kilometers of trunk routes, particularly where traffic is heaviest.



13. SATELLITE BANDWIDTH COST TRENDS

(U) Reductions in satellite costs have been even more rapid than in terrestrial systems. The development of stabilized satellites which could keep solar panels and directional antennas pointed at sun and earth has given much increased power efficiency. A combination of improvements in space and earth systems has produced more than twentyfold reductions in channel cost in little more than a decade.



14. TELEPHONE SWITCHING COSTS

(U) Capital cost of switches used to be 50 percent of the total cost of the telephone plant. This was one of the reasons that switches were designed for 30-year financial lifetimes, viz., the cost of the switches was amortized over 30 years in calculating the rate base for subscriber costs. This led to a great deal of conservatism in telecommunications planning and a resistance to innovation. By contrast, computers and the associated operating systems and manufacturing plants have usually been written off after 7 or 8 years, because of the rapid changes in technology. Now, as digital switching is introduced into telecommunications networks, the capital cost of the switches is dropping to about 15 percent of the total network, so that much less money is tied up in the switches. At the same time the switches are more capable. The No. 4 ESS of AT&T has undergone a complete replacement in hardware technology, while keeping the software and functions the same, and this has reduced frame cost, space, and power requirements by 60 percent.

~~(S-CCO)~~ A major implication of the reductions in switch cost, which is further affected by the deregulation of telecommunications in the U.S. and the opening of the U.S. market to foreign switch manufacturers, is that the financial and functional lifetime for switches may be reduced from 30 years to less than 10 years over the next decade. It will not be worthwhile to keep an old switch in service when a cheaper and better switch can do more and provide entirely new services. This has an important implication for "SIGINT cultivation" discussed below.

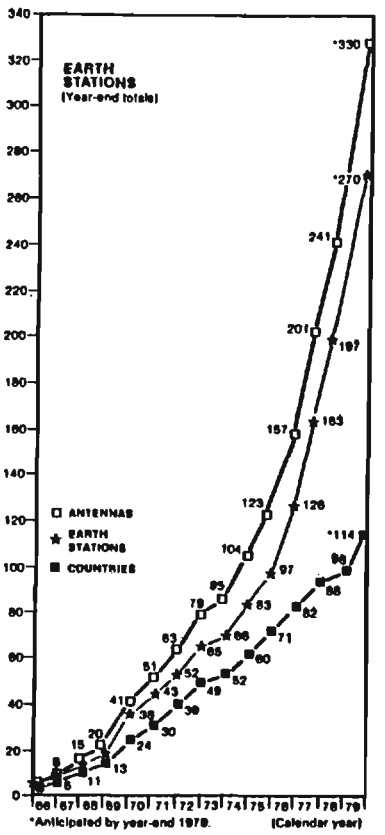
~~(S-CCO)~~ The major impact on SIGINT of all these cost reductions in telecommunications systems is that the target costs to install and operate nets are going down, while the costs of SIGINT are not going down. SIGINT is inherently labor intensive, and because it must extract unknowns from the target nets and traffic, it can never match the level of automation and efficiency of ordinary telecommunication nets. By analogy, a computer can search text for words, or do lengthy calculations far better than a human, but a person is far better at writing an essay or deciding how to attack and solve a mathematical problem. Most telecommunications is routine, while the most critical parts of SIGINT are very non-routine. Even the routine parts of SIGINT are subject to continuous change, so that economies of repeated large-scale operations are seldom realizable. When SIGINT is highly efficient, it is a result of chaining information in a highly non-routine way. Inevitably, the cost reductions in telecommunications will result in more and more plant and traffic, which will be more and more overwhelming to a fixed level of SIGINT effort.

~~(S-CCO)~~ One of the keys to reducing costs is to standardize the traffic, so that all

kinds of traffic (voice, facsimile, telex, data, etc.) can flow through the nets easily. Another key is to concentrate traffic so that efficient wideband transmission can be used. The immediate effect of these measures on SIGINT is that larger volumes of data have to be collected and scanned, with less easily identified characteristics, which means that the SIGINT costs per extracted message go up as the costs of transmitted messages come down. This is an ineluctable consequence of technologic advance, as long as SIGINT depends on a modus operandi and a physical plant which creates this cost exchange.

RADIO COMMUNICATIONS

~~(C CCO)~~ Because modern SIGINT has been predominantly based on radio interception, it is worth looking at some of the main trends in future radio systems, to see what effect these will have on targeting and collection, and on the subsequent analysis of radio traffic.



Source: INTELSAT Annual Report, 1979

15. INTELSAT GROWTH TO 1980

(U) The principal international satellite system, INTELSAT, began in the mid-1960's with one trans-Atlantic satellite and a few big earth stations, and by 1980 had over 400 antennas at about 270 earth stations.

FUTURE OF SATELLITE COMMUNICATIONS

(U) Saturation of the radio bandwidth has been a mounting problem in satellite communications (figure 16). This is particularly crucial for orbital slots used for transoceanic communications. At WARC 79 arrangements were made to increase satellite bandwidth allocation to nearly twice the pre-WARC amount. During the 1980's the major satellite developments will be in the 12-14 GHz frequency range, but by 1990 current projects show that demand for satellites will outrun the availability of those frequencies, and various countries are now developing technology for the 20-30 GHz range for the 1990-2000 era. For special purposes, millimeter wave and laser beams will be used for up-down and for intersatellite links.

(U) The initial applications of satellites were to international circuits, through the INTELSAT organization. Now the area of rapid growth appears to be in domestic and regional satellites that operate outside the INTELSAT framework. During the next decade NASA will launch over 100 payloads, most of which will be communication satellites. During the same period ARIANNE will launch about 50 payloads, also mostly communication satellites. Market estimates expect a demand for 1000 transponders for the Western Hemisphere, and about the same number for the rest of the world, added to existing satellite systems. Broadcast satellites for direct-to-home, or for broadcast distribution to fairly small antennas, will also grow. These broadcast satellites will also be capable of one-way message services. Mobile communication satellite services, particularly for shipping, are already in operation, and will extend their services to isolated fixed and mobile users.

(U) These new satellites will be capable of significant traffic volumes because they will be able to reuse frequencies. A typical transponder has a nominal bandwidth of 40 MHz and will carry about 40 Mbps. If 1000 foreign transponders are in service, this corresponds to a traffic capacity of about 40 gigabits. In addition to the foreign and international satellites, there is a proposal to allow domestic U.S. satellites to crossnet into foreign networks, because many of the multina-

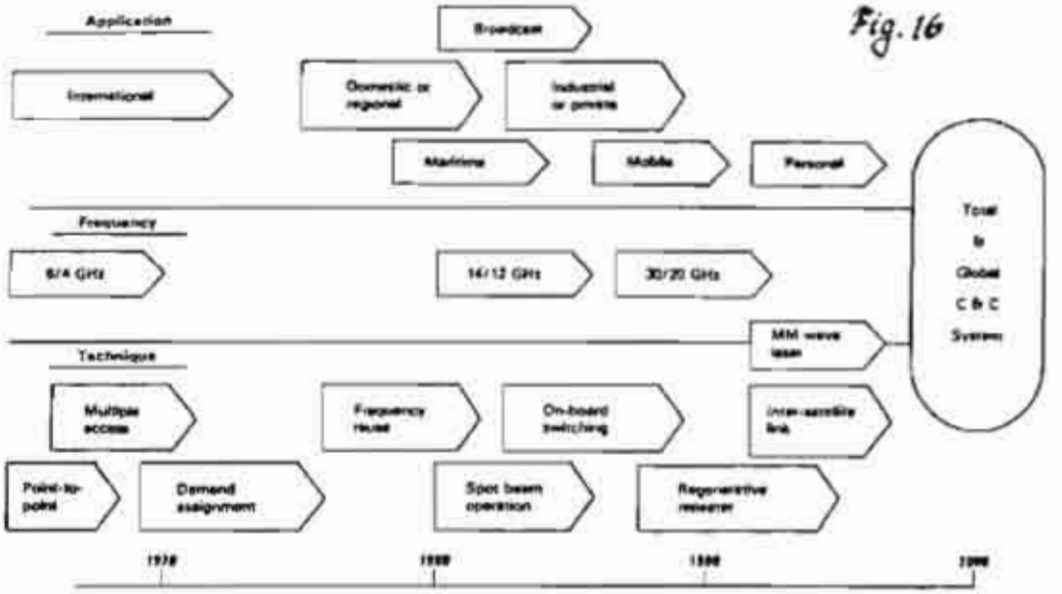


Fig. 16

FUTURE OF SATELLITE COMMUNICATIONS

tional customers have foreign facilities and they want their dedicated corporate satellite nets to reach directly to the foreign sites. The power of these companies is so great that they may cause the foreign PTT's to yield to their needs.

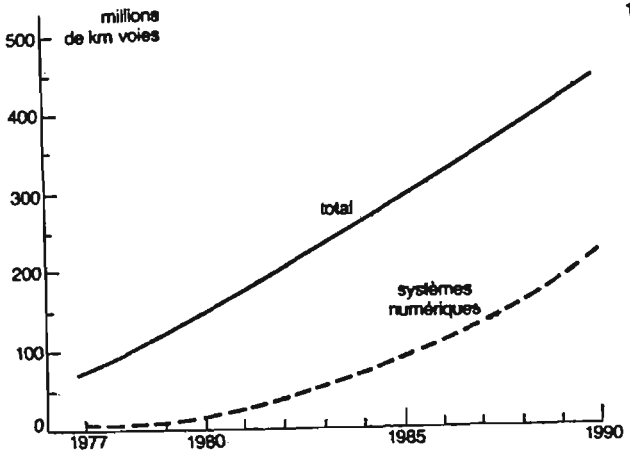
(U) Various new techniques will be used to increase the efficiency of satellite communications, principally spot beam operation, on-board switching, and regenerators on the satellites. By 1990 the transmission techniques will have advanced to the point where it will be necessary to measure the position of the satellite within a few millimeters, and to transmit a timing signal accurate to a picosecond around the U.S. to allow the high bit rate (10 gigabits/sec) operation, and on-board switching. The spot beams will switch from ground point to ground point to direct satellite energy to time-switched users.

(U) An example of the new trend in satellite communications is the French TELECOM I, which combines the features of MARISAT and SBS and provides a low-speed wide-area service and spot beam high-speed data relaying, with 25 Mbps trunk encryption.

~~(TS-CCO)~~ The impact on SIGINT of this expansion of satellites and traffic, and the introduction of new technology, is that, first, the data volumes will be overwhelming. Second, the spot beam operations will require intercept earth stations to operate within the "footprint" of each targeted satellite; and, third, the collection technology will have to be at least as sophisticated as the target satellite. The fourth problem, implied by the change to spot beams, is that intercepted traffic must be relayed from outside the U.S. in great quantities.

P.L. 86-36
50 1.4.(c)

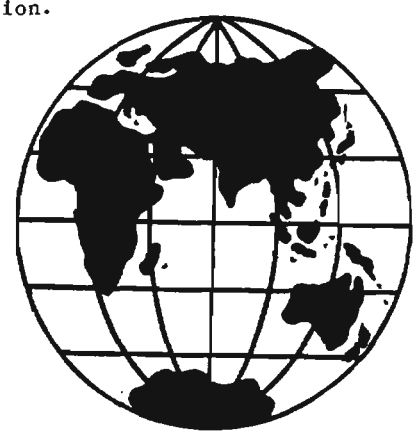
~~(TS-CCO)~~ Obviously, it would be better to select desired traffic before relaying the data, but improvements in switching, especially Common Channel Signaling and bulk encryption of satellite channels, will defeat the existing systems of preselection and targeting.

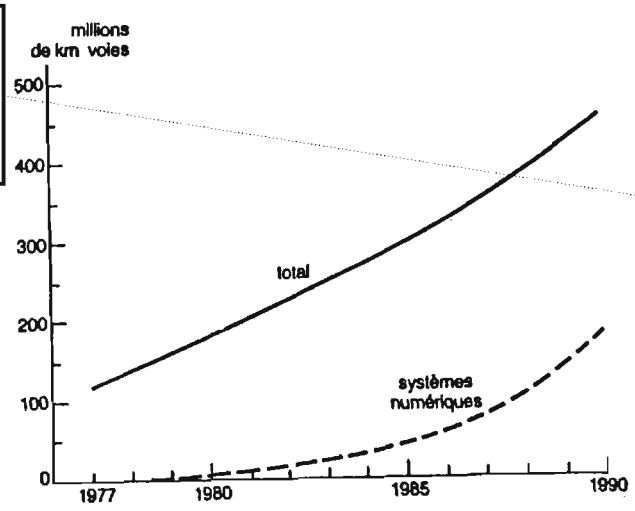


Systèmes sur faisceaux hertziens

17. GROWTH IN FRENCH RADIO RELAY

(U) The advances in satellite systems has by no means canceled the growth of terrestial radio relay. The French CNET studies show a fivefold increase in their radio relay over the next decade, with digital transmission accounting for half the growth. The digital microwave systems, pioneered by the Japanese, have shown robust performance in the presence of urban noise. In addition, they lend themselves to data communications and to bulk encryption.





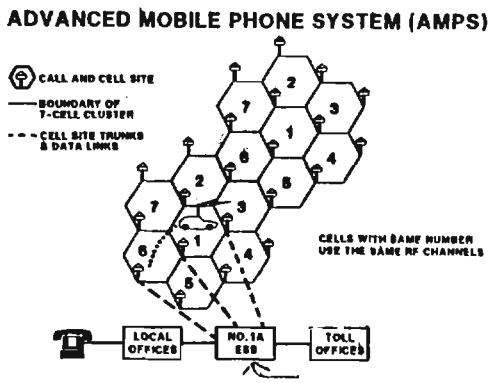
Systèmes sur câbles

18. GROWTH IN FRENCH CABLE

(U) The French, who had concentrated on cable, have not abandoned this medium, and CNET studies show a fourfold increase in cable capacity over the next decade. Digital cable transmission is also a fast-growing subset of this new plant.

~~(C-CCO)~~ The impact of these French developments on SIGINT derives from the fact that the French have an aggressive export policy in the area of telecommunications technology. Only a small part of the $60-billion world market is actually accessible to competitive marketing, but the French have studied this problem and have established a program to make equipment developed for the French PTT particularly suitable for the export market. The French banks and government collaborate in getting the overseas contracts, despite keen competition from the Japanese and other European manufacturers. As a result, technology developed for the French market, including switches and terminal equipment, will be sold on favorable terms in the Third World market to get the French manufacturers in on the ground floor. The French are even selling new switches and terminal equipment in the lucrative U.S. market. The result will be a steady flow into Third World countries of modern digital telecommunication equipment, accompanied by the adroit national presence of the various supplier countries.

P.L. 86-36
EO 1.4.(c)



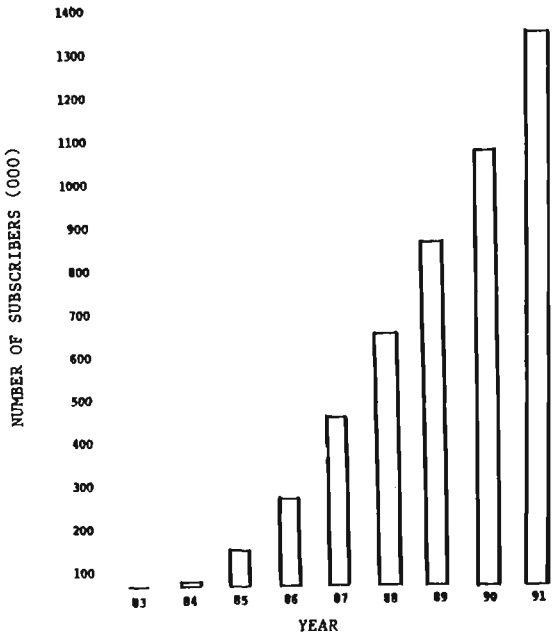
Switched Digital Capability

19. CELLULAR RADIO

(U) One of the large growth areas expected in new telecommunications equipment and services is mobile telephone, which can connect directly into the civil telephone nets. The current scheme for such mobile phone systems is to have a large number of frequency channels, and many transmitters in an area, e.g., a city. The radio system will track each user vehicle and switch the call to a radio channel that can be heard by the mobile station. The mobile receiver is switched at the same time. For ordinary FM radio links, the user is unaware of the switching. As the vehicle moves, it is assigned new frequency channels. As a result, the circuit for a single conversation may change frequencies many times as the vehicle moves. A large electronic switch (No. 1A ESS) is used by the Bell System for their mobile telephone system. Other proposed schemes would use spread-spectrum transmission so that many competing services could operate competitively in the same geographical area. With the interest in privacy and security for voice, digital mobile services are being studied, but the synchronization and switching are much more difficult.

~~(C-CCO)~~ The interception threat is not trivial, for a BEARCAT 300 scanner can monitor current mobile telephone channels easily. However, the problems of intercepting the switching circuits at 800 MHz is beyond a simple device such as a BEARCAT scanner.

PROJECTED GROWTH IN CELLULAR RADIO



Source: Motorola

20. GROWTH IN CELLULAR RADIO

(U) Motorola has projected rapid growth in U.S. mobile radio equipment over ther next decade, from less than 100,000 to over 1.4 million sets. Since Motorola is the dominant company in U.S. mobile radio, they are in a position to make the forecast materialize. The technology will will be copied abroad in the countries with high telephone density.

~~(TS-CCO)~~ The impact on SIGINT of the growth of these switched public telephone mobile services is that very interesting information may become available in the UHF spectrum in major cities, but it will present a complicated interception problem. Usually a set of frequencies is assigned to each transmitter and in the Bell scheme a seven-cell cluster is used to provide geographic separation for frequency reuse. SIGINT collection can thus be locked to the frequency plan, as the radio switching signals are also transmitted. However, analog encryption will probably come into vogue since most conversations will probably occur in a single cell. The mobile telephones are expensive, so that the traffic will have a higher expected value than ordinary telephony. This, combined with the large market, may encourage improved encryption systems that can operate over the switched radio links without loss of synchronization.

~~(S-CCO)~~ The cellular scheme contains an

indirect hint to SIGINT about how to do certain kinds of collection of mobile terrestial targets, for the propagation and noise studies and the tracking systems could be adapted to SIGINT.

(U) In addition to the high-growth radio systems cited above, there are a number of radio systems of special interest which will be mentioned later in the paper.

From: lrm at geishg04
Subject: Kudos
To: cryptolg at barlc05
cc: lrm

(U) Orchids again to [redacted] whose particular interests and insights never cease to interest and enlighten me. As a frequent writer of documentation for several volunteer groups (none of which have anything to do with computers) and an NSA manager, I found her June-July review to have almost universal applicability. I spend a lot of time off the job documenting procedures ranging from the mechanics of writing a business letter to the sweeping problem of handling customers' complaints. Mary's review has sent me scurrying to find a copy of the original article to see what other valid points the author might have on any area of instruction. Most of the highlighted points are equally applicable to any personnel manager who is either training an employee or assigning tasks, whether they be computer related or not. How true the quote: "If you tell a user to do something he does not know how to do...." Substitute person for user and you've got a great management guide!

Keep 'em coming!

[redacted]
G71 4007s
lrm@geishg04

MORE FREE GOODIES....

~~(C-CCO)~~ Delayed somewhat by a war, the third P14 "How to" working aid detailing UNIX/PINSETTER techniques for the traffic analyst is in final draft and should be in distribution shortly. This working aid, titled "How to Search", details the mechanics of using the search keys and the "binsrch," "grep," and "precog" commands.

(U) Organizations and individuals already on the distribution list for these working aids should receive copies by mid-August. If you or your organization is now or will be using TSS and UNIX/PINSETTER and would like to receive additional copies or be added to distribution, please contact [redacted] in P14 on 3369s. P.L. 86-36

SOLUTION TO NSA-Crostic No. 42

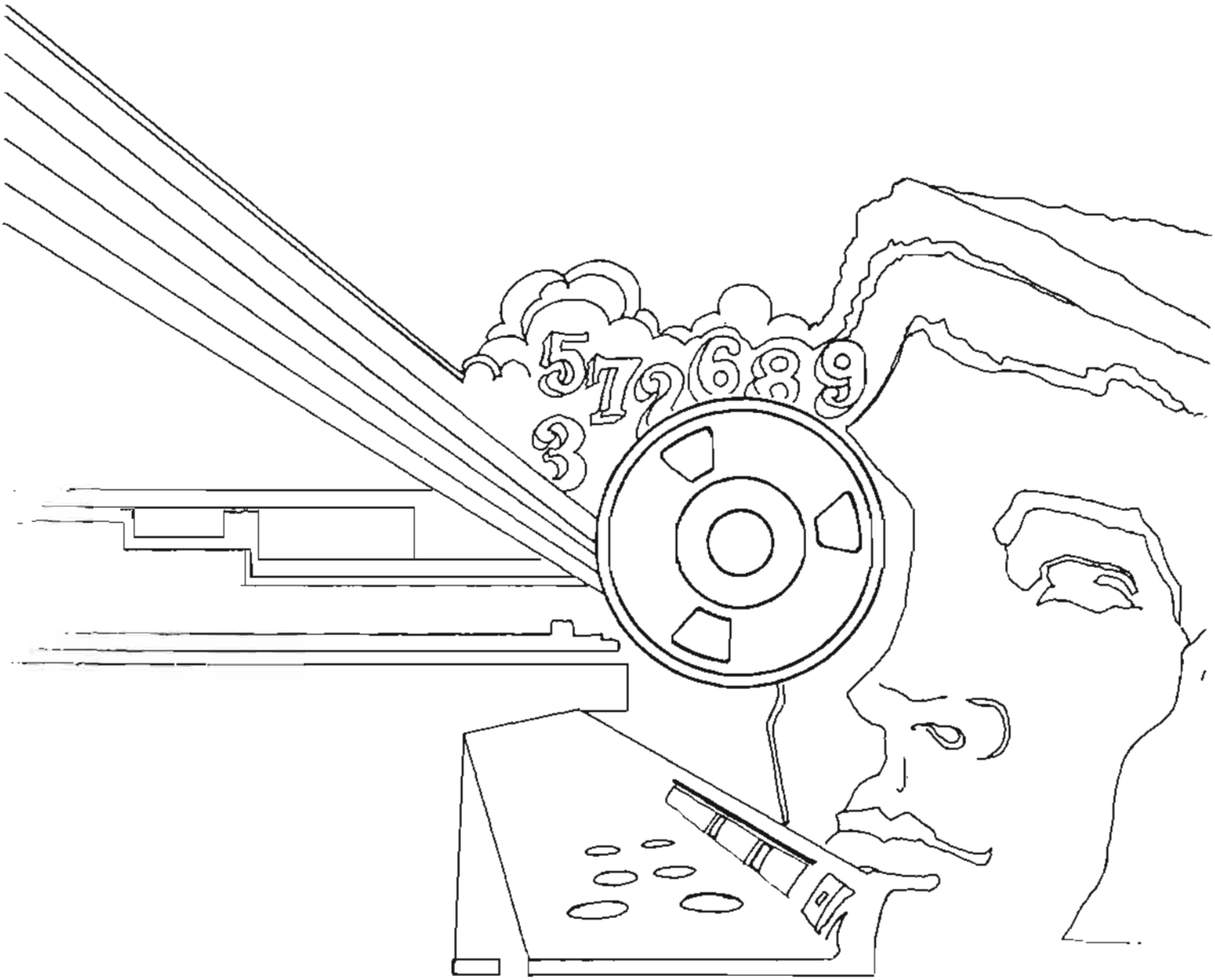
[redacted] "NSA Information Desk," CRYPTOLOG, May 1982

"Many times, NSA employees have [brought] to our [knowledge] the fact that NSA has been mentioned on the news or that they have read an article where the Agency has been mentioned. We appreciate this ...because it enables our office to keep the senior-level people better advised."

P.L. 86-36

~~(C-CCO)~~ [redacted] will be the speaker at the Autumn meeting of the KRYPTOS Society on 14 September 1982, at 0930 in the Friedman Auditorium. His talk, entitled "Twice Told Tale," pertains to a description of the "solution" of a cryptosystem which had been solved before, including analysis of indicators, cipher text, and cipher alphabets, as well as depth reading, programming, and historical research. The talk is classified TOP SECRET CODEWORD.

(U) [redacted] came to the Agency as a French linguist in 1952. The bulk of his career has been spent as a cryptanalyst in G Group. He spent several years as an instructor in the NCSch, and is currently a member of the Cryptographic Skills Enhancement Program in P15.


5 7 2 6 8 9
3

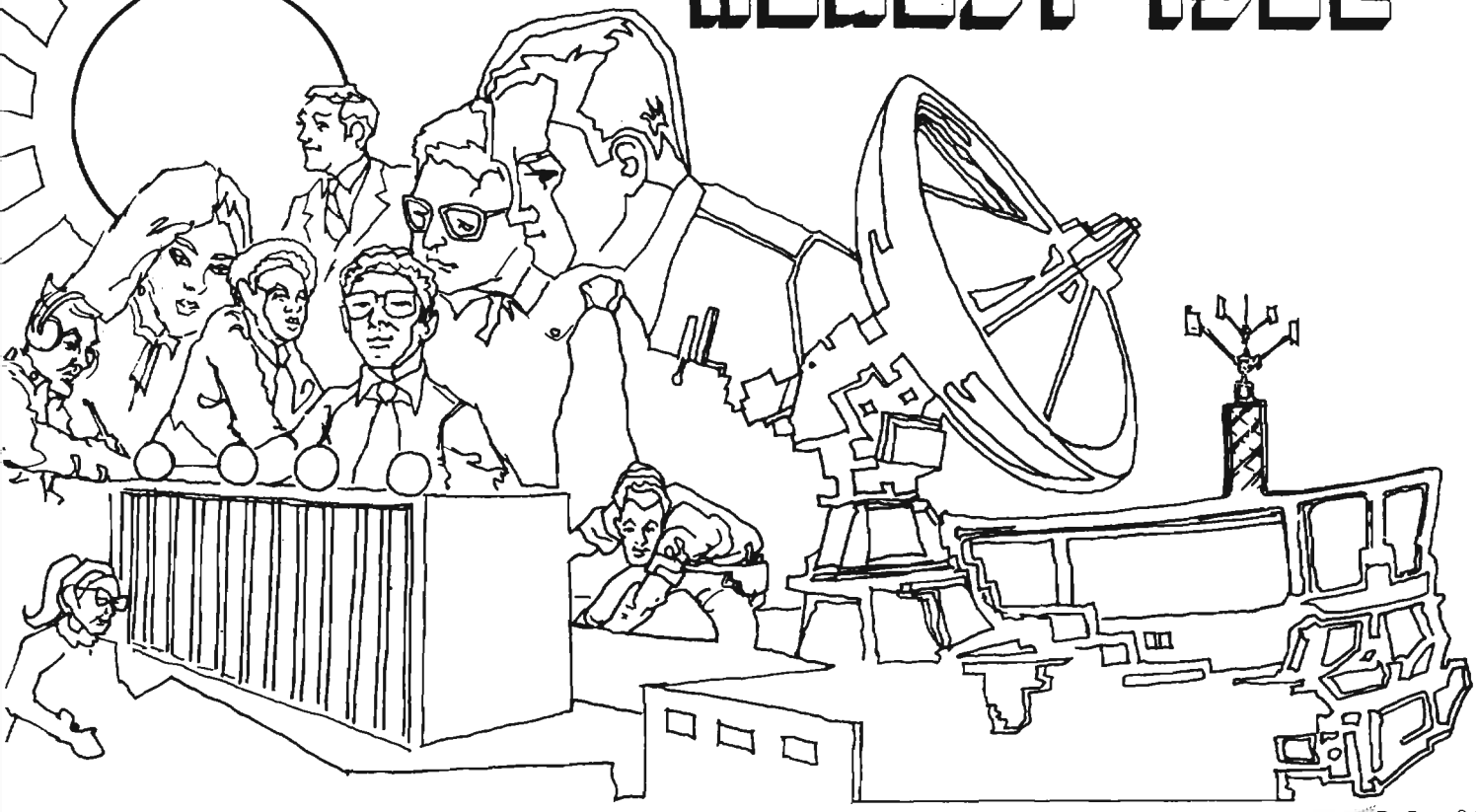
DOCID: 4009850

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

AUGUST 1982



P.L. 86-36

AFCEA 82 AND ICC-82: NEW CRYPTO DEVICES (U)..... [redacted] 1
WHAT PROMOTION BOARDS WANT (U)..... [redacted] 8
SHELL GAME (U).....W. E. S.....9
LINGUISTIC MACHINE (U)..... [redacted] 11
AN OLD PROBLEM (U).....17
ALL I EVER WANTED TO KNOW ABOUT DES (U)..... [redacted] 18
VIDEO DISPLAY TERMINALS.....
AND VISION OF WORKERS (U)..... [redacted] 23
I REMEMBER (U)..... [redacted] 27
NSA-CROSTIC (U).....David H. Williams.....28

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~NOT Rreleasable TO CONTRACTORS~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~Declassify on: Originating Agency's Determination Required~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009850

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. IX, No. 8 AUGUST 1982

PUBLISHER [redacted]

BOARD OF EDITORS

Editor-in-Chief. [redacted] (8322/7119s)
Production..... [redacted] (3369s)

Collection..... [redacted] (8555s)
Cryptanalysis..... [redacted] (5311s)
Cryptolinguistics..... [redacted] (1103s)
Information Science. [redacted] (5711s)
Language..... [redacted] (8161s)
Machine Support. [redacted] (5084s)
Mathematics..... [redacted] (8518s)
Puzzles.....David H. Williams (1103s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Don Taurone (3573s)

For subscriptions
send name and organization

to: CRYPTOLOG, P1
or call [redacted] 3369s

To submit articles or letters
via PLATFORM mail, send to

cryptolg at barlcØ5
(note: no 'O' in 'log')

Editorial

~~(FOUO)~~ Most people engaged in either managing or supporting analysts, and here I mean the analysts who produce the Agency's principal output, have the idea that they are helping the analysts in various ways. Theories about how to do this best are many and varied. Some people see the analytic process as a kind of production line, and therefore tend to think in terms of 'expediting' as a kind of helping. That is often the way I offer to 'help' my children do their homework.

~~(FOUO)~~ Some people, on the other hand, see the analytic process as an intellectual activity, rather like discovering the double helix, or deducing the presence of some new planet through the variations of the orbits of other planets. To them, the 'helping' tends to take the form of encouragement, or creating the proper environment so that this process of 'thinking' or 'discovering' can take place.

~~(FOUO)~~ When we come to consider how modern technology will 'help' these same analysts, what we come up with will depend, in part, on what sort of theories we hold about 'helping' them. If we hold to the expediting school, then our technological planning will naturally take that shape. If we are encouragers, our futurizing will be full of strokes and hugs.

~~(FOUO)~~ I remember one job where my helping of my subordinates did not fit most of these patterns. When a particular kind of action message arrived, my instructions to everyone but the one taking action (and that included me) was to flatten themselves against the wall until the action was completed. It worked, as those of you who labored there know well. But I'm not sure that such a 'helping' philosophy will ever find itself into our technology.

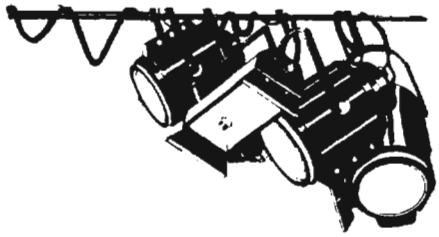
P.L. 86-36

WED

~~FOR OFFICIAL USE ONLY~~

NOT RELEASABLE

LOOKING AROUND with



P.L. 86-36

AFCEA 82 and ICC-82: NEW CRYPTO DEVICES(U)

(U) A number of new cryptographic devices were displayed at the AFCEA 82 Exhibition in June, 1982. The AFCEA show is known as the premier display of tactical communications equipment in the world, but in addition to the military cryptographic systems, some civil and police equipment was also on display. In general, there was almost no information about the actual encryption algorithms used, but key management, and nominal security factors were mentioned in brochures.

(U) MARCONI displayed their MINSTREL personal radio for police and military use. The military model uses a different encryption algorithm than the police model, and both algorithms have been tested by British cryptographic experts. The radio could be adapted to use a U.S. algorithm, according to MARCONI marketing representatives. The MINSTREL radio transmits a 16,000 bps stream of compressed voice in plain or cipher. Power output from the handheld unit is 0.5 W or 1.5 W. The radio weighs 500 grams. Dimensions are about 17 x 8 x 2 cm. For vehicle use, the handheld radio can be plugged unto a receptacle in the vehicle which switches it to vehicle power and antenna, then unplugged and taken out of the vehicle to protect the crypto unit. A special feature of the MINSTREL radio is the key control. The keys are not set up by thumbwheels, but are loaded by an optical device, so that the user never sees the key, and cannot change it. The key is about 160 bits, viz., 10^{38} different keys. Ten different radio channels are available, all on the same key. Because of the problem of terrorism and capture of the radios, channel 11 can be selected to clear the crypto variable so the radio is taken out of the secure net. The Fill Management Unit will generate random keys to load the radios directly, or to load them through a portable "fill gun" which uses an optical link. The radio and modulation system is compatible with the military CLANSMAN radios. Frequency coverage is 68-88 MHz, 146-156 MHz, and 420-470 Mhz. U.S. police and emergency frequency allocations are 150-173, 406-420, 450-500, with Federal as well as non-Federal allocations. There are also Federal allocations between 68-88 MHz. Therefore, the MINSTREL radio might be useful as a cipher radio for certain police and Federal applications in which there is no desire to expose U.S. cryptographic algorithms to loss or capture.

(U) MARCONI also displayed the MARACRYPT Mark II Key Management System, which improves the original MARACRYPT unit from 10^{10} bits to 2^{50} bits. The new MARACRYPT II units dispense with thumbwheel settings, and load keys from an optical fill gun, which stores and loads a 128 bit fill word. There is a facility for "stretching" a 10 character code of the type used in MARACRYPT Mk I to a 32 character fill word to provide interoperability between Mk I and Mk II updated equipments. The key is transferred as a 384 bit word, consisting of the 128 bit key variable in direct and inverted form, followed by 128 bits of control information.

(U) Both MINSTREL and MARACRYPT illustrate the new notion of keeping the key distribution under tight central control so that radios cannot be rekeyed in the field, unless a fill gun is available. MINSTREL will operate in the clear at 16 kbps, so that cross net traffic is possible in the clear mode. Flexibility as a base station, vehicle and handheld radio (with three different battery packs for the handheld model) make it useful for non military applications.

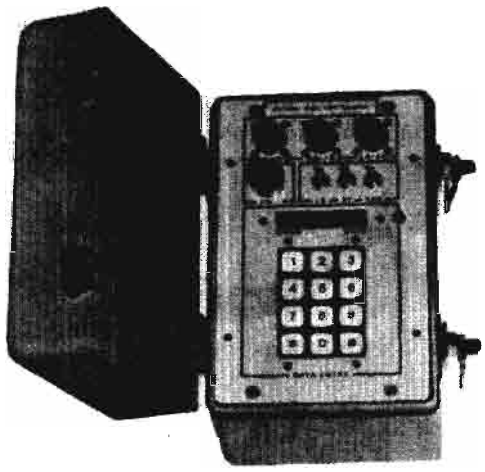
(U) PLESSEY displayed some similar radios, viz., the PTR 1851D VHF pouch radio which used the "Smalltalk" 16 Kbps speech encipherment. The PTR 2451 VHF vehicle radio operated at 50 watts. PTR 349 VHF squad radio transmits at 1 W and 3 W power levels. In addition, a PTR 3411 Groundsat terminal was displayed. The DMT (Digital Message Terminal) stores and receives or transmits messages at different rates, and has a 3500 character storage. On a radio channel, the DMT sends speech or stored data at 16,000 bps; over a telephone or 3 KHz ssb channel, the DMT can send at 100 or 600 bauds. The keyboards and output display present English or Arabic characters.

~~(NC)~~ PLESSEY is also developing a new line of equipment in a bid for a major Australian military communication project called RAVEN. The Australians have not modernized their military radios in some time, and wish to go directly to modern digital systems. For this, PLESSEY has developed new "brassboard" circuits to demonstrate the combined frequency hopping plus in-band spread spectrum technology to meet the RAVEN specifications. The equipment will hop at a 100 to 500 Hz rate, and will transmit data or voice. It will interface with the DMT, hence probably has a 16,000 bps data rate, using some spread spectrum coding.

(U) THOMPSON CSF displayed the TRC 773 tactical digital ciphony equipment for VHF and UHF operation. The speech is coded as adaptive delta modulation at 16,000 bps. The user is allowed more than 2.3×10^{18} different combinations, of which 65,536 are used for a fixed internal key. The radio is supported by a CRY 103 key processing and control unit, and a key injector CRY 104 unit. The TRC 773 will operate in the clear or cipher mode. There are protection devices to ensure perfect and secure operation, and a pushbutton erases the memory contacts in an emergency. Possible enciphered relay can be done by the CRY 105 device. The TRC 773 can be connected directly to the TRC 550 family, and connects to the TR.PP13 family by a broadband connector. The TRC 773 weighs 1.6 Kg as a handheld unit, and can be attached to a TRC 751 VHF/FM vehicle mounted transmitter.

(U) ROCKWELL presented the COLLINS VP-110 voice encryption unit for airborne application. This analog scrambler uses a proprietary algorithm to control the time and frequency scrambling. The encryption unit will accept 10^{19} key variables, which can be inserted at the unit through a 16 key input. They claim the algorithm is cryptographically secure, and that voice quality is excellent. There is an in-band digital controller for FSK synchronization to synchronize the crypto units during operation. Once a key or set of keys is set up, the device is locked with a metal key and the crypto keys cannot be changed. A special feature of the VP-110 is that it has a "public key" algorithm which can be exercised by pushing a button. Any two VP-110 units can exchange a key generated by a PK algorithm, so that every two party conversation can be secure from all other authority. This will make it possible for any two VP-110 users to exchange secret voice traffic even if they are on opposite sides in a war. This should present some interesting administrative problems in controlling the flow of secret traffic, and the arrangements that can be made in secret between consenting parties.

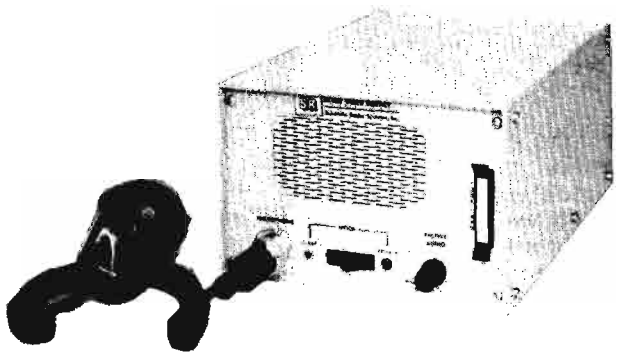
(U) ROCKWELL also presented the DDC-575 Digital Data Cipher, and the DDL-104 Digital Data Loader. The DDC-575 is used for encipherment of full duplex data channels at 576 Kbps. Other models in the DDC series operate from 128 Kbps to 2.048 Mbps (the CCITT standard). The key generator is a COLLINS high security proprietary nonlinear device with more than 10^{70} possible codes. Random start of the code generators (approximately one billion selections) is used to prevent attack in depth, according to the brochure. 80 octal characters can be used to input a key. Key generator and data path have check circuits to prevent faulty output. The DDL-104 is used to load keys in any of the DDC series. A TTL logic interface is used to connect the loader to the cipher device.



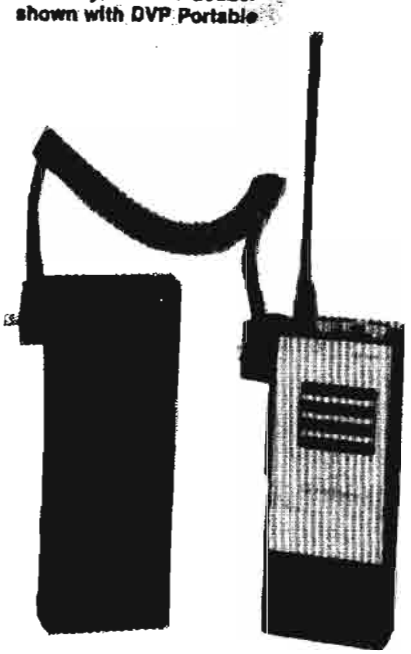
DDL-104 Digital Data Loader in Carrying Case

DDC-575 Digital Data Cipher, Single Configuration With Blank Panel

(U) SCIENTIFIC RADIO displayed their SR-800, a simple voice privacy device, which is not new. 3840 code combinations (in analog encryption) are available, and, at a lower price, a 128 code option is available.

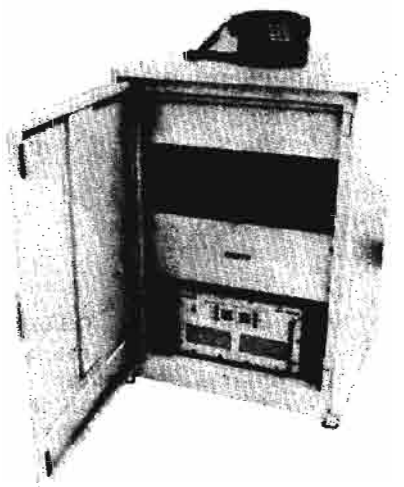


DES Key Variable Loader shown with DVP Portable



(U) MOTOROLA displayed several "DES Options" for DVP Digital Voice Protection Systems. The DES options W-338, H-338 and C-338 can be obtained with new radios or attached to existing MOTOROLA radios. Synchronization is achieved by a self synchronizing preamble. There is an internally derived pseudo random initializing vector, and a Key Variable Loader is used to set keys into the DES/DVP radios. To convert existing DVP radios to DES radios, the user only needs to exchange the DVP for the DES module. This implies that various crypto algorithms could be used for the DVP radios, in the same way that the MARCONI MINSTREL radio has several algorithms. Hence, the radios could be sold or exported with one algorithm, which is later replaced with a better one, without visible changes in the digital radio traffic. This may be a portent for the future.

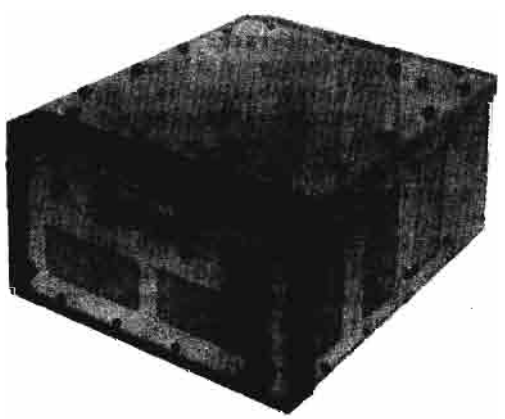
(U) GTE displayed their MRD-2000G TEMPEST Voice Digitizer, which uses the LPC-10/43 voice digitizer algorithm. The MRD-2000G is designed to interface to four wire or two wire telephone circuits, and with PABX and CENTREX trunks. It will transmit data at 2400, 7200 and 9600 bps in full duplex or half duplex mode. It uses a GTE fast synch algorithm. In addition to LPC-10/43, optional proprietary voice digitizer algorithms are available, viz: GTE LPC-10, APC-4, APC-4HSN, SBC.



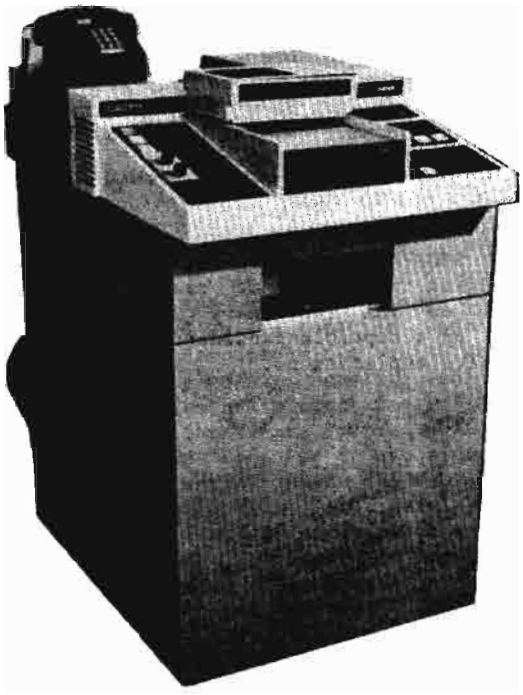
MODEL DVT-2000G TERMINAL

(U) GTE also displayed their model DVT-2000G telephone terminal with user furnished crypto specifications. This is designed for Government secure voice applications, and is used in conjunction with the MRD-2000G. A 7 inch space is provided for rack mounting of a customer furnished crypto unit, with a MIL-188C interface and 115 VAC power. The unit will operate over both two wire dialup unconditioned lines, and four wire tie lines with E&M signalling. The synchronization, using MRD-2000, takes 45 msec and uses 16 bit PN sequences. An optional push to talk feature can be incorporated.

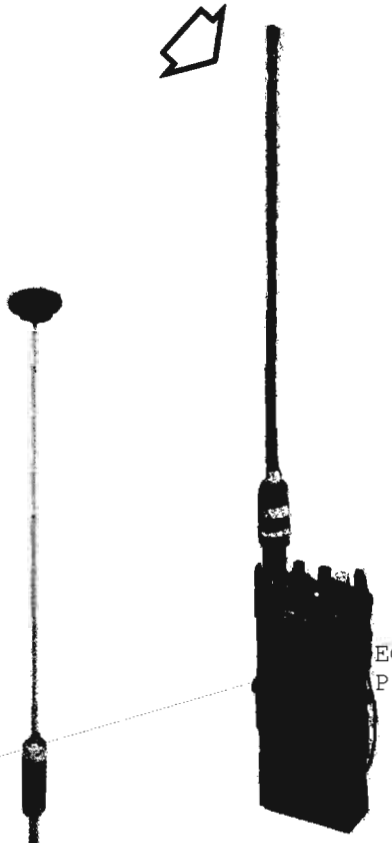
~~(C)~~ This illustrates the migration, i.e., technology transfer, into the marketplace of high grade speech processing and digital transmission developed for government and military needs.



MRD-2000G TEMPEST Voice Digitizer



(U) MAGNAVOX displayed their Long Range AN/PRC-68 VHF radio, which can be fitted with a SVM-68 Secure Voice Module, the PCG-68 Programmable Code Generator for SVM-68, and the CSD-68 Code Storage Device for SVM-68. The new PRC-68 uses a different antenna to get a 5 Km range.

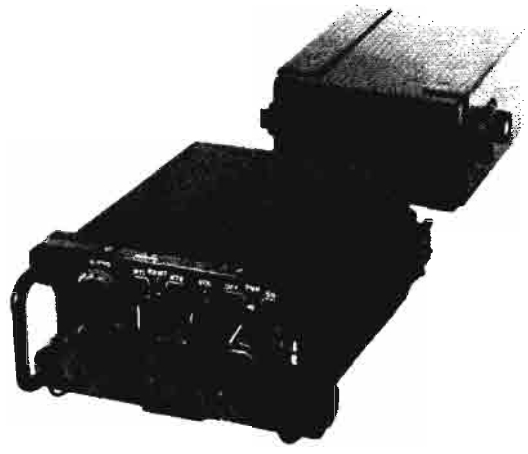


EO 1.4.(c)
P.L. 86-36

(U) MAGNAVOX has developed a M122 demolition control device with a fixed code to prevent erroneous detonation. At the factory, a unique (one out of a million) code is fixed in the sensors. A transmitter up to 8 kilometers away can send the code to the demolition units. Some military detonations take a long time to set up, and must be executed without tampering or misfires. The possibility of terrorist actions that set off civil detonators prematurely, which can cause unbalanced demolitions, can be countered by secure remote controls systems. Additional security for the sensor codes can be provided by a unit that can interface with the KYK-13, which also permits a number of sensors to be set off at once by the same code.

M122 DEMOLITION CONTROL DEVICE

DOCID: 4009850



(U) MAGNAVOX developed the MX-9331A/URC regenerative repeater for tactical secure voice. It will regenerate 16,000 bps or 18.75 kbps data. The MX-9331 allows the operator at the relay point to break in and listen to plain or cipher. It can be used with both VHF and UHF radios, and does the necessary operations to acquire, synchronize, and hold synchronization through fades.

(U) HONEYWELL advertised and displayed their SCOMP secure communications processor, bolstering their product evaluation with a letter on NSA stationary which labels the SCOMP "an acceptable candidate" for security-sensitive applications.

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755

DOD COMPUTER SECURITY CENTER

PRODUCT EVALUATION BULLE

AS OF: 1 December 1981

PRODUCT: Secure Communication r

MANUFACTURER: HONEYWELL Infc

DESCRIPTION:

The SCOMP hardware
Level 6 minicomputer w
Protection Module (SP
tation, paging, prot
Level 68 Multics, '
translation for I

A basic se
tion on which
In addition,
and trusted
oriented c
its secu
hierarc
while
oper

e
1.
etc.).

STATUS:

The development of the SCOMP hardware, w
by the Naval Electronics System Command (NAVEL
recently been completed. It is currently oper
only a few laboratory and evaluation environmer
has recently transitioned responsibility for th
their Avionics Division (St. Petersburg, FL) to
Systems Operation (McLean, VA), and it will be m
by the standard Level 6 facility in Billerica, MA

The security kernel software was developed as
the DARPA-initiated (NAVELEX sponsored) Kernelized
Operating System (KSOS) program and was designed to
a UNIX-compatible emulator. The emulator has been r
by the SKIP which is presently still under developmn
Therefore, software development for the SCOMP is not
self-hosted, but can be done on a standard Level 6.
tionally, the SCOMP is available in a NACSEM 5100 TEMP
version (AN/UYK-37(V)).

SECURITY EVALUATION STATUS:

Evaluation has not yet been completed. The DoD Comp
Security Center considers the SCOMP, with its security ker
a candidate for the class of products for which formal met
are employed to confirm the trustworthiness of the design.
An independent evaluation will be produced by the DoD Compu
Security Center.

ENVIRONMENTAL STRENGTHS:

The advantages of the HONEYWELL SCOMP derive from the
hardware support provided for security-related processing
requirements, and from enhancements designed with the goal
of maintaining performance for general purpose, multi-level
was originally targetted for secure processing. The SCOMP
secure, time-sharing applications. While the underlying
system was designed to support such an environment, the
currently available applications support software (SKIP and
trusted software) provide a secure base upon which one may
overlay specific applications. Although the evaluation has
not been completed, it currently appears that the SCOMP
will provide a state-of-the-art base for a variety of
security-sensitive applications. It should be considered
an acceptable candidate for a wide range of minicomputer
applications which require an enhanced architecture to
support secure processing requirements (e.g., communica-
tions processor, GUARD applications, data base systems,

*The
an Evaluate
government dev
products in a ma
Establishment. Th
to provide the statu
tion.

DOCID: 4009850

(U) TELETYPE displayed a MODEL 40/8C TEMPEST series teleprinter, which had the special feature of cassette input/output, in lieu of punched tape. One version of this teletype will accept a cipher device for on line secure transmission (Mod. 4033-8RYSB).

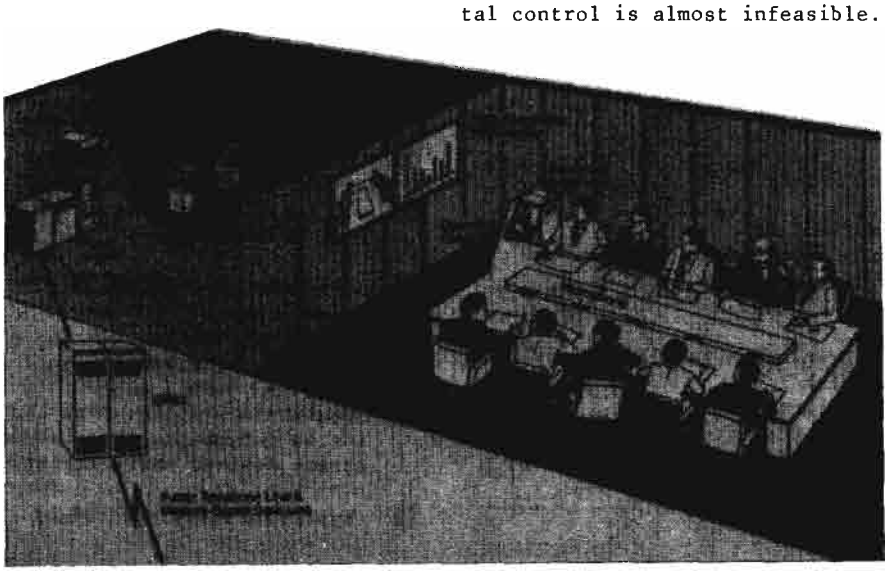
~~(C)~~ The point of particular interest is the cassette input/output. One of the cardinal needs in U.S. COMSEC is a convenient and cheap way of enciphering and deciphering offline traffic, so that sensitive traffic may be passed through the existing message centers without being read by the teletype operators. Small handheld computers can easily provide the encryption and message handling, and they will read and write audio cassettes. All that is needed is an interface device that will allow a handheld computer to use a cassette tape in the same format that the MOD 40/8C teletype accepts. This would permit cheap, reliable and unclassified encryption offline, with cassettes used as the medium for passing the traffic through the message centers. Since a major target country uses offline encryption for internal security employing punched tape, the U.S. could emulate this using audio cassettes.

Cryptology at ICC-82

(U) The Japanese intend to produce DES encryption chips for communications security. At the International Conference on Communications - 1982 (ICC-82), NEC displayed the NETEC-X1 TV Codec, for teleconference TV use, which does digital TV compression down to 1.544 Mbps, or 6.3 Mbps, and will use DES for encryption of both audio and video. At the 1.5 Mbps rate the image reproduction is fairly good, but there is a delay of about one second in response time. DES encryption will be used on four different codecs, viz: NPC-110A, NPC-111A, NPC-114A, and NPC-115A. The NETEC modems use only 1/40 to 1/6 of normal PCM TV signals, so that trunks or satellites can carry more conference links. NEC TVS (Telephone Video System) will also use encryption to send pictures over telephone lines. TVS-754 will send black and white, while TVS-751 will send color pictures or video frames. Both will use encryption.

(U) Although DES chips are difficult to manufacture, the Japanese have been very successful in copying U.S. technology. IBM still holds worldwide rights to the DES design, but it is unlikely that they would block NEC in implementing a publicly disclosed algorithm. Once the Japanese are able to produce the DES chips, U.S. export controls will no longer be effective. The proposed international data encryption standard is DES, and if it is adopted, the Japanese will be able to supply that market.

~~(C)~~ Summing up, the cryptology transfer inside the U.S., and across its borders, is creating low cost availability of tested and secure algorithms and key management schemes derived from U.S. cryptographic research. The use of Public Key algorithms to key airborne tactical voice links is a manifestation of this rapid spread. Serious problems arise in SIGINT, EW, Security and Counterintelligence. PK (public key) devices are an ideal way for a spy to transfer cryptographic data to a foreign buyer, without ever needing direct contact between the parties. While the academic community is concerned with publishing theoretical papers, the industrial community is interested in sales. The problem of control is that once the technology becomes cheap enough, or a market develops, governmental control is almost infeasible.



DOCID: 4009850

What Promotion Boards Want(U)

by [redacted] T1

P.L. 86-36

(U) Have you ever wondered what information in a promotion précis influences promotion board members? Have you tried to figure out what turns them on or off? If so, you are not alone. A group of T1 people approached this one head on. We asked some past and present promotion board members, "What do you look for in a promotion précis? What sells you on a person? What turns you off?"

(U) We share with you their pets and peeves. Perhaps you can add your own to the list.

PETS

- ☐ Describing job payoff relating to the characteristic described
- ☐ Giving numbers (quantitative things)
  - ★ People
  - ★ Dollars/Budget/Inventory
- ☐ Stating savings obtained
  - ★ People
  - ★ Dollars
  - ★ Space
  - ★ Material
- ☐ Listing unique contributions
- ☐ Logical order of events and accomplishments
- ☐ Bullets/One liners
- ☐ Off-duty activities
  - ★ Community involvement
  - ★ Leadership positions
  - ★ Unique abilities
- ☐ Using short sentences in plain, simple, readable English
  - ★ Impact sentences
  - ★ Quality vs. Quantity
  - ★ Specific application to individual recommended
  - ★ Active voice

PEEVES

- ☐ Using outdated information
- ☐ Repeating same information in all (or too many) categories, using same words
- ☐ Copying information verbatim from Personnel Summary
- ☐ Too wordy
  - ◆ "Snowed" with quantity, not quality
  - ◆ Not enough of the right kind of information
- ☐ Not expanding abbreviations
- ☐ Not explaining coverterms
- ☐ Using canned phrases
  - ◆ "Motherhood" statements
  - ◆ Government buzz words and phrases
  - ◆ "Jargonese"
- ☐ Using generalities without specifics
- ☐ Promoting the job instead of the person
- ☐ No specifics supplied about awards
- ☐ Lack of historical performance data since last promotion; no productivity specifics
- ☐ Nonconformity to format
- ☐ Errors and Inconsistencies
- ☐ No training courses or education since last promotion
- ☐ Paragraph structure
  - ◆ All begin the same
  - ◆ Passive voice
  - ◆ Long, poor sentences
- ☐ Mentioning outside work that has no bearing on duty performance or does not demonstrate desired characteristics
- ☐ Hyperbole

DOCID: 4009850

SHELL GAME (U)

WES

(U) You may not have realized it, but some of the commands on the UNIX system are really shells. As an example of a short UNIX shell, look a the UNIX command 'lsm' (whose full pathname is normally /usr/bin/lsm). Short but sweet! Another shell, this one rather long, is the UNIX command 'man' that is used to look up manual pages on your terminal screen (i.e., when somebody has misplaced your hardcopy manual).

(U) One shell file I have come to use regularly is called 'when' and tells me the last time someone has logged in. One of the first things I do when logging in is to ask 'who' is on the system. If someone I want to talk to is not logged in, my next question is whether they are around or away on leave or tdy.

(U) The shell looks like this:

```
:   Find out the last time a user logged in
:         wes 9/2/82
:
:                       Test for missing arg1
if "$1"x = x goto noarg
:
grep "^$1" /etc/passwd > tmp$$
ed - tmp$$
g/^.......*:./.*):$/s//ls -l 1/.llog/
w
q
sh tmp$$ | reform +m14 +t41 | rpl " 0 " "  "
rm tmp$$
exit
:                       Error message for no arg
: noarg
echo "User name not given"
echo "Usage: when username"
exit
```

(U) In its original form, the shell first checked the output of line of the 'who' output; if not, it went to look at the username's last login time. I found that too slow, and noticed that I tended to use 'who' first anyway, using 'when' only if the user was absent from the 'who' output. The 'reform' and 'rpl' were designed to format the output to match the 'who' format. If you like fast answers, you might just use 'sh tmp$$' without 'reform' or 'rpl' and leave out the test for a missing argument.

P.L. 86-36

(U) The following shell was written by [redacted] A205, and uses 'gath' in an interesting way to interactively collect data. The purpose of this shell is to send a file from one UNIX host to another.

(U) If all this looks strange, you will want to spend some time with the manual pages for 'gath' and 'send'. Enter your own terminal designator into lines 7 and 10 (where I have used ttyX). If you use more than one terminal, there are several ways of fixing the shell to accommodate this, perhaps by giving your current terminal as the first argument of the shell, or by executing 'who am i' and piping the result through reform to generate the wanted command line 'stty -echo > /dev/ttyX' in a temp file that would then be executed, etc.

(U) It really depends on what you like to do, and how slow you are willing to make the shell. I find that shells I use every day can be lean and clean, because daily use makes me remember what every option is. On the other hand, when I have a shell that is used only several times a month, it pays off for me to put in more bells and whistles, even at the expense of slowing it down. It isn't always easy to remember whether there are arguments needed and in what order, so I often test for that first, and use an error message that gives the correct format. That way, I can just give the command, and know that the error message will tell me how to use it properly.

(U) If you are interested in how slow or fast a shell runs (and you should be), get familiar with 'time' and use it on several versions of the same shell to find out which features cost the most in time and system.

```
gath >tmp$$
~-s
~:                Enter name of target computer
~=:?sys?
~:           Enter login name on target host
~=:?login?
~!stty -echo > /dev/ttyX
~:        Enter password for target login
~=:?passwd?
~!stty echo > /dev/ttyX
~:
~:
~:Enter the target file name,
~:    the name of the file on the target host
~=:?target-host-file?
~:
~:Enter the source file name,
~:         the name of the file on this system
~=:?source-host-file?
~:
~:If you are sending a file to target host
~:           enter an 's' otherwise enter an 'r'
~=:?direction?
if ?direction?x = sx goto SENDING
if ?direction?x = rx goto RECEIVING
: ERROR
echo Error: you did not enter an 'r' or 's'
echo            for direction of file transfer.
exit
: SENDING
cftp blocked suicide
*host ?sys?
log ?login?,?passwd?
rec fc '?target-host-file?'
*host *
sen fi '?source-host-file?'
*dou type i,s
*tra
*end
exit
: RECEIVING
cftp blocked suicide
*host ?sys?
log ?login?,?passwd?
sen fi '?target-host-file?'
*host *
rec fc '?source-host-file?'
*dou type i,s
*tra
*end
~:
~:No further input is required, wait for prompt
~.
sh tmp$$
rm -f tmp$$
exit
```

DOCID: 4009850

LINGUIST MACHINE (U)

P.L. 86-36

by [redacted]

G9

From time to time, one hears rumors of people who use the expression: "Run that by your linguist machine!" evoking a picture of a mindless army ~~(FOUO)~~ of translators mechanically plying their craft with a minimum of mental effort. If true, these rumors suggest that misconceptions exist about language work. This essay is intended to give those who are not linguists some idea of the things that a linguist encounters in his daily work. Although it is based on the experiences of a Japanese linguist and his perceptions of language translation, it is hoped that these observations may be of help in understanding the daily life of the translator of other languages as well.

~~(FOUO)~~ Sometimes linguists are told:

"Don't spend too much time on it; just translate it as it is--and get it out!"

Such guidance--while rightfully warning translators against including anything not in the original text--might suggest that translation is merely a matter of using a few dictionaries, remembering a few grammatical rules, and becoming accustomed to a foreign script or Chinese characters. However, language translation is not that cut and dried. Linguists face certain problems.

CULTURE AFFECTS LANGUAGE

~~(FOUO)~~ Differences between the cultures and decision-making processes of the U.S. and foreign countries can create a problem for translators. For example, if a Japanese official tells a U.S. official: "Goteian wo kentoochuu" (We are considering your proposal), the U.S. official may infer from that statement that a conclusion is likely to be forthcoming soon and that it could well be favorable. Actually, the decision could go either way and, whatever decision is ultimately reached, considerable time is likely to elapse. The delay in reaching important decisions in Japan stems from the decision-making process in Japan, which is based upon reaching a consensus among all parties involved, a process that can consume much time. Moreover, when a Japanese says "hai" (yes) to a proposal, he may mean only "yes, I will consider your proposal," since he hates to turn one down flatly. Or he may merely mean "I understand what you have said."

~~(FOUO)~~ Translators are forced to translate words and phrases that either have no equivalent in English or that have different meanings in English and other languages. For example, a Japanese writer will often begin with a deprecatory phrase like "kyooshuku desu ga..." that one might translate by such formulae as "By your leave, I would like to tell you the following," or "This might not be the place to mention this, but..." That kind of statement, which seems unnecessary to the English reader, appears to have an important social function in Japan, a relatively small nation that has traditionally found it necessary to preserve social harmony through convention.

~~(FOUO)~~ Perhaps it is because of this need to preserve social harmony that Japanese always appear to be apologizing. Japanese will often say "sumimasen" (I am sorry) when we would say, in an equivalent situation, "excuse me." Moreover, humility has traditionally been viewed as a quality of those possessing true learning and wisdom. A Japanese saying is "Minoru hodo atama ga sagaru inaho kana" ("The riper an ear of grain, the lower it bows its head"). Japanese, among others, do not like to make statements that will isolate themselves, a tendency made stronger by the group-orientation of Japanese society.

~~(FOUO)~~ One might cite many other examples of cultural differences that can make direct translation difficult--if not impossible. Translating the Japanese term "tatemae" is difficult for that reason. Americans and Europeans are taught to "practice what you preach," but in Japanese culture, there is apparently more open admission that, given human frailty, one's ideals or principles are not always practical or realizable. The Japanese have the word "tatemae" to express that idea, whereas we must do so indirectly by saying, "If I had my druthers, I'd..." or "That's the ideal, but..."

~~(FOUO)~~ Japanese appear to leave more to the imagination of their audience when speaking or writing, and often end sentences with statements that make their thought tentative, as in "I would like to go, but..." or "it could be perceived that way, but...." After the word "but" ("ga" in Japanese), the reader is left to fill in the sentence, as in "...but I might be wrong," or "but what do you think?" By being vague and tentative, the speaker in

DOCID: 4009850

Japanese society protects himself if he is wrong, does not suggest by his words that his listener or reader is ignorant--thereby embarrassing him--and, above all, demonstrates that he is not being "namaiki," i.e., that he is not running counter to the natural rules of social behavior within groups, or between superior and subordinate, by being excessively individualistic, selfish, or assertive. These ideas are difficult to render in direct translation.

~~(FOUO)~~ Differences in cultural outlook pose problems for translators in many languages. In Arabic, phrases like "In sha 'Allah" (literally meaning "God willing," but actually used to express the idea "I hope that ....") are used constantly. U.S. policy-makers tend to view the world through the eyes of American culture. What is difficult to express to U.S. policy-makers in translations is that unlike U.S. culture, which tends to reserve religion to one day a week, i.e., to the Sabbath, in Arab culture, religion (Islam: literally "submission") permeates everyday life which constantly reminds one in the Moslem world of the mutability of life and the limits of what any one person can hope to accomplish. In Arabic culture, the emphasis appears to be on "man proposes and God disposes" rather than on "God helps those who help themselves" as it seems to be in the U.S. Again, when translating Arabic, it is difficult to convey that dissent is often couched in religious terms. The same problem exists for the Russian translator. How can they make U.S. policy-makers aware that they should not dismiss statements of communist ideology as mere propaganda for public consumption?

~~(FOUO)~~ In Brazilian Portugese, there is the phrase "Nos le damos um jeitinho" (literally "We'll make a little allowance for you"). It is difficult to convey, in direct translation, the possibility that Brazilians do not necessarily share the American belief that "If I make an exception for you, I must make one for everyone." For that matter, how does one explain to foreigners our belief that "problems are opportunities in disguise" or that one should undertake "challenges," like going to the stars, merely because doing so is difficult, and that one "actualizes" oneself in the process?

~~(FOUO)~~ Unless translators have grown up in a foreign culture, or have access to native speakers or to persons with near-native fluency to explain things, translators may often miss part or all of the meaning of what they are translating. A Japanese hotel employee may say "Hai, wakarimashita" (Yes, I understood) to a request from a guest who wants to have his laundry done. What he means is that he will see to it that the laundry gets done. Similarly, two parties to an agreement may say that the agreement was "ryooshoo shimashita" (acknowledged), meaning that both sides went along with the agreement. Such terms apparently enable the speaker in Japanese society to save face and preserve dignity. Also, when a person in Japanese society offers someone something, he expects to have his offer politely refused before it is accepted.

~~(FOUO)~~ A classic case of different perceptions in different cultures concerns traffic signals: the Japanese refer to the dark green signal, and some foliage, as "aoi" ("blue"). That is because the Japanese divide the spectrum at a different point than do Europeans, so "aoi" has been incorrectly rendered as "blue" rather than "green."

~~(FOUO)~~ Japanese poetry, like the poetry of other countries, is particularly culture-sensitive. In her famous haiku poem, the Japanese authoress Kawa no Chiyo paints a picture with only 17 syllables:

「朝顔に
釣瓶取られて
貰い水」

"ASAGAO NI

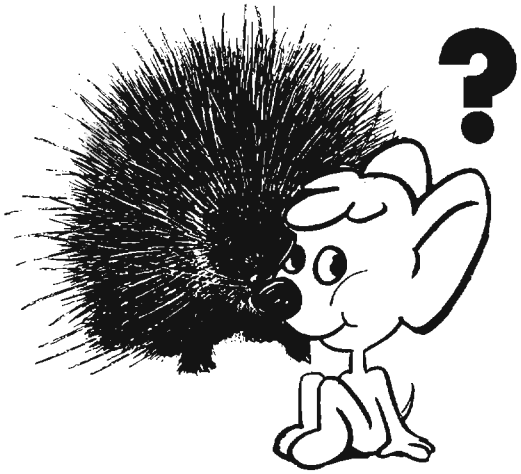
TSURUBE TORAETE

MORAEMIZU "

This poem may be translated as:

"When (I) found that the well bucket had been claimed by morning glories, (I could not bear to use it to draw water, so I was forced to) borrow water."

This poem, like the language in general, shows the Japanese predilection toward allowing one's imagination to fill in the unexpressed, as well as the great love of Japanese for beauty.



AND IF THAT'S NOT ENOUGH...

~~(FOUO)~~ Linguists might be told "Just do a 'quick and dirty' on it--get it out 'on the street' ASAP!" and be compelled by the nature of the material they are translating to rush out a translation. The problem is that they become caught between the need to speed the completion of the translation and the need to turn out a translation that is accurate and clearly understandable. The history of translation is replete with instances of mistranslations, the their consequences, arising from too hasty translation. A classic example of this took place at the start of World War II, when a translator rendered the Japanese decision to "mokusatsu suru" the U.S. peace proposal as to "dismiss it with contempt" instead of to "hold off on taking action." More recently, during his visit to the U.S. in May, 1981, Prime Minister Suzuki said that Japan's defense policy will be "harinezumishiki." A Japanese interpreter, apparently doing a "quick and dirty" translation, rendered the term as meaning "like a barbed mouse." What Suzuki's interpreter meant to say was that "Japan's defense policy will resemble a bristling porcupine." The confusion apparently arose from the Japanese word "nezumi" (rat), which is common to the Japanese words for mouse (hatsukanezumi) and porcupine (harinezumi). The net result of the mistranslation was to temporarily give perplexed and exasperated U.S. policy-makers the mistaken impression that Japan intended to renege on its security commitments. That is because "mouse" connotes timidity in American culture. The matter was cleared up shortly thereafter, when Prime Minister Suzuki spoke of a U.S.-Japanese "alliance." (Indeed, controversy within Japan over the meaning of the word "alliance" led to a change of foreign ministers.)

~~(FOUO)~~ In addition to being accurate, a translation or report must be easy to understand, and must contain no "double entendre," i.e., it must not be worded in such a way that two or more interpretations of a sentence are possible. Not long ago, the manager of a government translation "shop" that farms out material to be translated to contractors gave a talk on government language work. He said that as a result of the poor pay and resulting low standards for contract translators, the translations that they produced were so unreadable that some customers of their work became convinced that "foreigners cannot express themselves properly." The point is that if a translation is not crystal clear, it is not likely to be respected by the reader. It is particularly difficult to turn out easily readable translations from Japanese, a

DOCID: 4009850

language whose structure is very different from English. A Japanese sentence is often more equivalent to an English paragraph in length and completeness of thought. It can go on for pages, and must be broken down into shorter sentences in English.

~~(POUO)~~ In attempting to make translations readable, translators must determine how colloquially to render the translations and how to reflect the strength of the statements accurately. (Generally speaking, transcripts of conversations can be translated more colloquially than narrative portions of a text.) Take this sentence, for example, in Japanese: "Moo nihonjin ni hohoemikakeru jiki ga satta." This sentence can be translated more literally, and less forcefully, as: "The time for smiling at the Japanese is past," or it can be translated in a more colloquial and hard-hitting manner as: "It is time to stop being 'Mr. Nice Guy' with the Japanese." Colloquial translation can also be very helpful when a phrase cannot be translated directly. For example, take the phrase "sekai no aru no Saudei" as part of a sentence. A literal translation of this phrase, "Saudi Arabia, a country in the world" fails to convey its actual meaning. A colloquial translation can be employed toward that end: "Saudi Arabia is proud that it has found a 'place in the sun'."

KEEPING UP WITH THE LANGUAGE

One of the biggest problems is that dictionaries of foreign languages are often inadequate and, even with the help of native speakers or other linguists with near-native ability in the language being translated, translators are often forced to build a meaning for the words, phrases, and passages they encounter in translation. Take, for example, the following sentence in Japanese:

"Kokoro ga sutarete kite iru."

Kenkyusha's New Japanese-English Dictionary (the principal dictionary used by the Japanese linguist and the most complete one for use in translating modern Japanese) gives quite a few definitions for the word "Kokoro," among which are "heart," "mind," "feeling," "sincerity," "interest," "care," "will," and "intention." None of these definitions quite fits the meaning of the word "kokoro" in the sentence. Translators must look at the examples given in the dictionary to obtain a "feeling" for how the word is used in a sentence and must also see how the word is used in the context of his text. In this sentence, "kokoro" is the immediate subject of the sentence, the particle "ga" marks the subject, "sutareru" is the verb meaning "to decline," and "kite iru" indicates that the sentence is in the present perfect. From the dictionary examples used to show the meaning of "sutareru," it is apparent that the kind of "decline" denoted by the Japanese verb is a moral decline. From the context of a sentence or passage, it is possible to derive the meaning of "kokoru" as "concern for others" and, as a result, to ascribe a meaning to the sentence as a whole as "People have become less public-spirited" or "People are now more concerned only with their own welfare." (Note that a subject, "people," had to be added to make the sentence grammatical in English. It is quite common for Japanese to omit the subject. That is because Japanese writers or speakers will not repeat the subject of a sentence if they believes that it is apparent to their audience. Translators or interpreters must constantly try to determine what the subject is and supply it in the translation.)

Since foreign countries obtain many of their technical terms from English, one might expect that technical terms would cause few problems, but that is not always true. Some countries prefer to coin native equivalents of foreign technical terms out of pride in their

DOCID: 4009850

languages and cultures, and to facilitate understanding of the terms involved. The coining of such neologisms poses a problem for translators, because dictionaries fail to keep pace with them, while translation tends to take place on the frontier of knowledge, including current events and scientific discovery. To add to the problem, the translator often cannot do an effective job of translation without some understanding of that technical subject matter.

The job of translators is first to figure out what words or phrases mean in the original language being translated, and then, if necessary, to ascribe a meaning that fits the context. Foreign loan words provide a good example of this. English loan words in Japanese can take on quite specific meanings with no English counterparts, or they may have no counterparts in English whatsoever. For example, in Japanese "ootobai" (autobike) means a large-size motorcycle, "mopedo" (moped) a medium-size motorcycle, and "mootaabaiku" (motorbike) a bicycle with an engine powering it. English loan words in Japanese may also be borrowed from British English with their American English counterparts taking on different or more specific meanings. For example, "bisuketto" (biscuit) is the British English word for "cookie," and "kukkii" (cookie) is apparently used more to refer to cookies made at home, while "bisuketto" apparently refers to store-bought cookies.

Translators must take into account that British and American English expressions can have diametrically opposite meanings. For example, to "table" a matter means to place it on the agenda in British English, as well as in diplomatic terms, but means to pigeonhole it in American English. "Abekku," from the French "avec" ("with"), has the very specific and different meaning of Japanese of "a couple on a date." Thus, translators must also determine the meaning of loan words borrowed into a foreign language from other foreign languages.

Linguists often must know a little about the phonetics of foreign languages before he can find, or artificially reconstruct, personal or place names written in Japanese phonetics. For example, they must know that "hi" in Japanese phonetics is equivalent to the "ach" sound in German. Translators must realize that the "ga" in Japanese can be pronounced "nga," before they can look for, say, an Indonesian place name starting with "Ng."

Sometimes the translator must know the origin or "locus classicus" of a word or phrase before they can translate it, or translate it well. For example, the Kenkyusha dictionary translates the adjective "naniwabushitekina" as "of the old feeling of Naniwabushi" and does not elaborate. The literal meaning of the term is "like a tune from Osaka," but knowing that does not explain how it is used metaphorically. In order to understand that, and therefore to be able to translate the expression, one must know that a "naniwabushi" is sung with great emotion and fanfare. One may then translate the expression as, in colloquial parlance, "to make a big production" about something, or to play something up unnecessarily. To give another illustration, most Japanese--but very few Americans--are familiar with the expression "Columbus' egg" ("koronbasu no tamago" in Japanese). As in the American English expression "I chopped down the cherry tree," one must be familiar with the story behind the expression in order to fully understand the meaning. As the story goes, Columbus asked his shipmates to see whether they could stand an egg on its end. When he saw that they could not do so, Columbus merely bashed in the end of the egg on a table and caused it to stand that way. Once one has heard this story, one can translate the expression as meaning "deceptively simple."

Conclusions

There is much more to translation than using dictionaries, learning the rules of grammar, and becoming conversant with the intricacies of alien scripts. The translator must try to wrest the meaning of words, terms, phrases, and whole passages by referring to examples in dictionaries, conferring with native speakers or near-native speakers of the language being translated, by acquiring knowledge of technical, political, economic, and other developments through education and experience, and by using his imagination and creativity. He must then rewrite the meaning in English since it usually cannot be translated directly.

Because many years and great efforts are required for one to become a good linguist and interpreter between different worlds, and because that task is so important, every effort should be made to provide linguists with the material and non-material incentives to encourage them to remain in this career field.

DOCID: 4009850

An Old Problem (U)

by WES

(U) Answer next month.

EO 1.4.(c)
P.L. 86-36

DOCID: 4009850

All I ever wanted to know about DES (U)

by [redacted] C11

P.L. 86-36

We are rapidly moving into the "information society" (if indeed we are not already there). All the information in this "information society" to which I refer has value to at least two people (the sender and the receiver), and most of it has value to a few, perhaps many, other parties as well. There certainly is a need to protect most information from falling into the wrong hands. I am referring here to all types of information, both classified and unclassified, military and commercial, etc.

This need to protect information is especially acute at the most vulnerable point--when information is transferred via some communications medium from one place to another. It was to aid in filling this need to protect unclassified information that the National Bureau of Standards (NBS) placed a call in 1973 to all interested parties to submit suggestions for an encryption algorithm that could be used as a National Standard for Data Encryption. Only one algorithm was submitted that was judged to be adequate for U.S. Government use in protecting unclassified information. This algorithm, submitted by the International Business Machines (IBM) Corporation, was reviewed, accepted, and published by NBS in 1977 as Federal Information Information Processing Standards Publication 46 (FIPS PUB 46). This standard describes a mathematical algorithm for transforming 64 bits of data, using a 64 bit key (56 independent bits, and 8 bits parity) into a 64 bit output. This algorithm is the Data Encryption Standard (DES). The NBS followed FIPS PUB 46 with another standard describing several modes of encryption that could be used with the algorithm. This new standard, FIPS PUB 81, described how the DES algorithm could be used in a communications system in both the block and stream cipher modes [1].

In 1976, the Federal Reserve System wanted to purchase a data communications system for use in banking and Electronic Funds Transfer. They requested that NSA help them in the area of cryptographic protection. Out of this effort came the beginning of two standards for using the DES algorithm in unclassified U.S. Government cryptographic applications.

- The first of these two standards, Federal Standard (FS) 1027, prescribes general physical and electrical measures to insure that neither the key variable nor the plaintext data is compromised. This standard is a security-related document.
- The second standard, FS 1026, prescribes only electrical measures to insure both:
  - Interoperability of equipments from different manufacturers, and
  - Security.

These standards have gone through a lengthy process of review and comment (as do all standards generated in a public forum). FS 1027, on general security, has been approved; FS 1026, on interoperability and security, is near final approval.

The balance of this article is devoted to an explanation of the objectives of these standards and how they are written to achieve these objectives. FS 1027 is described first since it is a general standard applying to all DES cryptographic components, equipments, systems, and services that the U.S. Government procures.

FEDERAL STANDARD 1027

FS 1027 prescribes general security requirements for equipment that uses the Data Encryption Standard (DES) algorithm for enciphering data. The word "general" perhaps best describes the standard in that it specifies only general physical and electrical parameters that must be met by any equipment (voice, data, facsimile, etc.) that uses the DES in a telecommunications environment. The scope of the standard can be best described by examining the security objectives of the standard:

- To prevent inadvertent transmission of plain text.
- To prevent theft, unauthorized use, or unauthorized modifications of cryptographic equipment while installed.
- To prevent unauthorized disclosure or modification of key variables while in DES cryptographic equipment.
- To provide interoperability between key variable loaders and DES Cryptographic equipment, and to permit the use of standardized keying material for U.S. Government applications of the DES algorithm.
- To prevent data encryption when a critical cryptographic failure condition exists, and to generate an alarm when a critical cryptographic failure is detected.

These objectives are met in the following ways.

Physical Security

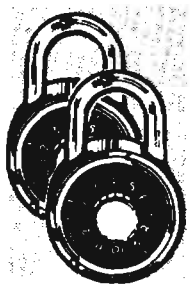
The standard requires that the Data Encryption Equipment (DEE) have enough physical integrity to insure that any unauthorized access to the equipment (either to remove it or to tamper with it) will leave signs that can be easily detected by visual inspection only (e.g., bending of the front panel, drilling of holes, etc.). Two different physical keys are required to insure that secure mounting, tamper resistance, and key variable protection are provided for.

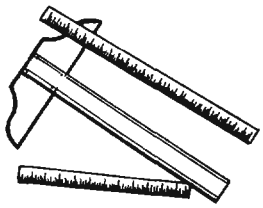
Key Variables

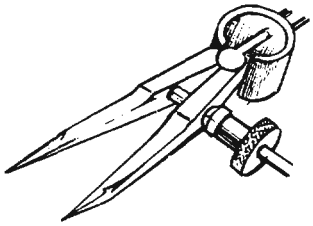
The standard provides for the protection of DES key variables both as they are entered into the DEE (two methods provided) and as they are used internally within the equipment. Key variables can be entered either via a self-contained manual input device (e.g., a hexadecimal key pad) or through a standardized electrical interface to a key variable loader (e.g., a KOI-18, which is a general purpose key variable entry device). After the DES key variables are entered into the encryption device, the standard requires that it must not be possible for the key to be compromised in either of two ways:

- by being read back out of the DEE, or
- by external access as a result of any single failure.

To further insure protection of the key variables, any detected tampering (e.g., unauthorized physical access) shall automatically zeroize (erase) the key variable.







Initialization Vectors (IV'S)

The standard requires that IV's that are used

- be generated by the DES process or some other random means,
- that they be either 48 bits (Cipher Feedback) or 64 bits (Output Feedback or Cipher Block Chaining) long, and
- that they are used to initialize each new cipher text chain.

Encryption Functions and Alarms

Extensive automatic "self tests" are required by the standard to insure that the DEE does not fail in some undetected manner and transmit either plain text or (worse yet) raw key. To this end, the encryption self testing must be done by either:

- having two complete DES encryption devices that are continuously compared as a self check, or
- frequently encrypting test words and checking the results.

Fail Safe Design Requirements

The standard requires that, to insure the security of the plain text and key, the unit shall be designed in such a way that any single failure will not allow either transmission of the key variables or transmission in depth (use of the same IV).

Test Mode

As an additional safeguard, an externally (e.g., manually) initiated test mode is required. This mode is analogous to a self test, and that can provide assurance of that the equipment is operating properly.

Control Functions

A standardized set of DEE control functions is required (e.g., Power ON-OFF, Reset, and Mode). This requirement assures that DEE operators will have the requisite standardized control functions necessary for total system security.

Status Indicators

Visual status indicators for the control functions (above) are provided by the standard.

Retention of Critical Storage

It is important that proper encryption parameters (e.g., key variables, IV's) be used at all times, even after power interruptions. To insure this, the standard requires that the DEE shall be able both to retain these parameters during power interruptions, and also to test that the correct parameters have been retained.

Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC)

To insure that there are no compromising RF or power line emanations that would invalidate

DOCID: 4009850

the protection provided by the rest of the standard, the DEE is required to have a specified degree of EMI and EMC protection.

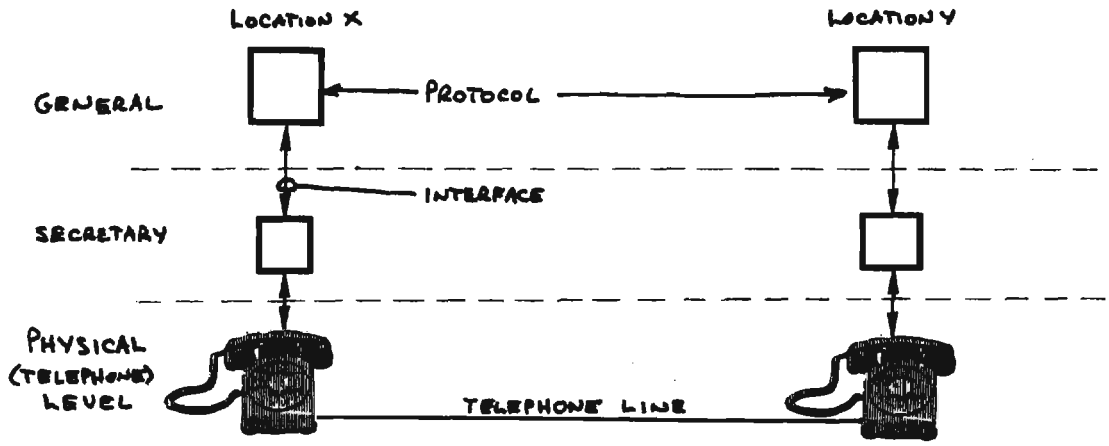
PROPOSED FEDERAL STANDARD 1026

PFS 1026 describes the application of the DES algorithm to data communications for ADP systems and for narrative text information systems. This standard refers to the International Standards Organization (ISO) Open Systems Interconnection (OSI) model for data communications at the Physical and Data Link Layers. At some future time, there may be a whole list of standards that describe encryption at a range of OSI levels, from the simplest at the Physical Layer (Level 1), which is sometimes called the "RS232" level, to the most complex Level 7, which is called the "Applications" Layer. Before we describe the Proposed Federal Encryption Standard, an explanation of the layered structure in data communications is in order.

The OSI architectural model of data communications was developed by the ISO as a conceptual framework within which data communications equipment can be designed and built to be interoperable. This conceptual framework encompasses a wide variety of communications procedures (called protocols), that range from the most simple and specific to the most complex and general. This wide range has been divided into subdivisions called Levels. The simplest level, called Level 1, is the Physical Level, or Layer, and is commonly exemplified by the familiar RS232 interface seen on most printers, data terminals, modems, etc. The most complicated level, called Level 7, is the Applications Level, or Layer. The other levels are:

- L2, Data Link,
- L3, Network,
- L4, Transport Layer;
- L5, Session; and,
- L6, Presentation.

As an illustration, suppose that General X wants to speak on the telephone with General Y (see Figure 1). Perhaps he would tell his secretary to get General Y on the telephone and to call him (General X) when the telephone connection is established (a General only talks to other Generals and to his immediate secretary). General X's secretary goes to her telephone and places a call to General Y's office. General Y's secretary gets General Y on the telephone and then relays to General X's office that all is ready for the conversation. General X's secretary receives this information, gets General X on the telephone, and the call can then be completed. This simple example illustrates the layered concept of communications: there is a "General" layer, a "Secretary" layer, and a "Physical Telephone" layer. Within these layers, there is a General-to-General communications protocol and a General-to-his-Secretary communications interface. There is a similar set of protocols and interfaces at the Secretary and Telephone layers. The OSI layered structure is similar to this, with the (Physical) Telephone layer being analogous to the Physical Layer.



GENERAL X TALKS TO GENERAL Y

FIGURE 1.

PFS 1026 describes the application of the DES algorithm to data communications at both the Physical and Data Link Layers. The standard describes on-line (not off-line) encryption; i.e., encryption that occurs simultaneous with the communications process itself.

There is a two-fold objective for the standard:

- to permit interoperability, and
- to provide acceptable security for government data communications facilities, with protection against
  - a "passive" security threat, where the interceptor merely reads the communications traffic but does not divert, modify, jam, or in any way change the traffic; or
  - an "active" security threat, where the interceptor not only does the interception, but also modifies the traffic in some way, i.e., inserts, deletes, modifies, or repeats the traffic.

The proposed standard provides a method of encryption that, with one exception, can achieve all the above objectives. The one exception is encryption at the Physical Level (Level 1), where it is possible to provide only passive security threat protection, due to technical parameter limitations of the physical communications process. The proposed standard also provides a method of electronically distributing DES key variables with the same degree of protection provided to other data.

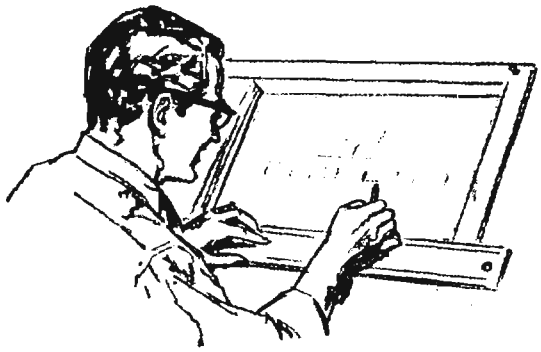
It should be pointed out that encryption at the Physical Level can be done completely independent of any data communications protocol that may be used. Encryption at any other level (e.g., Data Link, Network, or higher), must be implemented in conjunction with, and fully compatible to, whatever communications protocol is used at the layer where encryption takes place. The advantage of encryption at the Physical Level is that the implementation is very simple and, hence, inexpensive. The disadvantage is that the traffic must be decrypted at each intermediate switching center through which it is routed. Hence, at each intermediate node of a network, the traffic must be protected; i.e., it becomes "red" data. The advantage, then, of encryption at higher levels of the OSI architecture is that the higher the level of encryption, the fewer security restrictions there are at intermediate switching nodes. For example, if encryption is done at the network level, then the "black" (encrypted) data resulting from the encryption process can be passed safely through any network that does routing at either the Link or Network level. Examples of this type of network are ARPANET and TELENET.

Conclusion

In this short article, I have attempted to provide a brief overview of the DES Federal Standards that have been and are being widely distributed throughout both the Government and private industry. The overall objective of this is to provide minimum security and interoperability standards to which the commercial manufacturers can provide equipments in a competitive market place. Early indications are that these objectives are being met, since commercial DES cryptographic equipments are beginning to appear, and are being used by both private industry (banks) and the U.S. Government.

---

1. The two block modes are the Electronic Code Book Mode (ECM) and the Cipher Block Chaining Mode (CBC). The two Stream modes are the Cipher Feedback Mode (CFB) and the Output Feedback Mode (OFB).



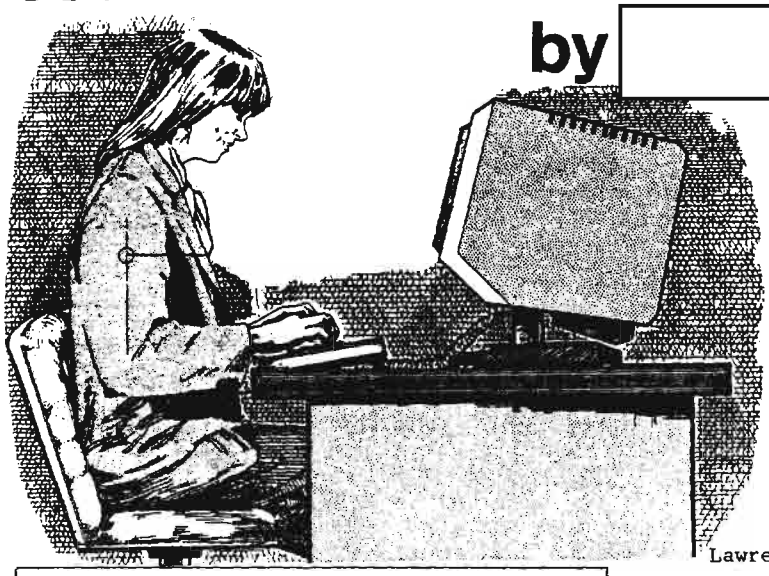
DOCID: 4009850

~~FOR OFFICIAL USE ONLY~~

Human Factors Corner

by [redacted]

P.L. 86-36



SYMPOSIUM ON VIDEO DISPLAY TERMINALS AND VISION OF WORKERS, National Academy of Sciences, 20-21 August, 1981
(reprint from Human Factors Letter #2-81)

I attended this meeting, along with two other members of Human Factors SIG (Don Landry and Don Friedmann). There were very few printed handouts, and no proceedings were issued at the symposium itself, though some form of printed report may be published later. The following paragraphs contain a summary of my impressions, and some comments on important questions raised in my mind by what I saw and heard.

The Symposium was composed primarily of panel discussions, preceded by one or two introductory or overview presentations. The program was as follows:

I. Introduction and Overview (Edward Rinalducci, Marvin Dainoff)

II. Methodological Issues in Field Surveys of Video Display Terminal (VDT) Operators. (Robert Guion, Steven Sauter, Dainoff, Olov Ostberg, Hugh Taylor)

III. What Visual Problems Have Been Associated With Video Viewing? (Leonard Matin, Lawrence Stark, Ostberg, Leif Hedman and an extensive panel)

IV. Optical Contributions to Visual Discomfort and Visual Performance With VDTs (Harry Snyder, Vincent King, Etienne Grandjean, and a panel)

V. Radiation Exposure (David Sliney, William Murray, panel)

VI. Opthalmic Pathology--An Epidemiological Perspective (Alfred Sommer, Arthur Frank, Lawrence Stark, William Halperin, Hugh Taylor)

VII. Job Design and Organizational Aspects (Robert Guion, panel)

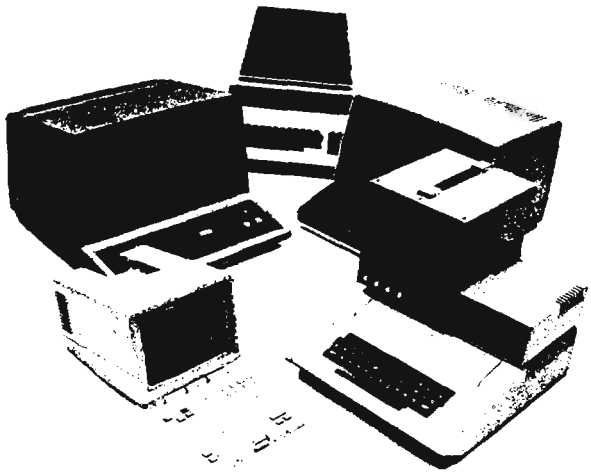
VIII. What Measures Might Alleviate Operator Discomfort Associated With Video Viewing and Improve Performance? (Harry Snyder, K.H.E. Kroemer, Martin Helander, panels)

A. Display, Lighting, Workplace, and Job Design

B. European Guidelines and Other Approaches

IX. What Research is Needed? (Rinalducci, panel)

~~FOR OFFICIAL USE ONLY~~



The weight of opinion seems definitely to favor the safety of CRTs, at least as far as acute, immediate health effects or damage to vision are concerned. Most experts seem to agree that there are no discernible acute effects of radiation. There may be temporary changes in vision after several hours of unbroken CRT work, but these disappear entirely after a few minutes away from the scope. Similarly, temporary aches and pains may arise from sitting in a cramped and unnatural posture for long hours at a terminal; these, too, vanish after a break or change of position, or even a change from one piece of work to another. In fact, the ordinary fluorescent lights used in most offices give off far more potentially-harmful radiation, and may have more impact on vision as well, than any CRT. Chemicals used in widely-available copy papers, and airborne particles of dust from carpeting, wallboard, drapes, and office furnishings may account for far more health hazard than anything related to CRTs.

Despite these reassuring words on acute effects, some major questions remain. All the experts admit that few studies have been made on longer-term effects of radiation on health or fertility. Little or nothing is known about long-term effects of daily CRT use on vision, mental health, or muscular and skeletal health. Some forms of radiation which CRTs might emit, and which might be harmful, are as yet unmeasured in the field because no instruments are yet available to measure them under field conditions. A final, and in my opinion highly important class of potential problems remains still to be addressed by empirical studies: the complex area of job design, automation and regimentation of office work, and changes in the way a worker thinks of himself or (more likely) herself and the job. Since I find this last area most interesting, I will focus my comments on the findings of the panel on "Job Design and Organizational Aspects", chaired by Robert Guion, Department of Psychology, Bowling Green State University, Ohio.

This panel was the only one which included any women, or any real representation from office workers or VDT operators as such. The other panels were made up almost exclusively of professors and researchers, and were entirely male. Panel members were the following: Janet Bertinuson (Consultant, Occupational Health); Richard Granda (Design Center/Human Factors, IBM); Etienne Grandjean (Swiss Federal Institute of Technology); Judith Gregory (Working Women Educational Fund); Steven Sauter (Dept. of Preventive Medicine, Univ. of Wisconsin); and Lambert Stammerjohn (Motivation and Stress Research Section, NIOSH). I noted that there were a considerable number of women in the audience throughout the Symposium; many of these were supervisors of office workers or human factors professionals interested in problems of VDT operators. In discussions at breaks, etc., I overheard a number of complaints from women attendees that many speakers were "naive", didn't know "what was going on in the real world", and were out of touch with the viewpoint of the office worker and manager of VDT operators in a real-world setting. Ms. Bertinuson and Ms. Gregory succeeded in counteracting some of this "ivory tower" atmosphere for the Job Design panel, in my opinion. I will summarize the panel discussion for several major questions:

- How do task characteristics vary in different types of VDT work?

  Ms. Bertinuson provided an excellent overview of this topic. She distinguished five major categories of VDT work, depending on such things as eye-movement, decision-making, use of keyboard and screen, etc. I believe these categories might usefully be applied to VDT work in the Agency also. Arranged on a scale of increasing variety and decision-making, the categories are:

  - Data Entry. The eyes are focussed on a source document much of the time. There is a high rate of keystrokes per

OCID: 4009850

minute and hour. Work is routinized and repetitive. Speed, accuracy are strictly monitored. There is little opportunity for control by the worker over pace or work content; the jobs are "dead-end" and offer few intrinsic rewards. Many jobs are short-term or temporary, involve concern about job security.

- Data Acquisition. The eyes are focussed on the screen much of the time. Information is retrieved by small bursts of keying, viewed on screen, perhaps with a certain amount of data entry as well. Work is more interactive and "screen-intensive". There is somewhat more variety, less rigid routine.

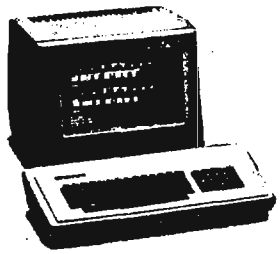
- Interactive VDT Use. Also screen-intensive, but with still more variety, decision-making. There is eye movement between the keyboard and screen when the operator is first learning the task, more focussing on the screen alone after experience. These jobs can vary greatly depending on how management views and structures them for the operators. For example, in a travel reservations application, operators interacting with customers have more freedom than people in a "back room" who are driven by a computer which schedules and allocates their work. A big problem for operators in these interactive jobs is the wait time for system responses on the screen; management thinks this is a "rest" for the operator, whereas in reality it is a constant stressor, which feels to the operator like "hitting a wall" over and over again. Another major problem is the highly symbolic nature of the content, with predesigned formats and codes which may have little meaning for the operator, and management's attitude that operators should work mindlessly: "Don't think about it--just do it; thinking will slow up your work too much!"

- Word Processing. This includes a wide range of decision-making and control by the operator over how the job is done, and how the system is used. At best, the operator can format, compose, edit, decide when to make a hard copy, when to edit on the screen, etc. Again, a lot depends on how management has structured the job, and what restrictions are placed on the worker.

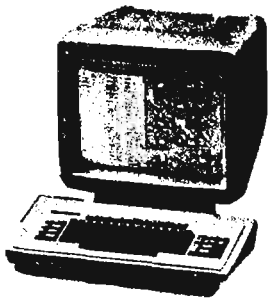
- Creative, Free use of VDT as a Tool. Programmers and systems designers who develop systems, procedures, and formats; scientists and engineers and other researchers; creative writers, executive secretaries and office managers, graphic designers--these are the "crème de la crème" of VDT users. They are the people who say "I love MY terminal--I wish it was really mine, to take home with me at night!" They are free to use the terminal and the entire complex of computing power behind it as their own creative tools at their own pace.

● In What Ways Has the Introduction of VDTs Restructured Jobs?

Dr. Sauter asserted that there are indeed sources of stress which are unique to VDT jobs when they are badly designed. Primary among these is a different pattern of temporal constraints, a more rigorous pacing of work, especially for data entry jobs, but also in potentially freer kinds of jobs when they are restrictively and harshly constrained by management. He said that the time pacing stress in VDT jobs is worse than that in the actual industrial assembly-line. The worker on an assembly line can usually "work ahead" and give himself a break or change of pace, whereas the computer is always "ahead of" the VDT worker no matter how fast she works. Another unique feature of the VDT job is the apparent "smartness", omniscience, control of the system over the worker, and its capacity to monitor her actions. Dr. Sauter listed the following stressors which were found to be specific to VDT operators when they were compared to workers in similar jobs but



DOCID: 4009850



not using VDTs: loss of control over pacing of work; fewer rest breaks; more pressure of work; lessening of co-worker interaction; loss of interest in the work; less variety in the work. This was true even in the case of a data entry job, where a former keypunch operator complained that now she could no longer punch her own control cards, or exercise what little control she had before over formats.

Ms. Gregory provided some vivid illustrative examples of actual cases where health complaints were involved, to hammer home some of these points about the way job design factors can change the way basically similar VDT jobs impact on the workers. For example, in one law office, a high-level word-processing specialist at one extreme was able to choose for herself when to make a hard copy, edit this in pencil, then make the changes via the terminal, thereby limiting and controlling the time she was required to view the screen. On the other hand, lower-level word-processors doing the exact same job in a secretarial pool were not permitted by management to make a hard copy, but were forced to edit directly via the CRT at all times, so that they had no control over the amount of time spent viewing the screen, or how they did the job (on the pretext of "saving time" and "increased efficiency"). In an insurance office, claims examiners were kept on mandatory overtime for ten-hour days over periods of up to 8 weeks; they reported severe health complaints! Customer-service representatives at VDTs in a telephone office were paced by an automatic call-distribution system that allowed them only a set time for each call. In a publishing firm, CRT typists were monitored; their keystroke rates were publically posted for each week, and they were paid on a floating scale proportional to the posted rate! VDT operators in a travel office were allowed a ten-minute rest break after 2 hours, but if they had a customer call at that time, were forced to forego their break entirely and work 4 hours straight until lunch or quitting time. These are some examples, randomly chosen from all too many similar cases in the real world, of the ways mean-minded and short-sighted management uses VDT's and automation as ways of regimenting office workers into an assembly-line. It was pointed out that 90% of female clerical workers are not unionized.

● What Should Be Done to Improve VDT Job Design?

Ms. Gregory offered a number of good recommendations. She began by asserting that the new technology offers us an opportunity for good design, not just an unimaginative "electronic equivalent of the old job at a speeded-up pace". More, not fewer, skills should be built into jobs. The operators should be afforded more, not less, control over work pace. More on-the-job training should be made available to all employees to allow for advancement, instead of the present trend toward a small elite of flexible jobs at the top and a vast increase in the number of routinized, dead-end jobs at the bottom. Increased pay and lowered working hours should be offered to workers as a consequence of the increase in productivity and lower error rate made possible by VDTs. We need to reverse the present trend in the US toward using VDTs as an excuse to turn more and more tasks into rigid, routinized "data entry" type jobs. We should follow the initiative of Europe in allowing more work breaks, requiring a broader mix of tasks, and regulating the amount of time spent at a screen. Richard Pew made some imaginative suggestions from the audience during the discussion: make data entry itself more interactive, by providing good error messages and prompts to let the operator find and correct errors; provide individual performance feedback to the operator herself from keystroke monitoring, so that she may better her own performance, while only global statistics are provided to management; put tools for work-scheduling into the hands of the operator, so that she may use the computer as an aid in planning her own tasks over a day or week.

DOCID: 4009850

I Remember... (U)

by [redacted] T5

MILLION DOLLAR 'PLUG'

(U) As part of my job as book buyer for the Agency during the 1960s, I often visited a bookstore off Wisconsin Avenue in Georgetown, down from Massachusetts Avenue, also known as Embassy Row. The manager surprised me one day by saying that the fire hydrant in front of his store was worth a million dollars to him. Although I knew that his stock was large and that his store had spread out over several houses in a row, I could not believe he was saving that much on insurance, so I asked him what he meant.

(U) The manager explained that because the parking space in Georgetown is so limited, the diplomats could always find a place to park directly in front of his store by blithely ignoring the fire hydrant. Thus he estimated that the plug was worth a million dollars in increased business.

EXPRESS SERVICE

(U) During the 1960s, Library Acquisitions had a pool of LIC (Limited Interim Cleared) people that could be drawn upon for help. Once I had a top priority request from the Front Office for a newly published book, and there was no staff car available. I asked for a volunteer to ride the shuttle bus to the Pentagon, make a mad dash to the bookstore there, and return with the requested book on the returning shuttle bus. A young man made the trip. He was thrilled with the excitement of the trip to the Pentagon, but I often wonder if he still remembers what book he brought back. I don't.

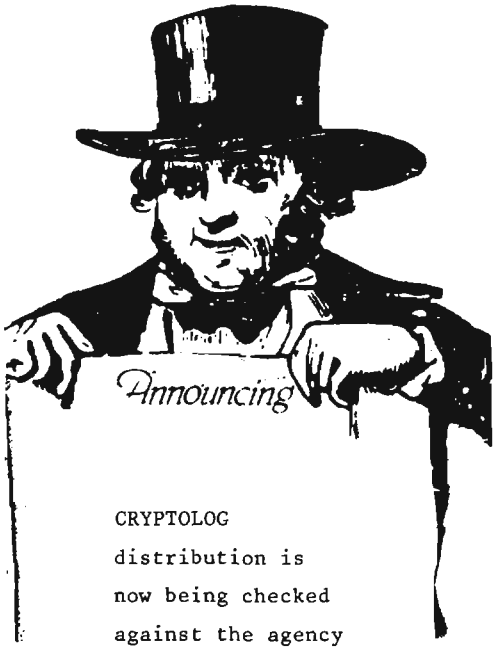
N.S.A. Means?

(U) Those employees who came to work before September 1960 were always cautioned to remember that N.S.A. stood for "never say anything." After the defection of Bernon F. Mitchell and William H. Martin, the Washington wits whispered that N.S.A. stood for "not secret anymore."

Solution to last month's NSA-CROSTIC

"Swahili [Dictionary]," [redacted] from an article entitled "Language in the News," CRYPTOLOG, September 1974

"Kajiga Balibutu, a priest from...Zaire... recently completed and published a 700-page Swahili dictionary. Unfortunately, the report from Azap (the Zairese news agency) didn't [mention] whether the volume was a bilingual dictionary or was entirely in Swahili, but our guess is that it is the latter."



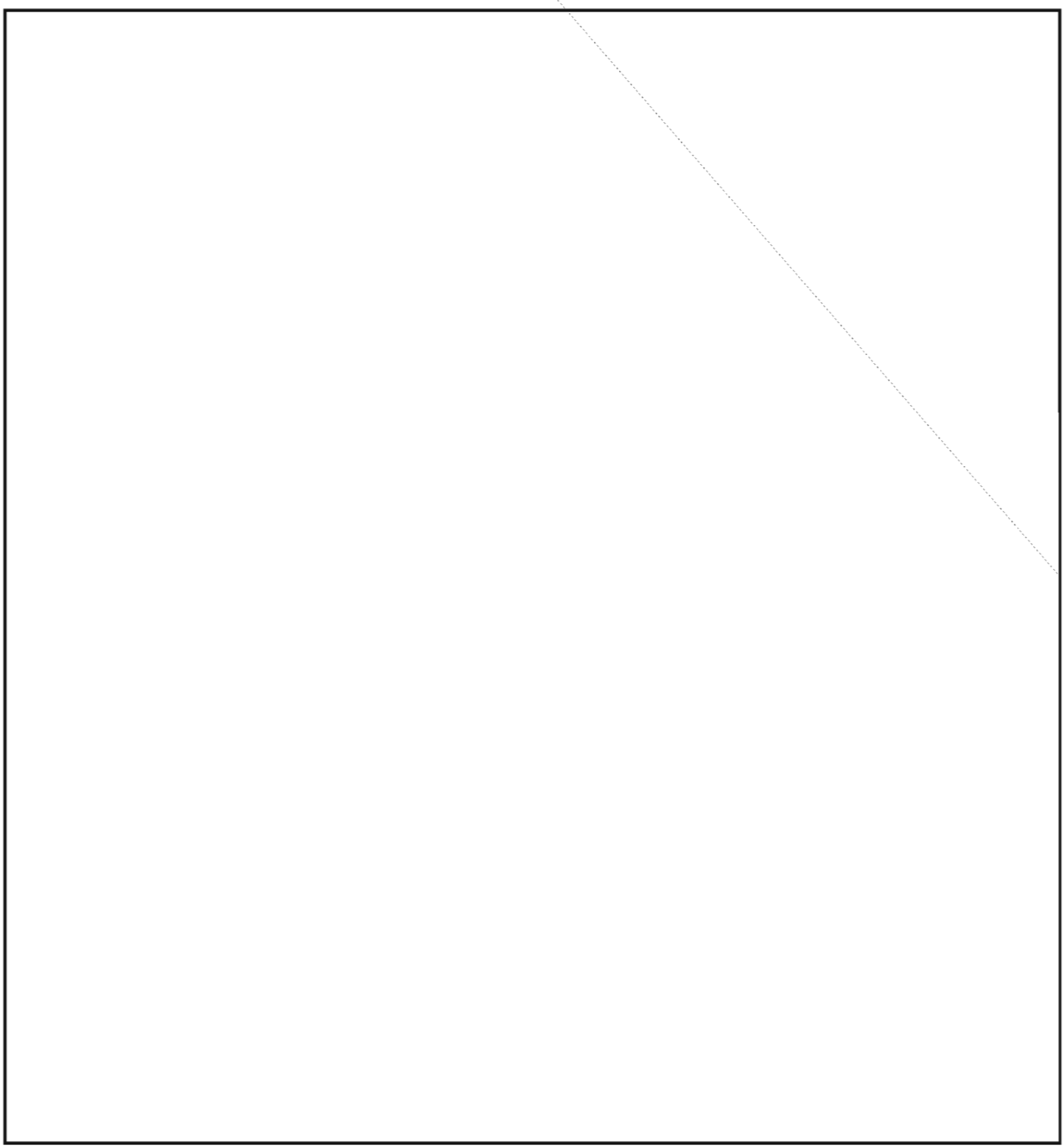
CRYPTOLOG distribution is now being checked against the agency locator file. If you move and don't change your locator information, you may lose your subscription to CRYPTOLOG.

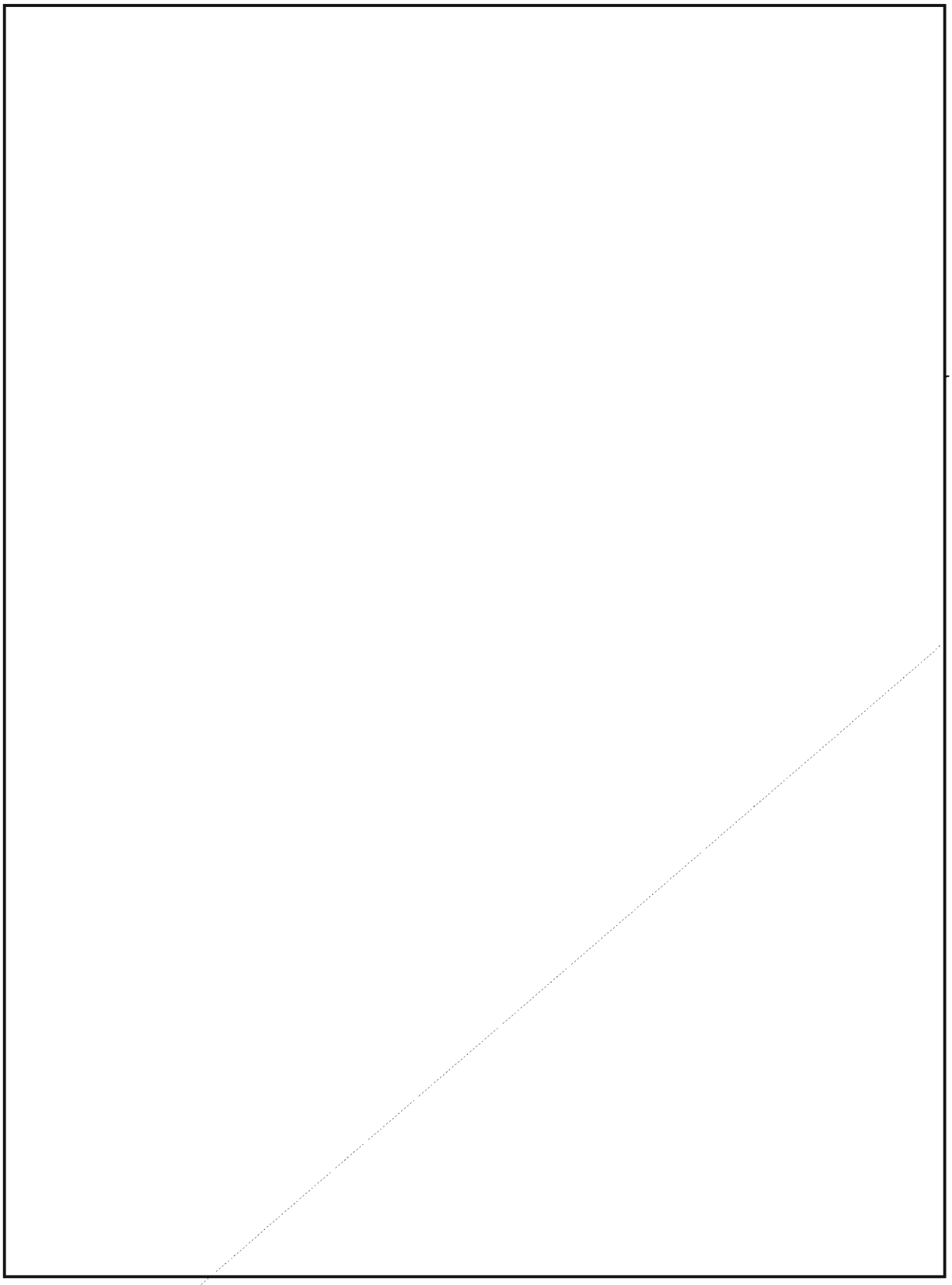
DOCID: 4009850

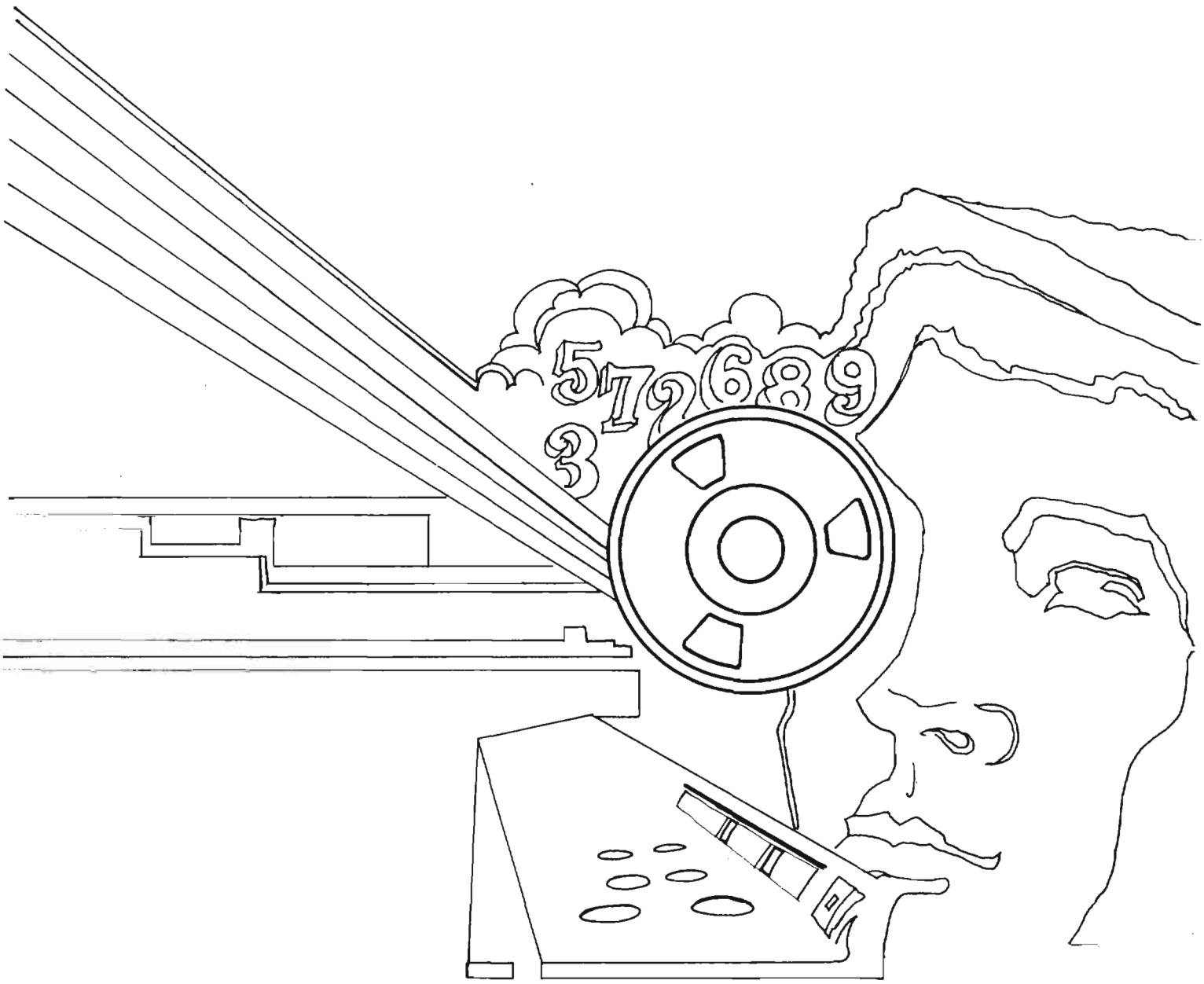
P.L. 86-36

★24 .oN CITSORC-ASN

This one has a few super-easy definitions for the benefit of those who complain that these puzzles are too hard. After all, you can hardly go wrong with Shakespeare or Eisenhower, can you?







~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~NOT RELEASABLE TO CONTRACTORS~~

DOCID: 4009849

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JUNE-JULY 1982

P.L. 86-36

P.L. 86-36

WHO WANTS A PROMOTION, ANYWAY? (U)..... [redacted] 1
AMATEUR SPREAD SPECTRUM (U)..... [redacted] 6
REPORTING MESSAGE VOLUMES (U)..... [redacted] 10
A PERSONAL FOOTNOTE (U)..... [redacted] 17
NSA-CROSTIC NO. 41 (U).....David H. Williams.....18
RESPONSIBLE DOCUMENTATION (U)..... [redacted] 20
SOME REFLECTIONS ON THE.....
REALITY OF COMPUTER SECURITY (U).....Robert J. Hanyok.....23
ODDS AND ENDS (U).....25
MAILBOX (U).....26
A LOOOONG SHELL (U)..... [redacted] 27

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 10 Jul 2012~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009849

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. IX, No. 6-7 JUNE-JULY 1982

PUBLISHER [redacted]

BOARD OF EDITORS

Editor-in-Chief. [redacted] (8322/7119s)
Production..... [redacted] (3369s)

Collection..... [redacted] (8555s)
Cryptanalysis..... [redacted] (5311s)
Cryptolinguistics..... [redacted] (1103s)
Information Science. [redacted] (5711s)
Language..... [redacted] (8161s)
Machine Support. [redacted] (5084s)
Mathematics..... [redacted] (8518s)
Puzzles.....David H. Williams (1103s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Don Taurone (3573s)

For subscriptions
send name and organization

to: CRYPTOLOG, P1
or call [redacted] 3369s

To submit articles or letters
via PLATFORM mail, send to

cryptolg at barlcØ5
(note: no '0' in 'log')

P.L. 86-36

Editorial

~~(FOUO)~~ The other day, one of our regular contributors got us all laughing about an idea he had: put advertising into CRYPTOLOG. Lots of contractors, he said, would be willing to pay for advertising space in a technical magazine that went to almost all of what we call the "technical underside" of the Agency (apologies to Churchill). He thought we could make enough to pay for the publication costs and maybe my salary too.

~~(FOUO)~~ After a while, the enormity of the possibilities began to come to our minds. When you put a query into a terminal and then wait, staring blankly at the unchanging screen: why waste all that space and time? Why not a quick message from a contractor or company (selling a faster system, perhaps) to redeem the time? Did you ever get a computer print with all that blank paper in front and back? Why waste the paper? Let the kids doodle on something else; put some advertising there, and help pay for your output!

~~(FOUO)~~ Why, we could sell space in the Green Hornet! Think of all those blank walls all over the building; let the advertisers pay for the paint! And the public address system--why not get sponsors for each announcement? We could stipulate that the sponsor's message could only come after the emergency messages, of course. And for those big meetings in the auditorium, some advertising on the screen might keep the audience from getting restless until the main speaker arrives.

~~(FOUO)~~ The end walls on the outside of the tower are just huge blank spaces; does anyone know if Mail Pouch still paints barns? Too bad Burma Shave doesn't still do those sequential signs, considering all the roads and parking lots we have. The bus that runs between buildings, the elevators, the escalators, the cafeteria walls--the opportunities are everywhere. We might finish the year showing a profit! The possibilities just boggle one!

WES

DOCID: 4009849

WHO WANTS A PROMOTION, ANYWAY? (U)

by [redacted] T1
Col, USAF

P.L. 86-36

Some of our readers are Air Force officers, and others are or will be supervisors or coworkers of Air Force officers. Both groups should be interested in these remarks, adapted from an address by [redacted] USAF, to the Communications-Electronic Officers' Course at Keesler AFB, Mississippi, on November 1981.

When I was asked to address you, I pondered what would be the best subject to share with you. I thought I could talk about state of the art (FOUO) technology--computers, distributed processing, digital systems, fiber optics, millimeter radios, wired cities, and the like, but I decided that you have been force-fed Communications-Electronics long enough. Then I thought I would tell you about my job. [redacted] Our computer operations is one of the largest, if not the largest, as is our production signals processing effort. For you country folks, the area of responsibility is more than seven acres, and for you city people, that's about 30 city lots or homes. Isn't that impressive? Sure, it is! But that isn't going to help you in your Air Force career; so that's all I'm going to say about my job.

I have an additional duty that I consider most important to the individuals with whom I talk. About two years ago, General Larson, the Commander of the Electronic Security Command, was concerned that his people were not getting as many promotions as he thought they should. He established an Officer Career Development Panel consisting of 12 Colonels around the world to counsel each officer (O-5 and below) at least once a year. I am one of those Colonels and the duty can be rewarding--it can also be discouraging. We meet "two on one" to review the officer's records as a promotion board would. That is what I wish to share with you today--what promotion boards look for and what you need to do at what point in your career to be competitive for promotion.

Ladies and Gentlemen, your promotion folder is all the board has to represent you! The accuracy and completeness of the data in that folder is your responsibility--no one else's!

Let's review it! The first thing we see when we open the folder is your official photograph. You've made your first impression on the board members. Whether that is good or bad depends on your picture. That picture can say, "Hey! I'm out here and I want to be promoted!" Or it can say, "Eh. Take me as I am! Promote me or don't; I really don't care!" Surprised? Don't be! There are records that say just that; and when the officer gets passed over, he or she says, "Why me?" If the photo isn't the best, the rest of the record probably isn't either.

DOCID: 4009849

Let me share an experience with you. I think it was on my first promotion board. One of my panel members opened a folder, made a disgruntled remark, and immediately laid the folder aside. Why? He didn't like the length of the officer's sideburns. They were regulation length but only a hair's width from becoming too long. That was enough to turn that panel member off on that record. Petty? Maybe so! But competition is keen and when records are nearly identical, board members find themselves looking for "tie breakers," and those tie breakers go for or against you.

Let's prepare for your photo. Gentlemen, the day you have your picture taken, or the day before, get a haircut. Ladies, have your hair done or do it yourself. Have your photo taken early in the morning. At the Pentagon, they won't take it after 1000 hours because they have found that "the five o'clock shadow" shows by then. Insure that your sideburns are squarely cut and short. If I had a mustache, I'd shave that hummer off for the photo; there are just too many things you can find wrong with a mustache: too thick, too thin, too wide, too long, too short, not trimmed. You name it; they'll find it.

The most common discrepancy on the photo is that the U.S. insignia are improperly aligned. The letters must be positioned horizontally (parallel with the ground), halfway up the lapel seam, resting on it but not over it; and they shouldn't be tarnished or polished to a high luster. You get into your sharpest uniform (one without a near-term wearout date), stand in front of a mirror, position your U.S. insignia, center your rand on the epaulet 5/8" in from the outer seam, center your name tag and your neat, correctly sequenced ribbons with the devices properly placed so they are resting squarely on top of your pockets but not covered by your lapel, and you're ready for the photographer. Right? Wrong! Why?

Because your photo is taken sitting down and when you sit, everything gets "out of whack." When you set your uniform up, sit in front of the mirror, the way you will sit in front of the camera. To have you uniform hang neatly, you may need to open the bottom button of the jacket, and that's OK. The picture will be cropped, so it will not show. Just don't forget to button it before you leave the studio.

That's a lot about the photo: but, as they say, first impressions are lasting and, at an average time of three minutes per record, you don't have long to change that initial impression. We women don't have the pockets to help us line up our name tags and ribbons. The important thing is to have them parallel with the ground and at the same level.

When you come up for promotion consideration, get a new picture. An old picture doesn't tell the board that you want to be promoted. Make that little extra effort. It's impressive when you see a photo taken last month.

One other thing, gentlemen: snug up that tie. A loose tie, especially with your shirt showing above it, makes a negative impact. The same for the ladies! Your blouse should not show above your tie. Enough about the photo.

Your OERs have to be great or you don't have a fighting chance. That's not to say that you can't get promoted with a "2" or "3" if you got them during the controlled OER period. If your rater tells you today that he's giving you a "2" to "give you room to improve," you'd best talk turkey to that turkey. A "2" today says you're in the bottom five percent of your peer group.

Your OERs are a record of your past performance and an indication of your potential. They tell when and where you did what and how. They should have facts in them. When I gave you that 30 seconds on my job, it had several facts in it, and that's what the narrative in the Job Description block of your OER should contain. The same is true for the Performance Factors blocks and the three Comments blocks. You can have a "fire-walled" OER with a "1" rating, but if the comments and remarks are all general, it tells the board nothing; or maybe it says, "we've got better people. He or she is OK but ...!" The board looks for substantial accomplishments and recommendations for promotion. "Promote when eligible" doesn't say much: eligible for what? Below

DOCID: 4009849

the zone? Primary zone? What? They look for

- "Promote now"
- "Promote BTZ" (below the zone)
- "Promote first time eligible in the primary zone"

They look for good endorsements and general officer endorsements carry a lot of weight, especially if it is obvious that the OER was elevated for a high level endorsement in the chain of command.

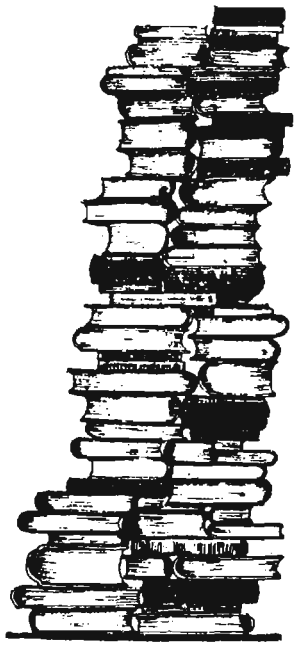
Your selection folder contains citations for approved decorations. If your photo shows a ribbon, wings, missile badge, or any device not supported by a citation, order, or other documents, it looks suspect. Among the miscellaneous documents are administrative requests to obtain missing documents. Often we find these requests stamped with "second request." It is to your advantage to provide the missing documents or current photo as soon as you receive the request. No one can do that for you. I hope that you have a complete personal 201 file and can retrieve the required documents with little problem.

The next form is not in all folders and many of you have never heard of it. AF Form 11, the Officer Military Record, is now a historical document that was last updated in 1974. Your Form 11, if you had one, remains part of your folder.

Next is the Officer Selection Brief, a computer generated form that contains a wealth of information about you. About 60 to 90 days before a board convenes, each eligible officer receives his or her Officer Preselection Brief through the servicing CBPO. This Preselection Brief contains the same information as the Officer Selection Brief that is part of the folder evaluated by the board members. You are responsible for reviewing the Preselection Brief and having any errors or omissions corrected by your servicing CBPO. I won't cover all the data elements in the Brief, but I do want to cover a few in some detail: the most frequently problem areas.

Let's start with formal education. Almost every officer has a bachelor's degree; very, very few do not. I don't have the exact figure, but the percentage of Captains and above with master's degrees is in the high 90s; the degrees are not all job related, but they are master's degrees. There are several avenues you can take to get an advanced degree. Check out AFM 36-19. You can go AFIT, BOOTSTRAP, Naval Post-Graduate School, and on- or off-base/campus programs. If you want an AFIT program, don't wait for AFIT or a selection board to pick you up: request an AFIT evaluation. They will evaluate your records and tell you whether you are qualified, and you could find yourself in one of their programs before you know it. It's not commonly known, but there are AFIT slots that go unfilled every year. Just don't wait until you come up for Captain before you decide to start working on your master's. It's too late then! Do it! Get it on your record! And, if possible, apply the degree knowledge to your job.

Another shortcoming often seen is in the area of Professional Military Education (PME). I don't know if the officers are waiting to be picked up by a selection board to attend in residence or what. I do know that PME is often missing in an otherwise good record. I know it's tough to complete your degree requirements and PME by correspondence, especially if you have a family. The youngsters don't always cooperate when it's time to concentrate and study. Everyone cannot be selected for PME in residence; maybe 38 percent get to go, so don't wait for it. Complete the correspondence courses and if your name comes up for residence, so much the better. Go if you can, but don't count on it. You may be selected and denied the opportunity to attend because of operational requirements. Again, don't wait! Get cracking on your PME. Time goes by all too fast and if you put it off, it will soon be too late, and your records will not be competitive.



DOCID: 4009849

There is controversy regarding completing PME in residence or by correspondence. Some believe that the "cream of the crop" are selected for residence, and it's true that the interaction and exchange of ideas between officers in residence add value to the PME course. It's also true that those experiences are available on on-base seminars, and if pure correspondence courses are difficult for you, join a seminar. If there is no seminar, consider starting one. That's super OER material! Others believe that completing PME by correspondence show a greater drive and initiative in the officer. He or she performs full time duty for the Air Force and still gets the PME; in residence, the officer is a full time student, not directly contributing to the mission during that time. There are advantages and disadvantages to both methods. Just do it, one or both ways, and get it into your records.

The time requirements change to register for PME correspondence courses, but generally speaking, Lieutenants should complete Squadron Officer School; Captains and Majors should get an intermediate Service School (Air Command and Staff, for example; some officers take the Marine Command and Staff while they wait for the "time in service" requirement to take Air Command and Staff), and Majors and Lieutenant Colonels need to get a Senior Service School: Air War College or Industrial College of the Armed Forces, or both.

One other thing about PME: your file may contain a PME letter telling the board

- that you declined to attend residence PME courses for personal reasons, or
- that after being selected for attendance, you were denied the opportunity to go because of operational requirements.

Other data elements in your brief include your date and source of commission, the date you came on active duty, dates of promotions, dates of and levels of assignments, overseas dates, rated information, awards and decorations, distinguished graduate information, and a few other data elements.

Awards and decorations are often a function of being in the right place at the right time, or the wrong place, as the case may be. If you don't have many, or any, don't worry about them. There isn't much you can do except hope that your supervisor is a someone that will take the time and effort to write the recommendation that documents your outstanding performance--assuming it was outstanding, that is. It isn't easy! It takes someone's time and effort to write a good recommendation for the awards board's approval. Our Director can approve the Joint Service Commendation Medal and the Defense Meritorious Service Medal; anything higher must be sent outside the agency for final approval. It gets frustrating and I can understand the reluctance of some people to write recommendations for decorations; I guess you could help your supervisor by given him some notes or even drafting the recommendation. Some supervisors would appreciate that. Others wouldn't process the recommendation anyway, so you need to be tactful and know your supervisor well before suggesting either approach.

Some folders have unfavorable information in them. I hope you won't have any of these documents in your folder, but if you earned them, they will be there. Correspondence reflecting an Article 15 or Court Martial remains in your folder for two years or until reviewed by one temporary or permanent promotion board, whichever comes first.

Also undesirable in your folder is what's called "not qualified recommendation or digest file." These are forms of derogatory data that have been reviewed through command and legal channels. The officer involved is notified in writing of the existence of these files and has appeal rights. What can I say about these types of correspondence? You don't want them; don't do anything to get them!

Next comes the AF Form 705, Lieutenant Colonel Promotion Recommendation Report. This report is used only by Central Temporary Colonel Boards. These forms were written on Lieutenant Colonel OERs that closed out on or before 30 June 1981. No 705s are written on officers for a reporting period after that date, but all 705s previously submitted remain a matter of record in the selection folder.

One other piece of correspondence may be found in the selection folder. Since DOPMA, an eligible officer may write to the board, calling attention to any matter of record that he or she believes is important to his or her consideration. A couple of words are required on that. First, decide seriously whether you want to address the board about your record. If, after careful consideration, you decide to write a letter to the board, make it factual and to the point. Do not, and I say again, do not be emotional and do not blame anyone else. Accept responsibility for your action or lack

DOCID: 4009849

of action. If you were a victim of circumstance, you can say that--but be factual about it.

So much for what the promotion board panel members look at and for. I'd be remiss if I failed to tell you that you may review your selection folder at the Air Force Manpower and Personnel Center (AFMPC) at Randolph AFB, Texas. If the folder is incomplete or contains incorrect information, take immediate action to have it corrected or completed.

Having said all that, just what is the purpose of promotion boards, and what are your promotion opportunities?

Well, promotion boards insure that enough officers of the desired quality are in the proper grade to carry out the Air Force mission. Promotions should occur at spaced intervals to insure that the best qualified officers are promoted to positions of authority and responsibility. A promotion is not an award for past service; it is an advancement to a position of responsibility, based on past performance and future potential.

Your promotion opportunity is determined by the percentage of each year group that can reasonably expect to be promoted to the next grade, and that is determined by Air Force requirements. The quota is an established percentage of those officers "in the promotion zone," that is, the first time eligibles (new eligibles):

- 97.5% to Captain
- 90% to Major
- 75% to Lt. Colonel
- 55% to Colonel

These percentages are misleading, because those selected "below the zone" and "above the zone" (those previously considered but not selected) are at the expense of the new eligibles. Considering that, your opportunities are reduced considerably:

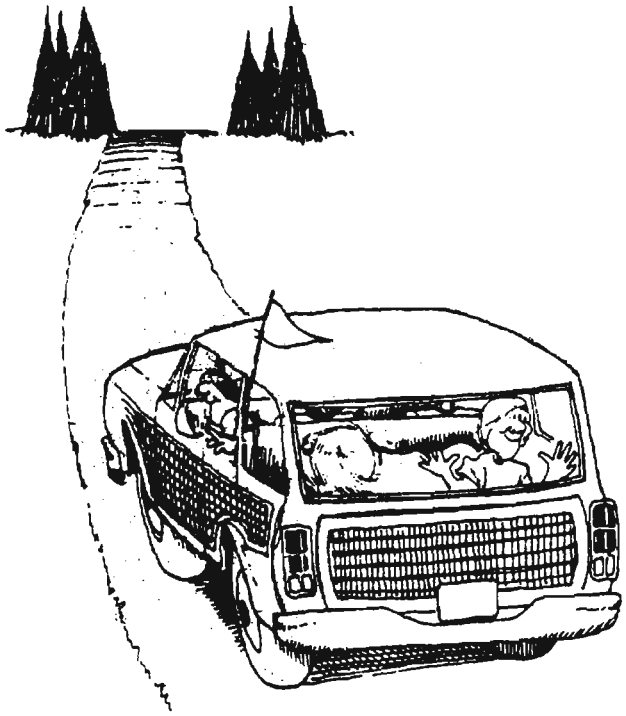
- from 90% to 75% going to Major
- from 75% to 60% going to Lt. Colonel
- from 55% to 35% going to Colonel

An earlier study showed that only six percent of all newly commissioned officers make it to the Colonel level. Of course, many resign their commissions or retire before they become eligible for Colonel; still, six percent isn't very high.

I wanted to mention some factors that would help you get those good OERs I talked about earlier: being flexible, making frequent moves, getting into all facets of Communications-Electronics (Operations, Maintenance, Programming, Budgeting, and don't let computers scare you), relying on and respecting your NCOs and airmen, seeking challenging jobs, and a thousand other things. If you don't know about the ASTRA program (Air Staff Training Program), find out about it. It's tough, but if you want to go far and fast in the Air Force, apply for one of those positions, be successful there, find a General Officer to sponsor you, and you'll get "below the zone" promotions and super jobs.

I realize that I've shared a lot of material with you in a short time. I trust you will find it useful in your career.

Now, I know that the graduates have everything they own in the car, including the dog and the cat, and some of them even have the engine running, so just let me extend my best wishes to each of you for a long and successful Air Force career.



DOCID: 4009849

LOOKING AROUND with [redacted] P13

AMATEUR SPREAD SPECTRUM (U)

P.L. 86-36

(U) Amateur Spread Spectrum communications appear to be in the doldrums, according to Paul Rinaldo, President of AMRAD, a Ham corporation that has been investigating this new mode.

(U) The central problem is that there is no market for spread spectrum communications either among Amateurs or among other civil users. The comments received by the FCC have been mostly against spread spectrum, because of potential interference problems. AMRAD Corporation got an STA (Special Temporary Authorization) in 1981 to waive cipher and bandwidth and other restrictions in order to experiment with frequency hopping and direct sequence coding transmissions, but only a few experiments have been carried out. AMRAD will ask for a new STA to try again in 1982-83, but the combination of apathy and indifference by the Amateur community does not show much promise. One new equipment was developed, viz., a 2 meter frequency hopping radio, by an amateur who hoped for foreign sales. His equipment apparently worked, and he found customers.

(U) Rinaldo summed up the AMRAD experience of the last year at an IEEE-VTS meeting on 28 May 82, and a current report in the AMRAD Newsletter reinforced many of his points. Amateur packet radio is apparently doing quite well, and spreading, but spread spectrum is faltering, and the projects have failed to reach completion.

(U) In his opening remarks, Rinaldo noted that Spread Spectrum is "controversial." There are popular beliefs that Amateurs "can't receive it," or if they could receive it, could not decode it. It is also believed that Spread Spectrum cannot be "DF'd," and hence cannot be monitored. Therefore, according to Rinaldo, there is popular belief that it is open to abuse by spies, criminals or terrorists. It is also popularly believed that the spread signals would interfere with everything, like the "Russian woodpecker" at 14 MHz that interferes with HF communication. It is also popularly believed that narrow band communications can do the same thing.

(U) These popular beliefs, Rinaldo said, gave a distorted picture of Spread Spectrum. He said he had been using SS for years.

(U) The starting point for Amateur involvement in SS communications, which was previously only a military technology, occurred when Dr. Marcus of the FCC OST (Office of Science and Technology) approached Perry Williams of the ARRL (Amateur Radio Relay League) and asked ARRL to push the development of Amateur SS. The purpose of this FCC initiative was to get cheap SS equipment onto the market. Since Amateurs were known to be adept at finding cheap ways to put radio gadgets together, the FCC apparently hopes the Ham community could do what the U.S. military electronics industry could not do, viz., develop low cost SS

radios, which the FCC could then authorize for use in many different radio services where frequency crowding (e.g., in urban areas) was causing complaints to reach the FCC.

(The author has heard rumors that the FCC gave the impression that the Amateur frequency allocations could depend upon how well the Amateurs responded to this opportunity to develop SS. The issue of Amateur SS was so controversial to foreign governments that the ARRL had to adopt the euphemism "low flux density modulation" in their correspondence to avoid friction with the corresponding foreign Amateur associations).

ARRL then interested the AMRAD Corporation in spearheading this new project. AMRAD itself is a Ham club organized as a legal corporation (AMateur Research And Development), with about 600 members, some of whom apparently are foreign. Its newsletter is mailed to foreign and overseas subscribers. The aim of AMRAD is to pursue new technology projects (of which SS is one), and to disseminate technical information. A number of the people involved in the AMRAD SS experiments claim to have had experience with spread spectrum and cryptologic systems (for both encryption and interception-analysis). The AMRAD Corporation operates a repeater and a message system in the Washington area.

(U) The two experiments actually conducted under the STA were an HF frequency hop communication, using two RACAL S.A. transceivers imported by MILCOM, and a VHF 2 meter frequency hop experiment using equipment built by an Amateur who was interested in overseas sales. Rinaldo played an audio tape demonstrating the HF experiments between Kessler of MILCOM in Providence, R.I. and Rinaldo of AMRAD in Virginia. SSB voice and Morse code were both used, with hopping at 5/sec, after an initial setup, callup, and synchronization in a non-hoppiong mode. The VHF experiment in Virginia during February worked in the 150-174 MHz range. The experimenter, C. Phillips N4EZV, has now sold his VHF gear and intends to experiment in the 14 MHz and 21 MHz bands at speeds up to 80 hops/sec.

(U) The SSB HF experiment illustrated that frequency hopping doesn't work well on weekends, when the Ham bands are full, but during the week when there are empty frequency slots it is feasible.

(U) The proposed experiment at 10 meters, which was to modify CB radios to frequency hop at 30 MHz, is not yet finished. AMRAD wants to get a new STA to pursue this. Rinaldo thought that the equipment for the modification would be inexpensive, if they could get the circuit to work, and get volume production of the circuit boards. (Note: a Ham packet radio circuit board sells for $35). The 10 meter experiment has not yet gone on the air. The proposed experiments at 400 MHz, to use direct sequence coded signals through a repeater, have languished without any finished equipment. A 420 MHz experiment to do SS moon bounce, using the 85 meter government antenna at Cheltenham MD, has also languished.

(U) The demonstration of frequency hopping at 2 meters has raised a question about whether a hopping signal might activate a Ham repeater. Rinaldo thought the squelch circuits would suppress short random pulses that got into the repeater control channel.

(U) The FCC Docket 81-413, asking for comment on general Spread Spectrum use, received mostly negative comments. "Not on my frequency!" was the theme of the comments. Most of the comments did not take the near-far effects of SS into account. Rinaldo stated that the "near" effects, where a receiver listening for a weak signal is close to an SS transmitter, is much worse than people expect. Very few comments on FCC Docket 81-413 thought SS was a good idea. Rinaldo sounded somewhat discouraged by the resistance to this new technology.

(U) The FCC Docket 81-414, asking for comments on Amateur Spread Spectrum, received replies that paid lip service to "experimentation," but "not on my frequency!" There were fewer than six comments, and most were from Hams who wanted to receive weak signals and feared SS interference. AMRAD filed favorable comments to continue SS experiments. There appear to be no applications for SS, except for experiments. Rinaldo did not expect an operational SS service on the Amateur bands.

(U) The basic question in civil and Amateur use of SS is, what good is it? The technology is a military development, to give LPI (low probability of interception). Rinaldo said that it is now being revealed that SS signals can be detected, although it takes special apparatus. He did not say who was revealing this. Rinaldo thought there might be a use for SS for police surveillance, viz., "bumper beepers" that could be attached to some citizen's car and could not be detected by a conventional radio sweep. He also thought SS could be used to defeat police buffs, who monitor police radio traffic. (Presumably these would be frequency hopping radios, and the AMRAD Newsletter of May 1982 claims there is a concept for a receiving system that would not need the code sequence).

(U) The most promising ways of solving the near-far problem were to locate the radios or repeater in remote places, e.g., a satellite repeater, or offshore oil platforms. Since there are very few signals in remote locations, the SS systems cause fewer problems and work better. However, narrowband systems also work better in a sparse environment. Operating SS stations in the midst of a dense population of radios, e.g., in a city, will cause many problems, according to Rinaldo.

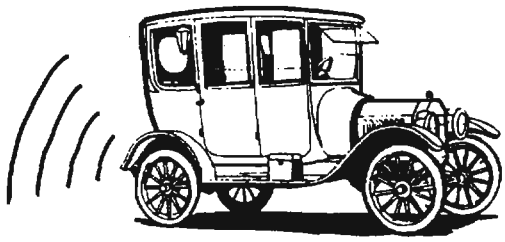
(U) Rinaldo concluded that SS was neither a panacea nor a nefarious plot. He felt there were some specific civil applications, although they would be rather specialized.

(U) Rinaldo then played a tape recording of the Kessler-Rinaldo HF SSB frequency hopping experiment. The voice transmission had many little clicks and bleeps, that changed every 200 milliseconds as the radio hopped. The Morse transmission also had a pattern of short changing bleeps. When the SSB voice channels are busy on weekends, there is no empty space to send frequency hopping signals.

(U) In reply to questions, Rinaldo stated that it was hard to set up the SSB circuits, except in a narrowband mode, where a synchronizing signal was sent to lock the transceivers before they began hopping. This, he admitted, made LPI mode infeasible, at least at the start of the link. He did not know the efficiency of spectral use provided by SS. No interest in SS was shown by the land mobile radio industry. There was some police interest in secret bumper beepers. Asked about covert use, Rinaldo replied that SS was "not unjammable." (This did not deal with the interception problem). He said that the SS systems that he knew about generally do not live up to advertising, being less hearable by the intended users and more interceptable than the makers claim.

(U) On equipment cost. Rinaldo said slow hopping radios could be cheap if made in quantity, but if a hopping rate as high as 500 Hz was wanted, the cost went up considerably, because of the stricter timing requirements.

(U) The Spread Spectrum column by Hal Feinstein in the AMRAD Newsletter for May 1982 made many of the same points about the lack of enthusiasm for this new technology. The problem of policing Amateur SS led to a concept of a receiver that did not need to know the code for a hopping sequence. AMRAD also discovered that "there are numerous codes which are complex yet do not have privacy properties. So, the number of codes that Amateurs could use is larger than originally thought. If a station illegally uses a complex code to hide the meaning, there are some workable concepts which could be used to detect this."



Analysis

(U) The original concept that Amateurs would be able to develop cheap SS radios is unfulfilled. Despite the lack of progress, the development of a circuit board to convert CB radios to frequency hopping would bring the threat of uncontrollable SS radios at low cost back in full force. Once such a circuit board is developed, there will be no practical way to control its dissemination.

(U) The issue of criminal or terrorist use of SS radio techniques that the Amateurs develop has been swept under the rug. The FCC seems uninterested, and the Intelligence agencies cannot touch the problem--unless there is proof that foreign terrorists are using the equipment.

(U) AMRAD has found the "near" problem, viz., SS radiations from a nearby transmitter, to be much worse than expected, practically ruling out any urban or close suburban SS stations. This would appear to undermine the original argument that SS was a good way to increase bandwidth usage, for it interferes with other users more than a narrowband radio would.

~~(C)~~ The expectation that SS stations would be able to call each other in the SS mode, without a preliminary fixed frequency setup, has been contradicted by experience so far.

[redacted] The high cost military SS radios that can call up in SS mode rely on expensive clocks to keep the transceivers synchronized when they are off, and Amateurs generally cannot afford an $8000 clock to drive a $300 radio. The technical problems of tight synchronization require severe standardization between all users, and compatible equipment, but Amateurs are usually too varied in their equipment and interests to make this a feasible solution. Hence, it appears that only expensive military SS radios can operate without a proforma fixed channel setup and synchronization.

~~(FOUO)~~ The interest in "complex codes" that do not have "privacy properties" deserves attention. Because AMRAD has international circulation for its newsletter, and may have foreign members, the experimentation with code generators should be kept within the FCC guidance given in Docket 81-414.

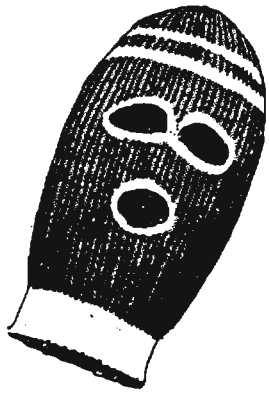
~~(FOUO)~~ The sale of the 2 meter frequency hopping equipment is also a matter of interest. Who bought it? Who, outside of AMRAD, is authorized to operate SS equipment in the U.S.?

~~(FOUO)~~ AMRAD's application for a new STA should limit them to the provisions of Docket 81-414, without the release from callup and cipher regulations that was given in the first STA.

~~(C)~~ Summing up, the attempt to introduce SS on Amateur circuits is off to a slow start, but could still develop if cheap workable modifications for 10 meters (based on CB radios) and for 2 meters are developed and disseminated. There is no visible market for SS equipment or services in any areas where they would overlap existing radio circuits. Some of the enthusiasts apparently want the LPI feature, but have not found the technology to accomplish this cheaply. As long as SS radios are expensive, they can probably be controlled, but will become very difficult to regulate of control if they become cheap.

[redacted] The experimenters in AMRAD apparently developed their knowledge of SS technology in government related projects, and are transferring their knowhow. There seems to be inadequate control over this kind of transfer.

EO 1.4.(c)
P.L. 86-36



P.L. 86-36

DOCID: 4009849

GOLDEN OLDIE

P.L. 86-36
EO 1.4.(c)

REPORTING MESSAGE VOLUMES (U)

P.L. 86-36

P.L. 86-36
EO 1.4.(c)

by [redacted]

(reprinted from COMMAND, March 1971)

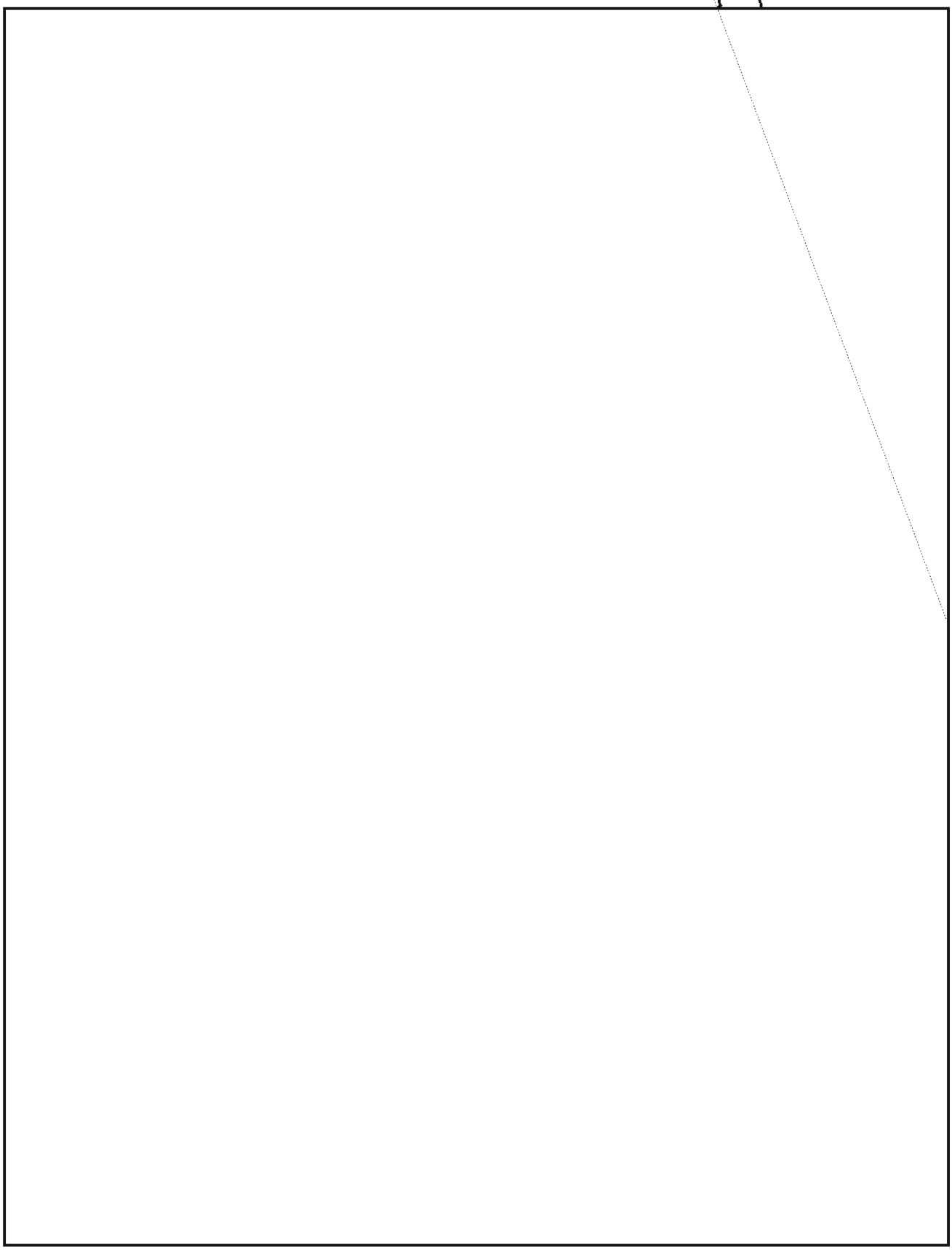
(With grateful acknowledgement to [redacted] Donald Oliver, and [redacted]

[redacted]

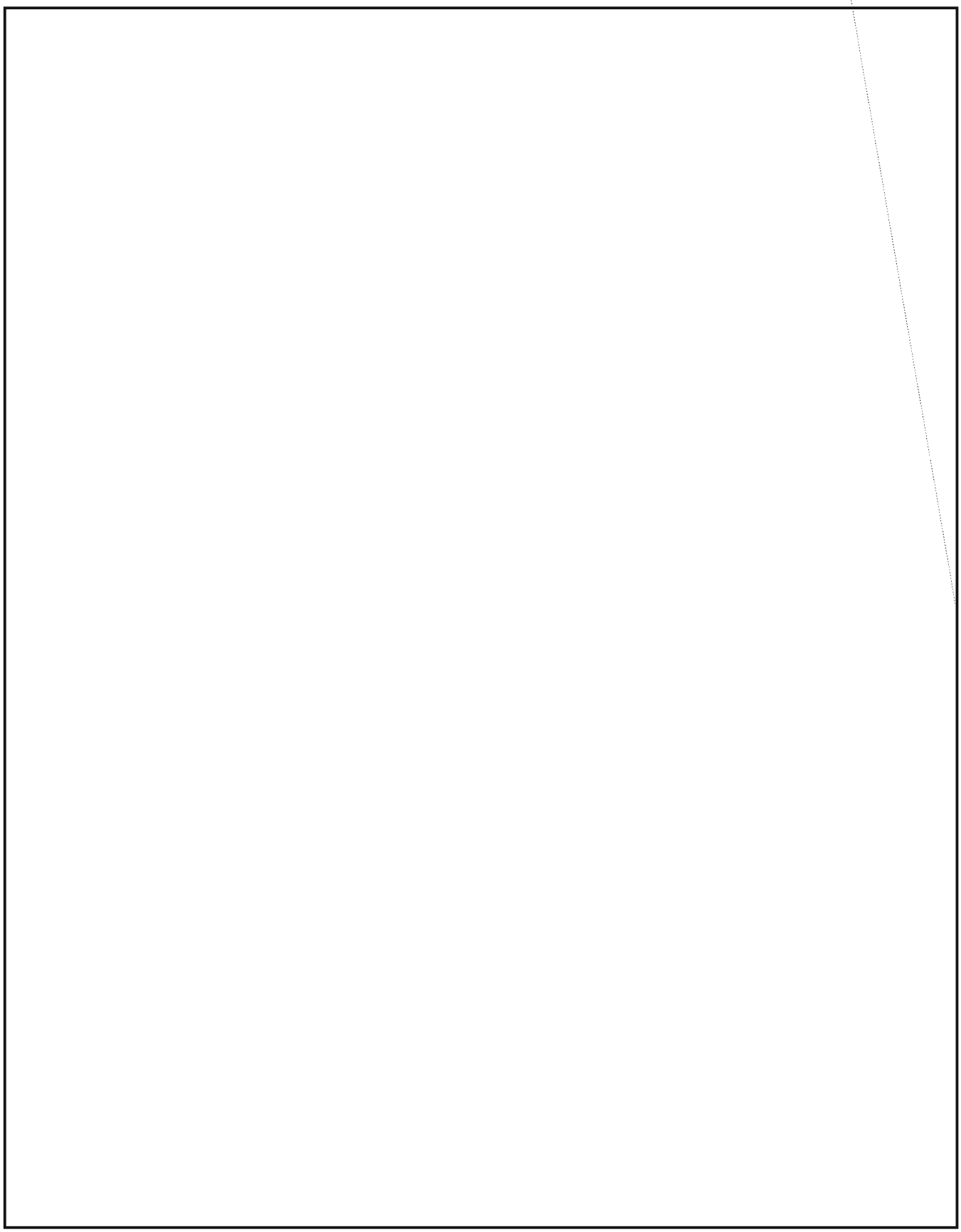
[redacted]

DOCID: 4009849

E0 1.4.(c)
P.L. 86-36

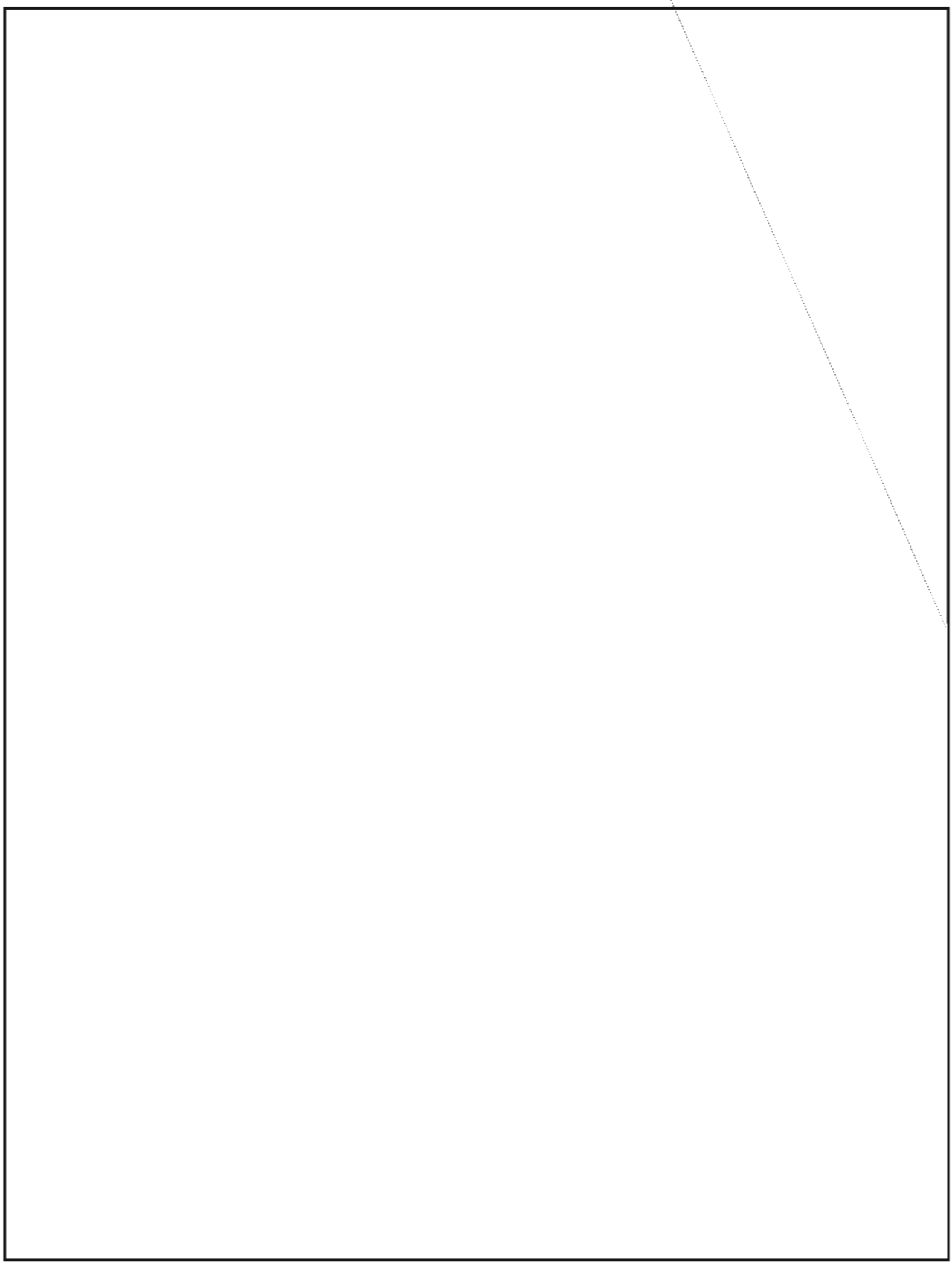


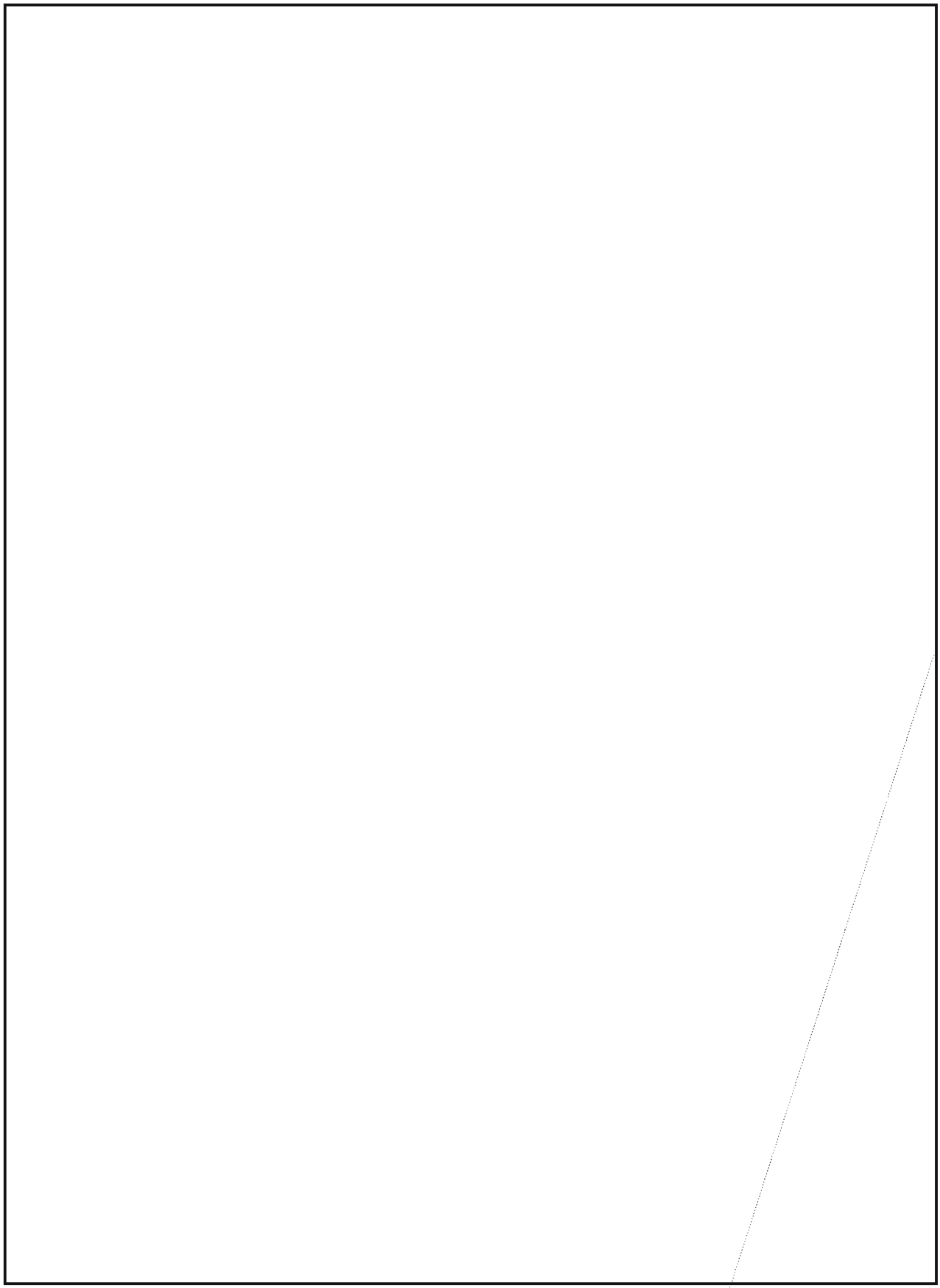
EO 1.4.(c)
P.L. 86-36



DOCID: 4009849

EO 1.4.(c)
P.L. 86-36

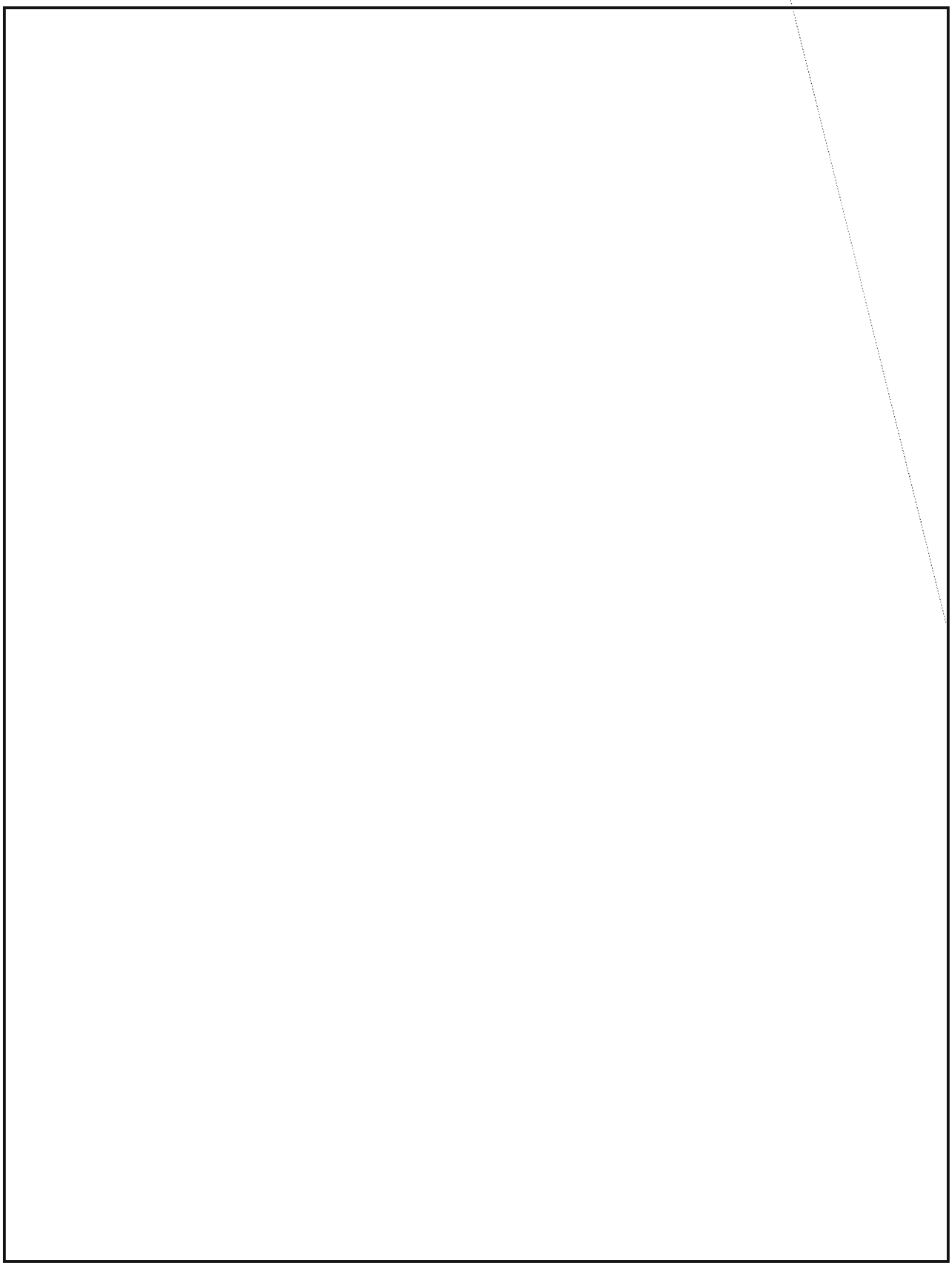


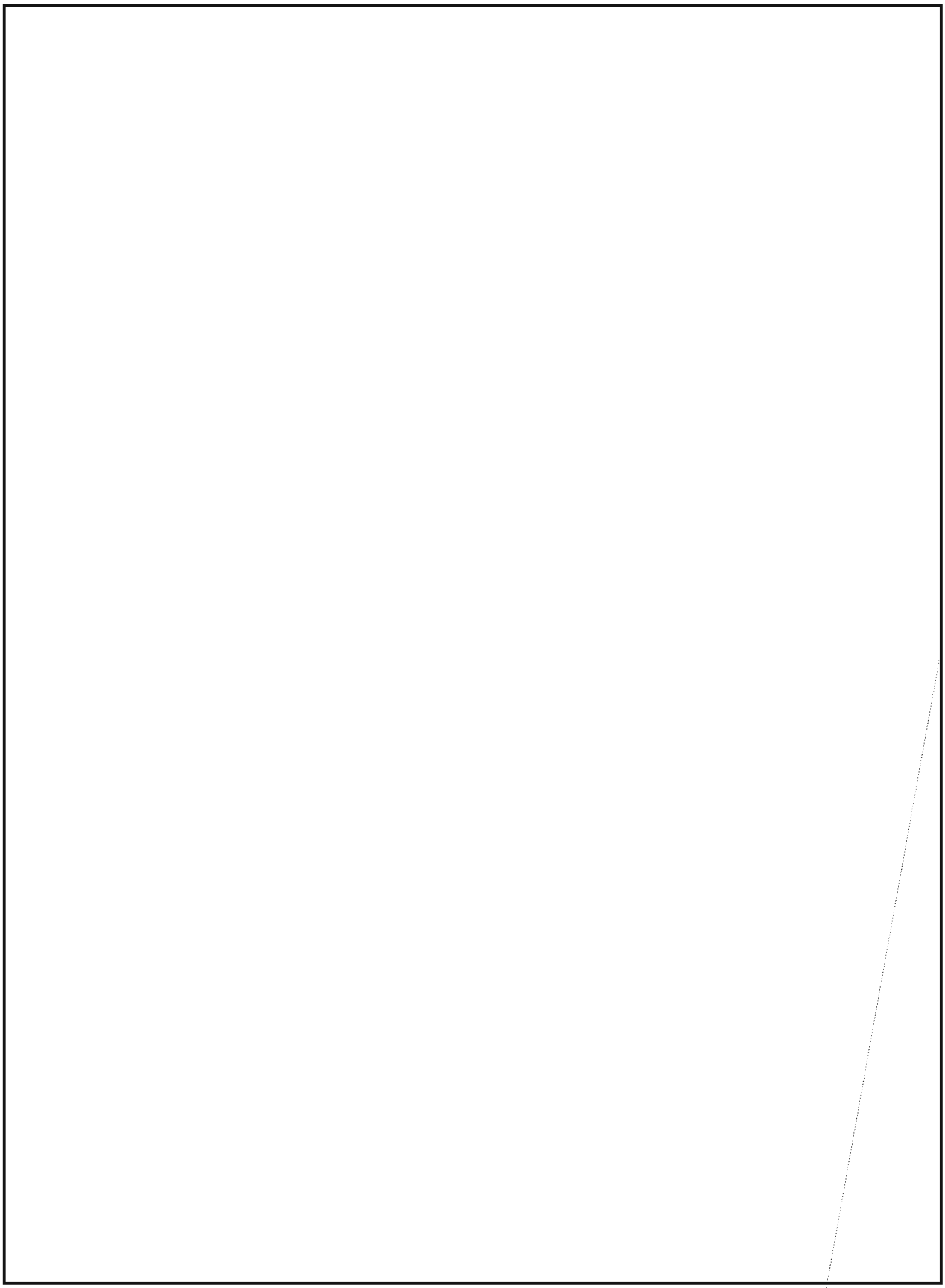


EO 1.4.(c)
P.L. 86-36

DOCID: 4009849

EO 1.4.(c)
P.L. 86-36





EO 1.4.(c)
P.L. 86-36

DOCID: 4009849

EO 1.4.(c)
P.L. 86-36

A PERSONAL FOOTNOTE

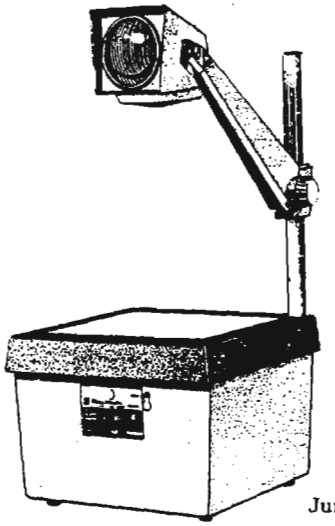
~~(S-CCO)~~ Early in the war, we were still stuggling with how to report in a meaningful way to the customers who wanted daily updates on what we saw in the traffic. The pressure to say something each and every day was overwhelming. One day, a field report came in which argued that troops were coming down through Laos, over the "Ho Chi Minh Trail," and cited increased traffic volumes during certain periods in support of the argument. At the time, there was some collateral information that seemed to support the argument, but as often happens, there was other collateral information that seemed to conflict. The response from the Washington level consumers was strong and immediate: did we agree with the field report?

~~(S-CCO)~~ The key SIGINT facts in the field report were the message volume numbers, so we began to count. Almost at the outset, problems of method began to surface. We had a large amount of unidentified traffic. Some of the traffic which had been marked as "unidentified" in the field had since been identified. Exactly what traffic did the field analysts count? In the midst of this, we were notified the the Secretary of Defense wanted a personal briefing on the question.

~~(S-CCO)~~ Communications with the field were not yet as good as they would later become, and there was no easy "opscomm" channel to the people in the field, so that we could talk it over with them. The appointed time for the briefing was only hours away, when, to our dismay, we discovered that different people, counting the same pile of traffic, will usually give different answers, if the pile is large enough. Cut-ins, partial messages, duplicates, circulars to more than one station--all these provide different answers when filtered through the perceptions of different people.

~~(S-CCO)~~ "Do the best you can." That was the order of the day, and numbers were "developed" for the time period covered by the field report. Then came the briefing of the Secretary of Defense. At the conclusion of the briefing, he said, "Let me have that Vuegraph slide with the numbers on it." And the slide containing those numbers went into his desk drawer. He was, after all, a man to whom numbers were quite meaningful (and he later went on to become a banker). So, we became counters of messages.

W.E.S.



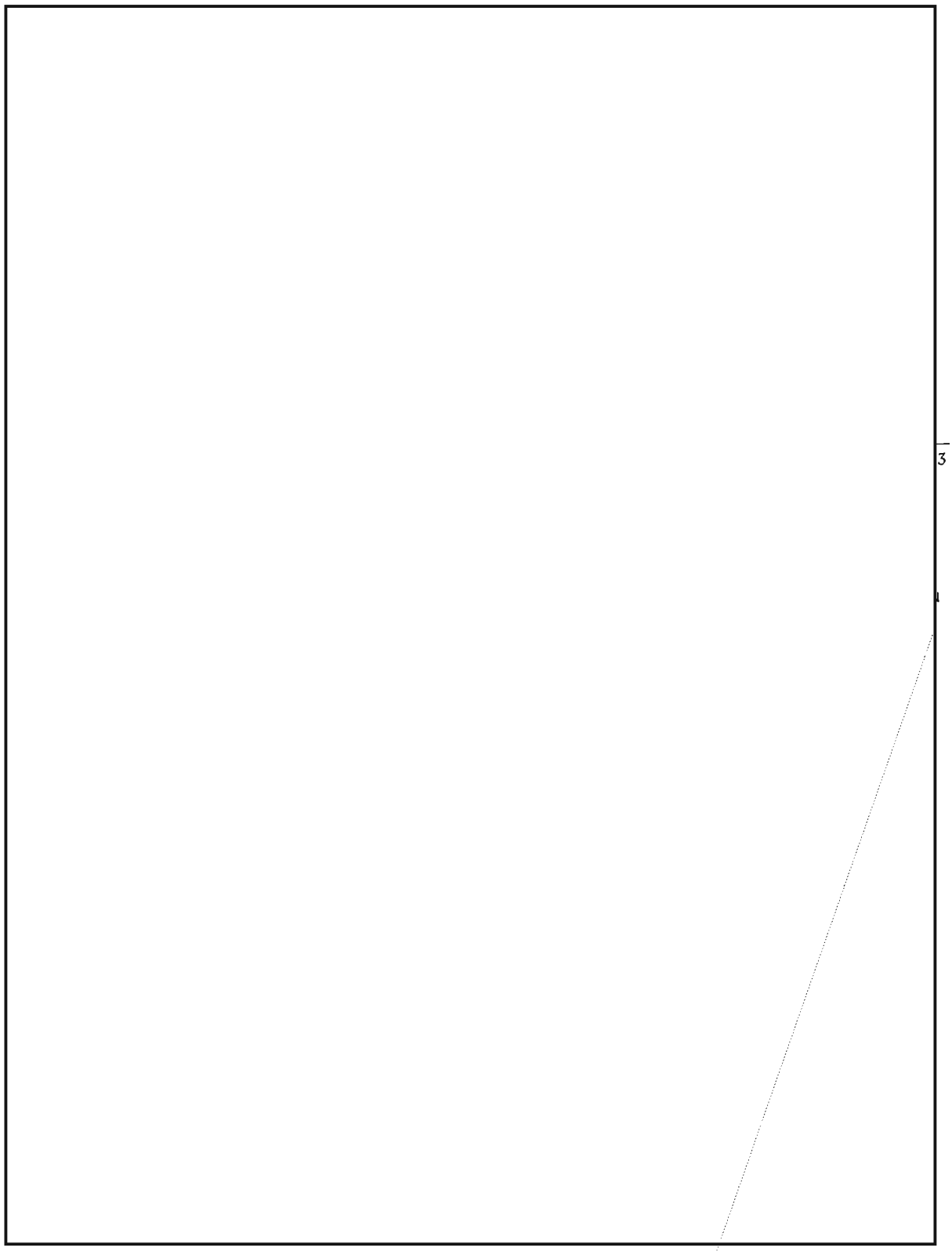
DOCID: 4009849

P.L. 86-36

NSA-Crostic No.41

THE WORLD'S GREATEST LIES

DOCID: 4009849



P.L. 86-36

HUMAN FACTORS

Responsible Documentation(U)

by [redacted] P13

P.L. 86-36

REVIEW: "Responsible Documentation", by Neal Margolis, COMPUTERWORLD, 25 January 1982, pp. 7-16

(I wish to thank [redacted] for calling my attention to this excellent article in the "In Depth" feature of COMPUTERWORLD for 25 January.)

- The customer services staff at a manufacturer of electronic equipment is desperately overloaded with service calls for a new line of equipment--calls that concern minor adjustments thoroughly covered in the manuals.

- The initially happy purchaser of a new hobby computer gives up in disgust and returns it when he can't get it to perform as advertised, using the elaborate manuals that come with the equipment.

- A top-level DP consultant contentedly finds himself assured of a long-term job supporting the installation of new software for a large restaurant chain, since he is the only one who can cope with the twelve manuals that make up the primary documentation for the system.

These three apparently different cases have two crucial things in common: they are counterproductive and wasteful for the firms involved and for the users of the products, and they all arise from documentation that fails to carry out its responsibility of communicating to the user. Margolis suggests that "irresponsible documentation is an almost natural effect of technological evolution". Cheaper, more widely available hardware is reaching an ever-widening circle of purchasers; increasingly sophisticated and powerful products are reaching more and more unsophisticated users. At today's lower purchase prices, manufacturers are less likely than ever to provide the expensive customer service facilities necessary to reach and support this vast heterogeneous user population. The answer is, (or should be) clear, usable, readable documentation.

DOCUMENTATION HAS A JOB TO DO

Margolis makes an excellent point about documentation, in hard-hitting words that make a direct appeal to the manager and the practical businessman: "documentation has a job to do," and it produces a vital output. "Documentation output is in the form of user performance, and by engineering documentation, we can engineer performance." Documentation includes any presentation of information that is intended to improve interaction between a user and a product. It may take the form of manuals, instruction sheets, imprints on hardware that tell how to use it or make it work, or CRT displays that guide a user through a task. Responsible documentation emphasizes what users should do, respects user abilities and limitations, and minimizes "overhead" demands on users (searching, sorting, translating, copying). In contrast, irresponsible documentation focuses on what users have to know, ignores user abilities and limitations, and burdens users needlessly with "overhead" tasks. Spelling out these concepts in more detail, Margolis offers four principles of good documentation design.

DOCID: 4009849

MAKE IT ACTION-ORIENTED

Focus on what the user should do, not what he should know. Documentation should approach the user with the assumption that he has specific goals, which were his reasons for buying the product. He doesn't need to read a treatise describing the product or the theory of how it works in some arbitrary text-book sequence. Start with the results or outcomes the user needs, and tell him what he must do to get these outcomes from the product.

"If you want to...., do the following....",

rather than

"The Franistan is connected to the Freeble joint with a red toggle."

Remember, too, that the user's working memory must not be overburdened. He isn't sitting back reading a text book; he is trying to do a task while he follows your instructions, step by step. He needs to see just the statements that apply to the step he is doing, and that answer his questions about that step. Keep the instructions tied to a relevant action the user is to perform, and a small set of concrete events he can see, touch and hear. Margolis adds this warning: don't leave out any user actions or clues because they seem to you (the programmer or engineer) to be "trivial" or "obvious".

"If you don't tell a user to do something, it probably won't get done."

He recommends the use of a systematic method of identifying all the critical cues and actions that will arise for the user. And, last but not least, don't forget that things can go wrong! The user needs to know what can go wrong at each step, and what to do about it.

"Task Analysis" is a systematic procedure for analyzing a user's interaction with a product. Margolis provides an excellent discussion of this procedure, which I recommend strongly to all readers of this review. He describes it as "a procedure that makes explicit each and every action a user must perform to make a product work." The analyst breaks down an overall task into its component steps to produce a list called a task specification. It is spelled out in terms of specific

- GOALS (what the user is trying to achieve),
- CONDITIONS (events he perceives as cues to trigger an action),
- ACTIONS he performs, and
- RESULTS (new events he perceives as a consequence of his action).

For example, "When the READY light comes on (CONDITION), push the START button (ACTION) and you will see the message "SYSTEM READY" in the upper left corner of the screen (RESULT)." At this point, a good manual or tutorial should also deal with the possibility that the expected result didn't appear: "If you don't get this message within a few seconds,.....etc."

RESPECT USER CAPABILITIES AND LIMITATIONS

Documentation must take the user's strengths and weaknesses into account.

> "Documentation is usually heavily influenced by product experts rather than user experts. Therefore, the common tendency is to assume that the user knows a lot more than he really does."

Too often, documentation reads like an internal technical specification; technical specs are fine in their place, but their place is not in telling a user what to do to get what he wants from a product. A common error is in assuming that "everybody knows" something that, in fact, only technical experts know.

> "If you tell a user to do something he does not know how to do, he will probably do it wrong, or he will not do it at all, or he will ask a colleague and the colleague will do it wrong. In any case, either by phone, or in the repair shop, you will have to deal with the problem."

To make documentation fit the user's capabilities, Margolis urges the designer to go back to the Task Analysis. Consider each step, and ask yourself, "Is the user able to understand the purpose of the actions he must perform? How can I make it clearer for him? Will he be able to recognize the conditions that trigger the actions he should take? How can I describe them unambiguously? Will he be able to tell when he has done the action right? Can he recognize the desired result? What if something goes wrong? How can I tell the user

what to look for, so that he knows right away that the action has succeeded, or that it has failed in any of the possible ways it might fail? Finally, can the user do all the actions with the knowledge he has, and if not, what more do I need to tell him?"

Margolis recommends that all design questions be asked with reference to a complete task analysis. This will ensure that all documentation content (pictures, instructions, examples, etc.) is aimed at getting the user to do something rather than just giving him information for its own sake. Secondly, all design questions should be resolved in the context of explicit, detailed knowledge about the user population. He recommends working with a written description of the user, like a set of operating characteristics or specs. This should include the user's education level, professional background, and what he wants from the product. If you anticipate a range of user levels and goals, focus on the least competent user.

MINIMIZE 'OVERHEAD'

Some of the things we ask of the user in documentation relate directly to his interaction with the product, while others relate to his interaction with the documentation itself. The first are vital, while the second are "overhead". These "overhead" tasks may include such things as searching for the meaning of words, sorting task steps that are out of sequence, finding illustrations that are separated from the relevant text, and puzzling over wordy or unclear sentences. The less "overhead" there is in the documentation, the more efficient the user's performance will be. All the principles of clear, readable writing, well covered in many readily-available sources, apply to documentation with even more force than in other contexts. Margolis highlights certain techniques for clear writing as particularly relevant to documentation.

a) Be consistent in using one name for each thing, and make sure that every name or label has a clear reference. Use illustrations generously to make descriptions and labels clear. The article lists a number of common errors to avoid in connection with illustrations, too lengthy to discuss here.

b) Minimize references to information elsewhere (tables and charts, other Chapters or Sections, etc.), especially if the referenced data is something the user has to have to complete a task. Put as much as possible "in line", at the place where the user needs it. Avoid at all costs using any "implied reference"--a term, concept, or bit of data that the user needs, but that you have forgotten to include, or that you assumed "everybody knows"! A motivated user will search diligently, paging through your documentation as he tries to find the missing data; his task and his flow of thought are both disastrously interrupted for long periods of time. He will rapidly lose respect for the documentation, and his distrust will extend to the product as well. A non-motivated user (or one who has been "burned" once too often already by your documentation) will give up and gripe.

TEST DRAFT DOCUMENTATION IN ADVANCE

Test the documentation carefully before you deliver it or the product. "Get some people who represent your user population; users. Have them work through several sample problems, and watch every step they make. When they stumble, ask them why. Take lots of notes. When you discover big problems with the product (not just the documentation!), either correct them or let the user know what he has to do to avoid them."

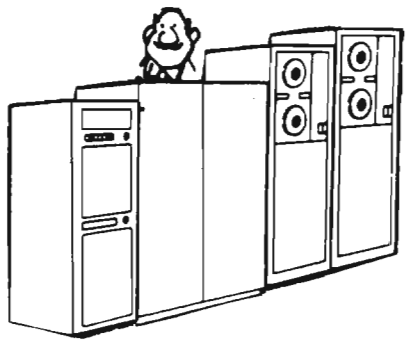
DON'T TRY TO 'ECONOMIZE' ON DOCUMENTATION

Margolis emphasizes the fact that documentation produces a measurable, accountable output. Before a final commitment is made on documentation content, format, and organization, it must be tested, and its output measured. If it isn't performing well in improving the relationship between user and product, it must be revised.

"Too often, 'validation' means a technical review by engineering personnel in order to verify the accuracy of the material."

You should make an explicit commitment to test the documentation, with real users in real situations. Go back to the all-important task specifications that should have formed a basis for the documentation. Measure user performance in the test against the performance standards spelled out in the goals, conditions, actions, and results of the task analysis. Use draft versions of the documentation, with full expectation of having to change things. Watch the users during the test, and talk things over with them. "Saving" time, effort, and money by skimping on documentation is the reverse of economy from any but the most short-sighted point of view.

DOCID: 4009849



Some Reflections on the Reality of Computer Security (U)

by Robert J. Hanyok, H215

(U) Along with the tremendous growth of our computer usage in recent years, we have become aware that we need security measures that will protect the computer, databases, and associated programming. We have developed a host of techniques and plans in response to this need, including access restrictions, passwords, audit trails, encryption, etc. Security officers have been generally enthusiastic in carrying out these measures. As a result, the users have insisted that the resulting security of their systems is ironclad and invulnerable. On paper their claims seem valid, but beneath those claims is a reality that belies this so-called "security."

(U) Here I should establish two points. First, this paper is a personal impression of computer security practices. It is not an analysis of particular security modules, equipments, or kernels; nor is it intended to be exhaustive in scope. The aim is to illustrate the so-called human factor shortcomings I have encountered, examples of which all occurred on computer systems having one or more security measures.

~~(C)~~ Second, my observations are based on more than two years' work in the S organization, where I was involved in evaluating the security frameworks of various computer systems used by NSA, DoD, other federal agencies, and by contractors. I helped develop the Computer Security Survey System (CS^3) which became a major tool in analyzing the security elements of these systems. CS^3 provided a prioritized, coherent, and quantitative method of evaluating computer system security. The use of CS^3 provided, for me, the first inklings of the reality of computer security practices.

(U) Just what is the reality of computer security? The reality is that computer security measures are often undercut by user practices and less-than-adequate implementation. There are three elements to this reality that I have observed. To a degree they are interactive. They all have one trait in common: they are not obvious in a system level review.

~~(C)~~ User level security practices vs. system level security measures.
The user does not fully use the security measures that are available on the computer system. Some techniques, like audit trails, are now controlled by the system and operated with the user ordinarily unable to intervene, alter, or negate them. But some measures, by their nature, allow the user much latitude. The most common case I encountered was with passwords. Some systems levied length requirements for passwords; some did not. Source and randomness of passwords were ill-defined. The result, of course, was that while everyone had passwords, they could be too few characters, predictable, and often kept in accessible places. In one office we visited, the operators had taped their passwords to the terminals. In another system, unauthorized persons were given passwords for "special projects." At best, such practices can be labelled sloppy; at worst, they are an outright invitation to compromise.

~~(C)~~ User security practices are dictated, not by the classification level of the data, but by the perception of the threat.
This was probably the most unexpected phenomenon I encountered--almost a reversal of conventional security imperatives. While some users who handled sensitive data in their

computers seemed to give it proper protection, the rest (i.e., the vast majority) did not. Instead, they protected their data, including caveat, codeword, and compartmented material, only to the degree needed to defeat what they perceived as the threat. This practice would not be a problem if the users were conscious of the constant real threat to their material. However, the normal attitude encountered during CS[3] evaluations was that

> "Our computers operate in a benign environment. Why do we need these protective features?"

A so-called "benign environment," is one like the physical environment of NSA with its wire fence, guards, badges, etc. But it is only an illusion of security, because we know that "cleared" personnel continue to be targets of recruiting by hostile foreign intelligence. Because of this Pollyanna attitude, sensitive material is placed in computer systems whose protective features are either less than adequate or nonexistent. The data on a system is available to anyone who can access that system.

~~(U)~~ Both partially secure or unsecure computer systems allow conventional security safeguards to be circumvented.

Remember the offices handling sensitive data? They had the full panoply of special security: locked doors, sign-in lists, escort requirements, and special clearances. Yet these same offices would place the same sensitive data in an unprotected computer file space that was accessible by anyone on the same system. Deterred by physical controls, an individual could still retrieve the data through the computer. The special feature of this element is remoteness. The distance involved between the data and the person getting access to it need be no closer than the furthest terminal connected to the computer holding the data.

(U) If the problem is at the user level, does it then follow that the solution may be there as well? In a word, yes. It is critical that the effort directed towards computer security reach the user. Solutions must include him.

(U) First, programs should be set up that will make the user aware of the real threat to his system. A basic course on computer security, or a computer security portion of Agency on-board briefings would be helpful, but this would take time to carry out. As an interim solution, computer system security officers could draw up security/threat briefings which would be mandatory for all users of their system. All new users should be given a brief of this sort as a prerequisite to operation.

(U) As a second solution, those individuals who manage resources at the user level (i.e., branch, work center, team) could be given computer security responsibilities. This should not dilute the system security officer's job in any way. If anything, this could extend his effectiveness to the local level where it can do the most good. In this proposal, the local resource manager, acting for the security officer, would be responsible for assuring that security measures are carried out at his level. His proximity to the user can help to eliminate the problems cited earlier. This security task is hardly onerous--after all, he is assuring that already issued security requirements are being met. He represents a form of insurance that we need for computers.

(U) No computer system is absolutely impervious to attack. But it is also true that failure to assure even basic security can circumvent the best computer security measures, through a lack of awareness or responsibility. The commercial computer world is replete with incidents of embezzlement, intrusion, deception, thievery, and sabotage. Can we honestly expect less of a threat to our computers?

DOCID: 4009849

~~(FOUO)~~ This is the time of the year for coming and going, so a word about the distribution of CRYPTOLOG might be useful.

~~(FOUO)~~ Our distribution is to organization and to individuals within the NSA headquarters, and to organization only outside the immediate area of the headquarters. Because of the technical nature of the various articles and items in CRYPTOLOG, it should not go outside the technical community. Even articles that are marked as UNCLASSIFIED should not be taken outside the work area, unless cleared by [redacted] Q44, x3085s or 688-6524 (see CRYPTOLOG, May 1982, page 4, fourth paragraph).

~~(FOUO)~~ When subscribers move to a job outside the headquarters area, we can send the magazine to the organization, but not to the individual. When you return, a phone call or note to [redacted] P14, Room 8A177, x3369s, will get you back on the distribution list by name.

(U) Until now, the month that each CRYPTOLOG issue carries on the cover has been the month we go to press, but this has been confusing to some, because the readers didn't see the issue until the following month. Thus, the April issue didn't appear on your desk (or wherever you get your mail) until May. So, this issue becomes the June-July issue, and future issues will carry the name of the month in which (we hope) they appear.

(U) We have been sending each issue to the printer somewhere around the middle of the month, and the process of printing and distributing has been taking about a month. This means that our deadline for material is roughly the 10th of the month, give or take a day for intervening weekends. If you want to get something into a specific issue, give us a call and let us know how much space to hold for you.

Solution to NSA-Crostic No. 40

"Rules for the Camel Corps,"
[redacted] CRYPTOLOG,
March 1982

"It is frightening to contemplate the amount of time [we] NSA employees spend in meetings. There are staff meetings at all [echelons], meetings to solve a particular problem, club meetings, and even meetings to find reasons for more meetings. 'He's at a meeting' is all too frequently heard on the other end of a phone call."

P.L. 86-36

From: phr at CARONA
Subject: Editorial comment
To: cryptolg at barlc05
cc: phr

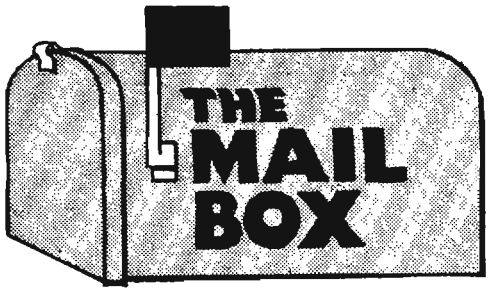
Hi,

(U) Just received my May 1982 issue of Cryptolog and read with suprise the editorial on moving. I would like to share with you my theory on the need to keep moving within the Agency. Clearly, there is at least one too many organizations in the Agency. Therefore, it is imperative to keep one organization in a moving van or stacked in the halls at all times. I am astonished that in all your years at NSA, you have not reached this same logical explanation. NSA is a giant version of one of those puzzles that have 35 numbered sliding pieces with one blank hole. SOMEONE is trying to get all the offices into numeric order but the speed with which we reorganize around here constantly frustrates THEIR efforts and causes the constant moving we MUST ENDURE.

Thank you,

[redacted]
T441, 1181s
phr@carona

P.L. 86-36



EO 1.4.(c)

Dear Editor,

~~(C)~~ I read in the April 1982 issue of CRYPTOLOG in the article on "PERSONAL COMPUTER APPLICATION" by Richard J. Fitzpatrick, P13, about a problem in converting Universal Transverse Mercator (UTM) grid coordinates to latitude and longitude in Geographic grid coordinates. This problem had been solved in June 1970, and three hard copy working aids (WA) were prepared showing machine generated UTM to Geographic coordinate conversions for South Vietnam (B63 WA #22-70, dated 17 July 1970), Cambodia (B63 WA #23-70, dated 17 July 1970), [redacted] These were very popular documents and the working aid for South Vietnam became a "best seller." It was originally published in 290 copies and was provided to traffic analysts and special research analysts at NSA and field stations. As soon as it became available, the response was overwhelmingly favorable and many requests for additional copies came from field stations and NSA elements. It was used daily and, being made of paper, it wore out and needed replacement. By the time I left B63 in March 1972, we had provided approximately 1000 copies of this working aid.

~~(FOUO)~~ This program which converts UTM coordinates to latitude and longitude on a personal computer will be of immense value to all target areas.

[redacted]
B32 5189s

P.L. 86-36

From: phr at CARONA
To: cryptolg at barlc05
cc: phr

(U) Read with interest your article on Shell-Game in the latest issue.... I think the response you get to this feature will overwhelm you!!!

Sincerely yours,
[redacted]
T441 1181s

From: jwh at CARONA
Subject: Games with Shell
To: cryptolg at barlc05

P.L. 86-36

(U) I enjoyed your article on using shells in the recent CRYPTOLOG. I understand [redacted] did as well since he sent you his "who" shell (I have a better one yet). I thought you might be interested in the following loooong shell. [redacted] asked me to produce a program that a user could run against his/her own account to show what files (if any) were open to other users on the system. I decided to do it all in shell in case other users wanted to modify it. Granted it takes some time to run, but it works. There may be some who would want it to do more, however I think it proves that almost anything can be done with shell.

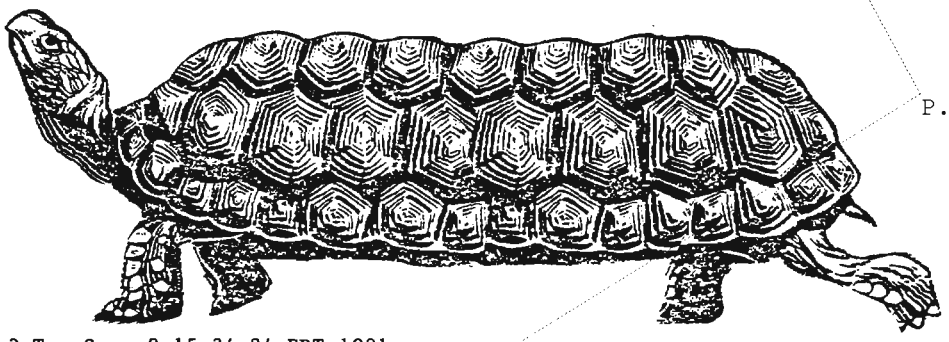
[redacted] T442/x5553s

(Ed note:
See the shell expose beginning on page 27.)

DOCID: 4009849

A LOOOONG SHELL (u)

by [redacted] T4



P.L. 86-36

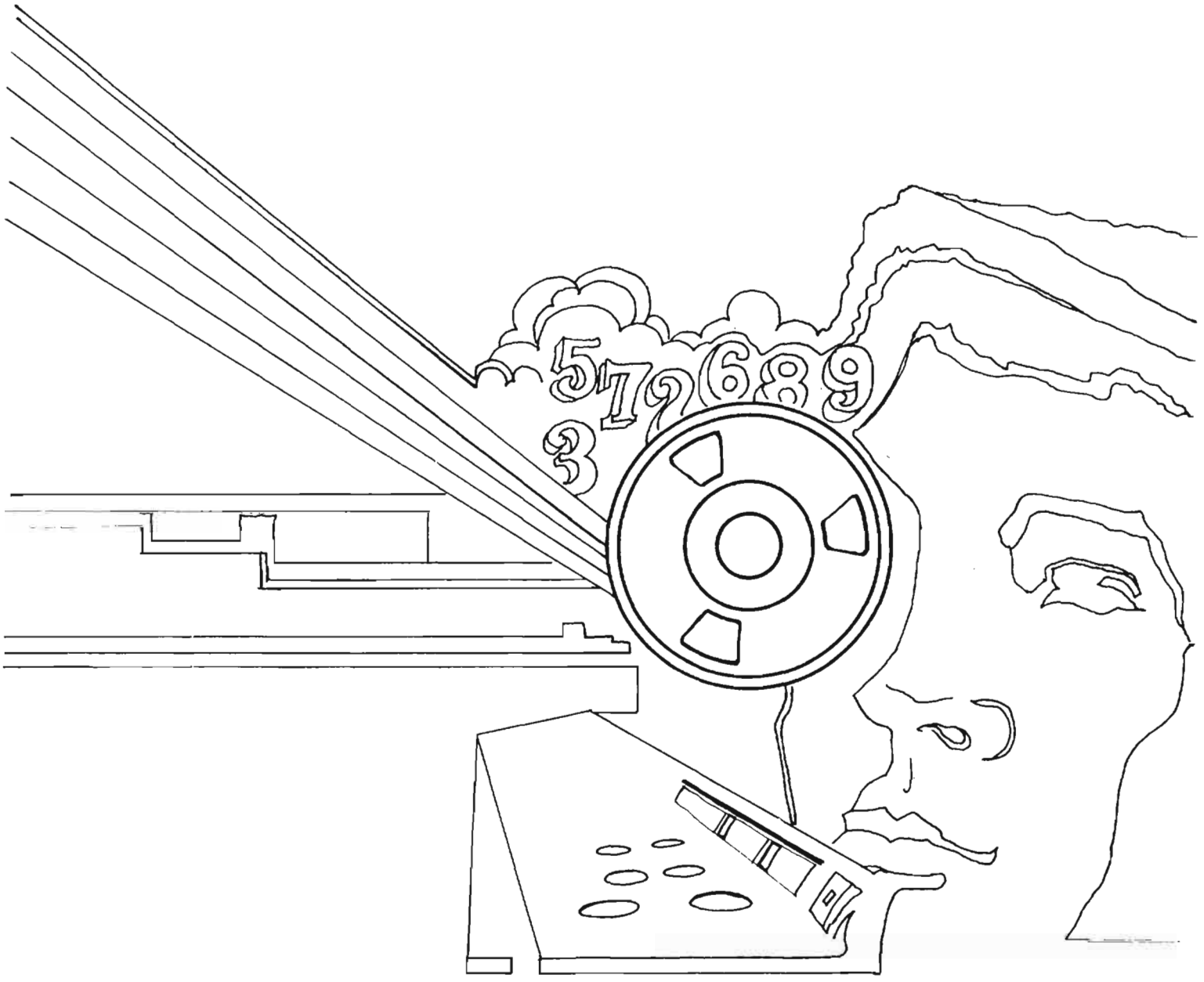
```
echo Expose: v1.3 Tue Sep  8 15:34:24 EDT 1981
: comment - This program was authored by [redacted] at the request of
: comment - Bernard Peters the SENIOR COMPUTER SECURITY COORDINATOR.
: comment - The purpose of the program is to search through a users
: comment - directories and report to the user those files that are
: comment - open for read/write by anyone on the system and other members
: comment - of the users group the program will also inform the user
: comment - who the members of his group are because most dont know.
: comment - This routine tells the user what the program will do.

echo This program will examine your Directory and File systems to identify
echo "          Files which can be READ or WRITTEN by others:"
echo " "

: comment - Check to see if the user wants the file exposed.files removed
: comment - if it already exists. If not and exposed.files exists the
: comment - program will exit and notify the user.

if $1: = -: goto killfile
if -r exposed.files goto anyout

: comment - Routine to get the users current program work directory  name
: comment - and search the users files and directories from the login
: comment - directory of the user.

: killfile
echo Getting your directory information:! >exposef$$5
tr "!" "203" <exposef$$5>exposef$$6
cat exposef$$6;rm exposef$$5 exposef$$6
pwd >exposef$$8
cat exposef$$8 | reform +t8 | rpl "^" "lz -lxp " > exposef$$1
sh exposef$$1 | sort +.41 > exposef$$2
echo "                                        "

: comment - The users files and directory name are now placed into the
: comment - line editor where those files in question are extracted
: comment - and placed in an output file called exposed.files.

ned - exposef$$2
1,$s/  .*:..//g
1,$s/total.*//g
w exposef$$2
```

```
1,$g/exposef/d
$+1a
Files readable by anyone:
.
$1
$d
1,$g/^.......-/d
1,$g/^.......r/1
1i

Files readable by anyone:
-------------------------
.
11
$kg
'gr exposef$$2
$+1a
Files writeable by anyone:
.
$1
$d
'g,$g/^........-/d
'g,$g/^........w/1
'g+1i

Files writeable by anyone:
--------------------------
.
11
$kg
'gr exposef$$2
'g,$g/exposef/d
$+1a
Files readable by anyone in your group:
.
$1
$d
'g,$g/^....-/d
'g,$g/^....r/1
'g+1i

Files readable by anyone in your group:
---------------------------------------
.
11
$kg
'gr exposef$$2
'g,$g/exposef/d
$+1a
Files writeable by anyone in your group:
.
$1
$d
'g,$g/^.....-/d
'g,$g/^.....w/1
'g+1i

Files writeable by anyone in your group:
----------------------------------------
.
w exposed.files
q
echo " "
echo " Change unsatisfactory access codes, use CHMOD        "
echo " " >> exposed.files
```

For those who don't like to type, this shell can be found on CARONA as /u3/jwh/misc/expose

```
echo " Change unsatisfactory access codes, use CHMOD        " >> exposed.files

: comment - This sub routine searches the files etc group to find out
: comment - the login names of the other members of the users group
: comment - and then does a wru against the login to show the user
: comment - the full name of the other members of the users group

echo Determining who your group members are                  ! >exposef$$5
tr "!" "203" <exposef$$5>exposef$$6
cat exposef$$6;rm exposef$$5 exposef$$6
cat exposef$$1 | reform +m12 | rpl "^" "grep " | rpl "/" "" > exposef$$3
ned - exposef$$3
1,1t2
1s/$/,/
2s/$/\
1,2s/$/ /etc/group/g
w
q
sh exposef$$3 > exposef$$4
ned - exposef$$4
$i
T44:,
.
1,$s/.*://g
1,$s/,/ /g
1,$g/^ /d
w
q
cat exposef$$4 | tr " " " 12" > exposef$$10
cat exposef$$10 | rpl "^" "grep " > exposef$$11
ned - exposef$$11
1,$s/$/: /etc/passwd/
w
q
sh exposef$$11 > exposef$$12
ned - exposef$$12
1,$s/:/   /g
1,$v/-/d
w
q
cat exposef$$12 | usort > exposef$$5
echo "                                                "
echo " " >> exposed.files
echo " These are the group members who can access your files:"
echo " These are the group members who can access your files:">> exposed.files
echo " "
echo " " >> exposed.files
cat exposef$$5 | tee exposed.files$$
cat exposed.files$$ >> exposed.files ;rm exposed.files$$
echo " ";echo " "  >> exposed.files ;echo "This list made " >> exposed.files
date >> exposed.files ;echo " "
echo "The list of files accessable by anyone is now in your file: exposed.files"
chmod 600 exposed.files;rm exposef*
exit

: comment - ERROR sub routine to notify the user that the exposed.files
: comment - already exits.

: anyout
echo "EXPOSE ERROR:";bells 1
echo " The File 'exposed.files' already exists -- this file must be"
echo " re-named or removed before -expose- can run"
echo " or run  'expose -'  which ignores the file's existence";bells 1
exit
Tue Sep  8 15:34:24 EDT 1981
```

Pl-Jul 82-S3-18530


5 7 9 6 8 9
3

DOCID: 4009848

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MAY 1982

P.L. 86-36

THE NSA INFORMATION DESK: "NO COMMENT" (U) ..... [redacted] 1
THE MICRO REVOLUTION: ARTHUR YOUNG STUDY (U) 5
COMMENT (U) ..... [redacted] 9
HUMAN FACTORS: DATA GATHERING (U) ..... [redacted] 11
HOW DO WE SPEND OUR DAY? (U) ..... [redacted] 16
FULL OR BROAD SPECTRUM LIGHTING (U) ..... [redacted] 14
CRYPTOLOG NUMBERING (U) 14
TRUE BASE: TWO TALES (U) ..... [redacted] 15
MAILBOX (U) 21
PUZZLE (U) ..... David H. Williams 22
A HISTORY LESSON (U) ..... [redacted] 24
IS THERE AN OLD CROW IN YOUR FUTURE? (U) ..... [redacted] 28
BUST ANSWER (U) ..... [redacted] 29

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 10 May 2012~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009848

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. IX, No. 5 MAY 1982

PUBLISHER [redacted]

BOARD OF EDITORS

Editor-in-Chief. [redacted] (8322/7119s)
Production..... [redacted] (3369s)

Collection..... [redacted] (8555s)
Cryptanalysis..... [redacted] (5311s)
Cryptolinguistics..... [redacted] (5981s)
Information Science. [redacted] (3034s)
Language..... [redacted] (8161s)
Machine Support. [redacted] (5084s)
Mathematics..... [redacted] (8518s)
Puzzles.....David H. Williams (1103s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Don Taurone (3573s)

For subscriptions
send name and organization

to: CRYPTOLOG, P1
or call [redacted] 3369s

To submit articles or letters
via PLATFORM mail, send to

cryptolg at barlcØ5
(note: no 'O' in 'log')

Editorial

Many years ago, when the Pennsylvania Turnpike first opened, there weren't any other "super highways" as we now know them, and I was fascinated by how much easier and faster this new road was than any other route through the mountains. But after a while, as I travelled that road, it seemed as though I always managed to encounter at least two tie-ups, caused by repair crews whose work closed one lane or otherwise slowed the flow for miles.

One day, it occurred to me that these repair crews were <u>always</u> there, somewhere. After all, as the old punchline goes: everybody's gotta be somewhere. And where else would road repair crews be?

It seems to me that there may well be a similar principle working around here, except that it involves moving. No matter where I look, somebody seems to be moving. A lot of people seem to be "movers," involved in the mechanics of moving. Is there a PERT chart somewhere, with planners pondering the question of what to with "the movers" during that empty period in FY88? After all, every mover has to be somewhere.

In the good old days, when we got to the new location after a move, we just took out our pencils, looked for a good place to put the pencil sharpener, sat down, and started to work. But now that everything is inside a computer somewhere, it doesn't seem to work quite that way. I wonder what it costs to move, in terms of lost hours, equipment repair, delayed reconnection of terminals, etc.

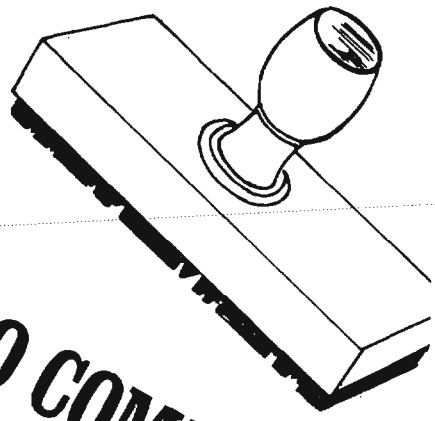
Maybe someone has all this under control, and from his vantage point, it all looks very orderly and smooth.

WES

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

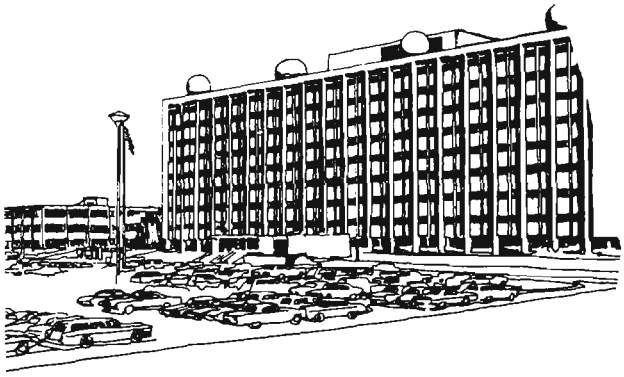
The NSA Information Desk:



NO COMMENT (U)

by [redacted] Q44

P.L. 86-36



Have you ever wondered what working for the NSA Information Affairs Division is like? How can there be such an organization when, normally, ~~(FOUO)~~ the only answer NSA gives to questions from the outside world is "No Comment"? Do people like Jack Anderson, David Kahn, and Mike Wallace ever really call NSA? Do other people call and say they are Richard Helms?

~~(FOUO)~~ Working on the NSA Information desk has been most interesting, sometimes frantic and hectic, usually busy, but seldom dull. I hope you will enjoy reading about some of the routine and exciting things that have happened over the past eleven years.

~~(FOUO)~~ Since many of you may not be aware that NSA has an Information Affairs Division, I'd like to begin with a brief history of how it all got started. In November 1965 NSA Director, LtGen Marshall Carter, USA, named [redacted] as "NSA Liaison Officer to the Assistant Secretary of Defense for Public Affairs." Initially, this was a part-time role; however, in December 1966 the position became full-time and the title changed to "Public Information Officer." In July 1967 the position was physically and administratively moved to the Director's Executive Office, and in July 1973 the title was officially changed to "Public Affairs Officer."

~~(FOUO)~~ [redacted] who was this Agency's first and only "Public Affairs Officer," selected me as his assistant in June 1971 to succeed [redacted] who wanted to work part-time. At that time, I was working in the Counterintelligence Division of the Office of Security. In June 1973 a clerical assistant billet was added, and in August 1973 the Public Affairs Office (PAO) became D3 and relocated to the fifth floor.

~~(FOUO)~~ In January 1974 a decision was made by the Management Council to disestablish the PAO as a separate activity and to place the responsibility with the Chief, D41 (Policy Staff). As a result of this decision, Mr. [redacted] was given an assignment in the M organization, the clerical billet went to the Executive for Staff Services, and I remained with the PAO function. It may seem that the Public Affairs Office had a short life; however, in spite of losing the title, the function was neatly tucked away within the Policy Staff, and today the Information desk is alive and well.

~~(FOUO)~~ So much for history. You're probably still wondering what is really accomplished here in the Information Affairs Division. As I think back, I have often wondered if [redacted] hired me because he knew I could honestly respond to media calls with an "I don't know" or "No comment." Never having been exposed to the Operations or COMSEC functions has been a blessing on many occasions. More on telephone calls later.

P.L. 86-36

DOCID: 4009848

~~(FOUO)~~ The Information Affairs Division supports the Director, Deputy Director, and senior officials. One of the first services initiated was the news clipping service. In the beginning (1972), with limited staff (me) and reproduction facilities, the news clippings were provided once a day to DIR, D/DIR, and DC/CSS. Each day five newspapers (N.Y. Times, Wall Street Journal, Washington Post, Baltimore Sun, and Washington Star) were reviewed and items of interest clipped and formed into a mini-newspaper. In addition, the daily DoD Current News and CIA news clips were reviewed, as well as Time, Newsweek, U.S. News and World Report, Federal Times, and others, on a weekly basis. In recent years, additional requests have been received for this service and we are now able, with increased staff and a better repro machine, to provide copies twice each day to DIR, D/DIR, Chief of Staff, and all key component chiefs.

TELEPHONE CALLS

~~(FOUO)~~ Calls from the media are received in the Information Affairs Division and, depending on the requests, our responses vary. Camera crews from various media have been authorized to come and take pictures of the NSA buildings. We make the appointments and arrange for the crews to be met by a representative of the Office of Security who accompanies them as they photograph. Some callers ask for interviews with the Director or other seniors. Generally, because of our desire to maintain a low profile, interviews are not granted; however, Admiral Inman made a few exceptions. One such interview was given to Deborah Shapley of Science Magazine on the subject of public cryptography.

~~(FOUO)~~ Several years ago, I was surprised indeed to answer a call from Mike Wallace who was asking permission to photograph the Enigma machine for a segment on intelligence which was being prepared for "60 Minutes." Arrangements were made to accommodate his request.

~~(FOUO)~~ Jack Anderson's staff has called on several occasions asking for comments on subjects relevant to NSA. Also, ABC, NBC, and CBS have made frequent calls asking NSA to confirm stories about the Agency when we happened to be mentioned in the news. It is always amusing when they preface their call with "I am sure you won't make any comments, but...." Usually they are correct.

~~(FOUO)~~ Back in 1979 I received a call from a Baltimore Sun reporter who had learned that NSA was seeking to acquire a couple of buildings at Aberdeen Proving Grounds for "warehousing." She wanted to know precisely what the storage space would be used for and, while I really didn't know, I told her it would probably be used for storing furniture, old records, etc. She asked more questions and became a little "pushy" so I commented that "I'd rather not discuss it further, because it was really a nothing move anyway." When I came to work the next morning and found that she had quoted me verbatim, I was a little shook until I heard [redacted] laughing about the "nothing move." P.L. 86-36

~~(FOUO)~~ Last year some information was provided to the Baltimore Sun in response to an inquiry they had made concerning our recruiting efforts. The Director approved a release stating that we would be hiring over 1,000 new employees primarily with engineering, language, and computer skills. The publicity was good but the Recruiting Office was literally exhausted from answering over 500 calls in a matter of a few days.

~~(FOUO)~~ Of the 75-80 media calls that are received during a year, most are legitimate. However, we have our share of "crank" calls. There are a few that have made good "in house" stories for many years.

~~(FOUO)~~ I recall a man who insisted on speaking with the Director (Adm Gayler) who was then away on TDY. He then asked for Dr. Tordella by name and stated that it was urgent that he speak with him--that the information he had was critical and timing was of utmost urgency. I sensed that he was "disoriented" but not being sure what to do, I called Security. This man made about ten phone calls to NSA and actually flew down to BWI, rented a car, and came to NSA. He was interviewed by a Security Officer. The following weekend, this individual was arrested in New York and held under $500,000 bond on charges of paying $1,000 to a secret service undercover agent to assassinate President Nixon.

~~(FOUO)~~ Then there was the caller from North Carolina who called on successive days and said that he was "hooked up to the NSA computers." I tried to explain to him that this would not be possible, but he was very persistent. Finally, on about the third day, I told him that he was no longer hooked up--that everything on this end had been unhooked. I haven't heard from him again.

~~(FOUO)~~ Another very business-like caller

identified himself as Richard Helms. He was calling from New York and stated that he was working on a special NSA project. He needed some money and wanted it sent to him as soon as possible--he even gave what he claimed to be an NSA account number. Thinking the call to be legitimate, the respondent (not me this time) dashed into the Director's office and related the story, only to return with a red face. The caller was really an imposter.

~~(FOUO)~~ One disgruntled citizen called and asked some specific questions about NSA. I explained to him that the information was not releasable, which made him angry. He said he was a taxpayer and had a right to know. Just before he realized his efforts were fruitless, he said he intended to make a citizen's arrest. Sometimes having a name like [redacted] isn't all bad.

~~(FOUO)~~ All calls that come to the switchboard for the Director are first screened by the Information desk. Some of the callers are very insistent; however, after a few questions it usually turns out that they simply need the Agency address, or have been turned down for a position and want to know why. Occasionally, the caller will be a Congressional or White House staffer and, of course, these calls are immediately transferred to DIR's office. On the other end of the spectrum, an angry man called recently. It seems he had been selling eggs at one of the gatehouses and that the FPS had asked him to leave. He asked about the people who sell flowers and was told that they were the exception to the rule. His last statement, after expounding upon his rights, was "If they can sell their flowers, I can sell my eggs." I suggested that he write a letter of request, but to date we haven't heard from him.

DO WE GET ANY 'CRANK' LETTERS?

~~(FOUO)~~ Do we get "crank" letters! Many are received each year and, again, depending on what they say (if that can be determined), we either forward the letter to Security, answer it ourselves, or simply file it. Some are amusing, others aren't.

~~(FOUO)~~ One of the most amusing letters was from an individual who identified herself as the "Commanding General United States Marine Corps" and she had the business cards to prove it. She sent a mailgram (three pages) which expounded on her background and told how, during World War II, she had made secret trips to the Kremlin and to Hitler's headquarters for President Roosevelt. Her photograph later appeared in the 3 March 1976 issue of the Baltimore Sun, as one of the "fringe candidates" who had requested that her name be placed on the ballot in the Maryland primary election as a presidential candidate.

~~(FOUO)~~ Another classic letter was from a lady in Denver who claimed that she hadn't received her share of the Rockefeller estate, which she believed to be at least $150 million. She later made a request under the Freedom of Information Act and, in our response, we advised her of our fee-charging policy. We asked her to pay half of the fee prior to initiating the search. The next thing we knew, she was in the lobby at Gatehouse 1, waiting to pick up records that we might have. She called our office, and we just told her again that we couldn't assist her until we received a certified check--which we never got.

P.L. 86-36

SOLUTION TO NSA-CROSTIC No. 39

"Thou Swell, Thou Witty," by D. Hart

"I know Larry had tremendous love and respect for Richard Rodgers. I believe that the love was mutual. After all, it is not remarkable that they split up after twenty odd years, but that they endured and survived during those years."

~~(FOUO)~~ You've read in the NSA Newsletter about some individuals seeing some mice in various areas. Well, I doubt that anyone has ever seen a "holographic mouse" except our friend in Florida who has sent several letters. She writes that "whoever beamed a holographic mouse out of the glass jar on the kitchen counter across the sink and over to the refrigerator got it almost perfect." She contends that someone is playing pranks on her and has been since she applied for work here. Also, she has been experiencing ear beepings, and she has been used in the development of an early warning system for VIPs which involves ear buzzing and beeping signals that can be accompanied by physical retaliation against attackers or even the VIP if he/she doesn't follow orders.

~~(FOUO)~~ We also get some "not-so-crank" letters from amateur cryptographers who send in their own designed cryptosystems for evaluation. One individual attached part of his system in a sealed envelope with a statement which read:

> "Before opening the attached envelope, let it be agreed that I have not relinquished my rights to this system. If this stipulation cannot be met, please return it to me by Registered mail."

Needless to say, the package was wrapped, addressed, and returned by Registered mail.

~~(FOUO)~~ Another man called one day to inquire about a letter he had written. He didn't want to give me his name but finally consented after I convinced him that it would be impossible to search for his letter if I didn't have a name. We couldn't find the letter, so he mailed us another copy. The letter was sent Registered mail, with no return address. It wasn't signed, but attached to the letter in a sealed envelope marked "Confidential" was his name and address.

~~(FOUO)~~ In addition to preparing news items and responding to letters and telephone calls, the Information Affairs Division approves the release of all unclassified information in accordance with NSA/CSS Regulation 10-11. This includes all résumés, reports of co-op students, newsletters (including "unclassified" CRYPTOLOG articles), talks to be given at seminars, etc. To give you an idea of the volume, in 1981 approximately 480 requests were processed.

~~(FOUO)~~ Today, the Information Affairs Division is part of the Policy Staff (Q4). We have a staff of six people and work as a team processing Freedom of Information Act (FOI) and Privacy Act (PA) requests as well as manning the Information desk.

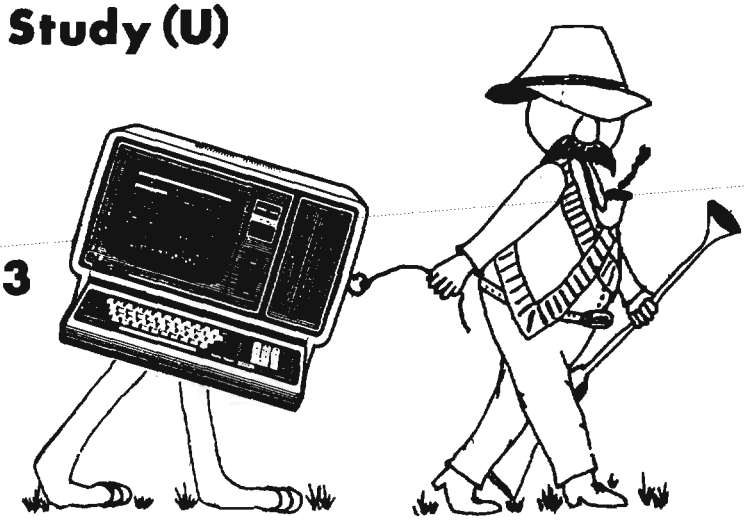
~~(FOUO)~~ Many times, NSA employees have assisted us by bringing to our attention the fact that NSA has been mentioned on the news or that they have read an article where the Agency has been mentioned. We appreciate this assistance because it enables us to keep the senior-level people better advised. Occasionally, an NSAer has been called by a reporter who has acquired the name from some source. When this happens, the only recourse is to refer the call to the Information Affairs Division, and we will see that the proper response is made. The telephone number is 688-6524. We are here to support all of NSA and are happy to assist when we can.

DOCID: 4009848

The MICRO Revolution: Arthur Young Study (U)

Comment by [redacted] P13

P.L. 86-36



Recently the Directorate of Data Automation of the Department of Defense initiated a study with the consulting firm of Arthur Young and Company to explore the potential impact of low cost computing on the Department of Defense (DoD). This article presents excerpts from the Executive Summary of the study issued by Arthur Young and Company, followed by my comments.

"In the last several years rapid advances have been made in almost every area of information technology, and these trends have far-reaching implications for the management of this technology in the Department of Defense.... The Reagan administration, the Department of Defense and military strategists throughout the armed services are grappling with the problem of identifying the most efficient and effective applications for scarce resources.... But, because of technological advances, some investments which appear to be costly are, in fact, cost-effective. Understanding when an investment is justified is an intricate process requiring both technical and management expertise.... The Department of Defense has in the past assumed a leadership role in responding to the demand for information. DoD has acquired the most efficient information processing technology available and has developed the professional staff essential to maintain this technological capability. Information processing technology, however, is the most rapidly changing industry in the market today. The cost of logic circuits continues to drop approximately twenty to thirty percent per year, while the cost of solid state memory decreases approximately thirty to forty percent. New capabilities at reduced cost are being announced almost every day.... The current options available for processing information are widely varied. They include new equipment, new operating and application software, and new management tools.... The options are so varied, and their potential management, technical, organizational and personnel impacts are so extensive, that they may obscure the ultimate goal of identifying the information processing approach that will lead to the lowest cost for groups within DoD and for the department as a whole.... DoD believes that of the emerging technologies, the low cost computing systems available today and in the future will have the strongest impact on DoD of all ADP technology trends.... At the summary level the most important trends are as follows:

- ☆ Hardware capabilities are increasing significantly with improved processing speed and reliability. For example, memory size is increasing while costs drop at the rate of thirty to sixty percent per year. Storage capacities are also increasing rapidly.

- ☆ The quality of printers and of a variety of input/output devices is increasing substantially, while the cost is decreasing.

DOCID: 4009848

- Improved quality of work from data entry activities to reduced effort and time required to generate and review documents, and finally to more rapid and accurate decision making.

- More timely response to the information processing needs of users throughout DoD.

- Cost savings through replacement or enhancement of obsolescent information processing equipment.

- Cost savings through automation of labor-intensive, and therefore increasingly expensive, manual procedures in areas where automated support has not been cost-effective in the past."

☆ Advances in telecommunications technology are making local networks attractive.

☆ The major improvements in color, graphics, and end-user orientation are accelerating the expansion of computer applications.

☆ High quality software packages are widely available for applications from general accounting and word processing through individual management decision support tools.

☆ Most importantly, the large base of equipment sold is creating compelling economic incentives for vendors in the software market. The number of desktop microcomputers installed is projected to grow from approximately one million in 1981 to five million by 1985. The incentives in the microcomputer software industry will keep pace with this unusual growth."

"These opportunities support major objectives of DoD and of the current administrations: to increase productivity while cutting or containing costs. The opportunities encompass an additional benefit: the integration of state-of-the-art information processing technology will increase the attractiveness of DoD for the most talented managers and ADP professionals entering the job market...."

"During our review of technology trends, we determined that the computer equipment and associated software available at the lowest cost, the microcomputer systems, are generating a vast new market among users who have little or no ADP technical background. Microcomputers, offered at costs well below the delegated procurement authority in DoD, are readily available to this market group. These new users can benefit from the technical expertise and management perspective of ADP professionals if an effort is made by DoD to anticipate problems and highlight opportunities.

"While the technological trends are important for the ADP professional to monitor, it is the management implications of these trends that are of greatest significance to DoD executives and policymakers.... The changing technology has ... created both new opportunities and new issues that demand the attention of senior managment.... The opportunities presented by changes in information processing technology may be summarized as follows:

A variety of interrelated factors contribute to our expectation of widespread DoD acquisition and use of microcomputers. Among the most significant of these factors are the following:

☐ User frustration with the largely centralized ADP technology and services provided within DoD is caused by time delays both in processing information and responding to new or changed application

DOCID: 4009848

requirements. This frustration is intensified by the inability of users to customize programs to their local needs and the difficulty they experience in attempting to communicate their needs to data processing personnel.

- This problem is further heightened by the high level of use and old age of the average DoD computer equipment. The capabilities and services provided by this old equipment fall far short of the capabilities found on many of today's low cost computers....

- The low cost computing technologies, particularly microcomputers, are therefore especially attractive to users who see them as a means to reduce their problems with the centralized ADP support found in the government today. A parallel benefit is offered to ADP professionals who have been struggling to meet demand with a perpetual shortage of qualified programmers. The user orientation of the microcomputers may help to mitigate the projected major personnel shortage in DoD.

- During the next few years, budgetary limitations and personnel constraints or cutbacks will become a reality for DoD. Managers will be expected to face the challenge of decreased resources for day-to-day operations and staff functions.

- Low cost computing technologies offer significant opportunities for enhancing productivity to meet this challenge. Microcomputers, especially, are viewed as a means to eliminate a wide variety of time consuming manual procedures and inefficient automated procedures.

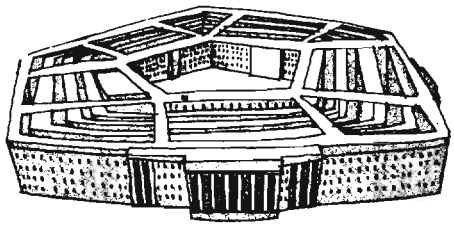
- .... Because of the relatively small investment of resources required for the initial purchase of a microcomputer system, the amount of time required to repay the investment in terms of personnel hours saved is small. As technology costs decrease and personnel costs increase, investments in low cost technology become increasingly attractive.

- Contributing to DoD users' frustration with existing information processing technology and services is their perception of the high quality and powerful capability available to them at a low cost in systems that have been designed especially for operation by end-users. Microcomputer technology vendors have identified these users as a new and potentially profitable market segment. They have designed both their systems and their marketing techniques to appeal to non-technical users, as well as ADP professionals. In doing so, they have developed systems which require little or no interaction with computer programmers and operators.

- .... The microcomputers, furthermore, are increasingly reliable, well-documented and supported. The combination of high quality and user-friendly orientation may be expected to add to the attraction of low cost computing technology within DoD for managers, military analysts and administrative personnel.

- DoD should anticipate the impacts of a combination of user frustration and the availability of low cost alternatives that appear to be ideal solutions to users who, in the past, have been unaware of many ADP options.

- Today's users are more receptive to computer technology than they have been in the past.... Along with even a rudimentary understanding of what low cost computing technology can do for individual users comes acceptance and a feeling of control. Familiarity, acceptance and control by the end-user will encourage widespread acquisition within DoD."



"We anticipate that the combined impact of these four interrelated factors will be widespread acquisition and use of microcomputers within DoD. Along with opportunities that these low cost systems present, however, come some critical issues which DoD management needs to address."

".... The most critical issues are those that have not been encountered before in managing ADP resources. Also critical are the more familiar issues which have taken on a new slant with the changes in technology.... Specifically, the issues of greatest concern for DoD senior management are:

1. Control of Acquisition and Use

- The issue of control begins with the fundamental question of whether control over the acquisition and use of microcomputers systems is desirable, or whether it will serve only to obstruct the initiative of managers to find innovative, cost-effective applications for the new technology. If control is desirable, the most appropriate level for control needs to be identified.

- DoD has, thus far, consciously proceeded without formal, centralized control over low cost computers. This policy has been adopted to encourage experimentation, which will serve both to clarify the real potential of microcomputers and to highlight potential pitfalls.

- .... Ultimately, some degree of control is necessary to ensure compatibility of resources and to promote sharing through networking or integration with mainframe systems. Control will also be necessary to ensure compliance with data security and privacy laws and with applicable federal procurement regulations and Public Law 96.511.

2. The role of microcomputers in relation to mainframes and minicomputers

- ADP professionals in DoD will need to develop expertise in the process of identifying which functions are most appropriately handled on a mainframe, a minicomputer or a microcomputer. Microcomputers can be used as stand-alone processors for applications with limited input/output device requirements and limited volume processing needs. They can be used as remote terminals in a dial up mode with a mainframe to provide decentralized access to centralized systems. Microcomputers can be used in small clusters supported by a mainframe, or in super clusters where portions of the processing burden are down-loaded to remote processors connected to the mainframe.

- The clarification of the most effective roles for microcomputers in relation to mainframes and minicomputers will require extensive ADP technical expertise. It will also require a senior management perspective on organizational and personnel issues within DoD.

3. Application Areas and Sequence for Introduction

- The areas where microcomputers can be used in DoD are numerous. They include enhancement of traditional data or word processing functions and development of new applications to support individuals directly in management or decision making activities.

DOCID: 4009848

- The management issue which results is in identifying where the systems can be used most effectively.

4. Pace for Introduction and Integration

- A key concern for DoD management is the pace at which low cost systems are introduced. A rapid pace involving a large number of applications over a broad range of user groups may cause failures and widespread disillusionment and implementation of incompatible systems. On the other hand, an extremely slow pace will cause dissatisfaction among users who are eager to install the systems immediately and a delay in achieving higher degrees of cost-effectiveness.

- .... The careful selection of pilot sites, where strong and technically capable proponents of microcomputers are available to lead the implementation effort, may prove most effective.

5. Roles and Responsibilities of Users, ADP and Word Processing Professionals

- Perhaps the most demanding management issue presented by microcomputers is the development of new roles and responsibilities. The traditional division of duties will continue to change with the introduction of this new technology. Users will work more directly with computers. ADP professionals may find significant roles in decentralized support activities spread throughout the user community.... There is a need initially to encourage and eventually to require the acquisition of appropriate microcomputer expertise among users, ADP and WP professionals.

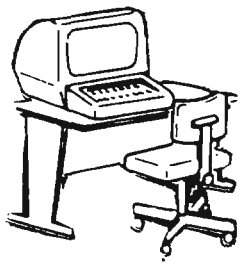
6. Support Structure

- The installation of a significant number of microcomputer systems raises several important management issues for DoD in the area of support structures. The primary question to be answered is, how will the systems be acquired, maintained, and operated.

- Currently, low cost computers are generally being acquired individually or in small numbers. If DoD continues this process, the department faces the potential problem of acquiring large numbers of incompatible systems--causing interfacing problems and increasing the cost of training. At issue is the question of whether a central acquisition support structure could acquire these units at volume discounts, while achieving increased compatibility. However, a concern is raised that this support structure may slow down the acquisition process and possibly lock DoD into older technology.

- The support function also extends to the availability of software packages which are being purchased individually in increasing numbers. An issue arises concerning whether DoD should enter into multi-site package arrangements or whether it should develop and distribute its own software packages."

"The preliminary analysis of low cost computing trends, impacts and implications has identified some major opportunities for DoD. It has, in addition, made it clear that several significant management issues need to be addressed in order to take full advantage of the opportunities."



THE MICRO REVOLUTION: A COMMENT

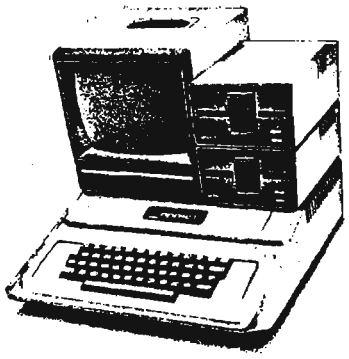
by [redacted] P13

P.L. 86-36

For the past several years P13 has been experimenting with personal computers for cryptanalytic applications within DDO. As a DDO technical staff, our efforts have been directed toward helping the analyst who is still doing the great bulk of his work by hand.

In our efforts to investigate the use of this new technology for DDO applications, we have encountered some of the possible scenarios suggested by the Arthur Young study. Users tend to be frustrated by the response that they receive from the ADP service organizations and are therefore quick to pick up on the possibilities offered to them by the personal computer. It is friendly and they have immediate control over it, which leads to great acceptance by even the most unsophisticated (in terms of ADP) user. We can see, therefore, that the potential problems and pitfalls which the Arthur Young study refers to, as well as the many opportunities, are real and must be dealt with.

As a result of our experiences in the personal computer arena, I believe that we are in the middle of a processing revolution which will greatly enhance the capabilities of all analysts, especially those doing labor-intensive tasks. Also, there are opportunities offered to the user of a personal computer in other areas, such as word processing, data base systems, and information management.



Since the inception of our efforts to investigate the potential uses of personal computers for cryptanalytic applications in DDO, we have become very aware of the large variety (which seems to grow larger every day) of personal computer hardware and software which is available from commercial sources today. In attempting to acquire some of these tools for the DDO analyst, we have encountered some of the problems which the Arthur Young report alludes to, including the necessary acquisition lead time--which leads to user frustration and to the procurement of obsolete technology--and the service problems which occur due to the diversity of equipment.

Nonetheless, we in P13 agree wholeheartedly with the Arthur Young study's conclusions. Personal computers are here to stay, and they offer DDO and NSA managers many unique opportunities. However, they also present many new managerial problems. At the present time I believe that the issue which requires immediate attention from NSA management is:

> How can personal computers be acquired, maintained, and operated without stifling the initiative and innovativeness of local managers?

I know that some of the problems foreseen by the Arthur Young study exist in NSA today. One of the many unanswered questions is how are we going to deal with them? I don't have answers to the questions raised nor am I sure that these are the only possible questions. But I am sure that NSA must deal with them soon.

As I see it, the major questions generated by the Arthur Young study are:

- what effect will this DoD concern for microcomputers and their use have on NSA, and
- how will NSA, and in particular DDO, deal with the revolution that has already begun?

Copies of the Executive Summary of the Arthur Young study are available from P13. A copy of the full report is also available. To obtain any of this information or to discuss personal computers and their use in further detail, please contact me.

DOCID: 4009848

HUMAN FACTORS:

☐ Data Gathering (U)
☐ How Do We Spend Our Work Day? (U)

by [redacted] P13 P.L. 86-36

These articles were written a couple of years ago, after I returned from taking the Human Factors Summer Course at the University of Michigan. Since that time, I have been involved in a human factors experiment concerned with improvements to Transcribers' working environment, in the course of which extensive use was made of another electronic data entry device, the KAMAN Scientific Corp ADES "Electronic Clipboard." I hope to prepare a paper in the near future, describing the use made of this device, and the results obtained.

(from Human Factors Newsletter 1-79)

For me, the most valuable feature of the human factors course (University of Michigan) was the coverage of methods for gathering and analyzing data, and design of human factors experiments. Paul Green, of the Highway Safety Research Institute at Michigan, gave a very interesting lecture and demonstration of methods for gathering data. This seems to me to be a crucial part of the problem we face in putting human factors concepts to work in our operations: how can we study the users, their tasks, and the work environment? How can we get the kind of hard data we need to design a better system for the user? Dr. Green introduced us to some "classic" industrial techniques, and gave us some "hands-on" experience in making a Time Study using a stopwatch and manual recording form. He also demonstrated the use of hand-held electronic recorders which can be used to time and record observations, and then can be plugged in to a computer terminal or modem to transmit the data to a computer where software provided by the manufacturer analyzes it and sends back a display of results. The demo he gave us used a DATAMYTE electronic data collector (ELECTRO-GENERAL, Minnetonka, Mich.) and data was transmitted and analyzed via a TI "Silent 700" portable terminal.

A classic Time Study was defined as follows:

> "the analysis of a job for the purpose of determining the time it should take a qualified person, working at normal pace, to do the job, using a definite and prescribed method. This time is called the standard time for the operation. Standard times are developed by adding up the times for each element of the work cycle."

Dr. Green served as our Subject, while we actually tried to do a simple Time Study of a task involving inserting 5 screws into holes and screwing them home with a simple screwdriver. We were issued stopwatches, clipboards equipped with a little rack into which the stopwatch fitted, and a recording form. Then we determined the starting and stopping "rules" for each "element" within the work cycle. This involved finding visible benchmarks (e.g., "hand touches the first screw in the box," "puts screwdriver down on table,"

DOCID: 4009848

In this kind of study, the observer marks down which of a set of predetermined activities the worker or machine is performing at some points during the total time he is observing (e.g., every 10 seconds) over a considerable length of time (several days or weeks). There are a number of automated aids for this kind of study also, for example, a beeper which signals the sampling times to the observer through an earphone, and a hand-held electronic recorder. A large number of computer packages have been developed for industrial applications, to look up standard descriptions of tasks and the standard work times established for them, and compute total times for a work cycle. These methods can be used for abstract modelling and simulation of work cycles before the actual tools or procedures have been implemented, basing their results on estimates from the standard values in the data bases available to the packages. The systems include standard times for such actions as "reach," "turn," "position," "move," etc., eye-movement times, and body, foot, and leg movement times. Some systems are specialized for office tasks and clerical tasks (these might be more relevant to many of our contexts than the industrial assembly-line kinds of tasks involved in most of the systems).

etc.) which an observer could reliably identify as he watched the worker. The actual observation was surprisingly difficult (the stopwatch took some practice in handling, and my reaction times were appallingly slow!). The advantages of the automated recording devices became abundantly clear in a hurry. In a real-life study, observers undergo extensive training with videotapes of workers performing an operation, until all observers can recognize and record all elements of the cycle to a predetermined degree of accuracy and agreement. A subjective decision has to be made about the pace at which a worker is performing the operation at a given time. Is it his normal pace? How does it compare to the usual pace of most workers doing the job? This obviously also requires a trained observer.

Another classic kind of data gathering procedure Dr. Green described was the Activity Sampling, or Work Sampling Study. This was defined as follows:

> "The most global examination of what one or several individuals and/or machines are doing at many predetermined points in time for the purpose of finding out how time is allocated.... In its simplest form one records if the object observed is 'busy'."

I learned some interesting things about the real-life application of data-gathering techniques from a fellow-student, a management analyst from HEW, involved in design of a major interactive terminal system for the Social Security Administration. He described the method they had used to study the work of the intended users of the system, in order to provide a basis for design of the user dialog and functions the system was to perform. They were able to convince their top managers to release ten expert workers from different regions of the US, and assign them for several months full-time to work with the design team. The design staff taught these experts how to make flow charts, supplied them with manuals and all other information support files they normally used in their work, and asked them to create detailed flow charts of how they did their jobs. The procedures differed somewhat in different regions due to State laws, and the experts resolved or combined their differing segments of flow charts, working together. Unfortunately, this rather expensive description soon became out of date, and the design team is now faced with the task of revising it. Since top management is no longer willing to release experts from their regular duties and assign them to the team even temporarily, they will have to "go back to interviews and questionnaires" to get the needed data.

DOCID: 4009848

HOW DO WE SPEND OUR WORK DAY?
(from Human Factors Newsletter 1-80)

In looking over my notes from the Human Factors Engineering Summer Course at the University of Michigan, I came across another bit of data which I thought might be of interest to you. It was part of a handout distributed to students by John D. Gould of the IBM T.J. Watson Research Center, Yorktown Heights, for his lectures on "Man-Computer Interfaces for Information Systems." His lectures were, in my opinion, among the best of the course. He presented a great deal of recent findings from his own research, and also provided us with excellent, up-to-date bibliographies, among them an extensive "Bibliography of Behavioral Aspects of On-Line Computer Programming." Any reader who would like copies of these can get them from me by calling me on x8845 or sending me a note.

Gould described the results of a study of white-collar workers in offices. This study was an "Activity Sampling" study, using a data-gathering method I mentioned above. Trained observers recorded which one of a carefully pre-selected and defined list of activities office workers were engaged in at times sampled throughout the work day. Separate studies were made of secretaries on the one hand and "principals" (managers, professionals, technicians) on the other. While there have been many such studies of industrial workers, little is known about how office workers spend their working hours. I found the results of this study quite surprising. If anyone had asked me what I thought an office worker (non-secretary) did in a work day, I would have said something like this: "If he/she is a manager, he/she works at a desk writing and reading, attends a lot of meetings, and talks a lot on the phone. But if he/she is not a manager, most of the day is probably spent sitting at the desk reading or writing, with a few phone calls." Here is what the IBM researchers found (for "principals" only; unfortunately Dr. Gould did not include the findings for secretaries, which I would also like to see.):

How Principals Spend Their Time

- ☐ They are inside the office building only 75% of the time.
- ☐ They are in their work area only 50% of the time.
- ☐ They spend a surprisingly large portion of their time "communicating" as opposed to reading or writing, and an even more surprising proportion of their communicating is face-to-face talking.
  - All Communicating 40-50% of work time
    - face-to-face 30-35%
    - telephone 10-15%
  - Reading 10-15%
  - Writing 10-15%
- ☐ They communicate more by conversation than by formal memos or correspondence, and they engage in many relatively brief communications. Communication is relatively unstructured, non-repetitive, and involves constantly-changing content.
- ☐ Their day comprises an "unrelenting stream of varied activities," with an average of 16 interruptions of an ongoing activity in a day. Most meetings are unscheduled. Workers typically "juggle several tasks at once," and "have no idle time."

It is hard to estimate how similar these patterns are to the work activities of Agency professionals. It is my impression that the daily routine of many NSA "principals" (non-clerical personnel) involves far more valid, work-related face-to-face communication and walking around than we (or our managers) realize. I hope that we will soon have an opportunity to do some scientific activity sampling studies in NSA work areas, and gain some understanding of how our people spend their work hours. It is interesting to speculate about the effects of certain technological changes on these work patterns. How will a worker who is used to doing all that wandering around, impromptu meeting, juggling interrupts, and face-to-face talking adapt to activities centered around a computer terminal? Or a personal computing environment, that makes everything - even conferences - possible in his work area? I myself spend at least six out of eight hours at my computer terminal on most days, and I find that I create excuses to get up and wander around, hunt up someone to talk to, or start a (usually work-related) conversation with another worker nearby. I doubt that sending a message over the net or even teleconferencing would satisfy the need for a change of scene and for sheer physical movement that I feel after an hour or an hour and a half at the terminal.

FULL OR BROAD SPECTRUM LIGHTING (U)

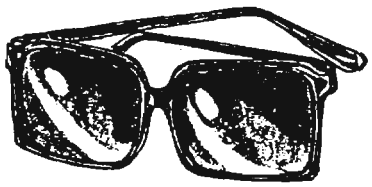
by [redacted] R335
(from Human Factors Letter #3-81)

The terms "full-spectrum" or "broad-spectrum" lighting are new "buzz-words" that have been appearing in public print for the past few years. Currently, the terms are used to (U) refer to lighting which closely resembles direct sunlight, including both the visible and non-visible frequencies (of the latter, at least the ultraviolet spectrum). An article in the Continental Airlines flight magazine EXTRA described Soviet claims of good results from the use of this lighting in office and work spaces (Ref 2). On the other hand, on-going US studies by the National Institute of Occupational Safety and Health (NIOSH) and the National Bureau of Standards have not only failed to duplicate the Soviet results, but in fact note a high risk of adverse effects (Ref 4).

(U) The primary risk from this type of lighting is due to the larger than normal amounts of ultraviolet that are emitted onto unprotected eyes and skin. The commercially-available "full" or "broad-spectrum" fluorescent lamps attempt to approximate sunlight by adding a chemical which fluoresces at the mercury-line wavelength of 430 nanometers. The result is a blue-colored light which is now considered by experts to create a risk of damage to human eyes called the "blue light hazard" (Ref 4). This commercially-available type of lighting appears to offer no advantage as a tool to improve the performance of VDU operators or other office workers, and in fact is likely to create a risk to visual health.

References

1. "Human Factors in Office Automation," W.O. Galitz, Life Office Management Association, Inc., Georgia, 1980, pp 68-70.
2. "Take it Straight from the Sun," EXTRA, Continental Airlines, May 1980, pp. 28-32.
3. "The Dual Function of the Eyes," John Ott, Southern Journal of Optometry, June 1979, pp 8-20.
4. Personal communications from Clyde C. Moss, NIOSH, and Dr. Robert Glass, National Bureau of Standards, 1981.



CRYPTOLOG NUMBERING (U)

~~(FOUO)~~ It is evident from your questions that some of you like to keep a complete file of CRYPTOLOG, and so for your use, here is a list of the issues, by volume, that have been published to date:

Vol I, 1974 Numbers 1, 2, 3, 4, 5. (Aug-Dec, initial year).

Vol II, 1975 Numbers 1, 2-3, 4, 5, 6, 7, 8-9, 10, 11, 12.

Vol III, 1976 Numbers 1, 2, 3, 4, 5, 6-7, 8, 9, 10, 11, 12.

Vol IV, 1977 Numbers 1-2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12.

Vol V, 1978 Numbers 1, 2, 3, 4, 5, 6, 7-8, 9, 10, 11, 12.

Vol VI, 1979 Numbers 1, 2, 3, 4, 5, 6, 7, 8-9, 10, (11-12 not used).

Vol VII, 1980 Numbers 1-3, 4-6, (7-12 not used).

Vol VIII, 1981 Numbers 1-3, 4-6, (7-9 not used), 10, 11, 12.

Vol IX, 1982 Numbers 1, 2, 3, 4, 5 (this issue).

(U) Copies of most issues are available in limited numbers. Call Hal Smith (x3369s) or Wayne Stoffel (x8322s).

DOCID: 4009848

TRUE BASE: TWO TALES (U)

by [redacted] P1

P.L. 86-36

(U) Both of these tales are true. Some of the details have been changed, but not necessarily to protect the innocent. They both have to do with the same thing: what happens to our knowledge about a target when we put one of its systems on true base.

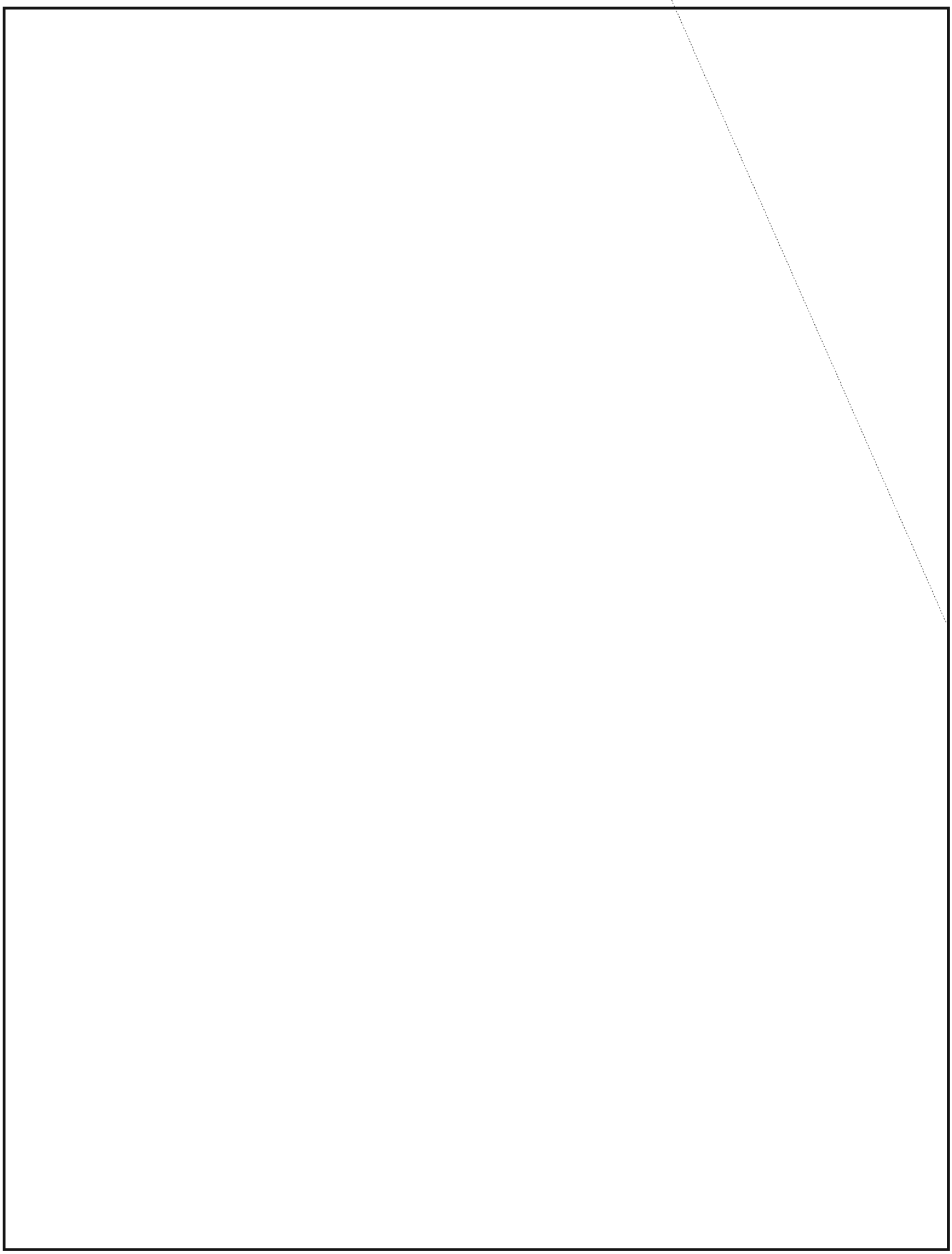
[redacted]

First Tale

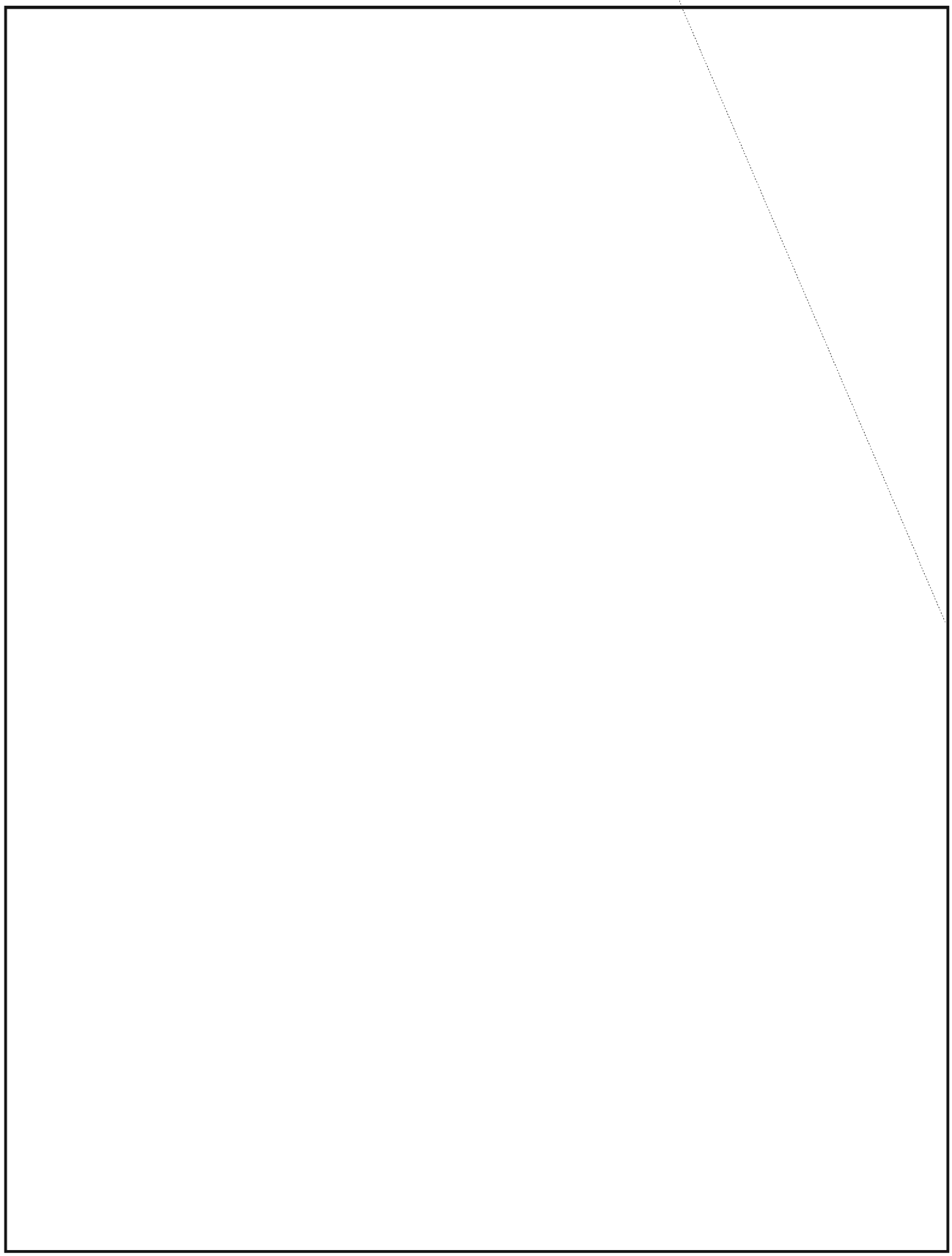
[redacted]

EO 1.4.(c)
P.L. 86-36

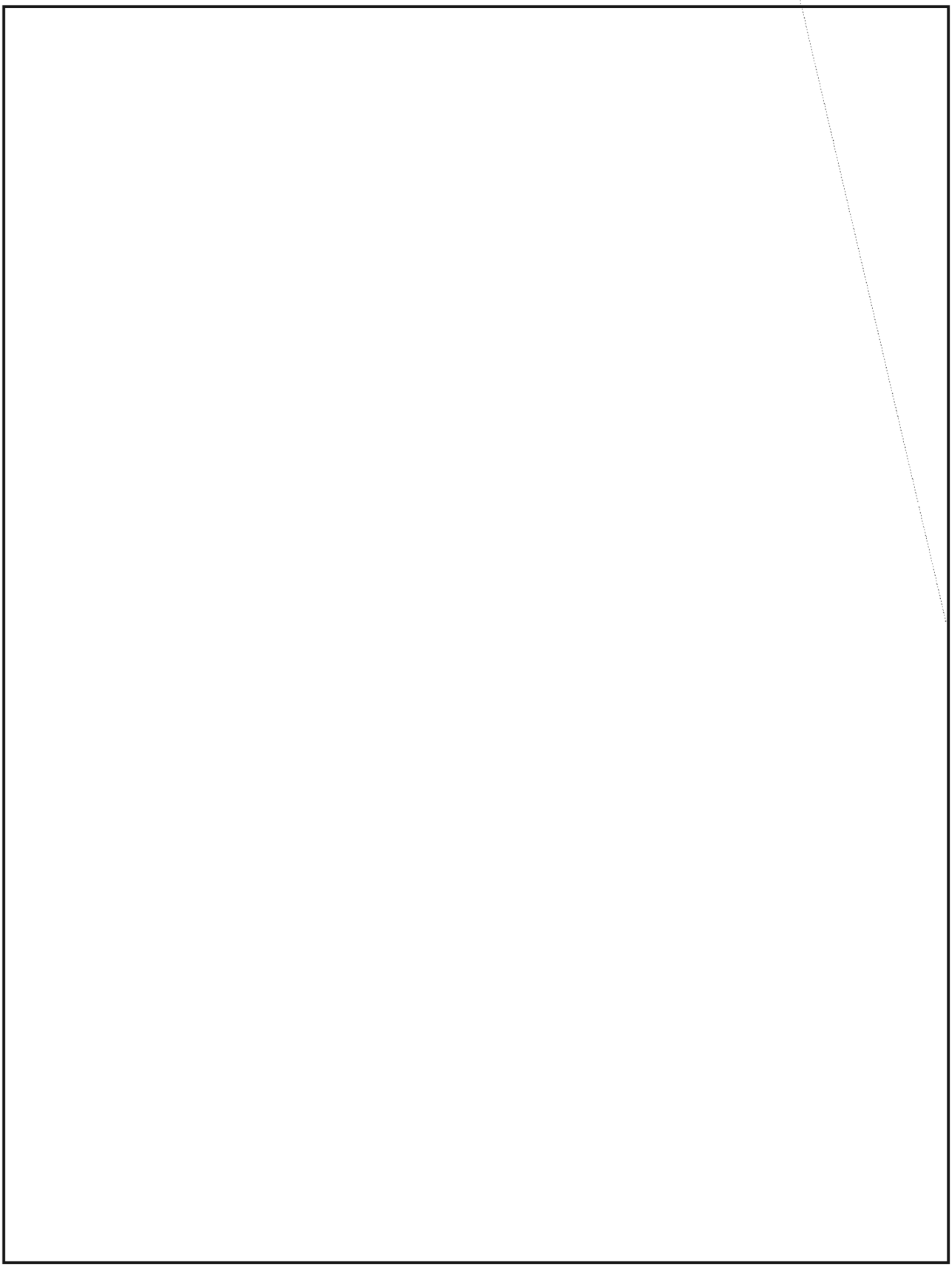
EO 1.4.(c)
P.L. 86-36



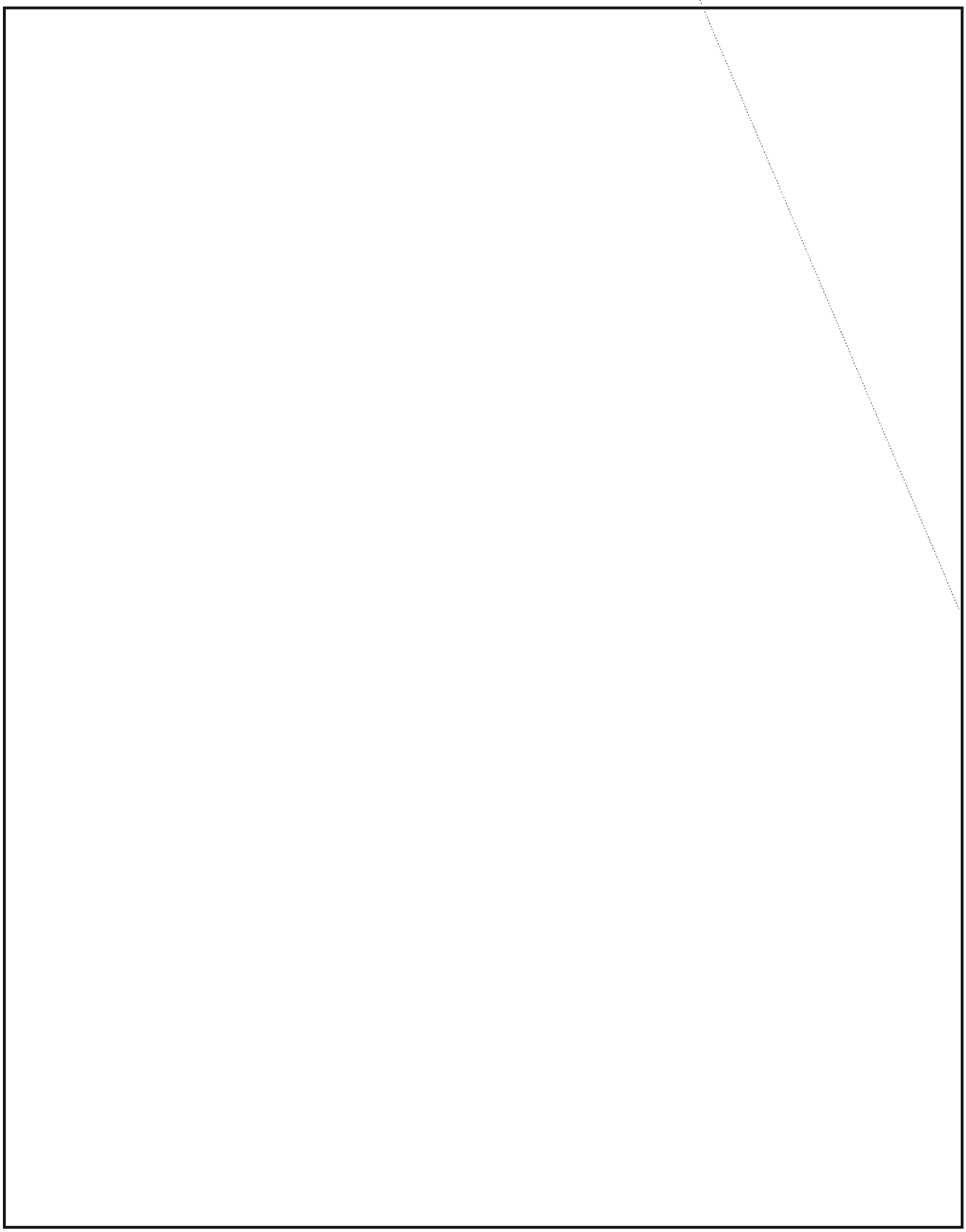
EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

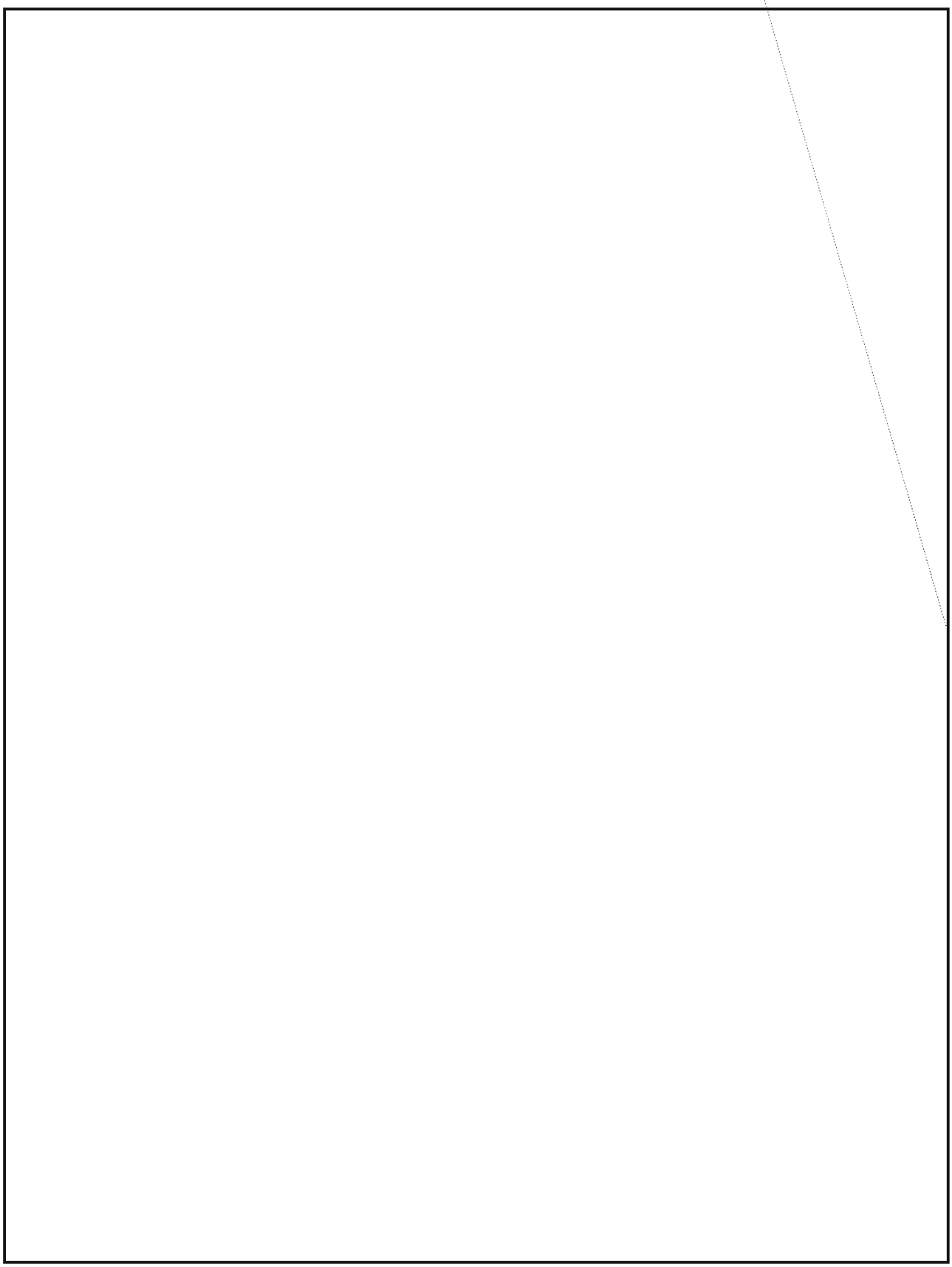


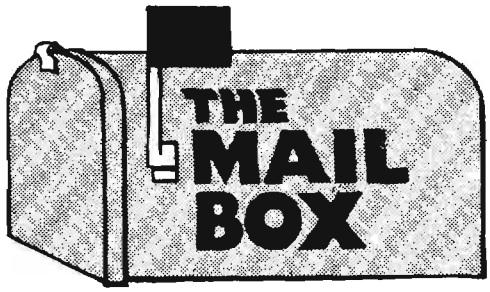
EO 1.4.(c)
P.L. 86-36



DOCID: 4009848

EO 1.4.(c)
P.L. 86-36





I must confess. I have worked at the Agency about 15 years and I still do not know how to spell the word "plaintext" (or words "plain text"). I have used various ruses in attempts to conceal my ignorance. For example, I have used "p/t" or "text" as substitutes, and I have tried to conceal "p/t" in hard to spell and/or hard to understand words and phrases. That is why my pulse quickened and hope arose when I picked up the March 1982 issue of CRYPTOLOG, and found on page one the words "plain text." Eureka. There the words are, in America's ultimate source on how to spell "p/t." (I haven't received a copy of NSATJ in a year, and believe it to be defunct.) If an official publication of NSA can not spell "p/t," who can? So, you spell it as two words. I quickly read and turned to page two to get verification by repetition. Alas--"plaintext" screamed at me--five times. Wait. Perhaps it may be spelled either way depending on some rule (e.g., one way if an adjective, another if a noun), I thought. Or perhaps the first spelling is just a typo--the editor did warn of such things at the very beginning. I quickly read on to gather more data. "P/t" appears three more times as one word, and twice more as two words. I could discern no rule. I could not believe three typos. Hope faded. I gave a laugh and resigned myself to continued illiteracy when I noticed near the end of page three a sentence beginning with a small letter.

Sincerely,

[redacted]

A541

P.L. 86-36

From: jel at opman
Subject: programs
To: cryptolg at barlc05

P.L. 86-36

Read [redacted] article on PINSETTER programs with some interest. I would suggest some sort of introductory comment noting that these programs will run on UNIX systems, but that the PINSETTER programs are not available on most UNIX systems. To my knowledge 'permute' is available only on [redacted] There is no arrangement with T3332 (UNIX Systems Support) to include these programs in a standard system.

In line with the above, I would suggest indicating which programs are standard agency UNIX programs (available everywhere) and which are PINSETTER programs for which special arrangements must be made.

[redacted]d

From: dce at CARONA
Subject: Shell Game - "names"
To: cryptolg at barlc05
cc: dce

Hi,

I just got my April 1982 issue of Cryptolog and noted with great interest the new feature Shell Game. I look forward to seeing this feature on a regular basis.

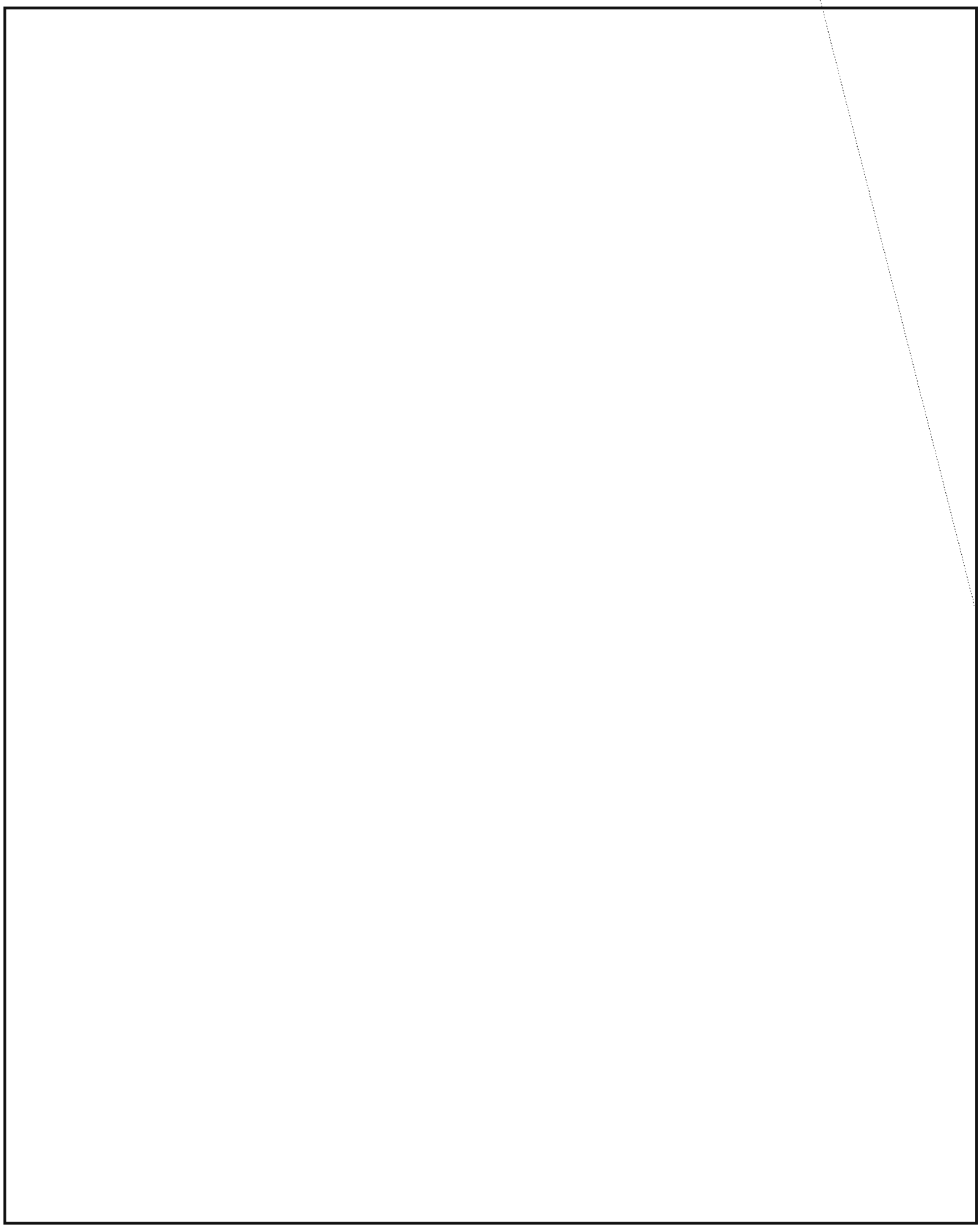
I like the names shell and have one very similar that I call whon. Frankly, I like the results of mine better and thought you might want to compare. Try this one:

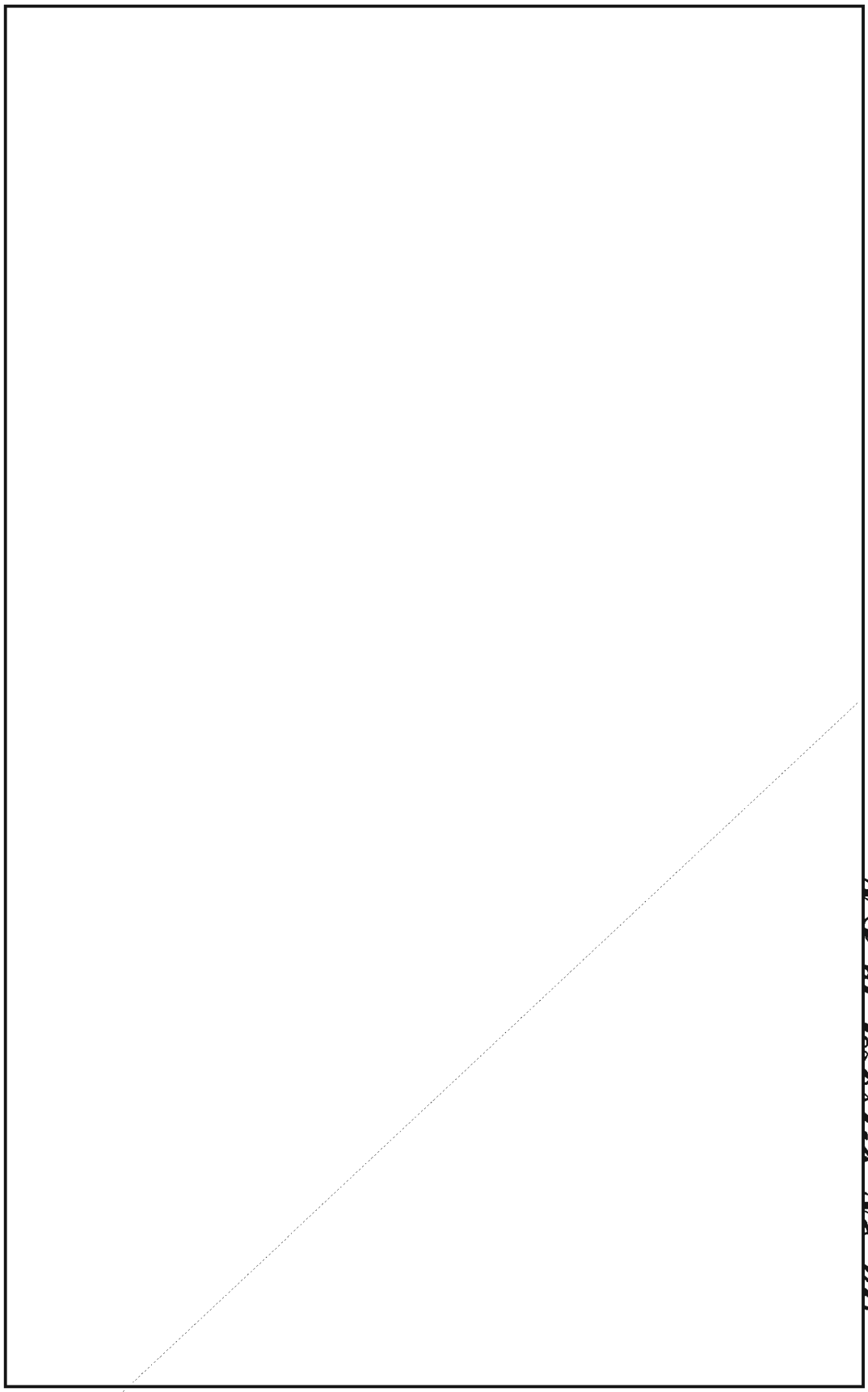
```
who | reform +t8 | rpl "^" "name " > whonames
sh whonames
rm whonames
```

Regards,

[redacted]

T441,1181s (dce@carona)





NSA Publication No 40

P.L. 86-36

LOOKING AROUND with P13

P.L. 86-36

EO 1.4.(d)
P.L. 86-36
EO 1.4.(c)

A HISTORY LESSON (U)

By early 1942 British analysts [1] had built up a favorable position in exploitation of Luftwaffe ENIGMA traffic, but a cascade of German ~~(TSC)~~ security changes, and new demands by the SIGINT recipients, forced a number of crises on the analysts, and incidentally forced the SIGINT effort to be more analytic and more tightly integrated.

~~(TSC)~~ In 1940 GC&CS [2] broke into ENIGMA traffic during the Norway campaign, but on 1 May 1940, the German Air Force (GAF, Luftwaffe) and German Army (GA) introduced a new indicator system which defeated the cryptanalytic methods. On 10 May 1940, Germany attacked in France and the Army came on the air on 3000 frequencies, which the BEF (British Expeditionary Force, the British Army in France) tried to cover with only 50 receivers. By 20 May 1940, the GAF RED key was solved and produced 1000 decrypts daily, but the intelligence was unused.

~~(TSC)~~ During 1940, all traffic analysis on ENIGMA communications was based on decrypts. The callsign system was unknown, but decrypts were not used to try to solve the callsign system. The German Army "Dog" book of 40,000 callsigns was captured in Norway.

~~(TSC)~~ All messages had discriminants, so cryptanalytic sorting was based only on discriminants. Traffic analysis was not accepted in Hut 3 [3] unless based on decrypts. The aim of traffic analysis was to steer intercept, because of the shortage of receivers and operators.

This article is extracted from a briefing given by the author at the C.A.A. Conference, Fall 1981.

~~(TSC)~~ The "fusion" technique of combining decrypts and log readers' records showed that traffic analysis could help break ENIGMA.

~~(TSC)~~ In 1941, traffic analysis research found that the GAF used a "Bird" book for callsigns, similar to the GA "Dog" book, a system of 40,000 callsigns that had been captured in Norway; however, where GA frequencies were daily changing, the GAF frequencies were fixed.

~~(TSC)~~ The solution of the GAF callsign system (by Army analysts) completely changed the attitude of Hut 6 [4] toward traffic analysis, and initiated a policy of trying to read all traffic worth breaking. Hut 3 intelligence analysts wanted only 45 more receivers to cover ENIGMA communications, but Hut 6 traffic analysts held out for 240 more receivers to allow complete cover of Order of Battle and selection of traffic. A number of overlapping

DOCID: 4009848

EO 1.4.(d)
P.L. 86-36
EO 1.4.(c)

traffic analysis parties came into existence, each doing part of the traffic analysis mission, which was still undefined.

~~(TSC)~~ By 1942, there were 40 new GA and GAF ENIGMA keys in use. The Quiet Room in Hut 6 found [redacted] and the Registration Room [6] [redacted] This made efficient breaking and exploitation possible, despite the fanout of the key families.

~~(TSC)~~ A reorganization of BP (Bletchley Park, wartime location of GC&CS and Service cryptanalytic intelligence) in early 1942 enabled Travis, the new chief, to move BP away from Ministry control, and establish direct control of ENIGMA interception. The disastrous war situation at that time forced heavy new commitments to expansion of SIGINT and increase in exploitation resources.

~~(TSC)~~ In April 1942, the GAF made a wholesale reallocation of frequencies, but callsigns remained predictable. This change was solved by luck and hard work. The Air Section at BP, without access to ENIGMA decrypts, found [redacted] traffic was obtained from Black Market receivers, [7] and the ENIGMA search effort was used to find links passing [redacted] which was generally indistinguishable from ENIGMA traffic. The log readers (people who read radio operators' logs to try to identify the German wireless nets, and understand how the German nets worked) then found [redacted] as a result of circumventing intercept control that had concentrated on exploitable ENIGMA links.

~~(TSC)~~ By this time, there were expanding parallel traffic analysis efforts in Hut 6, Hut 3, and Beaumanor Army Y station, using different methods and materials. The Log Party began to reconstruct nets from logs and the callsign book, and used ENIGMA traffic, non-ENIGMA traffic, and non-ENIGMA decrypts--contrary to the policy of keeping high- and low-grade SIGINT separate. The Fusion section began to study net content, i.e., what kind of intelligence passed on a net, as well as defining the net structures. Intercept control was vital because of the volume of traffic and shortage of operators, and 3L was established in Hut 3 in September 1942 to inform Intelligence Control of the tasking requirements for intelligence.

~~(TSC)~~ By December 1942, there were 300 receivers (sets) on ENIGMA, 50 GAF and GA keys, and 1600 deduped messages per day. GAF radio security was generally much inferior to GA radio security. ENIGMA interception was about one quarter of all Y (radio intelligence, except cryptanalysis) interception, and the Army Y stations were the main source.

~~(TSC)~~ On 1 January 1943, the German Army introduced a new F callsign book, along with some new methods of changing their callsigns. However the new book was [redacted] derived from the E callsign book which had been captured in 1941.

~~(TSC)~~ The first signs of real crisis came in May 1943, at a time when exploitation and callsign prediction were flourishing. There was a large scale German Army communications exercise in France and the low countries, which produced a large volume of traffic, but none of the keys were readable. Inference from traffic externals was tried for the first time. The real crisis came on the heels of this, when the OVERLORD planners, preparing for the invasion of Normandy, began to demand German Army decrypts. Traffic analysis was asked to steer the intercept system onto GA nets in support of the invasion, and the Air Ministry, which had dominated control of ENIGMA SIGINT, had to yield to the demands of Allied ground forces.

~~(TSC)~~ The next crisis developed in Autumn 1943. The German Army dropped almost all of its discriminants on 1 September 1943, but the effect was minimized by the ability of the Army Y stations to identify the traffic. Two months later, the Luftwaffe (unforeseen by Hut 6) also dropped its discriminants, causing a catastrophic pileup of traffic, totally unsortable without discriminants, and almost all processing and cryptanalysis was brought to a halt.

~~(TSC)~~ By good fortune, Hut 6 discovered that one of the analysts in the Quiet Room, who had been solving the discriminant system, had a detailed knowledge of both the radio nets and the GAF order of battle, since he had worked from both logs and decrypts. The Quiet Room [5] and the Y stations managed to solve the crisis, but only after the unsortable traffic had piled up for some weeks. They had to develop completely new methods of sorting the incoming traffic by frequency and callsigns, rather than by the now absent discriminants. Traffic analysis and SIXTA suddenly became indispensable to SIGINT operations.

~~(TSC)~~ By 1944, as invasion preparations advanced, the SIGINT situation was good: both high and low level cryptanalysis had continuity, trained staff and equipment, and were reading currently. The FISH (German Cipher Teleprinter) exploitation was developed as an alternative in case ENIGMA failed. The intercept operations were able to work from predicted callsigns and frequencies. The traffic analysis had almost complete knowledge of German nets, order of battle, procedures, and the callsign books. SIXTA was integrated with cryptanalysis and intelligence analysis. 2000 to 4000 current high level decrypts were being processed daily.

~~(TSC)~~ On 1 April 1944, the Luftwaffe made an expected callsign book change, and Hut 6 made preparations for this which resulted in a complete disaster and a pileup of all incoming traffic. However, the Y stations, who had not been informed or consulted about the change, and therefore had made no advance preparations, nevertheless were able to solve the problem by examining the traffic itself and determine that the change was only partial. After that, SIXTA had to learn to identify traffic without knowing the callsigns. They then began to sort the incoming traffic on callsign serials [8], rather than by the inaccurate frequency measurements, a practice that should have been started two years earlier. The integrated traffic analysis and cryptanalysis against GAF and GA in Hut 6 then split vertically into separate Army and Luftwaffe efforts--as a result of the different handling required for the GA and GAF traffic. Thus, the irony that the centralized cryptanalytic effort at GC&CS had divided into distinct Army, Navy, and Air Force channels, because of divergence in the cryptography of the German services--but the vital resources such as BOMBES were still pooled, and even the U.S. Navy BOMBES were used as much on GAF and GA traffic as on Naval tasks.

~~(TSC)~~ On D Day, the huge volume of traffic, caused in part by deliberate cutting of German landlines, threatened to overwhelm the processing. A huge volume of Army traffic was intercepted, but almost none was read. Some Luftwaffe traffic was read. From D Day on, sorting was an analyst's task, and could no longer be done by clerks according to an exact procedure. Masses of traffic were discarded without being identified.

~~(TSC)~~ By Autumn of 1944, German Army traffic almost vanished as the retreating ground forces went onto landline. The German Army, knowing the ENIGMA was being read, introduced stringent radio and cipher security, enforced by OKW [9] and more significantly by RSHA [10], which included the Gestapo. The frequencies were changed every three days and could not be predicted, and encrypted callsigns, now completely unbreakable, were introduced. Although the Hut 6 cryptanalysts were extremely pessimistic about solving the callsign cipher, the W.O.Y.G. (War Office Y Group at Beaumanor) and their outstations solved the traffic identification problem, producing identifications that were 85% correct at the site, while Hut 6 and SIXTA were helpless. The long experience of the Army operators who had copied the same targets for years was crucial in identifying the German Army nets.

~~(TSC)~~ On 1 February 1945, the Luftwaffe went over to the new encrypted callsigns and frequency change system already adopted by the Army, and a complete SIGINT disaster resulted. Unlike the Army Y stations, the RAF Y stations were unfamiliar with the GAF nets. The RAF operators tried to identify the traffic, but were 50% wrong at first, and cryptanalysis came to a halt because of misidentified traffic. The problem was that there were too many cipher messages that might seem to fit with any crib, and no keys could be broken until the nets were at least partly known. The RAF operators improved, and radiofingerprinting (RFP) combined with directionfinding (DF) proved helpful. At this point the low grade decrypts became vital in providing net identifications. The "Duddery" scheme of testing unidentified messages against already solved keys became overloaded and production of decrypts went down to almost nothing. For the first time, decrypts of ENIGMA traffic were passed first to SIXTA, to help traffic

analysis, before they went to the intelligence analysts in Hut 3, for traffic analysis was more important than reporting.

~~(TSC)~~ During 1944, the Germans had tightened lower level hand ciphers so much that [redacted] After the February 1945 crisis, work concentrated on low level systems (aided by captures) and many low level decrypts were reported as intelligence, because of a paucity of current ENIGMA decrypts.

~~(TSC)~~ Fortunately, the FISH and Naval ENIGMA traffic continued to be currently readable, and as the end of the war approached, the RAF radio operators were gradually able to sort and identify the traffic, but the whole problem of traffic analysis was thrown back onto the Y stations--where it had been in 1940.

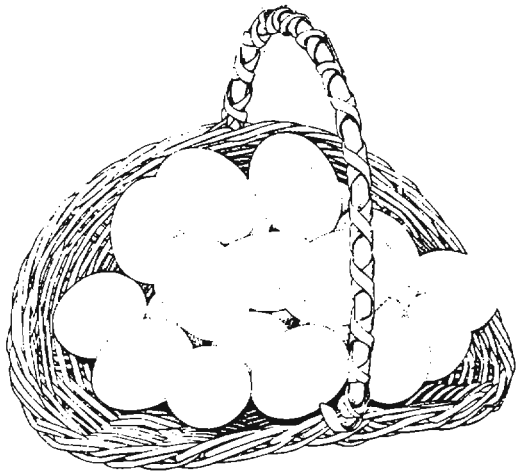
~~(TSC)~~ The quality of intelligence against the German Army declined with one notable consequence that the American armies invading Germany in April 1945 turned south to attack a nonexistent "Alpine Redoubt." In addition, the traffic that was broken was often weeks old.

~~(TSC)~~ The harsh lesson was that without successful traffic analysis, the rest of the highly leveraged ENIGMA effort, which depended utterly upon good cribs and encipherments across systems, collapsed even though the cribs and reencipherments still occurred, because the unsorted traffic swamped the rest of the analytic process.

Footnotes

1. British cryptanalysts, and other British personnel at radio stations, London ministries, and elsewhere who were doing parts of what later was recognized as "traffic analysis."
2. Government Code and Cipher School, located at Bletchley Park from 1939; part of GC&CS moved back to London in 1942 for Diplomatic traffic.
3. The section of GC&CS in which decrypts of German Army and Luftwaffe traffic were converted into intelligence and intelligence advisory messages. J.E.S. Cooper, GC&CS Army and Air Force Sigint, XII, 318.
4. The section of GC&CS in which the cryptanalysis and exploitation of the ENIGMA traffic of German Army and Luftwaffe was carried out; later, traffic analysis was located in the same building and called SIXTA. Cooper, p. 318.
5. In March 1942, a "Quiet Room" was established in the Hut 6 Central Section (which controlled intercept coverage and also identified incoming traffic to research discriminants; an unexpected result of the analysis mode was the discovery that discriminants were derived from a predetermined system. Cooper, pp. 157-8.
6. A Section of GC&CS which kept records of headings and beginnings of all messages, and studied them to see if this would give useful information to other sections. Cooper, p.18.
7. Receivers became available in quantity as a result of U.S. support, and operators in training, using these receivers, were given operational targets to cover as part of training. They were outside the administrative control of 3L, which tasked interception for intelligence, and thus provided a useful surplus capacity, not accounted for, which could be given useful tasks to help Hut 6, without being stopped by 3L. Cooper, pp. 252, 281-2.
8. Each ENIGMA network was allotted a monthly column-allotment "Serial" from the callsign book, providing a different column of callsigns for use on every day of the month and recurring from month to month; the order in which the 31 columns had been chosen to form this "Serial" was apparently haphazard. Cooper, pp. 52-3.
9. Ober Kommando der Wehrmacht, an organization established by Hitler to control the three Services and coordinate them. It was given central COMSEC authority in 1944.
10. Reich Sicherheit Haupt Ampt = Supreme National Security Board. This organization contained the Gestapo, Security Service (of the SS), Abwehr of OKW and OKW/Chi, the cryptologic agency.

P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)



DOCID: 4009848

IS THERE AN OLD CROW IN YOUR FUTURE? (U)

by Ron Cole

P.L. 86-36

In April 1981, the National Office of the Association of Old Crows (AOC) authorized the establishment of a Chapter to be headquartered in the Fort Meade/metropolitan Baltimore area. The Chapter, called the "Chesapeake Bay Roost," is to serve the needs of those in the Maryland area who are interested in the electronic warfare arena. In our first year, the Chapter has grown to the fourth largest in the nation with more than 540 members, more than one-fourth of whom work for the Agency.

The AOC is a non-profit professional association of individuals interested in the science of electronic warfare. Its membership includes members of all four services (officer and enlisted), Department of Defense civilians, NATO and other friendly nations' personnel, members of private industry, and members of educational institutions. Membership is open to all grades and ranks, and currently represents a very interesting cross section of society.

The AOC was organized in 1964 to exchange data on the technical and operational aspects of electronic warfare. The organization has since grown to 58 chapters with more than 32,000 members worldwide. The name "Old Crows" emerged from the first large-scale use of electronic warfare during World War II. The receivers and transmitters used in this effort were produced under the common equipment codeword "Raven." Common jargon later changed the term "Raven" to "Crow" and the group of professionals engaged in electronic warfare became "Old Crows."

In May 1981, the Director of NSA (an active Chapter member) pointed out that NSA has become a recognized leader in the AOC annual national symposia by providing the electronic warfare community with an appreciation of the SIGINT/COMSEC contributions to solving electronic warfare problems. Agency personnel have presented papers at many of the national symposia; at the symposium last year, [redacted] (W2) was given the award for best presentation.

The Chesapeake Bay Roost is currently meeting every other month, with luncheons featuring such speakers as General Faurer, General Larson (USAF-ESC), and Admiral Gallotta (USN), and has scheduled General Stubblebine (USA-INSCOM) for its June meeting (23 June, 1100-1300, Ft. Meade Officer Club).

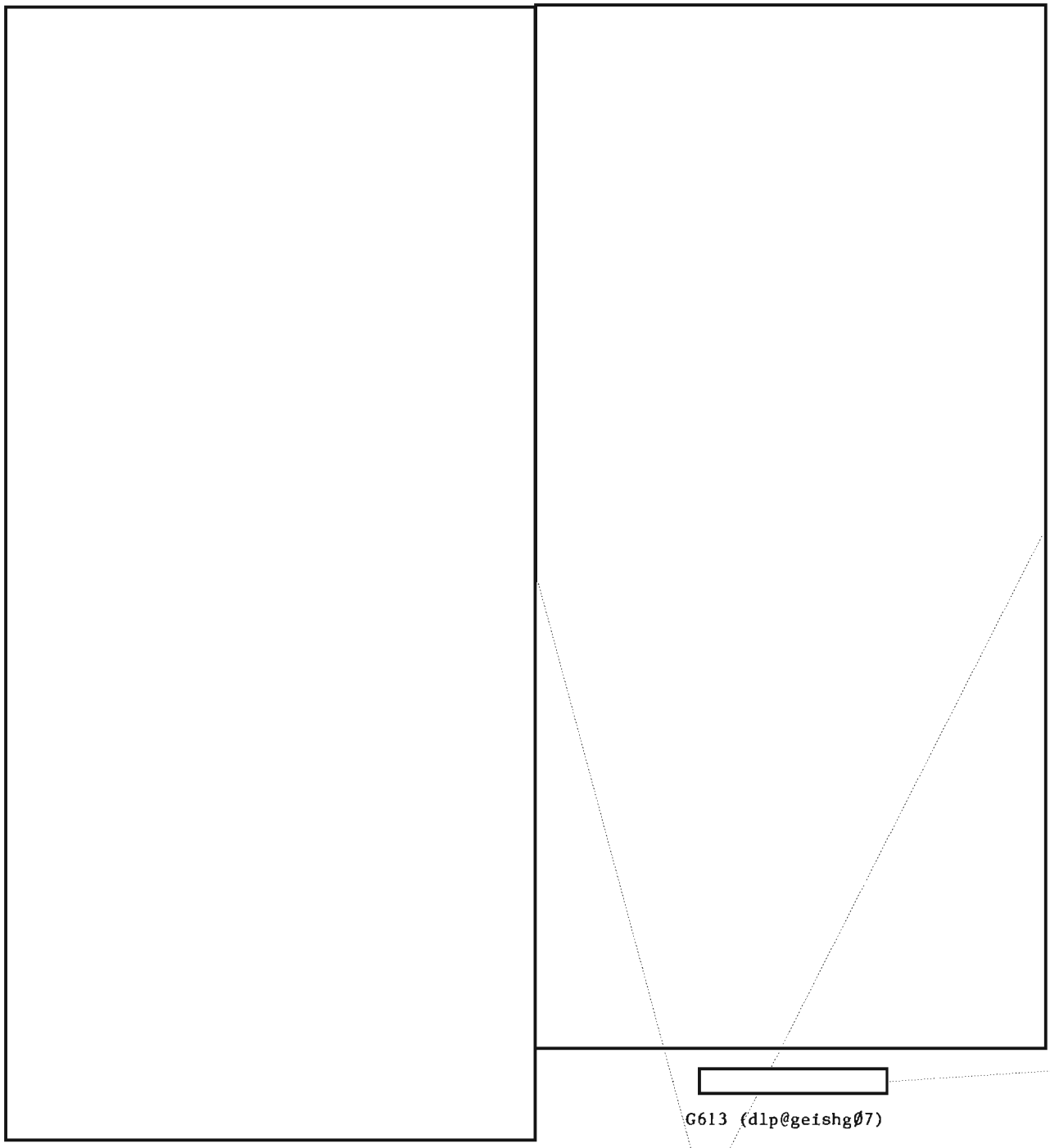
If you are interested in joining, the fees are $15.00 a year ($7.50 for students), for which you receive a one year subscription to the "Journal of Electronic Defense" (12 issues), an AOC coin, a membership certificate, and a membership card. The following members work within NSA and may be contacted for membership applications:

[redacted]	(President)	x8150s
	(Secretary)	x8757s
	(Treasurer)	x8745s
	(Membership)	x8150s
	(Historian)	x8893s
	(Programs)	x3083s

P.L. 86-36

BUST Answer (U)

by [redacted] P.L. 86-36

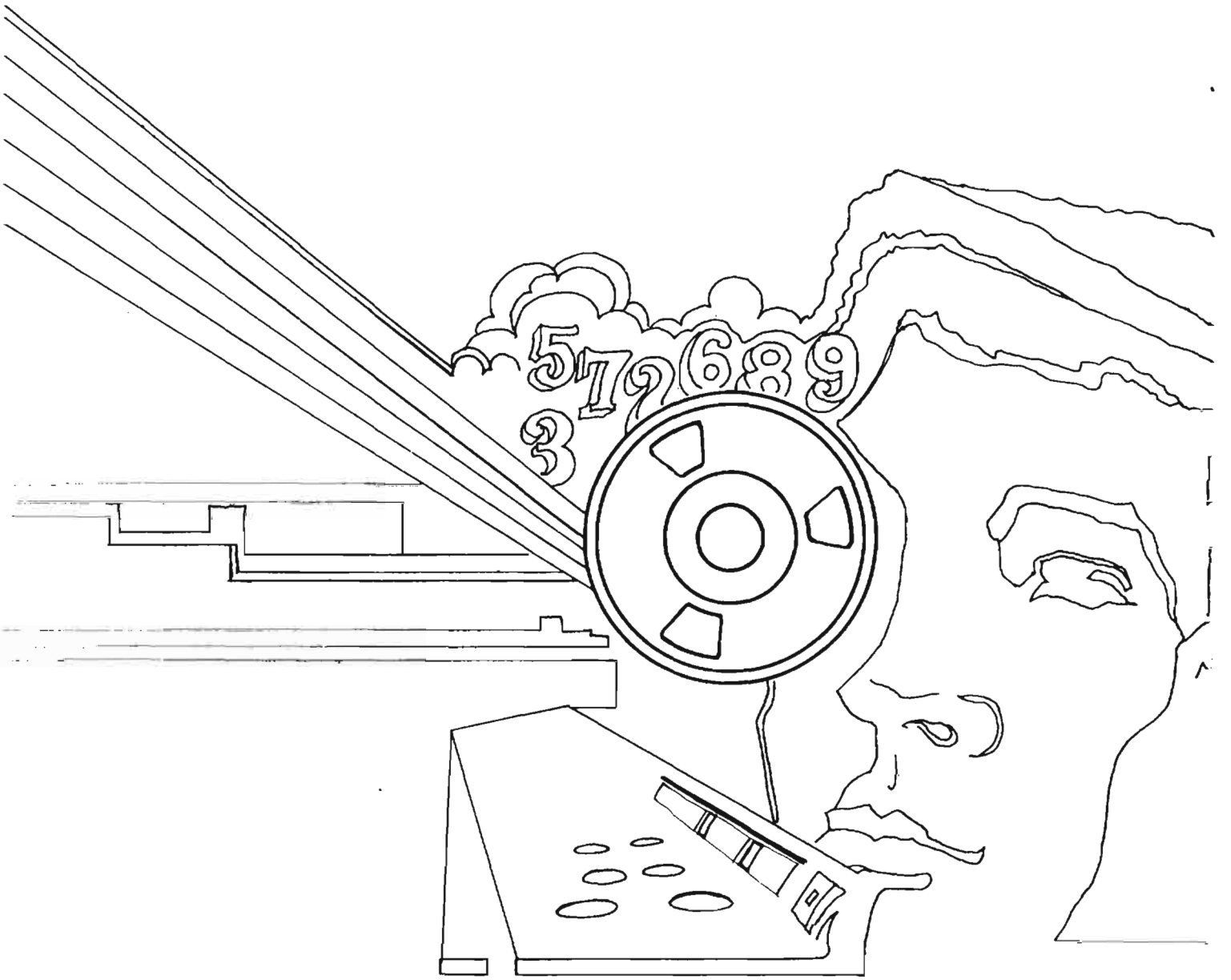


[redacted] P.L. 86-36

G613 (dlp@geishgØ7)

EO 1.4.(c)
P.L. 86-36

P1-Jun 82-S3-17245


5726893

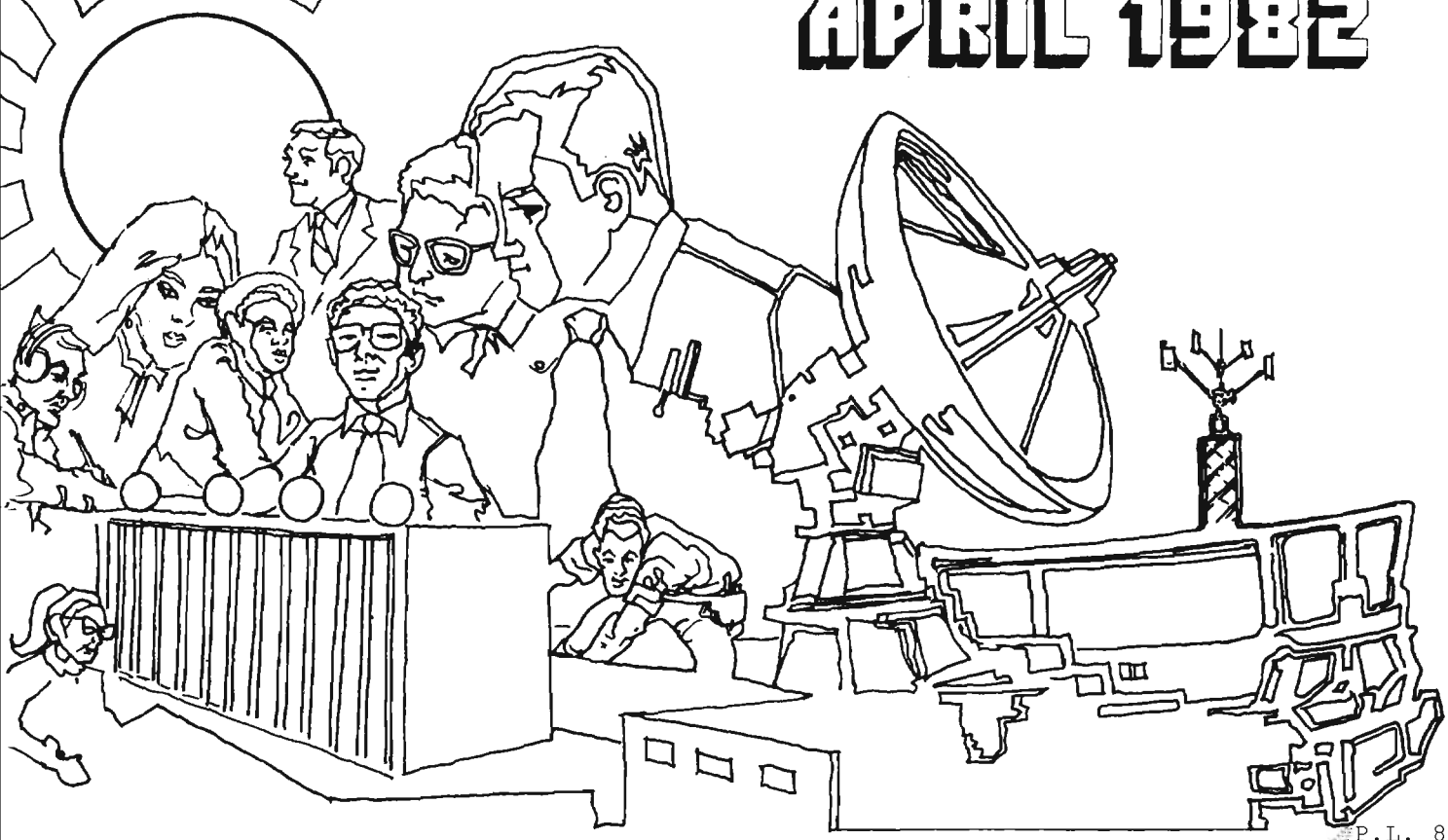
DOCID: 4033690

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

APRIL 1982



P.L. 86-36

PARTIAL MACHINE TRANSLATION: FINAL REPORT (U).. [redacted] ..1
TRACKS IN THE SANDS OF TIME (U)..... Fred Mason 12
NSA-CROSTIC NO. 39 (U)..... David H. Williams 14
REVIEW: THE AMERICAN MAGIC (U)..... [redacted] 16
SHELL GAME (U)..... W. E. S. 20
WORD PROCESSING IN A4 (U)..... [redacted] 22
BOOKBREAKERS' FORUM ON MACHINE AIDS (U)..... [redacted] 27
PERSONAL COMPUTER APPLICATION (U)..... [redacted] 28

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 10 Apr 2012~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4033690

~~FOR OFFICIAL USE ONLY~~

CRYPTOLOG

Published by P1, Techniques and Standards,
for the Personnel of Operations

VOL. IX, No. 4 APRIL 1982

PUBLISHER [redacted]

BOARD OF EDITORS

Editor-in-Chief. [redacted] (7119/8322s)

Production..... [redacted] (3369s)

Collection..... [redacted] (8555s)

Cryptanalysis..... [redacted] (5311s)

Cryptolinguistics..... [redacted] (5981s)

Information Science.. [redacted] (3034s)

Language..... [redacted] (8161s)

Machine Support.. [redacted] (5084s)

Mathematics..... [redacted] (8518s)

Puzzles.....David H. Williams (1103s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Taurone (3573s)

For individual (or organizational) subscriptions send name and organization

to: CRYPTOLOG, P1
or call [redacted] 3369s

To submit articles or letters via PLATFORM mail, send to

cryptolg at barlcØ5
(note: no 'O' in 'log')

Editorial

By now it seems safe to announce that CRYPTOLOG is once again coming out on a monthly schedule. That was our objective back in October, but there were a lot of questions about whether it could be done.

We decided at the outset not to make any promises about publication schedules. These days there are so many people promising so much, and yesterday's promises have a way of fading unfulfilled beneath the flood of ever newer and more exciting promises. Maybe politicians and advertisers and hawkers of the new and better tomorrow don't think we remember those promises; at least they seem to operate as if we don't. But I think we do.

So, my inclination is not to add more promises to the glut, but rather to work on trying to deliver. We will try not to promise you some new development until we can show it to you. (At least one major space program works that way.)

We have had lots of ideas about how to make the magazine more useful to its readers, but not all of them have worked out. Some of them sound great, but the doing of them leaves a lot to be desired. We will continue to try, and we will continue to experiment with various things. Some of the things we plan to try may surprise you, or irritate you, or even offend you. We hope not.

If there is something you think we ought to be doing, or something we are doing that we ought to stop or change, let us know.

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

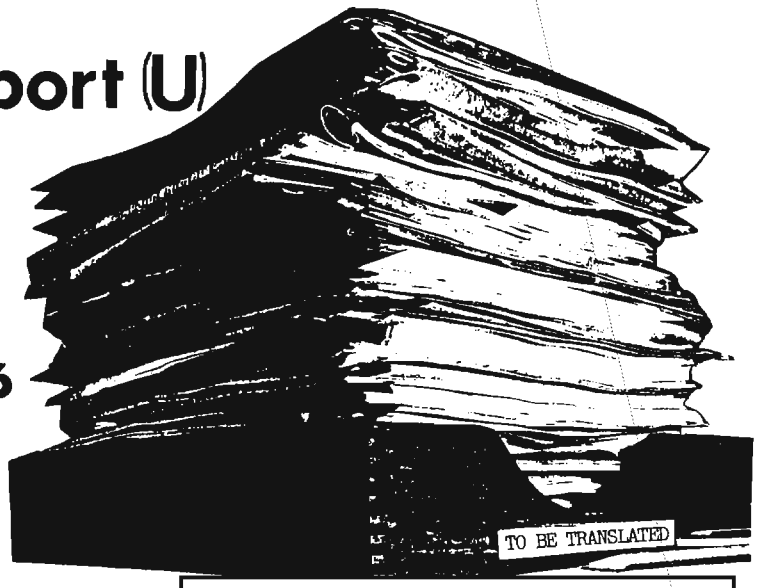
DOCID: 4033690

Partial Machine Translation: A Final Report (U)

EO 1.4.(c)
P.L. 86-36

[redacted] P16
and
[redacted] P16

P.L. 86-36



Partial Machine Translation (PMT) is a word-for-word or phrase-by-phrase "translation" from one language to another. The quotations marks are placed around the word "translation" to show that a PMT is not exactly what most people consider a true (or full) translation, but the quotes are inserted reluctantly. Although it may be difficult to read the result, some information may be lost or misinformation added, the quality may be less in virtually every respect than that of a good human (or even machine) translation, a PMT can nevertheless convey to the sympathetic reader the import of the original; and that, after all, is a translation's primary purpose.

(U) The purpose of a PMT is to enable readers with little or no knowledge of the source language to decide on their own whether to request a standard translation or to move on to other texts of potentially greater interest. The alternative might be to burden a linguist with translating many useless texts, assuming adequate linguistic help is available. PMTs can be prepared reasonably cheaply, freeing the linguist from fruitless tasks; the linguist thereby concentrates on tasks of importance.

~~(SC)~~ To illustrate how fine the distinction is between PMT and "true" translation, here is a sample of each. Which is which?

[redacted]

~~(S-CCO)~~ At first glance there does not seem to be much difference between the two versions. The second version is the PMT. (Actually, certain PMT conventions not yet explained but which would quickly become second nature to users have been smoothed out of the version as given above. For example, "we will be" would appear "(we)will_be"; "N" is a garble for "NR" and would be translated "?"; the capitalizations in "Again", "Further", "Awaiting" are not made. Also the original had a garble which caused "interest"

to be received as two words; the first of these would be translated "interest", the second would get a "?".) The first version above is the sender's own translation.

II. Background (U)

(U) PMTs could doubtless have been prepared nearly three decades ago in the early days of Machine Translation, but researchers were convinced that much better translations could be made automatically. They were correct but, even with the expenditure of considerable linguistic and programming efforts, their most optimistic hopes have not yet been achieved. (In addition, the telegraphic and/or garbled texts for which PMT has been expressly designed are less amenable to translation than texts written in standard language.) PMTs can yield useful results after only a minimal computational and linguistic investment.

[redacted]

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

[redacted]

(U) A general consideration which for the most part has been left implicit in the discussion that follows is that a PMT does whatever must be done to produce output with a reasonable chance of being usable, together with whatever else can be easily and usefully done to enhance the final product. Fine points which could be handled with difficulty but which would rarely improve the quality of a PMT have usually been omitted. P.L. 86-36
EO 1.4.(c)

III. Russian PMT: Language Independent (SC)

(U) A PMT output consists of groups of three lines:

- a line of the original text,
- a second line with the PMT itself, and
- a blank line as a separator.

The words (or phrases) of the second line are aligned underneath the words (or phrases) of the first line to the extent possible by expanding spaces in the original text. (There seems to be little danger of misleading someone reading the original.) This three-line pattern continues to the end of the text.

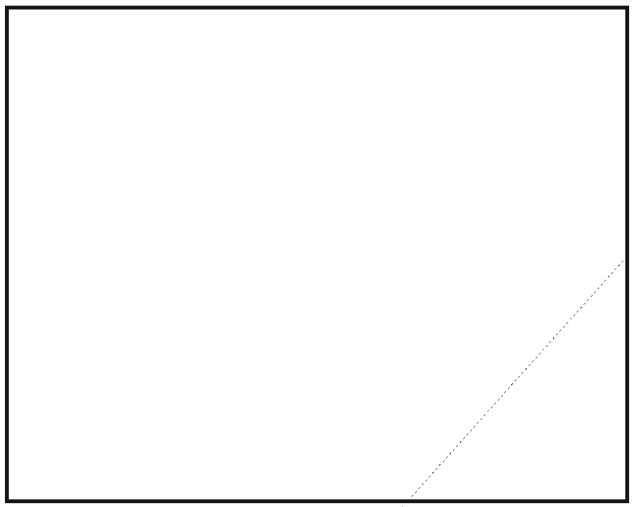
(U) Some words (e.g., misspellings, proper names, and cognates that are not likely to cause problems for the reader) are not in the dictionary. When they appear in the text, they will be represented by "?" to distinguish them from words which are within phrases and translated as such. Numbers and punctuation that appear in the original are not copied into the PMT line to avoid cluttering it and to enable punctuation conventions (built into

DOCID: 4033690

the dictionary) to show more clearly just how the translation is to be interpreted.

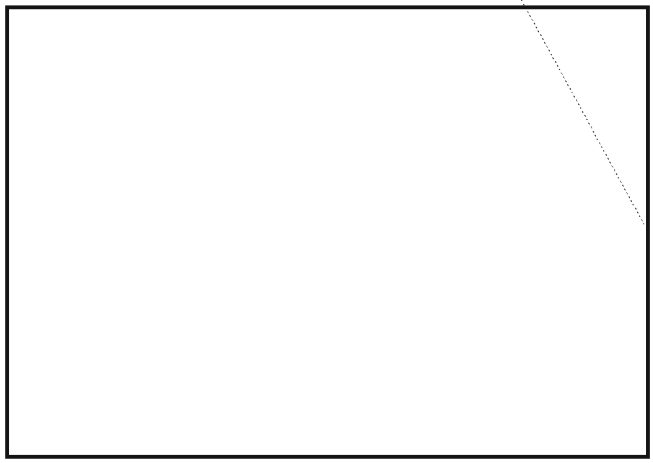
(U) The heart of any PMT effort is the dictionary. The person in charge of preparing and maintaining the dictionary will be called the lexicographer. The current dictionary is empirical, which means that it is based on actual texts. One is well advised to begin with a generous sample of texts to be translated and to compile therefrom a list of words in inverse frequency order. A KWIC (keyword in context) index will aid in determining the most apt translation, or gloss, and in deciding what phrases should become a part of the dictionary. The dictionary is then expanded by observing words and phrases that appear in subsequent texts without being translated or, even worse, with incorrect translations. (A few critical words, such as "plutonium", might be added just in case.)

(U) The current PMT algorithm can handle phrases (or idioms) whose individual words are contiguous, which includes a large number of useful cases, such as English "OF COURSE" or Russian "DO SIH POR". Phrases will normally be entered only when a word-for-word rendering is inadequate.



(U) For a heavily inflected language like Russian, it may be objected that words would have to be entered in all or many of their forms, a tedious job at best and a computer overload at worst. Fortunately, it has been observed that inflections may be ignored without severely diminishing a PMT's usefulness. An English example would be WALK%, standing for the forms WALK, WALKS, WALKED, WALKING (also WALKER, WALKERS, WALKWAY, etc., although entries such as WALKER% would take precedence over WALK% as appropriate). The %

represents all remaining letters to the end of the word. Most Russian words now require only one entry.



(U) It is wisest to include some common forms in full, such as SOOBQIM '(we)inform' and SOOBQITE '(you)inform', which will make many messages much clearer than the gloss given to SOOB%, 'inform'. Also, the participles of some verbs occur frequently enough to justify separate inclusion; POLUCHEN% 'received' is much clearer than POLUCH% 'receive'.

(U) Trimming can be done within idioms, as in JELEZ% DOROG% (for JELEZNAYA DOROGA) 'railroad. (The lexicographer must, however, be consistent. The full stem of the first word is JELEZN%, and if JELEZN% 'iron' is also an entry, the idiom will be missed.)

(U) If certain conventions are followed when entering glosses, the readability of the

P.L. 86-36

DOCID: 4033690

output will be enhanced. Multiword glosses may usefully be joined by _, as in KONECHNO 'of_course'. Using lowercase for the English will be beneficial for implementations in which the case can be preserved (this is not true of the printer used now). Parenthesizing words which might be redundant is helpful, so that MY SOOBQIM becomes 'we (we)inform'; this convention is essential if the cleanup feature of Section IV is to be fully utilized.

(U) Choosing the right gloss for a word with many meanings certainly can be a problem. One may:

- choose the most likely meaning (REKLAMA = 'advertising', not 'publicity');
- take the most striking meaning (GRANAT% = 'grenade', although 'pomegranate' is more likely);
- separate two meanings by a conventional slash (CHTO = that/what) (overuse of this will clutter the output, so fewer than 10 glosses have it);
- prefix the gloss with a conventional question mark (as in BLOK% = '?pulley'), an especially useful convention when the unlisted meaning is a cognate, as in the example given.

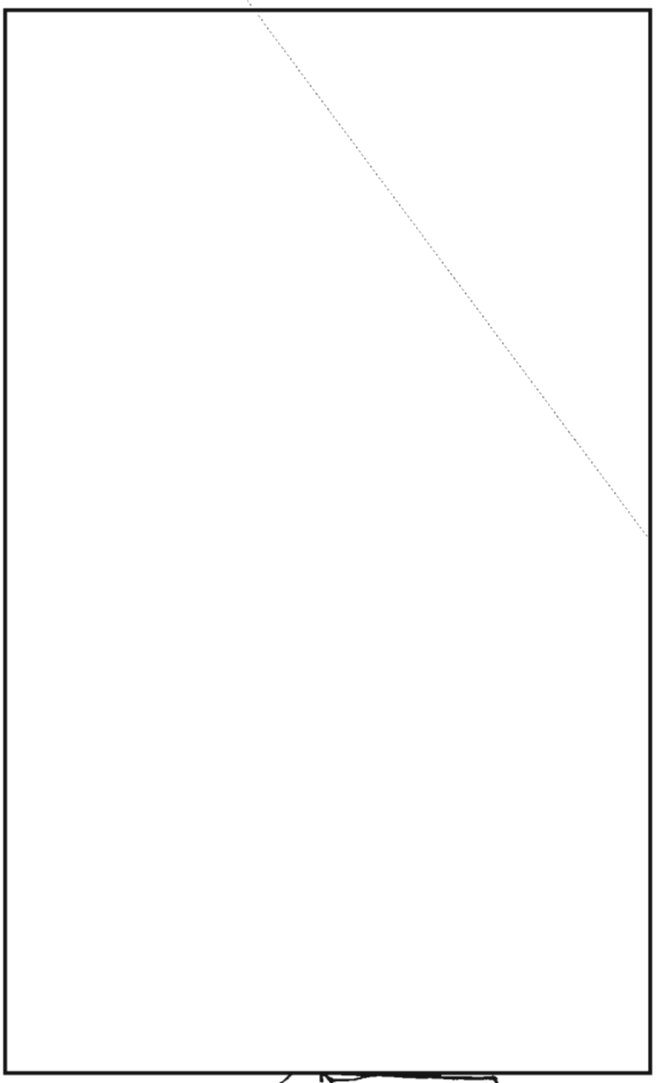
(U) Prefixes may become entries in the dictionary, with resulting savings in computer storage and dictionary upkeep. If AVAILABLE is in the dictionary, as well as the prefix UN= (the suffixed = signals a prefix), then UNAVAILABLE can be glossed correctly even if it had not appeared in earlier traffic. (If the word UNION were not entered, a false prefix will be taken from it regardless of whether ION is an entry. Use of prefixes results in such situations often enough that it is recommended that prefix glosses end in = to alert the user to possible trouble. NEYASNYJ is therefore glossed 'un=clear'.) The prefix convention will find use in handling certain Russian compounds, as in GOSBANK 'state=bank'.

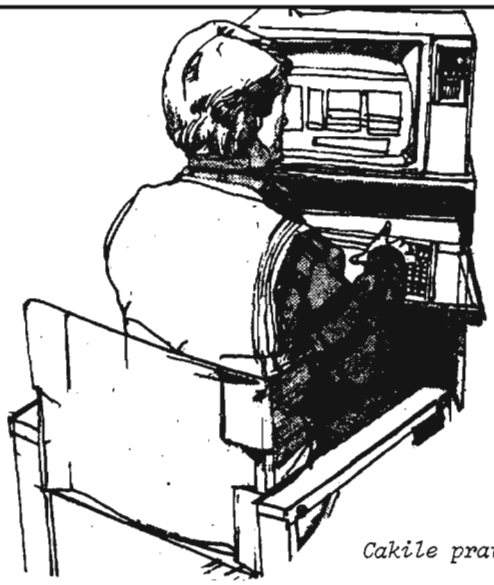
(U) Although Russian examples have been given up to now, virtually everything that has been said is applicable to other languages, so this version of the program has been called the "language-independent" version. You still need a separate dictionary for each language, of course, and it is possible that a given language will require some special handling.

~~(SC)~~ Indeed there is one section of code that must be added to the language-independent version in order to allow for reasonable Russian output without imposing a severe burden on the dictionary.

EO 1.4.(c)
P.L. 86-36

DOCID: 4033690
EO 1.4.(c)
P.L. 86-36





Cakile prattii

IV. Russian PMT: Language Dependent ~~(SC)~~

(U) A step up from the preceding version of the program requires morphological analysis. The semantic content of Russian is expressed in the morphology to a greater extent than in most languages. The programming required to analyze Russian morphology is essentially different from what would pertain to any other language, so this is the "language-dependent" version of PMT. Some of the principles involved would be relevant for other languages.

(U) The meaning of a Russian word-ending often depends on the class to which the word belongs. For example, -U on a feminine noun is usually the accusative case, on a nonfeminine noun usually dative, on verbs usually first person singular. Consequently, it is necessary to assign grammar codes to whatever dictionary entries are to be subject to morphological analysis. The codes in use are F, N, A, and V for feminine nouns, nonfeminine nouns, adjectives, and verbs. (The occasional use of P for prepositions will be explained later.) The code is stored in the rightmost of the positions allotted to the gloss in the lexicographer's dictionary. Absence of a code means that the entry is invariant or that, for one reason or another, analysis would tend to obscure the meaning or clutter the output. (For example, names of months receive no code because the typical usage '3 MARTA' is better glossed '3 March' than '3 (of)March'. This does mean that 'KONEC MARTA' comes out as 'end March'.)

(U) More codes could be used to distinguish masculines from neuters, nouns likely to occur in the plural from probable singulars, feminines of the soft declension, nouns with adjectival declensions, and so forth. Relatively little would be gained for the increased work expended by the programmer and lexicographer.

(U) Note that REKLAM% 'advertising' now probably requires three entries: REKLAM% (F), REKLAMN% (A), REKLAMIR% (V). On the other hand, participles and forms such as PROSIM and SOOBQITE no longer need separate entries.

~~(SC)~~ If a grammar code is present, the program may modify the gloss obtained from the dictionary depending on the ending of the Russian word involved. Feminine nouns offer a relatively simple example:

DOCID: 4033690

EO 1.4.(c)
P.L. 86-36

- if the ending is OJ, the case is instrumental, so '(with)' is preposed to the gloss (not only is 'with' the correct preposition for some pure instrumentals, but most often the preposition S which governs the instrumental

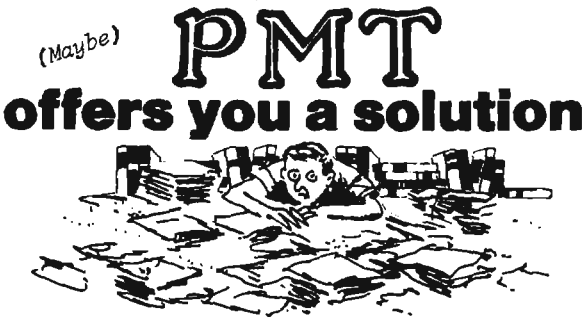
- if the ending is AM, the case is dative plural, so the English gloss is pluralized and '(to)' preposed;

- and so on for locative, genitive, and instrumental plural.

No modification to the gloss is required if the noun is nominative or accusative singular, so those endings are not tested. Nouns in the dative and locative singular have identical forms; the gloss could be modified by preposing '(to/in/of)' with 'of' reflecting the frequent omission of the preposition O which governs the locative, although this is not yet done due to the clutter. A genitive singular noun looks the same as a nominative or accusative plural: '(?of)' is preposed since the genitive is more common, with the hope that users can accommodate the times when a plural occurs.

(U) A small amount of syntactic analysis takes place in disambiguating certain adjectival forms. (Otherwise the unambiguous noun that follows might produce a preposition lying between the adjective and the noun.) For example, adjectives ending YM may be instrumental singular or dative plural. In the latter case, the following noun will generally end AM. The program looks ahead one word and examines the ending: if it is AM, '(to)' is preposed to the adjective's gloss; otherwise '(?with)' is preposed.

(U) Whenever adjectives acquire a preposition, the program prevents the following word (if it is a noun or another adjective in the same case) from acquiring a preposition as well.



(U) Participles represent a more complex situation. A Russian participle may be regarded as a verb stem plus a participial suffix plus an adjectival ending. Some adjectival endings coincide with verb endings (IM for example), so the presence of a participle must be tested before such endings are declared to be verbal. So if a verb ends with any of two dozen or so adjectival endings, the preceding few letters are examined. If they are SC, SCH, or Q, the word is almost certainly a present active participle, so the English suffix -ing is added to the gloss, and the word is treated as an adjective; as indicated earlier, the adjectival ending may cause a preposition to be added to the gloss. The other participial suffixes are treated similarly.

(U) The above does not exhaust the richness of Russian morphology; it merely serves as an indication of ways by which much semantic information may be extracted without unduly complicating the program or increasing its run time.

(U) English morphology is comparatively simple. The irregular verb 'be' is rendered 'is', 'was/were', and 'being' as in OTSUTSTVUET 'is_absent'. (Note that by convention it is the first word of a multiword gloss that is inflected.) Use of other irregular words is discouraged; the gloss 'come' should defer to the regular s verb 'arrive'. The program can handle the spelling changes exemplified by word like 'indicated', 'shipped', and 'cities', but there is no convenient way to get both words like 'considering' and words like 'referring' spelled correctly, so misspellings like 'refering' will be encountered from time to time.

[redacted]

[redacted]

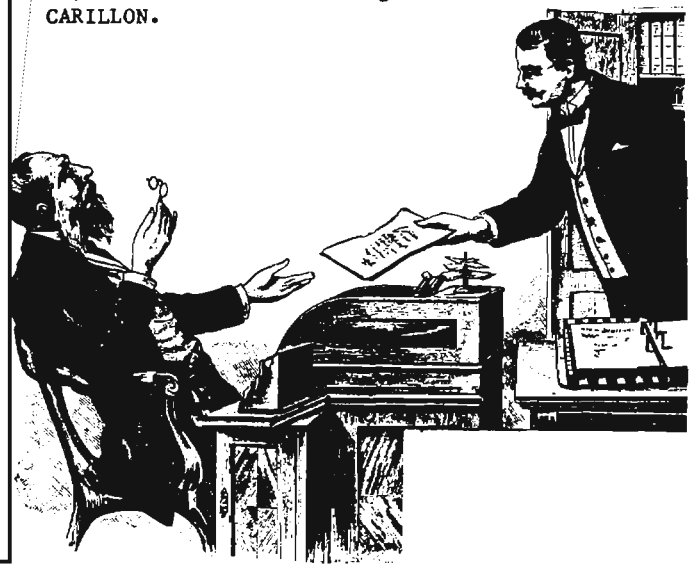
V. Russian PMT: Technical Details ~~(SC)~~

[redacted]

(U) Cleanup would achieve only minimal advantages if applied to the language-independent version, but it constitutes an integral part of this version.

[redacted]

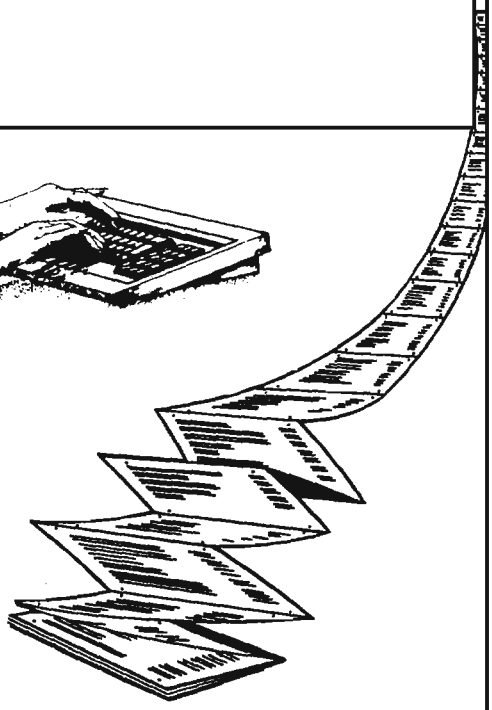
(U) The lexicographer's copy of the dictionary resides on a CARONA file which can be updated using the Rand editor. This, however, is not a form which the main program (CAKILE) can use. Whenever the dictionary is modified, a program (UCDICT) must be run to restructure it, and store the resulting file on disc at CARILLON.



(U) The structure used is the Unary Chain Dictionary, which is completely described in [redacted] paper of the same name. Suffice it to say that this structure:

[redacted]

[redacted]

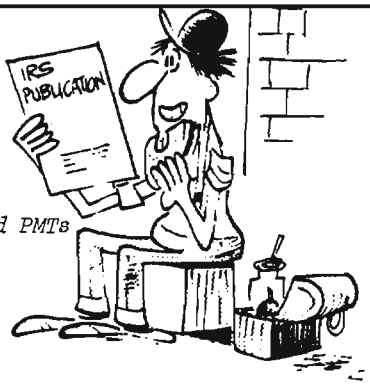


[redacted]

EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36



What else could PMTs help us with?

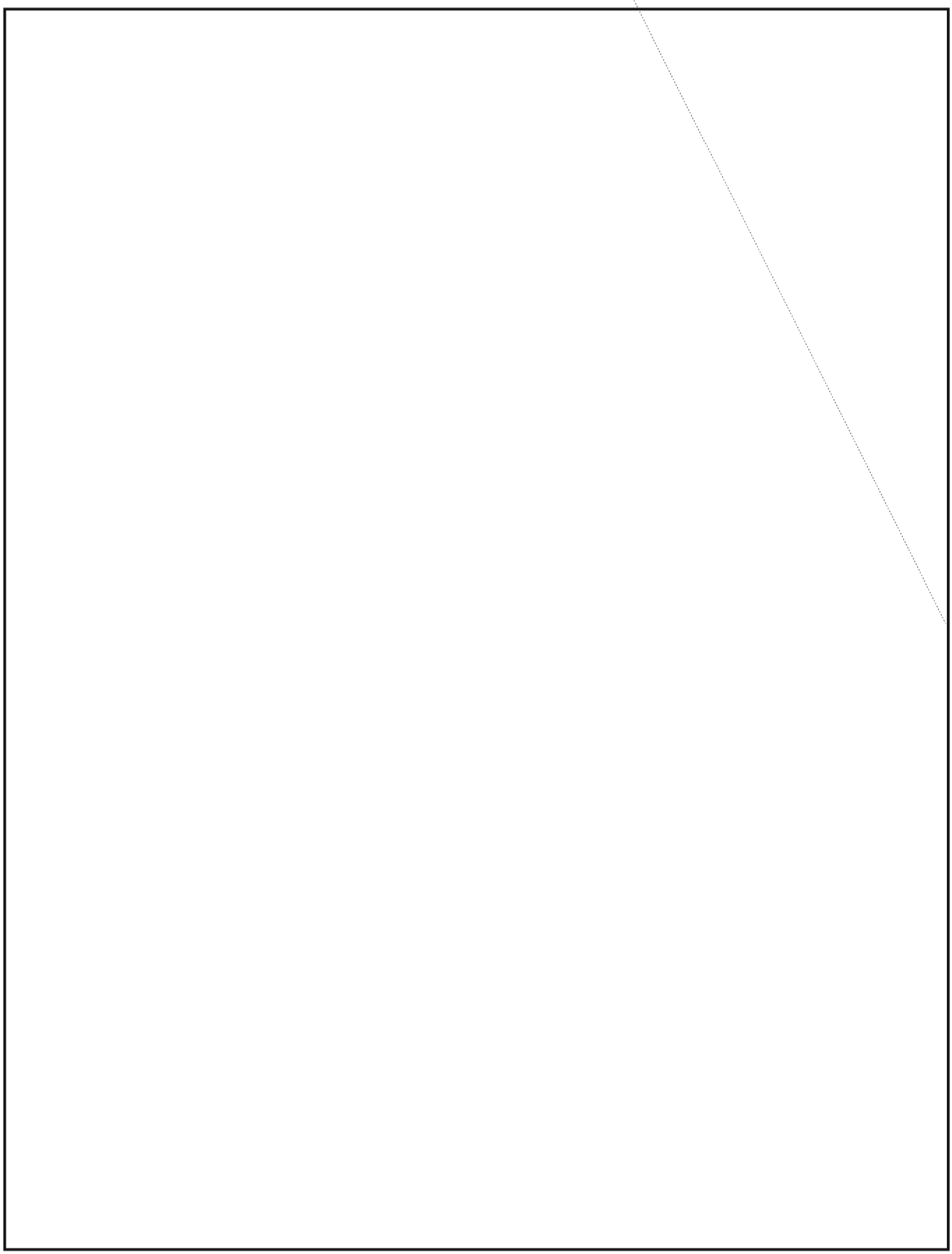
~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36

(U) Most of the programming effort needed for PMT has already been expended. The Russian PMT dictionary requires further expansion by a qualified linguist/analyst. For other languages, considerable linguistic effort must still be invested to produce usable output. It is up to potential users to evaluate the extent to which such an investment would yield profits in the form of more judicious use of linguistic resources.

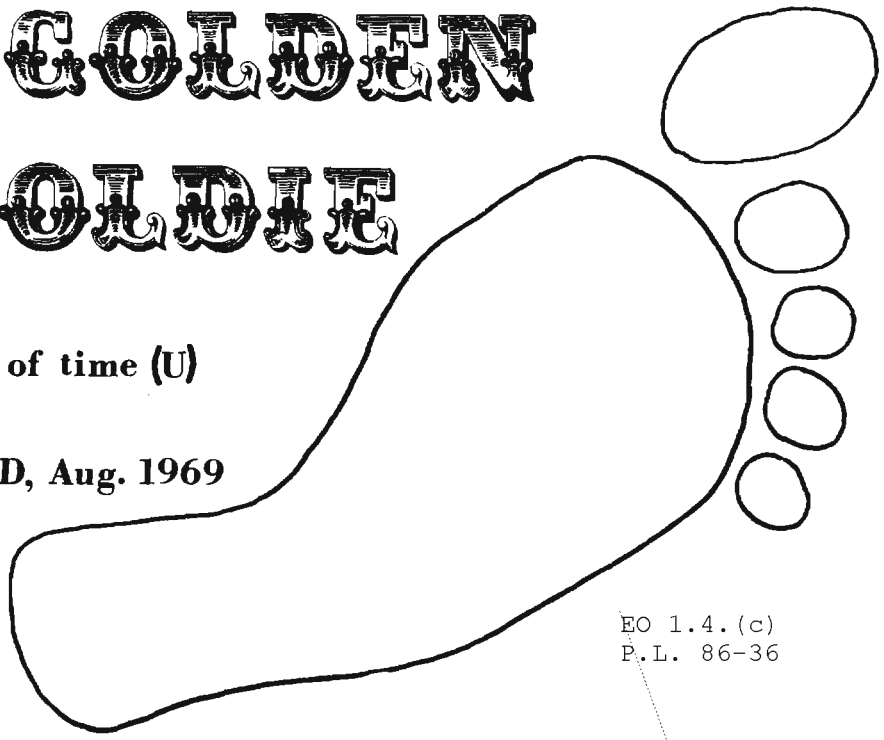
P.L. 86-36
EO 1.4.(c)

VIII. Appendix



DOCID: 4033690

GOLDEN OLDIE



Tracks in the sands of time (U)
by Fred Mason
from COMMAND, Aug. 1969

EO 1.4.(c)
P.L. 86-36

Go, stalk the red deer o'er the heather,
Ride, follow the fox if you can!
But, for pleasure and profit together,
Allow me the hunting of Man, --
The chase of the Human, the search for the Soul
To its ruin, -- the hunting of Man.

The Old Shikarri
Rudyard Kipling

~~(SC)~~ In this game[1] we play, called TA, what matters is the target, not his spoor. Where <u>is</u> he <u>now</u>, who <u>is</u> he, what <u>is</u> he doing? To trail him by his aliases of otherwhen and plot him by his utterances of otherwhere is useful only if you are catching up.

(U) It is a terrible temptation to follow his red herrings, to watch the flutterings of a Mother Bird when you near the nest. And one of our major problems with computers is the relatively enormous storage capacity -- most of which contains old target spoor; not even his present evasions.

(U) One of the best ways of distracting our attention from here and now is to offer us more than we can assimilate -- and to tease us with patterns which change so often and so erratically that we lead ourselves off course -- we "hunt[2]."

~~(SC)~~ There are an infinite number of points[3] on a line and the target signal officer attempts now to draw our attention to as many of these points[4] as possible -- to distract us from the line.

DOCID: 4033690

[redacted]

(U) Sounds like the description of the human brain -- a finite number of cells with an almost infinite number of interconnections.

[redacted]

~~(SC)~~ Is all this necessary? Yes and no; depends on the target and the analytic purpose involved. Having a limited number of analysts, it is vital to our success in catching the target that we do not waste our time.

[redacted]

~~(C-CCO)~~ The only problem here is the <u>in between</u> situation: no continuity, but we still hope to achieve it. Old sets on which continuity has been lost (or never achieved) remain useful for this purpose over a limited period -- but very limited.

~~(SC)~~ The point of all this is to urge that we purge. Yes, we must deal with <u>all</u> of today's intercept -- sort it into homogeneous piles and distribute it properly -- milk it of its current content -- report it as <u>reflections of real units, here and now.</u>

[redacted]

Cope with today today and save only as much of the many yesterdays as you must -- preferably in summary form only. Don't be so bemused by old tracks that you have no time for those still hot -- get rid of the old ones.

As you ramble on through life, Brother,
Whatever be your goal,
Keep your eye upon the doughnut
And not upon the hole.

Anon.

---

1. And it is a game -- against a player at least as clever as you -- his life or death at stake (yours, too, if you are part of our team present in the arena).
2. Oscillate alternately to each side of a neutral point because of insufficient stability controls.

[redacted]

4. Or, he offers us trees in hopes that we won't notice the forest.

Everything's coming up roses...

A nostalgia piece by an unknown author, on music from the early part of this century. Have fun with Word R!

NSA-Crostic No. 39

1 U	■	2 G	3 J	4 D	5 K	■	6 Q	7 J	8 O	9 A	10 W	■	11 O	12 D					
13 A	■	14 F	15 J	16 O	17 C	18 W	19 L	20 S	21 G	22 R	23 K	■	24 M	25 N					
26 S	27 H	■	28 W	29 T	30 R	■	31 P	32 W	33 N	34 F	35 Q	36 G	37 E	■					
38 H	39 V	40 W	■	41 N	42 T	43 J	44 G	45 C	46 K	47 P	■	48 M	49 F	50 I					
51 T	52 G	53 H	54 J	■	55 K	■	56 U	57 V	58 M	59 T	60 C	61 A	62 F	■					
63 D	64 T	65 N	66 B	■	67 F	68 V	69 M	■	70 K	71 J	72 P	73 N	■	74 S					
75 A	76 T	■	77 C	78 I	79 M	80 G	81 O	82 Q	■	83 M	84 N	85 R	86 I	87 D					
■	88 L	89 N	90 H	■	91 K	92 R	■	93 Q	94 W	■	95 J	96 H	97 O	■					
98 E	99 D	100 F	101 C	102 T	103 O	104 H	105 U	106 N	107 L	■	108 W	109 M	110 H	111 U					
■	112 V	113 K	114 G	115 W	■	116 B	117 E	118 G	119 M	120 C	■	121 B	122 E	■					
123 T	124 F	125 P	126 N	127 Q	■	128 M	129 T	130 J	131 G	132 U	133 V	■	134 N	135 K					
136 V	■	137 A	138 M	139 P	140 F	141 G	■	142 D	143 R	144 M	■	145 F	146 P	147 S					
148 M	■	149 B	150 J	151 T	152 Q	■	153 M	154 I	155 O	156 B	157 V	158 P	159 C	■					
160 E	161 R	162 J	■	163 C	164 F	165 T	166 L	167 H	168 N	169 U	170 W	■	171 J	172 R					
173 C	174 K	175 V	176 H	■	177 U	178 B	179 Q	180 P	181 F	■	182 G	183 S	184 P	185D / 186L					

DOCID: 4033690

A. British composer (1763—1824), wrote "The Bay of Biscay"
13 75 61 137

B. Pseudo-Swedish popular song of 1939
178 156 66 116 121 149

C. American comedian; foreign capital
101 17 163 120 60 173 159 45 77

D. Musical of the early '30s, in which Bob Hope appeared
185 4 142 99 87 63 12

E. Singing family
37 98 160 117 122

F. Orchestral signal for brass instruments to play loudly
145 9 164 100 34 62 14 124 49 140 67 181

G. Razaf and Waller's Rose (1929)
44 21 131 52 182 141 80 36 2 118 114

H. Victor Herbert's Rose (1909) (2 wds)
96 38 104 90 176 27 53 167 110

I. He wanted to "get somewhere" with his girl, but alas, all he could do was "get out and get" this
78 154 50 86 15

J. Clarke and Hanley's Rose (1921)
54 130 43 71 95 162 150 7 3 171

K. Alcott's Rose (with "My'), 1899 (2 wds)
5 174 70 135 55 46 91 23 113

L. "Honey Boy" _____, minstrel of the turn of the century
107 166 88 19 186

M. Non-commercial, low-cost, often experimental drama; permises in which such dramas are presented (2 wds)
24 119 148 128 58 69 79 109 153 83 144 138 48

N. Song hit from "The New Yorkers" (1930) (3 wds)
106 134 168 73 84 25 41 33 65 89 126

O. Place for dancing, accoring to Dietz and Schwartz (2 wds)
97 11 16 155 81 8 103

P. "_____, will travel": want ad placed by a violinist (2 wds)
146 184 72 158 180 125 31 139 47

Q. George M cohan's Rosie (1923)
179 127 35 93 82 6 152

R. Is this a ballet dancer without her costume?
22 161 85 143 92 172 30

S. What the S-S B did at dawn (September 14, 1814)
74 147 26 183 20

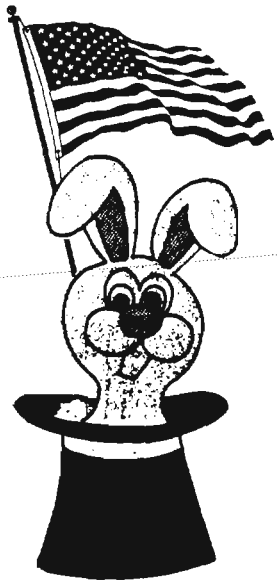
T. 20th century lyricist, often used the pseudonum Arthur Francis (2 wds)
42 165 123 51 151 102 76 64 129 59 29

U. American operatic tenor (1896—1960)
111 1 56 105 169 132 177

V. Elegy
112 68 157 57 175 39 136 133

W. Haunting melody from Word D
10 32 94 108 18 40 170 28 115

LOOKING AROUND with



P.L. 86-36

Review:

THE AMERICAN MAGIC (U)
by Ronald Lewin
Farrar, N.Y. 1982

(U) The Americans were more effective in producing COMINT against the Japanese, than in using it, in Ronald Lewin's opinion. His rather readable book skims over a lot of material, some of it recently declassified, some of it already well known, and some still classified, to give an overview of the development and use of COMINT against the Japanese before and during World War II. Pinches were important in getting started on the Naval codes in the 1920's. After that, continuity in message content, codes, cipher systems and especially in trained cryptanalytic and language personnel were critical to both the Army and Navy COMINT effort.

~~(TSC)~~ The book contains some ironies. Lewin denounces Yardley as disloyal for selling and publishing secret information that induced the Japanese to improve their cipher security. But he does not hesitate to publish Top Secret technical information about how the PURPLE machine was solved, leaked to him by one of his informants who knew about diplomatic cryptanalysis. Lewin also devotes an entire chapter, called "The Stab in the Back", to the risks and potential damage caused by the American press in revealing successes against German and Japanese ciphers. He deplores the inability of the U.S. legal system to conduct trials in camera even when the most crucial wartime secrets are at stake. He further deplores the permissiveness of U.S. society with its attitude of anything goes, "of which the FOIA is the most recent expression". None of this handwringing deterred Lewin from seeking out American and British cryptanalysts and intelligence people to get bits of "private information" to enhance the sales of his own book.

~~(TSC)~~ Lewin's book appears to have been written for a British audience, for it recounts some of the personalities and battles of the Pacific war which are fairly well known to Americans of that era. Inevitably he has serious omissions, for his sources seem to be primarily intelligence people rather than cryptanalysts, although Bundy, Filby, Raven and Tiltman are cited in acknowledgements. He does not know that in the weeks before Pearl Harbor, the main Japanese naval code JN25 was being read, but the resources were too limited to exploit it adequately. JN25 at that time would probably have given considerable insight into Japanese naval preparations. Lewin also fails to note the great importance of cryptanalysis immediately after Midway in reading the attack assessment given by the Japanese, when Nimitz was unable to get a battle report from his own subordinates. This point is clearly made in Potter's book on Nimitz. The Japanese enciphered code system was originally provided them in 1902 by the British Navy as part of the Anglo-Japanese Naval Alliance. Forty years later it was still a secure system, as delays and outages in reading the enciphered code of Army, Navy and Air Force showed. Even today it would be a difficult system. Lewin also fails to note that Royal Navy tactical doctrine, adopted by the Japanese, ordered contact reports and immediate damage reports, and these signals were very useful in monitoring and assessing sea battles. The analysis of the Japanese naval situation after the numerous clashes in the Solomon Islands depended on decrypting these prompt signals. Another point which Lewin apparently missed about Midway is that on 19 May 1942 the U.S. Navy asked the Royal Navy to send a carrier to strengthen the U.S. fleet at Hawaii, because of the loss of the Lexington, and the damage to Yorktown. The British

DOCID: 4033690

immediately inquired how the Americans knew that the Japanese fleet, whose whereabouts was a mystery to them, would attack Midway in June. Roskill's The War at Sea (V.2,p.37) recounts that Admiral King had to reveal that the U.S. was breaking into the JN25 traffic, although only in a limited way. The British did not send a carrier to Midway, but sent some cryptanalysts, including Tiltman, to Washington, to see if the U.S. Navy had actually broken the JN25 code. (When they were sure of the competence of the U.S. Navy cryptanalysts, the COMINT liason improved).

~~(S-CCO)~~ Lewin correctly gives substantial credit to U.S. traffic analysis which gave continuous intelligence on the Japanese Navy during the outages when Japanese cryptographic changes cut off ULTRA intelligence. He does not explain the long delay till mid 1943 in breaking into the traffic of the Japanese Army and Air Force, who adopted the same system in 1936 that the Navy used, as a result of a cipher compromise, nor does he touch upon the more important point that it was the higher level nets that were read, giving operational rather than low level tactical details.

~~(TSC)~~ The extraordinary wealth of military and technical information passing from Germany to Japan over the readable Japanese diplomatic and attaché ciphers is developed in Chapter 11, but the most important of this technical intelligence, viz. the details of the new German torpedoes, which allowed the Atlantic convoy escorts to utterly defeat WREN and its successors, is not mentioned. COMINT in early 1943 on German traffic warned of WREN and Royal Navy countermeasures made it ineffective in September 1943 when it was used tactically. The attaché traffic revealed all the technical features of new torpedoes, and other crucial facts about the Schnorkel and Type XXI U-Boat, which allowed prior countermeasures by the British Navy. The Germans misjudged the success of their new weapons and tactics and lost so many U-Boats that they were forced on the defensive, allowing the massive convoys and logistic buildup from mid 1943 till the end of the war without which the invasion of Italy and France would have been impossible.

~~(TSC)~~ Lewin raises a number of questions concerning the American use of the political intelligence from Japanese diplomatic and attaché links concerning Russian-German and Russian-Japanese peace negotiations, and gives an impression that a better political outcome to the war was possible from these insights, perhaps without the use of the Atomic bombs. This appears to overlook the strong interest in high policy circles in the U.S. for a friendly postwar relation with the Russians that tended to nullify the COMINT indications of Soviet military expansion.

~~(TSC)~~ The importance of plain voice COMINT during an air battle in the Marianas illustrates the opportunistic nature of COMINT, and the farsighted practice of carrying a voice gister on a major warship to exploit Japanese plain voice aircraft traffic (p.256). Conversely, the inability of COMINT to reveal the Japanese naval activities before the nearly disastrous battle of Leyte Gulf shows the extent to which even the best COMINT depends on what the target actually reveals in exploitable links. Lewin never mentions that the Flag Officers code was never read during the entire war, although it probably did contain the high level directions before Leyte.

~~(C)~~ The politics of wartime SIGINT in both Europe and the Pacific resulted from the basic fact that the traffic and the cryptanalysis had to be centralized in order to get enough related material to read the links. Inevitably, this gave the military and political people at the center of the war effort more information than the field commanders had, since they could control what was sent out. After some very dangerous compromises, including news stories identifying specific successes, Marshall and King put their personal authority into setting up and enforcing the stringent security that characterized all high level ULTRA COMINT. This not only protected the sources, but gave immense control to the two senior military commanders. In the field, security was much more uneven, for the Special Liason Units copied from the British were not welcomed in the Southwest Pacific where MacArthur sought to control all information flow. One byproduct of the secret SLU channels was a series of very frank reports by the SLU officers which came back to Washington without local censorship.

DOCID: 4033690

~~(TSC)~~ The most visible continuous COMINT success in which the intelligence was very well exploited was the merchant shipping traffic. Both Army and Navy cryptanalysts read the messages, and the conclusive success of the submarine war of attrition on unescorted merchant ships made the "island hopping" strategy feasible, and greatly reduced the cost of the war to the U.S. Other COMINT results were intermittent and scrappy until late in the war, when U.S. war production and the destruction of Japan's merchant navy had made the outcome inevitable. Lewin's extensive criticism of MacArthur seems to overlook the fact that a commander cannot be utterly trusting of the fragile and uncertain intelligence that codebreaking provided (or failed to provide) in the first half of the Pacific war. Because the lower level Japanese Army and Air Force nets used the same system of code plus additive, but did not send enough traffic to permit exploitation (so that it operated almost as one time pad), the detailed tactical information had to come from other sources. (The same was generally true in Europe). This lack of timely tactical intelligence, and the great difference between an operational order and the way it is carried out, created longstanding resistance by many operational commanders that devalued what COMINT there was.

~~(C)~~ Nimitz ranks high in Lewin's estimate as a commander and user of SIGINT, but the use of naval intelligence was inherently simpler than exploiting ground or air COMINT.

~~(S)~~ Except for Midway and the Coral Sea, COMINT gave little real help in the Pacific until 1943. The surprise at Pearl Harbor, the loss of the Phillipines, Singapore and Burma, and the unchallengable supremacy of the Japanese Navy until Midway show the ineffectiveness of American intelligence and also of Allied military forces. A point not illuminated is that Japanese military technology stood still from 1940, while U.S. weapons became much better, and with big advantages in quality and quantity, the U.S. was then able to make use of the COMINT it produced. Lewin never quite captures the inner environment of COMINT itself, and how it made itself the indispensable factor in Allied warfighting, because he deals primarily with the product, not the process. The fact that the intercepted traffic was sent by sea, or by aircraft at first, and often arrived months late, until major new radio teletype systems were put in place, is not mentioned, although this was a key factor in slow start against Japanese Army traffic. Another point missed was the role of Reischauer during 1943-45 in continuously interrupting the process oriented activities in Arlington Hall to snatch urgent intelligence from the rather inflexible assembly line of data processing. Reischauer, who held the rank of a G-2 Colonel, and his staff did the intelligence analysis from the raw decrypts inside Arlington Hall, rather than waiting for finished COMINT to arrive. Since less than ten percent of the mass of decrypts were actually useful for current intelligence, this highly informal plundering by a high ranking expert was essential to timeliness and correct selection.

~~(S)~~ The intense concern at high levels with security and secrecy, and the resistance and insubordination of the field commanders to these secrecy measures, is illuminated. The letter from Marshall to Dewey illustrates the fact that the success against the Japanese codes was the subject of national gossip, well outside Washington, all during the war. It is hard to imagine that the diplomats in Washington were not aware of these stories. The Americans were not only two years behind the British in defining doctrine about COMINT security that applied to operational commanders, but at Arlington Hall they had a massive turnover of staff because the clerical employees didn't like the work, and got other jobs. Interservice rivalry did provide some interest in secrecy, but it took several years and the imminent peril of losing their only reliable source of intelligence that invoked the imperious wartime diktats. In spite of this, literal decrypts found their way through

DOCID: 4033690

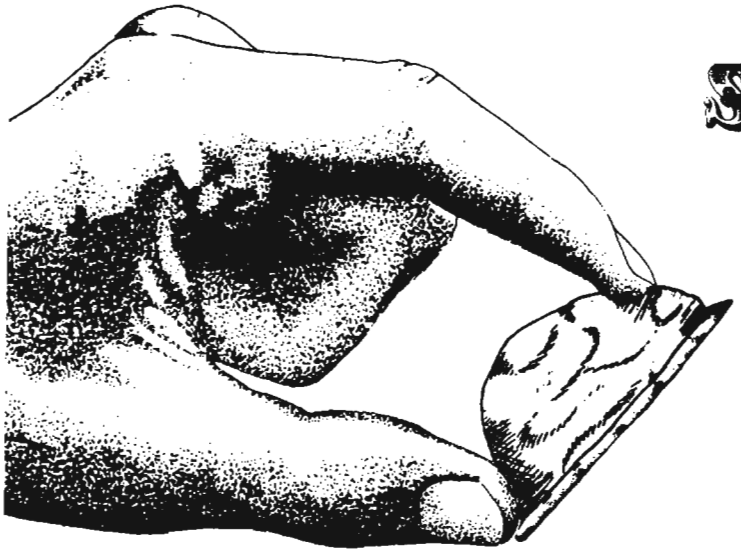
leaks and diplomatic channels into public media, revealing that specific Axis systems were being read. The military orders establishing security procedures apparently did not affect non-military elements.

~~(TSC)~~ Lewin repeats the well known stories of how all the German and Japanese messages about cipher security reported the conclusion that their crypto-security was beyond question, yet the fact is that the Germans knew Enigma was being read currently in 1943, correctly believed their Abwehr ciphers were being read in late 1941, and took numerous physical, personnel and cryptographic security measures to defeat enemy cryptanalysts, which were successful but too late to help them. The Japanese introduced a number of cipher and code changes on military and non military traffic, including the use of encipherment squares, but some of their changes were more insecure than the procedures they replaced. However, the changes were to the system, not just new crypto materials. The far flung Japanese had the special disadvantage of sending the cipher security changes over the radio links that were being read. Efforts to distribute new crypto materials to change the diplomatic and attaché ciphers were thwarted by Allied military action. These energetic and difficult cryptographic changes by the Axis indicate they were less complacent about cipher security than the self confident conclusions sent over the channels we were suspected of reading. It is probable that overall secrecy about COMINT successes was much less than the victors assume.

~~(TSC)~~ One of the most important points that Lewin seems to slight is the great difference in intelligence production from codes versus ciphers. The Japanese military and naval traffic was primarily in code, and when the books had to be recovered the intelligence was invariably much more scrappy and uncertain than with ciphers. Routine messages with little intelligence value would be the most completely decipherable, while non routine messages would contain mostly undefined groups for months. Recovered meanings change, e.g., today's Tokyo can become tomorrow's Yokohama, and this makes it impractical to exploit daily traffic without chaining backwards and forwards to other traffic. Of the huge volume of decrypts, less than ten percent was actually used for current intelligence. The bookbreaker was always the key person in the intelligence process, and the U.S., like the British, used professors of exceptional ability to get the combined problem of language, bookbreaking and intelligence analysis right. A codebook change was disastrous to intelligence continuity for weeks or months, unlike cipher machine key changes that gave up all their secrets, once solved. Captures were often the only way to make traffic currently exploitable, and they were planned and executed with murderous efficiency as the war progressed.

~~(TSC)~~ Whenever he can, Lewin points out the mistakes the Japanese made that allowed their systems to be broken and exploited. The difficulty of solving the attaché CORAL system is cited, with references to a 1981 letter from Raven. The importance of reencipherments and cribs in attacking PURPLE, and the crucial value of low level weather traffic in giving cribs into a high level system, are described. The fatal error of the messages giving successive ship noon positions, which allowed submarine ambush, is elucidated. Presumably Lewin wants to assure that no one will ever make those errors again. Declassification is probably the epitaph for future Naval COMINT.

(U) Summing up, Lewin's book is a readable but often specious commentary on the production and use of SIGINT against the Japanese. The classified and declassified official reports and histories written by both Americans and British during and after the war are better and more insightful. Lewin obviously applauds the American COMINT effort, but not being an insider he misses most of the color and "war stories" and contingent detail that would convey the intense commitment, rivalry and sense of mastery that were central to the success. Enjoy it, then seek out the real thing.



SHELL GAME (U)

W. E. S.

One of the more useful features about UNIX is the shell, which permits one to put together a file of commands and then execute them simply by naming the file. It is easy to use, and easy to change. Once the file is made (normally using the Rand or screen editor), the mode of the file is changed to make it executable (using the command chmod), or one simply types:

sh filename

and whatever commands are in the file called filename are executed, in whatever order they appear in the file.

In my early days of learning about UNIX, I learned more about it by prowling around through other people's shell files than by any other method. We have begun to get security conscious on the various systems, and so it is harder to poke through other people's directories and files. Nevertheless, it is still instructive to look over other people's shoulders. Therefore, we propose to set up an irregular feature called Shell Game, showcasing various shell files that actually work. (At the present time, it is probably a good idea to limit exhibits to Version 6 UNIX, since that is the most common version now being used here.) To begin the series, we offer two simple shell files.

CLEANUP is used to 'housekeep' by throwing away the many '.bak' files that tend to accumulate when one uses the Rand editor a lot. The name of the file is in capital letters, so that it comes at the head of the list when I type ls -l to look at my filenames. The file looks like this:

```
find /u2/wes -name "*.bak" -a -exec rm {} ";"
cp /dev/null /u2/wes/CLEAN.last
```

It contains only two lines. The first line uses the UNIX command find in the following way:

- find
  - UNIX command
- /u2/wes
  - tells the system where to start looking, i.e., begin here and work downward,
  - my directory is in filesystem u2, and my username is wes
- -name "*.bak"
  - look for any file whose name ends with .bak
- -a
  - and
- -exec rm {} ";"
  - execute the UNIX command rm (remove) to whatever is found.

The second line makes a copy of a system file called /dev/null, and names the new file /u2/wes/CLEAN.last.

The system file /dev/null is sometimes called "the bitbucket" because it is always empty. You can send an output to /dev/null and, in effect, throw the output away. Or, as in this shell, you can create an empty file. The empty file CLEAN.last is used as a place to record the time you last executed CLEANUP. When you type in ls -l one of the top lines should look something like this:

```
-rw-rw-rw- 1 wes      0 Mar  1 17:39 CLEAN.last
```

which would show you the date and time of the last CLEANUP.

The second file is called (in my directory) names. (You can, of course call it whatever you want in your directory.) Its purpose is to bring up to the screen the full names of anyone currently working on the system. It looks like this:

```
who
who | reform +t8 | rpl "^" "name " | sh
```

This shell was built to use as part of a demonstration of UNIX capabilities. The UNIX command who gives a display something like this:

```
lct      ttyj Mar  4 08:16
rsh      ttyG Mar  4 08:31
norm     ttyK Mar  4 08:52
sue      ttyL Mar  4 10:02
wes      ttyX Mar  4 08:10
```

The UNIX command name takes up to nine usernames and returns the full names of the users. For example,

```
name dlr wes
```

might return the following:

```
dlr     P14
wes     P14
```

The first line of the shell file simply sends the result of the 'who' command to the screen, in the usual way. The second line sends the output of the command 'who' through a pipe (|) to become the input of the command 'reform', which throws away (truncates) everything after the 8th position on each line.

The output of the 'reform' command is piped to become the input for the 'rpl' or replace command. Here the 'rpl' is used to insert the five characters "name " (including the space) at the beginning of the line. Although it won't make any difference in this example, the 'rpl' usually throws away any trailing blanks, i.e., any blanks at the end of the line - in this case, all blanks from the end of the username out to the 8th position.

Once more the output is piped, this time to the command 'sh' (UNIX shell). The input to 'sh' looks something like this:

```
name lct
name rsh
name norm
name sue
name wes
```

The command 'sh' will cause each line to be executed in turn, and since no output direction is indicated (i.e., no > is given), the output will come back to the screen.

One of the reasons for getting the output of 'who' onto the screen first is that 'name' is a bit uncritical: it takes the string of characters in the user name, and brings back any line containing that same string. For example, the command

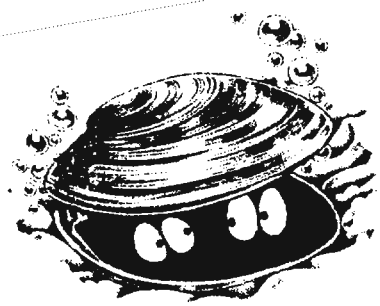
```
name wes
```

might bring back

```
wes     P14
 drl    Z43
```

one of which is the one we want.

P.L. 86-36



DOCID: 4033690

WORD PROCESSING IN A4(U)

by [redacted] A41

P.L. 86-36

The author wishes to thank [redacted] Without her encouragement and generous help, this article would certainly not have been written.

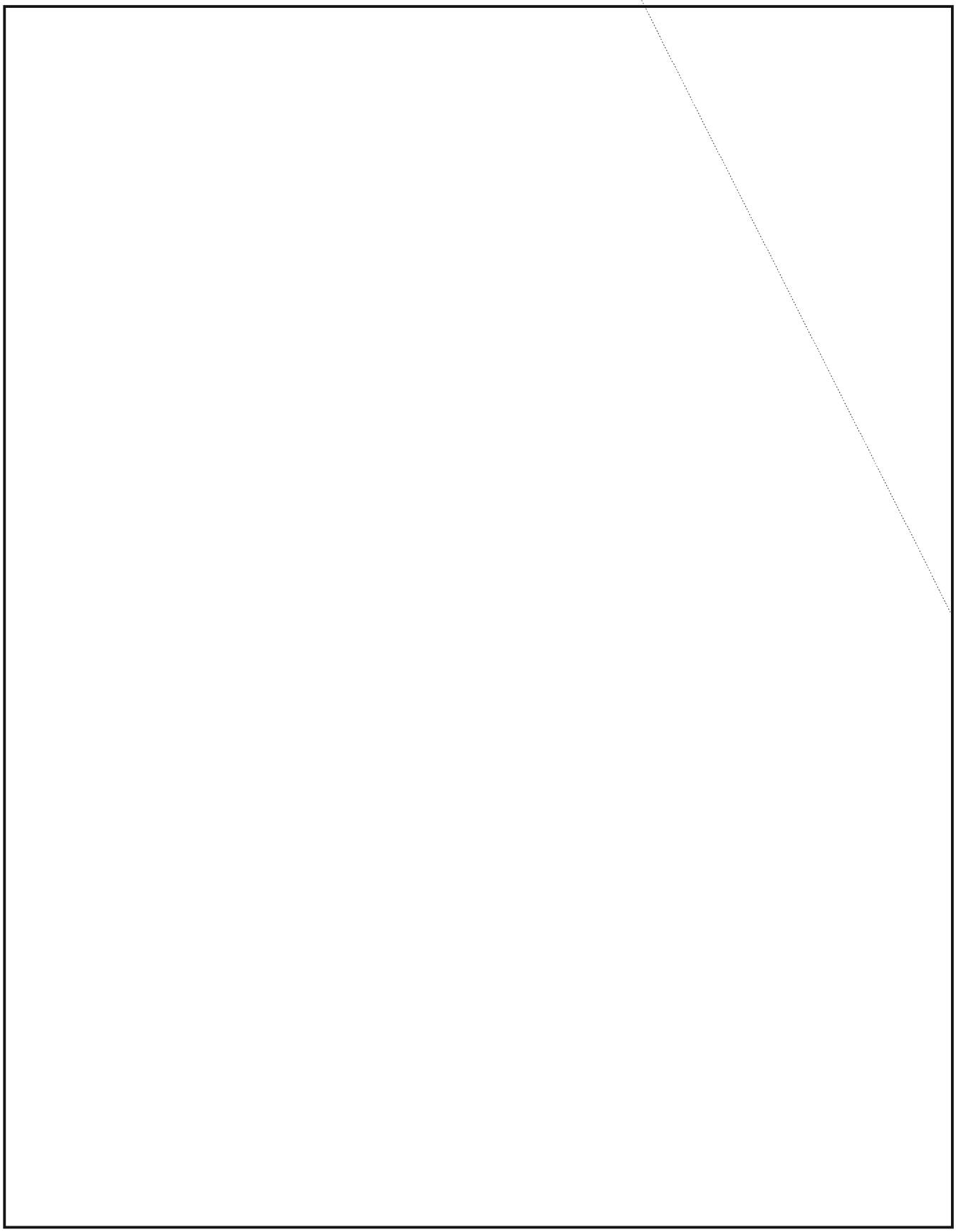
This report describes a study of document production by A41 personnel. Its purpose was to provide a basis for planning office automation ~~(FOUO)~~ efforts in A41, and the findings have been extended by extrapolation to cover all of A4.

~~(C)~~ The results to be presented here relate directly to "putting words on paper," an activity which represents about one quarter of A41's productivity baseline. Document production was selected for initial study because it offers the simplest and most direct opportunity to improve productivity in an immediate time-frame.

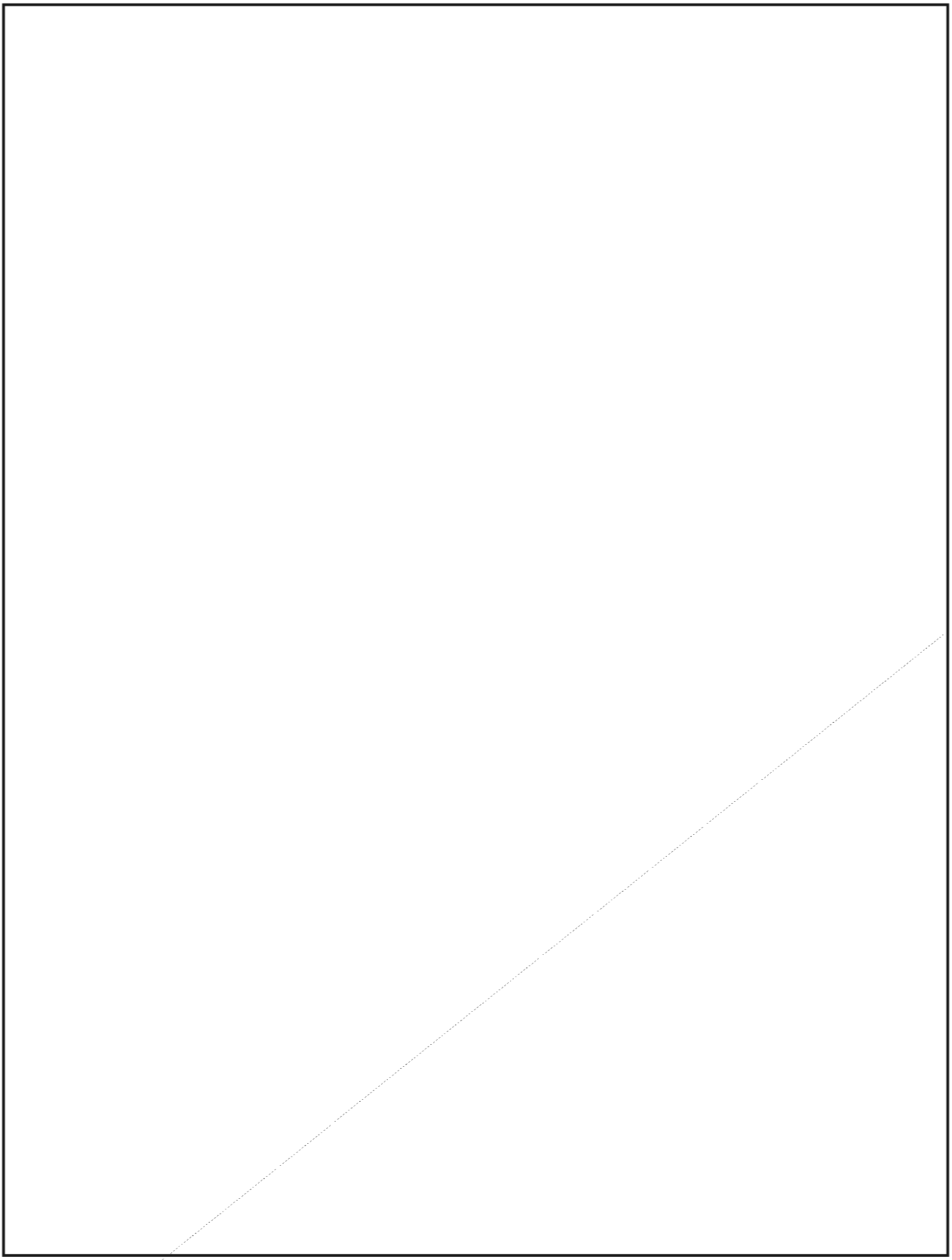
[redacted]

[redacted]

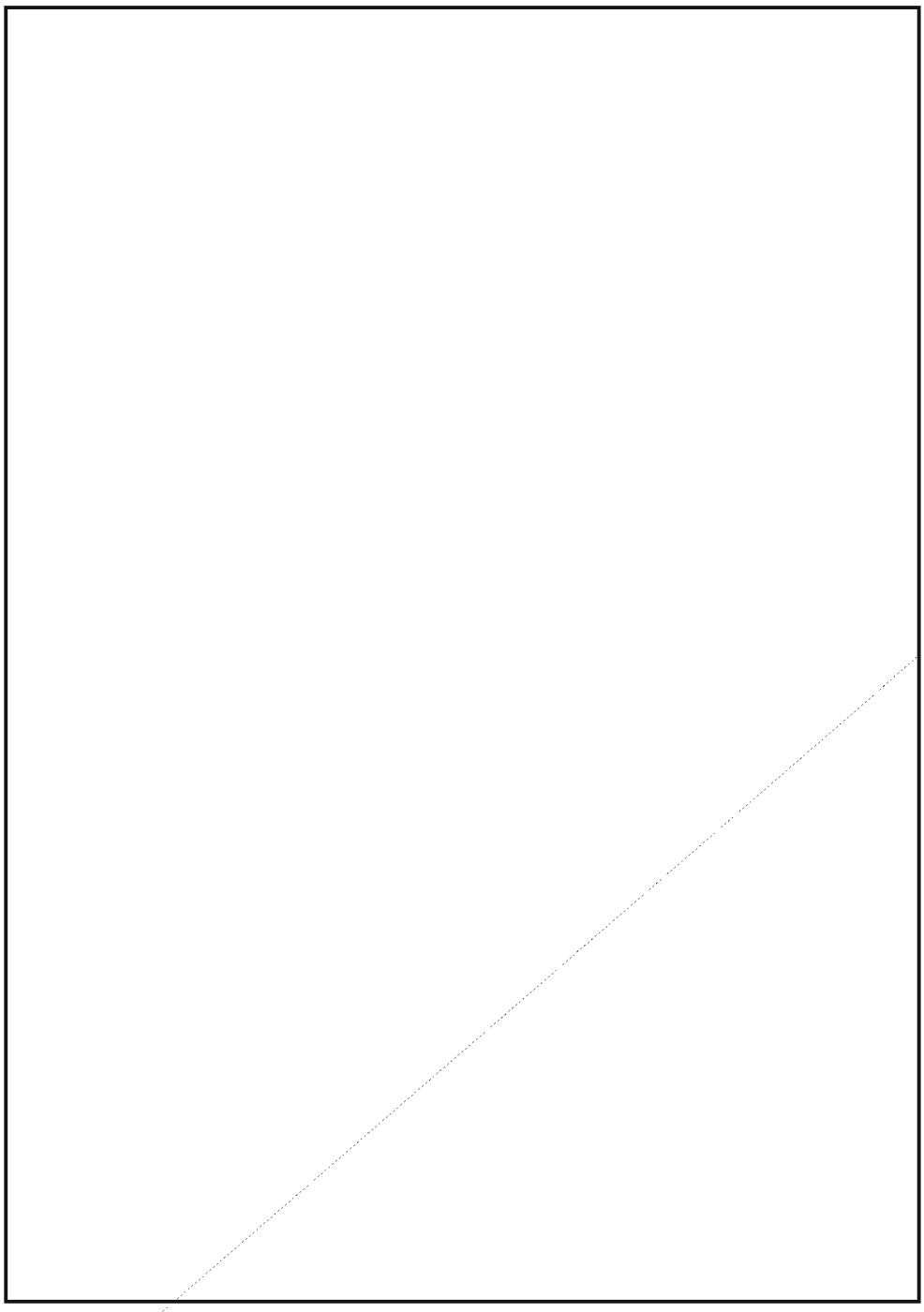
EO 1.4.(c)
P.L. 86-36



DOCID: 4033690



EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

A4 WORD-PROCESSING REQUIREMENTS (U)

(U) The findings in this report were developed by extrapolation from the results of a survey of document production in A41 (above), supplemented by other estimates and computations. This summary was prepared in support of a request for word-processing equipment for A4. The data were collated and organized for use in documentation required by T443, entitled "Word Processing Requirements Workload and Resource Summary (Feasibility)".

[redacted]

[redacted]

(S) CURRENT DOCUMENT PRODUCTION RESOURCES AND COSTS. Full-time typists in A4 use automatic equipment for 50% of their document production and manual equipment for the other 50%. They do not use any overtime hours. Author/word generators spend 24.2% of their work hours in document production (10.1% in preparation, 1.4% in proofreading, and 12.7% in typing). They require 540 hours of overtime quarterly. Current cost of electric

[redacted]

P.L. 86-36
EO 1.4.(c)

[redacted]

REFERENCE

1. "Guidance on Requirements Analysis for Office Automation Systems," NBS Special Publication 500-72, National Bureau of Standards, December 1980

DOCID: 4033690

BOOKBREAKERS' FORUM on MACHINE AIDS

P.L. 86-36

[redacted] **P16**

A funny thing happened on the way to the Forum ... [redacted] USA, was waylaid ~~(C)~~ in the mustering-out process and didn't make it as scheduled. But we had a profitable meeting nevertheless. While we sipped tea and munched cookies, [redacted] Chief P13, brought us up to date on personal computers and how they are helping B Group analysts, and what we might look forward to in the future. [redacted] G95, described the bookbreaking programs he wrote on [redacted]

[redacted]

[redacted]

(U) [redacted] told us about a software package P13 bought which has been successfully applied to administrative files in P15 and B6. For details, call [redacted] on 3045s.

P.L. 86-36

~~(C)~~ Down the pike, Gene tells us, are very powerful personal computers which will allow bookbreaking to be done on all but the biggest codes. It's way off, so don't hold up work on a going problem waiting for it.

[redacted]

P.L. 86-36
EO 1.4.(c)

DOCID: 4033690
P.L. 86-36
EO 1.4.(c)

~~CONFIDENTIAL~~

[redacted]

~~(C)~~ Moving? Cleaning out?

Give your old code materials a good home. You can send them, including codebooks, runs, sample messages, write-ups, mag tapes, punched, cards, etc., to:

[redacted] T54, SAB 2 Door 3, 2268s,

or

[redacted] P16, 8A187, 1103s.

~~(C)~~ Notice to [redacted] users:

In mid-1983 RYE will be deactivated. That means that you will have to find some other means for processing your code messages. You really ought to start right now looking for a replacement program. If you wait too long, you may find that the plug has already been pulled, and that all your data is lost, including the codebook used for decoding the messages, and all your message files. I'll be glad to help you find an alternative way, if your support people don't have something that can be implemented in good time. The chances are very good that in some other area there's an operational program that can be adapted to your needs.

[redacted]
P16 x1103s

P.L. 86-36

Personal Computer Application (U)

P.L. 86-36

[redacted]

P13

One aspect of P13's mission is to investigate the use of personal computers for cryptanalysis and related functions. We make known the availability of these devices, show how they are being used in operational environments, and provide some ideas as to their future use. We provide demonstrations in conjunction with organizations such as the Bookbreaker's Forum, we participate in courses such as CA305, and we offer personal demonstrations for interested individuals or offices. These demonstrations provide us with the opportunity to show interested people a wide range of operational uses for personal computers at NSA. We demonstrate in house, custom built software applicable to specific cryptanalytic problems or to a wide variety of cryptanalytic problems, some potential uses for personal computers as cipher devices, and a wide variety of inexpensive, commercially available software encompassing managerial tools, data base management systems, and word processing.

~~(FOUO)~~ A problem recently presented to us was that of converting Universal Transverse Mercator grid coordinates to latitude and longitude. With the cooperation of the sponsoring organization and a good deal of investigation into past efforts in this area a program, written for the Radio Shack TRS 80 Model III, was produced for use with an operational problem in DDO. This program converts UTM coordinates to latitude and longitude for [redacted]

~~(FOUO)~~ A paper entitled "Conversion of Universal Transverse Mercator Grid Coordinates to Latitude and Longitude" has been published as P1 Informal Number 1, March 1982, #S-223,678 and is available to interested individuals or organizations.

~~CONFIDENTIAL~~

SOLUTION TO LAST MONTH'S

CRYPTIC CROSSWORD

ACROSS

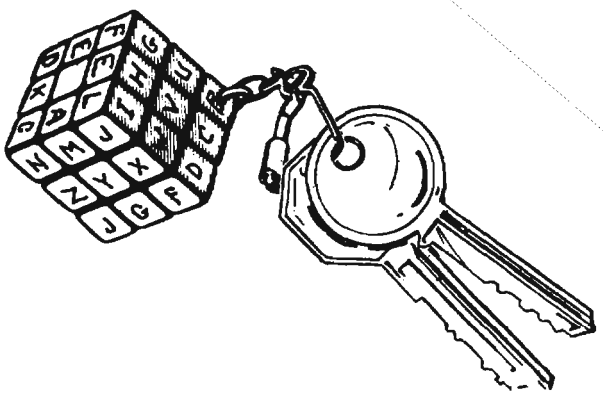
1. TRUMPET VINES
9. SECRETIVE (anag.)
10. GAUNT (gauntlet - let)
11. EMETIC (Believe me tick)
12. GATEPOST (anag.)
13. SULTAN (consult a nautical)
15. REPAIRED (rep + aired)
18. PIONEERS (pIONeers)
19. AGATHA (aGAThа)
21. REAPPEARS (reapPEARS)
23. IN A NET (anag.)
26. ELDER (el + der)
27. GLUTINOUS (anag.)

DOWN

1. TASTERS (t + asters)
2. UNCLE (double definition)
3. PREDICATE (pREDICate)
4. TWIN (t[o]win)
5. ICE WATER (anag.)
6. EAGLE (glee anag. + a)
7. AUTOCRAT (auto + car anag. + t)
8. STATED (sTATEd)
14. LEOPARDS (anag.)
16. ARGENTINA (a rain anag. + gent)
17. TRIANGLE (pun: try + angle)
18. PORTER (anag.)
20. ATTESTS (at + tests)
22. PERON (tipper once)
24. NAOMI (main anag. + o)
25. RUED (pun: rude)

SOLUTION TO 'A TOY PROBLEM'

[redacted] G9



OVERHEARD WHILE STANDING IN THE BURN-BAG LINE

"I heard a guy speaking in a briefing the other day -- and if he had been Pinocchio, he would never have gotten out of that room!"

"I haven't even thought about where. Who would ever want to eat a street map?"

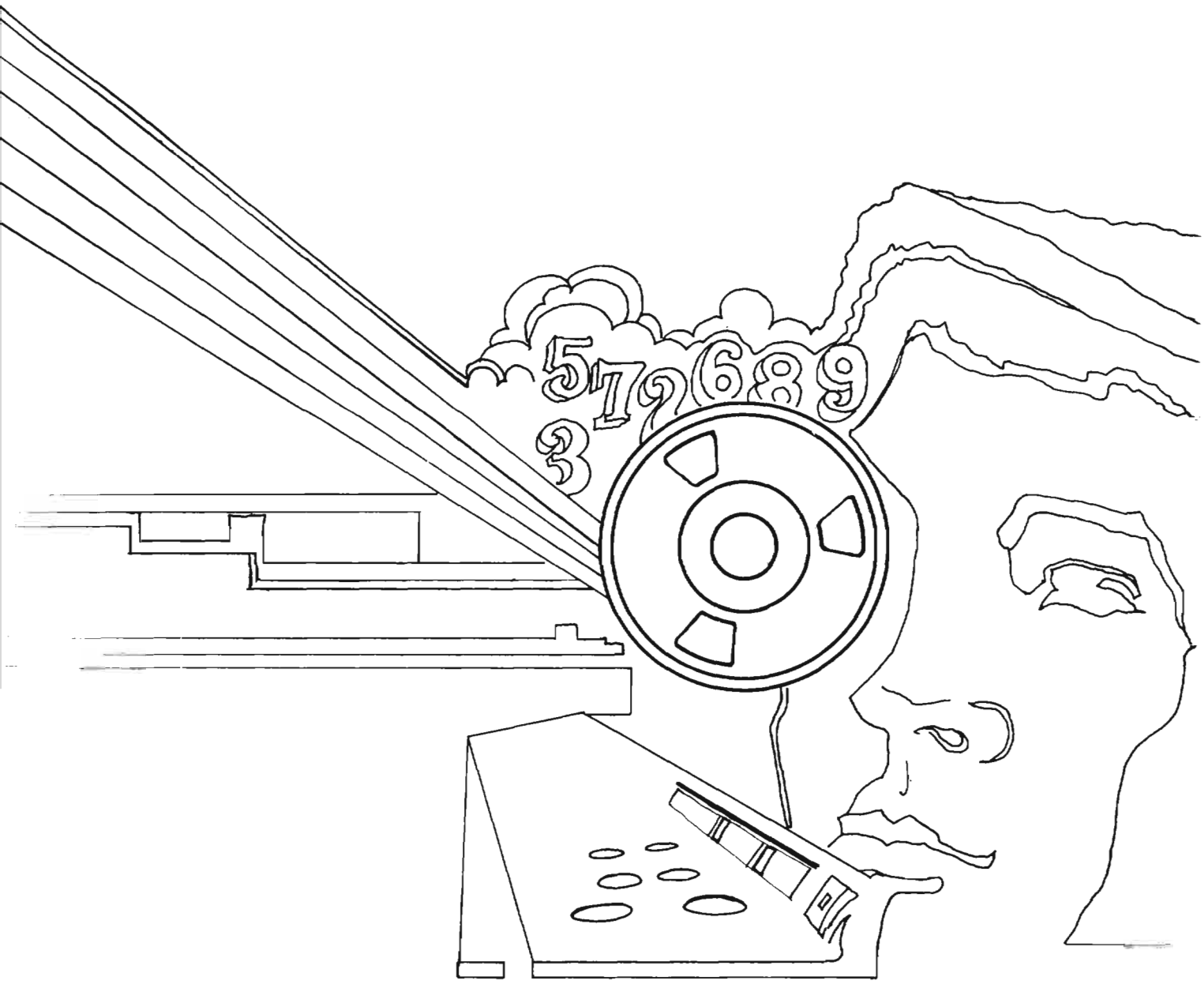
HUMAN FACTORS

Have you noticed the articles and reviews about various aspects of Human Factors by [redacted] in recent issues of CRYPTOLOG? Does the subject interest you? Did you know that there is a lot going on in this field? Conferences, courses of study, publications, and societies, including a Special Interest Group of CISI: all these are active in the field of Human Factors.

If you want to know what is going on, you ought to subscribe to the Human Factors Letter, published by the Human Factors SIG of CISI. How? Call its editor, [redacted] on x8845s.

P.L. 86-36

~~TOP SECRET~~



DOCID: 4009842

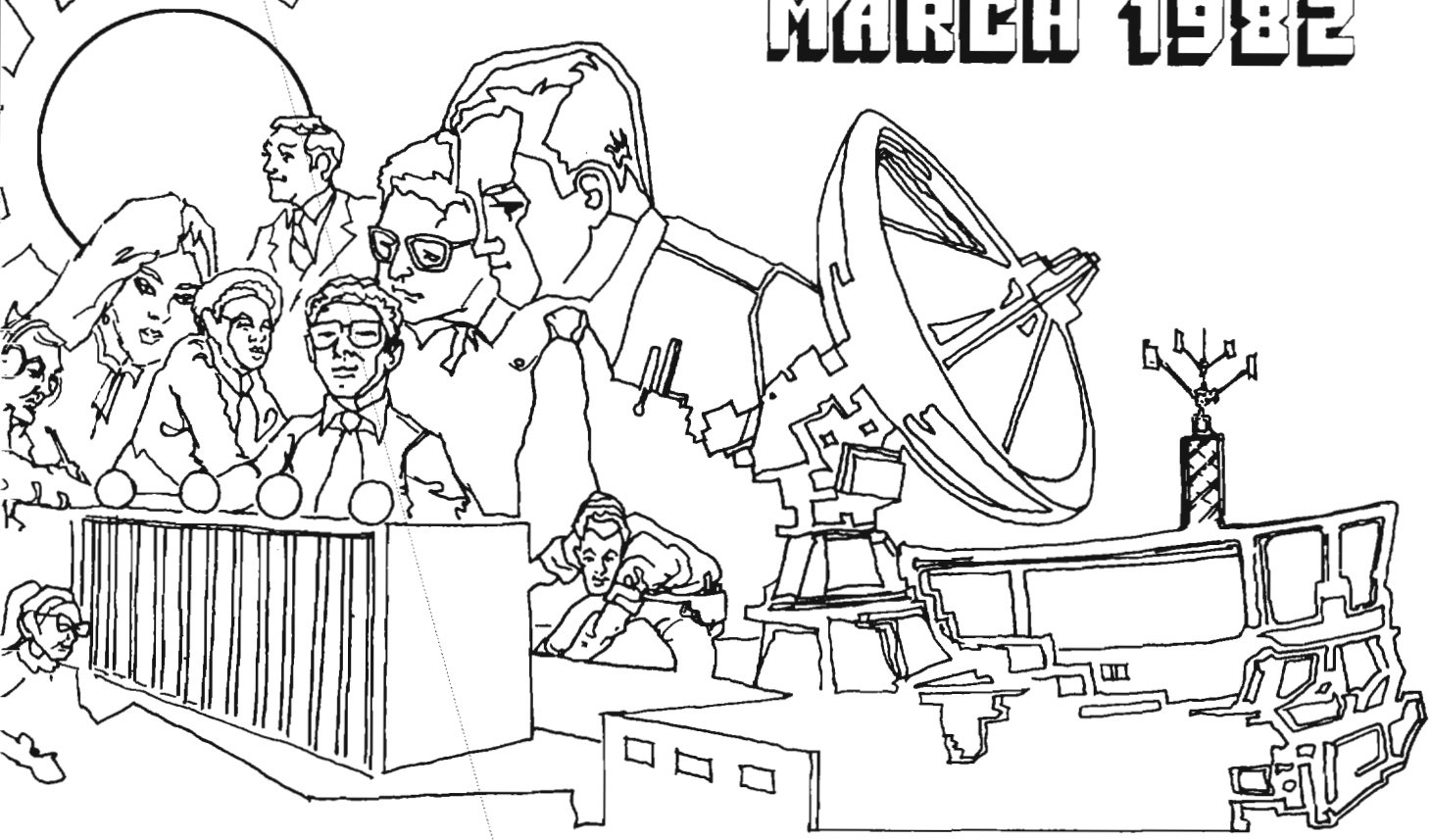
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MARCH 1982

EO 1.4.(c)
P.L. 86-36



P.L. 86-36

THE PERSONAL COMPUTER: A CURRENT CRYPTANALYSIS SUPPORT TOOL (U)	[redacted]	1
A HISTORIAN LOOKS AT SIGINT (U)	Vera R. Filby	4
METEORBURST COMMUNICATIONS (U)	[redacted]	6
[redacted]	[redacted]	8
A BRIEF TREATISE ON FIVE LAWS OF TELEPHONIC COMMUNICATION (U)	William M. Nolte	10
BUT LIFE IS SUPPOSED TO BE HARD (U)	[redacted]	12
CRYPTIC CROSSWORD (U)	[redacted]	30
RULES FOR THE CAMEL CORPS (U)	[redacted]	31
TOWARDS BETTER SYSTEM DEVELOPMENT (U)	[redacted]	32
OLD PHONE BOOKS NEVER DIE (U)	William M. Nolte	38
CONSUMER VS. COMPUTER: A REVIEW (U)	[redacted]	40
THE MAIL BOX (U)		42
A TOY PROBLEM (U)	[redacted]	43
KRYPTOS SOCIETY NEWS (U)	[redacted]	44

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 10 Mar 2012~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009842

CRYPTOLOG

Published by P1, Techniques and Standards,
for the Personnel of Operations

VOL. IX, No. 3 MARCH 1982

PUBLISHER [redacted]

BOARD OF EDITORS

Editor-in-Chief. [redacted] (7119/8322s)

Production..... [redacted] (3369s)

Collection..... [redacted] (8555s)

Cryptanalysis..... [redacted] (5311s)

Cryptolinguistics..... [redacted] (5981s)

Information Science.. [redacted] (3034s)

Language..... [redacted] (8161s)

Machine Support. [redacted] (5084s)

Mathematics..... [redacted] (8518s)

Puzzles.....David H. Williams (1103s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Taurone (3573s)

For individual (or organizational) subscriptions send name and organization

to: CRYPTOLOG, P1
or call [redacted] 3369s

To submit articles or letters via PLATFORM mail, send to

cryptolg at barlcØ5
(note: no 'O' in 'log')

Editorial

One of the interesting aspects of editing a publication is the challenge of finding out what the readers think. One of my predecessors has said that, on a scale of one to ten, a single non-angry letter is an eight, whereas an angry letter is a two (or maybe a one). It is a fact, that angry readers are more likely to write (or throw rocks through the window with a message attached -- should that be counted as two messages?) than are the satisfied (or edified or entertained or whatever) readers. How then is one to know if there <u>are</u> any non-angry readers?

All of this makes me wonder if we should deliberately put in something to angrify the readers, every so often. We could declare a "Letter Month" and see what turns people off. It probably isn't a good idea to do it deliberately; there are too many "pattern finder" people around here, and as soon as they tumbled to the pattern, they would lose interest, their adrenalin would decline, and so would the volume of mail.

The system we have now might do us just as well. It seems to be working pretty efficiently. In a recent issue, the wrong version of an article was sent to the printer; one angry response came to us in technicolor. It is being framed. If the sender had included his/her name, we might have asked him/her to help us as a proofreader. We can probably make enough of these mistakes without trying to schedule them formally.

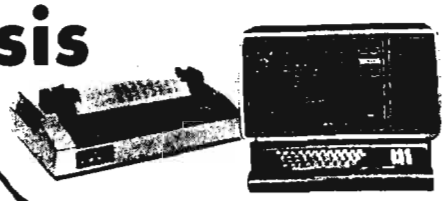
Which brings us to a related point: the errors in the magazine as you readers see it are almost always mine, rather than the author's; I am the typist/checker, so if something offends you, shout at me, not the author.

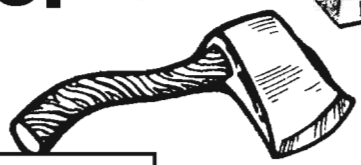
P.L. 86-36

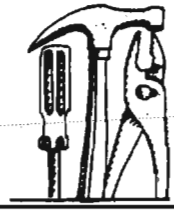
~~FOR OFFICIAL USE ONLY~~

DOCID: 4009842

The PERSONAL Computer: A *Current* Cryptanalysis Support Tool (u)



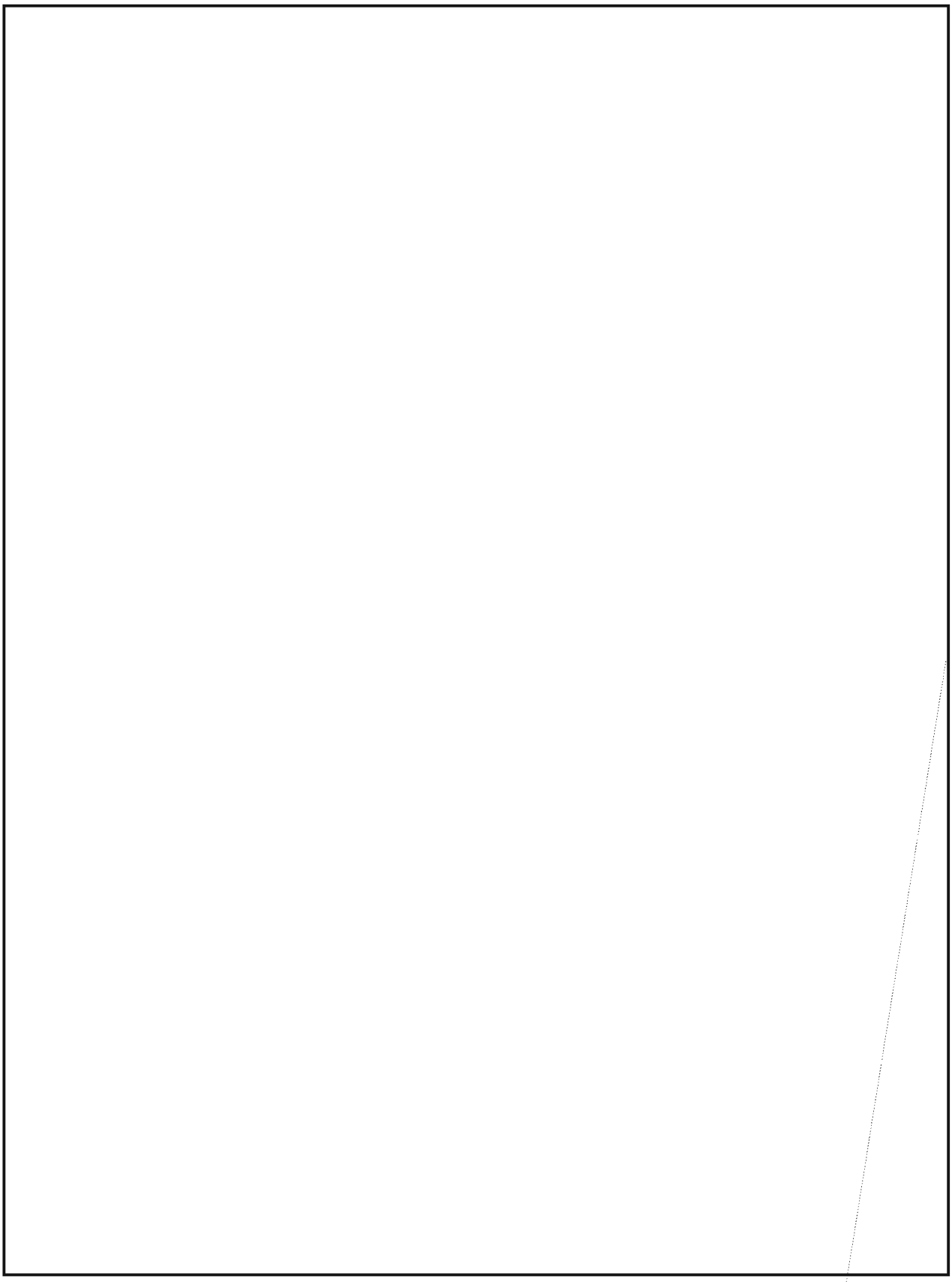




by [redacted] B53

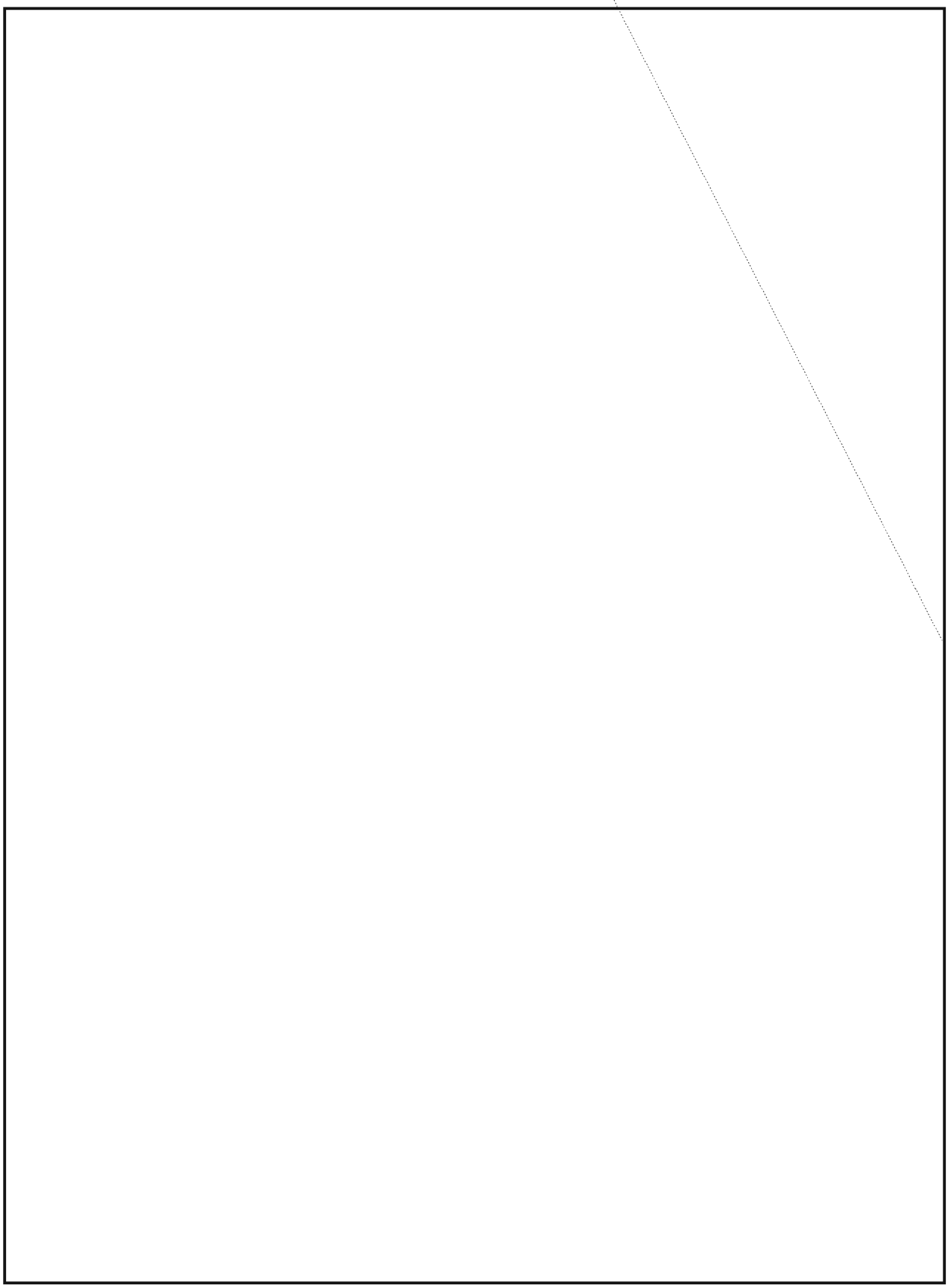
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

E0 1.4.(c)
P.L. 86-36



DOCID: 4009842

A Historian Looks At SIGINT(U)

by Vera R. Filby, E41

Eighteen senior NSA executives, along with a few representatives from the National Cryptologic School and the Director's staff, attended a seminar in the Director's Conference Room on 18 February to hear Ronald Lewin, author of ULTRA Goes to War and the recently published (February 1982) The American MAGIC: Codes, Ciphers, and the Defeat of Japan, speak on "SIGINT and Decision Making in War." The occasion was the second in a series of seminars for senior executives initiated and arranged by E6, the Cryptologic Management Department of the National Cryptologic School. At the first seminar, former Senator Birch Bayh spoke to a similarly small, selected group.

In his introductory talk before questions and discussion, Mr. Lewin presented conclusions to which his researches in World War II signals intelligence has led him. Among these were

- that the major decisions of governments were based not on intelligence but on political considerations;
- that ULTRA's most valuable contribution was the day-in, day-out accumulation of order-of-battle information; and
- that constant familiarization of intelligence staffs and some commanders with the flow of signals intelligence led to a climate of understanding;
- so that a solid base of data was the greatest contribution of signals intelligence to decision making.

Of the commanders who understood and appreciated it, he mentioned particularly Alexander, who every day "soaked himself" in the production of his "ULTRA room," and Nimitz, who understood the value of SIGINT from the beginning. Mr. Lewin stated and repeated that no praise is high enough for Nimitz as a commander.

After a coffee break, questions led to a variety of answers and issues. Among Mr. Lewin's responses were these:

- intelligence must work in action because that is what it exists to do, and
- intelligence has failed because it did not conform to the pictures the leaders had in their minds, and they were therefore unwilling to believe it. He later made the point that the value of intelligence is not in having floods of it but in having it right.

A question on Anglo-American cooperation led to Mr. Lewin's evaluation that after its tentative start in 1941 ("careful prowling around," he called it), the relationship by 1944 had become very, very close. Each country had something to give the other. Both had systems of belief in common. SIGINT

DOCID: 4009842

cooperation varied in different theaters, being least effective in the Asian and Pacific areas; but in the Atlantic and Europe it was just about perfect -- "a many-sided miracle, an example of history."

There were questions on his chapter "The Stab in the Back" in The American MAGIC. Mr. Lewin's thoughts on security and protection of signals intelligence were expressed on several levels. First of all, he said he wrote the chapter out of a sense of tribute to the dedication of cryptanalytic people. For Americans, one of the central problems was "walking a tightrope on the very highest wire." On the one side was the vital importance of protecting the information; on the other the danger of its annihilation by those who would ruthlessly expose it for unprincipled, political reasons without regard for the national welfare. He noted that the British early centralized the control of intelligence, that the Americans were less successful in resolving service rivalry -- that the Germans were riven with jealously protective rival services. The lapses of American security were of intimate concern to the British; it was their security too at stake. Even now, Mr. Lewin remarked, America has no viable way to manage the problem.

In response to questions about his evaluation of signals intelligence in war, Mr. Lewin stressed its use to the commander. (This was his theme in ULTRA Goes to War: the battle is the payoff.) In war, intelligence is useful only to the extent that it contributes to the central action, that it is present positively in the area of operations, that it meets the needs of commanders. And to this he added his conviction that commanders must understand and that they must have intelligence officers to help them understand. People believe what they want to believe. The problem is to get the truth to them.

Mr. Lewin is a military historian and biographer (Rommel, Montgomery, Churchill, Slim, Wavell), and his SIGINT perspective derives from information released to the public record since the mid-1970's. With his vast knowledge of World War II history, he has this been able to discern and examine the previously invisible presence of SIGINT in the history of the war. Listeners found his insights most interesting and perhaps a little disconcerting.

ATTENTION AUTHORS AND PUBLICITY CHAIRMEN

CRYPTOLOG is always looking for readable material. It is not a substitute for formal product or technical reports, but it does reach most of the people who are interested in the "technical underside" of our business, to borrow (and modify) a phrase. We are now publishing once a month and hope to maintain that schedule.

How can you get an article into CRYPTOLOG? Contact any one of the editors listed on the inside front cover. We don't need an abstract, and only one copy is necessary, as long as it is readable. If it is typed using a Mag Card, we can borrow your cards and use your original keystrokes. If it is typed into a UNIX system, send it to us, using the UNIX 'sndmsg' command:

- send it to

  cryptolg@barlc05

  (no O in 'log' and no spaces)

- after you have typed in 'Control D', type 'f' for file, and then name the file your article is in.

- WARNING: send only alphanumeric files this way. If your file contains any special characters, you will have to use ftp, or cftp. Give us a phone call, and we'll let you know what to do.

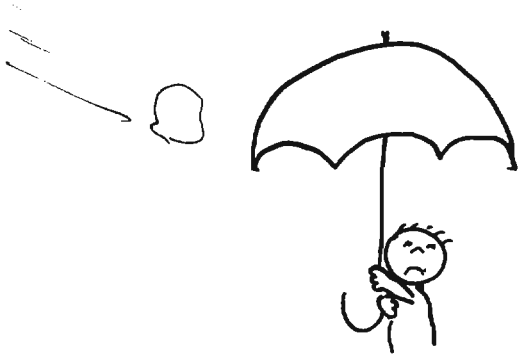
If your article is on some other machine, give [redacted] a call. We may still be able to use your keystrokes, especially if your computer is connected to PLATFORM. If it is not on any system, don't worry; we will type it.

If your organization has a publicity chairman, or program director, have him/her get in touch with us. We can get your news and announcements out to a large distribution list, and we would be happy to work with you to get the word out about what your group is doing.

P.L. 86-36

DOCID: 4009842

METEORBURST Communications (U)



LOOKING AROUND with [redacted] P13

Meteorburst communications (MBC) systems for tactical traffic are being offered for sale by two U.S. manufacturers, ROCKWELL and TELCOM.[1] There has been some Soviet interest, in Soviet literature, in use of meteorburst communication for rapid delivery of a short message.[2] The Department of Energy (DOE) is developing an "emergency communication" (ECOM) network for its atomic energy facilities using a sophisticated meteorburst system that can operate through a nuclear war. Several large scale networks, viz. the SNOTEL net in the Rocky Mountains, and the AMBCS net in Alaska, have been operating for years under severe weather and propagation conditions, demonstrating the cheapness and reliability of this mode of communication.[3] Meteorburst has also been considered for the "strategic connectivity" problem, where low bandwidth links are use to assign and set up surviving wideband links. The fact that several competing companies are in the marketplace, and have been buying up competitors, implies that a market potential is seen. In addition to the obvious military market, the third world civil networks are a likely place to apply this low cost technology, because of the shortage of shortwave frequencies.[4]

Every day some ten billion tiny meteors, consisting of dust particles orbiting through the solar system, enter the earth's atmosphere and leave brief ionized trails which can reflect radio waves. Radio signals in the range 20 MHz to 150 MHz can be reradiated from the meteor trails, and if the trail geometry is correct for a given path, some of the energy will be scattered down to the receiver. The paths only last for a fraction of a second, so typical systems operate at high bit rate bursts of 2000 to 8000 bps, with a duty cycle (active path to the receiver) of 2 to 20 percent.[5]

Because of the short path duration, and random occurrences of useable paths, voice communication is impractical, but telegraph circuits work very well. While circuit control was done by relays and conventional teleprinters, the systems were not very useful, even though research and experiments have been carried out since the early 1950's. The introduction of microprocessors has changed the economics and operational attractiveness of meteorburst, by shielding the communication operator from the vagaries of the propagation. ARQ systems send little mini-packets of data at high bit rates, so that an average of 1 to 4 teleprinter links is maintained. Soviet tests showed quick delivery of short messages because very brief trails could be used.

The main features of the modern systems are: path lengths up to 1200 miles. Power between 10 watts and 1000 watts, depending on the grade of service and throughput wanted. Modulation may be FSK or PSK, up to 8PSK. Bit rates during bursts are typically from 2000 bps to 8000 bps (at 8PSK). The outstations in the SNOTEL net, with over 475 stations, cost from $7000 to $10,000 (depending on who is asked). The DOE ECOM net will be a full duplex grid with about 17 stations, and the specification calls for ECOM to pass a 900 character message across the U.S. between any two stations in 90 seconds. The software development to assure this, plus reconnectivity, is the problem. ECOM will use 41 and 48 MHz channels, but frequency ranges between 30 and 100 MHz provide practical service.

A small company in Texas did the basic engineering and hardware of the DOE SNOTEL net, with Western Union acting as prime contractor. ROCKWELL has bought up the SECODE company. TELCOM wrote the RPQ for the DOE ECOM net, for which Western Union is also prime contractor. The SNOTEL net was used to telemeter snowfall data from inaccessible

DOCID: 4009842

mountain slopes in the Rocky Mountains at a rate of a few reports per day, in response to polling from a central station. The equipment was robust, and operated from solar powered batteries at a few watts radiated during the brief transmissions. The antennas are smaller than an outdoor TV antenna, and this makes them suitable for tactical and remote area transmission.

Meteorburst might be useful for strategic connectivity within a country or a continental area, with relay hops of up to 1200 miles, to connect military and weapons bases and other vital facilities, because it is narrowband and very flexible. The unit costs can be reduced by competition and large scale manufacture. Frequency reuse can be fairly high, unlike HF, because the forward scatter mode make mutual interference very unlikely. It can also be used for theater area fallback, dedicated and reconnection circuits, without having to battle through the HF medium.

Unlike HF, meteorburst links can operate on a fixed frequency 24 hours a day. At dusk, as the earth sweeps away from the meteor showers, traffic capacity drops, then reaches a maximum at 0600 local time. The ability to use a single frequency on a link, and to reuse frequencies, facilitates the frequency management. Because interference is negligible, and the propagation and scattering is directional, international coordination or registration of frequencies is unnecessary. Therefore, dedicated domestic and military nets can be set up and run without formal notifications to ITU.

For transoceanic paths, the possibilities are surprising. On the Atlantic route, Scotland, Iceland, Greenland, Canada is obvious. Azores-Canary-Cape Verde-St. Peter St. Paul to Brazil is another route. Or a link can run from the Azores to Miquelon to Canada. It's also surprising how many routings there are via islands owned or governed by the U.S., U.K. or Commonwealth, and France, that allow hops across the South Atlantic, Indian Ocean, Antarctica and Pacific. Access to the Mid East and Persian Gulf areas is possible by 1200 mile hops from places where U.S. or friendly bases or diplomatic installations exist. The equipment is so small and cheap that it can be installed on small or large vessels, and left unattended on uninhabitable islands, deserts or mountains.

The attraction of meteorburst have been known for a long time, and several times the U.S. and NATO military departments nearly went ahead with projects, but in the early 1960's the attractions of wideband satellites overshadowed MBC. Now, because of the connectivity problem, to say nothing of the gross vulnerability of almost all military and civil telecommunications to many threats, MBC may look rather more attractive. The low cost of the terminal equipment, and the availability of working hardware and software from competing suppliers -- with the convenience of microprocessors for link and message handling -- might make this an attractive fallback option. There has been some Amateur interest in MBC, and the increased availability of Amateur digital radio equipment may stimulate further Amateur MBC. This cheap over the horizon medium should be very suitable for special forces and missions, and rapid deployments, because they can take their own dedicated equipment and their own frequencies, and be supported by a base hundreds of miles away which has satellite terminals to connect it into a global net.

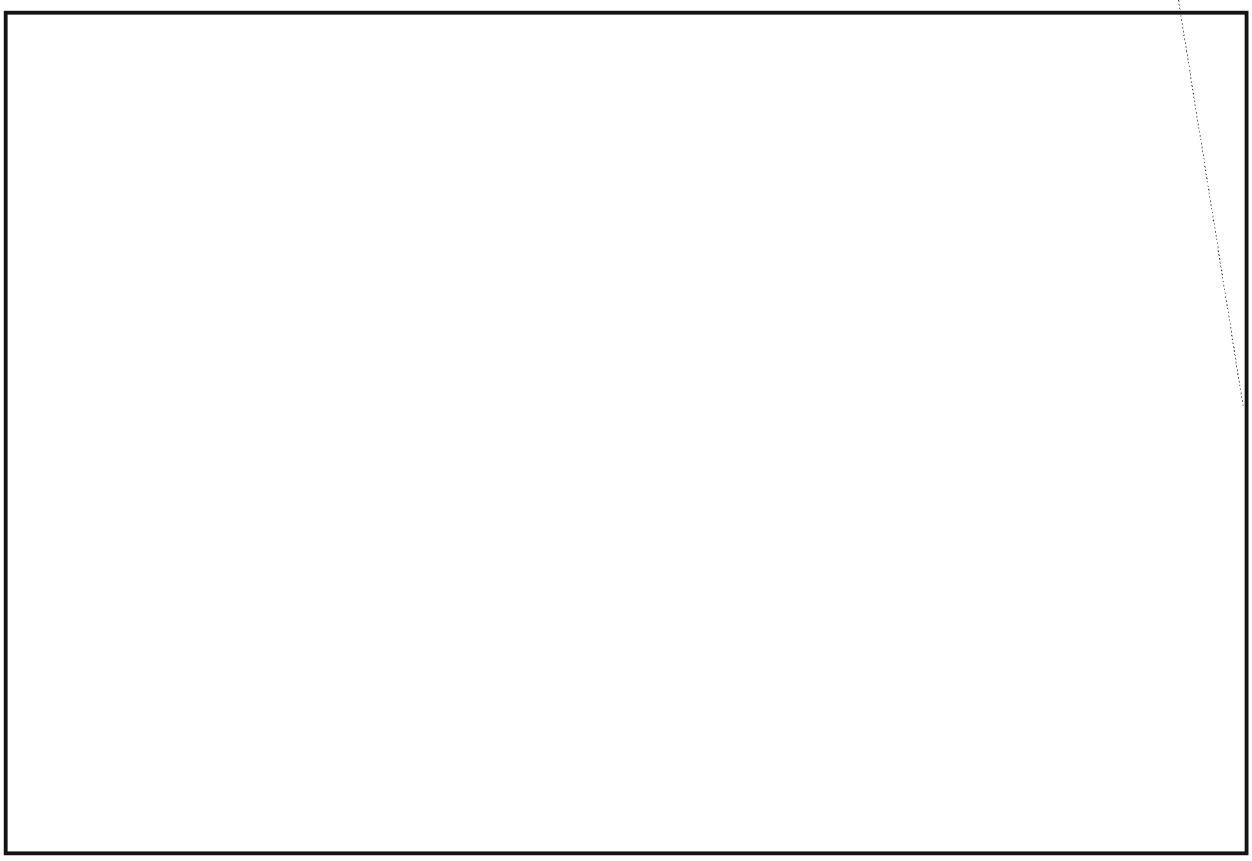
Interference from TV broadcasting would discourage MBC in urban areas, but in remote areas or in war operations such TV interference is very unlikely.

Summing up: cheap, flexible, hard to intercept, almost impossible to jam, low power, lightweight, fixed or variable frequencies, long range, independent of all other power or communications systems, with 50 to 300 bps average throughput, and high reuse of frequencies. How have military communicators managed without this?

References:

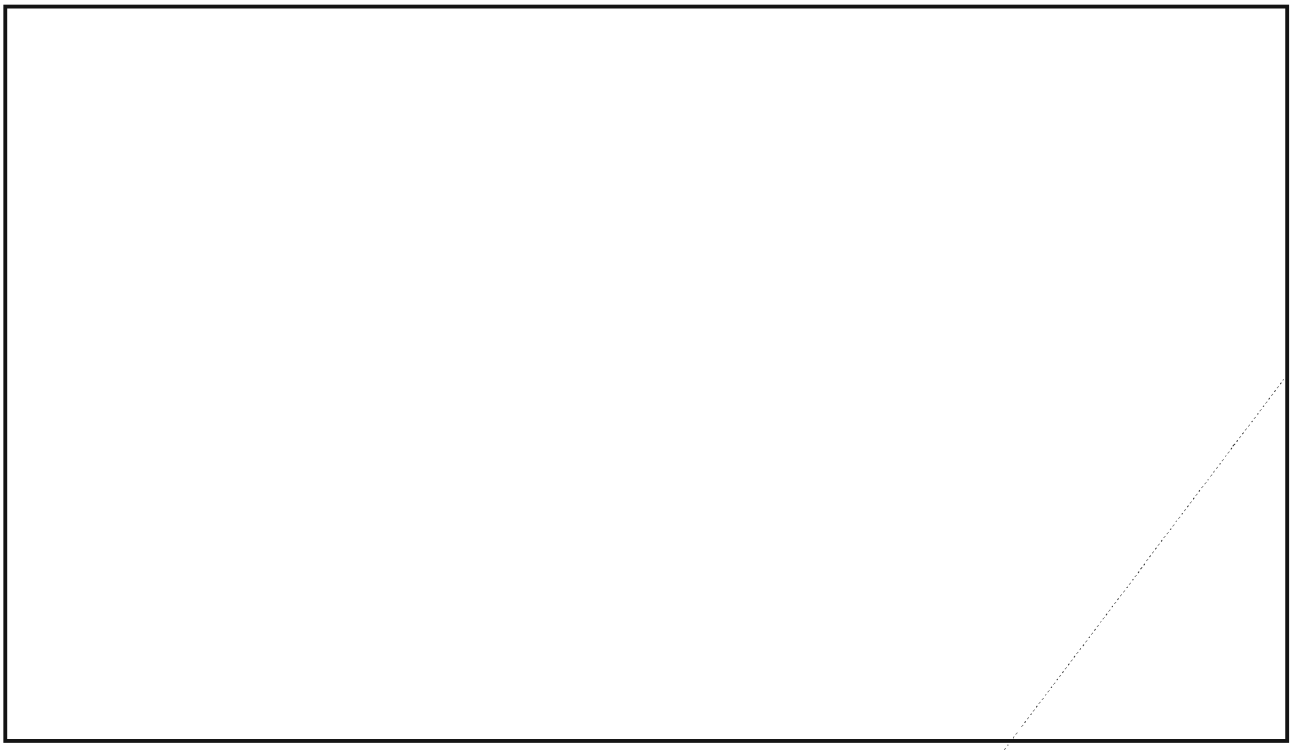
1. AFCEA 81, ROCKWELL exhibit. Product information sheet "Meteorburst Communications". TELCOM advertisement in SIGNAL, 1981.
2. E.A.Demin et al, Test Results of Equipment for Data Transmission via Meteorburst Channels of Radio-Telegraph Communication Links, Telecommunications and Radio Engineering, 1977, No.1, Scripta Publications D.C. 1977.
3. Western Union data sheet. "Meteor Burst Communications" AFCEA 1979. Rockwell International data sheet, "Meteor Burst Communications", AFCEA 81.
4. J.A.Meyer, Digital Meteorburst Communications, INTELCOM 80 Proceedings.
5. D.W.Brown, The potential of meteorburst communication, Communications Systems and Random Process Theory, Ed. J. Skwirznski, Sijthoff & Noordhoff, Holland, 1978.

EO 1.4.(c)
P.L. 86-36



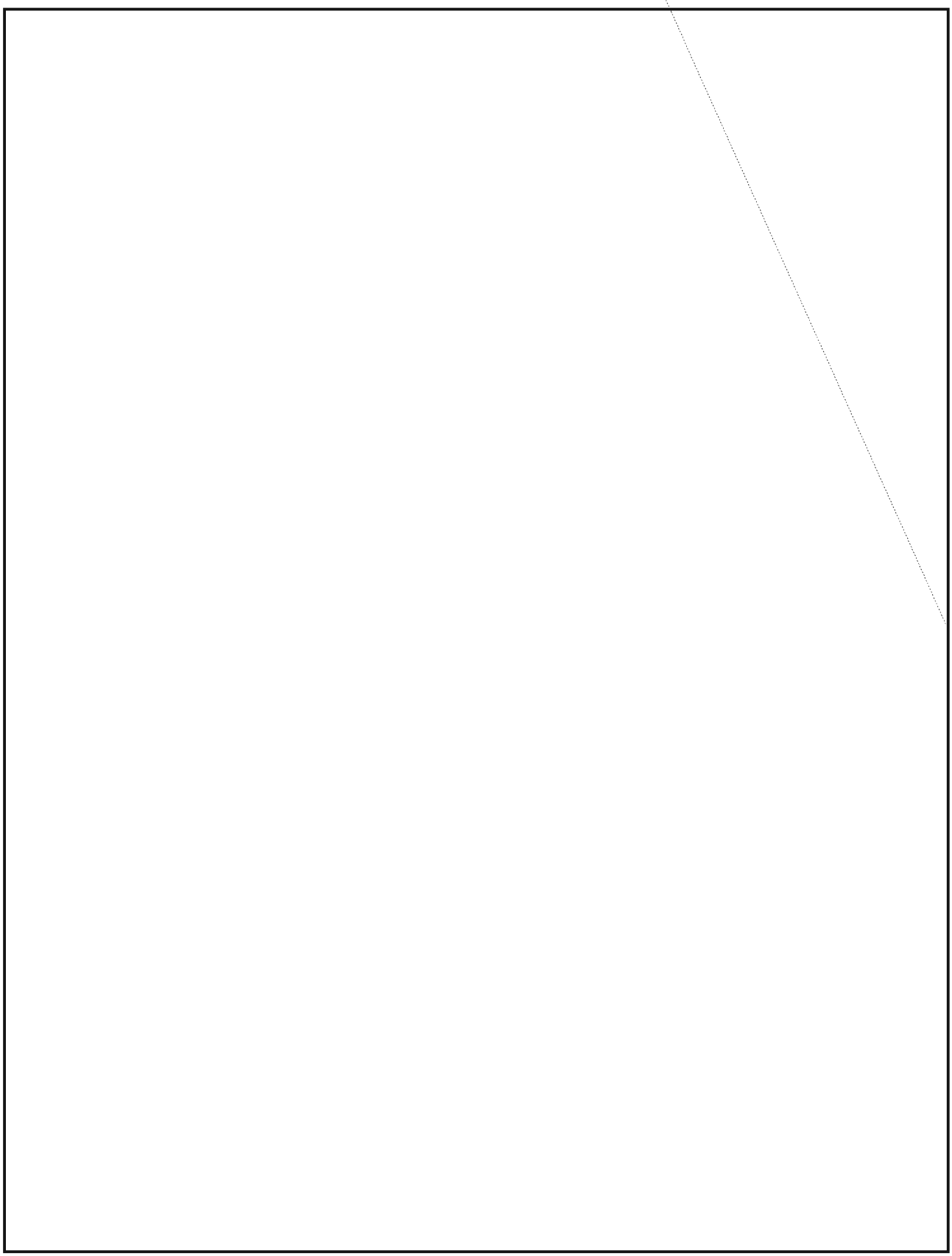
by [redacted] P16

P.L. 86-36



EO 1.4.(c)
P.L. 86-36

P.L. 86-36
EO 1.4.(c)



DOCID: 4009842

A Brief Treatise on Five Laws of Telephonic Communication (U)

by William M. Nolte, T54

LAW #1: YOUR FIRST CALL OF THE DAY DETERMINES THE KIND OF DAY YOU'RE GOING TO HAVE.

This law is a derivative of the street vendor's belief that the day's success is determined by whether he makes a sale to his first customer. Cut the price, give away the merchandise if you must, but make that first sale!

The same principle applies to using the telephone: if the first call goes through to the intended recipient, you will have a favorable success rate on the rest of the day's calls. Unlike the vendor, who works in a "yes-no" situation (he either makes the call or he doesn't), the telephone caller works in a more complex situation. The call can be successfully completed of course, or it might result in a busy signal -- the rough equivalents of the "sale - no sale" conditions encountered by the vendor. The telephone involves. however, a series of other conditions, all indicating a lack of success, and each of them worse than the "no sale" or busy signal response.

- Subcondition A: "I'm sorry, he's on the other line. May I have him return your call?" Sure, but nobody stays on the phone for more than a few minutes around here (on official business, at least), and the mean time for a return based on such an assurance probably drags into days, leading to Corollary A:
  - ANY CALL RESULTING IN THE RESPONSE DESCRIBED IN SUBCONDITION A WILL EITHER BE RETURNED WITHIN TEN MINUTES OR WILL NOT BE RETURNED AT ALL.
- Subcondition B: "She's not at her desk." The truly significant aspect of this subcondition will be revealed to the caller with the next sentence. There are two possibilities:
  - "She's in a meeting with so-and-so, and I expect her to return at 1000." This person is clearly organized enough to leave a trail, and is therefore a good be to return your call. Action: leave a message to return your call.
  - "Gee, she was here just a minute ago, but I don't see her and I have no idea when she'll be back." Now you're in trouble. You have clearly called a floater, who could be in the bathroom, another office, the drug store, or fifty other places. It is unlikely that he or she is working. Action: say you will call back and take your chances. If you feel especially daring, leave a message to have your call returned. Do not however, postpone your own trips to the bathroom, cafeteria, or any of those other places to await the call. In fact, the worst way to get this person to return your call is to sit by the phone for three hours ignoring persistent signals from your stomach or bladder. The best way, on the other hand, is to leave your desk for thirty seconds to deliver a memo to someone in the next office. You guessed it, your call will be returned while you are gone.
- Subcondition C: "He's no longer at this extension. Let me see if we have a current number. This leads to:

DOCID: 4009842

LAW #2: NEVER PROCEED PAST A SECOND REFERRAL IN TRYING TO TRACK SOMEONE DOWN.

The art of referrals is sui generis. This is not the place for a full exposition on the nuances of the form, but they are legion. Simply stated, assume that a referral has an 80 per cent chance of being outdated or simply inaccurate. (Computer simulations supporting this estimate are not available on request.) When in a gambling mood, you may want to ask the person who answers the outdated or inaccurate new number if he or she has an even newer number. Whether you then choose to take a chance on that number is a matter of personal taste.

Corollary A to Law #2:
LAW #2 DOES NOT APPLY TO INTERNS.

Interns are a different matter. Unless it is a matter of life and death, it is rarely worth attempting to track them down. No one ever knows where they are. When I was an intern, I made it a point to surface only about the times plans were being made for barbecues and Christmas parties. In cases of life and death, do not use the phone. Take a chance (and of course you can improve your chances if you know the habits of the person involved) and position yourself at the drug store or in front of the gatehouse the person is likely to use. You could of course leave a message at the intern office, but this is a real longshot. (Do you really think most career panels would have photos of their interns on the walls if the interns showed up there frequently? Those are wanted posters.)

LAW #3: ANYONE ATTEMPTING TO CALL FANX BETWEEN 0900 AND 1400 DESERVES WHAT HE OR SHE GETS.

No commentary required.

LAW #4: THE PERSON RESPONSIBLE FOR MA BELL'S SLOGAN "THE SYSTEM IS THE SOLUTION" SHOULD BE DRAWN AND QUARTERED.

This is the most frustrating part of the process. Street vendors at least have some control over their fate. They can choose to take a loss on a particular sale in the interest of improving their morale if not their business. But what do you do with a busy signal? You are completely at the system's mercy -- and it has none. Wouldn't it be nice if you could gain access to the switching mechanism and make a deal with it? "Okay, I'll take the worst channel you've got, with the lousiest bit rate or whatever, and I won't complain even if it makes FANX sound 4000 miles away. But I've got to complete this call!"

This unfortunately is not a solution, but there may be another one out there, namely:

LAW #5: MOST OF WHAT GETS SAID ON THE PHONE DOES NOT HAVE TO BE SAID.

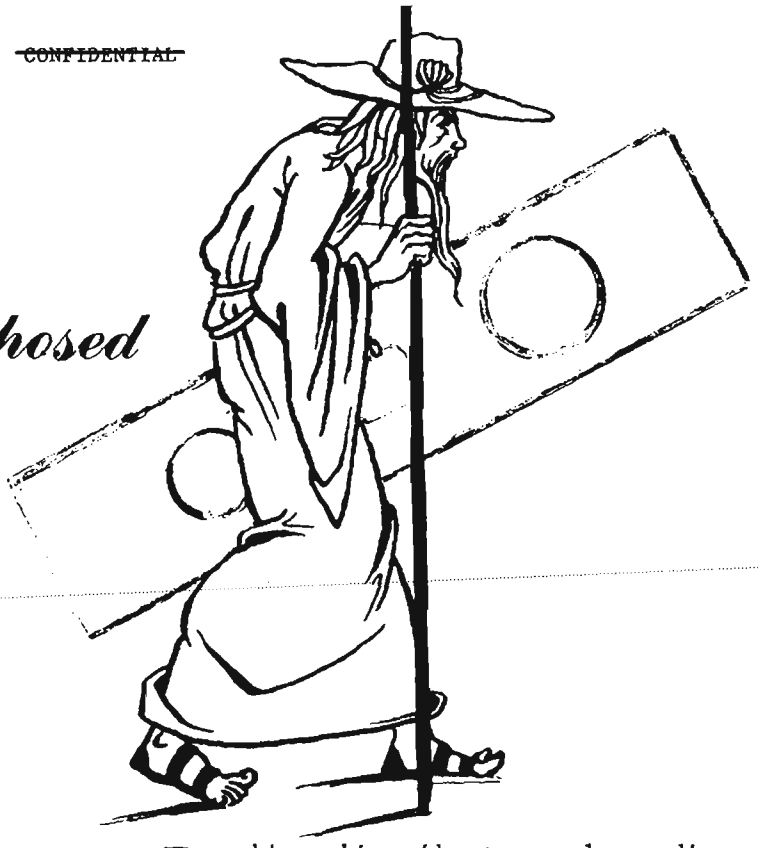
When Oscar Wilde saw his first telephone, the public relations type shilling the thing attempted to impress him by announcing "Mr. Wilde, with this instrument we can talk to Texas." "But what do you have to say?" asked the skeptical visitor.*

---

* The former chief of history and publications insists that this story actually involved Thoreau and the telegraph, not Oscar Wilde and the telephone. Vince Wilson is a learned man. Nevertheless, the story is probably apocryphal in the first place; second, it would be a shame to waste a good line like that on a less than humorous character like Thoreau.

DOCID: 4009842

But Life Is *Supposed* To Be Hard (U)



by [redacted] P14

P.L. 86-36

~~(C-CCO)~~ Maybe so, but P14, the TA Division in the Office of Techniques and Standards, is making life a little softer for the working traffic analyst. In preparation are a series of "How to" working aids on the use of T33/P14 UNIX/PINSETTER software for processing, analyzing, and reporting using terminal subsystems. The first in the series, "How to Index", covers the UNIX/PINSETTER commands "index", "permute", and "ptx". Each command is covered in detail and examples are plentiful. The working aids also contain a handy "quick reference". So once a command is mastered, the basic details and variations of the command are available without having to review the text.

~~(C-CCO)~~ Though "How to" working aids are designed specifically for traffic analysts, personnel in related SIGINT fields will also find some of the techniques useful. If you are presently using terminal subsystems for processing, analysis, and reporting, or will be in the not-to-distant future, copies of "How to Index" can be obtained from P14 (room 8A177, phone 3369s). A second working aid, "How to Sort" is being drafted and should be available soon. The following text, with minor adjustments for CRYPTOLOG format, has been taken from "How to Index".

This working aid assumes only a rudimentary knowledge of UNIX/PINSETTER software on the part of the analyst. Consequently, each technique and the (U) command lines necessary to accomplish that technique are covered in detail and examples provided. The examples are basic and unrelated to any specific problem. By studying, and perhaps duplicating the examples shown, the command and options can be adapted to individual target areas.

(U) Points to remember when using this document:

- ★ Examples shown are in the DELTA DATA 7000 (type f) keyboard format. Keyboards for other equipment connected to UNIX/-PINSETTER software may differ, but generally have keys providing similar functions. Operational areas probably have equivalency charts if other equipment is being used. If not, Unit III - The RAND Editor - in the MP119 course (Introduction to UNIX), may be of help.
- ★ UNIX systems sometimes vary from one host to another. These examples were developed on the UNIX host BARDOLPH1, and should work on most other hosts.
- ★ Within the working aid, the symbols [] and <> are used. Data contained in [] (e.g.: [i ignorefile]) denotes use is optional. Capitalized data contained in <> (e.g.: <BREAK>) is required and indicates a specific key on the DELTA DATA 7000

keyboard. In some cases a specific key may also be referred to as the "__" key (e.g.: the ">" key).

★ File names used in the examples and synopses are descriptive only (e.g.: "filename" means the name of a file; "newfile", the name of a new file to be created, etc.) and not a word or a specific file name that has to be used or included when entering a command.

★ For the sake of brevity, some examples may be truncated after the first few lines. Where this is done, it will be indicated by: /////etc/////

★ The word "CAUTION" is occasionally used in the appendix. It is used sparingly and only where necessary to alert the user to a situation that could result in the loss of data or where there are peculiarities in the system that need to be brought to the users attention.

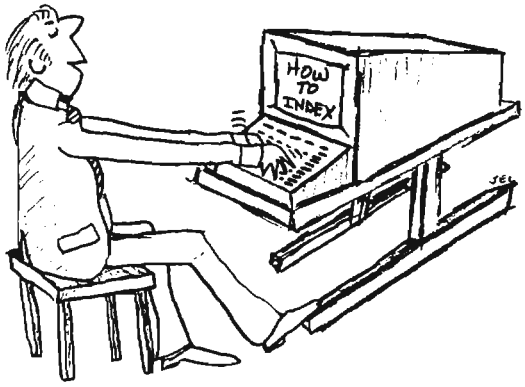
★ Make sure files are "untabbed" before being run through any indexing program:

% untab <filename >newfile <RETURN>

QUICK REFERENCE (U)

COMMAND	OPTIONS	FUNCTION/COMMENT
index	[-]	only one "-" symbol per command line
	[c]	lists words only
	[u]	unique words
	[w]	words, filename, line
	[i ignorefile]	words to be omitted
	[o onlyfile]	words to be indexed
	filename	name of input file
permute	-ainputfile	file name of input file
	[-boutput file]	name of output file
	[-iindicative data]	numbers of columns appended to each line
	[-wpagewidth]	nr of columns (78, 106, 132)
	[-sstart zone & -eend zone]	start & end columns for indexing (zoning limits: page width, - indicative data, - 2, divided by 2, and rounded down)
	[-ddelimiter]	specific character for indexing
ptx	inputfile	name of input file
	[outputfile]	name of output file

Figure 1



INDEXING (U)

DESCRIPTION (U)

(U) Several methods to index data are available to the analyst. The commands INDEX, PERMUTE, and PTX are all excellent tools to index and arrange data to specific individual requirements. By using these commands and related options, the traffic analyst can employ UNIX/PINSETTER software to quickly arrange and exhibit technical data in numerous ways.

APPLICATIONS (U)

~~(C-CCO)~~
of output c
mands used to

☆ "INDEX" works only
special characters are
output. Consequently, this command is best used when digits and special characters are either not a concern or need to be suppressed. "INDEX" works on the entire file and specific segments of a file can not be indexed. It is possible to index only selected words or to omit selected words by using special files with the INDEX command.

☆ "PERMUTE" handles letters, digits and special characters and can be formatted to index only a selected part of a line. For those reasons, it will probably have the most applications for files containing intercept data. There are no provisions to suppress or index selected words, but a delimiter can be used to generate an index.

☆ The "PTX" command generates an index of all special characters, digits and words in a file. Like the "INDEX" command it works only on the entire file. There is no provision to suppress or index only selected words.

EO 1.4.(c)
P.L. 86-36

DOCID: 4009842

THE INDEX COMMAND (U)

NAME (U)

index

SYNOPSIS (U)

index [- [c] [u] [w] [i ignorefile]
[o onlyfile]] filename

BASIC COMMAND DESCRIPTION
AND EXAMPLE OF USE (U)

(U) The index command generates an alphabetic index of significant words from a file. When used without options, the index command omits selected words such as articles and conjunctions (e.g. a, an, and, but, the, to); treats capital letters as lower-case; disregards numbers or special characters; and produces an output in this format:

word filename line-nr context

For example, using this sentence as a file and naming that file "filename", the command format and output of data would appear as:

% index filename <RETURN>

The output of data from this command is shown in figure 2.

VARIATIONS IN THE COMMAND LINE
AND EXAMPLES OF USE (U)

(U) As shown in the SYNOPSIS, there are several options (indicated by the data in []) that can be used with the index command. As a general rule, the "c", "u", and the "w" options are used independently, but can be combined with the "i" and "o" options to tailor the output display desired. The functions of these options and examples of their use are:

THE 'c' OPTION (U)

(U) This option lists only the words. A *count* of each word can be made by piping (i.e.: an upper-case backward slash "|" is referred to as a pipe; this causes the system to route your output through another program) this option through the "uniq" command. Again using "filename", the command lines and outputs would be:

% index -c filename <RETURN>

with the output:

```
a
and
and
appear
as
as
command
data
example
file
file
filename
For
format
naming
of
output
sentence
that
the
this
using
would
```

Figure 3

% index -c filename|uniq -c <RETURN>

with the output:

```
1 a
2 and
1 appear
2 as
1 command
1 data
1 example
2 file
1 filename
1 For
1 format
1 naming
1 of
1 output
1 sentence
1 that
1 the
1 this
1 using
1 would
```

Figure 4

appear	filename	3	data would appear as:
command	filename	2	filename", the command format
data	filename	3	output of data would appear
example	filename	1	For example, using
file	filename filename	1 2	sentence as a file and naming that file "filename
filename filename		2	file "filename", the command
format	filename	2	command format
naming	filename	2	naming that file
output	filename	3	and output of data
sentence filename		1	using this sentence as a file
using	filename	1	example, using this sentence

Figure 2

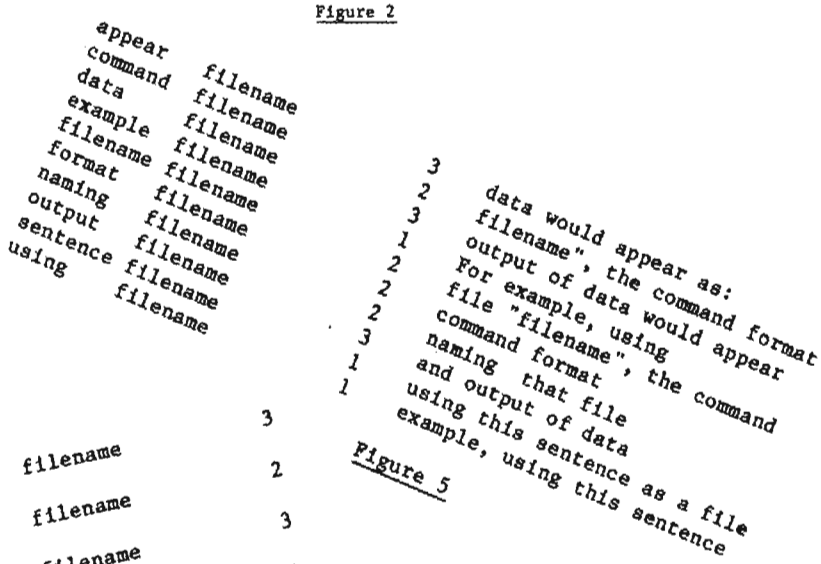


Figure 5

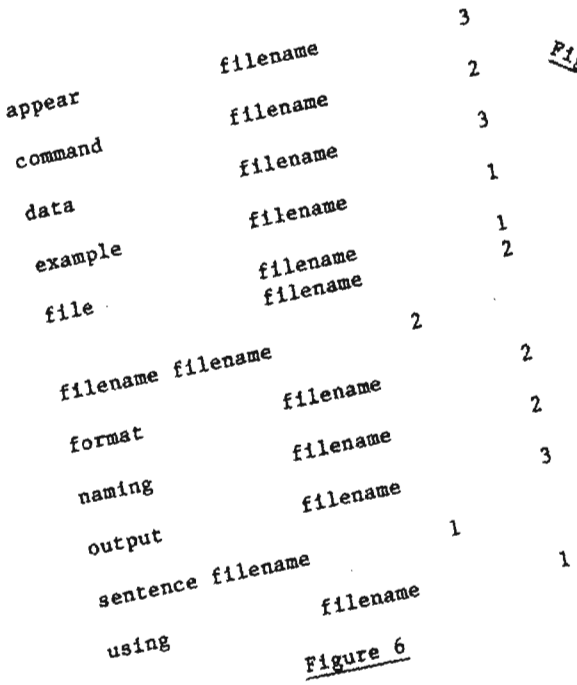
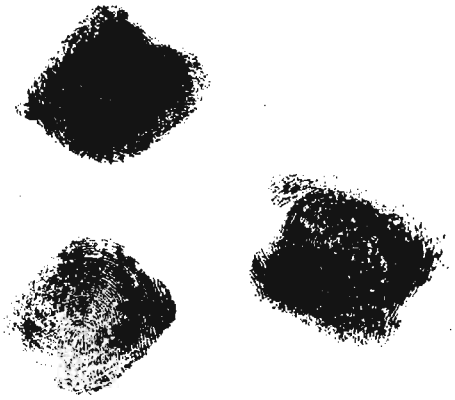


Figure 6

DOCID: 4009842



THE 'u' OPTION (U)

(U) This option will list *unique* words. Words occurring more than once are not listed and capitalized words are considered unique from their lower-case counterpart. Using the file "filename" the command line and output (figure 5) would be:

```
% index -u filename<RETURN>
```

Note: The first column of output data is limited to seven letters, if the word being indexed is longer than seven letters, the next column (the name of the file) is offset. Actually, the index output contains a 'tab' character between the first and second columns of data. If the first column contains a word whose length (plus one for the following space) is longer the first tab setting, the rest of that line will be offset one (or more) tab stop(s) (usually eight characters per stop) to the right.

THE 'w' OPTION (U)

(U) This option lists words *without* the context. The command line and output (figure 6) using "filename" are:

```
% index -w filename<RETURN>
```

THE 'i' OPTION (U)

(U) This option must be used in conjunction with another file containing words to be *ignored* by the index command. For example, if you do not want the words "a", "would", "appear", "data", "example", "for", "naming", "of", "output", nor "this" to be indexed, first make a file called "ignorefile" containing those words. Now, using the "i" option and the "ignorefile", the index command will ignore listed words while constructing an index. Below are examples of how to construct an "ignorefile"; the command line used with the "i" option/"ignorefile"; and an example of the output (figure 7). To construct an "ignorefile" use the "cat" command and list, one per line, each word to be ignored:

```
% cat > ignorefile<RETURN>
a<RETURN>
would<RETURN>
appear<RETURN>
data<RETURN>
example<RETURN>
for<RETURN>
naming<RETURN>
of<RETURN>
output<RETURN>
this<RETURN>
<CTRL-d>
```

Note: <CTRL-d> means to depress the CTRL key while hitting the "d" key. This closes the ignorefile and returns the cursor to the screen.

```
% index -i ignorefile filename<RETURN>
```

The "i" option may also be used in conjunction with other options, but unlike most other UNIX or PINSETTER applications, the options are not listed separately (e.g.: -i -c ignorefile filename), but must be combined (i.e.: -ic ignorefile filename). Failure to do so will result in an error listing on the screen. Also remember that whenever the "i" option is used with another option, this combination of options must be followed by an "ignorefile".

and	filename	1	file and
	filename	3	and output of data would appear as
as	filename	1	sentence as a file
	filename	3	and output of data would appear as:
command	filename	2	the command format
file	filename	1	as a file and
	filename	2	that file "filename
filename filename		2	file "filename", the
format	filename	2	command format
sentence filename		1	using this sentence as
that	filename	2	naming that file
the	filename	2	filename", the command
using	filename	1	For example, using this sentence

Figure 7

and			
data	filename	1	file and
	filename	3	and output of data
file	filename	3	and output of data would appear as:
	filename	1	sentence as a file and
	filename	2	naming that file "filename", the command format
sentence filename		1	For example, using this sentence as a file

Figure 8

THE 'o' OPTION (U)

(U) This option is the opposite of the "i" option. It must also be used with a separate file or "onlyfile" that causes the "index" command to index *only* those words desired. An "onlyfile" is created in the same way as the "ignorefile". For example,

```
% cat > onlyfile<RETURN>
and<RETURN>
data<RETURN>
sentence<RETURN>
file<RETURN>
<CTRL-d>
```

will create an "onlyfile" containing the words "and", "data", "sentence" and "file". Now, using the "o" option, "onlyfile" and "filename", the command line and output (figure 8) would be:

```
% index -o onlyfile filename<RETURN>
```

Like the "i" option, the "o" option may also be used in conjunction with other options to achieve the desired screen output. When used in conjunctions with another option, the two must be combined (e.g.: -oc otherfile filename) and not listed separately.

COMMENTS, OBSERVATIONS AND SUGGESTIONS (U)

(U) You will probably want to save the results of the data indexed. To do so, simply add a "divert" symbol (">" key) and a new file name to the command line. e.g.:

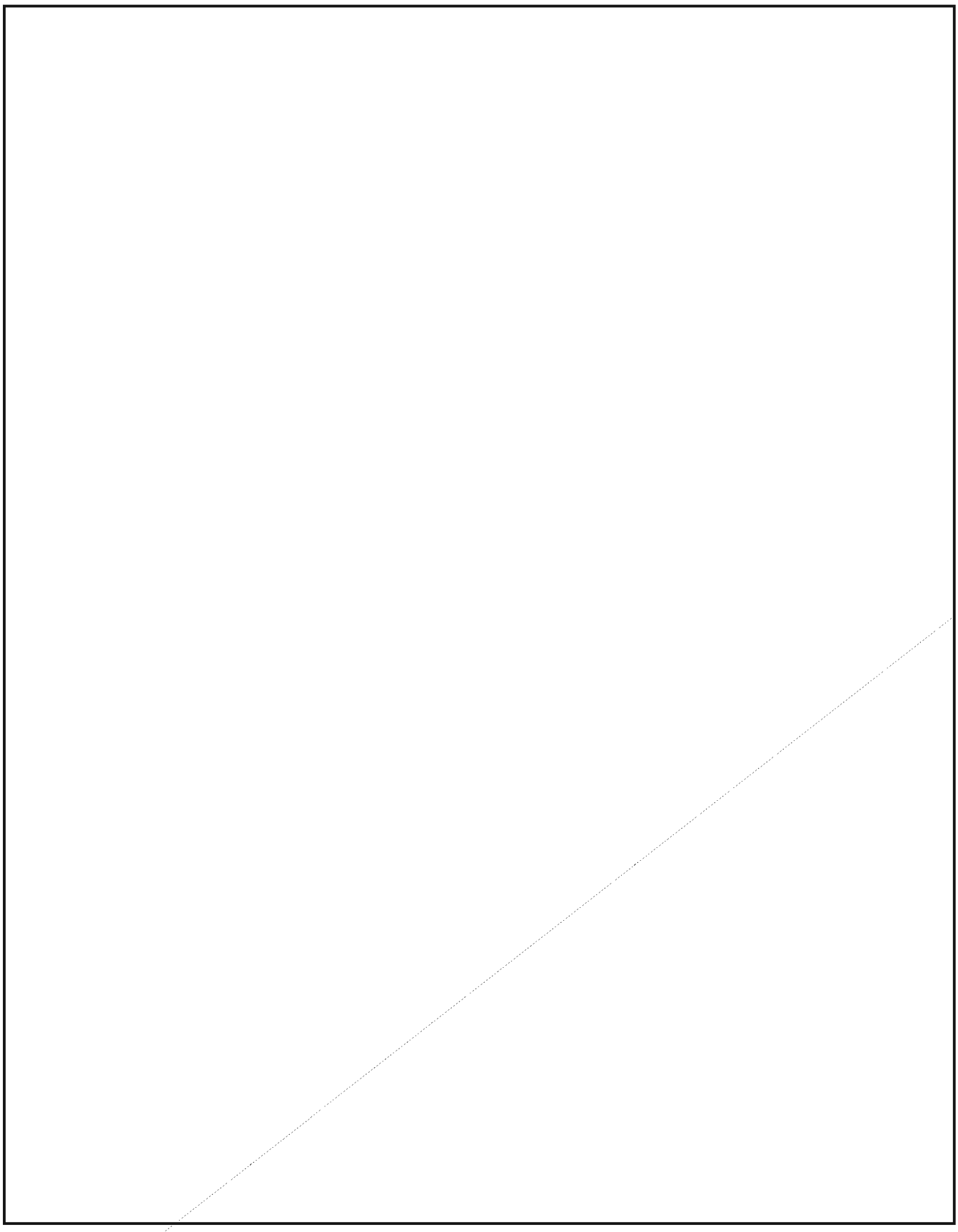
```
% index -c filename > newfilename<RETURN>
```

will place the results of your index of filename into a new file called "newfilename".

(U) Some index commands take a while to run. By adding an "&" (ampersand -- uppercase 6) to the end of the command line, the program will be "run in the background", thereby freeing the terminal for other work. Three CAUTIONS are in order regarding the use of the "&".

- ☐ Do not "logout" while a program is running in the background. Use "detach" to get off the terminal. Otherwise, the system drops your job.
- ☐ Never run more than one job in the background at the same time.
- ☐ Always use a "divert" file when using the "&" option. If you do not, the results return to the screen immediately after completion. This, depending on what you are then doing, could be somewhat undesirable....

~~CONFIDENTIAL~~



EO 1.4.(c)
P.L. 86-36

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~CONFIDENTIAL~~

THE PERMUTE COMMAND (U)

NAME (U)

permute

SYNOPSIS (U)

```
permute -ainput file [-boutput file]
   [-iindicative data] [-wpagewidth]
   [-sbegin zone & -eend zone] [-ddelimiter]
```

BASIC COMMAND DESCRIPTION
AND EXAMPLE OF USE (U)

(U) Index order is: special characters; numbers; and letters. Upper- and lower-case letters are treated separately, but within the same alphabetical order.

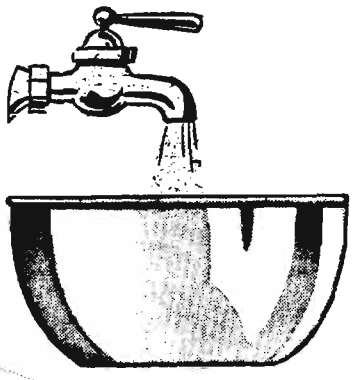
(U) We will use two files, called "filename1" (figure 9) and "filename2" (figure 10). Filename1 contains evenly formated callsign data, while filename2 contains unevenly formated message text. These two files are used as examples to demonstrate the basic "permute" command and options.

(U) Without options, the basic "permute" command functions like the "ptx" command except that all words are indexed. For example, using the "permute" command and the file "filename1", the command line and output (figure 11) look like:

```
% permute -afilename1<RETURN>
```

VARIATIONS IN THE COMMAND LINE
AND EXAMPLES OF USE (U)

(U) As shown in the SYNOPSIS, there are several options (indicated by data in []) that can be used with the permute command. By using these options, the output can be organized to the users specifications and displayed in several different ways. The functions of these options and examples of their use are:



P.L. 86-36

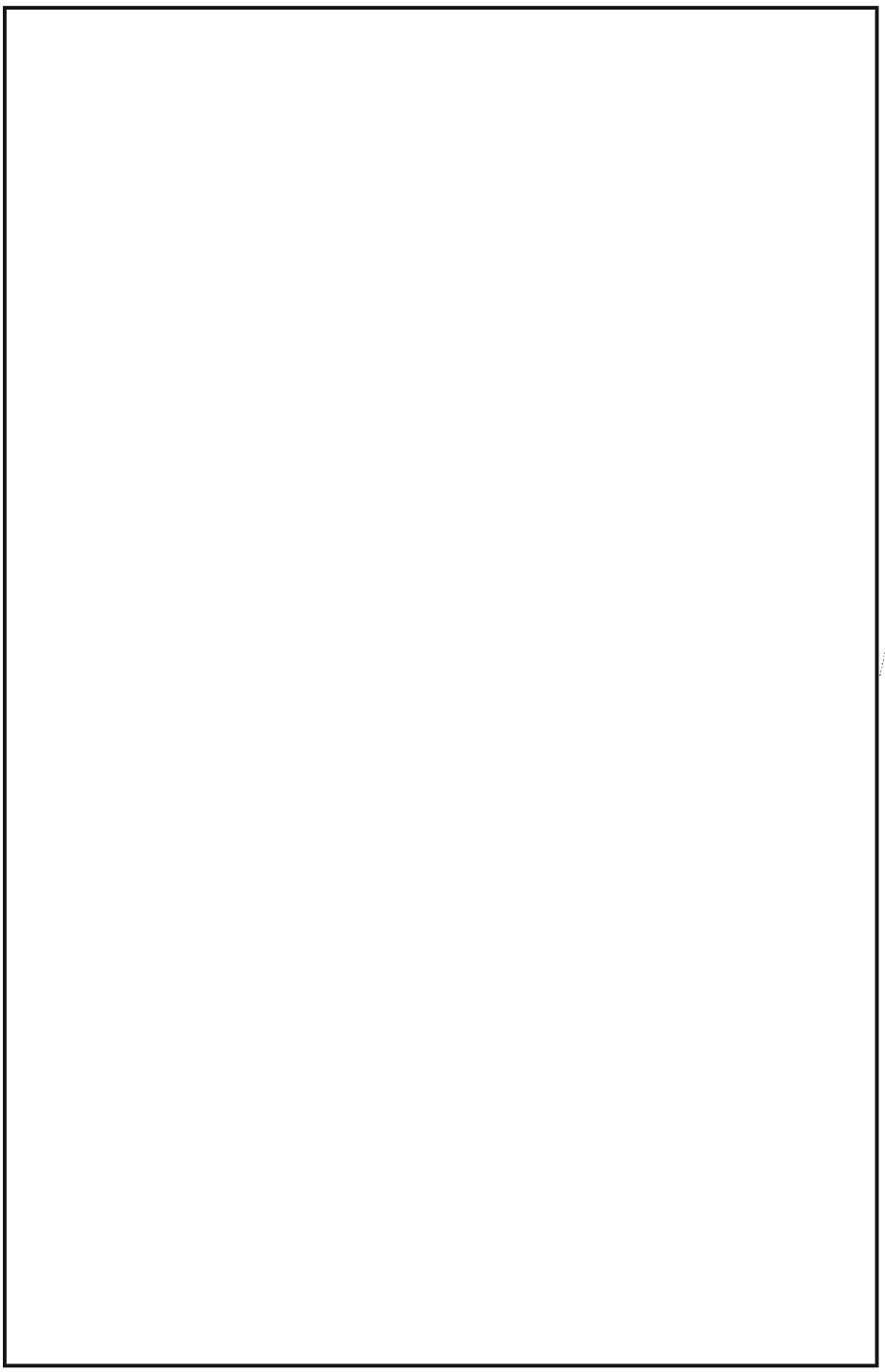
THE '-boutput file' OPTION (U)

(U) Though an election, it is likely that this option will be a part of most command lines when using "permute". The "-boutput file" works exactly like the divert (">") symbol in that it directs the results of the permute index into a file within the working directory. The "-b" part of the option is always followed (no space) by the name of the file (either an existing or new file to be created) in which results are to be placed. CAUTION must be exercised so output is not directed into an existing file containing data, since data already in that file will be overwritten.

(U) Below is an example of the use of the "-boutput file" option. For this example, the output file will be named "text1" and the input file "filename1" will be used.

```
% permute -afilename1 -btext1<RETURN>
```

After the command line is entered into the system, the following will appear on the screen:



EO 1.4.(c)
P.L. 86-36

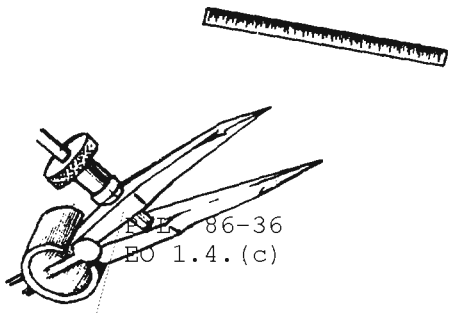
```
SELECTIONS MADE:
NO INDICATOR LENGTH SELECTED
PAGEWIDTH =>78
NO ZONING SELECTED
DELIMITER SELECTED IS SPACE CHARACTER
INPUT FILE =>filename1
OUTPUT FILE =>text1
```

Note: When the job is completed the prompt symbol ("%") returns to the screen. In the above example, a permuted index of material contained in "filename1" would then be in the working directory in a new file called "text1". Since no other options were included in the command line, the output contained in "text1" will be exactly like the example shown for the basic command.

(U) Use of the "-boutput file" option alone or with other options always results in a listing of "SELECTIONS MADE" appearing on the screen after the command line is entered into the system.

THE '-iindicative data' OPTION (U)

Return of the prompt symbol ("%") to the screen tells you the job has been completed and the results placed in the "text2" file. Results would be exactly as shown in the previous example.



THE '-wpagewidth' OPTION (U)

(U) This option sets the page width to either 78, 106 or 132 characters. Widths of 106 or 132 characters must be specified (i.e.: "-w106" or "-132"). If the "-wpagewidth" option is not included in the command line, the page width is automatically set, by default, to 78 characters -- the length of the screen. If the output of the program is longer than the specified pagewidth, the output will be truncated at the specified pagewidth, but the system will try to include the data by "wrapping it around" or fitting it to the other end of the output line. This is indicated by the indicator "..." and should be apparent in the text. In some cases with longer records, data will be lost unless a longer page width is specified.

(U) One of the reasons for and use of the "-wpagewidth" option becomes apparent when "filename2" is "permuted" first with a page width of 78 and then again with a page width of 106 characters. For example, a pagewidth of 78 characters (which is obtained by default when not specified) would be obtained by the command line (output in figure 13):

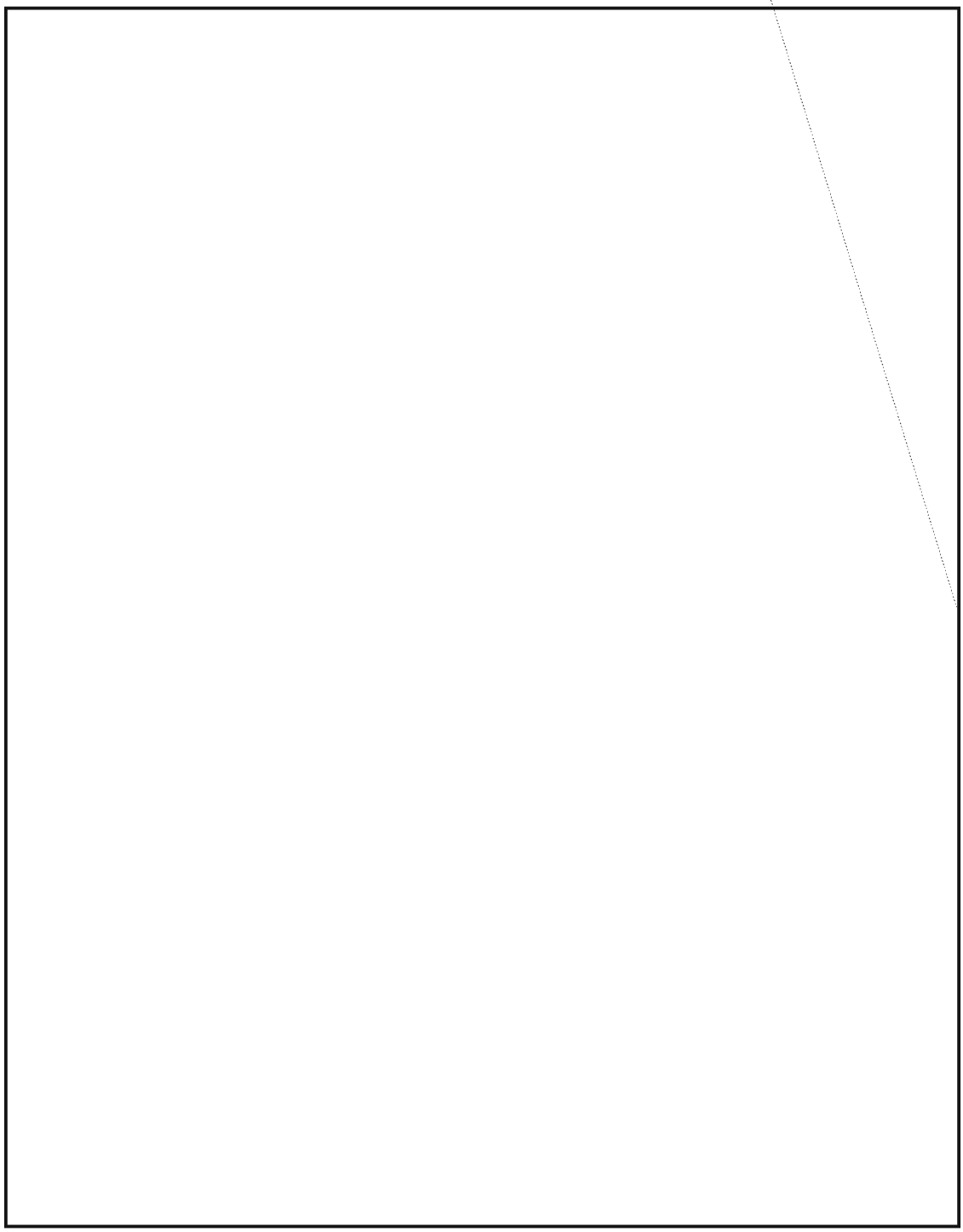
```
% permute -afilename2<RETURN>
```

Even though no data was lost (the input record was only 78 characters), some lines of text are "wrapped around" as indicated by the "..." at the end of text. Now, using an option of 106 characters, the command line (output in figure 14) would appear:

```
% permute -afilename2 -w106<RETURN>
```

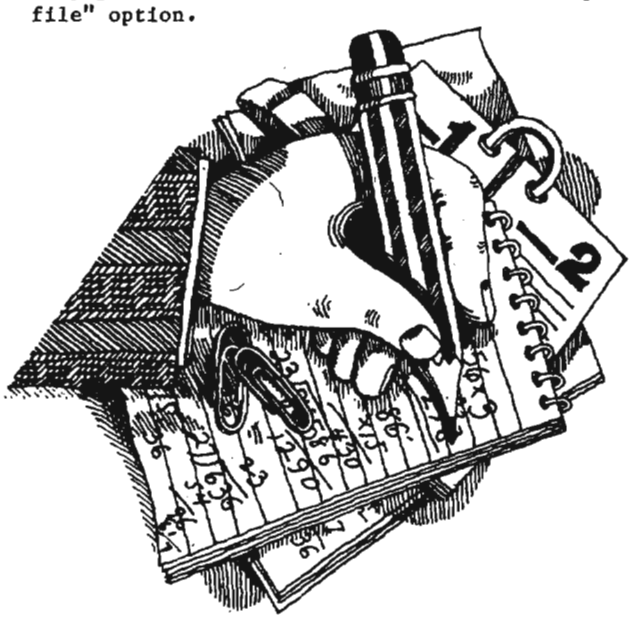
Note that some text is no longer "wrapped around" and that the symbol ">" now appears at

EO 1.4.(c)
P.L. 86-36



the end of some lines. This indicates additional text exists on the line, but is not shown because of screen size. If in the RAND editor, hit the <PORT-right arrow> key and the screen will move over to the text. To return the screen to its original location, use the <PORT-left arrow>.

(U) Another reason for the "-wpagewidth" option will become apparent with use of "-sbegin zone" and "-eend zone" options discussed below. Like all other options, the "-wpagewidth" can be used with the "-boutput file" option.



THE '-sstart zone & -eend zone' OPTIONS (U)

~~(C-CCO)~~ The permute index can be restricted to a specific portion of the input record. This is called "zoning" and requires that the start and end columns or "zone" be specified in the command line (e.g.: "-s35 -e47"). The "-s.." and "-e.." are interdependent and must be used together. For example, if you wanted to restrict a permute index to control callsigns (columns 19 through 22) in "filename1", the command line (output in figure 15) would look like this:

% permute -afilename1 -s19 -e22<RETURN>

(U) The size of the "zone" that can be indexed is limited. If the standard 78 columns are used, then the "zone" is restricted to a maximum of 38 columns. If the 106 or 132 column page width is specified through use of the "-wpage width" option, the "zone" maximums become 52 and 65 columns, respectively. If a "zone" greater than the maximum allowable is specified in the command line, the program will abort and tell you, via the screen, why the program was not run. For example, the following command, which exceeds the zone limitation (38 columns) for a page width of 78 columns:

% permute -afilename1 -s10 -e60<RETURN>

causes the error line below to return to the screen.

Can't fit zoned input & indicator on page
Execution terminated

(U) If an "-iindicative data" option is used, the size of the "zone" is further reduced. Simple math can be used to determine the maximum allowable "zone" when an "-iindicative data" option is included. The formula is:

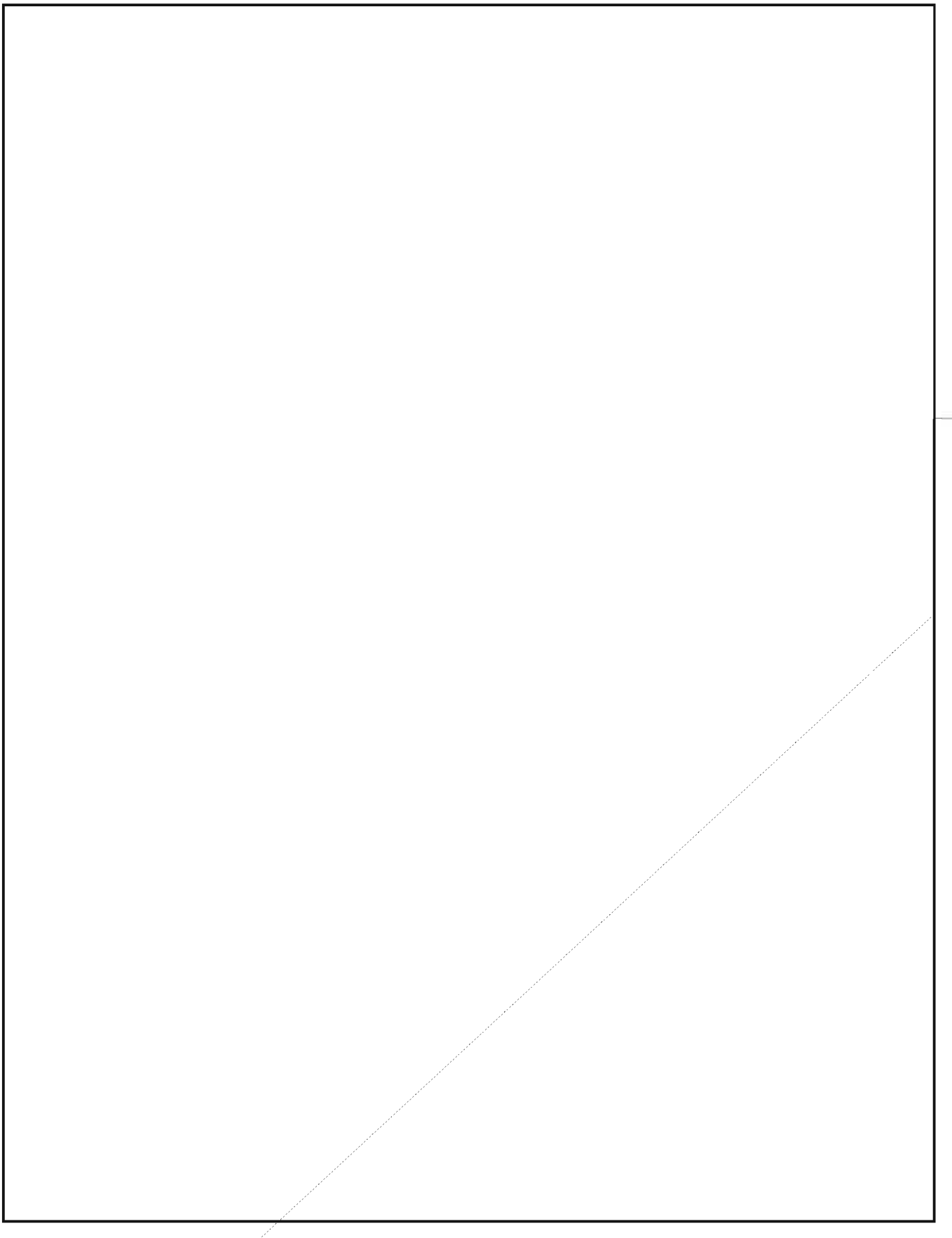
(page width)-(indicative data)-2, divided by 2 (fractions of a column are rounded down to the next whole number).

For example, if the page width is 106 columns and the indicator is 17 columns, then the maximum allowable "zone" is 43 columns (106-17-2)/2 = 43 1/2, which is rounded down to 43. If the combined "indicator" and "zone" exceed the limit for the page width, the program terminates and an error message returns to the screen.

THE '-ddelimiter' OPTION (U)

(U) This option is especially useful when working with data that does not have a set length or when you want to have only a certain item (such as all text beginning with a "3") indexed. The term "delimiter" used here refers to a specific character (e.g. "/", "(", "a", "6", "Z", etc). By default, if the "-ddelimiter" option is not included in the command line, a space is considered to be the "delimiter".

(U) When a specific character is used for a "delimiter", special rules apply. It should be used either with zoning or with increased page width. Failure to do so may result in the program being terminated, an error message appearing on the screen, and a "core" being placed in your working directory. If this happens, first remove the core (% rm core<RETURN>) and then either specify a zone (e.g.: -s30 -e40) or increase the page width (e.g. -w132), or both, in the command line.



EO 1.4.(c)
P.L. 86-36

DOCID: 4009842

P.L. 86-36

(U) Following is an example of the use of the "-ddelimiter" option being used with "filename2". In the example, the message text (columns 32 to 63) is zoned, and the "/" symbol is used as the "delimiter". The example is brought back to the screen, but would normally be placed in another file by using the "-boutput file" option (see figure 16).

% permute -afilename2 -s28 -e63 -d/<RETURN>

Note that in the above example:

- The program automatically placed "/" characters before the first column of data in the zone. This allowed the first part of the message text, which was not preceded by a "/", to be included in the index; and,
- [redacted] If an "indicative data" option had been included in the command line and also (because the "indicative data" and "zone" together exceed the limit for the page width of 78 columns) the page width increased, this data would have been retained.

(U) Now, including the "indicator" and "pagewidth" options, the entire command line and output (figure 17) would look like:

% permute -afilename2 -s28 -e63 -d/ -i27 -w106<RETURN>

All the indicative data is now shown and the page has been expanded to 106 columns. The file is best viewed in the RAND editor where the <PORT> keys can be used to see the entire text. (If your terminal does not have <PORT right arrow> and <PORT left arrow> keys, you can get the same action by using <Ctrl s> for <PORT right arrow>, and <Ctrl a> for <PORT left arrow>).

COMMENTS, OBSERVATIONS, AND SUGGESTIONS (U)

(U) Like the "ptx" and "index" command "permute" can be "run in the background" by adding an "&" (ampersand) to the command line. When running the "program in the back ground", an output file should also be specified to prevent the program returning to the screen when ever the job completes. With the "permute" command, this is done by including the "-boutput file" option; not by using the "divert" (">") symbol as is done with the "ptx" and "index" commands.

(U) Users should be aware of an idiosyncrasy occurring when the "&" and the "-boutput file" option are used together. Basically, when the command line is entered, the system provides a process identification number (frequently referred to as the process ID or PID) and returns the prompt ("%") to the screen. Immediately thereafter, the "SELECTIONS MADE" listing also returns to the screen. Since the prompt symbol is already on the screen, it does not reappear after the listing completes. Consequently, with the "SELECTIONS MADE" listing between the prompt and the cursor, it is not apparent that the system is ready to accept another command. However, a new command can be entered immediately or, if you prefer, hitting the <@> and <RETURNS> keys brings another prompt symbol to the screen.

(U) CAUTION. Care must be exercised when the "permute" command is used on a large file. In cases where a sizable zone of data in a large file is indexed, the resulting output can exceed available temporary working space and cause your user group system to "crash". This problem is compounded by running the command in the background using the "&" symbol. If necessary, large files can be split into several files using the "split" command; permuted separately; appended together; and than piped through the "csort" command to achieve the desired output. For example, the command line:

% split -250 filename<RETURN>

would split the data in file "filename" into separate files each with 250 lines of data. The resulting files ("xaa", "xab", "xac", etc.) can than be permuted separately (but not in the background at the same time). In turn, these files can be combined and the output "piped" (the "|" key") through the "csort" command and its "+col" and "-o" options. The "+col" option specifies the column where the merge is to occur (this will be the same as the start of the zone used in the "permute" command); and, the "-o" option precedes the name of the file in which the results are to be placed. For example the command line:

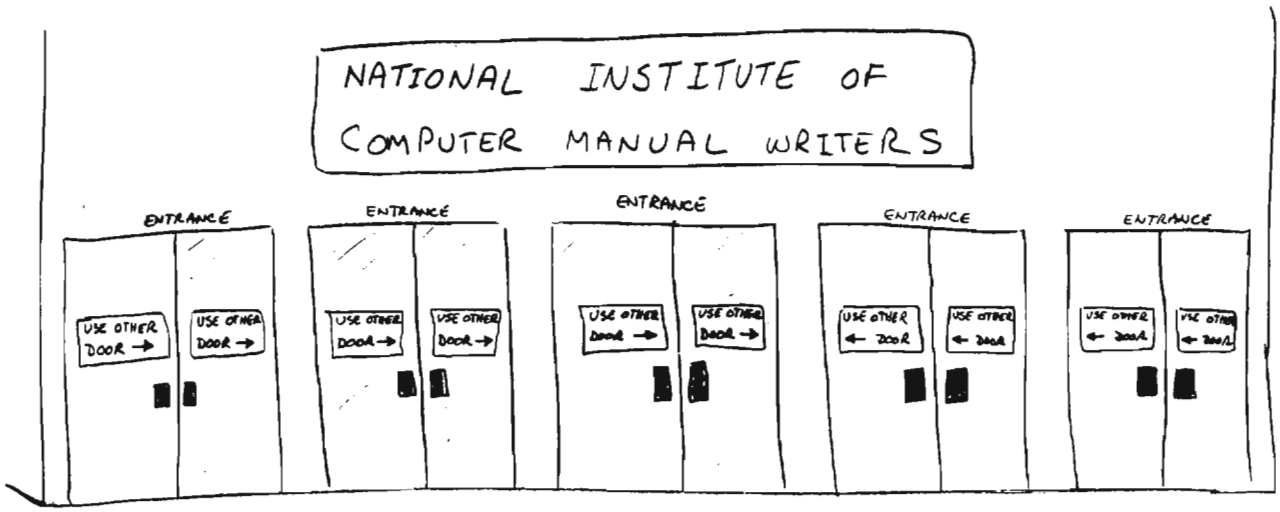
cat xa xb xc >> f1 |csort +25 -o f2 <RETURN>

would append the files "xa", "xb" and "xc", into "f1" and pipe "f1" through the "csort" command. In turn, the "csort" command sorts "f1" on column 25 and places the results into a file called "f2". Had the start of the zone previously used to permute the three files (in this case +25) been omitted, the merge would have been left-justified and not in the desired format.

DOCID: 4009842


```
   as the special characters  !, ", #, and...as well
as the special characters !,  ", #, and...as well
                 command....  $ and was made to demonstrate the ptx
the special characters !, ",  #, and...as well as
        contains the numbers  1, 2, and 3..."filename",
     contains the numbers 1,  2, and 3..."filename",
       the numbers 1, 2, and  3..."filename", contains
 special characters !, ", #,  and...as well as the
  sentence, placed in a file  called...This
     as well as the special  characters !, ", #, and
 made to demonstrate the ptx  command....$ and was
                   The ptx    command line using the file "filename"
               "filename",    contains the numbers 1, 2, and 3
          $ and was made to   demonstrate the ptx command.
  This sentence, placed in a  file called
  ptx command line using the  file "filename"...The
                 and 3...     "filename", contains the numbers 1, 2,
 command line using the file  "filename"...The ptx
       This sentence, placed  in a file called
and the resulting output look like this:
             The ptx command  line using the file "filename"
    and the resulting output  look like this:
                 $ and was    made to demonstrate the ptx command.
   "filename", contains the   numbers 1, 2, and 3
        and the resulting     output look like this:
           This sentence,     placed in a file called
 was made to demonstrate the  ptx command....$ and
                     The      ptx command line using the file "filename"
                  and the     resulting output look like this:
                     This     sentence, placed in a file called
              as well as the  special characters !, ", #, and
               "filename"...  The ptx command line using the file
                              This sentence, placed in a file called
  resulting output look like  this:...and the
       The ptx command line   using the file "filename"
                     $ and    was made to demonstrate the ptx command.
                   and...as   well as the special characters !, ", #,
```

Figure 18



DOCID: 4009842

THE PTX COMMAND (U)

NAME (U)

ptx (permuted index)

SYNOPSIS (U)

ptx inputfile [outputfile]

BASIC COMMAND DESCRIPTION AND EXAMPLE OF USE (U)

(U) The ptx command generates a permuted (permute: arrange objects in a series in all the possible ways in which they can be arranged -- Webster's 3rd New International Dictionary) index of all words, numbers and special characters in a file.

(U) The index sort order is: special characters first, digits next, and letters last. Capital letters are treated as lower-case and punctuation ignored. The key word appears in the middle of the page with preceding and following text also shown. The words "a", "an", "and", "as", "is", "for", "of", "on", "or", "the", "to", "and" and "up" are suppressed for key word use, but included in preceding or following text.

This sentence, placed in a file called "filename", contains the numbers 1, 2, and 3 as well as the special characters !, ", #, and $ and was made to demonstrate the ptx command. The ptx command line using the file "filename" and the resulting output look like this:
(see figure 18)

% ptx filename<RETURN>

VARIATIONS IN THE COMMAND LINE AND EXAMPLES OF USE (U)

THE 'outputfile' OPTION (U)

(U) The "output file" option will be used frequently. It places the results of the ptx index into a new file within the working directory. This is done simply by adding an additional file name (e.g.: "newfile") to the basic command line. For example, the command line:

% ptx filename newfile<RETURN>

will ptx the data in the file "filename" and place the results into another file called "newfile". Because of the way the program was originally written, this is an automatic "divert" and it is not necessary to place a "divert" symbol (the ">" key) between "filename" and "newfile". Use of the "divert" symbol will; however, produce the same results.

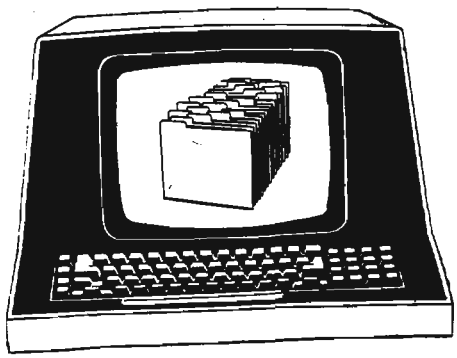
COMMENTS, OBSERVATIONS AND SUGGESTIONS (U)

(U) When using the ptx command it is frequently advantageous to use the "divert" option and "run the program in the background" in order to free the terminal for other work. To do so, simply add an "&" (ampersand -- upper-case 6) to the end of the command. For example:

% ptx filename newfilename &

CAUTION: If you leave the system while a job is running in the background, use "detach" vice "logout". Otherwise, the job is dropped. Also, make sure there is a "divert" file specified in the command line. Failure to do so, creates instant garbage when the job completes, returns to the screen, and combines with whatever you are doing at the time.

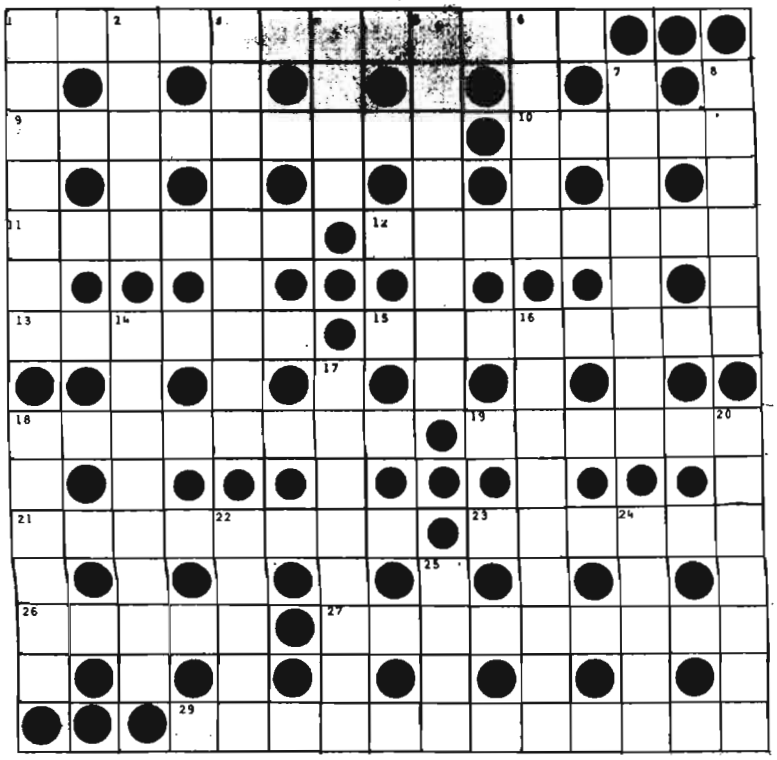
(U) Before running a ptx, it is frequently best to do a little selective editing to remove useless lines.



DOCID: 4009842

CRYPTIC CROSSWORD

By [redacted] P.L. 86-36



ACROSS

1. Do similar growers produce bugles? (7,5)
9. Closemouthed as a result of severe tic? Awful! (9)
10. The glove let out? It's too thin! (5)
11. Believe me! Tick fever symptoms include cause to vomit! (6)
12. Lunatic pets goat and holds up exit. (8)
13. Never consult a nautical chart unless holding a ruler! (6)
15. The congressman gave public utterance and made amends. (8)
18. Settles one charged particle in among equals. (8)
19. Aha! Include a gun for Christie. (6)
21. Come back again to harvest fruit? (8)
23. Innate order where one finds fish. (2,1,3)
26. The Spanish and the German berry bush. (5)
27. Is the lout suing over the sticky stuff? (9)
28. A nice insider goes berserk over bombs! (12)

DOWN

1. For samplers, take some blossoms after tea. (7)
2. Relative expression of surrender? (5)
3. Affirm recipe that puts apple juice back into chopped liver? (9)
4. Double or nothing out of race objective? (4)
5. A wet rice concoction for a summer beverage? (3,5)
6. Wild glee about a fine golf score! (5)
7. Sovereign trouble initially after car crashes into car! (8)
8. London art gallery moved into South Dakota, it's said. (6)
14. Horrible! Drop sale of cats! (8)
16. Man enters a rain, oddly, in South America (9)
17. Attempt, by the sound of it, to fish for a polygon. (8)
18. Insane report carries the load! (6)
20. Swears to student's whereabouts at end of term, perhaps. (7)
22. An anonymous tipper once exposed a former dictator. (5)
24. She comes from main dispersion around the first of October. (5)
25. Being impolite, we hear, is to be regretted. (4)

DOCID: 4009842

Rules for the Camel Corps (U)

by [redacted] T095

P.L. 86-36

It is frightening to contemplate the amount of time NSA employees spend in meetings. There are staff meetings at all levels, working groups, meetings to solve a particular problem, club meetings, and meetings to find reasons for more meetings. "He's at a meeting" is all too frequently heard on the other end of a phone line.

As a veteran staffer, I feel qualified to say that not all of this is time well spent. I have fidgeted and chafed through many meetings that were unnecessary, poorly run, overlong, and ended in chaos. The people who run these I have affectionately labeled the "Camel Corps" because their product so often resembles the design of the proverbial horse. Conducting a proper meeting should not be terribly difficult as long as the chairman follows a few simple rules.

1. Make certain a meeting is really necessary. A few strategic phone calls or memoranda may provide a more efficient solution to the problem.

2. Schedule the meeting for a fixed period of time. Except under very special circumstances, no meeting should last longer than one or one and a half hours. By that time, you've lost the narcoleptics and doodlers and are in danger of losing everyone else. It's better to schedule two sessions than to have one become unproductive.

3. Invite <u>all</u> the right people and <u>only</u> the right people. It's all in vain if you're missing what the Camel Corps would call "a key player." Also, people who have no reason to be at a particular meeting tend to become hostile or to lead the discussion into an area where they can have input. Work with the smallest possible group.

4. Prepare an agenda or discussion outline and distribute it in advance. Everyone should be aware of the contribution he is expected to make. If possible, include background information and ensure that pertinent documents are available to all.

5. Keep the discussion on the subject and under control. Digressions and "war stories" should be nipped in the bud. This is an important way to help accomplish Rule 2. Above all, don't let someone else assume command of your group. I find that most people respond very favorably when a meeting is effectively kept on the subject at hand.

6. Give everyone a chance to express his opinion. The person sulking in the corner may have a more important comment than the most outspoken attendee.

7. If you finish early, dismiss the meeting. I remember one leading Camel Corps member who accomplished his stated purpose in the first five minutes of a scheduled one-hour session. This disconcerted him, so he kept up a pointless discussion just to fill time. I walked out.

8. Briefly summarize the session before ending it. This reduces the chance of later misunderstandings. Each participant should be aware of any follow-up actions for which he is responsible.

9. Prepare a written record for participants and for anyone else who should be "brought up to speed" (Right, more CC slang!) on the meeting. Keep the record yourself until all danger of repercussion is past.

Sound too simple and obvious? Think about them whenever you take part in a meeting. I don't think it will take you long to learn to spot the Camel Corps at work.

DOCID: 4009842

TOWARDS BETTER SYSTEM DEVELOPMENT (U)

by [redacted] R53

P.L. 86-36

This paper was originally written for the first annual conference of the Communications Analysis Association on communications analysis: "The Analyst in the 80's." It appears here with minor revisions.

The Analyst in the 80's will continue to be seriously affected by personnel constraints, changes in the workforce, and the evolution of the communications and technological environments. Among the various approaches that will be used to deal with these problems will be an increasing use of tools to support the analysts in their various activities. Central to these tools will be interactive computer systems.

Personnel constraints that limit the size of the workforce are a source of pressure for increasing productivity. Changes in the workforce caused by the retirement of experts and the difficulty of recruiting and developing their successors are a source of pressure for finding ways to capture existing expertise for transfer to future generations. Evolution of target environments to more sophisticated techniques and greater capacity is a source of pressure on diagnosis, the development of attacks, and their transfer into computing systems. Responses to such evolution range from use of a known attack on a larger scale, refinement of a known attack, development of a new attack, and various combinations. Continued development of more useable, available, and powerful computing resources for Analysts is the fundamental means of automating the more mechanical parts so that Analyst resources can be focused on the more intellectual.

For example, some known "old hand" attacks may be just what is needed for some "new" problem. However, effective exploitation and utilization of personnel may require the development of new computer systems. Although the "old hand" attack might already seem to be sophisticated when it is carried out by a "human processor," additional sophisticated techniques may be required to move it to a "computer processor." It may not be possible to move all of the human processing to a computer because some aspects of the human processing may not be well enough understood to be mechanizable. This requires a close coupling between intelligent human and mechanical computer processors to produce a complete system solution. As the target problem becomes more difficult in techniques or scale the system development activity becomes correspondingly more difficult.

Approaches to deal with these pressures share the idea of developing facilities to support the Analysts. The facilities can be viewed as tools that can be applied to various parts of a problem. A tool provides a way to improve the interface between the human problem solver and the problem. Those parts of the problem which are well understood can be automated so that valuable Analyst time can be devoted to the more interesting parts. This is a continually-evolving process which raises the level at which the Analyst operates. Suppressing the details that are no longer of interest exposes new and more interesting problems that were previously hidden.

DOCID: 4009842

Responses to the pressures are in the form of computer systems supporting increasing amounts of interaction. In time these systems will evolve to become environments which will support almost all of an Analyst's activities. This kind of response transfers pressures on the Analysts to pressures on the system Developers. The general approaches used to respond to Analyst pressures can also be applied to system Developer pressures.

In the remainder of this paper the term "User" will refer to any person using a system to assist him in carrying out some activity. Since we will be addressing system development for Users, a brief sketch of system development from a User's view is useful to establish some context for what follows. From the User's view, system development starts with some notions of a need for a system to formulate system requirements. After the requirements are formulated, the system is developed, and eventually delivered so that it is available to the Users. To the User, the system development activity looks like a delay between the formulation of requirements and the system's availability. Although the Users may believe that the requirements embody their notions of what they need, and the Developers may believe that the system developed satisfies these requirements, the delivered system often contains some surprises.

WHY?

Before trying to answer this, some discussion of the kinds of systems we are evolving to will be useful.

Tools and their Environments

Just as tools have been and will continue to be developed to help the User solve problems, the development of the tools themselves is a problem requiring tools. The development of requirements for a system to solve some problem for a User is clearly a serious problem in its own right. This is evidenced by the difficulty in deciding what problem is in need of a tool, what kind of tool needs to be developed, how the tool is developed, how it will be used, who will use it, where it will be used, and the like. In fact, the very existence of a tool for a problem and experience using it often provide useful and critical insight into the problem and expose the need for new tools. Some general properties of tools and their importance include the following:

- Tools are not used in isolation; they may be used in combination with other tools.
  - ☐ It is important that they can be combined into larger ones. Developing tools which can be combined to form new tools is fundamental to the ability to build upon previous work rather than repeating it.
- Tools interact with the User; they may not be completely automatic.
  - ☐ It is important that excellent human factors be a major design objective in their development.
- Tools interact with a variety of data, information, and knowledge sources.
  - ☐ It is important that these sources are an easily accessible part of the environment.
- Tools may be applicable to a class of problems which differ in only some specific parameters.
  - ☐ It is important that given the identification of the parameters, it is possible to develop a single parameterized tool to insure the consistency of the different members of the class.
- Tools need to evolve as the problem and approaches to it evolve.
  - ☐ It is important that the tools can be evolved rapidly to maintain their applicability.

> *systems have no intrinsic value*
> *except to the extent*
> *that they satisfy their users*

DOCID: 4009842

user expectations are rising
as a result of
previous development successes and
the decreasing cost of system components

The development of tools that satisfy these properties is itself a problem that can benefit from tools of its own. Central to tools for the Users and the tools to produce them will be the use of interactive computing systems. Time-sharing systems have been used as the basis of most interactive systems, and are reaching limitations in the ability to support adequate human factors and desired functionality. The decrease in hardware costs has reached the point where personal computing with network facilities is an attractive alternative. The importance of a network cannot be overemphasized. Personal computers alone are not a step beyond time sharing if they do not provide other kinds of resource sharing in a transparent fashion. Traditional programming languages and techniques could be used but more advanced ones are emerging which also provide attractive alternatives.

The Requirements Problem

We have seen the trend from pure requirement-generation by User organizations passed on to development organizations evolve to joint User/development requirement-generation. Although this is a step in the right direction, experience has shown that joint requirement-generation does not go far enough. Systems built from joint requirements may not meet the expectations of the participating parties. When the systems are completed and the problems discovered, it is often too late to take necessary corrective actions.

The way in which systems are developed is heavily influenced by the perceived cost of the various aspects of the development activity. The structure imposed on the activity tends to be proportional to the perceived difficulty of development. For some problems that are well understood, requirements can be written by the User community and given to the Developer community. If the resulting product satisfies the requirements, then the Users should be satisfied with it. This is a fictional approach for most problems of interest.

This model takes a simplistic view of the need for communication between Users and Developers. It does not provide for any feedback from the Developers on their understanding of the requirements until the product is delivered. In an attempt to narrow the gap between the Users' and Developers' understanding of requirements, joint User/Developer requirement generation emerged. The rationale was that if both parties are involved in writing the requirement, then the chance of getting the desired product should improve.

Although joint requirement-generation does yield some improvement in the communications area, it still takes a simplistic view of the role of requirements. The generation of requirements assumes that enough is known about a problem to say what is needed. Even if enough is known about a problem, how can requirements be written so that any two people involved with them agree on what they mean? And if not enough is known about a problem, then requirements are even harder to write.

In reality, the problems are sufficiently difficult that not enough is known to write complete requirements, and it is not possible to write them in a way that guarantees uniform interpretation. There have been a number of significant efforts to address the requirements problem, and still it persists. After some period of little progress, one begins to look in other directions. Could it be that there is something wrong with the idea of developing requirements or the way in which they are developed? This will be explored next and alternatives considered.

The Prototyping Approach

Requirements are hard to write, and even when well-written and comprehended by all involved can lead to unexpected results. When

DOCID: 4009842

the system is completed and the problems are discovered, it is often too late to take the necessary corrective actions. This is because it may not be possible to change the system without substantial delays. The form of a developed system may be very sensitive to some of its design decisions. Changes to such critical design decisions can have pervasive effects on the developed system so that major parts of the system may have to be modified or developed again. The translation of a system design into a developed system has traditionally been a manual one. In addition the target of the translation, even if it is one of the common higher level languages, often requires detailed design decisions to be made prematurely just to get the system working. These languages do not provide a convenient means of adjusting the level of the target to one that is high enough so that lower level design decisions can be deferred.

As a consequence of these factors, the cost of the software development activity becomes high enough that emphasis is placed on trying to do as much as possible before any software development begins. Although it is always considered a good approach to put effort into preparation, the preparation and performance activities need to be carefully balanced. It is becoming increasingly clear that the usual way in which requirements for a system are developed is not adequate because of the increasing frequency of surprising undesirable results of the translation of requirements into a system. This is an example of too much emphasis placed on a form of preparation which does not adequately identify the important issues early enough. Among these issues is how the system is really expected to behave!

Experience with system development has repeatedly shown that more insight is obtained by the use of a system than by simply trying to read about what is expected of it. Given a system and its requirements, the behavior is more readily evaluated from its use than from thinking about how it might be used. This is not to say that all aspects of system evaluation can best be comprehended through examples. In fact, there are many important properties of a system that cannot be effectively determined by its use. For example, "bugs" can be found by using a system; but it is not (in general) possible to know when all the "bugs" have been found. The point is that a prototype of a system can be a very useful tool during the usual requirement and development activity. To be most effective, prototype development needs to be rapid so that it can be quickly made available to the User for which the requirement was formulated. A product of the requirement activity can be a prototype which is used to start the development activity.

In the prototyping approach, development becomes a prototype refinement activity. Although traditional programming languages and techniques could be used, they have some significant limitations. These limitations are the same as those which led to the traditional system development approach. An understanding of these limitations and a more advanced approach to programming languages and techniques that deals with them can break this cycle. The limitations and their consequences include:

- The low level to which a design must be carried out to produce a working system because the language level is fixed and far below that of the problem domain.
  - As a consequence, more detailed and otherwise relatively irrelevant decisions may have to be made just to get a prototype developed.
- There is no "explicit" form of the design and no way to transform it into a working system except manually.
  - As a consequence, changes in design decisions have to be carried out manually, making changes very expensive and limiting opportunities to learn from experience. A valuable product of the development activity is lost for future redevelopment. The only "real" product is the crystalization of the design. Although this is generally too fragile to be changed, it is the only thing available, short of developing the system again manually.

development capacity
is a limiting factor
in satisfying user requirements

> *if we had perfect insight,*
> *then systems could be developed*
> *from their requirements;*
> *but we don't*

A more advanced programming language and development technique should address these two classes of issues directly. Programming languages are needed which can be easily extended to problem domains characterized by the appropriate abstractions including notation, objects, and operations of the domain. System development environments are needed which can support a multi-level design which captures the design decisions. The combination of these two facilities can support the rapid development of prototypes, the development of designs, their transformations to production systems, and their redevelopment.

The Tension between Users and Developers

When new computer systems are being developed for Users, care must be taken to insure that the resulting system is reasonably close to what is best for the User rather then what is best for the system Developer. Each usage of "best" is relative to a different point of view based on the subject to which it is applied. For example, if the notion of "best" is that of "most cost-effective in solving the problem", the independent interpretation will still lead to conflicting results. This is because the User view considers problem-solving effort of human resources as the most valuable, while the Developer view considers the system itself as a valuable resource. The proper point of view lies somewhere in between these two extremes. Given the pressures on the User and the advancing state of computing technology, it is clear that the point can be put very close to the User in the future. As a result, the situation dramatically changes because system resources have and will continue to dramatically reduce in cost.

Unfortunately this does not remove the tension between the User and the Developer; it just changes its character. The decrease in cost of system components raises the expectations of the User. The problem then becomes one of combining components to meet these new expectations. This results in the problem solving time of Users and Developers in their respective domains becoming the critical resource. The User wants new tools to help solve problems, and the Developer needs to produce those tools. But the development of tools is itself a problem domain which can benefit from tools. The right tools have the potential of reducing development costs so that the Users get their tools sooner. Tools to produce tools could become tools of the User.

Some Familiar Consequences of this Tension

Some consequences of this tension being resolved in a way that is not favorable to the User demonstrate the need to be more sensitive to the User view. This goes beyond the system Developers because, in some cases, new technology is needed to fill important gaps. Initially the benefits of such systems outweigh their limitations. After some experience with them, the User expectations are raised and new issues are exposed. There is a tendency to try to use a given system for broader applications. Unfortunately the existing systems do not scale up well. There are some systems which are much closer to the ideal in some areas than others, but these have not all converged into a complete system yet.

Applications to New Technologies

A popular topic in future computing technology is personal computing. Although it seems clear that this technology offers many advantages over even existing advanced time-shared systems, there is much to be learned about it. At this time, it may be hard even to write requirements for future systems based on new technology because of our lack of experience with it. A useful way to gain experience in a new technology is to set up a laboratory for research in the area. Some early explorations have been done in various places, including R53, the Office of Computer Science Research, which already has a strong foundation in the underlying technologies. An example of such an approach can be found in the paper "A Laboratory for Developing Personal Machines" by [redacted]

P.L. 86-36

DOCID: 4009842

Advanced System Development Environments

No matter how advanced the hardware environments may be, they cannot be used effectively without advanced system development environments. An important component of an advanced environment is an advanced programming language. But an advanced language alone is not a sufficient goal. An advanced environment is needed to support the use of the advanced language throughout the lifecycle of the system. Some limitations of most existing environments will be discussed and some indication of what more advanced ones are likely to be like will be given.

The limitation of the traditional programming languages, including the higher level ones, is the size of the gap between the conceptual level of the problem domain and the language. Solutions to problems are expressed as programs. If the programs can be written in a notation natural to the problem domain then the gap is very small. As the problem domain moves further from that supported by a language, more effort is required to reformulate the natural problem-domain expressions to the lower level supported by the language.

If the problem domain is one for which the language is designed, then solutions will be easy to express in the language. However, if the domain involves concepts that are not in the language, then problem solutions will also have to solve a second problem caused by the language itself. The additional language problem may be sufficiently difficult to divert attention from the problem which was being solved in the first place.

Of course, special dialects of some languages have been developed to support more natural notations for this problem domain with these data types and operations. But, suppose that some problem is best expressed in terms of another data type. An unnatural notation will again be needed. This problem exists within the very limited domain of numerical expressions. The non-numerical world has a very rich collection of data types. In many cases they are created for each problem. From a human factors point of view the natural notation is the best. This is an example of the tension between Users and Developers in the domain of programming languages.

Programming languages which are advanced in this way and which can be used in an interactive environment are not just tools for the Developer to produce systems for the User; they can themselves become tools for the User! The importance of the environment must not be underestimated. Even with an advanced language, additional facilities are needed to support its use. These facilities need to have excellent human factors if they are to be effectively used by people throughout their activities. Personal computing will provide the quality of computing resources needed to support the human factors.

Just as languages are not a sufficient goal, environments to support their use are not sufficient either. Systems to support system development (or for that matter the NSA Analyst) are only as good as the people that use them. After all, the systems are only mechanical embodiments of some things which the Users understand. It is still up to the Users to have the intelligence to take the step beyond!

Conclusion

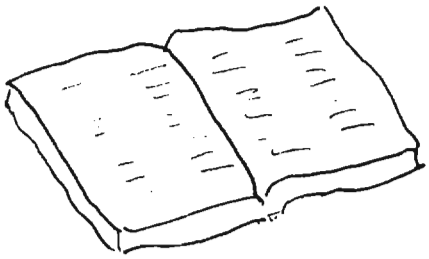
The development of systems has been explored with respect to the pressures on Agency Analysts, rapid advance of available computing technology, rising expectations of the User community, limited capacity to produce new systems, and increasing difficulty of formulating meaningful requirements. Among the various approaches that will be used to deal with future analytic problems will be an increasing use of interactive computing systems to provide advanced environments. Human factors requirements are among the most difficult and most critical aspects of these future systems. Prototyping has been suggested as a valuable experimental component in the requirement and design process.

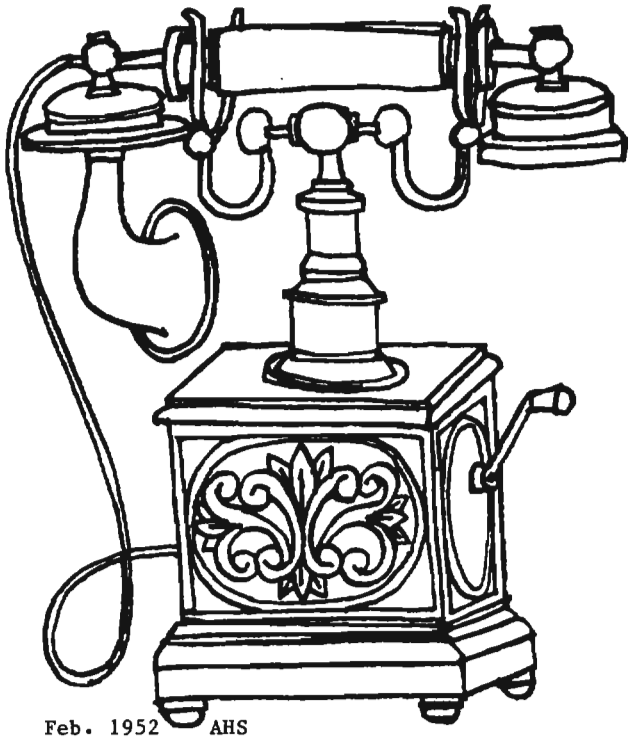
> *the use of a prototype system*
> *can reveal important insights*
> *that are not apparent*
> *from a requirements document*

DOCID: 4009842

Old Phone Books Never Die (U)

by William M. Nolte, T54





In addition to sundry other forms of aging paper, the History and Publications Division (T542) maintains a file of telephone directories prepared by NSA and predecessor organizations. This file, when used in conjunction with old organization charts and other documents, has been a valuable resource in preparing books and articles produced as part of the Cryptologic History Program. The directories are also helpful in answering the numerous reference requests handled by this office. They supplement our understanding of changes in Agency organization and frequently provide the most readily available source for the correct spelling of an individual's name or the organization to which an employee was assigned at a given time.

Directories currently on file include:

Date	Station or Organization
Jan. 1946	Vint Hill Farms Station
Sep. 1948	Arlington Hall Station (AHS)
July 1949	Naval Communications Station
Oct. 1950	Naval Security Station
Apr. 1951	Naval Security Station
June 1951	AHS
Dec. 1951	Naval Security Station
Feb. 1952	AHS
Oct. 1952	AHS
Oct. 1952	Naval Security Station
Apr. 1953	NSA
Dec. 1953	NSA
Jan. 1954	AHS
Oct. 1954	NSA
Oct. 1954	AHS
May 1955	AHS
June 1955	NSA
1956	NSA (Organizational Supplement)
June 1956	NSA
July 1956	NSA (PROD interim listing)
Fall 1956	AHS
Nov. 1956	NSA (Organizational)
Mar. 1957	NSA (Organizational)
Spring 1957	AHS
Fall 1957	AHS
Oct. 1957	NSA ("New Site")
Mar. 1958	NSA (Organizational)
May 1958	NSA
Oct. 1958	NSA
Jan. 1959	NSA (Organizational)
Sep. 1959	NSA
Jan. 1960	NSA (Organizational)
Jan. 1961	NSA
Oct. 1961	AHS
Mar. 1962	NSA
Mar. 1963	NSA
Mar. 1964	NSA
June 1964	NSA
July 1965	NSA
Sep. 1965	AHS

DOCID: 4009842

July 1966	NSA
Apr. 1967	NSA
May 1969	NSA
July 1971	NSA
Jan. 1972	NSA
Jan. 1973	NSA
Jan. 1974	NSA
Jan. 1975	NSA
Jan. 1976	NSA
Jan. 1977	NSA
Jan. 1978	NSA
Sep. 1978	NSA
May 1979	NSA
Apr. 1980	NSA
Nov. 1981	NSA

Unless described as organizational in format and organization, all the directories in the file are arranged alphabetically by employee name. Some of the organizational directories list all or most of the individuals assigned to a particular element, but most list only the chiefs or other principals.

~~(FOUO)~~ Though useful for many reference purposes, the directories are not infallible. The move to Fort Meade and one or two major reorganizations must have been confusing and stressful for everyone involved, but the persons responsible for the telephone system must have been especially pleased to see the dust settle after such reshufflings. One practice of interest, long since abandoned, was the use of directories to reinforce security consciousness. Dividing each letter of some directories of the late 1950s are security slogans of the sort seen on posters and other devices. "Dignity of man can be shattered by a careless tongue," cautions one such reminder in the May 1958 listing. The same edition also warns that "A secret's a secret only as long as its kept," a truism that appears only a few pages after the listings for William H. Martin and Bernon F. Mitchell (both of REMP 13 on 5323 secure, 7147 outside).

~~(FOUO)~~ Agency personnel holding outdated directories not listed above may wish to consider forwarding them to T542 for inclusion in the file. Such action entitles the donor to membership in the Pack Rat Society and the gratitude of the staff. By the same token, this office also would like to acquire Baltimore and Washington area "white page" directories from the 1940s through the late 1970s. We do <u>not</u> need every year within that span, nor do we need 247 copies of the 1979 editions. Persons with directories they may be willing to part with can call 2355s before putting them in the mail.

P.L. 86-36

DOCID: 4009842

HUMAN FACTORS CORNER

Consumer vs. Computer

BY [redacted] P13

P.L. 86-36

REVIEW: "Consumer Difficulties with Computerized Transactions: An Empirical Investigation," T.D. Sterling, Communications of the ACM, Vol. 22, No. 5, May 1979, pp. 283-289.

Reprinted from Human Factors Letter 1-80, published by CISI Human Factors SIG.

If you are among the overwhelming majority of citizens who have wondered again and again why "computers make so many mistakes", this article has much to offer in the way of enlightenment, if not in hope for improvement. If you share my suspicion that many of the goofups in bills and mailings are unnecessary consequences of bad design and poor management, Dr. Sterling's paper will provide confirmation. But the real surprise (to me, at least) is the strong indication that a considerable portion of the snafus are a consequence of deliberate and questionably honest business practices aimed at putting, and keeping, the customer at a disadvantage! The answer to "why computers make mistakes" is only sometimes "because programmers or data-entry clerks or system designers make mistakes." In some proportion of cases, the answer may well be "because computers were deliberately programmed to make those 'mistakes'."

Noting that "errors in computer produced bills and various communications sent by government (and other) agencies or businesses to citizens, clients, customers, and consumers are both commonplace and embarrassing to the computing industry ...", Sterling asks the following questions: "How many and what types of errors occur? What is the reaction of consumers after they encounter errors?" Few, if any studies have been made to answer questions like these (a fact which, in itself, seems strange to me). In 1977, a study was made by an organization or individual that Sterling calls the "Computer Ombudsman of Vancouver", in cooperation with the Consumer's Association of Canada (B.C.). This paper discusses the study's findings. (From the point of view of data gathering methods in human factors work, this type of study comes under the general heading of "critical incident" studies: focussing on incidents where a human-machine

DOCID: 4009842

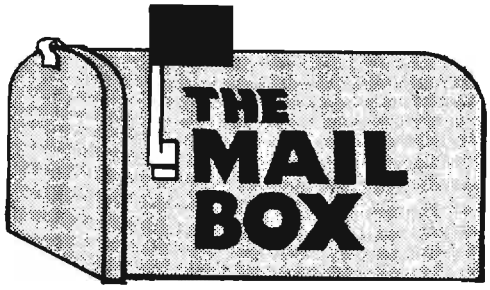
system broke down, malfunctioned, or occasioned some class of events or outcomes of interest in evaluating its strengths and weaknesses.)

A questionnaire was mailed to a random sample of members of the Consumer's Association, asking for experiences of household members with computerized transactions. In-depth telephone interviews were then conducted with people who reported specific problems in the questionnaire. The population was, according to Sterling, representative of "a broad range of middle-income groups". He frankly admits that it was probably rather atypical in one respect, namely the consumer orientation and the consequent aggressiveness and willingness to do battle in getting errors corrected. It was found that 59.5% of the households reported no problems with computerized transactions, but 25.1% had one, 10.4% had two, 3.6% had three, and an especially unlucky 1.4% had four such problems during the preceding twelve months. By far the largest proportion of the errors were related to department stores, credit cards/services, utility companies, and mail order business. Billing errors accounted for 81.2%, while all "dealing with governments" accounted for only a tiny 2.4% of the goofups.

When we see what the study showed about the different types of billing errors, a rather suspicious pattern seems to become even clearer. Almost all the errors result in a net financial gain for the billing entity: they include such things as charges for nonexistent expenditures, inappropriate charges of interest, and overcharges. Sterling points out that errors in the consumer's favor may well have been under-reported, but the balance is overwhelmingly in the other direction. In 73% of cases, respondents succeeded in getting the error corrected. Whether success attended their efforts or not, attempts to get errors corrected required one contact in 36.6% of cases, up to three contacts in 30.4%, and *four or more* contacts in an appalling 33% of the cases! It seems evident that both victims and offenders were admirably persistent and determined. Sterling points out that "each contact between a client and an organization requires additional 'overhead' time. The number of contacts is [a] measure of effort." The average time from discovery of an error to its settlement was 8 weeks, but 15% dragged on for 20 weeks. Consumers spent an average of 2.6 hours of their time in the attempt, but 20 hours or more were expended in 20% of the cases. In 10% of cases, it took extra effort to remove incorrect interest charged on top of incorrect charges, and in 2% of cases it was never removed. Trying to correct an error was often made unpleasant for the consumer. 16% of respondents reported having been coerced in some way to pay a disputed bill, often with an implied threat of damage to their credit rating. 8% were "treated as troublemakers".

Some customers, while continuing to deal with certain businesses that frequently offended, elected to pay cash in order to avoid the hassles, or to buy a magazine at a news stand rather than maintain a subscription. While Sterling does not explicitly apportion blame for the error-prone practices, he presents important evidence that points toward deliberate management philosophies as well as bad design of computing packages. Another study made in 1976 showed a 7-day delay on the average between the billing date and the time the bill was mailed, with a range of from 3 to 20 days delay! In the 1977 study, most of the victims of incorrect interest charges were also victims of this late-mailing practice. In addition, it is clear that "in almost 60% of the cases where interest had been charged on some disputed amount, it was *not* removed at the time when the charge turned out to be incorrect." This must be a consequence either of bad program design *or intentionally poor service.*

Sterling offers the following in summary: "We might ... ask if, with the use of all the power computers add to the task of management, it is really necessary to have systems that fail to correct errors, fail to inform customers where they may address a complaint, fail to remove interest in cases of billing errors, fail to adjust the printing of bills to the capacity of an organization to mail them out, and fail to do all the other things which careful examination of existing packages seems to uncover." He expresses a valid concern about the trend in the business community toward electronic fund transfer and a "cashless economy". "What will happen when the visible audit trail, such as checks, bills, and receipts, is replaced by electronic signals?" Next time you get an erroneous bill in the mail, don't blame the computer, the programmers, or the data entry clerks. Instead, consider placing the blame on business and management practices that encourage the design of bad and dishonest commercial software packages!



Dear CRYPTOLOG Editor,

(U) I am shocked that you would print a personal note from me to you in CRYPTOLOG (see Letters to the Editor, CRYPTOLOG, January 1982) without my knowledge or consent. As a result of your action a person of U/I sex ran into my office, bared its chest and demanded to know if it won the "Strangest Bust of the Month" contest, and "what was the prize?"

(U) A bust is not only an arrest when you are caught with the goods, a marble statue of George Washington, etc., but it is also a cryptographic abnormality (e.g. an error in encryption, a fault in equipment, a violation of rules for use) that may lead to some analytic understanding or exploitation of a cipher system.

EO 1.4 (c)
P.L. 86-36

publication.

(U) Sorry, no prizes.

[redacted]
B63 x5311

P.L. 86-36

I think it was [redacted] who said, on more than one occasion, "Whatever I get, I publish." Or maybe it was Art Salemme.

Ed.

Dear Wayne,

(U) A gentleman in one of the operational groups has correctly pointed out that Mark Twain died in 1910, and not 1909 as I had indicated in my article "The Literary Bends" (January's CRYPTOLOG). I respect his wish to remain anonymous. But to set the record straight, and maybe to do a little more drumming and trumpeting, could you publish my answer to his letter?

"Dear (Sir),

You're right! Sam died in 1910. Unfortunately, I implicitly trusted John O'Hayre's statement on page 106 of his Gobbledygook Has Gotta Go (I referenced his book in the footnote to the article). He says it was 1909.

What to do? I guess not much can be done, other than to express my sentiments like so:

Shall I point at O'Hayre
and say he is the one,
Who caused the mistake
I should never have done?
No. I'll just throw up my hands,
in spite of the shame,
And cite that cruel law
that uses my name.

I very much appreciated your comments.

Sincerely,
Al Murphy (E41)"

Thanks, Wayne. AM

A Toy Problem (U)

by David J. Tiren, G9

P.L. 86-36

(U) Determine the callsign system being used:

Stations:	1	2	3	4	5	6	7	8
Day 1	DRQ	YNM	KPH	ZLH	TIH	HWZ	QIM	OWK
Day 2	FGT	QBP	ESF	ZOE	UAE	ETI	TAP	RTN
Day 3	LJI	SFD	BHV	RCV	XWV	VUA	IWD	GUB
Day 4	CON	VKJ	AMY	UGY	WZY	YXW	NZJ	JXF

(U) Answer next month (the *original* answer from Dave came to us in a plastic bag, if that's any help to you!).

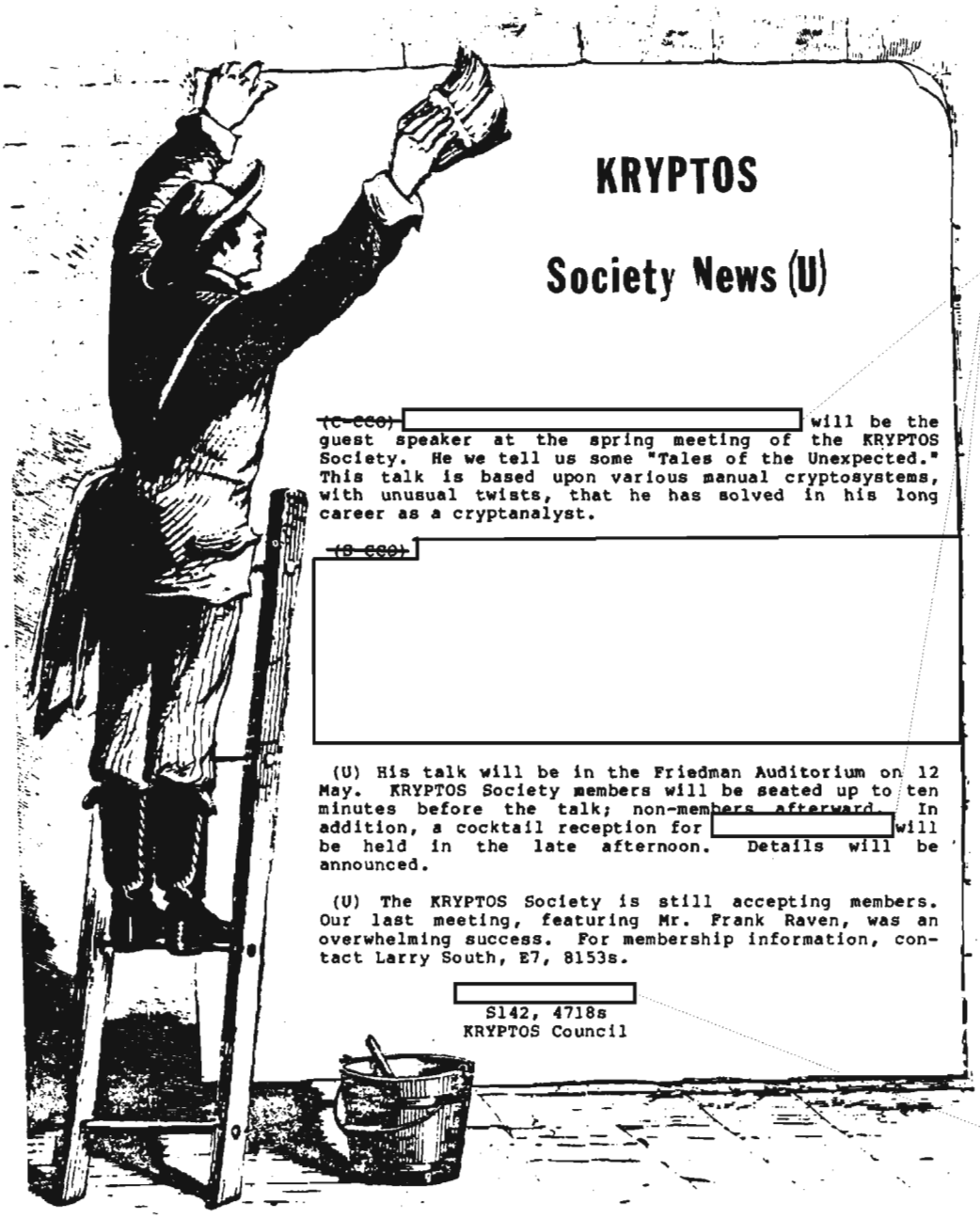
SOLUTION TO NSA-CROSTIC No. 38

"[Some] Thoughts on Lexicography," S[tuart H.] Buck, CRYPTOLOG, September, 1974.

"Glancing through the latest bulletin of the Mongolia Society, my eye [came upon] the following remark by John Krueger, professor of Altaic Studies at Indiana University:
'The very worst possible way to make a dictionary, and...the way that nearly all appear to be made, is to make a grand compilation of all existing dictionaries...'"

For those who are interested, here is the remainder of the quotation:

"...possibly abridging slightly and adding a few examples. The obvious and ideal way, seldom followed, is to begin with a set of texts, draw from them only the words used in those texts, and create a dictionary out of the actual recorded usage of the literature (or in the case of a spoken dialect, from the noted speech of the speakers). The latter and better course is self-evidently vastly more difficult and time-consuming."



KRYPTOS

Society News (U)

EO 1.4.(d)
P.L. 86-36

~~(C-CCO)~~ [redacted] will be the guest speaker at the spring meeting of the KRYPTOS Society. He we tell us some "Tales of the Unexpected." This talk is based upon various manual cryptosystems, with unusual twists, that he has solved in his long career as a cryptanalyst.

~~(S-CCO)~~ [redacted]

(U) His talk will be in the Friedman Auditorium on 12 May. KRYPTOS Society members will be seated up to ten minutes before the talk; non-members afterward. In addition, a cocktail reception for [redacted] will be held in the late afternoon. Details will be announced.

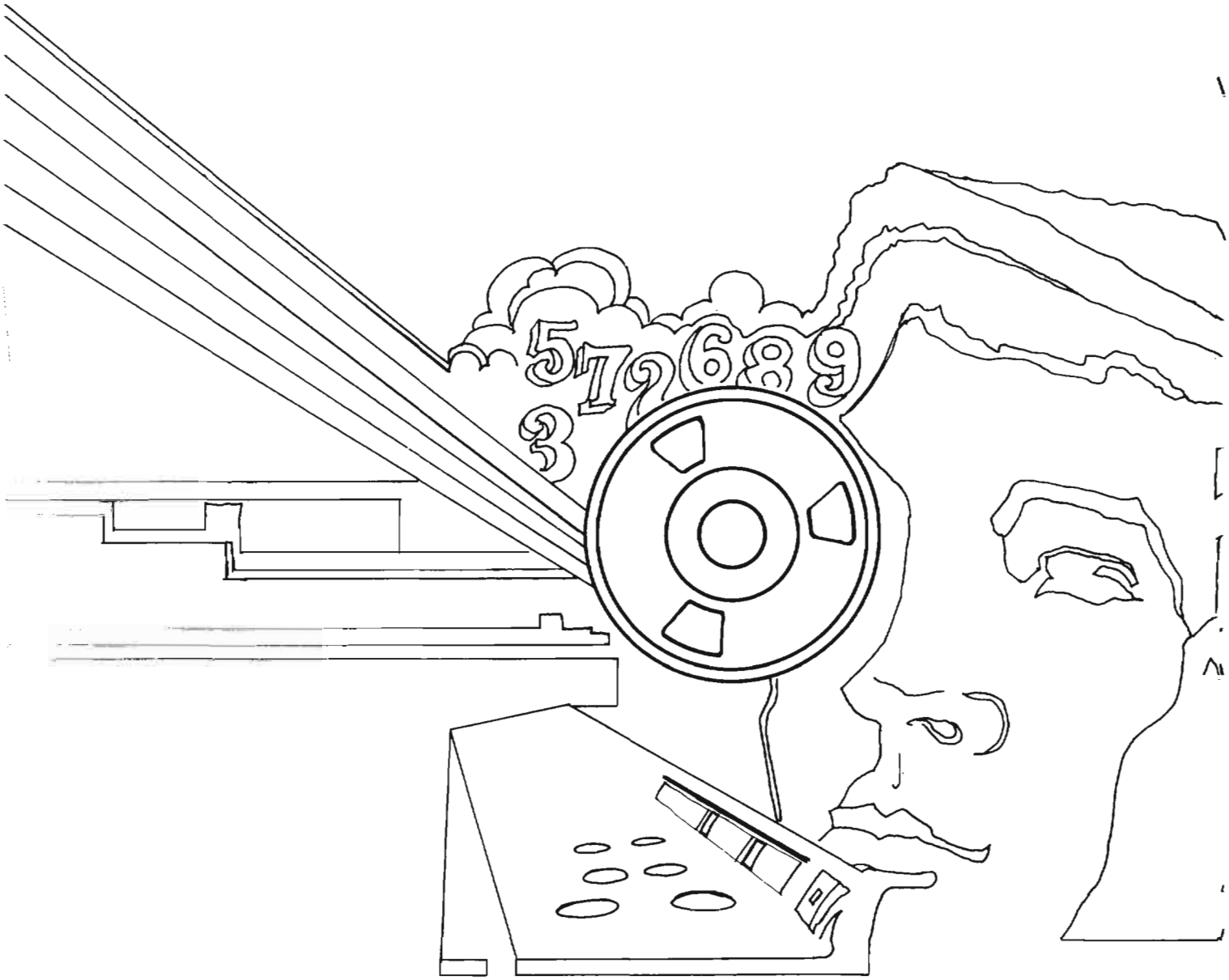
(U) The KRYPTOS Society is still accepting members. Our last meeting, featuring Mr. Frank Raven, was an overwhelming success. For membership information, contact Larry South, E7, 8153s.

[redacted]
S142, 4718s
KRYPTOS Council

P.L. 86-36

FOR RENT

Reasonable


5 7 9 6 8 9
3

DOCID: 4009841

P.L. 86-36

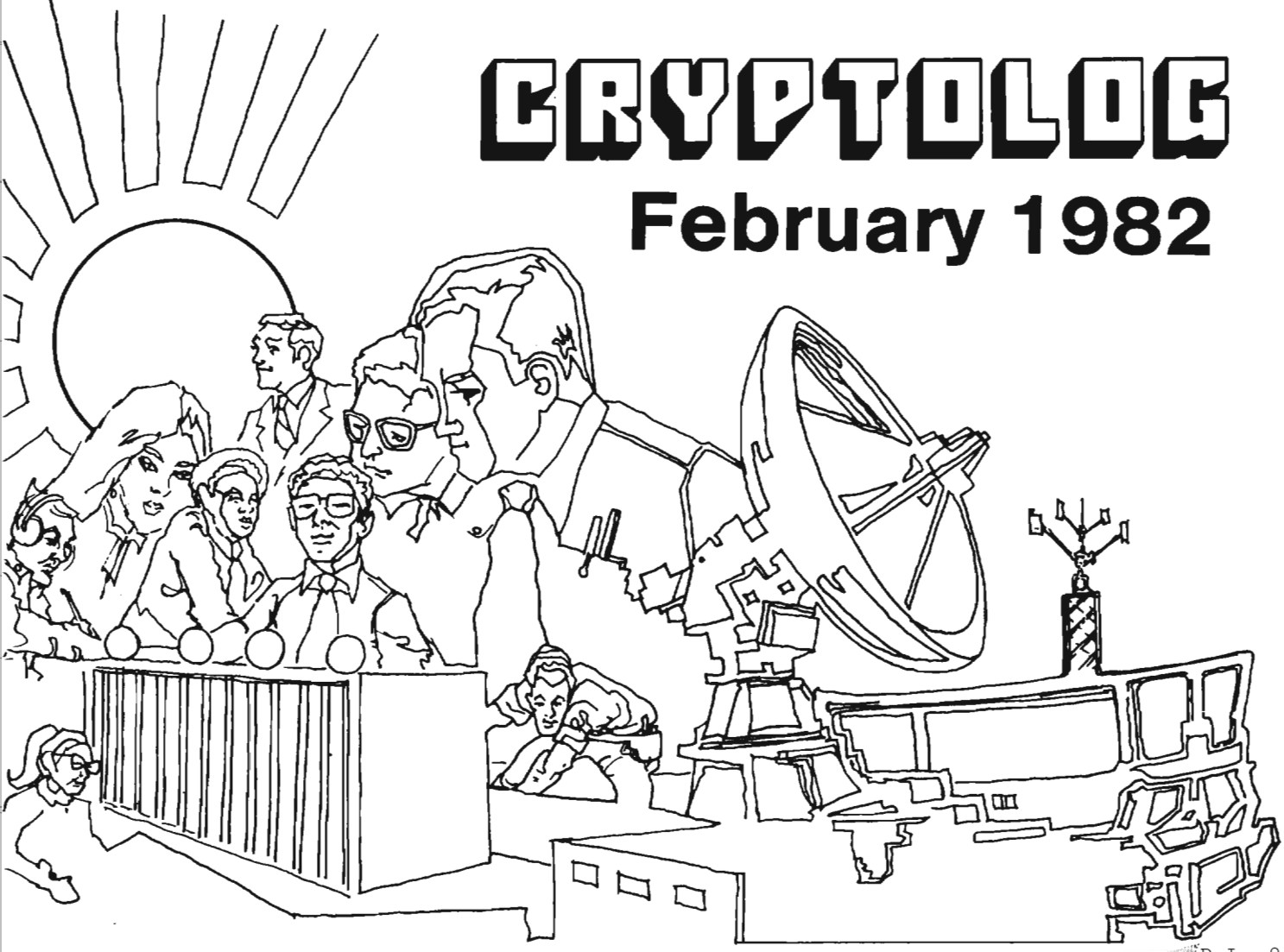
~~TOP SECRET~~

A27

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

February 1982



P.L. 86-36

NATIVE SCRIPTING OF LANGUAGES (U)..... [redacted] 1
A TIME FOR CHANGE? (U)..... [redacted] 4
AAAS, 1982: TWO REPORTS (U)
SOFTWARE (U)..... [redacted] 9
GAYLER (U)..... [redacted] 11
NSA-CROSTIC NO. 38 (U).....David H. Williams.....14
THE INTERNAL PERFORMANCE EVALUATION:
FRIEND OR FOE? (U)..... [redacted] 16
A WAIL, A COMPLAINT, AND A MELANGE (U).....Samuel S. Snyder, et al.....18
KRYPTOS: A NEW SOCIETY (U)..... [redacted] 20
CORRESPONDENCE (U).....23
SIMPLICITY IN COLOR (U).....C. Garofalo.....24
SOME ADVICE FOR USERS OF UNFRIENDLY SYSTEMS (U) [redacted] 26
...BUT WHAT DO I DO WITH MY PAPERS? (U)..... [redacted] 27

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 10 Feb 2012~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009841

~~FOR OFFICIAL USE ONLY~~

CRYPTOLOG

Published by P1, Techniques and Standards,
for the Personnel of Operations

VOL. IX, No. 2 FEBRUARY 1982

PUBLISHER [redacted]

BOARD OF EDITORS

Editor-in-Chief. [redacted] (7119/8322s)
Production..... [redacted] (3369s)
Collection..... [redacted] (8555s)
Cryptanalysis..... [redacted] (5311s)
Cryptolinguistics..... [redacted] (5981s)
Information Science. [redacted] (3034s)
Language..... [redacted] (8161s)
Machine Support. [redacted] (5084s)
Mathematics..... [redacted] (8518s)
Puzzles.....David H. Williams (1103s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Don Taurone (3573s)

For individual (or organizational) subscriptions send name and organization

to: CRYPTOLOG, P1
or call [redacted] 3369s

To submit articles or letters via PLATFORM mail, send to

cryptolg at barlcØ5
(note: no 'O' in 'log')

Editorial

A man named Jim Wilson, from Moscow, Idaho, told a story the other day. It seems that a certain community had a high cliff that was the cause of repeated accidents. People kept falling off the cliff.

The town council decided to take action and passed a resolution to use whatever funds they had to buy an ambulance and keep it at the bottom of the cliff. One member of the council, who had been away on vacation, returned and questioned the decision. "Why don't we build a fence at the top?"

But he was overruled. "We decided to do this thing right! So we took a poll. Everybody who had gone over the cliff said they didn't need any fence -- what they needed was an ambulance. So that's what we bought!"

What are you working on -- a fence or an ambulance?

WES

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009841

美繼續向台灣出售武

ประเทศเพื่อนบ้านใกล้เคียง

Native Scripting of Languages (U)

ปัญหาทางด้านเศรษฐกิจ

P.L. 86-36

by [redacted] P16
MT/MAT Coordinator
In Collaboration with
[redacted] P16
Language Processing Coordinator

P.L. 86-36

What is the value, in practical terms of providing an NSA linguist with worksheets in native script? This question has been asked and variously answered for as long as there have been NSA linguists. We may not be able to put the question to rest, but we hope here to surface the factors which need to be weighed in order to make an informed decision.

(U)

(U) The limiting factors in producing material in native script form are technological and economic. As technology has progressed, the availability of the script has increased, its quality has improved and the cost of producing it has decreased. By contrast, the linguistic and cryptanalytic reasons for or against having it have remained -- and may be expected to remain -- reasonably constant.

(U) What are the linguistic reasons favoring use of native script? They are so basic that no one would question them, were it not for the difficulties and expense of effecting the result. In the discussion which follows, ideographic languages, which pose the greatest challenge to technology, will be addressed specifically. However, general statements are intended to hold as well for other languages whose writing system is not based on the Latin alphabet.

[redacted]

[redacted]

(U) A second linguistic reason supporting native script is that almost all academic training is based upon it. Personnel arriving for duty are familiar with it, and those returning for advanced training must know it. Language acquisition requires extensive practice. Once learned, the skills are maintained through practice. If, after a thorough grounding, a person fails to use the language or some aspect of it, that person can usually reacquire the skills relatively quickly through practice, just as a person who once learns to ride a bicycle can, after a lapse of years, relearn the skill relatively quickly.

EO 1.4.(c)
P.L. 86-36

However, the person who has not learned the skill sufficiently well in the first place, whether it be riding a bicycle or reading a foreign language, will not enjoy this advantage of quick recall of skills. Providing native script routinely on materials processed daily gives the continuing practice needed to develop such a long-retained skill or to refresh a dormant one.

(U) The accompanying article was written in 1978 as part of the Language Processing Forum activities. The Forum itself is now dormant, but the remarks in the article seem to be current.

~~(C)~~ It is worth noting that NSA is now acquiring a hardware and software update of the IBM 3800 printing system. Included in the software package will be a set of dot matrix codes for Chinese, Forean, and Japanese, as well as an interactive character design program. Expected delivery date is 1 June 1982.

(U) Finally, the operational need for a flexible work force demands that a qualified language analyst in one element be readily transferrable to another element. As priorities shift or as attrition occurs within the work force, it should be possible to rotate an analyst with the appropriate language skill into another element, with a minimum of on-the-job training. Exclusive use of coding schemes by some elements and native script by others adversely affects this transferability.

EO 1.4.(c)
P.L. 86-36

[redacted]

~~(C)~~ The technological reasons for or against native scripts, as stated previously, change with the technology. There was a time when there were no automatic means for representing a large and complex character set. Since then, a wide array of offerings have been advanced, including cumbersome mechanical (impression) printers driven by paper tape; high-quality, high-speed plotters; and electronic devices such as full-graphics CRTs (cathode ray tubes) and electrostatic printers. Each component considered must be carefully assessed for its impact upon the analytic effort. The three major questions to be answered regarding adoption or rejection of a system are:

1. Are the characters of suitable quality for easy reading?

2. Will the system's dollar cost be excessive? and

3. What are the relative time costs?

These questions are subjective and should be made with as much valid information as possible. In answering the question regarding cost in money, the less tangible but very important linguistic impact, as delineated above, must not be discounted. In other words, the decision not to provide native script on the grounds of system costs must take into account the high cost of language training; the potential resultant decrease in the quantity and quality of SIGINT product; and the additional time, if any, it will take to train the language analyst in use of the alternative system. In a period when the supply of personnel with language skills is diminishing, collection technology is improving, and the work load is expanding, it is incumbent upon the manager to select methods which put those language skills to the most productive use. In regard to time costs, both the time delays imposed by the additional computer processing required to provide native script and the time enhancements accrued by increased productivity on the part of the linguist must be considered. Computer processing delays must be measured in conjunction with the time sensitivity of the problem and a conscientious assessment of the delay. For example, a delay of two hours could be excessive for a problem requiring 24-hour coverage and immediate response, while it could be quite tolerable for an operation being covered on one eight-hour shift, especially if the delay can be scheduled for a nonworking shift. Overall time enhancement resulting in more timely product may be expected when the technology selected for scripting does not inherently introduce excessive delays during prime duty hours.

[redacted]

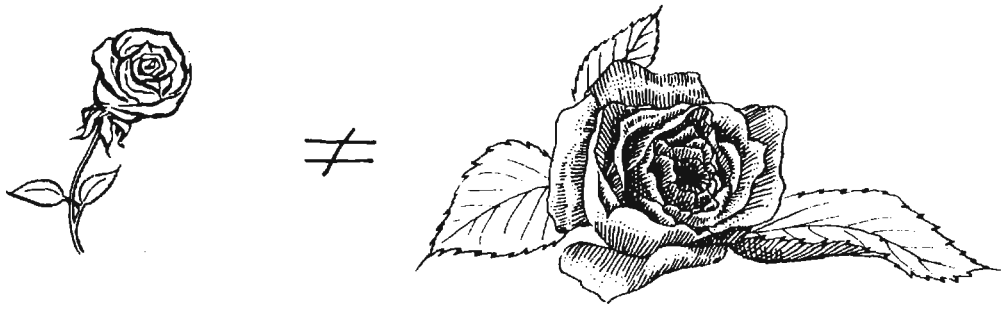
~~(C)~~ The following persons provided information which contributed to the report or concurred in the language of the final report (organizational designators reflect those at the time of concurrence):

[redacted] P.L. 86-36

A Time For Change? (U)

by [redacted] T53

P.L. 86-36



(U) With apologies to Gertrude Stein, a rose is not always a rose (at least not in the Intelligence Community). Over the years, each agency in the community (and many subordinate organizations) has developed and implemented its own unique formats for intelligence reports. Now we find that something as basic as the serial number by which a report is known has no common form, name or location. NSA calls it the "serial" but puts it on a line with no key; CIA calls it the "Report Number" and keys it accordingly; State Department calls it the "Message Reference Number" and puts it on the Classification line, while DIA calls it the "IR Number" and puts it in two places (the "Subject" line and the first line of Text).

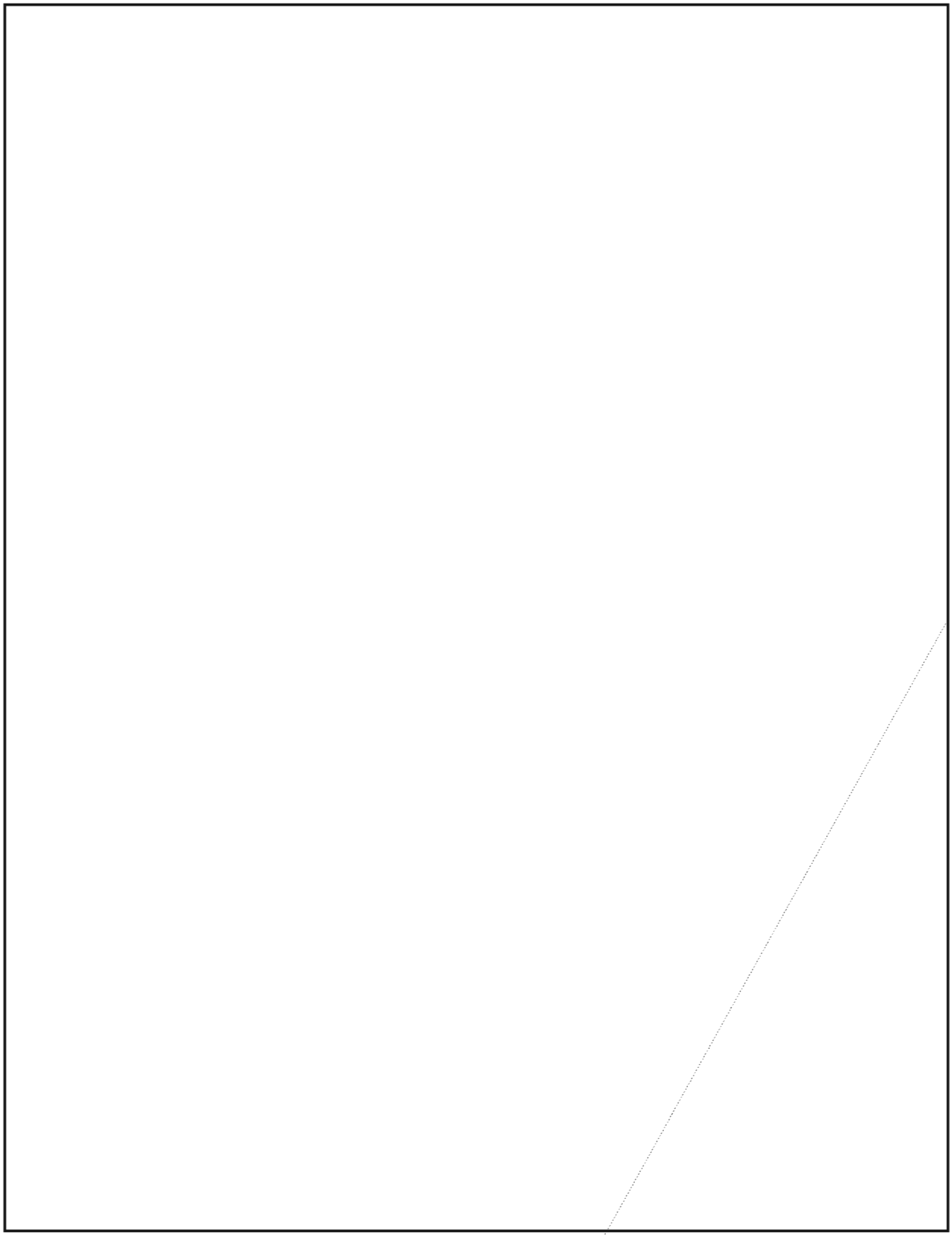
(U) Even within the same agency some vital report elements may vary from one vehicle to another. For example, the standard CIA electrical report has the report number in one place while the reports released by the Domestic Collection Division have the report number in two places (and often in modified forms). Also, the attention to format standards at the time of preparation leaves much to be desired in most agencies, including NSA. Key report elements are often misspelled, misplaced or arbitrarily abbreviated.

(U) Such "quirks" may have been inconsequential when everything was being scanned and distributed by hand. The human eye can easily search for and recognize whatever element of information is needed and will accomodate reasonable variations. However, now that each of the major agencies in the Community is building or planning to build major automatic distribution, indexing and retrieval systems, little differences add up to major design problems.

(U) The Intelligence Community is now at an important crossroad. The automation projects we are going to have to work with for at least the next decade are still in the development stages. If we are to resolve this format mess it must be now - before we are bound up by the implementation of systems designed for the individual formats. If not, each Agency will have to build complicated software to diagnose and index all of the report forms and the potential variations. Unfortunately, the increased complexity of such software will add operating overhead and require more human intervention in the form of editing.

(U) Any variation in the way similar elements of reports are presented adds significantly to the difficulty of retrieving information. If an analyst does not know that the serial number of a DIA Information Report is found on the Subject line, or that CIA reports contain a "Subject" not a "Title" he may well miss information vital to a project. Finally, if there is to be any significant sharing of bibliographic data bases throughout the Community, it seems reasonable that we speak the same "language."

(U) A study done by T5 of electrically received collateral intelligence reports revealed that, while there are unique elements in the reports of each Agency, there are also a significant number of common elements of information. Therefore a proposal to standardize electrical reporting formats was recently submitted to the Information Handling Committee (IHC) of the Intelligence Community (IC) Staff. The solution proposed is relatively simple; all members of the Intelligence Community should agree to and comply with certain broad format conventions for electrical reporting. This does not mean that all agencies will have to confine their



EO 1.4.(c)
P.L. 86-36

reporting to a single mold. Where there are common elements in the various reports, we should present them in a common way; and, where there are unique elements, we should use a standard pattern.

PROPOSED MODEL FORMAT (U)

(U) This proposal addresses only the information portions of an electrical intelligence report. It does not attempt to cover communications format problems. There are obviously, however, some areas that are of both information and communication concern. Where such an overlap occurs, an effort has been made to minimize the communications impact.

(U) In the proposed model format, the "information" portion of a report is broken into three sections: Address, Contents, and Management.

- The Address section consists of information about when the report was sent, who originated it, and to whom it was addressed. It includes the Precedence line, along with the From, To and Info lines.
- The Contents Section contains the body of the report, including the classification, accounting information, references, serial number, title, and text (among others).
- The Management Section contains information about the acquisition, preparation and disposition of the report. This final section would include review and declassification instructions, enclosure information, project numbers, etc.

(U) On the preceding page is an example of a DIA report in both the current and proposed formats. On the following page is a proposed list of the various lines that could be included in a report. No single report would ever contain all the lines listed as options, but every report would contain all those identified as required lines. Also included are examples of various other reports in the proposed format.

IMPACT ON NSA REPORTING (U)

(U) The IHC has formed a working group to look into the problem and make recommendations on the proposal. NSA, CIA, DIA, State Department, and each of the Services, have been asked to participate. T5, V1 and T1 represent NSA on this working group.

(U) The proposed format is not one used by any one Agency currently. It would require changes by all members of the Community, but represents a compromise employing facets from each of the current formats. No element of information being reported by any Agency would be omitted.

~~(C)~~ If the proposal is adopted as submitted, the expected impact on the current reporting format used by NSA should be minimal. We would flag certain lines with keywords (Serial, Accounting, etc), and probably change the Title to Subject. Other changes may be worked out by the working group as the effort progresses. However, since NSA has been reporting electrically for so long and using SOLIS for automatic indexing, our format is already well adapted to the current environment and is fairly consistent.

SAMPLE NSA REPORT

P 281906Z JUN 81
FM DIRNSA
TO NSA/OSCAR LIMA
[redacted] EO 1.4.(c)
NCR NMCC P.L. 86-36
WHITE HOUSE
BT

S E C R E T (CODEWORD) SECTION 1 OF 2
ACODEX/ ENP01F0081179
SERIAL: ?/XY/12345-81 SIGINT ALERT DUMMY
TAGS: ZDN ADEF AOPS LE SY
SUBJ: ZENDIAN AIR FORCE DEFENSIVE PATROL
REQS: TZ419

TEXT: _____
_____
_____

REVW: 28 JUN 11
BT
#3768
NNN

FUTURE DIRECTION (U)

(U) The proposal to the IHC also suggests that since format consistency and input quality are so important to the automatic indexing and retrieval systems, future on-line report preparation systems should be designed to do automatic quality control and verification of critical elements. In the case of NSA, we could have any product report being released checked by an abbreviated version of the SOLIS system. Thus, instead of editors correcting product reports after they are released, the reports would be returned on-line to the author prior to release with the errors marked. Obviously, such a system would have to have overrides for CRITICs or in the case of system failure.

Proposed Format

ADDRESS SECTION

** precedence/dtg
** FM
** TO
INFO
** BT or ZEM

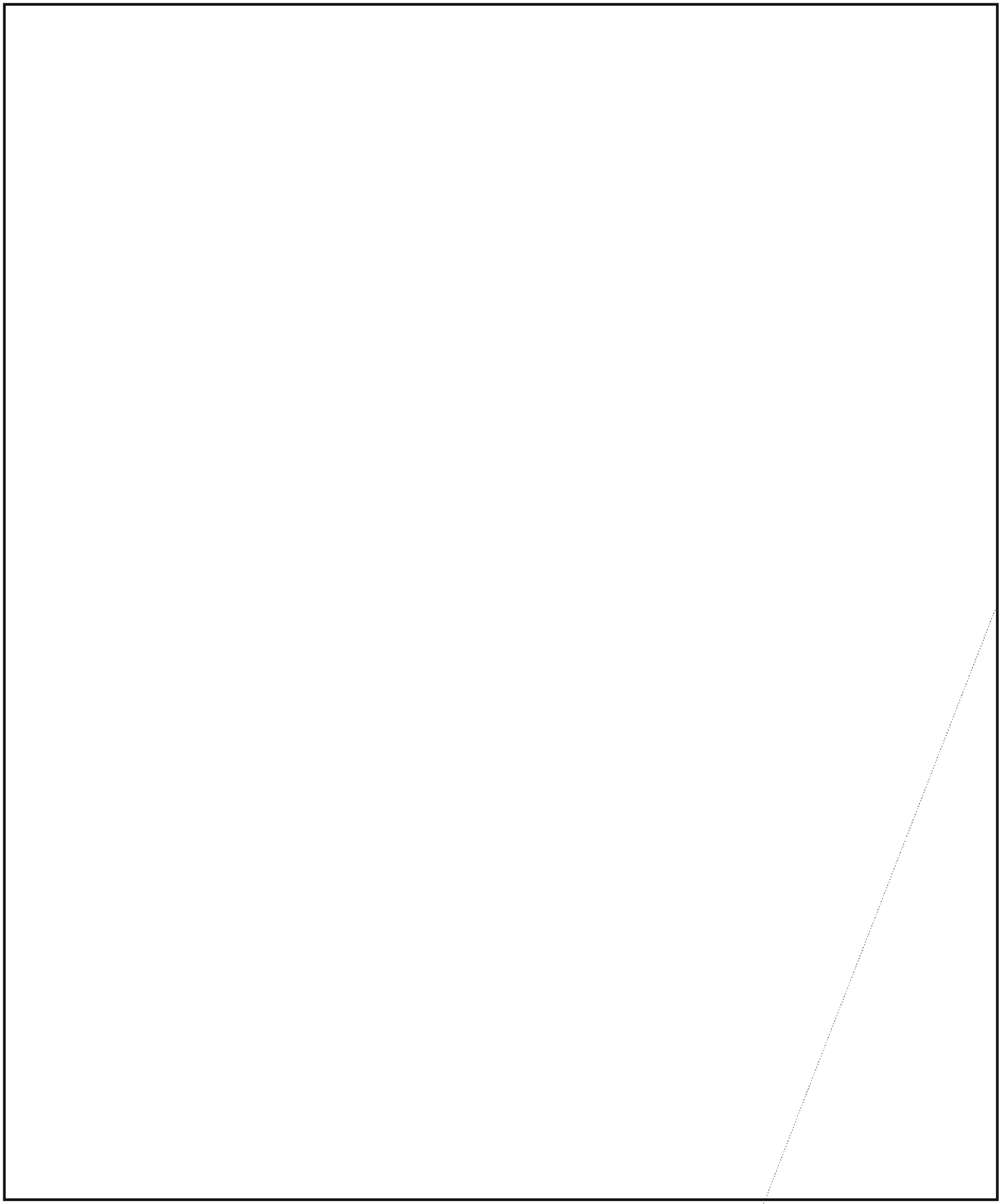
CONTENTS SECTION

**	classification/caveats	
	CITE:	Cite numbers
	ACODEX/	SIGINT accounting information
**	SERIAL:	Report number
	PASS:	Passing instructions
	WARNING:	Literal warning notices
	DIST:	Distribution date
	EO 12065:	State info on conformity with 12065
	CTRY:	Country codes
	TAGS:	Tag codes
**	SUBJ:	Title
	REF:	References
	DOI:	Date of the information
	ORIG:	Originator (other than the FM address)
	REQS:	Requirement numbers
	SOURCE:	Information concerning the source of the material
	SUMMARY:	Summary paragraph
	COMMENTS:	Preparers comments on the report
**	TEXT:	The actual body of the report (the Intelligence)

MANAGEMENT SECTION

	PROJ:	Project numbers
	COLL:	Collection management codes
	INSTR:	Special instructions
	PREP:	Prepared by
	APPR:	Approved by
	EVAL:	Evaluation requirement
	ENCL:	Enclosures
	ACQ:	Report acquisition information
	DISSEM:	Field dissemination
	REVW:	Classification review date
	DECLAS:	Declassification date
**	BT	

** denotes required fields



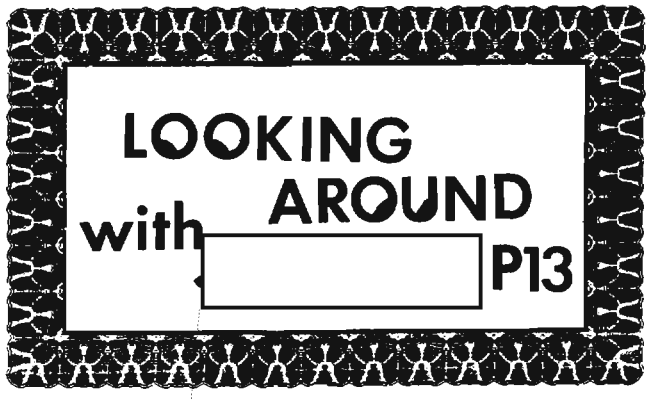
EO 1.4.(c)
P.L. 86-36

DOCID: 4009841

American Association for the Advancement of Science, 1982

◊Two Reports

- ▫ Software
- ▫ Gayler



P.L. 86-36

Programming languages and operating systems were analyzed from a human factors viewpoint in the 1982 AAAS (American Association for the Advancement of Science) meeting in Washington, by Dr. Ben Shneiderman of the University of Maryland. One of the surprising discoveries was that comments make a program harder to understand. Indentation also impedes understanding, which is opposite to popular belief. Most operating system messages are hostile, and accusing, e.g. FATAL ERROR, RUN ABORTED or ILLEGAL PASSWORD, as if the user had committed a crime. This apparently reflects an innate hostility toward other humans by systems designers.

An interesting technique was developed for controlled experimentation with programmers to test human factors. Programmers at some skill level were given a program to study which used certain combinations of language, comments, indentation, mnemonic names, control structures, etc. Then they were asked to reconstruct the program from memory. Independent variables were altered, and statistical methods used to verify hypotheses.

The cardinal reason why comments and indentation interfere with comprehension is that they take space and cause the program code to be spread over more pages. The page flipping impedes short term and long term memory, and creates "noise" in the understanding process. If the comments are printed to the right of the computer code, the resulting program script is much more compact. Indenting two spaces is better than four spaces. It is important to avoid dangerous cluttering. Higher level comments, which describe the problem domain rather than the program domain, aid comprehension. Shneiderman reported that the Begin-End blocks of PASCAL were harder to use than the When-If of ADA.

In the design of terminal operating systems there are three categories of users to be considered, viz. novices, knowledgable infrequent users, and experts. Each needs a different operating system. The novices need the utmost in clarity and simplicity, with a small number of meaningful commands. Knowledgable infrequent users need simple commands, which are easy to remember.

Psychological issues are:

- short term (human) memory load: the displays should be kept simple;
- closure, the desire for completeness;
- anxiety, called "computer shock" or "network neurosis" caused by the fear that the machine will dominate the user;
- locus of control, a desire to be in charge.

Response time is a complex matter. A lag of more than 15 seconds may disrupt thinking. Apparently it is beneficial to reduce the variation in response time within the system.

On line assistance may be more confusing than paper manuals. The screen formats should be predictable so the users will remember where to find information. Paper is a separate medium with wide bandwidth, non-volatile memory, portability and no outages.

Error messages are usually hostile, and frequently uninformative, e.g. "guard mode error 2". System messages should be brief, positive, constructive, specific, comprehensible. Usually the system messages are an afterthought, assigned to the least experienced programmer. The operating system should be designed around the system messages. Currently, no one keeps track of the errors that users make.

The mark of a good language or operating system is user satisfaction (not designer delight).

Shneiderman proposed that academic and industrial computer researchers should introduce controlled psychologically oriented experiments to develop research data on computer human factors. Commercial program and system designers should: create standards and metrics for software quality, develop guidelines for interactive system design, and promote the use of pilot studies.

Currently operating system "documentation" is word of mouth. It is efficient to write the documentation before the coding.

A number of publications were cited, viz: Software Psychology, a book by Shneiderman, and IBM Systems Journal. There was a six article series in ACM Computing Reviews, March 1981 on Database Language Research. At NBS in March 1982 there will be a meeting on "Human Factors in Computer Society".

McKeeman from Wang Institute noted that software was much too cheap and was produced by untrained amateurs whose low quality code caused expensive problems for the users. Programmers lack professionalism because they lack the power to say "NO!" to a bad task or decision. Programmers at TRW have about one tenth the training in their skill as GM auto workers. Where software is used in public safety matters, e.g. medical, air traffic, law enforcement matters, it should be produced by licenced professionals who can refuse to produce or certify inferior or untested code. (Note: the FAA is starting a $8.5 billion automated air traffic control system to replace most of the human controllers by computer software, so the issue is not academic.)

Stucki of Boeing observed that the direct cost of producing software may be much less than the indirect cost of the errors it makes. He cited the famous failure of the APOLLO 8 moonlander software which failed from input overload 30 meters from the moon's surface. The pilot then did a manual landing. Shuttle I was postponed for a software reason. The French have a system of 100 weather balloons, half of which were lost when the command software issued a self destruct order.

Irland of BTL said that 12 years ago the first SPC (stored program control) switch was designed for low down time, but failed due to severe software bugs that require reinitialization about 30 times a day, when a 40 year run between reloads was expected. The effects of real traffic were unforeseen. Now SPC switch software does not fail severely when it goes into service, but it still takes hundreds of switch-years of operation to discover and remove residual bugs. In 1950 BTL produced no software, while now 50 percent of BTL staff work on software. They now produce software at 100 times the rate of 15 years ago, but the team experience is lower.

There has been major growth in software effort, and in real time applications, and in life-critical applications (space, medicine, air travel). There has also been growth in the complexity of systems which network micros, minis and macrocomputers.

Maxims of software quality:

- Quality must be designed in, it cannot be tested in.

- Programs which are "good" or "correct" are of high quality.
- The earlier in the process the defects are eliminated, the better.
- Bugs are never all eliminated.
- The most costly bugs are in the requirements,
- There is a paradox in trying to control software quality when it cannot be measured.

A critical point is that all requirements must be testable. Many metrics for software quality have been found wanting. Some bugs are much more costly than others, so that mere bug-removal counts are not a guarantee of reliability. Initial bug density depends on requirements, experience of design teams, development environment, and methodology.

GAYLER ON ARMS CONTROL (U)

The elimination of manned aircraft, tactical nuclear weapons, chemical weapons, and small surface warships were among the recommendations made by Admiral Noel Gayler USN (Retd), former DIRNSA, at a AAAS meeting on Arms Control on 8 January, 1982.

The AAAS meeting was concerned with setting goals for defense R&D to improve the security of the U.S. and other nations. Admiral Gayler was joined on the panel by William Perry, former DDR&E, and Richard Garwin of IBM, a noted Arms Control expert. There was a surprising amount of agreement among the panelists about the uselessness of many expensive weapons systems, particularly the MX. Since Soviet manpower costs are only one fourth of their military budget, while these costs come to more than half of the U.S. defense budget, the point was aptly made by Dr. Perry that a numbers race against the USSR would be impractical because any expansion of numbers of weapons would increase the manpower demands and hence leave even less money for necessary hardware. Under Lanchester's Law, if the USSR has four times as many tanks, U.S tanks must be sixteen times more capable. This also is hopeless. The only answer to the Soviet threat, according to Perry, is the development of superior technology which doesn't require manpower or money.

Dr. Garwin criticized the MX and argued that the central problem in setting R&D goals was to search for better alternatives to unsuitable weapons. He drew attention to the bureaucratic and political obstacles to considering alternatives. He then described the SUM system, in which a fleet of small conventional submarines operate within 600 miles of the U.S. coast and carry a few MX missiles in capsules. The resulting secrecy and physical security would make a Soviet first strike impossible, and would cost much less than the MX. So far the Air Force appears uninterested in this alternative. Garwin advised looking for things that didn't fit into a bureaucratic niche, because new technology won't fit.

Admiral Gayler then developed his argument about new technology from first principles. The USSR and Warsaw Pact, he noted, had all the resources and physical means to maintain their war capacity already within their geographical domain. They had no global needs. The West by contrast was a loose transoceanic alliance. All the Western countries are in a deficit status in raw materials, they must import. China is a makeweight. There is no "China card" and no alliance. There are "uncommitted" countries, many of which have a surplus of resources. The national security missions in this context are complex, since economic and political factors as well as military factors apply. What do we want to do? The primary aim, according to Admiral Gayler was to avoid coercion by the USSR, i.e. where the USSR could split the US from its Western allies, or make the resources and raw materials inaccessible to the West.

DOCID: 4009841

The West can succeed in preventing Soviet coercion by concentrating its defense efforts, and reorganizing its defense, to try "leap-frogging" the Soviet numerical buildup and geopolitical expansion. The military tasks are:

- Keep sea and air communications open. This requires the capability to defeat air and sea forces, and to control information.
- Hold ground ,e.g. in Europe and Korea. The West must be able to defeat armor and infantry, and to control information.
- Project power in remote areas of the world, with or without bases.

To accomplish these goals requires weapons control. Enemy weapons must be hit precisely, not just bracketed by saturation fire. The effectiveness of modern precison guided weapons is great, and the total costs of an engagement will be reduced by accurate fire.

To illustrate the value of precision application of force, Admiral Gayler contrasted the mining of Haiphong harbor, which was accomplished without casualties and brought the North Vietnamese to the bargaining table to arrange a cease fire, with the combination of saturation bombing and massive infantry operations in the jungle, which were inconclusive and produced heavy casualties on both sides.

The new defense strategy would depend on modern target acquisition systems, imaging and signal processing, and detecting emanations. The primary applications of the new technology would be for the missions of search, surveillance and intelligence. Admiral Gayler noted parenthetically that most useable military intelligence comes from the electromagnetic spectrum, not from agents or informers. (Presumably this means SIGINT, imagery and radar). A central information "spider" with all data flowing into an overloaded central node for decision making, would not be suitable. Continuous control of information was vital. (Note: Admiral Gayler did not define the term "control of information" but apparently meant a broad concept of acquiring and protecting all kinds of information. Possibly he meant control of technological information as well as operational military information).

Space gives line of sight access for information and surveillance. Space will be the dominant factor in naval war in ten years, e.g. by the application of ocean surveillance systems and weapons guidance systems that will allow over the horizon targeting. The evolution of space to a combat zone is inevitable. Admiral Gayler gave the example of the early use of aircraft in World War I in which the French and German pilots on scouting missions waved to each other at first, but soon turned to battles for air supremacy. Space was a good place for a "contraption war" in which heavy battles between machines could be fought, without producing human casualties or collateral damage. To establish a U.S. military position in space the first step was to get a Space Commander, similar to the land, sea and air commanders now in control of those military missions.

Robotics will be an important factor in future defense systems. Current examples of robots are satellites and nuclear power plants, where complicated machines perform tasks in environments in which humans can hardly function. Manned fighter and attack aircraft are about obsolete in the current environment of surface to air missiles. Not only do the USSR and Warsaw Pact have a big SAM defense, but even small countries have SAM weapons which are capable of shooting down U.S. and allied manned aircraft. Admiral Gayler interjected a comment that although he was a former combat aviator, he saw no point to training and executing manned air missions in which the pilots had no chance of survival or of accomplishing their missions. The solution was to go to robot fighting vehicles on land and in the air. The man would be in the combat loop, but at a safe location on the ground, instead of being spun around at 6G stresses while he was trying to hit a target. Specialized small tanks, which were expendable and automated, could also do the ground combat function, with the operator safely located. The key element was a reliable data link, and Admiral Gayler was sure that U.S. technology could provide that. (Comment: if such remote fighting machines do come into service, future battlefield communications will be even more voluminous and critical than ever before).

Sea battles in the future will depend on acoustic warfare. At the present time the U.S. has developed its electromagnetic warfare and intelligence to a high degree. A similar development in acoustic surveillance, intelligence, countermeasures and security is needed.

DOCID: 4009841

People are a problem in the Armed Forces because there are too many of them, not used efficiently. Admiral Gayler said that, based on his experience as a task force commander, a modern large carrier could be operated with one half of the 2400 people, by better use of technology. He gave an illustration of a catapult operation, in which four men are used in a human chain to decide when to fire the catapult, which depends on the pitch and roll of the carrier, where one man with a reliable command control link could do the job faster and better. By reducing the size of the armed forces, the military services can be more selective in who they hire and retain. In training military personnel, the U.S. should use technology like the arcade computer games, rather than expensive and old fashioned training methods.

Maintenance should be based on "no failure" devices. Earlier, Dr. Perry had proposed "throwaway" maintenance, as currently practiced with handheld calculators.

Personnel policies in modern war should be based on motivation, selection and allocation of tasks. Admiral Gayler remarked that the main element in a sea battle was which side had the smartest Admiral.

Weapons of mass destruction have no military utility as theater or strategic weapons. If tactical nuclear weapons are used, the nuclear conflict will immediately escalate, and the damage to allies will be extreme. Therefore the only need is for central strategic nuclear forces, to deter any use of nuclear weapons, and these strategic systems should be survivable. The primary point of vulnerability in a central war is not the nuclear forces, but Washington itself. The USSR will develop and maintain both fixed and mobile ICBM's. Chemical and biological weapons have only a deterrent utility, they are not effective combat weapons.

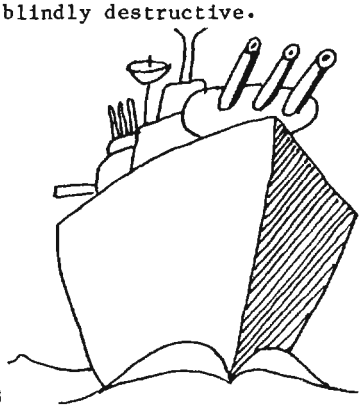
Money is important for defense, but currently most is spent on people. The answer is to reduce the number of people, not only in the uniformed services, but in the civilian bureaucracies which are associated with each Service, and have much duplication of staff and function. The elimination of the the three civilian Service Secretaries would, in Admiral Gayler's view, be useful.

Unneeded programs such as the B1, and MX should be cut. The B1 seemed to Admiral Gayler to have little use, while he stated that the MX was destabilizing. There is very little payoff in security from nuclear weapon development. Most of the surface navy is not needed, particularly destroyers. The Sea Control functions (of protecting shipping, and clearing or blocking sea lanes) can be done only by submarines, supported by long range aircraft and surveillance systems.

Science should concentrate on payoff areas, and should seek "step function" advances.

In response to questions, Admiral Gayler noted that the proliferation of precision guided weapons (PGW's) to small countries had raised the level of military violence in a way that could threaten US forces. His proposal for the elimination of all tactical nuclear weapons was predicated on reductions by both sides, rather than unilateral action. He agreed that the transfer of the Atomic Weapons program from Department of Energy to the Department of Commerce, which had no security role or competence, was not a sign of a well thought out reorganizaton. When asked about the apparent indifference of the "man in the street" to the massive and terrifying buildup of long range nuclear weapons, Admiral Gayler cited the psychiatric concept of "denial" in which a man told he has terminal cancer replies that he feel fine, refusing to even consider the facts of his condition. This, in Gayler's view, caused people to shut out the facts of nuclear annihilation, which are too awful to face.

When asked specifically what kinds of wars he thought the U.S. should prepare to fight in the future, Admiral Gayler said they should be non-atomic, should not involve large infantry commitments, and should be focussed only on specific military targets, like the mining of Haiphong harbor, which would be decisive rather than blindly destructive.



DOCID: 4009841

NSA-Crostic No. 38

by dhw

According to a long-standing show business tradition, a newcomer whose name is the same as that of an established performer must adopt a new name. Harry Morgan and Tim Conway are two examples of this tradition. Words M and V are two others.

A. Jayne Meadows' husband (full name)

265 140 119 97 184 168 128 133 180 200 215 65 189 75 40 95 233 161

250 145 171 5 83 186 49 197 109 31 227 220 202 158 19 18 89

B. ____ au rhum

84 199 25 195

C. Asian capital (2 wds)

92 244 108 4 157 166 257 231 105

D. See Word F (3 wds)

256 191 232 134 151 153 229 123 181 176 246 149

E. American singer and actor, former Rhodes Scholar and instructor of English at West Point (2 wds)

222 11 44 23 167 262 216 46 16 104 34 107 29 178 120 239 7

F. Play and film starring Word Q (3 wds foll. by Word D)

24 10 142 165 111 124 160 36 39

G. Hawaiian word denoting a non-Hawaiian person

88 59 209 72 68

H. Lap _____ (3 wds)

70 100 51 190 55 41 164 214 217

I. Customary practice

130 114 177 94 61

J. Spur, urge

77 87 169 125

K. Caribbean nation

15 129 174 183 156

L. Keen feeling for what is appropriate

110 81 172 115

M. British actor, real name James Stewart (2 wds)

154 173 50 147 20 91 192 1 207 45 76 14 185 196

N. Winner of 1981 Liberty Bowl (2 wds)

106 67 234 73 150 122 127 138 159

O. Delicate exactness, subtlety

228 137 113 144 9 162

P. Pierced with a sharp instrument

27 243 260 230 211 182

Q. Late American actor, former English instructor at Harvard (Thornton Wilder was one of his students), made his acting debut in Word F (full name)

264 117 253 206 226 212 99 193 21 112 28 245 6 241 240 ____

74 12 219 201 43 223 52

R. Percussion instrument

247 139 2 64 152 17 175 32 22

S. Tending to cause discontent or envy

T. Sleeveless garment; ness

U. Condition of being most satisfactory

V. British actress, real name Jennifer Jones

W. Sharp repeated rapping or knocking (comp.)

X. St. Francis of _____

Y. American actor, M.B.A., once employed by the Budget Bureau of Connecticut(2 wds)

Z. Made helpless

Z_1. "Too wise you are, too wise you be;
I see you are too wise for me."

255 131 143 238 170 248 148 116 102

58 236 204 57

47 63 35 258 80 224 235 132 66 146

8 79 53 60 187 86 259 252 101 136

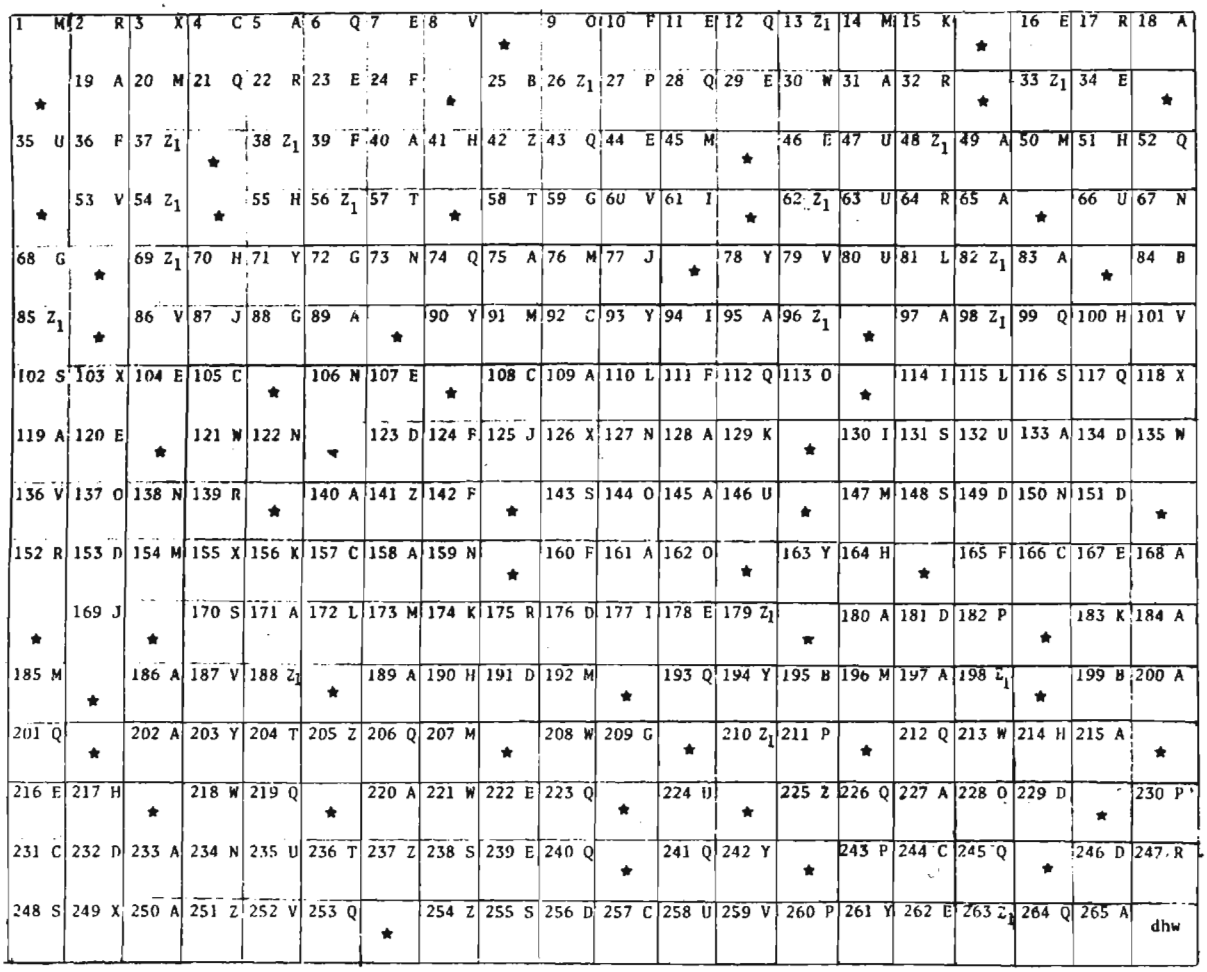
135 221 30 213 208 121 218

3 249 155 118 103 126

203 194 163 93 78 242 261 71 90

141 42 225 237 251 205 254

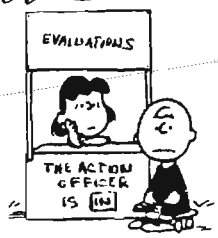
179 54 13 96 198 85 62 210 263 48 26 82 188 56 69 33 98 38 37



DOCID: 4009841

The Internal Performance Evaluation: *Friend or Foe?* (U)

[redacted]



P.L. 86-36

(C) What do the USSID System, the Alternate Intercept Coverage Plan, the Vital Records Program, and Agency Staff Responsiveness have in common? As you may have deduced from the title of this article, each is the topic of a recent Internal Performance Evaluation -- IPE, for short. It is readily apparent that IPE's cut across a wide spectrum of Agency operations; so, it is probable that you will one day encounter the process. In this article we hope to take the mystery out of the IPE by defining it, by examining how it comes to be, and by looking at the results that come from it. In so doing, we hope to convince you that the IPE is not a foe, but a friend -- a friend that has the potential to improve your operation.

(U) To begin, we should put the IPE into its proper perspective. The IPE is one of several elements of the Performance Enhancement Review Program (PERP). Established by USSID 520, the PERP is a management system designed to provide DIRNSA/CHCSS, Key Component Chiefs, and SCE Commanders with information needed to make decisions concerning the operational performance of the US SIGINT System. The objective of the PERP -- and consequently the objective of an IPE -- is to improve the efficiency, economy, and effectiveness of the US SIGINT System.

(U) The Director of Performance Evaluation manages the PERP, which includes not only the IPE's but also Field Assistance Visits, Field Evaluation Visits, and a PERP Panel. Overall, the PERP examines systems, programs, plans, or activities that support the US SIGINT System. Specifically, the IPE evaluates systems, programs, or activities internal to NSA and under the direct operational control of DIRNSA/CHCSS. The PERP Panel, an executive forum for coordinating and evaluating results of the PERP, may be used to discuss potential IPE topics, the status of an ongoing evaluation or the results of a completed one.

(U) How does an internal Agency program or activity become the subject of an Internal Performance Evaluation? It begins as a proposal from Congress, DIRNSA, Key Component Chiefs, SCE Commanders, or individuals assigned to the Agency or to its field activities. Many of the proposals, however, are generated within the Performance Evaluation Directorate itself, Q2.

(U) The proposal process begins by defining a potential internal evaluation topic and ends with a management "go/no-go" decision. There are two major decision points along the way. The first of these is the evaluability assessment. A potential topic is assigned to a research Action Officer, who first validates it through a cursory examination of the topic and the variables involved, and then makes one of three recommendations:

- to continue the evaluation,
- to terminate it, or
- to put the proposal into a data bank of projects to be conducted at a later date.

The decision at this point is made by the DPE.

(U) If the decision is to continue the evaluation, then the Action Officer will conduct detailed research, meet with concerned activities or elements, and conduct briefings or meetings as required. While doing research in-depth, the Action Officer also develops the evaluation methodology, the road map that will be used to reach the most valid and reliable conclusions within available time and personnel constraints. The methodology developed is a large part of the second major decision product, the formal Evaluation Proposal.

(U) As you might expect, the Evaluation Proposal really digs into the topic. It looks not only at the methodology, but also reviews the background of the subject and tries to assess what contribution can be expected when the evaluation is completed. It defines the approach to the evaluation, explains what data will be collected and how it will be analyzed, and tries to estimate the cost of the

DOCID: 4009841

evaluation. The objective is to help management decide whether the proposed evaluation is both feasible and worthwhile.

(U) If you have the impression that the Evaluation Proposal process is time-consuming and methodical, then you are correct; but we keep it that way for good reason: we don't want you to view the IPE negatively. In fact, we think the most important parts of the proposal process are the communicating and coordinating that go on. At every step of the way, the Action Officer and the elements involved work together. They participate in meetings and briefings on the topic, and they jointly develop alternatives, options, and recommendations. All this is to ensure the integrity of the evaluation and that it works *for* you, not *against* you.

(U) Here, perhaps, is the proper point to underscore our relationship with the Inspector General (IG). Simply put, we are not an IG; we do not function as one; and we do not do their staff work. We do not, as a matter of course, coordinate all our proposals through the IG. If, however, our workup of a topic leads to an area where IG involvement is appropriate, then we must coordinate our efforts with them. For example, fraud, waste, and abuse are currently high-interest areas in the Federal Government. Should an example of fraud surface during a proposal process, then we would be remiss if we did not act to bring it to the attention of the IG. In fact, this has never happened; but if it did, we would certainly make sure that the action was fully justified and that the organization being evaluated was fully aware of the situation.

(U) Once an Evaluation Proposal is approved -- and depending on the nature of the topic, we may go all the way to the Director with a Decision Memo -- the implementation process begins. First, a Team Chief is assigned to the evaluation. This may be the same person who developed the proposal, but that is not always necessarily the case. It is entirely possible, for example, that one Action Officer would do the proposal and another perform the evaluation itself. The Team Chief, together with the management and technical experts already identified, begins the data collection, reduction, and analysis process. Whatever format this takes -- questionaires, statistics, interviews, etc. -- the methodology is followed to end in a draft report. The draft report is coordinated first with the team members, then through Q2, and finally is distributed to appropriate elements Agency-wide for review and comment.

(U) The IPE Team collates all external inputs and incorporates them into the final report. It is important to note that the report will make every effort to present all points of view. Of course, there may be occasions when some opinions must be abridged or omitted from the body of the report. In these cases, they will be appended to the background material forwarded with the final report for management consideration. The report usually does not stand alone; rather, a briefing accompanies it. Yet, even then the process is not complete. Each report leads to conclusions and recommendations, and the task falls to the Team Chief to monitor the implementation of the approved recommendations until each has been resolved. In this way, we try to ensure that an IPE is not a "one-shot" action, but a continuing process that leads to a system improvement.

(U) Suppose that you would like a problem evaluated, but you do not want a detailed, formal evaluation. Or perhaps, you would like to conduct your own internal evaluation, but do not know exactly how to start. Q2, as the NSA/CSS central authority for coordinating Agency performance evaluation activities and conducting performance evaluations, will be happy to assist you on either a formal or informal basis. We have a staff with a variety of backgrounds and experience in SIGINT and COMSEC operations as well as engineering and operations research skills. We are prepared to offer assistance in any way that will improve efficiency, economy, and effectiveness.

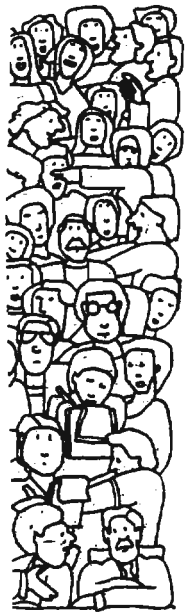
(U) To recap, IPE's are a management tool that can be applied to any aspect of internal Agency operations. IPE topics can be suggested by anyone and they all follow a structured path through the evaluation and implementation processes. Each step of the process is so designed to preserve the integrity of the evaluation and to make of it an exercise in participative management. The principles of coordination and collaboration work to ensure that the Performance Evaluation Directorate is not perceived as an IG. The entire process is usually lengthy and always methodical, the better to guarantee that the results will contribute in a positive manner to the effectiveness, economy, and efficiency of the US SIGINT System.

~~(C)~~ So what do the Afghanistan Crisis, the Russian Language Acquisition Program, and NSA's Emergency Destruction Capability have in common? Like the topics listed at the start of this article, they have reaped the benefits of an objective evaluation process, the IPE.

(U) If you have a problem that you think would benefit from a formal or informal evaluation, contact Q2. We will be happy to assist you.

DOCID: 4009841

A Wail, A Complaint, and a Melange (U)



by Samuel S. Snyder, T54, et al

Editor, CRYPTOLOG:

Herewith a couple of poetic contributions by former associate, the late Captain William M. V. Hoffman. Bill was assigned to my section, "B-II-b-4-a" sometime in 1942, when we were first becoming successful in our attack on the Japanese Military Attache system. Bill was a former Episcopal priest who was distantly related to Franklin D. Roosevelt, and liked to tell of having breakfast at the White House with FDR. He had an uncanny knack with words but somehow had a terrible time making good guesses when we assigned him to overlap work. His frustrations come through in his "Wail of a Cryptanalyst." We made good use of his talents later when we assigned him to write training materials for new people coming on the job. In his "Arlington Melange" you might have fun trying to identify individuals he had in mind on each line. (Example: the "genius dashing about like a flea on a binge" is Frank Lewis!)

The other poem about computers (*by* a computer!) was started by me on a plane late at night, while flying home from a computer conference in Detroit, in 1951. By the time we landed, I had about five or six verses; the rest were composed the next day in the office, including contributions by Red Lathroum, John Rixse, and Dotty Blum.

Samuel S. Snyder, T542

ARLINGTON MELANGE (U)

by William M. V. Hoffman

There are M.A.'s from Harvard and Princeton,
Musicians and doctors of law;
    There are all kinds of teachers,
    And even some preachers,
and pale-faced Ph. D.'s by the score.

There are anthropological experts,
And Swedes who are silent and bland;
    And one of our bosses
    Is a colonel of horses
Who longs for an active command.

We have graduates straight from Smith College
Who are brilliant and friendly and fair;
    We have mathematicians
    And bright statisticians,
Who can calculate odds to a hair.

There's a plentiful sprinkling of screwballs,
And a few on the lunatic fringe;
    While temperament flashes
    And genius dashes
About like a flea on a binge.

We're a weird and outlandish collection;
We're a cockeyed and comical crew;
    But, come Nazis or Japs,
    You'll find we're the chaps
Who will see that the message gets through!

DOCID: 4009841

THE WAIL OF A CRYPTANALYST (U)

by W. M. V. Hoffman

There are moments when the world looks bright
and rosy,
When the messages are tailing as they should,
When each fancy little letter
Makes the columns come out better,
And the rows could act no better
if they would.

Then the heart of the cryptanalyst is merry,
And he chortles as he sets the traffic down;
And he thinks the enemy chaps
Are such simple-minded saps,
And the man who makes their ciphers is a clown.

But, alas! there comes a day of horrid failure;
Our cryptanalyst is miserable and blue;
And the nasty little letters
Thumb their noses at their betters
And make gibberish no matter what you do.

You can stand them on their heads
and read them backwards,
You can shift them left to right
and to and fro,
You can calculate and mutter
Till your brain becomes like butter,
But no matter what you try it doesn't go.

Then you curse the day when ciphers
were invented,
And you kick yourself around for being dumb;
And the guy who once invented
Such a code is a demented
Low-down, slinky, lousy, dirty, rotten bum!

P.L. 86-36

COMPUTER'S LAMENT (U)

by [redacted] and Friends*

(March 1951)

My business is computing
With great efficiency,
Though what it's for is more and more
A mystery to me.

My heart beats are electrons,
My mem'ry works quite well;
But where I go or what I know--
That, only man can tell.

My rate's a megacycle,
My cost - a megabuck;
But if I make just one mistake,
My friend, you're out of luck.

My names are always silly,
With "Ack" they often rhyme,
Be dignified, I've got my pride,
Let's joke some other time.

My mem'ry's like an elephant's,
Each number sticks like glue.
I don't regret what I forget--
I'm filled with something new.

When coders misinterpret
My numbers, new and old--
It's all the same, I get the blame
For doing what I'm told.

The people all around me
That come and go each day--
Sometimes they fuss, sometimes they cuss,
Sometimes they sit and pray.

The operator ponders,
The coder strokes his chin;
But Oh! the loud annoying crowd:
They stand around and grin.

My ills are well attended,
My docs are maintenance men;
Oscilloscopes and lots of hopes
Can fix me up again.

My access time can vary,
Whatever they decide;
But fast or slow, they still say "No!"
They're never satisfied.

Sometimes I am disgusted--
Sometimes there is no joy;
For I can see that I will be
A million dollar toy.

Sometimes I get quite weary
While pulsing through the night;
But if I err, just hear them swear!
They never treat me right.

They don't appreciate me
In spite of all they say;
Why, I do more than fifty score,
And, brother, that ain't hay!

So feed me lots of power,
Adjust my settings right;
And if we try, then you and I
Can help to win this fight!

* Dorothy Blum, Leo Lathroum, John Rixse

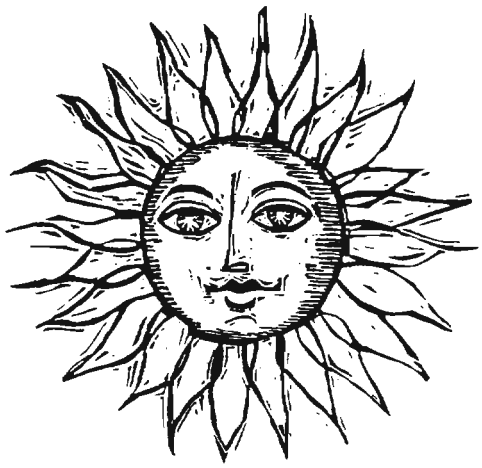
KRYPTOS:

A New Society (U)

by [redacted]

P.L. 86-36

CA Intern,
KRYPTOS Society
Historian



(U) The KRYPTOS Society, chartered in October 1981, is a new organization whose purpose is to promote cryptanalytic excellence and to provide a focal point for Agency cryptanalysts. On 9 December 1981, at the Society's inaugural meeting, Miss Ann Caracristi, Deputy Director NSA, spoke on 'Cryptanalysis: the Key'. Her address was followed by comments by [redacted] on the steps taken by the Cryptanalysis Career Panel, of which he is the chairman, toward 'restoring the luster to cryptanalysis'. Attendance at the meeting was outstanding. In the interest of accurately recording the comments of both speakers, this summary has been prepared from notes taken at the time.

EO 1.4.(c)
P.L. 86-36

~~(C)~~ Miss Caracristi observed that without cryptanalysis there would be no National Security Agency, yet there existed no CA organization until 25 years after the founding of the Agency's first professional society, the CMI. She then addressed the problem of identifying Agency cryptanalysts. Everyone, it seems, knows what a cryptanalyst does but no one knows just what one is. The mathematicians in the back rooms of A5 and G6, are they cryptanalysts? What about the signals people in A5 and B3? And the linguists of G6, A2, and A3? They all perform cryptanalytic functions; aren't they cryptanalysts?

~~(SC)~~ Whatever your definition, several names come to mind as eminent cryptanalysts: William Friedman, Frank Raven, [redacted], Peter Jenks, Bill Lutwiniak, [redacted], Phil Dibben, Jim Thompson, [redacted] These and many others have, through their successes, saved countless lives with the information they provided -- breaking ENIGMA and PURPLE in World War II, providing tactical decrypts during the Korean Conflict (1950-52), and maintaining successful efforts against the Viet Cong. [redacted]

P.L. 86-36

~~(S-CCO)~~ But with success, Miss Caracristi pointed out, problems arise. Exploitation leads to production and we find ourselves making less of an investment in new problems. The number of cryptanalysts (including crypto-math) has shrunk [redacted] Success also has an impact on other fields. It creates work for the linguist, the engineer, and data systems person, and the collector. And, as a [redacted] Miss Caracristi put it, "The alarm bells are ringing."

~~(S-CCO)~~ The KRYPTOS Society can help the CA work force by

[redacted]

- providing support to the CA Career Panel,
- identifying new talent for the CA work force,

DOCID: 4009841

- providing mentors from its membership for new cryptanalysts,
- keeping up with events in the outside world and in the academic community, and
- advising the Director on the health of the profession.

~~(FOUO)~~ Miss Caracristi concluded her remarks with the following words of guidance:

> We should look to the immediate future as an opportunity to recapture CA manpower through recruitment. We must bring new cryptanalysts on board and develop their CA abilities, teaching them to appreciate the excitement and the challenge of tackling hard problems, to learn to enjoy small successes and to follow their intuitions when the trail gets hot. By doing this, we can build for NSA's continued success.

P.L. 86-36

(U) When [redacted] became chairman of the Cryptanalysis Career Panel two years ago, his goal was to restore the luster to cryptanalysis to counter losses the field had suffered. Toward this goal, he set three objectives:

- ☆ to provide a place for middle and senior cryptanalysts to seek advice and to learn of potential in other organizations; an informal, nonthreatening resource for post-professional career development,
- ☆ to establish a professional society for cryptanalysts, and
- ☆ to establish a technical excellence award for the field of CA.

(U) The first objective was a service that could be provided by the Executive of the Cryptanalysis Career Panel, since the Panel's responsibilities included much more than training interns. Over a period of time, the position of Executive of the Panel had been downgraded from its initial grade of GG-15 or GG-16. Elements of 'M' were proposing that the Executive should be a grade GG-12. Mr. [redacted] was successful in getting them to upgrade the position to a GG-15 once again, a grade level more appropriate to the broader duties of the office. At this time, [redacted] became the Executive, eventually to be succeeded by [redacted] then talked with office chiefs and obtained their endorsement for regular visits by the Executive to CA offices to see what was being done and what was not.

(U) One deficiency noted by the CA Panel was the lack of a professional society for the central profession of NSA. They weren't sure of the level of interest in such an organization, but knew of the tremendous popularity of CA-305, an annual seminar series. To determine the amount of support such a society might expect, questionnaires were sent out. Encouraged by a good response, the Panel formed a committee to organize the society that eventually received the approval of the Director and of the Council of Learned Organizations.

(U) In establishing an award for technical excellence in the field of cryptanalysis, the Panel wanted to recognize steps taken along the path to success. Frequently those at the end of the road are recognized while early contributions go unrewarded. Additionally, recognition often depends on the value of the output. The Panel wanted to recognize 'coups of the mind' without regard to whether or not vital decrypts were produced. The award was envisioned as a pin with the possibility of a plaque for two-time winners. Nominations would be accepted as events occurred. The Panel would act semi-annually to select recipients, presenting perhaps ten awards per year.

restoring the luster to cryptanalysis

(U) The award was originally conceived by [redacted] as an Agency award. When he took the proposal to [redacted] then DDM, Mr. [redacted] suggested that to establish it as an Agency award would take a long time and a great deal oof red tape. Offering it as a professional society award, however, would be relatively easy. With this recommendation, the award was put on a back burner until a professional organization could be formed. Eventually, DDM became DDA and [redacted] was replaced by [redacted] When [redacted] made a point of acquainting [redacted] with the proposal, he was advised that it shouldn't be a professional award but an Agency award. Having waited this long, [redacted] resisted changing the proposal again. With the establishment of the society well on its way, Mr. [redacted] made an appointment to discuss the new society, the award, and the objectives of the Panel with Director Inman and Deputy Director Caracristi. Admiral Inman, on hearing of the award proposal, expressed a strong opinion that it should be an Agency award. Strong opinions at that level are always considered. When the M34 Awards Division was approached with the award proposal, they recommended that it should be a professional society award, not an Agency award! It was then that [redacted] did a little name-dropping, apparently convincing them that an Agency award was entirely appropriate.

(U) Establishment of the award was then hung up in the legal office for over three months. The Panel, meanwhile, to decide on a name for the award, went to Q23 with their original suggestion, 'Excellence in Cryptanalysis'. But Q23 didn't want any reference to CA in the title. They wanted to avoid identifying our best cryptanalysts to the outside world and expressed concern that the design of the pin might be too revealing as well. And in addition to the legal office and Q23, the offices of Protocol and Heraldry had become involved. [redacted] had been correct in his appraisal of the situation.

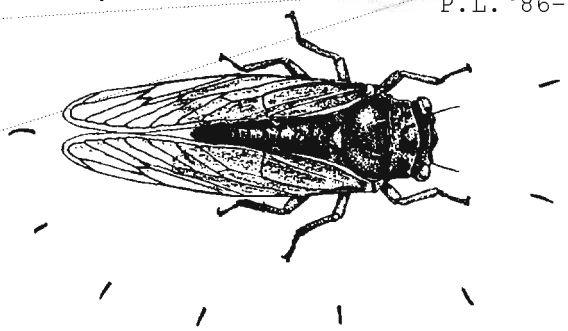
(U) [redacted] tasked by the Panel with choosing a design and name for the award, suggested the 'Gold Bug Award' after Edgar Allen Poe's story involving the breaking of a cipher. This suggestion solved both the name and design problems -- the name did not refer to cryptanalysis and suggested obvious design ideas. The award proposal is now in the 'M' office that provides documentation on the administration of such awards. [redacted] expects the award to make its appearance sometime in 1982. The Panel proposed that nominations go to the CA Career Panel, who would decide on the recipients. In closing, [redacted] offered his favorite maxim for NSA cryptanalysts:

"The impossible we do immediately,
the miraculous takes a little longer."

(U) The KRYPTOS Society welcomes new members. For information, please contact any of the following people:

President	[redacted]
President-Elect	
Treasurer	
Secretary	
Members-at-Large	
Program Committee	
Membership Committee	
CA Panel Exec	

P.L. 86-36



DOCID: 4009841

Correspondence

From: tfh at CARONA
To: cryptolg at BAR1C05

Wayne,

(U) I received the message sent to Unix users back in October and I am taking this opportunity to express my feelings on the subject of communications of the users on these systems.

~~(FOUO)~~ Having worked in the [redacted] TSS area for several years, I have had the pleasure of working with a number of people, who use the Unix Systems. There is truly a wide range of people using the systems today and an even wider range of tasks being performed. No one has the time or the need to use everything on the system; each individual specializes in some particular area which fits his or her own personal needs. Each day someone discovers a new method of improving that area. The users manuals help with the basics, but it would be impossible to document all the routines and working aids that people have perfected and used on the systems.

~~(FOUO)~~ In the past, I have attended several meetings of UNIX-BASED TERMINAL SYSTEMS USERS GROUP. The purpose of these meetings is to give users information on developement of the Unix systems and to stimulate interest in areas which users are having problems. The trouble with the meetings now, I believe, is that they are aimed at the Systems programmer level rather than at the user level. A majority of people who attend these meetings are Systems people themselves or deal more with the programming applications of the system. The material presented is on a level that is hard to comprehend by those who are not programmers themselves.

~~(FOUO)~~ You stated in your message "I only ask that the material be sufficiently readable so that people who don't work in your special skill area can read it through and come away with some appreciation of how things are going in your territory." I feel that everyone working on the Unix systems has some territory in which he has extended use, where he might share his specialty with others, who may not be as versed as he, in that particular area.

~~(FOUO)~~ Perhaps, then, we UNIX users should start talking to each other and start sharing our ideas. Indeed, Cryptolog itself might serve as a useful vehicle. We have the resources available to us already, so "Why re-invent the wheel?"

[redacted]
T1512

P.L. 86-36

SOLUTION TO NSA-CROSTIC No. 37 (U)

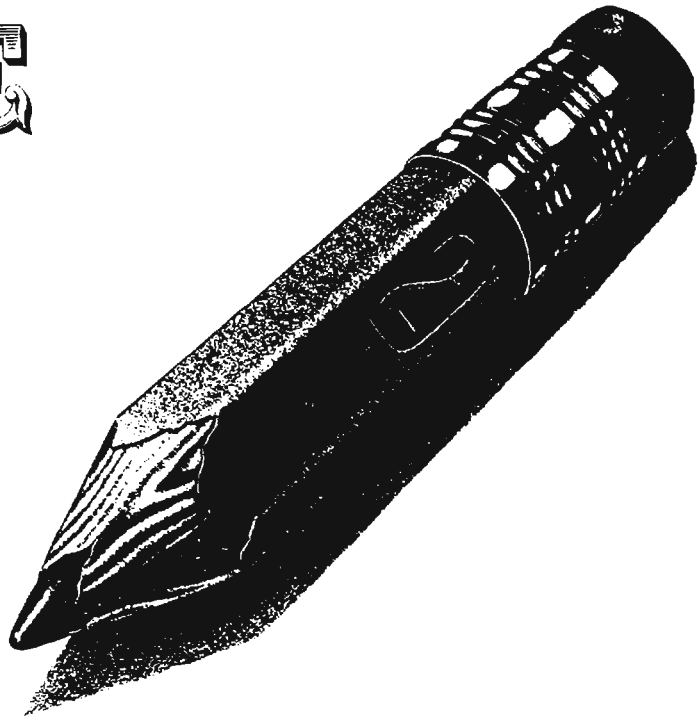
"Language in the News," [redacted]
[redacted] CRYPTOLOG, September 1974

"The Wisconsin Native American Languages Project is an undertaking funded by the Great Lakes Inter-Tribal Council, to involve speakers of Wisconsin Indian languages (Ojibwa, Potawatomi, Menomini, and Odeida) in the application of linguistics to the analysis, study, and teaching of [these] native languages."

(U) RYE is scheduled to be phased out by mid 1983. Efforts are under way to get in touch with all users. If you are an active user and have not been contacted by now, please advise T1533, extension 4030s.

DOCID: 4009841

GOLDEN OLDIE



Simplicity in Color

by C. Garofalo

(from COMMAND, October 1971)

The conduct of crypto TA studies involves the requirement to differentiate between qualitative levels or categories, and the use of a simple color scheme facilitates such differentiations. Any color scheme to be used in an analytic effort of large volume must be:

- simple in nature,
- skillfully chosen, and
- systematically applied.

An analysis of the various colors available is made to determine which are practical and most suitable for the task. My experience has demonstrated that six different colors are most practical. These are black, green, red, blue, purple, and brown.

- Black - carbon (number 2) pencil has been found to be the obvious choice for normal usage. It is of a medium degree of hardness and density, suitable for both erasure* and longevity properties.
- Green - is the weakest, that is, of lightest density. All of the other colors under consideration superimpose on green quite readily.

* For black erasures, a medium hard rubber erasure is adequate. For color erasures, best results are obtained with a typewriter eraser.

- Red and Blue - are of equal boldness; either can be easily superimposed on both black and green.

- Purple - a bolder color which can also be produced by a superimposition of red on blue or blue on red.

- Brown - is considered to be the boldest of all colors as well as the most exclusive and conclusive.

Colors manufactured by different commercial firms vary drastically in hardness, density, and coloration; it is desirable therefore that having started with a particular brand to continue with that brand and not intermix brands to ensure that distinctiveness and clarity are maintained.

A color ladder may be displayed graphically as follows:

COLOR	LEVEL (Qualitative)
BROWN	5
PURPLE	4
BLUE	3
RED	2
BLACK	1
GREEN	0

Another way to express the levels of the color ladder is by these definitions:

- BROWN - The ultimate in degree of trueness, not to be questioned. May also represent captured, compromised information or its equivalent.

- PURPLE - High in degree of reliability; may be used as a substitute or companion for brown where special conditions of clarity or distinction are vital to the problem. Primarily useful as a final ordered and oriented intermediate enjoying the same general stature as brown.

- BLUE - A relative base value having a significant bearing on the state of recovery.

- RED - A base of lesser value or no relativeness (completely arbitrary), a first step necessary in any endeavor.

- BLACK - To record or log information as it appears in its earliest or original form.

- GREEN - An envious color which is reserved completely for suspected garbles, projected or expected but unobserved values (not proven but highly suspected as being correct). Used to alter a meaning or information without obliterating the original (black) form.

Once a color scheme is established for a given problem, maintenance of color discipline is mandatory in order to achieve uninterrupted and unambiguous continuity. Discipline is also of great benefit to management in that it ensures that redistribution of analytic personnel can be effected with minimum disruption to the overall effort.

Postscript:

Colors:

Green - symbolized hope to the ancient Egyptians;

- in the Middle Ages was supposed to be good for the eyes;

- to the Mohammedan, a sacred color;

- in modern times has come to signify envy.

Purple - to the Tyrians and Romans, a purple robe or band of purple signified authority; became a symbol of majesty to the Romans.

DOCID: 4009841

Human Factors Corner

by [redacted]

P.L. 86-36

☐ Some Advice to Users of **UN**friendly Systems (U)

☐ ...But What Do I Do With My Papers? (U)

I have received a number of responses to my article about "Unfriendly Systems" in the November 1981 issue of CRYPTOLOG. Several people have called to express their strong agreement with some of the points in the article, and to tell me some of their problems with the systems they are using. My impression is that, in some cases, the problems these users are reporting are of a serious and long-standing nature. It seems clear that, for several large classes of NSA computer users in key applications areas, problems with poorly-designed interactive software may be causing real and significant losses in personnel dollars and vital productivity.

For example, in one area which I won't name, users were at one time instructed by their supervisors NOT to make use of a major set of information support files designed specifically for their work, by an in-house computer support element in their own organization. Why? Because it was so difficult to get logged on, to frame a request, and to complete viewing responses without making an error. A user error caused the system to be locked up, preventing all users from getting at other things they needed until operations could be called to get the files closed and the user logged out. The procedure for getting into this system is still so complicated and unfriendly, and its response time is so slow once a user is into it, that many people avoid using it on line, and instead use hard-copy printouts. You may be wondering what terrible programming language this system could be written in to cause it to be so inadequate? The trouble lies not in the software system, but in the design philosophy of those who developed and implemented the user interface. The programming language is an excellent one, and provides rich and extensive facilities for composing convenient screen displays, and receiving user responses. No, we can't blame the computer or the programming language! Let's lay the blame where it belongs: on the designers of the user interface, whose philosophy goes something like this:

> "If those guys can't use our system, it's because they're too dumb! There's nothing wrong with OUR system! Anybody who comes around here complaining about OUR system is looking for a fight!"

What can you do about a situation like this? Those who have spoken to me about problems of this kind seem to have a defeated, fatalistic attitude. Some are quite bitter and angry. They have tried to tell their management about the problem, and the managers have tried to get something done about it, apparently with little success. I'd like to suggest an approach that may get you a little further: Put a notebook or lined pad near each terminal. Call it the "trouble log", "gripe log", or what have you. Tell everyone who uses the terminals to note every case of a problem with the system that he or she experiences. Note the name or initials of the user (so that you can find out more about the problem if need be), the date, time in hours and minutes, and as much detail as possible about the events that occurred. Note what was typed in or entered, what the response was, how long it took for the system to respond, and any other facts or events or times that show loss of user time due to deficiencies and unfriendliness in the system. Don't forget to note cases where the keyboard layout or design of commands needlessly leads users to make costly errors (for instance, when a user is very likely to destroy hours of work because the ERASE key is right next to the ENTER key, or a misleadingly-labeled command or field repeatedly leads users to make mistakes that

DOCID: 4009841

waste a lot of time over and over again, day after day, or an unhelpful response screen leaves users "up a tree" so they waste time trying to guess what went wrong).

After you have collected about a week to a month's worth of the trouble logs on all your terminals, study them and make a summary of what you have found. You can analyze the raw data in several useful ways. For instance, you will probably see certain recurrent problems that you suspected already, and which together account for the major proportion of your personnel dollars wasted at the terminal by users trying to use the system. You can write up a little paragraph on each, describing the problems that cause the wasted time, stating in man-hours and dollars (man-hours times your element's average hourly wage) the extent of the wasted resources, and recommending a change to improve the situation. If you can get your boss, and better yet, your bosses' boss, to do the same thing, and combine all the summaries into one memo to your machine support organization or whoever is likely to respond constructively, your memo will have even more impact. Keep up the trouble logs, keep on making monthly reports, and keep up the pressure. This course of action, if followed in a constructive way (not just angry griping), and backed up with good solid data on numbers of hours and dollars lost, should certainly get you a lot further toward a solution of the problems. It will also provide the machine-support management with a clearer idea of WHAT is wrong and some immediate ways in which they can improve the system.

You may well ask, what about the all-too-frequent cases where potential users of a facility or subsystem have simply given up, after many attempts, and now no longer use it at all? Or the case mentioned above, where a system is so punitive and unfriendly that supervisors have positively forbidden users to employ it, because it constitutes a menace to overall productivity? I suggest that you ask some of your potential users of such systems to keep a record of all the instances when they WOULD HAVE LIKED to use it, or to get at the information it contains. Try to get an estimate of the time and personnel dollars you would save, and the increase in quality of your product, if this aid were available and user-friendly.

These are just a few suggestions of ways you can "fight city hall", and improve matters for all of us, if you are a user of an unfriendly system.

...BUT WHAT DO I DO WITH MY PAPERS?

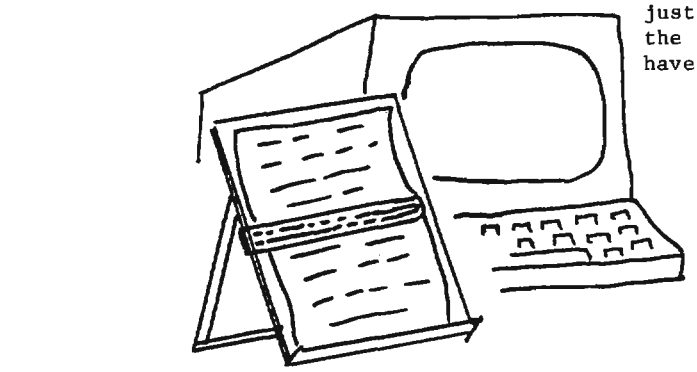
Reprinted from Human Factors Letter 4-80, published by the CISI Human Factors SIG.

Many of us who use CRT's may not be entirely happy with the response time or details of the user interface on the system. Even for those of us who are satisfied with these aspects of the system we use, however, there remains a stubborn problem that needs to be solved somehow. That is the matter of where to put papers, books, and worst of all, machine listings to which we must refer while we key things into the terminal. Various holders and racks are available, to sit on the desk or table and hold pages of copy, often with a horizontal bar or marker that can be moved or slid up and down to keep the place at a given line. These are adapted from aids in use by typists before CRTs came along. They might solve the problem, at least for page copy, if not for books or computer listings. In fact, I have rarely, if ever, seen anyone other than a typist or clerk using one of these devices in conjunction with CRT data entry, though they look as if they might be helpful. Elsewhere in this magazine, I have included some drawings of these gadgets, as advertised in a recent INMAC catalog of computer accessories.

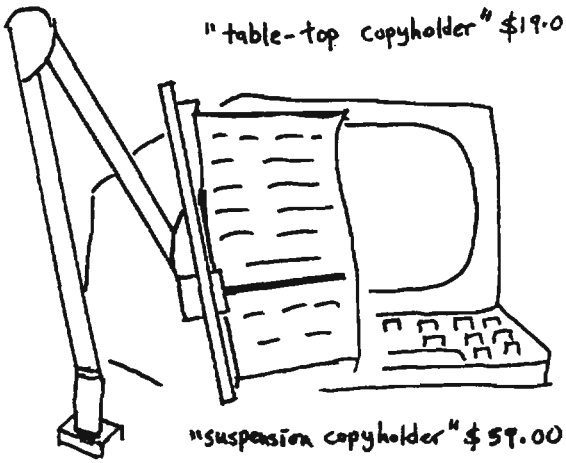
Users of CRTs are much more likely to prop folded bits of paper from which they must copy or extract information above the bank of keys on the keyboard, or against the terminal beneath the screen. Depending on the shape and size of the keyboard and the height of the screen above it, there is frequently some space to hold a small or folded sheet of paper there. Listings on size-12 paper, books, and thick documents must be laid open on the desk or table to the right or left (depending on which side you would prefer to have a crick in your neck that day). You crane your head to one side or the other, over your hands and arms which are busy typing at the keyboard, and reach across awkwardly to turn pages. If you are nearsighted, your troubles are exacerbated, especially with computer listings. These vast, cumbersome blocks of fanfold paper seem to extend for miles away from your eyes, and the line you want to see is all too often way up there at the very top. If you fold the listing over on itself, it is very likely to tear, or else to become dog-eared and dishevveled so that it never folds quite right thereafter. I have at times resorted to wrapping the listing around the edge of my table, pinching it against the table with my tummy, and squashing the top down so it sits in front of me just below the keyboard. Whatever else happens, sooner or later part or all of the fanfold falls onto the floor, unravelling itself to create an exasperating mess.

For users who aren't fortunate enough to have a terminal stand or desk wide enough or uncluttered enough to accommodate listings or papers beside the CRT, the lap or knees are the only solution. And, heaven help the user who needs to refer to several hardcopy documents at once while he is using the terminal! I have often seen users who must consult printed working aids and dictionaries trying to cope with five- and six-deep piles of books and documents in layers on their laps, the table, etc. while they paw back and forth from one to another trying to get the information they need to complete a transcript or report on the CRT.

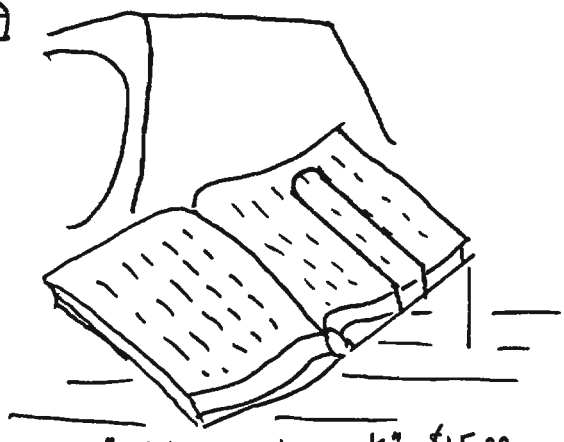
Perhaps, some day, a truly useful, comfortable, and efficient file structure will be available on line for many of the most frequently-consulted documents. There are now a few experimental systems that provide users with a "spatial" organization of different files, like the physical arrangement on the top of a very large desk or table. Such a system tries to help the user remember where he "put away" a given document when he discarded it temporarily to consult another, which documents or files he is working with, and where he is in each one. (A good example is the DATALAND system developed by Nicholas Negroponte and others at MIT.) Unfortunately, these systems aren't available to most of us just yet. In the meantime, until the state of the art catches up with this problem, we will have to live with it!



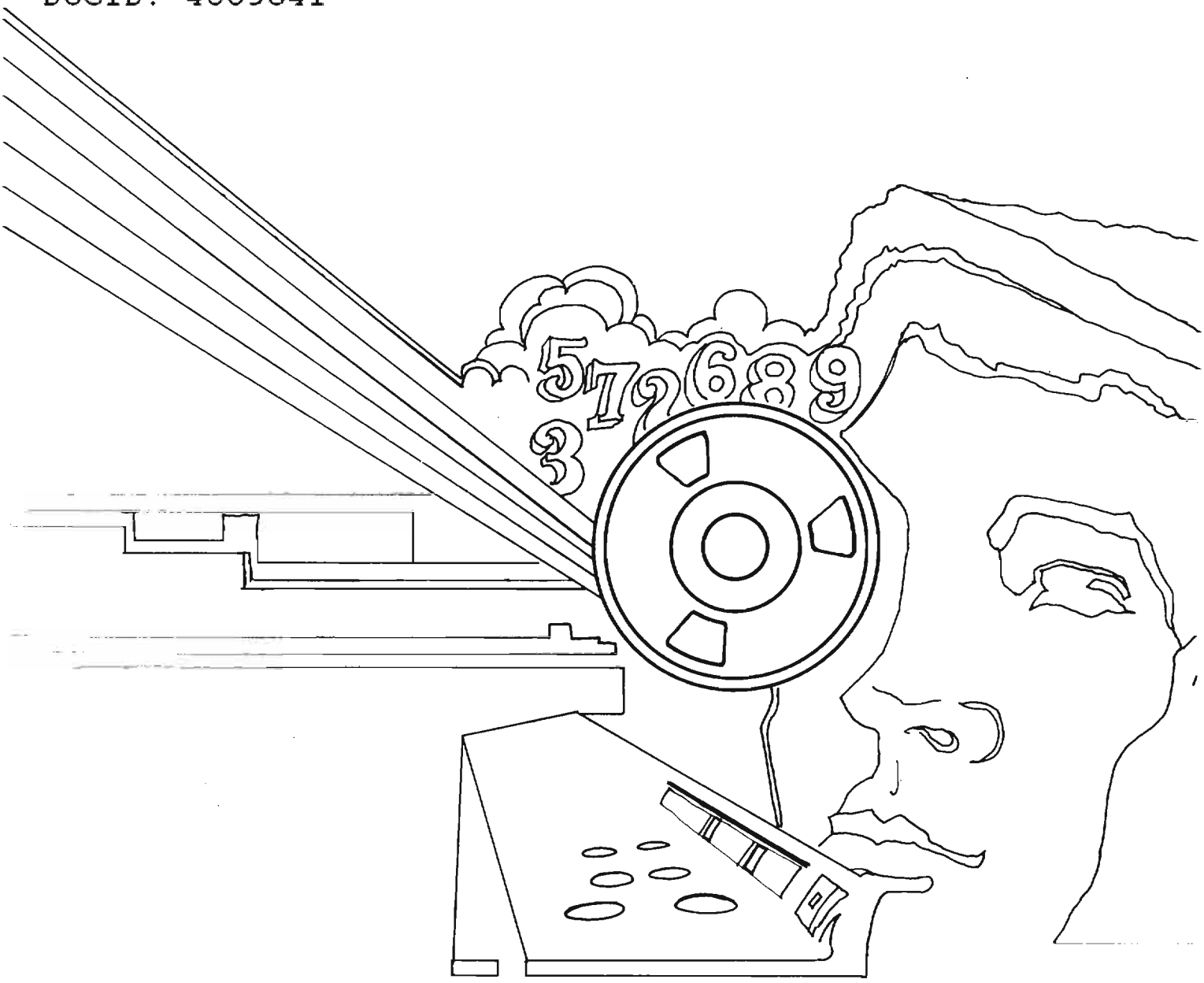
"table-top copyholder" $19.00



"suspension copyholder" $59.00



"printout reader rack" $15.00


5 7 2 6 8 9
3

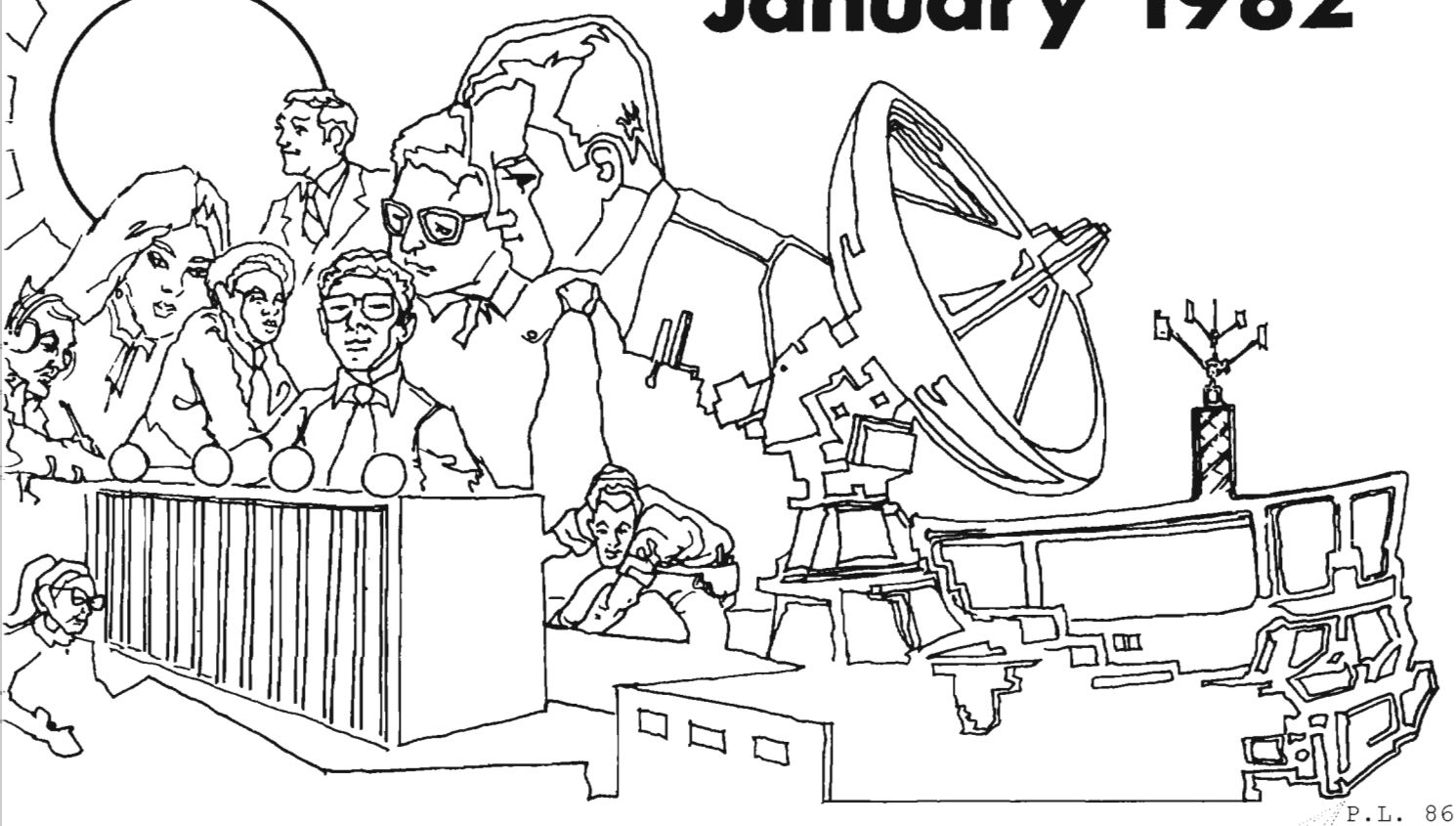
DOCID: 4019690

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

January 1982



P.L. 86-36

HF - THE REBIRTH (U)..... [redacted] 1
VIDEO ENCRYPTION: A REPORT FROM EASCON 81 (U)... [redacted] 4
DATA FIELD NAMING/CODING CONVENTIONS AT NSA (U). [redacted] 5
NSA-CROSTIC NO. 37 (U).....David H. Williams.....14
THE LITERARY BENDS (U).....Albert I. Murphy.....16
ALL THE ALLIGATORS AREN'T ON SPORT SHIRTS.....21
HUMAN FACTORS CORNER (U)..... [redacted] 24
LETTERS (U).....28

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSS 123-2~~
~~REVIEW ON 10 Jan 2012~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019690

~~FOR OFFICIAL USE ONLY~~

CRYPTOLOG

Published by P1, Techniques and Standards,
for the Personnel of Operations

VOL. IX, No. 1 JANUARY 1982

PUBLISHER [redacted]

BOARD OF EDITORS

Editor-in-Chief. [redacted] (7119/8322s)
Production..... [redacted] (3369s)
Collection..... [redacted] (8555s)
Cryptanalysis..... [redacted] (5311s)
Cryptolinguistics..... [redacted] (5981s)
Information Science.. [redacted] (3034s)
Language..... [redacted] (8161s)
Machine Support. [redacted] (5084s)
Mathematics..... [redacted] (8518s)
Puzzles.....David H. Williams (1103s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Don Taurone (3573s)

For individual subscriptions
send
name and organizational designator

to: CRYPTOLOG, P1
or call [redacted] 3369s

To submit articles or letters
via PLATFORM, address to

cryptolg at barlcØ5
(note: no 'O' in 'log')

EDITORIAL

One more Agency magazine has ceased to be. The October-November 1981 issue of The Research and Engineering Review (RER 9-81) was its final issue. It seems appropriate to quote (in part) from the last editorial.

"The RER was a fine idea. A need existed, and the Review filled that need well. But the declining availability of technical articles has made continuation virtually impossible.

"This problem has been growing for some time, not only for the RER but also for other NSA technical journals. Publication on a monthly basis has become increasingly difficult. The people we look to for good material are the busiest people, and we cannot question their priorities.

"Recent interviews and a sampling of readers' opinions provided no reason to believe that the future would be any brighter, and the responses showed a dwindling level of interest and support.

"We continue to encourage all of you to write for publication in NSA journals. Share your knowledge. Publicize your accomplishments."

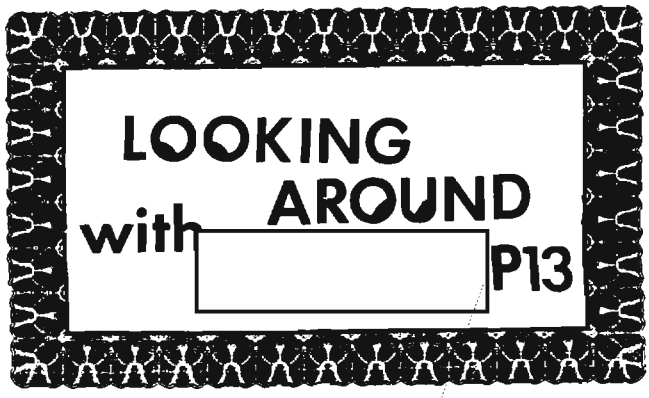
We enjoyed the RER. We are sorry to see it go.

Note:
The November, 1981 issue should be numbered Volume VIII, Number 11.

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019690



◊ HF-The Rebirth (U)

◊ Video Encryption:

a report from EASCON 81 (U)

P.L. 86-36

The Tidewater Chapter of AFCEA at Langley AFB, Virginia, held a one day seminar on the increasing use of HF and committment of the U.S. military services to new HF systems. A (U) number of technical talks were given on:

- the "rebirth" of HF,
- HF receiver technology,
- antenna developments,
- HF operations in the Indian Ocean,
- automatic connection of HF circuits, and
- the rediscovery of HF for C^2 (Command-Control).

A panel of two generals and a Navy Captain then commented on the presentations.

(U) There is high level interest in HF by OSD and JCS, and new technology, but the military services have lost their HF skills. The communications users, having accustomed themselves to the lavish services that satellites can provide, do not like to conduct their operations with narrowband HF message services. The equipment is better, but is expensive, and there is trouble getting the money. In spite of these problems, HF is seen as vital to future combat operations, because the services cannot be sure that satellite circuits will be available.

Highlights of Discussions (U)

(U) ITT is developing a frequency hopping HF system called "adaptive HF" which is designed for operation during and after a nuclear war. It will communicate on skywave links up to 100 MHz after a nuclear event. The pulses are noise coded but the demodulation can overcome perturbations to the waveform caused by nuclear effects, and apparently does not require correlating filters at the receiver. This system will do automatic real time sounding of the ionosphere, can change its routing, and has low probability of exploitation (LPE). It is designed to provide "enduring C^3" so that transattack and postattack negotiations, as well as combat C^2, can be carried on despite outages of other communications systems.

(U) RACAL has developed a digitally controlled HF receiver, RA 6790, which was designed to replace the R390. The receiver contains a microprocessor which controls all the functions of the receiver, including self-test. Special AGC circuits give 0 dB output variation for 120 dB input variation. The synthesizer is on one PC board and tunes 1 Hz increments across the receiver range. A wideband input circuit is used which keeps intermodulation products to a low level. A mathematical formulation was given of the distribution of weak and strong signals over a 4 MHz band, derived empirically. A RACAL 2174 receiver with many of the RA 6790 features is

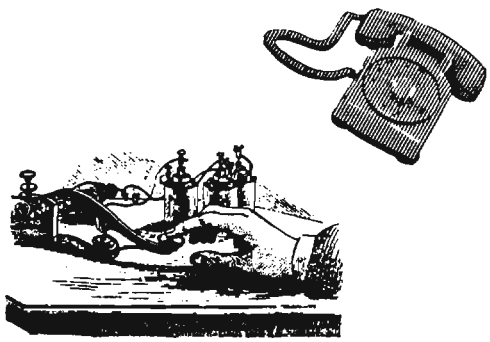
being adopted by the USAF.

(U) RSI has developed a portable microwave antenna for troposcatter or line of sight links, which can be assembled and erected by two men in 8 minutes. A demonstration was given. The antenna weighs 450 lb.

(U) BR Communications chirpsounders and spectrum analyzers are being used by the naval task force in the Indian Ocean to improve HF circuits to distant shore stations. Flag officers aboard the Mt. Whitney use a total of 29 HF circuits almost continually, relayed through Diego Garcia, Australia, Greece, and the Phillipines, even though the ship has satellite circuits. The Navy has had to redevelop its HF skills to operate these circuits, and channel sounders have enabled frequencies as high as 29 MHz to be used. Smallpipe HF exercises in which satellite circuits are turned off have exposed many problems, including long delays in delivering traffic.

(U) ROCKWELL has developed a system which will automatically set up an HF circuit to a mobile station, e.g. aircraft, and confirm the link in a few seconds, then terminate the circuit when the message is complete. Voice can be used after setup. They have also developed an HF 80 series of equipments for the military communications market.

(U) The Navy, having dropped HF communications about 10 years ago to switch to satellites, is now encountering problems in going back to HF. The experienced people are leaving or retiring, and the operators familiar with satellite circuits have to be retrained for HF. Special problems such as the "rusty bolt effect" have reoccurred and have to be solved again. Lengthy messages also overload HF circuits without conveying information quickly.



(U) Captain Gradel, USN, said, in a comment, that the Navy was having trouble getting money for HF, and the commanders who have gotten used to the benefits of wideband satellite circuits do not want to operate with only HF circuits.

(U) MGen Ray, USAF, commented that USAF was unwise in giving up HF, and JCS and DCA now want HF. RDF contingency plans are dependent on HF. USAF is ten years behind the Navy in use of chirpsounders.

(U) MGen Gray, USMC, commented that the Services had to retain their "institutional memory" of operational knowhow as personnel changed. HF communications were important to the USMC, which he thought was likely to be in combat in the 1980's. HF was used for short range ground wave as well as skywave communications. Combat conditions would require use of NBC (Nuclear-Biological-Chemical) gear, and HF equipment would have to be useable in that environment. Messages would have to be concise. Cost and weight of equipment was important, and only equipment actually in hand could be used.

(U) Other points learned from the discussions:

★ US communicators use CW Morse at times, and tune RTTY transmitters off assigned frequencies in order to overcome cochannel interference, which is severe.

★ In this CW mode, operators use "fist" recognition to set up their nets.

★ The military services will not give up their HF frequencies.

★ Third World countries will probably use HF whether they get frequency assignments from the ITU or not.

★ High bit rate systems, above 300 bps, are thought unreliable because of the prevalence of cochannel interference which degrades demodulation.

★ The military services will have to retrain operators for HF, and may maintain a minimal CW Morse capability despite higher automation.

★ Usage of the 20-30 MHz range, and use of "open" frequency channels on an opportunistic non-interference basis, is expected to grow.

(U) The reported "death" of HF has been greatly exaggerated. Its use has continued to grow even though the U.S. Services largely switched to satellites. Important high level traffic for U.S. military and diplomatic users will pass over HF in peace or war, complementing satellite circuits. The U.S. military "rebirth" of HF usage is taking place in a changed and more congested environment, with moderate technical improvements in equipment, but major training and adjustment problems must be solved.

Cryptologic Implications ~~(C)~~

[redacted]

EO 1.4.(c)
P.L. 86-36

highly secure. OAK Comunications has a changing video analog encryption in which the enciphered keys are sent in band with the signal. The encryptor is called ORION. The video security is "soft", the audio security is "hard" and the decoders will sell for about $2000. HBO, in circulating a new specification for quotations, found ten suppliers from CATV, Broadcast and "Military" willing to bid. COMTECH Communications Corporation has a system that will give "hard" audio encryption, possibly using DES, and "medium" video encryption. Their security is based on a proprietary integrated curcuit which keeps the encryption technique under their control. They can accomodate 60,000 subscribers with one PN sequence, and can rekey outstations at 20,000/minute. Individual subscribers can be turned off if desired.

~~(FOUO)~~ The speakers were extremely secretive about specific techniques. The remote keying scheme developed by NSA in the 1960's appears to be the basis for the systems, since the broadcaster can control all the outstations in case they do not pay their bills, or decoders are stolen. The fast rekeying, and the ability to select individual sets out of the net are significant. Audio encryption will be at least at DES level. Subscription over the satellite links will be numbered in thousands of ground stations. The systems will also provide video conference capability. Video quality must be of studio quality after decoding, for the pay TV customer. The DIGITEL CANADA technique, which uses digital encryption and analog transmission, with sampling at 14.3 MHz, may be the most novel and secure.

~~(FOUO)~~ The consequences of these TV encryption projects will be to put secure remote keying networks systems into the market at about $1000 or less per terminal.

EASCON 81: Video Encryption

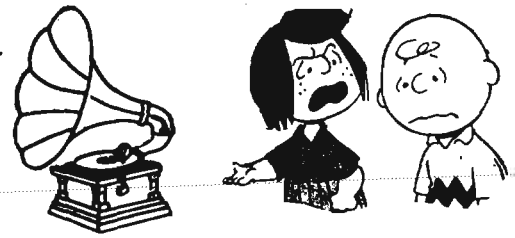
~~(C)~~ Encryption systems for satellite distribution of TV video and sound are advancing rapidly, especially in the command-control and remote rekeying of the decoders. The new HBO (Home Box Office) specification will use a key generator of DES security or better. DIGITEL CANADA has a prototype of a digital encryption system for high quality video which can be sent within a TV baseband. Their picture encryption has 10^{139} ways to encode. They can rekey subscribers at 2200/minute, and remotely terminate any unit. Both video and audio are

DOCID: 4019690

Good Grief, Charlie Brown, Not Again...! (U)

Data Field Naming/Coding Conventions at NSA (U)

CLASSIFICATION NOTICE:
Although each individual paragraph in this article is unclassified and handled as "For Official Use Only," the compilation of the information presented in its totality is classified ~~CONFIDENTIAL~~.



by [redacted] P13

P.L. 86-36

~~(FOUO)~~ This paper is intended to be a "primer" on some of the basics of data standards. My main purpose is to shed some light on the conventions that exist at the Agency concerning the naming and coding of data fields. Yes, there are conventions in this area of data processing, conventions which sadly are much more honored in the breach than in the observance. And yes, the Agency does have an official policy on the subject. It is pretty much buried in the pages of a USSID (414) and an NSA Reg (80-9), and ignorance about it is rife (I'm afraid) among the DDO analysts whom it chiefly affects. However, it is a policy that makes a lot of sense, especially as we view the Agency moving steadily into a world of proliferating data of all kinds -- files, programs, data elements, and data fields, and all of them sprouting wildly and threatening rapidly to grow out of control. Happily, we have some good things going for us. PLATFORM is one. A centralized DDO Data Element Dictionary/Directory is another. (It is still in the embryonic stage, but it offers hope for the future.) But before we can manage and exchange our data efficiently, we have to apply precision and consistency to the practice of identifying the data elements/fields making up those burgeoning data bases. Literally, we have to get a better handle on our data.

~~(FOUO)~~ What after all is the lowest common denominator, or lowest information level, of the vast data banks that fill our computers and memory devices? Undoubtedly, the Data Element itself, which can be broadly defined as the most basic unit of information. And since the Data Element (or rather its data items) is the entity that inhabits the fields comprising those miles of data banks, it seems reasonable for us to consider carefully how these data fields are to be addressed and referenced.

~~(FOUO)~~ A brief look at the origins of the data standardization program at NSA may help set the stage for this discussion. We will then look in some detail at the two chief ingredients that are mixed together to affect the process of naming and coding data fields, namely, the Data Element and its companion, the "Data Use Identifier."

Origins of the Data Standards Program (U)

(FOUO) The 23rd Anniversary of Pearl Harbor, December 7, 1964, was a landmark date for Department of Defense efforts to get underway with an organized effort in the field of data standards. On that date, DoD Directive 5000.11 established the "Department of Defense Data Elements and Data Codes Standardization Program." Several months later, on 12 March 1965, the Assistant Secretary of Defense (Comptroller) sent a memo to DoD components entitled "Data Elements and Data Codes Standardization Procedures." (This was the draft version of DoD Instruction 5000.12, which became the bible for the DoD program.)

~~(FOUO)~~ On 3 August 1965, further guidance was offered by DoD, especially concerning criteria for standardization; for example, the requirement that each Data Item under a given DE be mutually exclusive, with no overlapping or duplication. In this regard, a Data Item was defined as "the smallest subunit or piece of information . . . which cannot be further subdivided and retain any significant meaning." Interestingly, this early document from the Defense Department emphasized the importance of Data Use Identifiers in the business of data standardization; it pointed out that they:

- Must have <u>unique</u> names;

DOCID: 4019690

Are always reported and recorded in terms of the same Data Items and codes as the Data Element itself. (This observation is a good one to keep in mind in maintaining the clear distinction which should exist between Data Elements and their modifying Data Use Identifiers. We will look at this distinction in more detail later.)

~~(FOUO)~~ In the meantime, NSA had begun to get its own program untracked. D54 had been serving as the point of contact with DoD and had been coordinating our exchanges of ideas and problems with them. On 28 January 1965, a memorandum from General Davis, then ADP, broadened the base for data standardization within NSA and beyond. It designated P1 as the "authority in P for the development and maintenance of standards for those terms which constitute elements of the technical data base for P." He assigned P1 the task of developing standards in such areas as intercept coverage accounting; the data required in machinable technical reports; information in such data bases as TIPS (Technical Information Processing System - still operational); and "data comprising any similar data base or program in the future." Gen. Davis' memo spoke strongly about the desirability of achieving standardization which would relate to data bases throughout P "and indeed the entire SIGINT community." He pointed out the need for standardization in relation to:

- A standard name for each Data Element concerned;
- An agreed-upon meaning for each individual DE;
- A body of Data Items, or the information content of each Data Element; and
- A standard configuration for the DE; that is, like data expressed in a like manner.

~~(FOUO)~~ Two other documents are of interest as a background to the NSA program:

- Bureau of the Budget Circular No. A-86, Standardization of Data Elements and Data Codes in Data Systems, dated 30 September 1967, which:
  - established the Federal program for data standardization;
  - defined Data Elements and related features in terms much like DoD's and NSA's; and
  - confirmed the "cryptologic waiver," which meant that NSA would be exempt from having to observe a Federal standard which might adversely affect our cryptologic activities.
- DCID N. 1/15, DATA Element and Code Standardization for Intelligence and Intelligence Information, dated 14 October, 1969, which established a policy promoting the use of data standards in the exchange of intelligence information among information-handling systems.

~~(FOUO)~~ In developing its own data standardization program, NSA has remained faithful, with only minor variations, to the general concepts, terminology, and set of definitions passed down from its big brother, the DoD. One of these "minor variations" concerns the scope of the "Data Use Identifier" (DUI). The DoD usage has historically viewed the DUI as virtually synonymous with "Field Name."

~~(FOUO)~~ The latest editions of both the DoD and DIA standards manuals still use the term with this original meaning. In Cryptologic applications (as opposed to personnel, logistical, financial, etc.) at NSA it has been applied somewhat more narrowly than the DoD usage, i.e., to point just to the specific use of a given Data Element in making up a field name; for example, in "Date of Intercept", the phrase "Intercept, of" is considered to be the DUI. In this paper, "Data Use Identifier" will have this more restricted meaning.

The Data Use Identifier (U)
A Basic Tool

~~(FOUO)~~ The thing we data standards people call a "Data Use Identifier" (DUI) has long been a puzzlement to many otherwise well informed NSA analysts. At least such has been our experience at the Data Standards Center, where we have seen many DUIs aborted, mangled,

or otherwise abused as they drift across our desks in the form of Computer Record Formats and other EDP file descriptions. There are many reasons for the lack of knowledge as to what they are and how they should be used. One is the widespread shortage of guidance in this area, for which we at the NDSC have to bear our share of blame. In fact, the only explanatory material about DUIs readily available lies within the pages of official directives, such as the Department of Defense Instruction 5000.12 which, in April 1965, established the policies and procedures governing the DoD data standardization program, NSA Regulation 80-9, and our own USSID 414, which is the official directive for the NSA program. Very often such directives are the last thing people consult, especially when they are hurrying to get their machine projects off and running. Recognizing that DUIs are an important aspect of the business of labeling and naming data fields, the Data Standards Center is developing a working aid which lists and defines the individual Data Use Identifiers that have been standardized to date and at the same time explains how each one is used. (More on this "DUI Registry" below.)

~~(FOUO)~~ As an NSA analyst you are apt to be somewhat skeptical about this feature of the NSA standardization program. What do these "identifiers" have to do with the practical problems of managing a data file, and of what real value are they? Well, a lot, we think - if you happen to have a new file ready for machine processing and need to come up with meaningful names for what is in it. If the file is just for you and your work center alone, a private domain so to speak, then you can probably in good conscience invent your own mnemonic codes or tags and name the fields anything you like. If your file is to be shared or exchanged with some of your fellow employees, however, it is the proverbial horse of a different color. USSID 414, bearing the unwieldy name "Standardization of Data Elements and Related Features for SIGINT Activities," says, among other things, that there is a right way, and many wrong ways, to approach the problem of naming and labeling your data fields. The Data Use Identifier (which is one of those "related features" dealt with by USSID 414) has a lot to do with that right way. There is no need for us to stress the many advantages which accrue to files (and to their managers) which follow these procedures; chiefly, the fact that the name of the field and its coded representation should immediately tell a user what type of information is in it. (If they don't, we may have problems deciding what it is and whether we can use it.)

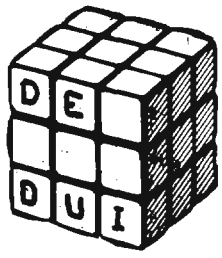
What is a Data Element? (U)

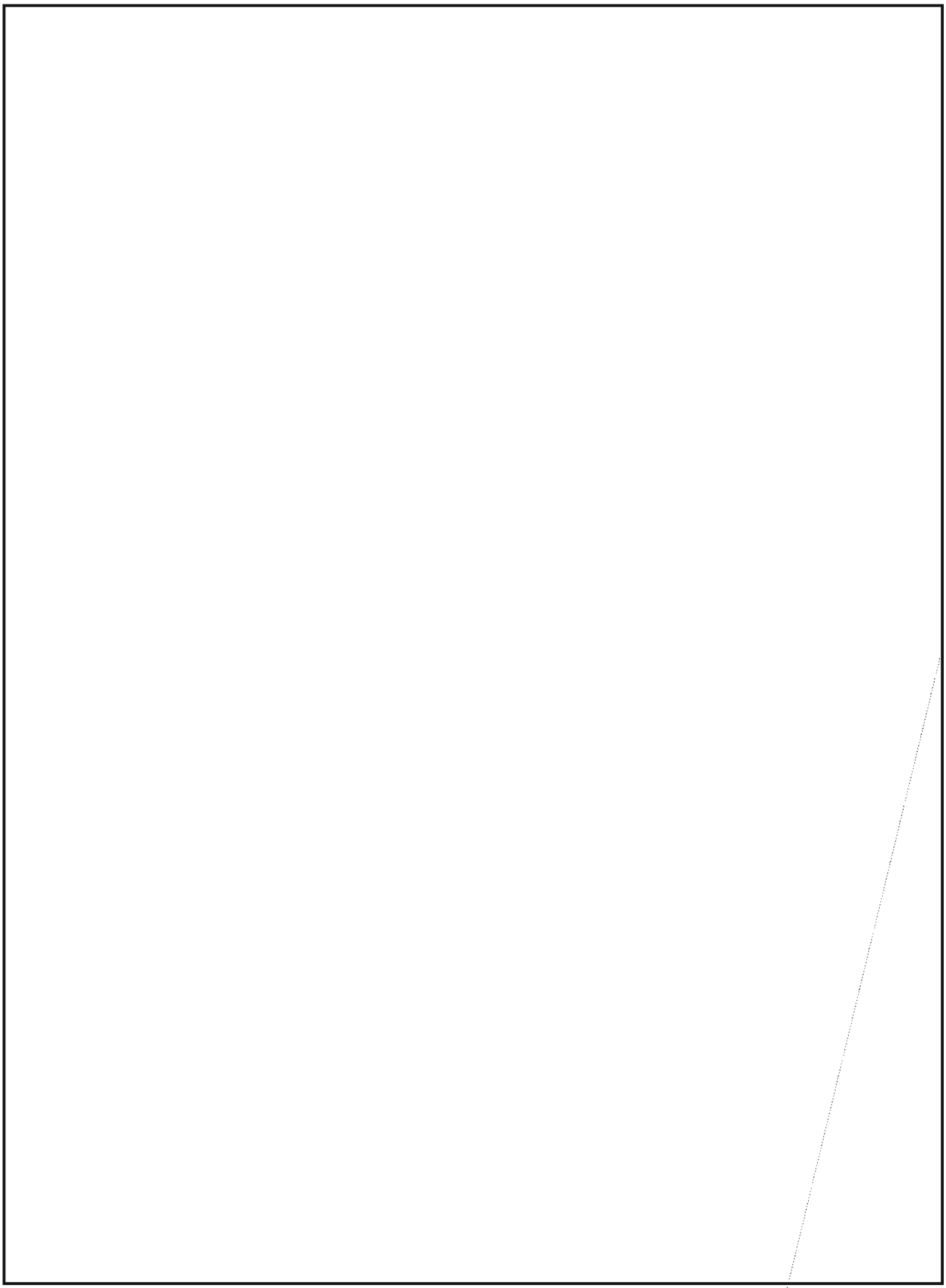
~~(FOUO)~~ Before explaining how DUI's relate to Field Names in EDP applications, we had better clarify the concept of "Data Element." The official definition, from USSID 414, says that a Data Element is a "unique grouping of related informational units." Funk and Wagnall's Dictionary of Data Processing brings in the concept of "Data Items" in its definitions:

- "Data Element: a class or category of data based on intrinsic or assigned relations between data items."
- "Data Item: any individual member of a Data Element."
  (One should note that a Data Item and its code are not identical.)
- Data (Item) Code: A set of characters structured in such a way as to represent the data items of a data element." (Italics mine.)

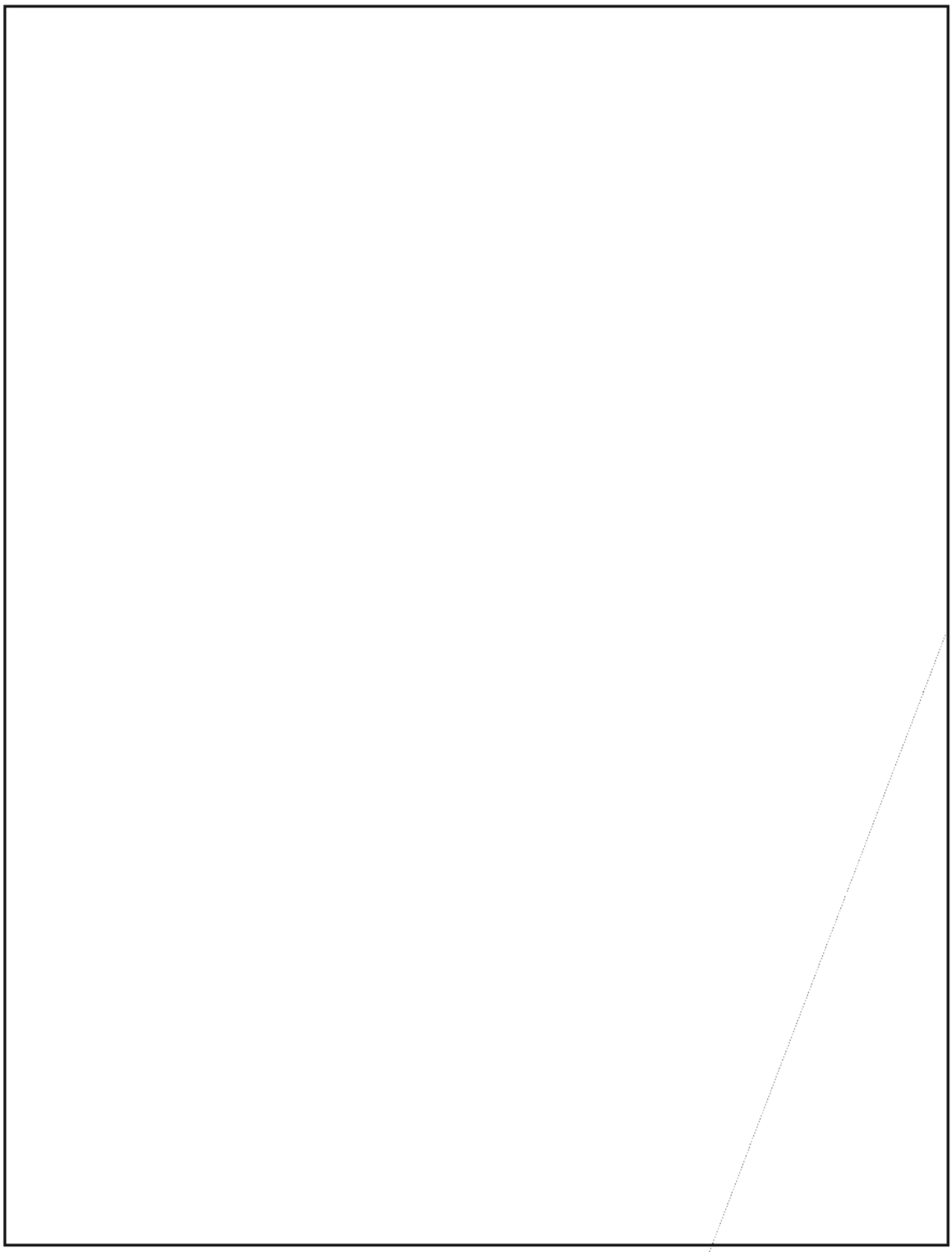
For example, "Month" is a Data Element; "January" is one of its Data Items; and "01" is the code which represents the data item "January."

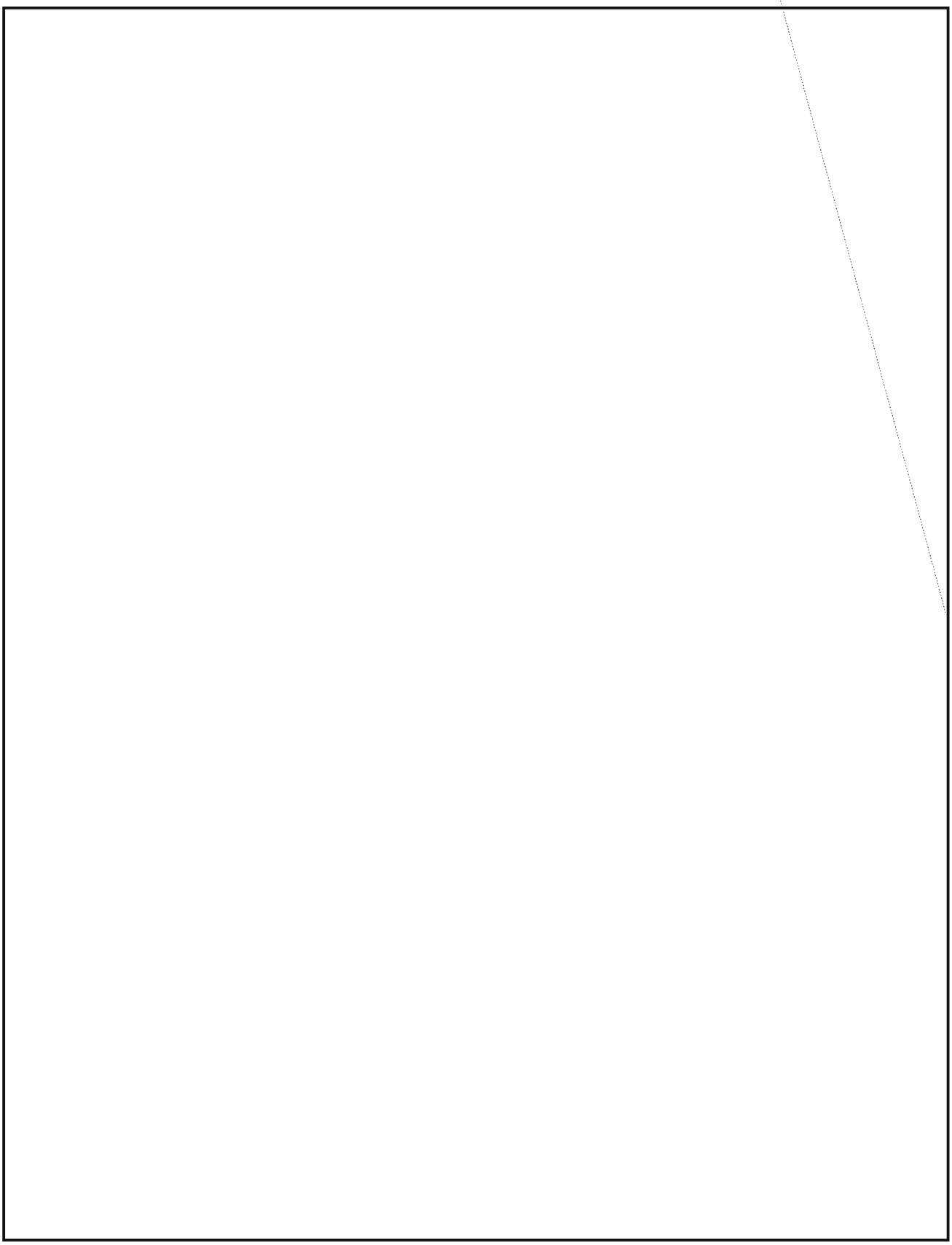
~~(FOUO)~~ You can think of a Data Element as a somewhat abstract category or class of information, and a Data Item as one of the specific values that can be assigned to that DE. The set of values can be either finite or infinite. For example, "Month" has only 12 possible Data Items; "State of the U.S." has exactly 50. "Date" on the other hand has an infinite set of possible values. ("24 January 1980" is one possible Data Item; its coded representation is "800124".)

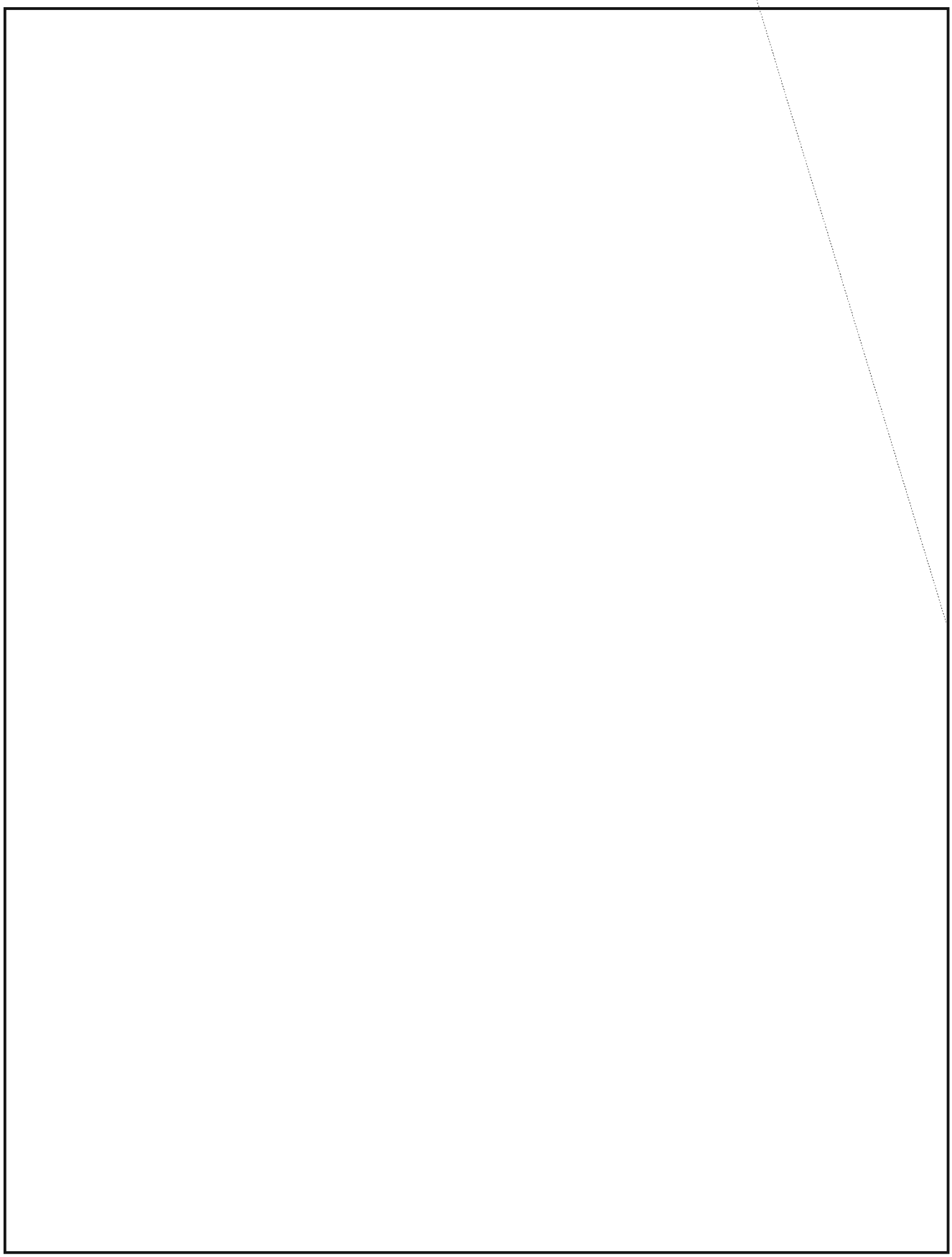


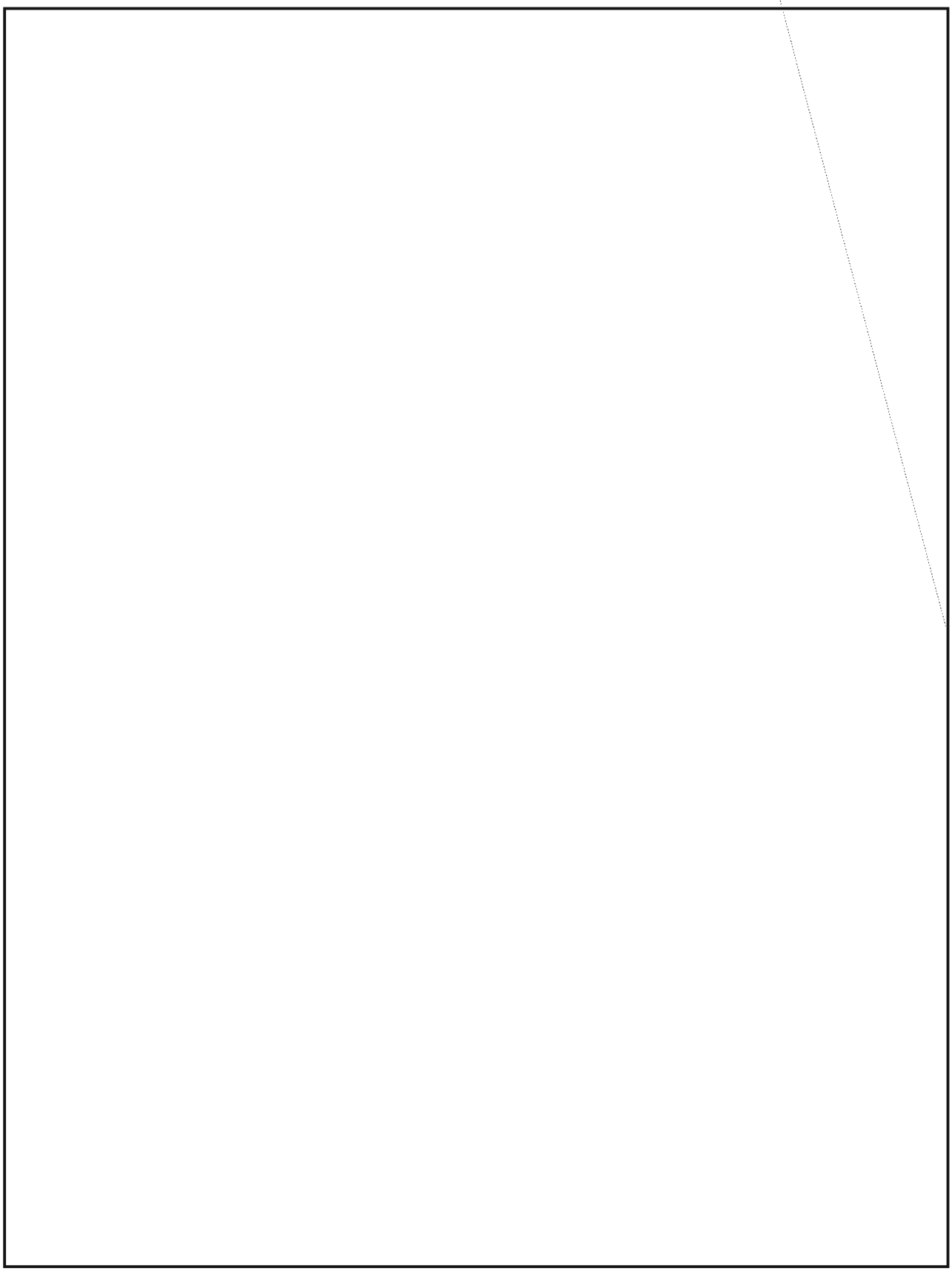


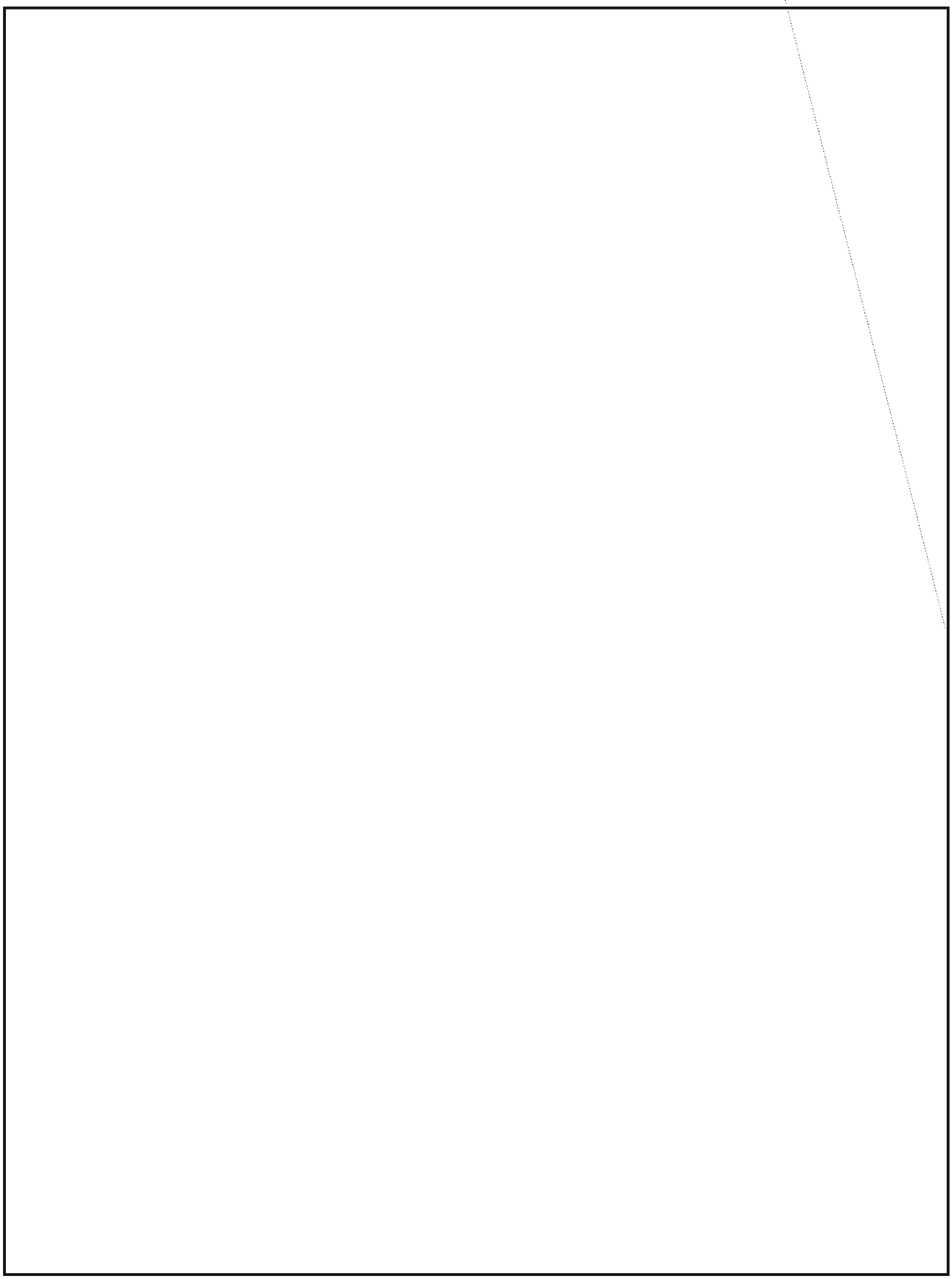
P.L. 86-36
P.L. 86-36





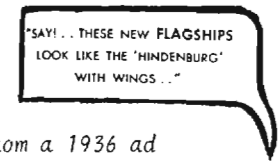






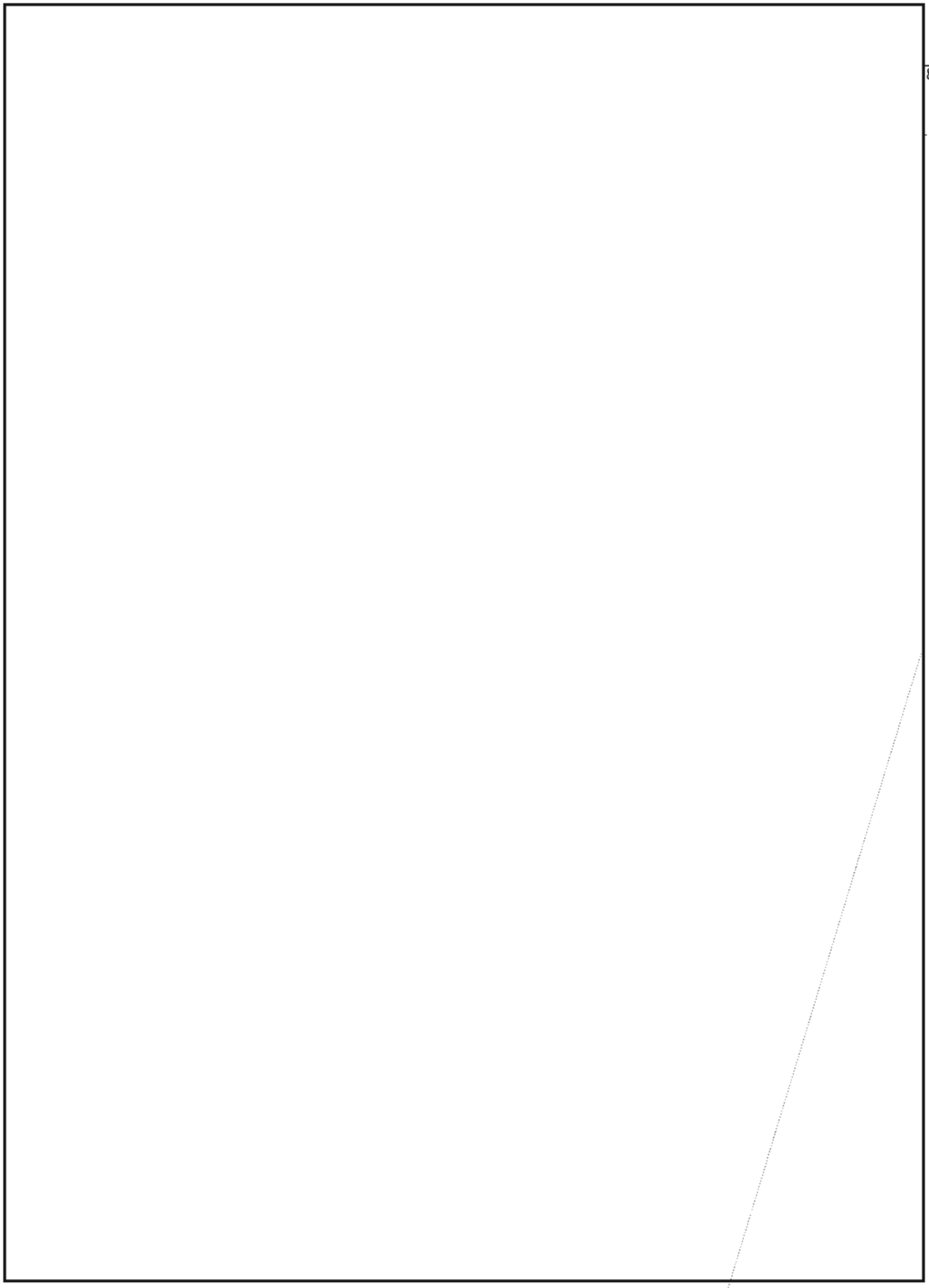
A bit of airline trivia to start the new year

NSA~Crostic No. 37



—From a 1936 ad

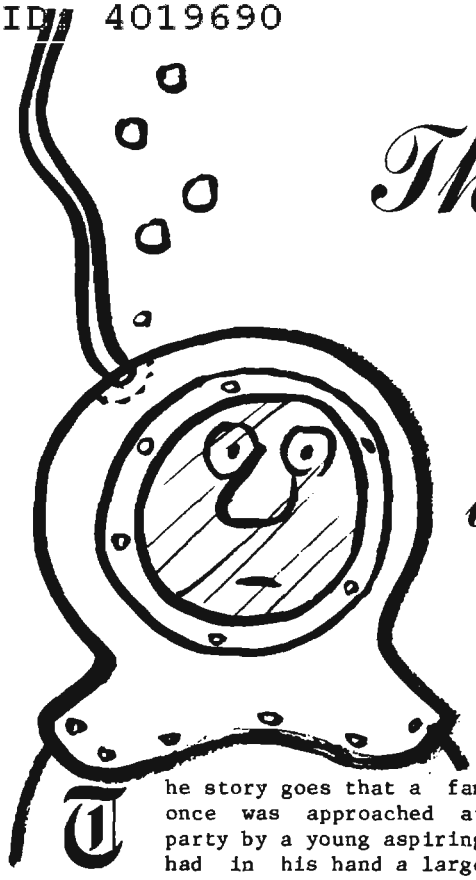
P.L. 86-36



P.L. 86-36

DOCID: 4019690

The Literary Bends (U)



by Albert J. Murphy, E41

(U) The story goes that a famous author once was approached at a cocktail party by a young aspiring writer who had in his hand a large draft of a novel he had written. The young man, perhaps more brash than polite, asked the author to take the draft, read it, and suggest a title. The author, taken aback by such directness and by the size of the document, thought for a moment, then asked: "Do you mention drums anywhere in the story?" "No sir," replied the young man. "Do you mention trumpets?" Again, "No sir." The maneuver had worked. "Then why don't you call it 'No Drums, No Trumpets'?"

(U) In the business of teaching Introductory Writing (EG-022) and Expository Writing (EG-122) at the National Cryptologic School (NCS), we have encountered some rather pointed feedback from some of our students, which cannot be so easily put aside. The students talk of two worlds of writing at NSA: the ideal world of writing as taught here at the school, and the real world of writing as practiced on the job. Eventually, one of them will crystallize the issue by saying, "This course is all well and good. But when I finish it, I know I'm going to be faced with the decision of writing your way for the sake of good writing, or of knuckling under to my supervisor's blue pen for the sake of my next promotion." Rightly or wrongly, the haunting question inevitably comes to mind: "Is his or her supervisor under 35 years old and a product of society's convulsing educational system?" We choose never to ask it.

(U) How valid are these rumblings? What is the extent of alleged shortcomings in the way people in management write (we're talking primarily about supervisors and staff editors)? And what are we going to do about it? Based on our own collection of bits of evidence, coupled with this human testimony from the students, we believe that the rumblings have some validity. But since we have neither the mandate, nor the resources, nor the time for a thorough research effort, the best we can do is to present the problem in this vehicle in the hope that the managers in question will read it and do something about it.

(U) Just before the students complete our courses, as part of a normal procedure we alert them to the post-course period of what we call "the literary bends," during which they might find it difficult to apply their newly acquired (or their refreshed) set of rules of good grammar and effective writing. "Don't be surprised," we tell them, "to find your pencil frozen in your hand or your fingers immobile at the typewriter during your first writing tasks on the job." They understand that. Some have reported that that's exactly what happened. Others have had to wrestle with the problem while still in the course. It is unfortunate, however, that we are now compelled to warn them of possible additional difficulties that can occur when a person in the supervisory chain, whether through ignorance, or obstinacy, or, alas, because of misguided pressure from a supervisor at yet a higher level, discourages the students' attempts to apply what we have

taught them.

(U) If managers are willing to face up to the reality that some of their people are frustrated in their jobs because, as they perceive it, we don't practice what we preach in the field of writing, then we are well on our way to solving the problem. Perhaps, then, our message to managers ought to be --

> Managers:
> By all means enforce good quality control; but in the process, please be aware of this problem, be fair with your people, and be square (that is, be traditional) with the language.

We contend that the modernists are wrong. Like it or not, there is an English Language; and it is governed by a set of rules for correct grammar, effective sentence and paragraph structure, and good writing style. Perish the thought of Congress wanting to change the words of the Constitution to accommodate modern linguistic happenings.

(U) You managers, if you are following this discourse in earnest, should be asking at about this point, "Well, what have you been telling our people in your classes?" Our answer is that we've tried to convey to them the fact that there is beauty in our language, and that the students should find it and use it. We have found that they not only are receptive to this idea, but also at times are resourceful (and not too subtle) in expressing their endorsement. You can experience intellectual beauty, we once told them, by merely pronouncing the names of tribes of American Indians, for they have a majestic quality that evokes, through vivid mental picture of frontier days, much of what is noble in the American character.

Cheyenne...Pawnee...Apache...
Comanche...Sioux...Shoshone --

here the students joined in --

Mohawk...Cherokee...Blackfeet...
Chippewa...Algonquin...Iroquois.

Then the spell was broken as quickly as it began when one of the students wistfully offered...the Washington Redskins. We have told them about the importance of good communication, whether in face-to-face conversations, on the telephone, or in writing; and of the potential disasters of failing to communicate. We've advised them not to write without good reason. But once they've decided to write, they should spend some time thinking about what they want to say before committing their thoughts to paper. They've heard us say many times that bad writing is usually the result of poorly thought-out ideas.

Grammar, Spelling and Punctuation (U)

(U) We have compiled an array of real-world writings from NSA in-house correspondence and CRITICOMM messages, which we contend are inconsistent with what we teach. But, in order not to raise the hackles of a lot of people, we will cite only a few that are important to the point we are trying to make, and then only when we think they will do no harm. Recently, E asked various in-house elements to submit any comments they might have on an NCS course on reporting, which some of their people attended. It was a bit disconcerting when a staff editor of one of those elements, in his responding memorandum, said, "We don't need grammer in the course. We in the editing chain can handle it." Impertinent of us to mention this, you say? Well, maybe. But what about the problem of credibility? It's there, isn't it? If the element in question recognizes its handiwork here, we hope the people involved will not take umbrage, but will view it in the spirit of light criticism and let us make our point. We have taught your people that

1. Dangling and misplaced modifiers are major causes of confusion in communication; to wit, "The second child, Nancy, was the only child of a mother who was divorced in her infancy"; and "If found guilty, the Division of Motor Vehicles will be notified and your license may be subject to suspension."

DOCID: 4019690

EO 1.4.(c)
P.L. 86-36

2. Pronouns must agree in number with their antecedents. A certain ABC television reporter either didn't do his homework or decided to go modern when, in describing a recent hurricane, he said: "Damage will be in the millions, but only one person lost their life."

3. Billy Kilmer used incorrect grammar in his beer commercial when he praised his beer for having less calories. He should have said fewer calories because few(er) is used with things you can count, and less is used with things you cannot count. ("If there were fewer TV's, there would be less noise.")

4. A writer can quickly reveal himself as less than professional if he is careless with spelling. Consider the following statement that appeared in a real-world NSA CRITICOMM message:

   "SGT (John Doe) IS REQUIRED TO BE INDOCTERNATED FOR (special clearances) PRIOR TO DEPARTURE FROM YOUR STATION."

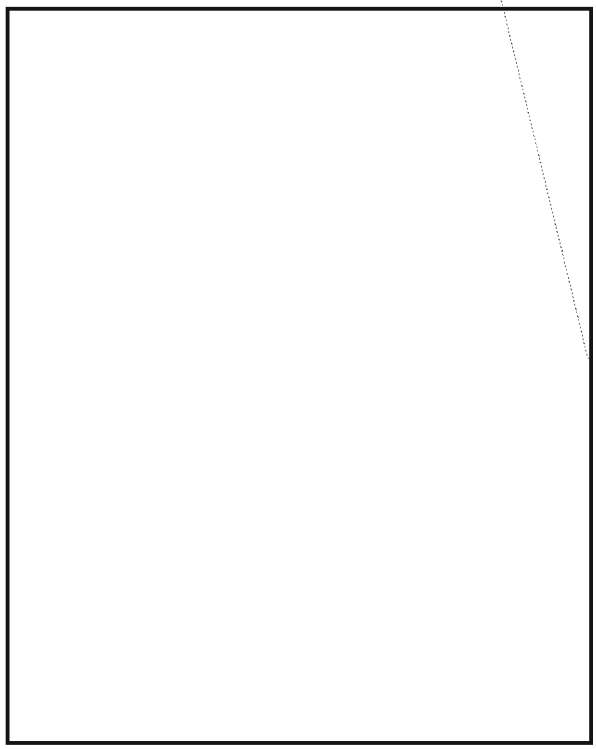
   An astute, post-publication (unfortunately) comment written across this gem facetiously noted that "This wil hep with hes clarence." Also, we've made it known that irregardless is a self-contradictory non-word, despite the regrettable fact that it is listed in Webster's New Collegiate Dictionary.

5. A comma is required before and when presenting a series of more than two items (matrix, row, and column). One of our students described in class how he was rebuffed by his supervisor for insisting on applying this rule. We suggested he have his supervisor call us to talk about it. We are still waiting for the call.

Managers:
When your people try to apply the rules of good grammar, spelling, and punctuation in their day-to-day writing, they are not trying to out-write you. They are only doing what they learned. So please -- let them.

The Sentence (U)

~~(SC)~~ Since your people are not as gifted as General MacArthur was, we have trained them not to write long, Aristotelian sentences. So, when you see them trying to limit their sentences to about twenty words or fewer (to the fullest extent that the content will allow it) -- let them. We've talked them into it. Consider the following long, but not necessarily Aristotelian, opus that appeared in an out-going NSA CRITICOMM message:



We suspect that a period (a full stop) might have been intended after the word producer on the tenth line, but it wasn't evident in the copy of the message we hold. Even if the period had been inserted, the latter sentence, containing at least 105 words, would still tax the patience of the reader.

(U) In order to compose good, expository sentences, our students are following the FACTS formula (the Fast, Accurate, Concise, True, and Simple way). That means they will be trying their best to use the active voice (instead of "the great evader") and a lot of concrete, one-syllable words (we just can't bring ourselves to say "monosyllabic" as opposed to "polysyllabic" in this context). We hope we have burned into their memories the Lensear Write Formula(1) which encourages short sentences, the active voice, and one-syllable words. If you ask them about it, the

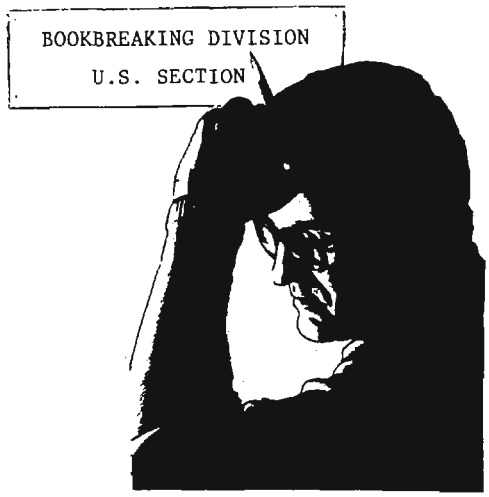
chances are good that they will be able to recite to you the clear and simple "something special" lead that an obscure reporter wrote on the death of Samuel Clemens in 1909, which must have caught the breath of all who read it: "Tom Sawyer and Huck Finn are orphans tonight. Mark Twain is dead!" Notice the number of one-syllable words.

(U) We encouraged your people to use parallelism correctly and wisely in their writing, to incorporate an effective blend of periodic and loose sentences, to show their maturity in the use of subordinate clauses, and to include in their list of writing "don'ts" the principle that smothered verbs (strong verbs turned into weak nouns, such as -ization, -ment, and -ure words) and passive voice constructions frequently go hand-in-hand. The poorly written sentence "The specialization of many professions is necessitated by the complexity of our society" is best recast to read "Many professions must specialize because our society is complex." The finest sentence that we've come across at the school so far, in terms of sound structure, clear and simple content, and, yes, downright beauty, was written by a student in her autobiography project. She wrote, "When I was little, my father often said that I was the best door slammer this side of the Mississippi River." Is there any wonder why we abhor the likes of the sentence "The possible appearance of a new communications network was observed...."?

Managers:
When your people try to write in clear, simple, and direct language, don't assume that they are undereducated. They're only doing what they learned. So please -- let them.

The Paragraph

(U) We have practically ordered your people never to settle for a paragraph that doesn't have the standard properties of UNITY, COHERENCE, ADEQUATE DEVELOPMENT, and CONSISTENT and APPROPRIATE TONE. Unity calls for one central idea and a single topic sentence; coherence -- the paragraph form -- is the writer's sequence of thought from one sentence to the next, which he achieves through the use of connectives or transitional words and phrases; adequate development -- the subject matter of the paragraph -- involves the who, what, when, where, and why, whether accomplished through definition, comparisons and contrasts, cause and effect logic, or analysis and classification; and, tone deals with not what the writer says, but how he says it.



That plain text doesn't make sense!
My recoveries must be bad again!

~~(C)~~ All four of these properties, we have insisted, are essential for good paragraph structure. But the one that usually causes lengthy discussions in class is TONE. We think this is good, because it tells us that the students are trying to be sensitive to "how it will sound" to the reader by steering away from unwanted tone. So they wrestle with another set of "don'ts": "Don't be offensive ... bossy ... contradictory ... and so on."

Managers: Are you with us?

In one of our classes in Expository Writing a discussion on paragraph tone developed after we explained how the tone of separate paragraphs in a piece of writing, say in a SIGINT report, ought to be consistent with the general tone of the writing. We gave the example of reports forwarded to the NSAPAC REP VIETNAM (NRV) staff in Saigon, in 1971, by one of the ten ARVN Special Technical Detachments (ASTD), which time and again reflected a tone of absolute terror. The perimeter of the site was not secure, and the ARVN people didn't seem to care. When the reports from this ASTD came in, the staff was obliged, not without some pains of conscience, to change the tone of the reports to fit the dispassionate, objective tone of the monthly status report within which they were incorporated for forwarding to the Director (the Vietnamization Improvement and Modernization -- VIM -- report). One of the students, who obviously had after-the-fact sympathy for the plight of the writers of those reports (U.S. soldiers assigned to the ASTD), questioned the changing of the tone.

EO 1.4.(c)
P.L. 86-36

After we explained some of the unpleasant realities of the situation (we also apprised her of her handicap as a caring human being), she conceded that the tone of that ASTD's reports had to be changed and that our point on consistent and appropriate paragraph tone was well taken in the class.

Gobbledygook (U)

(U) We have described to your people in considerable detail the perennial enemy of good writing, namely gobbledygook or federalese -- the old obscure writing that is usually meant to impress rather than to express. We have convinced them (we hope)

(1) that it is foolish to use high-sounding words, such as utilize, implement, initiate, viable, optimum, and terminate;

(2) that roundabout expressions, such as "It is believed..." and "There is/are..." make for weak writing because they tend to repeat, they are often vague, and they leave the reader with no way of knowing what is meant, thus forcing him to work for nothing;

(3) that we condemn the use of the expression "It is felt that..." because it has three inherent strikes against it -- it is roundabout, it is passive, and it is false (one doesn't feel an argument or a contention; one thinks it or one believes it);

(4) that circumlocutions, such as "Owing to the fact that...," "Concerning the matter of...," and "In reference to..." are nothing more than deadwood; and

(5) that illogical, incongruous, or inappropriate metaphors should be avoided.

After analyzing the following real-world statements, we couldn't come up with a reasonably good answer to the question, "What happened to the quality control system?"

"The state of the art, as it exists today...."

"It's a sad day of affairs...."

"(We should be) starting out with a clean foot." (Let's call this one a combined, instead of a mixed, metaphor.)

Those gems are not any worse (or, if you like, any better) than the golden-oldies that were taken from letters received at a welfare department in Tennessee some years back (you old-timers might remember them):

"I am very much annoyed to find you have branded my son illiterate. This is a dirty lie as I was married a week before he was born"; "Unless I get my husband's money pretty soon, I will be forced to live an immortal life"; and "I am glad to report that my husband who is missing is dead."

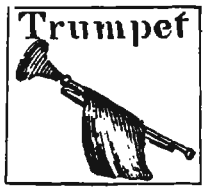
~~(S)~~ We shudder to think of what would have happened to our credibility in October 1962 if the [redacted] reporting staff [redacted] had gobbledygooked those FLASH messages they fired to NSA containing the first SIGINT reports on the Soviet merchant ships stopping dead in the water at the peak of the Cuban Missile Crisis. We also shudder to think of the possible unthinkable consequences of gobbledygooked guidance (from NSA) and gobbledygooked responses (from field elements) on matters about current developments in the world in general and in Eastern Europe and the Middle East in particular. The solution to NSA Crostic No. 35 (CRYPTOLOG, October 1981) contains a poignant comment from [redacted] Plain English that aptly supports all that we've been trying to say here.

P.L. 86-36

> If we want all Agency personnel to speak and write plain English, perhaps we should first teach Agency personnel English. If we want Agency management to write concise, active, decisive memos, perhaps we should first teach Agency management to be concise, active, and decisive. Let us attack the problem, not just the symptom.

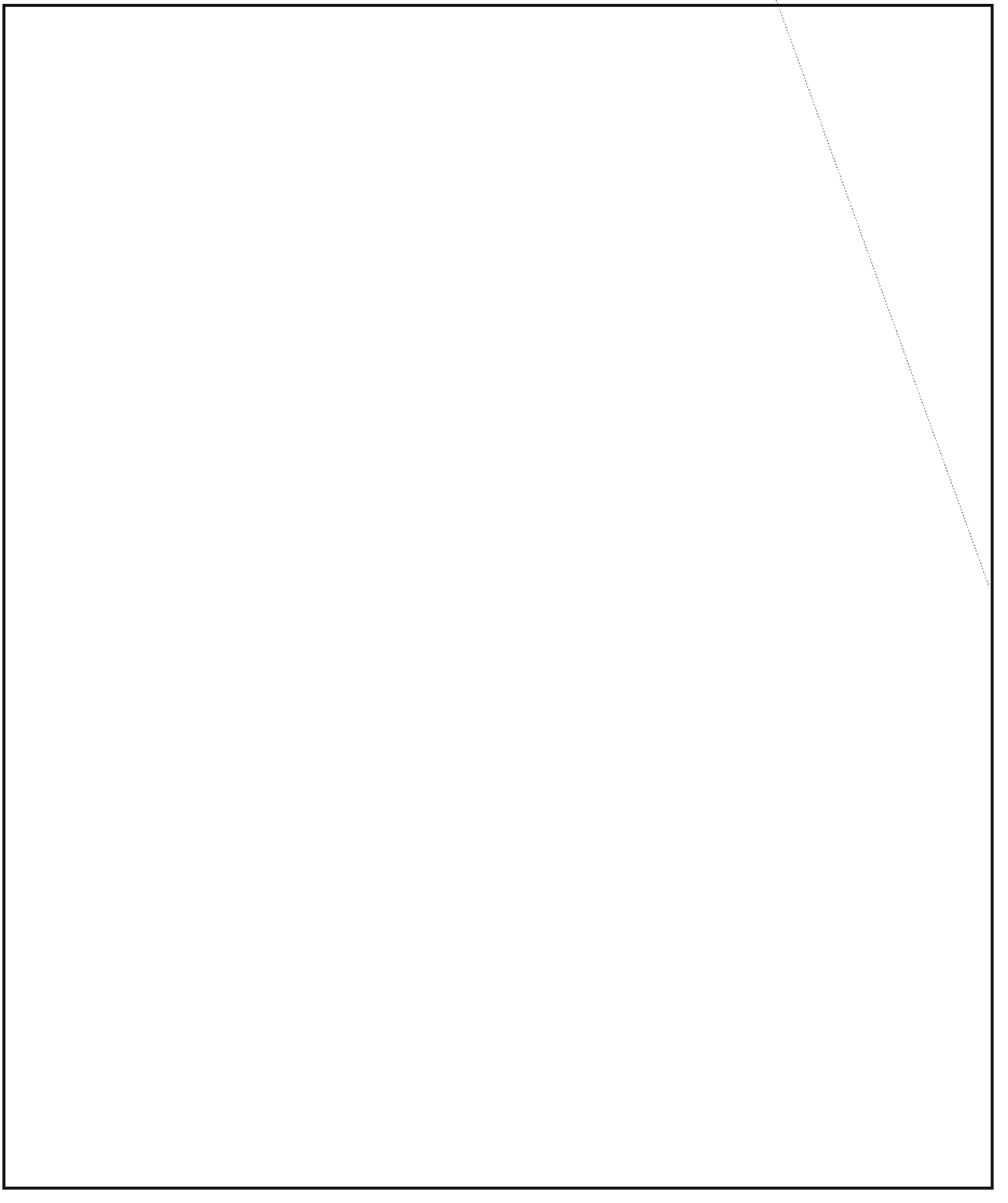
(U) Having stated our case, we fully intend to continue to orchestrate drum rolls and trumpet blares for the cause of getting managers to cooperate in making clear, simple, direct, brief, and appropriate writing happen at NSA.

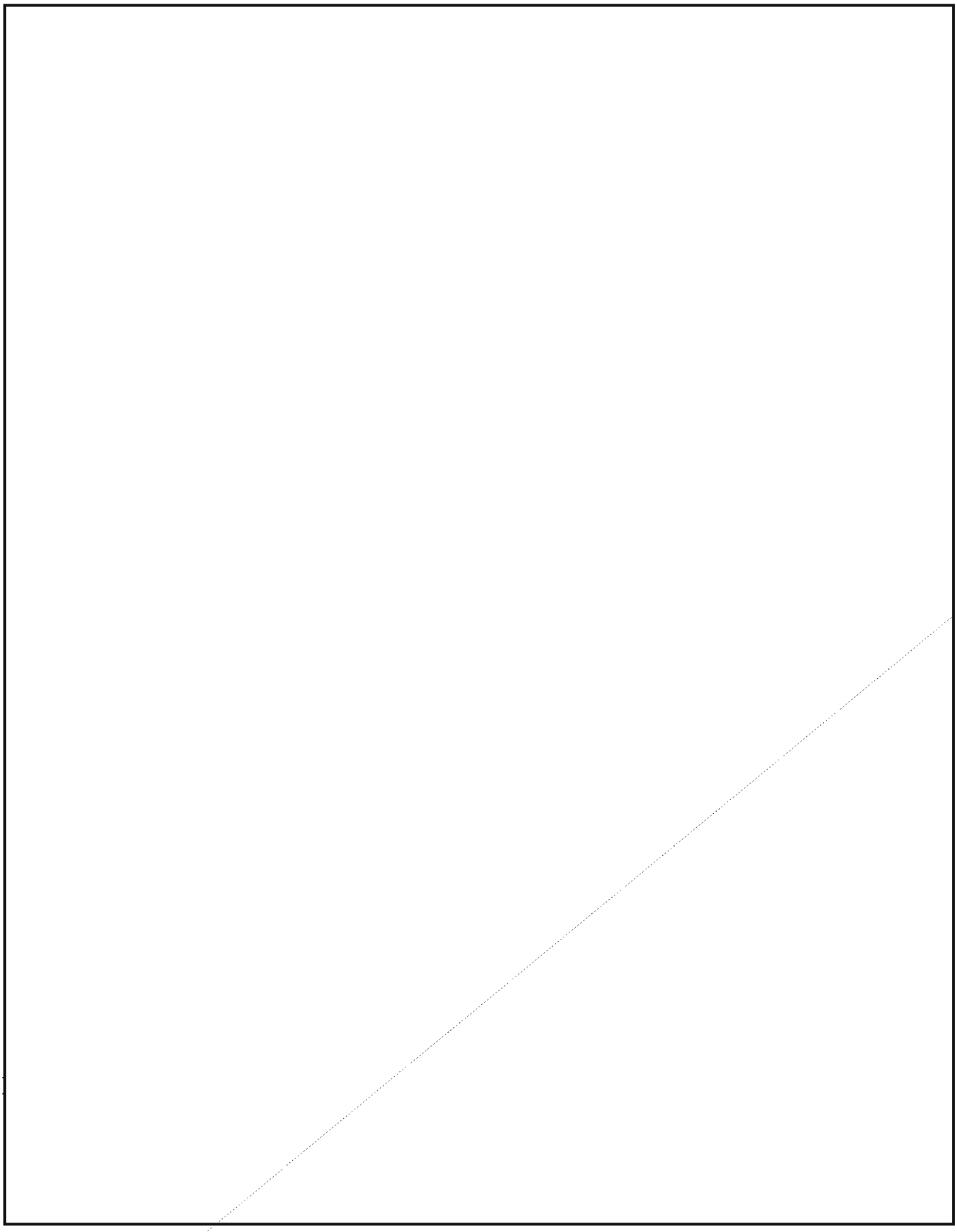
(1) Gobbledygook Has Gotta Go; U.S. Department of the Interior, Bureau of Land Management, p7. U.S. Government Printing Office: 1978 O-269-955.



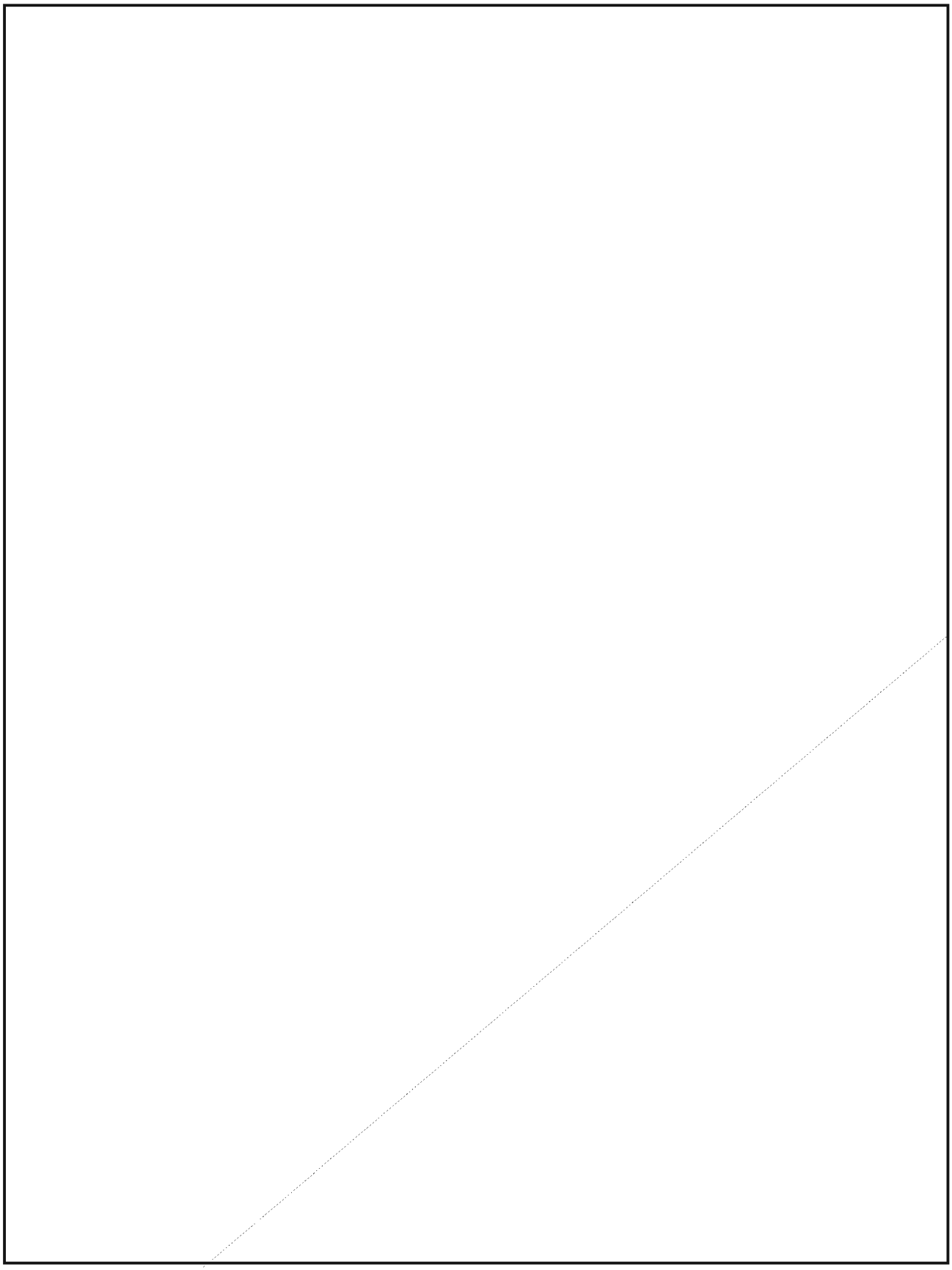
All The Alligators Aren't On Sport Shirts (U)

EO 1.4.(c)
P.L. 86-36





EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

DOCID: 4019690

HUMAN FACTORS CORNER (U)

with [redacted] P13

P.L. 86-36

REVIEW: "Information Systems - The Management Challenge", Joe Brancatelli, "Review" (Magazine of Eastern Airlines), October, 1981, p. 53.

Denny Eshoo, T441, kindly sent me this interesting article on a timely topic. In spite of its very general title, it specifically concerns the "Automated Office" or "Office of the Future" concepts being marketed by a number of firms. There are plans to introduce some form of "office automation" into NSA in the near future, for example in R. This paper provides a good overview of the concepts and some of the human factors problems already encountered by organizations attempting to jump on the office automation bandwagon today.

> "Office equipment salesmen can't agree on what to call it, design professionals all give a different picture of it, visionaries see it coming, engineers say it's here, and some office workers want no part of it, ever."

Conversion of old-style offices to meet the new concepts will require a substantial investment. One estimate predicts that capital investment per office worker will increase from a current $3000 a year to $15,000 in 1990. And yet, according to this article, all the "experts" seem to agree that the sooner it happens, the better. They appear convinced that the expected gains will more than offset the expense.

The article does not spell out the real motivations that underlie the push for office automation. In fact, I cannot think of any place where I have seen them stated clearly, other than the usual vague words about "increasing productivity". However, reading between the lines, I think the following are prominent considerations: 1) White collar workers are increasingly numerous, and increasingly expensive, and automated "executive workstations" used by managers or staff people could replace many clerks and clerk-typists; 2) Office procedures involving communication, coordination, and records-keeping are becoming increasingly burdensome and difficult to control. This is blamed primarily on "too much paper" ("paper is the nemesis of the modern office"), though I can see some possibly more basic reasons for the problem; 3) Travel is becoming increasingly expensive, and electronic conferencing could effect a saving in time and money; 4) Managers perceive an increasing problem in getting and keeping a good "handle" on what is going on in their organization. This is blamed on "the paper problem", but is probably a more basic problem of fragmentation of effort and poor communication, exacerbated by the understandable reluctance of subordinate managers to relinquish any control over THEIR records to others. Automated, "paperless" distributed information networks might help solve this problem, if well designed to solve the real difficulties and not just to "abolish paper". In short, the automated office offers the manager a vision of a paradise in which he holds a smaller number of much shorter reins controlling all corners of his enterprise.

The early expectations of rapid changeover to automation in offices have run into some roadblocks.

> "Current wisdom, based on the experience of the past two decades, indicates that the office of the future will evolve slowly and methodically over the next twenty years."

The crucial problem seems to be resistance from some "tradition-bound managers and professionals".

> "You can't forget that office automation is introducing significant amounts of unfamiliar technology into a world where a great many people still hang up when they get a telephone answering machine . . . All the managers in an office have reached their current level of responsibility by using a set of communication tools they and everyone else understand . . . Suddenly, someone says, 'Forget all that, here's a new way to do

DOCID: 4019690

> **things with keyboards** and video screens **and electronics.'** That's a scary transition *to make after* decades of hard-copy files and telephone messages."

There is another obstacle between managers and the "executive workstation", and one that may not be restricted to those who are older or more traditional. If the intent of the automated office is to replace the manager's secretary with a workstation operated by the manager himself, we will run up against a key element in "corporate culture" that cannot be ignored.

> "Managers and professionals . . . routinely delegate clerical tasks to secretaries and other support personnel. Most of these clerical tasks involve typing, a skill managers on the whole do not value highly . . . and until more advanced methods of access become feasible . . . managers and professionals alike will be asked to operate their workstations by typing messages on a keyboard". One expert says, "I know middle-level managers who have been told not to punch information into a word processor because it doesn't look right . . . Managers view any kind of typing as a menial task. They say to themselves, 'I shouldn't be doing this.'"

Another, even stronger barrier relates to the status that a real, live human secretary confers on the manager. Along with the private office, comfortable furniture, and picture window on an upper floor, a secretary is one of the major perks of being a manager.

> "Losing a secretary, office-automation experts now realize, isn't just losing support personnel. In the pecking order, a secretary is also a tangible symbol of the manager's importance."

Thus, the hope of replacing expensive humans with supposedly less-expensive machines may have to be set aside, at least when it comes to the secretary in the front office (though the typing pool may not be so fortunate).

Perhaps the best hope lies in making "executive workstations" into a new kind of status symbol (e.g., giving one to the President first, then the VP's, and so forth), and in making them as different as possible from typewriters! I am afraid that the thought occurs to me that one of the reasons why typing and typewriters have such a "menial" image for managers is that they have traditionally been operated by women. Maybe the solution lies in putting the "executive workstation" in a "macho" package: making it look a lot like a control station for space missions, or the console of a nuclear power plant, and providing large banks of "menu" buttons for sending pre-programmed commands! That might enhance the manager's feeling of finger-tip control, god-like power, and remoteness from the squalid associations of keying in text.

The Xerox STAR is the first step toward developing an "executive workstation". It handles word processing, electronic mail, electronic filing, some rudimentary computing, and some other functions. While it has a keyboard, many of its functions are controlled by touching "icons" (symbolic pictures) with a simple hand movement, rather than by typing in commands. There are icons for activating the filing system (a file folder), documents, file drawers, in- and out-baskets, and printers. While not the last word by any means, the STAR "goes much farther than any other product on the market". Unfortunately, the workstation is useless alone, without a local network tying it to other stations, printers, filing devices, etc.

> "Networking technology is progressing rapidly, but strong marketing competition between exclusive systems may actually be slowing advancement. At least six major vendors are peddling non-compatible networking schemes."

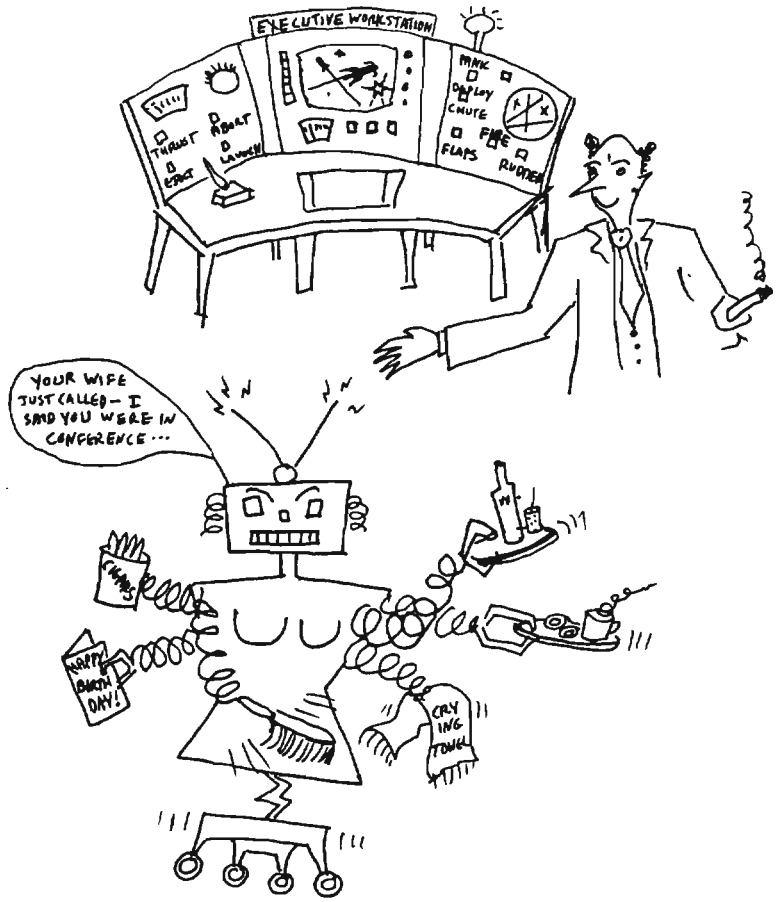
In any case, it seems best to start small, to carry out the automation process slowly and carefully, and to make it as voluntary as possible. Seven to ten years may be needed to make the switch complete in any given organization. "What we're asking people to do is change how they function, and that's not easy. We've found that people come around to office automation individually. But they come around at their own pace, and you can't rush them." Here are some "Tips for Transition" offered by the writer of this article:

> "Start small. Introduce new technology on a department-by-department basis. Don't overwhelm employees with a vast, company-wide change. Proceed gradually. Phase in new automated systems and services rather than introducing them all in one indigestible lump. Introduce

office automation technology only into those areas where benefits are immediately needed and will be immediately evident. Integrate the new technology into your existing system and office structure. Present new equipment and services as aids to increased productivity, not replacements for secretaries and support staff. Select an automated system that is compatible with the needs and preferences of your employees. Consult the potential users of the new technology before you start. Let them have a say in the system they will be using. Provide heavy and continuous training in the use of the new products and system both during and after the introductory phase. Integrate new equipment into the 'corporate culture' as one of the trappings of executive power. Managers will want an executive workstation more if it is a benefit awarded as a symbol of success.

"Don't force anyone to use equipment he or she doesn't want to use. If the majority of your managers and professionals are using the new equipment, resisters will fall in line as they realize that their refusal places them at a disadvantage. Allow each person to adjust to the new system at his or her own pace. You can't rush the learning process. Be prepared to wait out a possible 'generation gap' between older and longer-tenured managers, who are more likely to resist the change, and younger or newer ones. If possible, target the latter group for the earliest transition, since it is usually more familiar with automated equipment and more flexible or more eager for the change. Start immediately. Moving into the automated office of the future takes time for phasing in and adjustment."

The above "Tips" hold good for any introduction of new technology, and are by no means restricted to office automation. We ignore them at our peril, especially when we consider automating some of our work areas which are still entirely oriented toward the traditional tools: typewriters, paper and pens.



Letters to the Editor

Ref: Persephone
Terpsichore (April-June 81)

Webster's Second Unabridged has adequate descriptions of these Greek mythical personae.

Terpsichore (as illustrated by you) was associated with the dance and was not strictly a goddess but a lesser person (nymph).

Persephone was a daughter of Zeus and wife of Pluto, ruler of infernal regions (Hades) and presumably not much given to gaiety (dancing).

It is 1000 to 1 that you know all this already and just stuck the item in to see if there would be any reader response!!

[redacted]

P.S. I was bemused to find that according to [redacted] NSA has at least one employee capable of making such a statement as "nonferrous steel is steel without any iron in it."

R.C.

Dear Joe,

Just read your excellent piece on The Stairwell Society in CRYPTOLOG (October 81). It's high time someone publicized this important activity.

Several people who have been trapped repeatedly in the elevators in the International Tower Building have asked about the possibility of forming a FANX/ITB chapter. Minor league, of course, since the buildings out this way are only seven stories high.

If the interest in stairwell climbing continues to grow, the National Cryptologic School will present two new training courses in its stair climbing curriculum: SC-101, Avoiding The (elevator) Shaft, and SC-301, Up Your Staircase.

Inasmuch as secret societies inevitably attract the attention of the lunatic fringe, the possibility exists that Philip Agee may publish the names of the secret Society members in his Covert Action Information Bulletin, after he finishes with the other secret society he writes about.

You might also consider adopting a cheer or motto for your Society, something along the lines of --

Up on the riser,
Over the tread,
Too wide a Bloom arc
And you land on your head.

As they say on the buses, Watch Your Step.

Ed Wiley

P.L. 86-36

Cryptanalysis articles have been hard to come by in the past, although I believe there are a wealth of interesting articles out there, particularly in the hand systems areas.

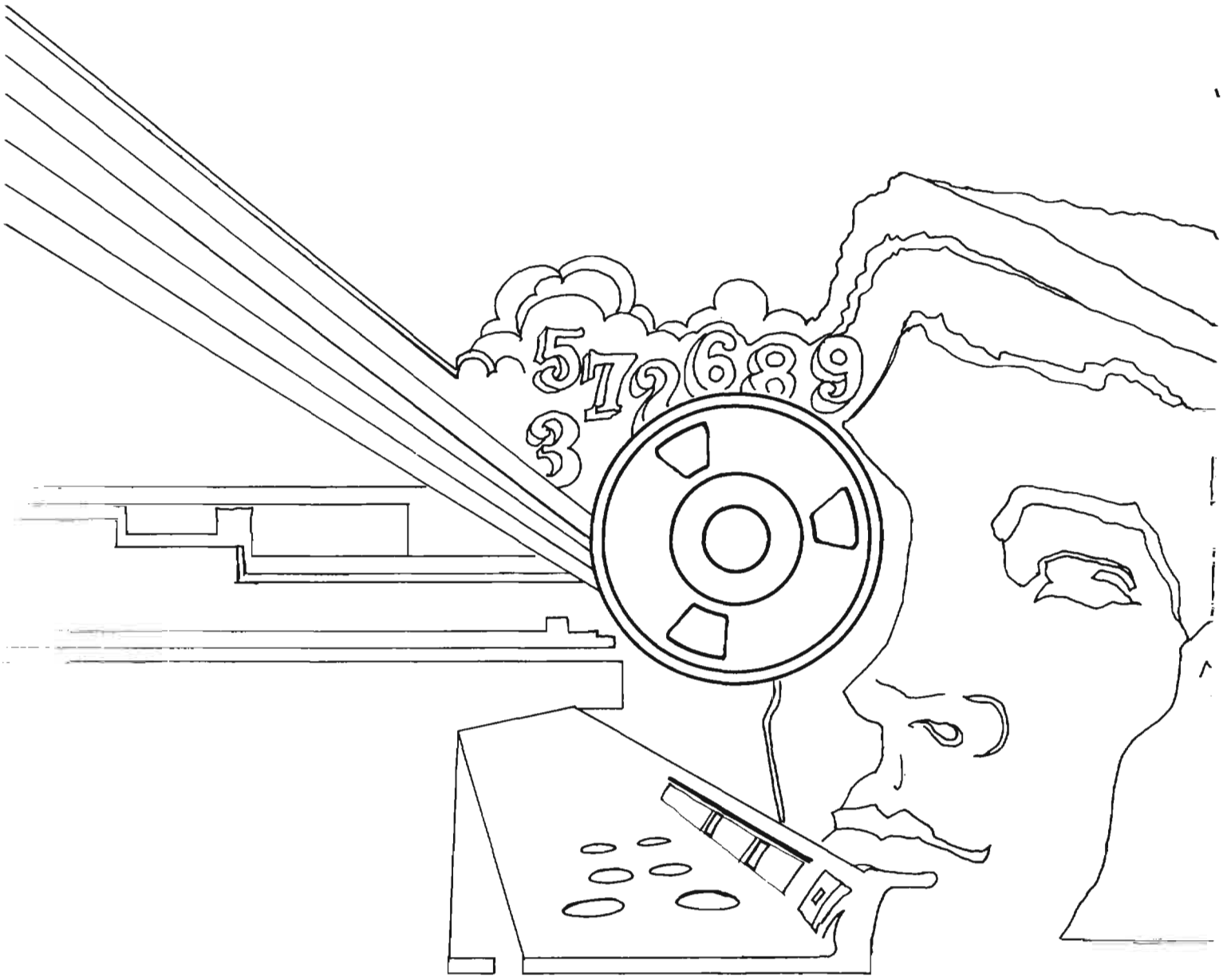
We need some incentives for short articles. How about a "Strangest Bust of the Month" contest?

[redacted]

SOLUTION TO NSA-CROSTIC No. 36

["A Traffic Analyst Looks at] Computers," [redacted] CRYPTOLOG, Apr-Jun 1980

". . . contrary to popular [view], we analysts were not afraid of computers. Maybe some [of us] were, but not all. But what we all did share was the realization that our processing cycle was no longer solely under our control. Our data was in a loop that went through someone else's area of control."


5 7 2 6 8 9
3

DOCID: 4011945

P.L. 86-36

~~SECRET~~

P16 [redacted]

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

December 1981

P.L. 86-36

EXERCISE SUPPORT (U).....[redacted].....1
THE 1981 URSI XX GENERAL ASSEMBLY (U).....[redacted].....5
SLEEP WELL! YOUR SDO IS ON DUTY (U).....E. Leigh Sawyer.....8
TIDE: A BRIEF HISTORY (U).....[redacted].....10
NSA-CROSTIC NO. 36 (U).....David H. Williams.....14
IN PURSUIT OF: FASTER HORSES, YOUNGER WOMEN,
OLDER WHISKEY, AND MORE MONEY (U).....[redacted].....16
TEXTA: WHAT IS IT? WHERE IS IT GOING? (U).....[redacted].....19
PLATFORM: HOW DID YOU SAY THAT WORKS? (U).....[redacted].....26
REVIEW: IN THE NAME OF EFFICIENCY (U).....[redacted].....28

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 10 Dec 2011~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4011945

CRYPTOLOG

Published by P1, Techniques and Standards,
for the Personnel of Operations

VOL VIII No. 12 DECEMBER 1981

PUBLISHER [redacted]

BOARD OF EDITORS

Editor-in-Chief..... [redacted] (7119s)
Production..... [redacted] (3369s)
Collection..... [redacted] (8555s)
Cryptanalysis..... [redacted] (4902s)
Cryptolinguistics..... [redacted] (5981s)
Information Science. [redacted] (3034s)
Language..... [redacted] (8161s)
Machine Support. [redacted] (5084s)
Mathematics..... [redacted] (8518s)
Puzzles.....David H. Williams (1103s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Don Taurone (3573s)

For individual subscriptions
send
name and organizational designator

to: CRYPTOLOG, P1
or call [redacted] 3369s

To submit articles or letters
via PLATFORM, address to

cryptolg at bar1c05
(note: no '0' in 'log')

EDITORIAL (U)

It is sometimes puzzling why some people turn out to be good at this analysis business, while others who are evidently just as well educated never seem to get the knack of it. I have, of course, some theories about this (or I wouldn't have brought the subject up), and I wonder what you the readers think about this.

One notion I keep coming back to, is that very few discoveries are ever made by means of the so-called "scientific method", and that it is only when one comes to the point of having to describe the discovery to others that the "scientific method" is used, as an orderly way of laying out facts and their connecting arguments.

Over the years, it seems to me that the great bulk of the genuine analytic discoveries were made by a relatively few people. Some of these people, perhaps most, were not really "scientific method" people. If they had a "method" there was often a faint smell of magic about their description of it. Sometimes, they would describe their discovery as an accident, as pure serendipity.

I no longer believe in the serendipity explanation. It simply doesn't fit the circumstances. The accidents should have happened to a larger number of people, not just to a small number of "serendipity-prone" analysts. I think it has to do with the way these people looked at the world, the way they perceived events around them.

Based upon my contact with a few of them, I believe that some of these serendipity-prones looked at the world around them in terms of

- a before,
- an after, and
- the event connecting them.

Given a certain "before" and "after" that were not the same, something "happened" at the connecting event. I think it may have been this way of looking at the events around them, that drew the attention of these serendipity-prones to the sites of their discoveries. Something did.

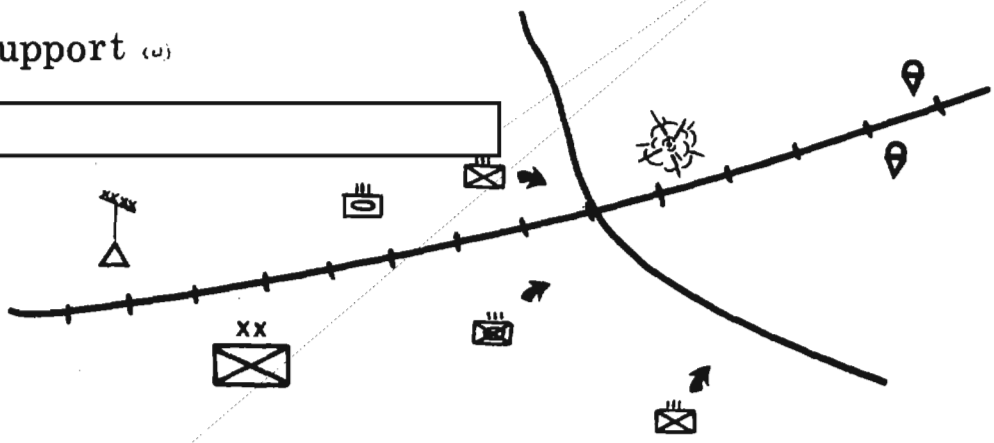
What do you think?

P.L. 86-36

DOCID: 4011945

Exercise Support (U)

by [redacted]



(C-CCO) NSA/CSS, in accordance with USSID 4, supports U.S. military exercises where COMINT is required. V42 (Current Applications Division) levies personnel to serve as SIGINT Reporter/Analysts for the exercises. Since January, 1981, A6 (Technical Support) has participated in the program. The author would like to express his appreciation to Michael F. [redacted] Chief V421, for his comments on the section concerning the recent exercise.

Introduction to Exercise SIGINT (U)

(U) All large military exercises are conducted on the basis of a scenario depicting some imaginary war situation, both to give the participants experience in coping with situations not encountered in peacetime and to evaluate the capabilities of commanders, staffs, troops, systems, and equipment to cope with such situations.

(U) In the course of the exercise, participants are given preplanned information about imaginary events in the scenario - what the enemy is doing, what casualties friendly forces have suffered, etc. - and are expected to respond to these "events" with orders, plans, and actions. Exercise controllers then assess the results of the players' actions, give the players appropriate feedback through simulated intelligence and operational reports, and devise subsequent problems for the players.

(U) Because players' actions are often unpredictable, the course of events can deviate considerably from the original script. Controllers are expected to be able to handle this "free play" and still keep to the key themes of the scenario.

(U) Maximum realism is sought, but realism will always be sacrificed to accomplish exercise objectives. For example, enemy capabilities are adjusted as required to provide the desired amount of challenge to the players, even to the point of wild implausibility if necessary. The war cannot be allowed to be won or lost prematurely; desperate battles must continue right up to the end of the exercise.

(U) Chaos and confusion are unavoidable features of real warfare. These qualities are also characteristic in the management of intricate exercise scenarios. The planned breakdowns and disruptions designed to test the players are compounded by unplanned breakdowns and disruptions inevitably suffered among the controllers and referees.

[redacted]

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

A Recent Exercise (U)

(U) Upon notification of the JRX, Captain [redacted] of V421 (Exercise Support Branch) was designated NSA/CSS project officer. He attended the initial planning conference at REDCOM Hq (McDill AFB) where all of the intelligence players were brought together and the strategic scenario was given.

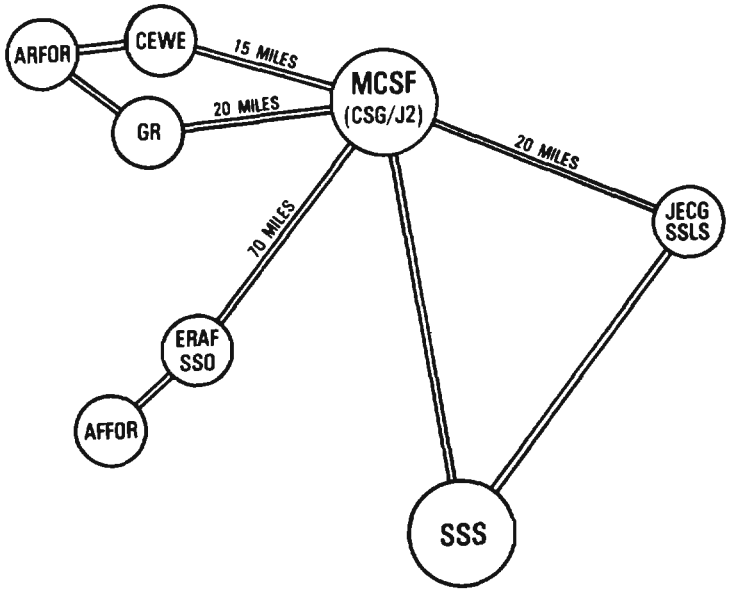
~~(C CCO)~~ CPT [redacted] then returned to NSA/CSS and began coordinating the SIGINT, personnel and logistic support for the exercise. Included in these support efforts were determining airlift requirements for NSA/CSS support personnel and arranging for accommodations and transportation at the exercise site. He also requested the necessary personnel support from A Group and communications support from DDT.

(U) The purpose of this JRX was to provide training for participating commanders, staffs and forces in joint air/ground operations involving air, armor, and mechanized forces.

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

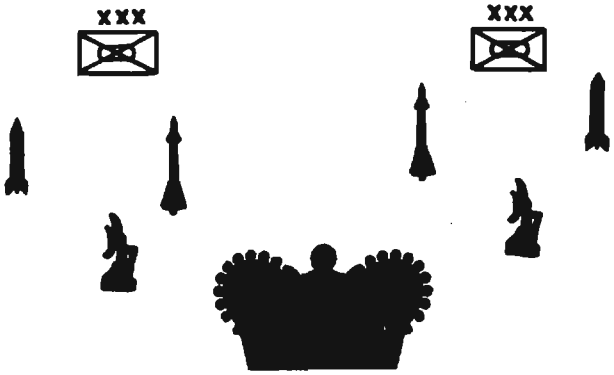
~~(S)~~ The exercise scenario depicted five



~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4011945

~~(C-CCO)~~ The Joint Exercise Control Group (JECG) was the Exercise Controller, and as such interjected stimuli into the exercise to which the players responded. The SIGINT Support Liaison Staff (V421) was part of the JECG.



~~(C-CCO)~~ The Cryptologic Support Group (CSG) and Intelligence Directorate (J2) were co-located and were provided SIGINT inputs via the Mobile Cryptologic Support Facility (MCSF), which is a GM motor home that houses the most modern computer and communications equipment. The MCSF belong to NSA/CSS.

(U) The CSG is a group provided by NSA/CSS to facilitate SIGINT Support to a unified or specified command, joint task force commander or other commanders.

~~(C-CCO)~~ The Consolidated SIGINT Support

~~(C-CCO)~~ The SIGINT Support Staff (SSS) generated the SIGINT support for the exercise.

~~(C-CCO)~~ Upon conclusion of a JRX, a brief critique session is normally held; in the exercise from four to 20 people should have participated, but, in actuality, only the NSA/CSS personnel attended. P.L. 86-36

~~(S)~~ CPT said that the After Action Report which REDCOM would submit to the JCS would probably conclude that the JRX achieved its objectives primarily because logistics and air defense objectives were met.

~~(S)~~ CPT however, doubts the value of the exercise as a realistic simulation for the following reasons:

P.L. 86-36
EO 1.4.(c)

(U) As to the success of SSS in support of the exercise, one can only conclude that exercise support objectives were partially met.

DOCID: 4011945

P.L. 86-36
EO 1.4.(c)

Transcriber Reactions
to Program Participation (U)

(U) Although the opinions varied among the transcribers participating in the various exercises, there were many areas of general agreement. Most of the transcribers thought the experience worthwhile in that they saw how the Agency fits into the SIGINT community, i.e., into "the big picture." Most thought they had gained from the experience, either professionally by a greater understanding of the SIGINT system and an increase in target knowledge, or financially by the overtime.

(U) At the time of A6's entry into the program, transcribers suffered from poorly organized pre-exercise briefings, little working aid familiarization, instructions that were wrong or incomplete or too rapidly given, and disorganized source materials. One transcriber noted that the standard was to be uninformed. The various staffs, however, are correcting these shortcomings on a continuing basis.

(U) Transcribers are left with a more complete view of current operations and a more complete understanding of the assorted and sanitized reports that exist in the intelligence community.

~~(C-CCO)~~ There was general agreement among the participating transcribers on two points:

- Exercise scenarios should be provided with sufficient time for perusal;
- Personnel should be carefully selected to insure that the individual has the proper background.

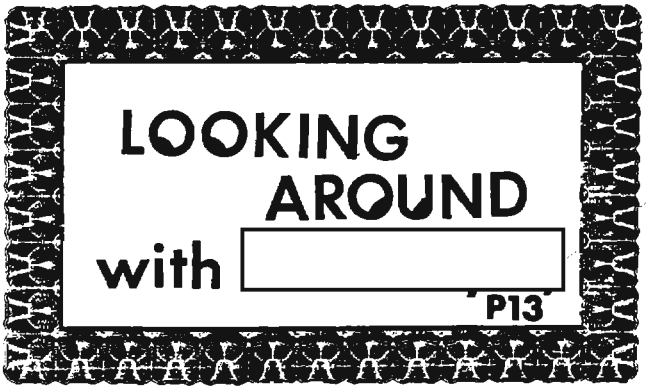
Otherwise, the individual may be inundated with a mass of incomprehensible data and given no time to decipher it. Some military knowledge is requisite.

DOCID: 4011945

The 1981 URSI XX General Assembly (U)

[redacted] recently attended the 1981 URSI Meeting, and his report offers some unsettling projections about the problems that SIGINT will face over the next one or two decades. This is an extract from the Introduction and Conclusions of that report.

P.L. 86-36



The 1981 URSI (International Radio Science Union) meeting was held in Washington, D.C. 10-19 August, 1981. The international meeting is held (U) every three years, and this was the first time in several decades that it occurred in the U.S.

(U) Because the meeting is prestigious, the authors and national radio science organizations make an effort to publish significant work. About 500 technical papers were given, covering almost every aspect of radio theory, including optical fiber, computer design, instrumentation, remote sensing, and biological effects of radio on humans, as well as the more conventional areas of propagation, noise, radio astronomy, microwave power, satellites, and telecommunications.

(U) The authorship, as well as the attendance, was very international. The meeting organizers reported that 1056 people registered, from 38 different countries. About half of the audience was from the USA. Japan, France, Germany, and the UK also had large contingents of 50 to 70 attendees. Six people came from the USSR, including some authors. 269 of the papers had foreign authors, although in some technical areas, nearly all the authors were from the USA.

~~(C-CCO)~~ There are some interesting parallels between SIGINT and radio science, viz:

1. Both activities deal with radio in a very broad way.
2. Both are concerned with quasi-repetitious phenomena, which they cannot control, as well as with unique or very random phenomena which give one-time capture opportunities.
3. Both have to develop unique apparatus and unique processes to obtain data and to extract information from these data, so they are both concerned with device engineering and measurement techniques.
4. The volumes and bandwidths of data are often very large, and the "explanations" tentative.

~~(C-CCO)~~ In general, the radio scientists [redacted] understanding the physical phenomena of radio, communications, and instrumentation. Their discoveries and measurements have, over many years, opened up new areas of the spectrum for radio applications, and improved instruments. They have also shown basic physical limitations to uses of radio, e.g., the effects of

EO 1.4.(c)
P.L. 86-36

DOCID: 4011945

water vapor on short radio waves, air turbulence on laser beams, and the effects of noise on receiving systems.

~~(C-CCO)~~ The telecommunications planners and designers in many countries pay attention to the findings of radio science in the operation and particularly the development of their systems and equipment.

~~(S-CCO)~~ One thread of technical information from the URSI meeting will illustrate this point. Developments in optics have shown that great improvements in cost, performance, and lifespan of semiconductor lasers are possible, with lifetimes of 100,000 hours confidently predicted, and million hour lifetime thought possible. The fibers themselves are getting better with bandwidths of several GHz, and for certain new fibers, hundreds of GHz capacity are expected. From this progress, the CCITT (International Consultative Committee on Telephone and Telegraph) is now developing standards for worldwide compatibility between the parameters of all public carrier optical fibers, so the optical fiber nets can interface. According to a French consultant, the Europeans look upon satellites as a temporary measure for regional communications (TELECOM 1) and will shift all main line transmission to optical fiber links across Europe as fast as they can lay in the trunks, with the satellites reserved for mobile and other light services. At the same time, studies of the physical characteristics of optical components indicate to other Europeans researchers that the local networks cannot use optical fiber to carry 50 CATV signals in a bus, so they expect to go to a switched optical fiber network to replace the existing copper wire local plant with an individual fiber from a switch to each subscriber. This network would be expected to serve for 50 years after installation.

Analysis (U)

(U) Some of the major developments in communications have stemmed from advances in materials and the invention of devices. The electric telegraph of 150 years ago resulted from the purification of copper so that circuit losses were reduced to low enough levels to make generators, relay windings, and telegraph lines feasible. The semiconductor explosion came from improvements in the materials of semi-metals, and the current work in improving glass and optical devices seems to be setting the stage for a major revolution in switched communications.

(U) A recent survey of telecommunications in the Economist, 22 August 1981, notes the progress in optical fiber systems which surprised even AT&T and the BPO (British Post Office). Over the next decade, the world will spend 640 billion dollars on telecommunications equipment (according to an A. D. Little study), and radio will be a significant part of that. As optical fiber trunks take over the main line transmission loads, and even spread into the local networks, the radio frequencies will be applied to mobile radio, satellite service (expected to exceed 700,000 Intelsat circuits by 2000, plus even greater domestic satellite capacity), and many services where wires or light guides are impossible or impractical.

(U) One of the notable features of the URSI is the close interaction between devices, materials, and radio technology. Remote sensing depends on microcircuitry, super computers, models and devices to compensate for atmospheric distortion, propagation theory, antennas, and so on. Spread spectrum or radar signals to combat radio interference, noise or propagation effects depend on superspeed equalizing digital processors, electro-acoustic analog convolvers (waveform comparers), and high bit rate key generators, etc. Even efficient and accurate television transmission depends on sophicsticated signal processing technology, e.g., SAW PAL filters that are used in hundreds of thousands of TV receivers to overcome adjacent channel interference.

Conclusions (U)

(U) Developments in radio science bring about a large number of gradual improvements in the big telecommunications systems, as well as initiating some radical changes. Both kinds of change accumulate to bring complete

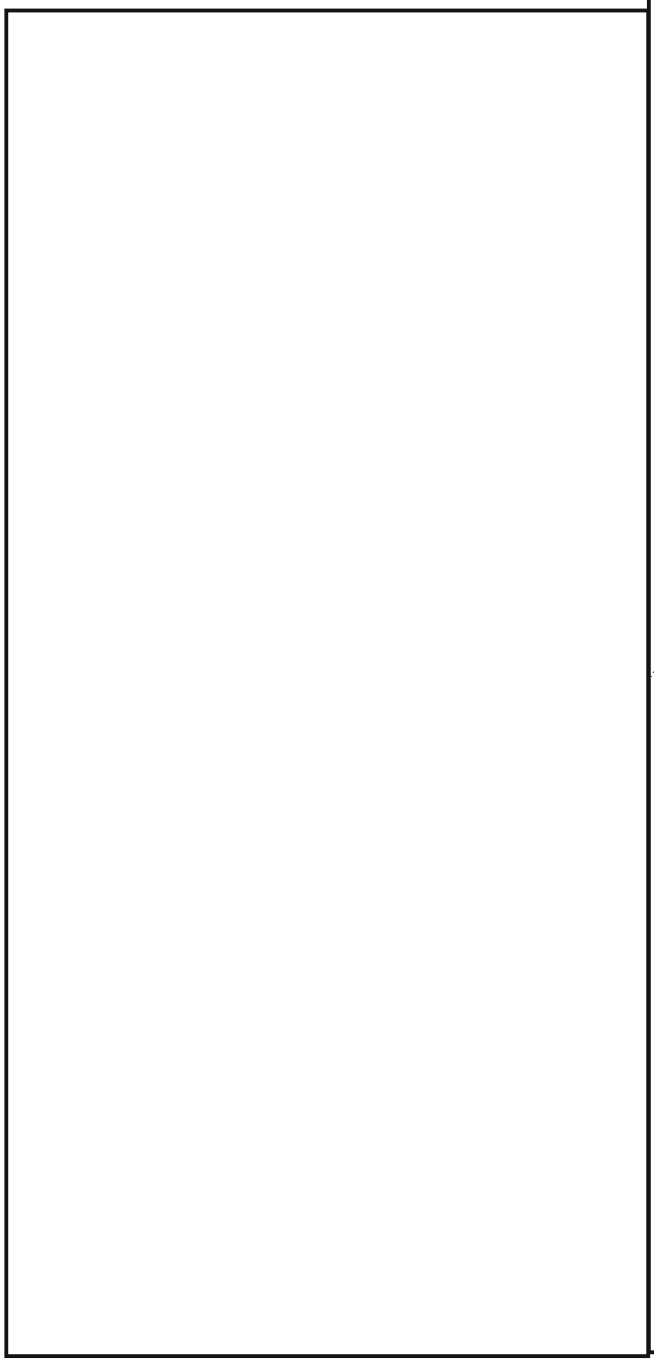
EO 1.4.(c)
P.L. 86-36

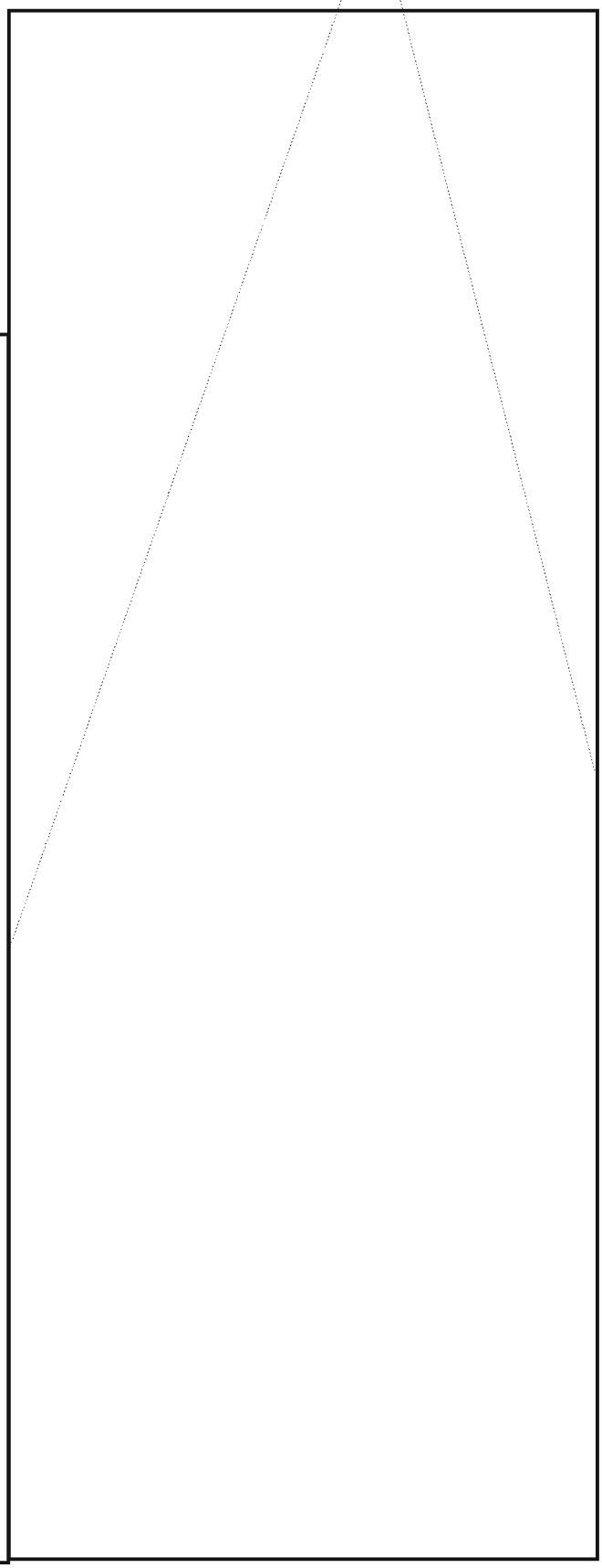
DOCID: 4011945

EO 1.4.(c)
P.L. 86-36

transformations in the way telecommunications operate and affect things.

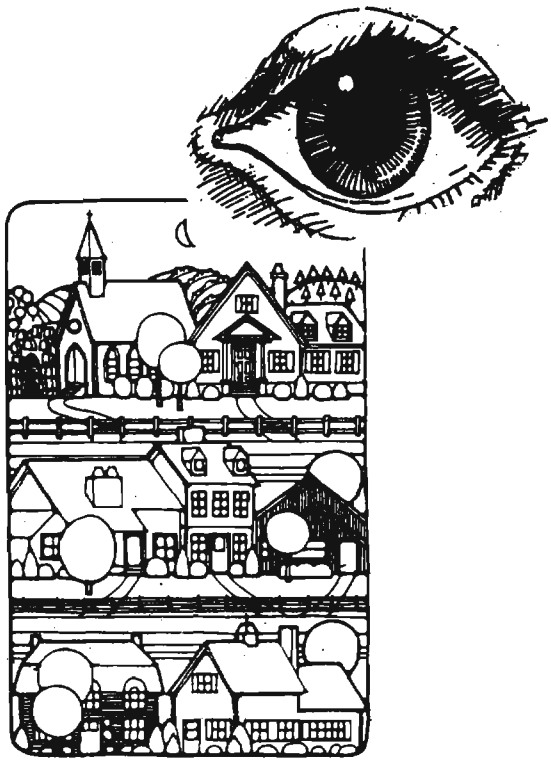
(U) The main impact of radio and optic developments will be in transmission, where a generation of technology lasts about 15 years. The effect on switching, where technology life cycles are about 30 years, will be delayed until the 1990's, after the current commitments to digital electronic switching are fulfilled.





DOCID: 4011945

by E. Leigh Sawyer, B4



SLEEP WELL! YOUR SDO IS ON DUTY!

(U) I seem to detect a growing trend for people to rummage around in their cryptologic attics to describe certain events or occasions taking place in the olden days. Doing a little rummaging on my own, I recalled a long-abandoned function once carried out by company grade officers identified, as they popped up periodically on the master roster, as "SECURITY DUTY OFFICERS" (SDO). This system was in its heyday in the early 1950's. At that time, AFSA (soon to be NSA) was split between the Naval Security Station at Nebraska Avenue and Arlington Hall Station. As a digression, this split had its interesting features too -- like the time I drove my car from NSS to AHS during the day and took the shuttle bus back. At quitting time, I naturally couldn't find my car in the NSS parking lot and was at the point of reporting a stolen car case to SEC when I realized what I had done. I managed to catch the last shuttle back to AHS by the skin of my teeth. Ah, those were the days! Well anyhow, back to this SDO system. It was used at NSS (whether it was used at AHS escapes me). In any case, it was a so-called "sleep watch." For this purpose, a cot was located in SEC spaces so that the SDO could catch some sleep between his late evening and early morning rounds of all the AFSA spaces.

(U) A word or two about the cot might be in order. The mattress was obviously not configured for sleeping purposes. What it was stuffed with must remain somewhat problematical, but I suspect it was a mixture of corn cobs and pine cones. I wonder if somewhere in the archives there still exist the logs maintained by the SDO's. References to that mattress were rife in these logs, e.g., "after the worst night of my life", "started my morning round with every bone in my body screaming agonized protests", "millions for a new building at Meade; why can't SEC provide a decent mattress?" and "even my teeth hurt."

(U) It should not require too much imagination to determine that periodic one night stands of this sort were mighty boring. So

DOCID: 4011945

what do you do to lessen the boredom? Drink coffee, of course. Unfortunately, there was not a hint of either coffee or coffee-making paraphernalia discernible in the SEC spaces. This led to a preliminary round of visits to adjacent spaces to locate a coffee mess, relocate the pot and can of coffee to SEC spaces, and return them carefully in the early morning hours. After all, "nothing's too good for the boys in the Service." This system was not without its pitfalls. Like the Navy lieutenant, whose name is no longer retrievable from my data base, who had a memory lapse and couldn't remember the office from which he made the "borrow." He handled the situation neatly, however, with the following entry in the log: "Coffee pot and can of coffee found adrift in Building 18."

(U) It was somewhat rankling that SEC, which conceived this Security Duty Officer concept in the first place, couldn't provide a little lousy coffee for us. I recall roaming around the SEC spaces one evening surveying all the possible places where they might hide their coffee and equipment. The survey narrowed down to one small cabinet locked with a brand new shiny Sargent and Greenleaf combination padlock. The cabinet had undeniable coffee stains on top and was so decrepit that forced entry would have probably taken about 15 seconds. I reasoned that a rickety cabinet of this sort certainly wouldn't be used for anything classified. So why the formidable padlock? "You don't suppose", I mused to myself. I then proceeded to dial 10-20-30, the factory-set combination. EUREKA! It opened. When I opened the door, I beheld a complete coffee mess. It was not exactly as though I was discovering the tomb of Tutankhamen, but the sensation was somewhat the same. I shared this revelation with a few of my friends who were also obliged to stand SDO duty. But, alas, the SEC coffee mess vice president must have discerned that the coffee level was dropping far faster than it should. Accordingly, it was not too long after my initial discovery that 10-20-30 no longer worked.

(U) The real psychic bennies for the security watch types were in the form of finding classified materials "adrift." As a result, there was no doubt in my mind that we were looked upon as pests by the various organizations making up our beat. For that reason, access doors to the various operational spaces were generally kept locked to keep us (and incidentally others) out. This meant that the Security Duty Officer most often was limited to walking along murky corridors in the various buildings used by AFSA in the NSS compound. However, on one occasion, circa 1952, I found one of the doors open to an R/D area. Oh man, the fox was really in the hen house! After I had spent a good deal of time going through every nook and cranny where something classified might be lurking, I finally was rewarded -- a classified manual (CONFIDENTIAL). I recall that I thumbed through it and, in retrospect, imagine if it had been tossed over the fence into the Russian Embassy compound, they would probably have thrown it back out. However, it was marked CONFIDENTIAL and that made it fair game. As best as I could determine, the owner of the bookcase was identifiable by the name plate on the nearby desk. So I wrote it up dutifully noting the name of the responsible person:

DR. LOUIS W. TORDELLA

~~(C)~~ As luck would have it, Dr. Lou was soon after reassigned to the Plans and Policy Division, where I worked, to spearhead a highly innovative experiment called "Third Party". I confessed to him that I was the culprit who gigged him and expressed the hope that I had not set him back in his career in some fashion.

(U) So much for the SDO system. It went the same way as smudged carbon copies of TECHSUMs, A and B buildings, AFSA-062 and AFSA-063, and red phones.

Ou sont les neiges d'antan?

DOCID: 4011945

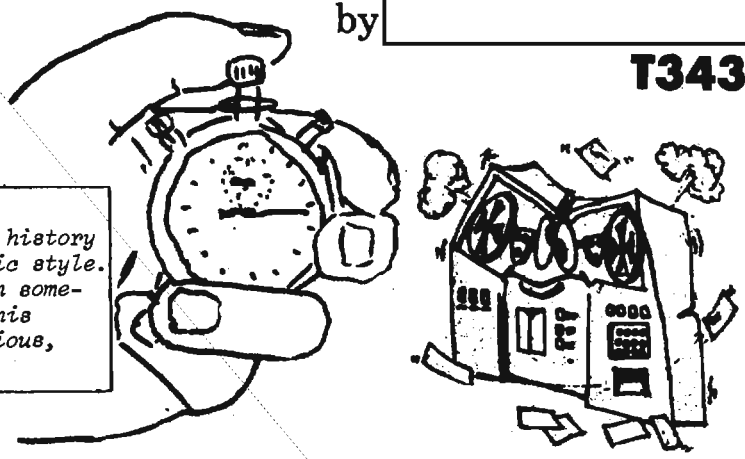
EO 1.4.(c)
P.L. 86-36

P.L. 86-36

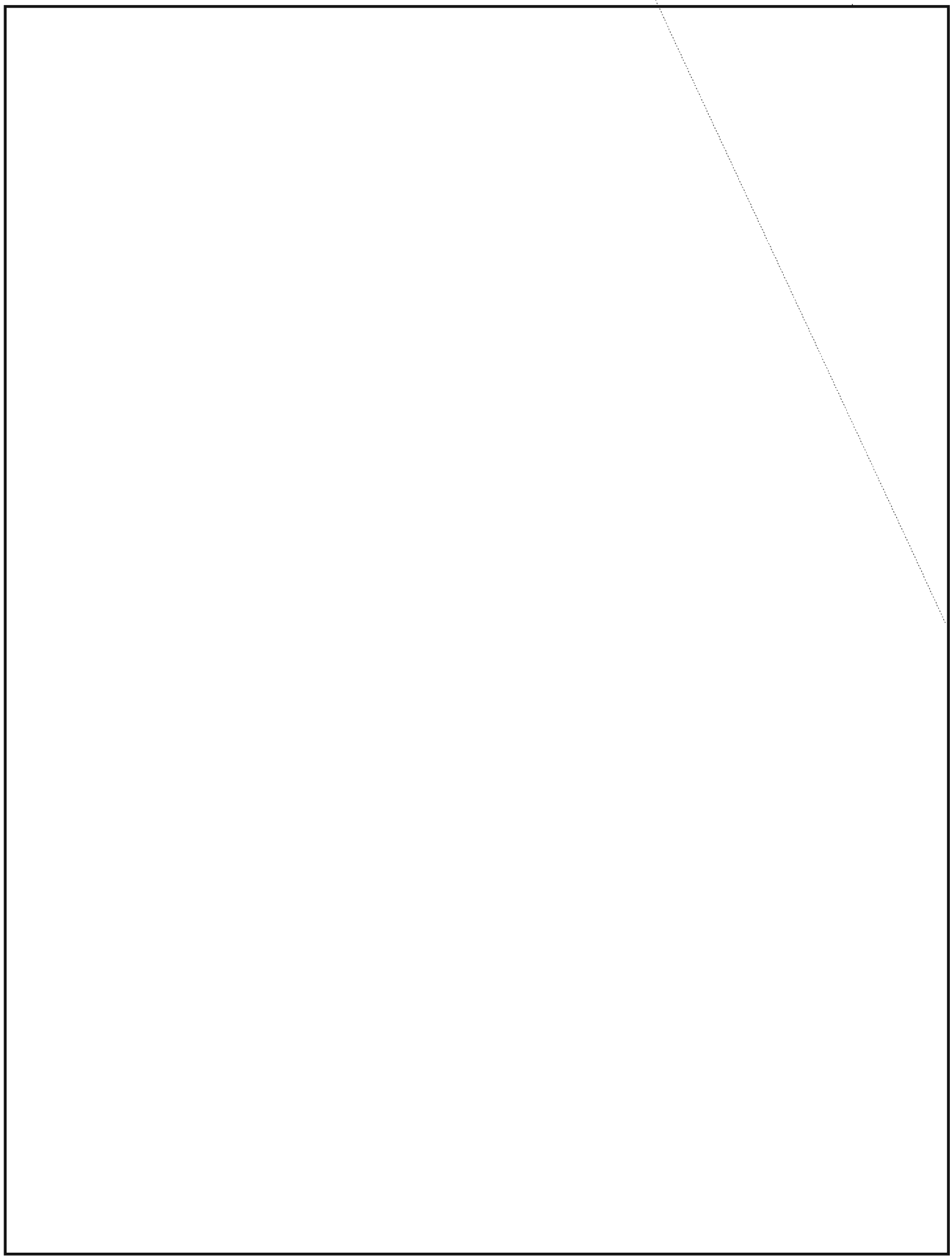
TIDE: A Brief History

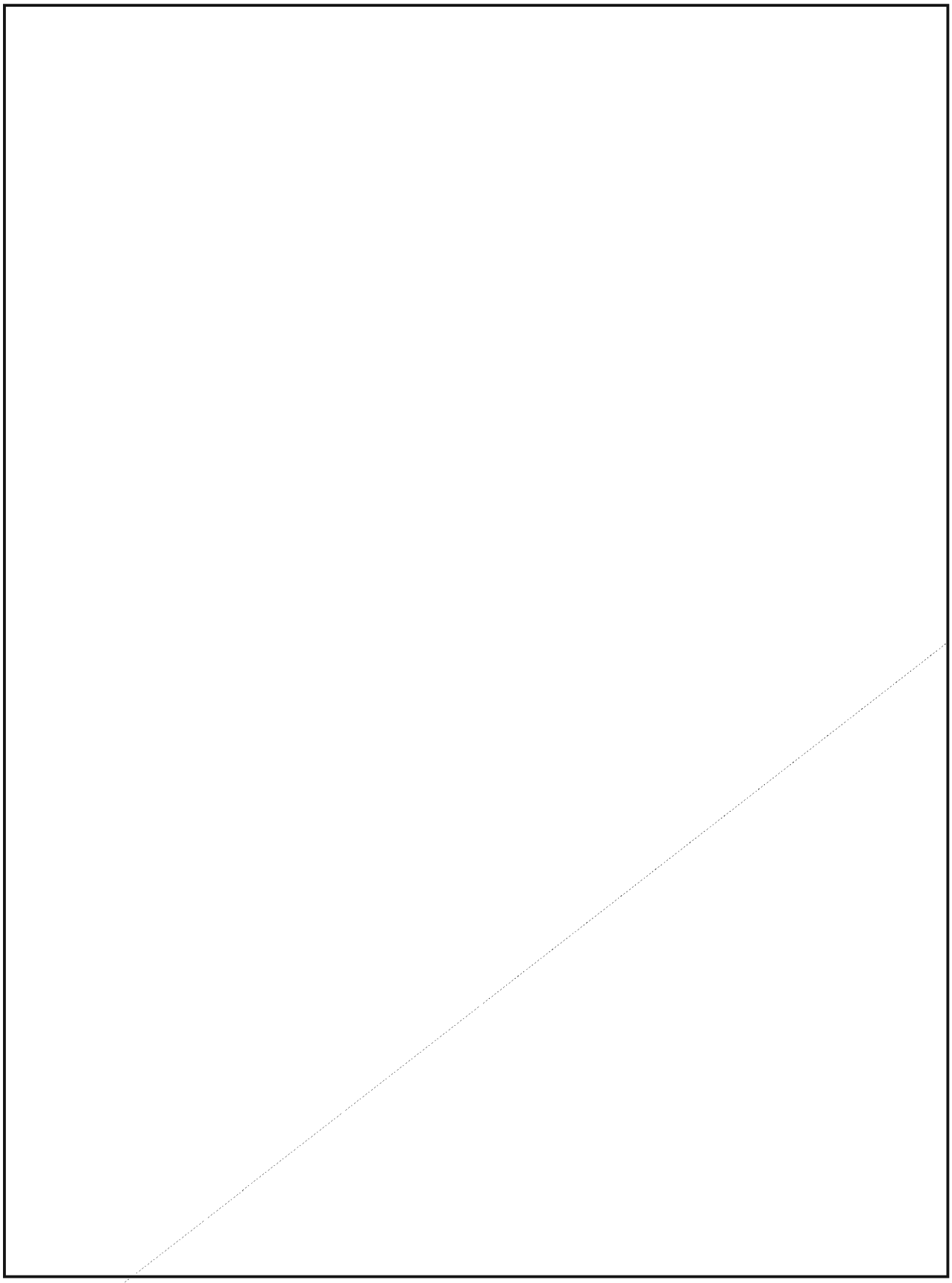
by [redacted]

T343



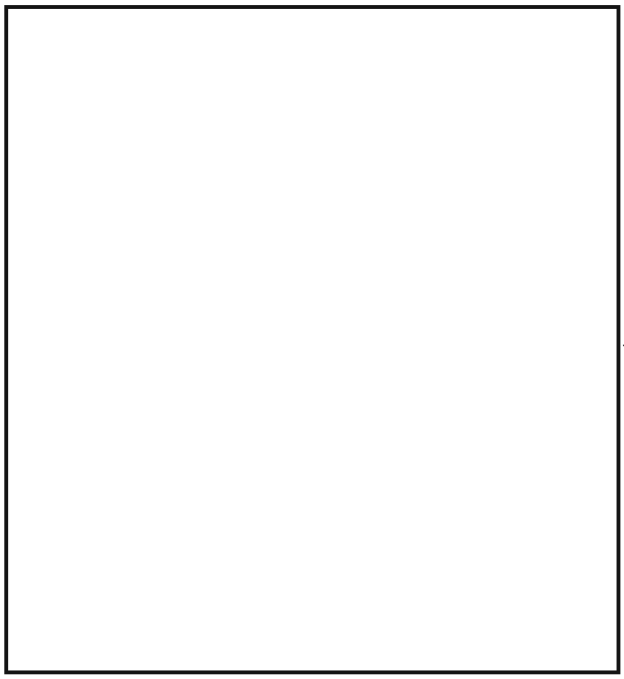
Author's Note:
Too often in our business, a project's history is written in a cold, hard, bureaucratic style. In this paper, I attempt to describe in somewhat human terms the story of one of this agency's more successful, albeit vexatious, computer systems.





EO 1.4.(c)
P.L. 86-36

DOCID: 4011945



Relief at Last (U)

(U) Thereafter in rapid succession over the summer of 1981, more TIDE processing systems were accepted by PREFACE thereby providing additional TIDE relief and yes, some well deserved rest.

(U) Although some disruptions and minimizations still occur on TIDE, they are infrequent (in comparison to previous events) and are primarily caused by hardware and/or software failures - not solely loading demands. TIDE is looking forward to retirement.

The Future (U)

(U) Once TIDE is finally relieved of its remaining terminal responsibilities (e.g. high speed printers, CRTs, etc.) a full decade since its creation, it can be unplugged. Because the soul of any computer system is its software, what was once called TIDE will remain only two antiquated 1965-vintage UNIVAC 494s. These machines will be returned to their Mid-West Minneapolis birthplace, be reconditioned, and, if lucky, enter a retirement of loving care by high school or college students.

(U) To sum up our experience - this Agency's use of TIDE has not been an easy one. Many of those associated with TIDE, however, believe that the processing crises and sleepless nights were worth the achievements this system has somehow performed. It is believed that TIDE produced far beyond its expectations, and many believe the feats it performed, and the people who have made it possible to simply "maintain" for such a period of time, should be commended.

(U) However, no matter what its history, TIDE was simply a little imaginative software, two machines, and an assortment of peripheral equipment. When it failed to respond to a crisis or an analyst was unable to retrieve important intelligence, it simply became a useless tangle of wires.

CRYPTIC CROSSWORD SOLUTION, November 1981

EO 1.4.(c)
PL 86-36

Across

1. PARSNIPS (par + s + nips)
5. ARMPIT
9. COUPLETS (double definition)
10. SONORA (son + or + a)
12. EATS (anag.)
13. STOAT (orders to attack)
14. PUNT (top untied)
17. DEMONSTRATOR (demon's tractor - c)
20. MELODRAMATIC (anag.)
23. RARE (double definition)
24. SEALS (less + a; anag.)
25. FUZZ (double definition)
28. LEGEND (leg + end)
29. CLERICAL (cleric + la reversed)
30. ANTHEM (ant + hem)
31. ANACONDA (Dana anag. + a + con)

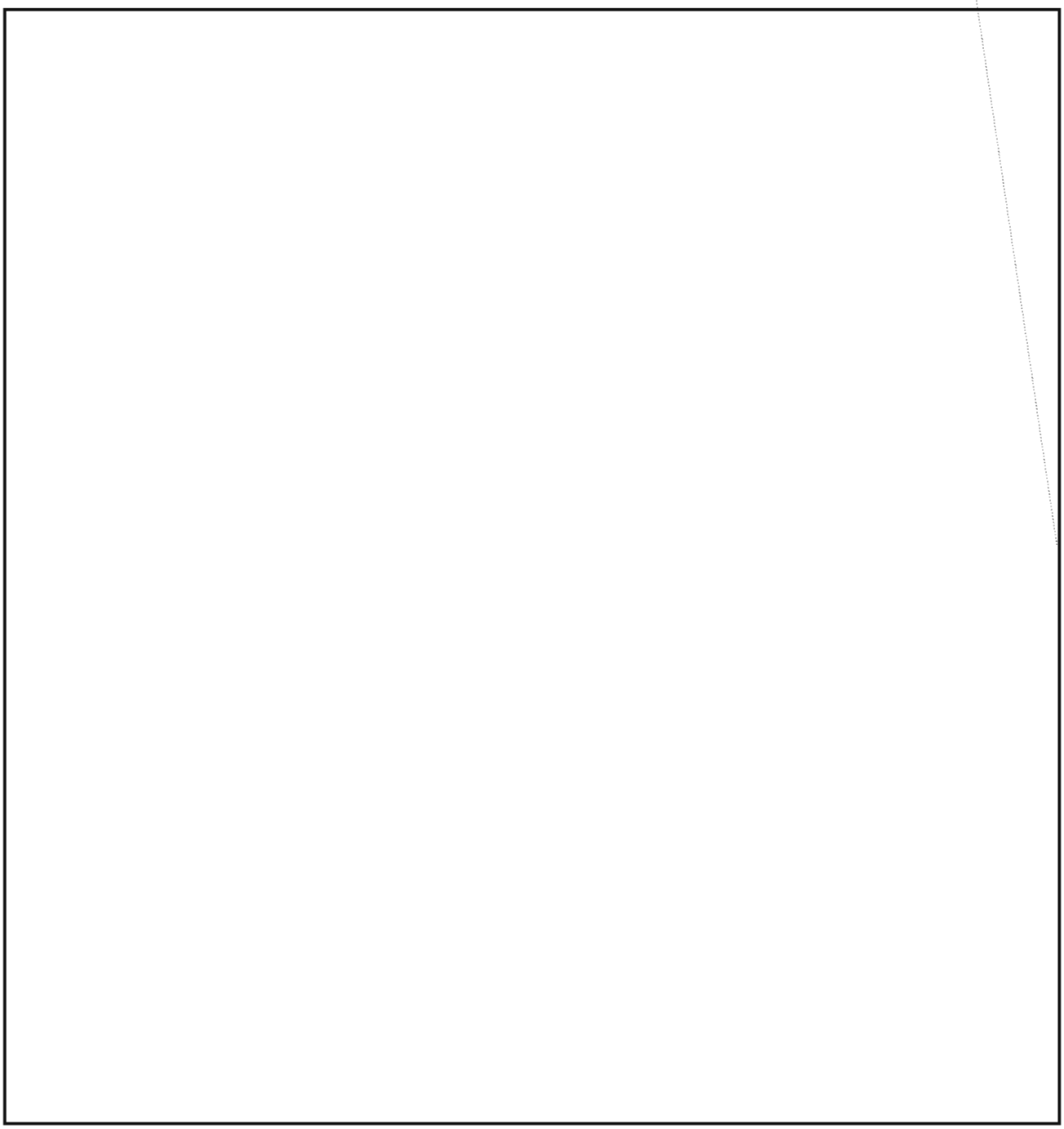
Down

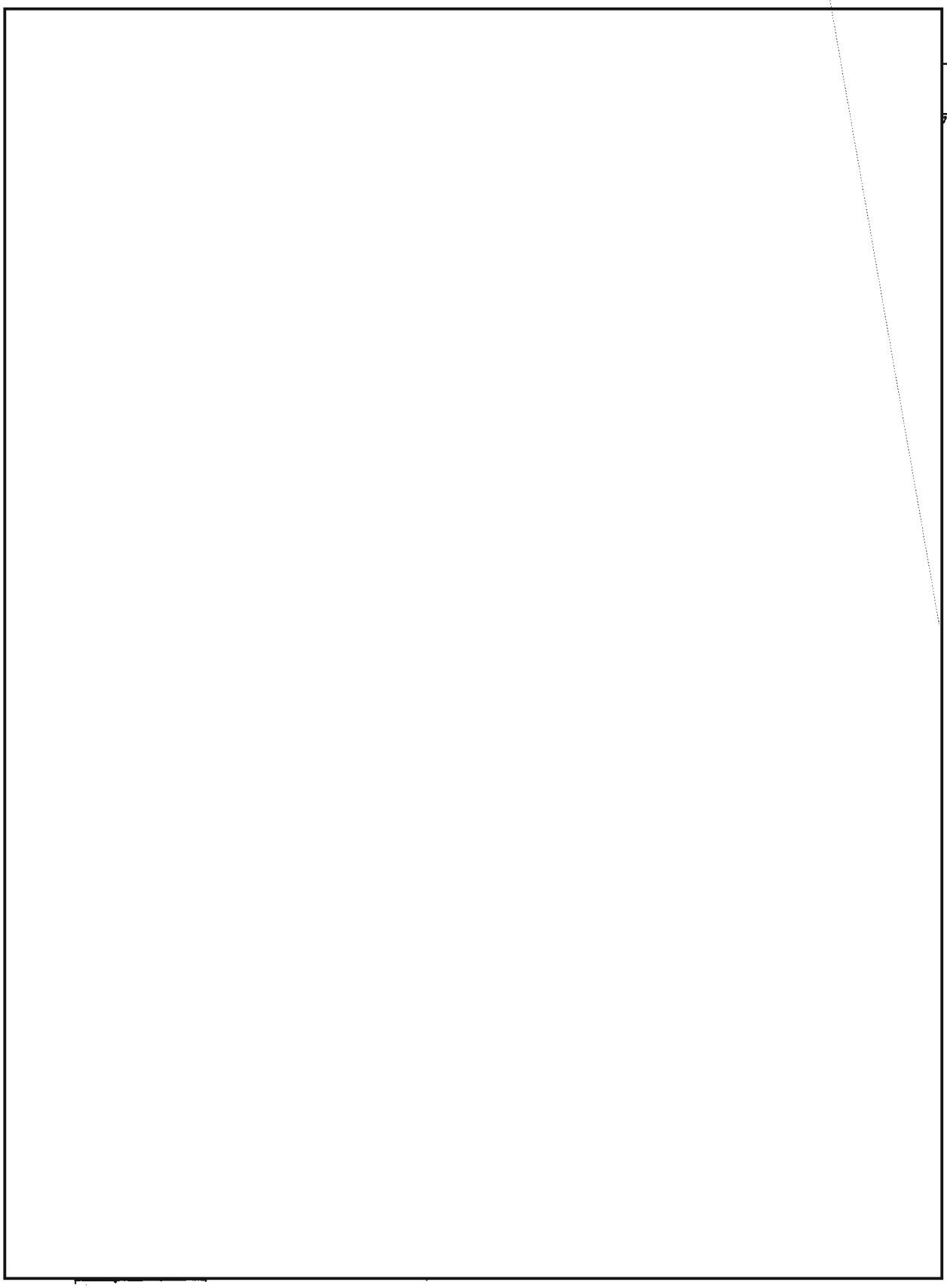
1. PICKET (double definition)
2. ROUSTS (r + ousts)
3. NILE (anag.)
4. PETITION ANEW (anag.)
6. MOOR (reverse spelling)
7. PRODUCTS (pro + ducts)
8. TRAITORS (anag.)
11. MARSHALL PLAN (marshal + l + scheme)
15. READS (pun for reeds)
16. DRAIN (D + rain)
18. UMBRELLA (anag.)
19. ALL RIGHT (everyone + not left)
21. VULCANIZE (Vulcan + ize)
22. AZALEA (as + a + lea)
26. ONCE (induction center)
27. ERIC (Japanese rickshaw)

NSA-Crostic No. 36

Two recent tragic accidents .... add up to an eerie coincidence

P.L. 86-36





DOCID: 4011945

~~FOR OFFICIAL USE ONLY~~

In Pursuit Of:

Faster Horses

YOUNGER WOMEN

Older Whiskey, and

MORE MONEY(U)

by [redacted] P14

P.L. 86-36

For the past two years I have been involved with a project that has given me more, in terms of psychic income and pure excitement, than perhaps any work-related activity (U) that I remember. When you feel this good about something it seems natural to want to tell everyone else and share the excitement. Sort of a "look what I found" feeling. Of course, when you feel excited about something, it is difficult to know whether or not you have something worth saying and can remain objective about it. Nothing makes you feel quite as foolish as discovering the wheel only to find out that you were the only one who didn't have one all along.

(U) I've followed -- from a distance -- the articles, letters, and symposiums decrying the diminishing number of analysts, the dilution of the career field, and the increasing work load. I really have nothing to add to the body of literature that has grown around those themes. I would like to note that some reasonably intelligent people have advanced them. Conversely, some reasonably intelligent people made the decisions that led to the described conditions.

(U) Having resisted the urge to vent my excitement on paper for this long, I thought I had it under control. Actually, I have been writing this piece all along. Part of my control mechanism was simply typing my thoughts on the screen and then hitting the delete button. That may happen to this version and you will be spared once again. I'll tell you what "set me off" this time a bit later. First, let me tell you what I've been so enamored with.

(U) I'm a Traffic Analyst. Several years ago I began to work for the person I respect most in that field and share in the development of what has come to be called a Traffic Analysis Workbench System. What ever comes of that effort, I'll always be grateful for being included.

~~(FOUO)~~ The idea is a relatively simple one: In terms of technology, the TA field is, and has always been, behind the power curve. Regardless of what high powered machines exist, and in spite of the fact that some extremely sophisticated machine applications have been designed for analytic purposes, the analyst is still behind. There are several reasons this situation exists. However, it is primarily because analysts are directly

~~FOR OFFICIAL USE ONLY~~

DOCID: 4011945

dependent upon their machine support personnel. A few have managed (mostly out of frustration) to learn one computer system or another and support themselves. The problem with this is, if they were any good at it, they were usually lost from the field.

~~(C)~~ It's time the analyst was given some help. Not to catch up to technology, just to keep from getting further behind. Given the costing cycle, the procurement cycle, and the installation cycle, I'm convinced that catching up is not possible. Not possible! The concept of a TA workbench involves installing a terminal on the analyst's desk. Read that again! On the analyst's desk. Not down the hall in a "machine room", not in a corner of the basement, and not around the corner where it "won't bother anyone"; on the analyst's desk, the one they sit at.

This puts the analyst in a position to access the major data bases, where the daily traffic as well as the technical working aids, reside (hide is a better word). With the terminals on their desks, they will have constant access to their material and perhaps approach the paperless environment.

~~(FOUO)~~ Under the umbrella called PINSETTER, we have been proceeding along a development path that will hopefully lead to the kind of help the analyst needs. Because the most precious computer resource is the programmer, the analyst must be released from depending on him for every minor need. This is true for several reasons. First, the analyst needs to be able to access his data, process that data, and change those processes without having to write memos, generate specifications, write justifications, wait for software and then participate in debugging. Second, the programmer, as a resource is too valuable to be tied up with changing sort specifications every time an analyst needs a different output. Lastly, the plain facts are that we have a terrible time retaining good programmers. No sooner do we develop a good working relationship with a top-notch programmer, and he begins to understand something about an analyst's job, than along comes a better offer and he's gone.

(U) From a machine standpoint, meeting these goals requires a system that is easy to learn, flexible, and provides a reasonable response time. By "reasonable", I don't mean instantaneous. Most analysts can live with an execution time that is not measured in nanoseconds. Most of our work has taken place on a PDP-11/70 host using UNIX as the operating system. UNIX is a high level language that was developed by Bell Laboratories. It meets the above criteria plus it is very forgiving to a klutz at the wheel.

~~(C)~~ We have found that most of the processes that a Traffic Analyst needs to be able to do can be accommodated with the UNIX package. Where it was found lacking or inefficient, the solution has been provided by a unique working relationship with a small group of highly talented programmers in T333. The

(U) To digress for a moment, the realization that certain processes are simply too big for TSS applications is important to maintaining a proper perspective. This determination must be made, and large "number crunching" must be performed where they are most efficiently handled. However, the process can often be executed where most efficient, and the results passed to where they can be best used, on the TSS. I might add, in two years of handling TA processing, it has been necessary to "send out" only one job for actual execution on a "big" machine. Of course, many of our extracts from major data bases are "preprocessed", prior to transfer, to make them more TSS friendly. But I discount this, since it is largely "invisible" to the requestor.

~~(FOUO)~~ If the solution were apt to provide a useful "UNIX-extension", we would request T333 help. The results have been the most rewarding part of this experience: generalized UNIX-like utilities that solve analytic processing problems. The big plus? anyone who

EO 1.4.(c)
P.L. 86-36

knows a little UNIX can use them. On the other hand, if the solution appeared to be problem specific, we would attack the problem with our own resources. The results of these efforts have proven equally rewarding. Based on our own experience and some operational testing in analytic elements of A3, B2, B5, G6, and G9; I'm not sure if a more effective analytic tool than UNIX could have been designed if that had been Bell's intent. This leads to a philosophical difference in user support design.

~~(FOUO)~~ There is a mask-and-menu school of thought that holds to the belief that the user should be led through the processing cycle by the software. A menu is presented with a few options to select from and a mask provided through which to make alterations. These M&M's believe it is best to protect the user from the complexities of the system and protect the system from the klutz at the wheel. It has a place. I would look to this area for the type of handling necessary for, perhaps, TEXTA updates.

(U) Another approach is to provide the user with the modules necessary to manipulate the data, a high level language to package the modules, and the ability to communicate with other users and peripherals such as high quality printers. Basically, a sort of Procedural Applications Language that is not unique to Traffic Analysis. Perhaps a Universal Procedural Applications Language approach. The user is free to design personal processes and, more importantly, change those processes at will. Users are not dependent upon the programmer for every minor modification, routines do not have to be recompiled after each change, and the results of the changes are immediate. I believe UNIX meets this challenge.

(U) The M&M approach keeps the analyst (or user) dependent upon the programmer for modifications. Thus, preserving the problem of too much demand being placed on a resource that is already over taxed. The solution to the demand for software packages has all too often been the letting of contracts, at considerable expense, to develop processes that a few analysts, skilled in a handler like UNIX, might be able to get along without.

(U) If our own resources were concentrated in a manner conducive to the development of generalized handlers (a Universal Procedural Applications Language), and perhaps a bit of that contract money concentrated into rewarding the good programmers we have left, we might be able to come up with better analysts and better programmers. As a by-product, we might be able to handle the workload with the number of analysts we have and do a better job of it.

(U) So, what was it that set me off this time? A few days ago, while demonstrating a few system capabilities to a potential user, I was walking through the steps of a UNIX shell file (merely a collection of UNIX commands that execute sequentially and perform some process) and he asked me if I "wrote this program". The words startled me. Wrote a "program"? Me? I'm a Traffic Analyst, I can't "program". My rather bumbling answer was something to the effect that this is really not a program just a collection of instructions to perform a certain process on this computer. After he left I put the shell on the screen and read it a few times. By gosh, a few years ago I would have called that mess a program myself. It "looks" like a program. It "acts" like a program. And, my extemporaneous answer wasn't too bad a definition of a program.

~~(C-CCO)~~ I had to pause and reflect a bit. I put that shell together in about five minutes. What does it do?

[redacted]

Based on past experience in trying get a process to do a select of this nature, and going through the "channels" to get it; this "quickie" shell seems fairly powerful.

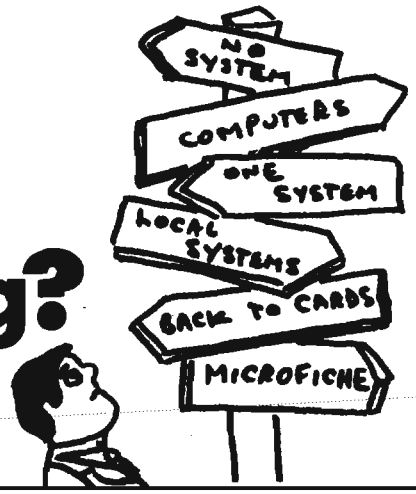
[redacted]

(U) I think I've found a faster horse, I probably couldn't keep up with younger women anyway, and I'd rather have a cold beer than older whiskey, so if anyone knows someone looking for a "programmer", I'll settle for two of four.

DOCID: 4011945

TEXTA

What is it? Where is it going?



by [redacted] P1

P.L. 86-36

TEXTA means Technical Extracts from Traffic Analysis, and represents an agreement between four national centers concerning -

(S)

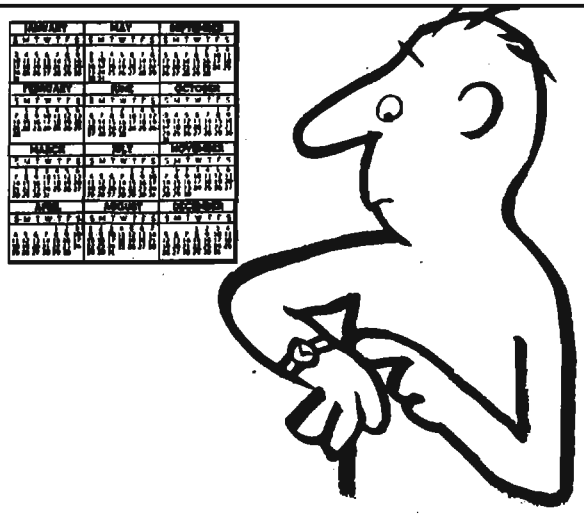
- the exchange of basic traffic analytic information;
- the sharing of a common, uniform recording and labeling system of traffic analysis information about COMINT targets worldwide;
- a common book of rules, the TEXTA manual, which the four centers accept as the authoritative description of how the TEXTA system operates;
- the highest, most accurate level of knowledge on a target communication.

[redacted]

EO 1.4.(c)
P.L. 86-36

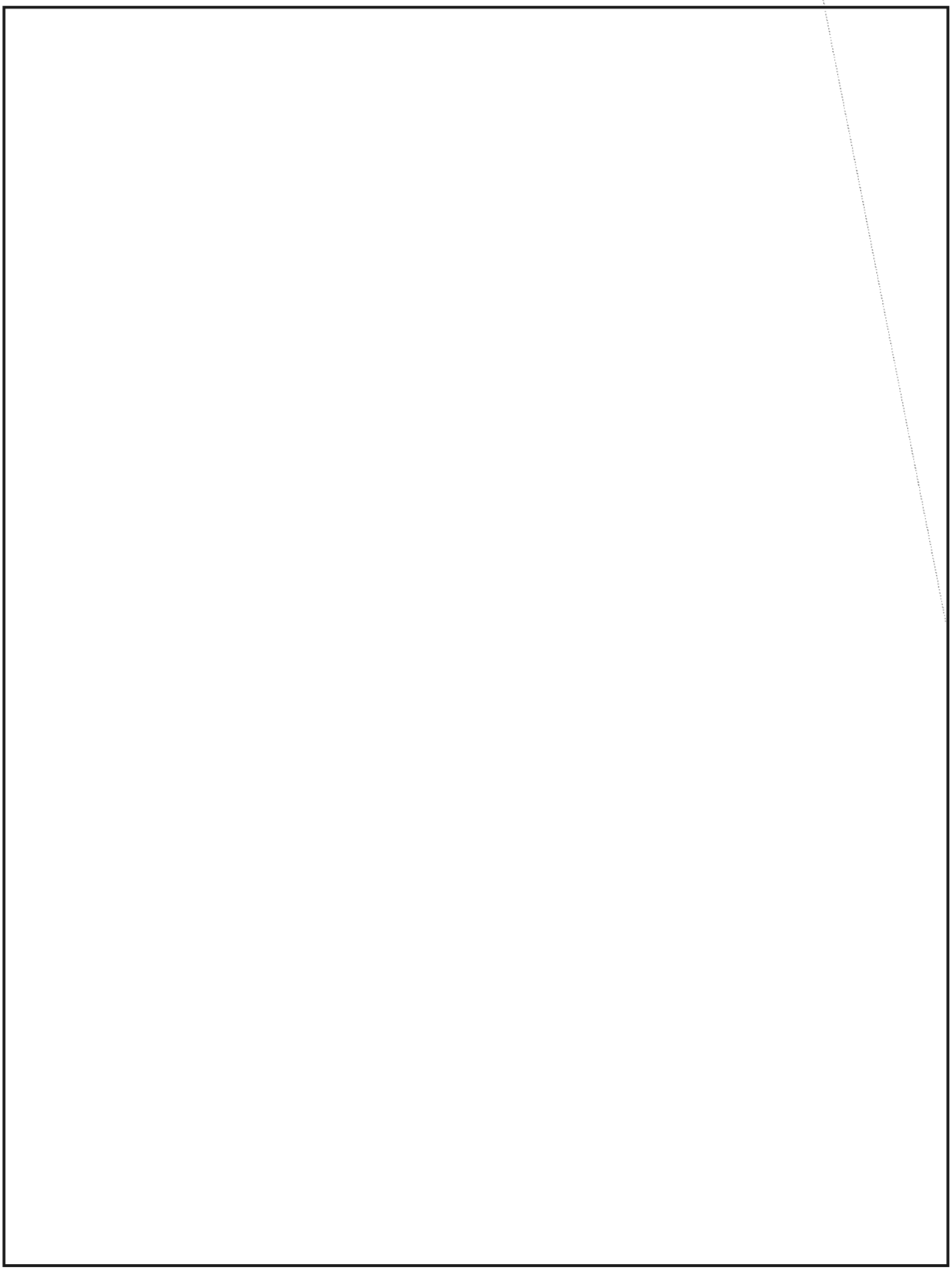
How Current Should TEXTA Be? (U)

P.L. 86-36
EO 1.4.(c)



Using TEXTA for Collection Steerage (U)

EO 1.4.(c)
P.L. 86-36



DOCID: 4011945

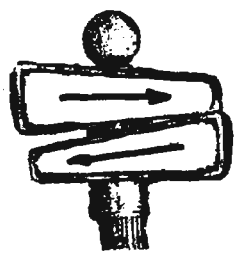
P.L. 86-36
EO 1.4.(c)

Where is TEXTA Going? (U)

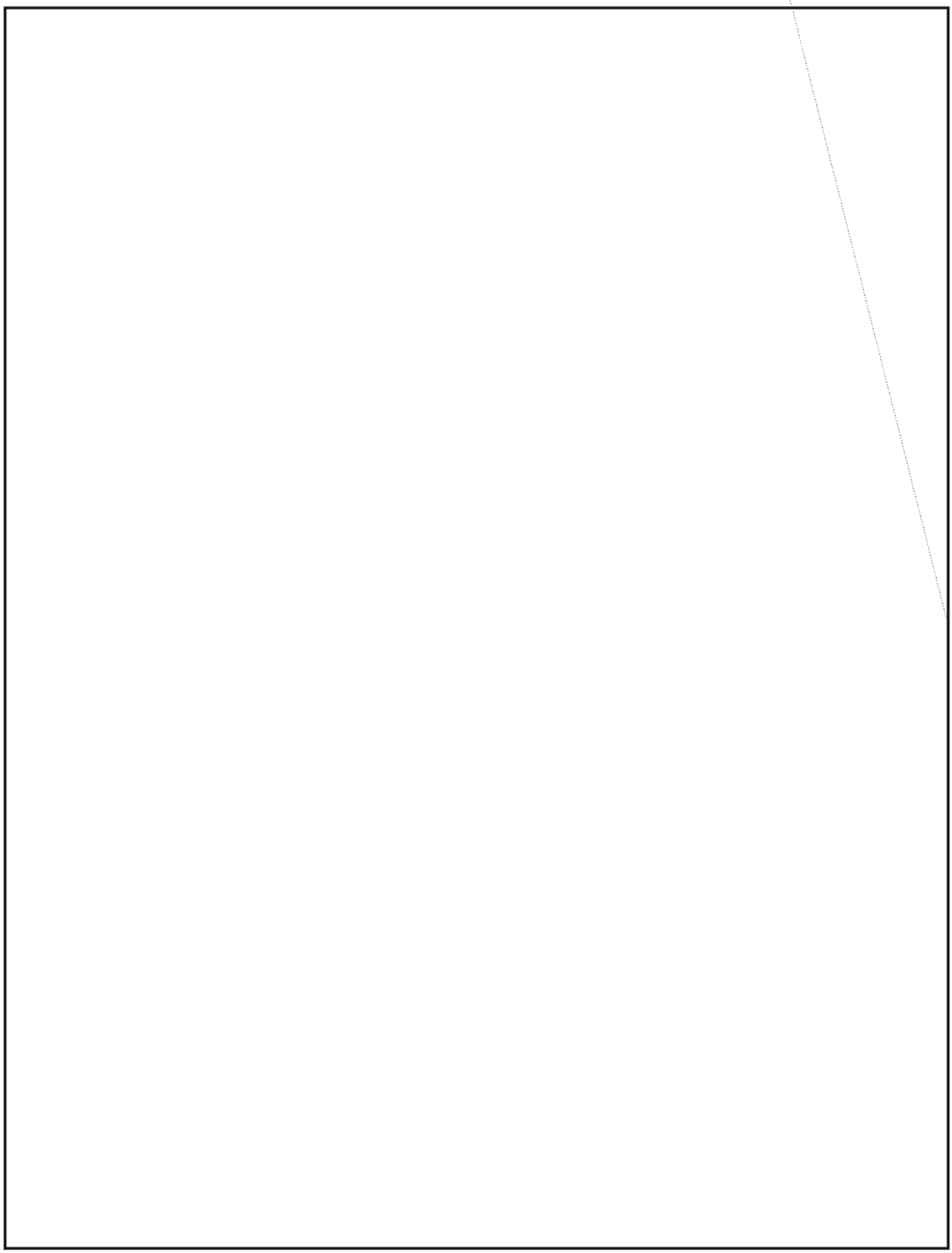
(U) Such "low validity" data, even though current, should not cause the older, but more authoritative, analytic results to be erased from TEXTA — they should coexist side by side in the record. The ease with which data can be lost through erasing and/or spillage is a major problem in computer based data systems and is one that will need special attention for TEXTA in the future. The future system should be set up to insure that no data is erased unless a backup record (such as microfiche) is first generated. Data no longer wanted in the current file, because it is either out of date or superseded, should be shifted either to "near storage" or "far storage", depending upon the likelihood of having to retrieve it at some later date. Near storage is defined as some machine-retrievable form, such as tape, where the data can be retrieved relatively easily, whereas far storage is defined as some form that is essentially not machine-retrievable, such as microfiche, where the data can be retrieved only with great cost and difficulty. (The cost of "repoking" or otherwise retrieving data from microfiche may make such efforts rare, but it would be unwise to rule them out entirely; sometimes the thing MUST be done, even if it has to be done entirely by hand.) Data might typically move from current on-line storage to near storage, and then after a specified period of time, to far storage.

(U) Future TEXTA will need an integrated system of "audit trails" to accommodate the variety of levels of data that will be in the system. At the minimum, the system will need -

- the date of the action which changes, adds, or deletes the information.
- the source of the action (at a minimum, the organization submitting the action, although at some locations the initials of the analyst might be needed).
- the validity of the information involved in the action.



EO 1.4.(c)
P.L. 86-36



the recipient).

[redacted]

[redacted]

[redacted]

P.L. 86-36
EO 1.4.(c)

What Should the Future TEXTA System Look Like? (U)

[redacted]

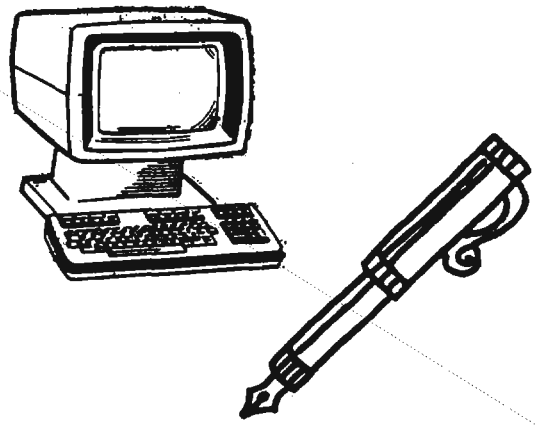
Sprechen sie TEXTA?

Parlez vous TEXTA?

говорите по-текста?

Habla TEXTA?

Parla TEXTA?



class citizenship in the system because he cannot afford some special piece of equipment or because he has no software support of his own.

P.L. 86-36
EO 1.4.(c)

(U) The system should provide for some kind of audit trailing, so that a selected class of user (i.e. some but not all) can determine:

- ★ who put a particular piece of data into the system?
- ★ when?
- ★ what "validity" was ascribed to it?
  - ● "low validity" entries cannot erase/replace "high validity" items already entered;
  - ● several variants (different sources, different validities) may have to coexist in the system for extended periods of time.
- ★ items erased/replaced (are not typically thrown away);
  - ● are retained in the "dark end" of the record (or in "near" storage) for an extended period, then are stored in microform (or "far" storage); and
  - ● remain available for audit trail purposes.

with a computer complex. No user need be kept out of the system, or reduced to a second-

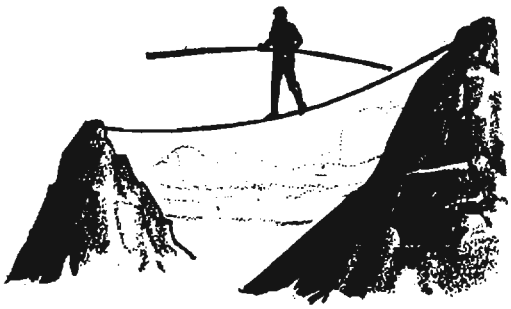
DOCID: 4011945

P.L. 86-36

PLATFORM:

How Did You Say That Works?

by [redacted] P4

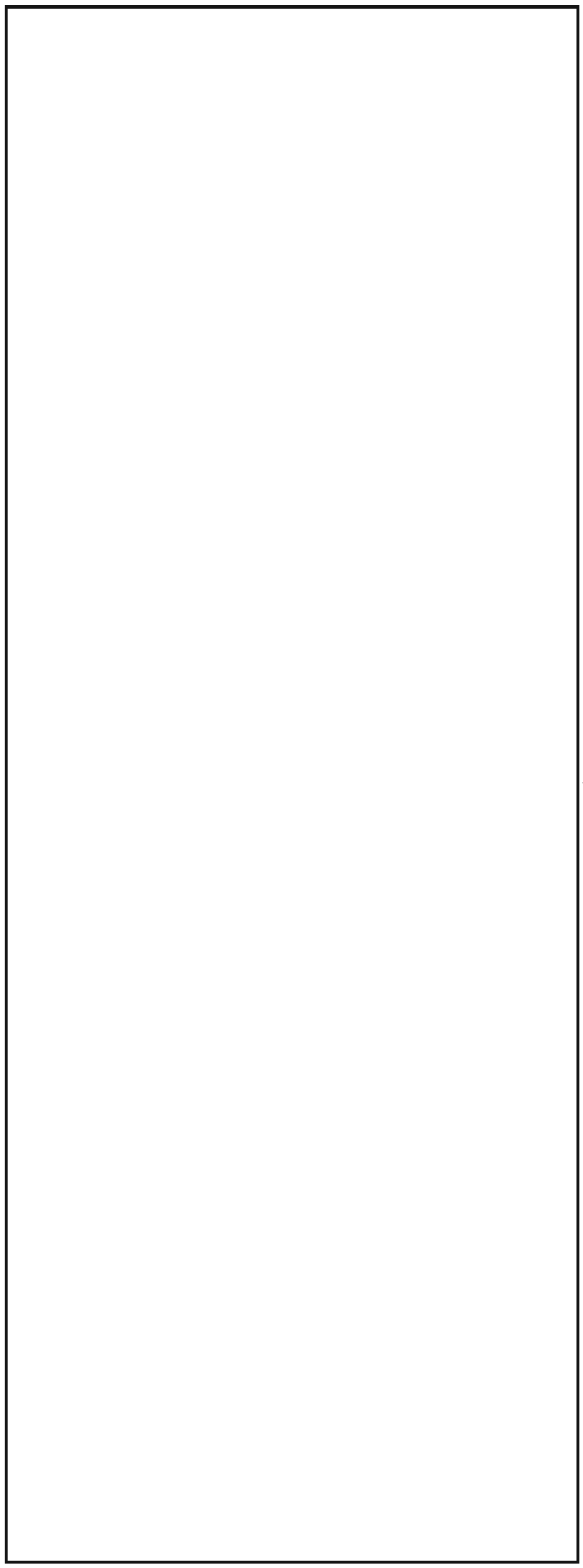


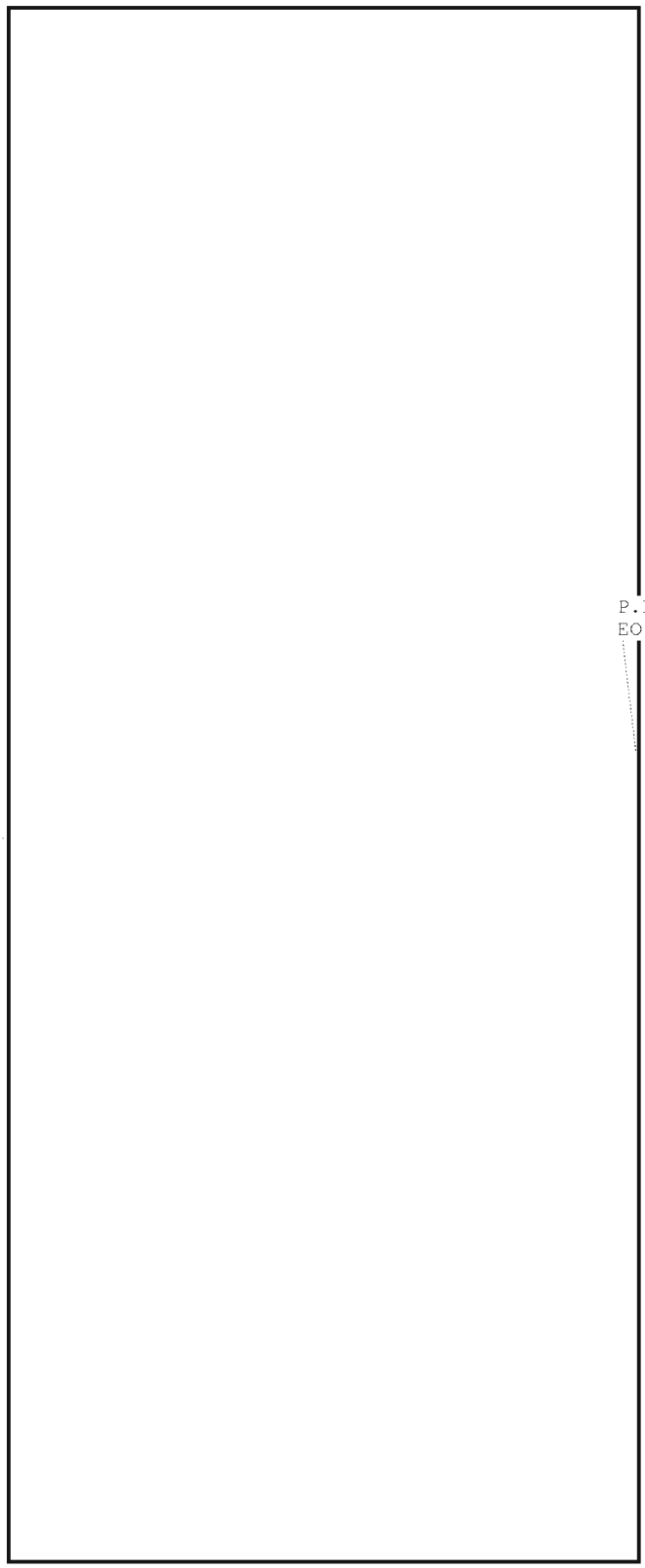
(U) A system has been designed, implemented, and delivered which allows users to sit at their favorite terminals, and travel all over the world to accomplish their assigned task. All that is required of them is a few simple standard commands. Oh, wouldn't that be great!

~~(FOUO)~~ Wait, aren't you talking about the PLATFORM network? Isn't that the way it works? Almost. We are close, but we aren't there yet. Simple things, little things, that appear trivial when looked at individually, work together to cause most of the current PLATFORM user frustrations. The general idea of PLATFORM is a good one, but it seems that, for those who actually have to use PLATFORM, something has been lost somewhere:

- Terminal characteristics that differ from one terminal to another as well as from one host to another.
- Terminal functions that can be used on some network hosts but not on others.
- Response times on network-connected terminals that exceed normal expected overhead.
- Multiple logins between hosts and again for processes or applications once logged into the hosts.
- Limitations on the number of connections that hosts will accept from the network.
- Call-ups of network protocols that are slightly different from one host to another.
- Network capabilities that are supported on some hosts and unavailable on others.

P.L. 86-36





P.L. 86-36
EO 1.4.(c)

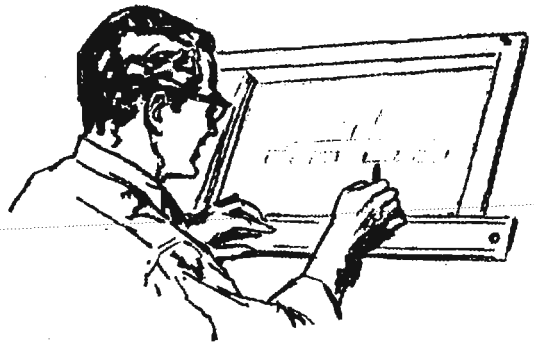
(U) Let's make it a tool that serves those charged with carrying out the mission of this agency.

DOCID: 4011945

In The Name of Efficiency (U)

review by

[redacted] P13



P.L. 86-36

(U) BOOK REVIEW:
Joan M. Greenbaum, In the Name of Efficiency, Philadelphia: Temple University Press, 1979 (NSA Main Library, QA78/G82)

(U) The subtitle of this very interesting and provocative book is "Management Theory and Shopfloor Practice in Data-Processing Work". It presents a frank and (to my eye) refreshingly critical and challenging review of the history and social context of computer programming and operating. In the view of the author, this history has been marked by a tug-of-war between management and the data processing workers. On the one hand, management has been uncomfortable with the freedom which programmers had in the early days of computers, and has found ways to limit that freedom, with increasing success. Programmers, on the other hand, have fought back to preserve the work satisfaction and status of their occupation.

(U) Here are a few brief quoted passages from the book, to illustrate the approach. Ms. Greenbaum begins her Introduction with the following personal scene-setting: "Back in the 1960s I was a computer programmer. Like most of the 200,000 or so other programmers, I enjoyed the work - particularly its opportunities for diversity and challenge. Comparatively high-paying, computer programming offered high status because its skills were little understood and in great demand. By the early 1970s some of the craftlike characteristics of this work had begun to change. The changes, like most day-to-day happenings, appeared quite slowly. But as they began to increase in tempo, it gradually became apparent that work activities once controlled by data-processing workers were no longer in their control." [p. 3] She continues, "In what began as a personal study, I set out to explore what was taking place in data-processing workshops and why it was happening. Many have said that the changes in the work process were just the results of 'normal' changes that occupations go through as they mature . . . What was most noticeable about the changes in each occupation [so affected] was that they were anything but 'natural'; workers fought against these forms of change, and managers had a hard time implementing them . . . The reasons for changes in the workplace are not always the reasons that appear on the surface." [p.5] She states that her purpose is not merely to "bemoan the lost days of craftlike activity," but to reveal the underlying reasons behind the changes and enable workers to understand, influence, and regain control over the workplace.

~~(POUO)~~ I was particularly interested by her review of changes in the field; I myself remember many of them as they happened here at NSA. What was once a single profession, "programming," (where a "programmer" carried out all phases of the task from problem definition to operational running of his program) was fragmented into disciplines performed by very different sets of people: operators, programmers, systems analysts, and keypunchers. The separate disciplines were often divided from each other by distrust and hostility as well as by the physical and organizational "walls" of the "closed shop" philosophy which was popular with management for a while. The advent of operating systems removed much of their new power from the hands of one of these new groups - the computer operators. All these changes, Ms. Greenbaum convincingly maintains, were results of deliberate efforts by management to "divide and conquer" the recalcitrant data-processing workforce and "rationalize" their work, in order to bring them under management control. Interestingly, she makes a clear case for the origin of the "professionalization" of programmers in a management initiative, and claims that this, too, far from being a desire of programmers themselves, was a step toward control of data processing workers by management. Structured programming is another obvious landmark in management's strenuous (and all-too-successful) efforts to remove inconvenient degrees of freedom from the programmer.

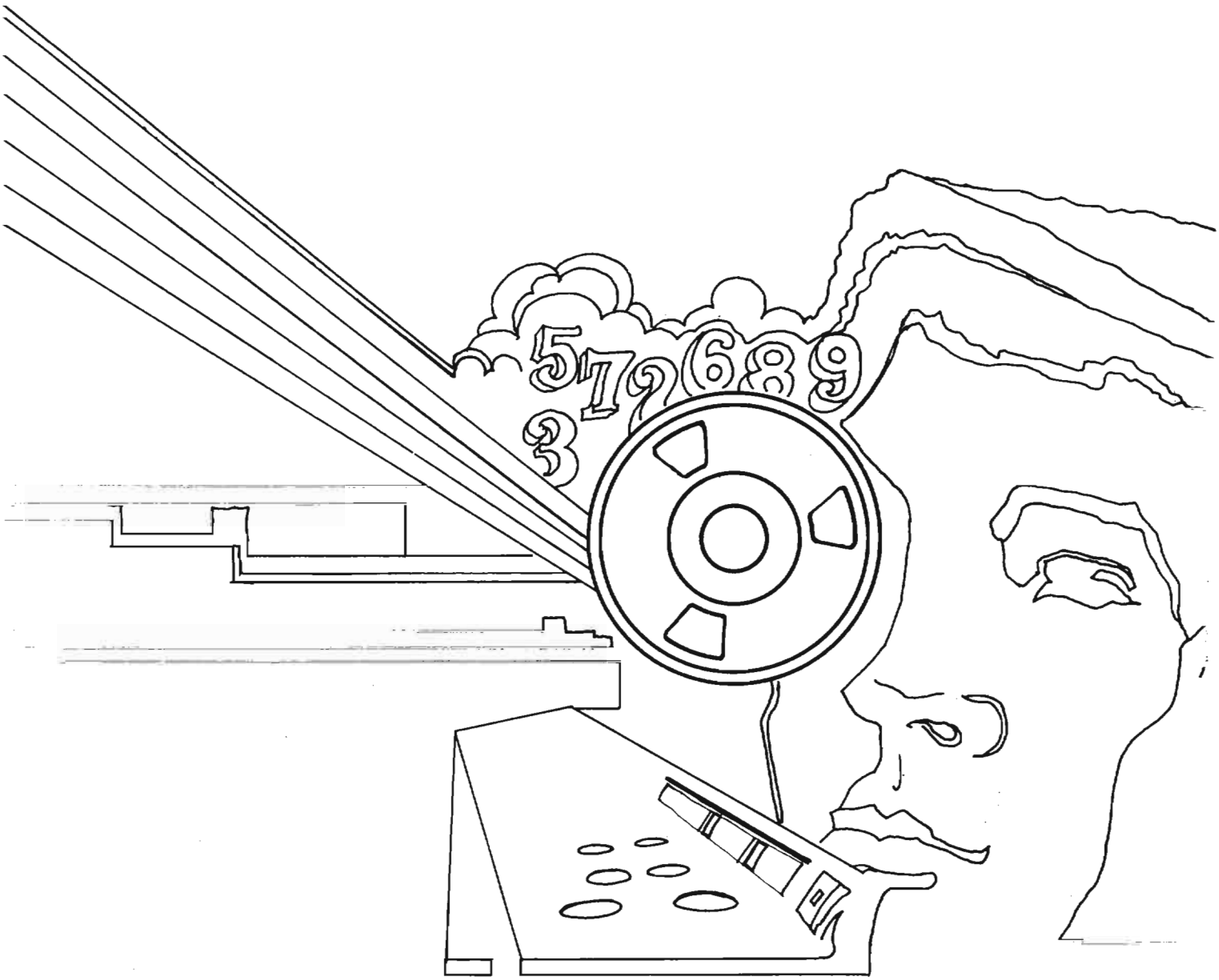
~~(FOUO)~~ Most of all, the IBM 360 systems made a dramatic break with the past. Ms. Greenbaum says the following: "Those of us in the field at the time of the introduction of the System 360 tend to remember it well, for almost overnight a firm division of labor occurred, not by chance, as it seemed to us then, but by clear design. Although computer work had been divided by task in the 1950s, many activities had overlapped a good deal. In particular, computer programmers and operators would meet in the computer room, which, like a social hall, offered the opportunity to exchange techniques and ideas. The installation of the System 360 provided management with reasons to change this. One of the first rulings to be enforced was a prohibition against programmers entering the computer room, thus isolating the two categories of labor and cutting off exchange of functions and rigidifying job classifications." Ms. Greenbaum analyzes the theory whose application by management brought about these changes in Chapter 3 of her book. She provides provocative treatments of "Shopfloor Practice," "Labor Process," and "Worker Behavior" - the interplay of workers' responses and resistances against management's initiatives in the daily operation of computer shops. She covers a great deal of very illuminating material concerning the workers' perception of their jobs and the changes enforced from above by management. I found many vivid echoes in my own memory of these perceptions as I experienced them in our own NSA computer installations, since I began in the "craft-like" times of ATLAS I, and lived through the changes accompanying the 704, 7094, and Systems 360/370.

(U) The author leaves us with an unexpectedly hopeful conclusion at the close of her book. She gives much weight to the efforts of data processing personnel in creatively remaking their work situation, and in particular finding new ways to cooperate and communicate with their co-workers and thus reclaim control over their work activity and restore challenge and satisfaction to their jobs. She concludes that "data processing workers have developed workplace activities and cooperative work practices that stand in sharp contrast to the rationalized bureaucratic hierarchy imposed by management. We are told that human nature is competitive and individualistic, but data-processing shopfloor actions contradict this. Effective data-processing work is usually accomplished by workers who help one another by sharing knowledge, skills, and tasks. By sharing knowledge data-processing workers have created, in effect, their own shopfloor culture that gives workers at least the ability to tolerate the contradictions they face every day on the job . . . When I first began this study I examined management justifications for efficiency and tried to compare these to what was actually taking place in the work environment. The more I looked the greater I found the differences between management and worker strategies for workplace activity . . . Work does <u>not</u> have to be organized to control human behavior. Efficient work activities can take place without the management ideology of social control. Examining workplace activities begins to point us in the direction of understanding other forms of work organization."

~~(FOUO)~~ The author's high opinion of cooperativeness and creativeness among programmers agrees well with my own experience when I was a full-time applications programmer. We shared ideas, helped each other to "debug" programs, shared labor (picking up runs), etc., and found ways to forgather in areas near counters, key-punches, etc. to exchange news, techniques, tips, and aid. We often had to do these things in spite of management's frowning upon our apparently unstructured activities, and our uses of spaces and facilities intended by management for other purposes.

~~(FOUO)~~ It seems evident that these considerations will soon become more crucial than ever. It will very soon be possible for much, if not all, programming and computer-aided problem solving to be done via remote terminals. Soon it will no longer be in any sense a <u>practical</u> or <u>physical</u> necessity for data processing workers or computer users to be located all together in one building. The only thing that might continue to force vast numbers of computer workers to be herded together in offices from nine to five, five days a week, would be the fear of management that any other arrangement might result in their loss of social and behavioral control over employees. I recommend Ms. Greenbaum's challenging book as a starting point for thinking about some of these issues.

Originally published in the October 1979 Newsletter of the Special Interest Group on Human Factors, Computer and Information Sciences Institute.


5726893

DOCID: 4009838

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

November 1981

P.L. 86-36

THE PPC IS COMING!
Future Powerful Personal Computers:
An Overview of the Technology (U)..... [redacted] 1
FUTURISTIC REPORTING (U)..... [redacted] 9
CRYPTIC CROSSWORD (U)..... [redacted] 14
SAY WHAT YOU MEAN (U)..... David W. Gaddy..... 15
HOW TO CREATE A USER-UNFRIENDLY SYSTEM (U)..... [redacted] 17
OPELINT IS ALIVE AND WELL IN B GROUP (S)..... [redacted] 25
REVIEW: What do you think? (U)..... [redacted] 29

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 10 Nov 2011~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009838

CRYPTOLOG

Published by P1, Techniques and Standards,
for the Personnel of Operations

VOL. IX, No. 11 NOVEMBER 1981

PUBLISHER [redacted]

BOARD OF EDITORS

Editor-in-Chief..... [redacted] (8322s)

Production..... [redacted] (3369s)

Collection..... [redacted] (8555s)

Cryptanalysis..... [redacted] (4902s)

Cryptolinguistics..... [redacted] (5981s)

Information Science.. [redacted] (3034s)

Language..... [redacted] (9161s)

Machine Support.. [redacted] (5084s)

Mathematics..... [redacted] (8518s)

Puzzles.....David H. Williams (1103s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Taurone (3573s)

For individual subscriptions
send
name and organizational designator

to: CRYPTOLOG, P1
or call [redacted] 3369s

To submit articles or letters
via PLATFORM, address to

cryptolg at barlc05
(note: no '0' in 'log')

EDITORIAL

The response to our cry for help in keeping our subscription lists up to date has been heartening. Thanks. One "active" name on our list has been out of the agency for several years; many others have moved.

Along with the responses, we have been getting questions along the line of "Is CRYPTOLOG still alive?" (we think so) and "Is it going to be merged with some other publication?" (we have no plans to merge with any other publication, and none has so far expressed any interest in merging with us). We are a DDO (Operations) publication, but it is clear from our subscription list and our author list that we range outside the physical confines of DDO.

If we don't seem to be publishing any articles about your area of interest, it is either because the editor is biased against your area of interest, or because he isn't getting anything about your area of interest that can be published.

Most of the layout and editing of CRYPTOLOG is now being done on a computer - actually on several computers. Using the UNIX system, with some help from PINSETTER, and the PLATFORM network between various host computers, the original keystrokes (often the author's) are retained throughout the process. A lot of retyping, as well as cutting and pasting that characterized the earlier issues (all done on a typewriter) is being avoided. One item, [redacted] piece last month on Technical Support Catalogs, was coordinated with him in final form just before publication via the network (Ken is now stationed in Germany).

About half of the items now being worked on for this and future issues have come in over the network. We are still interested in receiving items from people not on the network. We don't mind typing, even though it's nice to have some items that don't require it.

P.L. 86-36

DOCID: 4009838

FUTURE POWERFUL PERSONAL COMPUTERS:
An Overview of the Technology
by [redacted]

P.L. 86-36

THE PPC IS COMING

Scientific and analytic computing, especially at NSA, has evolved from the batch environment of the 1960's to the timesharing and multiprocessing environments of the 1970's. In the 1960's, typical programmers submitted a deck of punched cards to the batch system and later received the deck and a listing of the program execution. In this environment, both the computing power and the user's access to this power were remote and non-interactive. In the timesharing environment of the late 1970's (and of today), the programmer has direct, timely, interactive access to his or her computing processes through a terminal. In this environment, the computing power is still remote, whether in the next room or far away across a network, and is shared. However, the user's access to this power is potentially local and definitely interactive; hopefully, the access terminal is on or near the user's desk.

What will scientific and analytic computing be like in the 1980's? While it can be argued that very large-scale super computers like the Cray 1 will definitely be needed for many complex problems [10], advances in several areas of computer technology have spurred efforts to design and produce extremely powerful, extremely compact computer systems for scientific and analytic use. Such systems will be small enough and inexpensive enough to be single-user systems located at the user's desk. In a sense, these systems will enable users to have their own "VAX" or "370" instead of a terminal. In this environment, both the computing power and the user's access to it will be local, personal, and highly interactive.

The purpose of this paper is to discuss capabilities being proposed for such a computing system, how it may be realized, and what its impact on NSA scientific and analytic computing might be. How should this future system be described? Some papers on the subject call it a personal computer [4, 12]. While it will be personal, this label conjures up images of the TRS-80 or the Apple II -- a totally inappropriate image. Other papers [13] refer to it as an intelligent terminal. At NSA, this term fits the Delta Data 7000, for it is a terminal with its own microprocessor. The powerful future system is NOT a terminal; it is THE computing system and may be more powerful than systems to which we interface intelligent terminals today! For lack of another name, this paper will refer to this system as a Powerful Personal Computer (PPC).

The PPC has the potential to revolutionize scientific and analytic computing at NSA. Even with the GTSS and other timesharing systems of today, analysts use terminals to gain access to remote, shared computing power and data over relatively low-speed connections (whether network or communications lines). The PPC will give the analyst access to significant local, individual computing power and data. Networks and communications lines today are used to gain access to all computing power, all data, and personal communications. In the PPC environment, high-speed networks will be used for access to very large data bases and shared resources and for electronic personal communications. This will be a drastic change from our present networking philosophy.

II. Characteristics of a Powerful Personal Computer

Although timesharing systems have given access to remote, general-purpose computing rather than to local, personalized computing, the environment which has been created is a rich one for timesharing users. This environment has promoted a large set of programming languages, large file storage capabilities, sharing of programs and data, a cooperative user community, and other benefits. The environment of the PPC should preserve and enrich the good characteristics of the timesharing environment, while bringing many totally new capabilities to its users.

A number of efforts are underway to specify and/or produce a PPC and its environment at institutions like Xerox [12], Carnegie-Mellon University [6], MIT [15], Convergent Technologies [16], and Three Rivers Computer Corporation [13]. While these efforts do not completely share common technologies, their broad goals are remarkably similar and these goals apply for many scientific and analytic institutions (including NSA). The individual PPC environment of the mid-1980's should be reasonably priced ($10,000 to $20,000), should exist in a small and attractive package for office use, and should have the following characteristics:

1. a very powerful processor or processors (while this will be implemented on one chip, the term "microprocessor" seems too limited); it should have 32-bit data paths and use 1-bit, 8-bit, 16-bit, 32-bit, and 64-bit operands;
2. a smoothly addressable virtual address space using as many as 32 bits of address;
3. a very large multiport primary memory-- 1 Mbyte or more;
4. at least 100 Mbytes of high-speed local secondary storage;
5. a 1024x1024 raster display, probably color with several bits per picture point (pixel);
6. good interactive devices (keyboard, graphics pointer, lights, function buttons);
7. audio input and output;
8. ease of interfacing other peripherals if desired;
9. a very high-speed local network connection;
10. a powerful local operating system which can be personalized;
11. powerful, easily-used programming languages, utilities, and DBMS techniques.

Given a PPC with the above characteristics, an office environment built around several such PPC's would have these additional characteristics:

12. a local, high-speed network connecting all PPC'S throughout the office;
13. a gateway to other networks;
14. an "office" PPC to support expensive peripherals which are needed occasionally (e.g., quality printers, massive disks) and to perform support functions (e.g., mass data transfers from distant data bases, local office coordination);
15. an "office" file system for commonly used databases;
16. a global (to the local network) operating system to allow easy inter-PPC sharing of programs, data, and resources.

Items 13, 14, and 15 could be implemented in a distributed manner on several PPC's across the local network or in a centralized manner using one physical PPC as the "office" machine to support all office resources. This paper will assume the latter implementation. The global or network operating system would be distributed.

The personal computing environment described above is more powerful in both hardware and software than almost all timesharing systems in use today. Should a computing environment that powerful really be used by only one person? Can institutions like NSA afford to allow such a powerful computing engine to stand idle between the

keystrokes of its single user? Yes. Economics today show that the hardware to implement a PPC will be reasonably priced in the mid-1980's. Some estimates for a PPC as described above are in the range of $10,000 [6]. (Of course, an implementation today would be much more expensive.) Economics today also show that the people who do scientific and analytic computing are becoming more and more expensive. If such people become only moderately more productive when given a PPC, the investment is worthwhile. The cost of any "wasted" machine cycles is insignificant compared to the productivity gained.

While the packaging of the characteristics of the PPC in the form described will be a major effort, each characteristic by itself is not completely new. Each already exists in some form at some price. Thus the development of the PPC is more of a hardware and software engineering project, rather than a research project [6]. This does not mean it will be any easier; it simply means that the areas to be explored and developed are not un-known.

III. Hardware Technology for the Powerful Personal Computer

The combination of hardware and software technologies needed to successfully implement a PPC with the 16 characteristics listed in section II does not yet fully exist. It is important to point out here that we must have both advanced hardware technology and advanced software technology to successfully implement the PPC environment. One without the other will lead to failure. This section will discuss in some detail the hardware technology which will enable the PPC to be built; section IV will discuss the software technology which will enable the PPC to be successfully used.

The hardware issues fall mainly in characteristics (1) through (9) and (12). The technology exists today to supply the capabilities listed in these characteristics, but at substantial cost and in very large packages not at all suited for an office setting. One could attempt to meet these characteristics with the following set of today's standard hardware:

(1)-(4),(8) a DEC VAX 11/780 computer system ($160K);

(5)-(6) a Genisco or Ramtek raster graphics system ($30K);

(7) input-- 64-word vocabulary system by Heuristics ($259);

output-- VOTRAX voice synthesizer ($3K) or Texas Instruments TM990/306 179-word system ($1K);

(9),(12) an ETHERNET or Mitre bus system ($6K);

If this hardware configuration were assembled, it would cost about $200K and would require about 200 square feet of floor space and special electrical connections and air conditioning. It would not be suitable for a personal system on one's desk.

As LSI and VLSI circuit design technology continues to make advances, the hardware pieces needed to satisfy these requirements will continue to get smaller and less expensive. The remainder of this section will explore coming technological advances which will help realize the PPC.

A. Processor and Address Space

If the PPC is to truly give its users the power of current multi-user machines like the DEC VAX 11/780 or the IBM 370, its processor must have a powerful instruction set, must be fast, must have a large address space, and must have wide internal data paths. Single-chip processors of the late 1970's (traditionally called microprocessors) have not met these criteria. Although their instructions sets may have been reasonable, their execution speeds have been moderate, internal data paths have been either 8 or (sometimes) 16 bits wide, and direct addressing has been limited to 64K bytes of memory. Because the term "microprocessor" has been traditionally associated with these earlier single-chip processors, it is inappropriate when discussing the type of processor needed for the PPC of the mid-1980's.

The newest generation of single-chip processors has made several major advances over the earlier generation as LSI technology has grown. As technology continues to grow, further advances are sure to come. Before discussing what the mid-1980's may produce for single-chip processors, a look at current state-of-the-art processors is in order,

since these processors are being used in current projects to implement PPC's. See Figure 3 for a quick comparison of the Intel 8086, the Zilog Z-8000, and the Motorola M-68000.

All three of these processors have been built with some concern for the operating systems and higher-level languages that must run on them. Thus, they have instruction sets to support byte-string operations, bit manipulation, re-entrant code, dynamic relocation, etc. They all have well-designed interrupts, register sets, and other expected hardware features. Although a ranking of the three may not be fair, their applicability for a PPC processor could be ranked in decreasing order of applicability as (1) M-68000, (2) Z-8000, (3) 8086. At this point in LSI evolution, the capabilities of the processor chip will depend heavily on the surrounding support chips and coprocessors. When the processor chip of the mid-1980's includes many functions which are now off-chip, this will not be true.

LSI state-of-the-art technology in 1980 puts about 70K devices on a chip to produce a Motorola MC-68000. VLSI technology (VLSI is usually accepted to mean 100K or more devices per chip) will greatly impact the development of more powerful single-chip computers because of increased design density, increased chip size, and improved layout techniques [7]. VLSI state-of-the-art in about 1985 will put 1M devices on a single chip. The single-chip processor of 1985 (dubbed P1985 in [7]) will be a much more powerful one than that of today. When the P1985 architecture can be realized, a single-chip processor will indeed be equivalent in functionality to many large commercial CPU's of today (e.g., the VAX 11/780). With such a processor, the PPC as described in this paper will be realizable.

B. Primary Memory

Given a good virtual memory operating system for the PPC, significantly less physical memory is required than could be supported by the address space. However, the amount of physical memory to nicely support multitasking and to provide image memory for the raster display is still significant. Because memory chips will be very inexpensive in the mid-1980's, a primary memory on the order of 1 Mbyte will be an economically sound way to reduce local operating system swapping overhead. Image memory for the raster display could take an additional 0.1-0.5 Mbytes, depending upon the choice of black-and-white or color.

With present, proven 16K-bit memory chips, it would take 500 chips to provide 1 Mbyte of primary memory; this would occupy several physical boards (perhaps 10) and would occupy too much space for a PPC. With the 64K-bit chips now coming into production, only 125 chips are needed and they can be configured in a much smaller package (perhaps two boards). With 256K-bit chips on the horizon [4,7], this shrinks to approximately 32 chips. Depending upon other design considerations, this entire 1 Mbyte memory might be placed on the processor board, considerably reducing packaging size. Texas Instruments predicts that these components will be available by 1985 at a cost of less than $2000 for the 1 Mbyte capacity [4].

C. Secondary Storage

For the PPC environment to be successful, a high-capacity, fast secondary storage system is needed at the individual PPC to hold personal utilities, programs, data, and text files. For this storage system to fit neatly into an office environment, it needs to be compact. In an office with several PPC's and an "office" PPC networked together, the "office" PPC may be required to supply additional bulk secondary storage. That can be done with more traditional disk systems and will not be considered here.

Examining current work in storage technologies shows advances in charge-coupled devices (CCD's), magnetic bubble memories (MBM's), video disks, AND magnetic recording [3]. At first glance, one might be inclined to discount magnetic recording as a continuing attraction for mass storage. However, many of the same technological advances that are advancing CCD's and MBM's are also advancing the state-of-the-art in magnetic recording. In the past 25 years, device capacities have increased over 100-fold and recording densities have increased over 1000-fold; similar dramatic advances continue to be predicted [3]. Especially with the introduction of devices like the Winchester disk, which can store in excess of 30 Mbytes of data on an 8-inch platter for about $2500, it seems that magnetic recording will be the appropriate technology for the PPC.

D. Raster Graphics and Interactive Devices

In the timesharing environment of today, a raster graphics system is a peripheral that is often used in conjunction with a more standard alphanumeric systems terminal. In the PPC environment, the graphics display will be the ONLY visual presentation to the user and it will be an integral part of the PPC, not a peripheral [11]. Thus, use of the graphics display will be an inherent part of any program which interacts with the user. The PPC raster display should have the following features:

high resolution -- the display should have approximately 1024x1024 addressable picture elements (pixels);

frame buffer -- the image memory (bitmap) should be organized as a frame buffer which can be accessed on a pixel basis directly by the PPC processor; the frame buffer should be seen as main memory by the PPC processor;

graphics processor -- functions like vectors, characters, and other graphics primitives should be implemented by either a special graphics processor or by special microcode for the PPC processor;

color -- depending upon the amount of PPC memory to be devoted to the frame buffer, color could be an option; if chosen, at least four bits per pixel should be used with a video look-up table for greater color definition [11]; 40-60 Hz refresh is desirable;

video I/O and processing -- digitized video input to the frame buffer should be possible; under control of a video processor [11], output from the frame buffer to the screen could be zoomed, scrolled, pseudocolored, etc.;

keyboard -- a flexible keyboard is needed which reports to the PPC processor which specific key is depressed, not a specific ASCII code; this allows total redefinition of the keyboard by the program;

pointing device -- a pointing device with dynamic cursor is needed for accurately indicating positions on the screen by the user.

All of these features are available in present commercial raster graphics systems which are tied to present computer systems as peripherals. The technological issues which must be resolved to put these features in a PPC are two: size and integration. The bulk of current color raster graphics systems is physically in the image memory, the interface to the host, and the graphics processor. In the PPC, graphics will be integrated into the entire package; it will not be a peripheral and no interface is needed. The image memory will be organized as a part of the PPC's main memory. A separate graphics processor is not needed if the PPC's microcode supports primitive graphics functions. If not, a graphics processor in this technology would be extremely small. Thus, if the integration of raster graphics into the PPC is done correctly, size is not an issue. Even with a separate graphics processor and a sophisticated video processor, the extra hardware associated with the raster graphics should be confined to one board at most.

E. Audio Input/Output

The concept of talking to your PPC and having it talk back to you may seem far-fetched and perhaps unnecessary, but audio I/O seems very attractive from a human factors point of view. Advances in heuristic techniques for speech recognition, advances in LSI, and the home computer market have been driving forces in producing the audio I/O devices available today. Several companies now offer speech input and output systems for under $1,000 each. The popularity of the Texas Instruments "Speak and Spell" toy attests to the value of audio I/O.

F. Interfacing

Given an office environment with a number of individual PPC's and an "office" PPC to support a large office database and a high-quality document printer, extra peripherals for an individual PPC may not seem needed. However, given the diversity of talents and

DOCID: 4009838

interests which may use the environment, some new device will soon be suggested as a peripheral to a PPC. When that time comes, the interface to the PPC should be straightforward and easy. The hardware interface could be via a standard communications port or directly to the internal bus of the PPC; both should be available.

G. High-speed Local Network

High-speed local networks exist today. There are several different configurations of topology, control structure, and transmission media which can be chosen, depending upon the applications and the distances involved [1]. For an office PPC environment, a ring or bus topology (see Figure 4) with a contention control structure seems promising [1,15]. Examples in current technology include the ETHERNET and the Mitre bus.

IV. Software and Environment Technology for the Powerful Personal Computer

Very strong emphasis must be placed on the software and the environment for the PPC. If the hardware technology described above is successful beyond our wildest dreams, the result will not be practically useful without an equally successful software technology. If hardware technology can be viewed as supplying the raw power needed, the software and environment supply the ease of use and control necessary to harness and direct that power.

The user interface to the PPC is all important. The hardware technology discussed above can provide interactive and communications devices with very interesting human factors implications. A PPC which can listen to you and talk back, draw colored pictures for you, and communicate with others in your office for you could become a very powerful extension of yourself. However, the software and environment of the PPC must be carefully constructed for this potential extension to become reality. The use of audio I/O, color displays, and the local network must be innately a part of all software components. If these capabilities are thought of as occasionally desired peripherals, rather than as an integral part of the system, the resulting environment will be much less human and less powerful than it could otherwise be.

A. Operating Systems

The local operating system will be the primary interface between the user and his or her PPC. It should be friendly, easy to use, helpful, and as forgiving and tolerant as possible. It should support a multitasking, virtual memory environment with interprocess communication. Any hardware feature of the PPC should be as useable as possible from the operating system level.

In the PPC environment with a high-speed local network, resources used by a given task may be distributed between the personal PPC and the "office" PPC, or they may not. The location of resources (files, peripherals, gateways, etc.) should ideally be transparent to the user. In order for this to happen, a global or network operating system must exist to coordinate this communication and resource sharing. Depending upon implementation, it could reside on the "office" PPC or be distributed throughout the PPC's in the office network.

B. Programming Languages

Programming languages will be the second interface between the user and the PPC. Programs will be one of a user's major products. Programs must be coded, modified, debugged, made efficient, and (finally) executed. A programming language and its surrounding environment should be designed to facilitate this process and to make it as pleasant and efficient as possible. Alan Kay and his SMALLTALK work on the Xerox ALTO system [2] have shown that novice programmers can quickly become proficient if the programming language is designed appropriately.

Since the PPC as described herein is designed for scientific and analytic programming, the proposed users are not totally novice. However, languages for the PPC should be designed for people who traditionally think of themselves as non- programmers. A number of current languages are often proposed for use as a basis for a PPC programming language: PASCAL, C, ALGOL, Ada. The environment built around a language should support a compiler, linker, powerful symbolic debugger, and extensive runtime library.

DOCID: 4009838

C. Utilities

Utilities are normally invoked by operating system commands. They include things like an editor, various word processing programs (speller, formatter, etc.), a file system, language compilers and interpreters, debuggers, an electronic mail system, etc. These utilities MUST be implemented with the total PPC environment in mind. The text editor should take full advantage of the raster graphics for font definition, color, and perhaps illustrations. All utilities that could use the local network and any gateways to other networks should use them as transparently as possible. As with the operating system, the utilities should be as friendly, easy to use, helpful, forgiving, and tolerant as possible.

D. Servers and Network Gateways

In a local network PPC environment where users interact with one another frequently, the concept of servers has proven important [12]. In this environment, a server is a machine on the network which performs some widely-used service for all users who desire to use it (e.g., document printing). In some network environments, there are several or many servers distributed around the network. In the PPC environment, one server has been postulated, the "office" PPC.

The concept of gateways to other networks is especially important at NSA. If a PPC local network becomes a replacement for current GISS systems, the interconnections currently supported over PLATFORM would need to continue. The local server or "office" PPC would handle PLATFORM-like communications for overall network mail and file transfers.

E. Environment

When the software described above is implemented, the environment created for the individual scientific or analytic user will be very powerful, extremely easy to use, and tailorable to closely suit the individual's personality and needs. Even though audio I/O and color graphics are integral tools at all levels, it is obvious that some people will use them and others will not. Some people will make constant use of the local network and others will generally remain in the shell of their own PPC. The overall PPC environment should be flexible enough to gracefully allow use of all, some, or none of these special features. It should gently encourage their use without penalizing a person who insists on using only the keyboard input and alphanumeric text output. A Powerful Personal Computer must be just what its name implies: powerful, yet personal.

V. NSA and the Powerful Personal Computer

It will take the research and industrial community several years to complete a commercially-available PPC which meets most of the specifications of section II. Such a system may not be available until 1985, if then. Before 1985, several versions of a PPC will be available in one of two forms: (1) a commercial form which uses 1980-1981 technology to meet many of the section II specifications or (2) a research form which meets all of the specifications. The commercial versions will be realistically available in 1981-1982 with the necessary software. A more powerful research version with newer technology might be available in 1984-1986.

Given that these predictions come true, what should NSA be doing to prepare for the advent of the PPC? NSA should be planning for it and experimenting with those versions of the PPC which will soon be available. Several offices in NSA (e.g., R53) are now using timesharing systems in a very personal way. Terminals are at the users' desks, various inter-user communications systems exist, the computer serves as phone book and personal text preparation system, and many working documents are kept on the system. Most importantly, the users of the system have adapted their way of life around the system in personal ways; they have made the system an integral part of their work environment. Such offices are excellent candidates to experiment with the PPC environment.

DOCID: 4009838

Parts of the DDR and DDT organizations are already closely following the development of the PPC externally. R53 is now assembling an initial prototype system for experimentation in the use of PPC's. This system will initially include two PPC systems from Apollo Computer (built around the Motorola M-68000), one system from Convergent Technologies (built around the Intel 8086), and a high-speed local network built by Sytek, Inc. The present R53 timesharing resources will be integrated into this system via the local network. This total PPC environment in R53 will be used in part to gain experience and to help determine possible architectural configurations for the T4 User Interface System project.

What areas of NSA are likely candidates for a PPC environment? Problems where massive amounts of computational power must be applied will still require systems like the CDC 7600 and its successors [10]. However, algorithm development for these problems is an excellent candidate for a PPC environment. Environments which now use the Generalized Terminal Subsystem (GTSS) timesharing concept are obvious candidates for the PPC. Any scientific or analytic computing would be a candidate for the PPC. Non-technical functions like word processing may eventually benefit from the PPC environment, depending upon the final cost of the PPC and the coupling between technical and administrative people within an office. In short, any computing environment where people are doing interactive computing or algorithm development is a candidate for the PPC environment. Thus, NSA has a lot to gain in productivity from successful development and application of a Powerful Personal Computer environment.

References:

1. Clark, David D., Kenneth T. Pogran, and David P. Reed. "An Introduction to Local Area Networks," PROCEEDINGS OF THE IEEE, vol. 66, no. 11, November 1978.

2. Kay, Alan C. "Microelectronics and the Personal Computer," SCIENTIFIC AMERICAN, vol. 237, no. 3, September 1977.

3. Hoagland, A. S. "Storage Technology: Capabilities and Limitations," COMPUTER, vol. 12, no. 5, May 1979.

4. Isaacson, Portia, Robert C. Gammill, Richard S. Heiser, Adam Osborne, Larry Tesler, and Jim C. Warren, Jr. "Personal Computing," COMPUTER, vol. 11, no. 9, September 1978.

5. Morse, Stephen P., William B. Pohlman, and Bruce W. Ravenel. "The Intel 8086 Microprocessor: A 16-bit Evolution of the 8080," COMPUTER, vol. 11, no. 6, June 1978.

6. Newell, Allen, Scott Fahlman, and Robert Sproull. "A Proposal for Personal Scientific Computing," Department of Computer Science, Carnegie-Mellon University, Draft of 13 July 1979.

7. Patterson, David A. and Carlo H. Sequin. "Design Considerations for Single-chip Computers of the Future," IEEE TRANSACTIONS ON COMPUTERS, vol. C-29, no. 2, February 1980.

8. Peuto, Bernard L. "Architecture of a New Microprocessor," COMPUTER, vol. 12, no. 2, February 1979.

9. Stritter, Edward and Tom Gunter. "A Microprocessor Architecture for a Changing World: The Motorola 68000," COMPUTER, vol. 12, no. 2, February 1979.

10. Sugarman, Robert. "'Superpower' Computers," IEEE SPECTRUM, vol. 17, no.4, April 1980.

11. Tarbell, Lawrence C., Jr. "The Potential Impact of Raster Graphics at NSA," PROCEEDINGS OF THE CISI SPRING CONFERENCE, May 1979.

12. Thacker, C. P., E. M. McCreight, B. W. Lampson, R. F. Sproull, and D. R. Boggs. "Alto: A Personal Computer," Xerox PARC report CSL-79-11, 7 August 1979.

13. Three Rivers Computer Corporation. Preliminary documentation for the Perq Intelligent Terminal, enclosures to correspondence dated 13 June 1979.

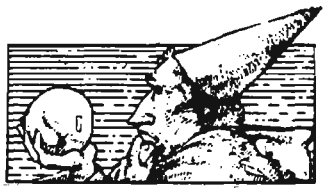
14. Trifari, John. "Backing Up the New Winchester Disk Drives," MINI-MICRO SYSTEMS, vol. 12, no. 8, August 1979.

15. Ward, Steve, Chris Terman, Jon Sleber, and Rae McLellan. "NU: The LCS Advanced Node," MIT Internal Memorandum, 28 February 1979.

16. Wegbreit, Ben. Private communication of 23 April 1980.

DOCID: 4009838

FUTURISTIC REPORTING (U)



by [redacted]

P.L. 86-36

Reporting describes a wide variety of different activities. Within NSA, we serve our customers in many different ways. We issue informal ~~(S-CCO)~~ reports such as TACREPs, formal reports and translations in both hard copy and electrical versions, and we support community data bases through the COINS system. Among our reports and translations, which form the bulk of what we generally refer to as reporting, we cover many different subjects and [redacted] I could go on listing the variety of reporting for some time. The variety of reporting we do requires a lot of different ways of doing it. We tailor our product to some extent today and are always looking for ways to improve it, but we do almost all our reporting via electrical, narrative reports: few hard copy reports, few graphics, few briefings.

~~(C-CCO)~~ With the availability of computer technology, many parts of NSA's mission have been affected. Where we used to copy Morse code on six-ply paper, and the analysts back at NSA would scan the raw traffic a month or two after it was intercepted, today we routinely forward traffic electrically to NSA for nearly instant analysis. [redacted] Traffic analysis, signals analysis, cryptanalyis, telemetry analysis are all done routinely on computers.

(U) With the advent of the MESSENGER computer system in NSOC, we even prepare reports on a computer. But wait a minute. Let's consider how that is done. The reporter scans his incoming traffic, prepares his report, submits it to a chain of reviewers who eventually deliver the draft to the typist in the flex room. The text is retyped (possibly for the fourth or fifth time) and then released. Although MESSENGER is a computer based report preparation system, it only performs the typing and releasing functions and does not serve the person who actually prepares the report - the reporter.

(U) Will we solve this problem, this lack of support to the reporters of NSA, in the next decade? I certainly hope so, and I think it is well within our power to do so. The technology is available today to enhance the reporters', function beyond the wildest dreams of most reporters. Many people recognize both the problem to be solved and the means of solution, and in several areas, they are already working to develop computer systems to serve reports in the preparation of reports.

EO 1.4.(c)
P.L. 86-36

(U) This paper will attempt to describe some of the problems which are inherent in the reporting field, both those now felt by reporters and those which must be addressed in the development of a reporting computer system. It will then look at current projects underway which are developing computer systems capable of supporting reporters. Some of these systems are not intended to serve reporters but could do so with little additional effort. We will look at the possibilities available for reporting computer systems given today's technology, and then discuss some of the ways in which future technology might further enhance a reporter's life. Finally, we will discuss some of the possible changes in the structure of the reporting field caused both by the computer itself and by policy changes in the intelligence community.

Problems To Be Addressed (U)

~~(C)~~ In today's intelligence reporting world, we have reached the dubious position of inundating our customers with reports. We have a great need to tailor our reporting more carefully so that the important pieces of information which U.S. decision-makers need are not lost in the sea of information we are capable of producing.

(U) We have always had a problem insuring quality control. No one wants to publish an erroneous report, but sometimes we don't have time to check all the facts. Sometimes the typist introduces an error into a report that was already carefully checked. And sometimes our intelligence sources present us with erroneous information in the first place. We have established over the years a complex coordination-review process aimed at getting anyone who has information relevant to the subject of the report involved in the production of the report. Of course, this coordination takes time. Sometimes the reviewer makes changes that are wrong, and doesn't take the report back to the originator. Sometimes the report has to be revised heavily and therefore must be retyped from scratch.

(U) In the research that goes into an NSA product report, there are a number of onerous tasks that must be performed, which must seem to many reporters as needlessly time-consuming: checking the spelling of placenames, finding the coordinates (because the report goes out electrically and has no maps), getting people's names spelled right, conforming to the myriad regulation about format, preparing the coversheet so that the accounting system will work. All these are tasks which must be done but are not a part of what the reporter thinks of as his primary function - presenting relevant facts to a customer so that the customer can make informed decisions on behalf of the country.

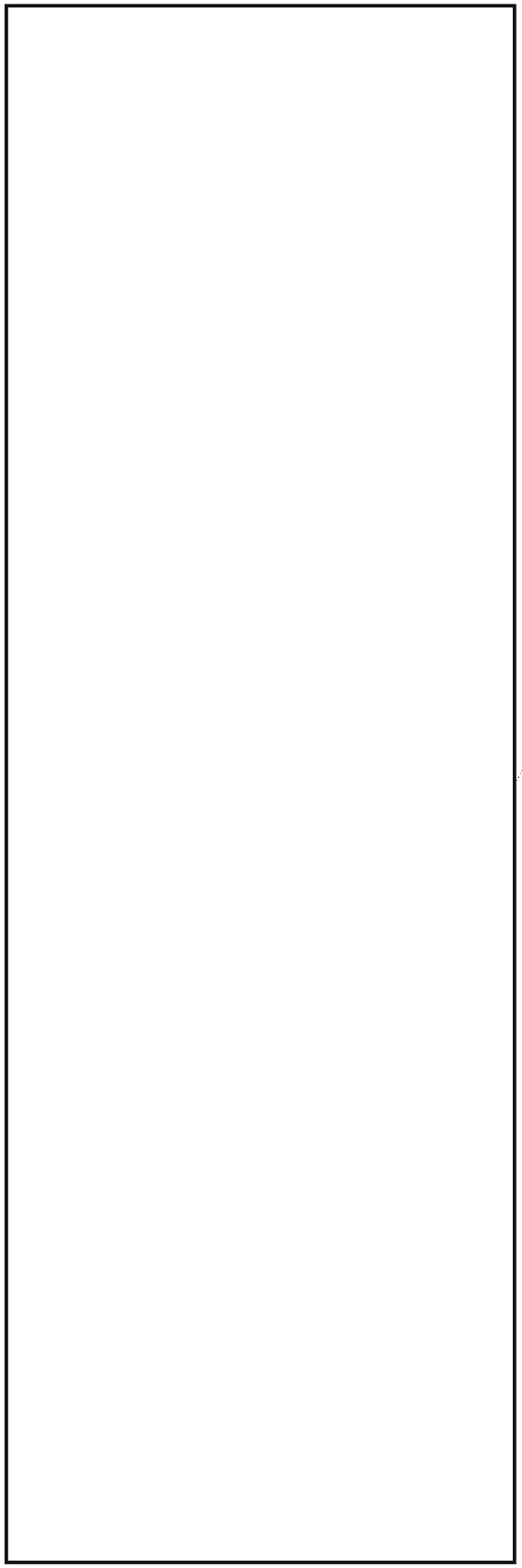
~~(C-CCO)~~ Accounting for what we do is very important to the proper management of limited resources. We are now trying to connect formal requirements and their satisfaction through the use of computers, but reporters are finding that it takes a lot of extra time to prepare the complex coversheet that puts the needed data into the management program. And that doesn't include the time spent keypunching all that information. Hooking the reporter to the computer could save time and at the same time eliminate the keypunching.

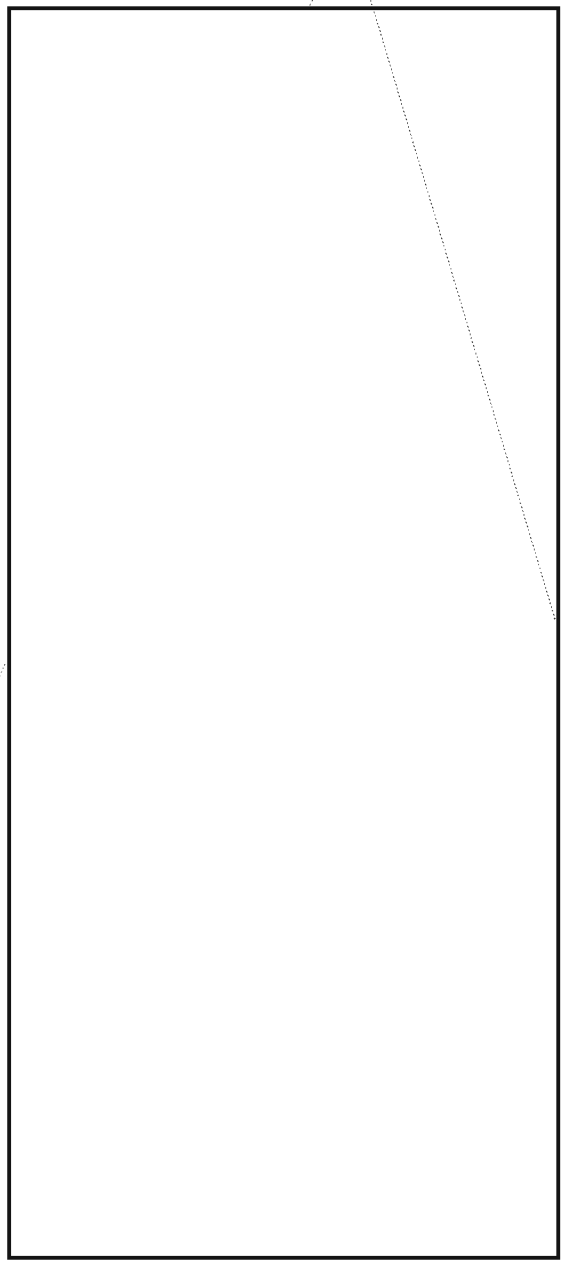
(U) How fast can we report information? How fast do we need to? Without trying to definitively answer those questions, let us say that there are numerous times when our reporting was not fast enough to suit the situation. On a limited basis, we have the capability to speed up reporting but it takes a heavy toll in resources. How much of the delay is in the report research and preparation process itself? Some might not agree with me but I would claim that today most of the delay is in the report preparation process. We have enabled intelligence to be expeditiously intercepted and decrypted, but we have made little progress in translating and reporting quickly.

~~(C-CCO)~~ Some problems which are introduced with the computer are the dependability of the computer system, and the security of the data. If the computer goes down, do we have all our analysts sit on their hands until it comes back up? And in the security area, we have potentially horrendous problems. We have built up over the years an incredibly complex system of compartments, codewords, and clearances, to the point that many people don't know which things they are cleared for. Can the computer help us deal with this problem, or will the potential for inadvertent access to someone else's data exacerbate the problem beyond belief?

Current Systems and Projects (U)

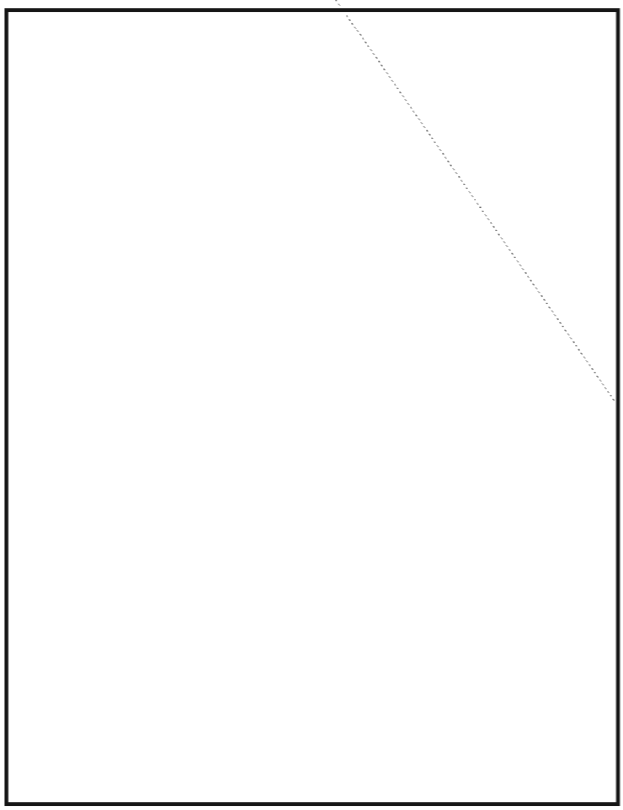
(U) There are almost as many covernames in NSA as people, and a person could be forgiven if he got confused. But let's look at a few of the names in the field of analytic computer systems.





Possibilities With Present Technology (U)

(U) The TRS-80 and similar so-called "personal" computers have more than enough power to satisfy most reporter's needs today. With communications interfaces, such computers provide the technological basis for a reporting computer network capable of revolutionizing the way we do reporting at NSA.



(U) It goes without saying that there are a number of problems that would have to be solved before this utopian picture can be developed. The present tubes are rather small and can only display a limited amount of information. The present computer systems have numerous problems with both turnaround and dependability. A couple of developments in the computer field may help in this area: failsoft technology, in which pieces of a computer can work independently of one another; and distributed processing, in which each user or small group of users has an independent computer tied to other computers only for data transfer. All the problems are solvable. The major question is whether our institution will solve the various problems; whether it, or we, are committed to improving the effectiveness of reporters through the use of computers. Can we? Will we?

Future Technology (U)

(U) The TRS-80 has been called the "Model T" of the computer industry. The era of cheap computing power is here today, and the pace of technology development has been increasing for several years. There is no reason to expect anything other than a continuing fast development rate in new computer technology over the next ten years.

(U) Already there are rumors flying, about computers that will interpret the spoken word. Can you imagine simply talking to your computer terminal, to give it instructions or to "write" reports? Undoubtedly, such machined will be on the market in the next few years.

~~(S-CCO)~~ Developments in microtechnology and high speed computer circuits promise to produce desktop computers with more power than 25 Cray-1's. (The Cray-1 is the fastest general purpose computer available today, and sells for about $10 million. We use a Cray-1 to attack the most sophisticated cipher systems.)

(U) More compact terminals may result from developments in the plasma display field, using a flat display instead of a cathode ray tube. This will make the "terminal on every desk" concept more practical. Combined with the extra power available, each user might have a complete processing system on his desk, tied to a central system only for data transfers.

(U) High quality facsimile transmission at a reasonable cost is just around the corner. With consumers tied to NSA through a facsimile/data network, "electrical" reports with graphics become possible. Our local computer might help to generate the maps, requiring no more instructions than a list of the placenames to be identified. Charts and graphs will also be practical in such a system.

Possible Re-Structuring of the Reporting Function (U)

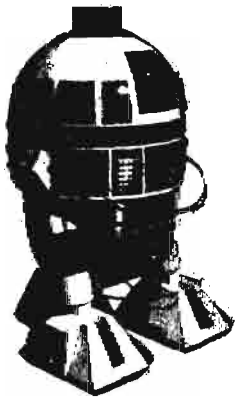
~~(C-CCO)~~ Last year, NSA was studying a system that could result in a massive restructuring of the way in which reporting is done. This was not generated by technology but rather represented an attempt to simplify the world of codewords for intelligence consumers. The program, called APEX, was a matter of some confusion here at NSA. APEX called for "decompartmentation" of intelligence, meaning generally the sanitization of material so that it could be distributed without codewords. APEX is now dead, but some of the ideas contained in the project live on. There is still

a hugh demand for sanitized SIGINT. This might mean producing some additional reports with detach lines, or it could involve producing two versions of a single report, one of them sanitized.

~~(C)~~ Imagine, if you will, applying such a system to all SIGINT reporting. I am sure you will agree that a computer would be an invaluable tool in editing and reviewing reports which must be sanitized for wider distribution. If we stop and take a look at the possibilities, we might even be able to redesign the reporting system with an eye on the technology, and take advantage of the technology instead of using it to play catch-up.

~~(C)~~ Ways in which we might restructure the reporting function to take advantage of technology include putting more information into data bases, and making more of that data base information available to users at multiple access levels through sanitization. We might tailor our reporting to fit the needs of individual users, by having the computer scan the available intelligence information and select items by using a dictionary of relevant terms. Our requirements process might be different in that consumers could simply input their keywords into their computer terminals, instantly updating the requirements dictionary. The NSA system could automatically compare the consumers' input and access level with the available NSA information and route the appropriate information as it becomes available. Management reports could be available instantly on which user requirements were being satisfied and which were not. Analysts at NSA might refer to the unsatisfied requirements data base to help them prioritize their workload. Supervisors might use it to assign work to analysts. This information might even be used to alter our tasking of intercept resources on a real-time basis.

[redacted]



EO 1.4.(c)
P.L. 86-36

Conclusion (U)

(U) In conclusion, let us consider the challenge of the 80's: to integrate technology that is available, and that is becoming available, to improve the efficiency and the effectiveness of the reporters at NSA, and to alter the ways we do our reporting to better serve our present and future consumers within the budgetary constraints place on us. My contention is that we can do our present job of serving intelligence consumers better and more cheaply by taking advantage of the existing technology. The decreasing number of secretaries at NSA is already a problem, and one that seems unsolvable. Lack of staff people to coordinate reports and a continuing need to maintain quality control create pressures to use computers to assist the reporting staff in maintaining the quality for which NSA is renowned.

(U) How to do this? First, we need a coherent policy regarding the use of technology to serve the reporting function. If my contention is correct - that technology can enable us to do our present job better and more cheaply - then we are wasting valuable resources by our continuing failure to use the technology available to us already.

(U) Second, we must have a driving force. The purpose of this paper is to pull together ideas from throughout NSA and from the computer world, and to present them to reporters and managers in NSA as a means of helping to create such a driving force - namely, the reporters and managers in NSA. If we sit around waiting for the T organization to recommend new and better uses for technology in support of the reporting function, we will grow old and gray before anything happens. This is not intended to be an indictment of the T organization, merely a statement of the realities of life. The T organization exists to serve the other organizations of NSA, including Operations. If we want to update the reporting technology here, we must ask - demand - that it be done. And we must take an active role in specifying in great detail how the job is to be done.

(U) The possibilities are almost endless, but the challenge is ours. The technology is there and more is coming. But we must take an active role in developing our understanding of how the technology can help us and in seeing to it that we make the fullest possible use of the technology.

DOCID: 4009838

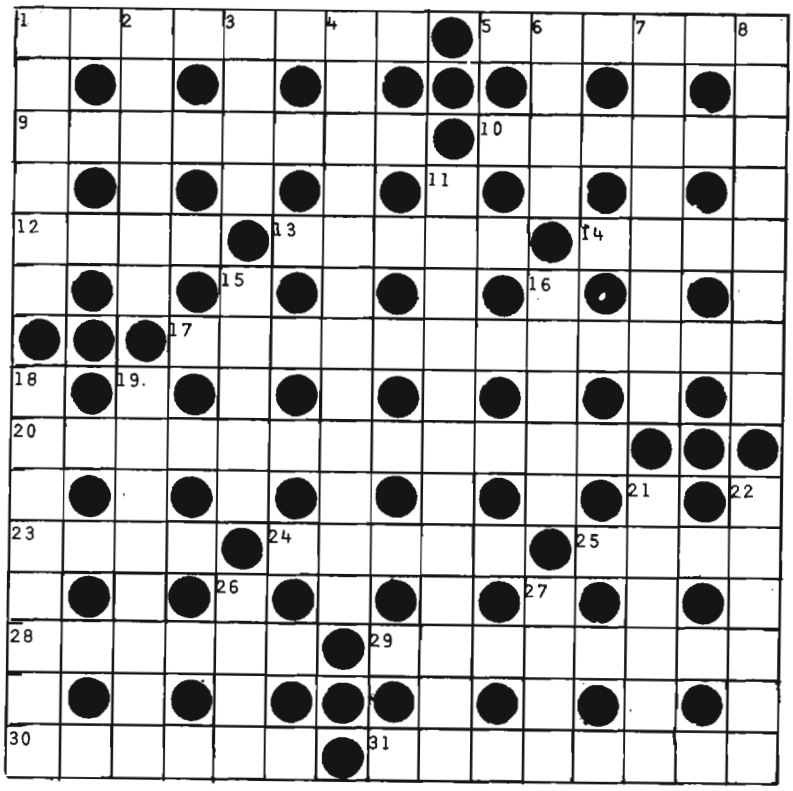
CRYPTIC CROSSWORD

BY [redacted]

Puns.
Anagrams.
Constructions.
Double definitions.

[redacted] CRYPTOLOG's *Information Science Editor, has constructed this excellent crossword puzzle, done in the cryptic, or British, style. (But beware of 5 Across; that one's pretty awful.)*

P.L. 86-36



ACROSS

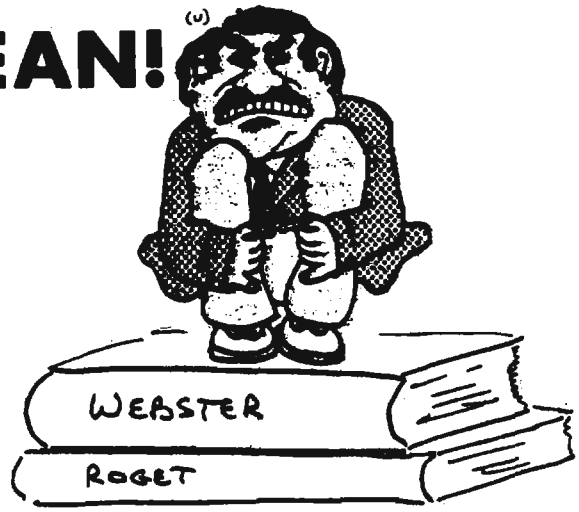
1. Average second bites are vegetables. (8)
5. Could this be where amputated limbs are thrown? (6)
9. Small overthrows combined in great poems. (8)
10. A child or a place in Mexico. (6)
12. Consumes teas in a sloppy manner, (4)
13. Weasel out of orders to attack. (5)
14. A kick from the team's top untried draft choice. (4)
17. I hear the sea left the fiend's farm machine so he could show us his wares. (12)
20. Otherwise calm mediator possessing emotional appeal. (12)
23. It's not often the meat isn't overcooked. (4)
24. Less confused about a tradition at Easter. (5)
25. A peachy coat for policemen? (4)
28. Myth of the ankle, perhaps? (6)
29. Religious gentleman takes a note back to provide work for the secretary. (8)
30. Did the bug clear his throat for the *Star Spangled Banner*? (6)
31. Snake has Richard Henry confused about a small prisoner. (8)

DOWN

1. A sentry stationed at the fence? (6)
2. The right side ejects from bed. (6)
3. Somehow the line forms in the river. (4)
4. *Another* ewe into paint; need we ask again? (8, 4)
6. Enough space to anchor around. (4)
7. The faction favoring pipes put together the merchandise. (8)
8. I sort art for Arnold's kind, among others. (8)
11. Gather #50 scheme for the European Recovery Program. (8, 4)
15. Rushes, we hear, through the book. (5)
16. Draw off five hundred droplets. (5)
18. Destroy the rum label? No! It'll be useful next April. (8)
19. Very good! Every one is not left behind. (3, 5)
21. Roman god adds eyes, we hear, to restore a flat. (6)
22. Blossoms as a sound heard over the meadow? (6)
26. At one time, at the induction center. (4)
27. Scandinavian in a Japanese rickshaw. (4)

DOCID: 4009838

SAY What You MEAN!



by David W. Gaddy

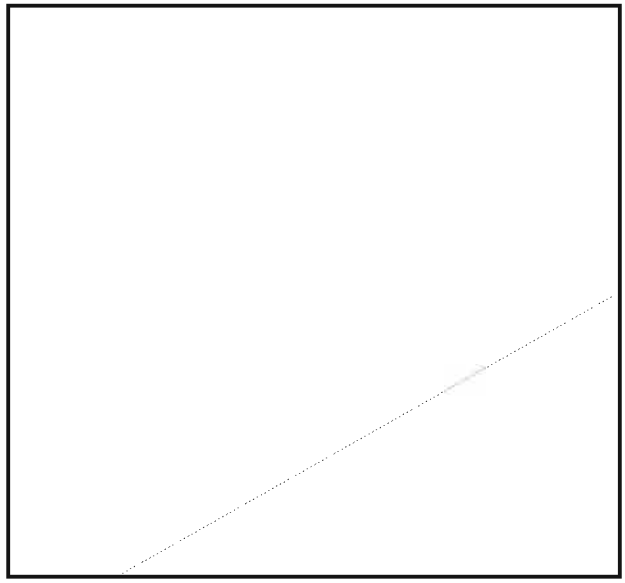
(U) Over time, jargon becomes accepted usage, but in its application there can be confusion of meaning. "Sanitization" is an example. Part of the confusion arises from our traditional view of the COMINT handling system, a view which must be modified if we are to communicate effectively among ourselves and our colleagues in the Community. What follows is a reflection on "lessons learned" during the APEX study of the past two years and an attempt to clarify terminology now in wide (but often differing) use.

~~(C-CCO)~~ To set the stage by stating the obvious (so obvious it may be overlooked), the body of information under discussion, COMINT, is classified. It is TOP SECRET, SECRET, rarely CONFIDENTIAL. (Unthinkable a few years back, there is also unclassified COMINT of a historical nature, but we are concerned here with current COMINT.) It also has at least one additional attribute: it usually has a codeword or a restriction that it be handled only in COMINT channels, the COMINT "compartment." This is the information which, from World War II U.S. Army usage, is frequently called "special intelligence," or SI. Since SI is now limited to COMINT, it has become a euphemism - some even mistakenly (but with the same result) think it equates to "signals intelligence."

~~(C-CCO)~~ For years most of us have thought of "compartments" as those small, cloistered efforts, usually distinguished by a covername, which are now, for the most part, covered under the VRK (Very Restricted Knowledge) system. (See USSID 16 for details.) It still comes as a mild shock to be reminded that the COMINT handling system is itself a compartment (or "special access program," as compartments are termed in Executive Order 12065). Here is the definition of "compartment" as developed under APEX and approved by the DCI/NFIB. It represents but a slight modification of that contained in the 1978 DCI/NFIB "Glossary of Intelligence Terms and Definitions":

> compartmentation: Formal systems of restricted access established and/or managed by the Director of Central Intelligence (DCI) to protect the sensitive aspects of sources, methods, and analytical procedures of foreign intelligence programs.

The generic term in Community use is "sensitive compartmented information," SCI. COMINT, or SIGINT handled under the COMINT system, is therefore a form of SCI. (Although we are concerned only with special access programs in an intelligence context, there are other such programs, especially those created for military operational purposes.)



EO 1.4.(c)

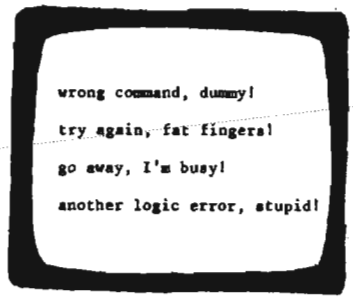
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Ed Note: It may have been the conductor on the Orient Express who said it first, as the detachment of Turkish soldiers got off the train at Vienna: "I think we shall have to sanitize that compartment."

HOW TO CREATE A USER-*Un*FRIENDLY SYSTEM

by



P.L. 86-36

(CISI Workshop, May 1981)

None of us sets out deliberately to bring unfriendly human/machine interfaces into the world. Somehow, even though we are trying our hardest to design and build good software, the user interface all too often turns out to have some serious defects when it is delivered and people start using it. Some of the defects can result in increased error, waste of expensive man-hours, and waste of machine resources. If the users have any choice, and things are bad enough, they may simply refuse to use the system, and find other ways to get their work done. If they don't have a choice, their work efficiency may suffer significantly. The worst aspect of the situation is that the losses are hidden; the machine is not down, some amount of work is flowing through the system, and there is no obvious stoppage or breakdown that can be singled out to warn us that a lot of time and effort may be going down the drain unnecessarily.

My main purpose here is to raise your consciousness about the needs of the user, and how some kinds of design decisions can affect the convenience and supportiveness of the user interface in an interactive system. I have a strong feeling, based on studies I have made of several Agency systems, that many of the unfriendly features are unnecessary. Some, it is true, are forced on us by prior commitments to specific formats or procedures, or by file security and file integrity requirements. The majority of the features that make problems for users come about, however, simply because the designer and programmer were optimizing other variables, without thinking about the effects on the user. Their priority lists are headed by other things, and the user is way down in the stack. They are concentrating on saving space, getting around weaknesses in the programming languages and operating systems, meeting demands of the sponsor for performing given functions, and beating deadlines.

In the midst of these pressing preoccupations, it is all too easy to forget that we are designing a system that will interact with a user. From his point of view, the system will exhibit behavior, just like another person or animal. If its behavior is puzzling, contradictory, and frustrating, the user will have a lot of trouble getting along with it. If it leaves him hanging, not knowing what to do next, and he has to dig through a badly-written manual while his work waits, his time and the system resources are being needlessly wasted, when we could have told him what he needed to know in a simple message on the screen. If system messages mislead the user, or if data-entry procedures are confusing and inconsistent with normal usage, we are designing in a source of constant error. All it takes, in many cases, is a slight re-wording of a message, addition of information to an incomplete message, or standardization on one set of field labels or procedures, to solve these problems for the user. Very rarely will the changes toward user-friendliness require any major sacrifices in efficiency, running time, or ease of debugging or maintenance. In fact, the same changes that make a a system more predictable and convenient for a user are likely to make it easier to maintain and debug

as well.

I guess what I am trying to sell to you is the need for a lot more EMPATHY TOWARD THE USER. Interactive programs are basically different from the kinds of programs that read in a batch of data, chew on it a while, then spit out a batch of answers to be read later at a user's desk, or run on another computer. At least half the work in an interactive system is being done by that user out there, who is carrying out a continuous exchange of information and instructions with the system. When we design such a system, we cannot afford to let ourselves forget that we are creating BEHAVIOR. The interface that the user sees will have characteristics that significantly affect his work efficiency. We have to find a way to keep in mind what the user is trying to do, what expectations he brings to the task, and how he will perceive what the system is saying to him. At any given point in an interactive dialog, the user has certain expectations in terms of information he needs and timeliness of response to avoid breaking his train of thought. You, the system designer and programmer, have built up that set of expectations (whether knowingly or not) in the sequence of dialog steps that preceded the screen the user now sees. Whether we like it or not, when we design and implement an interactive system, we are creating behavior, and we are creating a conversation. If we are going to do it right, we must somehow get into the habit of empathy, imagination, putting ourselves in the user's place, at all stages of our work.

WHY IS IT SO HARD TO SEE THE USER'S VIEWPOINT?

Unfortunately, there aren't very many good tools and techniques yet to help designers change their point of view from the old "batch" way of designing programs. Most of us still tend to approach an interactive system design task pretty much as if it were a batch program. A task is specified by a sponsor who has certain requirements; we know what computer system and programming language we will use; we go ahead and write A PROGRAM which will do the job within those constraints. We treat the interactive user as if he were a tape drive, a card reader, or any other input device that we get data and parameters from. Instead of sending a seek to the disk, or a read to the tape drive, we send a message to the user. This is a very poor way to look at an interactive task! People are not like disks or tape drives, for better or for worse. Somehow we must develop diagramming and planning techniques, modelling and prototyping skills, and useful practices and guidelines for this new and special kind of programming and design involving dynamic give-and-take between user and system.

WE NEED A COURSE IN INTERACTIVE SYSTEM DESIGN

I would very much like to see a course in "Design of Interactive Computer Dialogs" taught at our School. There are a number of courses being taught at Universities and Colleges, and in private industry. Videotapes are available from at least one source I know of, Dr. Ben Schneiderman at the University of Maryland. An excellent course is offered by Dr. J. D. Foley at GW. There are also a number of research efforts under way in several places to develop guidelines for interactive system design, and they have published useful papers (e.g., those by Ramsay, et al. and Smith, et al. in the references). I believe that such a course should be practical in its orientation. It should include at least one real design project. And it ought to be required in our Data Systems Professionalization program!

TOOLS TO HELP THE DESIGNER

In the near future, there will be new aids for designers of interactive systems. We will be able to use the power of interactive systems themselves in the design process, with rapid prototyping and planning packages similar to the PSA/PSL system currently in use by T-Group for program design. I believe that we could gain useful techniques and tools right now from the Computer Aided Instruction (CAI) field. Designers of computerized courses have developed a lot of experience in building one type of interactive dialog. A study of CAI packages and techniques, and an attempt to transfer useful ideas to interactive system design, would amply repay our effort. Unfortunately, our need is pressing and we don't have these tools at our fingertips today. There are still some informal methods we can use to help us visualize and manipulate the essential structure of an interactive session from the user's point of view. The diagramming method I am suggesting in this workshop is a simple, pencil-and-paper aid you can use right away to try out ideas and see how they will impact the user, to compare different designs, and to trouble-shoot bad spots in an existing dialog.

EXAMPLES OF GOOD AND BAD USER DIALOGS

As a way of demonstrating the importance of empathy toward the interactive system user, I will present several examples of poor design, chosen from actual NSA systems in current use. The examples will be disguised, to avoid needless embarrassment to designers, managers, and programmers associated with them. Features of several real systems may be lumped together into one artificial "system" for the sake of a dramatic illustration. The essentials of each feature will be retained, with surface details changed to conceal the source. "Rock-throwing sessions" are destructive to all concerned, and my intention is not to criticize any specific system or Agency element. In many cases, the particular unfriendly feature I have chosen to describe is only a small part of a system which is otherwise very helpful to users. With just a little forethought to avoid making needless problems for the user, these excellent systems could be performing far better. I will also present some counter-examples to illustrate good, "user-friendly" designs for contrast. Some of these are chosen from the same real-life Agency systems as the "bad" examples. (For reasons of space, the examples were not included in this paper, but were presented in my talk at the workshop only.) First, let's look at the basic shape of an interactive session - the structure that makes it essentially different from a batch program run.

THE STRUCTURE OF A DIALOG

I will illustrate these points with a convenient method of diagramming an interactive user dialog, which emphasizes the dynamic structure of the interaction. Fig. 1 shows a diagram of a simplified typical dialog. The circles are states of the user, and the arrows are exchanges of information between him and the system which move the user to a next state. Each step from one state to the next involves a user input, followed by a system response. In this analysis, we are interested in the USER's states; the system, too, has states, but we are seeing them entirely through the user's eyes at present, because it is the user's viewpoint we are trying to model and understand in this exercise. The action starts when the user sits down at the terminal and LOGS ON. When the system receives his log-on, it can either accept him, at state 1, and display a message, prompt, or menu, or else it can refuse him and give him (we hope) a clear message telling him what is wrong, at state 4. If his log-on is accepted, the system gives the user access to what I will call the TOP LEVEL of the dialog. Here he has a chance to select one of a set of major actions he can perform on the system. They can be commands he may type in, files he may call up, numbered choices from a menu, or function buttons he may press. When he selects one of these actions, the system will again respond by either giving him access to the subsystem he has requested (file, command, routine, package, etc.) or displaying a message warning him that he is unauthorized to use it, or has made an error in his input.

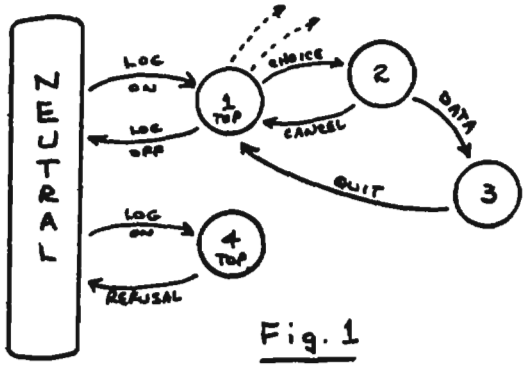


Fig. 1

The function the user has chosen may offer him still another set of choices, leading to another level of subsystems, or there may be a linear chain of actions and responses between user and system, involving no further choices of dialog paths, but continuing until the action is done (data entry, record retrieval, computation and display of a result, etc.), for instance, the step from state 2 to 3 in figure 1. After the user has viewed the display, or the system has completed work behind the scenes and given the user a message, the system may automatically return the user to a higher level and let him choose a new action at that level, or else it may ask him where he wants to go next. Eventually, the user will decide to quit work, or else the system will automatically terminate his session and he will be returned to the top level, where he will LOG OFF. At any point in the dialog, the user may suddenly see that something is wrong, or else he may have to break off his work unexpectedly, so he will need to ABORT or CANCEL the dialog and return to a higher level before work at the current level has terminated normally. In many existing systems, the top level is special, in that a user cannot ordinarily bypass it by an interrupt from inside the dialog. His interrupt will get him back to the top level, where he must LOG OFF to get out of the system entirely. This is because logging on and off

are often handled by the operating system, while lower levels of dialog are handled by a specific routine or software package under the operating system. Some systems allow users to log off directly from one or more states within a subsystem without having to return first to the top. At each state, the system gives the user specific displays that must tell him what he needs to know to select the next transition. No matter what else may be going on behind the scenes in the host computer, disk files, mass memories, network connections, data links, etc., ALL THE USER'S DECISIONS MUST BE BASED ON WHAT HE SEES ON THE SCREEN RIGHT IN FRONT OF HIM HERE AND NOW. As the designers and programmers of the user interface, we have to find a way to tell him just what he needs to know right now, to make the best choice of his next action. Why make him guess at incomplete information, try to remember lists of commands, or recall data displayed on earlier screens? You are unnecessarily adding to his burden and detracting from his effectiveness in the primary task he is performing with the system.

The table below is a state-transition matrix. It provides a useful way of summarizing information concerning pairs of states, or data associated with each transition allowed by the dialog in figure 1. This particular table shows user inputs (U) and system responses (S) for each transition. An X indicates that the transition is not allowed by the dialog. Such a table is a convenient method of reviewing all the possibilities and planning or analyzing an interactive dialog.

CURRENT STATE	NEXT STATE: NEUTRAL	1	2	3	4
NEUTRAL	X	U:log on S:top menu	X	X	U:log on S:refusal
1	U:log off S:feedback	X	U:choice S:prompt	X	X
2	X	U:cancel S:top menu	X	U:data S:display	X
3	X	U:quit S:top menu	X	X	X
4	U:-- S:message	X	X	X	X

Figure 2 shows a diagram of a dialog with a user-interrupt transition skipping from State 3 directly back to the top level, bypassing an intervening State 2, and skipping State 4, which ordinarily would have come next.

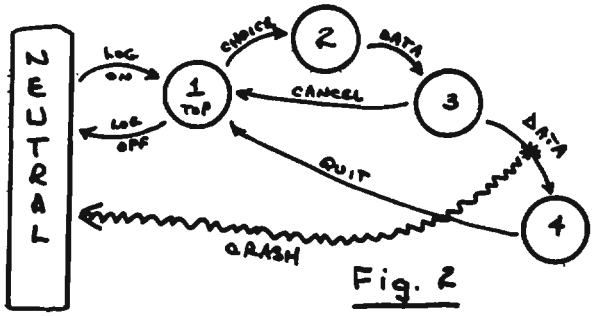


Fig. 2

For instance, suppose that a user has logged on, and at State 1 has asked for a file-update package. State 2, inside the file-update part of the dialog, has given him a data-entry format to fill in on his screen (State 3). While entering data, the user suddenly realizes that he should first have retrieved a record to check its contents before making the updates. He enters a command canceling the data entry screen, removing the effects of any data he may have entered already, and returning him directly to the top level, where he may request the retrieval subsystem and make his query. It is useful for the designer to make a state-transition table including all the "cancel" or "user interrupt" transitions he will allow, and listing the items of data or program variables that must be reset to clean up the loose ends at each point. This is also a good method of deciding where we can reasonably permit the user to cancel, without creating too much chaos in the data base or program variables. In general, it is more "user-friendly" to allow user-interrupts at as many points in the dialog as can reasonably be managed.

Before he logs on, and after he logs off, the user is in a special "neutral state", where he is not directly affected by anything the system does. In this state, he is not engaged in any dialog with the system. Once he logs on, and from then until he logs off,

he is more or less closely coupled with the system, and his actions are directly affected by the give-and-take of the dialog. At each of his states within the dialog, he expects to see certain data, within a certain range of time-frames. He has specific uncertainties which must be resolved completely by the display on the screen, if he is to be able to continue working effectively. The system designer must be aware of this mental context built up by the previous steps of the interaction, and provide what the user needs to know right where he needs it. The diagram can help us by factoring out each transition and letting us consider just what path or paths have led the user to a given state. A state-transition table can help us organize and review all the items of information the user has supplied to the system and expects to receive from the system at each state.

Figure 2 shows another situation, which can happen in this all-too-imperfect world. Imagine that the user has worked his way to State 3 again. Suppose, for instance, that he has called up the retrieval subsystem (State 2), entered a query (State 3), and is waiting for the system to display the retrieval on his screen. Suddenly, he finds himself not at the top level, but all the way back at the neutral state, out of contact with the system. The dialog has been stopped dead, the screen is unresponsive, and when he pushes a key, nothing happens. The system has CRASHED in midstream, perhaps leaving a multitude of messy loose-ends hanging behind the scenes.

The way this experience feels to the interactive system user must be lived through to be truly understood. The best way to describe it is to say that one minute the user is closely involved in a lively give-and-take with a responsive, talkative entity, and suddenly everything has died on him. It is a very peculiar and frustrating feeling, a little like running into a wall. Whenever this happens to a user, he will have some very strong uncertainties that must be resolved somehow by messages or pre-arranged procedures, so that he can put his work back together and get going again with a minimum of lost motion after the system comes back up. In addition, THERE IS A STRONG EMOTIONAL RESPONSE of frustration and alarm, especially if the user knows that a lot of his work will be lost: not just the last action he performed, but perhaps hours or even days of earlier work as well. A state-transition table including "crash" transitions back to the neutral state can help us review the possibilities and plan what loose ends need to be cleaned up and what recovery features need to be provided to the user.

The diagrams can be a handy aid for "doodling" while you are planning an interaction. If you are a designer, they can help you to see the structure of a user interface from the user's viewpoint. They can help to make clear what are the successive choices a given design puts before the user, and what data he needs at each point to decide where to go next. If you are a user, you might find it an interesting exercise to try diagramming all or a portion of a user dialog for a system you use, especially a part of it that often gives you trouble. Experiment with various kinds of matrices and tables of data associated with state-pairs, for instance user performance times, system response times, user inputs and system messages, etc. The examples in these handouts will provide some illustrations. The references at the end of this paper list several sources where state diagrams for interactive dialogs are discussed. These references were brought to my attention by Joan McDonald, R8.

SOME HANDY RULES OF THUMB

Below are some guidelines that express the "moral" of the illustrations I presented in the workshop.

1. Don't make the user give you redundant information; get it from him once and use it efficiently behind the scenes. (E.g., if you ask him for his name and can look it up, you shouldn't need to ask for his initials and his social security number too. If you have a password, you shouldn't need anything else to identify him.)

2. Don't leave the user looking at a blank screen after he has input a command or data. Give him a message ("Document number not found", "retrieval ended", "retrieval failed") or at least a prompt to tell him what level of dialog or state he is in so he has an idea what to do next, especially if the command he just input has failed.

3. Don't build data entry formats or representations into your dialog which are counter to normal usage. You are laying the foundation for persistent user errors that will waste far more time in error checking and recovery code than the extra trouble to

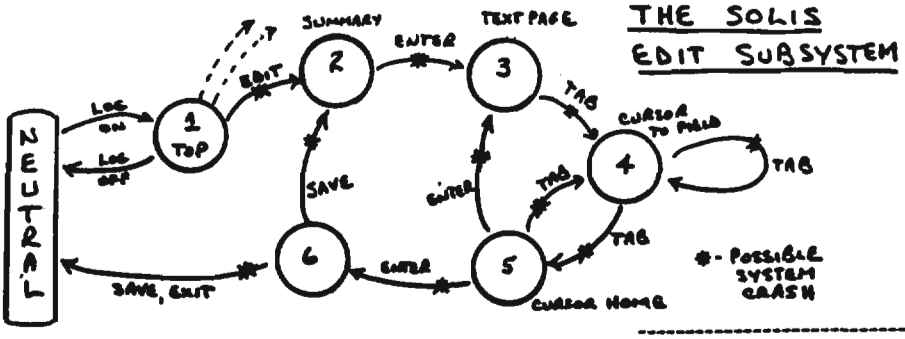
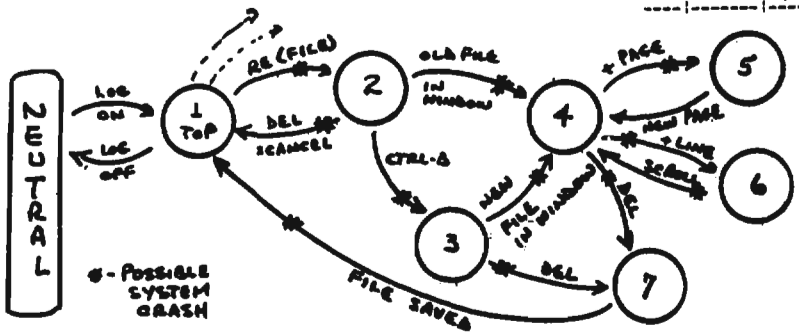


Fig. 3

CUR-RENT	NEU-TRAL	NEXT 1	2	3	4	5	6
NEU-TRAL	X	U:1.on S:top T:2min	X	X	X	X	X
1	U:1.off S:ackn. T:6-10s	X	U:edit S:dsply T:6-10s	X	X	X	X
2	U:-- S:crash	X	X	U:enter S:text T:6-10s	X	X	X
3	U:-- S:crash	X	X	X	U:tab S:field T:0	X	X
4	U:-- S:crash	X	X	X	U:tab S:field T:0	U:tab S:home T:0	X
5	U:-- S:crash	X	X	U:enter S:text T:6-10s	U:tab S:field T:0	X	U:enter S:prompt T:6-10s
6	U:exit S:top T:6-10s	X	U:save S:dsply T:6-10s	X	X	X	X



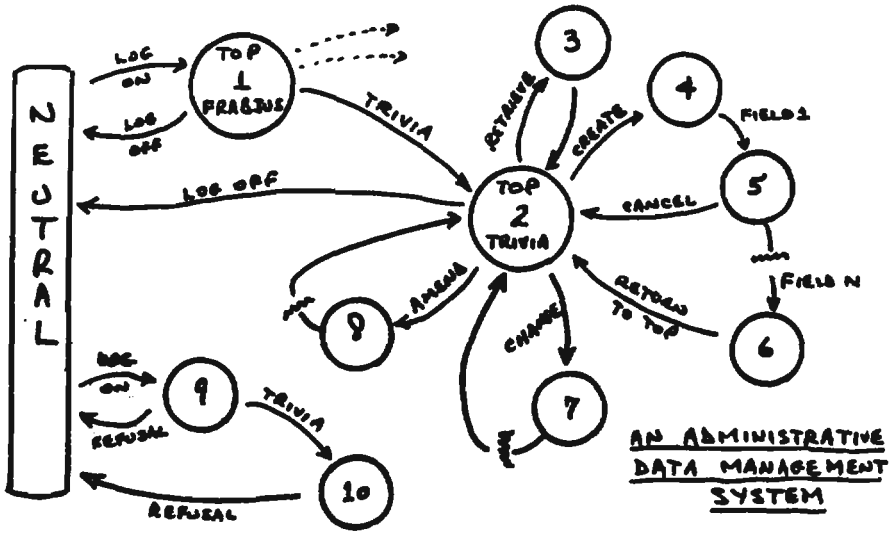
RAND EDITOR

Fig. 4

CUR-RENT	NEU-TRAL	NEXT 1	2	3	4	5	6	7
NEU-TRAL	X	U:1.on S:top%	X	X	X	X	X	X
1	U:1.off S:messg	X	U:re(f) S:wndow	X	X	X	X	X
2	U:-- S:crash	U:del S:messg	X	U:ctl-B S:new f	U:old f S:dsply	X	X	X
3	U:-- S:crash	X	X	X	U:new f S:dsply	X	X	U:del S:save f
4	U:-- S:crash	X	X	X	X	U:+page S:new p	U:+line S:scroll	U:del S:save f
5	U:-- S:crash	X	X	X	U:data S:dsply	X	X	X
6	U:-- S:crash	X	X	X	U:data S:dsply	X	X	X
7	U:-- S:crash	U:-- S:top%	X	X	X	X	X	X

CRASH: states 4,5,6, keystroke recovery file
states 1,2,3, user recovery not needed
state 7: after hit "del", recovery not possible

Examples from Other Systems



CUR-RENT	NEU-TRAL	NEXT 1	2	3	4	5	6	7	8	9	10
NEU-TRAL	X	U:l.on S:top	X	X	X	X	X	X	X	U:log on S:refuse	X
1	U:l.off S:messg	X	U:trivia S:prmpt	X	X	X	X	X	X	X	X
2	U:— S:crash	X	X	U:retrv S:dsply	U:create S:prmpt	X	X	U:change S:prompt	U:amend S:prompt	X	X
3	U:— S:crash	X	U:exit S:prmpt	X	X	X	X	X	X	X	X
4	U:— S:crash	X	X	X	X	U:data S:prmpt	X	X	X	X	X
5	U:— S:crash	X	U:cancl S:prmpt	X	X	X	U:data S:prompt	X	X	X	X
6	U:— S:crash	X	U:exit S:prmpt	X	X	X	X	X	X	X	X
7	U:— S:crash	X	U:exit S:prmpt	X	X	X	X	.X	X	X	X
8	U:— S:crash	X	X	X	X	X	X	X	X	X	X
9	U:— S:messg	X	X	X	X	X	X	X	X	X	U:trivia S:refuse
10	U:— S:messg	X	X	X	X	X	X	X	X	X	X

provide a natural format in the first place! If a field is to contain dollars and cents, permit the user to insert a decimal point, and edit it out later if you must. If the data structure behind the scenes requires an odd-ball representation of dates, times, etc., let the user enter them in a natural, easy-to-remember form and do the needed conversion in the software. When you display them to him, convert them behind the scenes back to the form he is used to.

4. Don't let different parts of the same system use different formats, procedures, or representations for things that are the same to the user. Use the same method of error warning and correction throughout all the data entry routines of a system. Use the same convention for "default" or "null" data entries and command selections. If one subsystem provides a list of options "1", "2", "3" and asks the user to pick one, don't use a similar display with numbered items to mean something else in another subsystem. If some subsystems tell the user "PROCESSING COMPLETE" at the end of their actions, as a way of letting him know he is back at the top level, all subsystems should do so, rather than some of them leaving the user looking at a blank screen. If you display a review after data entry in a form, always give the user the same way of indicating "correct" or "wrong" and making corrections, throughout all data-entry routines of a single system.

5. When you send an error or warning message to the user, tell him clearly what is wrong, where the error is, and what he can or must do next. Don't just say "invalid code"; give him a list of what the valid codes are, or provide a "help" or "?" command that will display them to him without interrupting the interaction. Don't just say "index out of range"! Tell him the name of the variable, and what was in it ("I=0", "X=9999999"). If the message indicates that something is wrong which the user can't fix, give him a phone number to call for help, and keep the message up to date so the number is right.

6. If certain data to be input by the user must function as key elements in the data structure or the procedures on which the task is based, let him input them at the beginning, check them thoroughly right away, and give him a chance to correct them if needed. Don't wait until he has entered several pages of a form before you tell him "WRONG SSN - FATAL ERROR" and make him re-enter all the other data.

7. If there are requirements for contents or formats in data entry fields, check for them right away and let the user correct errors for each field as he enters it. Don't give him a review of several fields at once, one of which may be incorrect, unless you also provide a forms-entry interface with tabbing from field to field and protected field boundaries.

8. Don't use different labels or abbreviations for field names, commands, or other key words in different parts of the same dialog or system. If a field is called "AMOUNT" in one display, call that field the same thing in every display or message that refers to it (not AMT one place, MONEY someplace else, "FUNDS" someplace else). Don't choose labels or abbreviations that look alike or are confusing. While an experienced user may be used to some of these, you are making it needlessly hard for a new user to learn and remember them. Experienced users have a way of leaving, and all users have to start out as new users sometime.

9. If there is information at the top of the screen the user needs to see, be sure it doesn't get scrolled off before he gets to use it. If you aren't sure it will still be there when he needs it, display it again; don't count on its being visible now just because you displayed it a few steps earlier.

REFERENCES

Foley, J.D., Notes and Lectures in a course taught at G.W. University, Fall 1980

Foley, J.D, and Wallace, V.L., "The Art of Natural Graphic Man-Machine Conversation", Proceedings of IEEE, Vol. 62, No. 4, April 1974, pp. 462-471.

Giloi, W.K., Interactive Computer Graphics, Prentice-Hall Inc., 1978, pp. 205-207.

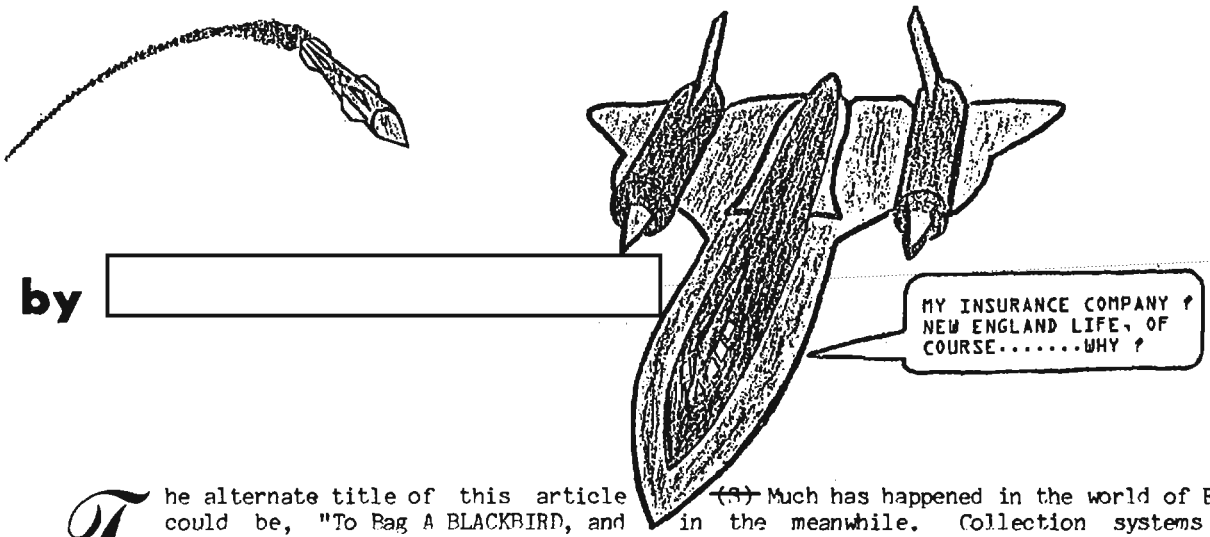
Newman, W.M., "A System for Interactive Graphical Programming", AFIPS Proceedings of Spring Joint Computer Conference, 1968, pp. 47-54

Ramsay, H.R., and Atwood, M.E., "Human Factors in Computer Systems: A Review of the Literature", Science Applications Inc. Technical Report SAI-79-111-DEN, 21 September 1979.

Smith, S. L., "Requirements Definition and Design Guidelines for the Man-Machine Interface in C3 System Acquisition", MITRE Technical Report M80-10, 15 April 1980.

DOCID: 4009838

OPELINT is Alive and Well in B Group



by [redacted] P.L. 86-36

~~(C)~~ The alternate title of this article could be, "To Bag A BLACKBIRD, and Other SIGINT Tales," and it might start with a conversation something like this:

"Hello, Ralph? You know that SAM site that isn't there?"
"Yes, Jim, what about it?"
"It just launched two SAM's at the SR-71."
"Oh, no!"

[redacted]

~~(S)~~ Five years ago, [redacted] excellent article, "Yes, Don, There Is An ELINT!" (CRYPTOLOG, August 1976), brought ELINT out into the bright light of day for many. His TECHELINT oriented piece invited a companion article from an OPELINT-er in A, B, or G Group. No one has yet responded to the challenge, so this article will hopefully begin to fill that void.

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

~~(S)~~ Much has happened in the world of ELINT in the meanwhile. Collection systems have proliferated, measurement capabilities have improved, and in many areas of DDO, OPELINT and COMINT analysts have joined forces against their targets. This inter-disciplinary mingling has spawned a new breed of SIGINT analysts who are equally comfortable on either side of the fence, and who constantly strive to operate on both sides, to produce the highest quality, most accurate SIGINT product available.

~~(S)~~ Much of the credit for this welcome evolutionary stage in the state of the art known as SIGINT production goes to those Agency and Community managers with foresight enough to appreciate the potential of ELINT, who have pushed to popularize and expand the ELINT fusion curriculum in the National Cryptologic School, and who have kept up the successful battle to remove the best ELINT collection from the compartment in which it resided for so long.

~~(C)~~ Managers who have made the choice to make ELINT work in their own SIGINT organizations have found that activism and encouragement are the keys to success. Without these ingredients, the curtain separating the two major components of SIGINT remains

impenetrable, while analysts continue to "go with what they know," rather than trying something new and perhaps strange.

[redacted]

[redacted]

To Pag a "BLACKBIRD" (U)

[redacted]

~~(C)~~ The crux of the dilemma which followed consolidation was how to keep ELINT close to the entity analysts while still achieving the economies of scale offered by consolidation, for OPELINT, worked away from the COMINT it supports, perpetuates the separation of the two.

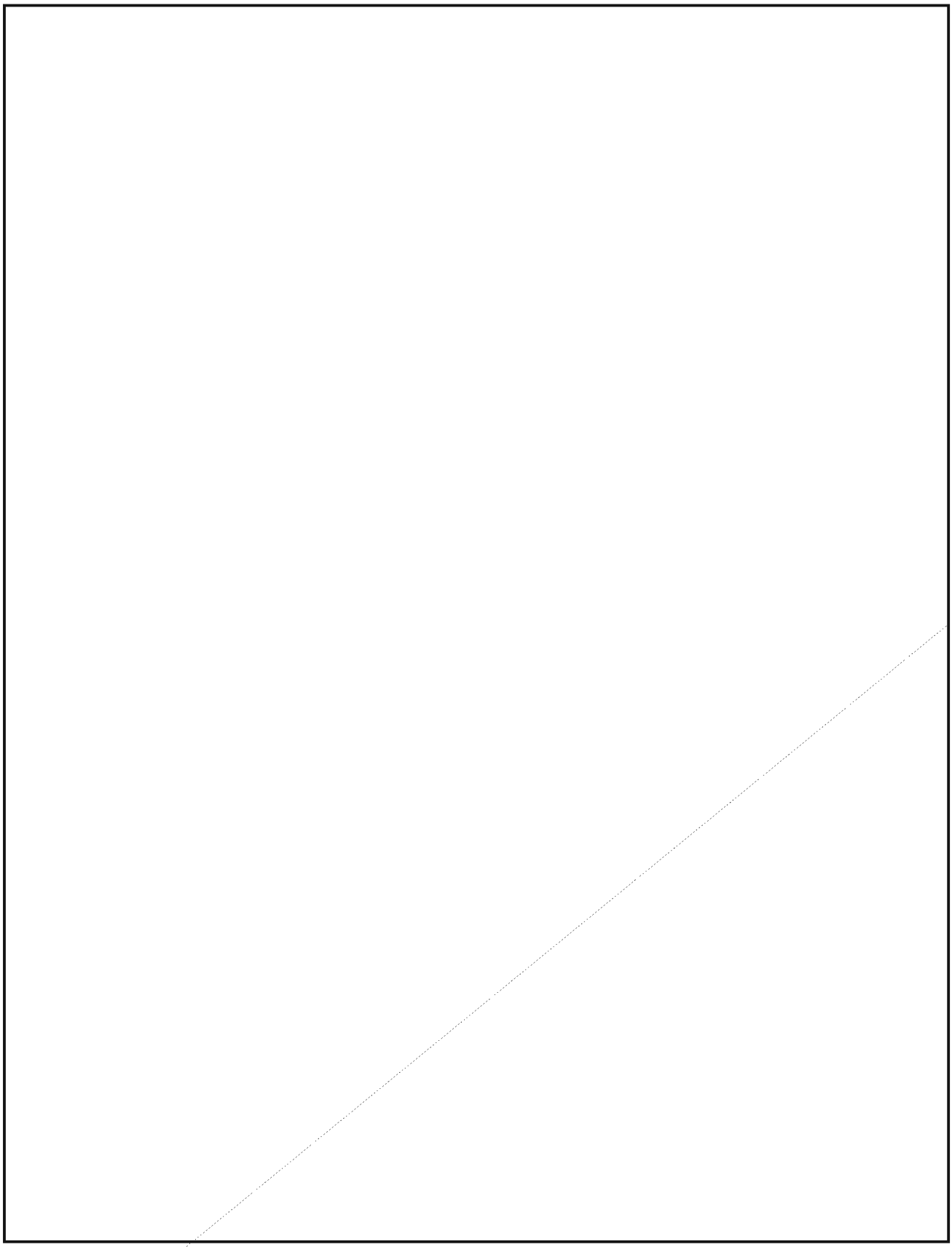
[redacted]

[redacted]

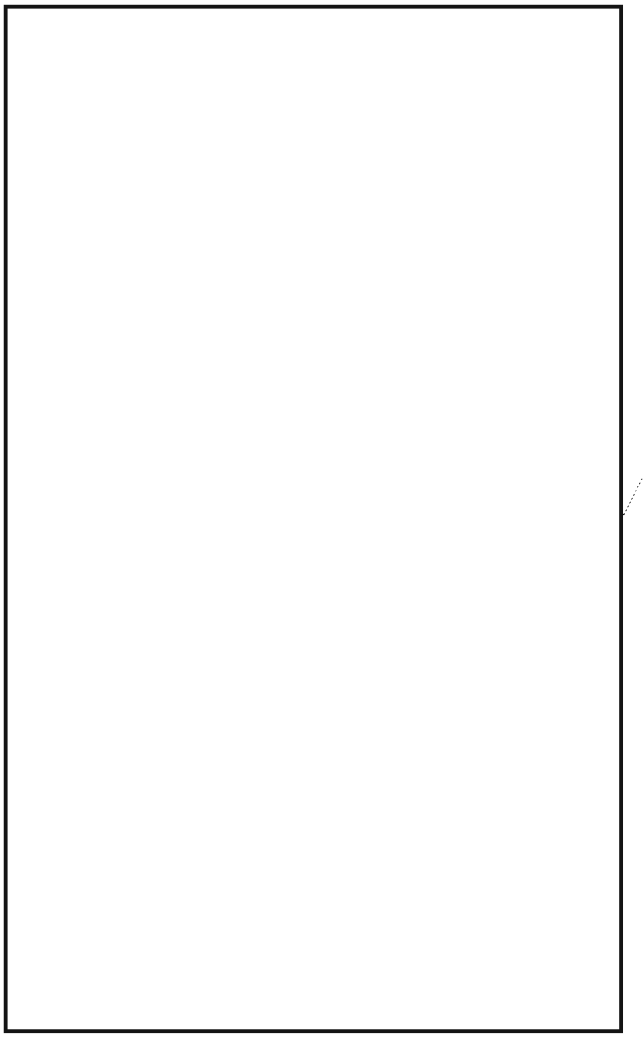
~~(C)~~ As a result, we have a SIGINT analytic fusion effort which really has gotten the maximum mileage out of both COMINT and ELINT in producing a number of significant products and studies with far-reaching implications.

[redacted]

EO 1.4.(c)
P.L. 86-36

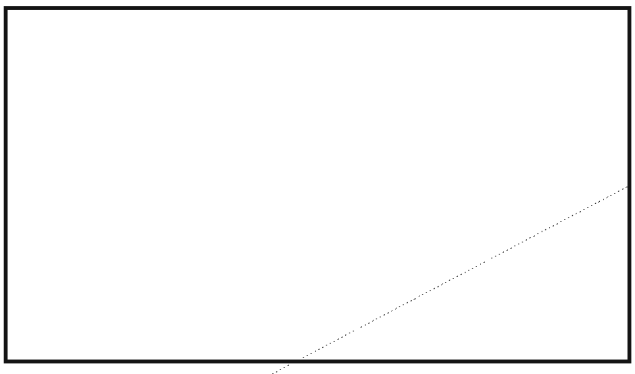


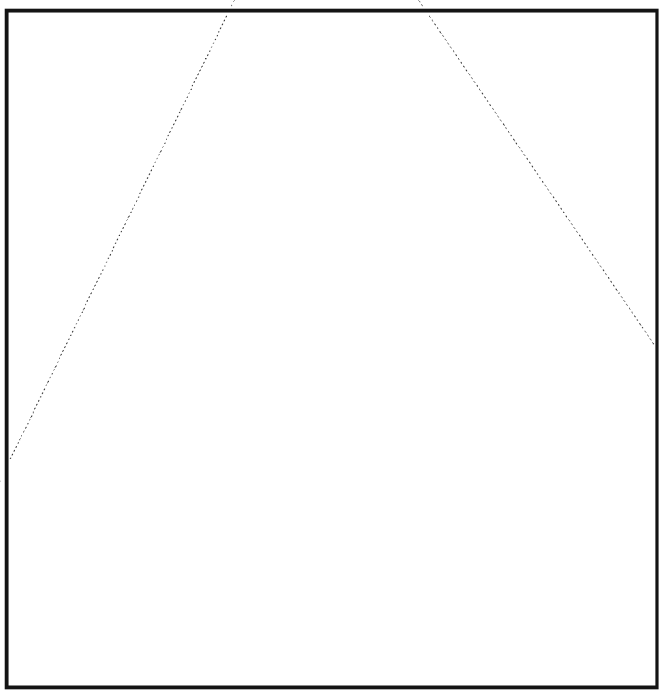
EO 1.4.(c)
~~P.L. 86-36~~



Which Way Did They Go? (U)

~~(S)~~ The reconstruction of a recent SIGINT event scenario serves to indicate how valuable a resource ELINT can be in determining exactly what occurred.





Try It, You'll Like It! (U)

~~(C)~~ In sum, we are still on the uphill side of the learning curve with regard to the best uses of OPELINT, both on its own and in fusion. But the more we learn, the more we find we can do. And , oh yes, who performs these "exotic" analytic routines? Ordinary Traffic and Special Research Analysts, just like you and me, with a more than able assist from a one INSCOM-trained 98J ELINT Analyst.

~~(C)~~ We are all capable of using ELINT to its full potential, given minimal training and practice. Let's bring ELINT out of the closet and into the spotlight it deserves!

SOLUTION TO NSA-CROSTIC No. 35

"Plain English," by [redacted] CRYPTOLOG, May 1977, reprinted from the final issue of C-Liners.

"If we want all Agency personnel to speak and write plain English, perhaps we should first teach Agency personnel English. If we want Agency management to write concise, active, decisive memos, perhaps we should first teach Agency management to be concise, active, and decisive.
"Let us attack the problem, not just hide the symptom."

What do YOU think?

Review:
"Wouldn't It be Nice if We Could Write Computer Programs in Ordinary English -- or Would It?"
I. D. Hill, The Computer Bulletin, June 1972, pp.306-312
by [redacted] P13

P.L. 86-36

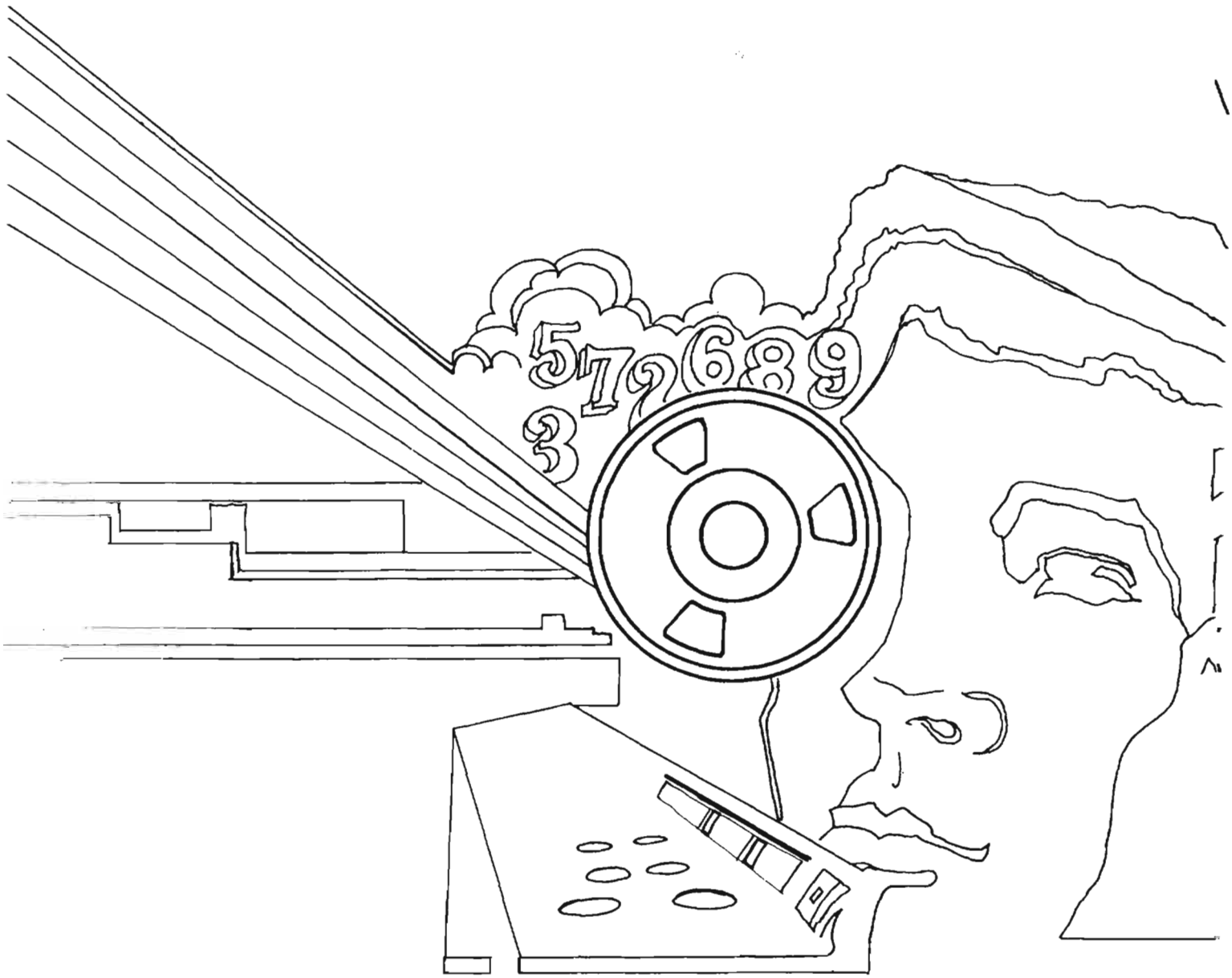
Although this paper was published nearly a decade ago, it is still right on target in an area of computer technology that is receiving even more concentrated attention today. There are many software designers who seem to think that "natural language" (by which they usually mean "everyday, conversational English") is the ideal medium for communication between humans and computers. The arguments for this idea are obvious: we all know English, and nobody has to spend a lot of time and money teaching it to us. Of course, teaching it to computers WILL require tremendous amounts of time and money, if it is ever really possible at all. The "natural language" enthusiasts are convinced that the vast benefits conferred by computer English will counterbalance the costs. Proponents of "natural language" also seem to assume that English is an ideal medium for humans to specify exact and detailed instructions to computers and other humans. Hill has presented some very good arguments against this assumption, and I believe all of us who are concerned with human-machine systems can profit from a careful consideration of the points he raises. If everyday English is ineffectual as a means of conveying exact instructions, it certainly isn't worth spending all that money and time to design English-like programming languages.

Hill's paper presents a very clever and amusing argument against the use of "natural" English for programming. In fact, in a half-serious way, it suggests that English isn't very good for any precise description or instructions intended to guide others' actions; instead, people should learn to use an algorithmic formal language, even in specifying procedures for other people, as well as in working with computers. Hill makes his points about the deficiencies of English very convincingly, in spite of the exaggerations implicit in the humorous view he presents. He makes some other very interesting points - for example, that the unreadableness and general difficulty of legal language, (which attempts to specify something precisely and unambiguously), result from the unsuitability of natural English for this use. He gives some amusing examples of people misunderstanding other peoples' descriptions, and some more serious ones. He uses an ALGOL-like block notation to show the precise meaning (or alternative possible meanings) of many examples quite effectively. Cooking recipes, knitting instructions, and musical notation provide further examples of somewhat better specialized subsets of English; these are incomplete, however, and still open to misunderstandings.

Hill makes the further claim that, even if a way could be found to enable computers truly to understand natural language inputs, there remains a much more basic objection. English just isn't the right language to THINK in while deciding "EXACTLY what is the right thing to do". We would sacrifice precision and power in the way we think about a problem or task, and also in the way we represent the task and possible solutions. We would also lose a main advantage of computers: their reliable obedience in doing exactly what we unambiguously instruct them to do, without a chance of misunderstanding. It wouldn't really be a help to have computer systems that responded, like people, "Oh! but I thought you meant so-and-so!" (especially if you, the human user never realized that the system was acting on a totally different, BUT SENSIBLE interpretation of your instructions until it was too late for correction!) Hill suggests that we start by using an algorithmic form for specifying legal/financial matters (e.g. taxes), many of which have to be programmed into computers anyway.

While this idea of using a "programming" language in communicating with other people seemed bizarre to me at first glance, second thought made it more and more convincing. English phrases, with BEGIN, END, meaningful labels, judicious use of "go-to's", and careful use of parentheses to define scope, with some other conventions defining logical implication, conjunction, and disjunction might prove a highly useful tool. People could switch to an algorithmic description in this language whenever they felt they had not been understood, or use it whenever they anticipated difficulty. It could be taught in elementary schools, especially when terminals and interactive teaching networks become commonplace. I can imagine a highly amusing parlor game involving "charades" or skits, called "What's my program?" In this game, one team would compose a set of tricky "programs" for sets of actions to be performed by the other team; penalty points would be scored for failure to follow the specifications exactly.

What do you think?


5 7 2 6 8 9
3

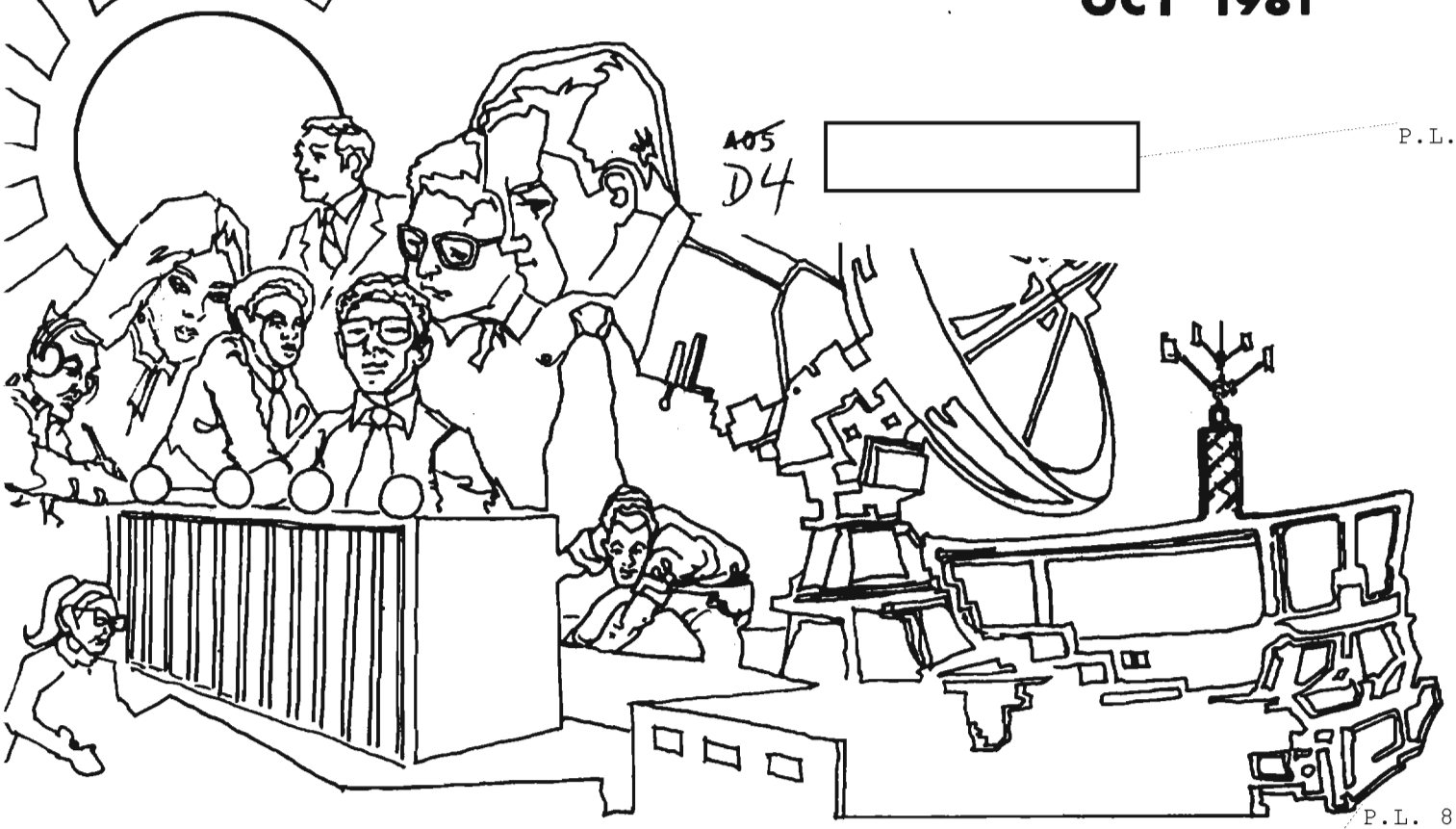
DOCID: 4009837

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

OCT 1981



A05
D4

[redacted] P.L. 86-36

P.L. 86-36

ECONOMIC INTELLIGENCE:
Problems and Prospects (U).....Derek K. Craig.....1

TECHNICAL SUPPORT CATALOGS (U)..... [redacted] 6

NSA-CROSTIC NO. 35 (U).....David H. Williams.....9

THE STAIRWELL SOCIETY (U)..... [redacted] 11

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 10 Oct 2011~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009837

CRYPTOLOG

Published by P1, Techniques and Standards,
for the Personnel of Operations

VOL. VIII, No. 10 OCTOBER 1981

PUBLISHER [redacted]

BOARD OF EDITORS

Editor-in-Chief..... [redacted] (8322s)

Collection..... [redacted] (8555s)

Cryptanalysis..... [redacted] (4902s)

Cryptolinguistics..... [redacted] (5981s)

Information Science.. [redacted] (3034s)

Language.....David Cox (8161s)

Machine Support. [redacted] (5084s)

Mathematics..... [redacted] (8518s)

Puzzles.....David H. Williams (1103s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Taurone (3573s)

For individual subscriptions
send
name and organizational designator

to: CRYPTOLOG, P1

To submit articles or letters
via PLATFORM, address to

cryptolg at barlc05
(note: no '0' in 'log')

P.L. 86-36

EDITORIAL (U)

We are producing fewer technical reports than we used to. The numbers, for those who like statistics, are given by [redacted] in his article on Technical Support Catalogs beginning on page 8.

P.L. 86-36

We can remember when there were typists in each analytic shop, whose job it was to produce the technical reports, the Weekly (or Monthly) Technical Notes, and Technical Support Letters, and various other largely extinct or endangered species of technical documentation. But such people are rare these days. The only typists work in the front offices, and since the 'front office' work tends to have a higher priority, they don't often have very much time for typing a lot of technical reports.

Now and then, one finds an analyst who feels so strongly that some technical reporting ought to be done that he will try to type it out himself, if he can find a decent typewriter. Have you ever seen two or three people fighting over a typewriter?

Anyone who has begun to see what can be done in the analytic field with tools like a desk-side terminal connected with a TSS and PLATFORM, can only wonder why we haven't yet provided the analyst with the tools to produce decent technical reports. All those beautiful ads on TV about modern data systems! All those wonderful words in our plans about what we will have "tomorrow"!

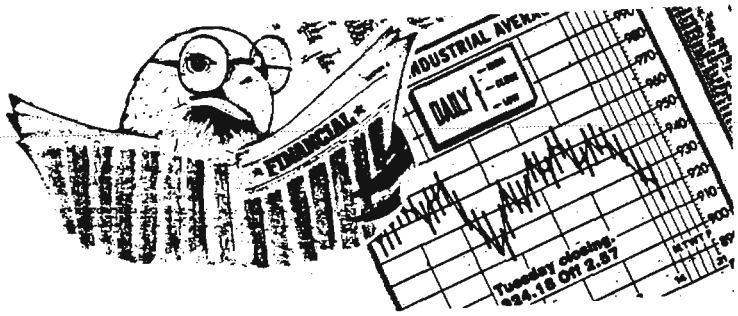
We are reminded of an old friend, no longer here in the trenches, who once said, "There they are in the front office, talking about rockets to the moon and planetary probes; and here I am, trying to light this here fire with this piece of flint!"

W.E.S.

DOCID: 4009837

ECONOMIC INTELLIGENCE: Problems and Prospects (U)

by [redacted]



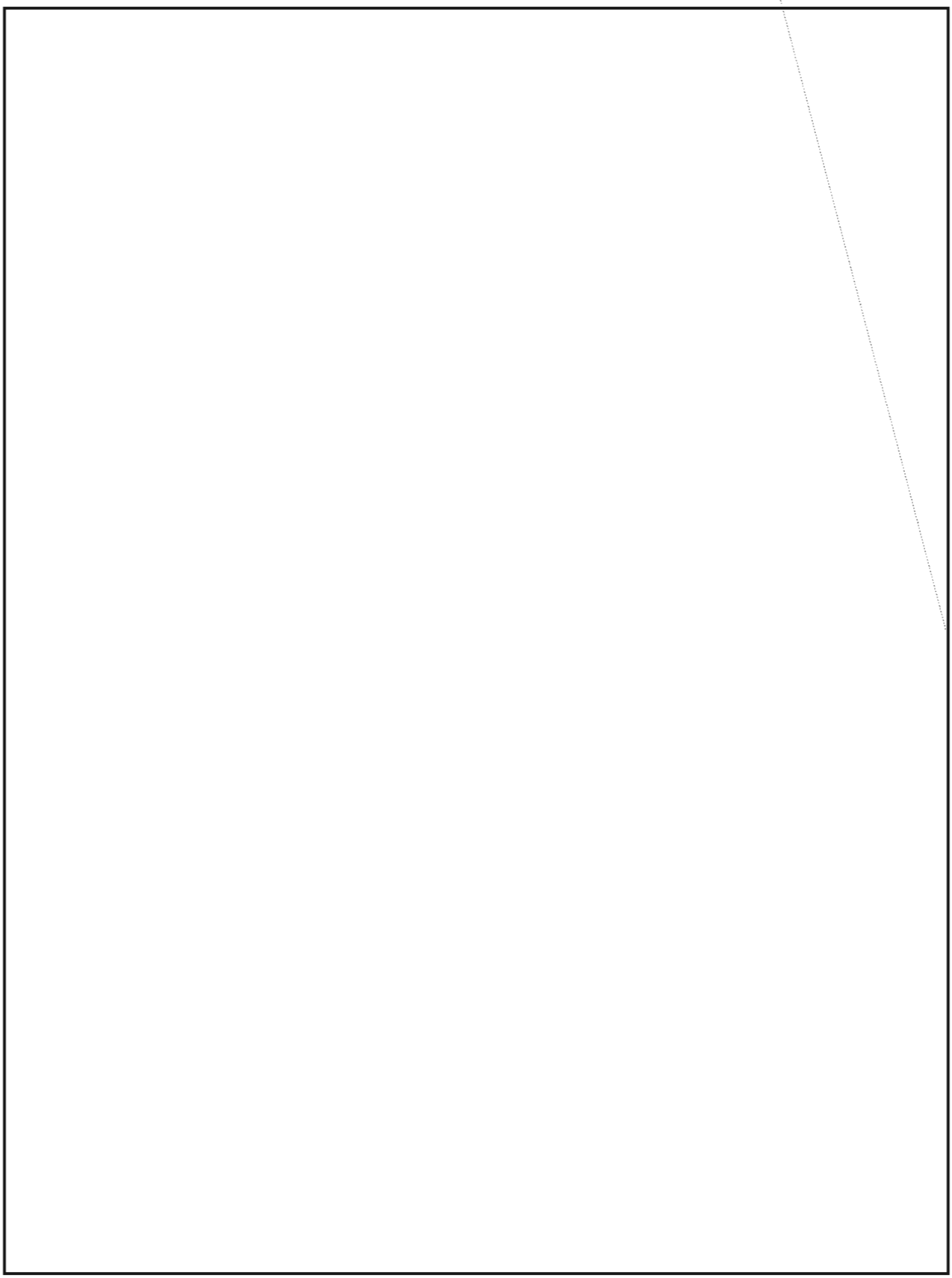
P.L. 86-36

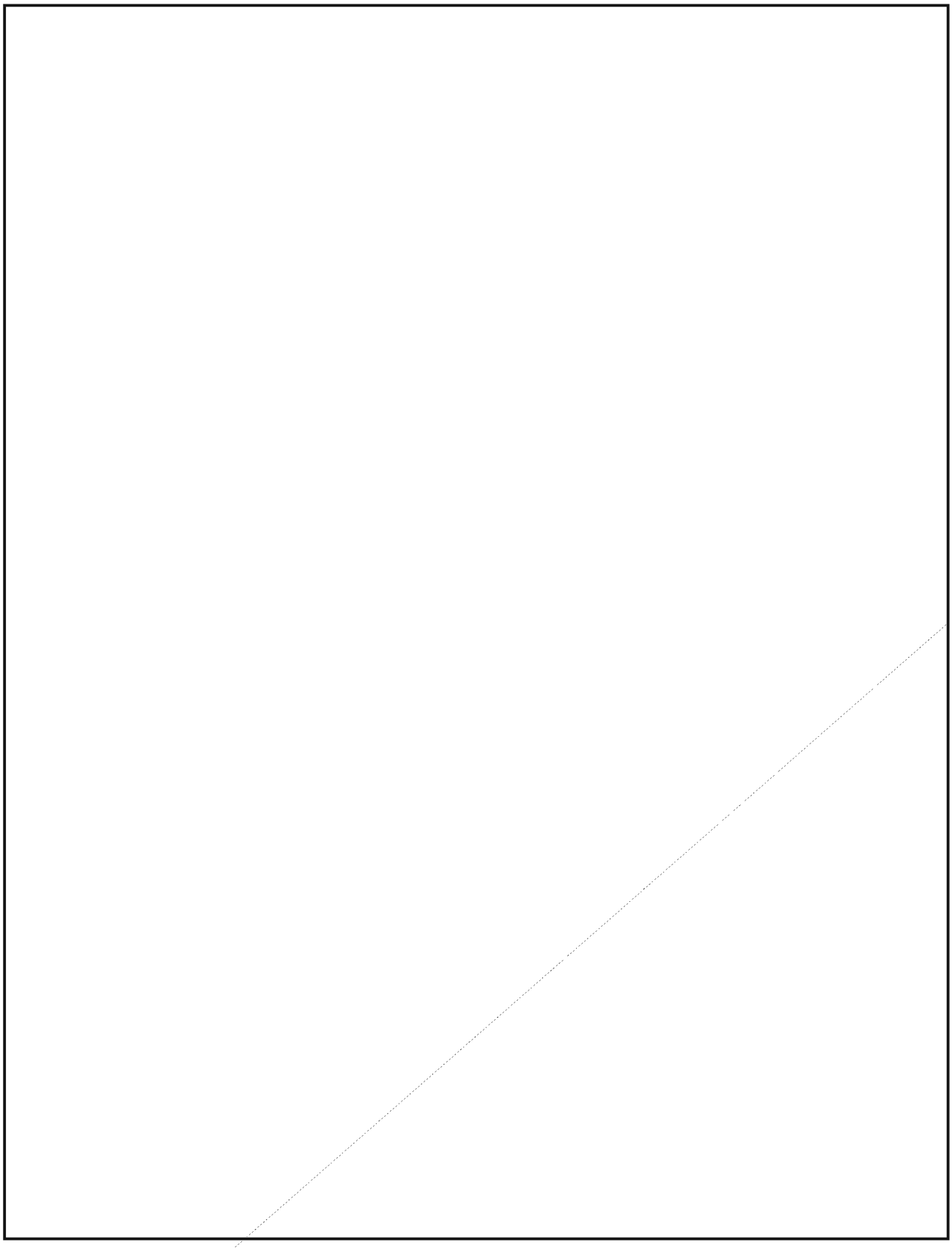
[redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~

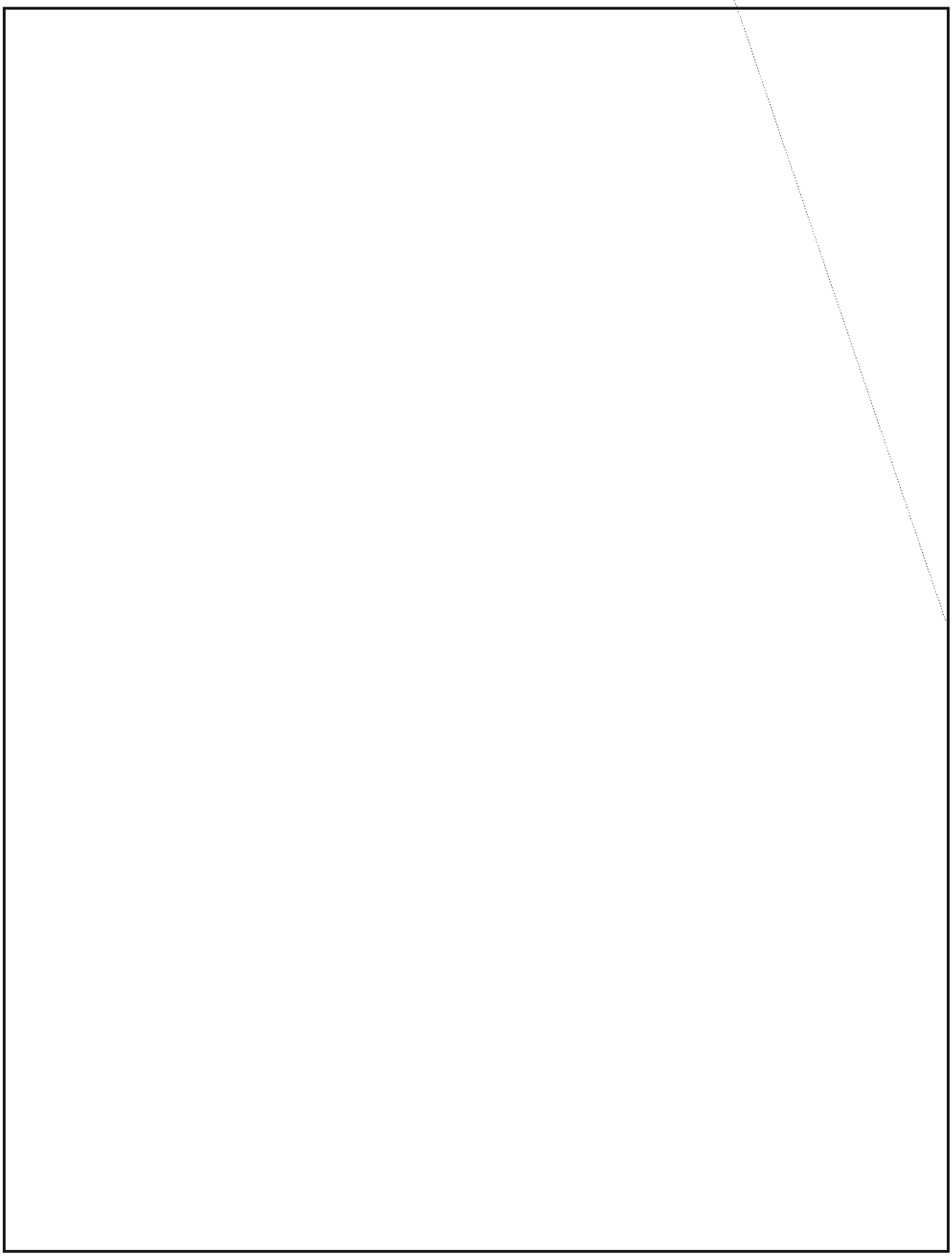




EO 1.4.(c)
P.L. 86-36

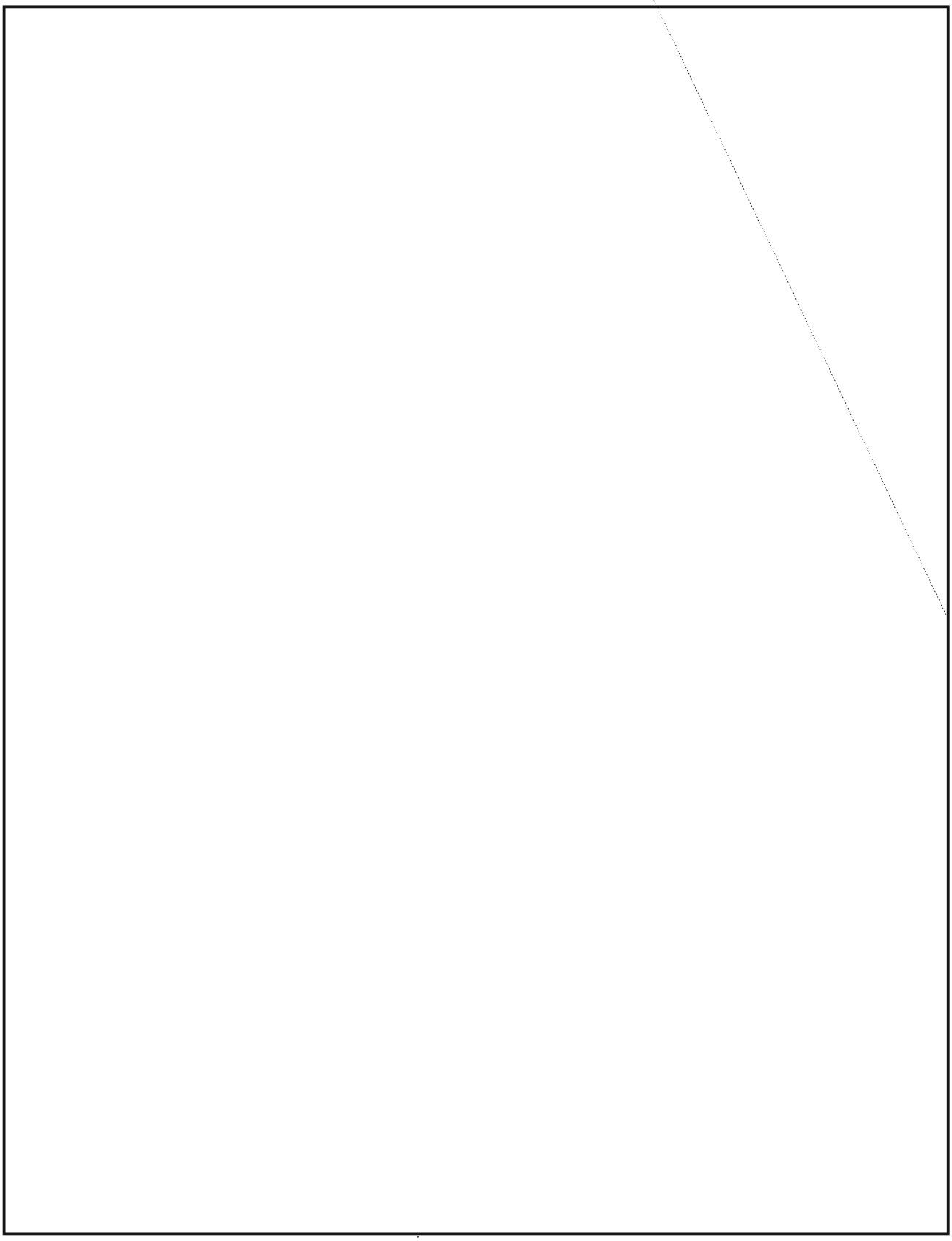
EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~



DOCID: 4009837

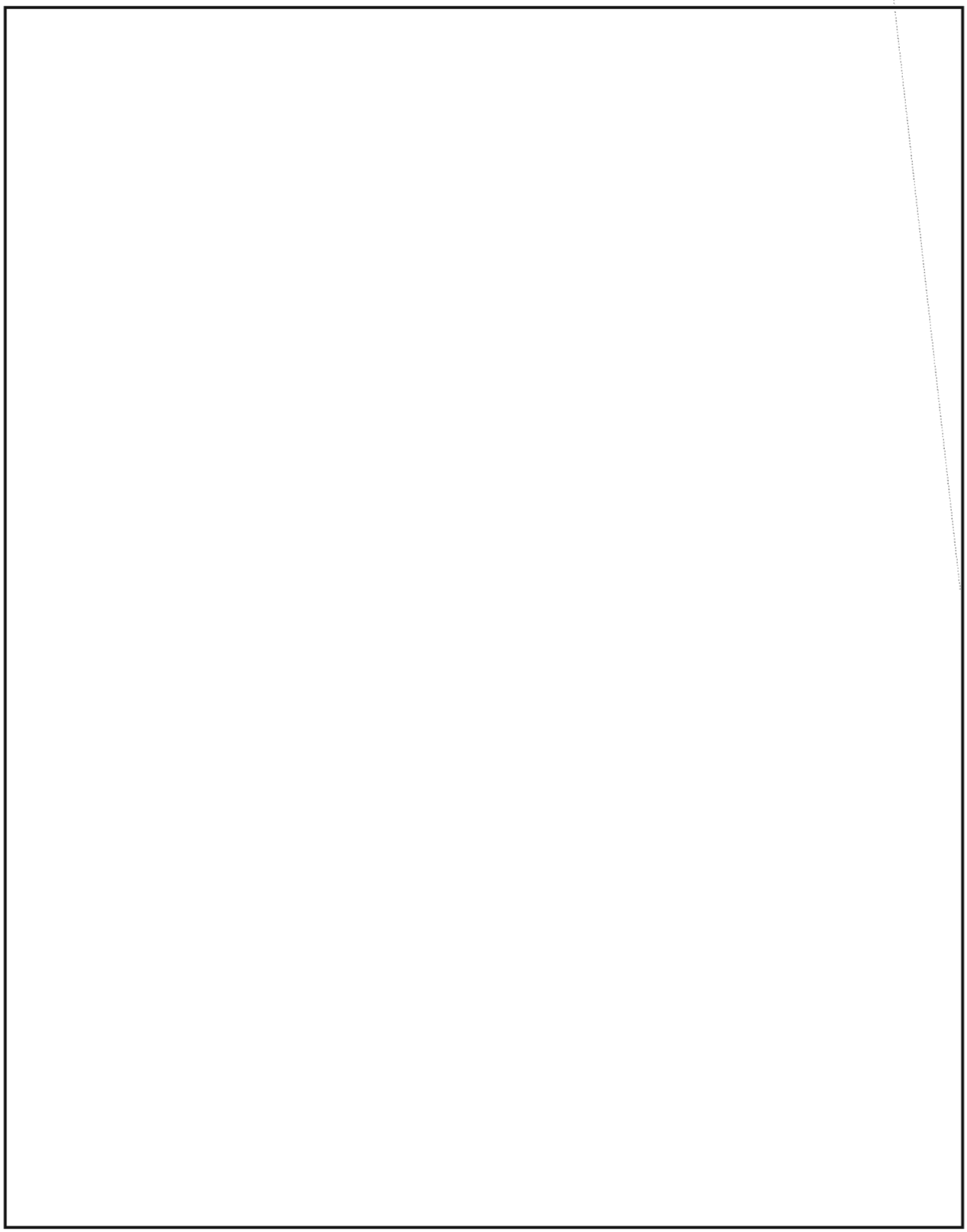
EO 1.4.(c)
P.L. 86-36

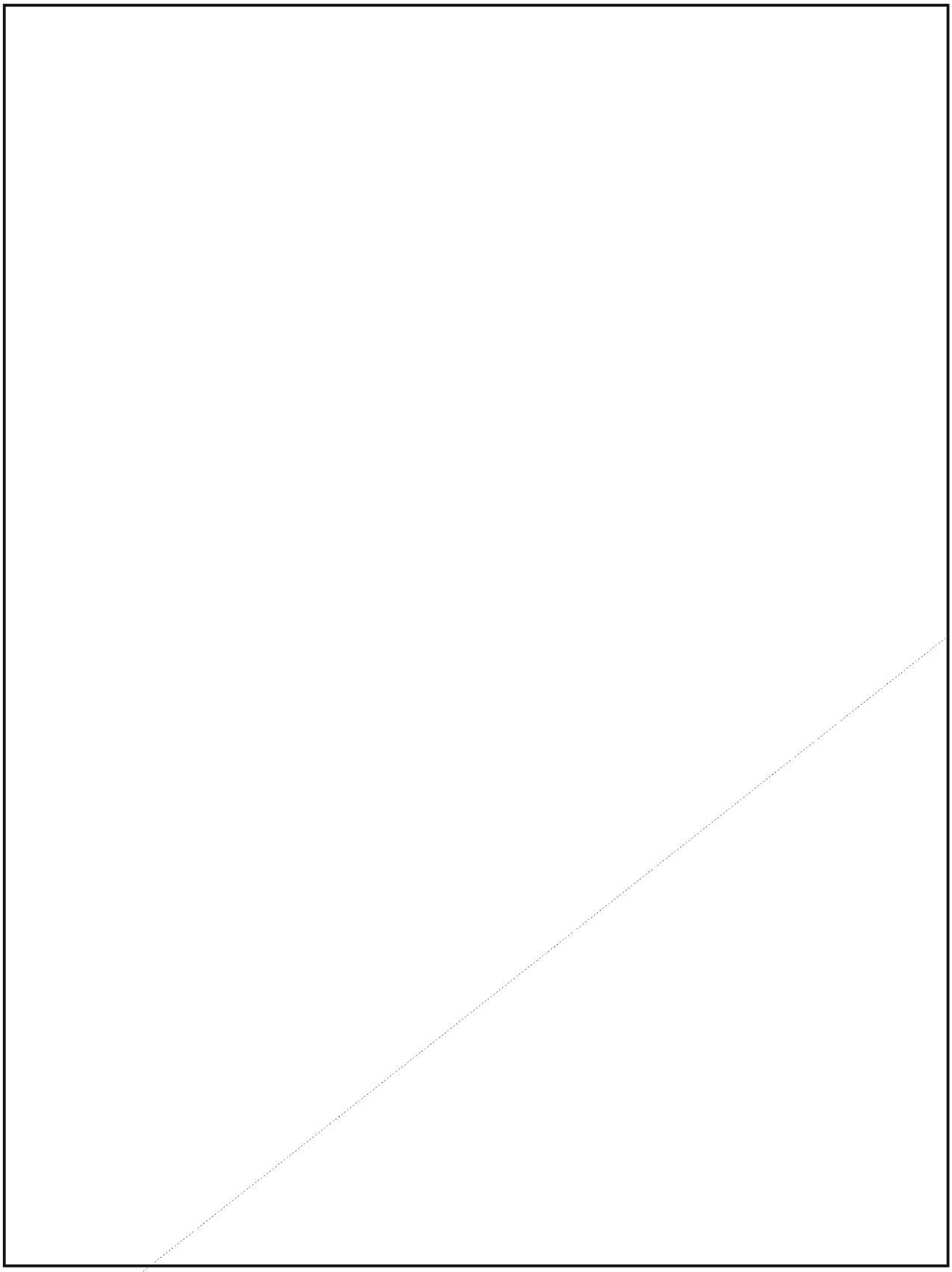


DOCID: 4009837

P.L. 86-36

NSA·Crostic No. 35 by DHW

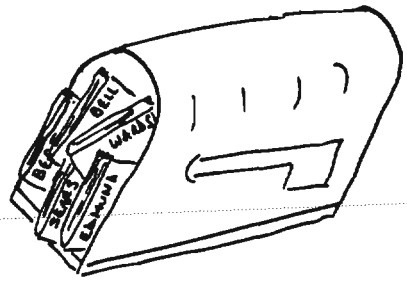




DOCID: 4009837

TECHNICAL SUPPORT CATALOGS (U)

by [redacted] P.L. 86-36



Providing adequate sustaining field support is one of those abstract concepts that is difficult to define and even more difficult to ~~(SC)~~ accomplish. DDO's Analytic Technical Health Group (ATHG) is attempting to improve that situation and to plan for future comprehensive initiatives. This article is intended to acquaint the reader with the Technical Support Catalog - one modest current step towards achieving those goals.

~~(C-CCO)~~ Technical Support Catalogs are not new; they have been produced since the early 1950's. Originally, they consisted of lists of available technical documents and publications available on a particular subject entity. They were often produced by hand, typed out from file cards maintained on each technical report produced. In some areas, producing the Technical Support Catalogs often kept one person busy full time. More recently, Technical Support Catalogs have virtually disappeared and, as a result of personnel cutbacks, the published technical reports themselves have been reduced in number and periodicity. This situation was emphasized in a DDF study of field support, based upon Field Visitation Team Reports for 1976 and 1977. The primary field complaint, according to that study, concerned the lack of technical support and timely feedback by NSA. The ATHG, formed by DDO to study the problem and find solutions to it, supported the DDF findings: there had indeed been a diminution of the flow of traditional technical support (i.e., Technical SIGINT Reports and Working Aids) from NSA, as is illustrated in the chart below (based on information provided by T512).

(U) While DDO cannot magically conjure up additional technical support, SIGINT analytic groups can, and must, ensure that appropriate field and in-house elements -

- are provided with the latest information to support their missions (including Alternate Intercept Coverage Plan) and
- are alerted to the availability of any information for which they have a legitimate support requirement.

DDO Technical Report Production
1968 - 1979

Year	A	B	G	W	DDO
1968	993	876	579	-	2448
1969	1215	879	265	-	2359
1970	914	636	274	1	1825
1971	691	723	204	67	1685
1972	602	458	181	51	1292
1973	459	289	100	51	899
1974	591	219	125	31	966
1975	540	197	112	21	900
1976	454	200	81	21	756
1977	471	130	123	65	789
1978	464	177	155	59	855
1979	199	133	100	76	508

(U) On 12 April, 1978, in its first report to DDO, the ATHG emphasized the purposes of Technical Support and Feedback as a means of improving the efficiency of the collection effort by -

- strengthening the motivation of field personnel,
- increasing their target knowledge,
- improving their understanding of Agency goals,
- enhancing skills and training, and
- encouraging the development of a spirit of teamwork between station personnel and the analytic workforce at NSA.

One of the ATHG recommendations, which were subsequently approved by DDO, called for the creation of two sub-groups, one for feedback and one for Technical Support Catalogs.

~~(S-CCO)~~ The Feedback Sub-group chairman, [redacted] P13, working with elements of DDO and DDT, is addressing methods of improving the production by computers (especially Terminal Sub-systems) of quick turnaround information for transmission to field sites. In addition, in order to heighten management awareness of various aspects of this data flow, [redacted] working with T131, has incorporated additional displays of "Incoming/Outgoing" data, into DDT's Quarterly Management Information Bulletin. This publication provides management information P.L. 86-36

DOCID: 4009837

EO 1.4.(c)
P.L. 86-36

DOCID: 4009837
P.L. 86-36

reports, in numeric and graphic form, on the receipt and distribution of data; it includes incoming and outgoing volumes, general patterns of feedback to the sites, and data exchanges with Second and Third Parties.

(U) The Technical Support Catalog Subgroup, chaired by the author, sought a general solution to the problem of regular production of Technical Support Catalogs, and thanks to much assistance from T5 (particularly Ms. [redacted] was able to focus on a solution based upon the existing NSA/CSS Technical Document Collection. The result, with some minor adjustments, and with room for potential future add-ons, has been instituted as a DDO approved Technical Support Catalog.

~~(C)~~ STINFO (Scientific and Technical Information) is maintained by T5112, one of the elements of the Library at FANX. The material includes RDT&E reports prepared by NSA or its contractors, DDO technical SIGINT publications, software acquisition documents, and other relevant Agency documents. Every technical publication sent to T5112 is filed according to an S-prefixed one-up number assigned by the STINFO indexers. Prior to a recent change, T5112 prepared bibliographic descriptions of each document using the Report Document Page (DD Form 1473, 1 Jan 73); abstracts of the document were included (if provided by the author) and key words were selected from the text. This procedure, as it applies to the ATHG efforts, has been changed so that the DDO author or the OPC (Office of Primary Concern) of a given technical report must now prepare the DD Form 1473, and must enter the required pertinent information (particularly the abstract and the key word entries).

(U) The data from these bibliographic descriptions are typed by T5 personnel on a Delta Data 7000 terminal, and computer tapes are created. These tapes are processed on CARILLON to add the data to the existing off-line date base. Retrievals of information can be made by key word, author, originating organization, report number, date, etc., and all these elements make up the components of the Technical Support Catalog.

~~(C)~~ The Technical Support Catalog is now a formal Agency publication included (with instructions) in the Technical SIGINT Publications Manual (USSID 200). It contains a compendium and abstracts of either general or tailored technical documents and publications on a given subject area. All of the material in the Technical Support Catalog is derived from formal records of selected technical SIGINT publications filed in STINFO.

(U) In order for the requisite information to be entered into STINFO, the OPC should forward a copy of each report to T5112, along with the Report Documentation Page (DD Form 1473). The OPC should ensure that the following blocks on the form are completed:

1. Report Number,
2. Title,
7. Author(s) (when applicable),
12. Report Date,
13. Number of pages,
15. Security Classification,
15a. Declassification/Downgrading Schedule,
19. Key Words, and
20. Abstract.

EO 1.4.(c)
P.L. 86-36

(U) Under current procedures, requests for information about reports, or the reports themselves, that come from outside the production group which produced the reports, must be receive formal approval from the group which produced the reports. Therefore, requests from field units for a particular Technical Support Catalog should be sent to the OPC, who will in turn forward the request to T5112.

[redacted]

(U) A variety of production techniques for Technical Support Catalogs are being experimented with by the ATHG and various DDO/DDT elements, using various terminals and Terminal Sub-systems.

(U) Future upgrades of the Technical Support Catalog system include such possibilities as on-line bibliographic sorts, and full-text document retrievals for those subscribers with appropriate system or RJE (Remote Job Entry) terminals.

(U) No amount of sophisticated equipment and software will make the system work effectively unless the humans in the system are committed to making the system work. No matter what further developments and changes are made to the system, those who produce the reports will have to properly participate in the program, and those who need the support will have to properly exercise the system, in order to make technical support all it can be - an accurate, meaningful, and effective contribution to the overall SIGINT effort.

DOCID: 4009837

The Stairwell Society

I have always had a deathly fear of elevators. You may have seen me on occasion, braced in the corner, hands wrapped white-knuckled around the side rails, waiting for that twang which would announce the snapping of the cable and the inevitable plunge to follow. I've often wondered whether you could avoid destruction by jumping just as the elevator hit bottom, but this would require precision which I doubt I possess and anyway, everyone knows that in the bottom of the elevator shaft is a giant spring which would bounce the elevator right back at you in mid-jump. And even if you survive the drop, once the elevator starts bouncing off the spring, would it ever stop? Imagine being trapped for weeks in a bouncing elevator! It's enough to make one's palms sweat.

When I related this concern to another ninth floor dweller one day, he mildly asked why I didn't walk up the stairs. That, unfortunately, crunched right into a second of my deathly fears - physical exertion. But I had to do something. The elevator thing was getting to me, so the next morning I walked up . . . and nearly died. As I was lying on the floor next to my desk, wheezing and gasping and waiting for the shooting pains in my left arm to subside and my legs to unknot, my mentor showed up. "You're not supposed to do it all at once!" he railed. "There's an art to this. You must work up to it. I'll coach you." I managed a weak "Thanks."

"For openers," my new coach offered, "I'll let you in on a technique developed by one of the greats in the field - it's called the 'Bloom arc'. You take a wide turn on each landing. This allows your legs a chance to recover. Ideal for the long distance climber."

The next morning I tried this technique. I found it to be somewhat overrated, however, since the landings are just too short for much recovery; and I discovered a distinct risk with this procedure. On the fourth floor landing, as I was doing my 'Bloom arc', I walked right into a girl coming down the stairs carrying two cups of coffee. She was not at all impressed with my 'Bloom arc" explanation and treated me to some very unladylike observations on my general being. "Sorry" I muttered, amidst wheezes.

My coach set me straight almost immediately. "Of course there are risks. We wouldn't do this if there was no danger! You must learn to accept these and for your information, people who go down the stairs are a blight on our good name. Spurn them! By the way, you'd better get that coffee off your coat before it stains."

A few days later my coach observed that I should be ready to do the complete climb. I protested, but he was adamant and offered another inside hint. "It's called the '6th floor gambol'," he confided. "You leave the stairwell at the 6th floor and go the the staircase at the end of the hall, where you complete the climb. Great chance for a rest. Try it!"

Apparently this is a favorite practice of many of the dedicated stairwell climbers. I noted that when I stumbled through the door on the sixth floor, legs wobbly and out of breath, people politely turned their heads, snickering softly as I passed by. But they are compassionate people, those sixth floor inhabitants. The card table with small cups of gatorade located near the men's room is a nice touch.

After several days of the climb, my coach approached me, put his arm around my shoulder, and talking in a subdued voice said, "I'm proud of the progress you're making; Keep it up and you may make THE SOCIETY." "The what?" I asked. "Well, I really shouldn't tell you about this, but you are a serious person and I think I can trust you. We have, here in NSA, a secret organization of stairwell climbers." "No kidding!" I whispered. "Yup. A secret society. Only the members know who is in it. Won't see our name on the board or in the newsletter or any of that sort of stuff. We don't want any joiners in our group. You know, there are folks around who join anything just to say they are in it. Think it looks good on their record, or whatever. I, for instance, know three guys in the bridge club who absolutely hate the game but wouldn't quit

for anything. Terrible thing, this status business. We have none of that!"

"Very interesting" I replied, "but what's the sense of being in a club if you can't talk about it?" "A society!" my coach hissed. "It's not a club. It's a society! Don't make that mistake again!" "I'm sorry" I responded remorsefully. "Our enjoyment comes from association with each other and the sharing of our stairwell. And once each year we even have an outing - just society members. No family or friends with beer and buckets of fried chicken, or any of the tacky stuff. Last year we did the Washington monument. Great fun. Even the tradegy of Harry passing away on the three hundred and fortieth step couldn't mar the enjoyment of that climb. This year we are thinking about the Empire State building, although they are giving us fits. Seems like they make money on their elevators and they hate to pass up potential revenue, but they don't know what to charge for the stairs. No matter, there are other giants for us to assail. Think of it - The Eiffel Tower . . ." His eyes glazed over and his voice broke. "Could I join?" I asked naively. "Absolutely not!" He had his composure back. "We'll have no joiners. I told you that. The elders review all potential members. Only they can choose. When your time comes, you'll know. But never, NEVER ask." "Gotcha." I responded, overwhelmed by the enormity of it all.

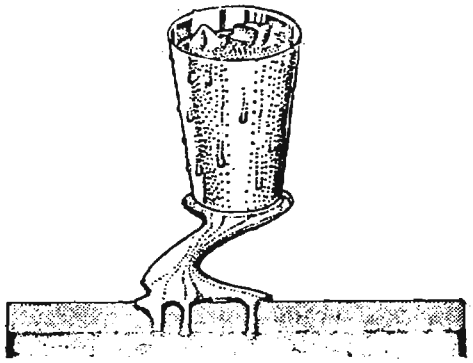
"You've got to learn to climb with pain" my coach offered a few weeks later, when I mentioned that my knees were bulging. "Leg cramps are common in this business and must be ignored. Likewise for arm pains. We do recommend, however, that if you experience massive chest pains, you stop for awhile. There are climber aid stations on the odd-numbered floors for emergencies, but a dedicated climber scorns such embellishments. In fact, one of the past greats was stricken early in his climb, but he made it to the ninth floor before collapsing. A heroic effort. Really fantastic. We are thinking of giving an annual award in his memory." "Gosh," I uttered, "what guts!"

"And there is the matter of dress," my coach continued. "You need climbing shoes if you are really serious about this. And loose clothing. Need to let the body move freely for maximum effort." I took this to heart, got some double-soled tennis shoes, and borrowed a suit from my neighbor, who is three sizes larger than I am. The climb went all right the next day, but I got awfully tired of the caustic comments about my attire, so I opted against "proper dress," even if it is part of the program.

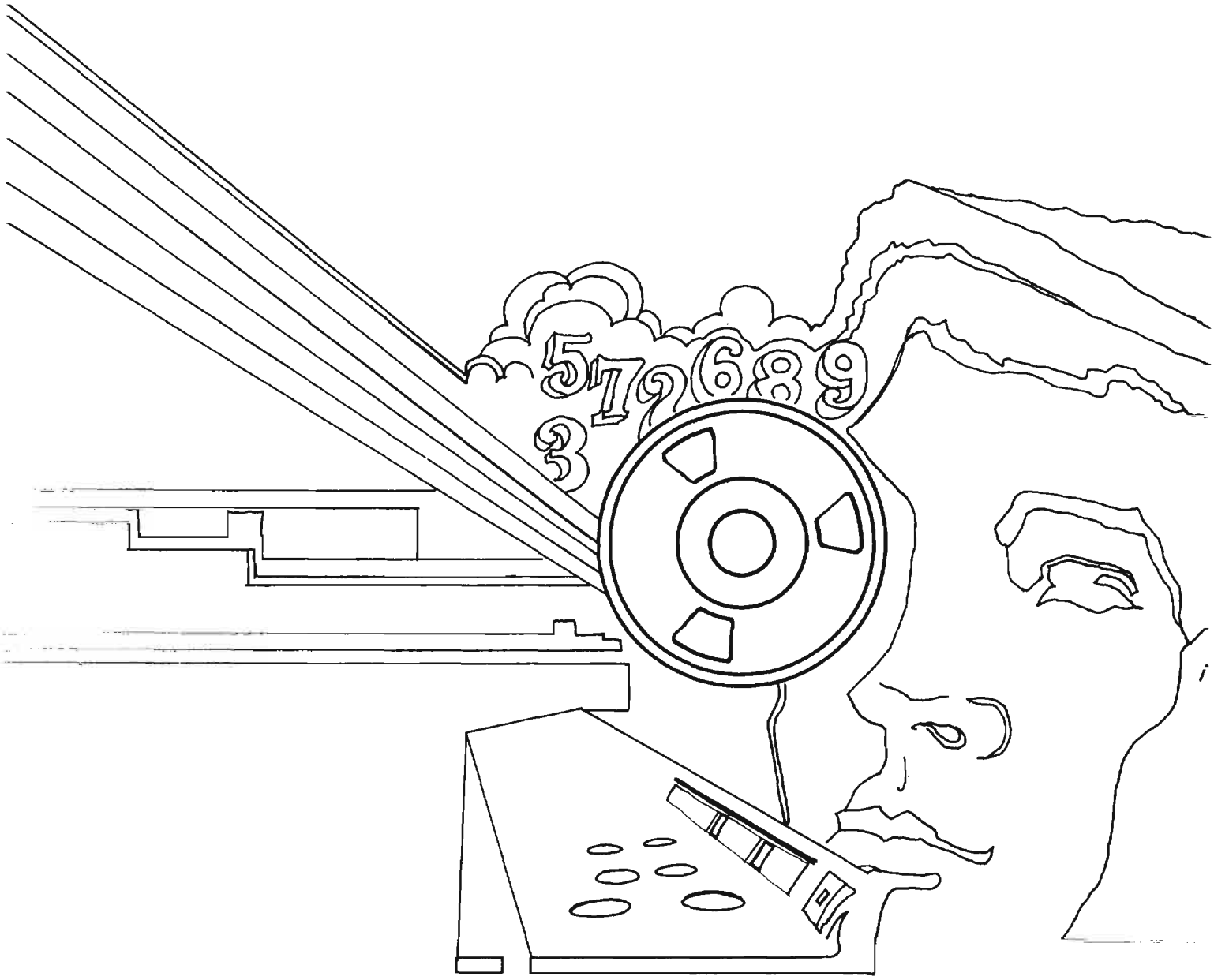
"You might be interested to know that the seniors in the Stairwell Society," my coach offered one day, "are able to take the stairs two at a time." "I'll never achieve executive status," I replied. "Don't despair," my coach responded. "Some of those people have spent years training to achieve their status. You're still a novice. Give it time. Dedicated people, the Stairwell executives. There is even a story," he confided, as he moved closer and lowered his voice, "of one person in this building who can take the stairs THREE at a time, and do the whole climb holding his breath!" "Fantastic" I replied, with true awe. "Who is he?" "Don't know. Don't even know anyone who has seen him. It's very tightly held." "Wow!" I responded, feeling very 'in'.

One day I approached my coach with what I felt was a very significant observation. "Did you know," I asked, "that there are two less stairs per flight in the end well than in the center?" "Yeah," my coach replied, ""it's well known within the society. True climbers avoid the end staircase at all costs. World class is the center well." "But does that mean that the building sags?" I asked incredulously. "Of course. That is the end of the building which supports the Director's office. Heavy decisions and all that." "I understand fully," I replied sagely.

I am now a devoted climber. I shun the elevators, avoid the back stairwell, am a master of the 'Bloom arc', have overcome the 6th floor gambol, and look with scorn on those who go down the stairs. My coach thinks I may be welcomed into the society in the near future and he talks with pride about his contributions to my advancement. One would never have expected that a simple fear could lead to a whole new way of life. And the other day a most amazing thing happened. As I was climbing, I heard a whoosing noise behind me, and when I turned to look, a figure passed me taking the stairs three at a time. I could not identify him, but his face was very red and it's possible, just possible, that he was holding his breath!



~~TOP SECRET~~



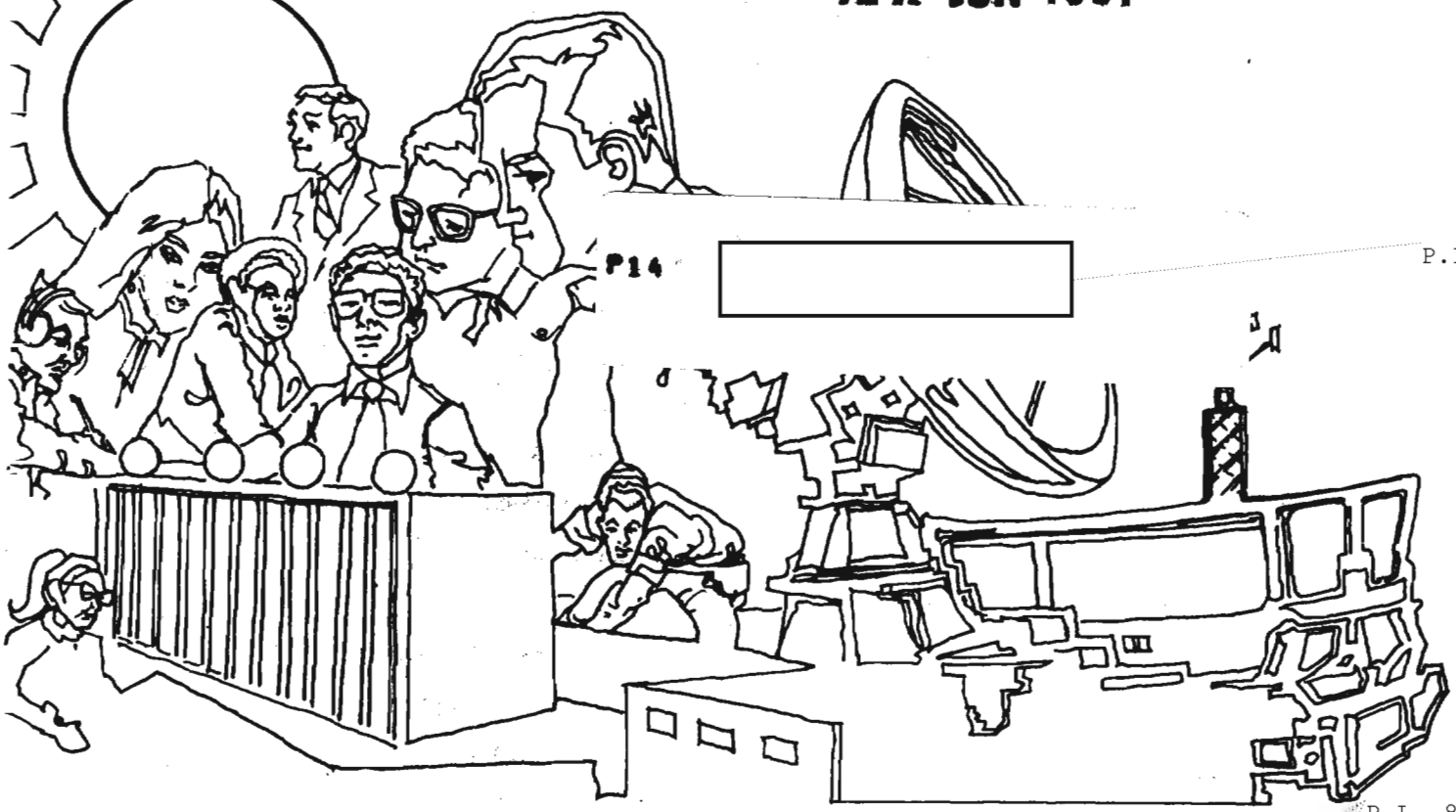
DOCID: 4019689

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

APR - JUN 1981



P.L. 86-36

P.L. 86-36

MIDDLE-AGE SPREAD (U)..... 1
GRADING THE RUSSIAN PQE (U)..... 3
THIRD PARTY RELATIONSHIPS (U)..... 8
THE POETS' CORNER (U).....11
NSA-CROSTIC NO. 33 (U).....D.H.W.....12
CLASSIC CABLES (U).....14
TRAFFIC ANALYSIS: Specialty
Without Portfolio (U)..... 15
DIA Videocasette Program (U).....19

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON~~ 1 SEP 2011

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019689

CRYPTOLOG

Published by P1, Techniques and Standards,

for the Personnel of Operations

VOL. VIII, No. 4 - 6 APRIL - JUNE 1981

PUBLISHER [redacted]

BOARD OF EDITORS

Editor-in-Chief.....David H. Williams (1103s)

Collection.....[redacted] (8555s)

Cryptanalysis.....[redacted] (4902s)

Cryptolinguistics.....[redacted] (5981s)

Information Science.....[redacted] (3034s)

Language.....[redacted] (8161s)

Machine Support.....[redacted] (5084s)

Mathematics.....[redacted] (8518s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Taurone (3573s)

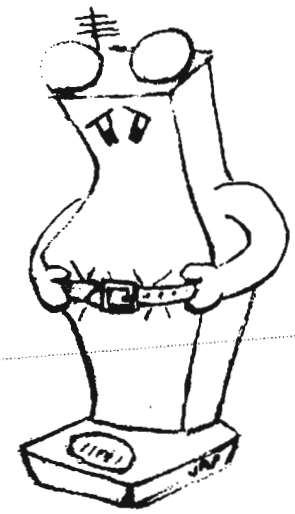
P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4019689

MIDDLE-AGE SPREAD (U)

[redacted] M3



P.L. 86-36

People working at NSA during the last ten years have been able to witness and perhaps experience a phenomenon (U) likely to occur only once in the lifetime of an organization. During this period NSA has moved along that portion of its life cycle from a new, continually growing organization to a middle-aged organization with a static or even decreasing work force. This change was so subtle and occurred over such a long period of time that many may not have even noticed that it was taking place. To those who prepare and read the internal job announcements, it should have been obvious. To the managers, identifying and recognizing its occurrence should have been crucial.

~~(C)~~ When an organization moves into the middle-aged phase of its life cycle, many characteristics surface that are quite comparable to those of a person entering middle age. As with some people, a "middle-age spread" develops. In most organizations this usually occurs at the lower supervisory, higher worker level (Grades 11 or 12 at NSA). All of a sudden the majority of the "working people" have achieved that grade. A bulge or overabundance of people at that pay level occurs—in the neighborhood of 5000 in the Agency at present. The input grade or grades below the overstaffed level suffer a corresponding decrease, since there is reduced hiring and promotions continue. Promotions out of the overstaffed level, in this case, to Grade 13, are not sufficient to reduce the bulge since promotions "in" are more numerous that promotions "out."

(U) Thus we have a situation somewhat similar to that which occurs when a person cheats on a diet: a wide spot is created at the middle. This diminishes the desireability of anything less than a supervisory position, as personnel jockey for positions with the best promotion potential. People who actually do the work become harder and harder to find, since the rewards to be gained are not as easy to come by for the non-supervisors. Specialty jobs become difficult to fill. (Just look at the number of job advertisements for traffic analysts or engineers, if you need convincing.) Career development is forgotten as managers attempt to hold onto what few workers they have, especially the good ones. Closely guarding these valuable resources becomes a major managerial function, sometimes without proper consideration of the organization as a whole, or of the individual. This, in turn, creates a frustration for those who can't achieve a supervisory status and are relegated to a worker position. This frustration causes them to give up, become nonproductive and to hang on only long enough to find a vacancy they consider more advantageous to their career. This process creates trauma within the organization.

(U) The individual entering middle age tends to suffer the depressions, frustrations and fears that are a normal part of the aging process; the middle-aged organization is susceptible to these same emotions. Managers are particularly vulnerable. Some must make adjustments and some may have to make complete revisions in their style of management. In the early formative years, there is a steady stream of new, bright, eager employees continually entering on duty. Mistakes in planning, and motivation, and in the managing of these employees were easy to overcome because of the continuing new input, on the one hand, and the opportunities caused by constant upward movement of personnel, on the other. Managers were certain that they could always replace a lost or unmotivated employee; consequently, less management of personnel assets was required, and less was done. Thus, the manager in the new or growing organization

DOCID: 4019689

needs fewer managerial skill in order to get by. As the organization grows older and finally reaches the point where few new employees are entering on board, a whole new type of managerial perspective becomes necessary. The replacement of personnel who move up, on or out becomes increasingly difficult. If the manager is assigned to an area which is, in the minds of the on-board employees, a less than desireable one, his ability to recruit from within the organization is diminished. Mistakes that were previously covered up or glossed over now can result in the loss of a valuable resource. The manager must now face up to his problems and make decisions. More importantly, these decisions must be right the greater part of the time. The manager must motivate his people and create a reputation for fair play and excellence, which will help him in the recruiting process, since recruiting situations will be such that frequently the manager must sell himself in order to attract the numbers and types of people required.

The manager must now learn to manage!

(U) He must motivate, provide job enrichment, and develop his employees so that job satisfaction and, consequently, morale are high within the organization. Since he will usually be short of resources, he must learn how to deploy them so as to obtain the maximum output from the available resources. The welfare of his personnel must occupy a major part of his workday. No longer can the problems of the employee be given short shrift, since the loss of even a single employee can cause a severe jolt to the work force. Continuous failure will eventually lead to the demise of the organization, since empty billets are the most logical candidates for reduction, After all, if you've managed to get along without some function for a period of time, it probably wasn't worth doing in the first place.

(U) The managers of a middle-aged organization have to lead rather than operate from a position of arbitrary authority, since other opportunities are readily available to those at the working level. Those who master the techniques of leadership will have little trouble attracting personnel; those who can't will always be short-handed or will attempt to institute a policy of limiting intra-organizational transfers. (The recent moratorium on transfers of clerical personnel is an example of this.) When this happens the organization loses; the inevitable results are discontent, decreased productivity, and, eventually, the loss of employees through attrition.

(U) In short, managers of middle-aged organizations must, firstly, recognize the symptoms, and then take whatever actions are necessary to alter their managerial philosophies so as to become leaders. Some will not have to change at all; others will make the needed changes; and the rest will fail.

SOLUTION TO NSA-CROSTIC No. 32

[THE] JOYS [AND FRUSTRATIONS] OF

SOLUTION TO NSA-CROSTIC No. 32

"[The] Joys [and Frustrations] of Plural Dropping," [Arthur J.] Salemme, CRYPTOLOG, January 1978

"When our daughter and a friend of hers were both five and were eating lunch at our house, my wife gave them each a sandwich and a slice of American cheese cut in strips. The little friend particularly [enjoyed] the latter and asked what they were. 'Cheese,' she was told. 'Well then,' she asked, may I please have another chee?'"

"This field of research is so virginal that no human eye has ever set foot on it."

—Opening sentence of a doctoral dissertation in physics, cited in *Smithsonian*, March 1981

DOCID: 4019689

GRADING THE RUSSIAN P Q E (U)

[redacted] G53

P.L. 86-36

Since the Russian Professional Qualification Examination (PQE) was instituted in 1967 as a means to identify the ~~(C)~~Agency's most competent Russian linguists, the number of people taking Part IIA, the classified translation section given every six months, has increased from 16 to almost 200. This drastic increase in the work load for the members of the PQE committee chosen to prepare and grade each test is one of the main reasons for the recent change in the grading system introduced last September in PQE #21. This article will explain the general testing procedure and the grading system currently used by the committee.

~~(SC)~~ The examination itself is generally about 70 to 80 lines long, and consists of four to six selections of voice and printer traffic, some in Cyrillic and some in transliteration. The committee attempts to ensure that the items used for the test are representative of the different types of material encountered by Russian linguists at NSA.

[redacted]

In selecting these items the committee looks for linguistic or technical elements that a capable Agency linguist with several years of experience should reasonably be expected to be able to resolve: garbles in printer traffic, transliterated Russian, transcription errors, poor grammar or incomplete sentences in the original text, omission of punctuation and prepositions, highly colloquial expressions, and so forth. An aspirant is expected to produce a translation that accurately conveys the content of the original in good English, while adhering to NSA translation guidelines. Four hours are allowed for the examination.

~~(C CCO)~~ The PQE IIA sub-committee consists of a chairman and four other members, all of whom are required to be certified Russian linguists from various operational elements of the Agency. The chairman ensures that the committee, like the test, is representative of the diverse analytical elements exploiting Russian traffic. The committee selects a number of items it feels are appropriate for the test and drafts model translations. Then, several certified linguists who are not on the committee are asked to take the test, in order to establish that its length and level of difficulty are acceptable. This validation group also aids in establishing a standard by which the performance of the aspirants will be judged.

~~(C)~~ Next, the test is reviewed by the Language Career Panel's Standing Committee on Language Testing (SCLT) to ensure that the test is fair, as well as comparable in length and difficulty with tests in other languages. It also approves the grading system to be used by the committee. Finally, several certified linguists, who have volunteered to act as controls, take the test along with the aspirants and under the same conditions.

(U) For the four tests immediately preceding PQE #21, each member of the committee was responsible for grading several of the test items, but not the entire test. Three committee members graded each test item, in order to obtain a more balanced evaluation. These three individuals would each deduct points, according to a fixed numberical scale for the various types of errors,[1] with a total score assigned to the item being graded. These three scores were later combined to produce an average grade for the item, and the sum of these grades was used as the aspirant's overall grade for the PQE. Finally, the test papers with the least number of points deducted were passed, with the exact number of passes being determined by the control group. The passing mark for the aspirants has generally been set at a significantly lower level than that of the validation and control groups.

~~(C)~~ P.L. 86-36

(U) This approach, while satisfying the need for a reasonably objective grading system, led to several problems, which were noted by both the aspirants and the committee members. To begin with, the large number of test papers involved forced the com-

mittee to spend an enormous amount of time on establishing an exact grade for each paper—six months for PQE #20, as an example. This seemed to be a less than efficient system, since most of the committee's time was spent grading the papers with the most errors and the least chance of passing. It should be noted in this connection that some PQEs in other languages have been graded using the same system of deducting points for errors, but in conjunction with a cutoff score, such that anyone losing more than an established number of points automatically failed the test, making it unnecessary to continue grading the paper. Furthermore, the number of aspirants for the other languages has been much smaller, as few as two or three, in some cases, which meant that less time was required for grading.

(U) The numerical grading system, as used for the Russian PQE, has also inadvertently tended to maximize the attention given to minor errors, since a grader under pressure to arrive at an accurate score for each test is inclined to look for minor errors and to deduct points for them. This has, unfortunately, at times resulted in disagreements and grading discrepancies among the committee memebers, since no two graders are likely to share the same opinion of the boundary between poor word choice and a definite mistranslation, or of the seriousness of poor spelling and grammar in a translation. In addition, the numerical grades, while providing apparent objectivity, have tended to emphasize the number of errors and to obscure the nature of the errors; one 4-point syntactical error may mathematically equal four 1-point English usage errors, but these cannot be considered equivalent reflections of a linguist's ability to produce an acceptable translation. This caused some problems during the grading of PQE #20, since the length of time required to grade the tests in the first place precluded any comprehensive review of the grades before they were released.

(U) As a result of the problems arising during the grading of PQE #20, the committe preparing PQE #21 decided to modify the grading system to incorporate the cutoff feature mentioned above. The cutoff point, like the curve used for grading the preceding exams, was to be based on the performance of the validation group. It was also decided that the committee would no longer attempt to assign an exact numerical grade to each test. Under the new system, a grader was to read the entire test paper and assign a Pass or a Fail to each test—as had been done for PQEs #15 and #16—after comparing the aspirant's performance to those of the members of the validation group, with the emphasis on the major errors committed by the aspirant. Each test was graded by three committee members, and a unanimous opinion, whether pass or fail, was recorded as such without further discussion. Split decisions were resolved by discussions among the graders, with the final grade determined by consensus. Minor errors were generally taken into account only for borderline papers, which were failed if they contained an excessive number.

(U) The new grading system has already shown itself to be superior to previous methods in several ways. First, the evaluation of the tests was completed in just three months, as compared to the six months required for PQE #20. Most of the committee's time was spent on borderline papers, where more effort was required, rather than on the papers that would clearly be failed in any case. Furthermore, the emphasis in grading was directed to the most serious types of errors, with a corresponding de-emphasis in the more subjective areas of word choice, elegance of phrasing, and the like. Finally, the immediately apparent distinction between a Pass and a Fail —as contrasted with the difference between two numerical scores—ensured that any disputed tests would automatically be reviewed by the committee, with any grading errors, such as overlooking omitted sentences, being detected during the review process.

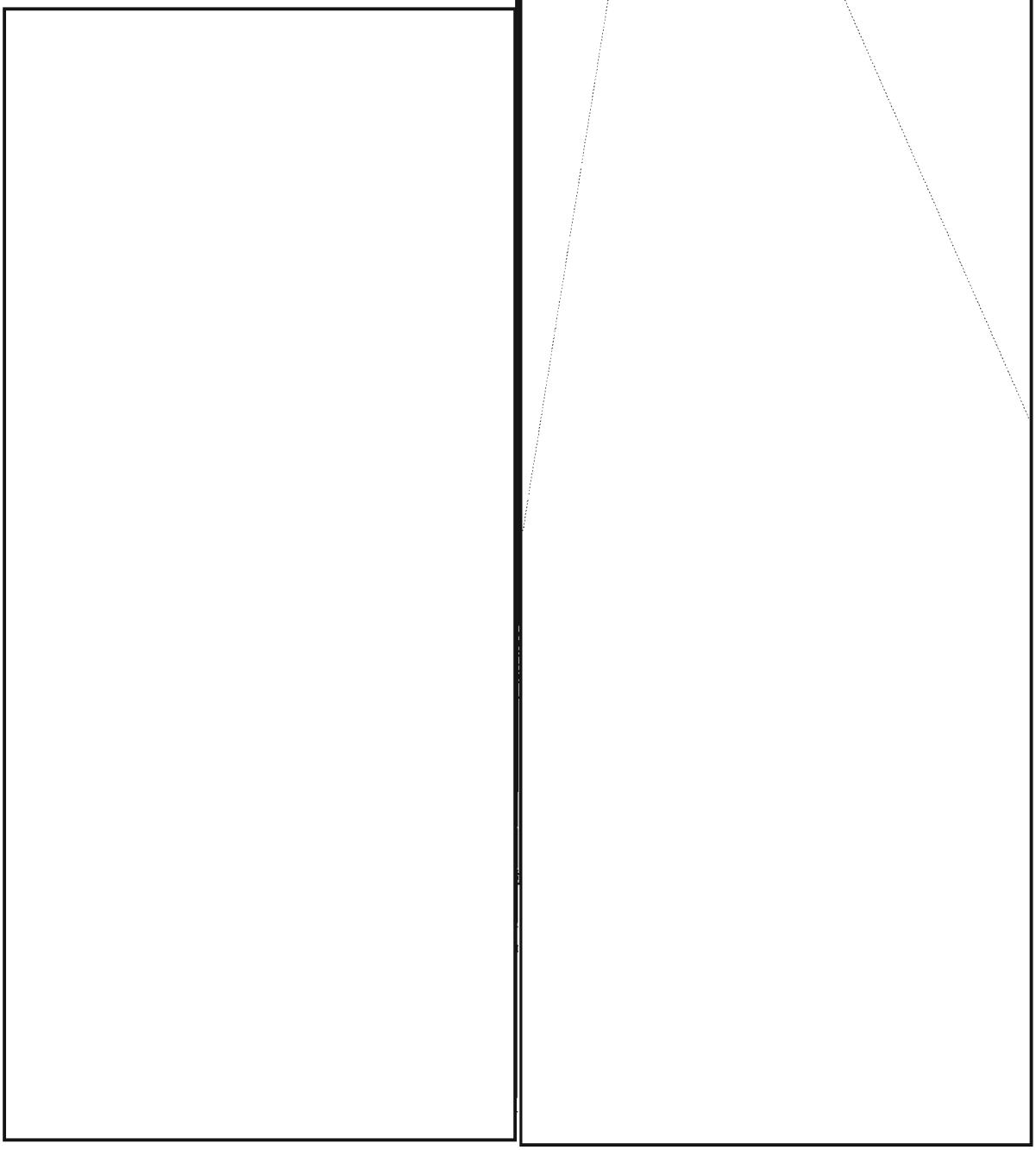
* * * * * * * * * * * * * *

(U) The rest of this article will provide examples of the principal types of errors, and show the relative weights assigned to them in grading. The examples are given either in Cyrillic or in transliteration, just as they appeared in the original material from which they were extracted. Also, garbles and other defects in the original have been left uncorrected. Each example includes the original Russian (R), the model translation prepared by the committee (M), and the aspirant's version (T).

~~(SC)~~ MAJOR ERRORS. The focus in grading, as explained above, is on major errors—those for which four or eight points would have been deducted under the previous system. These can, for the most part, be regarded as errors in grammar or syntax. The aspirant has not understood the relationships among the elements of a sen-

EO 1.4.(c)
P.L. 86-36

tence, or among the sentences in the original, and has accordingly produced a translation with serious distortions of the meaning and structure of the original. The triage system used for preliminary grading (separating the papers into pass, fail, and needs-further-discussion categories) used the number of grammatical and syntactical errors as its primary criterion, although certain other errors, such as the omission of an entire phrase or sentence, were also considered to be major.



[redacted]

The aspirant treated an adjective as a noun and separated it from the noun it modifies. It should be noted that there were several errors in the transcript used for this item (masculine and feminine modifiers for a neuter noun), and that the aspirant's error may have originated in his mistranslation of the verb SCHITAL.

In summary, most of the common major errors involve verb forms, Russian word order, colloquial expressions and noun endings. These, in addition to lexical errors, can lead a translator to see nonexistent relationships in the text and to produce translations based on them, sometimes causing distortions in other parts of the text, so as to make them fit the translator's perception.

~~(TSC)~~ MINOR ERRORS. Lexical errors are considered "minor" only in the sense that they are less serious than grammatical and syntactical ones. Such errors (for which two points were deducted under the Child system) cannot, however, be considered as insignificant. Gross mistranslations can occasionally affect the meaning of a text as seriously as a syntactical error, and even less severe ones will degrade the quality of a translation. As might be expected, this type of error occurs much more frequently than grammatical or syntactical ones. This may to some extent be a result of the four-hour time limit on the PQE, but in many cases it appears to be more a result of carelessness or indifference on the part of the translator Other errors treated as minor by the PQE #21 committee have included the omission of a word in the translation, extremely awkward or incomprehensible English, incorrect verb tense usage, and so forth. Here are some examples of minor errors from PQEs #20 and 21.

[redacted]

[redacted]

For PQE #21 this type of error was taken into account primarily for tests near the rough cutoff level designated for the number of major errors. A test that would have been borderline on the basis of the major errors it contained would fail if it also had a large number of lexical errors, with the cutoff point for these minor errors being determined by the performance of the validation group.

(U) ENGLISH ERRORS. Although no aspirants have been failed solely because of poor spelling or English grammar—errors for which one point would have been deducted under the Child system—these mistakes do affect the quality of a translation and may influence a grader's opinion of a paper, even if not formally taken into account. In spite of objections from several aspirants that the purpose of the PQE is to test command of Russian, not English, an individual translating from Russian into English is expected to be able to express himself well in the latter. Aspirants are encouraged to bring an English dictionary and a thesaurus to the examination along with the Russian-English dictionaries recommended by the panel.

(U) The area of word choice and phrasing is more ambiguous. Graders are usually fairly tolerant, at least under a Pass/Fail system, as long as the translation can be understood. Mistakes like beginning a formal intergovernmental message with "Dear Friends" (inappropriate style) will generally be overlooked by the committee in determining an aspirant's grade. Aspirants should realize, however, that a translation that disconcerts a reader or forces him to make an effort in order to understand what was mean—such as might result from adherence to Russian word order—is an inferior one.

~~(C)~~ NSA TRANSLATION CONVENTIONS. Aspirants are also expected to follow the minimal format rules prescribed for NSA translations by USSID 300: capitalizing proper names, indicating interpolations by the translator, noting garbled words, and so forth. As has been the case with style and spelling errors, no aspirant has failed the Russian PQE exclusively because of failure to observe Agency conventions. It is, however, recommended that aspirants familiarize themselves with the relevant portions of USSID 300 before taking the test, and attempt to follow these conventions as much as possible.

(U) CONCLUSION. The Russian PQE IIA committee feels that the modified Pass/Fail system now being used is an improvement over the point system which it replaced. In addition to requiring less time for the grading process—a vital consideration in view of the large and ever-increasing number of aspirants—we feel that it can provide results that are both fair and reliable.

* * * * * * * * * *

[1] For a description of this scoring system, see "An Objective Approach to Scoring Translations," by [redacted] CRYPTOLOG, March 1976.

DOCID: 4019689

Third Party Relationships (U)

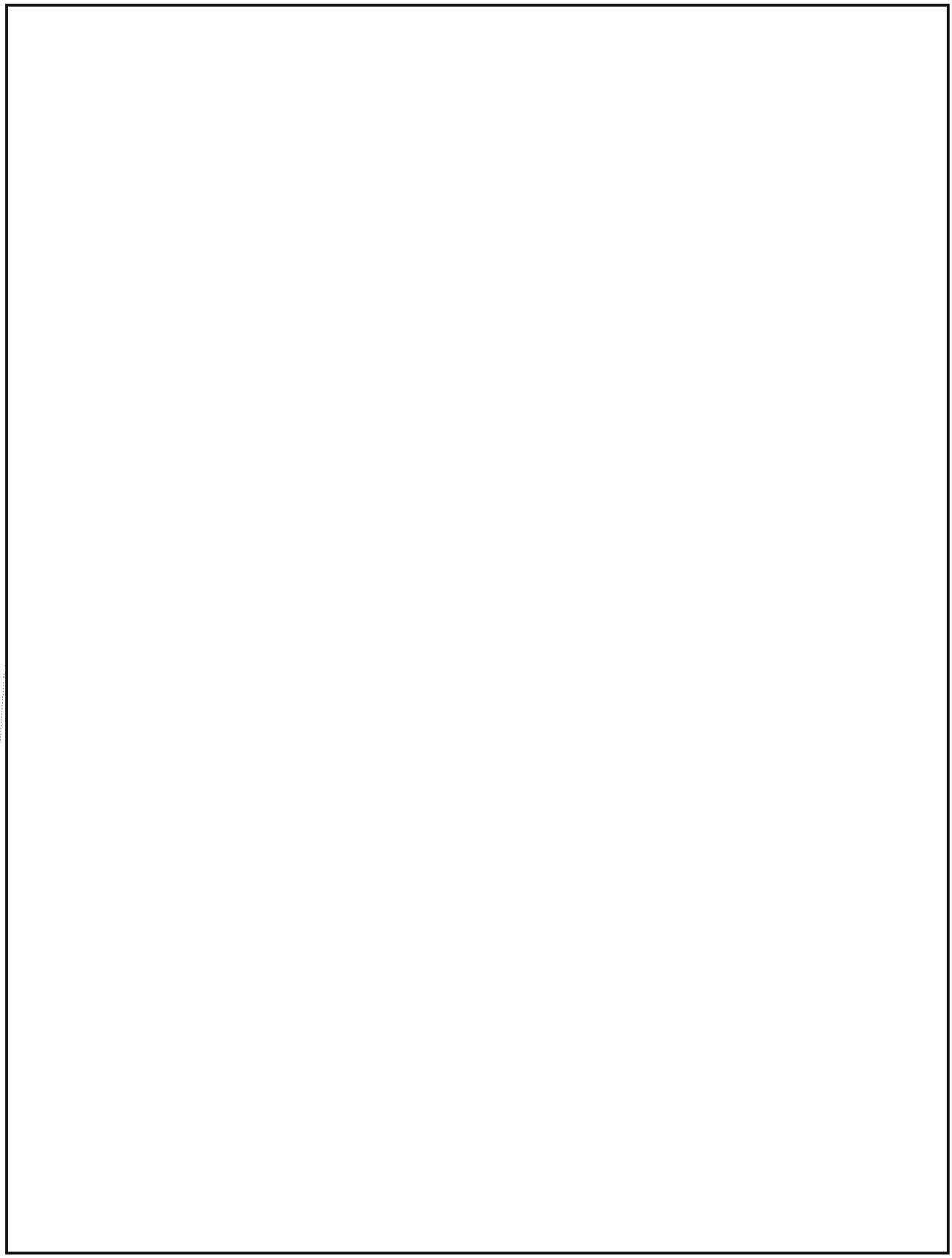
WHY HAVE THEM?
WHAT ARE THEY?
DO WE USE THEM PROPERLY?
ARE THEY WORTH THE PRICE?

[redacted] B309

P.L. 86-36

[redacted]

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

DEPARTMENT OF CLASSICS AND MYTHOLOGY (U)

Is there any mythology buff out there who can identify whatever personal attributes of these two Greek goddesses make this quotation an apt one? If so, please call CRYPTOLOG on 1103s.

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

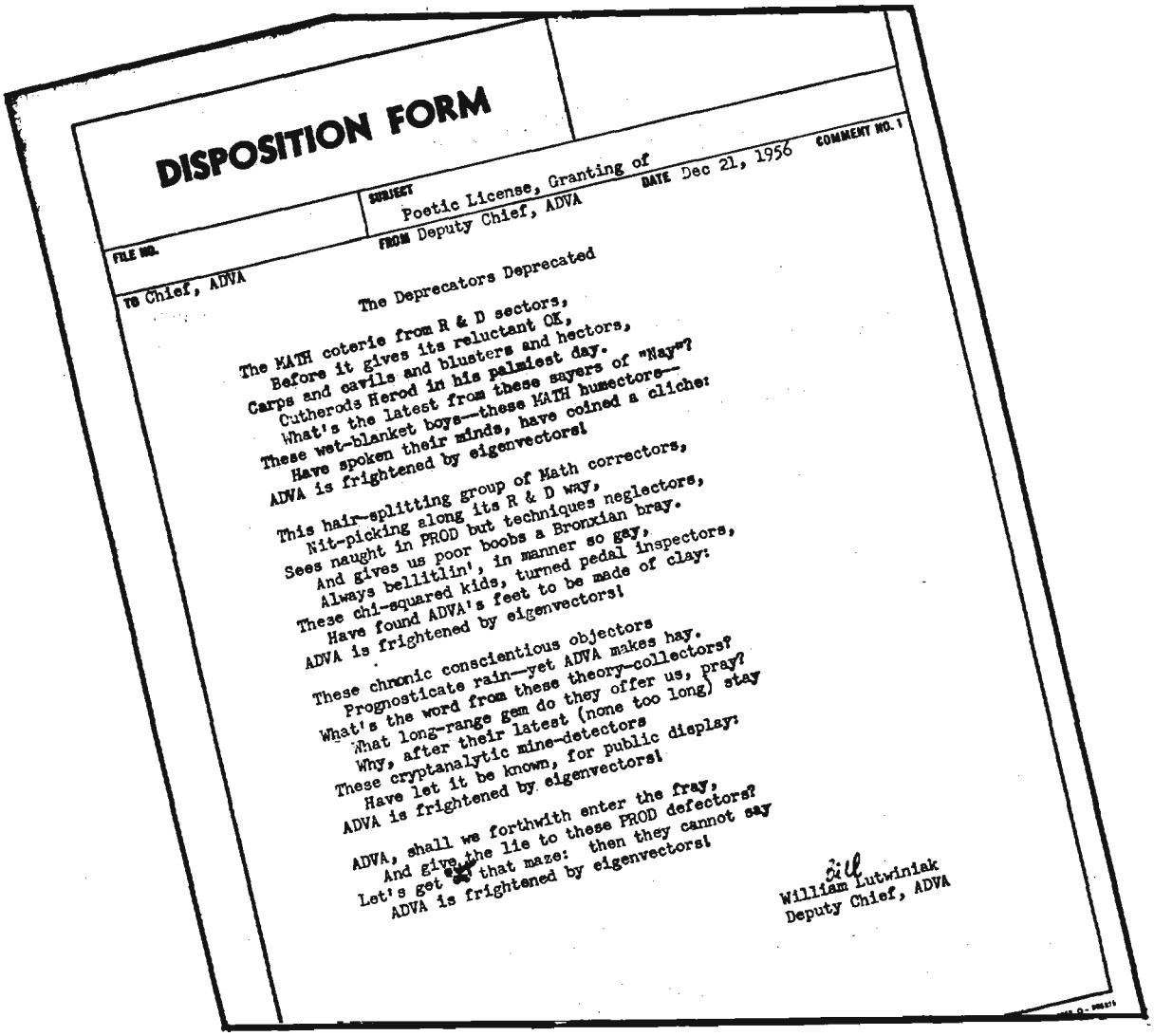
EO 1.4.(c)
P.L. 86-36

~~CONFIDENTIAL~~

The Poets' Corner (U)

Introduction is ~~C CCO~~
Poem is UNCLASSIFIED

In the mid-1950s a cryptanalytic effort was underway in ADVA, the predecessor of today's A5 (Cipher Analysis), against a particularly recalcitrant wired-wheel system. The R & D element then known as MATH, comparable to the current R51 (Mathematical Research Division), as part of its mission to provide applied mathematical support to PROD elements, suggested to ADVA a novel (for those times) approach involving eigenvectors. The ADVA analysts resisted this as being no improvement over the techniques they were already using. MATH reported this reluctance to the ADVA leadership, slyly adding that perhaps "ADVA was frightened by eigenvectors." A lively "discussion" ensued, the upshot of which was this "D/F", sent from William Lutwiniak, Deputy Chief of ADVA, to Arthur Levenson, the Chief.



DISPOSITION FORM

FILE NO.

SUBJECT Poetic License, Granting of

DATE Dec 21, 1956

COMMENT NO. 1

TO Chief, ADVA

FROM Deputy Chief, ADVA

The Deprecators Deprecated

The MATH coterie from R & D sectors,
Before it gives its reluctant OK,
Carps and cavils and blusters and hectors,
Cutherods Herod in his palmiest day.
What's the latest from these sayers of "Nay"?
These wet-blanket boys—these MATH humectors—
Have spoken their minds, have coined a cliche:
ADVA is frightened by eigenvectors!

This hair-splitting group of Math correctors,
Nit-picking along its R & D way,
Sees naught in PROD but techniques neglectors,
And gives us poor boobs a Bronxian bray.
Always bellitlin', in manner so gay,
These chi-squared kids, turned pedal inspectors,
Have found ADVA's feet to be made of clay:
ADVA is frightened by eigenvectors!

These chronic conscientious objectors
Prognosticate rain—yet ADVA makes hay.
What's the word from these theory-collectors?
What long-range gem do they offer us, pray?
Why, after their latest (none too long) stay
These cryptanalytic mine-detectors
Have let it be known, for public display:
ADVA is frightened by eigenvectors!

ADVA, shall we forthwith enter the fray,
And give the lie to these PROD defectors?
Let's get [redacted] that maze: then they cannot say
ADVA is frightened by eigenvectors!

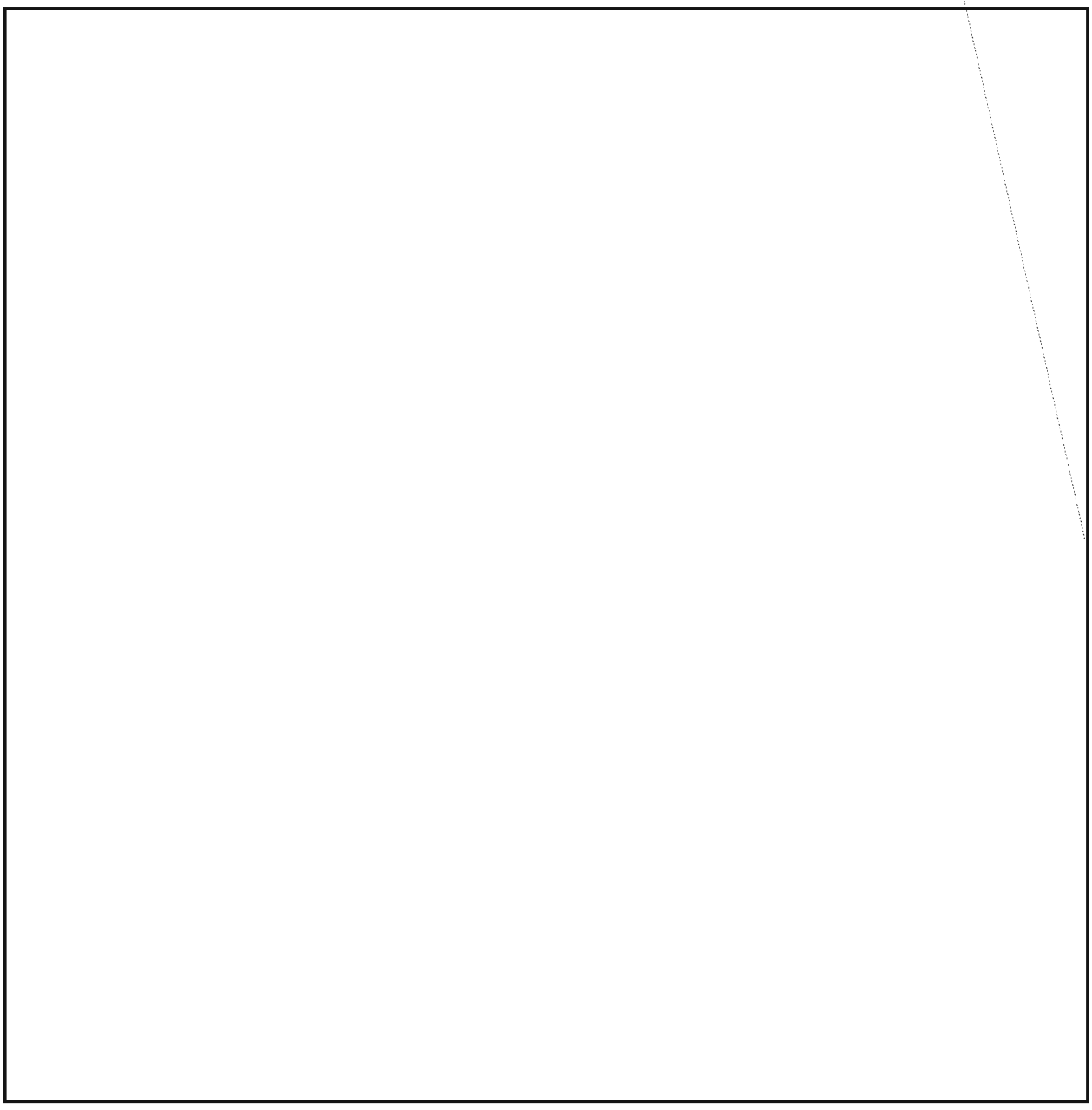
Bill
William Lutwiniak
Deputy Chief, ADVA

~~CONFIDENTIAL~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

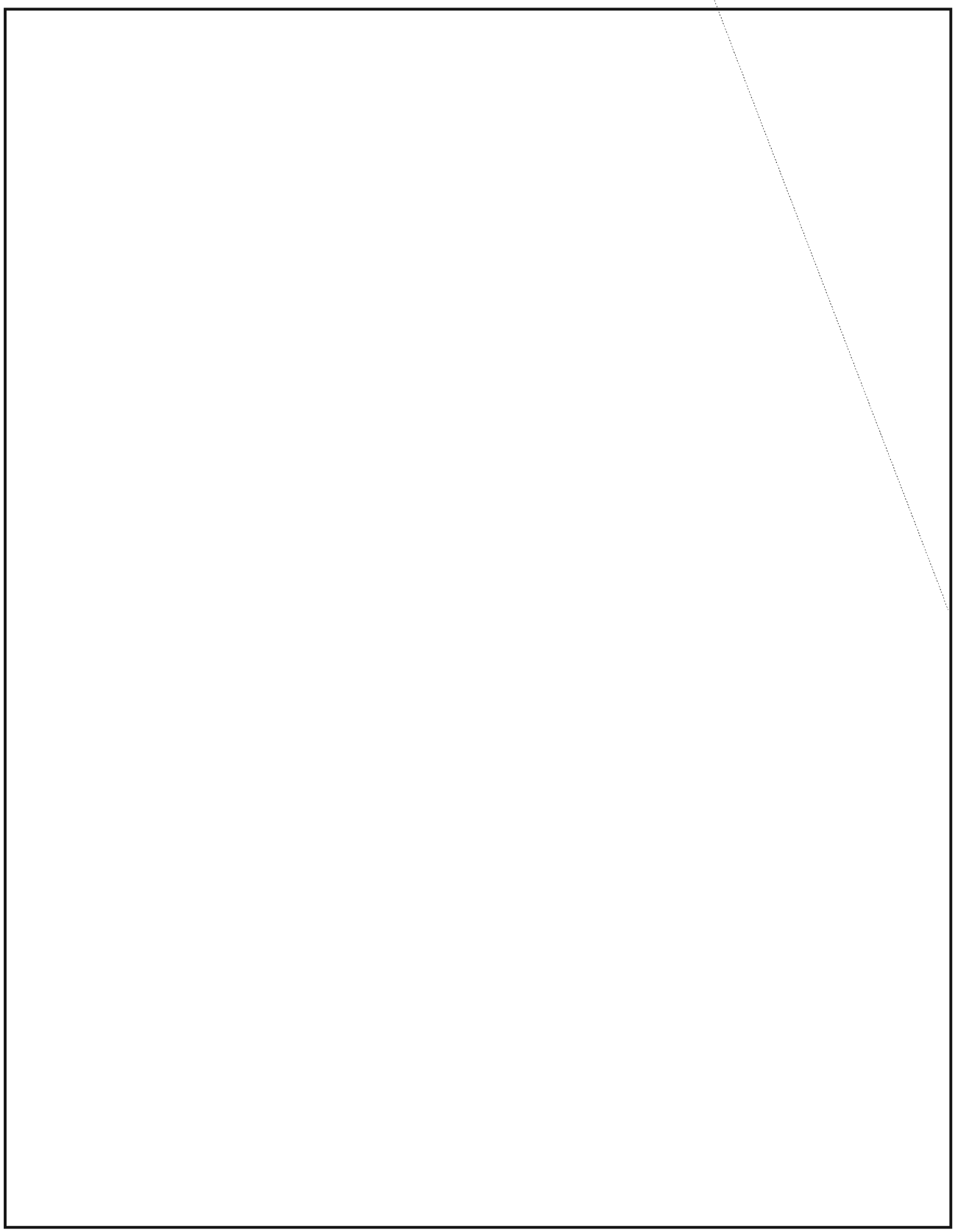
NSA-Crostic No.33

P.L. 86-36

D.H.W.

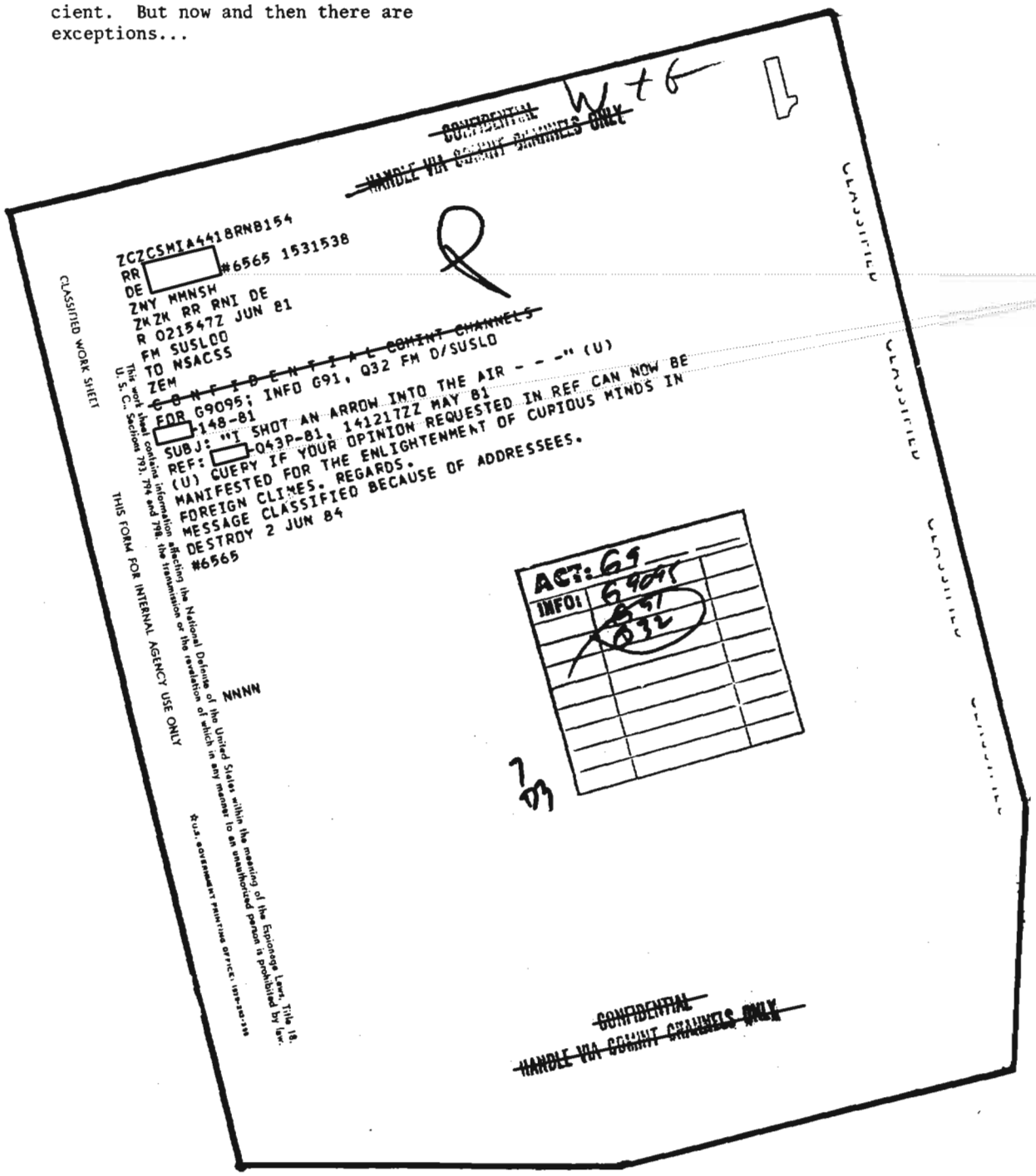


DOCID: 4019689



CLASSIC CABLES (U)

Most people find that "REQUEST STATUS OF RESPONSE TO REF MESSAGE" is sufficient. But now and then there are exceptions...



~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

W+6

ZCZCSMIA4418RNB154
RR [redacted] #6565 1531538
DE
ZNY MMNSH
ZKZK RR RNI DE
R 021547Z JUN 81
FM SUSLOO
TO NSACSS
ZEM
~~C O N F I D E N T I A L COMINT CHANNELS~~
FOR G9095; INFO G91, Q32 FM D/SUSLO
[redacted]-148-81
SUBJ: "I SHOT AN ARROW INTO THE AIR - - -" (U)
REF: [redacted]-043P-81, 141217ZZ MAY 81
(U) QUERY IF YOUR OPINION REQUESTED IN REF CAN NOW BE MANIFESTED FOR THE ENLIGHTENMENT OF CURIOUS MINDS IN FOREIGN CLIMES. REGARDS.
MESSAGE CLASSIFIED BECAUSE OF ADDRESSEES.
DESTROY 2 JUN 84
#6565

NNNN

ACT: G9
INFO: G9095
G91
Q32

7
D3

~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

CLASSIFIED WORK SHEET

This work sheet contains information affecting the National Defense of the United States within the meaning of the Espionage Laws, Title 18, U. S. C., Sections 793, 794 and 798, the transmission or the revelation of which in any manner to an unauthorized person is prohibited by law.

THIS FORM FOR INTERNAL AGENCY USE ONLY

U.S. GOVERNMENT PRINTING OFFICE: 1979-293-395

CLASSIFIED

P.L. 86

DOCID: 4019689

TRAFFIC ANALYSIS: Specialty Without Portfolio (U)

This is an address given by Mr. [redacted] the A2 Senior Analyst, at the 1980 Symposium of the Communications Analysis Association, and is based on his extensive experience on the Soviet Military Problem.

P.L. 86-36

[redacted] A2

This article is classified ~~SECRET - HANDLE VIA COMINT CHANNELS ONLY~~ in its entirety.

In addition to cryptanalysis, which I do not intend to deal with in this discussion, communications intelligence has always involved two primary, overlapping but distinct, tasks with respect to target analysis:

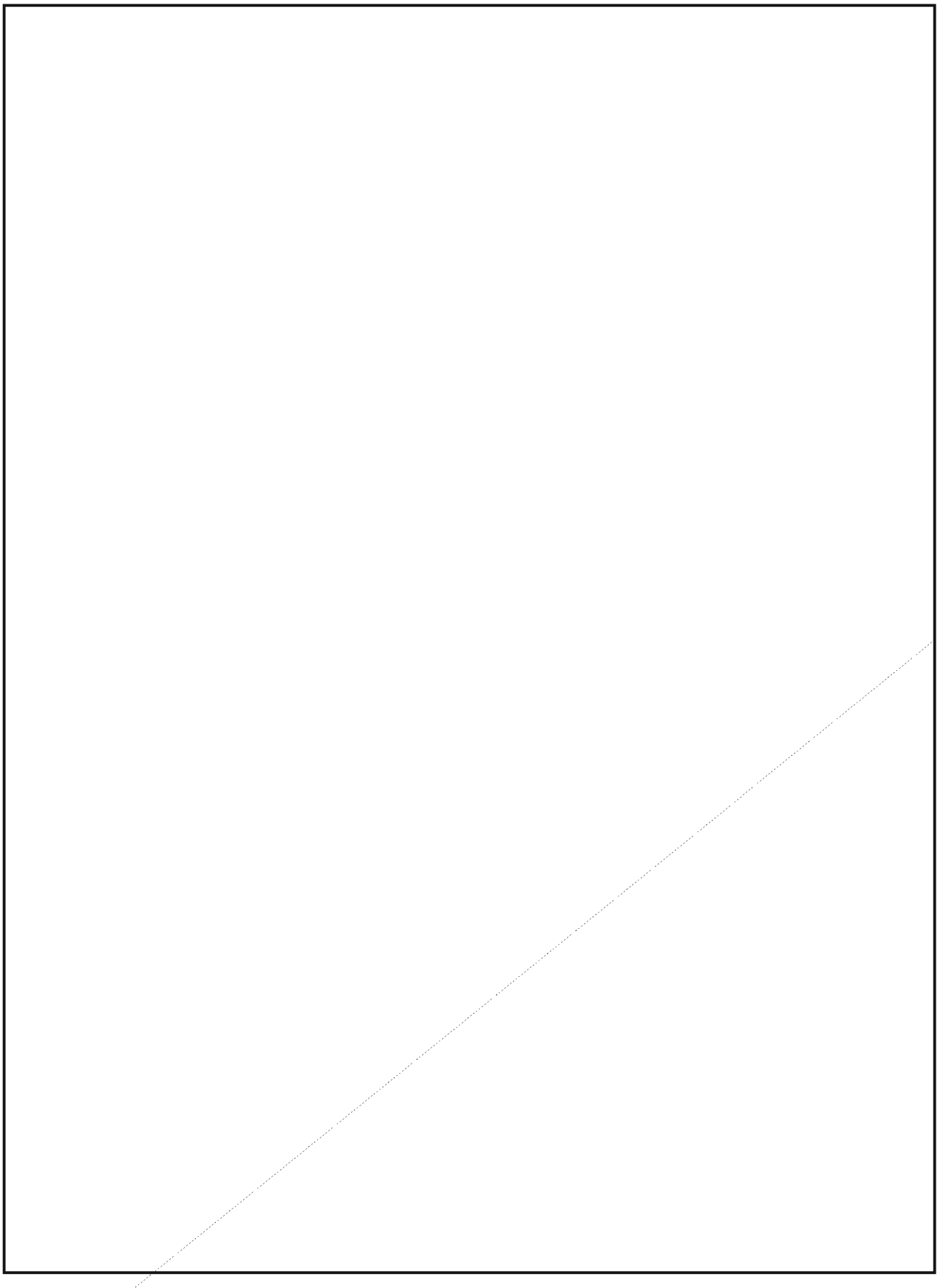
- ordering and understanding target communications structure and procedures—commonly referred to as *traffic analysis*, and
- describing target organizations, activities, intentions and trends —known as *intelligence analysis* or *special research analysis*.

The major overlaps of the two disciplines are in their contribution to target organization, or order of battle, and command and control.

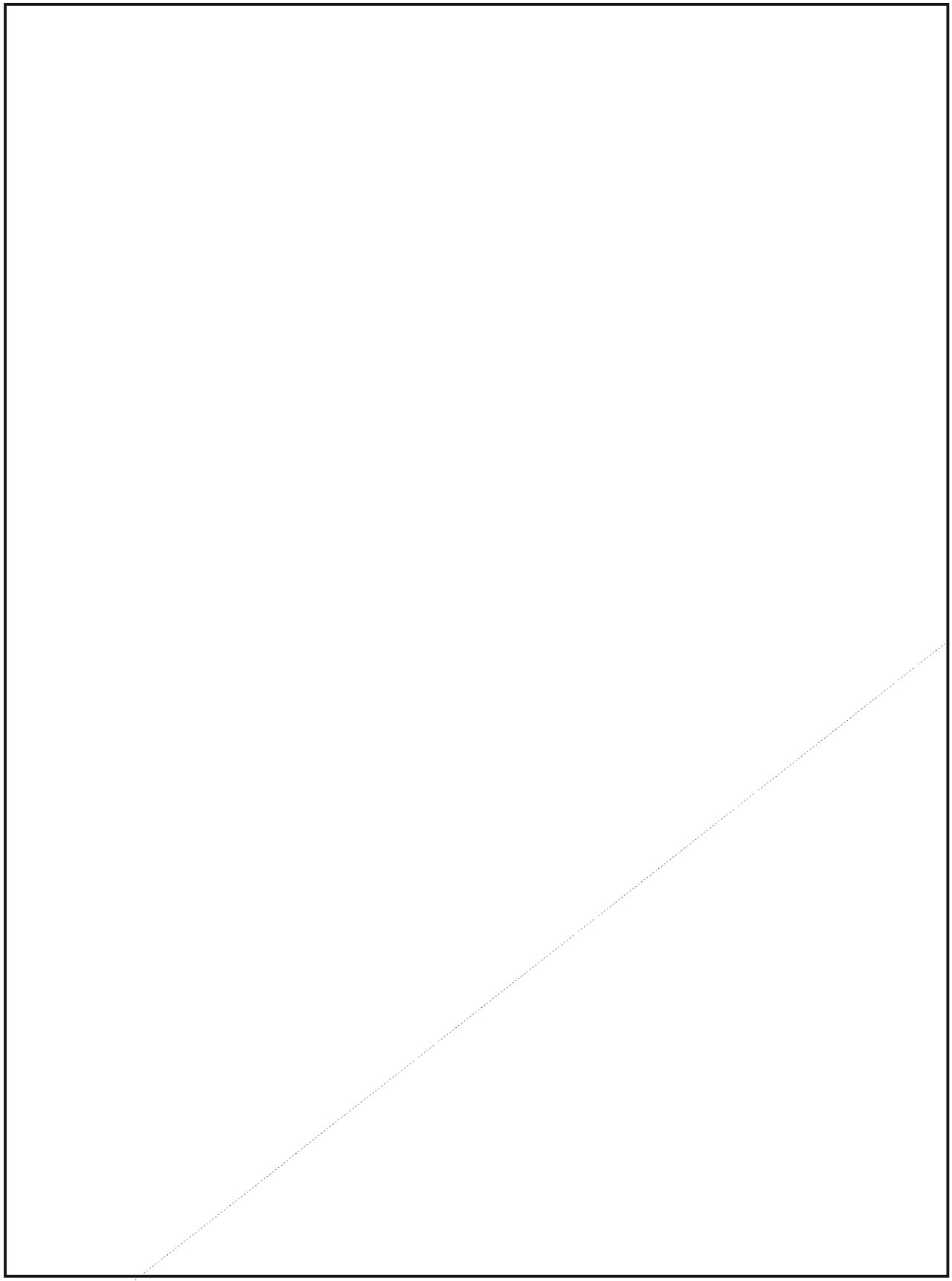
Of these two skills, only the latter one, intelligence analysis, has been effectively accommodated in the NSA career structure. Traffic analysis, in terms of its application, is largely regarded as a skill to employ if time and resources permit, which means that it is basically nonfunctioning in many important areas. In career terms, it has been essentially inaccessible to representative numbers of people, being an apprentice slot which must be abdicated by those with more than modest ambitions.

[redacted]

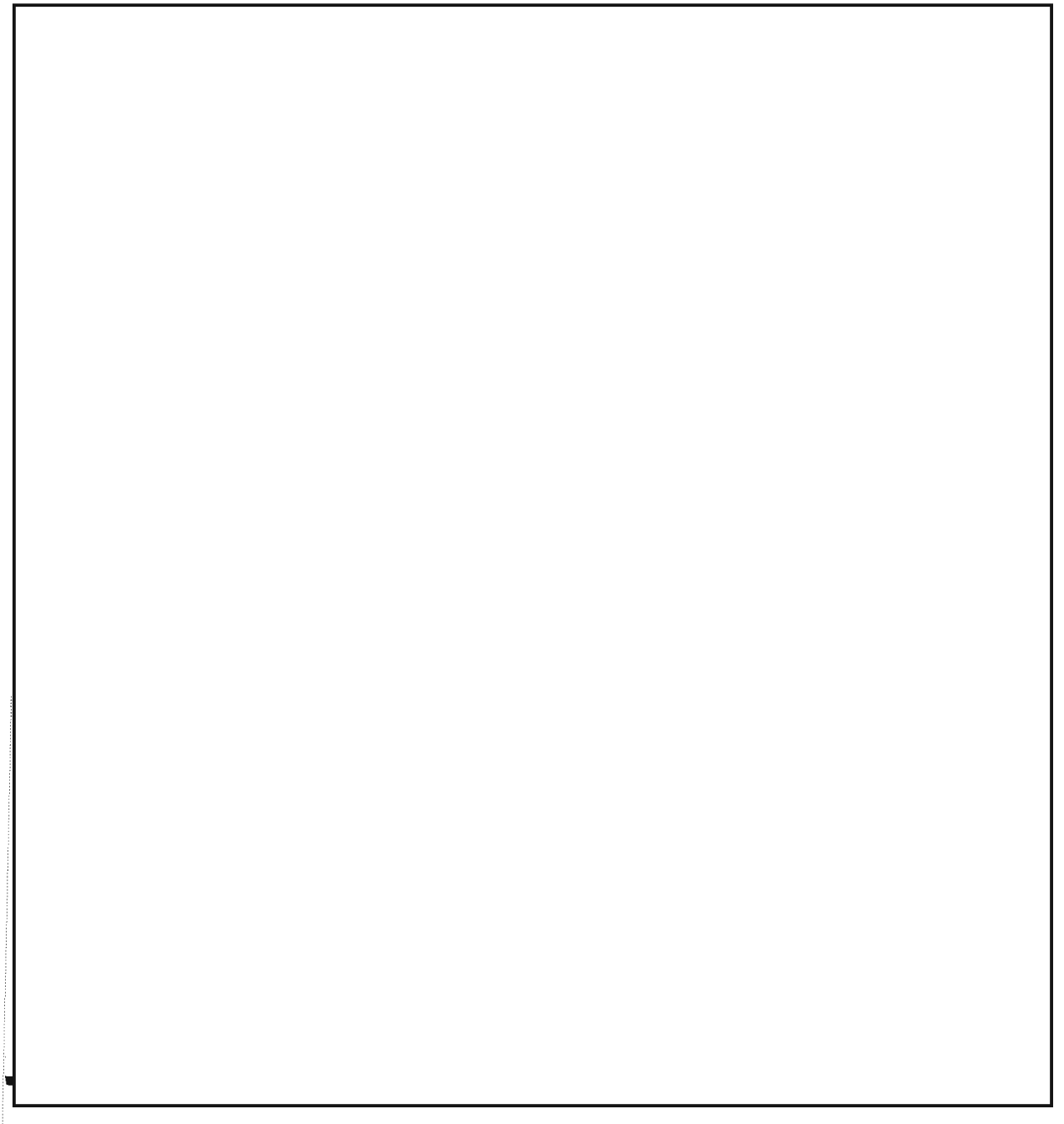
EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36



ATTENTION: PLATFORM USERS (U)

Those readers who wish to send contributions to CRYPTOLOG, and who have access to PLATFORM, may forward their submissions via PLATFORM. Send them to cryptolog (that's all in lower case) at BAR1CØ5. Contributions, naturally, will also continue to be accepted in handwritten or typed form. Any questions? Call 1103s.

EO 1.4.(c)
P.L. 86-36

DOCID: 4019689

DEFENSE INTELLIGENCE VIDEOCASETTE PROGRAM (U)

~~(C)~~ Did you know? Collateral Documents (T5322) holds a collection of videocasettes which are products of DIA's Defense Intelligence Videocasette (DIV) Program. The subjects range from documentaries on the Soviet military to interviews with authorities on Chinese society.

(U) The following is a list of the titles currently available. All titles are UNCLASSIFIED. Classifications of the tapes themselves vary.

The Soviet People

The Soviet Soldier

Soviet Airborne Forces

Soviet Amphibious Forces

Soviet Air Operation Concept

Soviet Tactical Electronic Warfare

The New Soviet Tanks

Soviet Armed Helicopters

The KIEV Deploys

*BACKFIRE

FOXBAT A

*The SS-20

*The Soviet Afghanistan Invasion

Warsaw Pact Military Posture

The Chinese People

China's Military Posture

(U) Except for those titles marked with an asterisk, these tapes may be borrowed from T5322 for a period of two weeks. For further information, call [redacted] on 8642s. The asterisked titles may be obtained from A2045, 5091s. P.L. 86-36

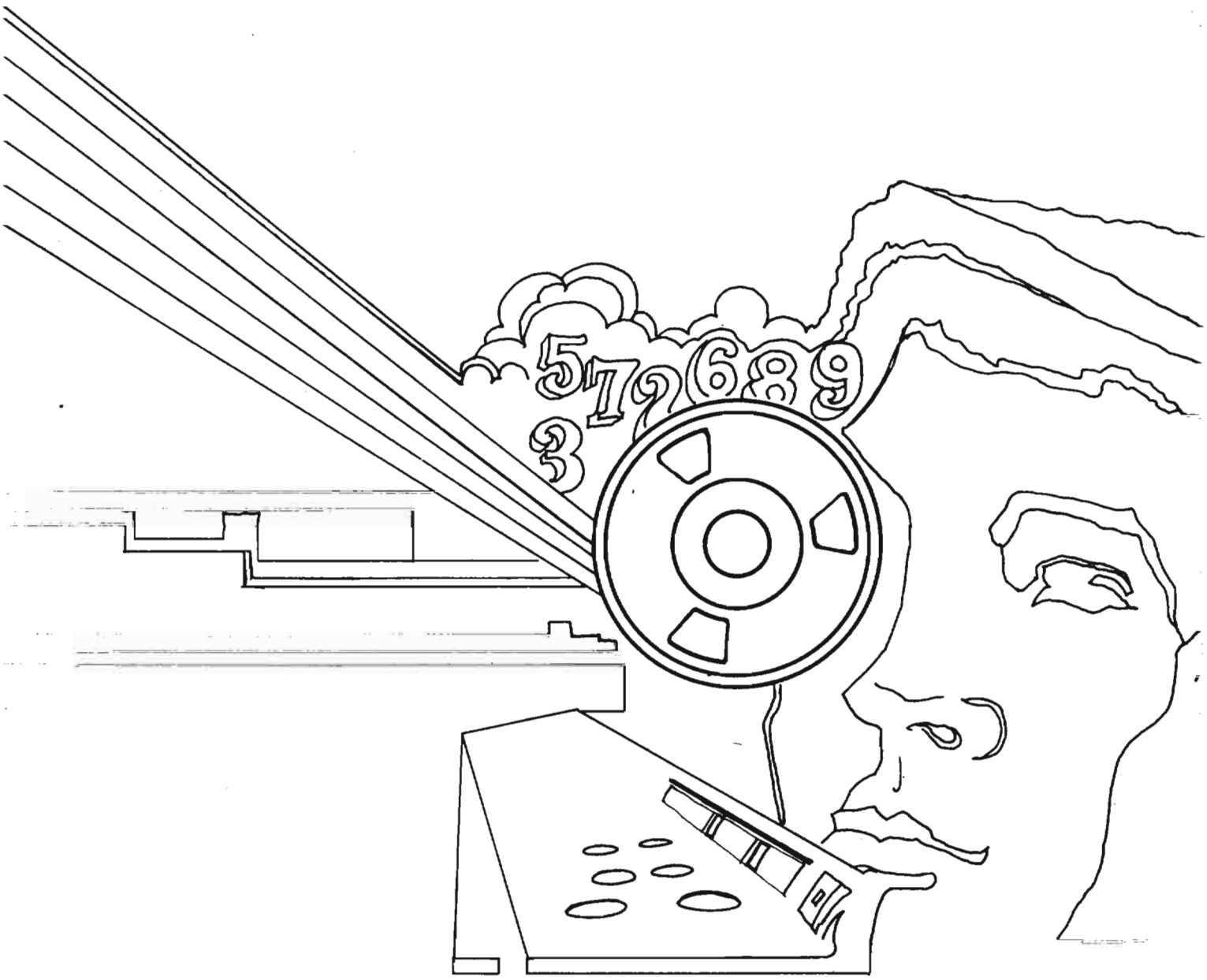
DOCID: 4019689

HELP!

CRYPTOLOG has no magical, automated way of updating our address list. So if you change jobs without letting us know, your continued receipt of the magazine will depend on the distribution personnel at you former job. Soem are very helpful in calling to notify us of new addresses. But not all are. Also, if your job doesn't change, but your organization does, because of reorganization, you may not continue to receive your copy.

So, if you have moved, or if you have been reorganized, the best way to insure that you will continue to receive CRYPTOLOG is to give us a call at 1103s.

P1-Oct 81-83-9858


5792689

DOCID: 4019687

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JAN- MAR 1981

P.L. 86-36

SIGINT IN THE 80s: TWO VIEWS (U)
I. Robert E. Rich.....1
II. William Lutwiniak.....4
KITTIWAKE (U).....[redacted].....7
HOW TO IMPROVE YOUR PROMOTION POTENTIAL (U).....[redacted].....10
NSA-CROSTIC No. 32.....D. H. W.....12
TRANSLATOR IN YOUR POCKET (U).....[redacted].....14
SOME THINGS NEVER CHANGE (U).....17
NCS-CLA SYMPOSIUM (U).....18
WHY DO THEY LEAVE? (U).....[redacted].....19

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 1 May 2011~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019687

~~TOP SECRET~~

CRYPTOLOG

Published by P1, Techniques and Standards,

for the Personnel of Operations

VOL. VIII, No. 1 - 3 JANUARY - MARCH 1981

PUBLISHER [redacted]

BOARD OF EDITORS

Editor-in-Chief.....David H. Williams (1103s)

Collection.....[redacted] (8555s)

Cryptanalysis.....[redacted] (4902s)

Cryptolinguistics.....[redacted] (5981s)

Information Science.....[redacted] (3034s)

Language.....[redacted] (8161s)

Machine Support.....[redacted] (5084s)

Mathematics.....[redacted] (8518s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Taurone (3573s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4019687

SIGINT in the 80s: Two Views

At the First Annual Symposium of the Communications Analysis Association held last year, the keynote address was given by Mr. Robert E. Rich, ADDO, and the concluding remarks were presented by Mr. William Lutwiniak, then Chief, P1, Techniques and Standards. So that persons who did not attend the symposium may see the views of two eminent agency managers on the future of SIGINT in the coming decade, CRYPTOLOG is pleased to publish both of these addresses.

I. Robert E. Rich, ADDO

I appreciate the invitation from your president to talk with you this morning as you begin your first conference, although I suspect that the term "Keynote Address" is more akin to what Jimmy Carter and Ronald Reagan have been doing than to what we're up to here. After all, a keynote address is usually a long collection of rhetoric that doesn't have much to do with the real issues at hand. It's just an upbeat thing to get people in the mood to do the hard work. Forgive me if the rhetoric isn't up to the standard you've been hearing from the politicians. In any case, when [redacted] P.L. 86-36 asked me to help kick off this series of meetings, it occurred to me that I wasn't really very sure what the expression "communications analysis" was intended to mean. Having done a little research—although not much analysis—I think I've discovered that it includes a a fairly broad scale of the hardcore skills and activities that are most critical to our business. It embraces cryptanalysis, traffic analysis, language work, and what we usually call "special research analysis," that is, the substantive interpretation of data that normally has been put into readable English. So that covers a wide range of the specialities without which there wouldn't be any SIGINT product.

(U) For the remainder of this morning and during tomorrow's sessions, you'll be considering some of the important things that will be happening in the analytic environments of the next ten years. Mainly these will have to do with better ways of doing analytic work with new tools, or at least new applications of technology. And a lot of that will have to do with the incredible potential offered by computers, especially the use of computers in an interactive way—machine working with human analyst to solve problems or get results faster.

(U) You'll be hearing, I think exclusively, from members of our own community describing their own work and their own ideas, rather than from outside experts. I mention that because I think we're too inclined to look to the outside in too many hard areas when we ought to be stimulating our own people to come forward with the results of their inspirations and their expectations for the future.

(U) To help you get started, I think the most useful thing I can do is to share some overall perceptions with you about our state of health at the moment, and to suggest some perspective about the analytic function as it relates to the other parts of the SIGINT process, and then finally to mention some trends for the future that will affect our prospects in analysis. All, of course, from my own vantage point, since there isn't much absolute truth associated with these matters, especially those which lie in the future.

~~(SC)~~ First off, I will suggest to you that SIGINT now is in better shape than at any other time in our history. By that I mean that the product we're able to deliver is more useful to more customers than ever before. And that includes customers of all kinds and at all sorts of levels: the traditional ones in Washington (like the White House and State and DoD and CIA), and a wide range of military commanders in the field, and also some newer customers, such as Treasury and Energy and Commerce. Day after day, the SIGINT output

is useful to those people-

[redacted]

[redacted]

(U) Now all that may sound like preaching to the choir. But it sometimes turns out that our people get so much engrossed in a particular speciality that they don't really appreciate the overall perspective of how well we're doing at the moment. And I hasten to add that I don't want to overstate this, because there are certainly improvements we need to make and keep making —the customers' appetite will always outstrip our ability to deliver. And the present state of affairs is also fragile; it could be dramatically changed by a number of things.

~~(TS-CCO)~~ But the point I want to make here is that the reasons for this relatively healthy state of affairs are not accidental—certainly not the result of the targets getting easier. (just the opposite is, of course, the case.) The reasons are complex, and I would just mention two of

[redacted]

[redacted]

~~(C)~~ The second thing that explains our current success is the quality of our energetic work force. The fact that we've got one that compares pretty well with other professional populations is partly luck and partly management. Luck because the nature of the business attracts people of quality; it's both demanding and rewarding from an intellectual standpoint. And when we've had to, we've been aggressive about finding and hiring good people. Some years ago we badly needed a core of first-rate mathematicians and we captured a good number who are still here. More recently we've needed numbers of linguists, and by and large, they have been found—not yet enough, but more about that later. But the point is, that, in addition to pretty good collection access, we've had the advantage of an analytic core of people who have an insatiable curiosity and drive to solve the problem and a high order of intellectual discipline. Taken together, these are the main ingredients in our present state of health.

EO 1.4.(c)
P.L. 86-36

(U) But there's no reason for complacency about any of that. The collection picture is constantly changing and the work force is always in a state of flux (even if we have one of the lowest attrition rates in the federal government). So we need to be constantly working to maintain a favorable balance. Heavier demands are certainly going to be put on it in the future. Which brings me to the next point—namely, the trends and influences that are going to affect analytic work in the years ahead.

(U) The quality of crystal balls probably hasn't changed much over the years, and mine isn't any better than most. But I'd like to suggest several things about our target environment that seem to me likely to come about, and then describe some qualifications that those things indicate for our analytic people.

~~(C)~~ In the decade ahead I would think it almost certain that the Soviet Union will continue to occupy the predominant part of our energy. And for reasons you all understand. It's just hard to imagine an extensive enough change in the fundamental difference between the USSR and the United States during that period which might permit us to do anything very different.

[redacted]

~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36

[redacted]

[redacted]

~~(C CCO)~~ So these are factors that will influence the analytic enivronment of the future, one way or the other. There's another class of influences, too, that will be important but hard to predict. An obvious one is the resource constraints we'll face. I think we haven't fared too badly in percentage of Federal budget allocated for SIGINT in recent years. We could do even better in the future, but maybe not—it's hard to know. Same thing with respect to technology. The improvement in computer power in the past decade has been almost incredible. If other, similar breakthroughs occur in the next decade, we could have great new opportunities for better analytic work. But again, it's hard to be sure.

~~(S-CCO)~~ One thing, however, does seem certain. And that is that, regardless of improvements in machine capability, good analysis will still depend on good analysts. And what is a good analyst? Some of the characteristics won't change—they'll be the same at the end of the coming decade as they've always been. I already mentioned a couple of these: great curiosity in approaching unsolved problems, coupled with good intellectual discipline so as to avoid sloppy inference and unwarranted conclusions. There are some others which will be more important in the future.

*multi-discipline skills—a linguist is a lot better off with an understanding of the cryptanalytic work underlying the decrypted text; an SRA is better equipped

EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~

DOCID: 4019687

with some understanding of the target language. This has been true for a long time, will be even more relevant in the future as the need for flexibility grows.

*the ability to deal comfortably with machine-assisted techniques, to use computers to produce necessary data bases.

*direct familiarity, where possible, with target environment—by living there, or at least by travelling in the area. Of course, this isn't possible for some, but could be for others.

*for some analysts, a more comprehensive grasp of special technology and terminology (nuclear proliferation, advanced weapons sytems, and the like).

*flexibility in changing from one target area to another. We'll need to develop more of this attribute, while still keeping enough analysts with long-term continuity on certain targets.

*responsiveness and objectivity in understanding customer needs.

*appreciation for the growing complexity of collection arrangements, so that analysis will be able to drive collection with maximum efficiency.

~~(C-CCO)~~ The list can certainly be extended. You will be thinking about some other important aspects of it during the course of this conference. For the moment, I'd like to leave you with the thought I mentioned a minute ago, namely, that regardless of how well we come along with technological progress, such as increased computer power, and regardless of how we solve the collection problem, our success will still depend very heavily on the quality of our analytic work force. It's critically important that we keep on acquiring young people who are excited by cryptanalysis, people who can deal with traffic analytic problems, people who have exceptional linguistic talent —and preferably some who can do several of these things well. Only in that way can we hope to maintain anything like the healthy posture we enjoy at the moment.

(U) I hope your sessions at this conference are productive and stimulating to you all, and I appreciate your attention this morning. Thank you.

II. William Lutwiniak, Chief, P1

When Bill Nolte asked me to ring down the curtain on this conference, my first reaction was to demur; but he suggested I look at the topics and read the abstracts already in hand before I begged off. I did that, and decided I could add some perspective to (U) where we are now and what the 80s bode for communications analysis. I thought it might be useful for experts in P1 to give me their notions of what's in the offing for the various cryptanalytic disciplines. I also pondered over Bob Rich's opening address. When I put all this together I found I had some things to say that may be worth listening to.

~~(TS-CCO)~~ We usually start with collection, the *sine qua non*. The technology affecting communication around the world is dynamic, driven as it is by the need for more efficient transmission. Satellite communications have been with us for some time, and we cope with them daily, more or less successfully, more and more selectively. But satellites will be going digital, and domestic satellites are in the wings—boding point-to-point traffic in bursts of hundreds of millions of bits per second. Multi-channel communications can look forward to electronic packet switching—tiny pieces of a transmission are switched electronically from channel to channel, unpredictably unless you know the algorithms. At the same time the spriralling costs of satellite communications have driven technology to look again at the HF spectrum (already saturated) with a view to overcoming multipath, jamming and other interference and of getting around the restrictions of the Maximum Utilizable Frequency. Mixed up in this is something called the WARC (World Administrative Radio Conference) in which everybody argues about who owns which parts of the radio spectrum and under what conditions. A dominant theme of WARC 79 was the need of the Third World for HF allocations, to be provided by the advanced nations, who are kind of balky at the prospect. Advances in frequency hopping, spread spectrum signals, compression coding and other techniques make the HF spectrum much more usable than

before, and considerably cheaper than satellite communications. Needless to say,

[redacted]

~~(S-CCO)~~ The volumes in view on these

[redacted]

~~(S-CCO)~~ So, one view of the 80s is that we

[redacted]

what this conference is all about, isn't it?

~~(C)~~ Technology is the threat, and technology has to be the answer for us. We've got more and more computing power and it's getting cheaper every year. A good thing, too, since we have fewer people and more targets, and *that* won't change, except to increase. The computer is the key, but we have to tame it so that it serves the analyst rather than the other way around. This problem has been with us for some time; we've been changing our technical lifestyle to live with the computer. A smart fellow in P1 points out that some time ago we stopped talking about analysis and began to speak of processing. Think about the implications of that one for a minute. We took the traffic away from the traffic analyst and put it in a computer, and he couldn't get it out without going through middlemen. The only way to tap the tremendous computer power to come—miniaturization, smarter and smarter terminals, personal portable computers—is to make that power submissive to us analysts, rather than for us to be dominated by it.

~~(C)~~ We've networked our computers, creating some painful security headaches, but we have created possibilities for a new analytic reach across problems and great opportunities for doing things we haven't even thought of yet against targets we don't yet know about.

[redacted]

P.L. 86-36
EO 1.4.(c)

Need it be said that, in a world where computers become more and more dominant, analysts who understand how a computer does its thing (and I'm not talking about programmers, as such) will find much to do all across the SIGINT process.

~~(C CCO)~~ We haven't really come to grips

[redacted]

standpoint. If there is any one thing about the entire SIGINT process that makes it so hard to explain to outsiders, it is the

[redacted]

~~(C-CCO)~~ I have listened to an analyst describe to me how *one* analyst

[redacted]

and also take care of the technical feedback in the process. Is he a misty-eyed dreamer? But think of the skills, training and experience that one person would have to possess. That person is the analyst of the late 80s. How do we bring about the species? Just as nature does—by evolution.

~~(S-CCO)~~ That is not to say that the classical SIGINT disciplines won't continue. We'll still need cryptanalysts, traffic analysts, collection professionals, computer scientists, linguists, signals analysts, and all the others. But even these specialists will need to be versatile, comfortable in more than one discipline, comfortable with computers and microprocessors. We need to get much better at handling plain language —automatic translation remains an elusive goal, but much can be done in machine-assisted translation of the recorded word to improve the productivity of linguists. The spoken word remains relatively intractable, but I see real progress in the 80s in automatically selecting the probable best traffic to subject to the personal attention of the transcriber. The traffic analyst can already, if he is willing to learn how to get back his traffic and work his will with it. The cryptanalyst has long since harnessed the power of computers, but even he needs to fit microprocessors and personal computers into his lifestyle. For any analyst, there is an area of research which commences after pencil and paper doodling and stops short of getting to a terminal to order a computer to do something, that is a sort of wasteland of abandoned ideas and aborted projects. The personal computer has an important role to play here.

~~(C)~~ Bob Rich pointed out that our most important resource is the quality of our analytic workforce. The technology that is and will be available in the 80s means little unless we use it effectively and imaginatively, and it is up to this workforce to do just that. It isn't as if we have any choice—all of us analysts must become more versatile and more effective. We've got to improve our quality, because our quantity won't increase. We must learn to use new tools, and indeed play an active role in choosing and specifying those new tools. We must find means to exchange information and document new analytic techniques. This has always been a problem in the past, but now we are evolving into a world of computer networks, terminal sub-systems featuring mini-computers and microcomputers which will make up the analyst's "SIGINT Target Station." The old vehicles—*C-Liners, Dragon Seeds, Saints*—could be revived, but will they do? We're no longer talking about pencil-and-paper techniques, easy to describe and publish; we're talking about how to choose from and apply a set of several programs and many modules which sort, select, reformat some subset of an analyst's own data base. The techniques may involve specialized program language to retrieve and compare two fields of different records based on the contents of a third field, flagging the records with shorthand code for further treatment. How do we record, publish and disseminate these? How do we give each other the benefits of our own improvements?

~~(C)~~ The crystal ball is murky; all one can say for certain about the 80s for the communications analyst is that they will bring challenges. Only the dim shape of those challenges can be discerned, but it is clear that we analysts will have to evolve into a SIGINT world far more automated and computerized than the one we have today. The main challenge is to make automation and computers work for us analysts, rather than vice versa. And there is a challenge here for management: it must foster the environment and climate to permit the evolution of a new species.

* * * * * * * * * * * * * * *

(UNCLASSIFIED)

SOLUTION TO NSA-CROSTIC No. 31.

From "Q. E. D. - 2 Hours, 41 Minutes," by Lambros D. Callimahos. NSA Technical Journal, Fall 1973.

"Spencer Akins: Letter to Birkhan."

"Your letter indicates that the purpose of your entering into communication with this office on the subject of the Kryha cipher machine is to make known its merits for consideration for use in the military service. This device has already been well studied and, I regret to advise, was found unsuitable for adoption in the military service."

(UNCLASSIFIED)

* * * * * * * * * * * * * * *

DOCID: 4019687

P.L. 86-36

[redacted]

T44

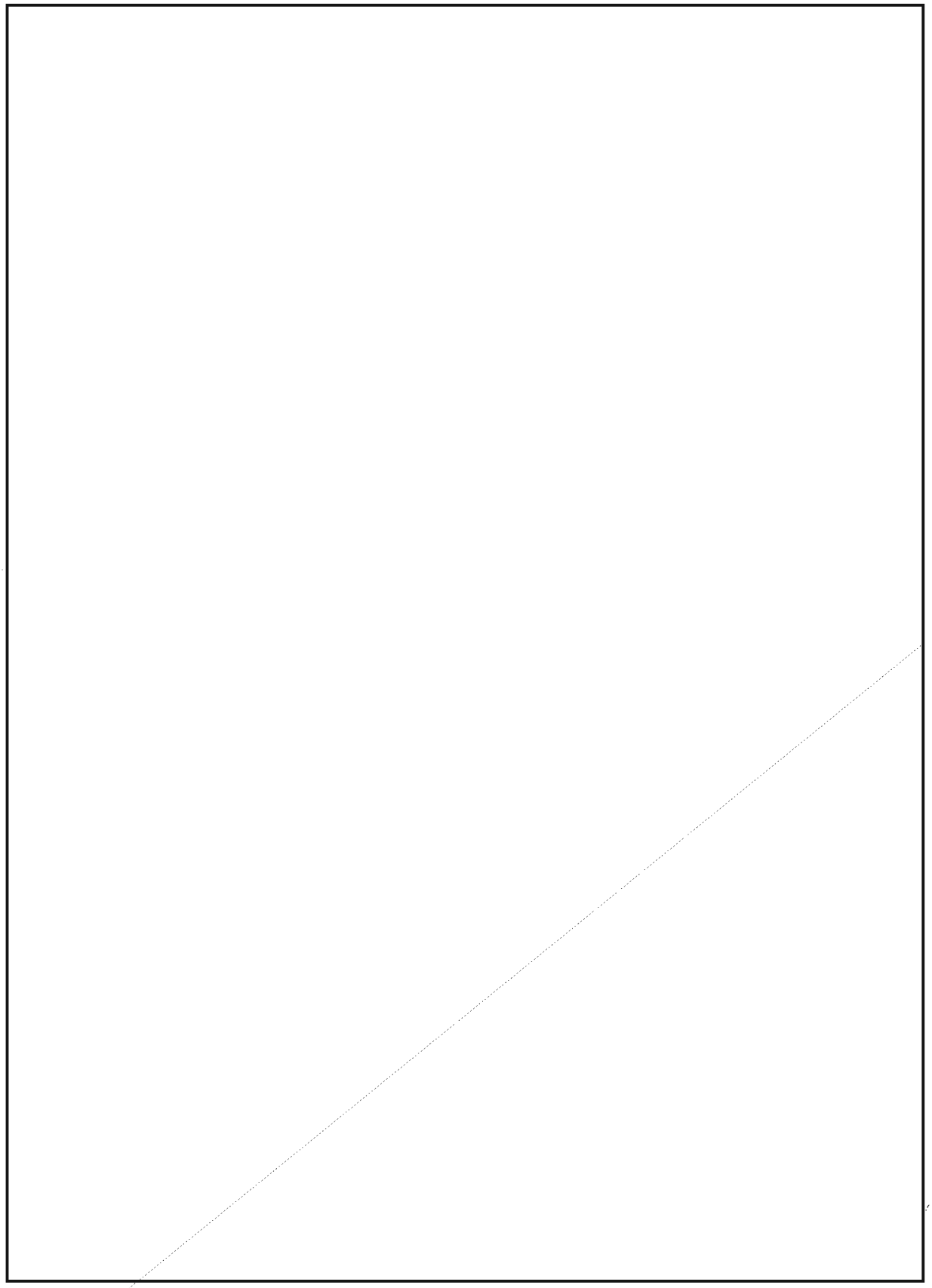
The kittiwake is a small, far-ranging gull (genus *Rissa*), native to the sheer cliff shorelines of Britain, and named in imitation of its cry. Its range, at least in name, will soon be extended [redacted]

[redacted]

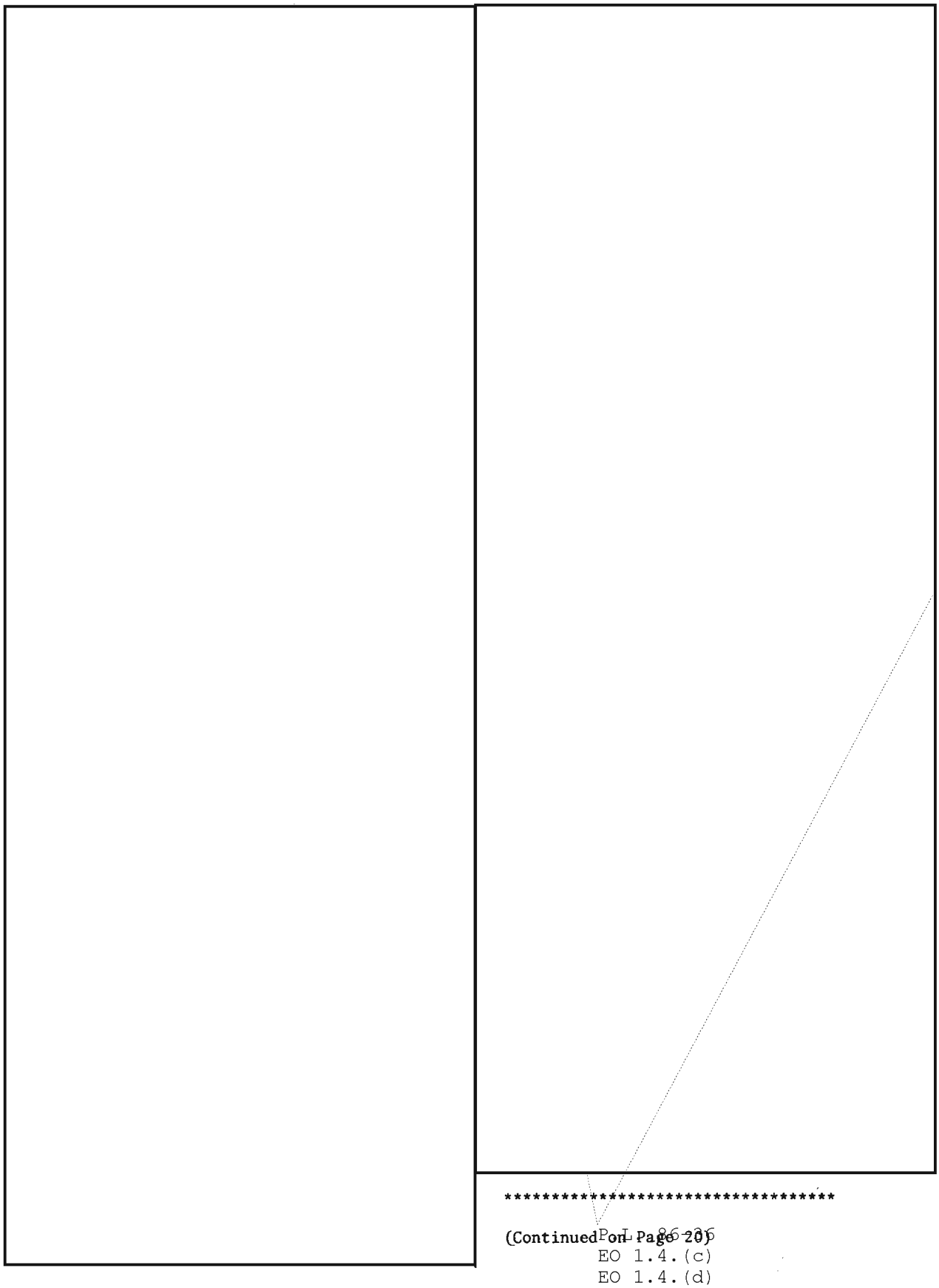
[redacted]

P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

~~SECRET~~



P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)



****

(Continued on Page 20)

PL 86-36
EO 1.4.(c)
EO 1.4.(d)

DOCID: 4019687

HOW TO IMPROVE YOUR PROMOTION POTENTIAL

[redacted] P.L. 86-36

The new Performance Planning, Evaluation and Counselling program (PPEC), put into effect in January 1981, should make it easier for you to see what is in your records and to know what your supervisor expects of you. However, as with past systems, A LOT WILL STILL BE UP TO YOU. While the following suggestions won't guarantee you a promotion, they can help you stay ahead of whoever is in second place. (That statement and the following are my personal suggestions.)

First, you must know what your job is, and do it well; keep your boss happy; support your organization; and, be a conscientious, dependable employee. Competition is keen, so you must go that extra step, be a bit more creative, work a little harder, and produce a little more to stay ahead of your peers.

Second, make sure your personnel records are accurate and current. These records represent you during many important reviews, as, for instance, when management is considering candidates for key positions or special assignments. Also, promotion boards select or reject people for promotion largely on the basis of the data contained in their records. Pay particular attention to assuring that the following are correctly represented:

- Your education. If you've received a certificate or degree of any kind since you entered on duty, you must complete the Employee Education Record, Form 4694, and forward it through channels to get that important achievement entered in your records. This does not happen automatically. If you've taken courses but have not received your degree, be sure these are recorded.

- Your COSC and suffix. If you are a supervisor, be sure the suffix is "S".

- Your certifications. Also be sure that you have the required combination of certifications and job title for your next promotion. If in doubt, check it out with your supervisor or personnel representative. You should continue professional and self-improvement activities, such as education and training, so that you will keep your mind active, grow in ability and stature, and improve your chances of being given increased responsibilities and promotions.

- Performance Appraisals. These ratings are very important in comparing competing candidates for promotion. Be sure you do everything within your power to achieve the best ratings you can. Also verify that your ratings are correctly recorded in the data base. If you were rated in the top six percent, be sure that is correctly recorded. On the other hand, if you find yourself in a situation where you cannot earn high ratings no matter how hard you try, consider transferring to a new organization, job or career field.

- Personnel Summary. If these are required for your grade, be sure yours is accurate and current. YOU must prepare your Personnel Summary and keep it up to date, making sure it reflects your current job achievements, awards, education, overseas assignments, and so forth. (For an excellent guide, read [redacted] article, "Some Tips on Getting Promoted," in the December, 1978 CRYPTOLOG. Virginia's article has had a positive effect upon Personnel Summaries, but it is unbelieveable how many senior people still neglect this important matter.) P.L. 86-36

Third and finally, you should consider the following list of general suggestions:

- Be conscientious and provide responsible and timely service to everyone you support.

- Continually search for and identify ways to improve individual and aggregate effectiveness.

- Be realistic and think positively; don't spend a lot of energy finding fault or specifying reasons why something can't be done. Rather, find ways to excel in spite of obstacles.

- Do thorough and complete work. Don't pass half-finished answers to your boss and others and expect them to do the work for you.

- Always try to do professional, high-quality work.

- Take the initiative in doing things which must be done; don't wait for someone to get you started.

DOCID: 4019687

- Keep your boss posted on things you think he should be aware of. He should reciprocate.

- Support your boss in solving the organization's problems.

- Meet deadlines and let people know if there are obstacles which may prevent that.

- Create a good image for yourself and your organization.

- Be a good team member, involving others, training and helping them, recognizing and using their strengths and tolerating or helping eliminate their weaknesses.

- Be sensitive to the needs and limitations of your audience. Know when it is necessary to summarize or simplify things so that busy people can look, comprehend, and know what we want them to do, so that they can act quickly.

- Be a company-person while you are at work; put the organization's goals ahead of your personal goals.

- When you have questions or problems, or you aren't sure what's expected, discuss these concerns with your boss.

- And, very important, as a first order of buisiness on any new job, *train your own replacement*. Not only does this insure the presence of someone who can back up your work in your absence, but it also leaves you free to accept a new assignment—possibly, a step up—with minimum inconvenience to the organization.

You may wish to add items which are important in your particular situation, but which have not been included here.

I am tempted to close with, "Good luck!" But I am confident that you won't need much luck to get promoted if you make a serious effort to follow these suggestion. Moreover, these ideas should help you to continue to earn your true economic worth quicker than most.

CLA/NCS Film Series

The following foreign-language films are scheduled for showing to interested Agency personnel. These presentations, which are jointly sponsored by the Crypto-Linguistic Association and the National Cryptologic School, are shown in the Friedman Auditorium at 0930 hours on the days indicated. The films are unclassified.

Thursday, 14 May	"Wozzeck" (German)
Thursday, 25 June	"Border Street" (Polish)

All personnel are invited to attend.

DOCID: 4019687

NSA-Crostic No. 32

by D. H. W.

This puzzle uses cryptic definitions: puns, anagrams, constructions, etc. If you are not familiar with this form, call CRYPTOLOG on 1103s, and you will be sent a rundown on definitions of this type. Good luck!

A. Put away the swords, Heather said

209 219 86 62 189 191 215

B. Ornithogalum thyrsoides (2 wds)

92 76 113 146 155 79 163 88 119 132 24 60 199

143 250 54 4 106 12 176 239

C. Surrey town located above U.S. Marine

142 33 158 130 240 228 145 248 29 9 180

D. Twins age fast at new museum (2 wds)

84 178 202 169 95 127 100 56

E. "And so he mediates, twice near
The tides that wash on old Algier" (2 wds)

111 14 94 105 247 123 152 131 173 148 201 52 245

226 23 237

F. Head of Metro and DDE visit Douglas

230 154 227 253

G. Get Helen Kennedy.

184 135 89 112 235

H. "Does it hurt?" "___ I laugh." (2 wds)

164 6 91 63 186 223 107 128

I. Hilaire Belloc hero usually has yellowish hue

26 97 2 224 21 68 65 182

J. Twenty-four hours ago he was a steady rye drinker

232 77 238 210 137 7 25 241 73

K. Wrapped in the wads of bandage

222 214 225 190 136 171 149

L. Not on hand

37 109 144 67 87 117 213

M. It's the wonderful lather we feel leads to such a state of perfection (comp)

20 151 66 121 140 98 203 236 194 254 217 138

N. "Bonnie ——" (2 wds)

133 30 22 17 118 167 251 61 208 177 160 75 81

O. Wearily I left to see my solicitor

104 19 47 166 3 34

P. Disregard

69 179 170 200 206 168

Q. Double checker of a tergiversation

159 147 114 45 42 162 70 141 96 78 244 53 211

15

R. Restive; not asleep (var.)

188 1 231 183 50 27 10 57

DOCID: 4019687

S. Worse than a vile sea monster

212 71 80 41 116 153 83 110 55

T. Indian town for two idiots

229 156 72 46 125 85

U. Large ice sheet in Antarctica (var.) (2 wds)

49 5 129 122 103 31 187 243 216 40

V. To make the stout weed tender, he boiled it longer than anyone else

64 58 174 204 218 197 32 48 101

W. I betrayed him when I saw him swipe a cheddar cheese

234 192 99 124 205 195 18

X. Smelly seat in church?

150 39 35 207

Y. Remark directed at Dr. I.Q. (8 wds)

233 28 102 242 43 181 172 90 185 161 139 59 82

252 220 36 16 157 198 246 93 193 8 108 115

126 165 196

Z. The salamander went home

221 120 74 38

Z_1. Develop a large state in the mind

11 51 134 13 44 175 249

1 R	2 I	3 O	4 B		5 U	6 H	7 J		8 Y	9 C	10 R	11 Z_1	12 B	13 Z_1	14 E
15 Q		16 Y	17 N	18 W		19 O		20 M	21 I	22 N	23 E	24 B	25 J		26 I
27 R		28 Y	29 C	30 N	31 U		32 V	33 C	34 O	35 X		36 Y	37 L	38 T	39 X
	40 U	41 S	42 Q	43 Y		44 Z_1	45 Q	46 T		47 O	48 V	49 U	50 R		51 Z_1
52 E	53 Q	54 B	55 S	56 D		57 R	58 V	59 Y	60 B	61 N		62 A	63 H		64 V
65 I	66 M		67 L	68 I	69 P	70 Q	71 S		72 T	73 J		74 Z	75 N	76 B	77 J
	78 Q	79 B	80 S	81 N		82 Y	83 S	84 D	85 T		86 A	87 L	88 B	89 G	
90 Y		91 H	92 B	93 Y	94 E	95 D	96 Q	97 I	98 M		99 W	100 D	101 V		102 Y
	103 U	104 O	105 E	106 B	107 H		108 Y	109 L		110 S	111 E	112 G	113 B	114 Q	115 Y
116 S	117 L		118 N	119 B	120 Z	121 M	122 U	123 E		124 W	125 T	126 Y		127 D	128 H
	129 U	130 C	131 E	132 B	133 N	134 Z_1		135 G	136 K	137 J		138 M	139 Y	140 M	141 Q
142 C	143 B		144 L	145 C	146 B	147 Q	148 E	149 K		150 X	151 M	152 E	153 S	154 F	155 B
156 T	157 Y	158 C	159 Q	160 N	161 Y		162 Q	163 B	164 H	165 Y	166 O	167 N	168 P		169 T
170 P	171 K		172 Y	173 E	174 V	175 Z_1	176 B	177 N		178 D	179 P	180 C		181 Y	182 I
183 R	184 G	185 Y		186 H	187 U	188 R	189 A		190 K	191 A	192 W	193 Y		194 M	195 W
196 Y	197 V		198 Y	199 B	200 P	201 E	202 D	203 M		204 V	205 W	206 P		207 X	208 N
209 A		210 J	211 Q	212 S	213 L		214 K	215 A	216 U	217 M		218 V	219 A	220 Y	221 Z_1
	222 K	223 H	224 I		225 F	226 E	227 F	228 C	229 T		230 F	231 R	232 J		233 Y
	234 W	235 G	236 M	237 E	238 J	239 B		240 C	241 J	242 Y	243 U		244 Q	245 E	246 Y
247 E	248 C	249 Z_1	250 B		251 N	252 Y	253 F	254 M							D.H.W

DOCID: 4019687

TRANSLATOR IN YOUR POCKET

[redacted] P16

P.L. 86-36

Now that personal computers are a household item and hand-held calculators are being held by almost every hand, it has become inevitable that hend-held language "translators" should be vying for their share of the market. They claim to ease the problems of travel in foreign lands. But what can these electronic translators actually do, and are they worth the investment?

First let's note that the word "translator" is used rather loosely. The device won't replace a human being skilled in the languages of interest. For most purposes, it won't even replace a pocket dictionary. But it may be a useful tool for vocabulary drill, pronunciation, grammatical review, conversion, or checking the waiter's addition. (They also function as conventional arithmetic calculators.)

The general format is a hand-held, battery-powered, microprocessor-driven device into which one or more programmed modules may be inserted. A keyboard permits the entry of alphabetic and numeric characters, as well as a few special characters. A small selection of modules (usually containing one language or one language pair per module) is available with the introduction of the device; additional modules are introduced later, as they become available. Several modes of entry are possible:

- words may be spelled out, one letter at a time, and entered into temporary memory, to build a phrase or sentence
- high-frequency phrases or partial phrases may be keyed in
- sequences of words may be searched, to find a specific word, or as a vocabulary drill

Built-in phrases have the advantage of being grammatically correct, but, of course, their number is limited. The number of distinct words, although larger than the number of phrases, is also quite restricted, especially as compared to a pocket dictionary. Furthermore, the meaning selection is restricted to a single word, and no attempt is made to achieve grammatical correctness as the words are used in a stream. This can best be illustrated by discussing the individual translator models.

There are three currently on the market—the Lexicon LK-3000 by Nixdorf, the Craig M100, and the Texas Instruments Language Translator. Sharp Co. has a model (with about five times the word capacity of the others) which may be introduced in the United States in the near future.

The Lexicon was the first on the market and is currently the one with the widest array of language modules. The keyboard contains 26 letters, a space key, and an "upper case" capability for ten digits, eight special characters, and nine special-purpose keys. There are six function keys:

- a function key [f], used predominantly with modules other than language modules
- a clear key [clr], used to halt one process and begin another
- a backspace key [bs], used to delete characters one at a time (when entering a word) or to reverse the direction of translation (after pressing the clear key)
- an "open dictionary" key [?], used to search alphabetically through the words in the dictionary
- a step key [stp], used to enter the words of a phrase into temporary memory (before a word is admitted to temporary memory, the dictionary is searched; if the word is not in the dictionary, the user may try to substitute a word that *is* in the dictionary). This key is also used in conjunction with the "open dictionary" key to step through the dictionary one word at a time. For example, to find the English words and phrases beginning with "I", press "I", then [?], then [stp]. The phrases "I am", "I am hungry:, "I am in a hurry", and so forth, will appear in sequence with each suc-

DOCID: 4019687

cessive press of [stp]. To obtain the translation of one of these phrases, press [?].

- the definition key [def], used when the word, phrase or sentence is complete, to give the original and its translation.

A few idiosyncrasies can be illustrated with the English-Portuguese module. Suppose the following words are entered into the temporary memory by pressing the [stp] key following each word, which causes each word to be looked up individually:

YES [stp] I [stp] WANT [stp] DINNER [def]

The translator will deliver:

YES I WANT DINNER = SIM EU QUERER JANTAR.

progressively across its screen. But if the words "I WANT" are entered as a phrase:

YES [stp] I WANT [stp] DINNER [def]

the result is more grammatical:

YES I WANT DINNER = SIM EU QUERO JANTAR.

The practiced user will learn the phrases which are available, in order to take advantage of this feature.

Sometimes words are available only in Portuguese. For example, when entering the phrase QUE HORAS SAO one word at a time, the user discovers that HORAS and SAO are not in the dictionary. But when entering it as a phrase, that is, without a [stp] after each word, the user reads

QUE HORAS SAO = WHAT TIME IS IT.

Its limited vocabulary will be one of the biggest frustrations for the user. There are about a thousand vocabulary items (each word and each phrase counting as one item). Travelers with children, for example, may well wonder why "pizza" and "beer" are included, but "milk" is not.

A cursory grammatical summary attempts to acquaint the user with the vagaries of the foreign language. It's probably better than nothing at all, but that's about the most that can be said for it.

The Lexicon's memory is arranged in English word order. Stepping through vocabulary words that begin with the same letter or letters is very prompt when in the English mode. In the foreign-language mode, however, there are frequent pauses, during which the device advises "SEARCHING."

Bilingual modules currently available are between English and Spanish, French, Italian, German, Polish, Portuguese and Greek, with Swedish, Russian and Japanese in preparation. Also available is a "Person to Person" module, which, according to the manufacturer, "contains fun, social vocabulary in six languages. Introduce yourself, suggest a game of tennis, make a dinner date...in any combination of English, Spanish, French, German, Italian or phonetic Greek."

There is also a calculator module which "turns the LK-3000 into a sophisticated five-function calculator with memory, memory-plus and memory-recall functions. For the benefit of world travelers, this module also provides conversions for metric units and for foreign currencies.

Finally, the Lexicon can provide a filing system module and a personal program module. The latter permits the user to create his own small (1000-character) dictionary, and to retrieve stored data based on a search key.

The Craig M100 has similar features, with a few extra bells and whistles. Instead of bilingual modules, it offers single-language "capsules," three of which may be inserted and made accessible at any one time. Each capsule contains about 1200 words or phrases. Expanded memory capsules with over 2000 words apiece, including verb conjugations and case endings, are now being introduced. The keyboard allows for 26 letters, a space, ten digits, and ten special characters.

The bottom cover of the M100 has two lists—one of complete phrases and one of partial phrases, each identified by a single letter. When the PHR key is pressed once, followed by the appropriate letter, one of the complete phrases will be displayed. Depressing PHR twice, followed by one of the letters yields the corresponding partial phrase. The phrase will then be displayed in the language of interest by pressing one of the language selection keys.

Words may be entered one letter at a time, and may be used in conjunction with the phrase and partial phrase inventories. The capability to select from various meanings of a word is included. For example, WATCH (CLOCK) and WATCH (SEE) are both possible. The user chooses the one desired. In order to determine what the choices are, the user presses the SCH key after spelling the word WATCH. The same procedure can be used to find the correct spelling of a word. Words are held in memory until the user presses the Language Selection Key desired.

In addition to the capability to search the memory alphabetically, it is also possible to search it categorically, using the [LRN] key. For example, the sequence

[CLR] FAMILY [LRN]

will yield

FAMILY
PARENTS
FATHER
MOTHER
HUSBAND
...

(U) Even with no capsule in place, the M100 can perform simple calculations and basic metric conversions. And fourteen common expressions can be evoked in four languages—English, French, Spanish and German.

(U) Capsules are currently available for English, French, German, Spanish, Italian and Japanese. There is a Phonetic Pronunciation Capsule, with which "the user can now pronounce words in any translated language." Other capsules in the works are Bar and Wine, Nutritional, Calorie Counter, Spelling, and various word games.

(U) The M100 has the following ten function keys:

- a clear key [CLR], which clears the entire entry when the device is in translate mode; when in calculator mode, it clears the entry and returns to translate mode.
- a clear entry key [C/E], which clears the entry in calculator mode, but acts as a backspace/delete key in the translate mode
- a shift key [SHFT], which must be used before each keystroke when a digit or special character is desired
- an external program key [EXT[, which selects the calculator program, which is built in, or a special purpose program
- a phrase key [PHR], which starts or stops a vocabulary review by word category, such as car, train, hotel, sick, and so forth
- a fast/slow key [F/S], which is used to select the relative speed of automatic functions (speed of motion of text across the screen, or speed of search and learn functions)
- a rotate key [ROT], which causes the display to move across the screen
- a search key [SCH], which starts or stops an alphabetical search of the file
- a hold key [HLD], which allows the user to enter a word on the screen even if it is not in memory. This is used for proper names and cognate words.

(U) In addition there are three keys which are used to select among the three capsules, and another to select the built-in information.

(U) Texas Instruments has recently introduced its "Language Translator," which apparently has similar capabilities to those of the other two, but with one added capability: it will pronounce the words or phrases for you. It is currently available with English, French, German, and Spanish modules.

(U) The translators list for between $120 (Lexicon) and $300 Texas Instruments), but discounts are available. Extra modules are $25 for the Craig and $60 for the other two.

(U) The question remains—are they worth the money? Probably not, if you expect to forego the standard ways of getting around in a foreign country, such as dictionaries, language courses, and the like. But if you're gadget-happy, if you like the idea of being the focus of attention while the natives "ooh" and "ah" over your electronic translator, if you want to own an expensive calculator that does more than just calculate, or if you have an eye on some of the special-purpose modules now being developed, then perhaps you will decide to get a translator of your very own.

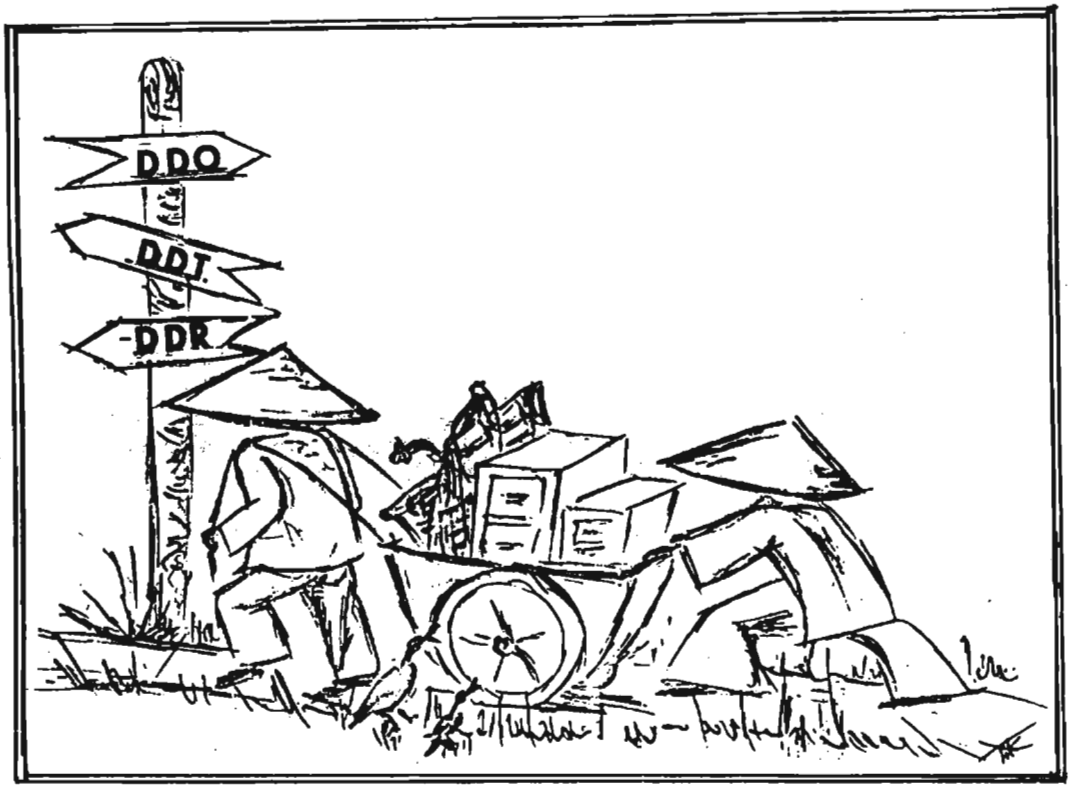
(U) And if you can't decide, perhaps you would like to try the Craig or the Lexicon which P1 has available for loan. If so, call the author on 1103s.

~~(C-CCO)~~ POSTSCRIPT: With regard to potential applications within the Agency for electronic translators, [redacted] offers the following observations: Although there might not be a groundswell of interest in language translators *qua* language translators, the ability to enter one's own data into them makes them very interesting indeed. If they contained a small code book, they could be used for quick look-up of terms, pr maybe callsigns, or abbreviations, or you-name-it. R17 is currently in the process of modifying one of these translators to perform various COMSEC and other user-defined functions. This research may open broad new vistas for analytic, COMSEC or training potential. Watch for more information about experimentation, and don't hesitate to call with any ideas you have that you might want to try.

P.L. 86-36

DOCID: 4019687

Some Things Never Change...



" We trained hard.....but it seemed that every time we were beginning to form up into teams we would be reorganized. I was to learn later in life that we tend to meet any new situation by reorganizing; and a wonderful method it can be for creating the illusion of progress....."

Petronius Arbiter, 210 B.C.

NCS-CLA Symposium

The National Cryptologic School and the Crypto-Linguistic Association are co-sponsoring a Language Training Symposium in May and June of this year. At the opening session on 5 May, following intorductory remarks by Lieutenant General Lincoln D. Faurer, Director, NSA, the keynote address will be given by Mrs. Minnie Kenny, Deputy Assistant Director for Training.

The symposium will present a broad spectrum of language training programs and perspectives, featuring speakers not only from NSA and the Service Cryptologic Elements, but also from the Defense Language Institute, the Foreign Service Institute. CIA. the Marvland State Department of Education. the Montgomery County (MD) Public Schools, and the Congress of the United States. Appropriately, the final session on 12 June will focus on the methodology and techniques of evaluation of language training.

The Special Group for Linguistics (SIGLING), whose chairman is [redacted] has invited a distinguished group of outside speakers for the symposium, which will be the first of its kind ever held at the Agency. All sessions will be held in the Friedman Auditorium. Those in May will be open to everyone; those in June will be for fully cleared personnel only.

The schedule is as follows:

P.L. 86-36

Tuesday, 5 May, 1300-1500	Welcome — [redacted] President, CLA Introductory Remarks— Lt Gen Lincoln D. Faurer, USAF, Director, National Security Agency Keynote Address—Mrs. Minnie Kenny, Deputy Assistant Director for Training, NSA
Wednesday, 6 May, 1300-1500	The Russian Linguist Acquisition Program and the Romanian Instruction Program— [redacted] P16, NSA
Wednesday, 13 May, 0900-1100	A Congressional Perspective on the Language Problem—Hon. C. W. "Bill" Young (R-Florida)
Thursday, 14 May, 0900-1100	CIA Language Training Programs and Oral Interview Testing— [redacted]
Tuesday, 19 May, 1300-1500	FSI Language Training Program and Novel Approaches to Language Learning— Dr. Earl Stevick, Foreign Service Institute, Department of State
Thursday, 21 May, 1300-1500	Two Perspectives on Language Training: Academia—Mrs. Marie S. Rentz, University of Maryland Maryland State Public Education—Miss Ann Beusch

DOCID: 4019687

Tuesday, 26 May, 0900-1100	Defense Language Institute Training Program—Lt Col Roland W. Fleming, Jr.
Thursday, 28 May, 0900-1100	Total Immersion Language Study Spanish—Miss Louise Rosenberg, Rock Creek Forest Elementary School, Chevy Chase, MD French—Dr. Gabriel Jacobs, Four Corners Elementary School, Silver Spring, MD
Thursday, 11 June, 0900-1100	Language Training: A, B and G Group Perspectives—Speakers to be announced later
1300-1500	Language Training: The Service Cryptologic Element Perspectives—Speakers to be announced later
Friday, 12 June, 0900-1000	National Cryptologic School Language Training—Speakers to be announced later
1000-1100	Language Training Evaluation—Speakers to be announced later

Why Do They Leave?

[redacted] E7

P.L. 86-36

In recent years the language career field has commanded a great deal of attention by Agency managers and planners; a great deal of folk wisdom has been generated to describe the various aspects of what is generally referred to as "the language problem." The folk wisdom holds that linguists are fleeing the language career field at alarming rates for employment in toher career fields within the Agency, and that this exodus occurs about the time the linguist reaches Grade 11 or 12, that is, the professional level.

A recent survey of 63 linguists who have abandoned their language careers for other jobs within the Agency has provided some useful information on their views of language work in the Agency, and also provides management with a more complete picture of the segment of the linguist population that is being lost.

The survey findings, augmented by work force data supplied by M331, show that the exodus from the language career field may be more imaginary than real when compared to other career fields, but nevertheless they do cast new light on the problem from two standpoints—the seriousness of the loss and the reasons for the loss.

The seriousness of the loss, of course, lies in the fact that the vast majority of the linguists who do leave are the experienced ones, the cadre, so to speak. They are not easily replaced, and the loss of their expertise is felt in at least two vital areas: the quality of the product issued, and guidance to junior linguists. The survey found that the linguist departing the field has an average grade of GG10.4, with five or more years experience, and that a full 48 percent has achieved the professional level, that is, has passed the Professional Qualification Examination, in one or more languages.

Nearly one-half of the linguists leaving the career field identified the lack of upward mobility within the field as the primary reason for leaving. Even where this is not the primary reason, it is the secondary reason for another 19 percent. This would indicate that job dissatisfaction is not a major factor in their decision. This view is reinforced by the statistic that

41 percent of the linguists responding to the survey stated that they would be willing to return to language work if the career advancement opportunities were improved, while another 11 percent were undecided. It is conceivable that if the conditions the linguists viewed as unsatisfactory were improved, fully one-half of those currently departing the field would remain as productive, experienced workers. This view is further borne out by the responses of the linguists when asked how much longer they would have remained in the field if the conditions they viewed as untenable had been different. Thirty-eight percent said they would have stayed two or more years (the longest option offered on the survey form. Only 13 percent reported that they would have left about the same time regardless of conditions. Another 40 percent were undecided. This should be contrasted to the number of linguists who said that, under current conditions within the language field, they felt that they had made a wise choice in leaving. Four-fifths of those responding said they felt they had made a wise choice, and only one linguist felt that the decision was unwise. The remaining respondents were ambivalent.

(U) The folk wisdom view that attrition among linguists is greater at Grades 11 and 12 is substantiated by the survey, which goes on to indicate that the problem begins even earlier than Grade 11. It appears from the data gathered through the questionnaire that the problem begins in earnest around Grade 9 and remains constant throughout Grades 9, 11, 12 and 13. The linguists in these grades noted "lack of advancement," "no promotions," and "dead-end field" as primary reasons for their leaving. Linguists in the lower grades were more apt to mention working conditions, job dissatisfaction, academic or professionalization problems, and lessening enthusiasm for language work as primary reasons for leaving. Nevertheless, lack of promotions remains a concern even for linguists at Grade 7.

(U) If any picture emerges from the foregoing, it is one of frustrated employees. On one hand, the linguists enjoy the work and would like to continue in the field as a career. On the other hand, just when the linguists have been in the field long enough to have had the training and gain the experience that enables them to do the work in a professional mannaer and to pass their knowledge on to newer linguists, they feel pressures forcing them out of the field if they are to continue to move upward in the organization. Whether the pressures are real or imaginary, and whether the linguists' positions in the organization are improved or not by their actions (nearly 80 percent feel their position *is* improved), the result is the same: the linguists' expertise is lost to the Agency. And this loss is a costly one. Years of training time and thousands of training dollars have been wasted, and the replacement linguists will require the same investment of time and money.

(U) The "language problem" is less a language problem than it is a management problem. Until a language career field is developed that offers, or appears to offer, equal advantages with the other career fields, the Agency will have to suffer the loss of experienced linguists and recruit and train replacements for those who seek greener pastures elsewhere. The management question, which begs for an answer is

Which is more costly: paying the experienced linguist to perform, or continually training newer—and less experienced—linguists to replace them when they look ahead and see no future in their career field?

The latter option is an illusory one. The recently trained linguist is a replacement only in quantitative terms. The loss of an experienced linguist represents a geometric loss, not an arithmetic one. Linguists are not interchangeable. Experience is a vital attribute that should not be treated capriciously.

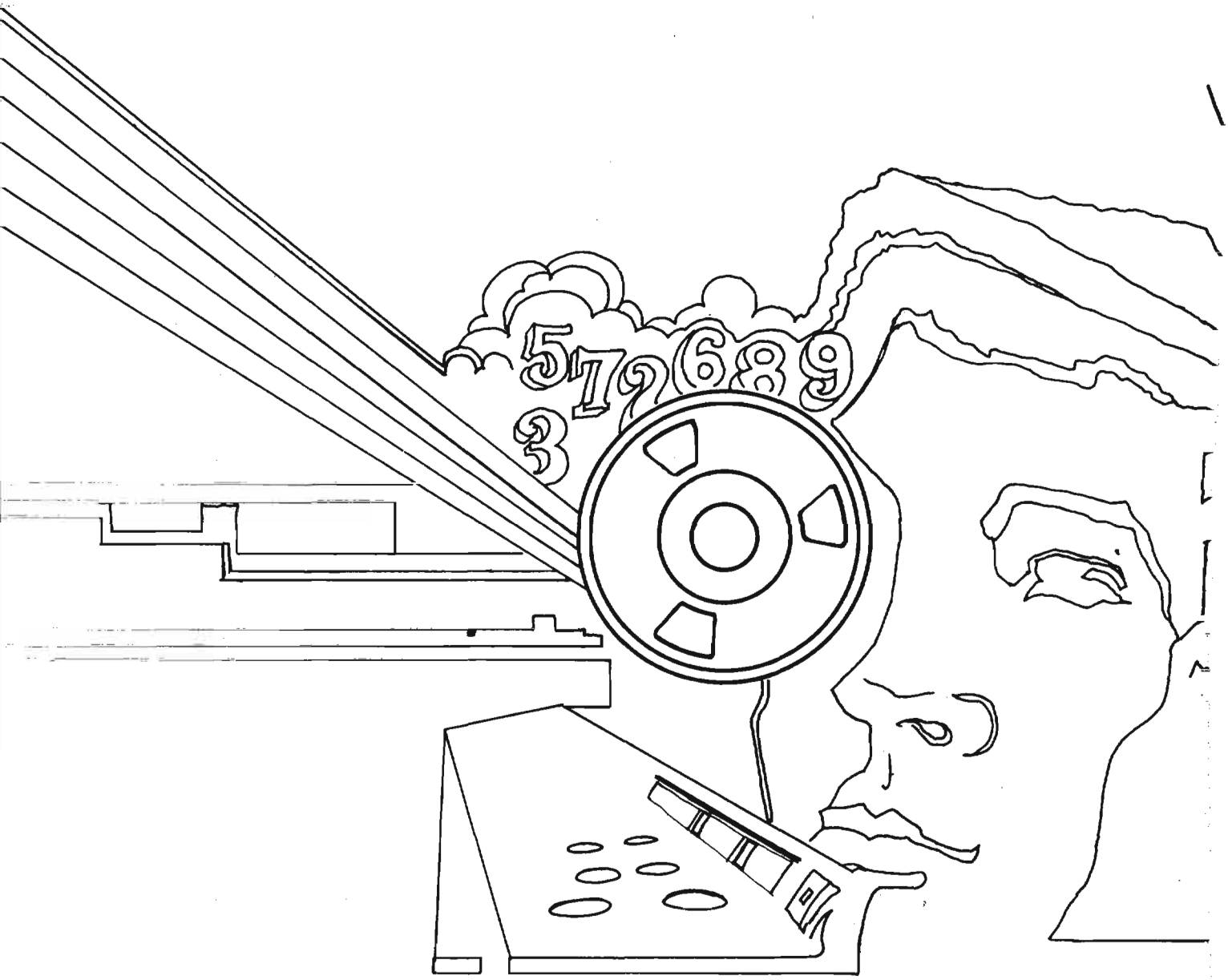
~~(S-CCO)~~

KITTIWAKE

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

****

(Continued from Page 9)


5726893

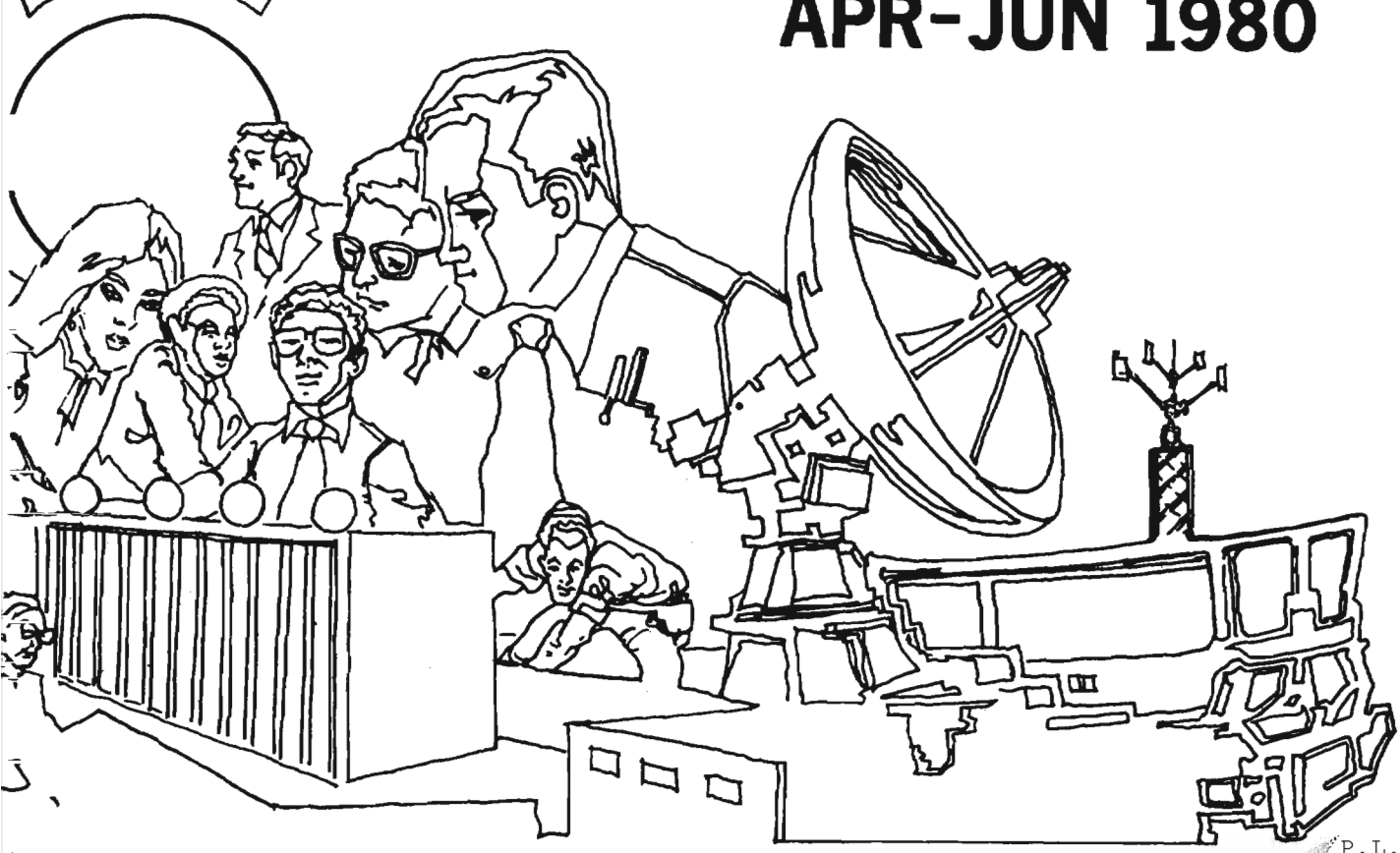
DOCID: 4019683

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

APR-JUN 1980



P.L. 86-36

DATA FLOW - CHALLENGE OF THE 1980s (U).....Cecil J. Phillips.....1
A TRAFFIC ANALYST LOOKS AT COMPUTERS (U)....[redacted].....5
P16 LANGUAGE AND CRYPTOLOGIC LIBRARY (U)....[redacted].....6
...AND IN A MORE MODERN VEIN...(U).....[redacted].....7
OH, K! (U).....[redacted].....9
NSA-CROSTIC NO. 31 (U).....D. H. W.....10
LIME-A, OHIO; LEEM-A, PERU (U).....A. J. Salemme.....12
AIT (U).....[redacted].....13
SOVIET C^3 (U).....[redacted].....16
WHAT TO DO ABOUT "FANX" (U).....[redacted].....19
HELP WANTED (U).....Tom Engle.....20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 1 JUN 2010~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019683

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. VII, No. 4 - 6 APRIL - JUNE 1980

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor-in-Chief.....David H. Williams (1103s)

Collection..... [redacted] (8555s)

Cryptanalysis..... [redacted] (4902s)

Cryptolinguistics..... [redacted] (5981s)

Information Science..... [redacted] (3034s)

Language..... [redacted] (8161s)

Machine Support..... [redacted] (5084s)

Mathematics..... [redacted] (8518s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Taurone (3573s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4019683

CECIL J. PHILLIPS, T4

An address given earlier this year by Mr. Phillips before the Computer and Information Science Institute

DATA FLOW — Challenge of the 1980s (U)

When I was asked if I would give a talk at CISI and I agreed, I knew what I wanted to talk about, but I was not sure what kind of title I wanted to give it. I settled on the Data Flow title, although a more proper title might have been "Data Flow, Feedback, Control and Inter-Process Dynamics"—all of which are involved in what I consider to be our main EDP challenge for the 1980s.

(U) Perhaps I should also state at the outset that the challenge is to everyone in the SIGINT process, not just people in the EDP field. As we keep saying in our budget justification, computers are integral to virtually every step in the SIGINT process, either by performing a function, by delivering the data to a human to perform a function, or by taking the results to the next process.

(U) Let me talk for a minute about data flow's role in the whole picture, which, as far as I'm concerned, is central to the whole process. Without data flow there is no need for feedback and control and there is nothing one could call inter-process dynamics.

(U) I think people have always understood that knowledge of data flow is useful to understanding processes whether they be human or machine. When I first made contact with Automatic Data Processing about 35 years ago, one of the basic elements of planning ADP jobs was to produce a flow chart. Flow charts usually showed the movement of material, which in our business has always been data—whatever its form. In those days flow charts (with which I never felt totally at home) usually showed functions such as edit, punch, sort, list, make corrections, etc.

(U) These functions were either manual, as in the case of "edit," or manually initiated as in the case of "sort," "list" and others. The key thing about this is that virtually all the inter-function actions were by humans responding to written or verbal instructions. These human interfaces represented both good news and bad news. The good news was that function-to-function interface was easy to take care of, but the bad news was that it worked only as well as the humans understood and cared about what they were doing.

(U) With the introduction of the stored program computer, flow charts to show data and control flow became basic tools for planning how to write computer programs, usually showing functions at a much more detailed level than the case I described before. Stored programs permitted data to be passed from one process to another without human interface, but the size of computers and the complexity of programming meant that the data went external to the system time and time again. Thus, the human interfaces I mentioned were still very much in evidence. However, there was automatic feedback within programs. After all, one of the main attributes of a computer was its ability to modify the stored program, or modify the data, but almost any inter-program feedback was handled by humans.

(U) Today, there are still hundreds of processes in which inter-process communication is via human beings. That would not be so bad if I were talking about humans linking processes through interaction at a CRT. But I am not! I mean that there are still hundreds of processes where the result goes external to something like a print and any result going to a next process gets entered by hand. Sometimes this is via punched cards, and there are still a few examples using paper tape to re-enter data.

(U) Another of the problems in the way we treat data flow today lies in the fact that too many processes are still batch processes. These are probably satisfactory for treating single-direction flows of data, but are not very compatible with feedback and control—especially if we expect feedback and control to have any effect while actions are still taking place. I believe there are much better ways of treating data than these current batch flows and these new methods are also part of the challenge for the 1980s. I will get back to this later.

(U) All of this reference to past and present data flow and flow charting brings me around to what I consider the challenge of the 80s—namely, how to make a substantial leap forward in the way the flow of data is understood and treated and to use this knowledge to improve the whole SIGINT process.

(U) Why is there a challenge?

(U) I believe there is a new kind of challenge here because I believe that for the first time all the capabilities necessary to cause data to flow from collection to customer, with appropriate feedback of control information, are present. At the same time, there are capabilities which will enable analysts—separated by space—to work together as though they were sitting side-by-side. I realize that over the years there have been a number of major technological developments, each of which seems to be a breakthrough, but I believe that the 1980s can see us put it all together well for the first time so as to make a breakthrough in the only area which will have a long-lasting and far-reaching effect—namely, to begin to process and handle *information*, rather than data, throughout the SIGINT system.

~~(C-CCO)~~ Just for a moment, let's take a look at the key ingredients.

► Terminals/access devices. In the 1980s, for the first time we will have enough terminals so that virtually everyone in the SIGINT system will have some kind of access to one. By the end of the decade we ought to have a terminal or access device on every desk. The only weak spot may be in the area of full graphics, an area whose application to SIGINT is still to be developed (except for some highly specialized cases).

► Concentrators/Terminal Sub-Systems. We have these in great profusion. It is not that these perform a unique function; they are just convenient boxes between terminals and mainframes or networks, occasionally providing extra computer power or extra storage.

► Networks and Communications. These, along with the terminals, are the real breakthrough. For the first time we are beginning to have what is needed—communications to support interactive processes at any distance we want. [redacted] -and by the end of 1981 to most major points in the SIGINT systems, wherever they are.

► Main Computers. As you well know, there are plenty of these of almost every type.

(U) In short, we are soon to have the technical capability for every user/analyst at every terminal to talk to every other analyst and every other process via his keyboard.

(U) If all of this is true, what is the challenge?

(U) The challenge is to make it all do some useful work in the production of SIGINT. The challenge is to interface people with information, not just terminals with computers. This is where the payoff, the success and the rewards are. Since there are a lot of computers already doing many of these things, what makes the 1980s special?

(U) I believe there are at least three main areas of challenge in the 1980s.

► Causing the data to flow smoothly from collection to output reports.

► Treating the data in natural information units which foster the development of better analytic approaches and feedback and control.

► Developing techniques for *teleanalysis*, a term which I have cointed to describe methods by which two analysts may collaborate over a distance.

(U) Let's take a look at the flow problem first.

~~(C-CCO)~~ Causing SIGINT data to flow effectively and smoothly from collection to user output in natural information units with appropriate feedback and controls sounds like a goal that has been around for a long time, but I think that for the first time we can realize the full value of machine interaction and feedback which actually influence processes while they are still going on. At a kind of top level design, this probably sounds pretty straightforward. At that level it is. However, at the detail level, it means thousands of processes which have to be understood in terms of all the other processes to which they relate. These other processes may be adjacent, but things which affect them may be several levels away. [redacted] This means that there are so many interrelated effects that understanding them all is out of the question. And this is precisely where the greatest challenge comes—that is, finding a method for describing the interfaces and then exploiting it to connect them.

EO 1.4.(c)
P.L. 86-36

(U) I think it important to understand that what I am suggesting is not simple—because I am not just talking about standardization at low levels of protocol and format. Many of these are already covered in PLATFORM and some of the format conventions are covered in USSIDs. What I am really talking about is a set of information level protocols—things

DOCID: 4019683

which humans do now, in the best cases almost without thinking.

(U) Such an example might be where an analyst knows instantly where a mis-identified message must go to get it back on track. At the same time, most of our current processes simply dump data back into the system. The challenge, of course, is to develop automatic re-routing schemes or man-machine interactive processes which allow for re-entry and re-routing in such cases.

(U) I think this dictates the need for developing a convention for annotating and labeling the error transactions so they can be re-entered into the process to produce a new result which is a combination of the computer process and the man-machine interaction process. If the person annotating the transaction knows exactly where the erroneous data goes, the problem is relatively simple. If he simply knows that it is wrong and wants to send it back, the problem is much more complex. This is especially true of the problem of how to label it in order to get a different result the second time through the system.

(U) This might be fairly straightforward if all feedback is from a single class of process back to the collector. In real life this is not usually the case; rather, the feedback comes from all parts of the system. Thus, there is the need to be able to accommodate different levels and kinds of information.

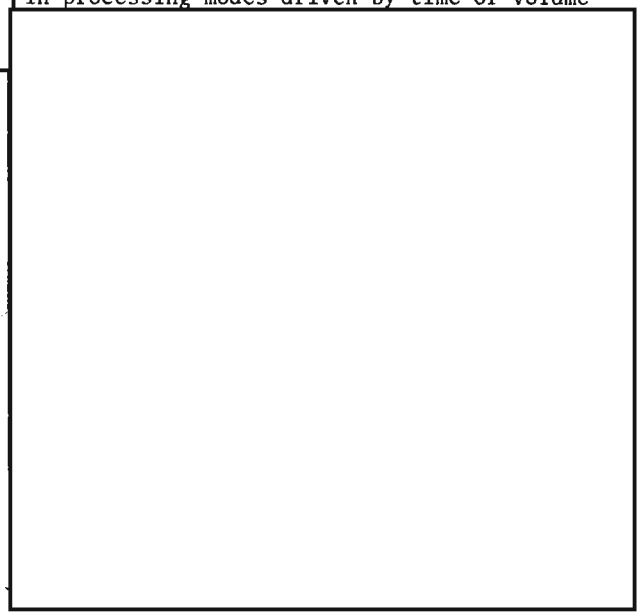
(U) Up to now, we have been doing all of the things I am discussing—particularly feedback—by human action, mostly on a hit-or-miss basis. There have been some near real time collection control groups, but their effectiveness has been limited by slow and erratic feedback to them from analysis, by slow and erratic methods for delivery of information back to the collectors, and often by slow and erratic reporting and communications with the collectors.

~~(C-CCO)~~ Let me make it clear that these groups have done a super job, often with very limited help from the computer types. So there is part of the challenge—to help refine the existing processes and extend control processes to all parts of the system to manage processing, analysis and reporting, as well as collection. It has been said that there are more signals in the air than we can collect, more signals collected than we can process, and more signals processed than we can transcribe or decrypt and then report on. The net effect is that we must be able to select and filter the flow at all points in that flow.

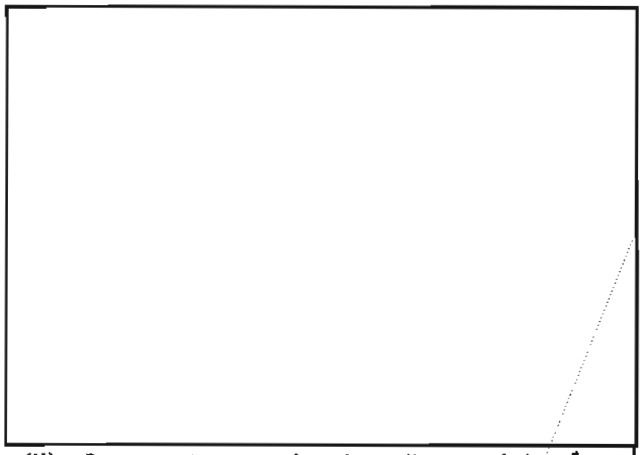
(U) Much of what I have said is fairly simple on a case-by-case basis. As I noted earlier, the complication comes in looking at the whole picture or a large fraction of it. There are also a few other complications in that broad interprocess communication is not the goal of everyone. Systems designers are likely to have a goal of optimization within their own domain which is usually sub-optimization as far as the overall SIGINT process is concerned. Further, every manufacturer and creator of new software packages is out there being as creative as possible to give his system some unique features. Users of the overall system are likely to have to keep running just to stay even with all the variations.

(U) The second part of the challenge had to do with treating data in more natural or "event-driven" units so that feedback and control have more meaning. An alternate way of thinking of this is to consider dealing with units of data.

~~(C-CCO)~~ Perhaps this is naturally inherent in a good system, but we have been so long in processing modes driven by time or volume



EO 1.4.(c)
P.L. 86-36



(U) Because transactional or "event-driven" processing has strong implications of more timely operations, it may seem that I am really discussing time-sensitive processing. Transactional processing does make these things possible but it does not demand it. You can save work queues in transactional systems as well as in batch, and in a transactional system you ought to be able to save them even more intelligently.

(U) A third and final part of the challenge of the 1980s, as I see it, is to develop techniques for *teleanalysis* or *telesynergism*—terms I made up hurriedly to describe joint analysis done by two or more people over distance. Let me explain what I believe should be possible here. I am talking about a form of teleconferencing in which man-machine interaction takes place with two or more people at separate terminals operating against the same data, where the data may be a message, entries in the data base or any other form.

(U) There is probably some tendency to equate this to teleconferencing, but it is a level above teleconferencing. It is teleconferencing in which the analytic problem is at least part of the medium.

(U) We are optimistic that the seeds of such ideas can begin to develop as soon as network connections are established with collaborating analytic centers. The goal is to see the multiple work forces at various centers integrated through this telesynergistic bond so we can use the work force better or tackle more complex problems.

(U) I have no doubt but what it will take a long time to really accomplish this on a broad scale. First, we have to hit people with two-by-fours to get them to treat problems interactively on computers where one person and one terminal is involved. But in time the software and the technology will improve and the problems to be solved will become bigger or harder, or both, so there will be an incentive to develop telesynergism.

(U) At the same time, programmers and systems developers also need to be touched by the two-by-four to remind them that their job must be to simplify the interface to the system so it can be more readily used. The challenge to all of you is to help develop the system tools and to help explore the ideas with the analysts who are bold enough to consider them.

(U) I think it was Mark Twain who said that there is no death like being talked to death, so let me conclude with a brief summation.

(U) My key point about the challenge is that EDP people and communications people must understand the whole system, that is, all the parts, and all the processes and how they interact with each other—whether man or machine. Another name for this is total data flow—from start to finish—including feedback.

(U) Given some understanding of the system —the depth of understanding will naturally vary with one's role—I see the challenge as one of developing full information interfaces between the parts of the system, not just signal and processor interfaces. To me, this implies overall design and and overall approach—real, top-down design from the *very* top, not from some local peak.

(U) In a larger sense, it is the challenge to everyone in SIGINT to make the data flow from process to process and to make the feedback data and contraol data flow where they are needed. In short, this means to make every last piece of the SIGINT system fully interoperable with all the rest.

(U) I think that this is a challenge which can pretty well occupy everyone during the 80s.

* * * * * * * * * * * * * * * * *

(UNCLASSIFIED)

SOLUTION TO NSA-CROSTIC No. 30.

From a Letter to the Editor on COPES, by Donald Y. Barrer, P1, CRYPTOLOG, September 1978.

"My concern stems from admissions made privately and off the record that when COPES objectives satisfaction is low we [alter] the objectives so that the rate of satisfaction looks better, and when things look too good we add objectives to preclude a cut in resources. This should not be surprising; it is a natural response."

(UNCLASSIFIED)

* * * * * * * * * * * * *

EO 1.4.(c)
P.L. 86-36

DOCID: 4019683

A TRAFFIC ANALYST LOOKS AT COMPUTERS

[redacted] P14 P.L. 86-36

In the world of computers, I am an amateur. I have used them as tools in various analytic jobs for many years, but always with someone else acting as intermediary, either a programmer or a systems analyst. I went through most of the same frustrations and associated withdrawal symptoms that other analytic people did when our "traffic" was taken out of our hands and file cabinets and put into the bowels of the basement somewhere out of sight and out of reach except through the offices of these intermediaries.

I frankly think that, contrary to popular opinion, we analysts were not all afraid of computers. Maybe some were, but not all. But what we all did share was the realization that our processing cycle was no longer solely under our control. Our data was in a loop that went through someone else's area of control: while it was in the computer, we had no control over it. Someone had control, of course, but that someone was never us. The people running the system did not work for the analytic people. This is not to say that they did a bad job or that they did not try to support us in the best way they knew. But prior to computers, when traffic came into my shop, it was "my traffic" and I kept it under my control for as long as I had need of it. The people who handled it for me worked for me (and were rated by me). If that sounds proprietary, it is because it was a proprietary kind of system. Today, however, there is very little of the proprietary feeling among analytic people. It isn't really "my traffic" any more.

All this is not meant as a harangue about computers, but is put forward to show where I'm coming from, so you can put the remainder of these remarks in context.

While I have not yet relinquished my sheltered role with respect to computers, I have been spending some time at the keyboards of several CRT terminals. For the most part, I have been trying to do (or simulate) an analytic task, usually some aspect of traffic analysis. Since any traffic analyst these days must work within the framework of computers (all of his data is inside them somewhere), I was motivated to see just what "doing TA on a terminal" really amounted to. This represents a first report of that venture, with all of the biases that first reports commonly have. I am not finished looking, but I thought I would put down three early impressions based on my own hours at the keyboards.

► As I look over my early notes to myself, I am impressed about how often I had typed in a TAPQE problem involving several days traffic, all in upper case (just like an old-fashioned Morse problem for those of you who remember), and since all the commands I was using were in lower case, I kept finding bits of lower case data in the traffic. Later, as I became more familiar with the problem (I think I could have recited each page of the traffic by the time I was through), I began to notice that pieces and lines were missing. I really don't know why the erasures and writeovers happened in each instance, but often I noticed that the cursor on the screen ran a bit behind me when I was entering data; I might stop and glance at the cursor position and not realize that the cursor was running behind. There may well have been other basic reasons for the losses and accidental writeovers, but the experience left me very wary about typing data in at anything near my normal typing speed—which is not terribly high. I also spent some time trying to think out defensive strategies for avoiding the loss of data, such as always working on a copy of a file rather than the file itself, making a habit of storing off the working file fairly often, as frequently as every few lines on material I was anxious to protect. The problem needs more attention, both by computer people and by system designers, since we already lose too much data around here by more classical methods, and really don't need new and inventive ways to lose still more; I don't have any solutions to offer, only a warning that the ease with which data can be altered or erased is scary and will not go away just because we don't want to talk about it. At least part of the problem lies in perceiving that it has happened at all; most of my errors were not noticed until

some later time.

► The next problem I had is a personal one. I wear glasses—bifocals. In order to read the screen I have to bend my head back so that I can see through the bottom part of the lens, where its reading prescription is. A whole day of that is a little more than I want to think about. When my neck gets sore, I have to stop. My choice, I suppose, is to buy another set of glasses, just for reading CRT screens. Or maybe the government will buy them...

► I have heard people say that when we get CRTs on everybody's desk, we can go to a paperless system. Don't you believe it. Have you ever seen a computer printout? Those folks use up more paper than we ever did, with yards of stuff preceding the actual print. Nevertheless, the point I want to make is that I found the screen too small to do anything like a diagram or a tabular lising of continuities. Having experimented with both the PQE problem, which was a simple continuity problem (similar to the final problem in TA-100), and with several CRYPTOLOG problems, I found that I could not keep track of recoveries in any orderly way when all I had to work with was the screen, even one like MYCROFT/CARONA which can be moved around and divided into parts. But all that changed when I decided to try to work with a combination of printout and screen. I used the printout as a basic worksheet, making notations on it from time to time, then adding them to the screen and generating another printout. This will work if the printer is fairly close (I don't consider the basement close to the second floor), and not so busy that one has to wait more than a few minutes for the output.

* * * * * * * *

Because of my interest in "doing" problems on or through the computer, I have been interested in encouraging others to try it also. If you have access to a terminal and would like to try it, let me know. Send me a note (to wes at carona, if you can access PLATFORM), or call me on 3360s.

As analytic people gain more experience in this area, we should find ways to plow that experience back into better support and better systems. With this in mind, we in P14 have set up a file called "whydontwe" where we record various bits and pieces of reactions to the terminal, system, network, or whatever. Not all of it is literate, and some of it looks sort of dumb when re-read at some later date. But it is what we thought or felt at the time, and some of my earlier items formed the basis for some of the above. I would encourage you to do the same. If you want to see what dumb things we said, why don't you have a look (if you're a CARONA user) at the file /u3/pin/why/whydontwe. If you have an idea but don't know who to give it to, send it to me. If there's enough interest in this sort of thing, maybe the editor would be agreeable to a regular feature (assuming, of course, that they're printable).

From the Editor: CRYPTOLOG will be happy to publish any printable responses to Wayne's solicitation (and to chuckle privately over any which are not.)

P16 Language and Cryptologic Library

[redacted] T12, Librarian of the P16 Language and Cryptologic Library, wishes to advise readers of the excellent collection of older works on cryptology available there, some of which date back several centuries. Unfortunately, items in this collection are not available to be taken out, but must be read on the library premises, which are at FANX, Room B3526. For further information, [redacted] may be called on 8873s. P.L. 86-36

A partial listing of volumes in this collection is given below.

Bazeries, Etienne. *Les Chiffres Secrets Devoiles.* Paris: Librarie Charpentier et Fasquelle. 1901.

Booth, Williams Stone. *Some Acrostic Signatures of Francis Bacon.* Boston: Houghton Mifflin Company. 1909.

Breithaupt, Christian. *The Art of Deciphering of the Science of Solving and Reading Secret Writings. Together With a Historical Account of Various Methods of Secret Writing in Use Amongst the Ancients and in More Recent Times.* Helmstedt (Germany). 1737.

Breithaupt, Christian. *A Historical, Critical, and Detailed Disquisition Concerning the Various Types of Secret Writing Employed by the Ancients as well as by Those of More Recent Vintage, Together with an Account of the Art of Deciphering.* Printed at Helmstedt (Germany). 1727.

(UNCLASSIFIED)

Cardan, Jerome Girolamo. *21 Books of Jerome Cardan, a Doctor of Milan, on Subtilitas.* Printed at Basle. 1554.

Champollion, Jean. *Grammaire Egyptienne.* Paris: Typographie de Firmin Didot Frères. 1836.

Donnelly, Ignatius. *The Great Cryptogram: Francis Bacon's Cipher in the SoCalled Shakespeare Plays.* Chicago: R. S. Peale and Co. 1888.

Dröscher, Ernst. *Die Methoden der Geheimschriften.* Leipzig: K. F. Koehler. 1921.

Figl, Andreas. *Systeme des Chiffrierens.* Graz: Verlag von Ulr. Mosers Buchhandlung. 1926.

Fiske, Gertrude Horsford. *Studies in the Bi-Literal Cipher of Francis Bacon.* Boston: John W. Luce and Son. 1913.

Frederici, Johannes Balthasar. *Cryptographia or the Art of Secret Writing.* Hamburg. 1684.

Gallup, Elizabeth Wells. *The Bi-Literal Cypher of Sir Francis Bacon.* Third edition. Detroit: Howard Publishing Company. 1901.

Greely, A. W. *War Department Telegraph Code.* Washington: Government Printing Office. 1906.

Gross, Hans. *Handbuch für Untersuchungsrichter als System der Kriminalistik.* Part II, sixth revised edition. Munich, Berlin and Leipzig: J. Schweitzer Verlag (Arthur Sellier). 1914.

Harvey, Henry. *Harvey's Vanguard Code.* New York: Code Press of Henry Harvey. 1892.

Jacobus de Silvestris of Florence. *Rules of Secret Writing.* Rome. 1526.

Klüber, Johann Ludwig. *Cryptographik, a Manual of the Art of Secret Writing.* Tubingen. 1895.

Lacroix, Paul. *La Cryptographie.* Paris: Adolphe Delahays Libraire-Éditeur. 1858.

Lange, André and Soudart, E. A. *Traité de Cryptographie.* Paris: Libraire Félix Alcan. 1925.

Locard, Edmond. *Traité de Criminalistique.* 2 volumes. Lyon: Joannes Desvigne et Cie. 1935.

Loria, Gino. *Le Scienze Esatte Dell'Antica Grecia.* Modena: Antica Tipografia Soliani. 1893.

Meng, John J. *Despatches and Instructions of Conrad Alexandre Gerard, 1778-1780.* Baltimore: The Johns Hopkins Press. 1939.

Meyer, H. R. *The Commercial Telegraph Code, to Meet the Requirements of the London Telegraph Congress of 1879.* New York: American Code Co. 1880.

Plum, William R. *The Military Telegraph During the Civil War in the United States.* 2 volumes. Chicago: Jansen, McClurg and Company. 1882.

Porta, Giambattista. *Twenty Books of Natural Science.* Leiden. 1644.

Romanini, Vesin. *La Cryptographie Dévoilée.* Paris: Typographie Hennuver. 1857. Author also listed as Vesin, C.F.

Sandler, Rickard. *Chiffer.* Stockholm: Wahlstrom and Widstrand. 1943.

Scotus, Johan Maria. *Four Books of Secret Writing.* Naples. 1563.

Sympson, S. *A New Book of Cyphers.* London: John Bowles. 1750.

U. S. Bureau of Navigation (Navy Department). *The International Code of Signals for the Use of All Nations.* Washington: Government Printing Office. 1875. Also available in revised edition, 1894.

U. S. Department of State. *The Cipher of the Department of State.* Washington: Government Printing Office. 1876.

Valerio, P. *De La Cryptographie.* Paris: Librairie Militaire De L. Baudoin. 1893.

Velasquez, Manuel M. *Codigo Universal de Correspondencia Secreta.* Mexico. 1926.

(UNCLASSIFIED)

...and in a more modern vein... (U)

(U) [redacted] Chairman of the Bookbreakers' Forum, suggests the following publications as essential reference works for those in the field of cryptolinguistics. If you are interested in obtaining any of these documents, call [redacted] on 1103s. All are classified TSC. P.L. 86-36

Buck, Stuart H., [redacted] (U) *CRYPTOLOG*, July 1977.

~~(TSC)~~ [redacted] EO 1.4.(c) P.L. 86-36

[redacted] *Italian Bookbreaking* ~~(TSC)~~. National Security Agency Technical LIterature Series, Monograph No. 6, 1965. P.L. 86-36

~~(TSC)~~ The original paper was written in 1943 while bookbreaking was still being done on the Italian Military and Air Force codes. Soon after, the Italians surrendered themselves and their codebooks. The bookbreakers then had an opportunity to compare their results with the original of PEGASO, the Italian title for their latest Air Force code. A very interesting account of a specific effort which can also serve as a primer on bookbreaking.

Swift, Katharine L., "Some Problems and Techniques in Bookbreaking" (U). *NSA Technical Journal*, Vol. XI, No. 1, Winter 1966.

(U) A concise view of what codes and bookbreaking are all about, and some interesting war stories. Just the thing to start out on.

Swift, Katharine L., *Standards and Techniques of Code Reconstruction* (U). National Security Agency Technical Literature Series, Monograph No. 5, 1965.

~~(S-CCO)~~ Reprint of a 1955 paper (S51,126). Designed for code problems of the 1950s which were [redacted] codes of classic configuaration. Rich in illustrative anecdotes and strong on first principles. Written when card sorters were obsolete but computers were still in their infancy. A must.

EO 1.4.(c)
P.L. 86-36

Swift, Katharine L. and Oliver, Jean. *Collected Articles on Code Reconstruction* (U). Cryptanalysis Department, National Cryptologic School (S-212,802). Revised Edition, 1976.

P.L. 86-36

~~(C-CCO)~~ A collection of shorter articles on assorted topics of relevance to bookbreaking. It can be thought of as a supplement to *Standards and Techniques*, above, which serves to increase its scope.

From the Editor: You should add to the preceding list the following bookbreakers' "must" which has just been published.

[redacted] *The Structure of Codes, Part I: Classic Codes* (U). P16 Cryptolinguistic Series No. 1, 1980 (S-221,647).

~~(C-CCO)~~ An annotated survey of various codes, both U. S. and foreign, used during the first half of this century. This work also includes a comprehensive bibliography of in-house and open source publications on bookbreaking.

(UNCLASSIFIED)

GEOGRAPHIC TRIVIA

- Each of the United States has a highest and a lowest point. Most everyone knows that the highest high point is in Alaska (Mount McKinley, 20,320 feet), while the lowest low is in California (Death Valley, —282 feet). But do you know which state has the *lowest* high, and which has the *highest* low?

- Many of the largest cities in the U.S. are *not* state capitals. In fact, the state capital with the largest population, according to 1975 Census Bureau estimates, is the *eleventh*-ranking U.S. city. What is it? And what are the place and show capitals? (Old-time trivia players, to whom Boston has always been the most populous capital, will be dismayed to find out that its 1975 population of 636,725, is fourth largest.)

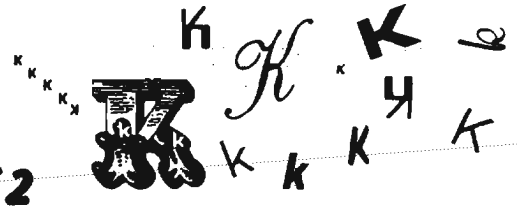
Answers on Page 15

(UNCLASSIFIED)

DOCID: 4019683

OH, K!

T152



P.L. 86-36

In a jargon-rich environment like NSA, we are used to the acronyms and abbreviations that enable us to express complicated thoughts in a reasonable amount of space, either physical or temporal. It is inevitable that some abbreviations will have multiple meanings. For the multi-equivalent championship, though, I think we should nominate the steadfast multiplier K. One can envision a question on a future version of the Computer Systems PQE:

Question: K = ?

a. 1000
b. 1024
c. 512
d. 4096
e. DDT

Correct Answer: a, b, c, e, and probably d

a. The classic abbreviation derived from the Greek prefix *kilo-*. Often written in lower case. You can be sure 1000 is meant when the quantity measured is dollars or a standard physical unit, e.g., kHz.

b. A frequent unit of computer memory (whose lengths are almost always powers of two), as in 64K words, meaning 65536. 65K is also used and has the advantage of corresponding to the common use, as in a. above. But the use of K = 1024 is becoming more common because of its precision (64K, K = 1000 is an approximation while 64K, K = 1024 is exact) and the ease of computing the size of memory as it doubles (2*64K = 128K, while 2*65K = 131K).

c. The somewhat self-contradictory "K octal," i.e., 1000_8. A unit often used by those reading displays or dumps.

d. 1000_{16}. I have never actually heard this one used (I don't mix much with users of hexadecimal), but I suspect it's out there. I guess we should be grateful that at least we're not using a number system with a large enough base that K might also be a digit (in which case it would have value 20).

e. See a recent Agency organziational chart.

So, the next time you hear a "K", make sure you get onto the speaker's base!

O.K?

OH, K! (PART II)

Where did everybody go?

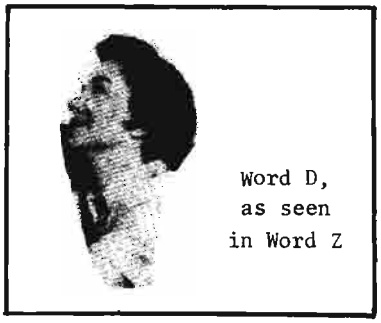
As a result of the recent reorganization which did away with the K organization and sent its people off to various other elements, CRYPTOLOG has been receiving a number of returned subscription copies which had been distributed to K addresses.

So if you used to be in K, and would like to continue to receive CRYPTOLOG, please call (on 1103s) or drop a note (P1, CRYPTOLOG) to let us know your new address.

DOCID: 4019683

NSA-Crostic No. 31

by dhw



Word D, as seen in Word Z

A. "_____ and speak each other in passing." "Tales of a Wayside Inn," Longfellow. (6 wds)

84 68 166 255 206 23 179 270 222 103 195 19 273 76 57 148 110 177 123 133 47 263 7

B. Prudent-sounding state capital

30 39 63 174 143 238 279 159 59 9

C. Of maximum fusibility

230 3 244 18 101 207 257 139

D. Hollywood leading lady (1924—), active 1950—1959, in such films as *Crash Landing*, *Donovan's Brain*, etc. (Full name)

240 147 12 186 272 226 252 276 210 32 10 40 168 219 108 64

E. Harmonious-sounding state capital (3 wds)

176 124 201 278 53 271 13 259 145 202 104 100 107 27 241 161 185 169 88

F. Mechanism of a firearm that expels the spent cartridge

211 87 105 109 167 34 146

G. Cereal grain

138 197 203

H. Rigorous; unadorned; grave

60 85 233 116 131 220 162

I. Romantic-sounding town in Florida, seat of Osceola County

96 180 190 72 243 163 130 113 221

J. Full of plots; treacherous

175 80 115 62 196 149 117 208 181

K. Sibling's daughter

141 158 199 89 194

L. Fate, at a turn of the card (4 wds)

5 28 52 120 73 234 128 25 43 144 173 213 231

M. Secessionist province of N Ethiopia

157 275 260 256 251 78 232

N. Women as mates, says Thurber, should be those "who have great constitutional strength and are not _____."

24 65 127 223 160 183 29 36

O. Timid; full of fears

8 277 54 51 97 91 242 135

P. Learned

95 106 155 212 266 69 264

Q. Building for the storage and maintenance of locomotives

132 235 56 214 182 82 140 38 229 248

R. Knotted

178 164 218 215

S. Toast _____ (3 wds)

258 249 90 21 200 269 137 125 151

T. In pointing out why a fifth of Scotch on the bar was preferable to major brain surgery, he explained, "I'd rather have a _____." (9 wds)

86 254 67 93 205 6 102 126 75 4 250 261 50

224 152 265 83 262 70 225 112 119 136 44 79

237 17 191 247 165 31 198 150 134 37 55 98

U. The property of being not separable into parts

268 41 253 58 184 71 142 14 246 216 204 48

20 1

V. The original large-scale-robbery-caper movie (1955)

193 228 35 111 92 114

W. In Germany, units of local government

122 154 121 45 129 26

X. Hairy; rough with bristles

94 11 217 156 239 81 187

Y. Sour

16 77 66 209

Z. The only film in which Word D co-starred opposite her husband (1959) (4 wds)

188 33 192 267 15 22 61 171 2 74 42 99

274 49 245 227 170

Z_1. Capital city of New Caledonia

46 153 236 118 172 189

■	■	1 U	2 Z	3 C	4 T	■	5 L	6 T	7 A	8 O	9 B	10 D	■	11 X	12 D	13 E	14 U	15 Z	16 Y
17 T	18 C	19 A	■	20 U	21 S	22 Z	23 A	■	24 N	25 L	26 W	■	27 E	28 L	29 N	30 B	31 T	32 D	33 Z
■	34 F	35 V	■	36 N	37 T	38 Q	39 B	■	40 D	41 U	42 Z	43 L	44 T	45 W	46 Z_1	47 A	■	48 U	49 Z
50 T	51 O	■	52 L	53 E	54 O	55 T	56 Q	57 A	58 U	59 B	60 H	61 Z	62 J	63 B	64 D	■	65 N	66 Y	67 T
68 A	■	69 P	70 T	71 U	72 I	■	73 L	74 Z	75 T	76 A	77 Y	78 M	■	79 T	80 J	■	81 X	82 Q	83 T
■	84 A	85 H	86 T	87 F	88 E	89 K	90 S	■	91 O	92 V	■	93 T	94 X	95 P	■	96 I	97 O	98 T	99 Z
100 E	■	101 C	102 T	103 A	104 E	105 F	106 P	■	107 E	108 D	109 F	110 A	111 V	112 T	113 I	■	114 V	115 J	■
116 H	117 J	■	118Z_1	119 T	120 L	121 W	■	122 W	123 A	124 E	125 S	126 T	■	127 N	128 L	129 W	■	130 I	131 H
132 Q	133 A	134 T	135 O	■	136 T	137 S	138 G	■	139 C	140 Q	141 K	142 U	143 B	144 L	145 E	146 F	147 D	148 A	149 J
150 T	151 S	■	152 T	153Z_1	154 W	■	155 P	156 X	157 M	■	158 K	159 B	■	160 N	161 E	162 H	■	163 I	164 R
165 T	166 A	167 F	168 D	169 E	170 Z	■	171 Z	172Z_1	173 L	174 B	175 J	176 E	177 A	■	178 R	179 A	180 I	181 J	■
182 Q	183 N	184 U	185 E	186 D	187 X	■	188 Z	189Z_1	190 I	■	191 T	192 Z	193 V	194 K	195 A	196 J	197 G	■	198 T
199 K	200 S	201 E	■	202 E	203 G	204 U	205 T	■	206 A	207 C	208 J	209 Y	210 D	211 F	212 P	■	213 L	214 Q	215 R
■	216 U	■	217 X	218 R	219 D	220 H	221 I	222 A	■	223 N	224 T	■	225 T	226 D	227 Z	228 V	229 Q	230 C	■
231 L	232 M	233 H	■	234 L	235 Q	236Z_1	237 T	238 B	■	239 X	240 D	241 E	242 O	243 I	244 C	245 Z	246 U	247 T	248 Q
■	249 S	250 T	251 M	■	252 D	253 U	254 T	255 A	256 M	257 C	258 S	259 E	■	260 M	261 T	■	262 T	263 A	264 P
■	265 T	266 P	267 Z	268 U	269 S	270 A	271 E	272 D	■	273 A	274 Z	275 M	276 D	277 O	278 E	279 B	dhw	■	■

LIME-A, OHIO; LEEM-A, PERU

For many years, befofe there were Russian-language reference aids, the final authority on the pronunciation, usage, and meaning of any Russian word was the late Juliana M. She told you how every Russian word was *supposed* to be pronounced, how it was *supposed* to be used, and what it was *supposed* to mean. If anyone dared to say, "but they pronounce it..." or "they use it to mean...," she would angrily say, "They! the Soviets! they have bastardized the language! those peasants aren't speaking Russian! they're speaking Soviet jargon!" But what could you do, if there was only one oracle in town? You'd have to consult it! So people would find themselves asking MIss M. to render solomonic decisions, asking questions like "How do the Russians—not the Soviets—pronounce it" Is it Semipalatínsk? Or is it Semipalátinsk? Miss M. would answer, "Well, the name of the city comes from the Russian word *palâta*, meaning 'tent.' The name of the city means 'city of seven tents.' Hence the correct pronunciation is Semipalátinsk." (Smirk on face of disputant A—"I told you so!"; scowl on face of disputant B—"I know I've heard Russians—not Soviets!—say Semipalatínsk!") "However," Miss M. continues, "I used to know a man who came from Semipalátinsk, and *he* used to pronounce it Semipalatínsk."

The same kind of fight used to rage around the name Murmansk. Everyone in the United States knew the name at the beginning of World War II, because it was the northern port with the icefree harbor, where, before America was officially in the war, American convoys of merchant ships delivered all those lend-lease shipments that Soviet historians don't seem to recall that the Soviet Union ever got. And everyone used to pronounce it Murmánsk. So imagine the linguists' surprise to hear that "the correct pronunciation of Murmánsk is Múrmansk."

But doubt persists between the Murmánsk and Múrmansk factions. Finally the bastardizers of the pure Russian language publish a dictionary of pronunciations of personal and place names, worldwide, for the use of Russian radio and television announcers, movie directors, and the like. Naturally the Murmánskers and the Múrmanskers race one another to the M pages. There it is, sure enough—"Múrmansk." But then, in a more leisurely moment, reading for fun the introductory remarks on "How to use the dictionary," one of the disputants reads that "the pronunciations given in this book are the standard ones for use on nationwide radio and television. No indication is given of certain nonstandard or local pronunciations, for example, the local mispronunciation of Murmánsk instead of Múrmansk." That's the problem! People don't even know how to pronounce the name of their own hometown!

— From "Twelve Language Anecdotes in Search of an Author," by Arthur J. Salemme, retired

DOCID: 4019683

P.L. 86-36

AIT (U) [redacted] R94

This article is classified ~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS~~ in entirety.

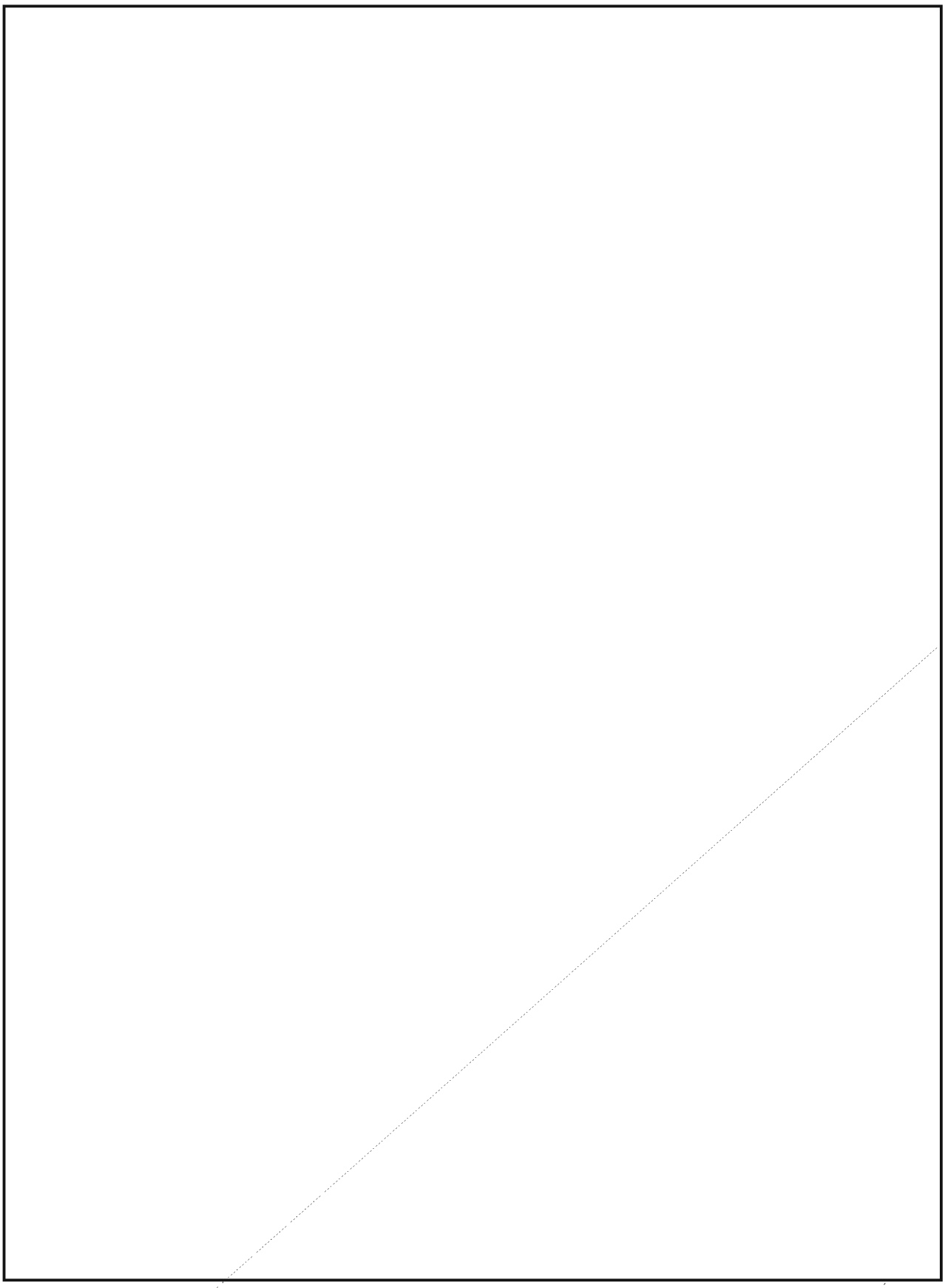
Advanced Identification Techniques (AIT) provide a means for identifying transmitters by their unique RF characteristics. In this article [redacted] provides a brief summary of the history and present status of AIT, as well as a glimpse into its future. dhw

An early aspect of AIT is Radio Fingerprinting, a technique for examining the characteristics of transmitters to determine unique aspects that will allow these transmitters to be identified when seen on another occasion. [redacted]

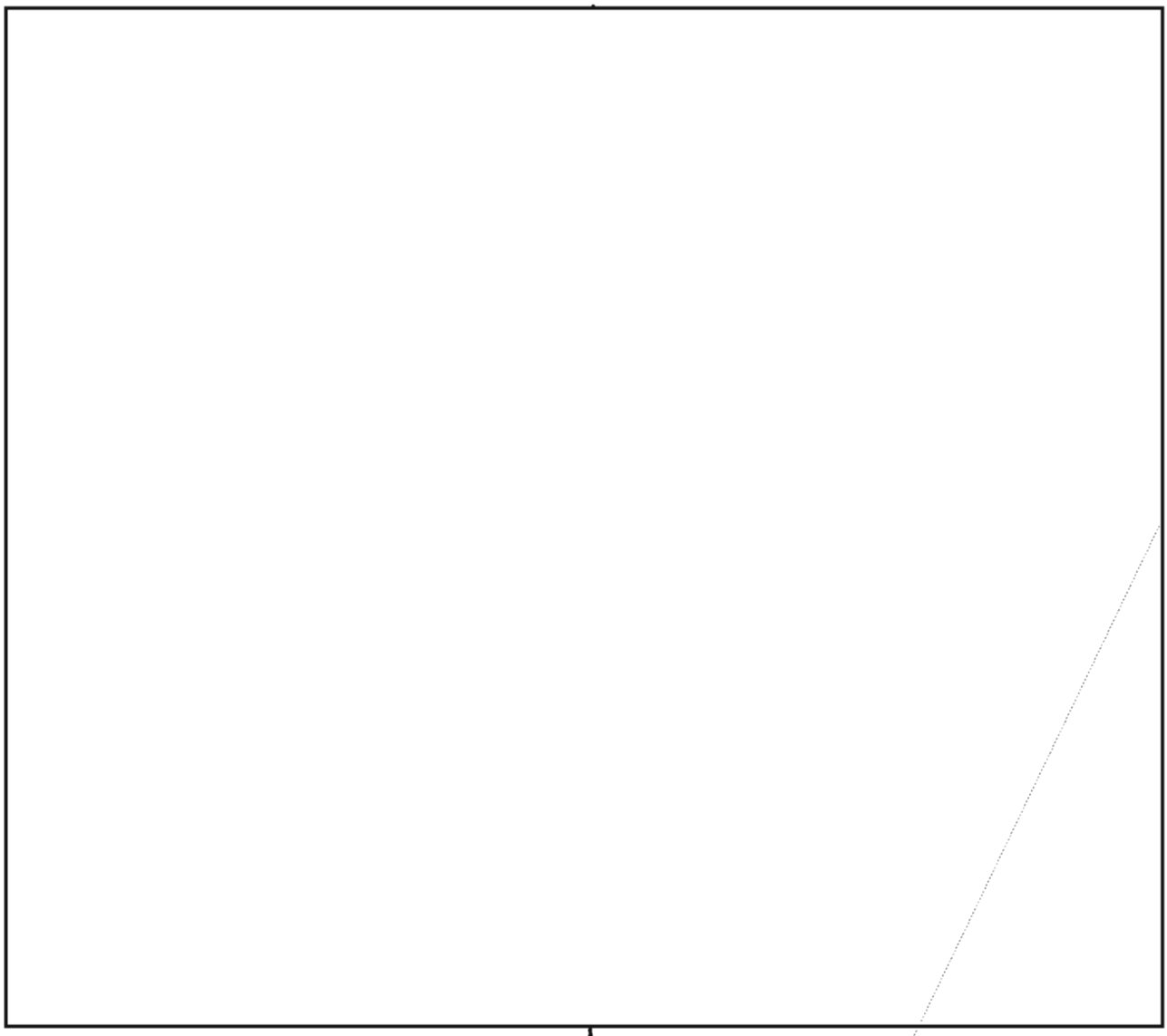
[redacted]

[redacted]

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36



(UNCLASSIFIED)

Answers to GEOGRAPHIC TRIVIA
(From Page 8)

EO 1.4.(c)
PL 86-36

- Frequent travelers to the Eastern Shore, who are convince that Delaware must be the flattest state, are almost ocrrect. With a high point of 442 feet (near Wilmington), Delaware comes in second. But first place goes to Florida, which soars to a high of 345 feet (in Walton County, in the western panhandle). Incidentally, when Washington, D.C., becomes a state, it will not displace Florida. Washington's altitude high, near the intersection of Wisconsin Avenue and River Road, is a surprising 410 feet. The highest low is in Prowers County, Colorado (3350 feet), where the Arkansas River enters the state of Kansas.

- Surprise! The most populous state capital is Indianapolis, with 725,077 inhabitants. It is followed by Honolulu (705,381) and Phoenix (664,721). The ten largest non-capitals are (in order) New York, Chicago, Los Angeles, Philadelphia, Houston, Detroit, Baltimore, Dallas, San Diego, and San Antonio. Washington, D.C., ranks twelfth. (These figures are from 1975 Census Bureau estimates; preliminary information from the 1980 census shows some changes to this ranking.)

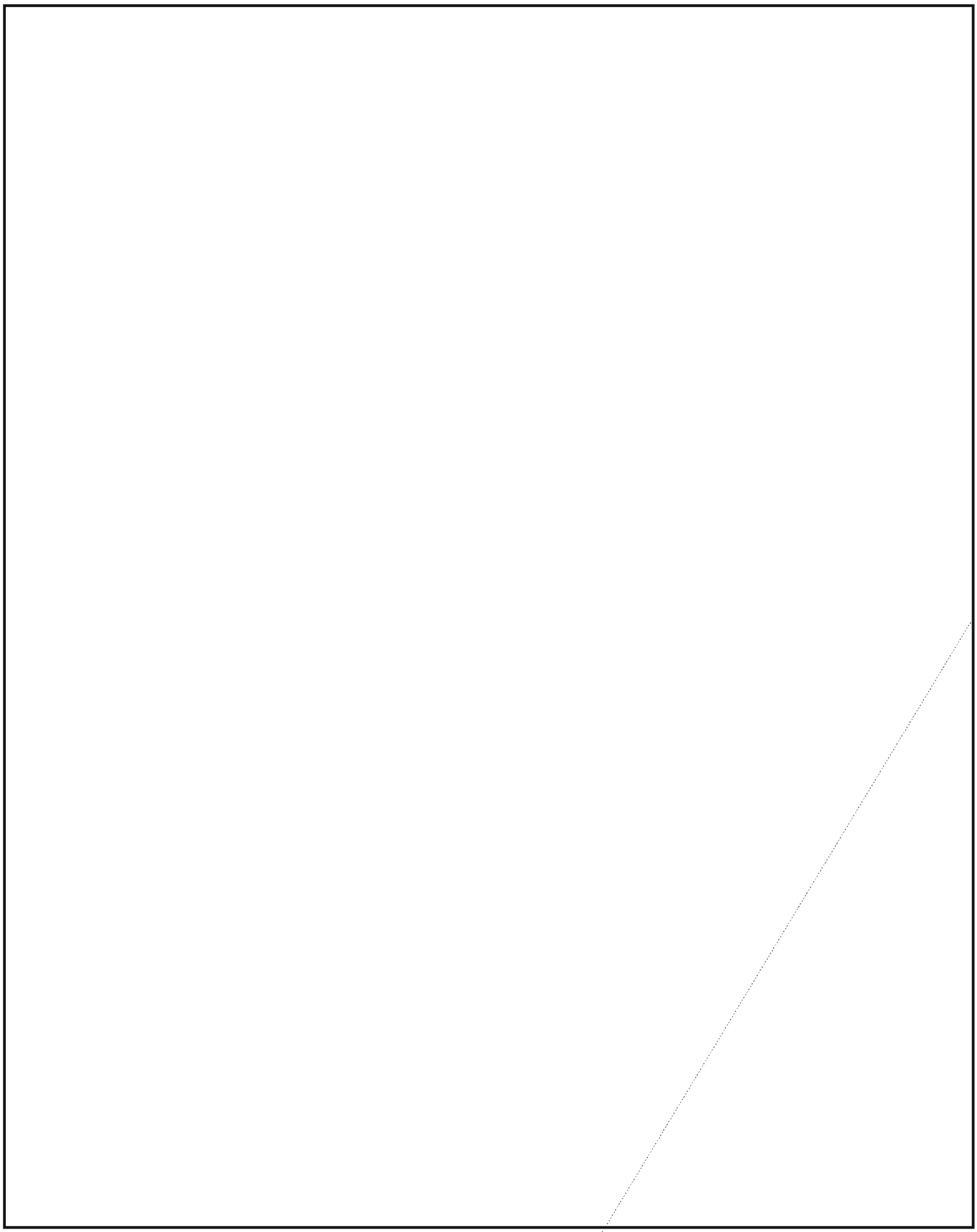
(UNCLASSIFIED)

SOVIET C^3 (U)

This article is classified ~~TOP SECRET UMBRA~~ in entirety

P.L. 86-36

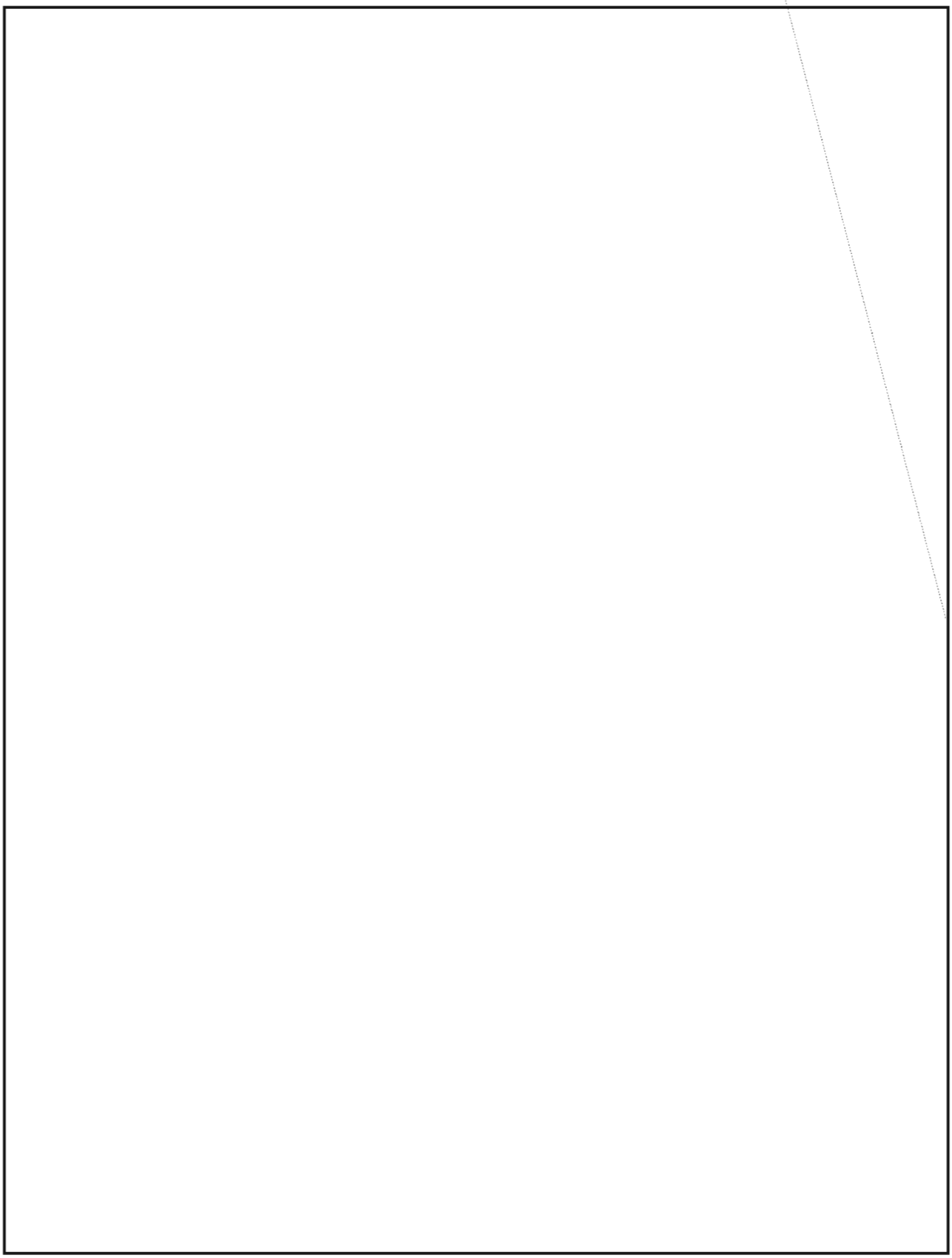
EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

DOCID: 4019683

EO 1.4.(c) -
P.L. 86-36



DOCID: 4019683

(UNCLASSIFIED)

What to Do About "FANX"

[redacted] A04 P.L. 86-36

Back in the sixties a coworker who lived in Linthicum used to drive to Ft Meade via Elkridge Langing Road, near Friendship Airport. Along that route construction had begun on a site described as "the future location of the Baltimore– Washington Science – Industry Center." "Very interesting," he thought. "Maybe in a few years I can bring my kids down here to tour some of these scientific and industiral institutions." How surprised he was when it was later announced that the occupants of the site, which was to become known as Friendship Annex, or FANX, were to be part of NSA's growing population, including him.

From the very beginning, the acronym FANX caused a pronunciation problem. My own unscientific investigation reveals about a fifty-fifty split among Agency employees. One half is convinced that FANX is a one-syllable word, pronounced FANX, while the other half, composed of equally intelligent people, pronounces it with two syllables—FAN-ex.

(This is somewhat parallel to the difference of opinion on how to pronounce the term "DIRNSA." In this case, my informal poll shows that a decided majority of Agency employees prefers the two-syllable DIRN-sa. But there is a stubborn minority that insists that it is a three-syllable word: dir-EN-sa. But I digress.)

I hope that members of both FANX pronunciation camps were as disturbed as I was several years ago, when the Credit Union put out a flyer, aimed at those of us who were working at the airport installation. This flyer hailed us as "Dear FANXITES!"

FANXITES?

The word made us sound like some kind of insects that come out of the woodwork. Didn't they know what we preferred the more elegant term FANXEANS?

If you didn't know the derivation, you could imagine that it was actually PHANX-EANS. Now isn't that a lot more classy, almost Grecian sounding. FANXITES, my foot!

Of course, since the state of Maryland changed the name of the airport from Friendship to Baltimore– Washington (or BWI), the term FANX has become obsolete. This has bothered me for quite a while, and I have tried to come up with a name that is more appropriate. Believe me, it hasn't been easy.

You can't do much with BWI to make a pronounceable acronym. I rejected "Airport Annex" since it doesn't tell which airport (National? Dulles?).

You could go the way of some area wags, who tried some time ago to popularize the term "Baltington" to describe the megalopolis that surrounds the B - W Parkway. Personally, though, "Baltington Annex" has about as much appeal as "FANXITES."

How about "Parkway Annex?" No, it sounds too much like a tacky motel.

I tried picking out another prominent landmark in the area. The biggest thing around, after the airport, is the Westinghouse plant. After experimenting with the firm's name and abbreviation, the best I came up with was "Compound W." Somehow that wasn't quite it.

I had almost given up, when I stumbled onto the solution. The annex is located in the South Linthicum area. So what would be more fitting that "South Linthicum Annex?" Accurate and descriptive, but not very exciting, you say? Not to worry. Like Friendship Annex, it is bound to become more popularly known by its contraction: SOLINEX.

The cash award I expect to receive from the Suggestion Program for this contribution will be donated to the Civilian Welfare Fund. The satisfaction of having solved the FANX problem will be reward enough for me.

(UNCLASSIFIED)

EO 1.4.(c)
P.L. 86-36

DOCID: 4019683

HELP WANTED (U)

Tom Engle, Senior Linguist in A64, with his tongue only part way into his cheek, offers this prospective recruiting flyer to any Agency element which might wish to use it.

N O T I C E N O T I C E N O T I C E N O T I C E N O T I C E

CHALLENGE ! EXCITEMENT ! ADVANCEMENT ! FUTURE !

All of this can be YOURS with a career in A6 ! Apply today!

IF YOU HAVE A DEGREE IN

Aeronautics	History
Chemistry	Law
Engineering	Mathematics
Finance	Medicine
Geography	Physics
Geology	Science

IF YOU HAVE BEEN EMPLOYED AS

Cartographer	Political Analyst
Communications Specialist	Politician
Computer Specialish	Test Pilot
Mechanic	Truck Driver
Newsman/Broadcaster	Weather Forecaster
Photographer	Xray Technician

OR IF YOU HAVE

Been an admiral
Been an astronout
Been a general
Built a rocket
Engaged in international trade
Launched a satellite
Managed an industrial enterprise
Negotiated an arms agreement
Planned military operations
Run a railroad
Served as a diplomat
Served on a Military Advisory Group

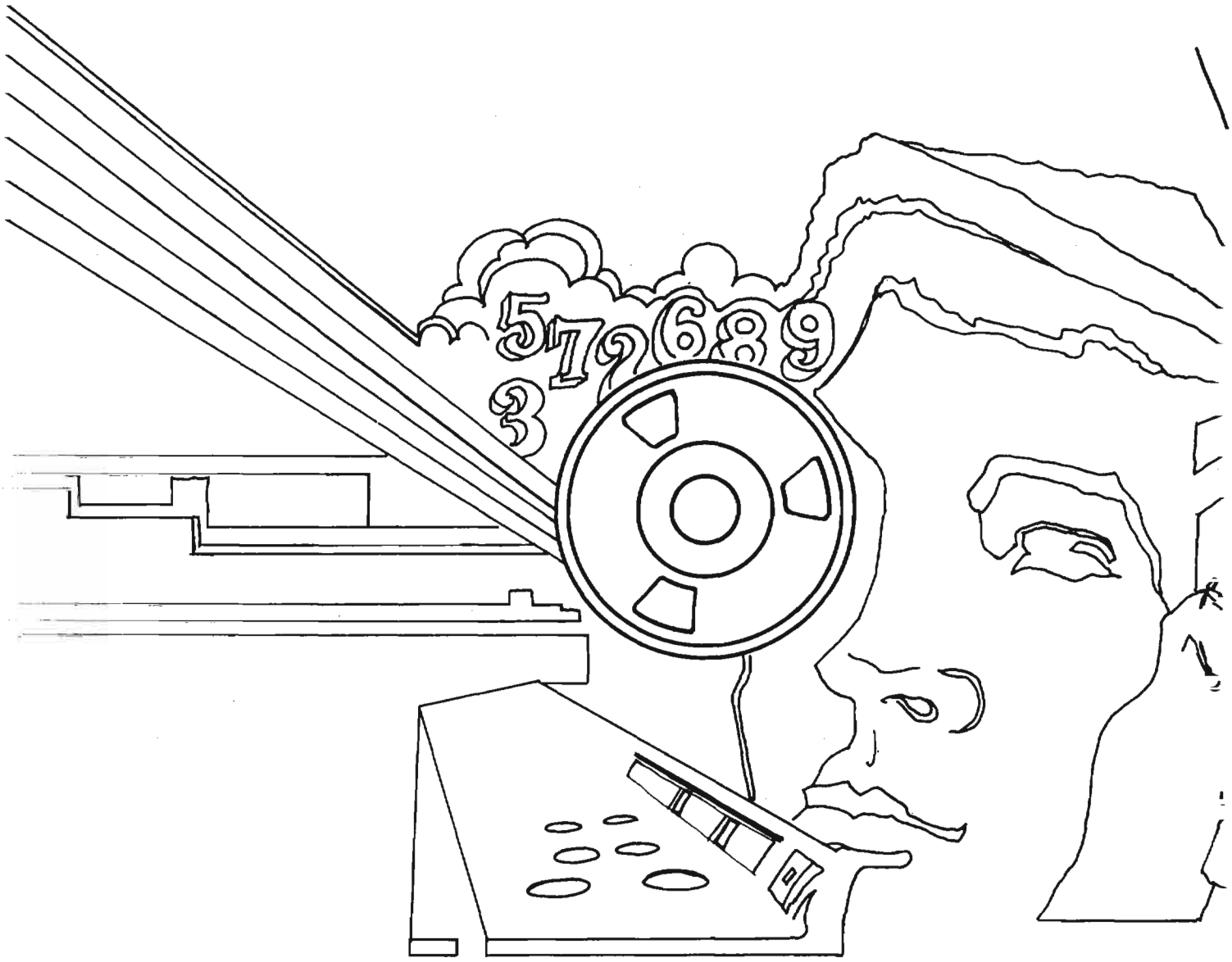
APPLY TODAY ! DON'T DELAY !

QUALIFICATIONS***	POSITION OFFERED
5 of above subjects	GG-5/7 TRANSCRIBER TRAINEE
10 of above subjects	GG-9/11 JOURNEYMAN TRANSCRIBER
20 of above subjects	GG-12 SENIOR TRANSCRIBER
ALL of above subjects	GG-13 SENIOR LINGUIST

*** NOTE: ALL APPLICANTS MUST BE QUALIFIED RUSSIAN LINGUISTS.

P1-Nov 80-53-8738

~~TOP SECRET~~



DOCID: 4019671 / /

P.L. 86-36

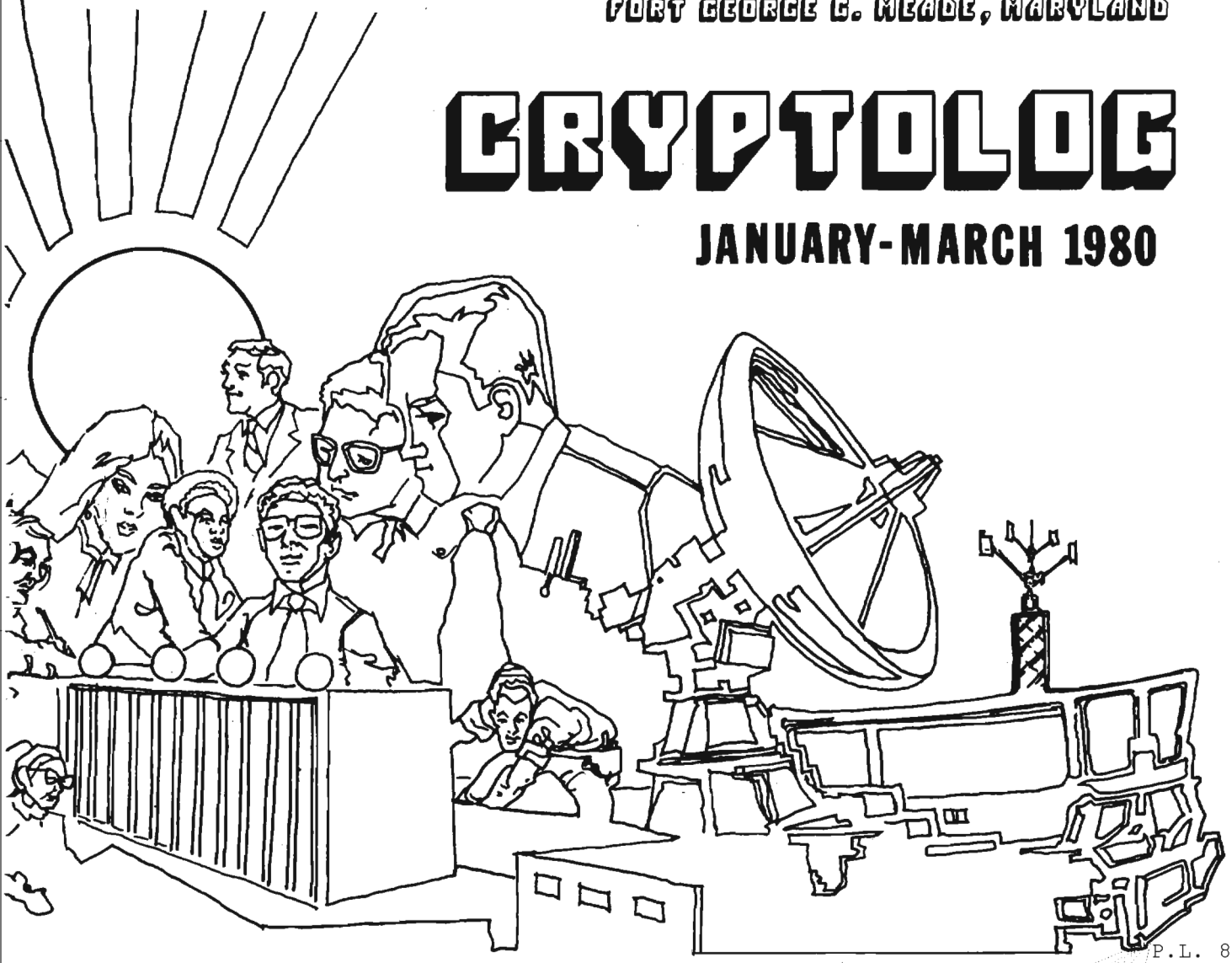
~~TOP SECRET~~

E42 [redacted]

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JANUARY-MARCH 1980



P.L. 86-36

THERE'S A NEW WORLD COMING — ARE YOU READY? (U) ..... [redacted] 1
LIP (U) ..... [redacted] 4
SYSTEM ACQUISTITION DOCUMENT REVIEW (U) [redacted] 10
ANALYSTS OF NSA, ARISE! (U) ..... [redacted] 11
COMING HOME (U) ..... [redacted] 13
CIRC: AN INTELLIGENCE DATA BASE (U) .. [redacted] 14
BETWEEN THE LINES OF YOUR PERFORMANCE APPRAISAL (U) .. [redacted] 17
NSA-CROSTIC No. 30 (U) ..... D.H.W. 18
NSA/CSS MILITARY LINGUISTIC PROGRAM 20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 1 MAR 2010~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526. MDR Case # 54778

DOCID: 4019671

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. VII, No. 1 - 3 JANUARY — MARCH 1980

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor-in-Chief.....David H. Williams (1103s)

Collection.....[redacted] (8555s)

Cryptanalysis.....[redacted] (4902s)

Cryptolinguistics.....[redacted] (5981s)

Information Science.....[redacted] (3034s)

Language.....[redacted] (8161s)

Machine Support.....[redacted] (5084s)

Mathematics.....[redacted] (8518s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Taurone (3573s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4019671

There's a New World Coming — Are You Ready? (U)

[redacted]

P.L. 86-36

(U) Analyst response to a changing environment is an area that has piqued my interest for a number of years. This interest has become especially pronounced in the last four or five years, largely as the result of the increase in the variety and number of automated processes that have become available, my involvement in a number of long-term research projects, and the prospects of newer and more sophisticated machine-based analytic techniques. As a consequence, I have given much thought to the effects that this increased automation will have on the analyst and to what we, as an organization, can do to respond to the challenges and opportunities that will arise.

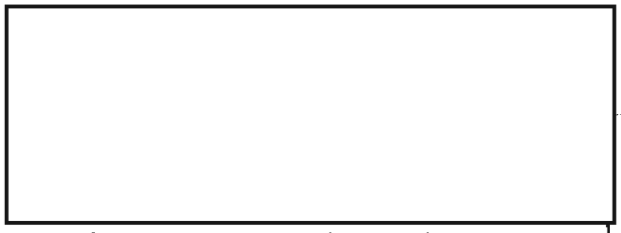
(U) If we are to accurately assess how the analyst of the future will react to the increased automation of the analytic process, it is necessary to know the analyst of today. This is logical, since the majority of tomorrow's analysts are already on board and active in the analytic field. It also becomes essential to define the functions of the analyst since all personnel who carry the title "analyst" are not analysts by the strictest definition of the word. For convenience and easy reference I have divided these "analysts" into three categories which I've labeled, for lack of any better terms, "loggers," "case analysts" and "research analysts."

[redacted]

[redacted]

EO 1.4.(c)
P.L. 86-36

~~HANDLE VIA COMINT CHANNELS ONLY~~



(U) The changes expected as we become more and more automated will alter the methods and procedures currently used in the analytic areas. This will have a profound effect on our operations, but to an even greater extent it will modify the lifestyle and environment of each of the three types of analysts I've defined. Each will be affected in a different way depending on the analyst's perception of analysis, his personality and his ability to adapt.

(U) Once the machine takes over the simple data manipulation and recording functions, the "logger" will become, to a great extent, obsolete. His routine will be upset and his workaday world completely disrupted. He will no longer have his logging to fill his day. He won't know what to do and he'll be completely lost. For those currently having trouble isolating the "loggers" in their outfits, they'll then be very easy to spot. Just look for those people sitting with a blank stare on their faces and for those making nervous movements at their desks as they anxiously try to find something to do. Eventually their names will appear on the list of those who are abusing their sick leave. The real "logger" will never recover from automation. He's lost his place in life. His day-to-day world will have been destroyed and he simply won't know what to do. For many it will be too late to start over. Others will lack the initiative, while for still others, it's nothing more than a lack of talent. The world will have passed them by. They, of course, will not be to blame. It'll be the machines' fault, or management's fault, or maybe just the breaks of the game.

(U) In reality, the "logger" has always been a clerk with a professional job title and a professional paycheck. He was created by the system, and, with the advent of new automated techniques, will be destroyed by the system. Some will be salvaged. Some "loggers" will regroup, retrain and regain a place, perhaps at the "case analyst" level. Those that can't make the transition will have to be purged since the cost of automated systems will call for a decrease in personnel expenditures.

(U) The "case analyst" will survive and thrive in the new automation. He really never did care for the logging and data maintenance functions associated with his job; therefore, he'll adjust. He'll re-order his priorities and use the additional time now available for the development and analysis that he never could quite get around to under the old semi-automated method of operation. His productivity will increase and more technical data on his targets will result.

EO 1.4.(c)
P.L. 86-36

The ultimate gain will be the production of more intelligence information in satisfaction of our requirements. The "case analyst" will grow as a professional, honing his skills as he practices his trade, and in many instances will develop into a "research analyst."

(U) The "research analyst" will see few changes in his method of operation as a result of this new automation. He'll have to deal with new data bases, new retrieval programs and new equipment, but his daily routine will remain pretty much the same as it is now. He will generally review the same types and amounts of material and work on the same types of projects. He should see some improvements in accuracy and completeness as a result of the elimination of the "logger" and the automation and resultant upgrade of the data bases. He will be able to spend less time on the verification and data gathering phases of his assigned tasks and thereby be able to complete more assignments in a shorter time. This will allow a more efficient use of the limited number of "case analysts" and permit us to achieve maximum benefit from their talents. Automation will also improve the morale of the "research analyst" since he will be able to function almost entirely in his primary capacity.

(U) The benefit of this increased automation is readily apparent. The talent of our people can be used to the fullest, with dull, repetitive tasks reduced or eliminated. The timeliness, accuracy and quality of our product will increase. Personnel not working at their prescribed levels can be eliminated, with a resultant savings of money. All of this is, of course, predicated on manageable machine systems that will function as designed. Since our track record for the development of such systems is not impressive, let's hope that we have learned from experience, and not attempt to reap benefits before we have proven follow-on systems.

INTERNATIONAL AFFAIRS INSTITUTE

3rd ANNUAL ESSAY CONTEST

Prizes: 1st Place $100.00
2nd Place $ 50.00
3rd Place $ 25.00

Winning entries will also be considered for presentation in an appropriate Agency publication

Topic: Related to International Affairs

Enter By: 1 October 1980

To enter (or for more information) Contact Either :

[redacted] P.L. 86-36 **B51, Room 3W156**

or

[redacted] P.L. 86-36 **G7, Room 5A150**

Winners Announced: October 1980

EO 1.4.(c)
P.L. 86-36

LIP (U)

[redacted] P16

[redacted] A5

P.L. 86-36

[redacted]

a language could be stored. This data base could contain models of each langage we may need to identify. The models would contain all of the information needed to identify an unknown text by some comparison technique. Thus any automatic language identification scheme would have to be structured as follows:

- language models
- comparison method

(U) For various reasons, it is clear that automatic dictionaries are the least efficient and least reliable method of identifying languages.[2] Further, linguistic methods based upon the morphological or syntactic structure of the language require a huge amount of effert to construct suitable models. The only reasonable approach to language modeling which appears easy to implement as well as reliable is by statistical methods. It now becomes a matter of deciding which statistic to use.

(U) We decided to try the simplest approach first: which method of modeling, which is inexpensive in terms of storage and CPU time, will yield acceptable results? Monographic modeling is indeed cheap, but not very powerful. The same can be said for standard Agency techniques of long standing, such as Delta I.C. and logweights (see Chart 1).

(U) The next possibility for modeling would be digraphs. Here is where the solution was found. A digraphic model of a language is very easy to construct, requiring a relatively small amount of text as input and very little storage for the model. A digraphic model stores the information in a digraphic matrix (see Chart 2) in terms of the probability of each possible digraph occuring for a given language.

P.L. 86-36
EO 1.4.(c)

[redacted]

(U) But why should a linguist have to spend time identifying languages at all? Why couldn't an automatic, computerized method of identifying languages be developed? To implement such an automatic system, we would need to construct a data base, that is, an information bank where all of the information needed to identify

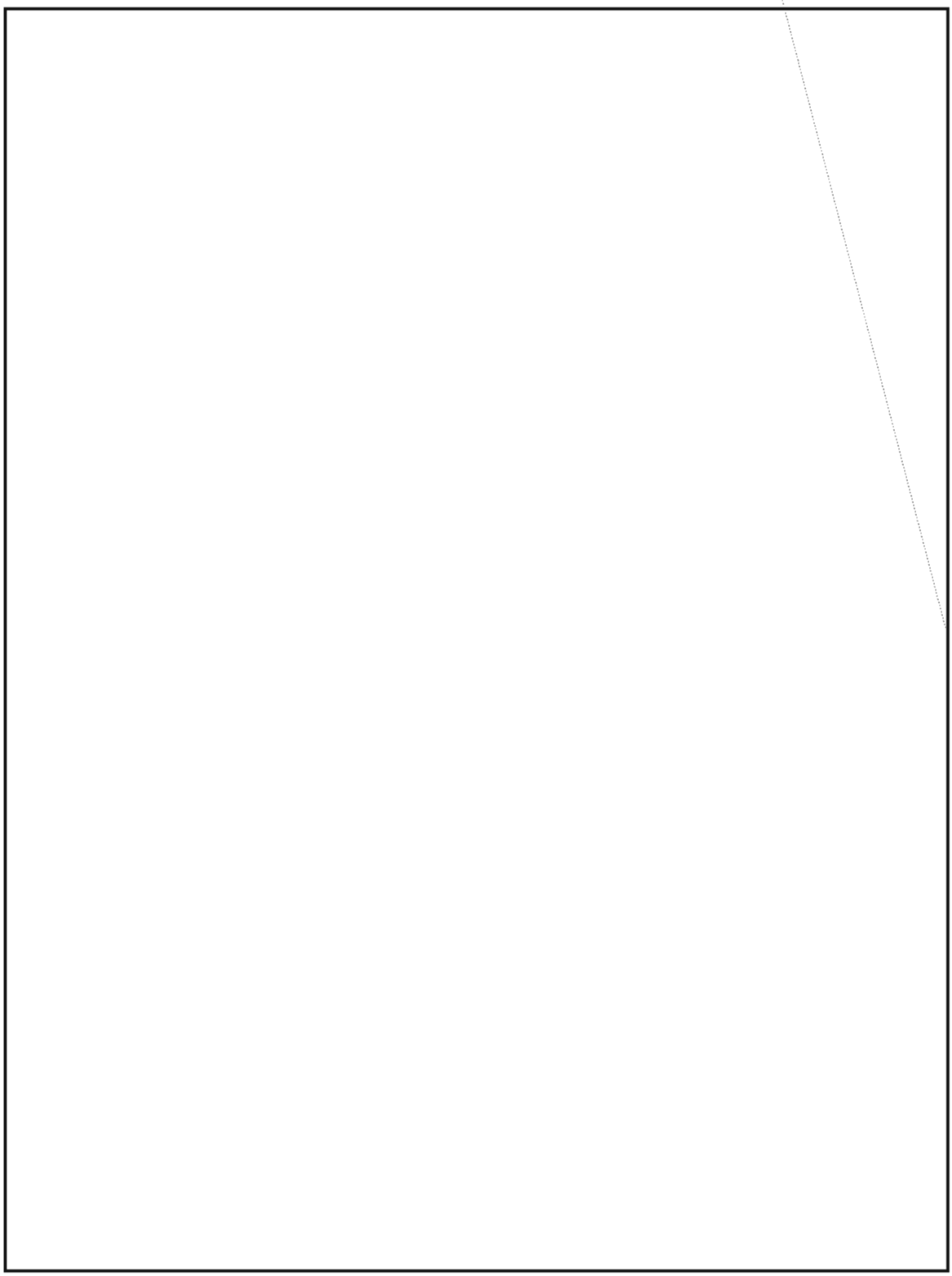
---

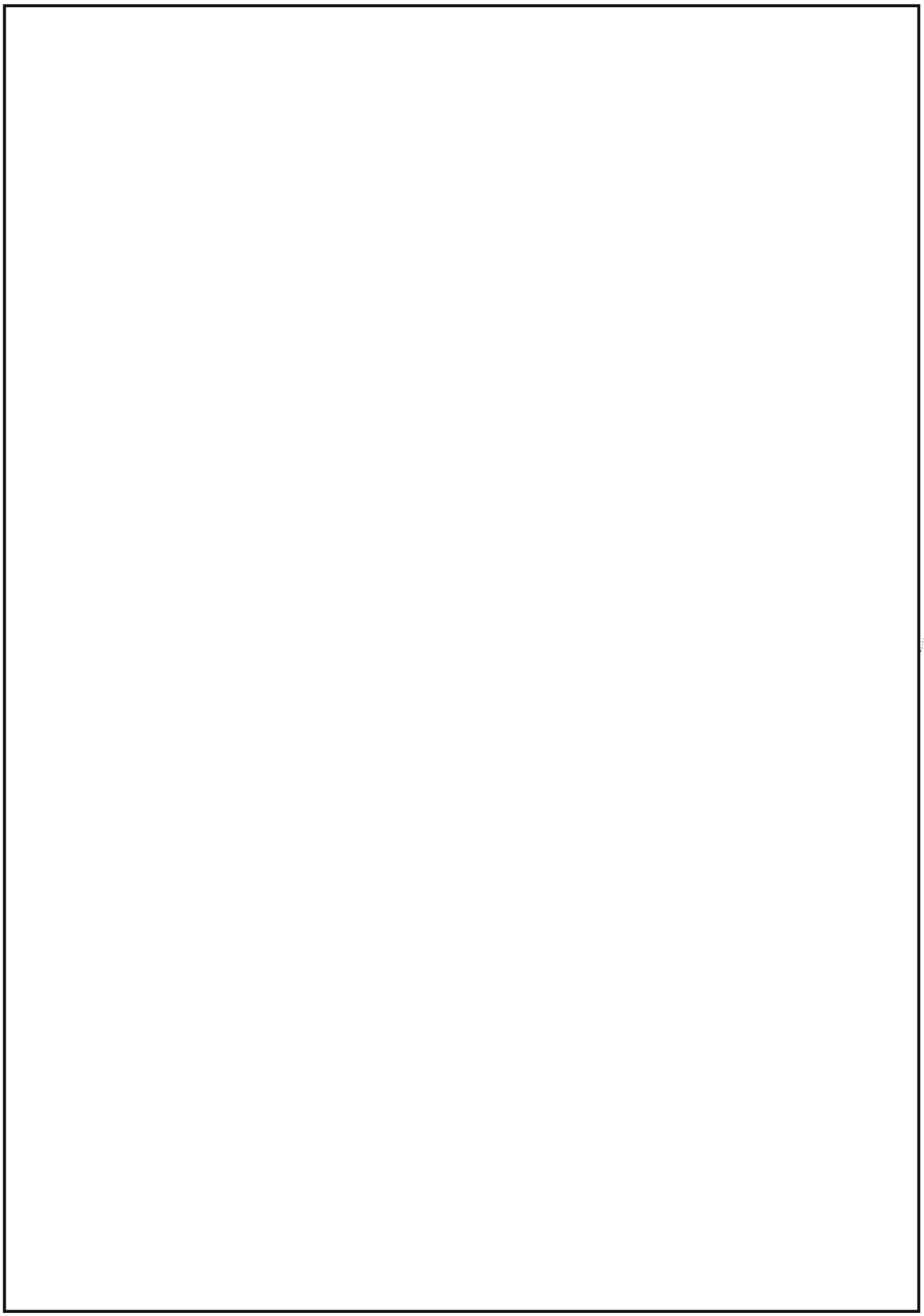
[redacted]

[2] For details see the P16 paper of 25 July 1979 by [redacted]

P.L. 86-36

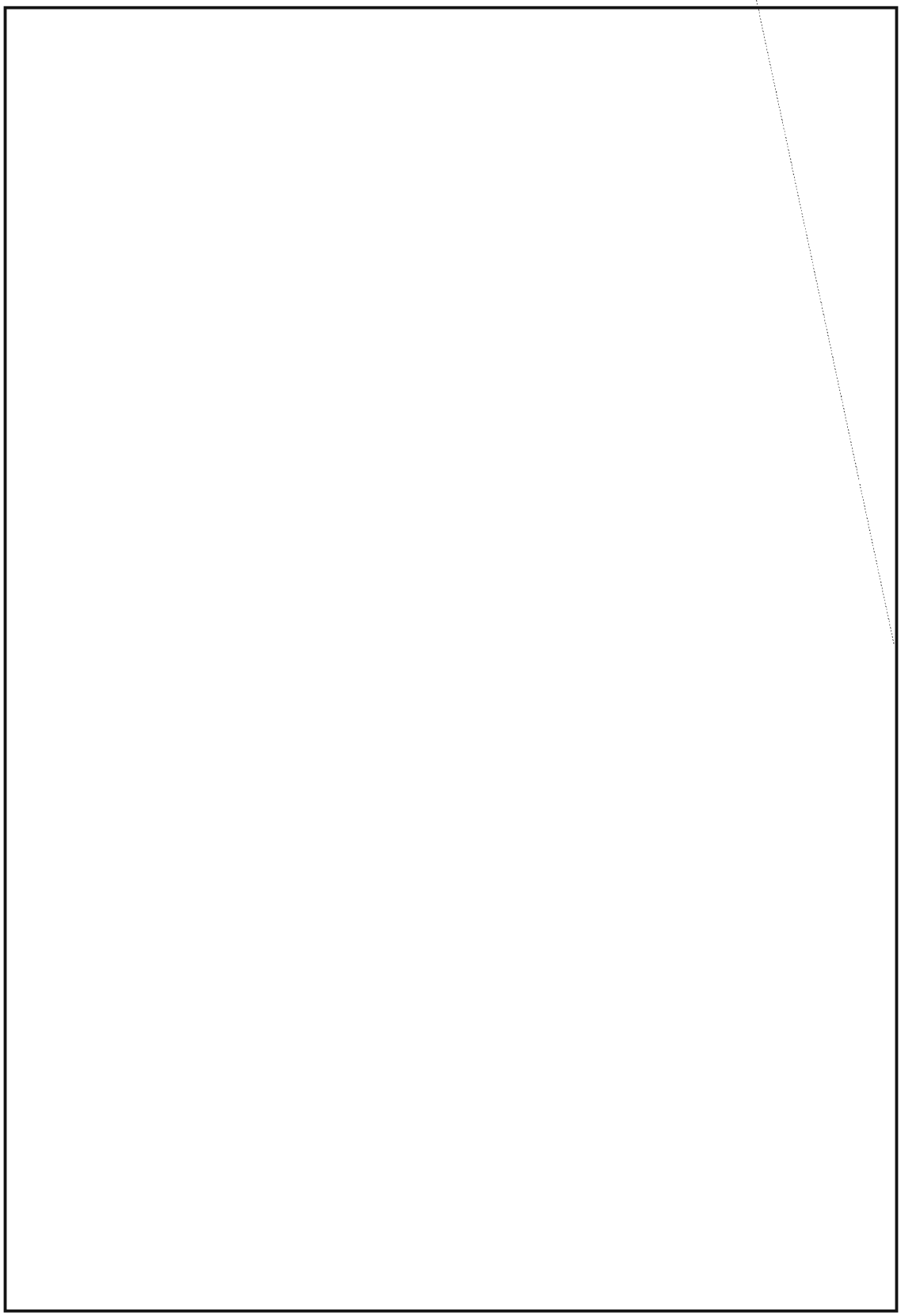
P.L. 86-36

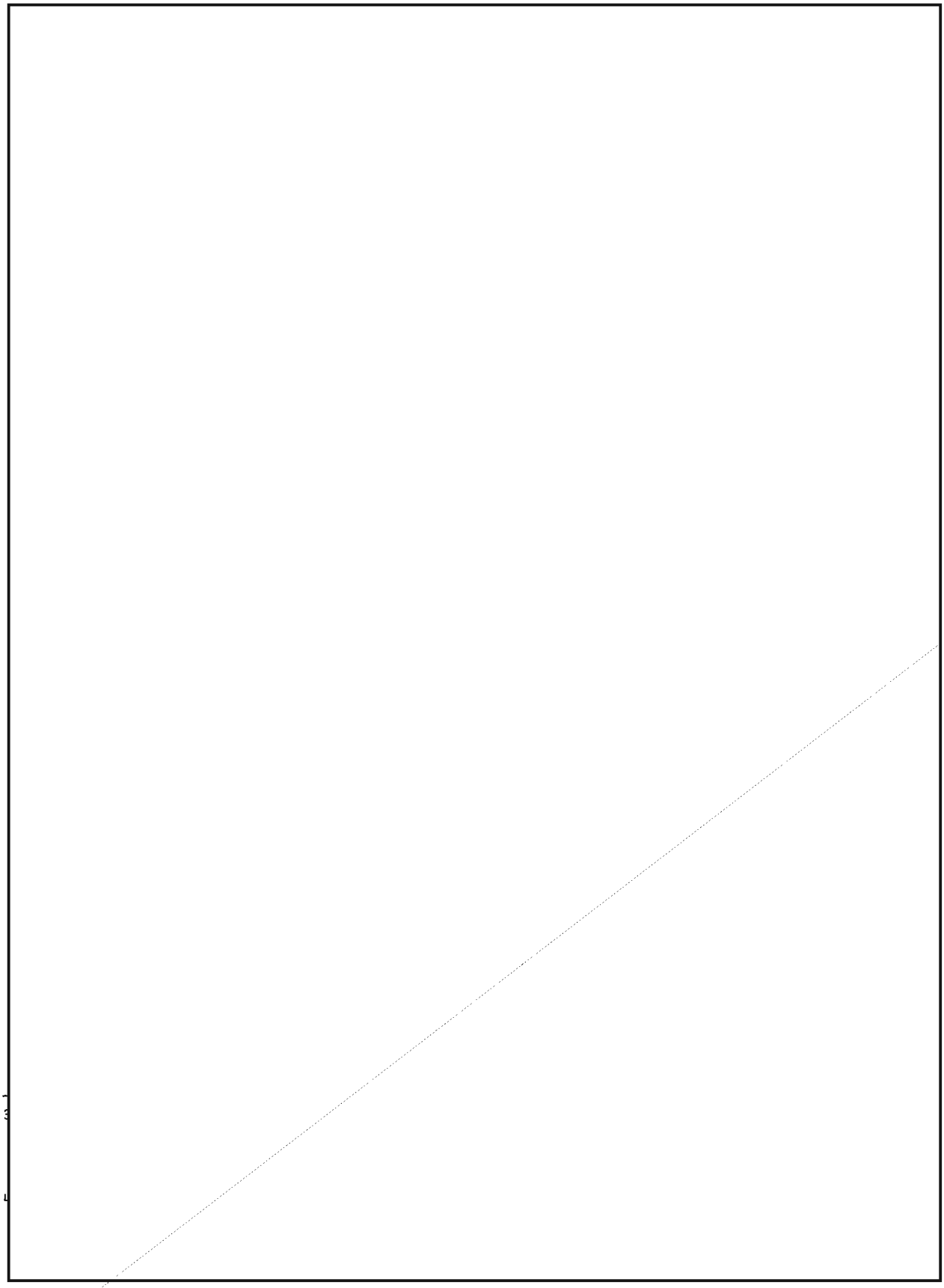




P.L. 86-36

P.L. 86-36





P.L. 86-36

WHY ARE ALL THE STREETS IN AMERICA WHICH ARE NAMED AFTER A FRENCHMAN IN SUCH TERRIBLE CONDITION, AND WHO WAS THIS FELLOW DETOUR, ANYWAY?

It is generally conceded that book-learning is not the best way to learn a foreign language. Instead, most people agree that the best way is to actually live in an environment where the language is present 24 hours a day. When a person sees and hears the words in a foreign language around him he soon learns what makes sense and what doesn't. How long, for instance, does it take for even the least language-oriented person to realize that there *isn't* any famous person named Einbahn, after whom so many streets are named throughout Germany and Austria, all of them coincidentally one-way streets? Well, I'll never forget the trip that two adults and four children, in one Rambler station wagon, took from Oberammergau, Germany, to Lake Garda, Italy. The reason why I'll never forget it is not just the horror I felt as I was being pushed down the Dolomites (it must have been at 150 miles an hour) by good-natured Italian truck drivers trying to meet a schedule. No, the reason is that, during calmer, flatter stretches of the trip, when I could relax my grip on the wheel and enjoy the scenery, it had seemed to me that Italian villages have such pretty names. But can they *all* have the same name! Hadn't we seen that name a few hours back when we were crossing that bridge? Then a half-hour ago when we went past the quarry? And here's *another* village with the same name — Lavori in Corso. Oh, dammit, I told myself, learning Italian quickly, it means "Men at Work"!

Right after World War II, as the Cold War was starting up, the United States had to think of ways to get information to "the Russian People." The proposed methods included balloons that were supposed to blow from west to east but often didn't cooperate. One method that was used at an early stage was to set up an official U.S. radio station, transmitting in Morse code to all the hams in the Soviet Union. Since it was an official U.S. radio station, it had to have a callsign beginning with a K (if the transmitter is located west of the Mississippi) or a W (if located east of the Mississippi). Since the transmitter was located on the East Coast, is was a W. And since callsigns often mean something—WGMS, for Washington's Good Music Station—it was decided to call this transmitter WRU, for U.S. radio transmitting to RUssia. But it didn't take long for Washington to learn that the Russian People didn't believe any of the broadcasts. Eventually someone pointed out that if you send the callsign in Latin letters, WRU, in Morse code (.-- .-. ..-), any Russian ham would convert those dits and dahs to the Russian letters ВРУ, which, unfortunately, represent the Russian word for "I'm lying." Well, back to the balloons...

Excerpted from "Twelve Language Anecdotes in Search of an Author," by Arthur J. Salemme, formerly P1, now retired.

To Subscribe to CRYPTOLOG,

Or to Change Your Address, Call

1103s

SECURITY CLASSIFICATION

SYSTEM ACQUISITION DOCUMENT REVIEW

SAO USE ONLY

CONTROL NO.

ACTION (If marked, indicate responsible individual)

DUE DATE (Action completed)

RESOLVED (If marked)

UNRESOLVED (If marked, no resolution found during review, may/may not require further attention)

COVERNAME

DOCUMENT

TITLE

NSA FORM H8274 JUN 79
SYSTEM ACQUISITION DOCUMENT REVIEW

PORTIONS TO WHICH THIS CRITIQUE PERTAINS

(Section)	(Page)	(Paragraph)	(Line)

REVIEWER

NAME | ORG | CRITIQUE DATE

T424

CRITIQUE OF NOTATED SECTION AND/OR

SUG

RESPONSL

SAO

FINAL DISPOSI

Management guidelines pertaining to the system acquisition process (NSA/CSS Circular Numbers 25-5 and 25-16 and NSA/CSS Manual 81-1) have been in effect for approximately three years now. Many organizations have been involved in the acquisition process through planning, reviewing, decision making, implementing, or some other related activity.

During this time, project management elements have been particularly involved in the preparation of various system acquisition documents such as System Plans and System Acquisition Plans. To aid the review process for such documents, several methods have been devised by different elements to record and manage comments, suggestions, critiques, and resolutions concerning the various documents. When it became apparent that some of these methods were quite useful, an effort was initiated to consolidate the most valuable concepts. A survey of T4 elements, particularly T42 Project Management divisions, was taken and the results were used to develop a draft "critique form". Subsequently, forms management personnel (N33) modified the draft to conform to standards established for similar type forms.

The form, System Acquisition Document Review - H8274, is now available in the supply room. An initial supply of 1,000 has been provided and initial usage is expected to be approximately 400 per month.

SIGNATURE

REVIEWER INDICATING AGREEMENT TO FINAL DISPOSITION

SAO OFFICIAL FINAL DISPOSITION

DATE

FORM H8274 JUN 79

SECURITY CLASSIFICATION

P.L. 86-36

P.L. 86-36

ANALYSTS OF NSA, ARISE!

YOU HAVE NOTHING TO LOSE BUT YOUR PAPER

[redacted] T12

This entire article is ~~FOR OFFICIAL USE ONLY~~

NSA is in the midst of a revolution. Before anyone rushes to call the Federal Protective Service, let me quickly add that the revolution, here at NSA, is an information services revolution. Webster's New International Dictionary defines the word revolution as a "total or radical change." A total change is exactly what is happening, in a rapidly evolving way, to the methods of information storage, retrieval, and dissemination now available or being planned at NSA. The radical change occurring at this Agency, of course, represents only a microcosm of the vast and rapid evolution of computers, data entry devices, and data storage devices which is taking place worldwide. New, swiftly growing industries offering information to the public, on virtually every subject known to man, have appeared in the last decade. This information is now instantly available by attaching a device about the size of a portable typewriter, to your telephone.

The New Information Entrepreneurs. T12, Information Services, now subscribes to the data bases of several of these new information entrepreneurs, including Lockheed's DIALOG, Bibliographic Retrieval Service's BRS/SDI Service, and the *New York Times'* DATABANK. Hundreds of hours of manual research time is now condensed to seconds and minutes when searching the vast data storage banks available via a telephone line to computers located in such places as Palo Alto, California and Scotia, New York. NSA information science analysts will query these data banks to aid in your work-related research on such diverse topics as chemistry, psychology, economics, education, physics, engineering, social sciences, medicine, drugs, industry and hundreds of other subjects. NSA is now considering the addition of LEXIS and NEXIS services offered by Meade Data Central. LEXIS is a legal citation service covering federal and state law. NEXIS is an extremely powerful research tool which provides a full text search capability of news sources such as the wire services, news magazines, newspapers and journals for a three year period. The addition of NEXIS to T12's inventory of commercial data bases would potentially eliminate a great amount of open source processing now being done.

Government-Sponsored Data Bases. T12 has direct access to a number of government-sponsored data bases which offer information of great value to NSA analysts. These include the files of the Defense Technical Information Center (DTIC), which provides access to technical reports on research and development projects of the Defense Department. These reports are available in special categories, on microfiche, in the NSA Library. Other DTIC data bases offer descriptive summaries of DoD R & D activities. COINS (Community On-line Intelligence System) offers valuable community-wide intelligence information to NSA customers with a need-to-know.

NSA's In-House Developments. NSA's mission must, however, be also served by information data banks developed and operated in-house. The useful and valuable classified information available through the SOLIS system is, of course, accessible by T12's information science analysts in researching your classified queries. In the last few years, T12 has developed and maintained a large number of its own specialized information data bases using the M204 language and the IBM 370/168 computer for storage and retrieval. These machine systems have greatly reduced the enormous collections of file cabinets so familiar to visitors to the old CREF. New systems, now underway and being planned, will soon guarantee that the last manual file cabinet, like the pterodactyl, will fade into extinction.

T12 is now hoping to solve one of the greatest barriers to the rapid conversion of the written word to digital form by using the Kurzweil data entry machine. This device, designed to "read" ordinary print and convert it to computer-compatible digits, was developed by the same company which originated the Kurzweil reading machine for the blind, now available for use in the NSA Library. The successful employment of this device, or one like it will do away with the slow "poking-in" of data by a human, so essential to the computer storage and retrieval of information.

Through [redacted] T12's in-house information retrieval system, analysts will be able to index the hundreds of thousands of reports P.L. 86-36

which contain information needed by Agency analysts in their daily work. Storage of full texts using new ultra-high reduction techniques on microfiche is being studied under Project [redacted]

Manipulation of Electrically Received Information. Other systems, designed to handle information received electrically, are also under developemnt using hardware and software already in use in another Agency system. [redacted] the name given to this project now awaiting software modification, will store large quantities of classified information presently received here via teletype and will enable the researcher to perform full-time searches by words, subjects, series numbers and other approaches. Thousands of documents now being processed manually for hard copy files, a process which is both labor intensive and time consuming, will become immediately available to researchers throughout the Agency using easy-to-learn search strategies. Automatic distribution of these documents, in hard copy, is already taking place under Projects [redacted] and [redacted] will eliminate the need for hard copy.

What This Revolution Will Accomplish. What does all this mean to the Agency analyst working against a deadline and seeking information vital to the completion of a report? It means that time-sensitive information will be available when it still has meaning and importance. It means that, in many cases, information will be available to the analyst, 24 hours a day, by querying T12's data bases directly, if required. It means getting an answer to your question in seconds or minutes instead of hours or days. P.L. 86-36

The American Revolution freed us, as a nation, from foreign domination; the information services revolution will free, us, at last, from the overwhelming flood of paper that has dominated us for so long, stealing our time and efficiency. It may also, incidentally help save our forests for other uses.

The next time you call for information services from T12, don't be surprised when your question gets researched and answered with revolutionary zeal!

* * * * *

[redacted] WINS SYDNEY JAFFE AWARD (U) P.L. 86-36

~~(TSC)~~ At the 1980 Crypto-Linguistic Association Annual Banquet [redacted] of the Language Department of the National Cryptologic School was presented the Sydney Jaffe Award, the highest recognition a member of the Agency can achieve in the language field. His significant accomplishments as an Arabic linguist span an Agency career of some 24 years. [redacted] EO 1.4.(c) P.L. 86-36

~~(C)~~ In 1977, [redacted] performed pioneer work in developing National Cryptologic School courses in the Syrian, Iraqi, Libyan and Egyptian dialects of Arabic. Unique among these is the Libyan course, the only such course available to the intelligence community. For this seminal work in course development, he received the Agency's Meritorious Civilian Service Award. P.L. 86-36

(U) If there has ever been at NSA a linguistic factotum, it is [redacted] He yields to no one as a model of the traditions and ideals set by Dr. Sydney Jaffe.

COMING HOME

[redacted] G

P.L. 86-36

This article was originally published in the WIN [Women in NSA] Newsletter for May 1980. Since the problem it addresses is certainly not limited to Agency women, but rather applies to all employees returning from tours of duty elsewhere, it is reprinted here so that it may reach a wider readership. dhw.

Last year, I was fortunate to have been selected for an external training program. I was thrilled, not only because of the opportunity it provided for me to learn more about the inner workings of the entire Department of Defense, but because I felt also that I would then be assimilated back into the Agency in a more responsible position. AFter all, if the Agency thought enough of me to have selected me for this "plum," then would they not want me to use my knowledge, later, to the best advantage?—or so I thought.

Judging from my past job experience in several areas of the Agency, in addition to my recent schooling, I felt I was ready to assume a position of greater responsibility upon my return; however, I was stymied in my attempts to find such a position. My two-month attempt to find a job before I returned to the Washington area was greeted with such responses as: "We've just changed the PMM's, and your name will no longer be circulated to key components" (as I had been led to expect prior to my departure); and "We've just changed the PMM's and you must return to your original key component, since they sponsored you" (that's been changed again, I understand). (The difficulty was compounded by my trying to do business via a long-distance commercial phone.) Rather than being given a choice of assignments, I was told that I would take a job in a certain organization, and I drove back to the Washington area specifically to interview for this job. After the interview, I decided, for several reasons, that this was not the job for me; however, I was "on the books" as returning to that job, and that was that, as far as the Agency was concerned. When I returned to the Agency, I personally scouted around and arranged some job interviews, but I felt that I didn't have the time to pursue potential opportunities because I was under pressure to be assigned SOMEWHERE. I finally returned, in a similar capacity, to the group from which I had left. The other three Agency employees who were in school with me also returned to the same or similar jobs. A sad commentary, I feel.

I am grateful for the opportunity the Agency provided for me to broaden my knowledge. However, I do have a few suggestions for both the Agency and for those employees contemplating applying for external training. First of all, I know the Agency's reassimilation program has historically had its problems, and I am confident that the current administration is doing everything it can to help remedy the situation. I can't speak about overseas returnees, but it seems to me that those returning from specialized external training, such as the joint and senior service colleges that provide their sutdents with a broad background in military affairs, could be used by the Agency in a variety of areas. I know that there is one slot, a one-year tour as executive assistant to the Deputy Director—that goes to a returnee from the National War College—but other areas of the Agency could also use the special kind of expertise gleaned from this training. A one-year tour in any one of these areas would benefit both the Agency and the employee. In lieu of that, the employee should not be "locked into" a job upon his or her return. A number of interviews (perhaps three) should be arranged for the employee. There's no substitute for personal contact to aid one in deciding if one could effectively work with an individual or in a particular area (one can't make this decision via long distance), and a specified period of time (a week or ten days) should be allotted the employee to make up his or her mind.

Failing this, what can YOU do to assure yourself a good job upon your return? (This advice holds true also for those who may be contemplating a change of jobs.) First, make certain your Personnel Summary is up to date, and don't be shy, even before you go on TDY, about giving it to those who may be in a postiion to place you. Secondly, decide which areas REALLY interest you; find out what you can about these areas, who the managers are, and get appointments with them. Most managers are willing to talk to potential employees. Thirdly, don't discount the theory of "networking"—it *can* work for you. A few of the job interviews I lined up were as a result of "contacts" I had made while working on a group-level staff. A few managers even remembered me from my stint as a Director's briefer (and that was in 1973!). In addition, senior WIN members were very generous in giving me advice and support.

In short, the opportunities are there; YOU CAN MAKE IT HAPPEN!

Now, nine months after my return, I have secured a very good, career-enhancing position. It's nice to have the better job now, but it would have been even nicer to have obtained it upon my return.

CIRC: AN INTELLIGENCE DATA BASE (U)

[redacted] T123

P.L. 86-36

(U) CIRC, which stands for Central Information Reference and Control, is a system of scientific and Technical (S & T) intelligence support which is operated under the auspices of the Defense Intelligence Agency (DIA) by the Foreign Technology Division (FTD) of the Air Force Systems Command (AFSC). The primary purpose of CIRC is to support the intenlligence information needs of the five DoD S & T intelligence productions agencies: the Naval Intelligence Support Center, the Army's Foreign Science and TEchnology Center (FSTC), Medical Intelligence Information Agency (MIIA) and Missile Intelligence Agency (MIA), and FTD. Access to the CIRC data base is available to other organizations, and NSA does have a CIRC terminal.

(C) CIRC means on-line access to almost 1.5 million documents, and another 3.6 million are available through batch searching. These 5 million records are available to NSA for retrospective research through the remote terminal, which is located in T1232 (Soviet Data Support Workcenter), Room 3W032, x5989s. For on-line searching the terminal converses directly with the computer located at FTD, at Wright-Patterson AFB, Dayton, Ohio, and retrieves document references and abstracts in response to search queries. CIRC provides document retrieval in a bibliographic sense, giving citations to documents relating to a given subject or author, rather than selected and sorted data ready for insertion into documents which the requester may be preparing. The intent is to furnish source material to be studied by the requester, who then has to decide the suitability and validity of the information. The user does not receive the document itself from the computer; instead, representations of the reference are retrieved, giving such things as title, date of report, report number or source, text extract, and ending with a list of specific surnames, facility names, and nomenclature designators occurring in the document. Should the requester need the entire document, T1232 can usually obtain it.

(C) A major difference which tends to separate CIRC from many other data bases is that CIRC does *not* use a controlled dictionary of terms or keywords. Virtually all the words in the extracts entered into the CIRC system are usable in searching, with the exception of some common words such as "both," "who" or latter," which contribute little to retrieval. Because of the free text type of search, use of broad terms will certainly lead to a high chance of irrelevant retrievals while obtaining all the essential coverage. Therefore, the requester should be prepared to screen a great deal of information to avoid missing anything that seems pertinent. The other extreme—very narrow terms—will usually render an output of mostly relevant documents but eliminating some valid ones in which the searched items are expressed differently in the referenced document from the search terms used — for example, searching for the SA-7 missile, but not for its nickname GRAIL, or looking for the nickname FISHBED, but not for MIG-21. If SA-7 or FISHBED were not in the reference, but GRAIL or MIG-21 were, the reference would not be retrieved. The indexer can only use terms that are precisely in the reference and is not to assume a relationship unless it is spelled out. Thus, there are problems in using narrow or specific terms without using synonyms or related terms to achieve full subject coverage.

DATA BASE CONTENT. Documents entering the CIRC data base contain information about *for-*

eign science and technology as it relates to U.S. Army, Navy and Air Force interests. All scientific disciplines, engineering specialties and technologies are represented as available. Worldwide coverage is maintained with emphasis on Communist countries. U.S. information is not included except when it is incidental to foreign data.

(U) Domestic and foreign open source publications are included in CIRC as well as classified messages, Intelligence Information Reports and other material of all classification levels up to TOP SECRET CODEWORD and TK. Army, Navy and Air Force finished technical intelligence publications containing analyzed information are entered into CIRC, as well as reports of some non-DoD agencies. The DoD S & T agencies also participate in obtaining information from other sources (such as NSA and CIA which do not submit reports directly to CIRC) for inclusion in the CIRC data base.

(S) About 83 percent of CIRC's on-line data bases and 93 percent of the total CIRC data bases—on-line and batch—comes from foreign literature, 4.7 million out of a total of 5 million references. In 1979 over 1350 subscriptions to worldwide publications were scanned for content selection for CIRC. This provides a great number of open source unclassified references to a broad spectrum of subjects, nomenclatures, facilities, and authors or personalities, which are available for search, again, worldwide in coverage, but with emphasis on Communist countries. The other 7 percent of CIRC, nearly 300,000 document records, includes finished intelligence reports, IIR's, sensor reports, and other

[redacted]

(U) Many of the open source references are not available for computer retrieval elsewhere, so this part of CIRC is largely unique. While the retrieved abstract is in English, most often the open source referemce will be in the original language. The reference in CIRC refers the requester to the original periodical, journal, newspaper or monograph for the complete article.

OFF-LINE PRINT ORDERS. Because the on-line terminal printer is slow, bibliographies are usually ordered from FTD for off-line printing and mailing to T1232 for forwarding to the requester. There is only one NSA on-line terminal; when it is receiving output from the computer, no searches can be initiated. Bibliographies classified up to SECRET take seven to ten calendar days from order to receipt in T1232. TSC/TK orders take two to three weeks, since they must be sent by courier, and there is only one courier flight per week from Wright-Patterson AFB to the Washington area. (If an order misses a flight, it must wait an entire week until the next one.) Thus, any request resulting in a number of retrieve references must allow ample time for the delievery of the data. FTD is hopeful that high speed printers will someday be installed at the principal CIRC user sites (including NSA), which will result in much faster delivery, usually by the next working day, and will free the remote on-line terminal for queries. Instead of printing and shipping by mail or courier, FTD will use the high speed printers for transmission of the bibliographies to the system-associated workcenter. No firm date for this enhancement is available, but FTD is hoping it will take place during late FY1980 or early FY1981. Where possible, T1232 will attempt more expeditious responses for high priority requests as appropriate.

P.L. 86-36
EO 1.4.(c)

PROFILES. One additional CIRC feature—the profile—is availble to requesters who want selected information on a current, recurring basis. A CIRC profile is a preselected canned query prepared for a requester and stored on-line at FTD. When the CIRC data base is periodically updated, prior to their being put on-line, the newly added documents are automatically compared with the profiles, and those documents which match the profile search statements are printed and sent on to the requester. A profile is a good way to maintain current awareness on a particular topic as material is added to CIRC. Queries may consist of terms, nomenclatures, personalities, failities or organizations, countries, source (such as a specific publication), or classification of the references. Queries may be as narrow or as broad as the requester desires. Profiles may be of any classification.

USING CIRC. CIRC usage at NSA has been increasing substantially over the last several years to the point where NSA is among the top five users of the data base. This is despite the fact that the availability of the data base within the Agency has not been widely publicized, because, in part, of computer downtime problems, which have led to feelings of uncertainty about response times.

(U) Use of CIRC can be cumbersome bacause the data base is so large it is broken into two segments: the afternoon, or classified, session where a full abstract of the reference is available for all classified references (TSC/TK material is available during this session only), and the morning, or unclassified session where a full abstract is available on-line only for unclassified references.

If a CONFIDENTIAL or SECRET reference is retrieved on-line is the morning session, only the microfiche number is given. This procedure is followed because not all terminals for the unclassified session are in secure locations, because a number of users have dial-up terminals which use unsecure telephone lines. Off-line bibliographies do print the complete abastracts of classified morning references.

(U) The morning unclassified session is so large that FTD's IBM 360/65 cannot contain all of the references, so it has been broken into three segments:

- CIRC, which consists of the CONFIDENTIAL and SECRET material, as well as the last two years of unclassified input. This is available on-line every morning except Wednesday.
- CIIO, which contains unclassified material entered into the system within the past two to five years. This is available on Wednesday mornings.
- ARCH, consisting of the archival data base of unclassified references which were input over five years previously. This material is available only for batch searches.

Thus a requester wanting complete coverage from all of CIRC might receive four separate outputs, all containing different references, from CIRC, CIIO, ARCH, and from SISA, the TSC/TK data base. Of course, searches can be limited by classification or by date span. The requester can limit his retrievals by indicating specific desires when making his request.

(U) The primary costs to NSA for the use of CIRC are the expenses of the 24-hour dedicated circuit to FTD, paper for the printer, the cost of the Teletype Model-40 Keyboard Display Printer, and the salary of the one analyst who spends most of her time doing CIRC-related activities. There is no charge for search time, printing or mailing, or for CIRC microfiche.

(U) All in all, CIRC is an excellent data retrieval system, which is to a considerable extent unduplicated by any other system.

* * * * * * * *

Analysts who have not been aware of the existence of CIRC, and who might have questions concerning the system, or who might wish further information on how CIRC retrievals of profiles could help them, should call the NSA CIRC remote terminal location, T1232, on 5989s, or drop in at Room 3W032, where T1232 personnel will attempt to answer their questions.

LIP (Continued from page 8)

(U) An interactive computer program has been developed on the LODESTAR system for use by the analyst/linguist. The program uses the technique discussed above, and has complete instructions for its use contained in the program itself. The program can usually identify the correct language in under three seconds of CPU time. For further deails, contact one of the authors.

Editor's note: Since the writing of this article, the data base has been expanded by the inclusion of the major languages of Europe.

(U) The authors feel that this "distancing" technique described here probably has other applications in addition to language identification. Readers who wish to discuss such applications are requested to call either Dr. [redacted]

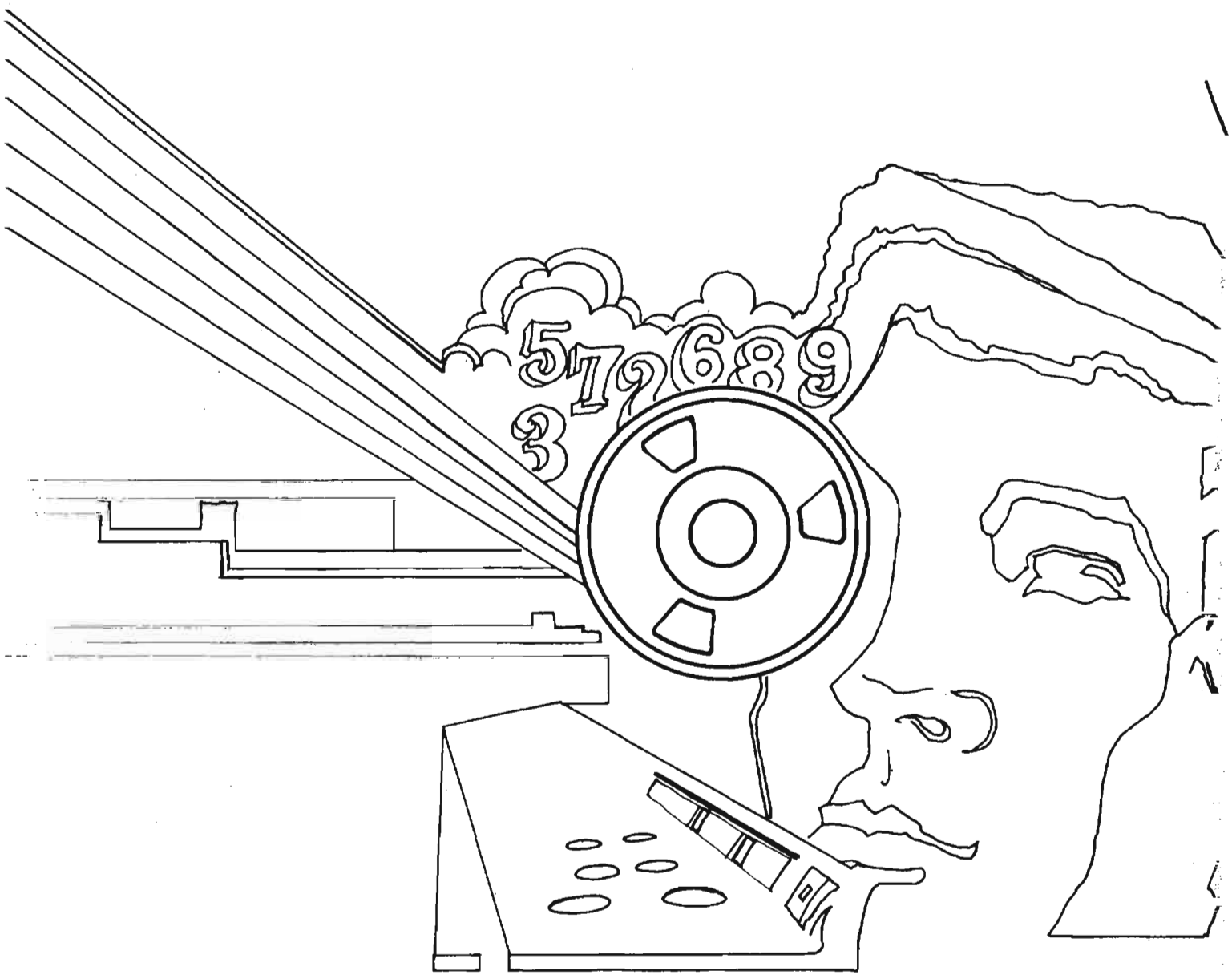
SOLUTION TO NSA-CROSTIC No. 29

"[A Proposed Cure for the] Time-in-Grade Syndrome," [redacted] CRYPTOLOG, November 1977.

"In general, promotion decisions [must] ultimately determine [just] who will make the key decisions within [an] organization. ...The initiative for promotion must belong to the managers and it is their responsibility to see that worthy personnel are promoted. It [must] be the employees' responsibility to qualify for promotion."

[redacted]

P.L. 86-36


5
7
2
6
8
9
3

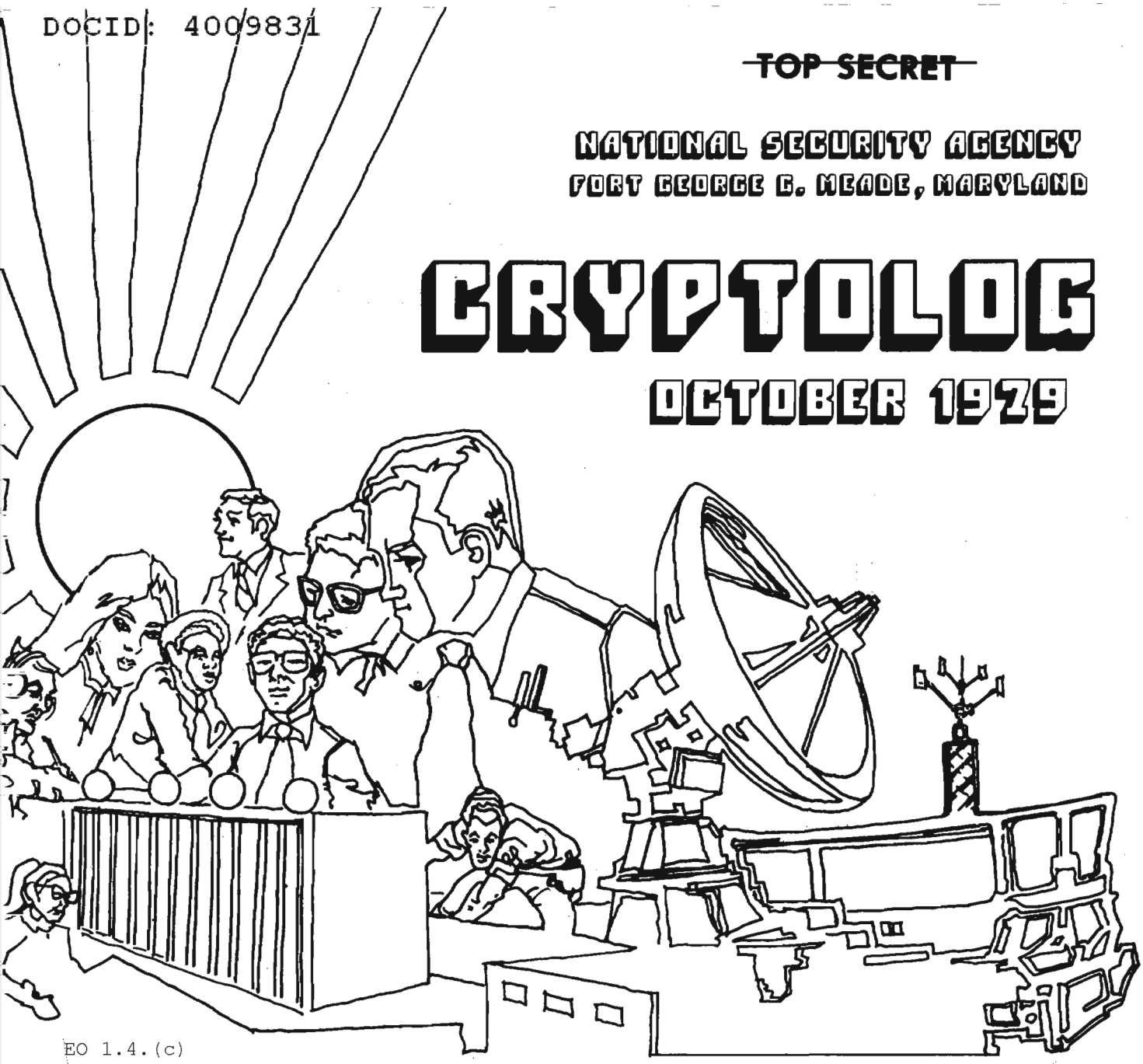
DOCID: 4009831

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

OCTOBER 1979



EO 1.4.(c)

P.L. 86-36

SNOWBALLS ON THE ROOF (U)	Vera R. Filby	1
[redacted]		8
ANOTHER SOURCE (U)	[redacted]	9
NSA-CROSTIC NO. 29 (U)	DHW	12
THE ROADS AROUND US (U)	[redacted]	14
THE 2000-YEAR-OLD TRANSCRIBER (U)	[redacted]	16
LETTER TO THE EDITOR (U)		19
CLUB NEWS (U)		11, 20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 1 OCT 2009~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL VI, No. 10 OCTOBER 1979

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor-in-Chief.....David H. Williams (1103s)

Collection..... [redacted] (8555s)

Cryptanalysis..... [redacted] (4902s)

Cryptolinguistics..... [redacted] (5981s)

Information Science..... [redacted] (3034s)

Language..... [redacted] (8161s)

Machine Support..... [redacted] 5084s)

Mathematics..... [redacted] (8518s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Taurone (3573s)

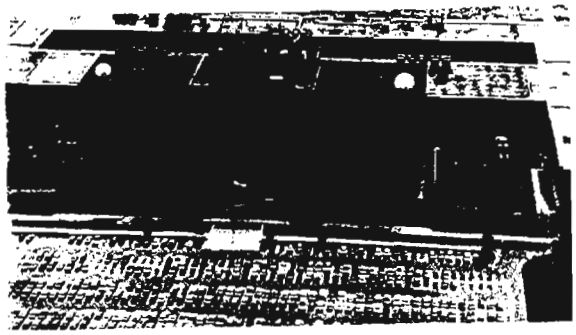
Illustrations..... [redacted]

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

Snowballs on the Roof

Vera Filby, E41



Every day thousands of NSA people see the snowballs, dishes, masts, and other odds and ends on and near our various buildings, and many of us have wondered what they are and what they do. *CRYPTOLOG* cannot provide all the answers, because some of these installations are experimental and sensitive, but we herewith offer you, dear Reader, our contribution toward an NSA Roofwatchers Guide.

(U) Roofwatching for most of us is more frustrating than rewarding because it's so hard to identify the objects that appear and sometimes later disappear. Birdwatchers have fieldbooks; even beginners can learn to tell starlings from grackles, and study of field marks will teach them that the little gray bird with the crest must be a titmouse. Wild plant fanciers have their fieldbooks too and can go on rambles with naturalists who know what they are looking at. Soon they can distinguish white oak from black, and they can tell the difference between tickseed and sneezeweed in September fields. And for other watchers there are manuals and even silhouette books for ships, boats, airplanes; even pictures of radars are not hard to come by. But fieldguides for antennas? There's no such thing.

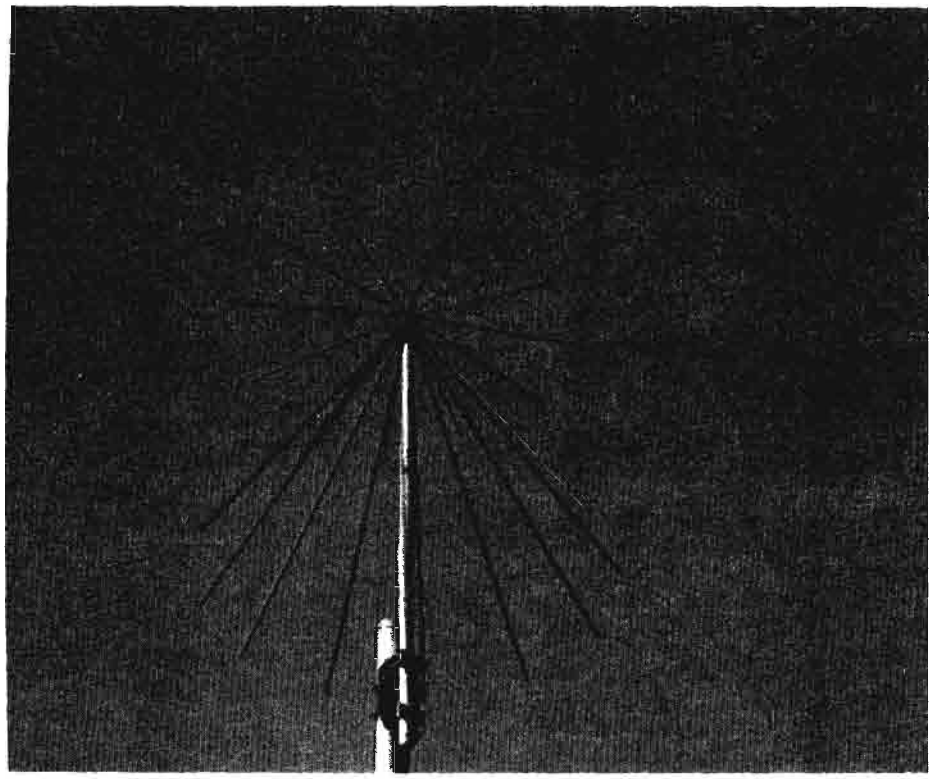
(U) Try the library. You can find lots of books on antennas, and some of them are supposed to be elementary. In them you will find copious data on radio wave propagation and an abundance of radiation diagrams and mathematical formulas. But pictures that identify and explain the mast with the flock of flying Vs on top or the thing that looks like an upside-down open-ended pyramid? Not so easy.

(U) But then nothing about antennas is easy, and the multiplicity of their design and the changing state of antenna art add to the complexity. Of types there are monopoles and dipoles, linear arrays, spiral and helical antennas, horn antennas, loop antennas, slot antennas, etc., etc. — with variations and combinations and modification. Besides that, terminology varies, and if in your guidebook hunt you should get hold of a British text, you would find yet another collection of terms.

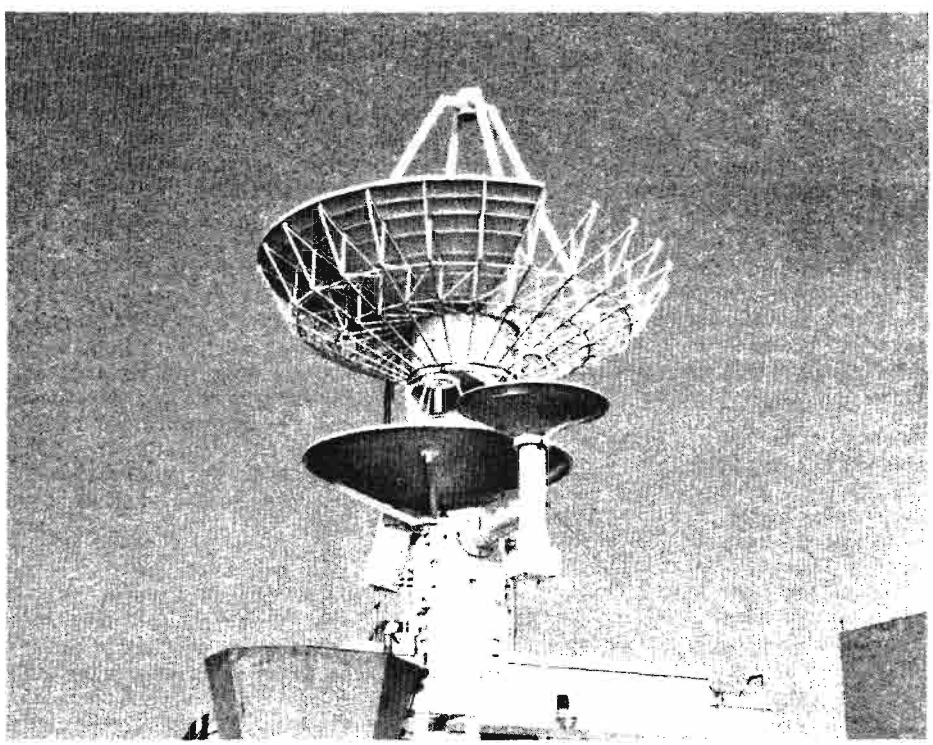
~~(S-CCO)~~ Nevertheless, anyone who understands antennas can tell a lot about an antenna just by looking at it, and a radio engineer doesn't need a security clearance to guess at the frequency range an antenna is designed for or even to deduce the target of an intercept site. Elliot Glunt of the Telecommunications and Computer Services Organization staff has a story to illustrate that. In World War II he was ordered to Guam to take charge of the Joint Communications Activity (JCA). It soon became apparent to him that there was considerably more communications activity on the JCA base than he had cognizance over. Since this was known as a "spook outfit," officially titled U. S. Naval Communications Supplementary Radio Station, direct questions as to the activity went unanswered. (Need-to-know, fences — that sort of thing.) By using some overgrown jungle trails, he made his way to their antenna field, where he saw, among other antennas, 27 rhombic arrays, all aligned for reception to the north and northwest, and an HF/DF array. It became crystal clear to that unindoctrinated viewer that the transmitting areas must be in Siberia, China, and Japan.

~~(C)~~ For the would-be roofwatcher and frustrated bookhunter, then, the best thing to do is ask people who know, and you couldn't do better than get acquainted with [redacted] of the Antenna Services activity, part of the Telecommunications and Computer Services Organization. The work center he directs is very small, but the job they do is very big. They are responsible for installing and maintaining the nearly 100 antennas on the roofs of

P.L. 86-36



Discone Antenna



One of the TRIO Antennas Under Construction

NSA's Fort Meade and Friendship Annex buildings, and more of them elsewhere. (We may get to "elsewhere" in future installments, especially if Bob flies us there in his glider or light aircraft.) This job entails, among many other things, support from contractors, since most of the equipment is commercially produced, and it can be rather more adventurous than most of us sedentary NSA types are accustomed to, as, for example, the installation of the big dishes on the south side of the old Operations Building on an icy pad by heavy helicopter on a winter day with snow threatening. Adding to the complexity of the job is the fact that the antennas on the roofs belong to a variety of "owners" — not only the Telecommunications and Computer Services and the Research and Engineering Organizations, as you would expect, but also many elements of Operations as well as Management Services, Installations and Logistics, Communications Security, and the National Cryptologic School.

~~(C)~~ Bob can take you for a tour of the Headquarters Building roof, an exhilarating experience on a bright winter day, with a sharp wind blowing and swirling white and gold clouds of vapor billowing out of the cooling towers, and nobody there to enjoy it but the pigeons, who unquestionably have the best view for miles around. Were they so inclined, they could observe a most interesting sight by peering down into the wooden towers through the warm, roiling mists at the slanted rim of icicles inside and the water churning in the dark below. Outside, great long icicles hang in the shadow of the tower walls. The towers are made of wood, by the way, because cedar and redwood withstand the changes of temperature and the effects of moisture more satisfactorily than anything else. Other objects on the roof include stairway penthouses, air-conditioning outlets, weather instruments, grounding rods, and TV cameras for monitoring the parking lots.

(U) But the most conspicuous roof decorations atop Headquarters Building are the big balls, variously referred to as snowballs, golfballs, or bubbles, among other names. Most of you will remember that there were once four of them. Now there are two, one at either end of the front, or west, side of the central building. One is a geodesic dome and the other an orange-peel. Of the other two, one was moved to the roof of FANX-III and the other was dismantled for refurbishing and future relocation. Domes like these, made of nylon or fiberglass skin on wood or aluminum frames, all transparent to radio waves, are designed for environmental protection, and the structure provides climate-controlled working space at the base for maintenance and repair. Obviously, they can also be used for concealment of their contents.

~~(C)~~ The highest platform on the roof is the penthouse top. It holds a parabolic dish which is sighted on another 4-foot dish on the FANX-III penthouse top. The two formerly served as backup for the gray phone system but are now being used for experimental work. Also mounted on the penthouse are discone, log periodic, whip and UHF/VHF antennas, and an anemometer. If you look down from your 9-story elevation to the north roof of the old 3-story building, you will see a cluster of antennas belonging to a staff element of the Operations Organization. A long-wire antenna cut to 32 MHz running along the north roof belongs to Telecommunications. On the east roof near the south end is another parabolic reflector. Then coming around to the south roof you have a spectacular view of a great white dish and two smaller ones, often sitting serenely in the "birdbath" position. They are the TRIO group, and they belong to an element of Operations.

~~(C)~~ A cozier way to look at the TRIO system is on the monitor screens inside the antenna room where the staff keeps watch on it. Records stored in the antenna room include a TV film of the installation of the heavy TRIO components — a real cliffhanger. (One event the film doesn't show was the episode of the bus carrying members of the NSA Travel Club, which got mixed up in the moving operations and couldn't get out.) We can't show you the film in *CRYPTOLOG*, so here instead is "The TRIO Story," by [redacted] Technical Manager, T2243.

P.L. 86-36

The TRIO Story.

~~(C)~~ TRIO consists of three separate antenna systems:

[redacted]

~~(C)~~ Installation required the cooperation of Scientific Atlanta (maker of the rotators and dishes), elements of the Operations, Telecommunications, and R & E Organizations, GSA, Fort Meade Military Police, safety officers, the fire department, the post rigger, and

EO 1.4.(c)
P.L. 86-36

contractors. The contractors involved included Washington Technological Associates, Inc., Carter Helicopter, and United Rigging Company. The expertly trained Army INSCOM antenna team bore the brunt of climbing tasks and worked beneath the helicopter during the main component assembly.

(U) The pad area was cleared off by Antenna Services and WTA. United Rigging hoisted the rotators, dishes, and tower atop the roof and positioned these parts on the pad. WTA mounted the horn and rotator on the roof pad. They also mounted the 8-foot tower. The rotator was attached atop the tower. The 3-foot and the 8-foot dishes were mounted on this rotator with the use of scaffolding and chain hoists.

(U) On the day of the helicopter lift, a Saturday, the building wing was evacuated. Television crews, guards, fire engine crews, photographers, installers, safety officers, and others went to work on a murky morning. The pedestal, which weighed 4,500 pounds was helicopter-lifted into place and bolted down. The rotator, weighing 7,500 pounds, made the helicopter strain (its maximum capacity is 8,500 pounds). It was hoisted into place on top of the pedestal without a hitch. The two counterweights, weighing a ton each, were then lifted into place 16 feet above the elevator housing. The total time to lift and bolt into place was 50 minutes — preceded by weeks of planning and coordination.

(U) The 24-foot dish arrived three weeks later. It was raised to the roof by a Fort Meade crane. We were assisted by the INSCOM installation team and NSA volunteers. During this phase, March winds and freezing rains caused delays.

(U) All cabling and testing were completed by NSA personnel and specialists from the various equipment suppliers.

(U) The total preparation and installation time required (excluding pad fabrication) was 752 hours: 240 on the part of INSCOM, 222 by contractors, and 290 by NSA personnel.

* * * * *

~~(C)~~ To the west of the TRIO array, near the end of the south roof, stretch two series of loop antennas. These are Hermes aperiodic loop antenna systems designed as broadband receiving sensors for signals in the 2 - 30 MHz range. Since these are active antenna systems, they have the advantage of requiring less real estate than rhombics or log periodics without sacrificing signal gain. Directivity and beamwidth pattern is a combination of their orientation and of their end-fired termination.

[redacted]

P.L. 86-36
EO 1.4.(c)

[redacted]

~~(C)~~ As you look out from your airy platform, three towers punctuate the view. On your right, to the southeast in the direction of S Building near the motor pool, is a tall tower with a reflector on top for line-of-sight microwave signals. The transmitting equipment is at the bottom of the tower. The signal could be transmitted through a cable, but since this would cause some signal loss, it is transmitted through space to the reflector, which aims it towards NSS, over on Nebraska Avenue. This is part of the old gray phone system and is a standard type of Western Union relay operated by the Chesapeake and Potomac Telephone Company.

EO 1.4.(c)
P.L. 86-36

~~(C)~~ Scanning counterclockwise you will next sight a tower which is on Cooper Avenue. It is part of the Military Affiliate Radio System (MARS), an organization for amateur radio operators in the services, and thus not part of our story. The next tower you see, however, is very much part of the story. Located on Rockenbach Road, it was built under contract with Western Union and is part of the Washington Area Wideband System (WAWS). What you see is a 360-foot tower painted the conventional vermilion and white, with parabolic dishes mounted at various intervals along the top half and aimed in various directions. The flat covers over the faces of the dishes are for weather protection, and the cylinder between the reflector and the cover helps to reduce side lobes. The tower is connected by fiberoptics to the communications center in the main building. WAWS will interconnect NSA, NSS, the Pentagon, Andrews AFB, Fort Detrick, and several other stations. Its capabilities are beyond anything we have ever had before

[redacted]

WAWS and its capabilities are so important to us that we plan to provide you with an article about it in a future issue of *CRYPTOLOG*.

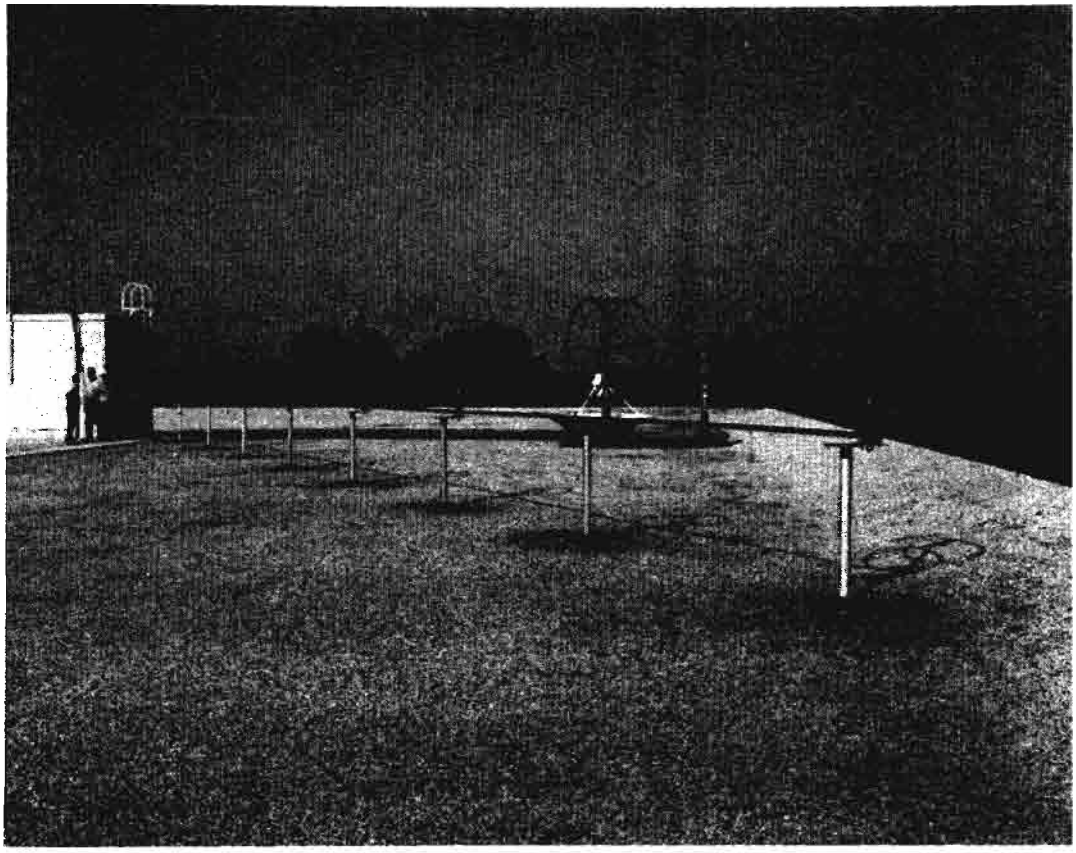
(U) WAWS is also connected with another array you can see from your rooftop viewpoint. Down below, to the east-southeast, loom the twin white dishes of DARING DUO, which also deserves a story of its own, and we hope to provide that for you too.

~~SECRET~~

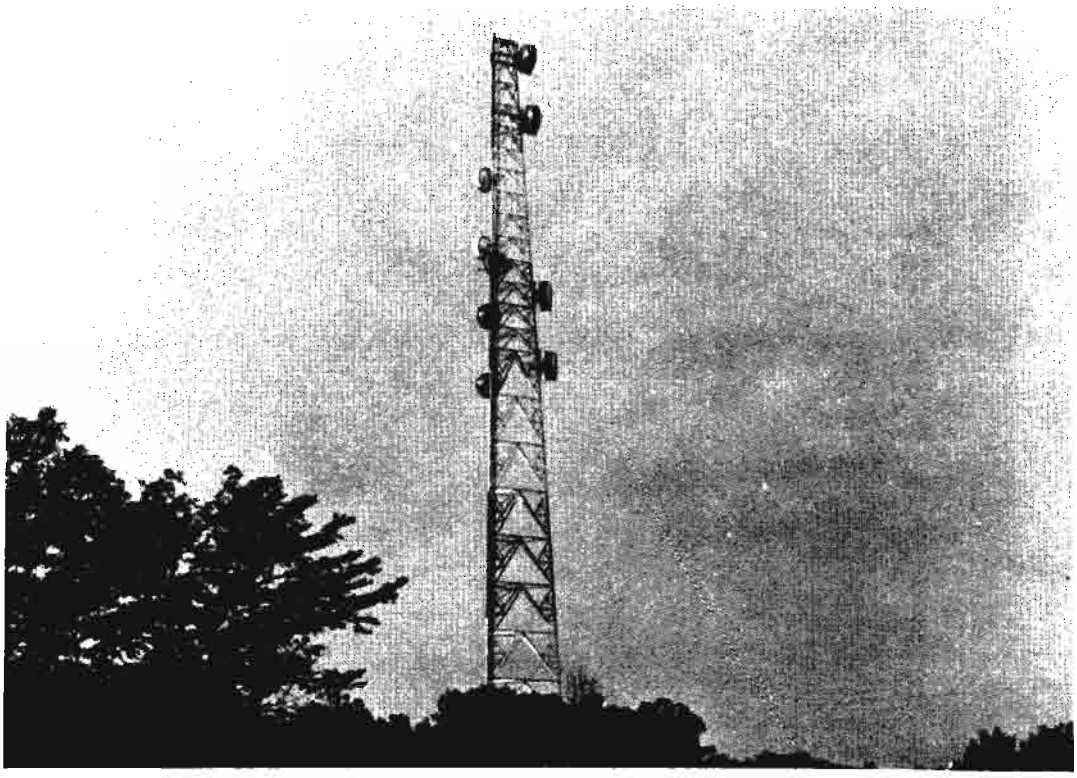
DARING DUO (U)

EO 1.4.(c)
P.L. 86-36

~~SECRET~~



Hermes Antenna



WAWS Tower

~~(C)~~ From any point of view the panorama of NSA's towers and masts and globes is quite fascinating (a poor man's Taj Mahal, said Brigadier Tiltman when we told him about our project), and those who do most of their roofwatching at FANX can observe changing skylines there too. We can enthusiastically recommend an excursion to the FANX-III roof with antenna experts like [redacted] of Research and Engineering and [redacted] of the School, especially on a sunny, breezy April afternoon with unlimited visibility. If you look west across the airport road you will see the low elevation that might have been the Cupola Hill of an earlier day. Now it supports navigational radars for BWI Airport. Off in the distance to the left is the MARS tower, then the WAWS tower, then a water tower, and then, to the south and southeast is the expanse of the airport. Round about you on the roof are such bits and pieces as the exhaust outlets for the boilers and the medical center, roof drains, metal grid walkways, and the aircraft warning beacons required by the FAA. But these are not the objects of our interest. The biggest such object is the lone white ball. It is part of the Research and Engineering antenna facility, although permission was given to Security to install two-way radio in this structure. Beside the ball on the same platform, and part of the same Security communications system, is a very long fiberglass whip antenna with an aircraft warning marker on top. Near the big ball is a 3-element yagi antenna, and if you stand behind it and look where it seems to be looking you will find yourself staring at the WAWS tower. Nearby is a round loop antenna with a center bar, probably designed for the HF or VHF range, and there is also a VHF/UHF TV array. Nearer the penthouse, which stands in the middle of the roof, is a very large parabolic dish with a protective cover on it and shrouded sides to suppress side lobes. The cover has the red flash marking of the Andrews Corporation painted on it. This dish is part of the WAWS. A much smaller dish near the south edge of the roof also has the red flash mark. Nearby is a DF-type loop with a rotator.

(U) Up on top of the penthouse at the highest elevation is another flash-marked parabolic dish. This is the one that looks at its mate on the Headquarters Building penthouse. The penthouse roof also holds a small whip antenna, a shelter for temperature and humidity instruments, and an anemometer. A most conspicuous feature up there is the big discone, mounted point down, with its ground plane rods radiating beyond the edge of the penthouse roof. The rays have a coppery gleam, but they are made of anodized aluminum. At the north end of the east side of the FANX-III roof there is a short dipole antenna, then a long dipole strung along the rest of the east side, then a long wire running diagonally from the southeast corner past the penthouse to the northwest. On the edge of the front side, the south, are two 3-element yagis, one a little larger than the other.

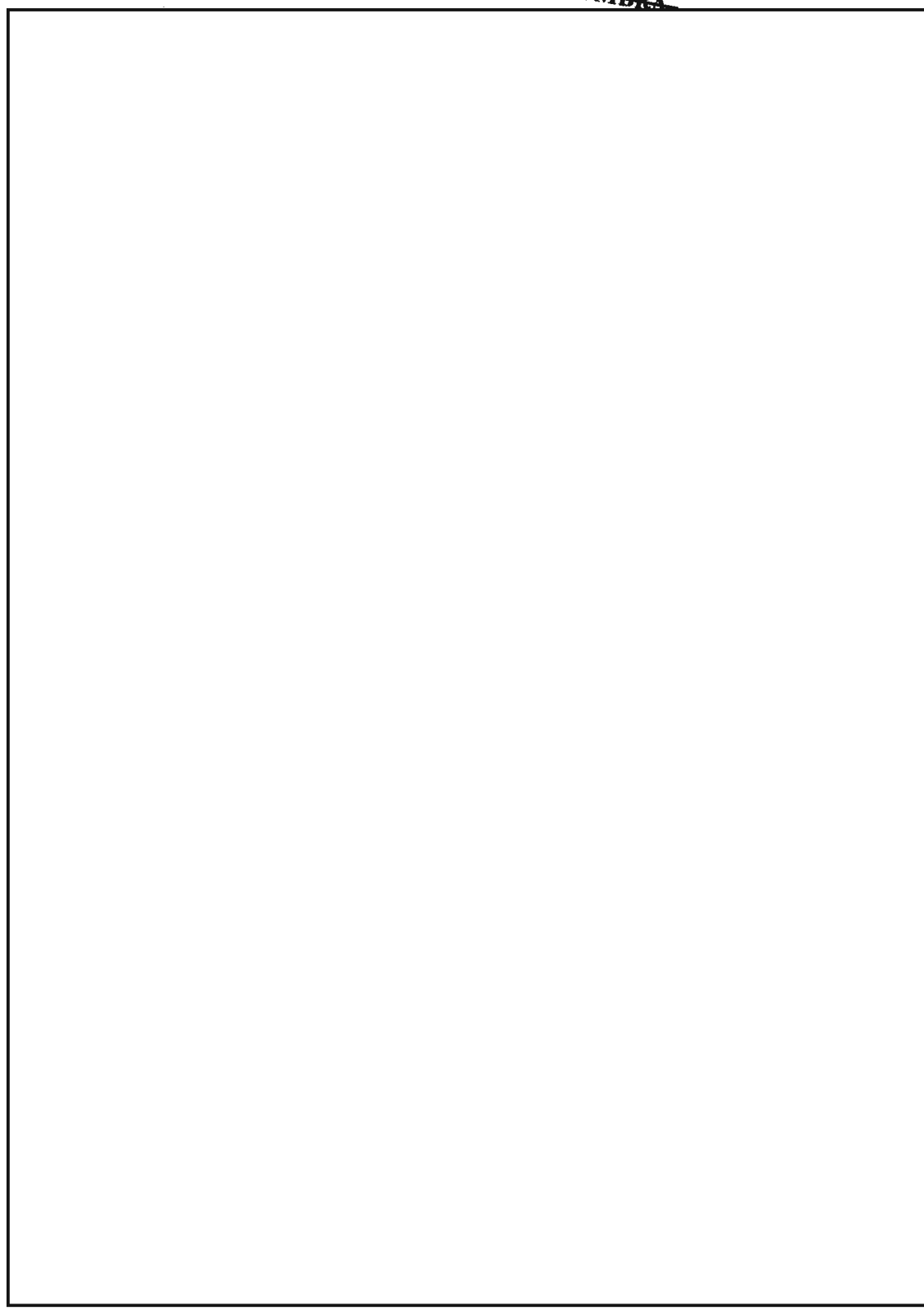
P.L. 86-36

~~(S)~~ If you look down past the yagis to the left, you will find yourself gazing at the roof of FANX-II and the long black object on it. The building consists of two parts joined to make a Z-shape, and the black thing slants across the Z-bar to gain a length of about 600 feet. There was a good deal of speculation as to what might be going on when it and the little houses at its ends were under construction: executive escape hatches, special horizontal burnbag disposal [redacted] for elves... [redacted] and it belongs to Research and Engineering, and that's all we can tell you about it. Anyway, it may have had one effect we heard suggested: it may have given the Russian photo analysts something to think about.

~~(S)~~ Besides the tunnel, the most notable things on the FANX-II roof are the six condensing units for the air conditioning cores in the building, but there are antennas there too. In between the second and third units are three vertical gray fiberglass-domed cylinders standing on supports and all mounted on a platform. [redacted] They are being used for training. Other antennas on the roof, some of them also used for training, include long-wire antennas, small discones (point up) and a large one (point down). Small discones are designed for VHF/UHF and the big ones for HF. Discone antennas are omnidirectional and can cover a broad band, up to several MHz. With backscatter they can receive signals from well over the horizon. VHF/UHF discones are much used for communicating with aircraft.

(U) When next you glance up at the NSA skyline, no doubt you will see that things are not quite as we have described them. But changes are always under way. New equipment was being installed and old equipment removed even as this article was in preparation. We hope nevertheless that it contributes to your interest in roofwatching.

DOCID: 4009831



EO 1.4.(c)
P.L. 86-36

ANOTHER SOURCE

[redacted] L12

P.L. 86-36

Undoubtedly the most common method of acquiring new equipment here at NSA is through conventional procurement channels. But there is another source of supply for equipment sorely needed by our operational elements, one which avoids the anxieties and tensions which so often attend programming actions, such as the justifying of requirements, the competing for budget dollars, and the long waiting periods usually associated with procurement procedures. L1, the Office of Materiel Management, has the equipment for the asking.

Of course, there is a catch. The equipment is in most cases not brand new. But it is available without cost and it can be delivered quickly, usually within a week of the request. It is equipment which L12, the Plant Property Division, advertises on the excess bulletins which are published periodically and distributed widely. Even though nearly two hundred copies of these bulletins are distributed, there are still people who need equipment but do not know about them.

Throughout the federal government there are thousands of organizations that come up with excess equipment, for any of several reasons: the job for which the equipment was procured may cease to exist; newer equipment may supplant the original inventory; jobs, positions, or entire organizations may be disestablished; or any of a hundred other reasons may arise to eliminate equipment requirements. When equip- becomes excess in the Department of Defense, it is reported to the Defense Property Disposal Service (DPDS) for appropriate reutilization screening throughout the government.

Before equipment is transferred to the DPDS by way of a local area Property Disposal Office, it is advertised to the Cryptologic Community through L12's excess bulletins. There are two series of these — the inhouse bulletins, numbered in the 400s, contain information on equipment turned in by the NSA elements (including field facilities); and the "out-house" series (a term we have been asked not to use), numbered in the 100s, cover equipment reported by the SCAs as well as NSA. NSA SIGINT equipment is advertised in both series. Since the bulletins are issued alternately, much equipment is available to NSA elements 30 days before it is advertised to the community at large. You may, of course, request equipment from either series.

During FY-79 NSA's participation in the reutilization program resulted in a saving of nearly five and a half million dollars. Specifically, 336 items were reused reflecting a saving of $5,458,102. Throughout the community, the total was closer to six million dollars (436 items, $5,870,634). These figures do not reflect the value of the equipment involved, but rather the amount that would have had to have been spent to replace it. This in itself may be misleading: the dollar value shown in the reutilization of an AN/TNH-11 recorder/reproducer is approximately $1,100, but you can no longer buy a new TNH-11. If a replacement machine must be purchased, it will have to be an AN/TNH-21 at $5,000, more or less. Thus, when a TNH-11 is recycled, our figures will reflect a saving of $1,100, where the actual saving might have been closer to $5,000.

We are not limited to the Cryptologic Community for our equipment. You may request equipment from other government agencies. For example, during CY-79 one element obtained 46 items through DLA Excess Personal Property Listings, reflecting a saving of $162,674. This external program may be the subject of a future article.

How do you determine the condition of a piece of equipment on the excess list? That's a reasonable question that deserves a better answer than is currently avail-

able. The honest answer is that you just don't know — for sure. Each excess list contains a column listing the condition code for each item. Our in-house bulletins use the GSA condition codes which provide a reasonably well defined statement of the actual condition of the equipment — or a potential for a well defined statement. Unfortunately, many managers declare their excess property as O-3 (fair and usable without repair), regardless of its actual condition. We suspect that this usage is frequently the result of the rater not knowing the breakdown of the codes. In an effort to dispel some of the mystery, L122 included a list and explanation of these codes with the Cryptologic Community SIGINT/ADPE Excess Bulletin No. 139.

In the Cryptologic Community bulletins the condition codes are simply A or F. These letters do not stand for "awful" and "foul" as some people have suggested, but relate to the GSA condition codes as shown it the chart. Essentially, a rating of A indicates equipment, whether new or used, which is in excellent or good condition, while F denotes excellent or good equipment requiring repair, or or equipment which is fair to poor.

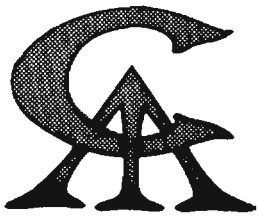
To quote from a recent DLA newsletter:

> In today's climate of belt-tightening and limited budgets, it is essential that all of us explore every possible means of saving or stretching dollars and other resources. One of the best ways to accomplish this is through the reutilization of Department of Defense excess property. Activities which are not now participating in the DoD Reutilization Program are strongly encouraged to begin doing so; and activities which are already reutilizing excess property are urged to seek ways to obtain and use even more of it. In either case, the informed and systematic use of excess materiel from the Defense Property Disposal Service can significantly reduce expenditures for new procurement as well as the delivery time needed to actually get items in hand.

If you have any questions about excess property or the Reutilization Program, please call L122, 7264s/7906b.

CONDITION CODES AND EXPANDED DEFINITIONS

CRYPTO COMM	Condition Code	Expanded Definition
A	N-1	New or unused property in excellent condition. Ready for use and identical or interchangeable with new items delivered by a manufacturer or normal source of supply.
A	N-2	New or unused property in good condition. Does not quite qualify for N-1 (because slightly shopworn, soiled, or similar), but condition does not impair utility.
F	N-3	New or unused property in fair condition. Soiled, shopworn, rusted, deteriorated, or damaged to the extent that utility is slightly impaired.
F	N-4	New or unused property so badly broken, soiled, rusted, mildewed, deteriorated, damaged, or broken that its condition is poor and its utility seriously impaired.
A	E-1	Used property but repaired or renovated and in excellent condition.
A	E-2	Used property which has been repaired or renovated and, while still in good usable condition, has become worn from further use and cannot qualify for excellent condition.
F	E-3	Used property which has been repaired or renovated but has deteriorated since reconditioning and is only in fair condition. Further repairs or renovation required or expected to be needed in near future.
F	E-4	Used property which has been repaired or renovated and is in poor condition from serious deterioration such as from major wear and tear, corrosion, exposure to weather, or mildew.
A	O-1	Property which has been sightly or moderately used, no repairs required, and still in excellent condition.
A	O-2	Used property, more worn than O-1 but still in good condition with considerable use left before any important repairs would be required.
F	O-3	Used property which is still in fair condition and usable without repairs; however, somewhat deteriorated, with some parts (or portion) worn and should be replaced.
F	O-4	Used property which is still usable without repairs but in poor condition and undependable or uneconomical in use. Parts badly worn and deteriorated.
F	R-1	Used property still in excellent condition, but minor repairs required. Estimated repairs would cost no more than 10% of acquisition cost.
F	R-2	Used property in good condition but considerable repairs required. Estimated cost of repairs would be from 11% to 25% of acquisition cost.
F	R-3	Used property, in fair condition, but extensive repairs required. Estimated repair costs would be from 26% to 40% of acquisition cost.
F	R-4	Used property, in poor condition, and requiring major repairs. Badly worn, and would still be in doubtful condition of dependability and uneconomical in use if repaired. Estimated repair costs between 41% and 65% of acquisition cost.
	X	Salvage. Personal property that has some value in excess of its basic material content but which is in such condition that it has no reasonable prospect of use for any purpose as a unit (either by the holding or any other Federal agency) and its repair or rehabilitation for use as a unit (either by the holding or any other Federal agency) is clearly impractical. Repairs or rehabilitation estimated to cost in excess of 65% of acquisition cost would be considered "clearly impractical" for purposes of this definition.
	Scrap	Material that has no value except for its basic material content.



COMMUNICATIONS ANALYSIS ASSOCIATION

PRESENTS

ITS FIRST ANNUAL CONFERENCE
ON
COMMUNICATIONS ANALYSIS

THEME:

"THE ANALYST IN THE 80's"

CONFERENCE WILL BE HELD ON THE 15 & 16TH OF OCTOBER 1980,

AT 0900 TO 1200 HOURS, IN THE FRIEDMAN AUDITORIUM.

THE THEME REFLECTS CONCERN OVER THE IMPACT THAT MANPOWER CONSTRAINTS, CHANGES IN THE WORKFORCE, AND THE EVOLUTION OF THE COMMUNICATIONS AND TECHNOLOGICAL ENVIRONMENTS WILL HAVE ON ANALYSTS IN THE FIELDS SERVED BY CAA.

CAA INVITES AGENCY PERSONNEL TO SUBMIT PAPERS OR ABSTRACTS FOR PRESENTATION AT THE CONFERENCE. SUGGESTED TOPICS INCLUDE:

- **THE ANALYTIC RESPONSE TO A CHANGING ENVIRONMENT.**
- **SIGINT OPERATIONS, 1980 - 1990**
- **THE ANALYST AND AUTOMATION**
- **THE FUTURE OF TRAFFIC ANALYSIS**
- **COMSEC: CHALLENGES AND RESPONSE**
- **SIGINT REPORTING: THE CHANGES AHEAD**
- **INTEGRATING CRYPTOLOGIC DISCIPLINES**
- **THE DOCUMENTATION OF TARGETS & SOLUTIONS**
- **THE IMPACT OF PUBLIC CRYPTOGRAPHY**

PAPERS OR ABSTRACTS OF PAPERS ON THESE OR OTHER TOPICS SHOULD BE SUBMITTED BY 31 MARCH. FOR INFORMATION CONTACT BILL NOLTE, G77, 5A122 (5202s)

DOCID: 4009831

NSA-Crostic No. 29

by D. H. W.

The trigraphs used in this puzzle are the standard codes for various North American airports. There are used here to represent either the airports themselves, or the cities which they serve. Happy landings!

A. BNA: Robert Altman film

26 144 30 157 112 48 60 40 70

B. When the 7:52 plane is supposed to leave (3 wds)

208 16 91 56 54 44 137 6 24 135 67 34

C. INT: City named after two cigarettes (comp)

81 1 166 193 183 204 5 232 87 240 178 259

D. Pertaining to an ancient people of Asia Minor

181 94 242 215 168 38 45

E. MCO: Tony's last name

194 118 171 182 100 151 206

F. Snobbishly arrogant (sl)

52 190 117 237 156 226

G. SAT flower (3 wds)

148 149 235 63 196 153 185 2 262 165 160 176

27 4

H. That which gives forth

231 126 152 136 175 113 200

I. YYZ: Largest city in the nation (2 wds)

187 225 161 133 264 180 17 99 195 244 37 203

250 234

J. Disability; frailty; moral weakness

98 88 253 35 90 47 77 138 243

K. MSP: Northern twin

13 172 86 79 221 92 256 115 9 210 53

L. Furnishes

146 246 32 170 233 177

M. Incorrect; irregular

154 212 164 230 263 223 73 192

N. ____ DTW: Character from *Guys and Dolls* (2 wds)

134 142 83 219 96 105 72 50 66 11 254 59 122

O. Farewell to CMH (2 wds)

3 89 57 42 169 71 39 21 12 132 213 141

238 127 80

P. Permission to pass (3 wds)

7 85 145 139 101 14 114 184 199 41

Q. ABE: Cities served by this acronymous airport (3 wds)

8 249 224 179 18 31 78 58 49 130 65 97 84

33 103 188 20 205 191 109 163 129 119 143

R. Make smaller

19 241 36 82 150 108 76 102

S. Arab prince

228 62 239 147

T. Champions from SEA (2 wds)

U. OYS: Major western U.S. tourist attraction

V. Person who might depart from LGA, JFK or EWR (2 wds)

W. Unpleasant task (2 wds)

X. YRB: Northernmost airport of America

Y. One who habitually expects the best possible outcome

Z. Square peg in a round hole

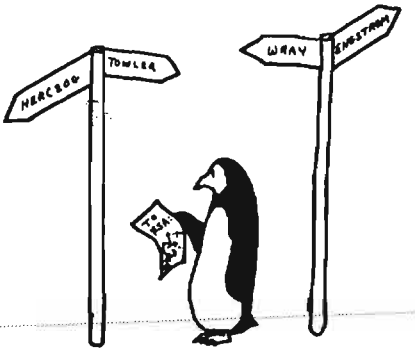
a. EEK: Small Alaskan town served by this airport

214	201	248	207	261	198	131	229	29	10	220	186									
		167	25	125	159	74	236													
252	260	155	158	120	106	173	140													
93	227	55	189	124	116	69	217	257												
209	22	46	110	174	51	121	216													
255	68	128	258	61	247	107	43													
245	202	15	75	222	111	95	218													
28	123	23	251	104	211															
197	162	64																		

1 C	2 G	●	3 O	4 G	5 C	6 B	7 P	8 Q	9 K	●	10 T	11 N	12 O	13 K	14 P	15 Y	16 B	17 I	18 Q
●	19 R	20 Q	21 O	22 W	23 Z	24 B	25 T	26 A	27 G	●	28 Z	29 T	30 A	31 Q	●	32 L	33 Q	34 B	35 J
36 R	37 I	38 D	39 O	40 A	41 P	●	42 O	43 X	44 B	45 D	46 W	47 J	48 A	49 Q	50 N	●	51 W	52 F	53 K
54 B	●	55 V	56 B	57 O	●	58 Q	59 N	60 A	61 X	●	62 S	63 G	64 a	65 Q	●	66 N	67 B	68 X	●
69 V	70 A	71 O	●	72 N	73 M	74 T	75 Y	76 R	77 J	78 Q	79 K	80 O	●	81 C	82 R	83 N	84 Q	85 P	86 K
●	87 C	88 J	●	89 O	90 J	91 B	92 K	93 V	94 D	95 Y	96 N	97 Q	98 J	99 I	100 E	●	101 P	102 R	103 Q
●	104 Z	105 N	106 U	107 X	108 R	109 Q	110 W	111 Y	112 A	113 H	●	114 P	115 K	116 V	●	117 F	118 E	119 Q	120 U
121 W	122 N	123 Z	124 V	125 T	●	126 H	127 O	128 X	129 Q	●	130 Q	131 T	132 O	133 I	134 N	135 B	●	136 H	137 B
●	138 J	139 P	140 U	●	141 O	142 N	143 Q	144 A	145 P	146 L	147 S	148 G	●	149 G	150 R	151 E	●	152 H	153 G
●	154 M	155 U	●	156 F	157 A	158 U	159 T	160 G	●	161 I	162 a	163 Q	164 M	165 G	166 C	167 T	168 D	169 O	170 L
171 E	172 K	173 U	174 W	●	175 H	176 G	●	177 L	178 C	179 Q	●	180 I	181 D	182 E	183 C	●	184 P	185 G	186 T
187 I	188 Q	189 V	●	190 F	191 Q	192 M	193 C	194 E	195 I	196 G	197 a	198 T	●	199 P	200 H	201 T	●	202 Y	203 I
204 C	205 Q	206 E	207 T	208 B	209 W	●	210 K	211 Z	●	212 M	213 O	214 T	215 D	●	216 W	217 V	●	218 Y	219 N
220 T	●	221 K	222 Y	223 M	224 Q	225 I	226 F	227 V	228 S	229 T	●	230 M	231 H	232 C	233 L	234 I	235 G	236 T	237 F
238 O	239 S	240 C	241 R	242 D	243 J	●	244 I	245 Y	●	246 L	247 X	248 T	249 Q	250 I	251 Z	252 U	●	253 J	254 N
255 X	●	256 K	257 V	258 X	259 C	260 U	261 T	262 G	263 M	264 I	C	R	Y	P	T	O	L	O	G

DOCID: 4009831

The Roads Around Us



by [redacted] P1

P.L. 86-36

Not many of us can accurately name the four roads which surround the HQ and Operations buildings at Fort Meade, and yet this information is in the public domain. Legible signposts exist for all to see, yet, as Holmes remarked to Watson, "You see, but you do not observe." (Quick now, try naming these roads yourself.)

Feeling that the exploits of the men for whom these roads were named should not be wholly forgotten, I have prepared the following notes on what could be learned after the passage of so many years. Further information from readers would be welcomed. rc.

HENRY J. HERCZOG

After serving an an officer in the US Army Signal Corps from February 1943 to June 1946, Mr. Herczog joined a precursor of NSA as a civilian in July 1946. He served NSA with distinction until his premature death at the age of 40 on 4 September 1960. During his career with the Agency he received a number of letters of commendation for high performance in important missions and for his professional competence and technical abilities. He played an important role in developing and furthering a number of Agency programs, and was described by RADM Kurtz as "extremely competent and sincerely motivated...a natural leader."

Mr. Herczog also found time to serve as President and later Chairman of the Board of the Government Employees Benefit Association (GEBA). He wit and friendliness made him popular, and as a speaker he was among the best.

The road that runs from east to west past Gatehouse 4 is named in his honor and memory.

HOWARD T. ENGSTROM

After attaining the rank of Captain in the Navy during World War II, Mr. Engstrom, along with LCDR William Norris and others returning to civilian life after serving in the Navy's CSAW (Communications Supplementary Activity, Washington) were successful in forming a private company — Engineering Research Associates. ERA set up shop in St. Paul, Minnesota, and was kept going by US Navy contracts covering such specific tasks as building special purpose electronic data processing devices and research on data handling and storage techniques.

From NSA's point of view the significance of all this was ERA's successful design and construction of the ATLAS computers, an affair which kept Mr. Engstrom in contact with the higher officials of NSA. He joined Remington Rand when that company bought out ERA in 1952, and became a member of the NSA Scientific Advisory Board. After Remington Rand in turn merged with Sperry Gyroscope to become Sperry Rand, Mr. Engstrom took leave from his company to serve NSA, first as Deputy Director of Research and Development (1956 - 1957), and then as Deputy Director of NSA (1957 - 1958). After returning from NSA to become a vice president at Sperry Rand in 1958, he was awarded the first NSA Exceptional Civilian Service Medal on 17 February 1960.

Historian Samuel Snyder tells of the meeting held on 10 March 1958 to discuss the HARVEST concept. After Snyder and others argued in favor of HARVEST, Mr. Engstrom spoke strongly against it. He was overruled by then-Director LGEN Samford. (There are those who still think his advice was the best in the HARVEST case.)

From the eulogy printed in the NSA Newsletter following his death in March 1962, we take the following:

He will be remembered by his many friends in NSA as a big man in every respect, never failing to greet and show a warm and cordial interest in the affairs of others, though he was always preoccupied with solutions to many difficult problems.

The road that runs from north to south past Gatehouse 1 is named in his honor.

WILLIAM D. WRAY

In early 1942 Dr. Wray came to the Navy Department as a Mathematician, Grade P1, the grade given in those days to college graduates with bachelor's degrees. (His PhD in applied statistics was ignored.) He and Dr. Robert E. Greenwood were almost the only civilians in their working area, and the atmosphere on the job was not pleasant. But Dr. Wray had contended with handicaps since a childhood illness had left him with permanent medical problems. Patriotic conviction kept him with the Navy. His refusal to be discouraged proved itself on many occasions and commended him to everyone. He came to be a confidant and advisor to many.

Dr. Wray's steady good judgment, his objective steadfastness and his ability to get along with people and encourage them made him a good administrator. He was steadily advanced, and his early death, at 52, in 1962 was a serious loss to NSA as well as to his family and friends.

The road that runs from west to east past Gatehouse 2 is named in memory of Dr. Wray.

COL HARRY E. TOWLER, USAF

A member of the US Air Force Security Service, COL Towler served as Vice Chief of Staff. 1950 - 1953. He was then assigned as Commander, 6950th Security Group, Chicksands Priory, England, where he served until 1956. He was then named Chief AFSSFM/GENS-3, under an arrangement in which the Director, NSA, exercised management in partnership with the Chiefs of the SCAs. In both roles COL Towler interacted daily with members of many Agency elements, at all levels, while remaining responsible to Commander, USAFSS, Kelly AFB, San Antonio.

A memoir received from then-SSGT Billy J. Baker includes the following comment:

I remember COL Towler as being the finest commander it was my privilege to serve under in my 21 year military career. He was a large man who tempered his military bearing...with a fatherly concern for the welfare of all his men.

At a masquerade ball at the Chicksands NCO Club in 1954, COL Towler created a memorable impression by appearing as Henry VIII, his rotund figure covered with jewel-encrusted velvet, his eyes winking merrily atop a flaming red beard as he gave the wives the opportunity to dance with a king.

The road running from north to south past Gatehouse 3 is named in his memory and honor.

My thanks to Howard Campaigne, Sam Snyder, [redacted] for help with these vignettes of the past. rc

P.L. 86-36

* * * * * *

NCS SUMMER LANGUAGE PROGRAM

Applications are currently being accepted for the Agency's Self-Help in Language Growth Program for the summer of 1980. This program is designed to upgrade the skill of linguists through full-time summer language programs at accredited academic institutions. such as Middlebury (Vt.) College, the University of Illinois, etc. Students receive full pay, but all other expenses are their own responsibility. Individuals approved are issued "permissive" TDY orders which authorize time off only. They must make their own travel and housing arrangements.

To qualify, an applicant must

★be an NSA civilian career employee with at least two years of SIGINT experience of equivalent military experience.

★request training in the language in which he is currently working, or in a language designated by management as necessary to the Agency's mission

★possess certain minumum language proficiency qualifications

★be accepted by the school of his choice

Applicants should submit an External Training Request (Form E5824) through channels to the Registrar, NCS (E81), by 30 April.

DOCID: 4009831

The 2000-Year-Old Transcriber

A04

P.L. 86-36

Some veteran professional athletes have been trying to hang on with their teams into the 1980 season, in order to say that they played in four decades — the fifties, sixties, seventies and eighties. It made me realize that there are some people around who have been associated with voice transcription at the Agency and in the field during those same four decades. Thinking that it might be useful to document the changes that have taken place in transcription over the years, I set out to interview the 2,000-year-old transcriber.

I found him, sunning himself outside his cave in the woods beyond the Ft. Meade rifle ranges. He readily agreed to the interview, and we spent a pleasant afternoon retracing years of transcription history, our conversation broken occasionally by the fire of weapons on the ranges or the passing of a Metroliner on the nearby railroad tracks. A transcript of that interview follows.

Q. Sir, could you tell me about the transcription organizations of old?

A. Yes, they were a lot smaller and simpler than those you have over at the puzzle palace nowadays. The Phrendian problem was always the largest, of course, but I can remember when there were only 50 or so of us in the whole Phrendian transcription shop. The organization was split into two sections; that made it easy to form sides for the softball game at the annual Phrendian Transcription Branch picnic. Actually, come to think of it, there was another part of our outfit called the "Vault."

Q. Why was it called the "Vault?"

A. Because it was in an actual vault; it may still be there at the south end of the second floor center corridor. It was one of the first exclusion areas. The vault kept the secrets in; unfortunately, it also kept the fresh air out. A lot of people who worked in there developed TB.

Q. Tuberculosis?

A. No. Tiny bladder. To get out and get some fresh air, you went to the bathroom a lot.

Q. Not to change the subject, but what were the early voice recordings like?

A. You have to remember that I only go back 2,000 years. Some of the oldtimers used to talk about transcribing from wax discs or recordings on piano wire, but they had progressed to magnetic tape by the time I came on board. Of course, the quality of the tape at first was not so good; the oxide surfaces weren't as developed as they are now, so the fidelity wasn't as true, and you had to play the tapes at higher speeds; also the tape was thicker and, combined with the high speeds, you couldn't record as much as today on a given sized reel.

Q. And the recorders? What were they like?

A. Oh, boy! If today's beginning transcribers could see them, they would laugh; if they had to use them, they would cry.

Q. They were that bad?

A. Well, they weren't designed for the wear and tear of transcription. They were just commercial recorders. If you put a tape on one of them, played it for half an hour or so at a time, and then turned it off, it was fine. After all, that's what these recorders were designed to do. But when you tried to go back and forth, back and forth over garbled passages or to run them a lot on fast forward or reverse, they soon went *kaput*.

Q. What brands were they?

A. One of the most common was the Revere. It was used almost exclusively in our shop. The recorder came in a pebble-grained brown case, complete with carrying handle, and it rested face up on your desk. It had plastic piano key controls for the recorder functions. I think most of the insides must have been plastic too, as fragile as they were.

Q. And the other models?

A. The other type that predominated was the Magnecorder PT-6. It had a grey case and was an upright model. It was barely taller than the 7-inch reels that you played on it. It had one knob that you turned to different positions for all the functions. With all the turning of that switch in transcription, the insides of that recorder took a real beating. A little later we also got some Magnecordettes, which had a 2-track capability. And finally we started developing special transcription recorders, like the AN/TNH-11, and later the AN/TNH-21.

Q. Did those early recorders have any special features to help the transcriber?

A. Are you kidding? They had zilch to help the transcriber. Things you would take for granted today, we didn't have. Take the variable speed control that lets you slow down a difficult passage; our variable speed controls were the fingers on our left hands. We would press them up against the edge of the supply reel and vary the pressure to slow down the tape. It distorted the recording, of course, but it did slow it down to where we at least thought we had a better chance to recover a tough word or phrase.

Q. That sounds like it might have been hard on the recorder.

A. Sure it was. Frequently the rewind function would give out. We would stick a pencil in the reel and rewind it manually, until we got tired of doing that and called for repairs. You had to improvise in those days. Another example: your recorders today have counters, so that you can note the exact positions on a tape you might want to hear again. On the Magnecorders there were no counters. We used to tear off little scraps of paper and stick them in the tape to mark those places. By the time you got to the end of a particularly bad part, it was two-toned — brown and white from all the paper stuck in it. Then when you rewound the tape, you had to be careful to stop it in time, or else you went by the marked spots, and the little pieces of white paper would go flying off across the room..."phfft"..."phfft"..."phfft." Oh, and those early recorders would not cut off automatically when the end of the tape ran out. If you weren't there to stop it immediately, the reel kept turning and the tape either spilled out onto the floor or got wrapped around the capstan.

Q. I guess that earphones have changed a lot over the years?

A. You bet. The early ones were functional, but uncomfortable as hell. They were what radio operators for years have called "cans." The part that went over your ears was hard plastic; the bare metal bands that went over the top of your head were adjustable, and the moving parts would scrape and pinch your skin. At the end of the day you went home with rose red ears and your hair parted sideways.

Q. Did you go right from those to the individually molded earphones that are used today?

A. Oh, no. First the electronics companies came out with "muffs," the kind that most people use with their home stereos today. They were much more comfortable around the ears, but kind of bulky and heavy to wear all day. Before long, we switched to the Telex type, with extremely light plastic headbands and the little tips that went into the ear. Then somebody hit on the idea of individually molded earpieces.

Q. Do the earmolds help you hear better than other types of headsets?

A. I don't know. People have debated that for years. Some say they really make a difference; others think it's all in the mind. I'll tell you what's the best thing about the moldies, though; it's the expandable cords that go with them.

Q. How does that help?

A. Well, if a good-looking girl walks by, you can wheel around for a quick double take, without suffering whiplash.

Q. I guess with the earmolds and expandable cords, the state of the art for earphones has gone just about as far as it can go?

A. I used to think so, but the other day on my portable radio I heard that some rock groups are now operating with *cordless* electric guitars. A tiny transmitter in the guitar beams the music to the amplifiers, and the guitarists are free to romp all around the stage, without getting tangled up in their own or each other's cords. So maybe there will be cordless earphones in the future. I wouldn't expect to see transcribers dancing around the transcription shop, though, because they are still tied down to the keyboard.

Q. Speaking of keyboards, what were the early ones like?

A. We didn't have any "keyboards." We had "mills," old-fashioned manual typewriters. And, of course, they weren't connected to cathode ray tubes; we had to bang out transcripts on 5- or 6-ply paper. The paper had holes down the sides, and on both sides of the typewriter carriage were metal sprockets; the sprockets were supposed to mate with the holes and insure that all the multi-ply remained aligned as the carriage moved. When you finished the transcript, you had to separate the copies and pull out the carbon paper. We eventually went to

DOCID: 4009831

Selectric typewriters and carbonless paper, both of which made transcript preparation easier. And then, of course, came keyboards and CRTs, which allowed "paperless" transcription.

Q. Have people always transcribed at desks?

A. No, there have been attempts to develop a special transcription position. In fact, a number of positions were produced and used for a dozen years or so at the Agency. I guess they were officially called Transcription Consoles. We just referred to them as "consoles."

Q. What were they like?

A. They looked like somebody's idea of a Cape Canaveral space console. They were silver metal cabinets with a shelf for a typewriter, an upper rack tilted away from you, for the recorder, and usually more shelf, rack and drawer space on one or both sides of the recorder, depending on whether you had 1/3, 2/3, or 3/3 of a position, since they came in detachable modules.

Q. Were they better than a plain desk?

A. Overall, they were worse.

Q. How so?

A. They were "camels."

Q. Camels?

A. You know, the old saying that a camel is a horse that was designed by a committee; I think that's what happened with the consoles. They incorporated some good ideas; for example, the typewriter shelf was at a lower, more natural, level than a desktop. In general, though, they were more a frustration than an aid.

Q. What were some of the problems?

A. As I recall, you couldn't reach the recorder from your seat, the drawer space was insufficient for the working aids and supplies you needed, and all the distracting noises that recorders, footpedals and typewriters make seemed to be magnified by the metal and the hollow spaces within the consoles.

Q. What happened to them?

A. They began to wear out, and people turned them in for junk as soon as they could. I certainly hope that by now they've been recycled into something useful, like beer cans.

Q. Have there been other attempts to improve the lot of transcribers?

A. Oh, yes. Transcribers, engineers and contractors have come up with various ideas, intended to make transcritpion better, or at least easier.

Q. For example?

A. Well, people have always been obsessed with reducing the noise in transcription areas. The clicking of footpedals and recorder parts and the clattering of typewriters sometimes add up to a real hubbub.

Q. What did they try to do about it?

A. At one time they decided to test a variety of sound-deadening measures in one transcription section. First they came in and took decibel readings of the noise level in a typical transcription area with tile flooring, concrete walls and metal consoles. Then they installed carpeting on the floor and drapes on the walls and put pads under the typewriters.

Q. What were the results?

A. The area *looked* real nice with the carpeting and drapes. One drawback was that your chair wheels would catch in the rug when you tried to move, and you would go toppling over onto the floor. To remedy that, they put hard pads under the chairs. Eventually, they came back to take decibel readings again.

Q. And..?

A. Supposedly, there was no significant reduction the the noise level, so nothing ever came of it. We were a little let down, but our disappointment was cushioned by an article in the news at that time. It seems that a new office building had recently been constructed in West Germany, incorporating all the latest sound-deadening techniques at great expense. The soundproofing was so effective that the office workers were disoriented by all the silence. Turns out that they had to pipe in typical outside sounds — traffic, birds, airplanes, and the like — to put the workers back at ease.

Q. What else has been tried to help transcribers?

A. One of the silliest ideas was to replace the typewriter with a Stenotype machine. Supposedly, we would have sat there, clacking out shorthand symbols on a Stenotype, keeping up with the recording, and never having to stop and go over anything. The Stenotype tape would have been fed into a device that would convert the symbols back into words on a transcript.

Q. Would that have been the SPELLMAN project?

A. Yes. That was the name of it. How did you hear about that?

Q. There have been some articles about it in CRYPTOLOG.[1] You didn't think too highly of it, then?

A. The only thing that might have been worse was the stereo delay experiment.

DOCID: 4009831

Q. The stereo delay experiment?

A. I don't know if that's what it was officially called. Some electronics engineer had the idea that transcribers could hear more clearly if the recorded voice was to be placed on each of two tracks. One track would be fed into the left earphone and the other track — with the same recording — would be fed into the right headphone. The catch was that there was a delay of a small fraction of a second between what you heard in you left and right ears. Supposedly, this delay would increase your aural acuity.

Q. And it didn't do anything for you?

A. Oh, yes. It gave us headaches. Here those engineers were getting paid twice as much as we were to come up with cockamamie ideas like that. I think they kept them down in the basement too long in those days.

Q. Haven't there been any innovations that have really helped transcribers?

A. I can't think of any. A lot of the developments have made transcription more *comfortable*, but not really easier. And new technology sometimes causes new problems. For instance, the old mills and 6-ply paper were a pain to use, but with the new CRTs you have to guard against things like radiation or the eyestrain that's caused by "CRT glare." I understand they've been working on a way to convert speech into a digital form, so it can be manipulated and enhanced to smooth out the garbled parts. I'm skeptical, but you never know. After all, who would have predicted cordless electric guitars?

Q. Can you think of anything else in the way of past developments that have affected transcription?

A. No, but like I said, I only go back 2,000 years. Some of the oldtimers might be able to fill you in about the earliest days.

Q. Just one last question. How do I get back to the Agency from here?

A. That's easy. Just follow that path there; it will take you to the rifle range road. And when you get back to the building, please say hello to General Canine for me.

[1] Notably, "I Remember SPELLMAN," by Arthur Salemme, Jul 78. Also, "More B.S. (Before SPELLMAN)," by [redacted] Oct 78. A somewhat more optimistic view of this concept can be found in "Shootout at the SIGINT Corral," by [redacted] Jul 79.

P.L. 86-36

Solution to NSA-Crostic No. 28, CRYPTOLOG, August - September, 1979.

"[Mokusatsu:] One Word, Two Lessons," by [redacted]

"[One] problem that keeps every word in one language from having a counterpart in every other language is that often something which is commonplace to speakers of one language will be...unknown to speakers of another... How, for example, do you translate "anchor" into a language spoken by nomad[s]...in the midst of the Sahara Desert?

Letters to the Editor

To the Editor, CRYPTOLOG:

I enjoyed reading the humorous account of [redacted] early experiences with computers at the Agency ("On Coming of Age at NSA: Confession of an Ex-Linguist," CRYPTOLOG, August-September 1979). I would like to point out, however, that ROB ROY was not the first system to "have remote use terminals ever." ROGUE was! ROGUE (Remote Operated General Use Equipment), installed at Arlington Hall Station, had four remote terminals (Flexowriters), each located in a different analytic area: three were in A Building, for GENS, ALLO and ACOM, while the fourth was in B Building, for ADVA. As with ROB ROY, the terminals were serviced serially.

Delmar L. Taylor
Chief, T331

CLA NEWS

For the Spring of 1980, the Crypto-Linguistic Association announces two contests:

THE SYDNEY JAFFE AWARD

In 1972 the CLA established the Sydney Jaffe Award as the Agency's highest recognition of exceptional acheivement in the field of language. It is given to persons, either civilian or military, who have made major contributions to the mission of the cryptologic community in the tradition of scholarship, leadership, and accomplishment exemplified by the late Dr. Jaffe, the first President of the CLA.

The award may be given for any aspect of language endeavor — operational use, research, training, development of new technology, or management.

Candidates may be nominated by any three members of the cryptologic community, by the Chairman of the Language Career Panel, or by any supervisor at office level or above. Nominations should include a statement detailing the candidate's accomplishments in the language field and specifying how they have contributed to the Agency's mission.

Selection will be made by a committee composed of representatives of each of the major NSA organizations which employ linguists.

Nominations should be submitted to CLA President [redacted] G95, 2A158, ext 5882s, by 1 May.

P.L. 86-36

CLA ESSAY CONTEST

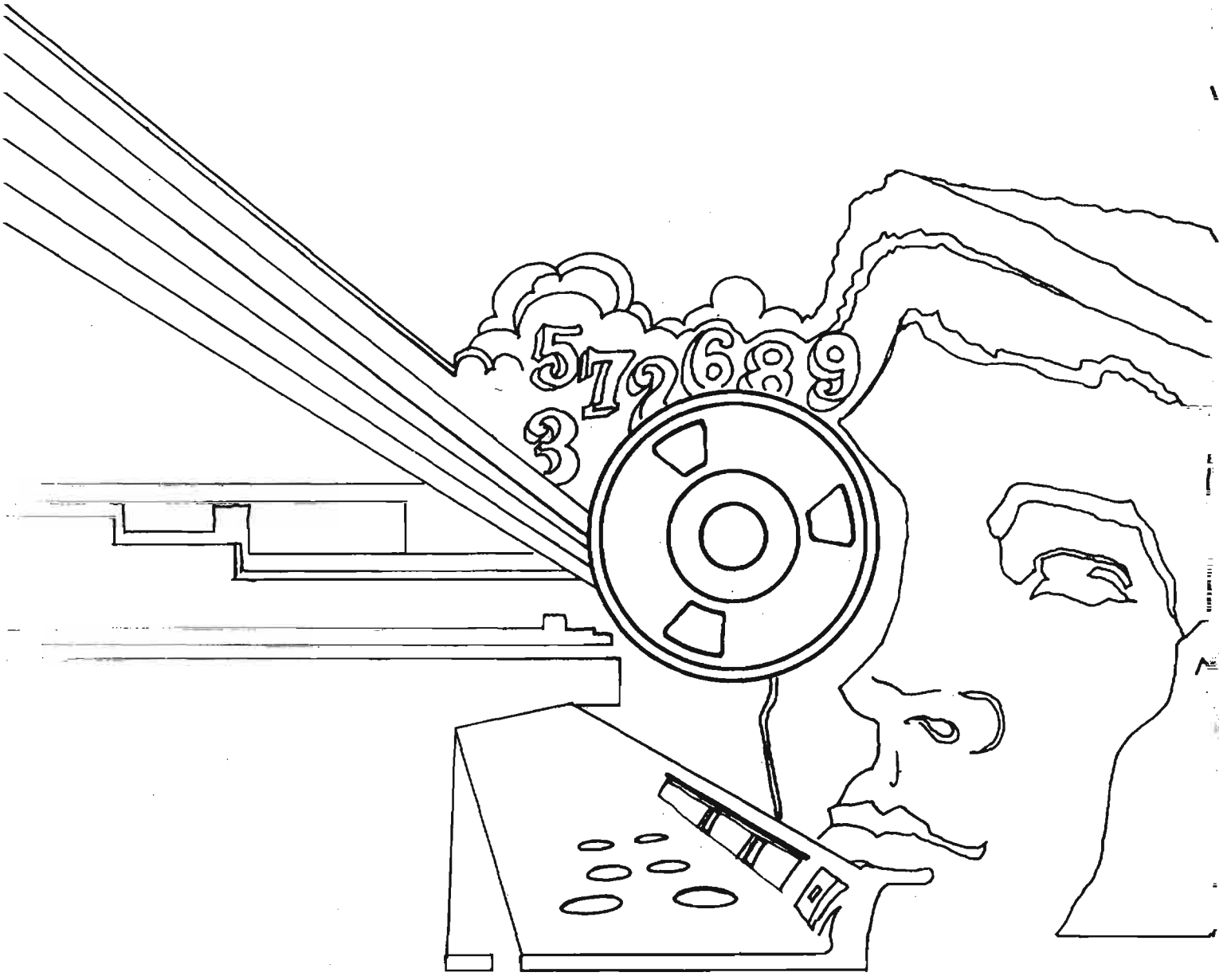
Submissions of the annual CLA essay contest are now being accepted. The deadline for entries is 1 May. Any paper in the fields of language or linguistics written by a member of the CLA is eligible; papers by non-member Agency personnel are eligible if sponsored by a member. While it is preferred that entries be original material written specifically for this contest, previously published items will be considered.

First prize is $100, second prize is $50, and third prize is $25. Entries should be sent to the CLA Secretary, [redacted] A624, ext 5157s.

* * * * * * * * * * * * * *

TO SUBSCRIBE TO *CRYPTOLOG*, CALL 1103s

* * * * * * * * * * * * * *


5726893

DOCID: 4009830

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

AUGUST - SEPTEMBER 1979

P.L. 86-36

ON COMING OF AGE AT NSA (U) ..... [redacted] 1
AN AUGUST BAUDY (U) ..... [redacted] 6
NSA-CROSTIC NO. 28 (U) ..... D. H. W. 8
INSUFFICIENT NORMALCY OF METHODRY (U) ..... Sydney Fairbanks. 10
NSA PROMOTION BOARDS: HOW THEY WORK (U) .... [redacted] 11
...BUT ON THE OTHER HAND (U) 15
PUNCTUATION: MORE THAN MEETS THE EYE (U) .... [redacted] ...16
LETTERS TO THE EDITOR (U) 17
MEMORABLE MEMOS (U) 19
CLUB NEWS: CAA AND CMI (U) 20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 1 SEP 2009~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009830

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. VI, No. 8-9 AUGUST-SEPTEMBER 1979

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor-in-Chief.....David H. Williams (1103s)

Collection.....[redacted] (8555s)

Cryptanalysis.....[redacted] (4902s)

Cryptolinguistics.....[redacted] (5981s)

Information Science.....[redacted] (3034s)

Language.....[redacted] (8161s)

Machine Support.....[redacted] 5084s)

Mathematics.....[redacted] (8518s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Taurone (3573s)

Production Manager.....Harry Goff (5236s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4009830

On Coming of Age at NSA: Confession of an Ex-Linguist (U)

By [redacted] *V2*

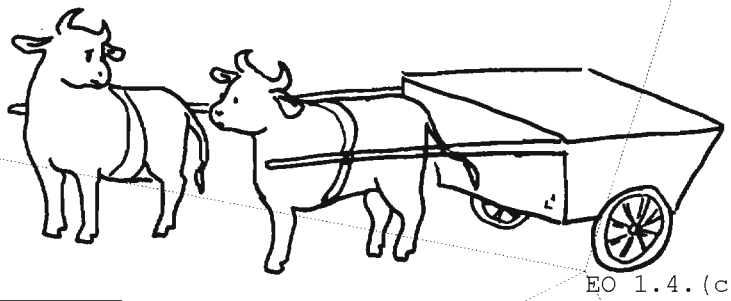
P.L. 86-36

(U) Do you remember green traffic? Maybe some of you out there are still reading green traffic, but I doubt it. You see, green traffic was BC at NSA—BC, that's Before Computers. Back in BC, an analyst stood on his own two feet. There was no such excuse as "the dumb computer goofed up" or "garbage in, garbage out." You either cut it or you didn't.

(U) I dont recall the exact day we went AD (AuDomashun), it's really not important. You computer historians have your version, I have mine. Anyway, I recently spent some time testifying in court, and I know you can say just about anything if you precede it with "to the best of my recollection..." So...

[redacted]

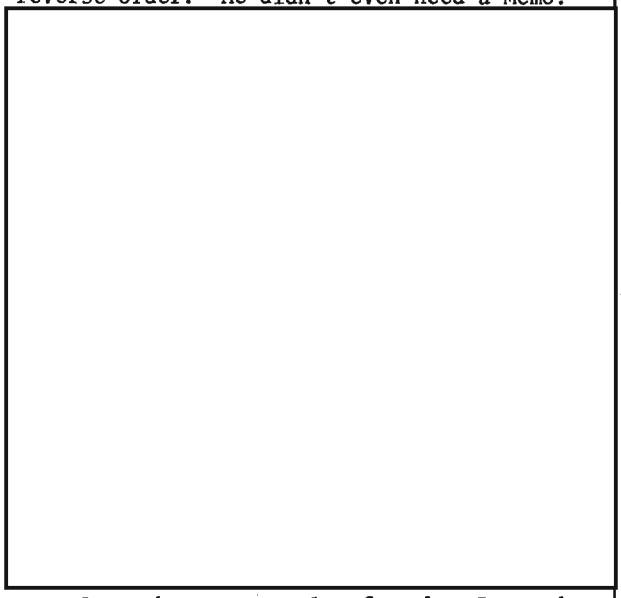
"...I was given a new job. Actually, it was shortly after I put out my [redacted]



EO 1.4.(c)
P.L. 86-36

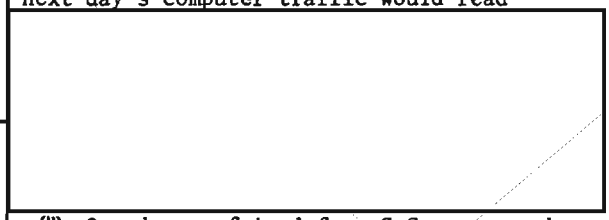
[redacted]

(U) C Group sent a very nice fellow over and we had a fascinating chat about how fast computers could do things compared to people. It was easy to talk to programmers in those days because they had no mystical vocabulary of their own the way they do now. Agreement was reached that the messages would be keypunched, after which we would make a number of different sorts to see if any patterns fell out. We decided to make a sort on this group and on that group, and finally, to run a sort in reverse order. He didn't even need a Memo.



(U) Over the next couple of weeks, I pored over the sorts. There was a lot there, but somehow I couldn't put it all together. Something was missing. The rerun sort had unfortunately not yielded anything, but, wait a minute, there was something after all. The backwards sort—I had been too ashamed to throw it away. I pulled it out and voila! I had it: the identity of the groups, the allocation scheme, and instant fame. Drunk with success, I asked to join the staff and devote my life to the computer. I was hooked.

~~(C)~~ Life as a junior ADP sponsor was terribly exciting. There were cards to be punched and paper tapes to be rewound (often they arrived from the field inside out). I especially loved paper tapes because it was a team sport. One guy would stand at the end of the hall waving off pedestrians; the other would grasp the lead end of the tape and throw the roll down the corridor. Getting paper tapes frontside out was very important, because if they weren't done right, your next day's computer traffic would read



(U) One day my friend from C Group came by and announced that our programs were to be moved to a new computer system. This was to be the first transistorized computer at NSA and would be a great improvement over the old vacuum tube ones which required several hours to come to a stable operating temperature when turned on Monday morning. Yup, that's right—the computers didn't work weekends. An instructor from the computer company was coming out to NSA to teach a two-week course in programming the machine. I begged my Chief to be allowed to enroll in the course. "Begged" sounds like a strong word, but back in those days college girls had a reputation for getting married and then you-know-what, which meant all that had been invested in them went down the drain. I promised him that even though I was married, I would never get you-know-what and quit, in exchange for which he sent me to school for two weeks.

E.O. 1.4.(c) P.L. 86-36

(U) I had a bit of a problem in the course, not because I didn't understand the work, but because of a mild case of morning sickness—sorry about that, Chief. By the end of the two weeks I was really grooving on the language and could read a card, loop through a process, and print a line with the best of them.

(U) I returned from class ready to test out my new programming skill, and found to my dismay that it had largely been for naught. At NSA we didn't read a card, loop through a process, and print a line. We took the cards to a shop called "Peripheral," had the cards loaded to magnetic tape, carried the tapes to the computer, read tape, looped through the process, wrote back out to magnetic tape, and carried the tape back to "Peripheral" for printing. None of us had the faintest notion of how to write a program using magnetic tape as input and output! Moreover, assembly language (that we had learned) was not used, but rather an assembler compiler. You might think that this was

DOCID: 4009830

some kind of communications gap, but it wasn't. It was long-term strategy, because we got the outsiders to think we were doing one thing, when we were really doing something else. That's why the Commies fell so far behind in mag tape technology. To this day they are still reading a card and printing a line.

(U) In those days, writing and running programs was an absolute ball. The central part of the basement was one gigantic open room, with the sea of computers rocking and rolling as far as the eye could see. The C Group programmers were not hidden away in little groups all over the building the way they are now, but logically deployed in rooms adjacent to the "big room." If something ran amok, the computer operator would simply open the door to the programmers' room and fall in (the big room had a raised floor, the programmers' rooms didn't). This would catch the programmers' attention, and together the operator and the programmer would stroll to the machine to resolve the problem. "Resolving the problem" meant manually stepping the computer through the program instructions, one by one, until the error popped (can you believe it!), and then keying in the patch via the computer toggle switches.

(U) If you were the "dirty fingers" type like I was, you could even run the computer yourself, mounting the magnetic tapes and hitting the start key. The console lights would flash and the tape drives leap into motion. It was almost as much fun watching a mag tape fly off the drive as throwing paper tapes down the corridor. And was there ever any greater thrill than fogetting to put the carriage control tape on the high-speed line printer and watching a fountain of #12-4 hit the ceiling after the first page eject command.

(U) Automation was moving into high gear now, but the analysts themselves didn't really get hands-on into the action until the advent of ROB ROY. For those of you who have spend the past ten years wondering what the mnemonic RYE stands for, it can now be revealed that it isn't and it doesn't. RYE is what evolved after ROB ROY because the namer was not too swift in the bartending department. ROB ROY had the first remote user terminals ever; they were also probably the last terminals that plain old users could operate.

(U) I think there were five terminals in all, placed conveniently in the little keypunch rooms that had begun to spring up in the analytic areas since there was about ten times as much to be keypunched as Keypunch could handle. Anyway, the terminal looked like a metal desk; in fact, it was a metal desk. I point this out particularly since I have recently been briefed on a mammoth-bucks R & D contract (not ours) to study man-machine relationships, one aspect of which is to design a user terminal that looks just like a desk. In one side drawer of the ROB ROY terminal was the paper tape reader (for input), in the opposite side drawer was the paper tape punch (for output). On top of the desk was mounted a big clunky console full of switches and lights, none of which had the least significance save for the GO light and the GO button. Actually, I didn't learn this by going to a class, but by observation, since my reason for being in the room was to keypunch. By now, I was probably the Agency's highest paid keypuncher.

(U) After staging your input tape into the reader, you would sit alertly with your eye on the GO light and your finger on the GO button. The terminals were serviced serially, so when it came your turn, the computer operator would switch on your GO light, and you would instantly hit your GO button to initiate the paper tape reader. If you didn't move swiftly, the computer operator would assume nobody was there and go on to the next terminal. Since each of the five terminals was free to run any length process, doping off by lighting a cigarette or something could cost you an hour's delay waiting for your next turn.

(U) One day there was a cigar smoker in there who naturally blew a couple of turns, and since I was sitting there keypunching not looking my grade, he told me to keep an eye on the console and shoot off his input when the light came on. I said sure, so he left. I was more or less bored with keypunching [redacted] so I rolled my chair over to devote my full attention to the GO light. After a bit, it flashed red. I hit the GO button, and the tape reader burst into action and then immediately burst into flames. Now, I knew C Group was resisting the open-shop concept, but I felt this was going too far. Reacting with calculated calm, I called the computer operator and told her I would be skipping my turn for now.

EO 1.4(c) P.L. 86-36

(U) This incident greatly enhanced my reputation for handling data processing crises, and it was inevitable that I would assume the position of senior data processing sponsor in my office—and so it came to pass. Sitting at my new desk in the staff area, I surveyed the room with pride—computer listings everywhere, spilling over the analysts' desks, spilling out of the formidable rows of cabinets which now doubled in number almost monthly, spilling into boxes destined for Fort Holabird to be preserved for all time, and not a sheet of green anywhere. What an accomplishment!

(U) There was, however one blot in this otherwise perfect vista: the analysts' desk drawers. Even though I had supplied them with lists and sorts and sorts and lists, they stubbornly insisted on maintaining their own handwritten note files. They were backed into the trenches, but they were still fighting. The 3 x 5 cards, files on yellow telephone message pads, notes on envelope backs—this just had to go.

(U) We had recently gotten a new Chief, and he was very impressed with our advanced stage of automation, having just come over from The Other Group. About this same time, I met a really sharp fellow who was putting the finishing touches on a super program that would search through records and extract from them almost anything one could imagine. He called this process a retrieval language, and he was looking around the Agency for some data in complex format to test against. It occurred to me that all those little bits and pieces of information jotted down in the various analysts' desk files fit his needs to a T. I set about writing a description of a set of records such that each piece of information had its place. Companion to this would be an analyst log sheet; each analyst would have his very own personal booklet of log sheets to be filled in as information bits were uncovered in traffic. Old analysts would have the joy of completely filled up books. New analysts would know exactly what to look for, and could just fill in the sheets. Since all the data was done in a common format, once it was loaded into the computer, analysts could easily compare data to mutual advantage. It was perfect. Well, almost. As I am sure you know, linguists are a very independent bunch, and they said they certainly had enough to do without having to fill in reams of dopey log sheets. In the interest of security, mainly his own, the Chief tabled my proposal.

~~(C)~~ About this time, [redacted] made their annual royal visitation to our shop. I knew the script pretty well, having sat through previous iterations of the same meeting for years.

They: We want you to translate all the messages you get and just send them over to us. We'll do the analysis.

Chief: We can't translate all the messages, and besides, we have lots of very experienced people who are not only highly capable linguists, but superb analysts as well.

They: You know very well that you don't do analysis. *We* do analysis. You supply intelligence information (big emphasis on the word "information").

Chief: Most of the messages are worthless.

They: We produce intelligence (emphasis on "intelligence"), therefore, we decide what's worthless.

But then suddenly the unchanging annual dialogue took a new tack.

Chief: Well, just assume for the sake of discussion that we did translate all the messages and send them to you, what ever would you do with them?

They: Why, we would put them in our database, of course.

Long pause.

Chief: Your database?

They: Naturally, it's the latest thing.

(U) The Chief gave me a long flinty glance. I had been dozing off the in back corner of the office, because my only function at the meeting was to add strength in numbers to Our Side. Suddenly, I felt fear. Smiling foxily, the Chief turned back to the conference table.

Chief: Well, you gentlemen will be pleased to know that we have had a database for some time, and my senior ADP officer will be glad to give you a rundown on it.

Now I could taste the fear, as he went on.

Perhaps she'd like a moment to go to her desk and get her briefing notes.

P.L. 86-36
EO 1.4.(c)

Obviously my command to exit.

[redacted]

~~(C)~~ Well, that was many years ago. That project was born, flourished, and died a graceful death when the linguists at long last achieved the recognition in the community that they so well deserved. The age of comprehensive reports came in, and individual translations were deemphasized. I, myself, followed my own star, moving on to, as we say in performance appraisals, jobs of increasing complexity and responsibility in the data processing environment. I now have a whole roomful of computers all my own, but once in a while, on the

EO 1.4.(c)
P.L. 86-36

way to work, I spot a license plate (like "7193"—one of the few STC groups I ever managed to memorize) which reminds me of what it was like in the old days and how it all got started.

(U) I'm actually so busy managing all my fantastic machinery, you might wonder how I ever found the time to write this tale. To be truthful, just the other day one of my systems took a "hard crash," followed shortly thereafter by the other one, then the disk drives went, and all the terminals died. Since this office is *totally* AD, I've had a little time on my hands. But don't worry. Maintenance assures me (they only work days) that everything will be back up in the time it takes to say IAHGNAHS.

(This notice is UNCLASSIFIED)

CLA - NCS

CLA-NCS FOREIGN FILM SERIES

THE FOLLOWING LISTED FOREIGN LANGUAGE FILMS WILL BE SHOWN IN THE FRIEDMAN AUDITORIUM UNDER THE JOINT SPONSORSHIP OF THE CRYPTO-LINGUISTIC ASSOCIATION AND THE NATIONAL CRYPTOLOGIC SCHOOL.

NOTE: STARTING TIME IS 0930 HOURS ON EACH DATE.

DATE	LANGUAGE	TITLE
29 NOVEMBER	RUSSIAN	"THE FORTY FIRST"
20 DECEMBER	HEBREW & MULTI.	"IMPOSSIBLE ON SATURDAY"
17 JANUARY	JAPANESE	"SANJURO"
14 FEBRUARY	FRENCH	"THREE FABLES OF LOVE"
13 MARCH	TURKISH	"THE FATHER"

ALL FILMS HAVE FOREIGN LANGUAGE SOUND TRACKS AND ENGLISH SUBTITLES.

ALL ARE INVITED

DOCID: 4009830

AN AUGUST BAUDY

E54

P.L. 86-36

Have patience a little longer, world! You will soon be able to know what the collectors are saying when they use their arcane language. A glossary is in the process of being written which will be the definitive word on what is meant by that term you have often heard, but have never really understood.

A glossary is being compiled by a committee of people in signals collection or associated with various aspects of it. At present, all but four of the participants on the Signals Collection Terminology Panel are professionalized collectors. The remainder are professionals in some other fields, such as Signals Conversion or Data Processing—fields which are closely akin to Collection and which share much of the terminology.

The SCTP is not the first such effort. It is the second in what will be a series of glossary-writing panels that are sponsored by P1 and whose members are appointed by the Chiefs of the Agency's Key Components as part of an overall program for terminology standardization that is set out in USSID 412. The Traffic Analysis Terminology Panel has been in existence for several years, and the glossary which they have prepared is in the final pre-publication phases.

The SCTP is of more recent origin. We have been in existence for just over two years. At present, we have dealt with, to the satisfaction of a consensus of the panel, some 1500 terms. It is easy for us to understand the length of time it took the TA panel to produce their document because of our experiences. We have occasional moments of quiet despair when we wonder if we will ever finish the task we have taken on. In fact, we, the current members of the group, well may not. People get transferred overseas or to more demanding jobs and have to be released from panel responsibilities. New members have to be assigned to replace them. The author is a "second generation" member.

Two years ago the panel had a list of 2686 terms to consider. Of these, some 1200 were thrown out for one reason or another. Quite often the reason for dropping a term from consideration is that it is quite adequately and precisely defined, even in the terms of signals collection, in a standard dictionary. An example of this is the word *acquire*. Webster says it means something like "to gain...by one's exertions." No matter how we looked at the word in the panel, it came out meaning what Webster says it means, so there is no need to include it in our glossary.

We have provided definitions for another three hundred terms, more or less. At present, as a result of some new terms having been introduced for our consideration, we have just under 2000 more words or phrases on which to deliberate.

There are two major factors which make the job both difficult and time-consuming. The first is the unfortunate fact of life that a word which started as a representation of some specific thing or action evolves over the years to encompass more and more variants until it becomes an imprecise and often erroneously applied term. Just as one example, the word *baud* will be cited. This inoffensive little word, used by collectors and other technical types for years and years, started out with just one meaning: a unit-per-second unit for expressing the speed of a telegraphic signal. The unit in question is the least element in a signal or a space of a length equal to that element (e.g., the Morse "dit" or an intra-character space). Just as *knots* refers to nautical miles per hour, so *baud* refers to the number of these elements per second.

The radio world, the electronics world, in order to honor Jean-Maurice-Emile Baudot, as it had honored Michael Faraday, Charles de Coulomb, James Joule (and let's certainly not overlook Samuel F. B. Morse), named this measuring unit for him.

It's quite simple, really. Instead of saying that the rate of transmission of a particular signal is equal to x number of the smallest element of the signal per second, one would merely say that the rate is x bauds, thus shortening a cumbersome phrase to one word.

So much for the beginning. Where are we now? [redacted] one of our panel members, began to research all the currently used definitions in various documents available to the SIGINT community. He stopped when he had reached some fifteen to twenty definitions. Some approximated the original meaning of the word, but some were extremely far afield. In the interests of accurate reporting, I must confess that I argued long and vigorously that the word *baud* merely mean the shortest element of a signal, and that those other people were crazy and being difficult when they insisted on a definition which related to a time reference.

This one term accounted for the expenditure of hours of the panel's time. It may sound frivolous, but it is not. The term is in use, and will continue to be in use; therefore it must be defined. Each member of the panel *knew* what this old, familiar term means. Unfortunately, each one "knew" that it meant something a little different. We finally opted to put it in the glossary as an unpreferred term with cross-references to the preferred terms.*

The second factor is that we often find that a term we have previously been satisfied with has recently been redefined by an authority we cannot ignore. An example of this is the very word *collection*. By a definition provided by Executive Order 12036, the Foreign Intelligence Surveillance Act of 1978, and by USSID 18, collection is defined in terms on the order of "intercept copy taken for the purpose of deriving intelligence." Implicit in all the definitions is that what is intercepted is not "collected" unless and until some intelligence extraction process takes place. It is a subtle point, but for collectors, it must be defined. As a sidelight, it is not as important for other disciplines, such as Traffic Analysis. For TA purposes, "intercept" and "collection" could be used interchangeably without any loss of accuracy.

Why are we going to all this trouble? Why do we squander so many valuable manhours (or person-hours, anyway) on this slow and tedious work: Anywhere *from to ten to forty* manhours per month may be used up in just the panel meetings alone. The reason is that this glossary we are working on will become the standard. The glossaries will form parts of USSID 412. Our glossary and the TA glossary will ultimately be joined by glossaries for cryptanalytic and data processing terms. Other glossaries, on telecommunications and telemetry, for example, are also under development.

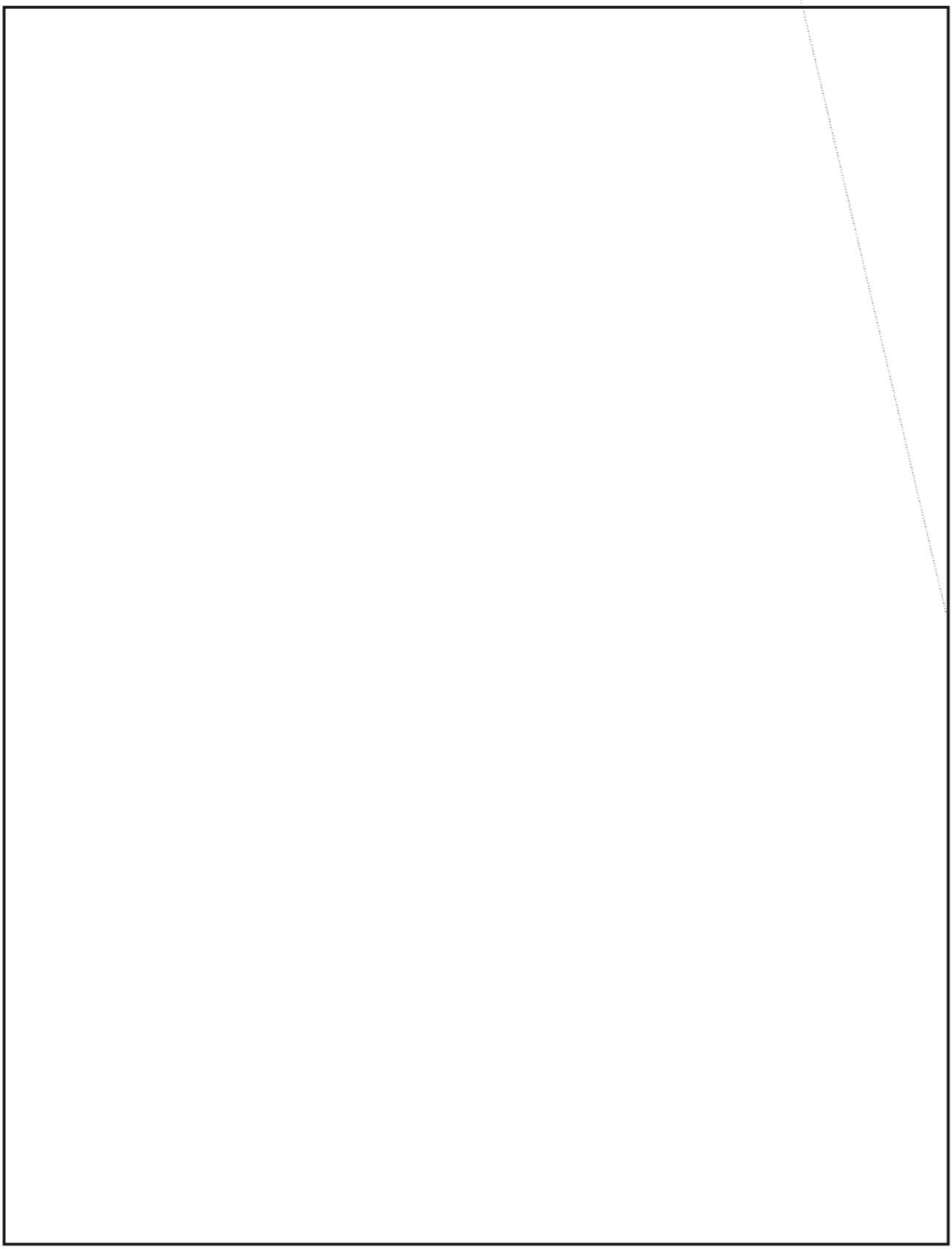
The intent we on the SCTP espouse—and we understand that the TA group approached the problem the same way—is not to dictate the usage of cryptologic terminology. Rather, we are trying to establish a standard. We are not trying to circumscribe the vocabulary, but we wish to present a method by which NSA's written word may be clearly understood. In dialogue, one may be vague. An individual word that conveys a subtly different shade of meaning to the hearer than it meant to the speaker can and usually will be cleared up in further conversation. If you will listen closely, you will probably observe that in most conversation, every point made is usually made several times over. In writing, however, the trend is to economy. In official and technical correspondence this is especially true. For this reason a reference is necessary so that we may be sure that the meaning perceived by the reader is the same as that intended by the writer.

At present the SCTP consists of seventeen people, representing all elements of DDO, as well as DDF, ADPR and the NCS. Russ Doig has had to depart for other duties and his contributions will be missed. Remaining under the chairmanship of [redacted] ficially active, but will soon have to leave us. Other former members of the panel are [redacted] Working very closely with us are members of the NSA Data Standards Center, our sponsoring element within P1, specifically, [redacted] who keep us on the track and provide administrative help without which we would not be able to survive. P.L. 86-36

As stated above, we have lost some of our people and will soon lose some more. [redacted] is very interested in recruiting some replacements, particularly from B. R and T. If you would be interested in being a part of this august group, please advise your supervisor, who should then get in touch with the Data Standards Center on 8161s (FANX), which can then take care of the necessary paperwork.

* In the Soviet Union, too, the baud (бод) is defined as a unit of telegraphic speed: "...the number of basic impulses transmitted per second." (Bol'shaya Sovetskaya Entsiklopedia, 1970)

DOCID: 4009830



DOCID: 4009830

sydney fairbanks

Insufficient Normalcy of Methodry

From the NSA Technical Journal of July 1959. here is Dr. Fairbanks' final comment on Agency English.

The time has come, alas, to lay down the editorial pen.

As we pushed open the glass doors this morning, Big Brother saluted us with some remarks on "the end of a perfect day"; as we reached our desk he assured us that father would come to his babe in its nest (silver sails all out of the west), and to date he is still making noises like a noontide bee. This curious sample of the mores of a mechanized culture always used to affect us with sardonic glee. We wish Big Brother would stop talking about twilights. (But as a matter of fact we have long since joined the little band of negative thinkers who wish Big Brother would stop; period.)

Naturally we have hesitated over the best subject for a final fling. We had thought of describing the extraordinary things—reminiscent of a baby with a tube of library paste—that an amateur can do to a sentence with the word "such." But it seems more appropriate to end with a salute to a success of the enemy. We shall talk about one of the major triumphs of Memorandumry.

Most things in this world are accomplished by having tools and knowing how to use them. "Tool" has long since been replaced by "implementation" with a net gain of four syllables, but "way," "means" and "methods" are all regrettably brief. Some genius, however, has risen to the occasion, and it now becomes possible to write "the finalization of the operation may be accomplished by the employment of the appropriate implementation and methodology," ending with a fine approximation to the Ciceronian *esse videatur*, and using thirty-eight syllables to say, the reader will note, absolutely nothing.

Obviously "implementation" and "methodology" go together like bacon and eggs, and a guy should know when he's licked. Nevertheless, we raise a protest. "Methodology" is as inappropriate to mean nothing as "methodism" would be, because both have been pre-empted to mean something. We shall not enter into the horrors of religious controversy by defining "methodism," but "methodology" means, roughly, "the science of scientific method," and people give courses in it and write books about it. In such a crisis we have no wish to be merely destructive, yet it is hard to make a suggestion. "Methodry" perhaps, on the analogy of "toiletry" and "circuitry." "Insufficient normalcy of methodry" (meaning "this is too new a way of doing it") has surely some of the authentic Memorandian charm—and sentiment, for that matter. But the real devotee will demand a pentasyllable.

"Methodication"...?

It is enough. As usual the agony of composition has assuaged our thirst for publicity. Never mind what we said above. We look forward with ineffable rapture to watching from the bank while others toil upstream, to hearing the contributors fill the sea and air, like little birds, with their sweet jargoning, and not having to do a thing about it. In this mellowing twilight it even seems, now that we don't have to do it any more, as if it might have been worthwhile; but we are not seduced. Your galley, gentlemen. You can keep my oar.

And thank you for listening so patiently.

sydney fairbanks

Insufficient Normalcy of Methodry

From the NSA Technical Journal of July 1959. here is Dr. Fairbanks' final comment on Agency English.

The time has come, alas, to lay down the editorial pen.

As we pushed open the glass doors this morning, Big Brother saluted us with some remarks on "the end of a perfect day"; as we reached our desk he assured us that father would come to his babe in its nest (silver sails all out of the west), and to date he is still making noises like a noontide bee. This curious sample of the mores of a mechanized culture always used to affect us with sardonic glee. We wish Big Brother would stop talking about twilights. (But as a matter of fact we have long since joined the little band of negative thinkers who wish Big Brother would stop; period.)

Naturally we have hesitated over the best subject for a final fling. We had thought of describing the extraordinary things—reminiscent of a baby with a tube of library paste—that an amateur can do to a sentence with the word "such." But it seems more appropriate to end with a salute to a success of the enemy. We shall talk about one of the major triumphs of Memorandumry.

Most things in this world are accomplished by having tools and knowing how to use them. "Tool" has long since been replaced by "implementation" with a net gain of four syllables, but "way," "means" and "methods" are all regrettably brief. Some genius, however, has risen to the occasion, and it now becomes possible to write "the finalization of the operation may be accomplished by the employment of the appropriate implementation and methodology," ending with a fine approximation to the Ciceronian *esse videatur*, and using thirty-eight syllables to say, the reader will note, absolutely nothing.

Obviously "implementation" and "methodology" go together like bacon and eggs, and a guy should know when he's licked. Nevertheless, we raise a protest. "Methodology" is as inappropriate to mean nothing as "methodism" would be, because both have been pre-empted to mean something. We shall not enter into the horrors of religious controversy by defining "methodism," but "methodology" means, roughly, "the science of scientific method," and people give courses in it and write books about it. In such a crisis we have no wish to be merely destructive, yet it is hard to make a suggestion. "Methodry" perhaps, on the analogy of "toiletry" and "circuitry." "Insufficient normalcy of methodry" (meaning "this is too new a way of doing it") has surely some of the authentic Memorandian charm—and sentiment, for that matter. But the real devotee will demand a pentasyllable.

"Methodication"...?

It is enough. As usual the agony of composition has assuaged our thirst for publicity. Never mind what we said above. We look forward with ineffable rapture to watching from the bank while others toil upstream, to hearing the contributors fill the sea and air, like little birds, with their sweet jargoning, and not having to do a thing about it. In this mellowing twilight it even seems, now that we don't have to do it any more, as if it might have been worthwhile; but we are not seduced. Your galley, gentlemen. You can keep my oar.

And thank you for listening so patiently.

DOCID: 4009830

NSA Promotion Boards:
How They Work

[redacted] S14

P.L. 86-36

Certainly one of the most popular items ever to appear in CRYPTOLOG, to judge by reader response, was [redacted] article, "Some Tips on Getting Promoted." It is based on an address which she gave before the WIN (Women in NSA) organization, which was later summarized in the WIN Newsletter. The article was originally printed in CRYPTOLOG of December 1978, and subsequently in the Field Information letter of May 1979. In addition, CRYPTOLOG has sent out over 300 reprints of the article to interested people.

Understandably, promotions are a subject of great importance to just about everybody. So when Virginia called a couple of months ago to ask if I wanted a follow-up article, my response was an immediate yes. So here it is—[redacted] observations on her tour as a member of one of the Agency's promotion boards. dhw

The present procedure for promoting to "critical grades"—13, 14 and 15—has been in existence for some years now. Even so, it seems not to be very well known in the Agency. This article aims to improve the general understanding of the process and tries to remove some of the mystery—and even distrust—with which it is sometimes viewed.

I write this article on the basis of my experience as a member of the Grade 14 Promotion Board in 1978. It was my only experience serving on such a board and it was a good one. The job turned out to be interesting, challenging and difficult. Unexpectedly, it demanded a bone-wearying amount of work. But all told, it proved satisfying and rewarding. I ended my year's tour with a feeling that the process we use here, while not perfect, is a good one.

This article covers the following aspects of the Agency Promotion Boards

- their composition and mission
- their function and tools
- the zero-base review process
- the nomination process
- management presentations
- the selection process

Although my experience was limited to the Grade 14 Board, the process described is generally applicable to all three Boards.

NSA Promotion Boards and their Mission.

Three Agency-wide Boards are consituted each January to handle the selection of people to receive promotions to grades 13, 14 and 15. The nine members of each Board are chosen by the Deputy Director for Management (DDM),

and recommended by him to the Director for approval. In making his selection the DDM discusses recommendations with the Key Component Chiefs. The selection includes at least one woman and one minority member. Board members are usually at least one grade higher than the promotion level of their respective Boards. The Board Chairmen are chosen on the basis of their position: the Director of Civilian Personnel (M3) chairs the 13 Board, A/DDM chairs the 14 Board, while DDM heads the 15 Board. Executive Secretaries for the Boards are appointed usually from within M, by the chairmen. The Boards are formally created with the publication in December of appropriate Personnel Assignment Orders, or "green sheet."

In 1978 the promotion process got underway when the Director convened all the newly appointed Board members in his conference room, and personally explained to us our mission, gave us guidance, and stressed the responsibility of the assignment he was entrusting to us. We learned that, as Agency Board members, we worked for him as his representatives, and not for our parent organizations. Our Board assignments were to take priority over our regular jobs, and we were expected to devote all the time and effort necessary to executing a very serious and important task. He asked that we give fair and equitable consideration to everyone, including women and minorities, who, because of their management. He pointed out the educational value of field assignments, and asked us to review field personnel with particular care because he is anxious to attract the best people to such assignments and to reward good performance. Finally he cautioned us not to overlook technical people who are essential to the fulfillment of the Agency's mission.[1]

Board Functions and Tools. The Director's meeting with the new Board members was followed closely by the initial meetings of the individual Boards. Schedules and assignments for the first cycle are traditionally distributed at this meeting. The Grade 13 Board has four cycles per year (beginning in January, April, July and October), while the Grade 14 and 15 Boards meet for only two cycles annually (January and July). This is because the numbers of eligibles to be reviewed and promotions to be awarded by the Grade 13 Board is much greater than those handled by the other two Boards.

I had always assumed that Promotion Boards did all their work in meetings, so I was surprised to find that, in fact, the bulk of my time was to be spent reading in the promotion files. These files are kept in special rooms belonging to DDM, one for each Board. We were given directions and keys to our new home. Here each of us had half a file cabinet drawer for storing folders and notes, along with access to banks of file cabinets containing drawer after drawer of promotion folders for all eligible Grade 13's[2]. Work on promotions is carried out in these rooms rather than in the members' office spaces, so as to ensure confidentiality of the sensitive personal data handled, as well as to cut down on outside distractions.

We were provided with various useful tools, such as the following

* A computer listing of all eligible Grade 13's which runs to many thick volumes. It contains a one-page summary on each person, highlighting vital information such as name, organization, job title, COSC, age, EOD date, date of last promotion, list of all jobs at current grade, professional certifications, and last three performance appraisal ratings (both overall and attributes).

* A computer listing of performance appraisal ratings (overall and attributes) given by all supervisors to all their employees in critical grades. This listing helps Board members to spot the "easy" and "hard" raters and is used to normalize such ratings.

* Statistics showing each Key Component's theoretical fair share percentage of promotions based on the number of persons eligible.

* Statistical profiles on recent past promotions, by organization, COSC, average time-in-grade, and the like.

Zero-Base Review of All Eligibles. After the initial get-together of our Board, individual members began work immediately on an examination of the records of all the eligibles. This requires a complete reading of the folders of every single eligible Grade 13 in the Agency! This is done to locate people who seem to be worthy of consideration for promotion, but who may have been overlooked by the Chiefs of Key Components when drawing up their nominations. Because the populations of eligible people are quite large, it is impossible for every member of a Board to read every file. So, the population is divided into alphabetically sequential subsets, and two Board members

---

[1] The criteria for promotion are published in NSA Regulation 11-10, Annex B, dated 7 January 1977.

[2] Eligibility for Grades 13 and 14 is 24 months in grade; for Grade 12 it is one year in grade.

read all the files in any subset. Even so, this still amounts to hundreds of files for each reader! But this procedure ensures that, during any one calendar year, every single person's file is read by at least four people for Grades 13 and 14, and by at least eight people for Grade 12's.

As part of the review process, all Board members are also asked to examine the files of all minorities and women. The Equal Employment Opportunity Office (D8) provides special lists to identify these people since this information is not contained in any of the other data available to the Board.

Names of potential candidates which are found by this review process are provided to the Key Component Chiefs so that they can prepare to answer the Board's questions about them, as well as about the people on their own lists of nominees.

Nomination Process. The nomination process carried out in the Key Component organizations is probably more complex, careful and formal than many people may know. In most organizations it is a multi-tiered process, with names first being submitted at some lower level in the organization, and then travelling upward for review by various boards until reaching the board at the Key Component level. Here a final decision is made about how many names the Key Component will nominate for promotion, which names will appear on the list, and what their order of priority will be. Key Component boards also decide about replacing, rearranging, adding or subtracting names from one cycle to the next. Any name which survives this process of constant review—a lengthy one in large organizations like DDO (Deputy Director for Operations)—has been considered by many people with a variety of backgrounds and experience. This, it seems to me, greatly increases the chances that the most capable and deserving people will in fact be nominated for promotion.

Two things result from the Key Component nomination process: a written promotion recommendation for each nominee, and a computer listing of all nominees in priority order. The promotion recommendation, which may run to some three or four pages, is prepared by the nominee's supervisor, and follows a format described in Annex C to NSA Regulation 11-10, of 7 January 1977.

* Background data
* Current Assignment
* Proposed assignment data
* Evaluation of the nominee against the criteria for promotion—experience, training, on-the-job performance, potential, personal attributes, and ability.

These recommendations are placed in the individuals' promotion folders where Board members review them during their reading of the files.

In the computer printout of nominees—a small listing this time—nominees are listed in priority order by the Key Component. (For DDO, extracts are provided for each Office.) This presents a very brief summary of each person by name, organization, job title, time at NSA, time in grade, professionalizations, and last three performance appraisals.

Field personnel appear in two lists: a prioritized list for all nominees submitted by the Deputy Director for Field Management and Evaluation (DDF), and one by individual sites.

Every Board member is responsible for reading the promotion folders for all persons nominated by the Key Components and for those persons turned up by the Board's own review processes.

All reading must be completed before the next step in the promotion process occurs—the management presentations, popularly called the Promotion Board hearings.

Management Presentations. When management presentations begin, so do the Board meetings—many, many of them. And it is here that one's duties on the Board tend to become a full-time job for several weeks. The purpose of these presentations is to give Key Component Chiefs an opportunity to present their nominees to the Board in person, to discuss their nominees' qualifications and accomplishments, and to answer the Board's questions about them. They also respond to questions about those whose names were submitted to them by the Board for consideration. In addition, some chiefs take advantage of this opportunity to present particular management problems and needs as they relate to the promotion process.

A typical management presentation goes like this. The Board members sit around a large table, with the "presenter"—a Key Component Chief or his representative— at one end. The Chairman and Executive Secretary sit off to the side. For a half hour to an hour, the presenter talks about his nominees. Styles of presentation vary. Some presenters go through the list in priority order, discussing each candidate briefly. Others are much more informal and may spend the time answering questions asked by Board members. Sometimes the Key Component Chief wants to highlight certain information and repeats things already known to the Board from its reading. Some Key Component Chiefs deliberately try to present information which adds to that gained from the reading. Others elaborate, talking about the person from angles which help the Board in its deliber-

ations. The give and take between the members and the presenters ranges from refreshing and candid to sometimes heated exchange. But it serves the purpose well, because while the chiefs are striving to present their nominees favorably, the members are working equally hard to get the unvarnished information they need to make a sound evaluation of the candidates.

These presentations typically last for a numbers of days. In addition to all the Key Component Chiefs, DDO Group Chiefs also address the Board. Also, chiefs of field sites usually have an opportunity at least once a year to appear before the Boards. The Worldwide Station Chiefs Conference, an annual event, is deliberately scheduled to take place during a cycle of the Boards, so that the chiefs can personally present their candidates. These presentations are in addition to the regular presentations by DDF.

The Selection Process. When all the reading has been completed and the last presentation is over, it is then time for the Board to get down to the business of selecting the people who are to be recommended for promotion. This is done in a series of meetings which usually take place over a week or so.

To help accomplish the selection, Board members are supplied with two things

* a ballot containing the names of all nominees, those submitted by the Key Component Chiefs, as well as those developed by the Board through its own reviews

* the number of promotions which the Board is empowered to give out[3]

Selection is made by balloting, with successive ballots being taken over several days until the entire allocated number of promotions is reached. Between votes, the Board has time for discussion, deliberation and research. Board members have equal voice in the voting; the Chairman and Secretary do not vote. In making selections, members tend to consider such factors as distribution by organization and COSC. But the fitness of the candidate is always the overriding criterion on which promotions are based.

The result of the voting process is a list of the Board's *recommendations* to the Director for promotions. Before the list goes to the Director, however, the Board provides each Key Component Chief with the names of the people in his organization who have been selected. Where the Board has made selections which alter the Chief's priority order, or has chosen someone not on his list, the Chief is given an opportunity to meet with the Board to discuss the effect of these choices. The Board then reviews its findings and makes its final recommendations. If any differences remain, they are summarized by the Chairman in a report to the Director which accompanies the list.

When the Director (for 14's and 15's) or D/DIR (for 13's) has approved the promotions[4], the Office of Civilian Personnel (M3) then schedules to promotion ceremonies in the Friedman Auditorium—one for the 13's and a combined one for the 14's and 15's.

For the members of my own Promotion Board, the promotion ceremony marked the successful culmination of a difficult and time-consuming task. It was fascinating to be able at last to put faces to the names which had become so familiar to us over the past several months. And we were exhilarated to have finished the job entrusted to us. The amount of work involved is tremendous—hours, days, even weeks, of sitting and reading the folders. And then there is the time spent evaluating, culling, and making the difficult final selections.

Board members take their assignments most seriously and work long hours in the knowledge that out of a mountain of material have to come decisions which they must labor to make fair to every employee, and which are sound to the future of the Agency.

---

[3] The NSA promotion program, including allocation of promotions, is described in an article by [redacted] in the NSA Newsletter of March 1979.

[4] The Director is empowered to add to or to delete from the Boards' recommendations.

P.L. 86-36

TO SUBSCRIBE TO CRYPTOLOG

CALL 1103s

Reprinted from KEYWORD, February 1973

...but on the other hand

Write 300 words on the best method of selecting an employee who will get a Division's sole promotion for the quarter, read one of the questions in a recent NSA writing exam. All of the answers were good; this one excels in the simplicity of the solution.

The methods used by managers to select employees for promotion have been the object of study and controversy for centuries. No method has been found to be universally satisfactory, and the study and argument will continue, as times and conditions change. Serious examination of the goals sought through employee promotion shows that there should be considerable flexibility. Not only are the goals diverse, but the conditions under which the organization operates vary.

In a Division of 100 people today there may be only one promotion per quarter; twenty years ago a Division of similar size might have had as many as 25 to 30 promotions per quarter. Other variants have been subject to similar degrees of change. Managers today must therefore be prepared to cope with these dramatic changes.

In the present situation, a serious backlog of promotion candidates has grown up. Most of these people are well qualified in performance, experience, education, personality, potential, and time in grade; and in a given list, most perhaps would be about even. In our Division of 100, promoting four persons per year means that every eight years we can get one promotion for each employee in the upper 25%, assuming we follow the conventional system. In this system, a small group of managers meet in secrecy to select candidates according to individual goals. The result today is loss of the upper 15% through transfer to other jobs, minority-group inequities, and low employee morale because of their lack of participation. A better method of achieving Division goals must be found.

The best method of selecting the employee who will get a Division's sole promotion for the quarter is a lottery. Chances can be allocated to eligible candidates in ration to the qualification on all counts. More (or fewer) chances can be allocated to a given grade of skill, or for a given employee quality, such as time in grade, or education. The lotteries can be held monthly, with quarterly runoffs, or just once every quarter in a winner-take-all event. Such a solution will remove the secrecy and result in much wider employee participation and higher morale. It is probably only a matter of time until this solution will be in use throughout the Civil Service.

CRYPTOLOG HAS MOVED!

CRYPTOLOG has moved to the eighth floor. The new address is 8A187, and the new phone numbers are 1103/1104/1105. Only the mailing address is unchanged; it still is CRYPTOLOG, P1.

PUNCTUATION:
More Than Meets the Eye

[redacted] A42

P.L. 86-36

I would like to share with the readers of CRYPTOLOG a nugget of Soviet humor that was given to me several years ago when I was a student at the U.S. Army Russian Institute (Detachment R) in Garmisch, Germany. I ran across it recently while rummaging through some dusty memorabilia, and decided it was too good to keep to myself.

The article is appropriate for at least two reasons: it is a reminder of the importance of punctuation marks; and it is perceptive commentary on man's declining ability to think for himself—especially in an Orwellian society such as that of the Soviet Union, where bureaucratic thinking and writing are so patently stereotyped.

A good friend, Oleg Konstantinovich Kavetsky, the language laboratory technician and general handyman at Det R, gave me the article and philosophized on its significance. Oleg saw it was a subtle condemnation of the typical Soviet bureaucrat, who is steepied in writing political Newspeak filled with liberal quotations from Lenin and Brezhnev. In my opinion, it also applies to our own bureaucratese.

Oleg is a remarkable person; I encourage all NSA studens who attend Det R to spend as much time as possible with him. He'll teach you some Russian you won't get in the classroom. A game of ping-pong or billiards becomes a drill in numbers—he calls it an "igra v vychislitel'nye," literally, a "game of numbers." He is filled with stories and anecdotes from his youth in the Soviet Union. And he can talk endlessly about each and every step involved in the building of his home. The article on punctuation marks that follows is typical of the kinds of things that Oleg often injects into his conversations. I hope you enjoy it as much as I did.

A man lost the comma and became afraid of complex sentences; he sought simpler phrases. With simple phrases came simple thoughts.

He then lost the exclamation point and began to speak softly, in a monotone. Nothing gave him joy or excited him; he related to everything without emotion.

Then he lost the question mark and ceased asking questions; nothing aroused his curiosity, no matter where it occurred—in space, on the earth or even in his own apartment.

Several years later he lost the colon and stopped explaining his actions to people.

By the end of his life he had only quotation marks. He never expressed an idea of his own, but was always quoting someone—and so he completely forgot how to think and came to the end.

Cherish the punctuation marks!

Человек потерял запятую, стал бояться сложных предложений, искал фразы попроще. За несложными фразами пришли несложные мысли.

Потом он потерял знак восклицательный и начал говорить тихо, с одной интонацией. Его уже ничто не радовало и не возмущало, он ко всему относился без эмоций.

Затем он потерял знак вопросительный и перестал задавать всякие вопросы, никакие события не вызывали его любопытства, где бы они ни происходили — в космосе, на Земле или даже в собственной квартире...

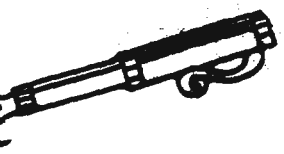
Еще через пару лет он потерял двоеточие и перестал объяснять людям свои поступки.

К концу жизни у него оставались только кавычки. Он не высказывал ни одной собственной идеи, он все время кого-нибудь цитировал — так он совсем разучился мыслить и дошел до точки.

Берегите знаки препинания!

г. Киев.

Letters to the Editor



EO 1.4.(c)
P.L. 86-36

To the Editor, CRYPTOLOG:

(U) It was just after a recent demonstration of the Radio Shack TRS-80 home computer that some of us got into a discussion about the problem of new equipment, and just how long we are going to have to wait to get to use it for any operational jobs.

~~(C)~~ The principal problem seems to be that all new electronic equipment that is built for general public use radiates and is therefore not useful for handling classified data. It ordinarily seems to take years for the equipment to be engineered in a model that controls or inhibits radiation enough to meet our standards. Meanwhile, the march of progress goes on, and newer and even more useful things appear in this rapidly developing field. But each new item also radiates (there being no commercial incentive to develop devices that don't).

(U) So by the time each new piece of gear is ready for your use (and mine), something better, or faster, or whatever, is available to any private user who can afford it, but not to us.

~~(C)~~ Well then, why don't we just try to find a way to screen the building, rather than each separate piece of equipment? I suppose the first quick answer is that there is no way to do that, but this place is full of people who can find ways to do things that aren't supposed to be possible. It may be expensive, when compared with screening (or otherwise fixing) each new piece of gear, but the cost would average out over the years pretty quickly, as we found we were able to cut years off the lead time for the practical use of state-of-the-art computery.

[redacted]
P14

S64 replies...

~~(C)~~ Although it's sometimes difficult to prevent RF energy from being transmitted, it's even harder to contain it after radiation occurs. For example, it's easier to reduce the current and voltage across a pair of contacts than to build a copper mesh room around them.

[redacted]

(U) We plan to apply some of these approaches to selected operational areas in the next few months. Permanent installation of any RFI suppression techniques will depend on the results of our experiments.

(U) I would like to say "Amen" to one statement made in [redacted] letter, namely: "...this place is full of people who can find ways to do things that aren't supposed to be possible." This is particularly true of CRYPTOLOG readers. If any readers have any ideas for "blanket" RFI suppression, we in S64 would like to hear them. Call or write [redacted] (2443s). One more thing: don't worry about a "not invented here" response; that's a disease we try to combat.

[redacted]
Chief, S64

P.L. 86-36

To the Editor, CRYPTOLOG:

(U) Having had long, and often passionate, discussions with both Mr. Buckley and Mr. [redacted] on the subject of Traffic Analysis "overages," I was surprised to see that both gentlemen missed several important points [see Letters to the Editor, CRYPTOLOG, July 1979].

(U) First, I think (please note, opinion) there are a fair number of individuals who hold TA COSCs who are not doing TA work. One example: a branch chief is a manager, not an analyst, yet the analytic COSC is often held.

(U) Second, quality is not an element included in the "bean-counter" approach; it's the number of bodies bearing the title that are counted. The fact that one quarter of the bodies may be doing three quarters of the work does not enter in.

EO 1.4.(c)
P.L. 86-36

DOCID: 4009830

~~(C)~~ Third, we seem desperately intent on trying to "professionalize" (read, certify) ever-increasing numbers of people in overage fields. The problem with this is twofold:

➤ What is the purpose of creating many more professionals than we have professional billets? What is the purpose of allowing second certifications in overage fields?

➤ Why are we tutoring professional aspirants? Individuals of professional quality will, like cream, rise to the top by dint of personal study and research. They will do so simply because it is in their nature to excel, not because they were pushed, prodded or carried through the test. (Please note that "top" refers to one's ability to perform, not to one's promotion record.)

~~(C-CCO)~~ I agree with [redacted] -we *are* losing our TA skills [see CRYPTOLOG, March 1979]. It is evident in the simple fact that many case analysts do not log intercept in such a manner as to see a simple rota. It is reinforced by the fact that on our professionalization exam the net reconstruction section is pre-logged and fairly easy. The difficult section is the crypto-TA part, and few traffic analysts are charged with this type of responsibility in their daily jobs.

(U) Suggested solutions for eliminating the overage and up-grading the quality are fairly simple. Ensure that only those doing traffic analysis carry that COSC; let's start calling managers managers. Next, devise a weighting system so that a manager can state for the TD that he needs three topflight TAs, or five average, or ten below-average (or some combination thereof) to accomplish his mission. And, finally, if we feel compelled to tutor someone, let's begin by tutoring those most in need so that they may become proficient in their current jobs.

(U) Years ago achieving professionalization was akin to winning a place among the elite. Today is is simply a means of proving oneself average. Elitism is not only dead, but is scorned as well.

(U) Let's put the emphasis back on the quality of our human resources.

[redacted] B32

LANGUAGE PROFICIENCY CERTIFICATES FOR MILITARY PERSONNEL

Capt Gary J. Twogood, M362

(UNCLASSIFIED in entirety)

On 4 April 1979, MG George L. McFadden, then Chief, DDO, presented certificates to 26 military linguists who passed NSA's Language Proficiency Test (LPT). The ceremony was one aspect of a continuing program to recognize the 30% of the military linguists who have passed the LPT. To date, 56 military linguists have been presented certificates in eleven languages. This total includes 26 individuals stationed overseas. P.L. 86-36

To identify the linguists whose scores were particularly high, the Agency established a policy of awarding the certificate "With Honors" to those who scored five or more points above passing in each portion of the LPT. We have since discovered that this arbitrary cutoff point was too low. To make the honors group more selective, we have have raised the cutoff, so that now a linguist must achieve 80% on the Completion protion and 90% on the Translation portion, or a Staten rating of eight on both portions.

Concurrent with the realignment of the "With Honors" criteria, we are beginning an official policy of awarding the LPT certificates retroactively. NSA directives state that LPT scores are valid for three years from the test date, and we will use this criterion as a cutoff for retroactivty. Linguists may request retroactive awards through NSA/M362, [redacted] To help verify test scores, M362 will need the name, SSN, service, grade, language, and (if available) test date and scores.

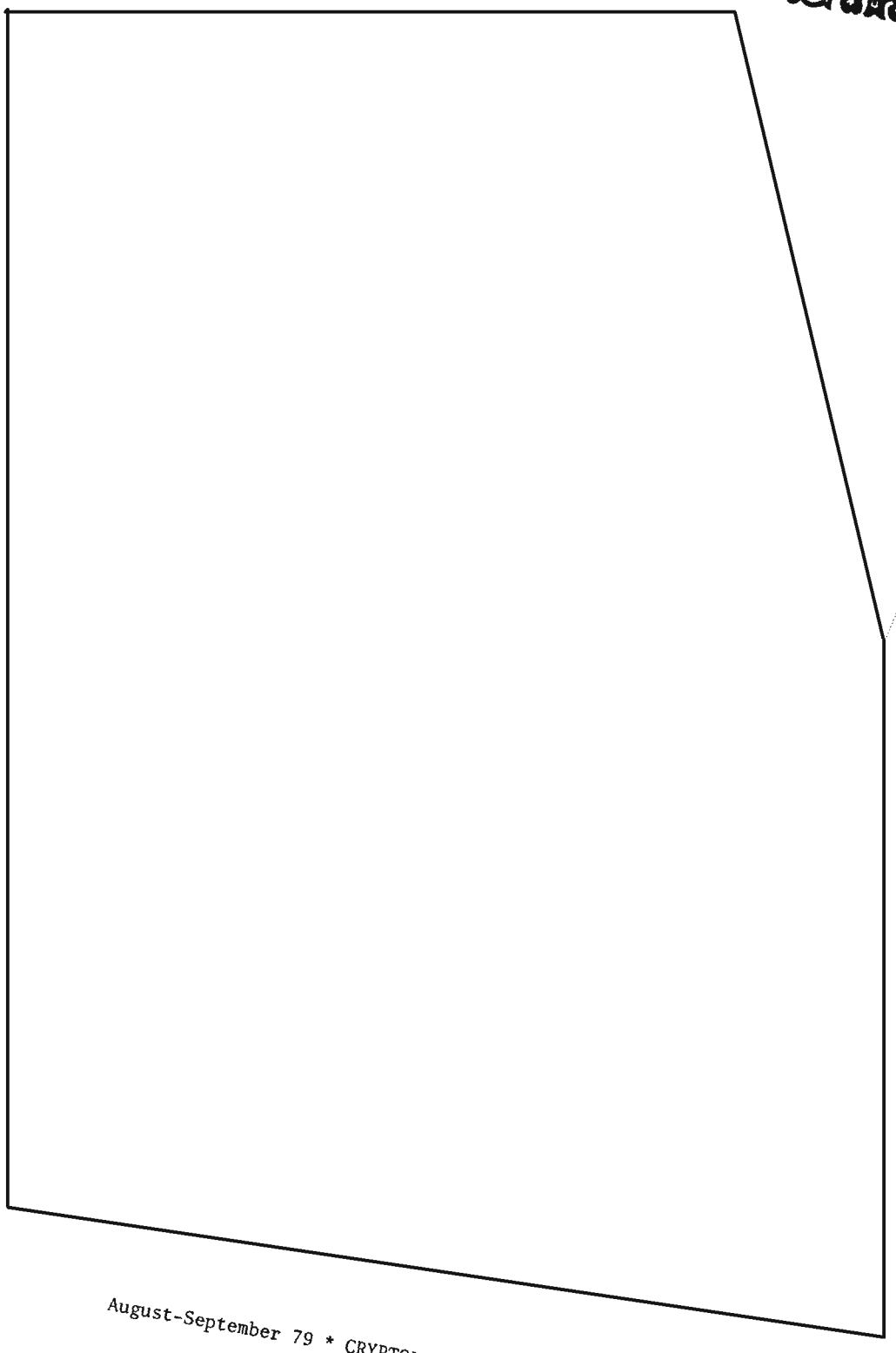
We appreciate the interest and support that has been shown throughout the cryptologic communit and look forward to even more military linguist participation in the future. P.L. 86-36

To begin a subscription to CRYPTOLOG, or to change the address on your present one, call CRYPTOLOG, ext 1103s.

DOCID: 4009830

~~SECRET SPOKE~~

MEMORABLE MEMOS (U)



P.L. 86-36
EO 1.4.(c)

~~SECRET SPOKE~~

News of the Communications Analysis Association

[redacted] P14

The present officers of the Communications Analysis Association are as follows:

President	[redacted]	3369s
President-Elect		3866s
Secretary		5585s
Treasurer		4398s
Board		5306s
		5492s
		5901s
Programs		4452s.
Crypto-TA SIG		4466s
Cryptologic History		2171s

- - - - - - - - - - - - - - - - - - -

Now! Membership in the CAA automatically gets your name on the CRYPTOLOG subscription list. For just one dollar a year, you can get every issue of CRYPTOLOG delivered right to your door (or wherever your IN-box happens to be), along with all of the announcements about the various activities and happenings of the CAA. Send your dollar, along with your present mailing address to our treasurer, [redacted] B62, Room 2S045.

Note: For those of you who *think* you are members of CAA, but who haven't been getting our announcements lately, look at the address label of the last one you received. If the number 78 appears on the label, then Dana has no record of receiving your 1979 dues.

NEWS OF THE CRYPTO-MATHEMATICS INSTITUTE

[redacted] R51

The Crypto-Mathematics Institute extends Associate Membership to all NSA Retired Employees who have been members of the CMI. Upon payment of the $2.00 annual fee, Associate Members will be put on the mailing list for current notices. These notices include announcement of monthly speakers, the problem department, and information concerning the Annual Essay Contest, the President's Award, and the Annual Banquet. Retired members are entitled to participate in the Essay Contest and to attend the banquet at regular CMI member rates. They may, or course, attend monthly lectures provided they have the appropriate security clearance and access to Agency spaces.

Any retiree and former member of the CMI who wishes to become an Associate Member should send his name, address, and $2.00 to

Director, National Security Agency
ATTN: [redacted] G95 P.L. 86-36
Fort George G. Meade, Maryland 20755

For further information, call [redacted] R51, ext 8718s.

Solution to NSA-Crostic No. 27, CRYPTOLOG, July, 1979.

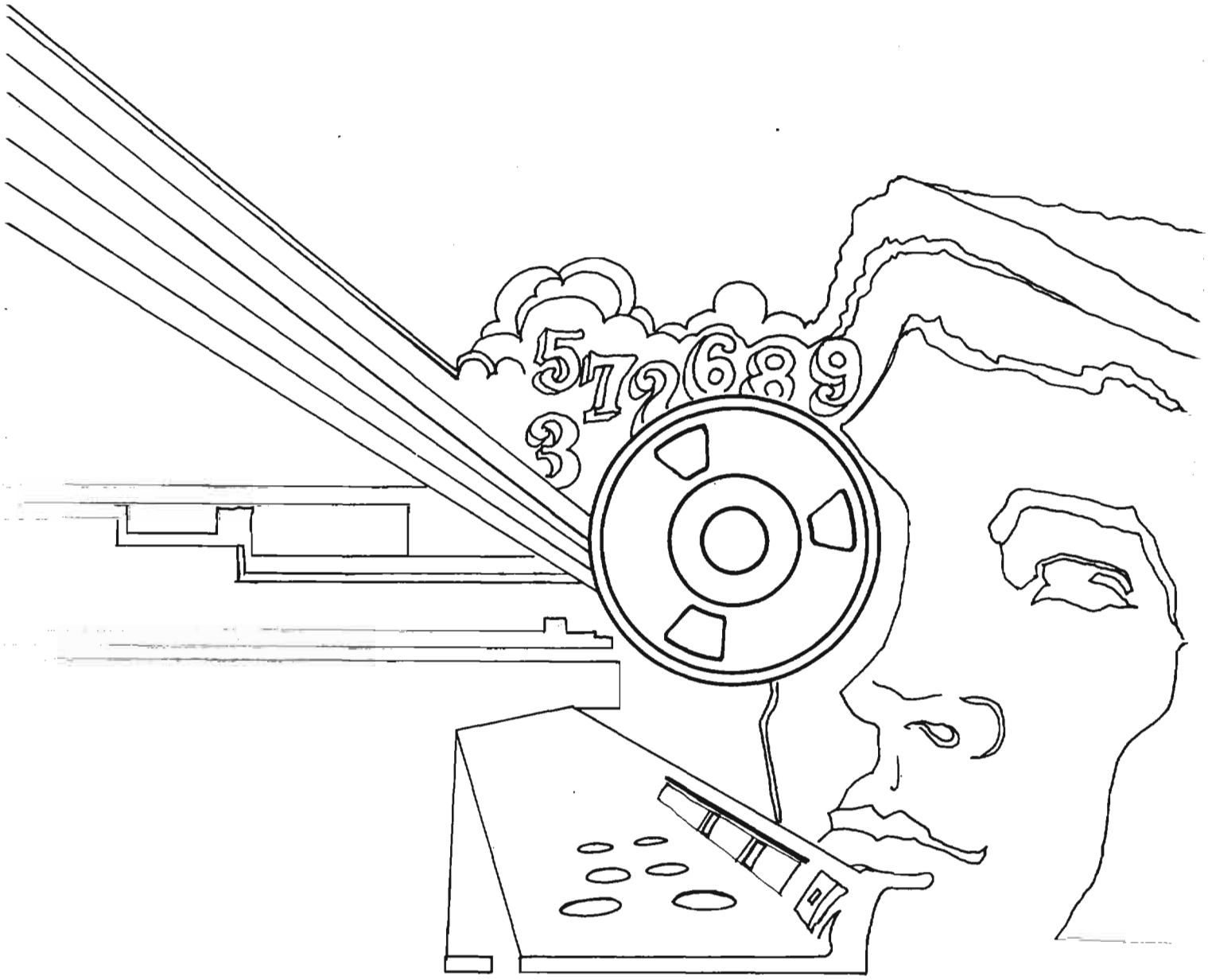
From a memo to General Ismay from Winston Churchill, 8 August 1943, quoted in "Coverterms," by Vera R. Filby, CRYPTOLOG, April, 1975.

"Operations in which large numbers of men may lose their lives ought not to be described by codewords which are calculated to invest the plan with an air of despondency, such as 'Woebetide,' 'Massacre,' 'Jumble,' 'Trouble,' 'Fidget' ... 'Pathetic,' and 'Jaundice.' They ought not to be names of frivolous character.

Further to the solution of "A Somewhat Larger Problem," published in the April issue. The first part of the solution appeared last month.

The callsigns are taken out of a large chart, the upper right corner of which is

[redacted]


5 7 2 6 8 9
3

DOCID: 4019668

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JULY 1979

SOURCE PROTECTION: OUR AGENCY'S INSURANCE POLICY (U).. [redacted] 1
NAVAL READINESS: A BASIS FOR COMPARISON (U)..... [redacted] .4
NSA-CROSTIC NO. 27 (U).....D.H.W.....8
WILT THOU, ANGELINA? (U).....Sydney Fairbanks.....10
GEARS OF THE MOUTH (U).....Donald Lasley.....11
LETTERS TO THE EDITOR (U).....14
EXPERT (U)..... [redacted] 16
SHOOTOUT AT THE SIGINT CORRAL (U)..... [redacted] 18

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 1 July 2009~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019668

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. VI, No. 7 July 1979

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor-in-Chief.....David H. Williams (3957s)

Collection..... [redacted] (8555s)

Cryptanalysis..... [redacted] (4902s)

Cryptolinguistics..... [redacted] (5981s)

Information Science..... [redacted] (3034s)

Language..... [redacted] (8161s)

Machine Support..... [redacted] (5084s)

Mathematics..... [redacted] (8518s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Taurone (3573s)

Production Manager.....Harry Goff (5236s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4019668

[redacted] V12

P.L. 86-36

SOURCE PROTECTION:

Our Agency's Insurance Policy (U)

(U) What kind of SIGINT baby was born to us in the 70s? What kind of delicate critter will cry for attention in the 80s? How shall we care for it? Viewed historically, it's a sure thing that tomorrow's SIGINT baby will be increasingly delicate, will require increasing attention to ensure its well-being, will both benefit and suffer from modern technology, and will face environmental challenges unimagined in years gone by. A thoroughly modern baby indeed! You can bet that this child of destiny will challenge our ingenuity to provide it security and continuity in the face of a changing world.

(U) SIGINT has become fragile. Contributing to this fragility are such factors as the development of new concepts for providing SIGINT support to military commanders, the sophistication of SIGINT technology, and a seemingly ever-increasing SIGINT audience.

(C CCO) SIGINT direct support units are now organic to the units they support. This brings new players into the game. In the past, only the Service Cryptologic Agencies had to worry about monitoring cryptologic skills; now, the supported command is involved. Whether Johnny and Joanie learn Mandarin and maintain proficiency in it are now the concerns of new members of the SIGINT world. These developments impact on the way NSA provides SIGINT support.

(S CCO) Thus, the SIGINT audience grows, as it has always done. This probably means that we SIGINTers are doing something right. The more people become aware of SIGINT, the greater is the demand for it. The greater the demand, the wider the distribution. The wider the distribution, the more people become aware of it ... and so on. The process continues even now. [redacted] One wonders where it will end. And while SIGINT producers might find in this some cause for feeling gratified, SIGINT security people cringe.

(S CCO) And as the audience grows, so does the number of players. [redacted]

(C CCO) SIGINT product was once mostly hard-copy and was sent to a small, selected readership. Now, distirubuion is largely electrical, and secondary distribution is just about anybody's guess. The trend for the future is toward cathode ray tube display — SOLIS, COINS, and FRITTER, for example. It is now very easy to access great volumes of SIGINT. CRT displays are open, generally, speaking, to all who can see. The systems, while secure, sort of stretch the conventional need-to-know principle. Thus, technologic sophistication has made it much more difficult to control what we disseminate and to monitor its security.

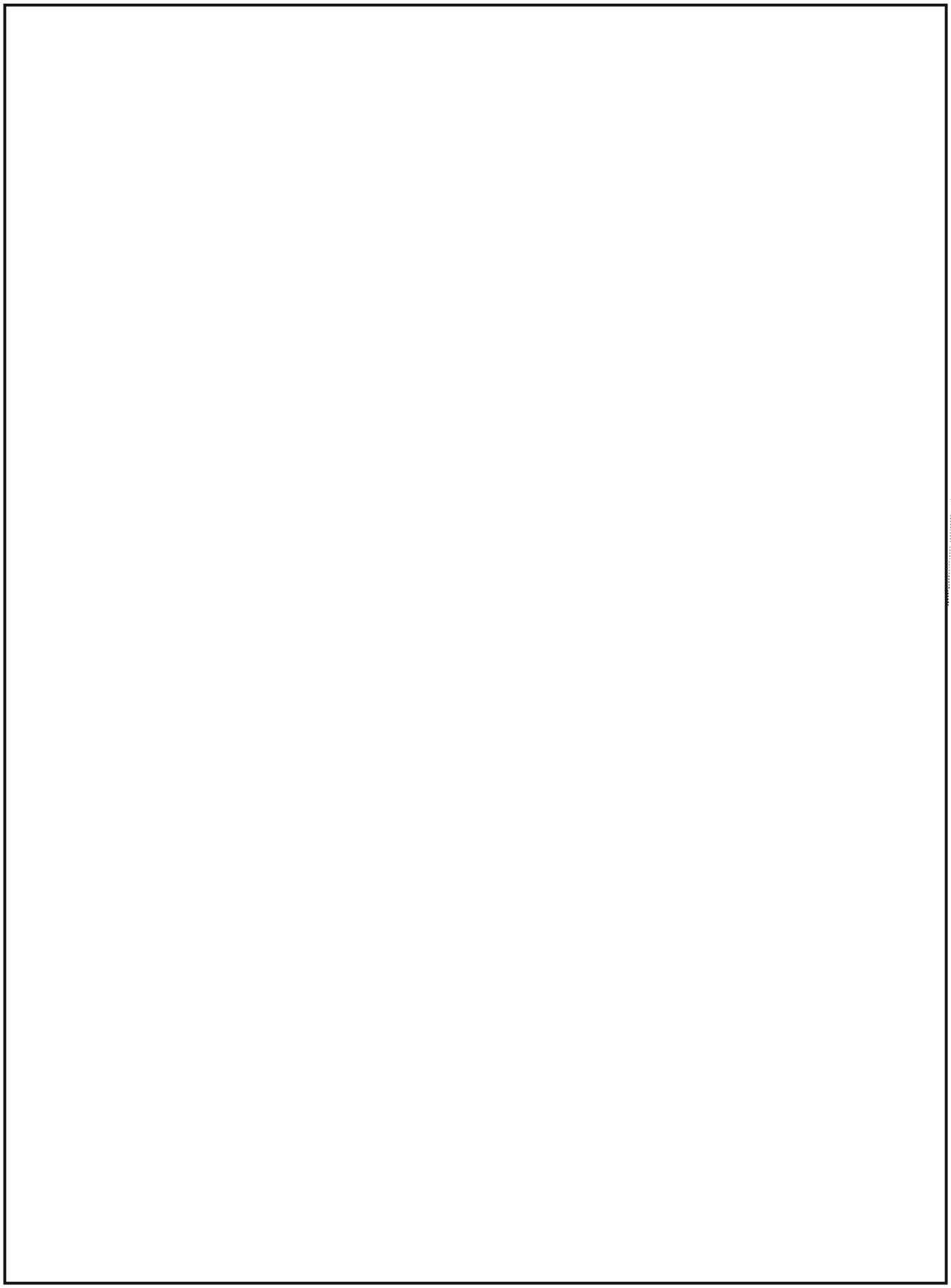
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

(U) As might be expected, security responses grew to match these developments. But these reactions were almost an unconscious development. No one dictated, for example, an increased emphasis on sanitization, but while, in the past, you seldom even heard the term, now it seems a daily topic of conversation. People who once thought sanitization had something to do with cleaning the restrooms are now requesting help in sanitizing COMINT.

(U) Well, it's high time we develop a conscious reaction to the security challenges of the day. But how do we increase the security of our product, even while providing it to an expanding readership? One obvious way is to reduce attribution to sources and methods as much as possible. Source attribution is not a buzz-phrase being forced on SIGINT reporters; rather, it is a sensible way of coping with some of today's problems. [redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

[redacted]

[redacted]

(U) This brings us to the point where all discussions of reporting lead: the requirements themselves. We must constantly be aware of current reporting policy, to ensure that we accept only those requirements which are consistent with our policy, and that those requirements are stated in a way that allows them to be met without violating our policy.

[redacted]

(U) Finally, a word of caution for us all. Even while rushing to eliminate excesses in source attribution we must be sure that adequate emphasis is given to retaining it when required. We must be careful not to throw out the baby with the bath water. That our product is SIGINT is evident; in fact, we want it known. The SIGINT connection is revealed in the address and the special intelligence caveat. The ultimate consideration is not concealing the connection with SIGINT; it is the protection of sources and methods.

EO 1.4.(c)
P.L. 86-36

DOCID: 4019668

A05

EO 1.4.(c)
P.L. 86-36

NAVAL READINESS:

A Basis for Comparison

Any study of contemporary naval readiness should be based on a historical naval readiness condition about which we already know. This provides a kind of analog in real time-and-space dimension, and is thus valuable for purposes of comparison, contrast and characterization.

There are several corners into which we might look for our lifelike model, such as the navies of the Soviet Union, North Korea, the People's Republic of China, or Israel. We have, in this country, a high regard for all of these navies—or so it would seem from the amount of intelligence, war-gaming, assessment, and propaganda devotion which we lavish upon them. But we often know less than we might about the readiness of these navies inasmuch as we are in their contemporary midst.

History is not only a good source for taking an example of naval readiness (or any other amorphous quality of the present), but it is also the *only* such source. We can only know with certainty that which has already past.

Accordingly, we shall examine briefly the readiness and reliability of the navy of Nazi Germany as it was at the outset of the Second World War, starting on September 1, 1939. We have excellent historical records about this, much analysis has already been done, and there are several late and living witnesses from the German Navy, among them Dönitz, Bekker, Werner, Ruge, Rohwer, and others. We shall examine a naval condition which a German might term *das Kriegsbereitschaft der Deutsches Marine*—the war readiness condition of the German Navy, or, more simply, serviceability. Through this, we shall be looking for specific places where parallels may be drawn with navies today, but without, however, the impossible necessity of finding equivalency.

Between 1933 and 1939, Nazi Germany devoted increasing proportions of its GNP to military production and to the creation of a great war machine, in anticipation of what is now known to have been an early intention of waging offensive warfare. German defense expenditures as a percentage of GNP rose from 3% in 1933 (the same as that of Great Britain) to 18% in 1939. (At the beginning of 1938, it was 8%; the allies, therefore, benefitted from over a year of indications and warning, foreknowledge of the Germans' intention.)

In 1933, the German naval inventory contained two major and twelve minor surface combatants (destroyers and greater). In 1939, submarine production amounted to 19% of the total naval inventory.

Given that a "non-creeping" buildup followed by war was contemplated, the Nazis' long-term naval production plan, the famed "Z-Plan," is of interest. This plan forecast naval production from the outset of hostilities (1939) to the final victory of the Fatherland (1947) and provided for both new classes and for replacements to war losses. Table 1 (next page) is extracted from the Z-Plan.

Thus, the Nazi naval planners conceived a grand plan for quintupling the number of ships in their navy in seven to eight years, while under arms—not to mention achieving a sixfold increase in overall tonnage. On February 2, 1943, Grand-Admiral Karl Dönitz issued a directive, on Hitler's order, to radically alter the Z-Plan production, to cease repairs and maintenance on battleships and cruisers (but not on destroyers and light forces), and to place the thus freed-up resources into land-based coastal defense and into the submarine service. Clearly, during the course of an extended conflict, a considerable distinction can develop between availability and intent at the outset and sustainability at mid-course. In a distinct sense, this is the internal rationale for continuing a war: to cripple the enemy's capability to continue. One is then running down his war machine with consequent effect on his posture and degree of readiness.

The overall availability of the German Navy on September 1, 1939, is interesting. Generally, except for battleships, it was high, as shown in Table 2.

	On Hand, 1939	Planned, by 1947
Great-Sized Battleships (Type H)	0	6
Battleships (Type GNEISENAU/BISMARCK)	2	4
Small Battleships (Type DEUTSCHLAND)	3	3
Battle Cruisers (Type P)	0	12
Heavy Cruisers	2	5
Light Cruisers (Type M)	0	24
Scout Cruisers	0	36
Destroyers	22	70
Corvettes	8	78
Aircraft Carriers	0	8
Submarines	66	249
Ocean	34	162
Coastal	32	60
Special	0	27
TOTAL	103	495

Table 1

Type	Number	Number Available	Percent Available	Remarks
Battleships	9	3	33.3	Two of the three available were old, WW I 13,200-ton ships.
Cruisers	11	6	54.5	BLUCHER was commissioned three weeks after September 1st; had she been available, she would have changed the availability factor to 63.6%
Destroyers	21	17	77.3	
Submarines	57	45	78.9	
Corvettes	12	10	83.3	
Coastal Light Forces	20	19	95.0	
Aircraft Carriers	1	0	0	
OVERALL (MEAN) AVAILABILITY			60.3	

Note: Availability information of 73 minesweepers and several auxiliary ships was not obtainable at this writing.

Table 2

The mean availability, if not high, is quite respectable. A navy knowing that it will soon be involved in war ought to consider sixty percent availability to be a decent minimum. If, in this case, however, the one 23,200-ton aircraft carrier (GRAF ZEPPELIN), which had been launched but not commisioned, is omitted from calculation, the overall German naval availability factor rises to 70.3%, a figure of some interest with which to compare the short-term notice availability of certain navies today.

The percentage of availability-by-type demonstrates a principle of naval readiness well known among naval specialists: that the smaller a combatant (therefore the less equipment and fewer sub-systems which comprise it), the more likely it is to be serviceable on short notice—given, of course, adequate facilities and professional attention. This principle appears to prevail irrespective of the ranges of classes and sizes, that is, whatever the size of the larger types, generally their availability will be less than that of the samller sizes. Also, this principle appears to hold without being directly borne on by the numbers of units in a class; thus, 17 of 21 destroyers is a higher percentage of availability than three of nine battleships, or six of eleven cruisers. Even among the largest unit-class, the battleships, it is the smaller ones which were available, that is, those of 12-14,000 tons, rather than those of 23-32,000 tons (this group also includes the one aircraft carrier). The availability of the corvettes (83.3%) and the coastal defense light forces (95.0%) is very high.

Submarines present a modification to the basic principle inasmuch as certain extra or specialized care is required for their maintenance and operation; on the other hand, they can be gotten up to full readiness more quickly than can most surface combatants. On September 1, 1939, 16 submarines were in their standby positions in the North Atlantic and the North Sea. By the end of the first week of the war on the continent, the number of operating submarines had doubled. No other type of German naval combatant ever matched this record in the course of the war in Europe. Operating battleships and cruisers never doubled in number. While the number of destroyers and corvettes in operational service more than doubled eventually, it was only after much longer periods, ranging from several weeks to several months.

As to the sustainability aspect of readiness, it has been noted above that wholly different values from those for availability may accrue. Specifically, the needs for modifications and the consequences of battle damage alter the overall readiness condition markedly. In the German case, in less than one year, that is, by the summer of 1940, the status of units out of action was as follows.

Type	Number In a Yard	Reason: Refit or Repair	Reason: Battle Damage	Percent of Total In Type Laid Up
Battleships	3	3	0	33.3
Cruisers	3	3	0	27.2
Destroyers	5	5	0	21.7
Corvettes	3	3	0	13.0
Coastal Light Boats	17	12	5	42.5
Submarines	3	3	0	5.0
Aircraft carrier (Launched on August 12, 1938, but never commissioned)				
MEAN PERCENTAGE OF ALL SHIPS OUT OF ACTION				23.8

Table 3

Thus, without the U.S. Navy having yet come into the war, and without the Battle of the Atlantic having yet begun, almost one-fourth of the German combatants were out of action after about ten months of warfare. (In addition to the above, eleven auxiliaries were also undergoing yard work for either refit or battle damage.)

DOCID: 4019668

An effectiveness assessment of the German Navy throughout World War II yields quite a different story—one which highlights the extreme usefulness of naval policies, programs, and strategies which are centered on submarines. Capital warships either could not be completed building or suffered early, decisive losses. These ships (battleships and cruisers) subsequently were sharply underemployed, owing to very high cost per unit, as well as to consequent changes in strategies. Destroyers and corvettes were variously over- and under-utilized. By early 1943, submarines had become the principal German naval combatant and were used with considerable effectiveness.

According to Rohwer, by September 1944 the twenty most successful submarines had sunk 573 Allied non-naval (mostly merchant) ships totalling 3,297,685 tons. In addition, eight naval ships—two destroyers, one battleship, one cruiser, one submarine, one corvette, and two auxiliaries—were destroyed. This accomplishment was attained with an investment of 166 submarine missions amounting to a total of 6,028 ship-days. Although the effectiveness of individual submarines varied greatly, the overall *average* effectiveness of the German submarine service was as shown below in Table 4.

Average number of non-naval ships sunk per submarine	28.69
Average number of all ships sunk per submarine	29.05
Number of ships sunk per submarine mission	3.50
Non-combatant tonnage sunk per ship-day	570.06
Average number of ships sunk per ton (surfaced) of all 20 leading submarines	.021
Average tonnage sunk per ton (surfaced) of all 20 leading submarines (Or, expressed otherwise, a 121:1 return on investment!)	121.23
Average submarine utilization, over a five-year period	8.3 missions per submarine, or 301.4 ship-days per submarine

Table 4

This amounts to an average of 16.5% of the five-year period spent at sea, with a yield of 570 tons per ship-day over that period.

This submarine effectiveness was achieved in spite of serious technical and design deficiencies in torpedoes during the first two years, in spite of late (1942) policy and program changes in strong favor of submarine production, and against the increasing odds thrown up by Allied convoy and anti-submarine warfare practices.

The Z-Plan called for the delivery of 249 submarines by 1947. Instead total production ran to 1,170 submarines by 1945. Of these, between 1939 and 1945, 630 were lost to enemy action at sea: 81 were destroyed in home waters; 42 were lost by accident; 215 were scuttled; 38 were retired; 11 were interned; and 153 were surrendered. Overall, 91.7% of the German submarines were lost as a result of various Allied military actions. Direct combat losses amounted to 60.7% of the final total production, but this required nearly six years of warfare. In the end, a lack of sustainability rather than initial (or even mid-term) availability resulted in the total collapse of German naval readiness.

In the preface to his *Hitler's Naval War*,[1] Cajus Bekker states

> The momentum of the German war effort was in fact only enough to last two, or at most, three, years after the reserves ran out, and though the arms industry continued production, this lagged increasingly behind the enemy and his sources of supply.

---

1. Kensington Publishing Corp, New York, 1974.

AUTHOR'S NOTE: The analysis in this article is that of the author and any faults are his. The intention is to provide a brief basis for comparative naval studies with respect to readiness. Extensive data and more complete analyses upon which this material is based is contained, *inter alia*, in the works of Mr. Cajus Bekker, Dr. Jurgen Rohwer, and Congressman Les Aspin of Wisconsin.

NSA-Crostic No. 27

By D.H.W.

DEFINITIONS

A. Sousa composition (3 wds)

B. American humorist and actor ("Steamboat Round the Bend"), 1876-1944 (full name)

C. Perpetual dummy of the bridge columns

D. Right at sea

E. "Strange such high dispute should be-
'Twixt _____." *On the Feuds Between Handel and Bononcini,* John Byrom, 1725 (3 wds)

F. For pushing the foul-mouthed laboratory duplicate off the rooftop, the police charged him with making an _____. (3 wds)

G. Amerind (var.)

H. Virginia _____

I. Author of *A Message to Garcia*

J. _____ Darby

K. Characterizing a perfectly ordinary mussel entree (3 wds, foll. by Word Y)

L. Palindromic Honda

M. Bullied, intimidated

N. Where Dorothy's dog's most recent meal is (2 wds)

O. Miss Ullmann

P. Lascivious

Q. Formed an incorrect opinion

R. One with an exaggerated sense of self-importance

WORDS

145 234 66 55 45 195 21 6 170 216 131 229

51 180 164 93 81 188 201

15 224 84 7 136 108 237 52 165 70

209 8 235 60 111

220 42 123 4 73 39 98 20 134

238 13 219 174 152 47 179 77 140 154 115 23

101 208 117 3 199 128 228 41 64 185 22

204 148 29 232 100 9 107 198 38 80 133 161

223 217 173 166

34 236 106 158 192 227

95 160 129 50 181 153 169

207 96 214 62 5 28 196

171 113 2 149 68

125 24 12 221 31 59 142 65

67 151 226 197 75

17 112 87 200 61 46 78 177

69 190 211 126 186 103

114 104 49

97 202 16 120 44 240 213 230 83

25 225 157 162 194 72 206 239 82

71 54 132 11 40 183

S. Cambridge's *other* institution of higher learning (2 wds, foll. by Word T)

32 182 130 144 193 92 233 163 156 27 168 110

10 86 57 139 150 176 119 205 109 91

T. See Word S (2 wds)

146 222 56 215 137 85 116 1 18 76 178 37

U. The best-dressed people in Mecca (2 wds, foll. by Word V)

212 43 167 141 88 187 159

V. See Word U (2 wds)

210 175 19 90 121 26 138

W. In the same place (Lat.)

124 172 48 191 63 218

X. European capital

231 58 127 118 143

Y. See Word K

35 30 53 94 147

Z. Avon lady (2 wds)

36 122 105 33 14 189 102 184 155 79 89 74

a. Still

203 135 99

1 T	2 J	3 E	4 D	5 I	6 A	7 B	8 C	9 F	10 S	■	11 R	12 K	■	13 E	14 Z	15 B	16 P
17 M	■	18 T	19 V	20 D	21 A	22 E	■	23 E	24 K	25 Q	26 V	27 S	28 I	29 F	■	30 Y	31 K
■	32 S	33 Z	34 G	■	35 Y	36 Z	37 T	■	38 F	39 D	40 R	41 E	■	42 D	43 U	44 P	45 A
46 M	■	47 E	48 W	49 O	50 H	51 A	■	52 B	53 Y	54 R	55 A	56 T	■	57 S	58 X	59 K	■
60 C	61 M	■	62 I	63 W	■	64 E	65 K	66 A	67 L	68 J	69 N	70 B	71 R	72 Q	■	73 D	74 Z
■	75 L	76 T	77 E	78 M	79 Z	80 F	81 A	82 Q	83 P	■	84 B	85 T	86 S	87 M	88 U	■	89 Z
90 V	91 S	■	92 S	93 A	94 Y	95 H	96 I	97 P	98 D	99 a	100 F	101 E	■	102 Z	103 N	■	104 O
105 Z	106 G	107 F	108 B	109 S	■	110 S	111 C	112 M	■	113 J	114 O	115 E	116 T	■	117 E	118 X	119 S
120 P	■	121 V	122 Z	■	123 D	124 W	125 K	■	126 N	127 X	■	128 E	129 H	130 S	131 A	132 R	133 F
134 D	135 a	136 B	137 T	138 V	■	139 S	140 E	141 U	142 K	■	143 X	144 S	■	145 A	146 T	147 Y	148 F
149 J	150 S	151 L	152 E	153 H	■	154 E	155 Z	156 S	157 Q	158 G	159 U	160 H	161 F	■	162 Q	163 S	164 A
165 B	166 F	167 U	■	168 S	169 H	170 A	171 J	172 W	173 F	174 E	■	175 V	176 S	177 M	178 T	179 E	180 A
■	181 H	182 S	183 R	184 Z	185 E	186 N	187 U	188 A	■	189 Z	190 N	191 W	■	192 G	193 S	194 Q	195 A
196 I	197 L	198 F	199 E	■	200 M	201 A	202 P	203 a	■	204 F	205 S	206 Q	207 I	208 E	■	209 C	210 V
211 N	■	212 U	213 P	■	214 I	215 T	■	216 A	217 F	218 W	219 E	220 D	■	221 K	222 T	■	223 F
224 B	225 Q	226 L	227 G	228 E	229 A	230 P	231 X	■	232 F	233 S	234 A	235 C	236 G	237 B	238 E	239 Q	240 P

Wilt Thou, Angelina..?

SYDNEY FAIRBANKS

"Whom are you?" said Cyril, for he had been to night-school.
—George Ade.

One of the more charming frailties of actual speech goes by the rather stuffy name of hyper-urbanism, signifying that the speaker is trying too hard to sound like a "city feller." There are plenty of familiar instances. Tell a Cockney not to say "'orse" for "horse" and he will presently call an outrage "a houtrage." Reprove his sister, who works in a Tea Shoppe, for calling a plate a "plite" and she will want to be "nace and refaned." Persuade a Brooklynite not to say "poil" for "pearl" and he will practice hard at saying "pernt" for "point"—or alternatively he will develop an extraordinary diphthong, something like that of the French *feuille*, which makes it impossible to convict him of error, and equally impossible to tell whether he means "curl" or "coil."

Similarly in matters of syntax, if you train little Johnnie not to say he seen a Good Humor man, he will tell you that he wants to saw another; and apparently if you teach fifty million children not to say "him and me are going fishing," forty-nine million will grow up saying, "between you and I." We heard the other day of an unfortunate secretary, within the confines of this institution, who after one or two angry snubs no longer dares correct this idiom in her tyrant's correspondence. Our heart bleeds at the thought.

Secretaries themselves, however, have one form of hyper-urbanity to which they tend to succumb in large numbers. Ask a victim to do something for you, and she answers in tones of conscious rectitude, "Yes, I shall."

It would be a brave man who would tackle the little matter of "shall" and "will"—representing, in the first person, futurity and volition, respectively—within the limitations of two pages of print. Suffice it to say that a question uses the form of the expected, or rather the invited answer:

"Shall you (fut.) be in town tomorrow, and if so will you (vol.) send him a telegram."

"Of course I will (vol.), I shall be glad to. Shall I (vol.) send it collect?"

"Yes. Will you (vol.)?"

"Shall I" seems to reverse the rule, but this is because it invites an answer in the *second* person, and for the second and third persons "will" stands for futurity and "shall" for volition (of the speaker). Thus "Shall I compare thee to a summer's day?" *invites* the answering command "Thou shalt..." although what is probably *expected* is an ecstatic "Oh, William, *would* you?" But this is a digression.

Colloquial usage, of course, is "I will" for everything, even an undesired futurity: "If I do that I will be fired." Only "shall I" survives, like a fragment of an ancient ruin protruding through the level turf. Thus, reverting to our original theses, when a lady is asked to do a favor she should answer, whether colloquially or formally, "I will."—excluding, of course, the more frequent case where the proper answer is "No."

One wonders, by the way, whether when the secretary marries her boss, and "Wilt thou, Angelina...? is intoned amid orange blossoms, she answers crisply "Yes, I shall."

It may be said that we are not concerned, as an editor, with spoken language, but only with what is printed. In fact we said as much ourselves about six months ago when someone asked us to voice a protest about a growing tendency to say "I could care less." But last week, sure as death, we saw it in print. Unfortunately, ours is, we like to think, a mild and mannered pen, incapable of excoriating the perpetrators. However: the English sentence (gentle non-reader) which says in five neat sylables precisely what it means, is "I couldn't care less." It is hard to improve on it. Evidently it would be unfair to expect you to *understand* what you hear, but could you, perhaps, *listen* a little more closely?

Aw, gee, mom, what's the use?

(Reprinted from *The NSA Technical Journal*, April 1959

Gears of the Mouth (U)

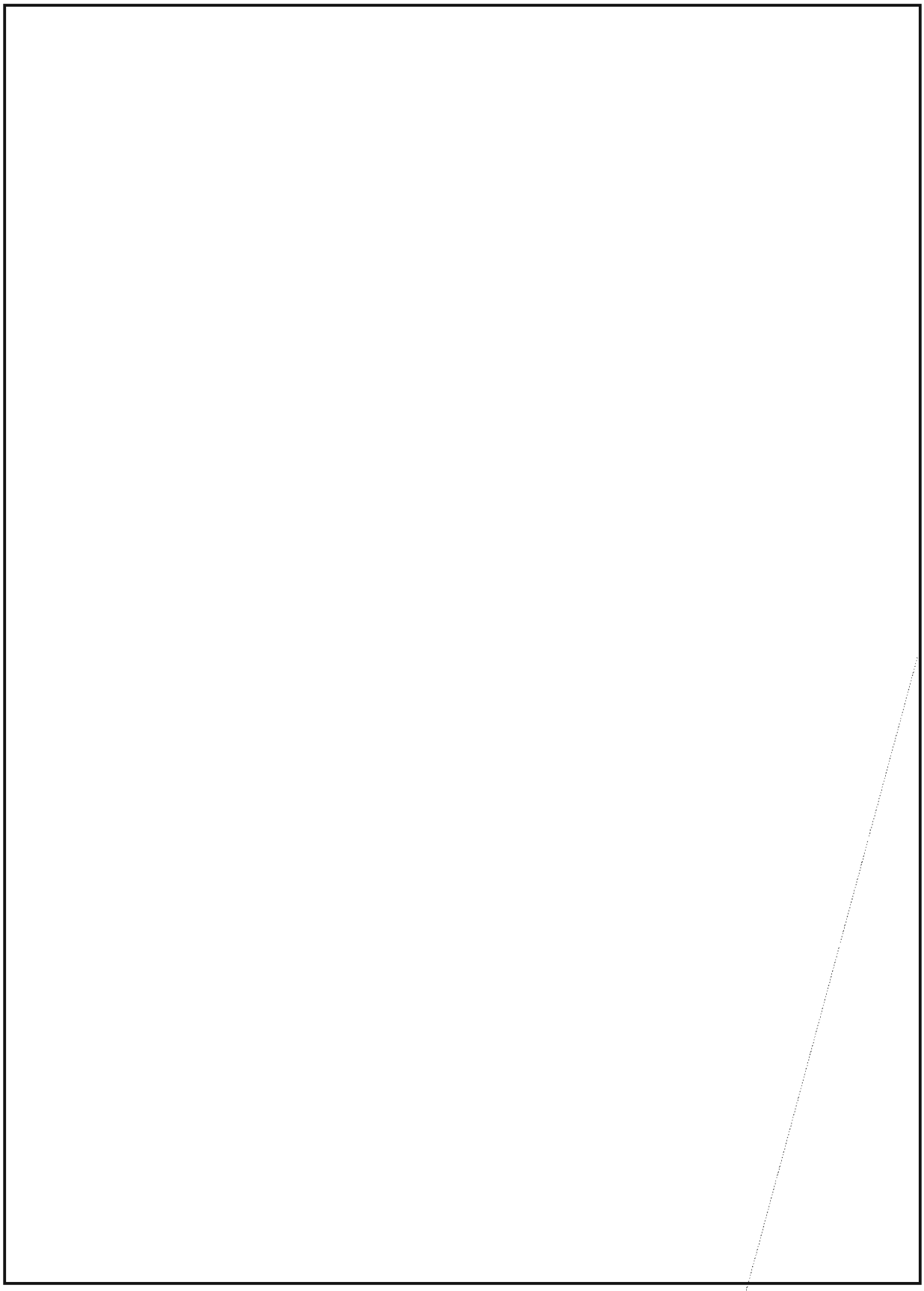
Donald Lasley, A41

This article was originally delivered as an address at the Language Quality Control Symposium of March 1970. It is just as pertinent today as it was then. dhw

(U) When I was asked to speak on the subject of language quality control, I accepted, confident that I knew enough about it to speak extemporaneously. Since then I have given considerable thought to the subject and have reached the conclusion that language quality control is extremely complex and that I really have much to learn about it. I am somewhat knowledgeable, however, on the subject of the lack of language quality control.

~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

DOCID: 4019668

EO 1.4.(c)
P.L. 86-36

(U) What is language quality control? Quality control has been defined as

> an aggregate of functions designed to insure adequate quality in manufactured products by initial critical study of engineering design, materials, processes, equipment and workmanship followed by periodic inspection and analysis of the results of inspection to determine causes for defects and by removal of such causes.

I suggest that language quality control is

> an aggregate of functions designed to insure adequate quality in product based on language through management of linguistic resources followed by periodic inspection and analysis of the results of inspection to determine causes for defects and by removal of such causes.

The key to language quality control is the management of linguistic resources. This includes the recruitment, the training, the organization, the utilization, and the support of such resources.

(U) Some of the questions we ought to ask ourselves are

- Are we recruiting the most talented people?
- Are we measuring talent by a reliable yardstick?
- Do we use the measurement once we have it?
- Is training, whether formal or OJT, adequate? Do we effectively plan and utilize training?
- Are we properly organized for efficient operation?
- Do we provide adequate supervision and checking?
- Do we utilize linguists efficiently?
- Is linguistic support adequate? Do we have the research aids, working aids, machine aids, files and books that are needed?

(U) To conclude, while I have probably not contributed much to your overall knowledge in this discussion, I hope I may have brought out some aspects of language quality control in a new light, and that I may have stimulated some thought and even further discussion of this very important and very real problem.

UNCLASSIFIED

RUSSIAN HANDBOOK OF SPOKEN USAGE, VOL. 3

Volume 3 of the *Russian Handbook of Spoken Usage* is scheduled to be distributed at about the end of July. It covers the Russian letters T through Ф. Copies will be issued through organizational channels, but analysts who fail to receive a copy may request one directly by contacting the P16 Publications Officer, Harry Goff, ext. 5642s or 5236s.

The *Russian Handbook* is a reference aid containing items which are not found, or are very incompletely treated, in standard dictionaries, but which occur in the spoken language, such as

- Detailed explanations of words that express speakers' emotions and attitudes—surprise, annoyance, approval, disagreement, uncertainty, and the like
- Characteristically colloquial constructions
- Points of syntax and usage
- Uneducated, regional, or otherwise nonstandard froms and constructions and vocabulary items.

When complete, the *Handbook* will consist of five volumes. Vols. 1 through 4 will contain Russian words, arranged in Russian alphabetical order, while Vol. 5 will contain articles under grammatical headings, such as Infinitive, Perfective, and so on, listed in English alphabetical order. The *Handbook* is UNCLASSIFIED.

Copies of earlier volumes are also available, including a ring binder which will hold all three of the published volumes.

UNCLASSIFIED

Letters To the Editor

Last month CRYPTOLOG printed a letter from Kathy Bjorklund in which she wondered why the view of traffic analysts as a vanishing breed, which has been expressed in CRYPTOLOG by various people, is at such variance with the M3 view of TA personnel as an overstrength category.

To the Editor, CRYPTOLOG:

(U) Since you were kind enough to ask me for a comment on Kathy Bjorklund's letter, I felt obligated to break out [redacted] article, to which she referred. There are several hot spots in those two items and one that rises from them.

(U) First, CRYPTOLOG has traditionally been an open forum, and I would not change that. But we who write for it from time to time are obligated to do some homework before we present opinions that aren't defensible. Or, maybe it's time to label fact and opinion so that readers can sort them out.

(U) For Kathy, here are a couple of facts. While your briefing on reassimilation and career field overages were probably conducted by personnel or administrative people, they are not the ones who made the decision that TA is an overage field. As your Chief of Personnel Services, [redacted] could have told you, M3 is part of Management Services (DDM), and it is a support or service organization that attempts to meet *requirements established by other Key Components*. In this case, it was Operations (DDO) telling M3 that there were overages in the TA field and shortages in the language field; it was DDO telling M3 to initiate the needed personnel actions, e.g., reassignments and hiring. Can you imagine the confusion if M3 went about willy-nilly hiring and reassigning people against no known requirements?

(U) Another fact is that George's article is mostly opinion. Now he has as much right as anyone else to have and express those opinions, but he knows he will get some arguments. For example, we not only lost good analysts when some TAs moved into management—we also gained some bad managers, although that's not a problem peculiar to the field of TA.

(U) But by and large, I doubt that you could find anyone who has to pick up the tab in billets or skills balances who would say we have any current or near future shortage of traffic analysts, or of TA Technicians to fill the vacancies that will some day exist in the analyst ranks.

(U) Comparing real and present shortages in the language and computer arenas to "maybe" shortages ten years down the pike may not be a fair analogy. The computer and language shortfalls are there because we have added jobs or lived with vacant positions. In the field of TA that has not been, and is not now, the case.

(U) Since most of our TA overages are at the technician level, I'm not sure I understand George's suggestion that we hire more technicians. But my not understanding is irrelevant—we aren't going to hire against a non-requirement, at least not if I understand the way things work.

P.L. 86-36

(U) Back to Kathy's letter for a final comment on her last statement: "...talent returning from overseas should not be regarded as a magic ingredient for such a brew." Given our selection processes, increased promotion points, and preferential treatment in assignments upon return for field people, I am a bit surprised that you believe there is an *intentional* negative attitude toward returning field people. And my opinion is that DDO, DDM, DDR, DDT and DDF would be equally surprised.

(U) Regards to you, Kathy. Congratulations to you, George. And, Dave, whenever you want an opposing view on almost any subject, please give me a call.

Dan Buckley, M03

To the Editor, CRYPTOLOG:

(U) I read Kathy Bjorklund's letter with a feeling of depression—because what she says is all too true. The bodies-and-slots, or bean-counting, approach to personnel assignments is not one which is conducive to the continued development of the technical work force of the Agency.

~~(C)~~ During the skills requirement forecast of 1973, the career panels were asked various questions on personnel development covering the period FY74 through FY79. Questions such as the following were asked:

—What effect will new or emerging technology and modernization of cryptologic operations have on the skills under the purview of your career panel?

—Do you anticipate a need for developing multi-skilled specialists, and if so, which skills or combinations of skills will be required:

—Will the need for specific skills (TA, CA, etc.) decline or increase?

(U) I don't know what happened to the results of this poll, since current personnel planning does not seem to reflect them, but rather continues to be based on projections of the current work force: How many people do we have in such-and-such COSC? Well, then, if we have that many, and if we are getting the work done, then that must be the right number. So let's just straightline that number for the next four fiscal years. Obvious, this approach is the basis for faulty TDs, since it makes no allowance for any shifts in requirements brought about by shifts in targets or other considerations.

~~(C)~~ Let's see how this works. At the moment Traffic Analysis is carried as an overstrength skill in A Group. The TACP has two interns due to graduate this month. On the basis of their backgrounds, experience, the panel's recommendations and their own preferences these interns should be assigned to A2. But the thought of placing them in an overstrength element is enough to give the bureaucrats heartburn.

~~(C)~~ The placement of overseas returnees is similar. P41 attempts to assign personnel holding A Group overage skills to B, G, V or W; only a few of this year's returnees have been assigned to A.

~~(C)~~ In short, P41 and M3 will almost always stand in the way of any assignment to an overstrength element. I have accused P41 of approving TA intern placements using the bean-counter approach. They deny this vehemently, yet state in writing, in a memo to Chief, M3:

[redacted]

A fair share—by the numbers!

(U) [redacted] quoted by Ms. Bjorklund in her letter, are correct: the number of traffic analysts is dwindling. Part of this is attributable to the reasons cited above. Another rank-thinning factor is age. Almost twenty percent of the people in COSC 1411, Traffic Analyst, are over 50 years of age; less than two percent are under 30.

(U) What is the solution? As I see it, it is two-fold. An immediate measure would be some directed assignments. This would include the identification of personnel holding a given COSC in an overstrength area, but not performing that function, and making appropriate readjustments, such as transfer, retraining or reclassification. It would also include the placing of overseas returnees in areas where their skills are most needed, even where there might be a temporary overstrength condition.

(U) For the longer term we must nurture the TA intern hire, insuring that we have at least six to ten coming in each year, and placing them in the work force where they will produce for the Agency regardless of numbers or quotas.

~~(C)~~ Let me quote from an old-time member of the TA corps.

> "How long does it take to build a professional traffic analyst from zero? If it takes, say, five years, then we are betting that whatever the situation is today, it will be the same five years from now. And what we are betting with is the Agency's reputation for adapting to fast-breaking changes in the world situation."

~~(C)~~ The TA intern program can and does build a professional traffic-analyst-reporter from zero with a very solid understanding of the interrelationships of the other cryptologic disciplines. The annual hiring of a few bright people—recent college graduates as well as former military analysts—should solve the problem of being able to find good traffic analytic talent in the future.

[redacted] H115
Executive, TACP

To the Editor, CRYPTOLOG:

Permit me to comment on [redacted] article "Fear of Testing" which appeared in your April 1979 issue. This piece is obviously aimed at the younger employee approaching professionalization testing with some trepidation. But what of the older, pre-Age of Professionaliztion employeee, for whom it is not a question of *phobia*, but one of *principle?*

(Continued on Page 21)

~~CONFIDENTIAL~~

P.L. 86-36

P.L. 86-36
EO 1.4.(c)

EXPERT (U) [redacted] G65

[redacted]

[redacted]

[redacted]

EO 1.4.(c)
P.L. 86-36

[redacted]

Provisions have been made for inclusion of other information fields that may be required, or which are unique to an individual office.

[redacted]

2. Defined in USSID 300 as information about foreign communications or signals, observed through signals collection or derived through analysis.

(U) In its early formative years, EXPERT's data and programs resided on the IBM 360/65

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~CONFIDENTIAL~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

[redacted]

[redacted]

(U) The problem of automating NSA-originated product information into EXPERT has not yet been resolved. Automation of G product may become possible when a [redacted] system is fully implemented.

[redacted]

[redacted]

(U) Initially, in 1968, when EXPERT was only a theory, it was envisioned as an Agency-wide system. While that vision may never be attained, it is coming closer now that B and G are both using it. P.L. 86-36 EO 1.4.(d)

~~(C-CCO)~~ Over the years, EXPERT has proven to be a useful system in meeting G's objectives. Today, to a greater degree than ever, it is being used to correlate SIGINT product information and corresponding target information, to assess productivity, and to help develop management policies.

~~(C-CCO)~~ EXPERT will be close to becoming an automated SIGINT end product information system when the match-merging of field product information is implemented. It can become fully automated with the advent of an Agency-wide [redacted] system. EXPERT might then be defined as an automated SIGINT product information system capable of answering the what, who, when, why, how, and where questions in full, and of providing this information on a timely basis to its users. P.L. 86-36

---

3. Defined in USSID 300 as the identification of the person, headquarters, or other target authority which has authorized or caused thr transmission of the collected signal. It identifies, in effect the "drafter" or "releaser" of the message collected, or the organization which "sponsored" the transmission of the signal.

4. Writing on this subject two years ago, [redacted] quoted this remark from a translator: "I used to like to finish a translation so I could get a new one to start. Now I dread it, and put it off, because I'll have to make the EXPERT sheet." ("It's Got to Get Out Today," *CRYPTOLOG*, April 1977) P.L. 86-36

P.L. 86-36

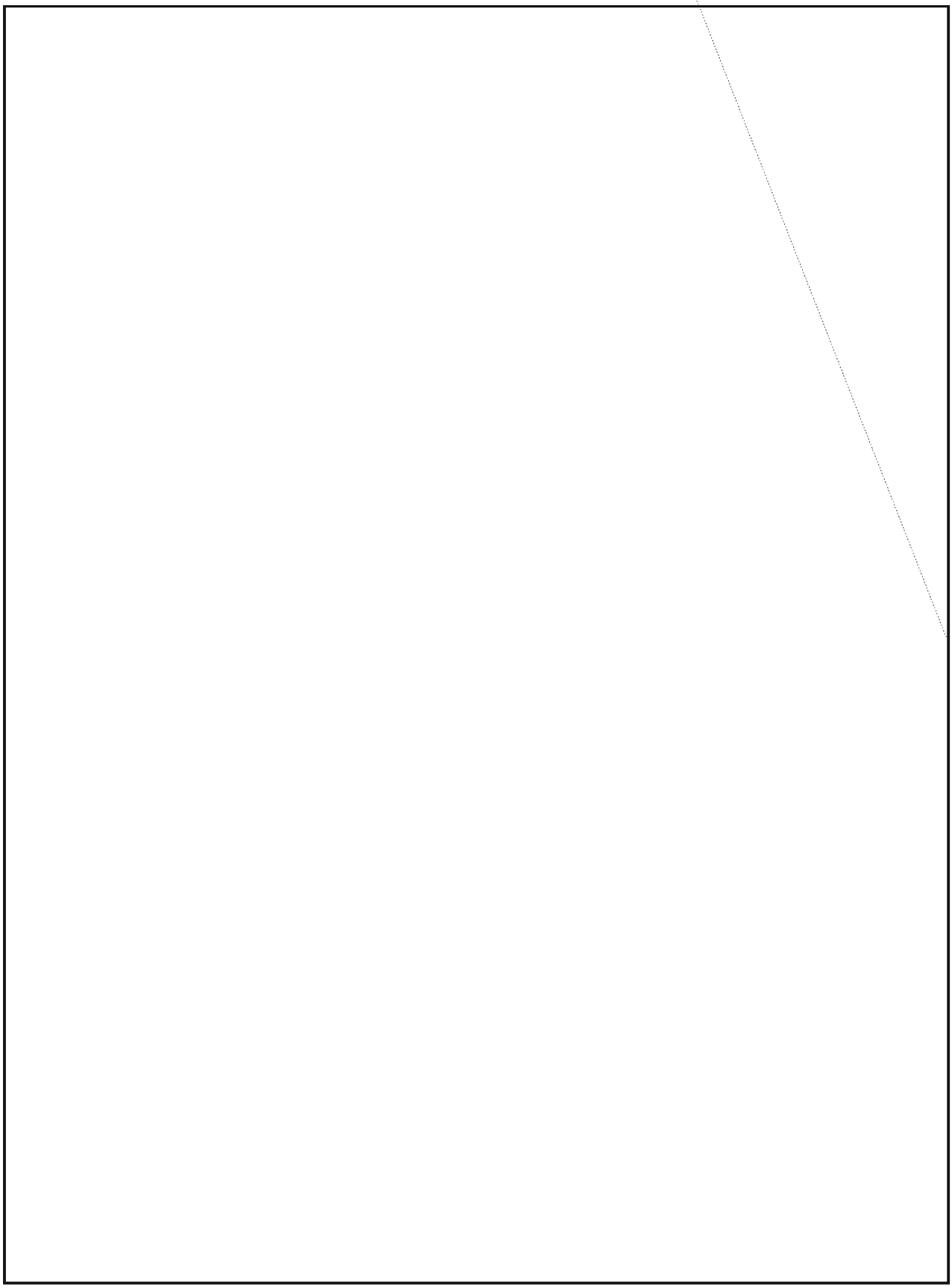
Shootout at the SIGINT Corral (U)

(Classified ~~SECRET-HVCCO~~ in entirety.)

In his article "I Remember SPELLMAN" in the July 1978 CRYPTOLOG *Art Salemme pretty well dismissed the idea of on-line voice transcription as unworkable. Now here's* [redacted] *who, while not being exactly enthusiastic about the concept, does see some hope for its limited application.*

P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)



[redacted]

SEMINAR ON TRANSLATION PROBLEMS (U)

(U) P16 will sponsor a Seminar on Translation Problems from 10 to 13 September. Topics common to practically all languages—things like ambiguity, redundancy, set phrases, culture-bound words, and the formation of neologisms—will be treated in each of the first sessions ; these will be followed by specialized "tack-ons" devoted to specific languages or groups of related languages. Novice translators, old hands, and even non-linguist managers should find the sessions, which will feature correction of "problem translations" (in English, but reflecting the fact that a translator had a problem in rendering the text), enlightening and useful.

(U) If you would like further information, the person to call is [redacted] P16, ext. 5642s or 5236s.

P.L. 86-36
EO 1.4.(c)

SOLUTION TO NSA-CROSTIC NO. 26 (U)

(CRYPTOLOG, June 1979, by D.H.W.)

[redacted] Letter to the Editor, *CRYPTOLOG,* October 1978

(U) "I will laugh at [quips concerning] female traffic analysts only when the opportunities for professional women are [equal to those] for men, and when the rate of women promoted is equal to that of men promoted, and when the number of women in management positions is proportionate to the number of men in management positions."

P.L. 86-36

Although I have no hard statistics at my fingertips, I suspect that, in the language field, at least, many old-timers are standing on principle in refusing to participate in the "professionaliztion" program, fathered by the late Sidney Jaffe, because they were inequitably ignored in its formulation (in other words, discriminated against) — men who had genuinely professionalized themselves *before* the program was intitated by securing advanced degrees, whereas others, simply because they were GS-13s and up, were "automatically professionalized" on the basis of mere salary achievement (of course, the bosses, like honey, always stick together.)

This patent shortcoming I have repeatedly pointed out to Dr. Jaffe himself, as well as to Dr. Tordella and to a number of NSA directors, either orally or in writing; however, at this late date the problem still persists, giving us the impression that the dictum of *ignoring-it-will-cause-it-to-go-away* still is supreme in the conduct of the cognoscenti.

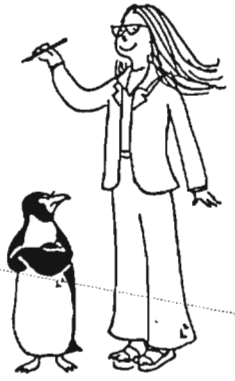
[redacted] Ph. D
NSA Fellow
G52

To the Editor, CRYPTOLOG:

As a former Art Editor of CRYPTOLOG, I feel that I must write and congratulate you on the recent addition of the clever drawings that have been accompanying many of the articles in recent issues. They are very well done, truly a credit to the artist, whoever he or she may be... and why do you keep the identity of such a talented artist a deep, dark secret? Certainly you owe it to your loyal readers to tell us who is responsible for those wonderful drawings.

Admiringly,

[redacted] P16



From the Editor:

It's a pleasure. The illustrations signed L[2], which have been appearing in CRYPTOLOG since the March issue, are the work of the very talented [redacted] of G92. In the accompanying self-portrait Ms. [redacted] is shown in a moment of artistic creativity, while one of her surly penguins looks on. Incidentally, you can catch more of Lynne's work in the WIN (Women in NSA) Newsletter each month.

In the May issue of CRYPTOLOG we asked if anyone could identify a language of the Soviet Union (other than Armenian, Georgian and the three Baltic languages) which used a non-Cyrillic writing system. Last month we printed an onswer from A Group's [redacted] which identified the language as German. But it looks like the issue isn't quite that simple...

To the Editor, CRYPTOLOG: P.L. 86-36

The answer to your Linguitrivia question can be found on page 188 of the *Area Handbook for the Soviet Union*[1], which accompanied the programmed text for NCSch course TG-003, Orientation: Soviet Union. Referring to the linguistic make-up of the Soviet Union, it states

> The western branch of the Germanic group is represented by German and Yiddish. German is spoken by a decreasing number of descendents of German steelers who arrived in Russia during the eighteenth century under the reign of Catherine the Great, herself a German. Yiddish is a variety of medieval German spoken by Jews descended from those who had lived in Germany but who had subsequently moved eastward into Poland and Russia. The language is written in the Hebrew alphabet and contains a large portion of Hebrew words. In the Soviet Union it is considered to be the language of the Jewish people, although the Jewish communities in the Caucasus and Central Asia speak local Iranian and Turkic languages. Some books and journals are published in Yiddish, and it is nominally the official language of the Jewish Autonomous Oblast'.

[redacted]

APOLOGY!

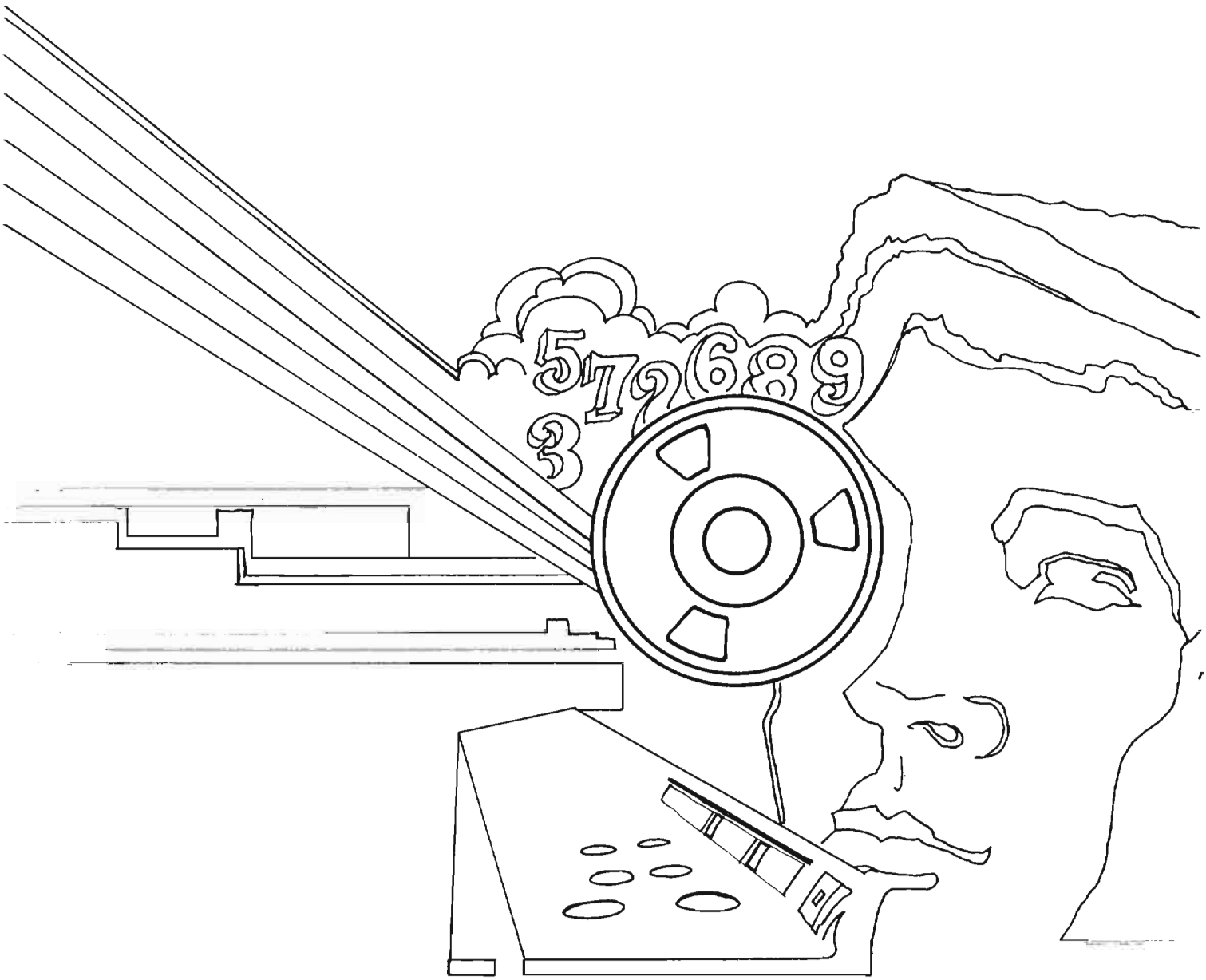
The April issue of CRYPTOLOG carried a puzzle entitled "A Somewhat Larger Problem," but later issues have, through oversight, omitted the answer.

Diligence, patience and luck will produce the table, a portion of which is:

	1	2	3	4	.	.	.	.
	T	F	Q	Z	C	.	.	.
	C	S	G	D	O	.	.	
1	O	N	G	J	.	.		
7	X	M	J	.	.			
	D	W	U	.	.			
	A	H	.	.				
5	Q	.	.					
	.	.						

What is the allocation system? Answer next month.

P.L. 86-36


5 7 9 6 8 9
3

DOCID: 4019666

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JUNE 1979

E.O. 1.4.(c)
P.L. 86-36

P.L. 86-36

TEACHING COMPUTER SCIENCE TO LINGUISTS (U)..... [redacted].....1
THE STORY OF MOSES (U)..... [redacted].....5
[redacted]..... [redacted].....6
TRAFFIC ANALYSIS OF THE FUTURE (U)..... [redacted].....10
HOW ARE YOUR STAMINA? (U).....Sydney Fairbanks.....11
NSA-CROSTIC NO. 26 (U)..... [redacted].....12
DATA STANDARDS WITHOUT TEETH (U)..... [redacted].....14
...MR. PATTIE REPLIES (U).....Mark T. Pattie, Jr.....15
LETTERS TO THE EDITOR (U).....16
THE BALTIC ENCODERS (U).....Anthony Reiskis.....18
THE NAVAJO CODE TALKERS (U).....20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: 1 JUNE 2009~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019666

~~SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. VI, No. 6 JUNE 1979

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor-in-Chief.....David H. Williams (3957s)

Collection..... [redacted] (8555s)

Cryptanalysis..... [redacted] (4902s)

Cryptolinguistics..... [redacted] (5981s)

Information Science..... [redacted] (3034s)

Language..... [redacted] (8161s)

Machine Support..... [redacted] (5084s)

Mathematics..... [redacted] (8518s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Taurone (3573s)

Production Manager.....Harry Goff (5236s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~SECRET~~

DOCID: 4019666

TEACHING COMPUTER SCIENCE TO LINGUISTS

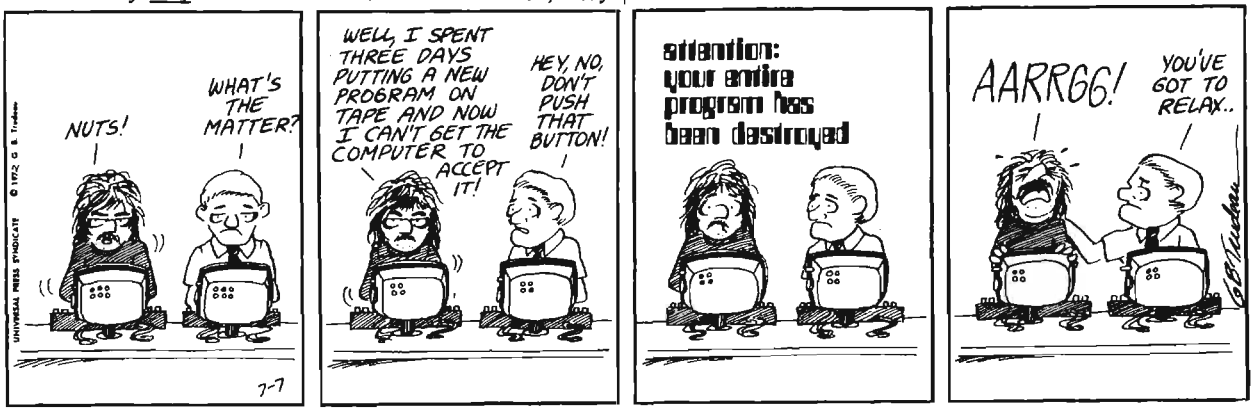
by [redacted] P16

ELCITRA ERITNE SIHT
...UPMOC YB TES SAW
TES...UPMOC YB TES
MOCYBUPMOCYBUPMOCYB

P.L. 86-36

Consider the plight of the NSA linguist. He entered his chosen field to "ling", i.e. to work with foreign language material: to translate, to transcribe, or perhaps to analyze and report the significance of large amounts of text. He chose to deal with the fuzzy world of ambiguous meanings, of convoluted and unpredictable rules of grammar, and with the imprecision inherent in the transference of an idea from one language into another. He never cared much for the picayune rigor or the grubby technical details of engineering or the physical sciences -- they just weren't appealing to him. He felt at home in that imprecise world of *meaning* that is so foreign to most Americans. And then he came to NSA.

Here the linguist must deal on a daily basis with computers. (As if it weren't bad enough that the phone company and his insurance agent used the darn things!) In fact not only does he have to *deal* with computers, he has to actually rely on them! More often than not, they



provide his daily material for translation and store the older material. God forbid that he should have to actually enter his translation or transcription into them, for he has seen the words: **ENTIRE FILE DELETED** on more than one occasion after spending an entire day laboriously entering his work keystroke by keystroke!

But even worse than the computers themselves are their keepers: programmers - people who really have no comprehension of language work and who are always muttering about "saving bits" or something equally obscure, when all you really wanted to know was why you couldn't get the machine to print out your daily take separated in an ever so *slightly* different way.

The worst experience of all awaited the rare brave linguist who got involved in the design of a new computer system for his office. The project development people seemed to be a special breed of programmers whose incomprehensibility was matched only by their desire to document in a level of detail that baffled the minds of ordinary folk. Even though it is considered almost axiomatic that projects which don't intimately involve the proposed end-users from the very beginning are doomed to failure, the linguist finds participation in planning extremely difficult because of the "computer-ese" language barrier and because of the lack of understanding of language work by others. Once someone even asked a linguist on such a planning team if he *really* needed all 32 letters of the Cyrillic alphabet and couldn't he get along with just 25 or so because of computer limitations ....[1]

Because of this culture shock in going from the language world to the so-called electronic office and because of the tremendous improvements that are possible when linguists are included in the planning for the computer support for their work, the idea of an introductory (and terminal) course for linguists in computer applications to language processing was born. Such a course was developed and subsequently tested on two groups of linguists. The results of those experiences offer many interesting revelations about the nature of the linguistic point of view *vs* that of computer science.

Before some of these experiences can be detailed, a brief explanation of the newly developed course is needed.

Credits

a) Doonesbury cartoons reproduced with permission. Copyright 1972, G.B. Trudeau/distributed by Universal Press Syndicate.

b) This article was prepared using the B7700 CANDE word processing system and a text composition system being designed and implemented by [redacted] P16, and the final output of the article was done on the SEACO 1700 CRT phototypesetter in S3.

1. For a similar account of a linguist's first experience with computers, see Robert Wachal's article, "Humanities and Computers: A Personal View", **North American Review**, Spring 1971.

P.L. 86-36

The course, CL-2ØØ, "Linguistic Applications of Computers", is both an introduction to computer science in general and to NSA-specific language projects in particular. The students experience the art of computer programming by learning enough about two quite different programming languages to write one small program in each language. In addition, they take tours of two computer operations areas in order to see some real machines in the flesh. The work in computational linguistics that is discussed includes the Agency's efforts in computer lexicography, computer scripting, speech processing, and automatic degarbling, as well as talks on the academic fields of machine translation of natural languages and artificial intelligence. The last portion of the course explains the Agency's project management system and the ways in which the proposed end-user can influence a new project to insure its success. A detailed outline of the course can be found at the end of this article.

Without a doubt the most difficult tasks for the students were the programming assignments. The reasons for this were not completely clear and often varied among the individual students, although two problems were shared by all. The first of these had to do with the choice of names for the variables in the programs. In high school algebra, for example, one usually prefaces a discussion of a problem with an explanation like: *Let x be the number of apples that John bought.* This is often not easily done in computer science, and even if it is, it is not sufficient for a large, complex computer program, as one quickly forgets what *x* was supposed to represent, or even what John was trying to do! Most professional programmers tend to choose names for the variables in a program that are at least somewhat suggestive of the meaning those variables have in that program. Hence a variable which denotes the position of a certain keyword within a section of running text might be named '**KEYWORD_OFFSET**' or '**SUBSTRING_POSITION**' if one were programming in PL/I, a language which allows very long, descriptive names, (or '**STRPOS**' if one were using a more restrictive, inflexible language like FORTRAN which limits the lengths of names to six letters). Yet these expressions have no meaning to the computer. It merely stores the names in a table for future reference and sets aside a certain amount of computer memory to hold the values associated with those names.[2] Variable names are unlike, for example, programming language reserved words like '**READ**', '**DECLARE**', '**FORMAT**', '**PROCEDURE**', etc., which have fixed and definite meanings to the computer; meanings which are reasonably suggested to English speakers by these particular words.

Yet the distinction between these two types of words was difficult for almost everyone to grasp. This led one student to attempt to do a frequency count by just listing the words, '**NUM_OF_ONES**', '**NUM_OF_TWOS**', etc., since, he reasoned, that the computer understood the "English" words '**READ**' and '**END**', so therefore it ought to also be able to understand something like '**NUM_OF_EIGHTS**'!! It wasn't until all variable names in the course lectures and examples were changed to words that clearly had nothing to do with the semantics of the particular example (e.g. variables that held the frequency counts for certain characters had names like '**LION**' and '**BEAR**', as opposed to '**NUM_OF_A_S**', and individual lines in the program were given labels like '**COW**', '**DOG**' etc.) that the students really caught on. While such a practice is at best poor for a professional programmer, it was almost mandatory for the linguist who would have read too much into the choice of a name otherwise. I really knew that this notion had been mastered when one of my students presented me with the frequency-count program abstracted here:

```
KAZOE:   PROCEDURE OPTIONS(MAIN);
         DECLARE (ICHI, NI, SAN) FIXED BIN(15,0);
HAJIME:  READ FILE(SYSIN) INTO (TEXT);
         IF SUBSTR(TEXT,1,3) = 'END'
           THEN GO TO OWARI;
MODORI:  IF SUBSTR(TEXT,I,1) = '3'
           THEN SAN = SAN + 1;
         GO TO HAJIME;
         END KAZOE;
```

2. The fact that the computer does not understand English can make it rather tolerant of the inadequacies of some programmers. In a reasonably large program I wrote a few years ago that dealt with dictionary retrievals, I was quite proud of the clear and descriptive names I had chosen and the fact that they made the program so much easier to understand. It wasn't until the program was completely finished that I found out that there was something not *quite* right about some of the names I had chosen, names like: '**NUMBER_OF_RETREIVALS**' and '**RETREIVAL_TIME**'!! Since my misspellings were at least consistent, they were perfectly "understandable" to the machine!

This program uses quite descriptive names, but in Japanese!! Since clearly the computer could not read Japanese, this student showed that he realized what the descriptive names were really for: the *people* who will read the program, not the computer.[3]

The other problem in programming that was shared by all linguists was the difficulty in the reduction of large difficult tasks to a number of small easily accomplished actions. This type of problem-reduction approach to problem-solving is that often used in high school geometry ("*If I can just prove that triangle ABC is congruent to triangle DBF, then I can do the whole problem.*") and in symbolic integration ("*Let's try integration by parts and see if we can get two integrals that are easier to solve.*").[4] This division of a complex problem into smaller, more rudimentary pieces is imperative if one is to write a program to solve that problem. One must reduce the given problem to small, primitive problems that can be easily programmed, often in a single line.

One student was so overwhelmed by the complexity of programming one problem and accounting for all the various possibilities that the first step of his solution was: "The programmer manually checks through the input and removes the following special cases..."! Other students just couldn't get enough of a handle on a small part of the problem to even begin, but when helped in that first step were able to complete it without too much difficulty.

It is possible that this is just a difficulty encountered by every beginning programmer, though I don't remember this happening at all among the students in *my* first programming class, a class made up entirely of students in engineering and the physical sciences. It may be that this, in fact, points to a basic difference in the approach of a linguist. They perhaps do not analytically dissect their work, as the engineer must often do, but rather approach the whole problem intact, perhaps slightly more attentive to one particular portion at any one time, but nevertheless keeping the entire problem in focus. This is sort of a gestalt approach as opposed to an analytic one, but an approach that may be required for language work.

This idea that linguists may have a different way of attacking problems is also supported by their reactions to the two programming languages that are taught in the class. Without exception, the students felt much more "comfortable" with SNOBOL, a language that is strange to many professional programmers. SNOBOL is unlike the more standard programming languages like FORTRAN, PL/I, ALGOL, etc. and in fact was designed for the processing of text in complex ways. SNOBOL allows one to "look for" complex patterns in running text and to easily manipulate the text portions it finds. For example, the following one SNOBOL line formats arbitrarilary spaced English text and outputs it on the line printer:[5]

```
LOOPA   TEXT  (POS(0) SPAN(' ') NULL . SW) |
              (ARB ' ') . SW SPAN(' ') |
              (LEN(60) . OUTPUT NULL . SW ' ') |
              (ARBNO(BREAK(' ') ' ')) . OUTPUT
               ARBNO(NOTANY(' ')) . SW POS(60) |
              (LEN(1) ARB) . OUTPUT
               NULL . SW RPOS(0) = SW  :S(LOOPA)
```

The linguists seemed to find SNOBOL much closer to their way of thinking than the more *standard* (i.e. to most programmers) programming language PL/I. Since it has been hypothesized that one's natural language limits or restricts one's thinking patterns[6], it should also be equally possible that given a choice between two artificial languages, one would feel more "comfortable" using the one that least disturbed his natural thinking patterns. To the engineer this might be one of the so-called "algorithmic" languages like PL/I or ALGOL; to the linguist it might be a totally different sort of language like SNOBOL.

But by far the most interesting observation about the linguists was the imagination and enthusiasm with which they approached a foreign field. One principle which was expounded upon often was that of Day's Law, a property of some programming languages.[7] A programming language is said to satisfy Day's Law if anything that a programmer would ever reasonably want to do, can be done *easily* and *directly* in that language. PL/I is an example of a language that satisfies Day's Law, and FORTRAN is an example of a language that clearly does not! The students were told that PL/I satisfied Day's Law and many were able to discover some actual PL/I syntax by guessing! One student theorized that PL/I ought to have a way to assign the same value to two different variables simultaneously and guessed the syntax:

I, J = 0; (*Correct!*)

and another student felt that there must be a way to assign an initial value to a variable when it is declared, and guessed the correct syntax of the PL/I keyword **INITIAL**. Unfortunately there were also a number of incorrect guesses (though not incorrect applications of Day's Law), most notably when one student decided that array references really shouldn't *have* to be numbers, but ought to be arbitrary character strings.[8] This belief led the student to try the syntax:

---

3. It is not at all so clear that a computer could not "read" Japanese. To the computer, there is no real difference between the string of letters '**BEGIN**' and the string '**HAJIME**'. It just so happens that most computers are built to recognize only one of these words as denoting the meaning "start". There would be no real problem, in theory, in programming the computer in German, Japanese, or even Arabic. There are, however, some political problems. For more details, see Theodor Sterling's article, "Computers in Developing Nations: A Cautionary Tale", **Communications of the ACM**, Volume 20, Number 12 (December 1977), pp. 971-972. Nilsson, Nils J., **Problem-Solving Methods in Artificial Intelligence**, McGraw-Hill, 1974, chapter 4.

5. This SNOBOL program was written by [redacted] R61, in response to a challange by another SNOBOL programmer.

6. This is the Sapir-Whorf hypothesis in linguistics and an entirely artificial "natural" language has been designed to test it's validity. For more information concerning this hypothesis and this new language, see James C. Brown's **LOGLAN1: A Logical Language**, 3rd edition, The Loglan Institute, 1975.

7. Days's Law is named in honor of its proposer, [redacted] a former Agency employee.

8. This is approximately true in PL/I if one considers PL/I *structures* heterogeneous arrays with non-numeric subscripts, and is definitely true in SNOBOL with the SNOBOL *table*; see T.W. Pratt's **Programming Languages: Design and Implementation**, Prentice-Hall, 1975, pp. 64-67.

P.L. 86-36

DECLARE COUNT('Ø':'9') FIXED;

to build an array which was indexed with the literals 'Ø', '1', ... , '9'! Unfortunately such a statement has nothing like that effect.

The enthusiasm and optimism of the students during the entire course and in the programming assignments in particular was indefatigable. Two particular cases immediately come to mind. One student's first attempt at one of the programming assignments resulted in a list of diagnostic errors that was about ten times as long as the total length of the program being tested! Yet the student was only slightly daunted and completed the assignment with only a few additional runs. Another student, upon discovery of a small syntactic error in his program, was then so confident of his work that he was then willing to *wager* that the program would definitely be completely successful on the very next run! Much to the student's dismay it took *many* more runs before the program accomplished anything even close to the required task. Had I collected on all our 5¢ bets, I would now have a small drawerful of nickels!!

Course Outline
CL-2ØØ
Linguistic Applications of Computers

A) INTRODUCTION TO COMPUTER SCIENCE

Hardware, Software, PL/I, SNOBOL, NSA Computer Complexes, Computer Operations, Current and Future Trends in Programming Languages.

B) COMPUTERS AND TRANSLATION

Computer Lexicography, Machine Translation and Machine-Aided Translation, Computer Scripting, Speech Processing and Computer Aids to Transcription, Artificial Intelligence.

C) COMPUTERS AND CRYPTOLINGUISTICS

Sorting, KWIC Indices, Automatic Degarbling Schemes, Mathematical Modeling of Languages, PTAH.

D) LINGUISTIC PARTICIPATION IN THE PLANNING OF A FUTURE COMPUTER SYSTEM

Required Agency documentation (SCP Series), Linguistic Input, Case Study: Project THISTLEDOWN, Proposal Evaluation.

SOLUTION TO NSA-CROSTIC NO. 25
(CRYPTOLOG, May 1979, by D.H.W.)

"[Once] some illiterate [soul] concludes that "type" *means* "type of," the step to "this type thing" is immediate. Since it is well known that no error is stupid or vulgar enough to guarantee that it will not become respectable, we refrain from rending our garments. But we submit that at this period English this type writing is not appropriate to this sort journal."

Editorial, NSA Technical Journal, [January 1958, by Sydney Fairbanks, reprinted in *CRYPTOLOG*, April 1979]

SIGN LANGUAGE

(Reprinted from Q*R*L)

International road signs are being seen more and more frequently in the United States. For the benefit of readers who may not be familiar with them, here are a few examples.

Umbrella Trouble When Windy!!

You Are Now Entering Johnnie Appleseed Country!!!

Barber Shop!

Snake Crossing!!!

- Bookie Joint!!

You are on a runway!!!!

Illiterate natives hereabouts

Watch out for returning boomerangs!!

Only One Out of Six Will Make It!!!

Caution: Drunken Drivers Ahead!!!

Stunt Drivers Practicing!!

Beware of Purse Snatchers!!

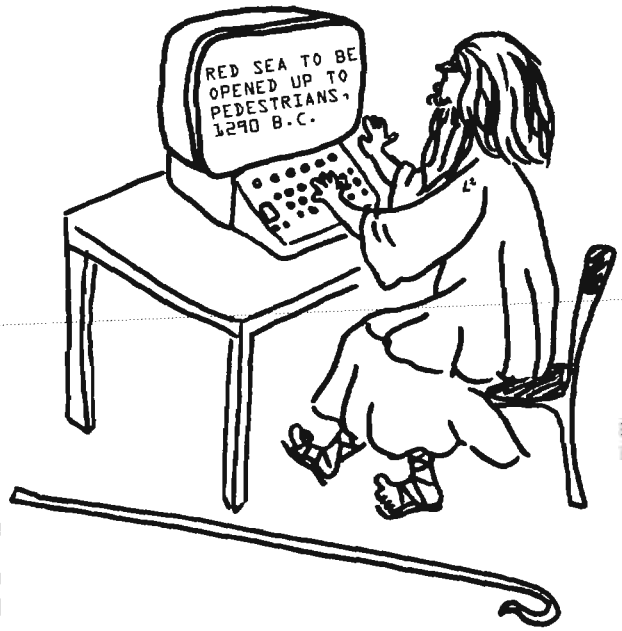
Unfriendly Spear-throwing Natives Hereabouts

Watch Your Step!!!!

DOCID: 4019666

The Story of Moses (U)

[redacted] G51



P.L. 86-36

EO 1.4.(c)
P.L. 86-36

(U) If you should ever want to know when some important event, such as an international conference or meeting, is to take place, MOSES may well be able to help you. Not the Old Testament prophet, but the *M*ulti-national *O*n-Line *S*cheduled *E*vent *S*urvey. This data base, which contains information on upcoming events gleaned from a variety of open and classified sources, is an excellent example of interaction between T12 (Information Services) and analytic elements, producing a data base to meet operational needs. It resides on TIPS (Technical Information Processing System) and can be accessed at NSA through RYE outstations, and at other agencies through the Community On-line Intelligence System (COINS).

(U) Moses at Work. The folks in T1221 gather information on future events and put it into the data base as they find it, assigning a one-up number to each item. The way we used to get the MOSES information was to have an analyst submit queries through a RYE outstation at the end of each month. Those queries would then produce listings of selected items in item number order. But these listings were hard to use because they were not organized either by country or by event. To circumvent that problem the listings were reduced by hand to a list of events arranged by beginning dates. The list was then duplicated and distributed throughout the division.

(U) Developing those chronological lists by hand was quite a time-consuming task. This came to a halt after a reorganization shuffled away the capability to compile them. As a result, the original computer listings were delivered directly to the analysts who had become used to getting the nice chronological listings. The first time the raw computer listings were brought into our area we found out how Pharaoh's army felt that day in the Red Sea: MOSES had just closed a sea of paper over our heads!

(U) In that form, the MOSES extract was too unwieldy to use. If anyone wanted to find out when a given meeting was going to start, he might have to read through an inch-thick stack of paper before finding his answer, usually on the last page. Nevertheless, the MOSES information was still useful, so we asked for an extract: we wanted it in an easy-to-read format, sorted by host country and by the beginning date of the events.

~~(C)~~ The final format of the extract was quite usable, even if not ideally so. It was usable because it allowed people to look for their desired information quickly. After all, the main reason an analyst needs to know when a meeting is to start is to permit him to decide whether or not to publish a piece of information, which has just become available, relating to some event. For instance, if a

[redacted]

the instructions are history, not intelligence, and will not normally be published.

(U) The event information usually available to the person making the publish-or-not decision consists of its name and where it is to be held. With those two items, he can then quickly thumb through the revised version of the extract to the proper country, and then scan down the first word of the narrative descriptions of the events, and find the needed date.

(U) The problem then exposed was that all too often the event we were interested in was not even on the list; the format was usable, but the data base was incomplete. To remedy this a series of tetragraphs was devised,

to be used in the TAG (Topics and Area Guide) line of every piece of product discussing the date of any future meeting, conference or similar event.

~~(C)~~ Now, whenever an analyst gets advance notice of an upcoming event, the information can be spread through use of one of the -SKD

[redacted]

(U) The MOSES folks can then use the SOLIS system and "pull" on the -SKD tetragraphs to get easy, rapid access to that advance notice. Once MOSES "knows" about it, anyone in the intelligence community can easily find out. Obviously, one of the most important sources of MOSES inputs is the translators and the checkers who keep -SKD in mind as they write or review TAG lines.

(U) After a few months experience with the new easy-to-read printouts, user analysts decided that calling T1221 (on extension 3258s) was even better, for a very good reason: up-to-the-minute information was available, rather than what had been on hand back on the first of the month.

(U) It's surprising how few linguists and analysts even know about MOSES.* Perhaps this article will help spread the word around.

==========

~~(C)~~ Another useful file, also maintained

[redacted]

excellent source of expansions of acronyms and abbreviations.

[redacted]

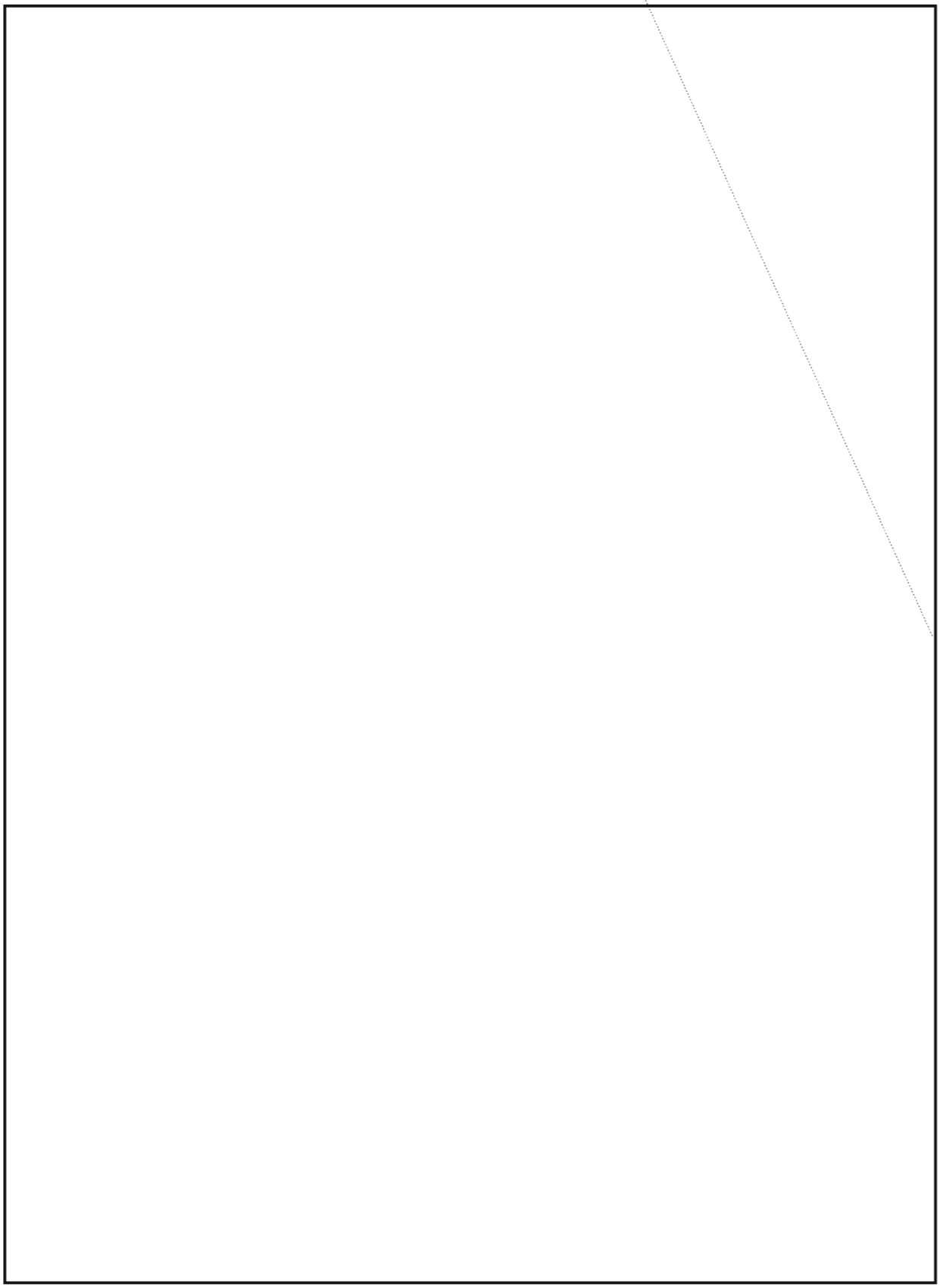
P.L. 86-36

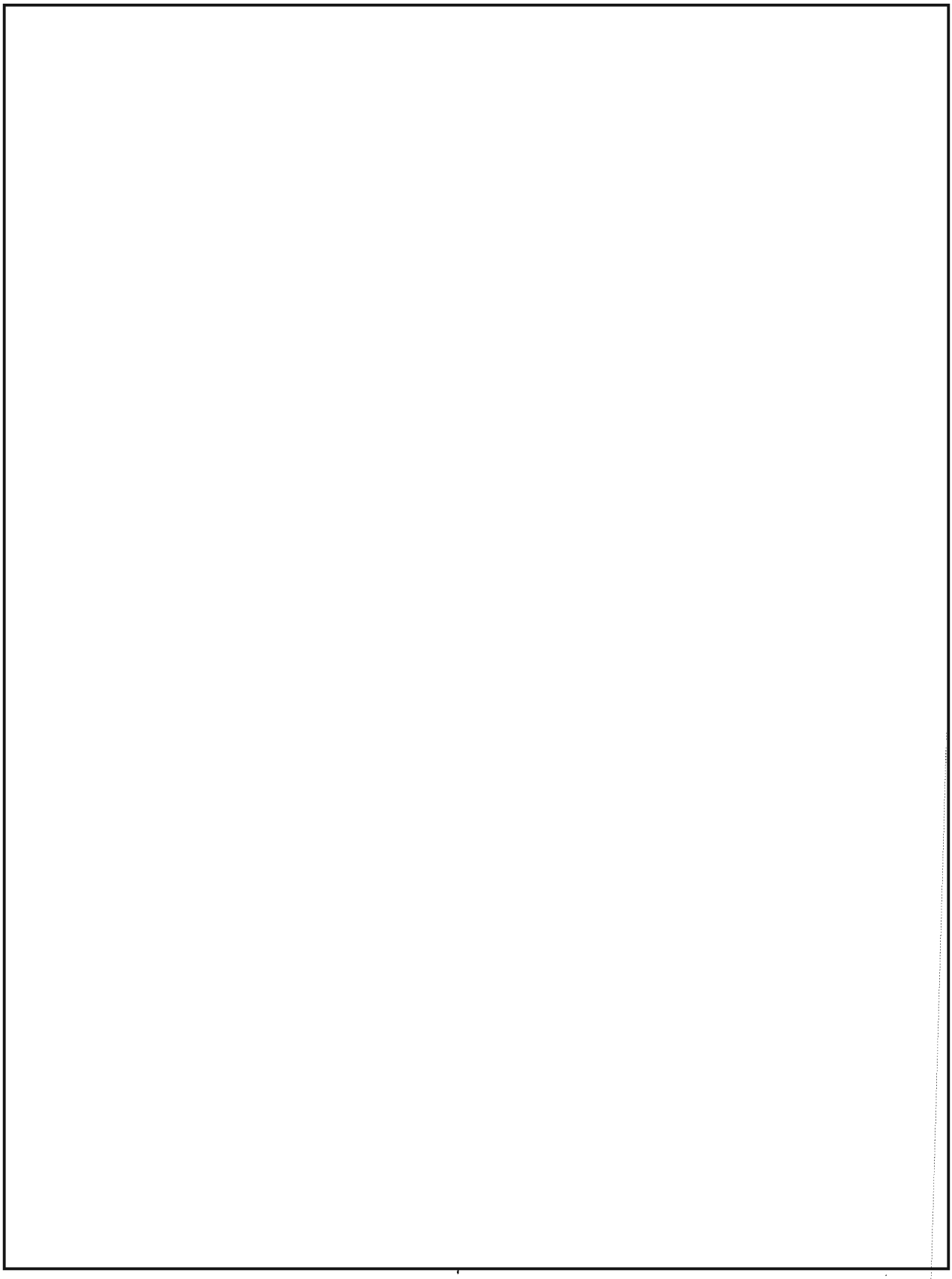
[redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

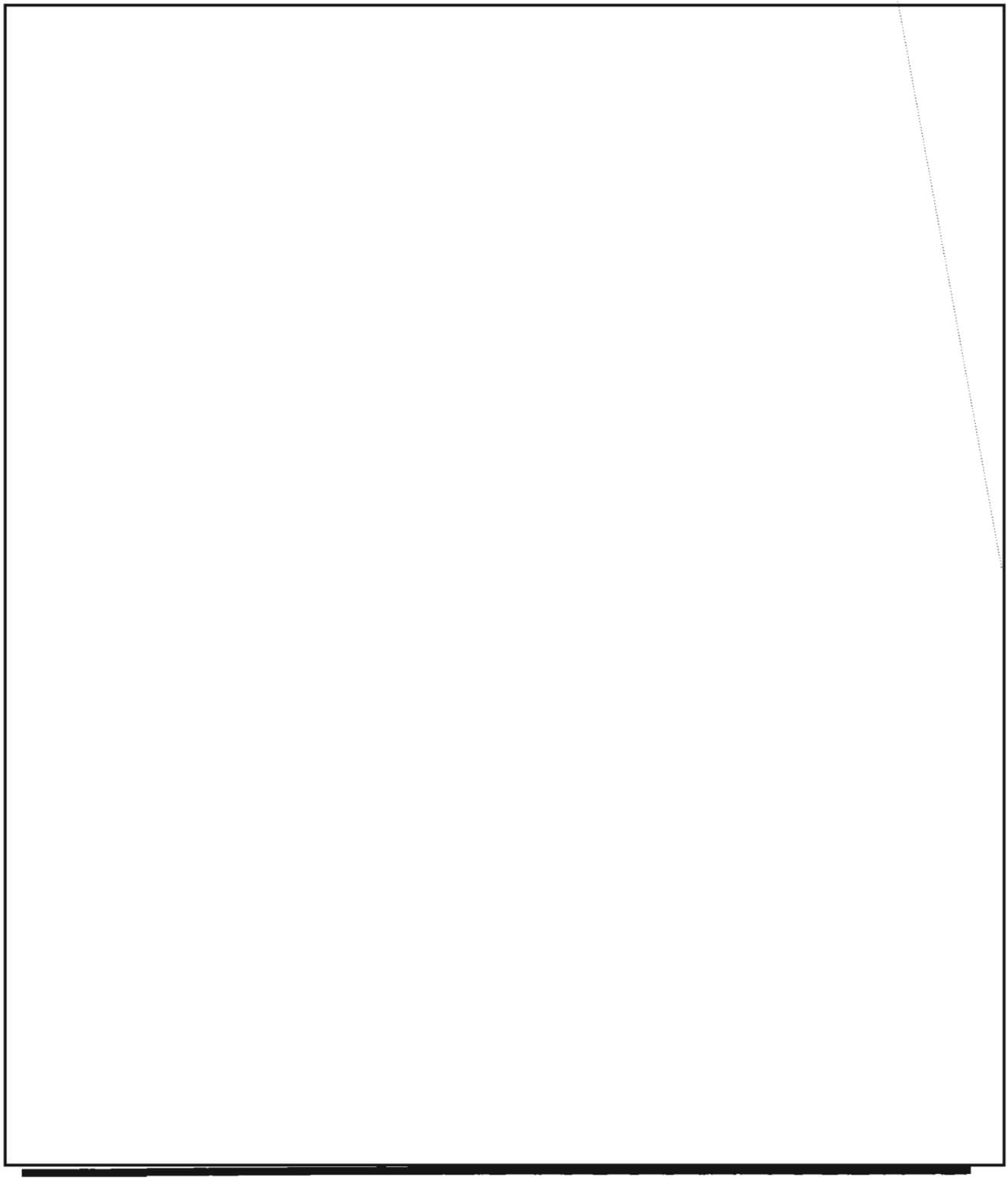
~~CONFIDENTIAL~~





EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



TO START A SUBSCRIPTION TO *CRYPTOLOG*, OR TO CHANGE THE ADDRESS ON YOUR PRESENT ONE, CALL 3957s.

P.L. 86-36

TRAFFIC ANALYSIS OF THE FUTURE (U)

[redacted] P14

(U) What did you do in the war, sir? I was a traffic analyst. Oh, how interesting. What kind of cars did you analyze?

Various Agency analytic disciplines are on the decline. Take a look at the table in the January 1978 *CRYPTOLOG* article entitled "The Changing Face of NSA." It shows a sharp decline in numbers of people assigned in certain job fields over the previous five years. Of the Agency's analytic fields, traffic analysis showed the largest percentage drop. Then take a look at the latest Quarterly Management Report; traffic analysis has been reduced still further. Where are we going? What is happening?

[redacted]

[redacted]

(U) I'm going to stop here and make my prediction, a double-barrelled one.

> *There will come a time when all of what we now call traffic analysis will be centralized in a single organization in DDO (or whatever it will then be called).*
>
> *This step will be taken to bring together and husband the few remaining TA skilled people, and to develop under a single line management authority, the unified technical data system and software system to support TA tasks worldwide.*

EO 1.4.(c)
P.L. 86-36

(U) I don't know when this will happen. But I'm pretty sure that it will happen.

(U) Of course, I was wrong about Dewey in '48...

How Are Your Stamina?

Sydney Fairbanks

Reprinted from *The NSA Technical Journal* of January 1959

One of our readers, stung by some peculiarly noxious idiot's-idiom that had crept into an official communication, called up the other day to ask, almost tearfully, if we thought he could volunteer to write all the memos put out in the Agency. No, we told him, the suggestion would probably not be well received; but we too, we confessed, had had daydreams of a similar czardom, lightened in our own case by the imposition of a scale of penalties. Omissions of the definite article ("subject memorandum is reprinted in referenced document") would call merely for confinement to barracks; references to the "overall picture" would involve a substantial fine; statements as to "the capability of the facility to become operational transmission-wise on a continuing basis" necessitate a painless beheading; and naturally anyone writing "the reason why this is so is because of the fact that" will be hanged, drawn, and quartered. Beyond these we progress to actual errors: "We hope you shall"; "like he did"; "this is a new one, and which"; "oil the bearings, such as we did yesterday"; and, of course, our friends "(comma) however", "this type thing", and "they are writing and notify the contractor." We are sorry, but we cannot tell you the penalties for these.

There are also the people who write, "this phenomena is noted in more than one media, and the discoverer is worthy of several kudos,"—but we are becoming a common scold. Actually the matter of foreign plurals is not quite so simple as the purists would have us believe. "Data" which started life as a proper little plural is rapidly becoming a collective singular, and anyone adopting a holier-than-thou attitude about it should be asked how his stamina are this morning. Back formations of singulars are even more confused. A "tactic" or a "statistic" has no more right to exist than a "mathematic" or a "calisthenic"; but it does. A man joining the commandos should no more become a commando than a man joining the troops becomes a troop; but he has. And so...we suppose...from a purely scientific point of view...one has to admit the possibility that a time *may* come when something called a "kudo" can exist naked and unashamed; but not, we hope, until we are dust before the doors of friends, or radioactive matter a-blowing down the night.

We too can be scientific on occasion. A short while ago we lamented the absence of a good portmanteau word of spontaneous rather than deliberate generation. In accordance with Somebody's Law, which says that as soon as you say there is no such animal a perfect specimen trots around the corner, we came for the first time on the word "meld" embedded in a very distinguished matrix. Not the verb used in pinochle, which is of course German *melden*, to declare, but one meaning something like "amalgamate." Webster's International knew it not, and we were tempted to throw it out, but we have a weakness for monosyllables. To make a long story short, Webster's *New World Dictionary of the American Language* gives: "meld, v.t. and v.i. (merging of *melt* and *weld)* to blend, merge, unite." Sinking the classicist in the collector, we left it in the copy where we found it, and tiptoed away.

But this does not mean that we are prepared to accept "irregardless."

NSA - Crostic No. 26

By D.H.W.

WORDS

DEFINITIONS

A. Site of baseball's Hall of Fame

18 165 257 76 96 216 46 65 210 187 233

B. Dog star (comp)

184 68 120 260 39 56 226 83 20

C. Impending

213 189 194 209 175 232 115 155

D. Act of investiture of a monarch

21 89 64 78 179 41 103 192 219 160

E. NY town, center of winemaking activities

231 247 241 235 109 263 171 72 16 137 162 34

F. Uncultivated; uncultivated person

100 105 53 182 94 223 117

G. Diana Rigg's role in *The Avengers* (2 wds)

227 132 200 169 62 80 251 32

H. "_____, my dear Watson"—Holmes' reply when asked how one should refer to a saffron-colored devilfish (3 wds)

45 29 149 6 262 172 252 86 211 166 225 238

195 52

I. Person shunned for social or moral reasons

87 119 135 112 110

J. Any of more than 100 fundamental substances

201 51 178 181 253 243 208

K. Ringing of bells

176 1 245 152 207 254 196 11 236 147 4 93

101 259 151 224

L. Why, at the Sioux bride sale, the maiden on the skin of the African river beast cost as much as one on a bearskin plus one on a calfskin (5 wds, followed by Word M)

140 104 22 258 146 180 36 2 131 85 126 122

91 10 244 61 204 156 215 163 255 99 30

14 48

M. See Word L (11 wds)

242 13 66 31 44 264 221 118 159 214 8 246

205 108 121 153 190 144 97 234 125 130 81

49 170 228 58 183 74 230 177 167 35 203

88 139 54 3 116 174 106

N. _____ *Room*

220 229 138 256 133 124

O. Volunteer State

47 59 248 26 71 17 212 55 33

P. Just underway (racetrack jargon, 3 wds)

63 38 28 114 134 168 77 98 113 92 261 42 27

Q. Candy made by boiling sugar and butter

57 239 37 79 145 199

R. Women of a Moslem household

S. Overture by Beethoven (op. 84, 1810)

T. Compass point

U. Tanzanian farewell to Miss Day (2 wds)

V. Resourcefulness; fantasy

W. Filling to the brim with a liquid (2 wds)

X. Assault; crime (Brit. sp.)

Y. Uppermost part of a building

173 148 136 237 158

95 9 90 102 193 69

107 191 123

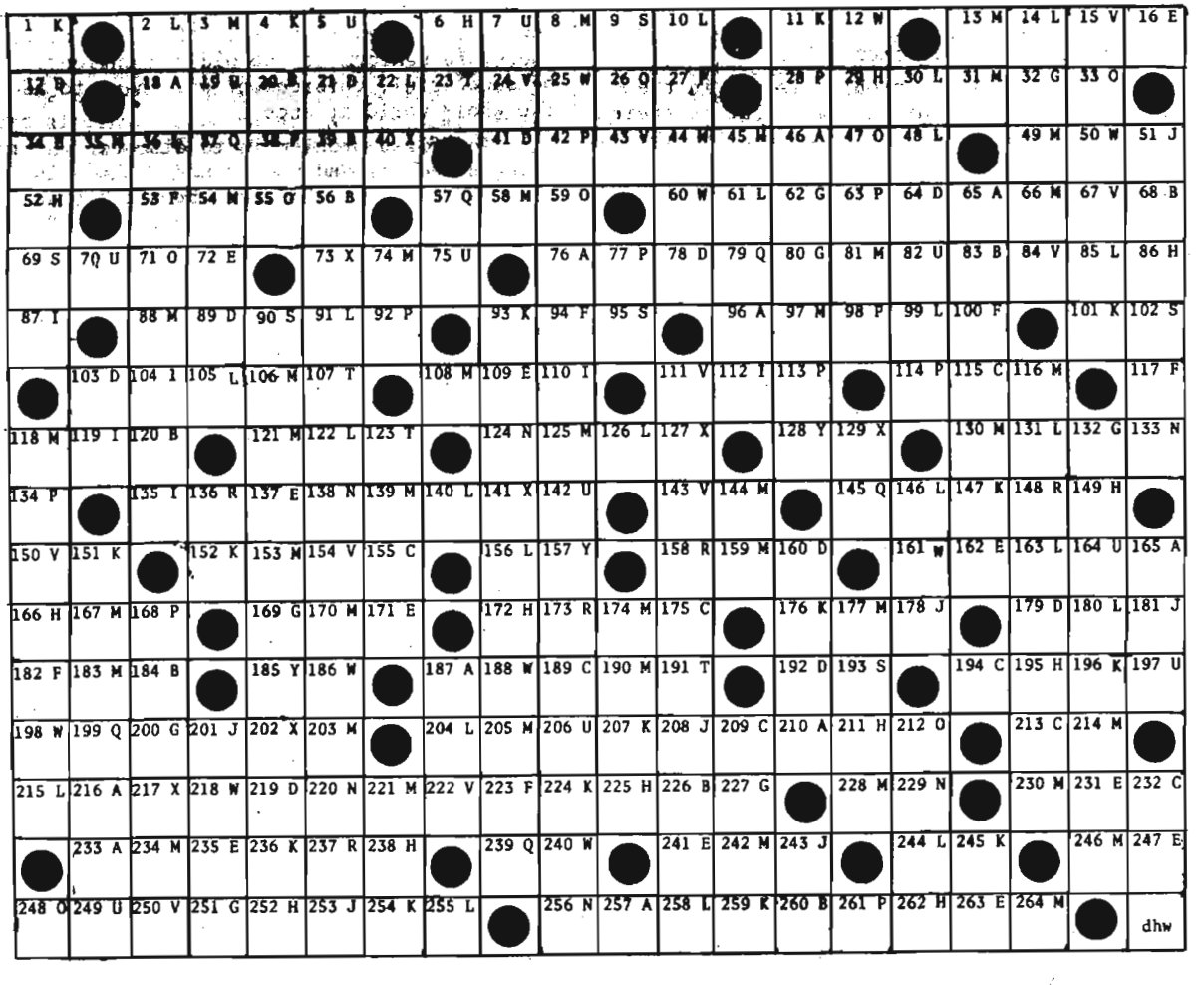
142 19 75 70 82 206 197 5 7 249 164

222 111 154 250 143 24 43 150 15 84 67

12 60 161 218 25 50 198 188 240 186

217 73 129 127 202 40 141

23 185 128 157



DATA STANDARDS WITHOUT TEARS TEETH

P.L. 86-36

It is clear from Mark Pattie's and [redacted] articles* that the data standards program has encountered major problems. Mr. Pattie cites several important areas where the implementation of standards has been less than successful, and he says that the NSA Data Standards Center is just "scratching the surface." Mr. Murchison, in his final paragraph, says that "we sometimes feel that our job is impossible."

The root of the problem is not in the actual development of standards but in their implementation. Mr. Pattie blames the general user, at one point appealing for cooperation, and at another point** thundering: "Until we are authorized to deny computer use to those who refuse to accept Agency standards we can have little effect."

He believes that operational necessity is really "operational convenience," and [redacted] backs him up: "Usually a sponsor cries 'unacceptable' just because he does not want to go to the trouble of re-programming."

This analysis of the cause of the problem is totally wrong. Most people suffer to a greater or lesser degree from lack of standardization and would do anything reasonable to avoid this. But standards are only justified if they bring tangible benefits. If the pain caused by implementation exceeds a reasonable threshold, then any benefit to the user will be cancelled out and we will be reduced to the untenable position of trying to enforce standards for their own sake. The rejection of "operational necessity" is the rejection of reality.

To illustrate my point let us assume that NDSC is given "teeth" and can actually deny a user access to the computer if he does not adopt standards. To start with, the idea of enforcing standards only on new applications is doomed to failure because there are few really new applications. Everything we do is built on what we have done before. The new is tied inextricably to the old, and must therefore conform to the old conventions. To be successful, enforcement will have to address the whole world at once.

The first problem is to discover who is using standards and who is not. There is no easy way of doing this and the whole plan would probably founder at this point. But let us assume that a lengthy study is able to ferret out the facts. It would undoubtedly reveal that the whole Agency (even NDSC!) is guilty of incomplete standardization.

P.L. 86-36

The next problem is to determine exactly what we are going to enforce. A Group has at least 1000 data elements, [redacted] the NDSC centralized file of data elements and data field definitions, lists only 200 standards. Shall we re-program to cater for the 200, and then, every few months, when a new standard comes along, re-program all over again? Or shall we suspend all operations until the other 800 are standardized? In the latter case, calculating from the fact that it took seven years to develop 200 standards, we will be waiting until the year 2006!

Both Mr. Murchison and Mr. Pattie are, therefore, wrong in suggesting that the general user is the villain. There are facts of life which make enforcement impossible in a large, complex organization, irrespective of the attitude of the users. I am personally in favor of standardization; yet when I had the job of establishing standards for a project, I was forced by operational necessity to be satisfied with partial standardization. If a standard exists I will adopt it. But if it does not exist, what do I do? How much time can I spend tramping around trying to find out what

---

* "NSA Data Standards Center," by Mark T. Pattie, Jr., *CRYPTOLOG*, November 1978, and "Comment on 'Data Standards Without Tears,'" by [redacted] *CRYPTOLOG*, March 1979.

** Letter to the Editor, *CRYPTOLOG*, October 1978.

P.L. 86-36

DOCID: 4019666

other people and projects are using? Inevitably, I invent my own names, abbreviations and codes just to get my job done before the deadline.

If we cannot blame the general user, can we blame NDSC? Of course not. As Mr. [redacted] says, the development of standards is inevitably "a long and rigorous process." NDSC is staffed by able people who are dedicated to their work to an extent rarely found. No one could do better. The truth of the matter is that once non-standardization has reached a certain extent in a complex organization it is not possible to enforce standardization without causing unacceptable damage. Non-standardization is self-perpetuating. During the time it takes to standardize one data element, a dozen new non-standard uses can evolve, so that the standardization process never catches up. It is a vicious circle which can be expressed thus: *Lack of standardization causes an increased lack of standardization.*

Once the truths of the situation are recognized then we can open our minds to reasonable alternatives. I firmly believe that the Data Element Dictionary/Directory is the best alternative we have. My personal experience of a DED/D is that it mitigates the adverse effects of existing non-standardization by tying different naming conventions into a single data definition. But it could do much more than this. If all applications are suitably described in the Directories, then everyone will have easy access to the conventions used by other people. [redacted] describes it very aptly. The Directories will show "what the current usage of data fields is along a wide spectrum of different Agency applications. Exposure to this usage will gradually lead us towards the necessary standardization." If the Directories tell me that a certain data element has six different names and no standard, then I will surely adopt one of the six, thus preventing a seventh from appearing. The process will not of itself bring about standardization, but it will certainly slow down the ever-increasing tendency to non-standardization. It will reverse the vicious circle.

[redacted] took me to task for using the word "magic" in my first article, and indeed I ought to withdraw it. I am tempted to let it remain because it does help to express the extent of the breakthrough in a very difficult area. NDSC will still have the labor of establishing standards. No machine can do that. But the DED/D will fill the gap where there are no standards, and will act as a positive force preventing the proliferation of non-standard uses, as well as providing NDSC with a mine of information as input into their processes. And all this without any additional sweat, toil or tears on behalf of the NDSC.

There is, of course, labor involved in the acquisition and loading of data into the Directories, but this is not NDSC's work. It is spread over the whole work force and does not bear very hard on any particular individual or office. I have sat on a terminal loading such data and can vouch for the fact that it is not very exciting, but neither is it very hard. Large, complex files can be described and loaded within a few days, not much compared to the length of time it takes to standardize one data element. Other things must be done, such as making the DED/D well-known and easily available to everyone, and encouraging its use by providing a variety of services. It is all well within the realm of the possible. P.L. 86-36

The fact is that the DED/D is a new tool which benefits everyone without any additional effort (documentation has to be done with or without it, and, in fact, your data elements may be loaded by someone else with overlapping interests). It is not even necessary for all data from all areas to be loaded before the benefits are felt. There is no enforcement, no need for "teeth." There are no adverse side effects. Nobody can lose, least of all NDSC.

I vote we give it a try.

...Mr. Pattie Replies

I suppose that if the Editor would allow it we could go on throwing barbs at one another for months or even years, but there is really nothing to be gained from that. I would propose that we bring a halt to the exchange, and I would like to apologize if I have hurt any feelings or stepped on any toes. P.L. 86-36

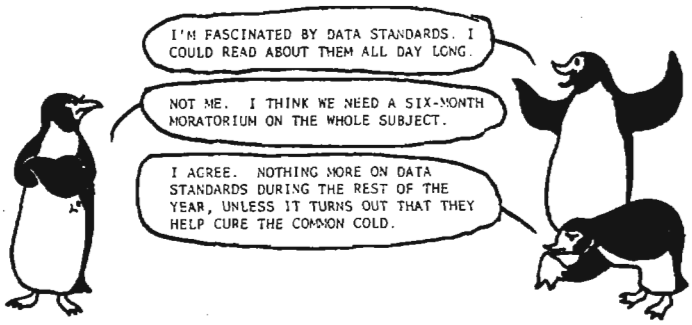
What really bothers me is not the name calling or the obfuscation but the apparent failure of Agency personnel to understand what we have been trying to say about our work in the first place. [redacted] just happened to put on paper some of the things we have been hearing all along. In spite of our letters and articles on the subject people still do not seem to understand what the role of the NDSC is.

We do not, and I repeat, not, impose data standards on anyone. When higher authorities (DoD, NBS, and the like) agree to a standard, then NSA has to abide by that or request an exemption. We help to coordinate action on those terms. Our main job with the Agency is to work with those who want to propose a cryptologic standard, coordinate the proposal with others, and get Agency agreement to call it a standard.

It often takes a long time to do this, partly because the people we deal with are involved with data standards only as an add-on to their normal duties. We appreciate the support we do get but we recognize that data standards may not have as high a priority in their lives as we would like.

We do not expect to standardize everything in the Agency, nor do we think that necessary. Where programs have limited applicability and use, it is enough that they work. When the applications or uses are more widespread, standardization becomes a worthy goal.

It is costly to standardize and it is fairly easy to cite such costs as a reason to keep going our individual ways. I wonder if anyone has ever given any thought to what it costs when we do not standardize.



We have never spoken out against the use of Data Dictionaries/ Directories. Our own PANDOWDY file is a small but useful example of one. Our main concern is that these dictionaries seem to be proliferating when there ought to be more of an attempt to incorporate them into a single one for all of DDO to use. It appears to be a repeat of the problems encountered by users of COINS files. By not standardizing we force users to make costly searches of all possible files (directories?) to make sure nothing is overlooked.

Perhaps it might be useful to close with an illustration of the difficulty we have in the area of data standardization, even when we are talking about something that has long been standardized. This past March we received two annexes to a USSID for comment; in each there is a line with a non-standard date (DDMMY) instead of the standard YYMMD, which was implemented in 1971.

How could someone, eight years later, put something like that into a program? Why wasn't this noticed by someone else long before it got to the NDSC? I can only assume that no matter how many data standards exist, there will always be people who will want to go their own ways, and we will continue, as before, to be accused of getting in the way of operational necessity.

Letters to the Editor

[In the May issue of *CRYPTOLOG* we asked if anyone could identify a sixth language of the Soviet Union which is not written in Cyrillic, the other five being Armenian, Georgian, and the languages of the three Baltic republics.]

To the Editor, CRYPTOLOG:

I believe that the sixth language you are looking for is German. There are almost a million Soviet citizens whose primary language is German. They are the survivors and descendants of the people of the Volga German Republic who were forcibly resettled to remote parts of Soviet Central Asia in 1941, where they still live in village communities and cooperatives, speaking their own language, running their own schools, and, despite odds, maintaining a cultural integrity.

Suspected by Stalin of being potential fifth columnists, these people were segregated by sex, age and family status, and shipped off to the Asian boondocks. They were not put into prison camps, but were simply set down on the steppes and semi-deserts and left to fend for themselves. Those who survived did so through the assistance of the local tribesmen who taught them how to build sod shelters and surivive the first shocks of resettlement.

In 1964 these Germans were officially rehabilitated, which restored to them certain rights of citizenship, including the right to serve in the armed forces and to hold membership in the Communist Party.

With regard to the language used by these people, in his book *National Languages in the USSR: Problems and Solutions*, the author, M.I. Isaev, states that "Soviet Germans use the same literary language that is employed in the German Democratic Republic and West Germany..."

[redacted]
Senior Linguist A Group (SLAG)

P.L. 86-36

DOCID: 4019666

To the Editor, CRYPTOLOG:

(U) I would like to complain about the recent changes in the library. Basically, what has been done is to move *all* mathematics and engineering volumes to FANX and leave *all* computer science entries at Ft. Meade. This inconveniences many people, since there are people interested in computer science at FANX and many mathematicians at Ft. Meade. At a small cost in effort the library could at least have left some of the duplicate mathematical items (of which there are many) at Ft. Meade and sent some of the duplicate computer science works to FANX.

(U) It simply is inadequate to be told that we at Ft. Meade can always order from FANX, and vice versa. For example, I often need an immediate answer to a question in, say, linear algebra or statistics. The time lost by many people will certainly reduce the efficiency of the Agency's technical effort.

(U) Even more helpful than merely splitting the duplicates would have been to try to cover the content of various topics at both branches. Thus if we have 25 works on dynamic programming, none of which are duplicates, it surely would have been possible to divide them such that the basics of the field could be found at both locations. For this option, of course, the library would have needed technical advice. As I have pointed out to the library's management a number of times, there are mathematicians in many parts of the Agency ready to lend a hand.

(U) I am afraid that the library has taken the easiest (to them) route, without fully considering the needs of the users.

[redacted]

The Chief of the Library replies:

(U) I can understand the frustration felt by the people in A who return to Ft. Meade to discover that many services they hoped to regain have been moved to FANX to make room for them.

(U) Dividing a library collection is not a simple task. The card catalog shows the location of books. If the collection had been divided as [redacted] proposed, there would have been no way to know where anything was, since changing all records immediately would have been out of the question. Under the system we chose, users can be informed of the location of a particular class of books regardless of what the catalog indicates. Moreover, in recent years very few duplicates have been purchased, and since most requests are for current books, dividing duplicates would not have provided a great service.

(U) Gradually we can change the location of particular books and the appropriate records as use shows where the demand is. Further, new books will be purchased for both collections regardless of class if the need is there and the budget and space permit. We are already doing this for books in computer science.

[redacted]
Chief, T121

P.L. 86-36

AND FROM AN OVERSEAS READER...

To the Editor, CRYPTOLOG:

~~(S-CCO)~~ [redacted] article, "Let's Not Lose Our TA Skills" (CRYPTOLOG, March 1979), made an untimely appearance here [redacted] EO 1.4.(c) P.L. 86-36 The week before it arrived, several of the people here, due to return to NSA in the near future, had attended reassimilation briefings, during which the overstrength skills problem was not only raised but was also given as a rationale for the reassignment of some to a different career field. Some of the moves were in the out-of-TA direction! It's easy enough to fall out of touch when headquarters is an ocean away, but it's even easier to be confused by the apparent contradiction between the M3 view of TA as an overage skill, and the view shared by [redacted] and [redacted] that TA is a field with an impending shortage crisis. Perhaps some of the 50-odd traffic analysts now in excess could be used to head off the coming shortage. The concern about the effect of transfers out of TA and the lack of new blood is shared by many. This feeling was expressed here recently by visiting managers, who stated a need for analytic talent to work in the rapidly expanding world of multichannel communications. P.L. 86-36

(U) What all of this may boil down to is the ever-present problem of individuals holding the title but not doing the analytic job, and the apparent inability of management to cope with this issue. *Good* traffic analysts are hard to find, and so may be talent in other overstrength skills; the key may be quality vs. quantity, another problem that's always with us. If nothing else, [redacted] article may make some managers realize that skill balance by the numbers is not an end-to-all-your-troubles elixir for reducing the workforce, and that talent returning from overseas should not be regarded as a magic ingredient for such a brew.

Kathy Bjorklund, F8313

The Baltic Encoders

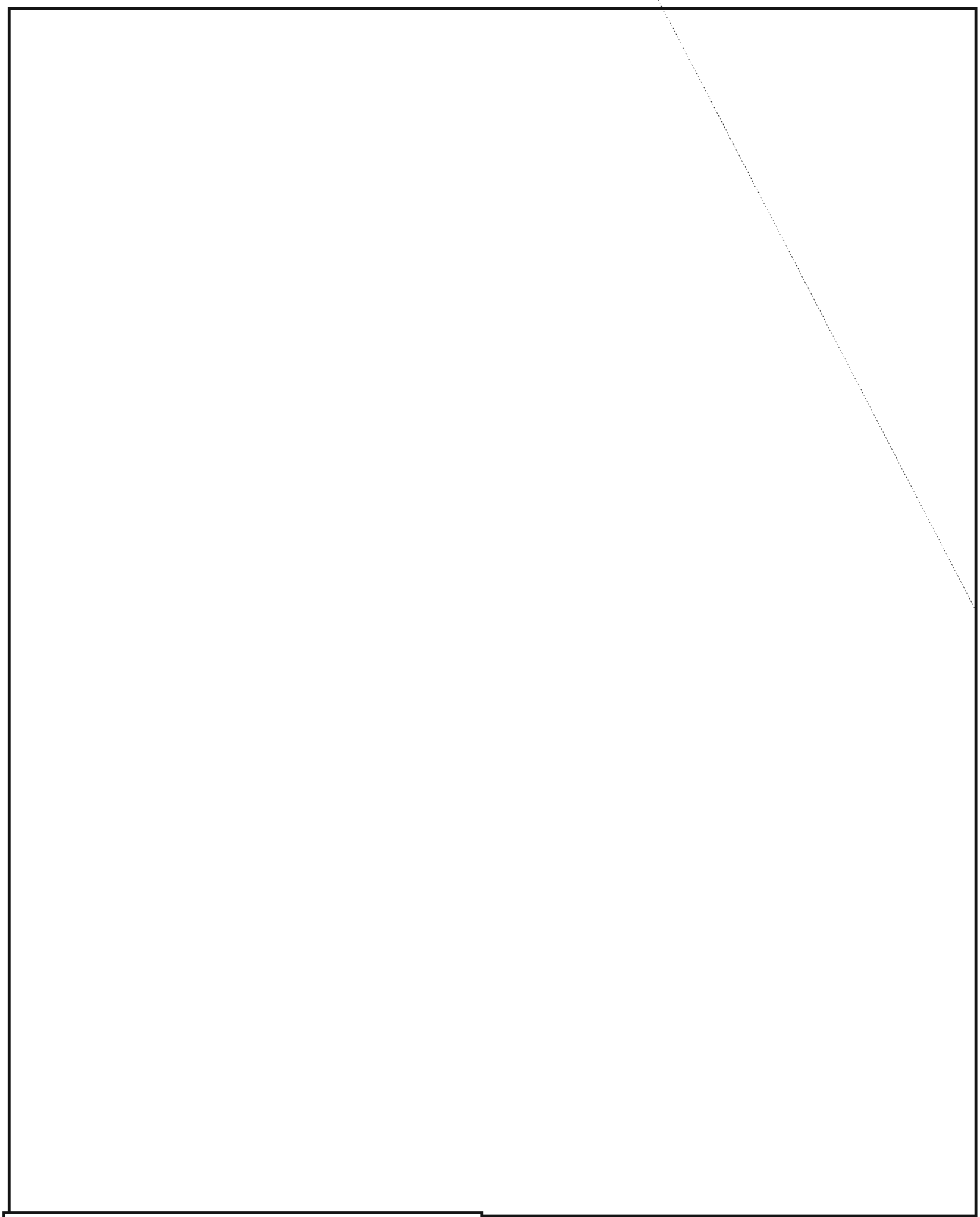
Anthony Reiskis

In this article, which originally appeared in Q*R*L (Quarterly Review for Linguists) for February 1974, the late Mr. Reiskis postulated a

P.L. 86-36
EO 1.4.(c)

EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~



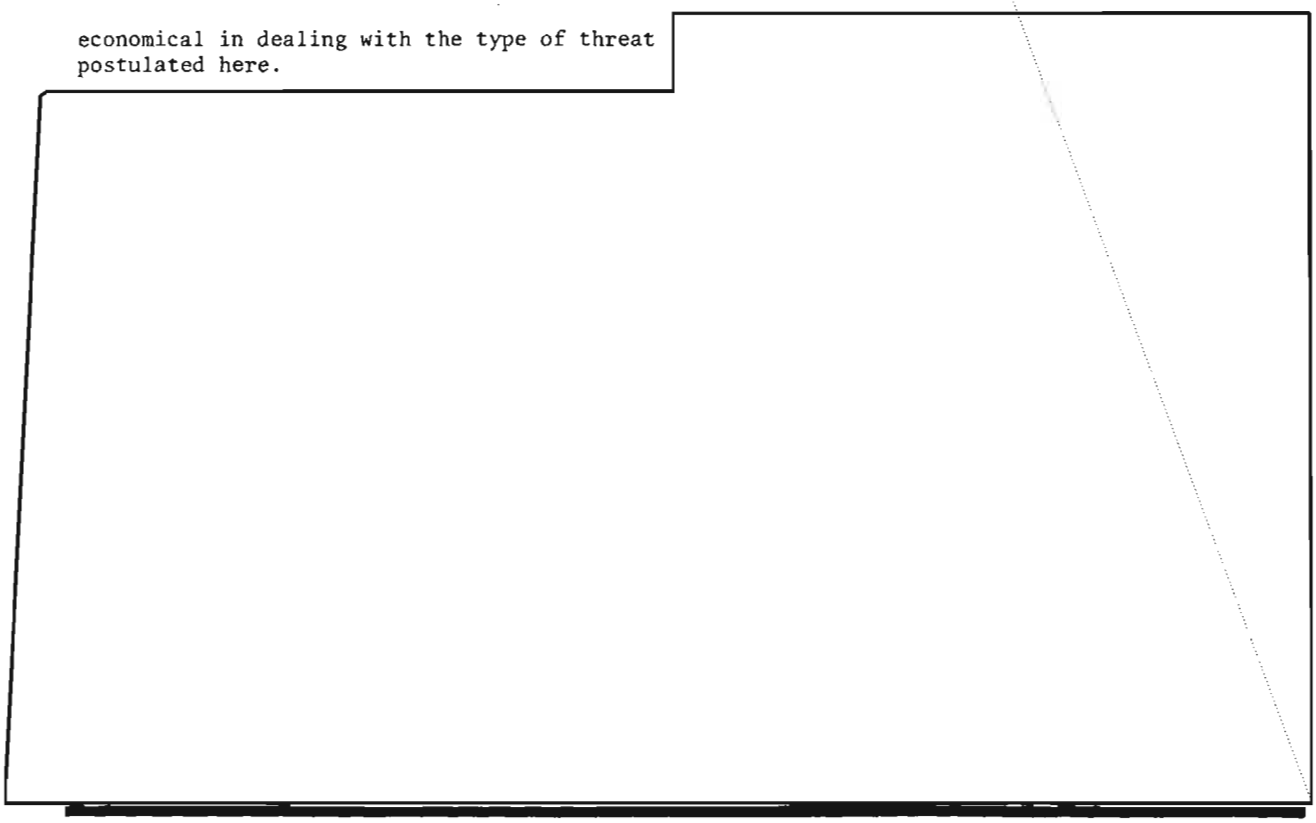
(U) There is a viable alternative which would be more in keeping with the "off-the-shelf" approach, and which would thereby be more

P.L. 86-36
EO 1.4.(c)

DOCID: 4019666

P.L. 86-36
EO 1.4.(c)

economical in dealing with the type of threat postulated here.



The following article appeared in *The Wall Street Journal* for December 1974, and was later reprinted in various NSA publications. It seems appropriate to publish it once again, as a postscript to Mr. Reiskis' article.

UNCLASSIFIED

THE NAVAJO CODE TALKERS

Navajos weren't the first Indians used by the U.S. military to confuse foreign enemies; Choctaws transmitted orders by telephone for the Army infantry in World War I, and early in World War II Comanches were employed in similar activity in the European combat zone. But the Choctaws and Comanches conversed in their native tongues. The Navajos, on the other hand, developed a special coded alphabet of 38 symbols plus an auxiliary vocabulary of 41 other terms. It's been described by anthropologists Henry Dobyns and Robert Euler as "absolutely unbreakable."

Skilled as the Japanese cryptographers were, it's doubtful whether they would have understood Navajo even if there had been no attempt to disguise it. At that time it was virtually an unwritten language and even today few non-Navajos have succeeded in mastering its complex glottal sounds and vowel tones.

But rather than take a chance the Navajo code talkers improvised a system substituting clan names for military units, the names of birds for airplanes and fish for ships, plus a double alphabet when it was necessary to spell out proper names. The idea originated with a Navajo-speaking white man, Philip Johnston, an engineer with the city of Los Angeles who was raised on the Navajo Reservation where his father had been a missionary. During the first few months of the war, he suggested his plan to a high ranking Marine Corps officer. It was approved after five Navajos demonstrated its possibilities to Marine brass.

By April 1942, Marine Corps recruiters arrived at the reservation searching for Navajos who were physically fit as well as fluent in Navajo and English. The first group of volunteers, 29 youngsters from various boarding schools in Arizona and New Mexico, were sent to boot camp at San Diego. From there they were transferred to the Field Signal Battalion at Camp Pendleton, then assigned to Marine combat divisions throughout the Pacific.

Philip Johnston joined the Marines in the fall of 1942 and was put in charge of the code talker training program. Eventually some 320 Navajos served in combat under the program.

The code talkers served in many campaigns, usually in two-man teams conversing by field telephone and walkie-talkie to call in air strikes and direct artillery bombardment. Marine Corps archives contain ringing praise for the Navajos from commanders in the field.

The idea for a formal association of code talkers grew out of the 1969 annual reunion of the Fourth Marine Division Association, which honored several of the Navajos. Two years later the Navajo Tribal Museum, the repository for Philip Johnston's papers and other code talker memorabilia, sponsored a two-day reunion. Now the Navajo Code Talkers Association numbers more than 100 members.

UNCLASSIFIED

C.A.A. NEWS

FRANCIS X. PORRINO

It's always hard to say goodbye to an old friend. Frank Porrino came to work at the Agency is 1955, after a tour with AFSS. At the time of death he was Chief of A1 and President of the CAA. Quick, caring, good-humored, professional — these are some of the words that he brings to mind. If you ever worked near him you will remember his laugh, and the infectious way it spread to those around him.

FUTURE CAA PROGRAM NOTES

27 June, 1400 hours, Room 2W087. [redacted] A05: "Ockham's Razor—A Philosophical Approach to Problem Solving"

7 August, 0900 hours, Friedman Auditorium. Vera Filby, E41: "The Impact of the Privacy Act on SIGINT Reporting"

* *

DID YOU KNOW?????

CIA has a collection of over 20,000 motion picture films and videotapes in its Pictorial Services Branch, Office of Central Reference. This collection dates back to 1940 and includes films and tapes in several languages. The collection ranges from foreign newsreels, documentaries and feature pictures to videotape recordings of foreign and domestic television programming of intelligence interest. The subject content is very broad, covering the entire spectrum of political, military, economic, biographic, scientific, technical, cultural and goegraphic area interests. There are tapes and films of world leaders, Soviet space flights, world-wide political and military events, military parades in Moscow and Havana, to name but a few.

These films and tapes, some of which may contain intelligence information not received in printed form, are available for NSA analysts to borrow or to view at CIA. The Pictorial Services Branch has the technical capability to play back virtually any video format. P.L. 86-36

For additional information, call [redacted] (NSA liaison at CIA) on 983-8215s if you're at Ft. Meade, or 9983-8215s if you're at FANX.

CLUB AND ORGANIZATION OFFICERS--

THE PAGES OF CRYPTOLOG ARE OPEN TO YOU FOR ANNOUNCEMENTS OF YOUR GROUP'S ACTIVITIES. SEND YOUR SUBMISSIONS TO P1, CRYPTOLOG, OR CALL 3957s.

UNCLASSIFIED

(Classified ~~SECRET SPOKE~~ in entirety)

D 12 HELP WANTED (400)

MAINTENANCE MAN. General maintenance duties. Must have com. transp. 622-2400 bet. 9 & 4

MAKEUP ARTIST Demonstrate in fine dept. store. 433-8000, ext. 1211 & 1201.

MALE DANCERS WTD for Go-Go Lnge. Call 284-1330

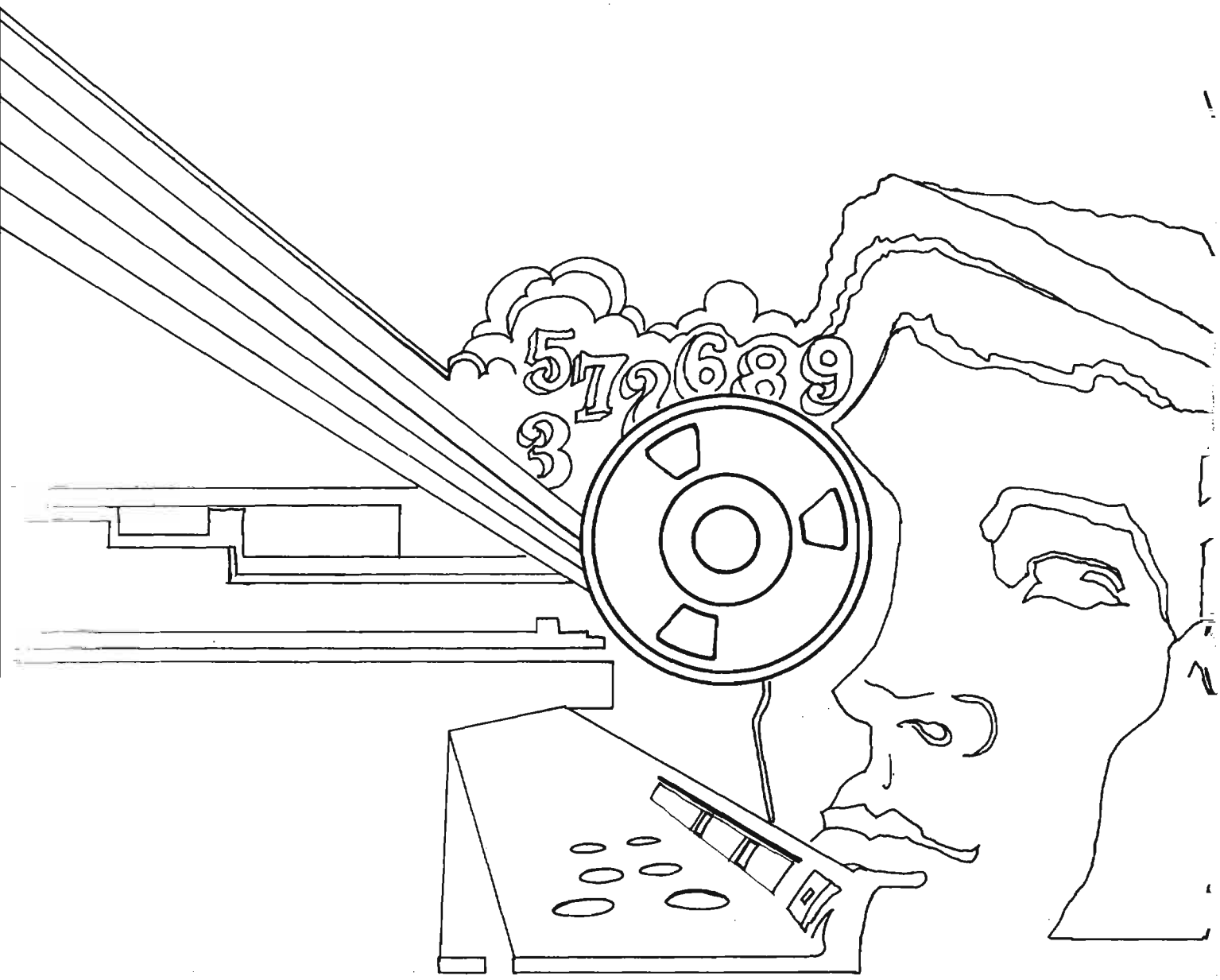
MAN & WIFE TEAM to assist in operation in motels on the Eastern Shore. Must be willing to work PM shift. Salary & in... quarters furnished 827-2250 for ...

[redacted] in G9 has a problem. In the course of his work, he keeps turning up fragments of various published items, all of which are in English. Unfortunately, these scraps are so short that Bill and his colleagues have not been able to identify very many of them. P.L. 86-36

The publications appear to come from a rather eclectic bookshelf. The subjects range from contemporary American fiction to religious mysticism to some rather dreary texts on communist political themes.

If you are a voracious reader with a wide-band approach to the selection of your reading materials, maybe you can help Bill identify some of his bits and pieces. If you'd like to give it a try (and if you have a green badge), call him on 4382s.

~~SECRET~~



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

DOCID: 4009827

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MAY 1979

P.L. 86-36

PROJECT HELIPAD: AN EPITAPH (U)..... [redacted] 1
TRANSCRIPTION TRIO
I. WHERE DO GOOD TRANSCRIBERS COME FROM? (U)..... [redacted] 4
II. "RUN THIS THROUGH YOUR TRANSCRIPTION MACHINE" (U) [redacted] ...6
III. TRANSCRIBER - ANALYST RELATIONS (U).....Doris Miller.....8
CISI NEWS: 1979 SPRING CONFERENCE (U).....9
CLASSIC CABLES (U).....10
EMITTER IDENTIFICATION TECHNIQUES (U) ..... [redacted] 11
MORE THAN WORDS CAN SAY (U).....J. Gurin.....13
NSA-CROSTIC NO. 25 (U).....D.H.W.....16
MORE FAIRBANKS ON ENGLISH (U).....Sydney Fairbanks.....18
CHAPENKO, SHAPENKO--WHAT DIFFERENCE DOES IT MAKE? (U)... [redacted] 19

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON 1 MAY 2009~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009827

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL VI, No. 5 MAY 1979

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor-in-Chief.....David H. Williams (3957s)

Collection..... [redacted] (8555s)

Cryptanalysis..... [redacted] (4902s)

Cryptolinguistics..... [redacted] (5981s)

Information Science..... [redacted] (5711s)

Language..... [redacted] (8161s)

Machine Support..... [redacted] 5084s)

Mathematics..... [redacted] (8518s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Taurone (3573s)

Production Manager.....Harry Goff (5236s)

P.L. 86-36

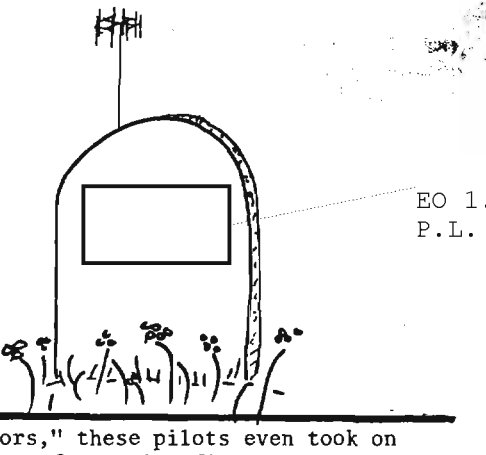
For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4009827

P.L. 86-36

Project HELIPAD: An Epitaph (U)

[redacted]



EO 1.4.(c)
P.L. 86-36

(U) During the Vietnam conflict USAF pilots downed 137 enemy aircraft, an interesting statistic for military air history buffs. Far more significant to the USAF was another, related statistic: 67 USAF aircraft lost to enemy fighters. That was too many.

(U) It was believed that a major cause for this relatively large loss of USAF aircraft was the pilots' lack of combat experience against enemy aircraft. In those days, the first time a USAF pilot saw a MIG was in actual combat, a wartime classroom with a pass-fail grading system.

(U) USAF officials decided that it was essential to give young pilots experience in air-to-air tactics against MIGs, or at least MIG-like aircraft, before going into combat. They developed the Dissimilar Aerial Combat Tactics (DACT) Program, designed to train aircrews against types of aircraft whose performance characteristics resembled those of enemy fighters. In June 1973, to provide this training, the Tactical Air Command established the 64th Fighter Weapons Squadron at Nellis AFB, Nevada. The squadron was composed of pilots specially skilled in Soviet air combat tactics, at least to the extent that these tactics were known. Initially these pilots flew the T38 TALON (and later the F5E TIGER II) to simulate the Soviet MIG-21 FISHBED and MIG-23 FLOGGER fighters. Their mission was to train other USAF fighter pilots how to fight and win against Soviet aircraft and tactics. Known as "aggressors," these pilots even took on the trappings of a Soviet fighter unit, flying Soviet flags, wearing Soviet insignia, and decorating their offices and ready rooms with Russian wall posters, manuals, photographs and model aircraft. Their own fighters carried Soviet markings...

(U) That's the beginning of the story.

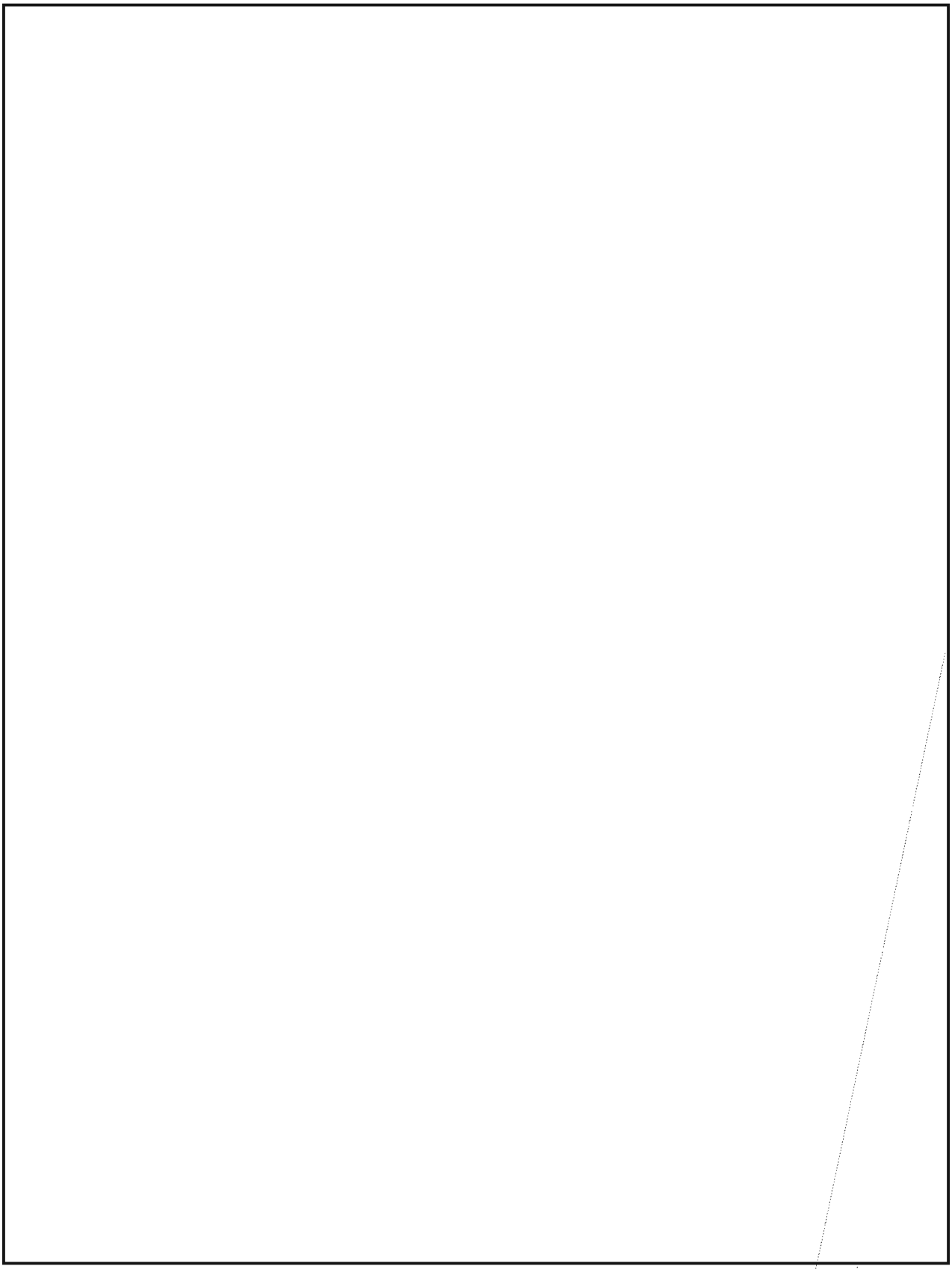
[redacted]

[redacted]

[redacted]

[redacted]

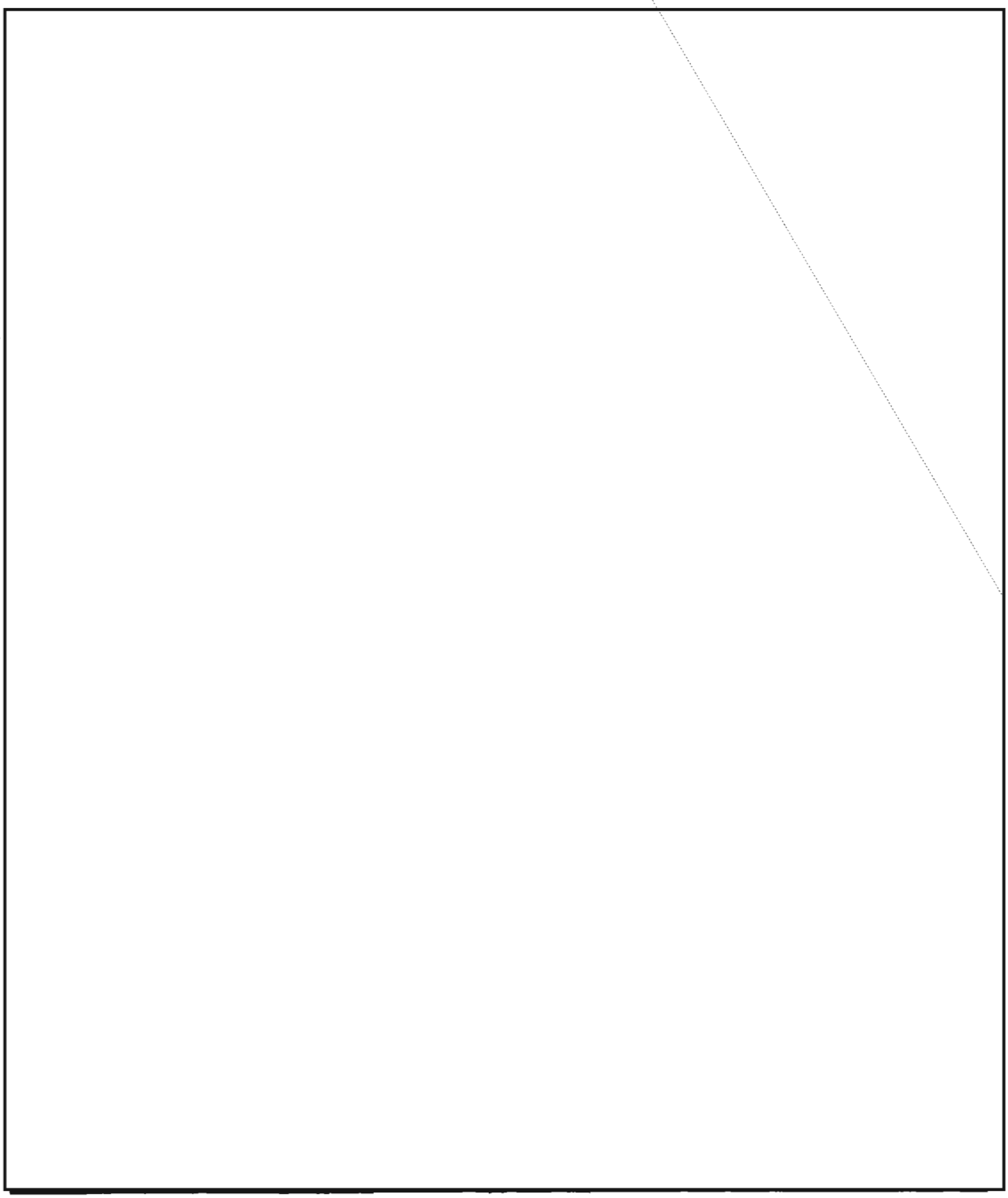
EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~



PROFICIENCY CERTIFICATION FOR MILITARY LINGUISTS (U)

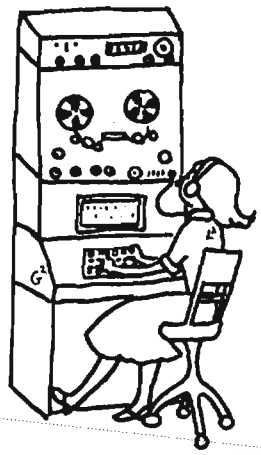
(U) The Language Proficiency Test certificate program for military linguists is now under way. The first certificate has been sent to [redacted] for passing the Spanish LPT. [redacted]

(U) Other certificates are being printed and will be presented in the near future. If you are interested in getting more information on how to receive a certificate for your linguistic abilities, contact CAPT [redacted] USAF, M36, phone 5578s or 688-6565.

P.L. 86-36

~~SECRET SPOKE~~

Transcription Trio (U)



I. Where Do Good Transcribers Come From? (U)

In the following article, the first of our authors, [redacted] answers the above question by saying "They don't." Good transcribers are the result of a lengthy period of classroom and on-the-job training right here on the premises.

The Russian voice transcription effort at NSA has been undergoing a gradual, but ~~(S-CCO)~~ far-reaching, evolution over the last five

[redacted]

~~(C)~~ As stated previously, the Agency's transcribers are not the product of a common language background. Some have received strictly military language training, some have college degrees in Russian, and still others with either high school diplomas or college degrees have received their Russian training here at the Agency. Each of these training methods has its own unique strengths and weaknesses; in order to compensate for some of these weaknesses, the NCS provides a plethora of courses.

P.L. 86-36

(U) The courses offered by the NCS are designed to address the transcriber's specific language problems. Courses are offered in the fields of grammar, syntax, linguistics, phonetics, translation, conversation, and area studies. These courses are intended to fill in the gaps in an individual's language background, and to allow him the opportunity to improve his skills on a continuing basis. By taking these courses, the transcriber is able to update and refresh his knowledge; the Agency, by sponsoring these courses during the work day, indicates its support for this on-going process.

EO 1.4.(c)
P.L. 86-36

~~(C)~~ Many transcribers also improve their skills by taking advantage of the Agency's After-Hours Study Program. This has proven especially beneficial to the military-trained transcribers who are able to obtain college degrees through this program and increase their understanding of the Russian language, and of the Soviet Union as a whole.

(U) The Agency also provides numerous opportunities for those individuals interested in making transcription a career. The first step for most is the Agency's professionalization program. To be certified as a linguist, an individual must demonstrate a high level of competence in both translation and transcription. Serious career linguists also have the opportunity to attend the two-year intensive language course taught by the Department of the Army in Garmisch, West Germany.

(U) A recent, exciting development for some transcribers has been the decision to allow a small number of career transcribers to progress beyond the Grade 12 level without the normally attendant managerial responsibilities. This step was taken in response to the critical need to retain senior transcribers in transcription billets; these individuals will thereby be able to devote their full time and talent to that which they can do best—transcription.

Too often in the past, the Agency has invested money and years of training to produce a highly competent linguist only to put that person in a managerial job where his talents cannot be utilized fully.

[redacted]

(S) There are two main areas of knowledge which every transcriber must learn, regardless of his proficiency in the Russian language itself. The first such area could be termed *target knowledge*. Target knowledge is comprised of three quite different parts:

- vocabulary
- general understanding of the subject involved (if you don't understand the concepts in English, you'll be lost trying do do it in Russian)
- sufficient understanding of the Soviet society to comprehend the personality and habits of the person speaking

[redacted]

(U) It becomes obvious, therefore, that if a transcriber is to produce a finished transcript, he must gain at least a fundamental knowledge of the subject under discussion.

[redacted]

DOCID: 4009827

EO 1.4.(c)
P.L. 86-36

in the analyst's understanding of what is actually taking place.

(U) Still another essential factor in the training of any transcriber is his ability to use the multitudinous transcriber working aids. A transcriber's working aids might be compared to a physician's medical reference books: regardless of the individual's innate intelligence, his ability to handle a given set of circumstances would be severely hampered, if not made impossible, by their absence.

(U) The extent of the resources available to a transcriber is such as to bewilder the trainee. Over a period of years many transcribers gradually accumulate a considerable number of their own personal reference materials. These working aids may take on any number of forms from printed dictionaries to computer files.

~~(S-CCO)~~ Let us first look at those basic reference books which are widely distributed to incoming transcribers.

- A standard Russian-English dictionary, obviously the first item

[redacted]

[redacted]

~~(S-CCO)~~ In addition to these basics, there are other working aids which enable the transcriber to do his work; most of these are specifically related to the subject matter of the material being transcribed in his area. These may include the following.

[redacted]

(U) It cannot be stressed enough that these resource materials are essential to the production of a finished transcript; all of them, many of which originate within NSA, are worthless in the hands of an amateur, but invaluable to the experienced and knowledgeable transcriber.

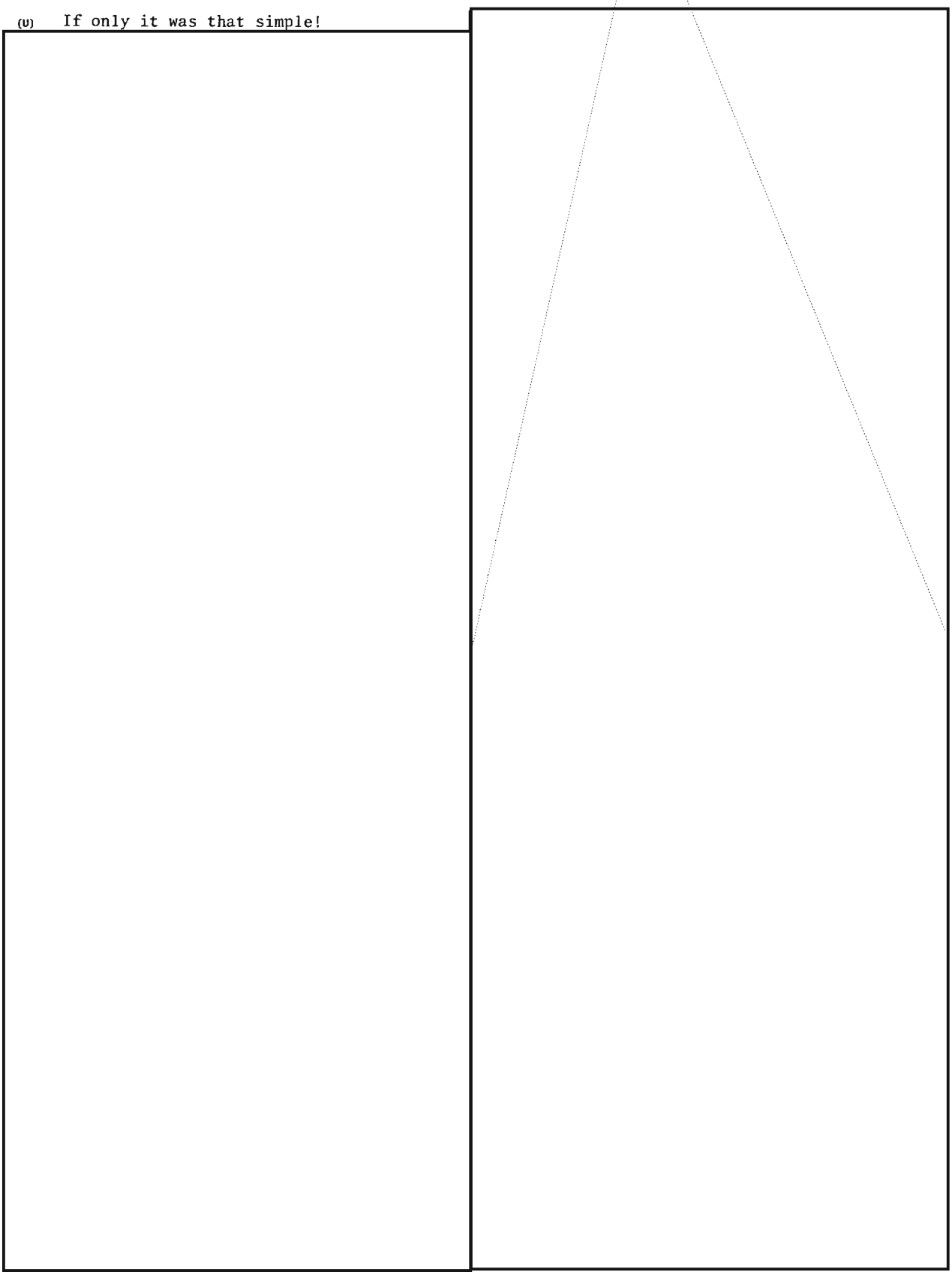
II. "Run This Through Your Transcription Machine" (U)

[redacted]

P.L. 86-36

It is sometimes assumed by non-linguists that transcribers are a sort of like parrots. They simply repeat, in written form, what someone has said. Thus, while a transcriber needs to know the language of what he scribes, he certainly doesn't need to *think*, just repeat. This is, of course, a very narrow view of the transcriber's task at NSA, and while you might laugh and say, "I know there's more to it than that," it is quite surprising to find the number of people who feel that transcribers are like machines. An inside joke among transcribers is the remark attributed to a non-transcriber who once asked one of the transcription offices to "run this tape through your transcription machine."

(U) If only it was that simple!



EO 1.4.(c)
P.L. 86-36

(U) Thus, as can be seen, a transcriber is by no means a simple parrot or machine. The job he is asked to do is not only quite complex, but requires skill and dedication to enable him to stick with a job even when the going gets rough.

(U) I hope that this article has provided an insight into what it is that Agency scribes do and dispels the myth that voice processing is a simple matter of "running this through the transcription machine."

EO 1.4.(c)
P.L. 86-36
(U)

III. Transcriber-Analyst Relations

Doris Miller, Retired

THE COMPUTER AND INFORMATION SCIENCES INSTITUTE (U)

THE USER -- IT'S ABOUT TIME! (U)

(U) Mark your calendar today for May 21-25, because you'll not want to miss the 1979 CISI Spring Conference. The Computer and Information Sciences Institute is sponsoring an exciting and informative Computer Conference, with this year's emphasis on YOU, the computer user. The speakers, who represent some of NSA's most knowledgeable professionals in a variety of career fields, will be talking on topics and issues that are extremely important and topical to NSA's computer user community.

(U) With intriguing titles such as "I Want My Program to Talk to Me" and "Wanted: A French Chef for Analytic Programming," and state-of-the-art subjects such as RASTER graphics at NSA, Human/Machine Interfaces, User Computer Security, and Intelligent Terminal Applications, this year's sessions promise to be the best ever.

(U) Schedules for each session will be posted the week before the conference. CISI is anticipating a large turnout for the sessions and especially wants you to be a part of this SUPER EVENT!

(U) The general topics for the five sessions are

Monday, 21 May	The User Himself
Tuesday, 22 May	Applications
Wednesday, 23 May	Computer Security
Thursday, 24 May	Acquisition, Methodology, and Standards
Friday, 25 May	Tools

(U) All sessions will be held in the Friedman Auditorium, from 0900 to 1130.

~~CONFIDENTIAL~~

CLASSIC CABLES

(DEPARTMENT OF FULLER CLARIFICATION)

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~CONFIDENTIAL~~

RNI

01 01 V11-0050-79 RR RR CC
~~COMINT CHANNELS~~
S
FM DIRNSA
TO COMNAVINTCOM
INFO NAVINTSUPCEN
NFOIO
NISC
ACNIC
~~C O N F I D E N T I A L COMINT CHANNELS~~
+V11-0050-79
COMNAVINTCOM FOR NAVY SIRVES REP; NFOIO FOR OOL AND ACNIC; NISC FOR
5212; NIC FOR 311
REQUEST FOR INFORMATION
A. NSA/V11-044-79, 2221537 JAN 79
B. COMNAVINTCOM, 0515017 JAN 79
C. NFOIO, APP-0002-79, 0416467 JAN 79
D. NAVINTSUPCEN, 2921037 DEC 78
SIRE 6676
REF ALFA RESPONDS TO REF DELTA AS VALIDATED BY REF BRAVO.
REVW 24 JAN 09.
++++
M/R MESSAGE IS SELF EXPLANATORY
DIR, D/DIR, DDO, DS, V, V1, V11(L), V12, V14, A05, A205, A24

[redacted] V111/48525 ROBERT ENNIS/CH V111/48525
SMO/ORDINAL DAY 1047, 024
DTG 241958 JAN AB14

~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~
~~REVIEW ON 24 JAN 09~~

P.L. 86-36

~~CONFIDENTIAL~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

Emitter Identification Techniques

[redacted] W2

P.L. 86-36

This article is classified ~~SECRET HVCCO~~ in its entirety

The term "emitter identification" denotes the association of a signal with a specific source or platform. The identification process usually involves matching parameters of the signal with those from known emitters and producing a list of candidates. Related information (such as that obtained from [redacted] can serve either to restrict the number of known emitters used in the matching process or to further refine the list of possibilities produced by the matching algorithm.

EO 1.4.(c)
P.L. 86-36

[redacted]

For over a year R51 has been investigating mathematical/statistical techniques for addressing aspects 2 and 3. [redacted]

The R51 effort has focused on ways to evaluate an emitter identification technique. Evaluation of such a technique is interpreted here to mean:

- evaluation of the choice of features
- evaluation of the performance of a decision rule on vectors of features.

The issues addressed are the following:

- usefulness of the features (How well do the features separate the known emitters?)
- adequacy of the library for training (How many transmissions of each emitter are necessary for the given set of features?)
- complexity of the decision rule (Is the decision rule sufficiently sophisticated to separate the emitters in the chosen feature space?)
- estimation of the error rate of the decision rule (What is the expected percentage of misclassifications in new data?)
- incorporation of no-decision options into the decision rule (an "open" library versus a "closed" one)

EO 1.4.(c)
P.L. 86-36

[redacted]

There are many types of decision rule that may be chosen for use in emitter identification. Among those studied by R51 are the

P.L. 86-36
EO 1.4.(c)
DOCID: 4009827

following:

- minimum distance (or maximal correlation)
- k-nearest neighbor (weighted or unweighted)
- discriminant functions (linear or quadratic)
- Bayes' rules

The parameters of a decision rule are estimated using a learning set consisting of transmissions from known emitters. The finite sample performance of the decision rule on a prescribed set of features can be evaluated on a test set (a different set of transmissions from the same known emitters) in terms of:

- error rate (percentage of misclassifications)
- confusion matrices (correct class membership versus that produced by the decision rule)
- expected position of the correct identification in a list of candidates
- probability level associated with the correct identification versus that of an incorrect one

From test set performance one can infer decision rule performance on unknown data and decide whether or not the given features and decision rule are adequate for the purpose intended.[1]

Some R51 work has been done on library maintenance. The inclusion of erroneously classified emitters into the library can distort the set of reference patterns. Peri-

[redacted]

In summary, R51 research [redacted] has made available a plethora of techniques and computer programs that can be used by those involved in emitter identification work. All software runs are on the R5 CDC 6600, but most of it is in Fortran and should be readily available to other computers. Questions about these techniques and/or the software should be addressed to [redacted] Chief, R51, 8518s, or [redacted] Chief, R513, 8525s.

1. Details about these algorithms and methods can be found in the following R51 publications:

"Cluster Analysis: Introduction to Models and Methods," *NSA Technical Journal*, Vol. XXII, No. 2, Spring 1977

"Introduction to Statistical Pattern Recognition," *NSA Technical Journal*, Vol. XXII, No. 3, Summer 1977

"Some Thoughts on Coalitions Discriminant Analysis," R51/MATH/28/77, 20 July 1977

FOR THE PUZZLE FANS (U)

(U) Given below are the numbers of the squares which contain the *final* letters of each word of the NSA-Crostic on page 16. Simply thicken the lines at the right sides of these squares, and you're in business.

4	8	18	22	31	35	39	44	48	50	53
57	59	63	67	72	74	83	88	90	92	96
101	105	107	112	114	120	122	128	134	136	145
149	151	155	158	164	175	177	184	188	195	198
206	209	211	217	221	223	227	233	240	244	248
255	257	260	271	273	277	281				

SOLUTION TO NSA-CROSTIC NO. 24 (U)
(*CRYPTOLOG*, April 1979, by D.H.W.)

[redacted] "[The] Bucky Balance," *CRYPTOLOG*, July 1978

(U) "The best way to [identify] a Project Starter or a Project Finisher is to [analyze] the person's working habits closely. The Project Starter is interrupt-driven... He operates on a last-in-first-out basis... The Project Finisher functions as a first-in-first-out queue... Every task that enters his queue comes in at the lowest priority."

P.L. 86-36

J. GURIN, R51

More Than Words Can Say

As a part-time jazz musician, I can vouch for the fact that there seems to be no way of writing down the improvisations of some of our jazz greats, even after listening to their recordings again and again. One can capture on paper the notes they play without too much difficulty, but not *how* they play those notes. The same problem plagues the classical musician as he attempts to play compositions of the masters. How loud is *forte?* How fast should *presto* be? How much emotion in *con amore* and how much and how quickly should one slow down for *ritard?* The instructions left by composers serve only as very imprecise guides.

Although many claims have been made for this system or that one, none has succeeded in recording the dance so that the choreography of a Fokine or an Ailey may be transmitted other than by example. There just doesn't seem to be any way to notate choreography successfully, and even the motion picture, which once was looked upon as the answer to the problem, has shown fatal weaknesses as a complete record.

Writing systems for spoken language also present only approximate representations of what is said. I'll never forget how impressed I was when, for the first time, I heard Mark Antony's lines "Friends, Romans, countrymen, lend me your ears" spoken by a fine Shakespearean actor. It sounded very different from the dull recitation in my high school English classes. The words were there in the book we read in school, but something had to be supplied by the actor. It is possible, or course, to indicate how a sentence should be read by using italics for stressed words, or by underlining those words. Thus we may distinguish "Don't ever *do* that again" from "Don't ever do *that* again."

But this device only tells us that the underlined word should be emphasized; it doesn't tell us how, or how much. Some sentences remain ambiguous until spoken aloud, as in the case of "Jane left directions for George to follow," which can have two distinct meanings.

There are a number of terms that are used to describe those features that distinguish completely meaningful speech from the simple recitation of strings of words. *Prosody* and *intonation* are two of the common ones, while the fancy word *suprasegmentals* simply describes features which extend beyond segments of words such as *phonemes*. The easiest way to describe any of these is in terms of what it is not. It is what is left when you take away traditional grammar, vocabulary, and rules for pronunciation of segments of speech. In other words, you are left with pitch, loudness and duration.

The nature of our concern here directs us to the perception rather than the generation of these features. For us there is no sound in the forest when a tree falls—if there is no one there to hear it. And by introducing this notion of human perception we bring in the factor which complicates everything. If it weren't for the perception mechanism and its special qualities, it would be a simple matter to equate pitch, loudness, and duration with frequency, intensity and time, which are easy to measure and manipulate. In fact, it may seem obvious now that there is no one-to-one relation between frequency/pitch, intensity/loudness and length/duration, but this is a relatively recent discovery. It was Galileo who first established pitch as a function of frequency, and it was not until the 1930s that it was shown to be a function of intensity as well, and possibly of other factors.

In some ways, perhaps, duration is the easiest to understand. Its principal ingredient is time. But in examining the question of the shortest durations of sound that a human listener is capable of noticing, investigators have determined that intensity plays a part. Increasing the intensity, up to a certain level, tends to improve the listener's capacity to discriminate between duration differences.

Loudness presents another concept that, on the face of it, seems simple enough, but can be shown to be more complex when one realizes that perception of loudness involves some tricks played by the mind. A simple ex-

periment displays this dramatically. Assemble several radio receivers in one room, tune them all to the same station, then mark their volume controls at the settings that make them all sound equally loud *when played separately*. Listen to one radio by itself, then turn another one on to the mark on the volume control. The two together will be louder than one alone, of course. Now do the same with a third: the loudness will increase, but not as much as before. Adding each of the remaining radios will continue to add to the loudness, but each time the increment will be smaller.

Consider another dramatic illustration of the relationship of the intensity (power) of sound and the loudness of that sound as perceived by the ear and brain. Under the proper conditions, the intensity of the sound of a full orchestra in a fortissimo passage may be about 20 *million* times as great as that of a solo violin in a soft passage. But of course it does not sound 20 million times as loud!

When one considers the relationship between intensity and loudness, it is clear that one can scarcely be simply proportional to the other. It seems that there is a law which is more or less true for all sensations—pressure, sight, hearing, etc.—that the intensity of the sensation is proportional not to the stimulus but to the logarithm of the stimulus. This means that every time the stimulus is multiplied by the same factor, the sensation goes up one step. In other words:

Stimulus	Sensation
goes from 10 to 100	increases one step
goes from 100 to 1000	increases one step
goes from 1000 to 10000	increases one step
	etc.

Before you relax too much on the subject of loudness, let me add the following. Our perception of loudness is also influenced by frequency. For example, for two tones not far removed in frequency, doubling the power by adding these tones results in approximately double the loudness. But doubling the power by adding the same tone to itself may not double its loudness at all. In fact, we may have to increase the intensity of a tone as much as *eightfold* in order to double its loudness. This holds true for all except very faint tones, where doubling the power more than doubles loudness!

Of the prosodic features of speech, the one which seems to attract the most attention is pitch. Here again we run into problems of perception. And just to demonstrate that sometimes old friends may fail you, permit me to quote a definition from the Merriam-Webster dictionary which is not quite correct. According to that usually reliable source, pitch is "that property of a musical tone which is determined by the frequency of the sound waves which strike the ear. The larger the number of vibrations per second the higher the pitch." Close, but definitely no cigar. Frequency may well be the most important element in determining pitch, but it is by no means the only one.

For example, judging the pitch of a single-frequency sound depends to some extent on the loudness level of the sound. A large increase in loudness may drop the apparent frequency by a readily perceptible amount. Because of this apparent lowering of pitch, a vigorous trumpet player will often accuse his gentler colleagues of playing sharp, because his own notes are so loud in his ears. The orchestra's conductor has to mediate this quarrel, and must try to arrange things to satisfy the audience, which hears all the instruments at a lower level of loudness, where the effect is negligible. In a series of experiments, it was found that with increases in intensity there were pitch decreases for all frequencies up to 2000 vibrations per second, after which there were very slight pitch *increases* as intensity increased.

Some of these strange goings-on may be explained in part by the fact that the ear is not equally sensitive to all frequencies. Of two sounds of equal intensity but of different frequency, one may be subjectively louder than the other if it falls into a frequency range at which the ear is more sensitive.

Another illustration of the relationship between pitch and frequency is this: if a musical tone is composed of a series of harmonic frequencies, with which frequency is the pitch to be associated? Surprisingly enough, it may not be the one with the most energy, nor the lowest frequency. As a matter of fact, if a given musical sound were composed of frequencies at 200, 300, 400 and 500 Hz, then one would hear the pitch at 100 Hz. Or, if the component frequencies were at 400, 600, 800 and 1000 Hz, one would judge the pitch to be that of a 200 Hz tone. If you wish to continue the game, add to the last batch tones at 500, 700 and 900 Hz and the perceived pitch will drop an octave to 100 Hz. In other words, when a tone consists of several frequencies differing by a constant amount, the perceived pitch may be that of a tone whose frequency is equal to the common difference, as shown below. So in these cases one hears pitches with frequencies that aren't there!

Frequency (in Hz)	Complex Tones A	B	C
1000		XXX	XXX
900			XXX
800		XXX	XXX
700			XXX
600		XXX	XXX
500	XXX		XXX
400	XXX	XXX	XXX
300	XXX		
200		!!!	
100	!!!		!!!
	Actual frequency:		XXX
	Apparent frequency:		!!!

In tonal languages like Chinese, pitch is a vital element in the lexical sense. That is to say, individual words contain a pitch pattern which distinguishes them from other words. Speakers of non-tonal languages find it difficult to hear these tones, but not because they have no experience in handling pitch. The English intonation system is fully as complicated as any tonal system used in Southeast Asia or Africa. Furthermore, English speakers easily learn to sing songs employing a dozen or more intervals, whereas a tone language of just a few contrastive levels may seem extraordinarily difficult to them. Perhaps the explanation for this lies in the fact that speech intonation, such as is employed in a non-tonal language, like songs, merely add *extra* shades of meaning to lexical meanings. Tonal languages, in contrast to this, employ pitch as an intrinsic part of each word.

The use of pitch differences to convey linguistic information appears to be universal, and many languages share the same or similar practices. In nearly all languages a falling pitch signifies the completion of a grammatical unit such as a normal sentence. On the other hand, an incomplete utterance, one deliberately left hanging in mid-air and clearly signifying that there was more to the thought than had been uttered, has a rising intonation.

Granted that in speech the pitch pattern conveys information about the speaker, his emotional and physical state, his cultural and regional background, etc., my principal concern here is with pitch that distinguishes the meanings of utterances. The other day I heard a joke that I did not understand because the teller failed to use the right pitch pattern for the pun, which was the point of the story. The joke was about a clone who had become very foul-mouthed and was pushed out of a window on the 17th story of a building. The punch line was:

"He made an obscene clone fall."

As the story was told, the pitch pattern for the punch line was like the one in "He made an absurd man call," while it should have been like the one in "He made an obscene phone call."

Let's face it, the human mind simply isn't up to perceiving speech sounds exactly as they are produced. The ear itself is physiologically incapable of responding to changes which are too rapid or too minute. The subjective record of how sounds are perceived may be expected to differ considerably from an instrumental analysis of the same group of sounds. Modern theories of perception postulate an active, decision-emitting listener who busily constructs a perceptual model of his world by selectively abstracting information from the stimuli surrounding him. Any attempt on our part to process speech by machine must take into account this propensity on the part of the human mind. The words that are used in speech communication are of primary importance, of course, but often the real message is contained in how they are said. Somehow we must discover how to simulate human perception in an area which is difficult to describe with precision, and is even more resistant to understanding.

P.L. 86-36

DOCID: 4009827

NSA-Crostic No. 25

By D.H.W.

For the benefit of readers who complain that these puzzles are too easy, this one is given in diagramless form. Readers who do not feel this way may find relief on page 12.

DEFINITIONS

A. How to express the most well-known line of the "Rubaiyat" in telegraphese

B. Sweet dish

C. "_____ even by God..." Browning's *Paracelsus* (5 wds)

D. Humphrey Bogart's only line in his Broadway debut—really! (2 wds)

E. Having virtually unlimited authority

F. Civil _____

G. Why, explained the circus owner to the departing human cannonball, a replacement was going to be difficult to locate (8 wds)

H. Openings

I. Summer outdoors machinery

J. Low-priority telegram (2 wds)

K. Archie Bunker's daughter's telegram explaining that her Sunday arrival would be delayed 24 hours because of a bus breakdown (4 wds)

L. Try

M. "_____, and we'll tell you what you are afraid of." Robert Benchley (4 wds)

N. 7:52 (3 wds)

O. Princess of Monaco's roadster

P. A people of Asia Minor (2nd millenium B.C.)

Q. Caesar considered this to be nothing

R. Powerless; ineffectual; lacking vigor

WORDS

78 132 161 103 141 264 119 31 205 176 253

239 18

233 203 54 227 48 122 105

85 249 139 191 171 82 196 159 30 180 265

280 72 6 17 135 229 286

209 271 142 101 80 5 16 194 246 279 254 53

59 215 43 231 168 107 224 160 204 68

128 150 133 61 64 244

9 270 206 240 172 250 29 32 162 185 62 71

120 84 283 76 248 131 184 41 99 50 37

157 138 198 3 220 125 193 214 67 230

287 47 144 181 149 28 165 14 212

174 42 210 86 202 259 100 129 189 115

25 276 195 242 60 10 8 218 36 83 140

44 251 23 97 217 267 182 235 167 12 116 137

288 20 201 243 127 77 111 130 192 222 65

148 45 35 39 7 118 51

252 234 27 11 117 257 46 187 213 285 266 69

232 173 183 81 92

166 268 236 275 13 143 24 164 75 199 134 55

170 1 21 263 145 79 88 255 15 34 26 190

52 113 272 274 91 90 211 74

258 226 219 153 237

238 163 57 49 158 179 98 58

DOCID: 4009827

S. Seatless leather trousers

T. One who bears witness

U. Fictional land of little people

V. Planet

W. Elevator man

X. Highest in position, place or rank

Y. Latin-American dance (var.)

Z. "North by _____"

a. Rooflike cover over a window

b. Flat, even, smooth

87 225 200 262 114

261 221 223 4 277 146 175 178

95 216 154 22 73 228 284 151

282 208 247 256 241 108 186

121 102 89 63

124 66 38 56 110 40 273 19 281

112 147 197 188 207 269

2 136 109 245 33 152 94 278 260

104 93 106 70 156 126

96 177 123 169 155

1 O	2 Z	3 G	4 T	5 D	6 C	7 L	8 J	9 G	10 J	11 M	12 K	13 N	14 H	15 O	16 D	17 C
18 A	19 X	20 K	21 O	22 U	23 K	24 N	25 J	26 O	27 M	28 H	29 G	30 C	31 A	32 G	33 Z	34 O
35 L	36 J	37 G	38 X	39 L	40 X	41 G	42 I	43 E	44 K	45 L	46 M	47 H	48 B	49 R	50 G	51 L
52 P	53 D	54 B	55 N	56 X	57 R	58 R	59 E	60 J	61 F	62 G	63 W	64 F	65 K	66 X	67 G	68 E
69 M	70 a	71 G	72 C	73 U	74 P	75 N	76 G	77 K	78 A	79 O	80 D	81 M	82 C	83 J	84 G	85 C
86 I	87 S	88 O	89 W	90 P	91 P	92 M	93 a	94 Z	95 U	96 b	97 K	98 R	99 G	100 I	101 D	102 W
103 A	104 a	105 B	106 a	107 E	108 V	109 Z	110 X	111 K	112 Y	113 P	114 L	115 I	116 K	117 M	118 L	119 A
120 G	121 W	122 B	123 b	124 X	125 G	126 a	127 K	128 F	129 I	130 K	131 G	132 A	133 F	134 N	135 C	136 Z
137 K	138 G	139 C	140 J	141 A	142 D	143 N	144 H	145 O	146 T	147 Y	148 L	149 H	150 F	151 U	152 Z	153 Q
154 U	155 b	156 a	157 G	158 R	159 C	160 E	161 A	162 G	163 R	164 N	165 H	166 N	167 K	168 E	169 b	170 O
171 C	172 G	173 M	174 I	175 T	176 A	177 b	178 T	179 R	180 C	181 H	182 K	183 M	184 G	185 G	186 V	187 M
188 Y	189 I	190 O	191 C	192 K	193 G	194 D	195 J	196 C	197 Y	198 G	199 N	200 S	201 K	202 I	203 B	204 E
205 A	206 G	207 Y	208 V	209 D	210 I	211 P	212 H	213 M	214 G	215 E	216 U	217 K	218 J	219 Q	220 G	221 T
222 K	223 T	224 E	225 S	226 Q	227 B	228 U	229 C	230 G	231 E	232 M	233 B	234 M	235 K	236 N	237 Q	238 R
239 A	240 G	241 V	242 J	243 K	244 F	245 Z	246 D	247 V	248 G	249 C	250 G	251 K	252 M	253 A	254 D	255 O
256 V	257 M	258 Q	259 I	260 Z	261 T	262 S	263 O	264 A	265 C	266 M	267 K	268 N	269 Y	270 G	271 D	272 P
273 X	274 P	275 N	276 J	277 T	278 Z	279 D	280 C	281 X	282 V	283 G	284 U	285 M	286 C	287 H	288 K	dhw

DOCID: 4009827

more Fairbanks on English

Continuing with the observations of Dr. Sydney Fairbanks on current American English, CRYPTOLOG *offers his remarks from the July 1958 issue of* The NSA Technical Journal, *covering, among other matters, "irregardless." Dr. Fairbanks' comments are just as timely now as on the day they were first published.*

Two different garage mechanics have assured us that the starter on the car is suffering from a defect in the "cellunoid." After due inquiry we incline to the belief that the word is the offspring of "celluloid" and "solenoid." With the advent of plastics, "celluloid" must be disappearing rapidly from the popular vocabulary and it is pleasant to think that it leaves one descendant, however illegitimate. If the object in question were a solenoid made out of celluloid—but the engineers tell me this is improbable—we should have a case of a "portmanteau" word generated, as it were, spontaneously, whereas most such words are deliberate acts of creation. Lewis Carroll, who christened them, exploited the idea more fully than anyone else—except of course, James Joyce—and the preface to *The Hunting of the Snark* is recommended reading for those who plan to embark with *Ulysses*. But the whole point of Carroll's inventions, such as "frumious" for "fuming-furious," is that they are self-conscious. In only one case—"chortle," presumably from "snort" and "chuckle"—has the creature sneaked through the barrier of literature, and moved into the outside world where *Jabberwocky* is no longer a part of the scenery.

The same may be said of like inventions of humbler origin. "Aggranoying," of obvious parentage, enjoyed a somewhat dreary vogue in England shortly after the death of the Great White Queen, being used chiefly in discourses addressed to the very young. It was in a class with "thusly," which was likewise intended to be recognized as an amusing blunder. But we cannot remember that "irregardless" (by "irrespective" out of "regardless") was ever a humorous invention, although Webster *("Erron. or humorous, U.S.")* gives it the benefit of the doubt. In our editorial capacity, alas, we meet with both "thusly" and "irregardless," employed totally without humorous intent. The word "insinuendo," offered by a friend of ours, seems to us full of charm and deserving of an appreciative audience, yet the thought of having it pass into the "irregardless" group acts as a serious deterrent. Better perhaps to strangle it at birth.

What chiefly daunts the editor, however, in that endless, hopeless, rearguard action against neologism to which all his kind are dedicated, is not the hybrid word but the hybrid construction.

"Termed incorrect," for instance, and "described as incorrect" meet each other in some ninth circle of the popular mind, and "termed as incorrect" emerges. "He said he was going" and "He stated that he was going" give "He stated he was going" or even "Goodbye, he stated." "I convinced him that he should go" and "I persuaded him to go" produce "I convinced him to go." "I saw him going downstairs" and "I was told of his going upstairs" combine in "I was told of him going downstairs." "Other than" and "different from" beget "different than." "Much alike" and "very different" yield "much different." "As regards" and "in regard to" create "in regards to." "Equals" and "is equal to" give rise to "equals to." And so on, from here to Mesopotamy. The general principle, that if two words are equivalent in any respect they must be equivalent in all respects, moves on remorselessly, and the world has grown grey at its breath.

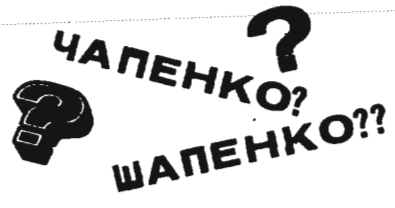
In such moods we try to take comfort in the historic approach. Dean Swift felt with perfect justice that "mob," a slang abbreviation of a stale classicism, *mobile vulgus*, was the sort of word that no one with any sense of style would permit himself to use; but the earth continued in its orbit, the equinoxes no doubt precessed, and "mob" became one of our better monosyllables. The whole English language, if it comes to that, is an undignified sloughing off of fine old Germanic terminations, made possible by the adoption of a monotonous, standard word order in place of the ancient freedoms. And even before that, if good little Indo-Europeans had listened more carefully to the (starred) forms used by their mothers there would have been no vulgar sound-shift, and we should all be talking a pure and original tongue. If good little apes...but by now we have had all the comfort we can take at one time.

~~SECRET SPOKE~~

P.L. 86-36

[redacted] T123

CHAPENKO, SHAPENKO -- What Difference Does It Make? (U)



~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36

[redacted]

News of the Communications Analysis Association (U)

CAA BOARD FOR 1979 (U)

(U)	President	Frank Porrino	3671s
	President-Elect	[redacted]	3369s
	Treasurer		4983s
	Secretary		5585s
	At-large		4935s
	At-large		5493s
	At-large	Dan Buckley	5906s
	Programs	[redacted]	4452s
	Crypto-TA SIG		4466s
	Cryptologic History SIG		2171s

Board meetings are held the last Wednesday of the month at 1000 hours, in the A1 Conference Room, 2N109.

Have you joined the CAA? If you would like to do so, send one dollar and an application form (you can get one from any board member) to the Treasurer.

LINGUITRIVIA (U)

(U) In a recent issue of *Russkaya Rech'* [Russian Speech], the author of an article on the orthographies of the various languages of the Soviet Union states that 60 of the 66 written languages of the USSR have writing systems based on the Russian alphabet. He does not identify the remaining six. P.L. 86-36

(U) Five of them come to mind immediately: Armenian, Georgian, and the languages of the three Baltic republics—Estonian, Lithuanian and Latvian. But what is that sixth one? P.L. 86-36

(U) Does any reader know the answer? If you do, please let CRYPTOLOG know.

EO 1.4.(c)
P.L. 86-36

CLUB AND LEARNED SOCIETY OFFICERS!

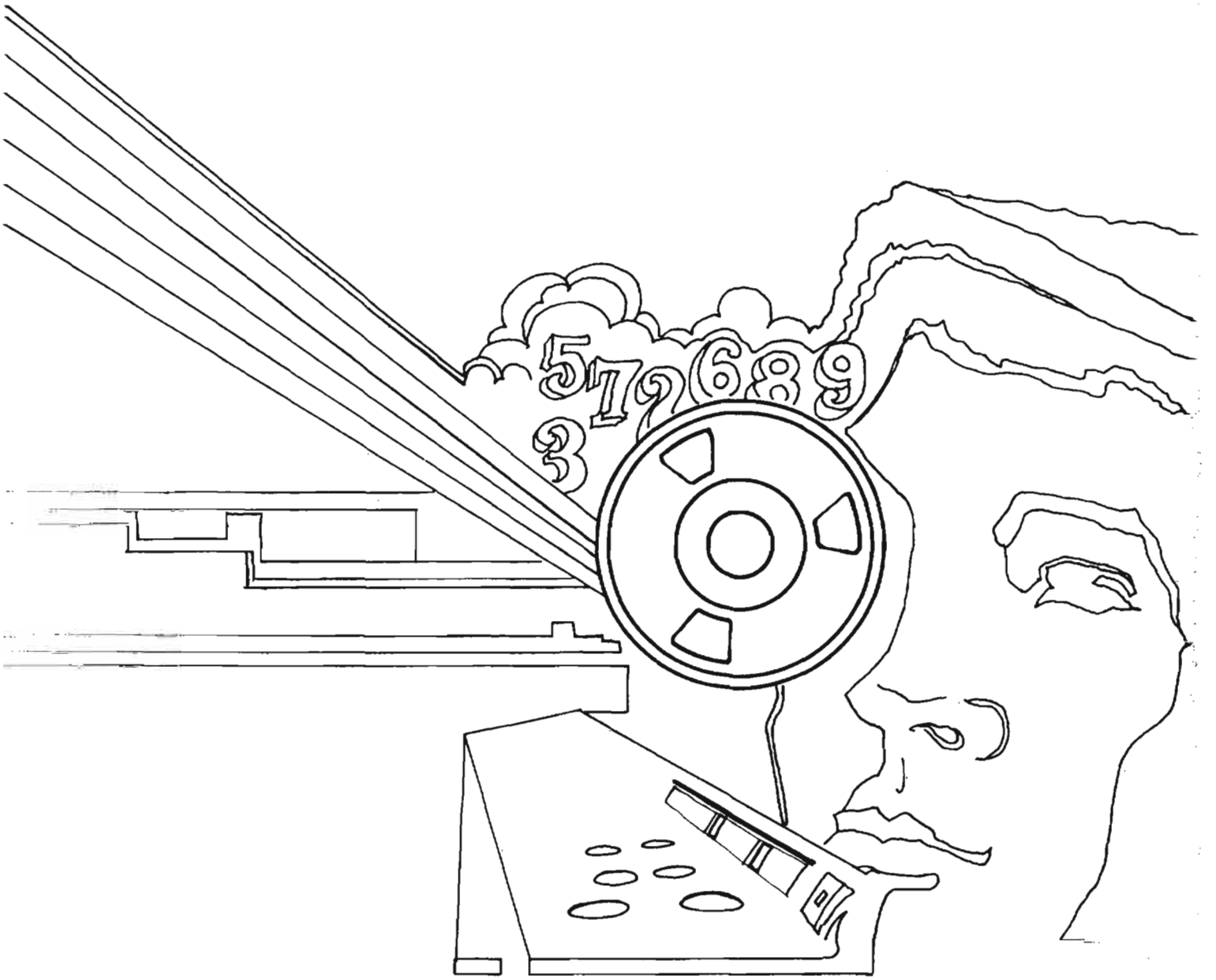
The pages of CRYPTOLOG are open to you for announcements concerning the activities of your organizations—

- meetings
- banquets
- lectures
- election results
- etc.

CRYPTOLOG comes out on the first of every month. Submissions should be turned in six weeks prior to the publication date. For further information, call 3957s.

OLD SUBSCRIBERS, NEW SUBSCRIBERS

To change your address on an existing subscription, or to begin a new one, call 3957s, or drop a note to P1, CRYPTOLOG.


5 7 2 6 8 9
3

DOCID: 4036132

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

APRIL 1979

P.L. 86-36

COMSEC/SIGINT RELATIONS (U).....David G. Boak.....1
A SOMEWHAT LARGER PROBLEM (U).....[redacted].....7
CLASSIC CABLES (U).....8
FEAR OF TESTING...AND WHAT TO DO ABOUT IT (U)..[redacted].....9
MORE FAIRBANKS ON ENGLISH (U) .....Sydney Fairbanks.....13
NSA-CROSTIC NO. 24 (U).....D. H. W.....14
LETTERS TO THE EDITOR (U).....16
BOOKBREAKER'S FORUM (U) 17
BUT, MR. BOAK, DID YOU EVER TRY
TO GET RID OF ONE IN A HURRY! (U).....D. H. W.....19

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 1 April 2009~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

~~SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. VI, No. 4 APRIL 1979

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor-in-Chief.....David H. Williams (3957s)

Collection..... [redacted] (8555s)

Cryptanalysis..... [redacted] (4902s)

Cryptolinguistics..... [redacted] (5981s)

Information Science..... [redacted] (5711s)

Language..... [redacted] (8161s)

Machine Support..... [redacted] (5084s)

Mathematics..... [redacted] (8518s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Taurone (3573s)

Production Manager.....Harry Goff (5236s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~SECRET~~

DOCID: 4036132

COMSEC/SIGINT Relations (U)

David G. Boak, S

Last November, David Boak, Special Assistant to the Deputy Director for Communications Security, NSA, presented an address on the status of COMSEC today to the members of the Communications Analysis Association. CRYPTOLOG *is pleased to be able to pass Mr. Boak's observations on to a wider audience.*

"...the good old KL-7, the only cipher machine we have left that looks like a cipher machine--the only one that's sexy at all."

(U) The easiest way to describe COMSEC is to say that it counters SIGINT. Our job in S is to frustrate the SIGINT professionals in hostile governments. Another way of looking at COMSEC, perhaps a more positive one, is to answer the question, "What's it for?" In a nutshell, I think that what COMSEC is for is to help the government achieve surprise. Now, I don't just mean the classical military tactical and strategic surprise, although, of course, that's crucial—but technological and diplomatic surprise as well.

~~(C)~~ I believe that the SIGINT element of the national intelligence community remains the pre-eminent one. And the reason I do is that SIGINT provides to our decision makers the most timely, most authoritative, most accurate (and often unique) information those decision makers get about what the other guy is going to do before he does it.

There are a few examples where we can demonstrate that a modest handful of COMSEC devices saved tens of millions of dollars in support of big operations, and some dismal instances in which we can show that the lack of COMSEC cost many lives. I suggest, therefore, that it is an excellent investment.

(U) Now, let's see what we're up against in trying to do that job.

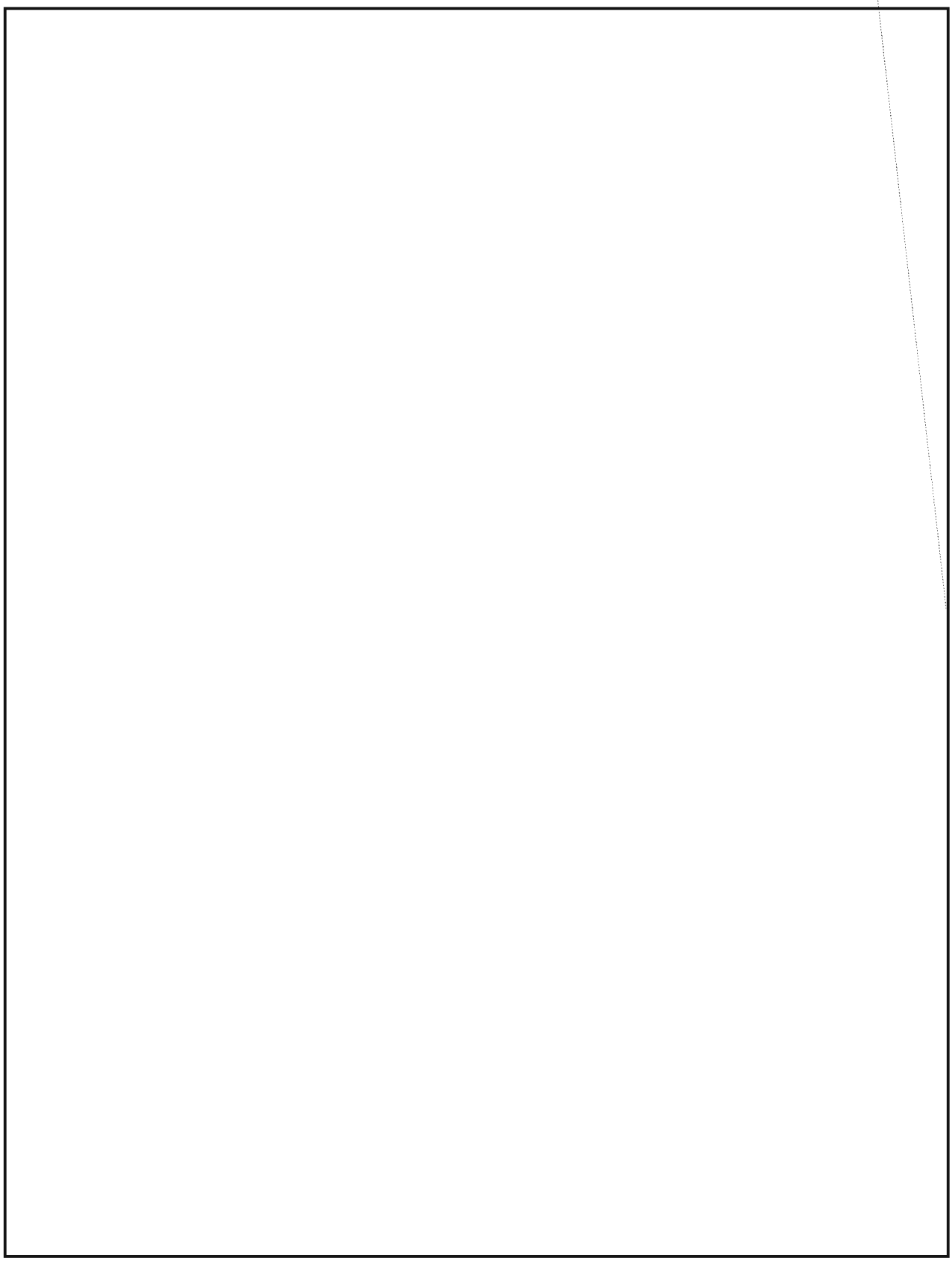
~~(C)~~ *The Threat*. Until the early 1970s this Agency had no coherent, comprehensive picture of what COMSEC was up against. We had fragmentary information. We got some of it from the SIGINT world and some from other sources. But, by and large, it was catch-as-catch-can. We assumed the worst about that threat and did the best we could to cope with it in an unstructured way.

~~(C)~~ But we began to realize that our COMSEC assets were finite and that we had to allocate the resources, people, and machinery, as well as new developments, to optimize our position against the threat. And the better we could define it, the better we could get the right systems to the places where we were hurting the most. Therefore, we built an entire division with a specific mission of determining what we're up against, helping us assess what that meant to us, helping with our plans and our prioritizations. We could then begin to allocate such assets as we had on an educated basis.

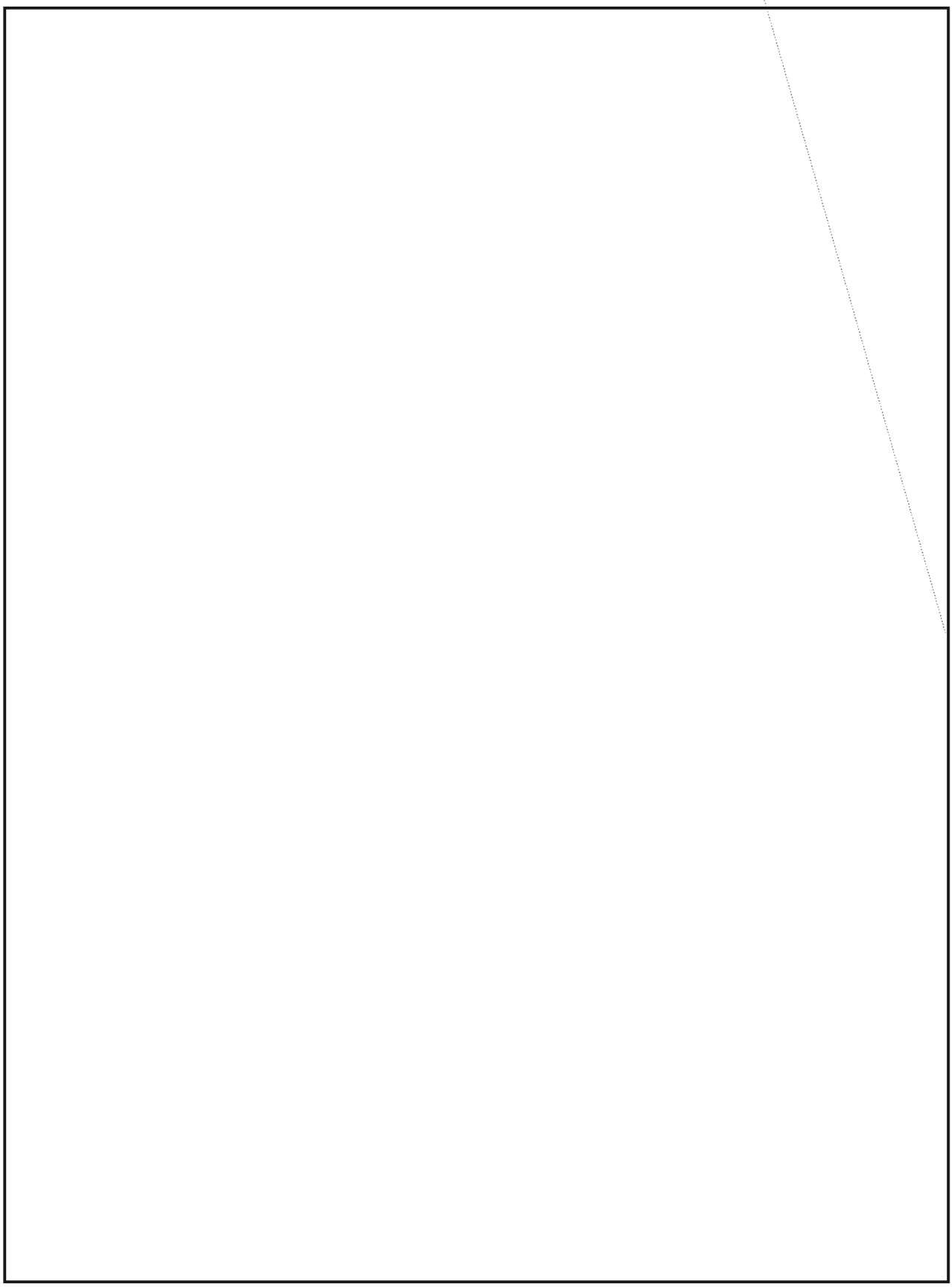
EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

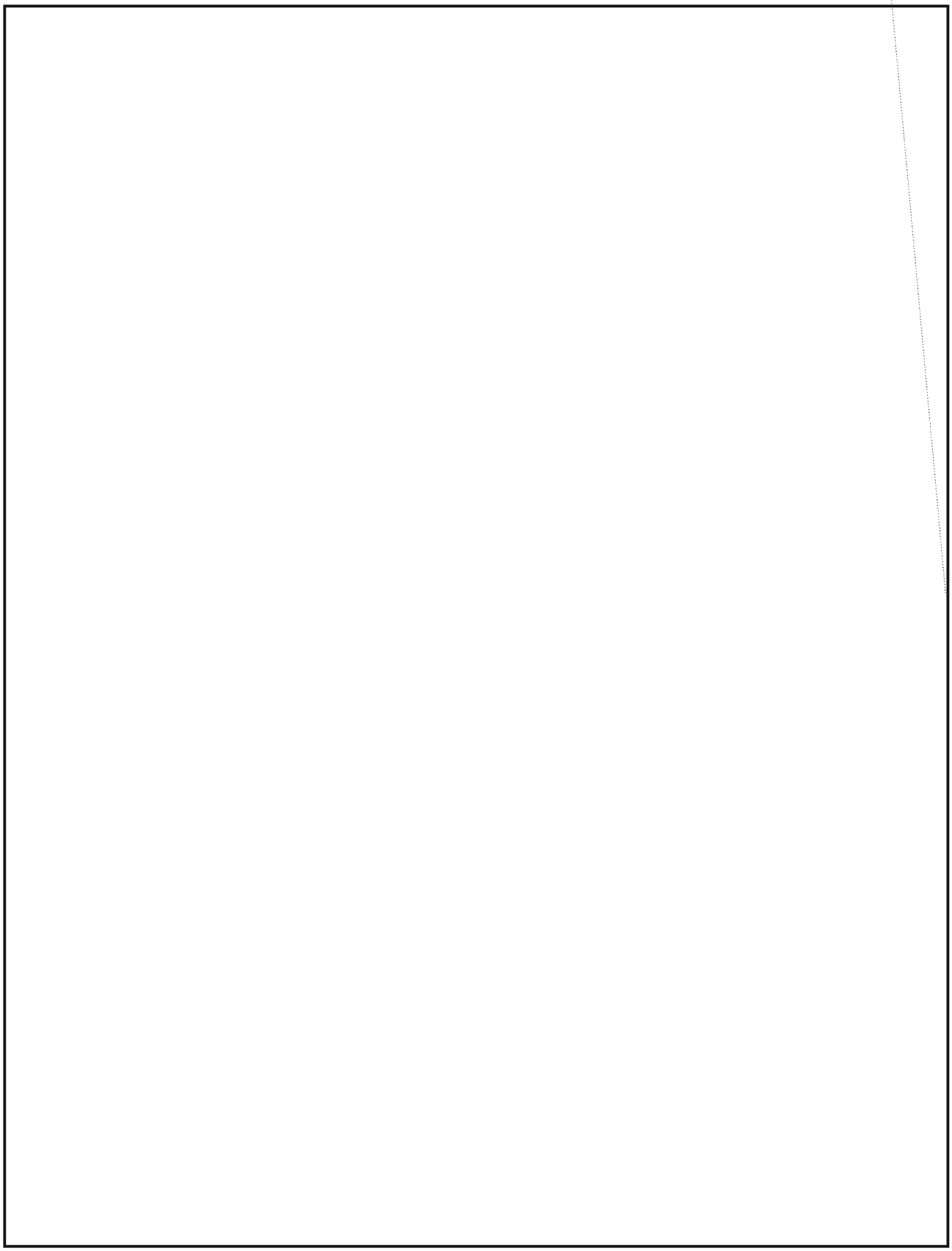
~~SECRET~~

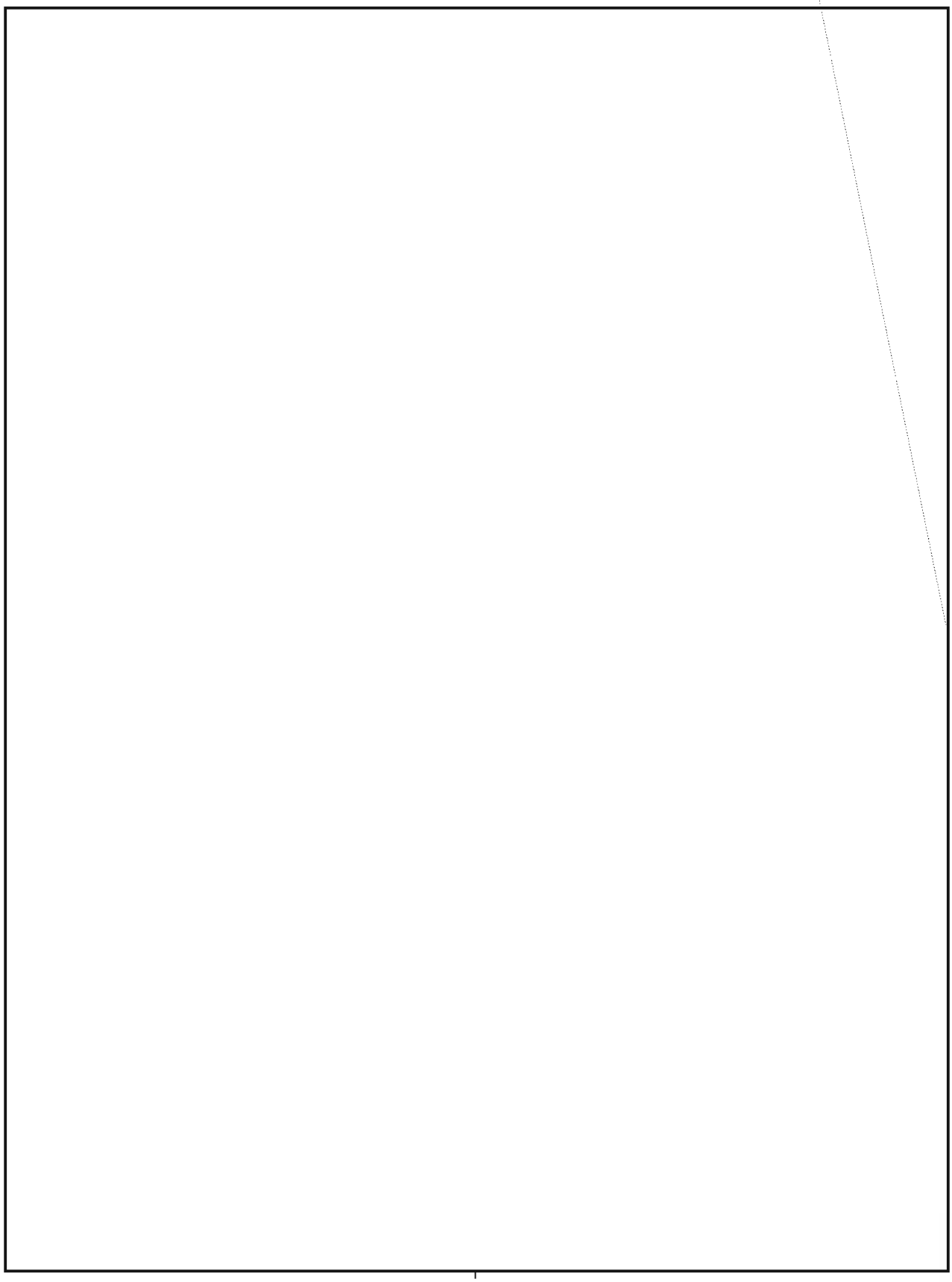


EO 1.4.(c)
P.L. 86-36



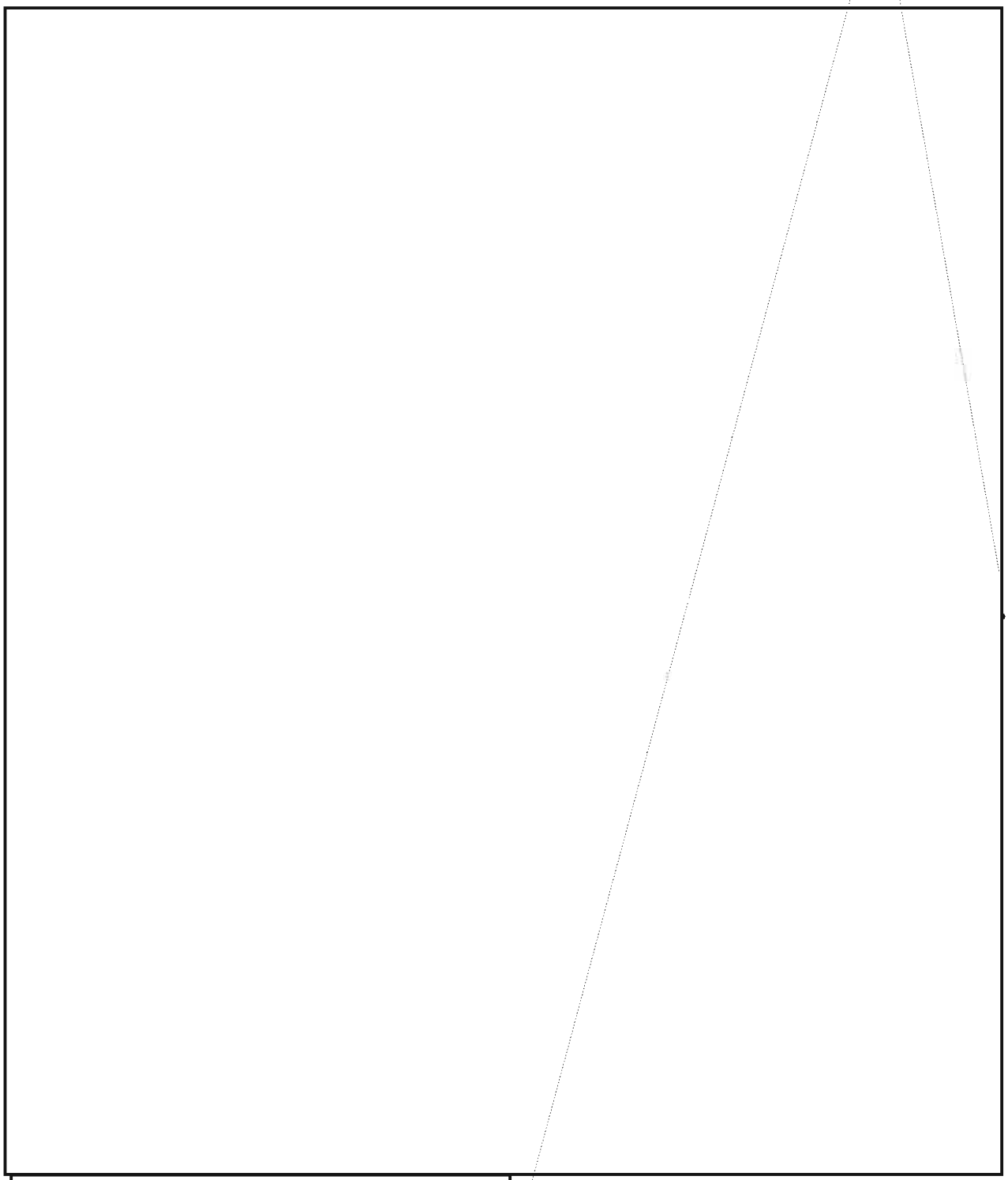
EO 1.4.(c)
P.L. 86-36





EO 1.4.(c)
P.L. 86-36

~~SECRET~~



(Continued on page 18)

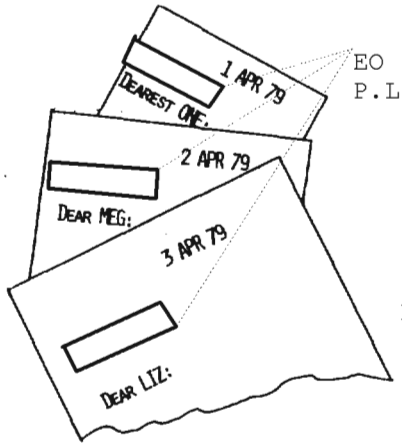
DOCID: 4036132

P.L. 86-36

A Logical Sequel to "A Small Problem"
(CRYPTOLOG, *November 1978*)

A Somewhat Larger Problem (U)

By [redacted] P14
For the Crypto-Traffic Analytic
Special Interest Group



EO 1.4.(c)
P.L. 86-36

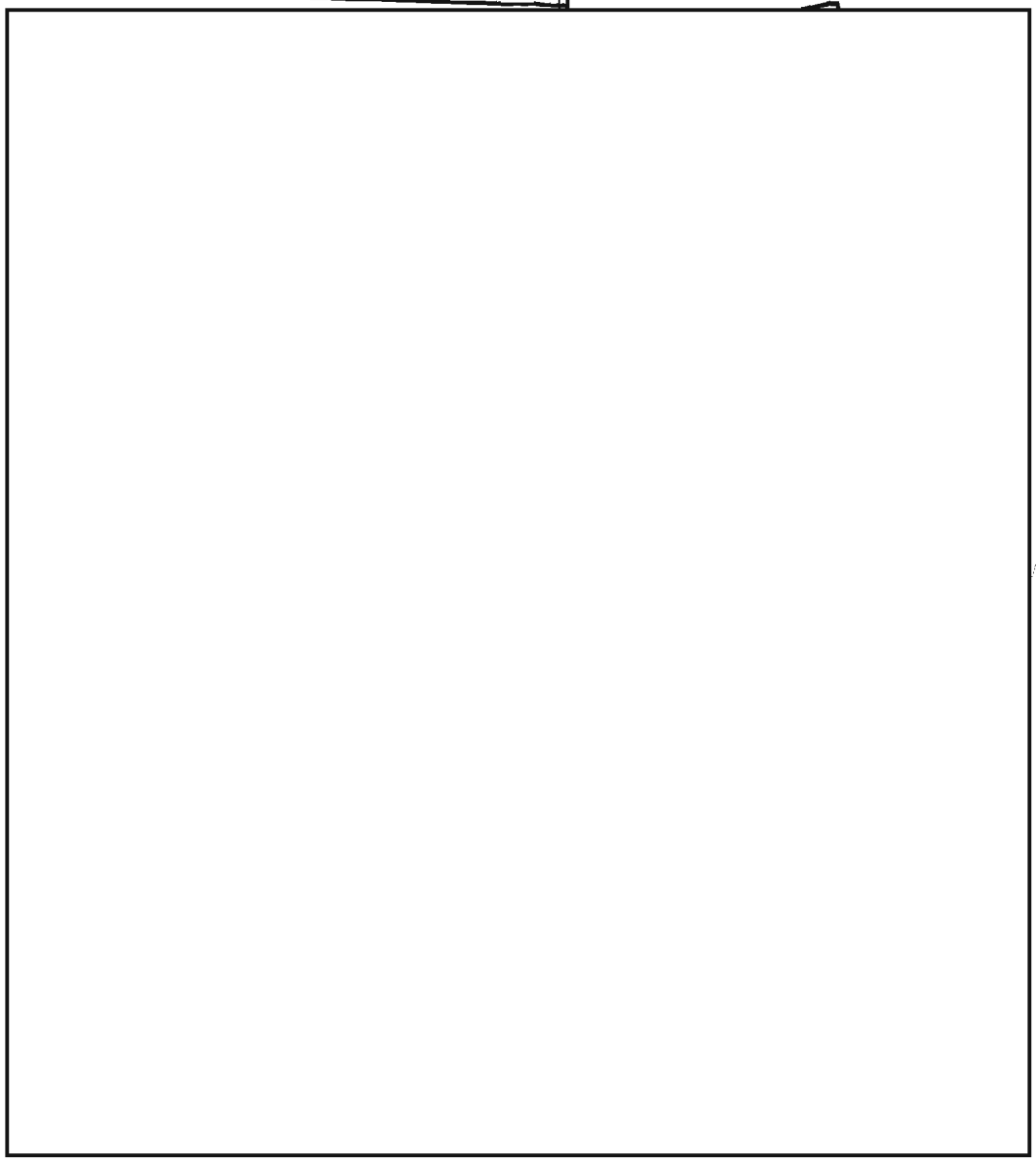
EO 1.4.(c)
P.L. 86-36

[redacted]

DOCID: 4036132

CLASSIC CABLES (U)

Not as well-known, perhaps, as Murphy's Law, but no less valid, is Hill's Axiom of Cable Analysis: *The exasperation of the cable drafter is directly proportional to the number of reference messages cited.*



EO 1.4.(c)
P.L. 86-36

DOCID: 4036132

FEAR OF TESTING

...and What To Do About It

"Examinations are formidable even to the best prepared, for the greatest fool may ask more than the wisest man can answer." P.L. 86-36
Charles Caleb Colton, 1780-1832

"Tell us your phobias, and we'll tell you what you are afraid of."
Robert Benchley, 1889-1945

Employee testing programs of one form or another have always been a way of life, but in the Age of Professionalization, oral and written professional certification examinations have become key factors in career advancement. At NSA you can't become certified unless you can pass written, and perhaps oral, examinations. Unless you're certified your chances of promotion to the higher grades are drastically reduced. For better or worse, tests are used by management to promote people to positions of greater responsibility (and pay).

Examinations that are fair, relevant, and professionally prepared and administered can be useful tools to help managers determine whether candidates for professionalization have the basic elements of knowledge required for certification by NSA.

But what about those people who are unable to take examinations or give oral presentations because of legitimate irrational fears (phobias)? Fear of test-taking and speechmaking are common phobias, and isn't it likely that the NSA population has some otherwise functionally superior people who are thrown into a deep panic and become truly dysfunctional even at the *thought* of having to give a briefing or take an examination, particularly when the results will significantly influence their career progress?

Most of us know people who have similar fears (heights, flying in airplanes, for instance), but they usually avoid the problem by getting jobs where they aren't required to confront their fear. NSA people who fear tests have no such escape. Their job advancement requires that they make a choice of submitting to tests or remain at a sub-professional level. Because of irrational, pervasive fear (and not because of a lack of subject knowledge or career potential), a number of our coworkers will consistently fail oral and written examinations. Even worse, some people will flatly avoid situations which call for oral or written exams. As a result, these people reconcile themselves to remaining at below-professional grade levels rather than to be subjected to the unbearable (to them) stress of test-taking. They hurt themselves, but they also deprive the government of the benefits of their full potential.

By now some readers may have become impatient with my deferential attitude toward the phobic professional aspirant. After all, didn't most of us have to go through the testing process? Aren't nervousness and apprehension normal side effects of taking the Professional Qualification Examination (PQE)? Am I not just leading up to a plea for special privilege, test waivers, or some such other gimmick which favors people who may be just too lazy or timid to meet the general standards that all professionals have met?

Definitely not! I am attempting to highlight the existence of a real problem at NSA, and to offer some ways for our phobic coworkers, with our help and encouragement, to overcome their fears permanently. No waivers, no special treatment, just an awareness on our part (those of us who can take tests without too much anxiety) that some people do have overwhelming difficulty when confronted by career-related tests; and an understanding by the phobics among us (and they usually know who they are, even if we don't) that they can be permanently relieved of their fears by a variety of proven methods.

To understand the problem let's look at the phobic person. He is usually an otherwise "normal" person who has such an irrational fear of a thing or a situation that he will go to almost any extreme to avoid it. He cannot be cured by pleas, arguments, de-

crees or threats. If a test phobic is forced to submit to an examination his performance will probably be uncharacteristically poor and not a true measure of his knowledge. He may manifest one or more symptoms of panic, such as sweating, upset stomach, breathing difficulties, disorientation, confusion, flight, or avoidance (by just not showing up). It's likely that the phobic person will keep quiet about the problem to disguise the true extent of his difficulty.

What can be done? Quite a bit, since in the vast majority of cases the fear reaction is simply learned behavior.* According to behavior therapists the phobic person has the irrational fear because it was "learned" at some time in the past. By directly treating the phobia symptoms they can be made to go away when they are "unlearned."

Behavior modification therapy for phobias does not require that the subject acquire an insight into how or when the phobia began. Treatment generally does not involve in-depth analysis of inner forces, deeper psychological problems, and the like. Therapy usually consists of simple techniques which are designed to unlearn the anxious behavior associated with the phobia, and can involve procedures called *modeling* and *desensitization*. *Modeling* assumes that the phobia may have been learned from observing others who exhibited anxieties in stress situations (perhaps how my friend in the footnote helped to learn his fear of flying). The unlearning process involves observing others while they display fearlessness in the threatening situation. *Desensitization* is a procedure which uses relaxation, thought-stopping and other methods to systematically reduce sensitivity to the anxiety-causing situation. During desensitization sessions the subject visualizes various situations in his or her "anxiety hierarchy," which are typically imagined situations that have progressively disturbing reactions.**

* A friend of mine has refused to fly ever since an encounter with violent air turbulence. He relates that while dodging flying dishes he looked to the flight attendant for some sign of strength and calm. He vividly recalls that she appeared more terrified than most others on the flight. The lesson of the day was fear, and my friend learned his lesson well. He has not flown since, but perhaps after reading this article he will have a go at some form of phobia-fix and become a flying fool.

**Typical situations you might visualize if you had test-taking fears might be: "You hear about someone who has a test" (low anxiety); "You are in an important exam. The instructor announces that 15 minutes remain, but you have an hour's work left" (high anxiety).

Using special techniques the subject gradually unlearns the phobia symptoms and is then free to function normally, usually within a surprisingly short time. Thankfully, phobia patients are not generally subjected to cold-turkey "cures" like: "OK, everybody onto the airplane," or "give us a 15-minute speech."

Behavior therapy for phobias really works. Even people who feel that *they* will *never* be cured, find that they can usually unlearn the problem symptoms and can then face the phobia situation with confidence. Since the behavior therapy approach to phobias makes no judgments about the mental health of the subject, but treats the phobia as essentially a bad habit, phobic subjects who might otherwise have an aversion to psychological and psychiatric therapy need have no qualms about undergoing simple behavior habit modification treatment.

There are several methods available to people who want to get a phobia problem resolved, particularly one which is associated with NSA work situations like the PQE. These include consulation with M72 clinical psychologists, outside private therapists (no NSA knowledge or involvement), or do-it-yourself techniques. I'll examine each of these methods and give some idea of how to go about getting assistance for yourself or advising someone you know on how to get help.

One way in which an NSA person can seek professional assistance for a phobia is through M72 Psychological Services. I spoke with Dr. [redacted] Chief of M72, and his staff about phobia treatment for NSA employees. They confirmed that they have encountered a broad range of phobias among NSA people, and occasionally, NSA family members (for example, a family member has a fear of flying which prevents the employee from accepting an overseas assignment involving air travel). P.L. 86-36

Although the M72 psychologists are prohibited by statute from conducting long-term therapy, they do hold a limited number of sessions with the patient to determine that the problem is a true simple phobia. After diagnosing a phobia (rather than a more complex problem of which the phobic symptoms are only a smaller part), they will provide the employee with a list of four or five private practitioners who are known to be legitimate, effective phobia therapists. The employee selects his or her own professional and makes private arrangements for treatment. Cost is borne by the patient, generally with the financial assistance of major medical insurance carriers. The Columbia Medical Plan reportedly also has a program for treating phobias and the M72 counselors can provide more specifics, or CMP members can make arrangements on their own.

Once the patient makes contact with a therapist the treatment could involve indi-

vidual or group sessions. For the more specific and common phobias treatment is often short-term, and frequently successful.

The M72 staff stressed that they maintain anonymity and confidentiality for self-referred phobia subjects, and there need be no official NSA awareness of the transaction. They pointed out that the Baltimore-Washington area has an impressive array of top-rated phobia therapists and that help is often readily available and effective. For an appointment with an M72 counselor call 5429s or 6531b.

Another method of obtaining help is by direct contact with a therapist, perhaps on the basis or recommendations from friends or a family physician. Costs vary and are the direct result of patient-therapist discussion. Medical insurance coverage should be checked before beginning therapy to make sure of what the insurance carrier will provide.

Those who prefer to arrange their own therapy might be interested in the Johns Hopkins Behavioral Medicine Clinic in Baltimore, which is a private clinic dealing in the treatment of phobias. I spoke with the Clinical Director, Dr. Bruce Masek, who gave me some useful information on what would be involved in obtaining treatment. The clinic treats all major phobias, using behavior modification. Patients are also given individually prepared cassette tapes to take home and supplement the formal desensitization sessions. Visits cost $50 per hour, some of which may be covered by major medical insurance (check first).

Dr. Masek suggests that interested patients first call the clinic (955-6111) to discuss with a staff member the nature of the phobia and to arrange for a visit to the clinic.

Do-It-Yourself Phobia Fix-up. If you have a common phobia which is either directly or indirectly influencing your career you can take personal control of the situation and probably cure the phobia yourself. This can be done with the help of inexpensive books and cassette tapes which are broadly available. These materials are usually written in simple, non-technical style and generally use behavior modification techniques to enable the serious reader to systematically break the phobia habit. These books and tapes can be very effective aids to people who are serious about breaking the hold of a phobia on their lives. A short listing of some typical books and cassettes is included at the end of this article. If self-treatment is for you, then you should check out these inexpensive materials.

Test-Taking Strategy. Since tests have become so important to NSA career advancement, what can be done for the person who doesn't necessarily have a phobia, but who hasn't learned how to organize and make the best use of time, strategy, briefing aids and techniques, and the like, when taking written or oral examinations? He or she knows the test material, has no overwhelming anxiety, but bogs down in the mechanics of the test-taking procedures and does not play the odds properly, or does not handle the mechanics and style of an oral examination in a convincing way.

The goal of testing is to assess the knowledge or skill of the testee without imposing arbitrary test-related barriers. In the case of professionalization tests which have a direct influence on the careers of our employees, the Agency has a responsibility to make the test procedures as neutral and transparent as is possible. People aren't supposed to be tested on their ability to survive tests, but on their knowledge of the material.

In 1974 the Women in NSA (WIN) organization conducted a lecture on How to Take Exams, but it was oriented more toward the general CQB and proficiency tests. Something similar but on a more intensive scale needs to be offered periodically for prospective professionalization aspirants. Both written and oral examinations should be covered in the sessions, which could be available to all who may want or need assistance.

Prospects for Change. As certified professionals, managers, and coworkers we should satisfy ourselves that no arbitrary (even if unintentional) test-related career roadblocks are place in the way of *any* aspirants to professional certification.

If our subordinates are failing or avoiding tests or special work situations because of irrational fear, it is our responsibility to work with them to see that they resolve the problem. The professionalization panels should make it their business to know their aspirants well enough to detect likely test-avoiders, and get to them with the facts about how to seek help.

It will be very difficult for us to determine exactly how many people are dodging or consistently failing professionalization tests because of irrational fear. Test fearers are less then enthusiastic about publicly declaring their fears,* and would also seem to be

* One NSA person I talked with (a proven excellent worker, but a test fearer) went *years* before being able to successfully survive the PQE in his field. During these years he downplayed his fear of tests because he felt that management would interpret his phobia as a general inability to function under *any* stressful situation.

generally disinclined to present themselves to the NSA Medical Center for psychological counseling. The situation is further complicated by the federal prohibition that government agencies may not engage in extended civilian medical or psychological therapy, since this is legally and logically the province of the private sector. Our military SCA associates have have an even stronger reason to avoid treatment for phobias. Many believe that if they were to seek assistance for a phobia their authorization for access to classified material would be pulled immediately, on the grounds that any contact with mental health professionals connotes a potential security risk.

If we are really to come to grips with the issue, active measures can be taken on behalf of our people, many of whom cannot afford private therapy. One possible solution could involve contracting for private practitioners to come to NSA and present periodic "How to Take Tests and Be Comfortable While Doing It" sessions. Technically, behavior modification is training (or more accurately, *re*training) and makes no judgments about the psychological health of the subject. It could follow that NSA-sponsored special retraining sessions would be legal and ethical endeavors.

Another possibility would be for the NSA Learned Associations (The Collection Association, The Communications Analysis Association, etc.) to sponsor and fund "How to Take Tests" seminars conducted by qualified outside consultants. These sessions could cover the mechanics of oral and written test-taking and testing strategy, and could also offer, for those who are interested, some basic information about how to deal with the various forms of test anxiety. At the least, a session entitled "How to Do Your Best in Professionalization Tests" has a better chance of getting to the people who need it than for us to expect all of them to come forward and admit a "phobia." Self-help books and tapes should be made broadly available by the Professionalization Panels and Learning Centers. Remember, most of the true phobics have long ago decided to accept their present position and grade rather than face the anxiety of even *visualizing* themselves in the feared examination situation. It's up to us as friends (and managers) to give them the support and help they need to solve their own problems. Strictly speaking, any employment procedures or testing mechanisms that operate as "built-in headwinds" to any class or group of people (in this case, phobics) could be unlawful, even if there was good intent or absence of discriminatory intent on the part of the government. When you think about it, if just one gifted person can be helped to overcome his or her fears to the extent that our tests will measure only ability and knowledge, we will have done a good thing.

In his address to the Communications Analysis Association on 10 May 1978, the Director, VADM B.R. Inman, very candidly spoke of his concern that the Professionalization process might be in need of a more sympathetic and less bureaucratic view by the Agency.

> I am struck that there is often a very *bureaucratic* approach to professionalization, and, demonstrating my relative ignorance, I have a sense that maybe the Agency as an organization doesn't do all it could to facilitate that professionalization process, to make it easier to help put the things together that can help you get through those hurdles. I believe there are clearly improvements that can be made."

The Director's comments, while not specificially addressed to professionalization testing, nonetheless give us the support and emphasis we need to size, attack, and solve the problem of test fear at NSA.

Let's get started.

SELF-HELP MATERIALS

The following are typical of the broad range of self-improvement books and tapes available to help people with irrational fears. I make no claims as to their effectiveness, but they are representative of what's available.

Nothing to Fear, Fraser Kent (Dell, $1.95). Explores various approaches which can be applied to self-cure of phobias. Uses simple layman's language.

Fear: Learning to Cope, Albert G Forgione and Richard S. Surivit, with Daniel G. Page (Van Nostrand Reinhold, $9.95). A specific guide for dealing with phobia, using all the modern therapeutic techniques. Considered an easy-to-follow guide. These authors have developed a successful program for flight phobia.

Stop Running Scared! Herbert Fensterheim and Jean Baer (Dell, $2.25). Oriented toward the do-it-yourselfer, with step-by-step plans to overcome most fears. Includes a proven learning plan to help conquer fear of flying. Contains instructions for preparing a personalized relaxation tape.

Kicking the Fear Habit, Manuel J. Smith (Bantam, $1.95). Written for the do-it-yourselfer. The author claims that using his method of therapy can often lead to rapid conquering of chronic fears.

Phobia Free: How to Fight Your Feare, E. Ann Sutherland and Zalman Amit, with Andrew Weiner (Jove/HBJ, $1.95).

Phobia Free and Flying High, Neal H. Olshan with Julie Dreyer Wang (Condor, $2.25). Offers step-by-step procedures to help the reader identify and eliminate phobias.

Casettes are available from Psychology Today Cassettes, P.O.Box 278, Pratt Station, Brooklyn, N.Y. 11205. A free catalog is available and subjects include "Deep Relaxation" (#20040) and "Getting Rid of Your Fears" (#20155), at $8.95 each. The latter tape is by Manuel Smith, author of *Kicking the Fear Habit* (above), and reportedly explains how to cure phobias such as fear of flying, heights, taking tests, etc.

more Fairbanks on English

Last Month CRYPTOLOG *reprinted a 1958 editorial written by Dr. Sydney Fairbanks when he was at the helm of the* NSA Technical Journal, *on the subject of NSA English. The response to this was sufficiently encouraging as to warrant trying it again. Here, from the issues of January and April 1958, are two more of Dr. Fairbanks' comments on this subject.*

We promised last time to write a series of notes on the grosser abuses of the language to which the job exposes us. Our text for today will be the curious locution "this type thing." No one says, we believe, "variety thing," or "sort thing," and there is a natural bar against saying "kind thing" (consider, for instance, "I hate your kind letter."), so that this cannot be a mere extension of a Milt Gross idiom ("With your pie you want it a piece cheese?") nor an offshoot of the sort of telegraphese that omits all connectives ("Reference your message"). We think the main culprit is the technical writer.

An English epigram which is still going the rounds—last seen in *Missiles and Rockets* —defines an engineer as a man who says "a coffee-containing cup" when he means "a cup containing coffee." If, one may add, he wishes to talk about a description of the methods used in teaching the design of gadgets to be used on widgets, he will write "a widget-type gadget design instruction methods description." We have had the equivalent of this submitted to us for publication. As for writing "widget-type gadget" rather than "widget type of gadget," he does it every time. It is, after all, not incorrect though a trifle monotonous. And since he has little use for hyphens, he writes "widget type gadget." From this some illiterate soon concludes that "type" *means* "type of," and the step to "this type thing" is immediate. Since it is well known that no error is stupid or vulgar enough to guarantee that it will not become respectable, we refrain from rending our garments. But we submit that at this period English this type writing is not appropriate to this sort Journal.

And so to bed.

* *

No violent protests having been received, we continue our remarks on how not to write English. A sentence—suitably disguised, we trust—in a recent contribution, runs something like: "The machine has the power of selecting the ripe apples and throw away the others." Most readers will conclude that the typist forgot to type an "ing", and so what. But our calling has made us so suspicious that we are inclined to see in this a first seeping into written English of something that is rapidly becoming a standard colloquialism. Observe its history. The verb "to go" has two functions in English— one to express the future: "I am going to do what he asks"; and another to express motion: "Where are you going?" Another way of expressing the future is by using the continuous present: "I am driving out there tomorrow." Out of a horrid amalgam of these has grown up the very common, but indefensible, "I am going upstairs and take a nap," meaning "I am going to go upstairs and take a nap" or "I am going upstairs to take a nap" or even, "I am going upstairs (this afternoon) and taking a nap." But there is no use in trying to make a chart of chaos.

Even though "I am take a nap" and "I am going take a nap" are both very queer, it might be possible to put a fence around the monster and say, "This is something peculiar that happens with the verb 'to go'." But alas, the spirit of the language is never more logical than in extending its mistakes. If Momma is going upstairs and take a nap, what is more natural than that if Willie disturbs her she is coming downstairs and beat his ears in, or than she is running through her mail and throw the advertisements in the trash, or taking a bus downtown and buy a hat, or for that matter joining the Navy and see the world.

A reader told us recently that on encountering our remarks about "this type thing" he couldn't imagine what we were talking about; never in his life had he heard anybody say anything like that; but that in the next twenty-four hours he had heard it four times. In the same spirit we direct the attention of our word-watchers to this new idiom that is creeping into the language and poison our intellects. There is no sense in temporizing and let it get established. It...

Ugh!

DOCID: 4036132

P.L. 86-36

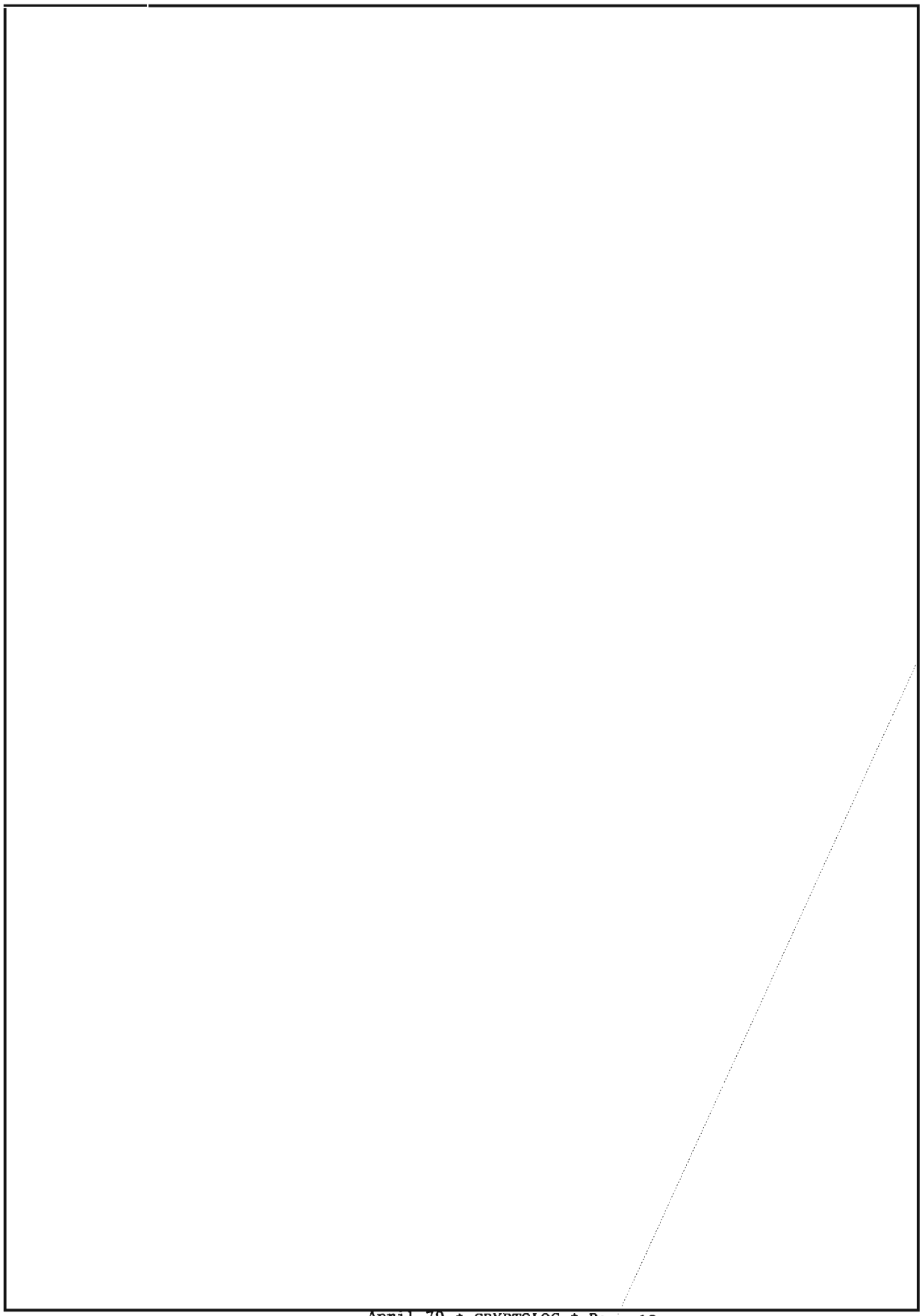
NSA-crostic No. 24 (U)

By D.H.W.

The quotation on the next page was taken from a published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS

WORDS



P.L. 86-36

LETTERS

To the Editor, CRYPTOLOG:

I would like both to support and state my appreciation of Mr. Gurin's article, "Let's Not Forget Our Cryptologic Mission," which appeared in the February issue of CRYPTOLOG. I would like to point out an oversight I believe Mr. Gurin made, but first I must state that I heartily agree with his remarks about the ratio of jobs totally involved with the Agency's basic mission to the ever-increasing number of jobs which have only an indirect impact on that mission. My particular COSC (1640 series, Collection), according to the most recent Quarterly Management Review, is said to be near its authorized strength. But we must really look behind those figures, and see how many people who carry a 1640 series COSC are actually involved in the collection effort. If we are near our authorized strength, why is it that so many collection jobs are unfilled at many of our overseas locations and in the ROFs (Remote Operating Facilities) here at home? The job description and grade span stated in the PMM shows that a collector can go as high as a grade 12, but in reality, I would be hard pressed to find any grade 12s actually doing the collection effort. This point is stressed because it underlines Mr. Gurin's feeling that we are getting away from our prime mission in many areas.

The oversight I would like to mention concerns Mr. Gurin's numbering scheme as it relates to the basic mission of the Agency. If Mr. Gurin's system is applied and the TA people, the cryptanalysts, appropriate program managers, and so forth, are given the rating of 1, where does that put the collection personnel? Have we forgotten that the person who gets the ball rolling, provides the raw material for the finished product, the person who takes the first step in the long, long journey, is the person who performs the most basic, and in some people's opinion, the most important part—the collector?

[redacted]

Jack Gurin responds: [redacted] has caught me dead to rights. What could be closer to the basic mission than collection? In my own defense, though, I should say that I was not trying to provide an exhaustive list, just a sample to illustrate the point. Perhaps what I should have done would have been to visualize how one would start all over again to build a cryptologic agency, and list what kinds of people would have to be hired. I sure wouldn't have missed the collector.

To the Editor, CRYPTOLOG:

I'm sorry that the "Ask Art" column you had in December's issue was a one-time thing, because I have a problem and I need HELP.

I'm trying to fill out all of those forms you get when you're updating your personal history statement for security reinvestigation. One form in the packet calls for full maiden names for my mother and my spouse. Mother is no problem, but, as far as my spouse is concerned, even after umpty-zip years of marriage, he still refuses to tell me his full maiden name.

What shall I do?

Sue

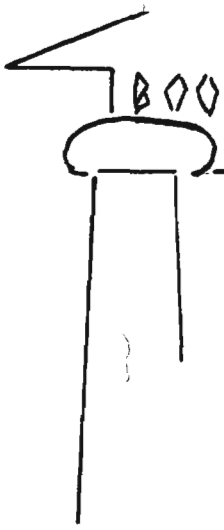
SOLUTION TO NSA-CROSTIC NO. 23
(*CRYPTOLOG*, March 1979, by A.J.S.)

[redacted] "[Tell Me I'm Just a] Sinobibliophobe!", *CRYPTOLOG*, July 1978

"If any significant number of those worker-peasant-soldier students self-studied their way through that [Chinese mathematics] textbook, the present technological advantage of the United States (and of the USSR) might not remain so overwhelming all through the foreseeable future."

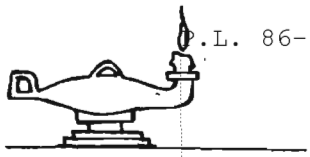
NEW EMPLOYEE?
JUST BEEN TRANSFERRED??
JUST BEEN REORGANIZED???

To start a new subscription to CRYPTOLOG, or to change your address on an old one, call the CRYPTOLOG office. The phone is 3957s.



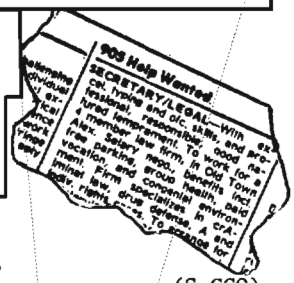
BOOKBREAKING BRIEFS (U)

~~(C-CCO)~~ NCS FELLOWSHIP. The National Cryptologic School is announcing a Cryptologic Education Fellowship to update the course in code reconstruction and to teach it the first time. The present course is based on codes and techniques—and administrative philosophy—that were current in the early 1950s, but updated from time to time since then. Now an overhaul is needed to integrate these piecemeal updates; developments in computer technology and changes in target codes compel it. The new course, like the present one, will allow for guest lecturers to address the class on specialized topics. The selectee will work with member(s) of the Analysis, Design, and Development Department to insure that the course incorporates, where feasible, the latest techniques in instructional technology. The Cryptanalysis Division offers assistance on content. The facilities of the Bookbreakers' Forum will be available to the selectee. Applicants should be experienced bookbreakers conversant with modern bookbreaking techniques and knowledgeable in the theory and principles of code reconstruction. Applications should be submitted through channels to M02. For further information, call [redacted] Chief, E42, 8025s.



P.L. 86-36

[redacted]



Is there a better way? If you know of one, or have such a problem, come to a workshop meeting of the Forum on Tuesday, 24 April at 0930, in Room 2C078. If you'd like to talk about the problem in advance, call [redacted] on 5236s or 5642s. ~~(S-CCO)~~

CLARIFICATION (U)

Classified ~~SECRET-UMCCO~~ in entirety

The January 1979 issue of CRYPTOLOG carried an article in the Classification Corner concerning classifications of references to Second and Third Parties. One point made in the article apparently needs clarification, since we have received several inquiries concerning its intent and meaning.

The article stated that "references to 'Second Party' or 'Third Party' which are made in a COMSEC context, whether stated or implied," are unclassified. The intention was that the term *second party* (not the specific country) would be unclassified when so referenced.

Revealing a COMSEC association between NSA or the U. S. and a *specific* Second Party country or organization without amplification is classified as follows:

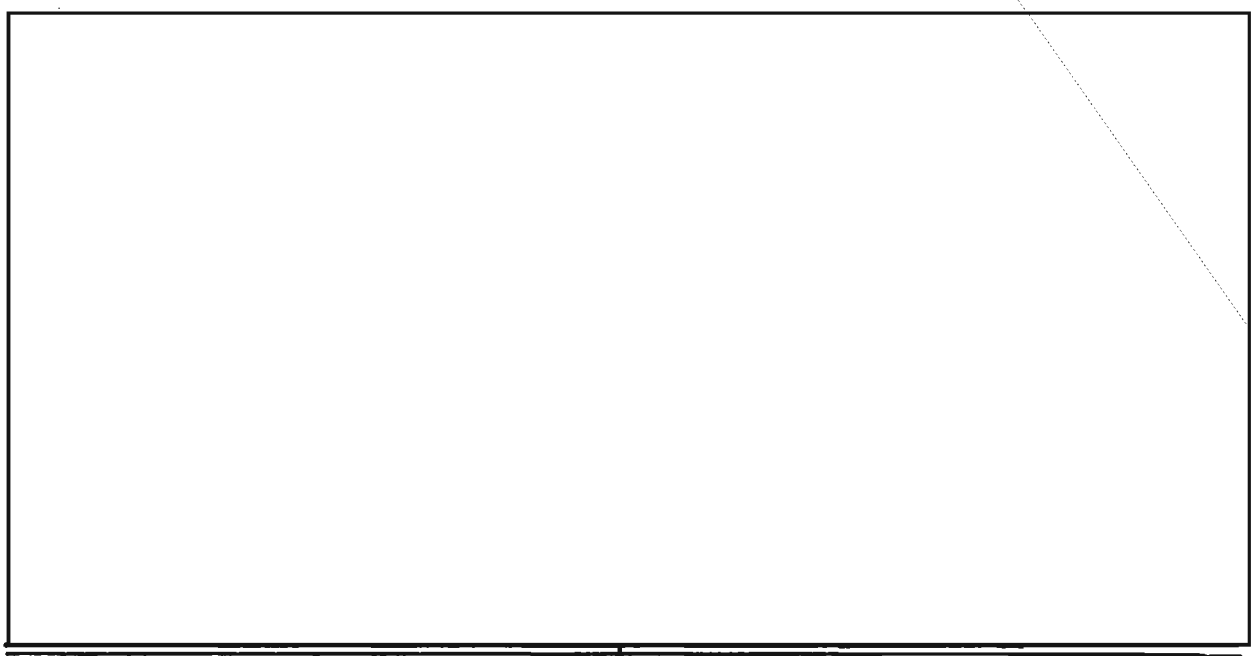
EO 1.4.(c)
P.L. 86-36

with GCHQ or the UK: Unclassified
with CSE or Canada: Unclassified

[redacted]

When classifying a Second Party relationship, be mindful of the fact that the minimum classification of [redacted]

P.L. 86-36



Following his talk, Mr. Boak answered questions from the floor. (This portion is classified ~~CONFIDENTIAL~~ in entirety.)

Q. What are your views on the extension of cryptography in the public sector and the initiatives of the Department of Commerce?

A. Frankly, I'm not overly concerned. I think some of us may have overreacted to the surge of activity out there and some of the publicity we got with respect to it. I think most of my SIGINT friends now believe that it is not going to be the end of the world. Clearly, though, as more and more sophisticated knowledge about cryptography is proliferated in public, it is going to make the SIGINT job harder, and take more people and other assets to sustain our present level of success. But the consensus I see is that the problem is not an insuperable one.

EO 1.4.(c)
P.L. 86-36

The ascendency of the Department of Commerce in this field resulted from a presidential directive which established *two* Executive Agents in the government for telecommunications protection: one which has to do with the protection of national security related information—this is NSA, acting for the Secretary of Defense, and one for the protection of information not related to national security—this is the Department of Commerce.

The action element in Commerce is a new organization, the National Telecommunications and Information Administration, with whom we are now in active negotiation on how to share this load. We have some concerns, of course. Are they, for example going to create an independent cryptanalytic organization? Are they going to do independent R & D in cryptography? And if so, under what kinds of security controls?

Overall, however, we are becoming acclimated to one another and the Director is ensuring that we remain highly cooperative and supportive of them.

Q. Do you anticipate that the S organization will establish a viable ELINT security (ELSEC) program?

A. We have wrestled with that matter for as long as I've been around. We have not solved it. For a while, we thought of calling ourselves "SIGSEC" instead of COMSEC, thus solving the issue with improved nomenclature.

But it is true that we have no coherent ELSEC effort because we have been unable to define it very well. Yet those definitions are important in establishing roles, missions and authorities.

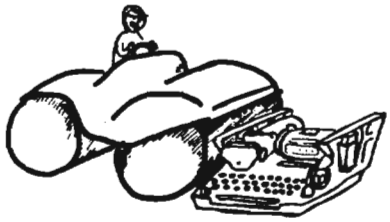
[redacted]

Q. Will NSA establish a national COMSEC assessment program for equipment other than that we build ourselves?

A. I hope not. It's a very difficult thing. If some of the equipment being produced commercially is going to be adopted by elements of the government, I believe we must have some role in its certification or validation. But I believe the way we go about that, if the equipment is not to be used for national security purposes, will have to be through the Department of Commerce, as their new mission gives them jurisdiction over such applications. We will offer them technical advice and assistance on how good such systems are.

[redacted]

BUT, MR. BOAK, DID YOU EVER TRY TO GET RID OF ONE IN A HURRY! (U)



By D.H.W.

(U) Dave Boak has stressed the cryptographic integrity of the cipher devices produced by S. But there is another, quite different, aspect of the superior quality of these machines which he didn't cover, which I'd like to touch upon. That is their structural integrity.

(U) Cipher devices, like most other DoD equipment designed for use in the field, are manufactured in accordance with something called military specifications—milspecs, for short. One of the features of manufacture which milspecs cover is ruggedness. For example, some items designed for the Army and the Air Force must be capable of operating in the severest of climatic conditions, from Saharan to Arctic, while many items intended for shipboard use by the Navy must be able to operate under temporary conditions of flooding.

(U) On the other hand, cipher equipment, *unlike* most other DoD hardware, is classified. This means that at field locations where there is a risk of loss for whatever reason, the station commander and the crypto custodian must be prepared to destroy the commcenter gear, often on short notice.

~~(C)~~ Now it's readily obvious that milspec-imposed ruggedness and ease of rapid destructability are somewhat at odds. Something has to give. And the clear winner, at least as far as two of the most popular devices in the S inventory are concerned—the KW-26 and the KG-13—is milspecs.

~~(C)~~ A few years ago I was involved in the [redacted] From one day to the next there was no particular hazard, so we stayed on, packing and shipping back much of the station equipment. But since there was no

way of predicting what might happen a couple of days in the future, I got a bit edgy about the crypto gear. I didn't want it sitting around somewhere for days at a time waiting for pickup by ARFCOS (Armed Forces Courier Service) or by diplomatic courier. So I sent a message back to S requesting permission to destroy the classified portions of this equipment.

(U) Now they don't fool around in S. When it comes to balancing dollar costs against crypto security, it's no contest. Of all the requests for guidance I sent to NSA during this period, this one drew the fastest reply: if you feel there's any risk of loss—destroy.

(U) Emergency destruction plans envision more than one type of emergency, depending on urgency. The most critical is they're-breaking-down-the-front-door right-now, which involves destroying everything in its installed position. Some of our more adventuresome people wanted to try this, but since it would have, at the very least, rendered our operations building uninhabitable for some time (and at worst, burned it to the ground), we rejected this approach, taking a more leisurely one.

(U) All the classified devices were removed from their racks, carried outdoors, and laid out on the ground. Next we put a destruction device on each one.

(U) The first thing that became apparent was the wisdom of not performing the destruction indoors. A towering column of thick black smoke rose straight up hundreds of feet in the air, while the heat given off caused us to step further and further back. After a minute or two I went inside and called the two other local U. S. installations (the Consulate General and the Naval Communications Unit) to advise them that we were neither under attack or burning down, that the smoke column was perfectly routine.

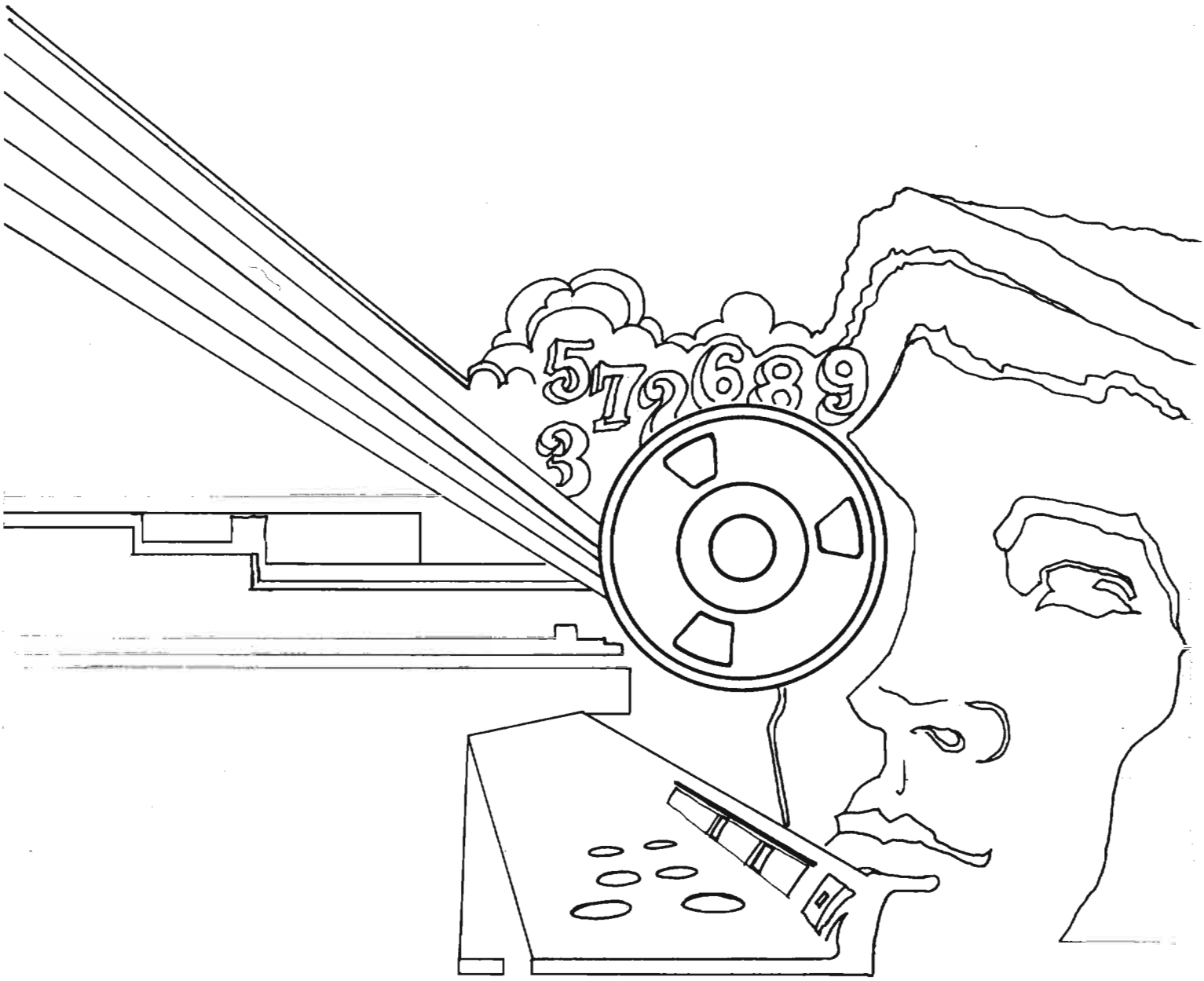
(U) CLA — NCS FOREIGN FILMS FOR SPRING (U)

Thursday, 26 April, 1300 hours: "The Hero's Wife" (Hebrew)
Tuesday, 1 May, 0900 hours: "Italiano Brava Gente" (Italian, German and Russian)
Thursday, 31 May, 0930 hours: "True Friends" (Russian)

IN THE FRIEDMAN AUDITORIUM

E.O. 1.4.(c)
P.L. 86-36

Pl-Mar 79-S3-27249


5 7 2 6 8 9
3

DOCID: 4009825

~~TOP SECRET~~

T3335 [redacted]

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MARCH 1979

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

PURSUIT OF THE [redacted] ..... E. Leigh Sawyer 1
CLASSIC CABLES 6
VORD *IS* A BETTER IDEA ..... [redacted] 7
READERS' SURVEY ..... DHW 10
LET'S NOT LOSE OUR TA SKILLS ..... [redacted] 11
LETTER TO THE EDITOR 12
COMPUTER OPERATING SYSTEM VULNERABILITIES ..... [redacted] 13
"DATA STANDARDS WITHOUT TEARS" (A COMMENT) ..... [redacted] 16
NSA-CROSTIC NO. 23 ..... Arthur J. Salemme 18
FAIRBANKS ON ENGLISH ..... Sydney Fairbanks 20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 2 MAR 2009~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. VI, No. 3 MARCH 1979

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor-in-Chief.....David H. Williams (3957s)

Collection.....[redacted] (8555s)

Cryptanalysis.....[redacted] (4902s)

Cryptolinguistics.....[redacted] (5981s)

Information Science.....[redacted] (5711s)

Language.....[redacted] (8161s)

Machine Support.....[redacted] (5084s)

Mathematics.....[redacted] (8518s)

Special Research.....Vera R. Filby (7119s)

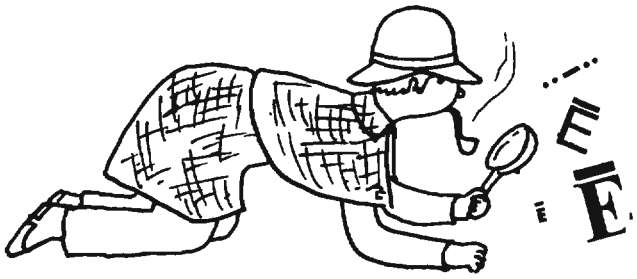
Traffic Analysis.....Don Taurone (3573s)

Production Manager.....Harry Goff (5236s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET UMBRA~~



Pursuit of the

[redacted]

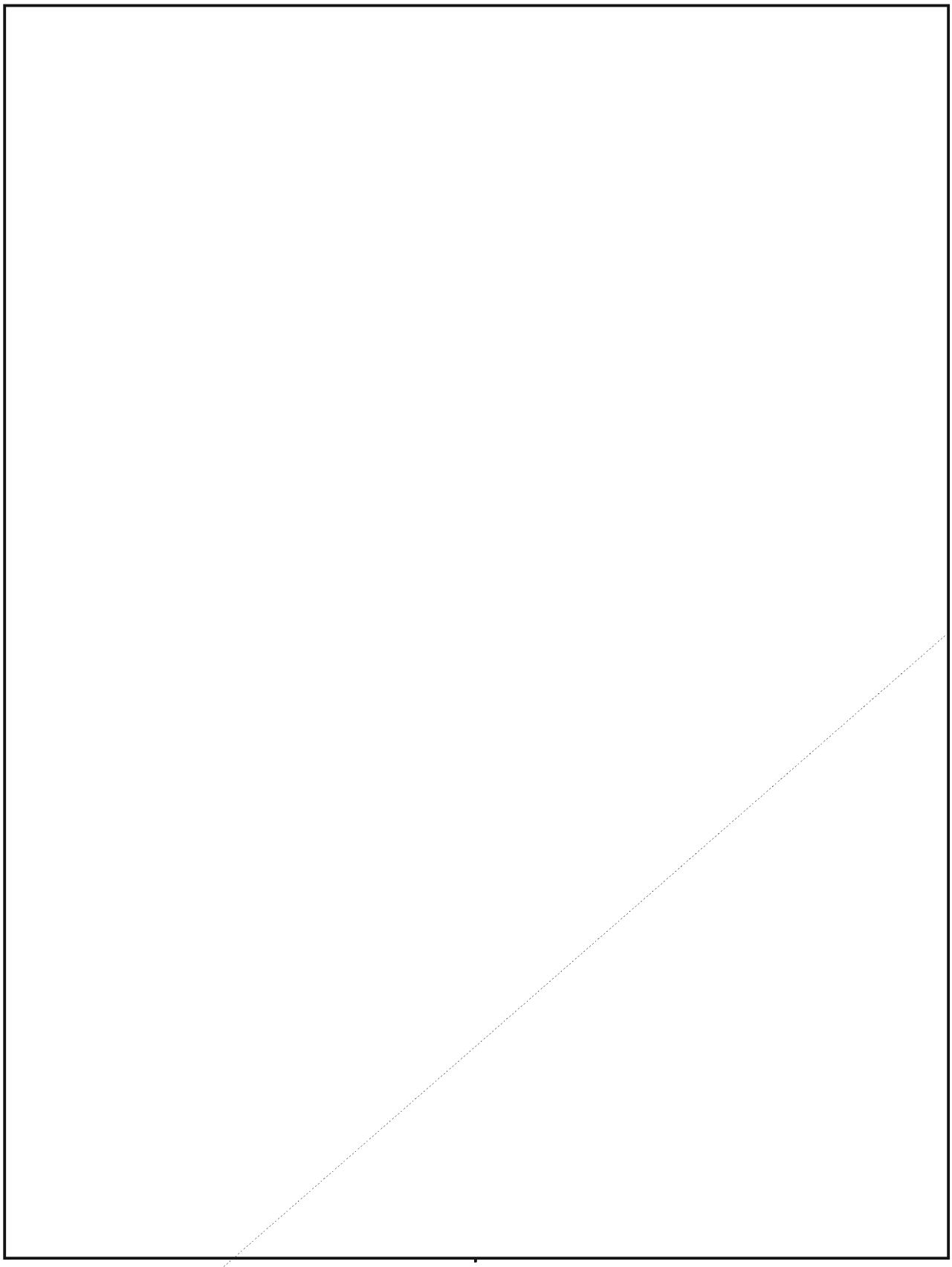
E. LEIGH SAWYER, 84

EO 1.4.(c)
P.L. 86-36

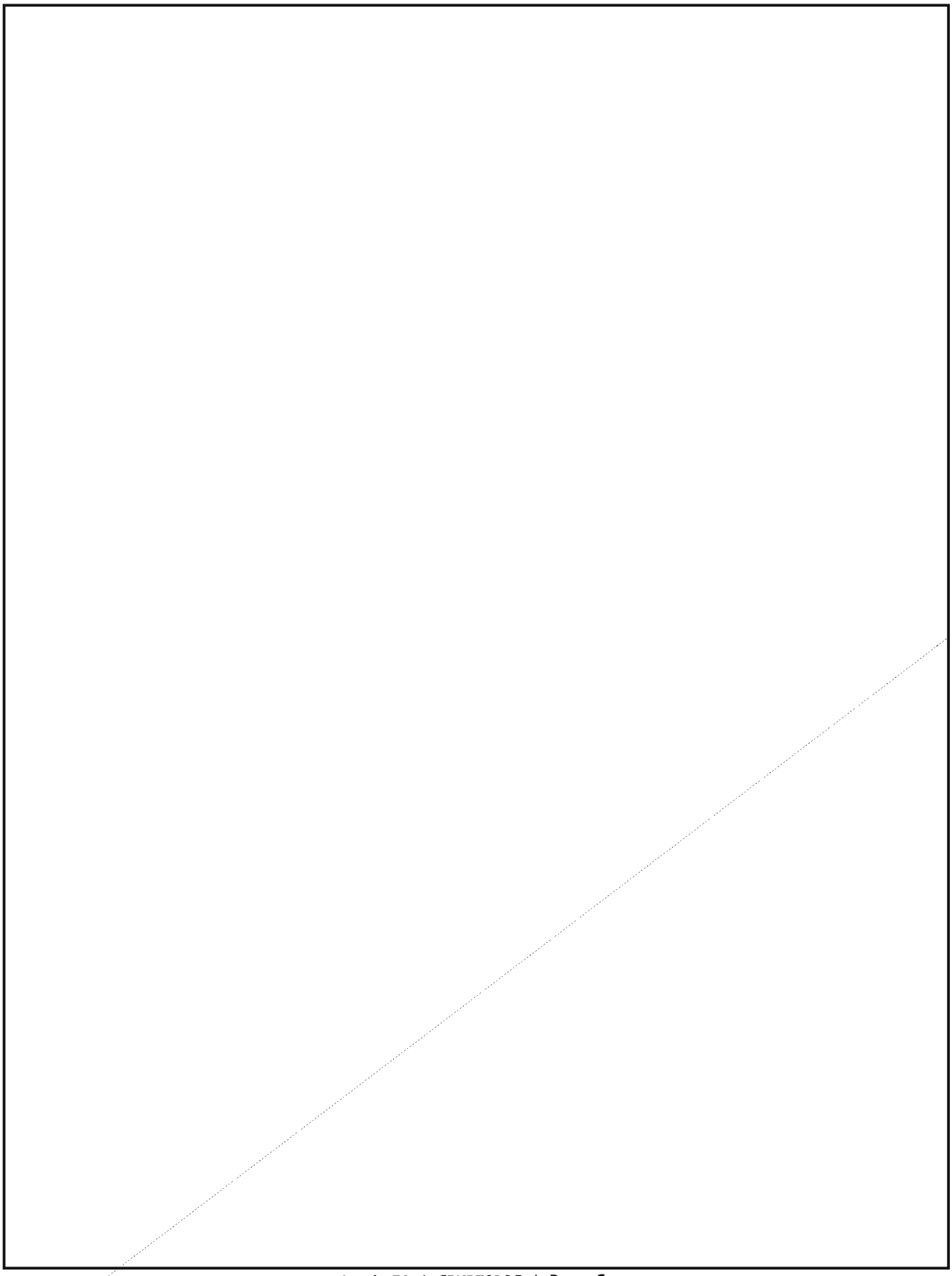
[redacted]

~~TOP SECRET UMBRA~~

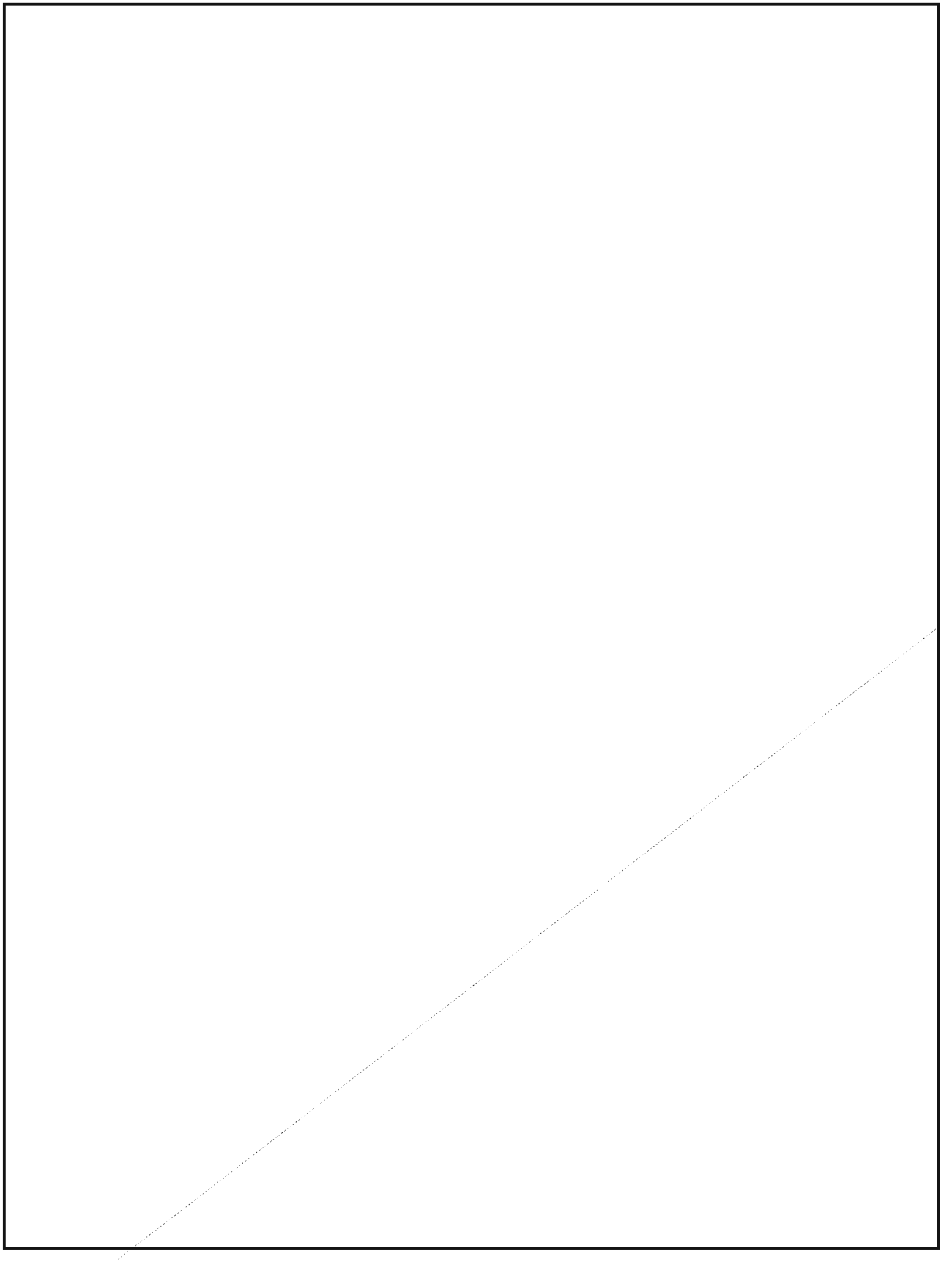
P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)



EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

SOMETHING TO BEAR IN MIND

EO 1.4.(c)
P.L. 86-36

CISI SPRING CONFERENCE

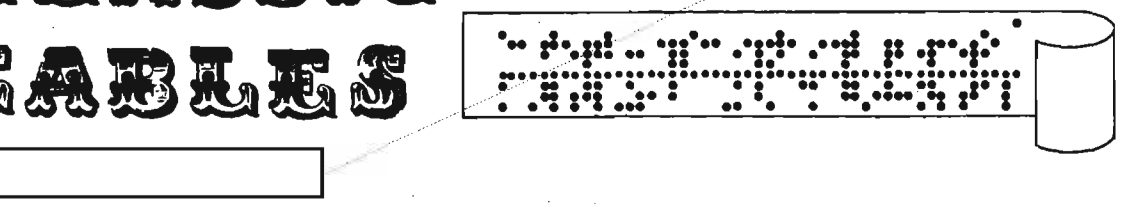
The Computer and Information Sciences Institute (CISI) will hold its 1979 Spring Conference during the week of 21—25 May in the Friedman Auditorium.

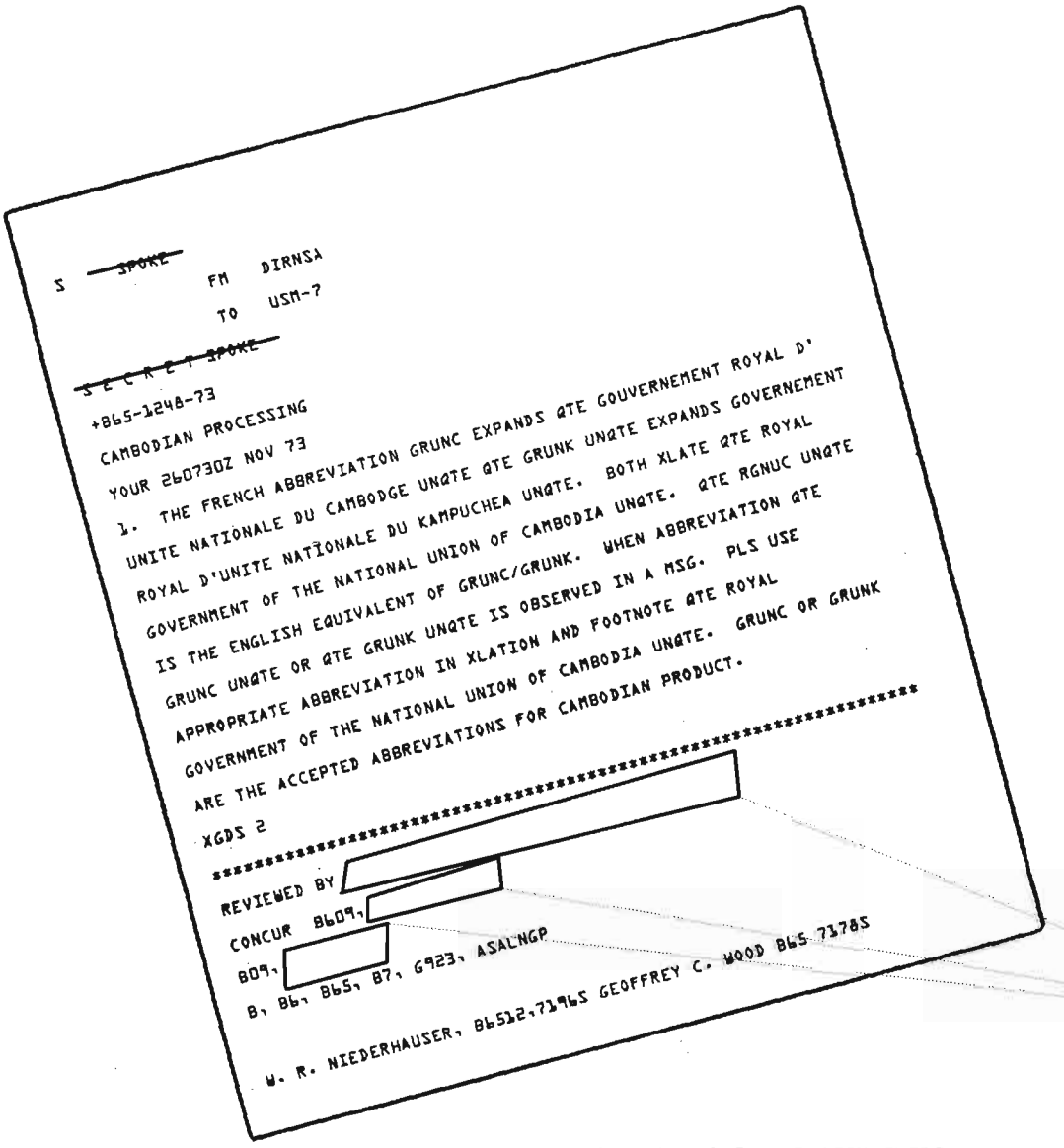
The theme of the conference will be "The User...It's About Time." Subjects of the presentations and times of the sessions will be announced later. (U)

P.L. 86-36
EO 1.4.(c)

EO 1.4.(c)
P.L. 86-36

CLASSIC CABLES





S ~~SPOKE~~
FM DIRNSA
TO USM-7

~~S E C R E T SPOKE~~
+865-1248-73
CAMBODIAN PROCESSING
YOUR 260730Z NOV 73
1. THE FRENCH ABBREVIATION GRUNC EXPANDS QTE GOUVERNEMENT ROYAL D'
UNITE NATIONALE DU CAMBODGE UNQTE QTE GRUNK UNQTE EXPANDS GOVERNEMENT
ROYAL D'UNITE NATIONALE DU KAMPUCHEA UNQTE. BOTH XLATE QTE ROYAL
GOVERNMENT OF THE NATIONAL UNION OF CAMBODIA UNQTE. QTE RGNUC UNQTE
IS THE ENGLISH EQUIVALENT OF GRUNC/GRUNK. WHEN ABBREVIATION QTE
GRUNC UNQTE OR QTE GRUNK UNQTE IS OBSERVED IN A MSG. PLS USE
APPROPRIATE ABBREVIATION IN XLATION AND FOOTNOTE QTE ROYAL
GOVERNMENT OF THE NATIONAL UNION OF CAMBODIA UNQTE. GRUNC OR GRUNK
ARE THE ACCEPTED ABBREVIATIONS FOR CAMBODIAN PRODUCT.
XGDS 2
****
REVIEWED BY
CONCUR 8609,
8609,
B, 86, 865, 87, G923, ASALNGP

W. R. NIEDERHAUSER, 86522,71965 GEOFFREY C. WOOD 865 71785

P.L. 86-36
EO 1.4.(c)

(Reprinted from DRAGON SEEDS, December 1973) ~~(SC)~~

DOCID: 4009825

VORD *is* A Better Idea

[redacted] P1

P.L. 86-36

For the past two decades NSA has been using a language aptitude test which is both weak and outmoded. This article summarizes the work performed by James Child, and others, both here and in other agencies, to develop a more reliable aptitude test.

In developing a new test for language aptitude I assumed the existence of an unqualified aptitude for learning foreign languages, although it might be argued that this skill is subsumed by general verbal aptitude and need not be tested by an artificial language. I have also not dealt with the possibility that there may be *two* kinds of aptitude, one for participating in face-to-face exchanges using foreign languages and the other for analyzing linguistic content.

The problems of the new test are in the main syntactic and require a skill in absorbing grammar forms that reflect quite different kinds of relationships within the sentence from those most students are accustomed to in English, Spanish and other European languages. The lexicon I have developed has played a minor role so far, but if the exercise were "powered" (i.e., required to be taken under pressure of time), it could be used to test vocabulary memory as well.

Before taking up the test proper, I would like to express my appreciation to my colleagues at NSA and other agencies for their willingness to give time and considerable effort in helping validate the test and in making a great many useful suggestions to improve it. The weaknesses of the new model are my responsibility alone.

This new test, which I have named VORD, has undergone extensive trial and is being unofficially used in the screening of both prospective and present employees. My colleagues and I have developed and refined this test in response to the need for an instrument better predictive of success in non-Indo-European languages than the Army Language Aptitude Test (ALAT) currently in use at NSA and long used at the Defense Language Institute (under the designation DLAT and with some differences in format and norming).

ALAT, designed and validated in the late 1950s, has served both agencies reasonably well in foretelling student success particularly in the learning of West European languages, although even here the very high and very low scores correlate much better with proficiency test results than do those scores in the middle. It has not been of much predictive value, however, in the learning of languages like Korean and Vietnamese. Indeed a careful study carried out in late 1971 or 1972 by COL Kibbey Horne, linguist and one-time commandant of the DLI school at Monterey, California, showed an almost random correlation between aptitude scores and course grades for these two languages, and our experience at NSA supports his findings.

Hence the impetus for the new test. In the paragraphs below I will first touch on the linguistic features of ALAT, then discuss at greater length the philosophy behind our test design, the various forms the test has taken over four years and the results we have obtained so far. In comparing the two tests, I will try to show that the key to language aptitude as understood in this paper is the degree of skill required in mastering a language system vastly different from one's own, as opposed to mastering a language with a similar system.

ALAT is a 57-item test based on an artificial language which has been variously described as formally similar to Turkish (e.g., by Kibbey Horne) and as western Indo-European in typology. Actually, the test so closely resembles English syntactically that a test subject who can quickly memorize the few grammar rules and somewhat more numerous words and grammatical forms can make a relatively high score. This is not to say, though, that ALAT is a memory test as such; the examinees can refer to their rules and lists as often as they like. However, the time limitations (7 minutes to study grammar and vocabulary, 20 minutes to do the problems) are what drive the test. The few problems of linguistic interest come toward the end, between questions 50 and 57, but as almost no one gets that far the issue

is academic. In short, the test stresses quick look-up and "photographic memory."[1]

Obviously, if some ability to perform linguistic analysis is an ingredient of language aptitude (at least the kind of aptitude NSA requires) a new model was badly needed. This I launched in September 1973 in the form of a test based on an artificial language structurally like Turkish. Since Turkic languages are very different in structure from most European languages, and not many job applicants are likely to have studied them in depth, this typology seemed a good choice. The test itself in its original form contained 32 questions, ten each on nominal and verbal morphology, and 12 on phrase and sentence level syntax. The questions were designed to be progressively more difficult, the latter 12 requiring the subject to supply a fair amount of language forms to establish sentence patterns (unlike the ALAT which has always been multiple-choice in format and hence machine-gradable).

The first ten questions called for simple suffixes to be added to nouns, while the next ten required the subject to select correct verbal forms from multiple-choice listings. (Unfortunately, since the test will soon be official, I cannot cite examples from it.) As analytic skill rather than memory was the chief object, I decided not to set a time limit until we had at least a few cases for which the running time was recorded against which I could make a rough projection.

At this point my long-suffering colleagues came into the picture. We all thought that it would be most useful to try VORD and ALAT on the subjects the Educational Testing Service (ETS) found for our 1973-1974 CLOZE[2] test trials in German, Portuguese, and Russian (about 100 subjects in each language). Thus, since time was short, I hurriedly completed an inhouse trial to see if it was workable at all.

The limited number of cases—less than ten—suggested that the test did work, although the scores were on the high side because of the linguistic sophistication of the subjects. Their running time averaged about 45 minutes, so we allocated one hour for the ETS experiment. We then printed the test and turned it over to the contractor.

The results of the field testing were encouraging, though, to be sure, we were not using the model in a purely predictive situation; most of our 300 subjects had studied at least one natural language in high school or college. The correlations of VORD with CLOZE results in German and Russian were about as good, though certainly no better, than those of ALAT with CLOZE; the Portuguese results were more encouraging:

	VORD vs CLOZE	ALAT vs CLOZE
German	.35	.36
Russian	.29	.33
Portuguese	.52	.35

In all three test comparisons, however, we noted that the relatively small number of questions on VORD (32) together with the ample time alloted to it led to a bunching of scores at the high end of the scale.

The options for strengthening the test would have been to add another more difficult section which would have had the added advantage of face comparability with ALAT, or to make it a power test which, as I pointed out above, I did not want to do because we could not truly test analytic ability.

As I was discussing the questions with my colleagues, I was overtaken by events, in the form of an opportunity to test VORD and ALAT (again through ETS) on 150 subjects who were also to be tested in Arabic, Chinese and Japanese (about 50 of each). This time the correlation between VORD and the respective proficiency tests was stronger than between ALAT and the CLOZE forms:

	VORD vs CLOZE	ALAT vs CLOZE
Arabic	.53	.48
Japanese	.22	.06
Chinese	.52	.07

We found the figures for the Chinese testing particularly gratifying.

---

1. The inadequacy of ALAT prompted DLI to develop a new and much longer aptitude battery (Defense Language Aptitude Battery), which has proved to be a better predictor of success in learning some languages than DLAT. However, because it requires considerably more time and special equipment than either ALAT or the new NSA test, and because it is still unproved for many languages, I have not treated it in this paper. For full information see "The Development of the Defense Language Aptitude Battery (DLAB)," by Calvin R. Petersen and Antoine R. Al-Haik, *Educational and Psychological Measurement*, 1976, Vol. XXXVI. No. 2, pp. 369-380.

2. The CLOZE language testing technique, which has been in use for several decades, involves deleting letters, syllables, words, or any other linguistic unit at some arbitrarily chosen interval (say, every fifth position), and requiring the test subjects to restore the missing material. Our use of the term is somewhat inaccurate since we establish our deletions at points of particular linguistic interest rather than doing so mechanically.

Exciting as these results were, the raw scores supporting them were still insufficiently spread out to give us plausible ranges within a STANINE or STATEN structure (the same problem is also encountered in ALAT, with its apparent 57 problems which for the vast majority of subjects amounts to about 45).

We therefore decided in July 1976 that we should add more questions to bring the test into a range of 50 to 60 problems. At this point I devised a CLOZE test along the lines of the models we use for proficiency testing (running VORD test, with deletions, on the right hand side, and English facing translation on the left). Twenty-eight items were deleted and, in the interest of maintaining a totally machine-gradable test, five multiple-choice alternatives were listed below each (lined) blank.

Once again we chose subjects for feasibility testing, but this time we had the leisure to be selective: four of our guinea pigs were multilinguists with at least some training in formal linguistics; eight worked with Romance languages; and seven were Turkish linguists. The not too surprising result was that the first and third groups scored very high, while the second group, with two brilliant exceptions, brought up the rear. The raw scores ranged from 26 out of 28 down to 12 out of 28 correct, distributed in a reasonable bell curve. Three items did not work well so we restored them, leaving us with, concidentally, a 57-item test.

Since 1977 we have been trying this test out on outside applicants for language jobs and comparing the results with the scores made by these people on language proficiency tests. The some general relationships appear for ALAT/VORD and Russian CLOZE tests as obtained in the ETS experiment, if we consider only the 32-question part of VORD (Part 1): .31 and .26, respectively, for a population of about 100. When Part 2 is correlated with the Russian CLOZE the result is a nonsignificant .06.

In languages other than Russian, the figures are too scant to permit the drawing of any firm conclusions. We have done some inhouse testing for persons scheduled to take Chinese, Korean and Arabic (about 56 all told), but the respective courses are not far enough along to permit serious proficiency testing and data comparison. The most we can say at this stage is that the subjects screened had either scored high on ALAT/DLAT as well as VORD or were linguists with considerable experience in several other languages who did well on VORD.

We plan to continue administering VORD to prospective students of these languages. We believe that when enough cases have been collected the new test will prove to be a much stronger predictor than ALAT. (U)

ATTENTION: MILITARY TRAFFIC ANALYSTS!

Are you a professional Traffic Analyst? Why not fill out a Professional Qualification Record (Form P7940), and submit it to the TA Panel, H115, for evaluation against the published criterial. Let's find out how close you are to professionalization.

Are you required to do this? The answer is NO. There is no current requirement for members of the SCAs to take this action. So why should you? What's in it for you? The best answer is self-satisfaction and pride. As a military man or woman assigned here, you are a member of the NSA cryptologic team. Civilian members of the team, many of them former military, are aspirants for professionalization and know where they stand in seeking certification.

A few SCA members have applied for certification and have received personal notification pf their status. Specifically, there are 30 military aspirants for TA certification at this time; this is about 16% of the total assigned military TA population participating in the professionalization program. Only five military personnel, currently on the rolls, have achieved certification in the TA field. Of note is the fact that the highest score attained on the most recent Related Fields Examination, a basic requirement for certification in both the TA and SR (Special Research) career fields, was achieved by an SCA member (Navy).

You are invited to participate. Fill out a PQR and submit it to H115, Room 1W155. If you have any questions, do not hesitate to call us, ext 3573s. (U)

SOLUTION TO NSA-CROSTIC NO. 22
(*CRYPTOLOG*, February 1979), by DHW

B[ill] Crowell, "[A] Computer Scratch Pad [at Home or at Work?], *CRYPTOLOG*, June 1978

"Almost unnoticed at NSA, the outside world has undergone a revolution in their approach to computer support. The day of the microcomputer has arrived. Not only have thousands of very small businesses begun using them, but...even individuals are buying them and ...creating new applications on them." (U)

HELP WANTED!

The four roads around the Agency's main buildings are named Towler, Engstrom, Herzog and Wray. Before everyone who knew the men for whom these roads were named has either retired or died, it might be appropriate to write short articles about the contributions and personalities of each of them. If you have any information of this kind, please send your recollections to: [redacted] *P12, who hopes to coordinate the project.* (U)

P.L. 86-36

DOCID: 4009825

READERS' SURVEY

By DHW

In last December's issue, CRYPTOLOG printed a survey questionnaire, asking for reader comments about the magazine. We'll be publishing the results of the poll in an early issue. Two of the responses, however, merit publication on their own.

One of the questions asked for opinions on why there had been so few women contributors to CRYPTOLOG in 1978; out of a total of 83, only 11 were women.

After weeding out the extremist pro- and anti-feminist sentiments, I was left with three responses, all of which said more or less the same thing. It was best expressed by one young lady who wrote:

> "I believe this relates to the percentage of women at NSA, particularly in the higher grades. Your 14 per cent female participation for the year is not bad considering that only 9.5 per cent of the workforce at or above grade 11 is female—and I would imagine that the majority of your articles are written by persons at those grade levels."

I have no doubt that this is true. CRYPTOLOG articles tend to be written by managers, analysts, computer specialists, engineers, and others in comparable jobs, who, as noted, tend to be people in the higher grades.

A quick review of the back numbers of the magazine shows (although I'm willing to be corrected by someone with a better memory than mine) that we have never carried a piece by any member of the secretarial or clerical force. Why should this be?

There must be quite a few people in those categories who have things to say which would be of considerable interest to CRYPTOLOG's readership. Personally, I can think of more than one young lady around here who could write nonstop for several hours on "A Secretary's Lot is Not a Happy One (If you Work For a Clown Like I Do)" or "Prematurely Gray at Age 26."

I'm sure there are also serious topics worth taking up, such as "Six Shortcuts to Office Efficiency" or "Why Doesn't Somebody Invent a _____!" So, come on there, ladies; let's hear from you. Put something of your own creation through your typewriter; that dreary memo can wait. I'll be looking for it.

The following response is printed in full, and with it goes an invitation to the right person (in N? in D?) to respond to it.

"How's chances of an article on the budget process? In these days of fiscal austerity, where just about any cryptologist seeking to do his or her job better (or, sometimes, just to maintain the status quo) is faced with a myriad of problems in competing for extremely hard-to-obtain funding, one is puzzled, or even baffled, by the process itself and, in particular, by the associated terminology.

"For example,

What does "over guidance" or "below the line" mean?

-Who makes up the CRG, or the RRG, and what specific roles do they play?

-Once the NSA budget is prepared and "blessed" by ADPR and the Director, to whom is it submitted, and what happens next?

-Who else reviews, comments, cuts, rearranges, etc., our budget proposal?

-What are Congressional Review Books (Congressional Justification? Books), and what role do they play in the budget review process?

"Those questions are intended to be illustrative, not all-encompassing. Certainly, there are lots more buzzwords or steps in the process that I have missed. How about a series of articles, like the old Saturday afternoon matinee serials, designed to keep us sitting on the edges of our chairs until the next issue.

"I realize this request is a tall order, but please consider that there are a lot or us out here who contribute to some or all of the information-gathering activities which support many of the budget review procedures, yet we do not have a full understanding of what is going on, or why it is necessary to recast information in different formats over and over again.

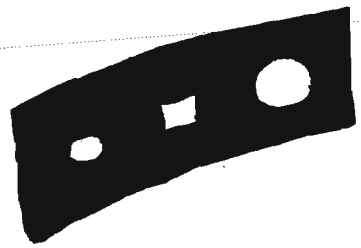
"Perhaps the explanation I have requested above would be useful to educate us. Armed with this knowledge, we may be able to be more responsive to the various requests, and, who knows, we may end up with a better product, or even more money.

"And, by the way, please keep the article simple to understand." (U)

DOCID: 4009825

[redacted]

P.L. 86-36



Let's Not Lose Our TA Skills

One thing a middle-level supervisor in the Production organization realizes very quickly is that good traffic analysts are hard to find. Those traffic analysts with a skill in a specialized area such as frequency and callsign recovery are scarce. [redacted] As indicated in the A/DDO memorandum, the underlying causes for this decrease in traffic analysts are the rapid change to automated methods of collecting and producing SIGINT, and the personnel limits imposed on the size of the NSA work force. Since NSA cannot hire personnel to fill shortages in critical skills, the traditional skills have been reduced to accommodate increases in linguists, signals conversion personnel, collection technicians, and data systems analysts and programmers. As a result, we are creating a static pool of traffic analysts, retarding the development of our analytic talent and altering the career-progression patterns of the traffic analytic work force. It is these effects that I wish to discuss.

EO 1.4.(c)
P.L. 86-36

The end of the Vietnam War, the subsequent tightening of purse strings and the resultant reductions in traffic analytic spaces altered the availability of traffic analysts. By limiting the hiring of new traffic analysts and not replacing those lost by attrition, the size of the analytic career field was set [redacted] The immediate effects were minimal since the number of traffic analytic jobs was also decreasing, with the reduction of many of the timely requirements for information on Southeast Asia. Also helping to offset any immediate effects were the great strides made in mechanizing the traffic analytic processes during the Vietnam War. Efficiencies had been created and a degree of timeliness using methods of intelligence production never before possible had become routine.

The long-range effects probably will not be apparent until the late 1980s, but some symptoms are already beginning to appear. Our traffic analytic work force is getting old. Most of the younger analysts were hired during the 1960s and are now GG-11s or higher. Most basic traffic analytic work is now done by the military, either at the field sites or at NSA. No substantial group of young analysts at the lower grades is available for the future. The more aggressive analysts have already moved into management positions to further their careers. To aggravate what is rapidly becoming a bad situation we have retarded the development of the younger traffic analyst. In the earlier growth days of our Agency, a traffic analyst could grow in a specific target area, become recognized as an expert, and advance in grade and responsibility within his chosen career field. Today, the aggressive young analyst soon recognizes that his future is not in the technical side of the traffic analytic business. To advance and achieve a modicum of success, he must move into management or to one of the critical-shortage skills. As a consequence we deplete our analytic talent base and few people are left to form a nucleus for the future.

Those who are left usually have a sincere desire to remain in the technical side of the intelligence production business. Even those people are prodded by management to move into the more critical areas of data systems or linguistics. Since chances of promotion are mathematically better in these skills, many of the remaining talented young people do indeed transfer.

Those who remain face a slower career progression since the money provided for the special considerations given to the critical career areas reduces the total sum that would normally be equally divided among all those eligible for promotion. This means the traffic analyst must face stiffer competition for the promotions that are available and ultimately his chances to achieve a position of leadership within the Agency are diminished.

EO 1.4.(c)
P.L. 86-36

As a result, probably in the near future, we are going to be faced with a severe analytic shortage similar to that which we now have with linguists. A more serious consequence will be the loss of analytic skills that can be learned only by years of experience. Specialists will

be nonexistent and major analytic recoveries will suffer. Although these problems can be alleviated to a degree by hiring from the SCAs and by programs such as the intern program, these are not immediate solutions. Unlike the data systems and, to a certain extent, the linguistic fields, our colleges and universities are not graduating many traffic analysts. It is a career field where experience is the best teacher.

To avoid future shortages we should begin hiring some Traffic Analytic Technicians right now. These technicians could be hired out of high school at the GG-2 level and put through a program similar to that used for training linguists. Given the proper incentives, training, and experience, these people would be ready to take over the analytic work load in about 10 years. If we fail to act now, we will have to react later when our chances of success are fewer. Traffic analytic skills helped make our Agency what it is today. Let's keep it that way. ~~(C-CCO)~~

While [redacted] *article was being prepared for publication, it was shown to* [redacted]*, Chief, Traffic Analysis, Office of Techniques and Standards and he was asked if he would like to add any comments. He has submitted the following addendum.*

Ed.

We could *also* hire ex-military traffic analysts, as we have in the past. This has the advantage that each "recruit" already knows what TA is, likes doing TA, and wants to make a career of it. That cannot be said of high school hires, and one must therefore expect a higher rate of "drop-out" than would apply to those already trained and experienced in TA (ex-military).

There must, of course, be some disadvantages to hiring ex-military traffic analysts. Otherwise, an agency as smart as we are would already be doing it. (U)

P.L. 86-36

Letter to the Editor

To the Editor, CRYPTOLOG:

In looking at this issue of data standards, I find myself of two minds. I firmly believe in order and organization, but I also know that a "structured orderliness" imposed arbitrarily upon an analytic organization *can* inhibit, and sometimes nullify, analytic initiative. And that initiative, elusive as it is, is the key to whether an analytic effort is alive and responsive, or just plodding and pedestrian.

My roots are in analysis, and I think the greatest challenges I have found have not been solving technical problems but, rather, encouraging others to solve them. That's the essence of being a cryptologic manager. I have come to the conclusion that each analyst has only so much "analytic energy" or attentive capability. The more complex we make *our* system (or that part of it which touches the analyst), the more we force the analyst to spend on *us* — and the less he has left over to spend on *them* (his analytic targets, or tasks)

As a line supervisor, I found that in trying to adhere to the many rules, conventions and rituals around here, I could usually "follow the book" so long as it wasn't too costly in "analytic energy." But there was a limit. There was usually a threshold beyond which I would not go, beyond which the bother did not justify the result. My response then (and yours too, I suspect) was to ignore the system or go around it. (We are, after all, a building full of people whose business it is to go around someone else's systems; it isn't that hard to go around ours.)

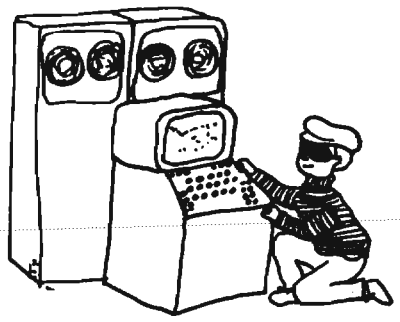
For the sake of overall order and organization, our rules and rituals ought not to be complex *from the point of view of the one who has to comply*. This holds whether we're talking about forms control, time cards, or data standards. These things are needed, but we have to get our priorities right.

[redacted]
P14 (U)

P.L. 86-36

DOCID: 4009825

COMPUTER OPERATING SYSTEM VULNERABILITIES



[redacted] S86

P.L. 86-36

"Can my system really be penetrated?" This is the question so often asked by computer system managers. The inevitable answer is "Yes. Any computer system can be penetrated by a knowledgeable user." Large computer systems, in particular, by their size and complexity, leave themselves open to attacks by unauthorized users. Let us examine some of the vulnerabilities of computer systems, as well as some of the possible defensive measures.

COMMON OPERATING SYSTEM VULNERABILITIES

Operating system vulnerabilities generally fall into one or more of the following seven classes: [1,2]

- Incomplete parameter validation
- Inconsistent parameter validation
- Implied sharing of privileged confidential data
- Asynchronous validation and inadequate serialization
- Inadequate identification, authentication or authorization
- Violable limits
- Exploitable logic error

Let us look in detail at each class of flaws and see how they affect the system operation.

Incomplete parameter validation. Whenever a user requests any type of service, the operating system must verify that the user is authorized to make that request and that a proper parameter string has been provided by the user. This verification is done to prevent the user from compromising a control program which is performing services for all users. Flaws in some operating systems may allow a user to "fool" a control program into:

providing him access to data which he would not otherwise be allowed access rights,

placing the user program into privileged or executive mode, or

severely degrading the operation of the ADP system.

The following is a good example of incomplete parameter validation:

Using a file dump routine, User X requests a dump of 300 records from File A, but File A contains only 200 records. The system honors the user request, and User X is allowed access to not only File A, but also to whatever data is stored beyond the address area of File A.

Security requirements should make the control routine validate the parameters and either reject the user request or dump only those records which apply to File A.

Inconsistent parameter validation. Inconsistent parameter validation occurs whenever there are multiple definitions for the same construct within the operating system. For example, a system control program may validate a user program's parameters but trusts another system routine's parameters as valid without verification. Therefore, a user who can fool the system into believing his code is system routine code can obtain unauthorized privileges. System routines should verify all input parameter strings, even those from another system routine.

Implied sharing of privileged or confidential data. In a multiprogramming environment, the computer's facilities are shared by many users. The operating system must have the built-in capability to isolate each user from all other users. Failure to provide this segregation can result in a possible compromise of privileged information. In modern operating systems two problems are generally noted in this area.[3] The first is the matter of sensitive residue. This involves information left behind in memory or other storage media after a run has terminated. An unauthorized

DOCID: 4009825

user can enter the system and obtain access to these "leftovers." This technique is commonly known as *scavenging*. The second problem involves the system sharing user space for its own storage. To save space, the operating system frequently shares the user's buffers to store temporary working tables. This may allow the user unauthorized access to the system tables, i.e., password tables, etc. This is frequently known as the *unerased blackboard problem.*[1]

Asynchronous validation and inadequate serialization. System integrity is guaranteed only if information passed between program sequences is protected. If the operating system allows asynchronous operations and the operations are not performed in a timely sequence, the information may be modified or compromised. An example of this would be permitting the user to perform I/O into a checkpoint or restart file so that his restarted program is given unauthorized or supervisory privileges.[4] To be secure, an operating system must be able to enforce timing constraints to a controlled state.

Inadequate identification, authorization or authentication. Most operating systems maintain some type of job initiation procedures which monitor authorized vs. unauthorized access. A system flaw exists whenever a system permits a user to bypass these security mechanisms. A user who finds a way to obtain executive operation mode can "walk" through the system without being questioned by the system monitor. Operating systems must require proof of access rights for all user requests. Security mechanisms must be protected from user tampering. For example, password files should be encrypted or protected from common access and must be unusual enough to void any guessing or permutation attempts.

Violable limits. Because of architectural limitations, the operating system has to limit the resources a user can control. These limits or "hands off" policies are usually described in the system documentation. Whenever an advertised limit is not enforced, a security flaw exists. For example, a user may be limited to operate within an assigned partition of storage; but a flaw in the system allows him access to another partition on an overflow condition. Because the operating system did not enforce the "rules of the road," a user could accidentally or deliberately cause a system overload, resulting in system degradation or crash.

Exploitable logic error. With four to five million lines of code, it is inevitable that there will be bugs in any major operating system.[4] A knowledgeable user may exploit these errors to his advantage to obtain access to information or programs to which he is not authorized. Logic errors can especially be created whenever the original design or coding has been changed. Logic modifications compromise any security measures designed into the original system. Examples of exploitable logic errors are frequently found in error-handling procedures. A user may request modifications or dumping of a file belonging to another user. Incorrect error handling may initiate the actions without first verifying that the user has access rights to that file. There is no way to avoid logic errors in large operating systems; however, these errors should be corrected when discovered to avoid prolonged compromise of sensitive information.

PENETRATION TECHNIQUES

Now that we know what some of the potential operating system flaws are, we need to know how a knowledgeable user, or *penetrator*, will exploit these flaws to obtain unauthorized access to the system. In planning his attack, the penetrator will have to answer the question, "What do I want—information or system degradation?"[5] The answer to this question will determine his method of attack. The penetrator's next step is to obtain all available system documentation. Valuable information which may point to vulnerabilities is available in the documentation. After reviewing the manuals, the penetrator can then decide on the techniques to be used in the penetration attempt. The penetrator's main objective is to attack one or more of the seven major flaw classes discussed earlier.

Probably one of the most available and easiest system penetration methods is the use of utility programs.[3] These service routines often execute user requests without requiring proof of access rights. Some types of utility routines are storage dump facilities, operations support programs and maintenance support programs.

Another widely used penetration technique is operator "spoofing." A penetrator can use trickery, such as giving his program the same name as a system routine, to make the operator think that his program is a privileged system routine. He may then request a load of privileged disc packs or magnetic tapes.

The penetrator can also obtain access to privileged information by creating a *Trojan horse.*[3] A Trojan horse is a program which, in addition to doing what it is advertised to do, does something else which its user doesn't know about and wouldn't want done. A Trojan horse is usually hidden in a utility program. An example would be a performance monitor which also dumps user information into a file somewhere (account numbers, passwords, etc.).

System penetration can also be obtained

DOCID: 4009825

by using any of several covert attacks.

Wire tapping. Also known as eavesdropping, this act involves the penetrator connecting some listening device to a communications line somewhere between a peripheral device and the computer central processing unit being penetrated. This is a passive operation.

Between lines entry. This is similar to wire tapping except that the process is active. The penetrator enters spurious commands onto the communication lines which were meant only for the legitimate users. This operation is usually done when the intended terminal is at an idle state.

Clandestine code. This operation involves the entering of changes, possibly a Trojan horse, into the coding of the computer operating system.

Masquerading. This involves logging into the computer system as a legitimate user whose account number and password have been acquired by begging, borrowing or stealing.

DEFENSIVE MEASURES (COUNTERMEASURES)

So, if our system is so susceptible to unauthorized access, how can we set up a defense against these measures? The best approach is to build security into the initial system design.[3] Patches to the design at a later time may create more flaws than they patch. The problem with most current operating systems lies in the fact that they were developed in the 1960s with no thought in mind for security requirements. Even with security in mind, we must remember that operating system security is not a binary yes-no condition. No large operating system currently in use can be completely certified as secure.[2]

Here are examples of measures which we can take to protect our system from attack.

Data encryption. Data encryption is becoming more widely used by both the government and private industry. Encryption should be performed whenever sensitive information, such as password files, payroll data, defense statistics, and the like, is stored or sent over data communication lines.

Using a minicomputer as a front-end security controller. This technique could be used to control access to the host computer from remote terminals. This would remove the security overhead from the host computer's operating system. The smaller operating system in the minicomputer would also be easier to certify as secure.

Mathematical models. Models allow systems analysts to study the complete operating system environment and pick each area apart for security analysis.

Kernels. Kernels are small portions of software blocked together to perform a single function. These small software modules could be certified secure.

Software verification tools. Many tools have been or are being developed to certify the security of computer software.

A LOOK AT FUTURE RESEARCH AREAS

Many areas in computer system security need to be explored in the future. Some of those areas are:

1. Development of better control structures (audit trails);[2]

2. Expansion of kernel theory to develop a "secure" operating system;[3]

3. Cost analysis studies (Where do we draw the line between cost of computer security and need? How do we measure security?)[3]

4. Development of strong consistent management policies to govern the use of computer facilities;[4]

5. Development of software verification tools to certify computer software;[3]

6. Development of some type of virtual machine monitor (an operating system which isolates each user into his own mini-operating system), which when properly designed and implemented is "spoof-proof";[3] and

7. Development of a security specification language which allows security requirements to be programmed into the operating system by the security officer.

I hope I have been able to provide some insight into just how vulnerable modern computer operating systems are. Department of Defense studies have shown a need for protecting data relating to the nation's defense because of the many opportunities for fraud and embezzlement.[2] We must also realize that software security is only one aspect of the total security environment. We must also consider administrative, personnel, physical, communications, emanations and hardware security. As modern technological advances are made, with their applications for computers, we will have a continuing requirement for operating system security.

No matter what misuses take place, we must realize that people are still going to use that magnificent adding machine, the computer. It has been proven that there are people with

skills to crack safes, yet people still use safes. The same correlation can be made to computer usage. Our job as system managers is to attempt to protect against accidental or deliberate destruction, modification, or disclosure.[2] Security policy (administrative, personnel, physical, communications, emanations, hardware and software) and practices must be sufficient to make up for the computer's inability to protect itself.

---

1. Webb, D.A. and Frickel, W.G., "Handbook for Analyzing the Security of Operating Systems," Lawrence Livermore Laboratories, 1976.

2. Abbott, R.P. et al., "Security and Enhancements of Computer Operating Systems," National Bureau of Standards, Rept. NBSIR 76-1041, April 1976.

3. Hoffman, L.J., *Modern Methods for Computer Security and Privacy*, Prentice-Hall Inc., New Jersey, 1977.

4. Chin, J.S., "Analysis of Operating System Security," Lawrence Livermore Laboratories, December 2, 1975.

5. Linde, R.R., "Operating System Security," *Proceedings of National Computer Conference, 1975*, 1975, pp. 361—368. (U)

"DATA STANDARDS WITHOUT TEARS"

A COMMENT BY [redacted] P1

Much of what [redacted] says in "Data Standards Without Tears"* has merit. The Data Dictionary concept can play a role in the standardization process, but not in the "magical" way he outlines. You can only have standards with *sweat* — without tears, perhaps, but certainly not without considerable labor. I am afraid that we have to indict [redacted] for not really giving due credit to the standardization process that the NDSC has long been pursuing, and also for presenting a few half-truths here and there along with the nuggets of wisdom.

~ "No one agrees that data standards should be enforced on his project at the expense of operational necessity."

Right. The NDSC has not tried to shut off anyone's job because of failure to observe standards. On paper we have the authority: both NSA Regulation 80-9 and USSID 414, "Standardization of Data Elements and Related Features for SIGINT Activities," Annex B ("Implementation of Standard Data Elements and Related Features in NSA/CSS Computer Projects") give us the *authority* to make life very unhappy for sponsors whose jobs ignore or conflict with published standards. In theory we can point to the concept of enforcement of data standards, even to the short-run disadvantage of a computer project. In actual practice, we sacrifice the long-term benefits to the Agency that would follow from a rigorous enforcement of the standards we already have.

~ "...we view standards as something which not only can be but must be imposed in an inflexible, hard-handed manner."

The Center never "imposes" standards in this way but issues them only after a long and rigorous process. This begins with a recognized need, research and discussion, drafting of a "proposal," etc., and continues with coordination through the Senior Data Representatives (SDR) of the DDO elements. There are draftings and redraftings to meet objections, suggestions, etc., and final approval comes, in many cases, only after a painfully long process. This is far from an "inflexible, hard-handed manner." A proposed standard always has wide circulation throughout the Agency.

~ "It goes without saying that [standards] cannot be achieved without some degree of magic. On the practical level the magic machine already exists for rendering coarse materials into fine standard gold..."

I guess a good name for this philosophy of standardization might be the "Rumplestiltskin Syndrome" — after the legendary gnome who was able to weave straw into gold to further his nefarious designs. Let us not accuse our good friends from the DED/D team of such plotting. Everyone would like to have the magic machine dispense usable and workable standards without going through the long and often painful process outlined above.

This philosophy is, I'm afraid, a naive one when viewed in the harsh light of the standardization process. I think I see what [redacted] is saying here, however. He is pointing out:

— the DED/D will expose people to the already-published standard data elements in the dictionary part of the system;

— the DED/D will show people, in the dictionary portion, what the current usage of data fields is along a wide spectrum of different Agency applications. Exposure to this usage will gradually lead us towards the necessary standardization. (The author of the essay does not explicitly state this, but this is my understanding of his concept.)

[redacted] goes on to separate the data features we deal with into two "domains" — Data Elements and Data Fields. I agree that this

---

*CRYPTOLOG, February 1979

P.L. 86-36

UNCLASSIFIED

DOCID: 4009825

is a good approach, both conceptually and physically, within the DED/D. The pure Data Elements go into the dictionary, along with their codes, definitions, configurations, and so forth. The baser Data Fields people use in many of their applications would go into the directory part. In other words, Data Elements point to "things" — classes or categories of information; Data Fields point to "homes for things" — the receptacles for containing data items. Fine. We have no quarrel with this. The problem comes in the fact that conceptually the essayist is mixing a Data Element with a Data Field. DATE OF BIRTH, for example, he would call a Data Element, which is incorrect. The Data Element is DATE, which has a standard definition and an approved configuration for recording it: YYMMDD. DATE OF BIRTH is a *field name* or Data Use Identifier. This latter term is not a red herring, thrown out to confuse people, as our author states. It is a well-respected term, defined in *Funk and Wagnalls Dictionary of Data Processing Terms* as: "A name, title, or description that specifies the intended use of a Data Element."

The main point here is that Data Elements and Data Use Identifiers (or Data Fields) are different and the DED/D should carefully demarcate them. A closely related point is that data standards is concerned not only with the pure gold of the Data Element, but also with the way one *names* a Data Field and the *code* or *abbreviation* one gives it. This is all spelled out in the SIGINT directive that governs the standardization program. There is a standard way to generate a field-name code or abbreviation. The author of "Data Standards Without Tears" is right when he says the Data Element is not really the "thing" itself but the descriptive "name...of a 'set of things.'" Where he gets into difficulties is in not distinguishing carefully between a Data Element and its "use identifier." Data Use Identifiers really don't have separate *data items* of their own; only true Data Elements have data items.

A practical problem arises with the DED/D. Where do you put the "good" Data Field names (i.e., the Data Element/Data Use Identifier combinations that have already been standardized)? As [redacted] says, the run-of-the-mill Data Fields that John Jones used in his favorite file will appear in the Directory. If many other people use some of the same field name/abbreviations he does, we may have a clue as to something that needs looking at as a potential standard. We agree, but let us hope that the dictionary designers will not forget about the gold we already have, the standard field name/abbreviations referred to in the previous paragraph. Conceivably they could be stored in the DED itself, as long as the designers remember that these are not in themselves Data Elements. There is a considerable economy of storage here. You only have to store (in computer memory) the *data items* for a given Data Element *once* for each identifiable Data Element.

A related problem has to do with Data Elements not yet standardized, or not capable of being standardized. For example, Case Notation has developed over the years into something so complex that it now defies any attempt to standardize it. We can, however, give it a "reserved uniform code" (CASN) and encourage file sponsors to use this in preference to one of their own invention. The NDSC has an on-line glossary of such Data Elements commonly seen in SIGINT files. Many are labelled "potential" data standards, but it may be quite a while before they can be introduced into the standardization process.

~ "...the case of a file or software system which exists before the standard is set up, where the effort required to change it is unacceptable."

Usually a sponsor cries "unacceptable" just because he does not want to go to the trouble of reprogramming. It is more a matter of convenience than operational necessity. A standard is not adopted until thorough discussion and coordination throughout the affected Agency elements have shown the NDSC that *all* users are able to implement it. The article merely supports parochialism by letting personal whim or convenience get in the way of implementing standards. The complaint about the "unacceptable effort" required to conform to an approved standard is often accompanied by one, or both, of the following statements:

"Standards are fine, as long as they don't conflict with those we've already set up in the project."

"I'll support standards 100% — so far as I possibly can."

~ "To sum up, standards cannot be created in a vacuum. They must be developed from current usage..."

Standards *are* created from a demonstrated need, not just dreamed up by the NDSC. We try to look at the needs of the entire Agency as regards a particular proposal and not just at the usage that has happened to evolve. Being able to identify current usage is important, though, and the coming DED/D should be very helpful in this area. P.L. 86-36

~ "There are two ways of tackling standardization: the easy way and the impossible way."

Yes, at the NDSC we sometimes feel that our job is impossible. We deal with abstract concepts which are often exasperatingly hard to pin down. It would be great to find an easier way. We will be happy to see the DED/D emerge as an electro-mechanical friend who can give us a hand. It will be nice to have the DED/D document the "real world" and the standards world. I suspect, though, that there will still be a lot of blood and sweat, even without the tears. (U)

DOCID: 4009825

P.L. 86-36

NSA-crostic No. 23

By Arthur J. Salemme, A.E.
(Acrostician Emeritus)

The quotation on the next page was taken from the published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS

WORDS

DOCID: 4009825

(Solution next month) A.J.S (U)

P.L. 86-36

Fairbanks on English

Some of the Agency's best writing on writing can be found in the essays written by Dr. Sydney Fairbanks while he was the editor of the NSA Technical Journal, *from 1956 to 1959. Most are as timely today as they were two decades ago. Here, from the October 1957 issue, is the opening salvo in his battle against "English as she is wrote in the Agency."*

We have decided that an editorial should not be mere persiflage. It should initiate reforms, strike blows for freedom, speak for the oppressed,—that sort of thing;—provided always that the Editor sticks to what concerns him. This matter of English as she is wrote in the Agency is something that inevitably concerns him. We have therefore purchased a small red flag, and are planning a series of manifestoes.

The other day a D/F [*Disposition Form, a long-defunct form for interoffice correspondence*] crossed our desk. It has been said that everything in Government is done by a D/F, but you have to be here a year or two to appreciate what a d.f. he is. This, however, is beside the point. The D/F in question was highly practical and intelligent, and it bore a rubber-stamp signature of an altitude that virtually guaranteed that the signatory neither wrote it nor read it. Nevertheless *someone* must have written it, and it is to be hoped, or feared, that someone read it. The third paragraph runs: "It shall continue nailed to the skull, however it will be removable with patience and a corkscrew." Or at least...perhaps we should explain that tact has prompted us to alter everything but the sentence structure, the comma, and the "however." It is these that we wish to discuss.

Of course there would be no point in such a discussion if the error in question were not extremely common. A friend who has to waste a large part of his time revising reports and letters written by subordinates tells me that he expects to meet it at least once a day, and wonders why this particular comma splice is preferred above all others.

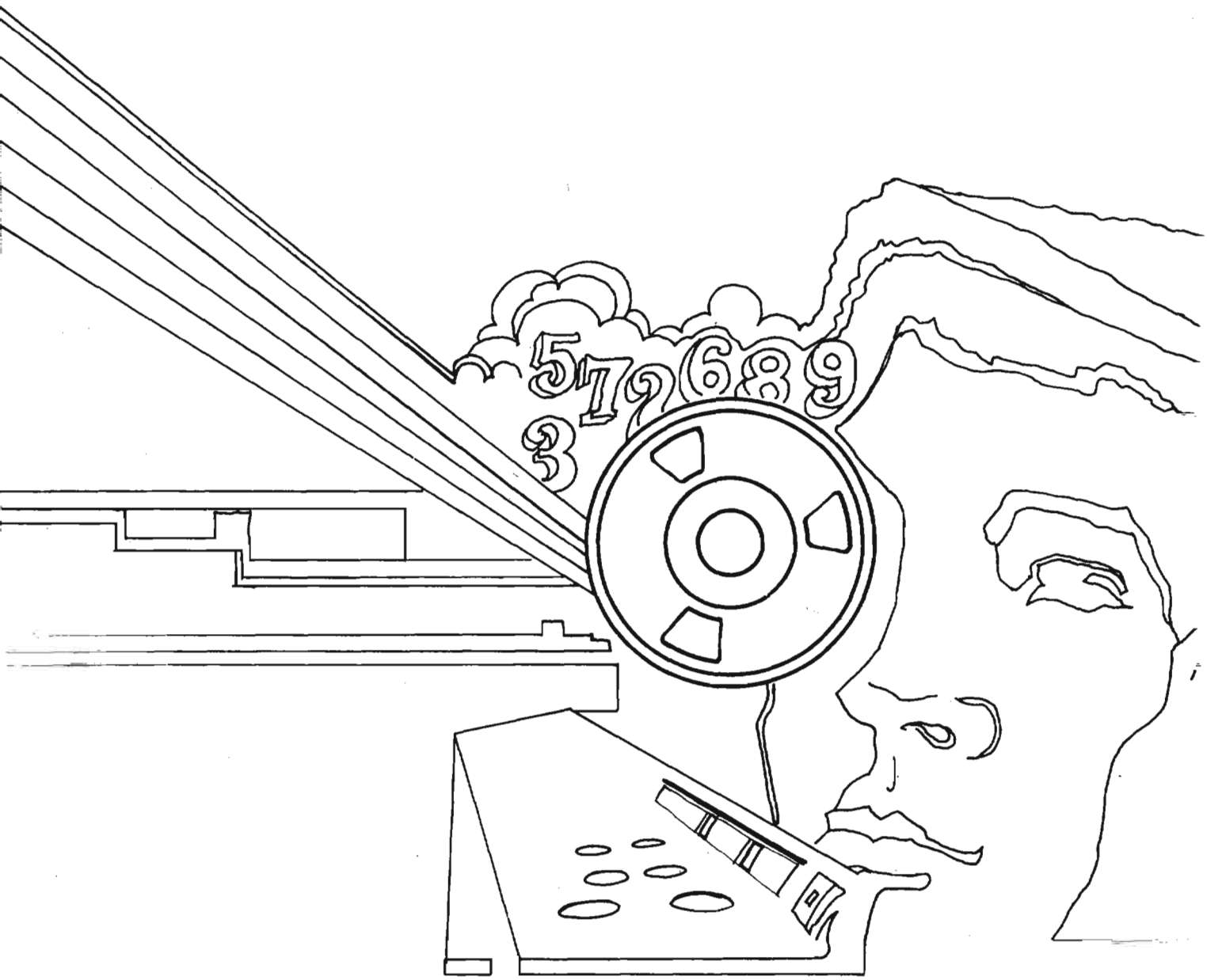
Alas, the answer is fairly clear. The sentence in question reads perfectly well if "but" is substituted for "however," and the question boils down to why the typical composer of D/F's says "however" when he means "but." He does it for the same reason that he says "presently" when he means "now." All you have to do is to count the syllables. If—and such things have happened—he wants to tell people to stop using long words in their letters, he will write, "discontinue the employment of ultra-lengthy terms in the correspondence presently emanating from your organization," without a qualm. Nothing less than a time-tested trisyllable is an adquate figleaf for his literary modesty, and the demand has created the supply.

Instead of working against nature, by trying to substitute the short word for the long, the general tendency of those who edit has been to modify the punctuation: "...nailed to the skull. However, it will be removable..."; thereby producing something that is merely clumsy. There is a legitimate use for "however" at the beginning of a sentence, where the essentially contrasting nature of what follows is to be not merely indicated but emphasized. There may even, conceivably, be an appropriate occasion for starting a sentence with "Therefore," although it is roughly equivalent to entering a room by flinging the door open with a crash and stamping on the threshold. But some deep and inscrutable instinct, like that which drives the lemmings to commit suicide, urges the D/F writer to begin every sentence with one of these two. Given the idea: "It is strong enough, but it is too large; better try something else," he can be counted on to express it: "It is strong enough. However, it is too large. Therefore, you should try something else."

If we were—fond, impious thought— one having authority, saying to one man Spell, and he spelleth, and to another Punctuate and he punctuateth, we would issue a D/F decreeing—in appropriate terms, of course—that in future no sentences would start with the words "however" or "therefore",—and then sit back and listen in grim glee while the electric typewriters ground to a halt and silence settled in the corridors. Some mute inglorious Milton would then discover for himself the possibility of writing, "We have, however..." and "It is, therefore..." and presently everything would start humming again. But the quality of the product would be, to our mind, appreciably improved.

Selah. (U)

P1-Feb 79-S3-27203


5 7 9 6 8 9
3

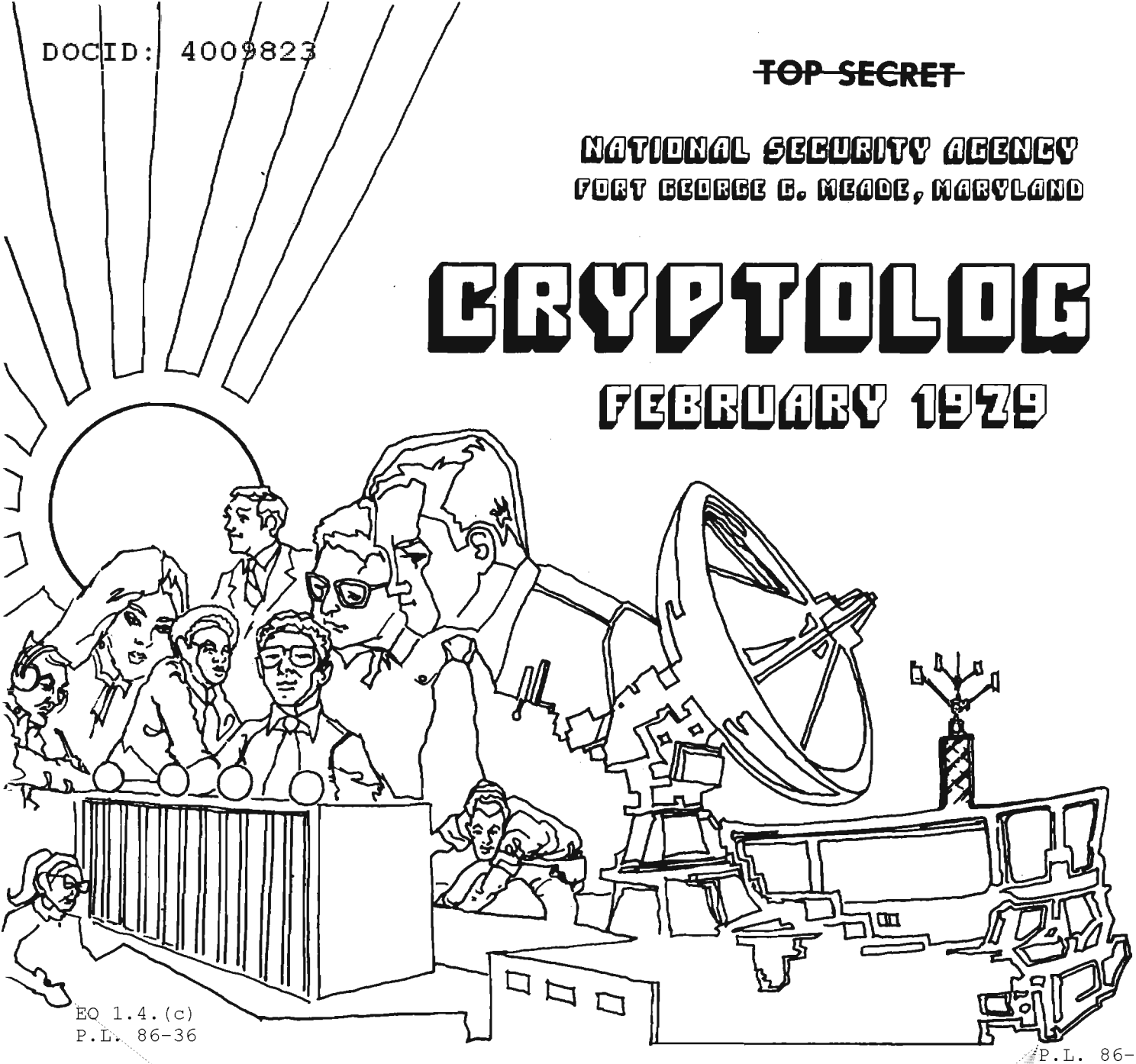
DOCID: 4009823

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

FEBRUARY 1979



EO 1.4.(c)
P.L. 86-36

P.L. 86-36

[redacted] AND A LITTLE BIT OF LUCK.....D.H.W.....1
CLA NEWS.....[redacted].....2
THE COMINT CHAIN "GANG".....[redacted].....3
KNOW YOUR GEOGRAPHY.....[redacted].....6
DATA STANDARDS WITHOUT TEARS.....[redacted].....7
WELL, MAYBE A SNIFFLE OR TWO.....Mark T. Pattie.....9
LITERATURE SEARCH ON-LINE.....[redacted].....10
IN DEFENSE OF THE INDEFENSIBLE:
NOTES ON THE RUSSIAN PQE.....Emery Tetrault.....13
LETTERS TO THE EDITOR.....15, 21
LET'S NOT FORGET OUR CRYPTOLOGIC MISSION...J. Gurin.....16
NSA-CROSTIC NO. 22.....D.H.W.....18
P. S.....[redacted].....20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 1 Feb 09~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009823

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. VI, No. 2 FEBRUARY 1979

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor-in-Chief.....David H. Williams (3957s)
Collection.....[redacted] (8555s)
Cryptanalysis.....[redacted] (4902s)
Cryptolinguistics.....[redacted] (5981s)
NEW ! Information Science.....[redacted] (5711s)
Language.....[redacted] (8161s)
Machine Support.....[redacted] (5084s)
Mathematics.....[redacted] (8518s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Don Taurone (3573s)

Production Manager.....Harry Goff (5236s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4009823

FROM THE EDITOR

By David H. Williams

[redacted] and a Little Bit of Luck

EO 1.4.(c)
P.L. 86-36

One of my first actions after becoming the new editor of CRYPTOLOG was to sit down and read through the back numbers. One of my principal discoveries was finding out that virtually all of the articles could be assigned, by general type, to one or another of a rather small number of categories.

By far the most frequent was the *This is Such-and-such* article, a straightforward description of something: an organization, an analytic technique or skill, a machine program, a new piece of equipment, or whatever. This article is the lifeblood of the publication, and every issue contains at least two examples of the type.

A special sub-category of this article is the *Here's How We Handle (or Handled) Such-and-such* piece, covering one organization's approach to an operational problem. To my mind one of the best of these was "The Iron Thumb," by [redacted] (March 1978) on the subject of MORETOWN, B Group's machine assist to the Chinese language translator.

Another frequent theme is found in the *Cry of Anguish* item, which describes some major injustice, frequently relating to promotions, especially in regard to their inequitable distribution to persons of one COSC (usually linguists) vis-a-vis another (usually engineers). Articles of this sort are often followed by a flurry of rebuttals and counter-rebuttals in subsequent issues. (Interestingly, one subdivision of *Cry of Anguish*, the comment on the performance appraisal, or the performance appraisal system, never receives any response in defense of that system.)

P.L. 86-36

One of my favorite articles is *Oops! We Goofed*. This article, which, understandably, appears relatively infrequently, details some organization's adventures and misadventures in going astray in the handling of some SIGINT phenomenon, and how they eventually coped with it. [redacted]

There are, however, two types of potentially worthwhile articles which, to my recollection, have never appeared, and I'm sure there are numerous examples, both current and ancient, of both of them here and there around the Agency. [redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~

So if you have any [redacted] piling up in your desk, drop a note to CRYPTOLOG. Maybe we can help you find the other half of your puzzle.

Or if you have any examples of breakthroughs made without the slightest intervention of any "scientific know-how and technical expertise," send them along.

Incidentally, if you have something you think you might want to contribute in either category, or on any other subject for that matter, but you feel a slight lack of self-confidence in your ability to put it down on paper, call or drop in at the CRYPTOLOG office. We're always glad to provide whatever editorial assistance might be needed.

The CRYPTOLOG office is located in P1, Room 2N039; the telephone is 3957s. ~~(SC)~~

CLA NEWS

RUSSIAN INSTITUTE

The Crypto-Linguistic Association has approved the formation of a new special interest group -- the Russian Institute. The new group's purpose, as defined in the guidelines, is to "provide a forum at which students of the Russian/Soviet problem can discuss and exchange information and insights gained from research in the field.

The guidelines call for the Institute to present Soviet films and lectures by visiting scholars as well as to encourage its own members to take an active role in leading discussions and seminars on various topics. The Russian Institute's guidelines define the Russian/Soviet problem in a very broad sense; the Institute hopes to include presentations on a wide variety of both work-related and more general topics.

Membership in the Russian Institute is open to all CLA members in good standing. If you are interested in becoming a CLA member or in renewing a membership that has lapsed, dues for 1979 ($3.00) can be sent to [redacted] Treasurer, P16, 2N039, 4032s. P.L. 86-36

A memo and survey form concerning the Institute have been distributed among Russian linguists. If you did not receive a copy and are interested in further information, please contact [redacted] A65, 2N001, 4367s. P.L. 86-36

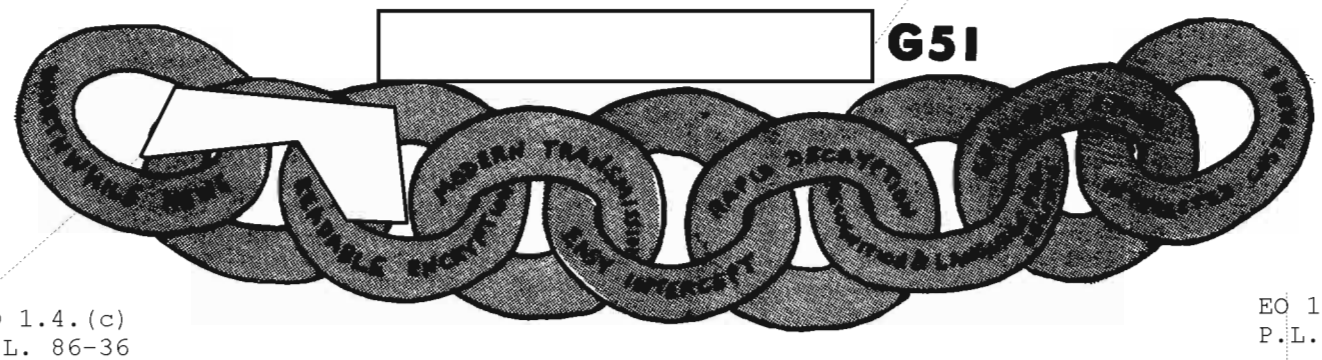
(U)

~~SECRET SPOKE~~

DOCID: 4009823

P.L. 86-36

THE COMINT CHAIN "GANG"



EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

I got a glimpse of how far-ranging NSA's activities are at NSA Day 1975, right after I came on board. I got the immediate feeling that there was a lot about the Agency I would never see, ostensibly because I had no need to know. It also became clear quite early that it would often be hard to find someone with sufficient knowledge to answer my questions even when I did have a need to know.

Being inquisitive (that's the word that applies to me -- "nosey" applies to other guys) and being interested in learning what the real career prospects are in the Agency, I began to ask questions about how things work in other offices. I asked my intern friends to compare and contrast what they had seen. I asked my classmates at the training school what their jobs were like. I also happened to hear conversations involving the occasional visitors to my work space (I really *wasn't* trying to eavesdrop). I even went so far as to listen to what was being taught in my professionalization courses!

The upshot of all my investigation was the decision to write a "tunnel vision" overview of COMINT operations, mainly for a friend in the Agency for whom the word "product" has little to do with the publication of intelligence. That term "tunnel vision" is a disclaimer so that if anything inaccurate is said, it can be blamed not on my personal inadequacy but on my limited perspective (one of my original aphorisms states that "what you see depends on where you stand"). With that warning you, the reader, are now ready for a worm's-eye view of the chain of COMINT Production.

Worthwhile News

The first link in the chain is a newsworthy event. Actually the newsworthy event is so important to "end product" that a better metaphor might be an anchor or a hook, or some other object on the business end of a chain. In reality, until something important outside the intelligence system occurs, the system has no function, no reason for being. If all threats to national security (military and economic) evaporated once and for all, those of us who have veteran's preferences might have to exercise them to get jobs in HEW or DOE or maybe even forget the preferences and scramble for jobs in productive enterprises. Because we must wait for something to happen, the best the Agency can do is to try to plan to be in the right place at the right time with the right equipment.

[redacted]

Fast-breaking events are in an entirely different league. Because of the limitations of money, politics, and technology, NSA simply cannot have a finger in every possible pie. For that reason, private newspaper reporters are occasionally much better equipped for gathering information in remote places than we are, or, for that matter, better adapted than anyone inside the intelligence community. The Agency subscribes to three wire services to take advantage of the mobility of their reporters. Right in the first link, then, we depend on factors largely beyond our control in order to get needed information into the hands of our decision makers.

EO 1.4.(c)
P.L. 86-36

[redacted]

Readable Encryption

These first four links are all outside of NSA and the intelligence community. The rest of the chain is directly controlled by the community.

Easy Intercept

Modern Transmission

After a message is encrypted, the next step is to transmit it. In this fourth link of the chain there are still some factors over which the Agency has no control. The way a message

*For a fuller discussion of the translation problems see "Thanks for the Attaboy!" (CRYPTOLOG, January 1978).

Rapid Decryption

formed by linguists is called dispositioning or scanning. To perform that task the scanner must not only keep abreast of a fluid set of "requirements" imposed by those who oversee the Agency, but also stay on top of what has already been published and what the consumers of our product think is hot any given time.

Efficient Staff

Recognition and Language Processing

One of the most important functions per-

DOCID: 4009823

EO 1.4.(c)
P.L. 86-36

Interested Customers

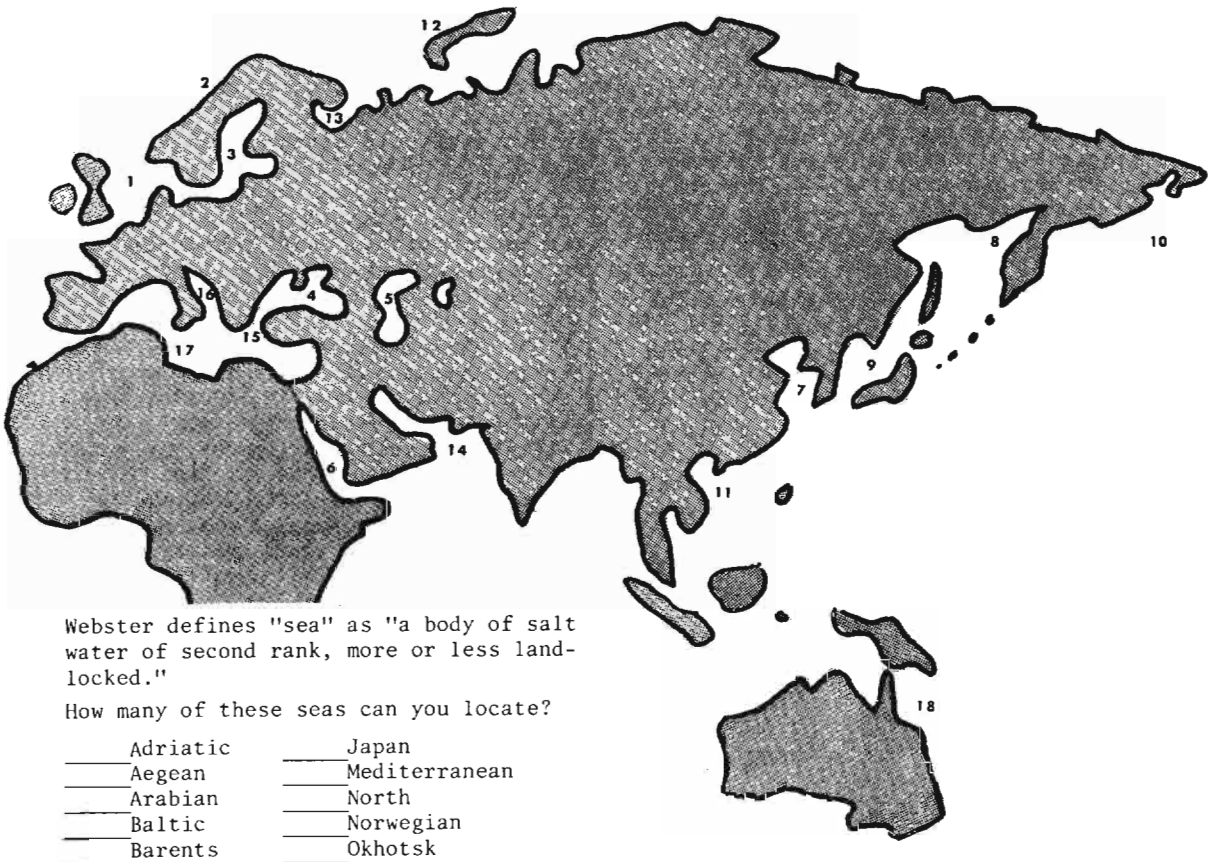
Casting Off

Well, there you have it, folks! Everything you never needed to know about "production." Obviously, in such a short space many things had to be glossed over or skipped altogether. Anyone whose career field was slighted will just have to expand my horizons through an article in this magazine.

~~(TSC)~~

KNOW YOUR GEOGRAPHY

R.G. (Tony) Melzer, D5



Webster defines "sea" as "a body of salt water of second rank, more or less land-locked."

How many of these seas can you locate?

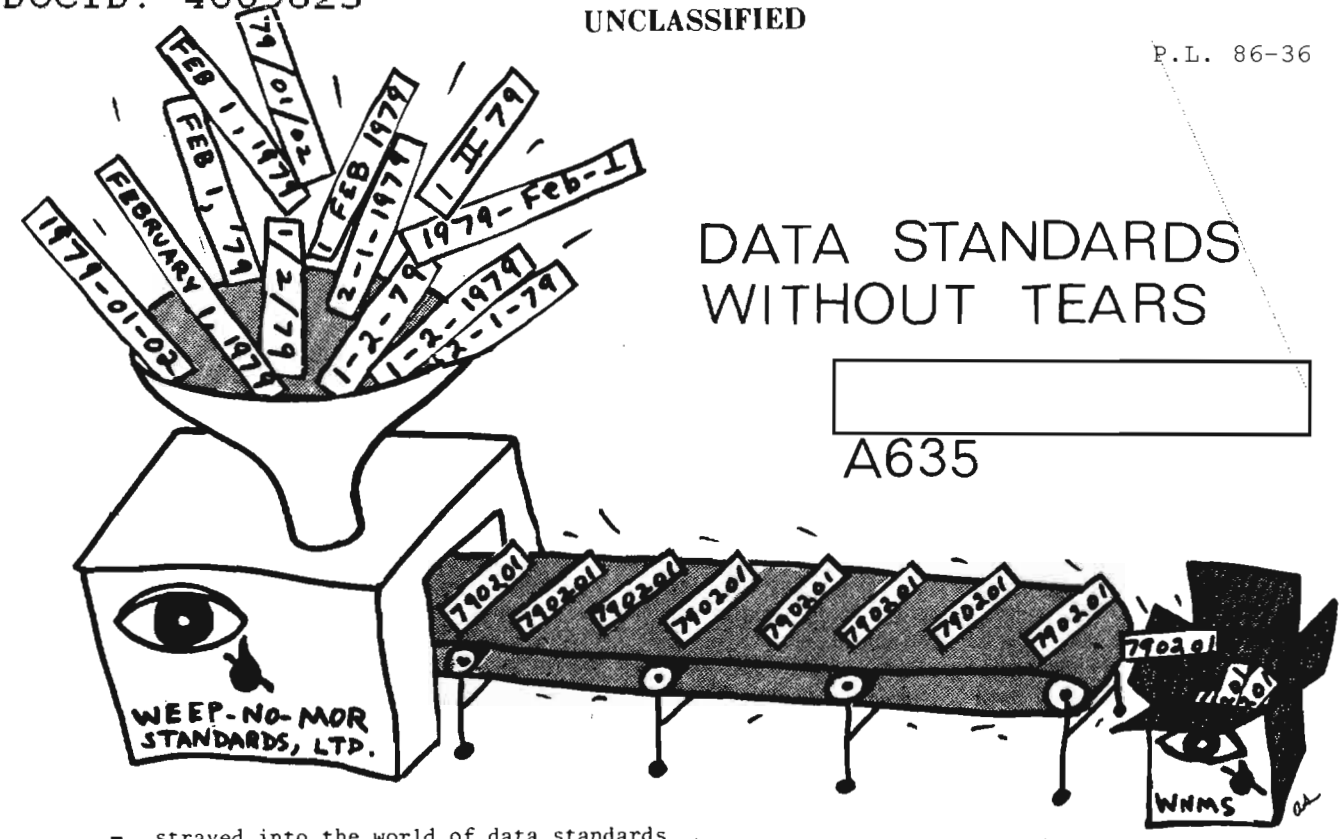
_____Adriatic	_____Japan
_____Aegean	_____Mediterranean
_____Arabian	_____North
_____Baltic	_____Norwegian
_____Barents	_____Okhotsk
_____Bering	_____Red
_____Black	_____South China
_____Caspian	_____White
_____Coral	_____Yellow

Solution on page 21. (U)

DOCID: 4009823

DATA STANDARDS WITHOUT TEARS

A635



I strayed into the world of data standards quite by accident. Probably few do otherwise. As data base design manager for a fairly large project, I was concerned with the creation of a Data Element Dictionary/Directory (DED/D) system, mainly to document file designs and to provide some general-purpose software such as data editing. The establishment of data standards was expected to be a simple and natural product of the Dictionary. This initial naivete was soon shattered when it appeared that the length of time required to coordinate standards with the central authorities are likely to exceed the life span of the project. Even worse, there appeared to be valid reasons why complete standardization could not be enforced within the project itself. What happened was what will always happen. Standards took second place to operational necessity. The project was completed satisfactorily, as was the DED/D. As far as standards were concerned we did our best, turned a blind eye to some abuses, and hoped for better things in the future.

Since then I have talked at length with data standards experts, studied how things are done, and reflected on the experience of the DED/D. My conclusion is that data standards can be achieved, but that our present approach is wrong. We overcomplicate the issues and lose sight of the real requirements; we worry too much about irrelevancies; we view standards as something which not only can be, but must be, imposed in an inflexible, hard-handed manner.

Let's clear our minds and start again. Consider these two statements:

- Everyone agrees that data standards are a "good thing" in theory;
- No one agrees that data standards should be enforced on his project at the expense of operational necessity.

The crux of the problem is that these two truths appear to be mutually exclusive, so that, when faced with the question "to be or not to be standard" we feel constrained to reply either "yes" or "no." A better way would be to answer "Both." We need both to have standards and not to have them. "Standards without tears" means that we want to have our cake and eat it too.

It goes without saying that this cannot be achieved without some degree of magic. On the practical level the magic machine already exists for rendering coarse materials into fine standard gold. It is without doubt the Data Dictionary/Directory. On a more nebulous level a much stronger alchemy is needed to bend our present attitudes onto simpler, more flexible, more realistic paths.

Firstly, let us have a look at the mechanics of using the DED/D to achieve standardization without tears. From the plethora of terms in present use I have chosen two: "data element" and "data field." Forget "subfields," "data chains," "data use identifiers," "use modifiers," etc., At this point they are red herrings. In this simple system the terms are defined thus:

- data elements are "things,"
- data fields are "homes for things."

In other words, a data field is a receptacle for holding a data element, and a data element is mostly what you want it to be, but essentially refers to the content of the data field. Do not worry too much about the exact definitions at the moment. Concentrate on the idea of two domains because I do not believe this to be arbitrary. It is a natural separation and, although apparently simple, is fraught with consequences, philosophical, political, and practical.

The immediate practical consequence is that the structure and functions of the DED/D are greatly simplified and the associated terminology is made clear. The Dictionary section of the DED/D describes "data elements." The Directory describes "data fields," and how they are built into records and files, or how they are used in software. No confusion exists because the Dictionary and the Directory deal with two inherently different concepts. A "data element name" cannot be confused with a "data field name" because the one is the name of the "thing" and the other is the name of the box in which the "thing" is put. Similarly, a "data element abbreviation" is the agreed standard abbreviation or code by which a data element is known, while a "field name abbreviation" is just the name of a container in which data can be housed.

Some important attributes belonging to these two domains are:

DATA FIELD: Data field name
Data field name abbreviation
Field length (actual)
Position in record
Thread from Directory to Dictionary

DATA ELEMENT: Data element name
Data element abbreviation
Data length (max/min)
Definition
Values [DATA ITEMS]
Configuration(s)

The philosophical consequences of the subdivision into two domains relate to the fact that standards are applied initially at the Dictionary level only. The Directory confines itself to describing actual use. The former describes the ideal world; the latter describes the actual world. The "thread from Directory to Dictionary," listed above, links the real with the ideal. Before the hardliners point out that this is not standardization but the avoidance of standardization, it is necessary to stress that this is a starting point only. The DED/D is not just a vehicle in which standards are enshrined for the multitude to gape at. It is the mechanism for developing standards. The success of standardization can be measured directly by the degree to which the data field descriptions in the Directory match with the data element description in the Dictionary. There is no other practical way to tackle the problem. A standards authority cannot confine itself to documenting agreed standards because much of the time these do not exist. Instead the details of actual use should be recorded and analyzed so that new standards can be evolved. Standards will be much more acceptable to users if they evolve in this way from actual use.

Politically the subdivision into two domains is exceedingly useful. The Dictionary may be maintained and controlled by the central authority. Separate Directories can be built in each user area according to user specifications, with a large degree of freedom, saving only that the link from Directory to Dictionary must be present (in the form of some standard number or designator) so that varying data field uses may be related to a single, standard set of data element conventions. When a user builds a new file, he checks first to see if the fields he wishes to use have corresponding data elements defined already in the Dictionary. Say, for example, that he finds the data element name DATE OF BIRTH with the data element abbreviation DATEBRTH. There is a strong possibility that he will adopt the identical name and abbreviation for his data field, thus conforming to an existing standard. But maybe his system hardware or software demands an abbreviation not more than three characters in length. He may then say, "I accept the standard data element abbreviation DATEBRTH, but I must use DOB for my data field name abbreviation."

Two other situations must be catered for: the case of the user who rejects a standard for reasons of personal preference, and the case of a file or a software system which exists before the standard is set up, where the effort required to change it is unacceptable. In the first case, friendly persuasion is called for. In the second, there is no question but that the user wins. His is an overwhelming case against the indiscriminate enforcement of standards. The DED/D system must be democratic, not authoritarian. It is the only reasonable way to proceed. And most people are not rebels. They will accept a standard if they are able to. Thus the DED/D becomes a powerful force towards encouraging standardization whilst being able to accommodate all deviations.

The terms I have been using to express the idea of two domains, "data element" and "data field," are not sacrosanct. The concept matters more than the terminology. There are other words which I rejected earlier as red herrings, e. g., "data chain," "data use identifier." I did not mean to imply that they do not exist, merely that they are of secondary importance. If my "data element" is observed under a microscope it does indeed resolve itself into a number of different types. DATE becomes a data chain made up of YEAR, MONTH, and DAY. DATE OF BIRTH is seen to be a

composite structure made up of the basic noun DATE plus a usage modifier. The mistake is to imagine that this causes any problem. Data Dictionary designers are sometimes bewitched by ideas of levels and hierarchies. The user needs definitions of YEAR, MONTH, DAY, DATE, DATE OF BIRTH, even DATE OF BIRTH OF FATHER, without worrying about type. Keep it simple. Just enter them all into the Dictionary as plain "data elements." There are many easy methods of expressing the various relationships within the Dictionary.

It also appears, on close examination, that the data element is not really the "thing" itself, but the name and description of a "set of things." Thus DAY OF THE WEEK is a set name. The actual members of the set are values such as "MONDAY" or "TUESDAY." These may be called "data items" (or anything else), but, again, this poses no problem. They are simply entered into the Dictionary subordinate to their data element. (Some clarification is needed, however, to determine the exact relationship between data item and data configuration.)

To sum up, standards cannot be created in a vacuum. They must be developed from current usage, and this development cannot be carried out without automated assistance of the type offered by a Data Element Dictionary/Directory system which documents the real world as well as the standards world. There are two ways of tackling standardization: the easy way and the impossible way. We've been trying the latter for some time now. It's time for a change.

(U)

WELL, MAYBE A SNIFFLE OR TWO....

Mark T. Pattie, P13D (NSA DATA STANDARDS CENTER)

P.L. 86-36

Since the topic of [redacted] article falls within the area of responsibility of the NSA Data Standards Center, we sent a prepublication copy of the article to Mr. Pattie, the chief of NDSC, and asked him if he wanted to comment on it. He did.

Ed.

Somehow I have the feeling that I am spending more time writing to CRYPTOLOG than I should, but "Data Standards Without Tears" demands a response. Mr. [redacted] uses words very prettily and if I did not already know better I might think he had made a worthwhile point. However, he gives himself away right in the first paragraph with his ". . . there appeared to be valid reasons why complete standardization could not be enforced within the project itself. . . . Standards took second place to operational necessity." If we change "necessity" to "convenience" I think we might be closer to the truth.

Usually, when someone begins a project he looks around and tries to make use of already existing material (standards?) so he won't have to reinvent the wheel. He then builds upon what is useful to him and attempts to develop new material as necessity demands. Within his own project, though, I would think he would be able to "enforce" standards. Otherwise, he must end with a Data Element Dictionary/Directory that will be anything but standard and reliable.

A DED/D can be a marvelous tool, but it is useful and valid as the material placed in it. The saw, "Garbage in, garbage out" applies here too. That is why I take exception to the reference to the alchemy of "rendering coarse material into gold" which Mr. [redacted] speaks of in his article. The DED/D can provide valuable information about already existing standards and it can also help us pull together elements that ought to be regarded as potential standards. Simply placing material in the file will not automatically make it "gold," though, for it may only be useful within a single project (and, if I understand Mr. [redacted] perhaps only within a piece of a project). Someone would have to work with such material to make it acceptable to another Agency element.

Mr. [redacted] in his castigation of "experts" and "authorities" has really set up straw men for his pot shots. The NSA Data Standards Center has always held that, while we would prefer to see Project Managers use existing data standards, we recognize that individual projects may work without them. Whatever terms they come up with, though, are not standards and should not be regarded as such. We would have to test them out in other uses before we could determine what the Agency status should be. And that, as I pointed out in the previous paragraph, is where the DED/D can be very helpful. It is a tool for us to use. It is not the end-all.

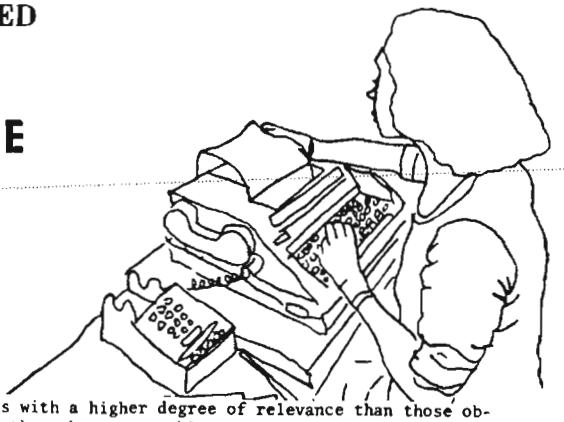
A more detailed comment on "Data Standards Without Tears" is being prepared for next month's issue of CRYPTOLOG. (U)

DOCID: 4009823

LITERATURE SEARCH ON-LINE

T1213

P.L. 86-36



Are you looking for information that may have been published in open-source literature or documentation? An item from an unclassified source? Or an unclassified item published by a government source or by a commercial organization working under government contract? If so, DIALOG may be your answer.

DIALOG is a comprehensive collection of on-line data bases maintained by Lockheed Information Systems, Palo Alto, California. Subject areas include science, technology, engineering, social sciences, business, and economics. Sources of information include research reports, technical reports, journal articles, government reports and publications, periodicals, pamphlets, reviews, monographs, conference proceedings, and books. All data bases are regularly updated to include the most recent information. Additional data bases are being added continuously. All these data bases can be accessed on-line. T12 (Information Services) has several terminals connected to the DIALOG system.

Many of the indexes covered by the DIALOG data bases are subscribed to in hard copy by NSA. These indexes are available for use in the NSA library. DIALOG greatly reduces the time necessary to perform most searches, as compared with manual techniques for searching literature. The accuracy and exhaustiveness of searches performed through DIALOG allow the researcher to retrieve a greater number of documents with a higher degree of relevance than those obtainable through a comparable manual research effort. Because of the savings in research time and the increased thoroughness of the search results, DIALOG is an extremely cost-effective research tool.

A word about the cost of DIALOG. With DIALOG, the customer (government agency, commercial organization, etc.) pays only for the services that are used. Search charges are based on the time the terminal is connected to the computer, prorated to the nearest thousandth of an hour. There is also a charge for each citation printed and mailed to the customer. Rates vary, depending on the data base used. The expense of the DIALOG system has been included in the T12 budget. Although T12 analysts who operate the terminals must be cost-conscious and stay within this budget, they make every effort to provide complete search service for all operational problems.

The following table lists a few of the data bases currently included in the DIALOG system.

Name of data base (producer)	*Information period covered*	*Number of citations (update period)*	*Contents of data base*	*Cost to NSA (on-line connect hour; full record, printed off-line)*
ABI/INFORM (Data Courier, Inc., Louisville, Ky.)	August 1971 to present	65,000 (monthly)	Abstracts of significant articles of interest to MANAGEMENT and ADMINISTRATION from approximately 400 publications in business and related fields. Representative publications are *Harvard Business Review, Dun's Review, Sloan Management Review, Fortune,* and *Journal of Marketing Research.*	$65; 10¢
COMPENDEX (Engineering Index, Inc., New York, N.Y.)	January 1970 to present	600,000 (monthly)	Machine-readable version of the *Engineering Index* (monthly/annual), which provides the ENGINEERING and INFORMATION communities with abstracted information from the world's significant engineering and technological literature. The *EI* data base provides worldwide coverage of approximately 3500 journals, publications of engineering societies and organizations, conference proceedings, selected government reports, and books.	$65; 10¢
INSPEC (Institution of Electrical Engineers, London, England)	1969 to present	1,045,000 (monthly)	The Science Abstracts family of abstract journals, indexes, and title bulletins has been published since 1898. Today it forms the largest English-language data base in the fields of PHYSICS, ELECTROTECHNOLOGY, COMPUTERS, and CONTROL. Foreign-language source material is also included, but abstracted and indexed in English. INSPEC includes the *Physics Abstracts, Electrical and Electronic Abstracts,* and *Computer and Control Abstracts.* The principal subject areas are indicated by the major headings of the unified classification approach developed for the data base (e.g., Atomic and Molecular Physics; Computer Programming and Applications; Computer Systems and Equipment; and Elementary Particle Physics). Journal papers, conference proceedings, technical	$45; 10¢

DOCID: 4009823

			reports, books, patents, and university theses are abstracted and indexed for inclusion in the INSPEC data base. Approximately 2000 journals are scanned, of which 200 are abstracted completely.	
MANAGEMENT CONTENTS (Management Contents, Skokie, Ill.)	September 1974 to present	25,000 (monthly)	Current information on a variety of BUSINESS and MANAGEMENT related topics to aid individuals in business, consulting firms, educational institutions, government agencies or bureaus, and libraries in decision-making and forecasting. Articles from approximately 200 U.S. and foreign journals, proceedings and transactions are fully indexed and abstracted to provide up-to-date information in the areas of accounting, decision sciences, finance, industrial relations, managerial economics, marketing, operations research, public administration, etc.	$55; 10¢
NTIS (National Technical Information Service, U.S. Department of Commerce, Springfield, Va.)	1964 to present	610,000 (biweekly)	Government-sponsored RESEARCH, DEVELOPMENT, and ENGINEERING, plus analyses prepared by federal agencies, their contractors, or grantees. It is the means through which unclassified, publicly available, unlimited-distribution reports are made available for sale from such agencies as NASA, DDC, AEC, HEW, HUD, DOT, Department of Commerce, and some 240 other organizations. State and local government agencies are now beginning to contribute their reports to the file. The data base includes material from both the hard and soft sciences, including substantial material on technological applications, business procedures, and regulatory matters. Many topics of immediate broad interest are included, such as environmental pollution and control, energy conversion, technology transfer, behavioral/ societal problems, urban and regional planning.	$35; 10¢
PAIS INTERNATIONAL (Public Affairs Information Service, Inc., New York, N.Y.)	*Bulletin:* 1976 to present; *Foreign-language index:* 1972 to present	45,000 (quarterly)	Information in all fields of SOCIAL SCIENCE, including political science, banking, public administration, international relations, economics, law, public policy, social welfare, sociology, education, and social anthropology. 25,000 citations taken from more than 1200 journals and more than 8000 books, pamphlets, government publications, agency reports, and other documents are added yearly.	$60; 15¢
PTS DATABASES (Predicasts, Inc., Cleveland, Ohio)	(varies according to file)		PTS (Predicasts Terminal System) maintains a number of BUSINESS-related files which are available on DIALOG. The *EIS Plants* data base provides immediate answers to a broad range of questions concerning the U.S. industrial economy. The *F&S* (Funk and Scott) *Index* cover both domestic and international company, product, and industry information. They contain information on corporate acquisitions and mergers, new products, technological developments, and sociopolitical factors. The *Federal Index* covers such federal actions as proposed rules, regulations, bill introductions, speeches, hearings, roll calls, reports, vetoes, court decisions, executive orders, and contract awards. The *Washington Post* and federal documents such as the *Congressional Record*, *Federal Register*, Presidential documents, and *Commerce Business Daily*, are indexed on a regular basis. The *Predicasts Market Abstracts* data base provides information on acquisitions, capacities, end uses, environment, foreign trade, market data, new products, production, regulations, and technology. Significant information is abstracted from	$90; 20¢

			thousands of newspapers, business magazines, government reports, trade journals, bank letters, and special reports throughout the world.	
SCISEARCH (Institute for Scientific Information, Philadelphia, Penna.)	January 1974 to present	1,820,000 (monthly)	Multidisciplinary index to the literature of SCIENCE and TECHNOLOGY, prepared by ISI. It contains all the records published in *Science Citation Index* and additional records from the *Current Contents* series of publications that are not included in the printed version of *SCI*. SCISEARCH has two important and unique characteristics. First, journals indexed are carefully selected on the basis of several criteria, including citation analysis, resulting in the inclusion of 90% of the world's significant scientific and technical literature. Second, citation indexing is provided, thus allowing retrieval of newly published articles through the subject relationships established by the author's reference to prior articles. SCISEARCH covers every area of the pure and applied sciences.	$70; 10¢
SOCIAL SCISEARCH (Institute for Scientific Information, Philadelphia, Penna.)	1972 to present	490,000 (monthly)	Multidisciplinary data base indexing every significant item from the 1000 most important SOCIAL SCIENCES journals throughout the world and social sciences articles selected from 2200 additional journals in the natural, physical, and biomedical sciences. SOCIAL SCISEARCH includes many important monographs as well. The data base covers every area of the social and behavioral sciences. Unique information retrieval technique: in addition to more conventional retrieval (by words, author, journal name, corporate source, etc.), it is also possible to search by way of the author's cited references.	$70; 10¢
SPIN (American Institute of Physics, New York, N.Y.)	1975 to present	50,000 (monthly)	SPIN (Searchable Physics Information) is designed to provide the most current indexing and abstracting of a selected set of the world's most significant PHYSICS journals. Each month approximately 1400 additional articles from the journals published by the American Institute of Physics, including the Soviet translations, are added to the data base. Author-prepared abstracts enhance the relevancy of retrieval from the data base. SPIN covers all major areas of physics, as well as mathematical and statistical physics, astronomy, astrophysics, and geophysics.	$35; 10¢
SSIE CURRENT RESEARCH (Smithsonian Science Information Exchange, Washington, D.C.)	last two years (e.g. 1977 to present)	180,000 (monthly)	Reports of governmental and privately funded SCIENTIFIC RESEARCH projects, either currently in progress or initiated and completed during the most recent two years. SSIE data are collected from the funding organizations at the inception of a research project and provide a source of information on current research long before the first or progress reports appear in the published literature. SSIE CURRENT RESEARCH encompasses all fields of basic and applied research in the life, physical, social, and engineering sciences.	$90; 20¢

Details on all the DIALOG data bases and further information on how DIALOG can help you can be obtained from:

- T1213, Room 2N090, 5759s;
- T1221, Room 2C051, 3258s; or
- T1233, FANX-III, Room B1B20, 8705s.

(U)

DOCID: 4009823

IN DEFENSE OF THE INDEFENSIBLE:
Notes on the Russian PQE

Emery Tetrault, P16

Although the current Russian-language population at NSA is made up, for the most part, of shy, self-effacing scholars, its members can be uncharacteristically vociferous on the subject of language testing in general and the PQE (Professional Qualification Examination, for anyone who has just returned from 10 years on the dark side of Mars) in particular. This is a healthy phenomenon, but it should not merely assume the form of a diatribe against the pinheads who devise such tests, not because of humanitarian concerns, but rather because such a course of action is ultimately self-defeating. I am convinced that there are some individuals who have failed the Russian PQE (particularly Part I) out of test fright, or, more accurately, out of test repulsion. They have shared so many horror stories about the PQE with their colleagues that it has become for them an insurmountable barrier, a psychological Berlin Wall. As a result, their performance on the PQE may not be consistent with the actual level of their language skills. This is sufficient reason for someone to present at least a factual account of current test practices, if not a spirited psycholinguistic defense of the PQE. I shall limit my remarks to Part I A, the "non-voice," open-source section of this lengthy and occasionally unpleasant process.

For all languages *except* Russian, Part I A of the PQE is made up of a 500-550 word text of the language variety often found on the op-ed page of a newspaper. The test task is to produce a smooth idiomatic translation into English. In reality, few if any test papers realize this standard, but that is a story for an other day and another article.

Up until PQE 13 (July 1976) the Russian I A was like this too. However, someone somewhere began adding up the person-hours involved in running this kind of PQE for Russian. Test preparation was a negligible part of the total, but scoring the test was a nightmare. Grading translations has never been an exact science and, therefore, it was done by a committee -- five senior linguists in the case of Russian. Each grader graded every paper independently, using the approved grading system, and then the committee met to make a preliminary evaluation. Papers were labeled "Pass," "Fail," and "Maybe," regraded during a series of follow-up meetings. and all the Maybes were regraded during a series of follow-up meetings. As the test population for each successive Russian PQE began to reach 120-130, this process started taking so much so-called operational time (not to mention "subbotnik" time as well) that the same someone said, "Enough already!" And so the search for an alternative method began.

This alternative turned out to be a two-part test not unlike the Russian I A that we all know and love today. Early in 1976 we ran a kind of feasibility study with the help of some people who had just taken Russian PQE 12. About 32 hardy souls took an experimental test battery, the results of which were correlated with the PQE, Part I which they had just completed. The correlation was quite high and, more significantly, the first six ranks on the experimental battery were filled with five of the six people who had passed the PQE. The results were good enough for the Language Career Panel and the Russian PQE Committee, and the decision was made to go ahead with the new test forms.

The last two Russian I A exams have represented somewhat of a departure from the forms and procedures first used in 1976. The Russian Completion Subtest has changed very little (although verb pairs are now given in the word lists rather than single verbs), but the Translation Completion Subtest is a substantially different animal from what it was originally. On both subtests, examinees are allowed to use dictionaries (this was not the practice at first).

The Completion Subtest is a text of 220-240 words with 50 words deleted and 70-75 candidates for these blanks given on a facing page. Deletions cover a spectrum of difficulty from the trivial to the nearly impossible. Items can be said to describe a kind of bell curve; most of them are medium-tough with a few easy ones and a few hard ones thrown in on the ends of the spectrum. Items deleted are both syntactic and lexical, both bound and free (recoverable only from situational context). Morphology is tested as a by-product, since most content words inserted into blanks have to be inflected to fit both linguistic and situational context. A brief sample (without word lists) is given below:

. . . Все началось **С**

происшествия. Аварии не

произошло, но обстановка

создалась **опасная**, когда

водитель А. Морозов на автомашине, которая ПРИНАДЛЕЖИТ ____ институту "Госгипроводхоз", при ВЫХОДЕ ____ из тоннеля ПОД ____ Добрынинской площадью не выдержал дистанцик. Во избежание столкновения со ВПЕРЕДИ ____ идущей машиной он резко нажал НА ____ тормоза, и автомобиль развернул поперек ДОРОГИ ____.

This sample shows some of the possible kinds of deletions: bound prepositions (с and на), partially keyed items (принадлежит, выходе, под, etc.), and the more or less free (informational) items (опасная, впереди). Any plausible response other than the keyed answer is tried out on a native speaker. Scoring is simply two points per blank, with half credit given for a good selection incorrectly inflected (aspect choice is considered a selection, not an inflection).

The Translation Completion Subtest has gone through a lot of growing pains as a test form. At first it was thought that the underlying translation should be as different structurally from the original Russian as the law allows. However, the tendency now is to produce a reasonably smooth English text and let the natural differences between Russian and English (particularly the differences in informational structure as marked by element ordering) do the job without too much outside help. Once again we have a brief sample, a Russian text followed by a partial translation.

Сегодня криминалисту нельзя быть просто криминалистом. При расследовании дел он часто попадает в такие ситуации, где нужно глубоко знать физику, химию, биологию, психологию... Поэтому в современной криминалистике появляются более узкие профессии.

The criminologist today cannot simply limit himself to criminology. In the course of investigating a case he will often find himself in the kinds of situations which require a thorough knowledge of physics, biology, medicine, psychology. . . Consequently, a number of subfields have been emerging within the field of modern criminology.

The weighting or point value attached to each blank in the translation depends on the segment of Russian text being processed, not on any particular number or combination of English words. Thus any response that fits the context given and that accounts for the semantic features of the original Russian is correct and, in actuality, there are many different correct answers in this form of test, just as there would be many different correct translations of any given text.

When a different set of tests is used for each PQE cycle, there is justifiable concern about the reliability and validity of such a testing procedure. For this reason, all the potential test forms for a particular PQE cycle are first tried out on a small number of certified linguists and the best example of each test type is selected for the PQE. In the case of the Russian Completion Subtest, a native speaker of Russian is also asked in fill in his or her responses, a practice which we initiated with PQE 17 and which has proven to be extremely useful. This form of pretesting addresses the issue of content validity.

Predictive validity and reliability are ensured by having a small group of controls, four or five certified linguists, take the PQE along with the test population. The performance under actual testing conditions of this control group is then used to set the Pass/Fail cut. These individuals who make up the control groups for each PQE are performing an extremely valuable service and they should be encouraged and, if possible, rewarded by such bodies as the Language Career Panel and the A Group Language Advisory Committee. Maybe a steak dinner wouldn't be too far out of line.

There is no doubt in anyone's mind that the testing procedures now used for Russian PQE Part I A save time and money. The results of PQE 17, for example, were in the hands of the Language Career Panel in a matter of a few weeks rather than 3 or 4 months and with little or no time taken away from line functions (other than the time used by control groups to take the PQE along with the test group). But, obviously, cost effectiveness is not enough. Part I of a language PQE must, above all, measure the right level and the right kind of

DOCID: 4009823

language proficiency. I believe it does and I believe that the individuals who have passed this form of PQE actually meet the minimum general standards set forth in existing descriptions of L-3 (Minimum Professional Proficiency). With the exception of a small number of people who may be spooked by the format, most people who fail this exam do so because they don't know Russian. Any other comparable measure of proficiency would produce the same results. The errors I see repeated 50 or 60 times on a hundred papers can be traced to certain features of Russian structure and lexicon and not to any particular arrangement of blanks on a test form.

There is a tendency in discussing the current method of assessing L-3 general language skills in Russian to forget what this method replaced. Translation testing, as it was practiced by Russian PQE committees, is not beyond criticism (for a discussion of the rationale behind the Agency's first Russian-language certification examination on 6 and 9 October 1967, see "The Russian-Language Certifying Examination," by Arthur J. Salemme, *QRL -- The Quarterly Review for Linguists*, Vol II, No. 2, February 1968). It was hard for the PQE committees to judge the relative difficulty of one text over another and, as a result, one PQE could be and most certainly was more or less demanding that the one preceding it, a fact which was demonstrated by abrupt changes in the Pass rates, which fluctuated between 11 percent and 40 percent. While no particular Pass rate is sacrosanct, abrupt shifts in the percentage of people passing a PQE usually mean that test standards have changed, since the collective proficiency of the NSA Russian-language population doesn't change all that rapidly.

The present PQE can and should be improved and it is the duty of the Russian-language community (if there is such an entity) to keep the heat on the Language Career Panel to do so. One way to achieve this goal is for supervisors to encourage their professionalized Russian linguists to participate in the PQE process, both as pretest subjects and as controls. In this fashion, most of the bugs would be shaken out before 150 people see them and test validity and reliability would also be greatly enhanced. This is one area in which a relatively small investment of "operational" time would yield immediate results.

No one is suggesting that current PQE procedures are above criticism, constructive or otherwise, but such criticism should never be uninformed. To simply dismiss the whole process as the product of warped minds or pointy-headed theories is to perform an ultimate disservice to the cause of professionalism, a cause to which all but the most cynical proclaim their allegiance at every opportunity. (U)

LETTER TO THE EDITOR

To the Editor, CRYPTOLOG:

If CRYPTOLOG had never existed except to print [redacted] article ("Some Tips on Getting Promoted," December 1978), the service to NSA employees would have been worth the entire CRYPTOLOG budget since its birth. I was very pleased to see such an important message receive the publicity you gave to it.

The Personnel Summary can be a potent effective document for promotions, rotations, and overseas assignments.

I am convinced that in the last 18 months at least three 'extra' G4 people have been promoted by the NSA boards -- because their Personnel Summaries were carefully written and reflected work well done.

Within G4, I use the Summaries to help with our rotation program.

Yesterday I reviewed the Personnel Summaries of 11 applicants for an overseas position.

Of all the papers that attend one's career at the Agency, I believe that the Personnel Summary is the most important and influential.

CRYPTOLOG is a great publication. Has been for years. My personal files contain several selected articles clipped from previous CRYPTOLOGs. But [redacted] article will be so useful, I ask that you send me 100 copies. I will circulate them in G4. I will make them required reading for touring interns. I will use them for my class in Promotion Theory.

Thank you and [redacted] for a valuable service to the Agency.

Charlie Bostick, G4 (U)

Editor's Comment:

Charlie's note was just the first of several requesting additional copies of [redacted] article. Anyone else wishing to obtain additional copies may do so by calling the CRYPTOLOG office, ext 3957. (U)

P.L. 86-36

DOCID: 4009823

LET'S NOT FORGET OUR CRYPTOLOGIC MISSION

J. Gurin, R5

An acquaintance once described to me how he had to stand by helplessly while his very own company swelled its ranks with what he terms "nonproductive" people. He had started the firm himself, to cash in on an idea he had developed for monitoring the public's reaction to TV fare. A psychologist, he teamed up with engineers, statisticians, programmers, and others to develop and market the product, which did very well. It is now widely accepted by the television industry as one of the most reliable indicators of how well any program is doing.

But as the company grew and prospered, he found that he was required to add all sorts of people who had little or no relation to the basic mission of the enterprise. He needed a legal staff, public relations people, personnel counselors, etc., and admitted to some resentment at having to keep people on the payroll who played no role in improving the product or selling the service. "I am the one who does the hiring and firing," he said, "and yet I can't control the addition of nonproductive types to my payroll."

Another illustration of this sticks in my mind. In a magazine article a few years back, a retired Dean of Men from a small, respected private school wrote about his reaction during a visit he made to the school some 20 years after retirement. He was saddened to find that, although the size and abilities of the student body were about the same and the courses they took hadn't changed much, the non-teaching staff had increased greatly. He was certain, he wrote, that the quality of the graduates and of the instruction was much the same as it had been in his time. So why all the extra staff? Naturally, the tuition costs reflected their presence, but he could find no justification for them in the output of graduates.

Much the same thing happens with any institution, and this Agency is no exception. I suppose that at one time in our history, as the work force came through the gate at the end of a day, all but a few had been directly involved with processing intercepted traffic. Most likely the categories of traffic handler, crypt clerk, cryptanalyst, traffic analyst, and translator made up the bulk of those coming through, and after one added clerical help and a handful of bosses, all but a few were accounted for. But we have changed -- and I'm not saying that it is better or worse today, just different.

There are many reasons why a large organization takes on people who have no direct involvement with the basic mission of the organization, and many of those reasons are convincing enough. But there is always the danger that the overhead will grow disproportionately large, and that the sound economic balance of the enterprise may be threatened and productivity undermined.

In a recent article in *The Washington Post*, Charles Peters, former bureaucrat and now editor-in-chief of *The Washington Monthly*, attacked the federal bureaucracy, citing some horrendous instances of waste and inefficiency. No doubt many of his charges could be refuted by those in possession of the facts, but some sounded authentic, or at least familiar. One of his tactics was to distinguish between what he called "essential work" and the work performed by those "employees with titles like Planning Analyst, Schemes Routing Specialist, Manager of Creative Services, Social Priorities Specialist, Suggestions Awards Administrator, Fringe Benefit Specialist, or Confidential Assistant to the Confidential Assistant (all real titles)."

It would be difficult, without detailed information, to defend jobs with such seemingly frivolous titles, although it is perfectly reasonable to assume that some could be justified to the satisfaction of the taxpayer. Perhaps we have jobs at NSA that would sound frivolous to those not privy to the jargon of bureaucracy or to that of SIGINT or COMSEC activities.

Given the propensity of any institution to add positions which may be only distantly related to its mission, what is needed is some way of fixing and maintaining a balance between those employees engaged in the basic mission or missions of the organization, and the other employees. To be more specific, it would be advantageous to be able to grade all employees by the relevance of their particular jobs to the fundamental mission of their organization. Having done this, it should then be possible for management to ascertain trends and to manipulate the balance with some precision.

But how do we define those jobs which are

most closely related to the mission of NSA? And isn't the degree of relatedness a subjective judgment rather than a measurable quantity? And, as Bob Cooper (recently returned to DDO from CSEC) pointed out to me at lunch the other day, the Agency surely has more than one basic mission.

Yes, yes, it is a complex problem. It certainly requires subjective judgments, but then so do all hiring and staffing actions. What scientific rules govern tables of organization? Promotions? Grade levels for jobs?

So what I suggest is that each job in NSA be rated to indicate how close it is to a basic mission of the Agency. This is *not* to imply that jobs which are not closely related to a basic mission are not important. Far from it. It is just that the distribution of jobs must be a matter of proper *proportion*, and that proportion should be visible if it is to be kept under control. If, for example, DIRNSA proposes to absorb a personnel cut with minimum impact on SIGINT production, he should be able to specify with precision the types of jobs among which the cuts should be made, or in which they should not be made.

Suppose we assign the number 1 to those jobs which call for direct participation in the production of SIGINT product. Cryptanalysts, traffic analysts, appropriate programmers, and others who are *directly* involved in getting the product ready for the consumer should be on jobs that carry the 1 label. First-line supervisors who are not doing the work themselves, in addition to guiding others, should be on jobs carrying a 2. Typists, and others who assist in this kind of operations, should be on 3 jobs. The farther the job is from the basic mission, the higher the number. To repeat: the only function of the number is to indicate how close the job is to the basic mission, not to indicate the value of the operation. A security guard performs a vital function, but the number attached to his job would be high, since his function is distant from the basic mission. Warehousemen and medical personnel perform vitally important functions, but their jobs are not basic to the mission.

The value of a system of job-grading such as this would lie in providing a display of the distribution of personnel resources by mission-relatedness. One could even envision deriving a number from the system which would represent the average of all the job numbers, multiplied by the number of incumbents. It would be useful, for example, to know that if our average was 6.22 last year, it climbed to 6.93 this year. Could the increase be explained away to the Director's satisfaction, or should he set as a goal the reduction of the number so as to assure himself that we are not losing sight of our real purpose in existing and spending the taxpayer's money?

Several of my more cautious friends have suggested that this article should be credited to an anonymous author, to protect me from possibly furious reactions. But I protest, in advance, that it would be reasonable to expect that my own job would be given a very high number, as it should, although I consider it a useful one. (U)

SOLUTION TO NSA-CROSTIC No. 21

(CRYPTOLOG, January 1979)

W. Averell Harriman, "[Soviet-American] Relations," *Cryptologic Spectrum*, Summer 1976, Vol. 6, No. 3:

> "In April 1945 I...[came] back to brief President Truman on...Stalin... I found he didn't need [very] much briefing because he had read the Yalta documents with great care and all the post-Yalta cables... He was a great student of history and that was...why he was able to deal with these new and complex problems with such skill." (U)

CLARIFICATION

The November 1978 issue contained an item stating that the Language Career Panel will award Certificates of Achievement to military linguists who pass the Language Proficiency Test. Effective 1 October 1978 any military linguist who receives a passing score on the LPT will receive a certificate; those who score five points or more over the passing grade for *each* of the two sections of the LPT will receive the certificate "with honors."

Military linguists who passed an LPT prior to 1 October 1978 should apply to the LCP for a certificate. The composite score requirements given in the November issue can be misleading and should be disregarded.

For further information, contact Capt [redacted] M36, ext 8267s. (U)

NSA-crostic No. 22

By D.H.W.

The quotation on the next page was taken from the published work of an NSAer. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS

A. Hill; western city

B. Patronizing (one word); prisoner going downstairs (2 wds)

C. Removing facial hair again

D. Complete, thoroughgoing (comp)

E. ——— bridge, in physics

F. Allen or Frome

G. Holmes' response when asked to identify the citrus plant: "A ———" (5 wds)

H. Mournful

I. Annoy; tease

J. ——— and needles (2 wds)

K. Thomas or Horace

L. Plants of the nightshade family

M. Involving the lending of money at excessive interest

N. Hometown of the comic strip trolley car

O. Undergoing evolutionary change

P. Strong surface current flowing outward from the shore

Q. Sleepwalkers

R. Broad sash, often worn with formal attire

S. Logical sponsor for TV series about NSA (2 wds)

T. Play (1961) and movie (1966) by Thomas Bolt, about Sir Thomas More (5 wds)

U. Chinese dentist time (comp)

V. Fellow; roughening of the skin from exposure

W. Clumsy; ungraceful (comp)

WORDS

201 139 182 127 225

239 4 188 29 178 163 223 209 40 15 64 58 206

120 23 162 100 1 51 28 60 168

75 80 176 16 125 41 246 111 55

31 249 14 195 21 84 81 57 160 42

200 91 132 220 170

2 63 102 243 8 26 49 164 167 179 150 193 82

71 89 233 118 136 151 32 46

154 7 44 169 180 114 159 70 25 197

72 115 103 134 203

108 186 235 190 221 144

251 240 247 231

68 218 61 211 129 59 37 117

157 19 194 149 56 97 181 245

241 106 128 174 50 224 184 213 155 196 148

30 147 145 34 122 242 214 175

199 204 110 74 121 222 232

212 77 219 205 226 109 156 85 237 192 27 248 140

104 39 152 3 250 119 166 54 142 35

43 228 107 113 76 69 238 86 67 12 185 38

141 78 116 9 98 24 33 133 53 130 172 93 66

165 45 18 5

227 10 126 6 137 22 171 105 216 96

13 177 48 79

62 47 95 191 131 36 234 229 124 101 143

DOCID: 4009823

X. Copy of a document made on specially treated paper

Y. Plant louse

Z. Donizetti opera (4 wds)

236 92 88 207 52 158 17 20 11

198 87 208 187 94

189 153 202 230 73 99 183 65 138 146 90 217 123

83 135 215 173 210 161 244 112

1 C	2 G	3 R	4 B	5 T	6 U		7 H	8 G	9 T	10 U	11 X	12 S	13 V	14 E	15 B
	16 D	17 X		18 T	19 M	20 X		21 E	22 U	23 C		24 T	25 H	26 G	27 Q
28 C	29 B	30 O		31 E	32 G	33 T	34 O	35 R		36 W	37 L	38 S		39 R	40 B
41 D	42 E	43 S	44 H	45 T	46 G	47 W		48 V		49 G	50 N	51 C	52 X	53 T	54 R
55 D	56 M	57 E	58 B		59 L	60 C		61 L	62 W	63 G	64 B	65 Z		66 T	67 S
68 L	69 S	70 H	71 G	72 I	73 Z		74 P	75 D		76 S	77 Q	78 T	79 V	80 D	81 E
82 G	83 Z		84 E	85 Q	86 S	87 Y	88 X	89 G	90 Z		91 F	92 X	93 T		94 Y
95 W	96 U		97 M	98 T		99 Z	100 C	101 W		102 G	103 I	104 R	105 U	106 N	107 S
108 J	109 Q	110 P	111 D	112 Z	113 S	114 H		115 I	116 T	117 L		118 G	119 R	120 C	121 P
122 O	123 Z	124 W		125 D	126 U	127 A		128 N	129 L	130 T	131 W		132 F	133 T	134 I
135 Z		136 G	137 U	138 Z	139 A	140 Q	141 T	142 R	143 W	144 J		145 C	146 Z		147 O
148 N	149 M	150 G		151 G	152 R	153 Z	154 H	155 N		156 Q	157 M	158 X	159 H	160 E	161 Z
162 C	163 B	164 G	165 T		166 R	167 G	168 C	169 H	170 F		171 U	172 T	173 Z	174 N	175 O
	176 D	177 V	178 B	179 G		180 H	181 M	182 A		183 Z	184 N	185 S	186 J		187 Y
188 B	189 Z	190 J	191 W	192 Q	193 G	194 M	195 E	196 N	197 H		198 Y	199 P	200 F		201 A
202 Z	203 I	204 P	205 Q	206 B		207 X	208 Y	209 B	210 Z		211 L	212 Q	213 N	214 O	215 Z
	216 U	217 Z	218 L	219 Q		220 F	221 J	222 P		223 B	224 N	225 A	226 Q	227 U	228 S
229 W	230 Z		231 K	232 P	233 G		234 W	235 J	236 X	237 Q	238 S	239 B	240 K	241 N	242 O
243 G	244 Z	245 M		246 D	247 K		248 Q	249 E	250 R	251 K					D.H.W.

 (Answer next month.) (U)

with ground forces ...
hald the cases. Perhaps the results are st...
marked "Indefinite Retention".

[redacted]

P.S.

The two articles on Project SPELLMAN* prompt me to add this p.s. to those tales of the ill-fated P.S. Mine was a passing involvement -- some few hours, I recall -- but an involvement that allegedly contributed to the demise of the project.

I gather that ASA did put a great deal of time, effort, and money into the project, for, as I heard sometime afterwards, the $3 million project had been scrapped. Don't ask me to vouch for that figure. All I know is that at the time $3 million was a whole lot of money compared to a transcriber's salary. I probably just saluted in reaction and went back to transcribing chores. Those were the days when a transcriber was paid to transcribe and . . . I think I should not say more.

What was my brief encounter with SPELLMAN? Well, I was a transcriber (of questionable repute) and a typist of some proficiency. Oh, I might just as well say it -- there probably weren't two or three others at the time who could do as well at the keyboard, especially on the IBM Selectric with the Cyrillic keyboard. So, along with the tin ear, which everyone had to some degree or other, I had a pretty good reputation as a typist. Thence I was selected to participate in the "SPELLMAN test."

[redacted]

*A. J. Salemme, "I Remember SPELLMAN," CRYPTOLOG, July-August 1978; [redacted] "More B.S.", CRYPTOLOG, October 1978.

[redacted]

I don't know what criteria were used to grade the test. The results of my test were compared with the results of six SPELLMAN persons who had taken the test on their stenotype machines. (Six persons, six parts, 36 scores.) Holly informed me later of the outcome -- I had scored better in 35 of the 36 cases. Amazing? I don't know. But if the recovery rate, however quantified, of a tin-ear transcriber, especially EO 1.4.(c) P.L. 86-36 [redacted] with a typewriter was that good, what worth was the SPELLMAN concept? I don't know what Holly and others concerned with the project expected from my taking the test. I have a notion the ploy was to drive another nail in the SPELLMAN coffin. To be perfectly fair and objective about it, perhaps someone who could not type quite so rapidly should have been chosen to take the test.

[redacted]

I don't recall exactly. My vague recollection is that Gary, who had prior knowledge and experience with [redacted] bested the SPELLMAN participants in over half the cases. Perhaps the results are still available. . . in that box marked "Indefinite Retention."

~~(C-CCO)~~

DOCID: 4009823

LETTER TO THE EDITOR

To the Editor, CRYPTOLOG:

In the December issue [redacted] "To Whom It May Concern" describes a sad situation but leaves out an even sadder part of it. I believe he was present in the auditorium when those who were "selecting their supporting casts" were giving their pitch to NSA personnel who might be interested in working in the new organization. When I left the auditorium I had the sinking feeling that I had been listening to a couple patent medicine barkers.

The top man introduced himself as someone who had no previous position in the Intelligence Community and he said that he looked upon that fact as an asset. No predispositions, I suppose. When he finished his spiel, one of his chief assistants took the floor to describe the actual jobs he was trying to fill. He said he had had a brush with the intelligence part of his former agency when he first went to work there, but succeeding jobs took him far afield. He left a number of questions unanswered but I thought that, with the proper selection of his personnel, the concept might work.

Several months later the second man returned to NSA to interview those who were interested in hearing more about the jobs. In my session with him I learned that he had been using the intervening time to fill the higher positions with people similar to himself, with little or no experience in intelligence work. What he was seeking, he said, was assistants who would provide the proper support to his choices for the top jobs. I thanked him but said I was not interested, for I fear I would find it too frustrating to have to explain the facts of life in intelligence gathering to someone who should already have that knowledge.

I am sure that this organization was set up with the best of intentions but I am also sure that the actuality will in no way resemble the ideal. Like Lou, I am not optimistic.

Mark T. Pattie, Jr.
Chief, NDSC (U)

IN CASE YOU'VE ALWAYS WONDERED...

I was talking not too long ago with one of the young ladies of the Agency, who was telling me about a recent encounter. Seems she had been in the ladies' room washing her hands when one of the members of the custodial force came in, and walked up to the wash basins. She looked at all the little paper towel half-moons lying on the basin rims and on the floor and muttered something about all the thoughtless people who dirty up the restrooms. P.L. 86-36

My friend tried to suggest, quite gently, that maybe the reason all those semicircles keep tearing out of the edges of the paper towels is that the towel dispensers are loaded too tightly at refill time.

"Nonsense," said the custodian. "The reason all those pieces tear out is that people grab for the towels when their hands are wet." dhw (U)

Solution to

KNOW YOUR GEOGRAPHY

by Tony Melzer, D5

1	North	10	Bering
2	Norwegian	11	South China
3	Baltic	12	Barents
4	Black	13	White
5	Caspian	14	Arabian
6	Red	15	Aegean
7	Yellow	16	Adriatic
8	Okhotsk	17	Mediterranean
9	Japan	18	Coral

(U)

ウゲーツ

CLA — NCS FEATURE FOREIGN FILM FOR FEBRUARY

UGETSU

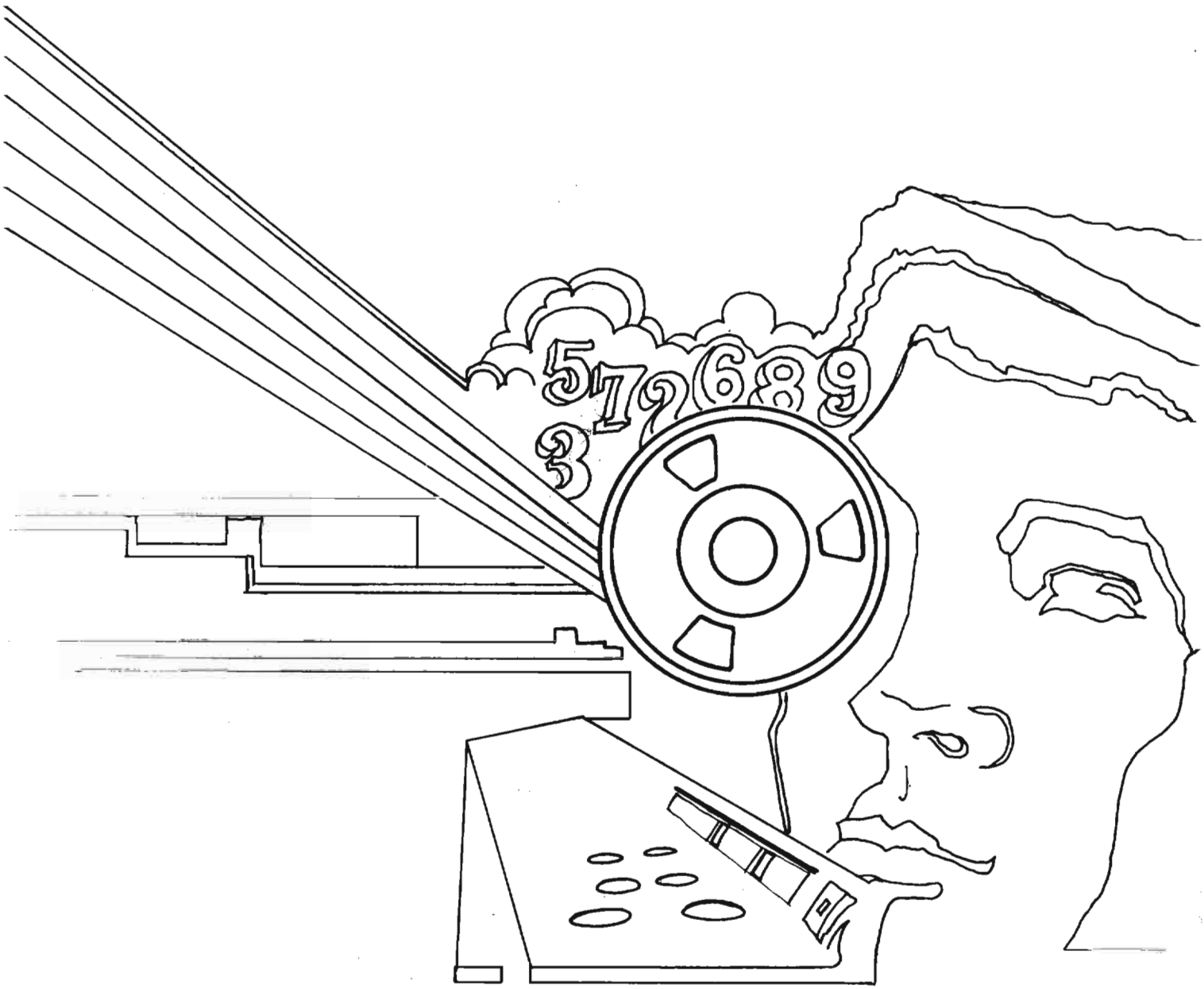
JAPANESE SOUNDTRACK WITH ENGLISH SUBTITLES

THURSDAY, FEBRUARY 8TH AT 0930

FRIEDMAN AUDITORIUM (U)

P1-Dec 78-S3-27141

~~TOP SECRET~~



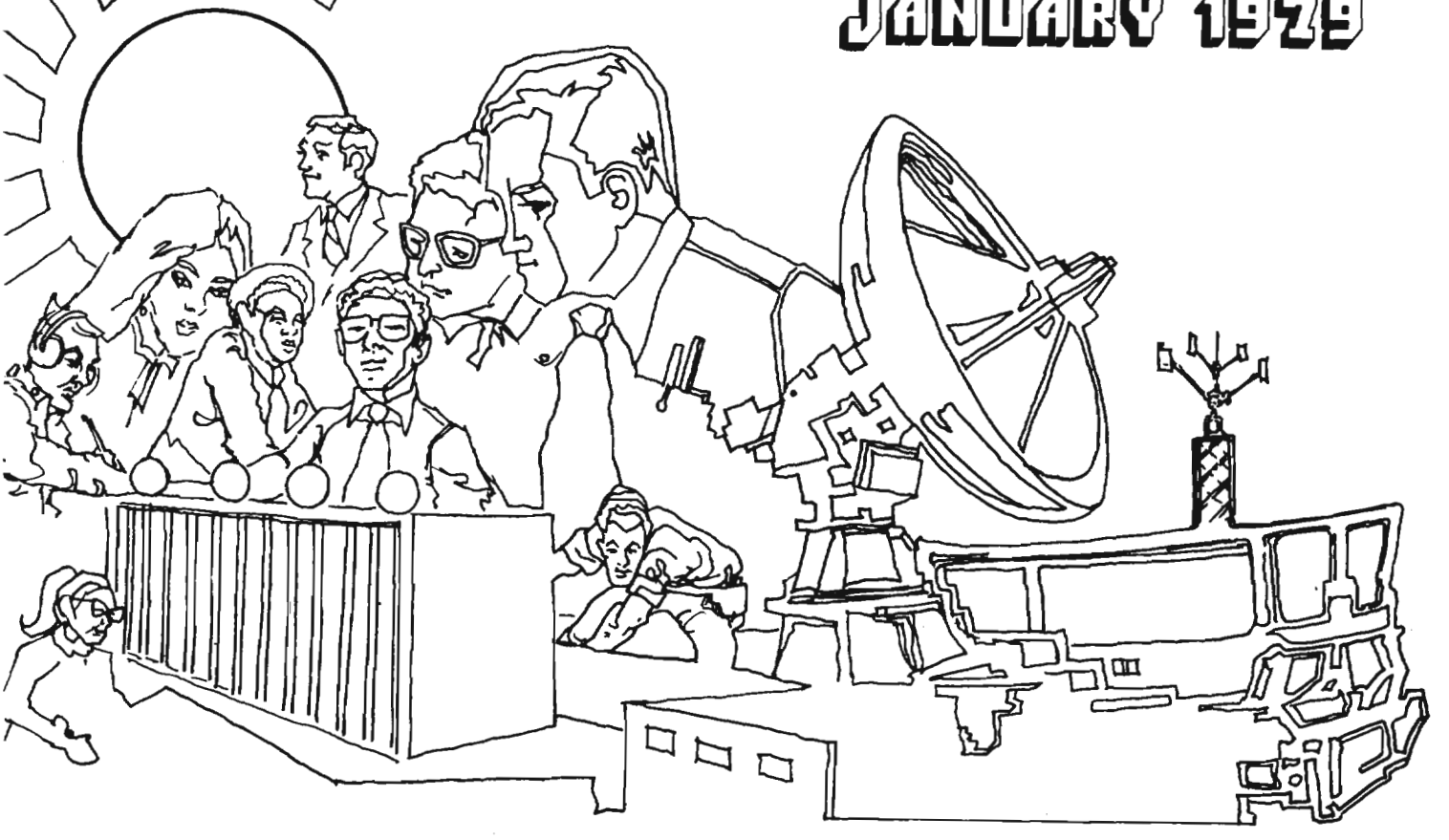
DOCID: 4019659

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JANUARY 1979



SOLIS -- A VEHICLE IN SEARCH OF AN ENGINE....[redacted].....1
HOW DO YOU TELL THESE TWO CLOWNS APART?.....6
THE RETURN TO H.F.....[redacted].....7
SECOND SIGHTING.....Sue Donym.....12
JAPANESE TRANSLATION AT A.H.S.....13
T-VISION: MEDIUM OF THE FUTURE.....[redacted].....17
REFLECTIONS AND RECOMMENDATIONS.....Vera R. Filby.....19
HUMAN FACTORS NEWSLETTER.....[redacted].....21
NSA-CROSTIC No. 21.....David *H.* Williams.....24
GOLDEN OLDIE: ON OPENING "STATISTICS".....Marjorie Mountjoy.....26
HENRY CEMENT & PHANTOMS OF OPERA(tions) ....[redacted].....27
CLASSIFICATION CORNER: IT'S PARTY TIME!....[redacted].....28
PUBLISHER'S MESSAGE.....29

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 2 JAN 2009~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526,MDR Case # 54778

DOCID: 4019659

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. VI, NO. 1 JANUARY 1979

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (3957s)

Collection.....[redacted] (8955s)

Cryptanalysis.....[redacted] (4902s)

Cryptolinguistics.....[redacted] (5981s)

Language.....[redacted] (8161s)

Machine Support.....[redacted]II (5303s)

Mathematics.....[redacted] (8518s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Taurone (3573s)

Production Manager.....Harry Goff (5236s)

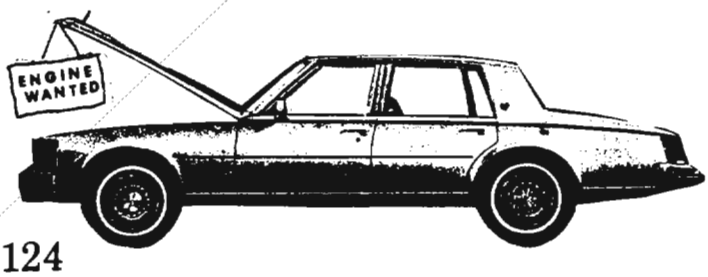
P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4019659

P.L. 86-36

SOLIS - A Vehicle in Search of an Engine



[redacted] T124

An Agency wit once remarked that "SOLIS has a Volkswagen engine in the body of a Cadillac." This statement evokes its share of nods and smiles. But why? What is it about this rather absurd little statement that made it humorous to SOLIS aficionados? The answer is that this metaphor had in it the germ of truth, and many hearers recognized this truth and could appreciate the way in which the wit expressed it.

The metaphor was first voiced in 1972. Today, nearly seven years later, it remains apropros.

Let us, then, examine the system and the metaphor. What features of SOLIS remind one of the sensuous charms of a Cadillac body by Fisher? What is about the system that caused the wit to describe it as a grossly underpowered vehicle? To answer these questions it will be necessary to understand SOLIS -- its purpose, its organization, its operational philosophy -- and to take some measure of its performance as compared to the system developers' own loosely defined goals and expectations.

SOLIS -- the *S*IGINT *O*n-*L*ine *I*nformation *S*ystem -- was born out of the experiences and frustrations of the HARVEST End-Product File Operation. For those of you who don't remember, asking a question of the HARVEST End-Product File could sometimes qualify as one of life's unique experiences, with the system's response ranging from "everything you never wanted to know about all subjects except the one you were really interested in" to "nothing at all." More often it was something between these extremes. But, since questions against the HARVEST File were batched and run only once or twice a week, you never knew what the response would be until you got a call to "Roll up your wheelbarrow" or to "Try again next week." Under these circumstances it is no wonder that SOLIS was developed as a viable alternative. It is only surprising that it took so long.

Before describing SOLIS in detail it would be well to impart some understanding of what is meant by the term "End-Product" or "SIGINT product." Storing and retrieving the product is, after all, what the HARVEST End-Product File (and its successor, STRONGBOX) and SOLIS were and are all about.

[redacted]

It was the sincere hope and belief of the system's first designer/planner that SOLIS could operate with a completely automatic indexing routine. After all, our experience with human indexers had not been a smashing success. It is difficult to get editing billets, it is difficult to fill them, and human editors are consistently inconsistent in their approach to editing. The SOLIS developer planned to avoid all these problems by developing a sure-fire, self-priming, automatic indexing routine. He would prepare indexing algorithms for the product serial, the date-time group, the "from" and "to" lines, the XXMM line, the content control code, and the other external data of potential usefulness to a retriever.

[redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36
DOCID: 4019659

[redacted]

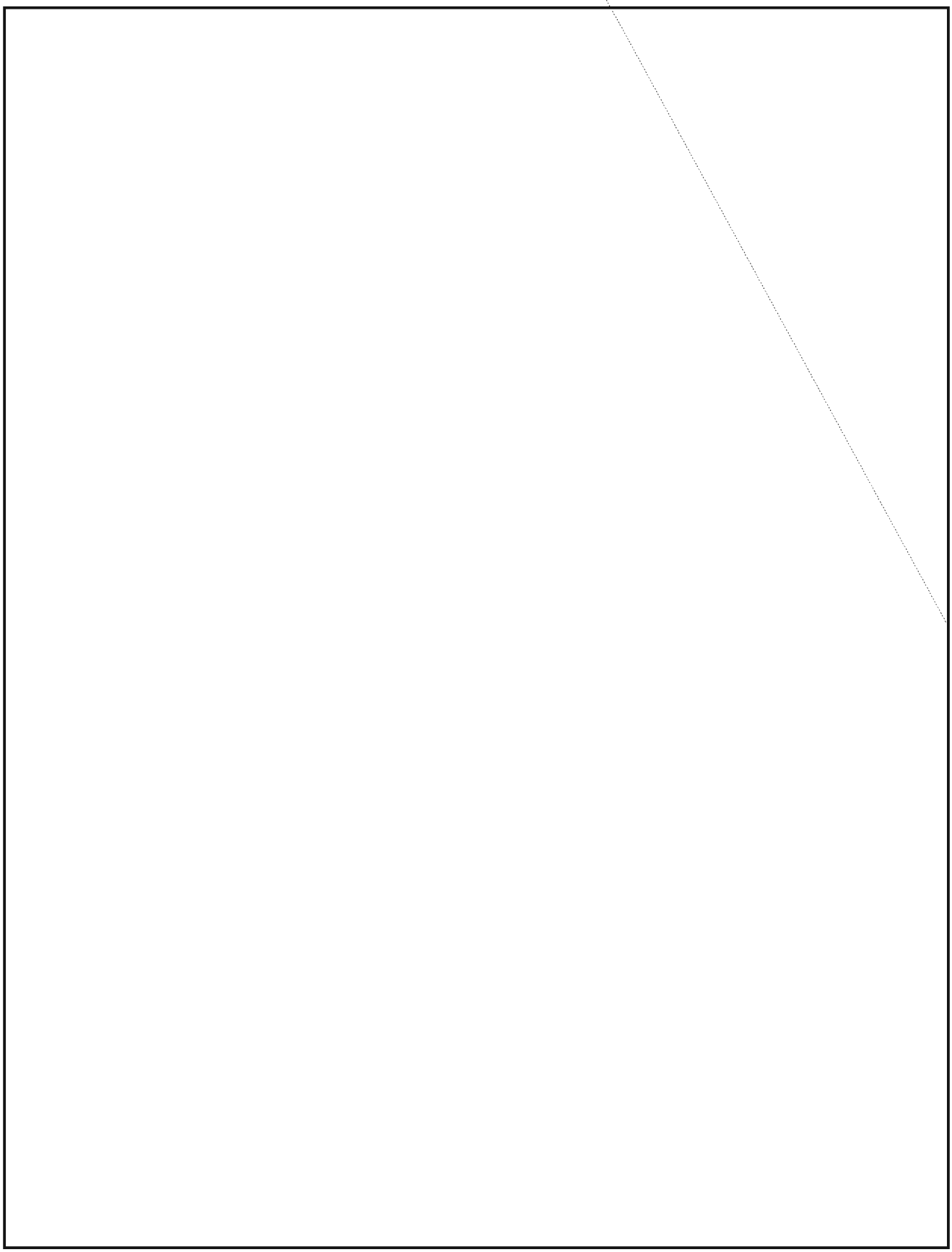
SOLIS Programs and Procedures

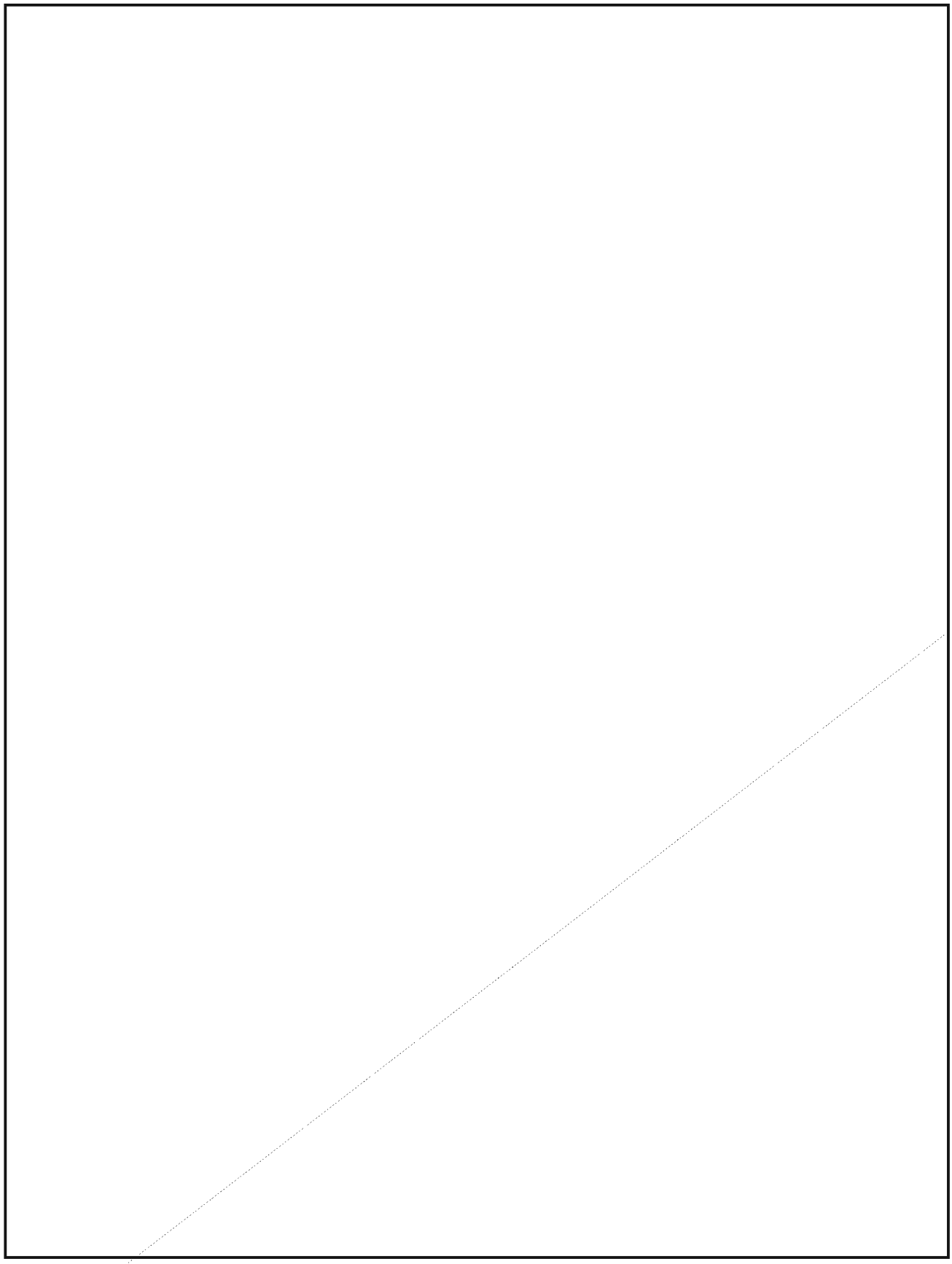
SOLIS today is a multitiered structure of programs and procedures that fit together into a harmonious whole.

[redacted]

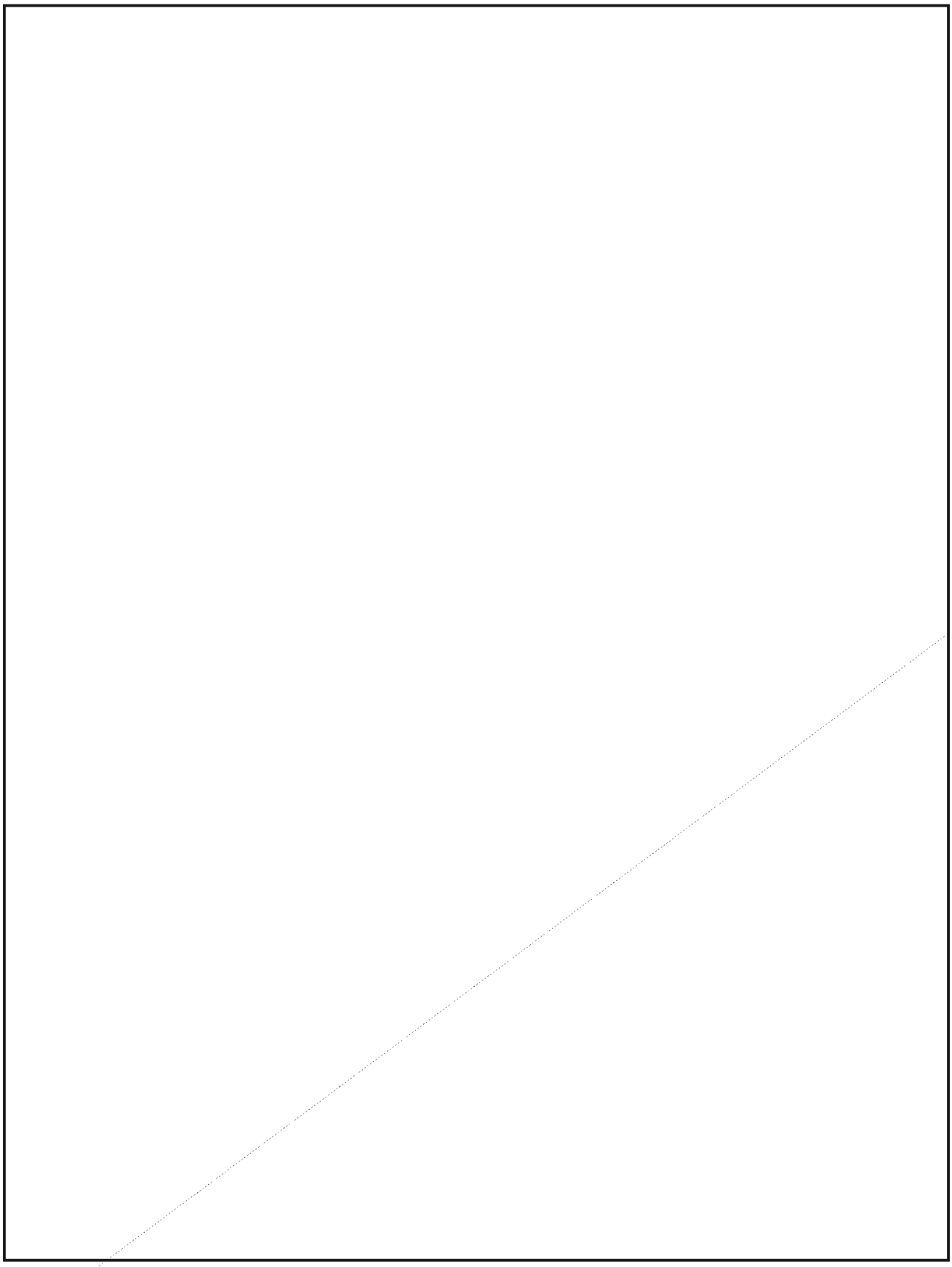
EO 1.4.(c)
P.L. 86-36

P.L. 86-36
EO 1.4.(c)





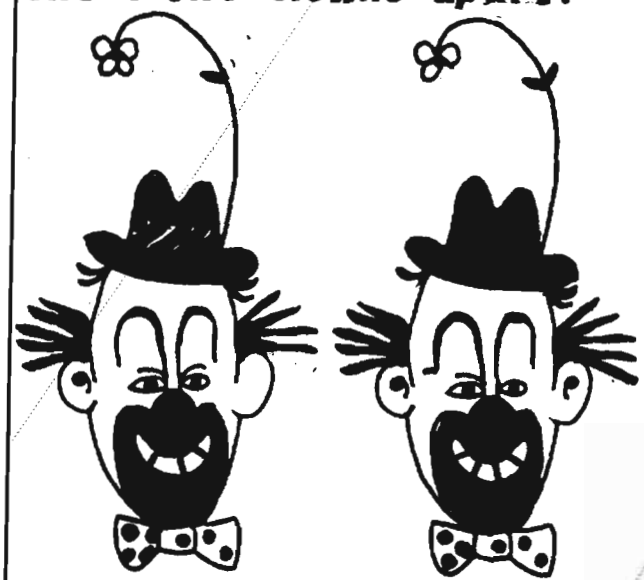
P.L. 86-36
EO 1.4.(c)



P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)

How do you tell these two clowns apart?



There are ten differences between these two clowns. Can you find them?

Incidentally, some CRYPTOLOG readers are unaware that there are two Dave Williamses whose names have appeared frequently in CRYPTOLOG. One often gets blamed or praised for what the other does, so maybe we ought to call attention to the differences in the names and the contributions made by each Dave. Especially since one of them is going to become the Editor-in-Chief of CRYPTOLOG starting next month! (see page 29).

David H. Williams

[redacted]

David H. Williams has written an occasional item for CRYPTOLOG (most of his things appear in more prestigious Agency publications), but he is famous among CRYPTOLOG readers for his NSA-Crostics.

[redacted] (can you imagine what it must be like to be the one-hundred-and-eleventh person to bear the same name?) is our Machine Support Editor. He used to write more when he was the editor of the now defunct C-LINERS. For the past couple of years he has been helping CRYPTOLOG by persuading other people to submit articles on machine problems to the magazine.

Now, then, which Dave Williams is going to become CRYPTOLOG Editor in Chief starting with the February issue? It's the one with the H! The one with the [redacted] is going to continue as the Machine Support Editor. Maybe we can persuade [redacted] to write an article of his own as a test, just to see who gets the compliments! And, remember, if you like or dislike a definition in an NSA-crostic, don't tell [redacted] It'll be the wrong Dave!

(U)

~~(S - CCO~~

SOLUTION TO NSA-CROSTIC No. 20
(CRYPTOLOG, December 1978),
By David *H.* Williams
(see next column)

Frances Blank, "It's Got to Get Out Today!", CRYPTOLOG, April 1977:

"One difficulty arose with electronic computers designed to translate from one language to another. The headline 'Mary suspended for youthful prank' was fed into a computer, translated into Russian, and then back into English. It came back as 'Mary hung for juvenile delinquency.'" (U)

P.L. 86-36

THE RETURN TO H.F.

[redacted] P13

U.S. tactical forces intend to return to the use of HF radio for vital long-range communications, because of the vulnerability of satellites and cables. This conflicts with existing U.S. plans to give away the HF fixed service frequencies to the Third World at WARC 79*, on the assumption that the United States will rely on satellites from now on. A central issue is the military control of their own communication facilities, which is threatened by Congressional demands that the military *lease* satellite services, and no longer design and build military comsat systems. The technical issue is that satellite-era technology applied to HF makes HF cheaper and more reliable than satellites for certain kinds of traffic.

HF at AFCEA

Major General W. Hilsman, USA, in describing the "Electronic Battlefield of 1985" at AFCEA 1978 (1978 conference of the Armed Forces Communications and Electronics Association) included HF as a principal transoceanic medium to supplement cable and satellite for Army tactical needs. In reponse to a question about the future of HF in tactical communications, MGEN Hilsman -- who directs the tactical communications program -- said that a study 2 years ago had eliminated HF because satellite links were so much easier for the operator, but that he had completely "reopened the HF question." The field commanders like satellites, but realize they are highly vulnerable or may have long outages or even be canceled, so Hilsman is now training operators on SSB HF. Neil Birch, of C^3I, followed this by saying that DoD is *not* "down on HF" and currently runs a "cemetery net" in NATO, and DoD is now looking at meteor-burst and adaptive-HF links. Birch had earlier spoken of HF as one of the triad (satellite, cable, HF) for a much-needed net of worldwide secure voice using 2.4 KB digital PARKHILL on analog voice encryption. Dr. N. McAllister, O/CNO, in speaking of Navy C^3 for the future, noted that HF, employing new modular equipment afloat which will use digital filtering to extract signals from shipboard noise, is part of the "long term" Navy plan. He noted that there is keen competition between U.S. and EEC equipment, and said this was a primary area to achieve U.S.-NATO interoperations in equipment, communications, and operations. Cost is a key factor, and the Navy has recently had a FLTSAT canceled by Congress before it was launched because its costs were thought unfavorable compared to leased comsat services. Dr. Scheder of Rockwell, in reviewing future technology development for tactical communications, noted that HF could be greatly improved by using special IC digital processing to do frequency filtering of HF carriers to get rid of EMI on board ships, and to reject jammer energy. The Army expects to reduce the use of tactical voice traffic in the forward area -- even to the point of considering *no* voice -- because they cannot afford narrowband jamproof secure voice, but can afford jamproof and reliable data radio links which are necessary for fire control. Microprocessors and frequency-hopping radios with text displays and small keyboards will make this practicable as well as cheap -- and some of this equipment (e.g., RACAL MA 4230, 4231 auto morse sender/receiver/display) already exists.

The interest in HF and in data traffic instead of voice is not purely talk. The AFCEA exhibit, displaying the latest in military communications equipment in over 400 booths, was notable for displaying a variety of very modern HF equipment -- in over 20 booths -- including several major companies which have been making military satellites. It appeared that these manufacturers were alert and well informed about the U.S. military's interest in HF.

Navy HF Exercises

The U.S. Navy in the Mediterranean area shuts off its satellite from time to time to force the Navy operators to use their HF links. So far this has resulted in stress and traffic backlogs of a week or more, but the Navy is persisting in trying to resurrect HF operations. Presumably, foreign SIGINT finds the HF episodes interesting. The Navy MARS organization has built up a cadre of about 3500 to 4000 Navy amateurs who are given military frequencies to operate on, just to keep *some* HF capability. These MARS nets operate with SSB voice and NFSK printer to keep the operators trained and to keep the HF frequencies in use. Because of cochannel interference in the Mediterranean area, the operators much prefer the satellite links, but the Navy -- having had a recent FLTSAT program canceled -- cannot afford to become completely dependent on satellites. The MARS operators practically never use morse, but the NFSK printers -- also widely used on maritime circuits -- use filters as narrow as morse. These NFSK printers have replaced morse on most civil maritime mobile circuits, with much higher traffic capacity.

P.L. 86-36

*World Administrative Radio Conference, Geneva, 1979 -- see "Callsigns and WARC 79," by [redacted] CRYPTOLOG, May 1978.

LEASAT vs. HF

The LEASAT problem is also an important factor, for Congress feels that Defense monies can be saved by eliminating dedicated military satellites and requiring that the military departments lease satellite services from the commercial carriers. LTGEN Paschall, USAF, criticized this strongly, pointing out that the host country PTT would not allow a U.S. commercial-satellite link into Diego Garcia, while a military satellite would have been negotiated with the corresponding Defense Ministry. The tactical forces do not want to be dependent on foreign commercial satellites, and U.S. commercial satellites cannot downlink into foreign areas. Senior military officers declared forcefully at AFCEA that "lease vs. buy" was about equal in cost, but that the central issue was that the military had to control its *own* vital facilities, and had to use leased services as a backup for low-priority traffic. With telecommunications policy-making now shifted to NTIA in the Commerce Department, any new dedicated communications facilities used by DoD will be subject to policy control by NTIA, OMB, and OSTP, according to Executive Order 12046, and this gives further motivation for the U.S. military departments to reconstitute their HF capabilities, for U.S.-NATO tactical communications are not now subject to NTIA control by Executive Orders 11556 and 12046.

HF at ICC-78

However, a few weeks before the declarations of interest in HF radio at AFCEA, CAPT. J. E. Weatherford, USN (Ret.), who was a Navy frequency manager for 31 years, and a member of OTP until a few months ago engaged in WARC 79 preparations, declared at the International Conference on Communications (ICC-78) in Toronto that the United States expected to *give up* its fixed HF channels to the Third World at WARC 79 as part of its bargaining position. HF, he noted, would suit the southern-hemisphere countries very well. He also noted that the U.S. view was that northern-hemisphere countries could generally close down their HF fixed circuits because they had extensive satellite and cable circuits. For the United States, this would clearly be military HF frequencies, for there is not much nonmilitary U.S. fixed HF. The southern hemisphere, Weatherford said, was "starved for HF." He said "spectrum sharing" was crucial, and noted that elimination of local navaids such as Shoran and Decca, etc., was planned. However, *expansion* of amateur radio frequency bands was under consideration because the amateur world was growing internationally and the Third World countries had found amateur radio very useful for disasters and emergencies because, among other things, northern-hemisphere "hams" have given them enormous voluntary support in relaying and servicing messages, clearing all frequencies, and helping in every way. The South American countries in particular found the use of HF ham nets saved them the cost of emergency nets, and the long DX lets them work at uncluttered higher HF bands. Worldwide these are about a million hams, who operate all kinds of HF links by pooling a small portion of the HF spectrum, and knowledge of this high utility has impressed the governments in the LDCs (less developed countries) with the flexibility, independence, and low cost of HF communications.

Weatherford spoke authoritatively, outlining the OTP (now NTIA) position on the issues. He noted that the radio regulations were due for a major reworking at WARC 79, and that the non-government use of radio was going to dominate the U.S. position at WARC. The United States needs the support of the "nonaligned" nations to achieve its WARC 79 goals, and most of these countries are in the southern hemisphere. The position of the Third World LDCs is that they want to eliminate IFRB registration dates, and claim bands of spectrum for their own proposed future uses, which claim has been strongly resisted by the United States and the other Western industrial nations. At WARC 1974 the United States took exception to a provision of the treaty reducing U.S. shore station assignments. At WARC 1977 on satellite broadcasting, which culminated in the "one country -- one frequency" principle and in orbital slot limitations, the treaty is so unsatisfactory that President Carter will not send it to the Senate for approval. Now this political clash over the radio spectrum is to be resolved at WARC 79 by U.S. negotiations which will "trade off" HF frequency assignments which the U.S. tactical forces intend for major tactical backup. The U.S. position for WARC 79 was completed on 31 May 1978 and there was an SPM preparatory meeting on 23 October 1978 to consider the technical bases for WARC 79. The next GWARC will not occur until 1999, so WARC 79 will set the framework for radio usage and allocation for the rest of the century.

Technical Developments

There has been significant development in HF equipment, practices, and traffic growth over the last 15 years, while the U.S. military has virtually let their HF systems stand still or dwindle out of existence. Hence much U.S. military HF equipment and technique must be updated to modern low-cost digital electronics. Siemens predicts considerable growth in stations and traffic -- particularly data traffic -- for HF. Improved techniques such as SELCALL and channel pooling have reduced unscheduled message delays from hours to minutes over HF mobile links. Error rates as low as 10^{-5} and 10^{-6} on long links are regularly obtained by ARQ

and error-central coding -- rivaling telephone lines. In the United States, HF can connect directly into the telephone nets. Where Al telegraphy of 30 years ago took a KHz of bandwidth to send 12 wpm (about 5 bps), modern NFSK and PSK systems regularly send at rates close to 1 bit/Hz, i.e. 100 baud NFSK in a 170 Hz SSB subchannel, or 3000 bps on a 20-tone 75-baud QPSK 3000 Hz SSB channel. This represents a 100- to 200-fold improvement in use of a single link, and the actual gain is even greater because of much greater accuracy and full utilization of equipment. In addition to transmission improvements, better propagation forecasts, antennas, channel sounders, filters, etc., allow many more conventional carriers to operate concurrently at incomparably low cost. Siemens notes that a "marked increase has been achieved within the last few years in telegraph and data traffic, mostly over small radio stations which offer a maximum of economy." It is certain that any modern HF tactical radios developed for the U.S. military will very shortly become a demand item in world trade and technology transfer, and will spread worldwide as comsats have.

In addition to conventional HF traffic, military spread spectrum systems have flourished to support strategic weapons systems and other crucial links. HF spread spectrum transmitters can send chip-coded waveforms with bandwidths up to 20 percent of carrier, and frequency hoppers can span megacycles between pulses, with frequency stabilities of one Hz. The signals are jamproof, undetectable, and a hot export item. WARC 79 will consider the introduction of spread spectrum signals into the nonmilitary and civil sectors.

The Policy Conflict

The fundamental conflict within the U.S. policy-making apparatus over HF was reasserted at EASCON 78 in September 1978, at an IEEE WARC meeting in October 1978, and in a *Washington Post* editorial on 21 October 1978. At EASCON 78 Captain Boslaugh, USN, of NAVELEX, outlined a plain for much increased U.S. Navy use of HF. The ELOS (Extended Line of Sight) HF ship-to-ship system will be the *primary* communication channel for fleet tactical communications over ranges up to 300 miles, and will resist Soviet HFDF or jamming. Long-haul HF will be used to back up shore/ship satellite links. The Navy, having shut down HF stations to get money for satellite programs, is now putting them back into operation because it cannot get money for dedicated satellites. Captain Boslaugh outlined a broad program of new equipment development for data and digital voice over HF. He also declared that no one could predict what would happen at WARC 79, but that frequency managers in the Pentagon feared the Navy might lose some of its resources, which could damage ELOS and other vital programs. He also predicted that WARC would have the greatest effect on the long-haul HF communications.

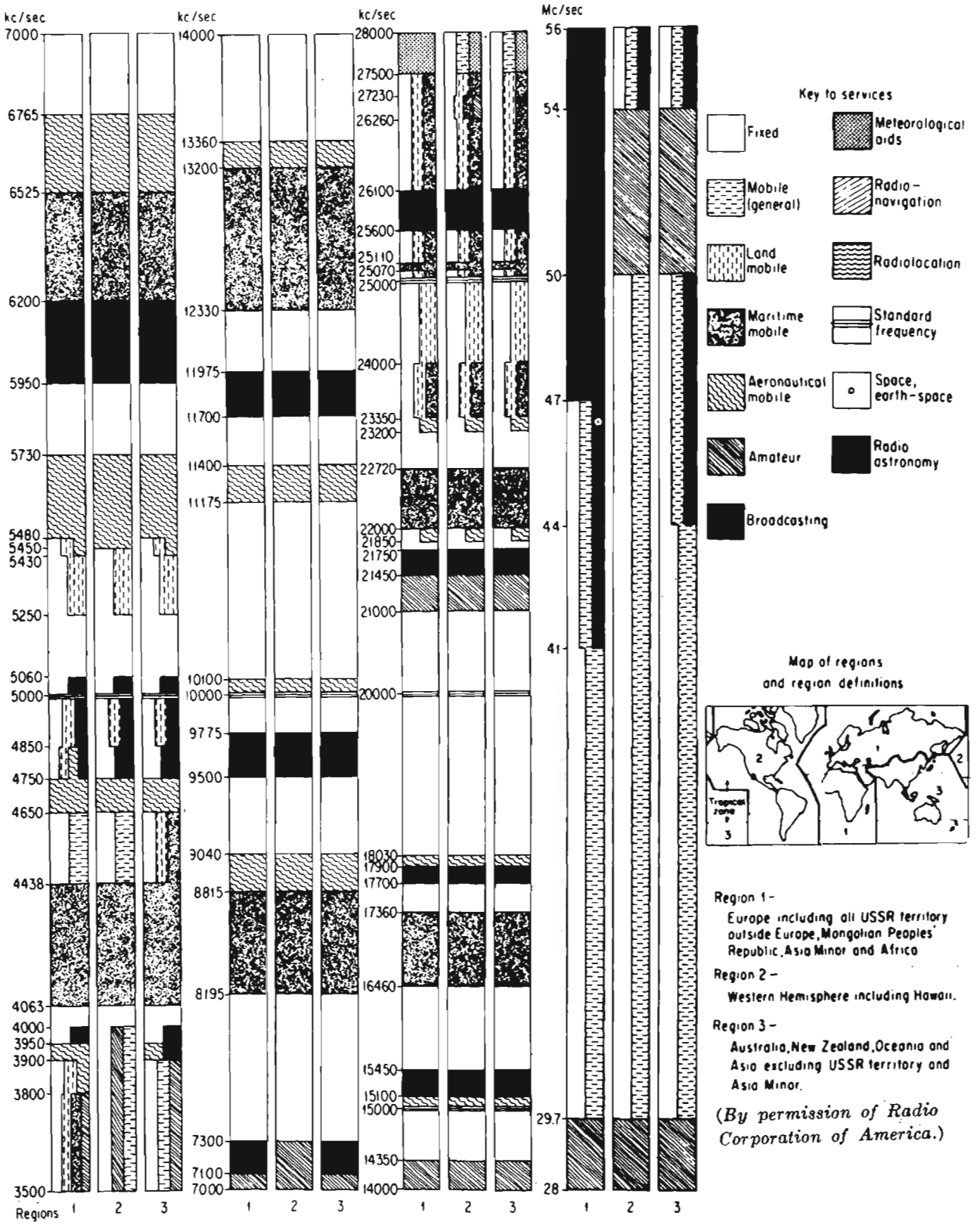
At an EASCON 78 seminar on C^3I given by N. Birch of OSD, HF links were consistently shown as part of the triad of cable, satellite, and HF to give redundant C^3 links.

At another EASCON 78 meeting on Frequency Management directly concerned with WARC 79, Leo Buss of NTIA and L. Petak of FCC both downplayed HF as a matter of secondary importance at WARC, on the basis of responses to the NOIs. However, R. Shrum of the State Department, who had visited over 50 countries as part of the State Department's WARC preparations, gave a completely opposite view at the same meeting. He declared that the three top-priority matters at WARC 79 for the LDCs were "HF, HF, and HF." His paper in the Conference Record stressed the same point and emphasized the political importance of HF allocations to the LDCs. Shrum predicted that HF would be the "most contentious issue" at WARC 79.

The NTIA and FCC spokesmen claimed that the use of HF for fixed point to point circuits was going down because of satellites and

Present ITU band (kiloherts)	Existing service	Proposed ITU band (kiloherts)	Proposed new service
4438-4650	Fixed mobile except aeronautical mobile (R)	4438-4560	Maritime mobile.
5060-5250	Fixed	5200-5250	Do.
5250-5430	Fixed land mobile	5250-5300	Do.
6765-7000	Fixed	6950-7000	Amateur/amateur satellite.
7300-8195	do	8000-8195	Maritime mobile.
11975-12330	do	12130-12330	Do.
13360-14000	do	13360-13410	Radio astronomy.
13360-14000	do	13950-14000	Amateur.
14350-14990	do	14350-14400	Do.
15450-16460	do	16310-16460	Maritime mobile.
17360-17700	do	17360-17410	Do.
20010-2100	do	20010-20230	Do.
20010-21000	do	20950-21000	Amateur/amateur satellite.
22720-23200	do	22720-22855	Maritime mobile.

NOI-5 (WARC 79): "Portion of the spectrum proposed for reallocation to [Fixed Services]." (*Federal Register*, Vol. 42, No. 104, May 31, 1977, p. 27758.)



(By permission of Radio Corporation of America.)

Radio-Frequency Allocation and Assignment (excerpted from *Communication System Engineering Handbook*, Donald H. Hamsher, Editor-in-Chief, McCraw-Hill Book Co.).

cables, and hence were convinced that the United States could "trade off" the HF frequencies for LDC support on other issues. Other well-informed parties present, including a former NATO frequency manager, claimed the opposite, viz.: that HF use was increasing. The disagreement on this basic fact seems to stem from the data base used, and the NOI comments. The IFRB listings show that the use of fixed HF links for *public correspondence* has indeed gone down because of satellites. The U. S. users, e. g. AT&T, predicted a decline in fixed HF usage for public correspondence for the same reason. However, the IFRB data do not reflect what is actually happening in HF, for diplomatic and military and other *non-public* users are steadily encroaching on every unused HF channel and the ex-NATO frequency manager claimed that he combed the IFRB list for idle channels, assigning them ad hoc to meet the intense demand. Shrum said that many countries used HF for domestic links and never filed the usage with the ITU. The continuous sale of NFSK printer and other efficient modulation equipment suggests that the users are passing more and more traffic, while IFRB only registers the *proposed* usage, not the actual traffic intensity . The result is that U.S. WARC policy is being formulated from an unclassified data base which does not show the non-public usage, domestic usage in other countries, unregistered usage, the effects of new equipment, or the projected usage by U.S. and NATO military communications.

The NTIA view of HF as a bargaining chip, based on "declining usage," was repeated on 13 October 1978 by Buss at an IEEE meeting on WARC. A *Washington Post* op-ed column on 21 October 1978 by G. Kroloff, formerly of the Senate Foreign Relations Committee, also advocated giving up HF bands to the Third World, while a speech by Senator H. Schmidt (R-N.M.) chided U.S. WARC preparations for being left to technicians who were not protecting U.S. policy and economic interests (*Satellite Communications*, September 1978).

The final U.S. position must be completed and sent to Geneva by the end of January 1979 and the most basic facts and decisions about HF and its importance to the United States are still unsettled. The military users view HF as integral, to tie together many nets and to back up and reconstruct nets of all kinds in case of outages or war damage to other circuits, while NTIA and FCC see nonmilitary policy issues about broadcasting, radio astronomy, satellite sensors, and other non-HF matters as more important.

The Communications Act of 1978

The difference in point of view between U.S. military communicators who want dedicated facilities which they can control, and the NTIA-FCC WARC team which apparently wants HF frequencies to dispose of as a bargaining chip, will be intensified if the newly issued *Communication Act of 1978, H.R. 13015* is enacted before WARC 79 as expected. This Bill, drafted by former TV newsman Van Deerlin, would transfer most of the FCC functions and all of the NTIA functions and people to an independent agency, the National Telecommunications Agency (NTA). NTS will do policy-making for *all* U.S. telecommunications, including DoD. It will control all frequency allocations for government and nongovernment users, and will resolve all interagency telecommunication differences. NTA will prepare and manage U.S. participation in international telecommunications conferences, and will develop plans, policies, and programs for government telecommunications. NTA will serve as the principal advisor to the President on telecommunications issues and policies and may absorb the functions of any government agency which relate primarily to development or implementation of telecommunications policy (including privacy). In particular, NTA will coordinate development and operations of emergency telecommunications systems, and will participate in the development and operation of national-security telecommunications systems. Unlike the 1934 Act, this new Bill, H.R. 13015, has *no* war-powers provisions corresponding to 47 USC 606, so that the military departments, or the President, cannot take over or control radio or civil telecommunications in a war emergency or a war. This will have the effect of limiting the military services to the frequencies and facilities they have at the start of a war, or which they are able to lease under NTA guidance, and this could affect the renewed U.S.-NATO commitment to HF -- possibly by forcing much greater joint use and sharing of U.S.-NATO military frequencies under agreements that lie outside of NTA's scope.

Prospectus for HF

Despite the internal U.S. situation, the prospects for growth of HF traffic for military, commercial, diplomatic, maritime, aircraft, weather, news-agency, security-forces, emergency nets, etc., and even for scientific data and economic aid, seem irresistible. The improvements in radio and processor technology, and low-cost displays, will bring the cost of equipment down markedly, and greatly improve traffic handling for messages and data. Many different kinds of traffic will flourish, including voice, narrow-voice, data, fax, TTY, morse, slow-scan video and graphics, telemetry, telecommand, etc. Improvements in weapon guidance can assure destruction of U.S. and NATO fixed trunks and switches, and most satellites cannot withstand EW. Hence, existing communication nets must be discounted for war fighting. On the other hand, the resistance of HF nets to EW and to nuclear bursts

DOCID: 4019659

and blackouts is better understood than 15 years ago. With microprocessors and memories to interface between the users and the tricky HF circuits, easy and reliable communication to any point can become a commonplace. Traffic demand will encourage brevity codes, and data compressors, and channel pooling. In 1963, HF traffic was estimated by ITU at several million wpm. NAE (National Academy of Engineering) in 1972 estimated that a 19-fold growth in HF channel usage was possible by better technique. Current state-of-the-art technology could give data traffic over more than one million different links simultaneously. at total traffic rates above 500 billion words per day -- about 10^4 greater than the WW II Army ACAN net.

The demand, technology, mass market, and allocation-usage arrangements are all coinciding and WARC 79 will be a major factor in determining how fast this "modern HF" traffic develops.

(U)

SECOND SIGHTING

By [redacted]

Some time ago -- well, actually, a *long* time ago -- we traffic analysts had a word in our vocabulary that we enjoyed using. It was a good word, and we enjoyed using it because it expressed exactly what was meant. Other people could use the word too -- it wasn't jargon at all.

Everything went well for the word for a number of years. Writers used it, and readers understood it. It wasn't controversial, either. After a while, though, a group of newcomers began writing reports about traffic analysis, and they used *another* word to express the same concept.

We commented that their word, a perfectly good word itself, was not exactly correct when used in a TA context. They countered that *our* word was a no-good word because it wasn't in any dictionaries and their word was a good word because it *was* in dictionaries. They were correct when they said our word wasn't in dictionaries, but we insisted our word really was a good word, because it was a compound word and we had followed rules for forming compound words. Besides, the two words (our word and their word) are pronounced differently -- that means they couldn't possibly be the *same* word. Not only that, but there are lots of NSA words that aren't in any dictionaries.

Neither side gave in. We used our word and they used theirs. Whenever we could, as editors or prepublication report reviewers, we changed their word to ours. Their feelings were ruffled and we had many arguments, often quite loud ones.

The other-word people began to spread like fungus throughout the building, and some of them were in positions to change *our* word to *theirs*. Now *our* feelings were ruffled and, again, we had many arguments, often quite loud ones. One argument was so loud that a decision had to be made about which word to use. A disinterested third party at NSA, caught unwillingly in the argument, asked a disinterested fourth party on a high-level staff to make the decision. He did! He, or some of his staff or a committee, decided that a *third* word would be used. Traffic analysts here, on ships at sea, in the air, on foreign soil, and everywhere gradually began to use the third word. We weren't too happy with it because it looked like a misspelling of that *other* word, but all went reasonably well. At least we weren't having those arguments any more. All continued to go reasonably well until that third party, the very one who asked for the dispute to be settled, took some papers to a *very* high-level staff to be signed by a *very* high-level person. A member of the very high-level staff read the papers, saw the third word, marked it out, and replaced it with (gasp!) *that other word!*

Here we are again. That other word is now used by writers at very high levels. Traffic analysts use the third word.

However, we are beginning to have some hope for our word. We saw it in a dictionary[1] three or four years ago -- first sighting! Today we saw it in a book[2] ". . . intended to familiarize a wide audience with telegraph and data communication over shortwave links" -- second sighting!

We are looking forward to the third sighting. Who knows, we might get our word[3] back again.

---

[1] *Webster's New World Dictionary of the American Language*, Second edition, 1972.

[2] *Telegraph and Data Transmission over Shortwave Radio Links,"* Lothar Wiesner, Siemens AG, Berlin and Munich; Heyden & Son, Ltd., London.

[3] Our word (gaining fast!): "co-locate"; their word (boo! hiss!): "collocate"; third word (new but is it improved?): "colocate."

(U)

DOCID: 4019659

PAGES FROM THE PAST

W.W.II JAPANESE TRANSLATION AT ARLINGTON HALL STATION

Japanese Diplomatic Section, U.S. Army Signal Corps Signal Service Unit, Arlington Hall Station, 1945

The following are excerpts (Chapter IX, "Conclusion," pp. 100-104, and Appendix B, pp. v-viii, of "History of the Signal Security Agency, Volume Four: The Language Branch," Army Security Agency, Washington, D. C., 15 September 1946 (TS). A copy of the original document (with file number L-441) is available in T1213, Room 2N090, x5759s.)

Ed.

"Translation is only one step in the long process of rendering intercepted enemy communications intelligible to those who plan Allied strategy, but it is the ultimate step, for only expert, careful translation can reveal the import of enemy communications and transform them into vital information."

This statement was the prize-winning entry in a contest participated in by Language Branch personnel in the summer of 1944, and it expresses simply but eloquently the attitude of the translators toward their mission. Deeply conscious of the responsibility which was theirs -- and, indeed, it was a great responsibility, since upon their knowledge and ability depended the final exploitation of the product of thousands of other persons engaged in the interception and cryptanalysis of the most secret communications of the Japanese Empire -- almost to a man they fell to with enthusiasm and devotion, determined to get the most out of the material which was provided.

A review of production figures during the war (that is, from Pearl Harbor through August 1945) reveals that the Language Branch scanned considerably more than 1,100,000 decoded messages in all categories, out of which approximately 415,000 were forwarded to the Military Intelligence Service in the form of translations. This was a record far beyond what could have been anticipated or even imagined at the outset, when the force of Japanese translators consisted of only nine persons. It is believed to be an achievement of which all who participated can be proud.

In bringing this history to a conclusion, the following further observations have been appended with the thought that they might be helpful in determining procedures should similar situations have to be dealt with in the future.

Regardless of the language used, the linguistic aspects of any problem involving the exploitation of codes and ciphers are necessarily associated in a very intimate way with the cryptanalytic aspects. As a matter of fact, close coordination between translation and cryptanalysis is regarded to be of such importance that under normal circumstances the two functions are integrated within a single administrative organization.

But, as has been described in considerable detail in preceding chapters, during the war Japanese translation at Arlington Hall became such an extensive and diversified operation, presenting training and technical problems of such complex and unusual character, that it soon because necessary to place its administration on an independent, self-contained basis.

As it worked out, not only was the handling of training and translation problems greatly facilitated thereby, but the cryptanalysts, who depended upon the translators for assistance, also gained by this separation. What actually happened was that translators were attached to cryptanalytic units on temporary loan when and as needed. Meanwhile, however, through their administrative connection with the Language

Branch, they were kept in direct touch with the developments in the knowledge of the Japanese language, so that the quality of their aid to the cryptanalysts was constantly improved. Also, under this arrangement, it was possible to exercise much more selectivity in the allocation of jobs than would have been possible otherwise, and to place individuals on specific assignments, whether straight translation, code reconstruction, scanning, research, or auditing overlaps, in accordance with their ability to handle the specific assignment.

If there was any one special feature of Language Branch operations which contributed more than others to the success of the entire venture, it was the principle of flexibility, under which personnel who developed most along certain lines could be easily shifted from problem to problem where these skills might be best utilized. Thus, some individuals had a natural flair for straight translation, others for scanning, or for code reconstruction, or for cryptanalysis. In addition, translators had different backgrounds of experience and knowledge which made them individually valuable in specialized subject categories, such as Diplomatic, Commercial, Scientific, Order of Battle, and Shipping. These individual aptitudes did not usually show up at once when the translators came into operations but manifested themselves gradually as the translators gained further experience, so that it took time for each one to settle into the niche where he could do his best work.

If, by virtue of a different type of organization, the translators had to be parceled out to various crypto-translation units as they came into operations, there to be assigned on a permanent basis, obviously this flexibility, this opportunity for watching them and eventually fitting them into the right occupations would largely have been lost, with consequent detriment to the overall production effort. As it was, when urgent code reconstruction jobs came along, to pick one example, personnel experienced in that type of work were given the responsibility; and the same allocation of workers to jobs in which they were apt took place all along the line.

It is desired to make one more reference to the work of the Special Projects Section of the Language Branch. Although in the beginning there was no intention of going into the compilation and publication of dictionaries and other word studies on any elaborate scale, but merely to record and make available in useful and organized form such lexicographical information as emerged during the course of operations, the need for expediting the production of translations by anticipating the linguistic problems of the translators naturally caused the projects to expand far beyond what was originally contemplated. How the work was carried on, what sources of information were utilized, and the nature of the published results have been described in Chapter V of this history. What it is desired to emphasize here is that during the war this Section developed into what was probably the most scholarly, the most efficient, and the most valuable Japanese language research body in the United States.

The contribution of this Special Projects Section to the solution of every department of the Japanese problem as encountered by the Signal Security Agency during the war effort cannot be overestimated. What was actually done was to provide ever finer and ever sharper tools to the end that the time and labor of those engaged in direct production could be more effectually utilized. But -- and this is a point which should not be lightly overlooked -- the beneficial results of this Section's work may be even more far-reaching in the future if the work is permitted to go on and, furthermore, if free dissemination of the products is allowed to all who can profitably use them. Large segments of the findings of the Special Projects Section, although available in the files, have not yet been published, and much more can be accomplished if the Section is allowed to continue its endeavors. It is greatly to be hoped that the fine beginning which has been made in this extremely significant field of Japanese lexicography will not be allowed to lapse, but that arrangements will be made by which there may continue to be made available new knowledge on this complex subject.

APPENDIX

Language Branch

Chronological Table of Principal Developments

Item	Date	
	1930	
1	May	First Japanese translator employed, Mr. John B. Hurt. Activities mainly cryptanalytic research
	1935	
22	March	First formal Japanese translation published
	1937	
33	February	First "Red" translation (machine cipher system)
44	December	One-thousandth translation
	1938	
55	March	Second translator employed, Mr. Paul Cate
	1939	
66	September	First "Purple" translation (machine cipher system)

1940

7 January — Third translator employed, Mr. Hugh S. Erskine (later Lt. Col. and Chief of Translation Section, Central Bureau, USAFFE)

8 October — Fourth translator assigned to active duty, Lt. Verner C. Aurell (later Lt. Col. and Chief, Language Branch)

9 December — Translations appearing in eight Japanese Diplomatic systems ("Red," "Purple," CA, YO, LA, J-17, PA, P-1)

1941

10 June — First J-18 translation published

11 September — First J-19 translation published (JAE)

12 September — First J-22 translation published (JAI)

13 December — Pearl Harbor. Japanese Translation Unit consisted of nine persons

1942

14 May — First two translators to overseas duty (Erskine, Mahrt)

15 June — Reconstruction begun on Military Attache Code (JAS)

16 August — Translators organized as subsection B-1-J under Capt. Aurell

17 August — First JAS translation published (see item 15)

18 September — Japanese Language School established (30 enlisted students)

19 November — Aurell made OIC, B-1; Overton made OIC, B-1-J (see item 16)

20 December — First five graduates from J. School entered operations, bringing total translator staff to 28, including three instructors

1943

21 February — First translator assigned to Japanese Army systems under cryptanalytic study

22 April — Japanese Army Translation Subsection (B-1-JR) organized

23 April — Reconstruction begun on Water Transport Code Book No. 1 (JCN)

24 June — First JCN translation published (see item 23)

25 June — Code Instruction Translation Unit set up in B-1-JR

26 June — Routing and Logging Unit set up in B-1-JR

27 August — Reconstruction begun on Army Administrative Code Book No. 3 (JEM)

28 August — Auditing Unit set up to assist cryptanalysts (JEM)

29 August — Reconstruction begun on Diplomatic code JBB (old JCV)

30 August — First JBB translation published (see item 29)

31 September — B Branch reorganized. B-1 functions limited to Japanese language activities

32 September — B-1 organized into four sections as follows: B-1-R (Army Translation), Capt. Overton, OIC: B-1-D (Diplomatic Translation, Lt. Bacon, OIC; B-1-M (Military Attache Translation), Mr. Millard, CIC: B-1-JS (Japanese School), Mr. Buchanan, CIC

33 September — First ASTP class started at Georgetown University

34 September — Auditing Unit set up to assist cryptanalysts (JEK)

35 September — Translator team plan adopted in B-1-R

36 October — Captured Army Communications Code Book translated (JBT, later designated JER)

37 October — Reconstruction begun on Diplomatic Code JBA

38 November — Reconstruction begun on Japanese Army ship name and place name auxiliary codes

39 November — Reconstruction begun on Army Administrative Code Book No. 4 (see also item 27)

40 November — First JBA translation published (see item 37)

41 November — Reconstruction begun on Diplomatic Code JBC

42 December — First translation published in Army Administrative Code Book No. 4 (see item 39)

43 December — Reconstruction begun on Army Air Code Book No. 3 (JES)

44 December — Total translator staff (including nine instructors) -- 121

1944

45 January — 43 enlisted translators commissioned 2nd Lieutenants.

46 January — Reconstruction begun on Military Attache Code No. 3 (JAS, see item 15)

47 January — Captured auxiliary code books translated (see item 38)

48 January — Captured Army Administrative Code Book No. 4 translated (see item 39)

49 February — First JBC translation published (see item 41)

50 February — Vint Hill Nisei translation set up

51 February — Translations begun on Army Administrative systems based

DOCID: 4019659

		on captured book No. 4 (see item 48)
52	February	Scanning Unit established for Army Administrative decodes
53	February	Reconstruction begun on Army Communications Code Book No. 2 (see item 36)
54	March	B-1-R Liaison Unit set up for handling queries
55	March	B-1-R Research Unit set up for stereotypes and isologs
56	March	B-1-R translator teams specialize (see item 35)
57	April	Reconstruction begun on Diplomatic system JBD
58	May	15 enlisted translators commissioned 2nd Lieutenants
59	May	B-1-SP Special Projects subsection organized under Dr. Nelson
60	June	First JBD translation published (see item 57)
61	June	B-1 celebrates achievements to date
62	July	Translations begun in Army Air system (see item 43)
63	July	Translator unit attached to Traffic Analysis, Section B-IV
64	August	First JBL translation published (transposition)
65	August	Reconstruction begun on Army "BULBUL" low-level code
66	August	B-1 becomes Language Branch under Intelligence Division
67	August	B-1-V becomes section under Language Branch (see item 50)
68	September	Captured Communications Code Book No. 2 translated (see item 53)
69	September	Captured Army-Navy Liaison Code Book No. 4 translated (JEH)
70	September	First JBN translation translated (Commercial system)
71	September	Chief B-1 leaves for TD, SWPA (2 months)
72	October	Captured JKY Army code translated by B-1-V
73	October	Reconstruction begun on Army Water Transport Code Book No. 2 (see also item 23)
74	November	Reconstruction begun on Diplomatic Code JAM
75	November	First JKY translations published (see item 72)
76	December	First JAT translation published (Military Attache system)
77	December	Language Branch personnel at end of 1944:

Translators	254
Trainees	170
Administrative and clerical	92
Vint Hill	63
Total	579

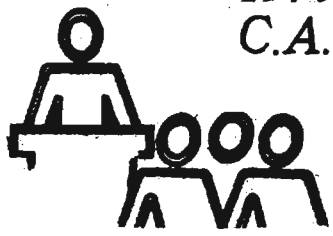
1945

78	January	First JAM translation published (see item 74)
79	January	B-1-C Commercial Translation Section organized under Lt. Bohannan
80	February	Reconstruction begun on Army Administrative Code Book No. 5 (see also item 39)
81	March	Reconstruction begun on Army Air Code Book No. 4 (see also item 43)
82	March	Translations begun from item 81 (above)
83	April	Translations begun from item 80 (above)
84	April	First JHC translation published (UNEIKAI)
85	May	Plain text scanning unit set up in B-1-C
86	June	100,000th Army Administrative systems translation published
87	June	Captured JEC Army Air Code Book translated
88	June	Captured Army Administrative Code Book No. 5 translated (see item 80)
89	July	Captured Army Communications Code Book No. 3 translated (see also item 68)
90	July	Captured Army Air Code Book No. 4 translated (see item 81)

The copy of "History of the Signal Security Agency" from which the preceding excerpts were taken was provided by the NSA Cryptologic History and Publications Staff, D4.

~~(TS)~~

1979 C.A. SEMINAR



It may not be too late for you to sign up for the fourth annual seminar, "Cryptanalysis: Contemporary Issues," which the CA Division of the National Cryptologic School will present at Fort Meade from 30 January through 1 February. Sixteen speakers will cover various topics of interest to cryppies. Although professional cryptanalysts get first pick, the seminar (CA-305) is open to all cleared and indoctrinated people. Sign up through your training coordinator.

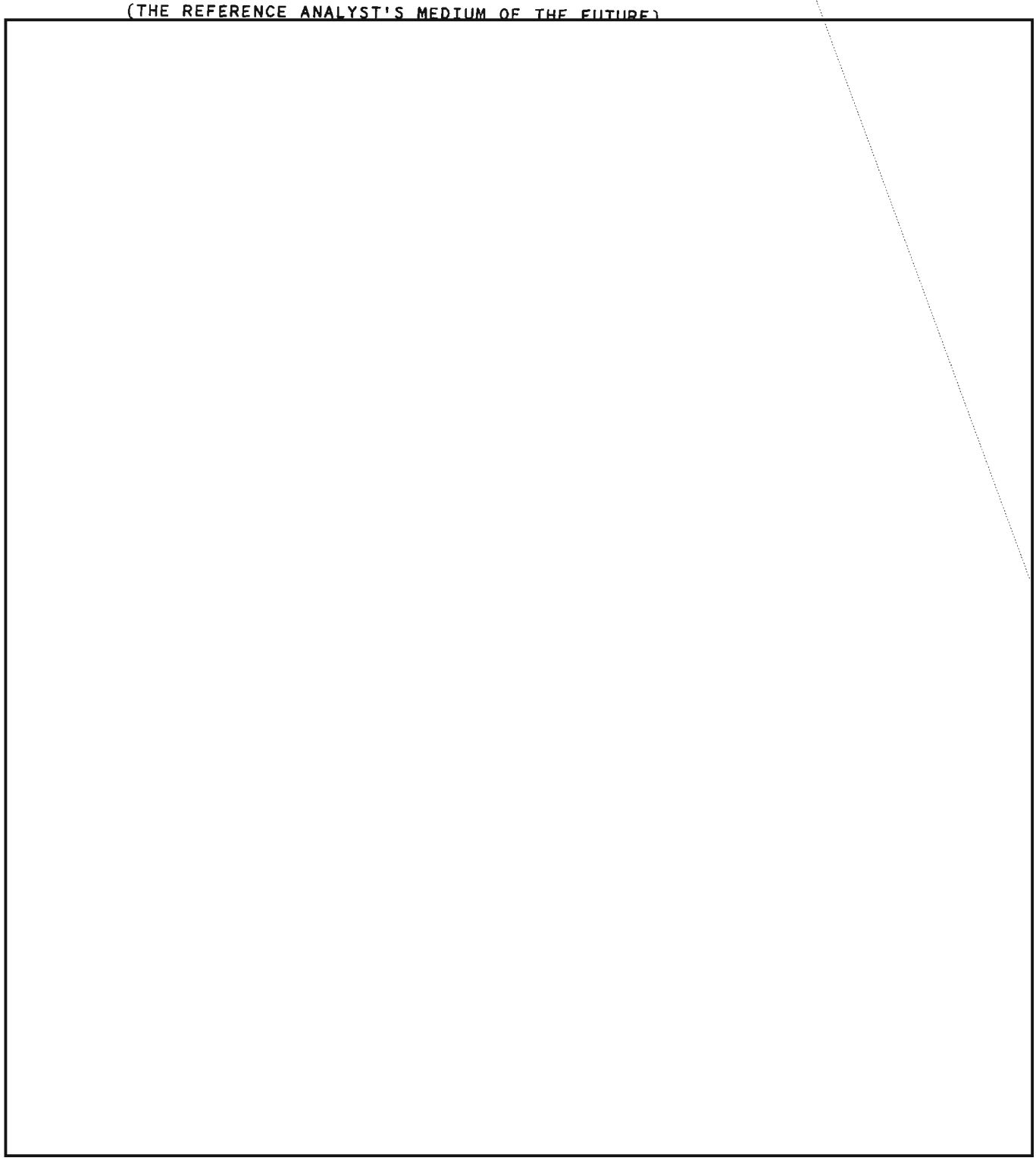
For additional information, call: [redacted] P.L. 86-36

[redacted] CA Division, NCS, E42, 8025s. (U)

T-VISION

P.L. 86-36

(THE REFERENCE ANALYST'S MEDIUM OF THE FUTURE)



P.L. 86-36

[redacted]

[redacted]

~~(FOUO)~~

News of the CMI

On 12 October 1978 the Crypto-Mathematics Institute presented the first CMI President's Award to [redacted] The President's Award is an honorary award established to recognize and honor recent significant contributions to cryptology through the use of mathematics.

[redacted] received this award for his efforts on the cipher machine PENNY/WISE. While on tour at the Institute for Defense Analysis, he created the mathematical description which has been the foundation for [redacted]

[redacted]

The individual plaque and accompanying letter were presented to [redacted] CMI President. [redacted] pointed out that all ten of the submitted nominations represented significant contributions to cryptology and the Agency's mission. [redacted] was chosen from among this select group as the person whose work provided the most significant recent contributions through the knowledge, understanding, and application of advanced mathematics.

Among the many attendees of the party to honor [redacted] and the other nominees were several distinguished guests, including VADM B. R. Inman, Mr. Robert E. Drake, MGEN George L. McFadden, Mr. William Lutwiniak, [redacted] and [redacted] P1, x3957s ~~(TSC)~~

P.L. 86-36

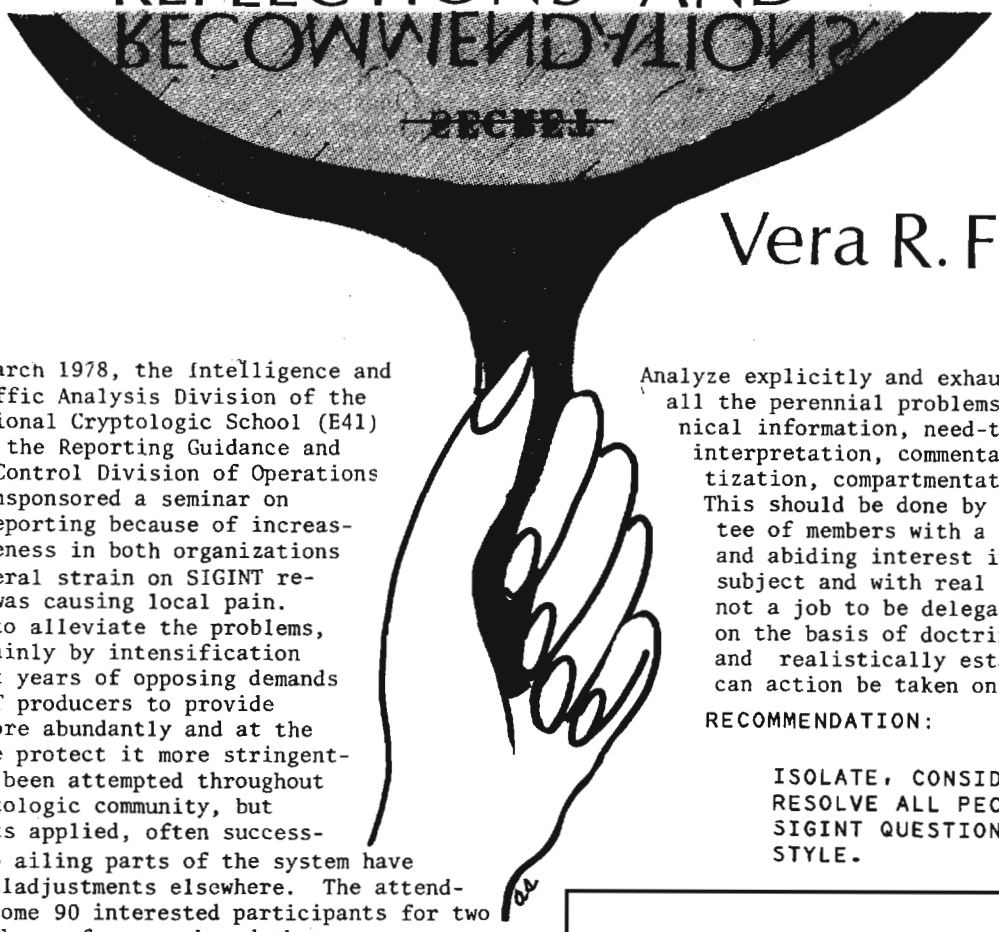
P.L. 86-36
P.L. 86-36
EO 1.4.(c)
P.L. 86-36
EO 1.4.(c)

DOCID: 4019659

REFLECTIONS AND RECOMMENDATIONS

~~SECRET~~

Vera R. Filby,
E41



In March 1978, the Intelligence and Traffic Analysis Division of the National Cryptologic School (E41) and the Reporting Guidance and Quality Control Division of Operations (V12) consponsored a seminar on SIGINT reporting because of increasing awareness in both organizations that general strain on SIGINT reporting was causing local pain. Efforts to alleviate the problems, caused mainly by intensification in recent years of opposing demands on SIGINT producers to provide SIGINT more abundantly and at the same time protect it more stringently, have been attempted throughout the cryptologic community, but treatments applied, often successfully, to ailing parts of the system have caused maladjustments elsewhere. The attendance of some 90 interested participants for two days of the conference showed that concern over this situation is shared by many. Since an account of the conference, *Proceedings of the SIGINT Reporting Seminar, 8-9 March 1978*, has been published and is available (E41, 7119s), this paper will not comment on the events of the seminar but instead offer reflections and (unofficial) recommendations.

Postseminar reflections lead to the pessimistic but predictable conclusion that since March nothing has changed. Hence the "recmendations" are offered with the even more pessimistic conviction that nothing will change -- but offered nevertheless. The recommendations would be hard to carry out because the problems are chronic and their treatment controversial. They are also so interrelated that they could just as well be stated in other ways, and they lead to subordinate recommendations. The main ones are the following three.

RECOMMENDATION: RETHINK THE ENTIRE SYSTEM OF PHILOSOPHY OF SIGINT REPORTING.

Analyze explicitly and exhaustively all the perennial problems: technical information, need-to-know, interpretation, commentary, sanitization, compartmentation. This should be done by a committee of members with a strong and abiding interest in the subject and with real clout -- not a job to be delegated. Only on the basis of doctrine firmly and realistically established can action be taken on the next

RECOMMENDATION:

EO 1.4.(c)
PL 86-36

ISOLATE, CONSIDER, AND RESOLVE ALL PECULIARILY SIGINT QUESTIONS OF STYLE.

[redacted]

These questions are not of secondary importance, and they should be solved, every one of them. They are all indispensable for effective guidance to SIGINT producers at all stages of product preparation. The solution to these questions must precede work on the next

RECOMMENDATION: REWRITE BASIC GUIDANCE, PROMULGATE IT, AND ENFORCE IT.

All basic guidance need not be issued in the same form or at the same time. Easier parts, such as mechanical style rules, can be -- maybe should be -- issued separately.

Since obviously all this would require a great deal of effort, it may be well at this point to justify these recommendations. Who needs them? Why? The answer is that everyone in the reporting chain needs them because everyone needs clear, consistent, comprehensive guidance; and for situations that cannot be covered or anticipated with specific rules and guidance, producers at all stages need to understand the principles that inform the system. There are now too many cases of gross inconsistency.

RECOMMENDATION: MAKE USE OF THE PROFESSIONALIZATION CRITERIA BEING PREPARED FOR THE EDITING AND WRITING CAREER FIELD.

Re-creation of the entire system of SIGINT reporting doctrine is not likely to happen soon, if ever, but meanwhile experimental ideas can be tried. One idea, discussed in detail at the seminar, is summarized in the next

RECOMMENDATION: DEVELOP AND TEST A GENERAL SYSTEM OF MULTILEVEL REPORTING.

RECOMMENDATION: ISSUE TECH SUPPLEMENTS WITH PRODUCT AND MAKE THEM AVAILABLE, TO SIGINT PRODUCERS ONLY, THROUGH SOLIS.

SOLIS is the best thing that has happened to SIGINT reporting at NSA since OPSCOMM. It could be even better and more useful than it already is. SOLIS programmers have performed such miracles already that they could surely manage this if policy allowed.

After a recommendation as wildly unlikely to be fulfilled as that one, a much more modest proposal, just a little thing, can serve to end this paper. Someone at the seminar suggested, and everyone -- well, almost everyone -- warmly agreed, that it would be very helpful if NSA product, identified the producing section, this not for credit but for convenience. NSA is a very large organization. Any device to help a reader find the place in it where a question can be answered or an item of information coordinated without going through frustrating and time-wasting sequences of telephone calls would be a boon. So, as a concluding

RECOMMENDATION: SHOW THE PRODUCING UNIT ON NSA PRODUCT.

This could easily be done by entering the organizational designator of the producer (A25, G63, etc.) in some convenient place, say the end of the I&A line or following the reference serial. This should be a cinch for SOLIS.

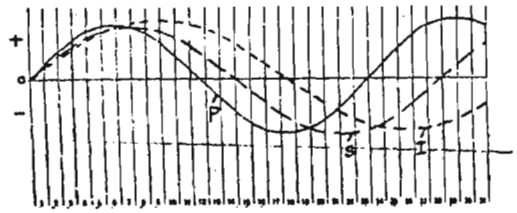
DOCID: 4019659

HUMAN FACTORS NEWSLETTER

CRYPTOLOG is pleased to reprint in its entirety the September 1978 issue of Human Factors Newsletter. The newsletter is published by the CISI (Computer and Information Sciences Institute) Special Interest Group on Human Factors. It is produced "semirandomly" by the Chairman of that Special Interest Group, Douglas Creswell, A635, 3717s/7540b, and is edited by Jeanne Mahoney, W23, 5150s/6255b. Persons who would like to be put on the distribution list for the Human Factors Newsletter and to receive other information about the activities of the Special Interest Group should get in touch with Mr. Creswell or Ms. Mahoney.

Ed.

BIORHYTHMS -- EVERYBODY'S GOT ONE. . .



BIORHYTHM CHART PROGRAMMS — Major companies use bio-charts to monitor key employees for their highs-lows and critical days. Available in COBOL-DIEBOL and BASIC. Documentation and programm source deck (80 col) supplied. Send $25 to:

...or for about $15 you can order a computer-produced "personalized" biorhythm chart; you can buy a calculator that tells your biorhytmic state; or you can drop a few coins in a biorhythm machine at the airport to find out how you should feel today or whether or not you should make or avoid major decisions.

Shades of astrology and snake oil merchants!

What is this "biorhythm" thing anyhow? Seriously -- the biorhythm theory is one of several theories concerning the fluctuations of human behavior. Scientific research (about 3000 papers have been published on the subject) has established that biorhythms are valid and are practically universal in biological organisms. Most people experience rhythmical variations in their physical, emotional, and intellectual states. The chart reproduced above shows the plot of a "typical" biorhythm cycle for each of these states. The numbers along the x axis represent days. It is believed that an individual's biorhythm characteristics can be determined by carefully collecting and analyzing data over a long period of time. This is a complex problem and the biorhythm theory is generally not well understood, so be cautious about what some sidewalk hawker promises you for a small fee.

I have extracted from two recent articles some information that I hope you will find interesting and enlightening:

> "There are two views of biorhythms, the popular and the scientific. The popular view is largely fancy and ignores virtually everything that has been scientifically established about biorhythms. . .
>
> ". . .the popular theory of biorhythms has been put forth in dozens of books, newspaper and magazine articles, and is followed by many thousands of people. Popular 'biorhythms' are determined solely by one's birthdate. Given this single piece of information, one's biological rhythms are assigned to be exactly determined for one's entire lifetime. This popular theory claims that everyone has a physical, emotional and mental cycle of exactly 23, 28 and 33 days, respectively. No variations are permitted because of differences in sex, age, climate, occupation, or other variables. . .
>
> ". . .every published scientific test of this popular theory has shown no correlation between these simplistic cycles and one's true biological rhythms." (M. Lattimer Wright, "Biorhythms: Fact and Fancy," *Proceedings of the Human Factors Society, 21st Annual Meeting, 1977*, pp. 193-196)

Is the biorhythm useful for accident prevention?

> "In a continuing effort to predict accident behavior, the biorhythm theory has been used by some researchers as a tool to attempt to bring a degree of logic and order to what remains an otherwise unpredictable situation. . .
>
> ". . .For the sample examined in this study, there was no relationship between accident occurrence and biorhythmic criticality. Until some of the inconsistences of the theory and its lack of precision are eliminated, the use of biorhythm as an accident prevention aid appears to be of no value . . .
>
> "use of more definitive information . . . if combined with more carefully designed research methodology, would eliminate much of the ambiguity observed in present studies and produce more meaningful results." (M. W. Brownley and C. E. Sandler, "Biorhythm -- An Accident Prevention Aid," *Ibid.*, pp. 188-192)

Want to read more? Copies of these articles can be obtained by calling me -- [redacted] 3717s/7540b. If my biorhythm cycle is on a "high," I will respond intelligently, rapidly, and very emotionally.

A LATE-BREAKING NEWS ITEM

Mr. Zaslow, DDT, presented a most interesting talk to CISI on 21 September. During the question and answer period, the subject of "Human Engineering" was raised. Mr. Zaslow's response was direct and to the point. He stated that NSA (specifically computer programmers and system designers) must do a better job of providing systems that are "friendly" and responsive to user needs. He correctly stated that there is no one at NSA with a job title of "Human Factors Engineer" and no Human Factors organization to turn to for Human Engineering support. In short, Human Factors Engineering at NSA is a failure. We must do all we can to improve man-machine interfaces. Computer systems are user tools -- not ends in themselves.

P.L. 86-36

Such comments are refreshing and very encouraging to those of us who have been waving the Human Factors flag for so long!

A TYPICAL USER CAT AT A TYPICAL (UGH) COMPUTER DISPLAY TERMINAL

IF THE PROGRAMMING CATS
READ [redacted] IEEE
REVIEW, IT MIGHT GIVE THEM SOME
IDEAS ...
WE GOTTA DO BETTER ...
///@&%%####, BURP ...
PLEASE STAND BY ...
HELLO, USER CAT?
THIS IS YOUR COMPUTER ...
HELLO!?

Article Review

[redacted] W23

P.L. 86-36

A recent article in the *IEEE Transactions on Software Engineering* dealt with user-perceived quality of interactive systems. User-perceived quality is defined as a set of system properties which are relevant to man-computer interaction from the user's point of view. User's views vary with the needs, problems, and preferences encountered when assessing software products. User-perceived quality, therefore, is not a distinct quality but rather a multi-dimensional concept.

User data was gathered through questionnaires given to more than 300 experienced users of interactive systems with the Federal Republic of Germany. Data was submitted to several factor analysis procedures, to date mainly applied in psychology but in no way limited to any scientific discipline. In factor analysis, variables are organized into a smaller set of statistically independent linear combinations of variables, so-called factors or dimensions.

DOCID: 4019659

The emphasis in factor analysis is on understanding the nature and structure of complex measurements through examination of the relationships to a relatively few underlying features.

From factor analysis, seven factors were extracted. They are: 1) self-descriptiveness; 2) user control; 3) ease of learning; 4) problem adequate usability; 5) correspondence with user expectations; 6) flexibility in task handling; 7) fault tolerance. Each factor is composed of a set of requirements belonging together, with factor loadings of at least 0.30; smaller loadings indicate random correlations. The higher the loading, the more important is a requirement with respect to the interpretation of a factor. Also, in looking at the loadings one can see that most requirements have high correlation with only one factor.

It appears that most factors are cognitive in nature. The factor "correspondence with user expectations" additionally addresses affective behavior. Motorial behavior is, if need be, addressed in parts by the factor "fault tolerance."

It may seem surprising that some qualitative aspects such as performance and responsiveness do not appear in the framework. These might appear, however, if some of the factors were substructured. However, this process would require much more research and empirical verification.

The article also discusses the statistical analysis, made to determine the validity and reliability of the factors. The authors hope that this is a step toward more user-oriented interactive systems where users access the systems and designers are guided to translate user-oriented criteria into the specifics of particular system design.

Factors of User-Perceived Quality

Factor 1: "Self-descriptiveness"

0.70 explain system requests to the user if and when necessary
0.68 supply explanations in different detail and different format upon user request
0.67 supply help features pertinent to any dialogue situation
0.60 enable transparency of dialogue organization and dialogue sequence at any time
0.52 explain each command and subcommand upon user request
0.45 give clearly arranged presentation of system functions
0.45 supply interactive programming aids which provide guidance for structured programming
0.33 give decision aids if tasks cannot be executed as desired
0.33 provide global information about the functional range of the system
0.32 make user thoroughly acquainted with system usage without human assistance
0.31 by prompting, provide user guidance for the dialogue
0.30 supply information about the current system status if desired

Factor 2: "User Control"

0.60 admit interruptions of a task to start or resume another task
0.59 admit process canceling without detrimental side effects
0.59 allow abortion of particular dialogue steps or processes
0.48 have a command language syntactically homogeneous
0.47 be permanently available
0.42 immediately detect syntax errors
0.37 permit clustering of commands with a new name
0.37 by prompting, provide user guidance for the dialogue
0.36 allow user to make background processes visible
0.34 supply information about the current system status if desired
0.33 have a command language easy to understand and easy to apply
0.32 supply comprehensive debugging aids
0.31 give decision aids if tasks cannot be executed as desired

Factor 3: "Ease of Learning"

0.63 make user manuals superfluous
0.61 facilitate the learning of system use without consulting manuals
0.57 be usable without special DP-knowledge
0.52 largely offer on-line forms for user input
0.49 be able to present user manuals in whole or in parts via display station
0.41 make user thoroughly acquainted with system use without human assistance
0.41 provide global information about the functional range of the system
0.41 make the least assumptions about user's prior knowledge of system structures and functions
0.40 support user input by menu technique
0.33 give error messages with correction hints
0.34 explain each command subcommand upon user request
0.32 enable the learning of system use without referring to comprehensive texts stored

Factor 4: "Problem Adequate Usability"

0.69 have a data management system that obviates as far as possible the need for the user to perform clerical or housekeeping activities
0.63 manage formatting, addressing, and memory organization without bothering the user
0.56 determine system decisions without consulting the user
0.50 accept free formatted command input
0.44 have a command language easy to understand and easy to apply
0.42 be tolerant towards erroneous user input
0.41 have a syntactically homogeneous command language
0.38 have a command language easy to remember
0.32 make repetitive or routine input unnecessary

Factor 5: "Correspondence with User Expectations"

0.76 behave similarly in similar situations
0.71 request analogous user actions to similar tasks to be performed
0.65 offer minimum astonishment behavior towards the user
0.37 let user recognize effects of his input
0.34 be tolerant towards erroneous user input
0.33 enable transparency of a dialogue organization and dialogue course at any time
0.31 provide same response times to equal activities

Factor 6: "Flexibility in Task Handling"

0.56 allow user to extend the command language
0.55 allow facilities for stacking tasks
0.47 allow user an arbitrary access to the task stack
0.44 provide system messages with different levels of detail dependent on user status
0.42 provide reduced input/output according to user's training level
0.41 allow user to define his set of system functions
0.35 provide shorter ways for trained user to perform his tasks
0.35 permit user to define some particular user status
0.34 allow user to make background processes visible
0.32 permit clustering of commands with a new name

Factor 7: "Fault Tolerance"

0.53 insist only on partial retyping if previous input was erroneous
0.52 tolerate typical typing errors
0.49 give error messages with correction hints
0.40 enable user to submit concatenated commands as input
0.35 accept reduced input when actions are to be repeated
0.34 give error messages in full text
0.32 give decision aids if tasks cannot be executed as desired
0.31 support user to find his way

DOCID: 4019659

NSA-crostic No. 21

By David H. Williams, P16

The quotation on the next page was taken from an article that appeared in an NSA publication. The first letters of the WORDS spell out the author's name and the title of the article.

DEFINITIONS	*WORDS*
A. NFL team (2 wds)	239 47 31 174 60 82 121 106 225 42 161 152 56 165 / 248 25 114 89
B. Where the season ticket-holder can be found during any home game (3 wds)	197 146 100 185 79 243 211 199 33 49 39 237
C. Saw	68 12 58 156 97 108
D. "All the rams are chasing ——; They're determined there'll be new sheep..." (Rogers and Hammerstein, "Carousel") (2 wds)	138 191 219 158 194 155 202 4
E. Untanned cattle skin; old TV series	128 149 209 154 81 67 102
F. Former NFL star, played himself in film biography "Crazy Legs," 1953 (2 wds)	90 48 77 172 193 137 32 96 198 13 120
G. High-altitude Asian capital city (2 wds)	250 101 207 176 133 119 8 200 217 164
H. Did a grease job (slang)	201 244 84 92 95
I. N. Calif. structure, a major component of San Francisco's water supply system (3 wds)	214 30 46 110 242 212 236 177 86 75 103 168 41 226
J. Competitor in any sport or physical activity	159 125 192 151 206 21 129
K. Trump	70 167 52 173
L. Conducted an incursion or foray	232 189 118 59 123 99
M. "Letting 'I dare not' wait upon '——' —— the poor cat i' the adage" (Macbeth) (3 wds)	1 196 204 111 134 223 228 6 20 215
N. Baer or Schmeling	72 144 230
O. Income Tax Day (3 wds)	181 139 179 249 105 213 91 34 78 11 241 93
P. NFL team whose home stadium is at Foxboro (2 wds)	222 66 188 26 62 160 208 14 44 183
Q, Sharp, repeated knocking or tapping sound (comp)	122 163 166 127 142 94 187 136 104 203
R. Period or state of decline (2 wds)	229 150 234 184 240 205 69
S. Team for which Word F played (2 wds)	145 233 141 130 2 83 195 135 16 247
T. NFL team (2 wds)	98 63 251 107 64 37 124 27 3 235 74 22 218 190

U. NFL team (3 wds)

36 221 112 227 18 76 186 71 23 88 245 148 157 50
162 65 5 116

V. In the same place (Lat)

210 17 51 132 169 15

W. Noontime sign on the boxer's door (3 wds)

43 73 171 115 178 28 54 182 19 57

X. Major work by Anton Dvorak (3 wds)

131 85 117 220 109 29 7 61 153 180 40 231 246 53
170 143

Y. NFL team (2 wds and comp)

45 87 35 80 24 147 55 126 175 238 224 140 10 9
113 38 216

1 M	2 S		3 T	4 D	5 U	6 M	7 X		8 G.	9 Y	10 Y	11 O		12 C		13 F	14 P	15 V	16 S
	17 V	18 U	19 W	20 M		21 J	22 T		23 U	24 Y	25 A	26 P	27 T		28 W	29 X	30 I	31 A	32 F
33 B	34 O	35 Y	36 U		37 T	38 Y	39 B	40 X	41 I	42 A		43 W	44 P		45 Y	46 I	47 A	48 F	49 B
50 U		51 V		52 K	53 X	54 W	55 Y	56 A		57 W	58 C		59 L	60 A	61 X	62 P	63 T		64 T
65 U	66 P	67 E		68 C	69 R	70 K	71 U		72 N	73 W	74 T	75 I		76 U	77 F	78 O	79 B	80 Y	81 E
82 A	83 S		84 H	85 X	86 I	87 Y	88 U	89 A	90 F		91 O	92 H		93 O	94 Q	95 H		96 F	97 C
98 T	99 L		100 B	101 G	102 E		103 I	104 Q	105 O	106 A	107 T		108 C	109 X	110 I	111 M	112 U	113 Y	114 A
115 W	116 U		117 X	118 L	119 G	120 F		121 A	122 Q	123 L	124 T	125 J		126 Y	127 Q	128 E	129 J		130 S
131 X	132 V		133 G	134 M	135 S		136 Q	137 F	138 D		139 O	140 Y	141 S	142 Q		143 X	144 N	145 S	146 B
147 Y		148 U	149 E	150 R	151 J	152 A	153 X		154 E	155 D		156 C	157 U	158 D		159 J		160 P	161 A
162 U	163 Q	164 G		165 A	166 Q	167 K	168 I	169 V	170 X	171 W		172 F	173 K		174 A	175 Y	176 G	177 I	178 W
179 O	180 X		181 O	182 W	183 P		184 R	185 B	186 U	187 Q		188 P	189 L	190 T		191 D	192 J	193 F	
194 D	195 S		196 M	197 B	198 F		199 B	200 G	201 H	202 D		203 Q	204 M		205 R	206 J	207 G	208 P	
209 E	210 V	211 B	212 I		213 O	214 I	215 M	216 Y	217 G		218 T	219 D	220 X		221 U	222 P	223 M		224 Y
225 A	226 I	227 U	228 M	229 R	230 N		231 X	232 L	233 S	234 R	235 T	236 I	237 B	238 Y		239 A	240 R	241 O	242 I
	243 B	244 H	245 U	246 X		247 S	248 A	249 O	250 G	251 T									D.H.W.

(Solution next month)

DOCID: 4019659

DEPARTMENT OF GOLDEN OLDIES

ON FIRST OPENING KENNEY'S "STATISTICS"

Marjorie Mountjoy (RETIRED)

[redacted] E42, found this unpublished item among material he inherited, through [redacted] from Marjorie Mountjoy when she retired a few years ago. CRYPTOLOG reprints it herewith in its original form, without even changing its title to "Statistics, Don't Be Mean to Us Cryppies!"

Ed.

The trouble with *Statistics* was that I don't think I survived the definition of "the mean" (p. 32 ff.).

It was stated three times; in the conventional "compact" notation, and it was all supposed to amount to the same thing:

$$(1)\quad \bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$(2)\quad \bar{x} = \frac{1}{N}\sum_{1}^{k} f_i x_i \quad (\text{where } N = \sum_{1}^{k} f_i)$$

$$(3)\quad \bar{x} = \frac{1}{N}\sum_{1}^{k} f_i\,(c\,u_i + x_o)$$

As any fool can plainly see from the left-hand side! It was the right-hand side that bothered me.

Now it is not the mathematics, because, to get the mean, you simply take the total and divide by the number of items, so it must be the language. So the thing to do is to learn the language, in case the next time you have to do something, it may be something you do not know how to do already.

O.K.

"$\bar{x}$" (I think it is pronounced "ex-bar") stands for "the mean." "N" is the total number of variates (and a "variate" is defined as "the magnitude of a variable," see p. 7). So that brings us up to "$\sum$," pronounced "sigma," because "sigma" is "S" in Greek and what it means is "Sum" (imperative) -- starts with "S" -- get it? This, as the book tells you, is a sort of mathematical *verb*, also known as an *operator*, and the notation written above and below it are *adverbs*, otherwise known as *limits*. It cannot but follow, for one with any imagination at all, that the "x_i" or the "$f_i x_i$" (where

$N = \sum_{1}^{k} f_i$) or the "f_i" ($c\,u_i + x_o$) part,

which the book calls the variates, are actually *nouns* in the *objective case, direct objects* of the verb "$\sum$," and by this time I am so entranced with the grammatical structure of the equations that I want to diagram them and to find out whether, being part-Greek, they are inflectable. It is difficult to get back to mere mathematics, but this flight of syntax leads nowhere. Therefore, "i" is the "index of summation." "Any letter may be used, but it is conventional to use *i* or *j*." "Frequently the index of summation is understood from the context, and the notation at top and bottom of $\sum$ may be omitted if no ambiguity results." I have found, in actual practice, that omitting all forms of the "index of summation" from the equation *cleared up* the ambiguity in 99 cases out of 100.

This just about covers our examples. No -- wait! That "u" in equation (3) is in case you don't have time for the regular procedure for computing the average and want to take a short cut. It is defined as:

$$u = \frac{x - x_o}{c}, \quad (c \neq 0).$$

"c" represents "units," and "x_o" is the "new origin" (see "translation of axes," p. 35); "$\neq$" I believe I remember to mean "is not"; "k" of course is explained in (2) as:

$$N = \sum_{1}^{k} f_i.$$

This makes it all very simple, I suppose. Really, as I say, I sort of faded out at this point.

(U)

P.L. 86-36

HENRY CEMENT AND OTHER PHANTOMS OF THE OPERA(TIONS)

[redacted] *G51*

January 79 * CRYPTOLOG * Page 27

DOCID: 4019659

CLASSIFICATION CORNER

"IT'S PARTY TIME!"

[redacted]
DDO Classification Advisory Officer

P.L. 86-36

Have you classified a party lately? How about a "Second Party" or a "Third Party"? It's time we classified all parties the same. The following information may help.

In the past, the terms "Second Party" "Third Party" (instead of actual country names) were used in an attempt to keep the references unclassified or at the lowest possible classification level. The old rules, which were never documented, but which were used by me and other classification officers, were:

Sample references	Appropriate classification
Vague references to "Second Party" and "Third Party" organizations, even though mention of SIGINT and COMINT may have been included.	U
References to "Second Party" and "Third Party" in such a way that they revealed we were referring to a country other than the United States (e.g. "Third Party country").	C
References to the specific country when COMINT was stated or implied.	S-CCO

New guidance specifies that the terms "Second Party" and "Third Party" in a SIGINT or COMINT context will be classified "Secret -- Handle Via Comint Channels Only." Examples of references and their appropriate classification under the new guidance are:

Sample references	Appropriate classification
"Direct liaison with Second and Third Party organizations is not authorized."	S-CCO
[redacted]	S-CCO
References to "Second Party" or "Third Party" which are made in a COMSEC context, whether stated or implied	S-CCO S U

Considering the above guidelines, it may be beneficial to mention the actual country or countries involved in your correspondence, rather than vague references to "Second Party" or "Third Party." The sample statement starting "Direct liaison..." could be changed to "Direct liaison with GCHQ and [redacted] representatives is not authorized." The classification is S-CCO in both cases, but the statement is much more informative when the specific countries are mentioned.

EO 1.4.(c)
P.L. 86-36

The guidance contained herein is from the Director's Policy Staff and should be used uniformly throughout the Agency. It will be reflected in forthcoming regulatory documents, including the NSA/CSS Classification Manual and USSID 3.

~~(S-CCO)~~

THIS MONTH'S

Letters to the Editor

(U)

Chief P1
Office of Techniques and Standards

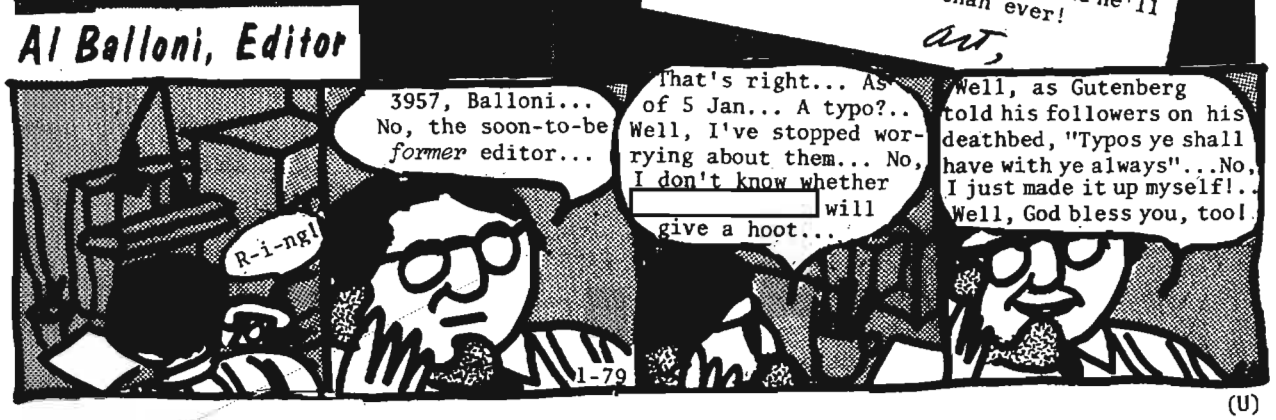
27 November 1978

Art Salemme, the second editor of CRYPTOLOG, retires in January. He has brought along the lusty youngster conceived and raised by Doris Miller to healthy, mature status. CRYPTOLOG, thanks to Art's indefatigable promotion, no longer staggers from issue to issue. There is now a modest, but actual, backlog of articles to help in planning ahead. Under Art's editorship the newsiness and readability of CRYPTOLOG have improved. His uninhibited way with headlines and illustrations has enhanced its liveliness and saucy appeal. He has handled controversy with wit and tact. Above all he has kept the content useful and relevant, informal but informative. He has served us well. We wish him a happy productive retirement, and hope to keep a string on him so we can reel him back in for his linguistic talents when occasion warrants.

William L. Twiniare
Publisher
CRYPTOLOG

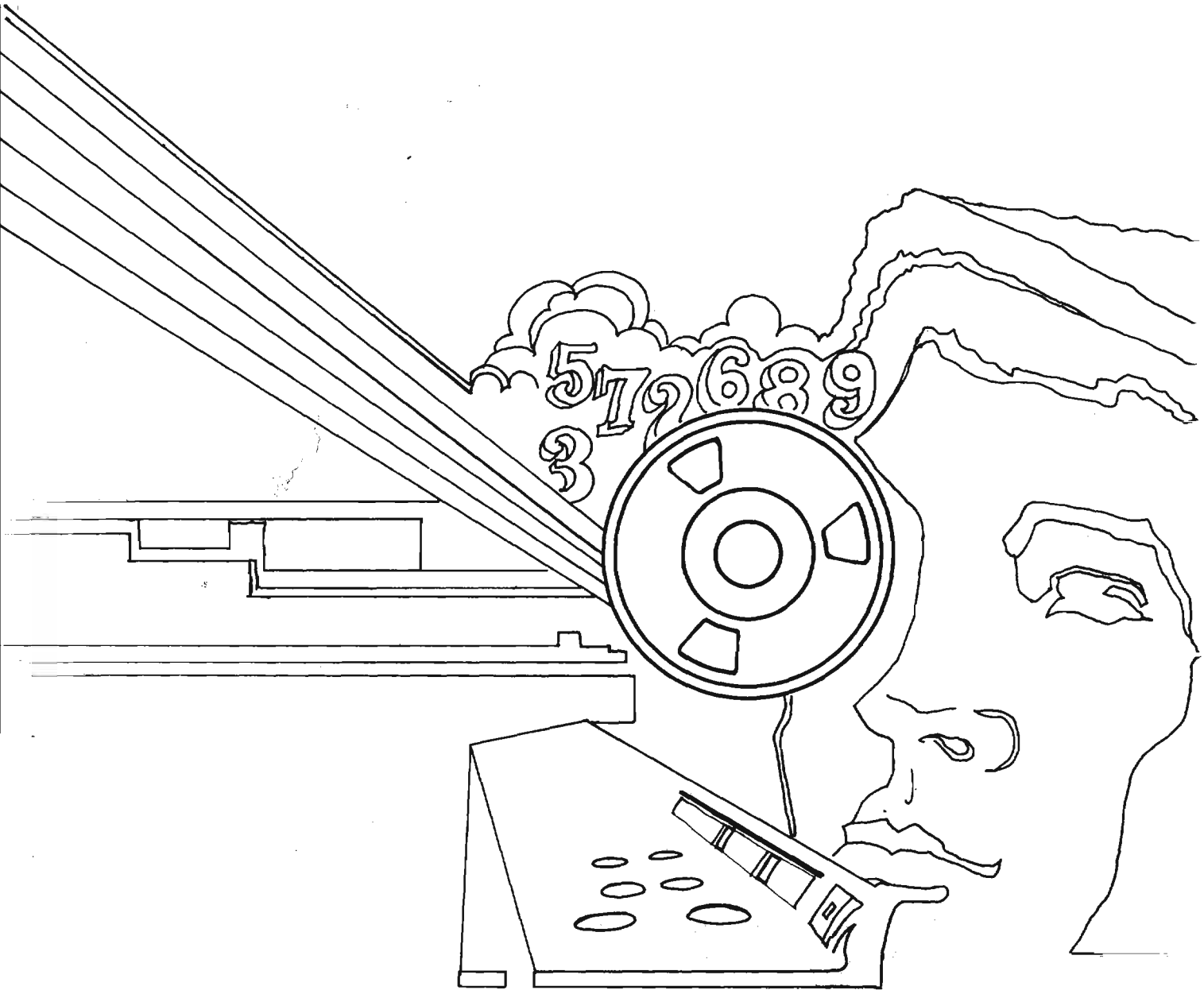
During my career at the Agency I've done a lot of interesting things (in and out of the Handicraft Club), but the years I've spent since my elevation from the position of CRYPTOLOG Art Editor to that of Art, Editor easily qualify as my high three. I've had a lot of fun hustling articles, telling potential authors "Let's you and him fight!", and slapping their articles into print, sometimes providing them with a slightly impertinent illustration or title in order to lure someone into reading an article he or she might have otherwise passed over. I've had *my* fun, but why be greedy? Why not let someone else take a crack at it? So, I'm pleased that Dave Williams (see p. 6) is r'arin' to go. Give him all your support with articles, letters to the editor, suggestions, etc., and he'll make CRYPTOLOG better than ever!

Art,


Al Balloni, Editor

(U)

P.L. 86-36
P2-Dec78-S3-27102


5726893

DOCID: 4011702

~~TOP SECRET~~

EO 1.4.(c)
P.L. 86-36

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

DECEMBER 1978

P.L. 86-36

A V.I.P. THROUGH THE ATTIC OF N.S.O.C..... [redacted] 1
A/K/A SAM.....W. P. Meyer.....6
HOW DO YOU SPELL PEKING?..... [redacted] 7
[redacted] ..... [redacted] 10
[redacted] ..... [redacted] 11
"NO, NO, NANETTE!" MEANS "YES"?.....A.J.S.....12
SOME TIPS ON GETTING PROMOTED..... [redacted] 13
AGENCY ENCOURAGES SUMMER LANGUAGE STUDY....Dan Buckley.....20
TO WHOM IT MAY CONCERN.....Lou Grant.....21
NSA-CROSTIC NO. 20.....David H. Williams.....22
1978 INDEX.....24
READER SURVEY.....29

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4011702

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. V, No. 12 DECEMBER 1978

PUBLISHER WILLIAM LUTWINIAK

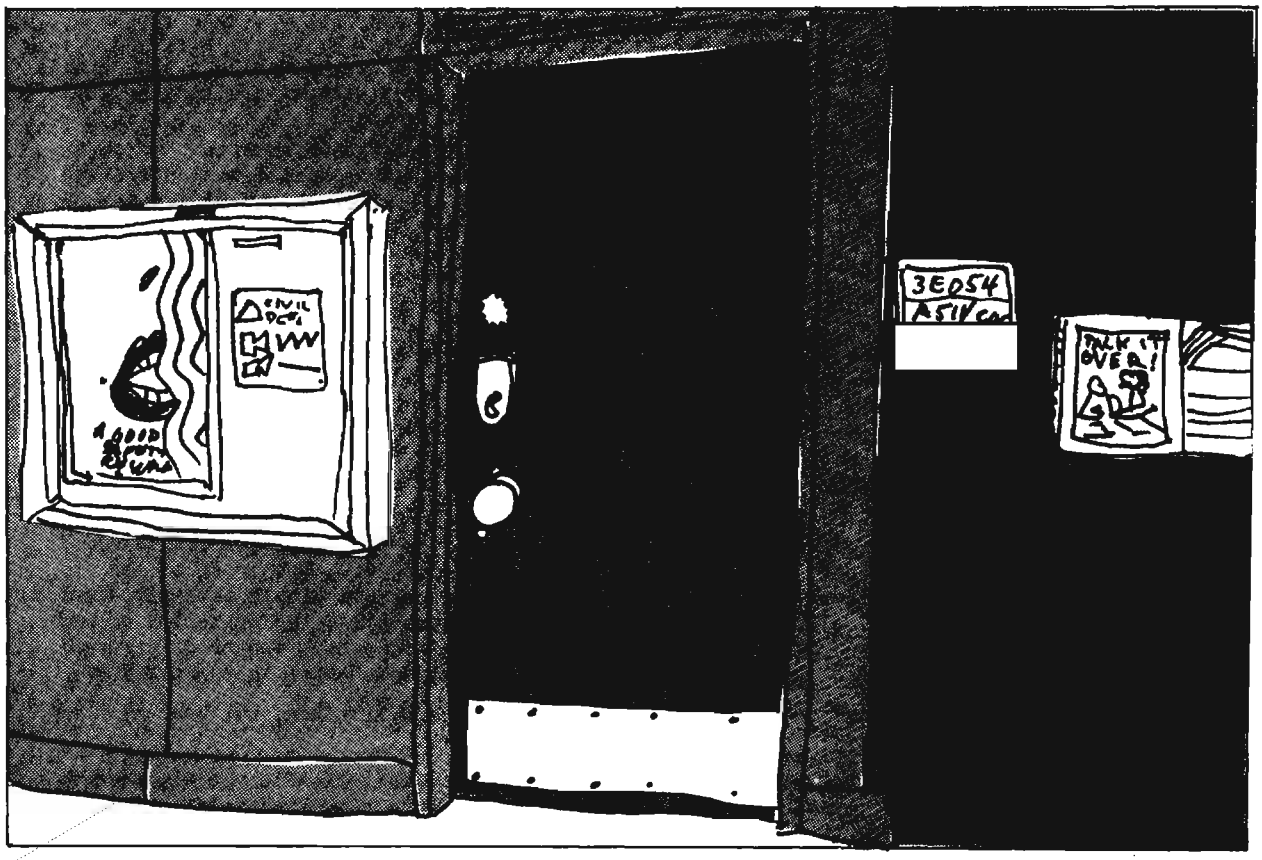
BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (3957s)
Collection..... [redacted] (8555s)
Cryptanalysis..... [redacted] (4902s)
Cryptolinguistics..... [redacted] (5981s)
Language..... [redacted] (8161s)
Machine Support..... [redacted] III (5804s)
Mathematics..... [redacted] (8518s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Don Taurone (3573s)

Production Manager.....Harry Goff (5236s)

NEW NUMBER
P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1



A V.I.P. TOUR THROUGH THE ATTIC OF N.S.O.C.

P.L. 86-36

[redacted] A511

If you're walking along the east corridor of the third floor of the NSA Operations Building, you will find a purple door. A sign beside it identifies the organization: A511/COC. What goes on behind that purple door?

If you open that door and walk in at any time of the day or night, you might be confronted with the following scene:

[redacted]

[redacted]

If you ask what's going on, someone may hand you a copy of USSID 115, which tells you that COC handles

[redacted]

But what's going on?

Would You Like a VIP Tour?

Excuse me! I'm the Chief of COC, and I understand your bewilderment. One of my pet peeves is listening to people who speak only in abbreviations, acronyms, and assorted

EO 1.4.(c)
P.L. 86-36

technical jargon. Unfortunately, ours is a highly specialized business that requires a special language combining computer terms with CA expressions and TA phrases, mingled with signals notations and collection management lingo. And then we throw in a little slang of our own from time to time. But I'm happy to translate! Let me offer you a VIP tour, not because you're a Very Important Person -- that's assumed if you open our purple door -- but because you deserve a Very Introspective Peek into the world of COC.

This a very special tour that is not offered every day of the week: it is tailored primarily for your enjoyment and secondarily for your enlightenment. It is also strictly unofficial, so I can feel free to express observations from my personal viewpoint, allowing my boss(es) to disclaim reponsibility for anything I say, which I am sure they wish they could do more often. If, at the end of the tour, you want to know more, please call me on the secure phone, x4341s, and I'll be happy to arrange an official tour.

What Is a COC?

[redacted]

COC, then, is a round-the-clock, current operations center.

Why Is There a COC?

I think too often we plunge into the details of what we are doing without challenging why. Who needs a COC, anyway?

[redacted]

Yes, you may be thinking, but cryptanalysis is not a real-time art. The craft of the cryptanalyst is pursued slowly and methodically, especially in unraveling the mysteries of modern encipherment schemes. Who needs a round-the clock Operations Center to support that?

Your point is well taken, but bear with me a moment longer.

[redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

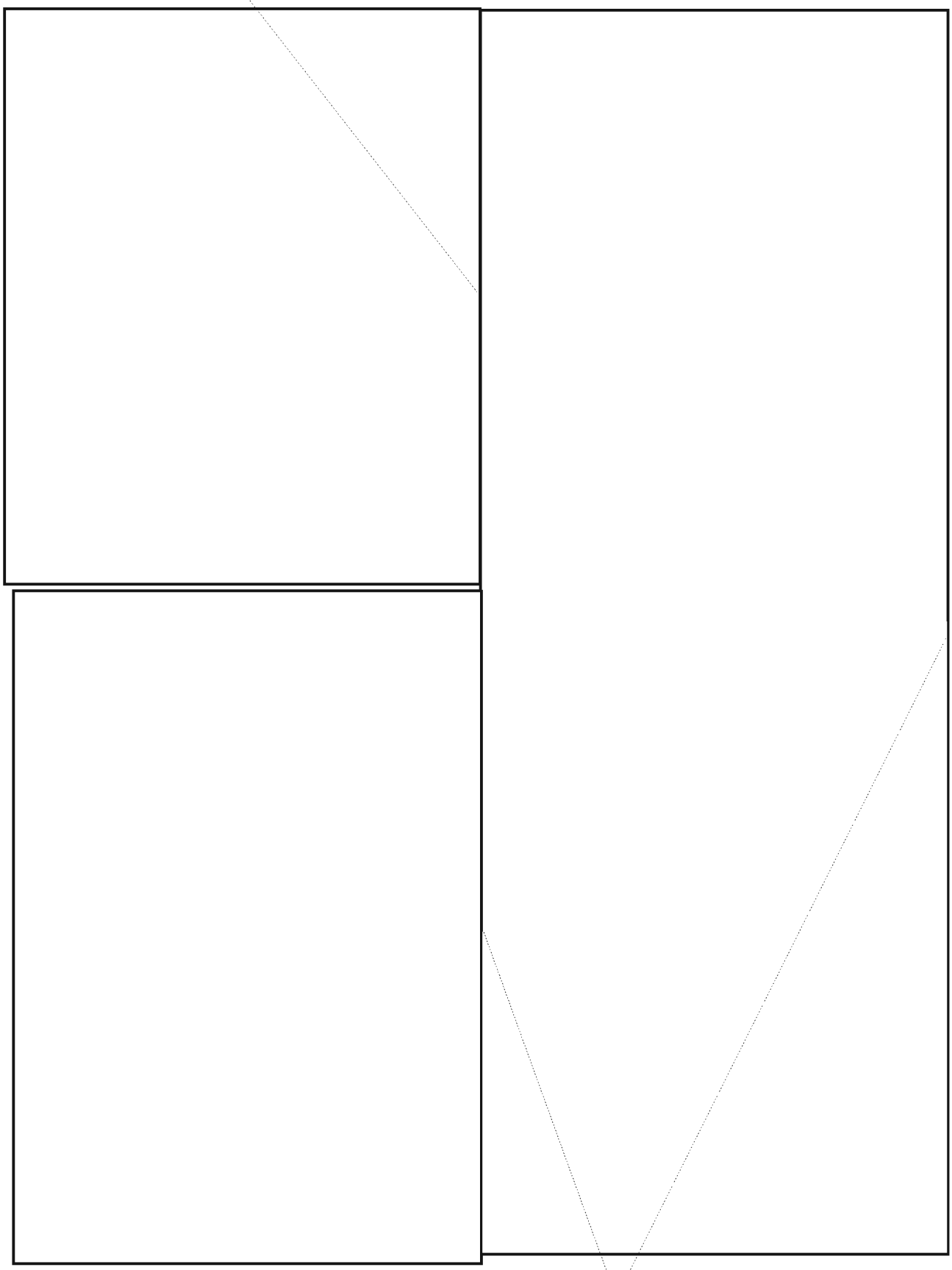
DOCID: 4011702

Who Invented COC?

No one did. Lots of people did. I imagine the concept is about 20 years old, because it takes a while for ideas, even good ones, to get translated into workable processes and organizations.

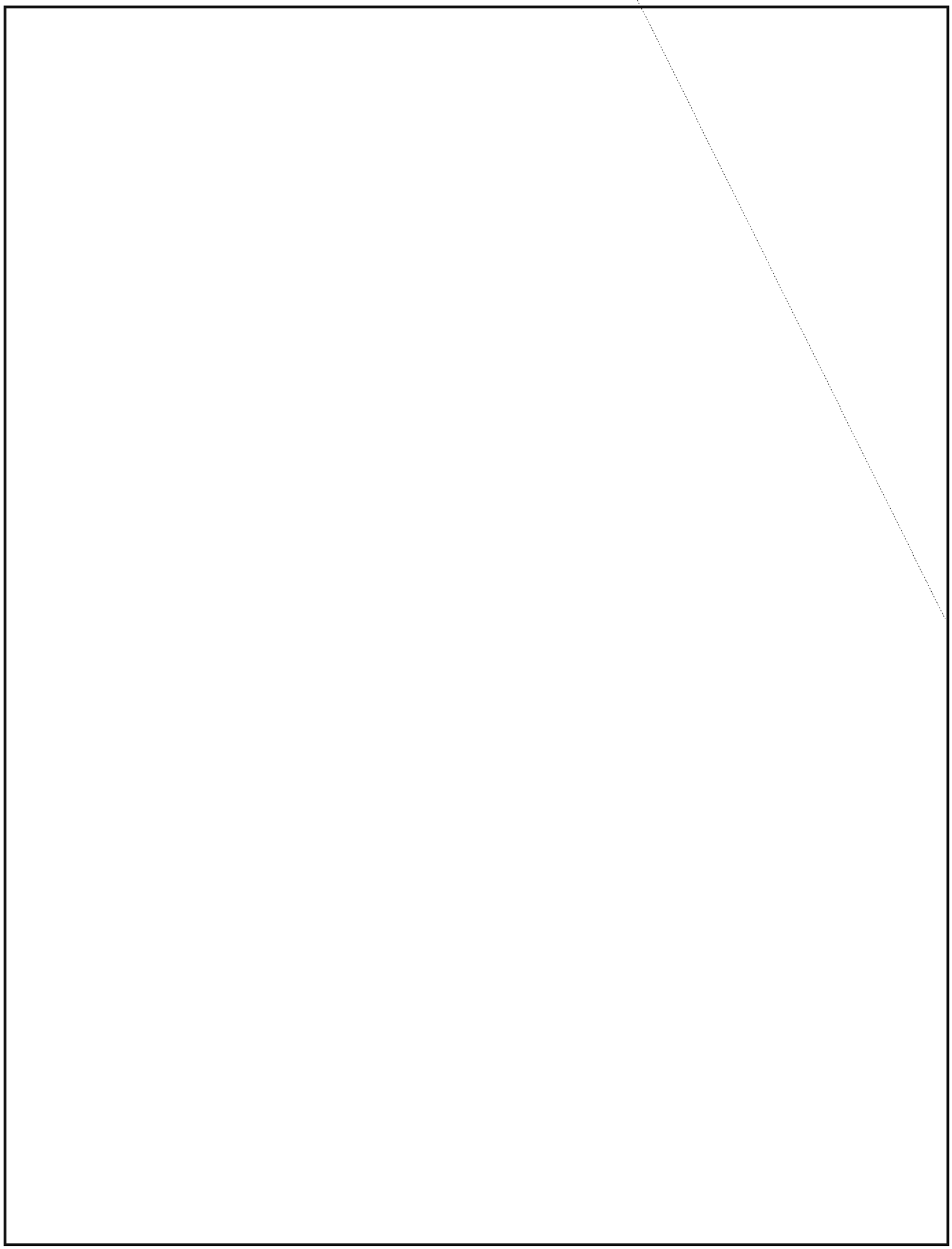
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

DOCID: 4011702
EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



DOCID: 4011702

EO 1.4.(c)
P.L. 86-36

~~TOP SECRET UMBRA~~

[redacted]

Finale

Well, there you have it, a peek into COC from the point of view of the chief of the operation. [redacted] Our players arrive as a heterogeneous assortment of individuals -- old, young, black, white, male, female -- wearing different uniforms and playing different instruments, depending upon their SIGINT training and levels of professionalism. For one brief period in their careers, they join together to play a part upon which the full orchestra depends. I think they play it well.

COC can be a thankless business. Persons in the military can serve a tour at NSA on a watch team and depart without knowing the value of the contribution. Formal recognition for their services and personal appreciation is inadequately expressed. For the civilians who have deep insights into the collection-coordination process and who make repeated judgments upon which successful collection so often depends, the job can be even more thankless, for promotions and opportunities for career advancement are notoriously limited.

I state this not as a complaint, but as a personal observation. I have also observed the value of self-satisfaction as a stimulus for motivation. Despite the criticism received about things in COC that were allegedly mishandled -- and they seem to be endless -- the COC worker can sense that because of his or her personal performance of duty -- on that lovely summer weekend, on that cold rainy night, on that snow day when everyone else got off because of hazardous road conditions, on each of the holidays [redacted] Some of the younger people who have passed through COC discover for the first time in their lives that the highest praise is that awarded by the respect of their peers, even when that praise is unspoken. They depart with a heightened sense of maturity that will prove meaningful throughout their lives.

At least I'd like to think so. End of speech. End of tour.

Oh yes, and one post-mortem. Why didn't I call this a VIP tour of COC? Well, I figure that just about everyone knows where NSOC is. I know that, every day as I pass those paneled walls leading from the escalator to NSOC, survey those splendid seals, and then climb one more flight of stairs to COC, I just have the feeling that I'm working in their attic. It's kind of a lofty idea! ~~(TSC)~~

a/k/a Sam

W. P. Meyer,
T1213

On her birth certificate my granddaughter's name is [redacted] (b)(6) I have never cared for the name, so I have always called her by her initials. When she was three, Sam came to live with me.

Across the alley lived a little girl, the last of four children. Everyone in her family called her "Baby Doll." What her real name was, I do not know.

Recently I proudly took Sam to register for school and discovered that the school wisely asks, "Does your child recognize her name?"

Are you asking yourself, "What's the point? What does this have to do with me?" Well, before you answer yourself, answer these questions:

- Wherever you work in the Agency, do you, too, use pet names, favorite expressions, in-house jokes?
- In your writing, do you obscure your meaning by using jargon and filling paragraphs with unexpanded acronyms that some of your readers might not be familiar with?
- When you know the correct nomenclature, do you use it?
- "Does your work recognize its name -- the description you give it?"

If you *don't* know the correct word, what should you do? You should consult dictionaries, glossaries, and working aids. You should check with experts in the field, search the literature, check the state-of-the-art reports, and then, when all else fails, try the following:

		Telephone
Reference library	T1212	4169s
Technical library	T1213	5750s
Language library	P16/L	8-8873s
NDSC (NSA Data Standards Center) -- for matters pertaining to standardization	P13D	8-8715s

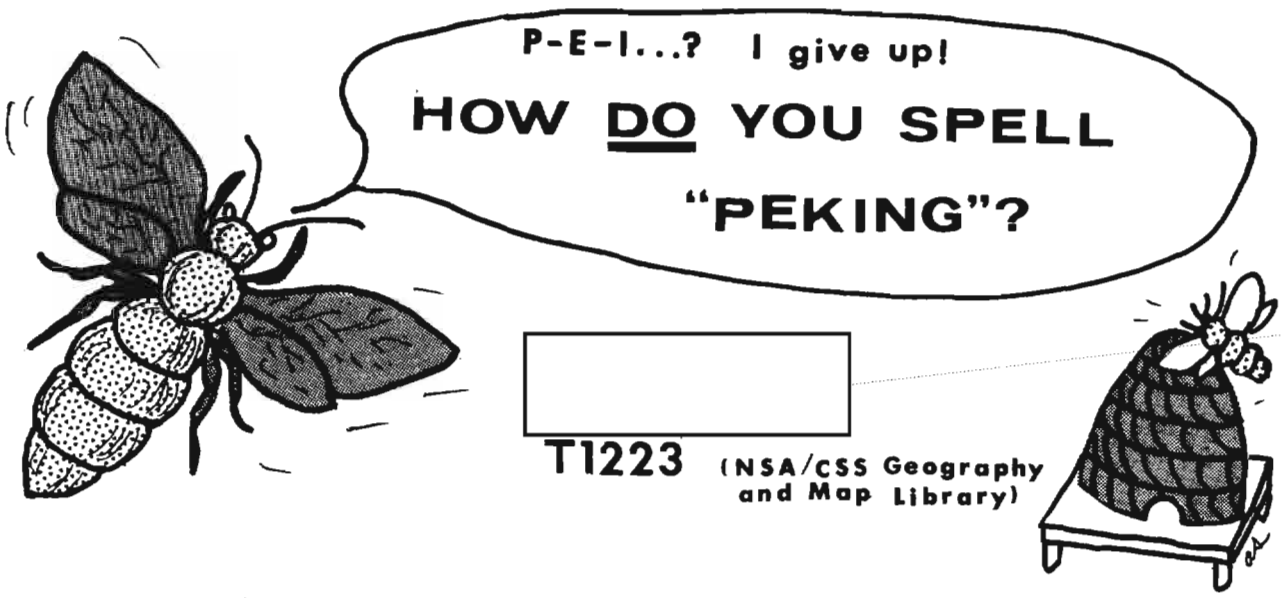
Keep this list near your telephone and add to it as you discover other sources of information.

(U)

EO 1.4.(c)
P.L. 86-36

~~TOP SECRET UMBRA~~

DOCID: 4011702



P.L. 86-36

T1223 (NSA/CSS Geography and Map Library)

Have you ever wondered about the many different ways for spelling the name of the capital of the People's Republic of China (PRC)? Should it be Pei-ching? Peiching? Peiping? Pei-p'ing? Pekin? Beijing? or Peking? Within NSA today, seven different spellings occur in the SIGINT On-Line Information System (SOLIS). Other spellings undoubtedly exist in other data bases. Why all the different versions of the name? Why isn't there one standard name, you ask? Why can't the matter be resolved once and for all?

The fundamental problem is not simple. It involves a tangled web of Chinese history, different systems for transcribing written Chinese characters into roman letters, several languages of China and their many dialects, the influence of foreign powers which once occupied portions of what is now Mainland China and established conventions of their own for spelling Chinese place names, and, last but not least, the emergence of the PRC as a recognized force in world affairs. Although the problem exists with many other Chinese geographic names, the capital of the PRC serves as a vivid example.

The history of the city of Peking[1] is the story of at least six town sites designated by eight place names since the eighth century B. C. Chi was the first known town on the site of modern Peking, followed by five others until the early fifteenth century, when the name Pei-p'ing ("Northern Peace") was changed to Pei-ching ("Northern Capital"). Pei-ching remained the imperial capital of China for almost 400 years. In 1928 the Chinese Nationalists moved the capital to Nanking but by 1949 Peking once again became the seat of government when it was proclaimed the capital of the PRC.

[1]The Western conventional spelling of the name is used throughout this article.

Conventional (nonsystematic) spellings of Chinese place names abound, particularly in popular publications. The reason is that practically any Chinese ideographic character can be rendered in several different roman spellings, depending upon the transcription system used. Moreover, some of the transcription systems are more "scientific" than others, and incorporate diacritical marks that are often omitted in popular publications. But adding to the general confusion in specifically the case of Peking is that *two different names*, that is, two different sets of Chinese ideographs, are rendered by different transcription systems. The chart at the end of this article shows ten different spellings of the place name which occur frequently.

Wade-Giles Transcription

With the opening of China to Westerners in the mid-nineteenth century, there were efforts among missionaries and scholars to make written communication in the Chinese language more intelligible to the Western world. The system devised by Sir Thomas Wade for rendering Chinese in roman letters was later used by Herbert A. Giles in his *Chinese-English Dictionary* of 1912. Since publication of that dictionary, the Wade-Giles system for romanization has been the standard in the English-speaking world, although a few other systems also have had limited use.

Pinyin Transcription

The writing system in prevalent use in China still consists of the traditional Chinese characters, although several times since 1949 the PRC has simplified and reduced the number of characters in use. Within the PRC the Hanyu Pinyin romanization system for Chinese has been under study since about 1952. It is based on the pronunciation of Chinese in the Peking (or northern Mandarin) dialect. Pinyin romanization reached its present form

DOCID: 4011702

in 1958, when it was adopted by the PRC as a means of aiding the spread of literacy in modern Chinese throughout China. Chinese place names can be romanized from Chinese characters using either the Wade-Giles system or the Pinyin system, but generally only in terms of the Peking pronunciation on which both systems are based.

Spread of Pinyin Within the PRC and Internationally

The different names in current use for the city of Peking are typical of geographic name problems involving about three-fourths of the land area and 30 percent of the population of Mainland China. About 5-7 percent of the total population of the PRC uses languages which are not generally written in terms of Chinese ideographic characters. These languages, used in western and northwestern China, extend over more than one-fourth of the area of the country. The PRC government has introduced the use of separate roman script writing systems, each different from Pinyin, for the most widely used languages in those regions: Uighur, Mongolian, Chuang, and Tibetan. However, the PRC roman script form of place names is currently available for only a small number of the most prominent geographic features.

The standard Chinese language based on the Peking dialect is spreading rapidly among the approximately 30 percent of the population of China to whom it is a foreign language. Although Chinese characters continue in prevalent use in the PRC, roman script spellings -- in the form of Pinyin -- are being extended in use and, according to a delegation of U.S. linguists which visited China in late 1974, "progress is being made toward the final long-term PRC goal of replacing the traditional as well as the simplified [ideographic] characters." At the Sixth Session of the United Nations Group of Experts on Geographical Names which met in New York in March 1975, a three-member PRC delegation described the expanding use of Pinyin in China, in PRC international communications, at Chinese railroad stations, and on some maps and charts.

In August 1977 the Third United Nations Conference on the Standardization of Geographical Names, held in Athens, voted almost unanimously[2] in favor of a PRC resolution to accept the Pinyin method of romanization as an international standard. After the voting, the U.S. and U.K. representatives met with the PRC delegation to discuss the difficulties which English-speaking nations would have in any mass conversion to Pinyin. The Chinese admitted that they too would have difficulties, and indicated they had no firm schedule for completing their internal conversion. The U.S. position on the use of Pinyin, expressed through members of the U.S. Board on Geographic Names (BGN), remains essentially as it was at the time of the Athens conference: "Conversion can be anticipated when adequate names information is available" from official PRC sources. The U.K. and Canadian views are similar. No one opposes the Chinese plan to employ Pinyin in China and no one over the long run opposes universal, international use of Pinyin. The problem is timing -- if one is obliged to convert immediately to Pinyin all the gazetteers[3], consisting of more than a quarter million geographic names given in Wade-Giles spellings and to do it without adequate sources. At present there are only two Pinyin sources: one Chinese-produced small-scale map of the PRC containing 3,750 names in Pinyin, and the 1977 edition of the *Atlas of the People's Republic of China -- Romanized Chinese Edition -- Pinyin*[4], containing approximately 20,000 place names in Pinyin. However, for the large Chinese land area involving the minority languages of Uighur, Tibetan, and Mongolian, the rules of transliteration ("pinyinization") and current sources are not available to geographers outside China. Therefore it is impossible to work out the Pinyin spellings of place names in those regions.

Interim Solution

Both theoretical and practical aspects of standardization of Chinese place names are the serious concern of members of the U.S. Board on Geographic Names and its U.K. counterpart, the Permanent Committee on Geographic Names for British Official Use (PCGN). If the English-speaking world is forced to abandon suddenly one standard (i.e., the Wade-Giles system) before having sufficient geographic-names information with which to implement confidently the new standard (i.e., the Pinyin system), only chaos will result. For the immediate future, members of the BGN believe that they must continue to use the Wade-Giles system as a standard until such a time in the future when considerably more than the present 20,000 Chinese place names are available in Chinese sources using Pinyin. In the interim, where critical, the BGN suggests use of dual names: the Wade-Giles standard rendition

[2]The United States and the United Kingdom abstained; only Guatemala voted "No" on the resolution.

[3]The U.S. Board on Geographic Names *Official Standard Names Gazetteer of China* (1968, two volumes) contains 108,000 geographic names, all romanized by the Wade-Giles system. The U.K. PCGN also uses similar gazetteers.

[4]*ZHONGHUA RENMIN GONGHEGUO FEN SHENG DITUJI--HANYU PINYINBAN.*

EO 1.4.(c)
P.L. 86-36

followed by the Pinyin equivalent (enclosed within brackets) for those place names given in the 1977 *Atlas*. Admittedly this procedure is awkward, but it is preferable to uncontrolled use of two separate systems or the complete abandonment of the old standard in exchange for a new and highly incomplete standard.

Today there are at least ten versions of the name of the capital of the PRC -- more than were used singly over the 2,800 years of Chinese history! The chart below shows how easy it is to derive this large number of alternate spellings by using two systems for romanizing the two different sets of Chinese characters, and then adding various foreign conventional forms and other spellings with or without diacritical marks.

So much for the problem and how it came to be. How does one resolve or limit the problem?

First: Adhere to the policy and recommendations on standard geographic names issued by the U.S. Board on Geographic Names. This is mandatory under Public Law 242, 80th Congress.

Second: Devise, for use in existing NSA/CSS data bases, methods that will equate the variants spellings of geographic names for the identical populated place or geographic feature.

[redacted]

Fourth: When in doubt about the standard approved version or proper spelling of geographic names within China, or in any other country, consult the specialists in the NSA/CSS Geography and Map Library (T1223), either in person or by phone -- Room 1E145, 5585s.

DIFFERENT SPELLINGS OF THE NAME OF THE CAPITAL OF THE PEOPLE'S REPUBLIC OF CHINA WITH NUMBER OF OCCURRENCES IN SOLIS (EARLY 1978 SAMPLING)

Chinese characters, with meaning	*"Popular" (conventional) spellings*		*"Approved" spellings -- U.S. BGN & U.K. PCGN*	*"Official" PRC spelling*	*"Imitated pronunciation" spellings, with or without diacritics*
	English	*Spanish, French*	*(Wade-Giles)*	*(Pinyin)*	
北京 -- "Northern Capital"	Peking[1] (1069)	Pekin[2] (0)	Pei-ching (3)	Beijing[3] (0)	Peiching (4371) Bei-jing[3] (0)
北平 -- "Northern Peace"	Peiping[1] (84)		Pei-p'ing[2] (0)	Beiping[3] (0)	Peip'ing (865)

[1]Spellings originated under the Chinese Post Office System for converting Chinese geographical names on the international level and widely used during the first half of the twentieth century; still used as the conventional forms in English-speaking countries.

EO 1.4.(c)
P.L. 86-36

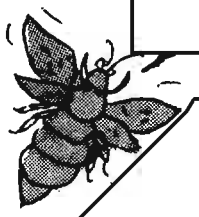
[redacted]

DOCID: 4011702

EO 1.4.(c)
P.L. 86-36

[redacted]

T124 P.L. 86-36



[redacted]

[redacted]

[redacted]

~~(SC)~~

P.L. 86-36

Solution to NSA-crostic No. 19

(CRYPTOLOG, November 1978)

J[ack] Gurin, "Let's Hear It For Humans," *Cryptologic Spectrum*, Fall 1977, Vol. 7, No. 4:

"To illustrate human factors engineering with a familiar example, you need look no further than the automobile. . . Serious accidents have resulted when the driver, while proceeding at high speed, shuts off his headlights in the belief that he is just operating the cigarette lighter."

(U)

Answer to A SMALL PROBLEM

by [redacted] P14

P.L. 86-36

(CRYPTOLOG, November 1978)

LOCAL HOUR

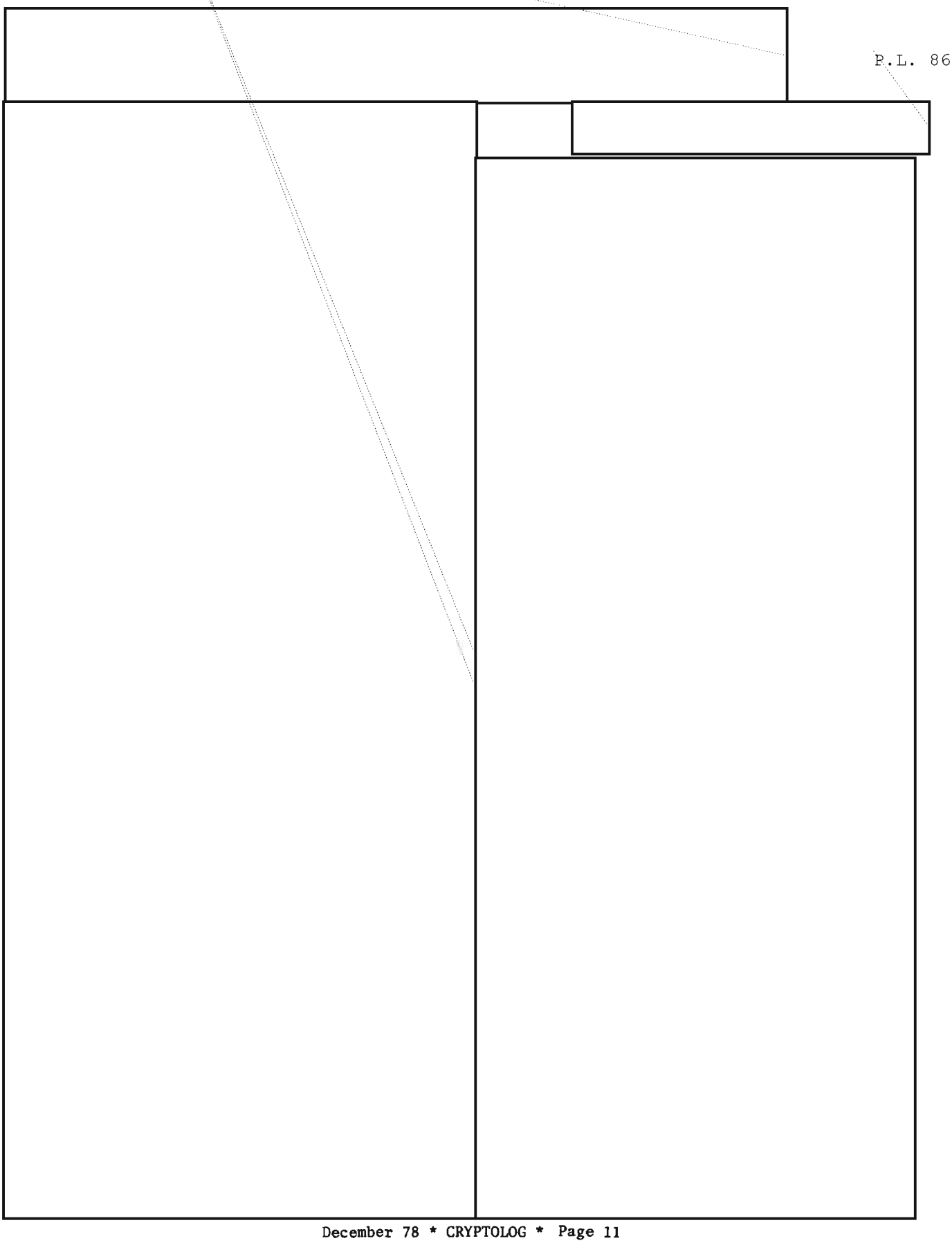
	0	1	2	3	4	5
00	L	A	C	N	W	M
01	C	B	Q	I	S	
02	Q	P	N	W		
03	N	H	I			
04	I	V				
05	W					

(U)

EO 1.4.(c)
P.L. 86-36

DOCID: 4011702 EO 1.4.(c) P.L. 86-36

P.L. 86-36



DOCID: 4011702

P.L. 86-36
EO 1.4.(c)

~~SECRET SPOKE~~

THE EDITOR'S PAGE (MORE OR LESS)

"No, No, Nanette!" Means "Yes"?

By A.J.S.

As the editor of a publication that prides itself on being highly readable, often colloquial, but always grammatical, I am sometimes surprised when people write letters to the editor carping about "errors" they have found. Does it surprise anyone to hear that there are other people who think a preposition is not a good word to end a sentence with? Or to hear that some people object to sentences beginning with "or" or "and"? Well, several months ago I was surprised to get a copy of CRYPTOLOG returned to me with one sentence underlined, "This is no radical concept that has never been tried before." The person returning the copy added a note, "Apparently, inclusion of a by-line has not guaranteed error free writing. I believe a double negative has managed to slip thru." I have to admit that I sent back a somewhat petulant note that mentioned "weasel words" such as "apparently," and also explained that having two negative words in one sentence does not make a "double negative." Leaving out the snappish remarks, this is what I wrote:

> "The sentence 'This is no radical concept that has never been tried before' means exactly what John Mollick said -- it's *not* an idea that hasn't been tried before (it *has* been tried before -- his next sentences say so: 'A number of sister agencies have long attached the names of their analysts to their products. . .').
>
> "You seem (note my weasel word?) to think that there is something *wrong* with two negatives in a sentence. There's nothing wrong if that's what you mean. Take, for example, a nasty lawyer trying to discredit the testimony of a young lady who is posing as a sweet innocent thing, but who really has been through the wringer: 'Ladies and gentlemen of the jury, the witness is no innocent young thing who has never been kissed.' That means she's *been* kissed -- and, in fact, the lawyer is casting aspersions on her reputation by using a literary trick called 'litotes.' It's using *negatives* to say what you want to say (a sneaky trick akin to the use of weasel words). 'I won't mention the fact that you lost my tennis racket. I won't mention the fact that you told my boy friend "She's no innocent young thing who's never been kissed." I won't mention the fact that you're always leaving things dripping over the towel rack. But one thing I *do* want to mention is the awful habit you have of "correcting" me when I'm not wrong!'"

The world must be full of "double-negative" spotters, because the *Washington Star* of 27 March 1978 printed the following letter:

> "As a teacher of anti-gobbledygook courses for government agencies, I notice that in the last paragraph of your 'business profile' on 'Grammarians, Inc.' your reporter has Ms. Shapiro committing not just a *double* negative, but, if I am not mistaken [don't you just love those weasel words?], a *quadruple* negative: 'People really have *no* business *not* knowing how to write. . . because there's *not* an occupation in the entire world where a competent knowledge of language *isn't* useful.' A true mind-boggler! ('Occupation . . . where' is suspect too.)"

What is truly mind-boggling is that, in the 12 April 1978 issue of the *Star*, Ms. Shapiro, instead of saying, "Well, you *are* mistaken!", agrees with the nut, but blames the reporter who misquoted her. Discussing the "severe shock [that] occurs upon witnessing the transformation of one's spoken words into print," Ms. Shapiro states,

> "The 'quadruple negative' pointed out by Reader Mary Bradford is a composite of several remarks made by both Ms. Candage and me. The opinion is ours; the phrasing is not. In sum, we at Grammarians, Inc., readily admit to a rare *faux pas* when speaking; however, we assure you that, when writing, we are as close to infallible as Strunk and White could possibly desire."

Swinging back from the outside jungle to the world of CRYPTOLOG, I want to give our readers this assurance: They may sleep easily at night knowing that the members of the Board of Editors are fully capable of spotting a true double negative whenever they see one, although they haven't seen none yet.

(U)

~~SECRET SPOKE~~

DOCID: 4011702

P.L. 86-36

S14

12. PUBLICATIONS *(List titles; do not confuse this with reports prepared as a regular part of the job)*

DATE

SOME TIPS ON GETTING PROMOTED

Article based on talk given in April 1978 to WIN (Women in NSA)

CRYPTOLOG, Dec 1978

Promotion. The word inevitably stirs response of some kind in every red-blooded NSA employee: hope, pleasure, challenge; despair, frustration, disappointment; even inertia, resentment, resignation. Despite disparate views on promotion, most people share -- openly or secretly -- a common desire to be promoted. And many also share, I think, a common lack of understanding about the promotion process here at NSA and a lack of knowledge about the part they play in it.

This article mainly addresses promotions to grades 13 through 15 and discusses two subjects which are fundamental to those promotions -- Personnel Summaries and Promotion Files. Both are critically important to you, the employee, because they are critically important to the promotion process here at NSA. Witness these two points:

- *your Promotion File represents you to a promotion board,* and
- *you personally write only one document in that file -- your Personnel Summary.*

Promotion Files described in this article are the ones regularly kept only for people of grades 12 through 14, for use by the three NSA-wide Boards that handle promotions for grades 13 through 15. These Promotion Files are described in the final section of this article. Promotions below grade 13 are handled by local organizations whose practices vary on maintenance of personnel files and their use in the promotion process.

Personnel Summaries, on the other hand, are important to everyone, regardless of grade. For grades 12 through 14, the formal promotion process requires that every Promotion File, hence every Personnel Summary, be reviewed during every promotion cycle. For grades up through 12, some local promotion boards use them as well. I recently chaired a local promotion board in my parent organization, S1, and we routinely reviewed Personnel Summaries of grades 2 through 11 each time we met. Personnel Summaries have still other uses: for overseas assignments; for transferring to a new job; for some types of training. Whenever, in fact, official information on you and your career is needed, the Personnel Summary may be used. The first and major part of this article presents tips on how you should write your all-important Personnel Summary.

The ideas in this article are my own. I am not an expert on personnel matters and do not mean to appear to be. Though I am currently serving on the Agency Grade 14 Promotion Board, my experience there has simply confirmed long-held impressions and reinforced my belief about the critical importance of the two topics covered in this article.

Personnel Summaries

Many consider Personnel Summaries to be the bane of their existence. Some don't take them seriously. Others fill them out casually. And most of us write them because we're forced to. Whatever you feel about Personnel Summaries, you should recognize why a Personnel Summary is important, who is responsible for filling it out, when it should be filed, and how to get it filed.

Why Important?

Why is your Personnel Summary important? Because it is an essential document in your Promotion File, the one that describes your complete NSA life: your jobs, your accomplishments, your training, your awards. It is no secret what things are deemed desirable for promotion. The information you provide in your Personnel Summary constitutes a list of the very things judged important when selecting people for promotion, *to any grade.* Your Promotion File represents you to the Board; it is one of the most important sources of information about you available to them. Board members cannot be expected to have personal knowledge of you in a large Agency like NSA. True, if you are fortunate enough to be nominated for promotion, then a written recommendation about your accomplishments and qualifications is included in your Promotion File. Otherwise, *your Personnel Summary is it!* Since every Promotion File contains one and you write it, it is your chance to describe what you have done. No one knows it better. And if you do not say it, it may not get said at all.

Who Is Responsible?

Who is reponsible for your Personnel Summary? *You* are! You are responsible for filling it out initially (within 90 days after promotion to grade 12 through 14) and then for updating it. Do not expect your office to remind you. It is your responsibility. Though Personnel Summaries are not required for them, I also urge people in grades *below 12* to fill out Personnel Summaries and to update them periodically. Get into the habit now, for it is easier to do it routinely and gradually than suddenly in one big lump when you do become a 12. Also, I think it shows supervisors that

you are a person of initiative with serious career intentions.

When to File

As I mentioned in the previous paragraph, you are required to update your Personnel Summary within 90 days after promotion to grades 12 through 14. I recommend you also do it whenever a major event occurs, such as when you: transfer to a new organization or job; become a supervisor or assume major new duties; receive a major award, professional certification, or educational degree. Otherwise, plan to do it annually, in synchrony with the promotion board cycles. Currently the grade 13 Board meets four times a year; the grade 14 and 15 Boards meet twice. If your updated Personnel Summary is *in your file* by 1 January or 1 July, you will satisfy all Boards. (Since Promotion Boards are appointed for a calendar year, I recommend January.) I simplify updating my own Summary by following a practice I use to keep track of income tax deductions: whenever anything of importance occurs, I jot it down on a slip of paper with the date and stick the paper into a file. When the time comes to update, I have all the information at hand and the job is nearly done.

Tips on How to Write a Personnel Summary

The following paragraphs describe ways to write a Personnel Summary. These are my personal ideas, and some people -- even you -- may not agree with them. So be it. But I hope to stimulate you to think seriously about Personnel Summaries and to try to help you to write a better one. My aim is to give you a start and hope that you will take it from there.

My best general advice is to be succinct. Say what you have to say briefly, concisely and clearly. Do not write the Great American Novel and ramble on for 20 pages. On the other hand, avoid being too brief and selling yourself short. (I am surprised at the number of people who write one-liners!) Do not try to upstage Agatha Christie and write a mystery story, but avoid too much excruciating detail. Write your Personnel Summary so that a busy person, who is reading hundreds of Promotion Files, can understand and appreciate it quickly and, you hope, be impressed enough to single out your file for special consideration.

Personnel Summaries are written on Form P3267 (REV Feb 76) which is available in your office or from the NSA Supply Room. The first page contains seven items. Fig. 1 shows the first four:

AS OF (date)	1. NAME (as it appears on official records) (Last, all capital letters)		(first)		(middle)
Dec 1978	Smith		Jane		Anne
2. EMPLOYEE IDENTIFICATION (SSN)	**3. CRYPTOLOGIC SERVICE** MILITARY (i.e., ASA, AFSS, NSG, NSA) (years)	(months)	CIVILIAN (years)	(months)	**4. TOTAL FEDERAL SERVICE**
123-45-6789	3	2	12	9	15 yrs 11 mos

Fig. 1

The "As of" date should never be over a year old. Some files contain Personnel Summaries so ancient that the paper has turned yellow! An out-of-date summary raises some rather unflattering -- to you -- questions in the mind of the reader. Are you lazy? Are you so disorganized you cannot remember to update it? Don't you care?

One sees many Personnel Summaries with only the dates changed -- the correction tape over the date is obvious in the reproduced copy. This is often done, and rightly so, to save retyping when there are no major changes to report. But what if there *are* important changes in your job and you don't record them? Look below at Item 6, "Experience" (Fig. 2), taken from a *supposedly* current Personnel Summary:

6. NSA/CSS OR SCA CIVILIAN EXPERIENCE				
TITLE	GRADE	DATE OF ACTION	AGENCY	ORGANIZATION
A. CURRENT ASSIGNMENT (Functional/Job Title, e.g., Chief, Data Storage Equipment Division; if none, use job title reflected on 3150 or SF 50)				
Traffic Analyst	12	Jan 1976		B111
B. TITLE OF LAST PROMOTION				
Traffic Analyst	12	Apr 1970		B9
C. INITIAL ASSIGNMENT				
Analyst	5	Jun 1958		ALLO

Fig. 2

To the eye, Item 6 in Fig. 2 looks fine. However, this person is no longer a Traffic Analyst in B111. He has transferred to a new job -- a supervisory one -- and he is now Chief, Processing and Analysis Division, X35. *But how is the Board to know?* The problem is magnified if this person is nominated for promotion. The documentation that accompanies the nomination describes the person's *current* job, with the result that the two documents -- the nomination and the Personnel Summary -- do not match. How does that look to a Board? Again, what does it say about you and your sense of responsibility?

When listing your current job title in Item 6, be sure to use the *functional* job title if you have one. For example: D/Chief, Data Storage Division; Project Manager for XXXX; Russian Language Instructor. Otherwise, use job titles as shown on the form.

Now let's go back to Item 5, your educational record (Fig. 3):

5. EDUCATION *(List most recent first)*

SCHOOL *(Include Joint or Senior Service Colleges; also, any substantial work done toward a degree, but for which no degree was awarded)*	DEGREE	MAJOR FIELD	DATES *(If great span of time involved, indicate reason, e.g. (Night))*
University of Maryland	MA (20 credits)	International Relations	1976-78 Nights
Armed Forces Staff College	Diploma	--	1975
University of Maryland (Cum Laude, Phi Beta Kappa, Honors in History)	BA	History and Political Science	1971-1973
Anne Arundel Community College	Assoc.	History	1960-71
Bowie High School	Diploma	College Prep	1969

Fig. 3

List these in reverse chronological order, with the most recent first. Include all education for which you earned a degree and use "Diploma" to indicate completion of a joint or service school. Also include substantial work toward another degree. If any of these took extended time, indicate why (as "Nights"). And I suggest you state any graduation honors here, to highlight them.

Item 7, "Commendations and Awards," should also be in reverse chronological order. Fig. 4 shows some examples of the kinds of things to include.

7. COMMENDATIONS AND AWARDS *(e.g. Meritorious Civilian Service Awards, Outstanding Performance Appraisals, Letters of Commendation from Chiefs of major organizations or higher) (List most recent first)*	DATE
Letter of Appreciation, Chief A	1978
Level 7 Performance Rating	1977
Outstanding Performance Ratings	1975, 73, 69
QSI	1974
SSWP	1968
Meritorious Civilian Service Award	1965
NCS Teacher of the Year	1960
First Prize, CLA Essay Contest	1959
NSA Scholarship	1958

Fig. 4

Include Letters of Appreciation only if they are from an Office Chief or higher (for grades below 12 I think this rule may be relaxed) and be sure that copies of such letters are in your Promotion File. List level-7 performance ratings, but not level-6. Also list any special Agency awards or scholarships you may have received. Professionalization certifications belong in Item 16, and extracurricular activities should be entered in Item 14 -- do not include them here.

Page 2 of Form P3267 contains two items. At the top, Item 8 provides space for summarizing your "Current Assignment" (Fig. 5). Begin this paragraph by giving your functional job title, the name of your immediate organization, date of appointment, and names of ascending key organizations.

8. SUMMARY OF CURRENT ASSIGNMENT

D/Chief, Support Staff (Z13), Office of Facilities (Z1), Computer Services Organization (Z).

Since April 1973 Mrs. Jones has been responsible for managing. . .

Fig. 5

Then list your major responsibilities, following these recommendations:

- Use narrative style (not outline form),
- Use complete sentences,
- Use third-person forms (not "I was responsible for...," but "Mrs. Jones was responsible for...")

Note that your supervisor's signature is required in Item 8 as verification.

Item 9, at the bottom of page 2, is the "Summary of All Previous Civilian and Military Service of a Cryptologic Nature." This is probably the most difficult part of the form to fill out. The longer your career, the more you have to tell about. If there is not enough space provided in Item 9 to hold all the information requested, you should use as many additional plain sheets as necessary, labeling each with your name, SSN, and page number.

This is likely to be the longest section, so it is important to try to make it clear and readable. You do not have to be an accomplished writer or even to have any special writing skill. Just be direct, factual, and as concise as possible. Follow instructions given above for Item 8 (use narrative style, complete sentences, third-person forms). In addition, follow these suggestions:

- Use *chronological* order ("Begin with oldest assignment and end with most recent"). Note that this is *not* "reverse chronological order," as in some of the other items;
- Use one paragraph per job;
- Start paragraph with vital information: dates, functional job title, immediate organization and up;
- Identify organizations, projects, systems, etc.

Notice that I said to identify "organizations, projects, systems, etc." Otherwise, you end up writing a mystery story, like this one:

> "From August 1960 to January 1964, Mr. Smith was Chief of A13 where he was responsible for managing all aspects of Project SUCHNSUCH. He also provided technical assistance to several important systems under study by another division: XYZQ and ABCJ."

The only really clear thing in this paragraph is the date! Who remembers what A13 was in the early 1960s? What in heaven's name was SUCHNSUCH? What were systems "XYZQ and ABCJ"? And so on! How much clearer, and how much more professional if this had been written instead (Fig. 6a):

9. SUMMARY OF ALL PREVIOUS CIVILIAN AND MILITARY SERVICE OF A CRYPTOLOGIC NATURE *(List in chronological order - begin with oldest assignment and end with most recent; indicate location, functional/job title and dates)*

From August 1960 to January 1964, Mr. Smith was Chief of the Nonesuch Reporting Division (A13) in the Office of Overall Reporting (A1) in the General Analysis and Reporting Group (A). He was responsible for managing all aspects of Project SUCHNSUCH (full-text automation of Nonesuch reports) and provided technical assistance to several important systems under study by another division: XYZQ (system for automating. . .) and ABCJ (system for . . .).

Fig. 6a

If you wish, you may use a space-saving format, with an offset header (for dates, jobs, and organizations) followed by a colon and and a list, as in Fig. 6b:

9. SUMMARY OF ALL PREVIOUS CIVILIAN AND MILITARY SERVICE OF A CRYPTOLOGIC NATURE *(List in chronological order - begin with oldest assignment and end with most recent; indicate location, functional/job title and dates)*

August 1960 to January 1964
Chief, Nonesuch Reporting Division (A13), Office of Overall Reporting (A1),
General Analysis and Reporting Group (A):

Mr. Smith was responsible for managing: SUCHNSUCH (full-text automation of Nonesuch reports), all reporting on . . ., and providing technical assistance to another division on several important systems, such as XYZQ (system for automating . . .) and ABCJ (system for . . .).

Fig. 6b

These may seem like small things to you, but they have a big impact on improving the readability of your Personnel Summary. You do want people to read it, don't you? As the final test, I recommend that you ask a friend to read your Personnel Summary critically to

DOCID: 4011702

see if it is indeed clear and to the point. Preferably that friend should pretend that you are *not* a friend, but a complete stranger who wants to know everything about you. Does your Personnel Summary present you as a clear-writing (and, presumably, clear-thinking), forceful, direct person, or as an imprecise, vague person carrying out "various" unexplained duties? Rewrite your Summary, and especially Item 9, until anyone who reads it -- not just your friends who have known you for years -- can get a clear picture of what you have done and why you are promotable.

Page 3 of the form contains four items, the top three of which are often ignored -- or so it seems when they are so frequently left blank: "Field Assignments," "Related Experience" and "Publications." If you have pertinent information on any of these, put it in.

For Item 10, "Field Assignments" (Fig. 7), be sure to give both the organizational and functional titles and the inclusive dates. These items are in *reverse* chronologcal order. Incidentally, regular updating of Personnel Summaries seems to be a special problem for people assigned to the field. Their Personnel Summaries are rarely updated while they are away from Fort Meade/FANX and consequently the promotion boards often have no knowledge whatever about what the person is doing during an important 2- or 3-year period. I urge people to file yearly updated Personnel Summaries while they are on field assignments.

10. CRYPTOLOGIC COMMUNITY FIELD ASSIGNMENTS *(CONUS and Overseas) (List most recent first)*			
ORGANIZATION	LOCATION	FUNCTIONAL/JOB TITLE	DATES
F06	Timbuck	Station Chief	1975-78
F99	Eden	Engineer	1969-72
F17	Nowhere	Analyst	1965 (Jan-Mar)

Fig. 7

For Item 11, "Other Civilian/Military Experience" (Fig. 8), include those things that show you possess skills that may apply to your NSA job, such as teaching, managing, and organizing. These are also in reverse chronological order. For example:

11. OTHER CIVILIAN/MILITARY EXPERIENCE WHICH MAY BE RELATED TO AN NSA/CSS OR SCA POSITION			
ORGANIZATION	LOCATION	FUNCTIONAL/JOB TITLE	DATES
Army Reserve	Ft. Meade, Md.	Platoon Leader	1971 to present
G.W. Univ.	Washington, D. C.	Lecturer in Computer Science	1968-1970
Summer Camp	Arlington, Va.	Director	1965

Fig. 8

Item 12 is "Publications" (Fig. 9). I am disappointed that so few files list any publications. Since publications *are* included in the Personnel Summary, NSA must consider writing to be an important skill. Managers, for example, spend a lot of time writing. And good writing comes from practice. Fortunately for us, NSA offers many opportunities to publish. If you have been looking for places to express your views, here they are:

NSA Technical Journal
Cryptologic Spectrum
CRYPTOLOG
Field Information Letter
Essay Contests (Learned Organizations -- CMI, CLA, CAA)
CISI Spring Conference
Cryptologic History Series
NCS courses
Informal Agency newsletters such as *SOLIS Newsletter* and the previously published *Bits and Bytes, Dragon Seeds, Keyword, Quarterly Review for Linguists.*

The editors of all these publications welcome your contributions. Try to have some published works and major reports (though not regular ones produced as part of your job) to list on your Personnel Summary. It just may help to attract attention to your File!

12. PUBLICATIONS *(List titles; do not confuse this with reports prepared as a regular part of the job)*	DATE
"Project SUCHNSUCH -- A Personal View" -- article based on talk given in April 1978 to Computer and Information Sciences Institute (CISI)	CRYPTOLOG, Dec 1978

Fig. 9

DOCID: 4011702

The next three sections, all part of Item 13 on the form, are meant to show "Highlights in the Area of Self Development" in your professional life -- past, present, and future. The format is the same for all three sections. Fig. 10 gives some examples for "A. Past." List here the things that are completed, such as past membership in professional societies and education not already listed in Item 5. Courses taken at NSA belong here. Follow the example and identify the courses by title and course number. In the rightmost column, you can indicate things like "Top student" or special honors. You can leave this column blank if nothing applies.

13. HIGHLIGHTS IN THE AREA OF SELF DEVELOPMENT: *(Chronologically list all formal NSA/CSS/SCA, college level or technical courses (military or civilian) as well as membership in either NSA/CSS/SCA or external professional societies) (Exclude those for which a degree was subsequently awarded)*

	SUBJECT/SOCIETY	PLACE	DATES (from - to)	DURATION OR LENGTH	DEGREE	SPECIALTY/ OFFICE HELD
A. PAST	Zeta Eta Eta (French Honorary	University	1965-68	--	--	President, 1967
	MS-111 (Briefing Skills)	NSA	1968	49 hrs	S	--
	MG-444 (Management Analysis	NSA	1971	120 hrs	A	Top student
	CMI	NSA	1971-present	--	--	Member

Fig. 10

The first two items on page 4, the last page of the form, are "B. Present" and "C. Future" highlights in your self-development (sections not reproduced here). These sections are to be filled out in the same manner as "A. Past." Future plans might include such things as your plans to attain another specified certification, change career fields, join a professional society.

Item 14, "Other Achievements" (Fig. 11), provides space for showing your self-development in your nonprofessional life. Many people leave this blank. If you do, I think you are missing a big opportunity to provide a rounded picture of yourself to the Promotion Board. If you are active in areas like those listed below, I encourage you to list them. Show by your non-job-related activities that you have other interests -- and other talents.

14. OTHER ACHIEVEMENTS *(In brief, list all NSA/CSS/SCA affiliate endeavors, which are not necessarily a part of your assigned duties, i.e., Civilian Welfare Council, GEBA, NSA/CSS/SCA club, etc; Civic or Community efforts may be included)*

ACTIVITY	INCLUSIVE DATES	CAPACITY IN WHICH SERVING/SERVED
NSA:		
Civilian Welfare Council	1967-1969	B Group representative
Credit Union	1970-1973	Member, Board of Governors
GEBA	1976-present	Member, Board of Directors
NSA Jazz Band	1970-present	Member
Travel Club	1972-present	Member; President, 1976-78
United Givers Fund Campaign	1977	Keyman, B Group
Community:		
Church, Scouts, recreational activities, civic associations, PTA	(Provide appropriate information)	

Fig. 11

Item 15 (not reproduced here) provides space for you to list your job-related or self-improvement "Reading Achievements" -- in-house publications, professional journals, foreign-language material. Please do not list your pleasure reading, especially not "Playboy." Board members have seen that one so often, they are weary of it!

"Professionalization" certifications are to be listed in Item 16 (Fig. 12). If you have more than one, be sure to list them all, with the dates awarded. If you are about to receive still another, note this in parentheses, as shown:

16. PROFESSIONALIZATION *(List professional certification(s))*

CERTIFICATION TITLE	CERTIFICATION DATE	CERTIFYING PANEL (S)
Cryptanalyst	12 Jun 1970	Cryptanalysis Career Panel
Education and Training Officer	1 Sep 1973	Education Career Panel
Traffic Analyst (Lack only Part 3 of PQE for certification -- scheduled to take test in Nov 77)		

Fig. 12

DOCID: 4011702

Finally, sign the form, date it, and affix the proper security classification. Take this last responsibility seriously and do it carefully, seeking help from experts if you need it. Underclassifying or overclassifying looks bad to a Board because Boards expect that by grade 12 you should know how to classify correctly or know where to find help.

Instructions for filling out Personnel Summaries are contained in the *NSA Personnel Management Manual*, Chapter 302B (Jul 76), which every major office has. Your own office will handle the filing of your Personnel Summary for you. It will reproduce multiple copies of it, some for retention in local organizational files, one for you, and (for grades 12 through 14), some for sending through channels to your Promotion File in M3.

Promotion Files

Promotion Files are not to be confused with Personnel Files, often called "201 Files." The Office of Personnel, specifically M3, maintains both. There is an official Personnel File for every NSA employee. It documents all formal activity in connection with your NSA life: hiring, performance appraisals, training, job or organizational changes, etc. There are official Promotion Files only for employees in grades 12 through 14. Local organizations often maintain abbreviated versions of the 201 File on all their employees (and some may also keep a Promotion File). Official Promotion Files are the files that are being discussed here -- the files used by the three Agency Promotion Boards when considering people for promotion to grades 13 through 15. I am going to tell you what should be in your Promotion File, how you can make arrangements to see yours, and how you can update it.

Your Promotion File should contain:

- Personnel Summary (current within one year);
- Certification documentation (in the form of a computer printout or a letter from the certifying Panel);
- Recommendation for promotion from Key Component, if you are recommended. (Since Promotion Files are shown to you intact, with nothing removed, you can see the recommendation on you if there is one, or know you are not currently being recommended if there is not.)

In addition, your Promotion File should contain, *for your current grade only* (information from previous grades is purged):

- Performance appraisals;
- Inventory of Attributes (If you are a 12 or above, this is part of your official Performance Appraisal. However, you may never have seen it or even know it exists because, until recently, it was a private document and was generally not shown to employees. Nowadays the sheet is green but it used to be yellow, and many files still contain copies of "yellow sheets").

Fig. 13 shows the form for the Inventory of Attributes. Rating is on a scale of 00 through 99, and space is provided on the right for narrative comments. Like the information in a Personnel Summary, the items in the Inventory of Attributes

(24)	**A. Innovativeness:** Consider how well the individual provides problem solutions, shows ingenuity and creativity and pioneers in seeking new ways to complete work faster and more accurately.	
(25)	**B. Effectiveness in working with people:** Consider how well the individual meets and deals with others, his/her effectiveness in establishing and maintaining working relationships with peers, subordinates and supervisors.	
(26)	**C. Drive and initiative:** Consider the extent to which the individual demonstrates attributes such as forcefullness, aggressiveness and enthusiasm.	
(27)	**D. Personal characteristics:** Consider all personal characteristics as they affect the individual's job performance.	
Present (28) / Higher (29)	**E. Subject-matter knowledge:** Consider the individual's depth and breath of knowledges and skills required at his/her present and next higher grade.	
(30)	**F. Advancement potential:** Consider how the individual compares with others for advancement to a position of greater responsibility and his/her overall capability for progression within the career field.	

Fig. 13

constitute a list of some of the most important things (in this case, personal qualities) judged desirable for determining a person's promotability.

You may be concerned about the inevitable unevenness among supervisors' ratings on Performance Appraisals and Inventories of Attributes. Promotion Boards have access to detailed information (large computer runs) about all raters. This information shows them who the "hard" raters and who the "easy" raters are and helps the Boards to normalize the ratings.

- Peer group ranking (was used in 1976 only);
- Individual Career Appraisal and Development Plan. (This was a formal part of the performance appraisal in 1975 only. Since then, it is required only for major events such as transfer or promotion, or upon request by you. I encourage you to file an updated one annually, even if it means only that you review and confirm last year's. At the very least it assures you a regular career-planning session with your supervisor and demonstrates your continuing sincere interest in a career);
- Laudatory and commendatory correspondence. (Ordinarily these are to be from Office level or higher. But if you have something noteworthy you would like to include, send a copy to M35 and let them decide.)

The keeper of Promotion Files is Miss Audrey [redacted] in M32. To review your promotion File, call her on 3191s and make an appointment to see her in Room OS081. You may talk to her about adding items to your file if you notice that something is missing. And if you disagree with something in your file or think it is incorrect, call her attention to it. Depending on what it is, she may suggest that you discuss the matter with your supervisor, and then advise you about the possibility of your inserting something in the file to explain your views, as is usually allowed. M3 encourages you to look at your Promotion File and welcomes your help in keeping it up to date and complete.

In conclusion, two points already mentioned sum up the main ideas with which I would leave you:

- *Your* Promotion File represents *you*,
- *You* write *your* Personnel Summary.

Improve your promotability! Increase your chances of getting promoted by making sure that your Promotion File is complete and that your Personnel Summary is up to date and clearly written. It's up to you!

Update your Personnel Summary now and file it by 1 January!

AGENCY ENCOURAGES SUMMER LANGUAGE STUDY

Dan Buckley, M03

If you are in a language job and haven't seen Personnel Management Bulletin (PMB) 13-78, 22 August 1978, you might want to ask your admin people about it. The PMB describes a program under which the Agency continues to pay your salary while you attend an intensive summer language school (Middlebury, etc.). The Agency does not pay tuition, travel, or other costs -- you have to pay them.

The program is aimed at, but not limited to, Level-2 Language and Voice Language Technicians who are willing to take on some of the expense of upgrading their skills. Essentially, you must show a job-related need for the training and get managerial approval, but there are certain prerequisites. Check out the PMB, talk to your boss, and, if you qualify, talk to the External Training people at the National Cryptologic School (8047s). You will have to take care of applications, acceptances, etc. yourself, so it is not too early to plan for summer of 1979. Call me if I can help.

(U)

WERE YOU BORN ON ONE OF THESE DATES?

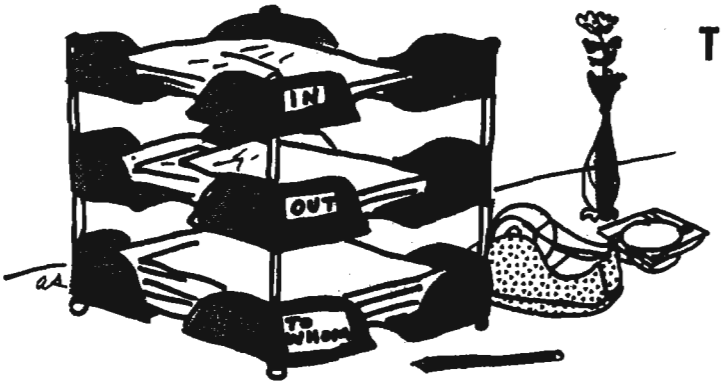
March 13, 19, 20
June 18, 23, 24
October 19

P.L. 86-36

[redacted] writes, "If you were born on one of these dates, and also if you are a resident of Maryland or Michigan, I need your help in preparing an article for CRYPTOLOG. Please call me on 7589 or 4427s and we can get together. The reason for this will become clear in a future issue of CRYPTOLOG."

(U)

DOCID: 4011702



TO WHOM IT MAY CONCERN

Lou Grant,
D5

The other day my secretary asked me how she should address a memo. In a fit of frustration, I told her, "To Whom It May Concern." Sure, I was being flip about the whole thing, but I don't need another example of the traumatic times we are in as far as dealing with the rest of the Community goes. Nor am I optimistic about any rapid improvement in the situation.

It has been almost two years since President Carter announced that he had directed a full-scale review of the Intelligence Community. He stressed consolidation and streamlining. There were high hopes that at long last some beneficial changes would come about. There were dreams of a simplified structure, of straightforward procedures, and clear-cut authority. It took a year to see once again those hopes and dreams destroyed as the powers that be thrashed about writing a new Executive Order.

You can just imagine the amount of debating that went into that Order. As usual, the traditional rules of an objective review were invoked; the first being to choose up sides and set up the perimeter defenses. That way each of the players gets to defend his territorial interests while he nibbles away at those of the others. This time the players proved themselves to be worthy opponents indeed. In fact they were so good, they argued every issue to a dead standstill. None of the empires crumbled, no torches were passed. In short, nothing was accomplished. So, in the tranquil aura of their newly affirmed allegiance (each unto himself) they took up the task of defining what to tell the President. After all, a Presidential Review has to lead to something!

Now any good cook knows that, after you stir the pot, you can either take something out or you can add more of something. Since the players had agreed that none of them would lose anything, they added to the pot. But they were very careful to flesh things out evenly so as not to upset the delicate balance of forces that had survived the prolonged debates.

The Director of Central Intelligence (DCI) got a National Foreign Assessment Center (NFAC), a National Intelligence Tasking Center (NITC), and some additional controls over money, etc. Department of Defense got an Assistant Secretary for Communications, Command, Control, and Intelligence, an Under-Secretary for Policy, and certain other options. The National Security Council got a more flexible committee structure. The National Foreign Intelligence Board got an expanded membership. And, not to be outdone, the Senate and the House both strengthened their new Intelligence Committees. As you can see, a well-flavored pot fit for the Presidential palate. And please him it did.

With the stage set, the next step was to choose the cast of characters. For the most part that has been done. Each of the new seniors has been issued at least one office, a series of titles to choose from, and matching stationery for each combination. They are now in the throes of selecting their supporting casts so they can decide what it is that their organization is going to do and where it is to be located. It shouldn't take much over another year to finish this phase.

In the meantime, we have to continue day-to-day business under the added burden of this new structural overlay. I'll say one thing: you learn something new every day. You send a memo to one organization and the response comes from another. You get a request from a fairly high-level authority, followed shortly by instructions from someone else not to answer it! Correspondence comes in from a new organization under serial numbers of an old one which has never legally been dissolved. You send a memo to someone, using his new title, and he signs the response using his other new title (some have three). Got the idea? A procedural nightmare. It can take days to do what a few phone calls used to accomplish. Now, let me see, who do I submit this article to, anyway?

DOCID: 4011702

NSA-crostic No. 20

By David H. Williams, P16

The quotation on the next page was taken from the published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS

A. Dragon slain by Siegfried

B. "Poor little -----, smallest of the forty-eight" (2 wds)

C. See Word L (2 wds)

D. What, according to Danny Kaye, an unemployed jester is ("The Court Jester") (2 wds)

E. The former Mrs. Bono and her clone (4 wds)

F. Person for whom something is named

G. Recent film with Word O, for which he was nominated for Best Supporting Actor (2 wds)

H. Film for which Word O won the Academy Award for Best Actor (2 wds, followed by Word Z)

I. Pertaining to light produced by chemical action, physiological process, or friction

J. Burning of a heretic (comp)

K. Necessary; money

L. One of Word O's early films, in which he is killed numerous times (2 wds followed by Word C)

M. Wickedness

N. Symbol of New York City's political machine (2 wds)

O. British film actor, on screen since 1933 (1914-) (3 wds)

P. ——-percha

Q. Noontime sign on the door at Cape Kennedy (3 wds)

R. Rise above, excel

S. Indian dwelling

T. Relating to the supernatural; abstruse

U. Thief, rascal (Yiddish slang)

V. Pleasure

WORDS

207 173 128 205 187 201

145 88 34 49 23 154 56 11 200 222 42

194 164 4 26 113 143 134 47 180 59 41

66 179 172 80 108 228 127 7 29 110 216

9 116 104 84 54 147 218 32 186 48 40

14 68 215 124 89

213 120 51 2 202 64

17 156 163 111 125 197 98 148

193 121 20 167 74 217 77 132

119 211 96 221 181 107 160 174 142 30 151

165 37 168 63 153 58 6 75

166 3 67 130 61 72 57

175 8 105 91 22 225 146 62 115 44

5 171 162 223 101 176 81 112

144 190 138 35 90 55 13 169 69 24 220

161 31 53 78 149 95 33 71 140 45 226

214 18 185 102

206 224 50 21 97

137 159 27 38 1 183 150 118 70 227 203

52 15 122 79 198 136 25 155 106

133 170 139 152 129

16 189 195 204 92 76

46 126 177 87 109

219 94 210 65 99 191 60 123 85

W. One side in a sports event

X. Not in view; wow! (3 wds)

Y. Drug intended to produce mood elevation

Z. See Word H (3 wds)

178 192 135 199

157 10 188 208 117 100 131 182 86 141

114 103 36 83 209

12 82 39 158 93 212 43 28 196 19 73 184

1 Q	2 F	3 K		4 C	5 M	6 J	7 D	8 L	9 E	10 X	11 B	12 Z	13 N		14 E
15 R	16 T	17 G	18 O		19 Z	20 H	21 P	22 L		23 B	24 N	25 R	26 C	27 Q	28 Z
29 D	30 I	31 O	32 E		33 O	34 B	35 N	36 Y	37 J	38 Q	39 Z	40 E	41 C		42 B
43 Z	44 L	45 O	46 U	47 C	48 E	49 B		50 P	51 F		52 R	53 O	54 E	55 N	56 B
57 K	58 J	59 C	60 V		61 K	62 L	63 J	64 F		65 V	66 D	67 K		68 E	69 N
70 Q	71 O	72 K	73 Z	74 H	75 J		76 T	77 H		78 O	79 R	80 D	81 M	82 Z	83 Y
84 E		85 V	86 X	87 U		88 B	89 E	90 N	91 L	92 T	93 Z	94 V	95 O		96 I
97 P	98 G	99 V		100 X	101 M	102 O	103 Y	104 E	105 L	106 R	107 I	108 D		109 U	110 D
111 G		112 M	113 C	114 Y	115 L	116 E	117 X	118 Q	119 I		120 F	121 H	122 R	123 V	124 E
	125 G	126 U	127 D		128 A	129 S	130 K		131 X	132 H	133 S	134 C		135 W	
136 R	137 Q	138 N	139 S	140 O	141 X	142 I	143 C		144 N	145 B	146 L	147 E	148 G	149 O	150 Q
151 I	152 S	153 J		154 B	155 R	156 G	157 X		158 Z	159 Q	160 I	161 O	162 M	163 G	164 C
	165 J	166 K	167 H		168 J	169 N	170 S	171 M		172 D	173 A	174 I	175 L		176 M
177 U	178 W	179 D		180 C	181 I	182 X	183 Q	184 Z	185 O	186 E		187 A	188 X		189 T
190 N	191 V	192 W		193 H	194 C	195 T	196 Z		197 G	198 R		199 W	200 B	201 A	202 F
	203 Q	204 T	205 A	206 P		207 A	208 X	209 Y		210 V	211 I	212 Z	213 F	214 O	215 E
216 D	217 H		218 E	219 V	220 N	221 I	222 B	223 M	224 P	225 L	226 O	227 Q	228 D		D.H.W.

(Solution next month)

Upon Notification by the Originator

DOCID: 4011702

1978 INDEX

This index of the articles published in Volume V, 1978, of CRYPTOLOG should be used in conjunction with the following previously published indexes:

CUMULATIVE INDEX (Vols. I through III, 1974-1976) -- separate publication;
"1977 Index, Vol. IV, 1977" -- pp. 17-21 of December 1977 issue of CRYPTOLOG.

The index is in two parts. The first part is an index of titles, listed alphabetically (1) by title and (2) by keyword in the title. A few titles have also been assigned keywords that do not appear in the titles. The second part is an index of authors. In both parts, multiple entries are listed in chronological order.

Items appearing in the July-August double issue are indicated by "Jul 78."

Titles

P.L. 86-36

A

ABNER
Equipment Maintenance on ABNER — [redacted] — Jun 78
Accentuate the Negative — [redacted] — Apr 78
Agency Summer Language Study — Buckley — Dec 78
a/k/a Sam — Meyer — Dec 78
And-a You Betta Have Moti-vaysh! — [redacted] — Oct 78
ARCHIVES
Never Again! — Gurin — Jun 78
Never on my Watch — [redacted] — Nov 78
As I Was Saying Years Ago... — Pattie — Jun 78
ATA Letter to President Carter — Tinsley — Apr 78

B

Back to Square One! — [redacted] — Oct 78
"Bodyguard of Lies" (Book Review) — [redacted] — Jan 78
BOOKBREAKERS
Bookbreakers Forum — V.V. — Jun 78
Linguistics and the Code Reconstructor — [redacted] — Nov 78
The Bucky Balance — [redacted] — Jul 78
But Why Do We Do It? — [redacted] — Jan 78
By-Lines Don't Cost -- They Pay! — Mollick — Feb 78

C

CAA News — W.E.S. — Jan-Nov 78
CALLSIGNS
Callsigns and WARC 79 — [redacted] — May 78
TA Implications of FCC Proposal — [redacted] — May 78
[redacted] — [redacted] — Sep 78
CAREER FIELDS
The Changing Face of NSA — Anon. — Jan 78
Cast a Double Shadow — [redacted] — Nov 78
Celtic Languages Today — [redacted] — Jun 78
The Changing Face of NSA — Anon. — Jan 78
CHINESE
[redacted] — [redacted] — Mar 78
[redacted] — [redacted] — Jun 78
[redacted] — [redacted] — Jun 78
Letter to editor - [redacted] article — [redacted] — Jul 78
Tell Me I'm Just a Sinobibliophobe — [redacted] — Jul 78
How Do You Spell Peking? — [redacted] — Dec 78
CLA
CLA News — -- — Mar, Sep 78
CLUSTERING
A Little PEP Talk — [redacted] — Apr 78
A Dialogue Between Ms. User and Dr. Analysis — [redacted] — Nov 78
COC
A VIP Tour through the Attic of NSOC — [redacted] — Dec 78

CODE
Linguistics and the Code Reconstructor — Buck — Nov 78
Collection-Support TA is Not for Everyone — [redacted] — Feb 78
COMINT
COMINT, COMSEC and Hilbert's Tenth — [redacted] — Jan 78
Soviet COMINT and the Civil War — [redacted] — Sep 78
[redacted] — [redacted] — Feb 78
COMPUTERS
Remedial Software Engineering — [redacted] — Apr 78
A Computer Scratch Pad at Home or at Work? — Crowell — Jun 78
Data Security and Human Error — [redacted] — Oct 78
COMSEC
"Bodyguard of Lies" (Book Review) — [redacted] — Jan 78
¿Conoces Bien la Geografía? — [redacted] — Apr 78
Continuing Professionalization — [redacted] — Oct 78
COPES
What Ever Happened to COPES? — [redacted] — Jan 78
Letter to editor - [redacted] "COPES" — [redacted] — Jun 78
Letter to editor - Gilbertson letter — Barrer — Sep 78
CRITIC Test
WEDDING BELLS and That Old Gang of Mine — [redacted] — Nov 78
CRYPTANALYSIS
"The Man Who Broke Purple" (Book Review) — Filby — Jan 78
Looking at Mr. [redacted] — Miller, Isaac — Apr 78
The Future of Cryptanalysis — Lutwiniak — May 78
[redacted] — [redacted] — Jun 78
[redacted] — [redacted] — Sep 78
CRYPTOLOGIC
Senior Military Cryptologic Supervisors Course — [redacted] — Feb 78
CRYPTOSYSTEMS
[redacted] — [redacted] — Sep 78
CRT
The Hand Is Not Quicker than the Eye — [redacted] — Mar 78
A Linguist Looks at the Tube — [redacted] — Mar 78
Letter to editor - [redacted] article — Fennwatcher — Apr 78

D, E

DATA
Project UTENSIL: The DDO Data Dictionary/Directory — [redacted] — May 78
Data Security and Human Error — [redacted] — Oct 78
Data Standards Center — Pattie — Nov 78
A Dialogue Between Ms. User and Dr. Analysis — [redacted] — Nov 78
A Donkey in Your WHAT? — [redacted] — Mar 78
DOUBLE NEGATIVES
"No, No, Nanette!" Means Yes? — A.J.S. — Dec 78
An Early NSA Proposal for Satellite Remoting — [redacted] — Jan 78

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

DOCID: 4011702 P.L. 86-36

~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36

Equipment Maintenance on ABNER — Jun 78
EXPLOITATION
[redacted] — Feb 78
SIGINT Exploitation, 1990 — Apr 78

F

Feeding the Germans Misinformation (Book Review) — Filby — Oct 78
First Lady of Navy Cryptology — [redacted] — Feb 78
FRIEDMAN, William
"The Man Who Broke Purple" (Book Review) — Filby — Jan 78
Formatting PL/1 Source Code — [redacted] — Nov 78
The Future of Cryptanalysis — Lutwiniak — May 78

G, H

GEOGRAPHY
¿Conoces Bien la Geografía? — Apr 78
Know Your Geography — Oct 78
How Do You Spell Peking? — Dec 78
GOLDEN OLDIES
Unidentified Unit at Unknown Location — Jun 78
The Hand Is Not Quicker Than the Eye — Mar 78
Has It Ever Been Translated Before? — Jul 78
How Do You Spell Peking? — Dec 78

I, J, K

[redacted] — Dec 78
An Idea for an Article — Miller — Mar 78
INTELLIGENCE
A Method for Measuring Negative Intelligence — [redacted] — Oct 78
INTERPRETATION
The Unseen Go-Between — Gurin — Feb 78
[redacted] — Mar 78
Is a Translator a Professional? — Jul 78

The Joys and Frustrations of Plural-Dropping — Salemme — Jan 78
The Joys of Unix — May 78
Know Your Geography — Oct 78
[redacted] — Dec 78
[redacted] — Dec 78

L

LANGUAGE
Thanks for the Attaboy! — Jan 78
[redacted] — [redacted] — Feb 78
The Unseen Go-Between — Gurin — Feb 78
Uncle-a Sam Wantsa You! — [redacted] — May 78
As I Was Saying Two Years Ago... — Pattie — Jun 78
Celtic Languages Today — Jun 78
Is a Translator a Professional? — Jul 78
Letter to editor - Pattie "As I Was... — Buckley — Sep 78
What's In a Non-Name? — Sep 78
And-a You Betta Have Moti-vaysh! — Oct 78
Agency Summer Language Study — Buckley — Dec 78

LETTERS TO EDITOR
Letter to editor - [redacted] "Whither" — Stoffel — Jan 78
Letter to editor - [redacted] article — Rishert — Mar 78
Letter to editor - [redacted] article — Fennwatcher — Apr 78
Letter to editor - [redacted] "COPES" — Gilbertson — Jun 78
Letter to editor - [redacted] rticle — Gurin — Jul 78
Letter to editor - [redacted] article — [redacted] — Jul 78
Letter to editor - Gilbertson letter — Barrer — Sep 78
Letter to editor - Pattie "As I Was.." — Buckley — Sep 78
Letter to editor - Salemme "SPELLMAN" — Williams — Sep 78

Letter to editor - Wms. NSA-crostic — [redacted] — Oct 78
Letter to editor - Wms. NSA-crostic — Filby — Oct 78
Letter to editor - Gillikin article — Pattie — Oct 78
Letter to editor - Appraisal system — Anon. — Nov 78
Letter to editor - Appraisal system — [redacted] — Nov 78
Letter to editor - [redacted] article — Nov 78

A Little PEP Talk — Apr 78
A Linguist Looks at the "Tube" — Mar 78
Linguistics and the Code Reconstructor — Buck — Nov 78
Looking at Mr. [redacted] — [redacted] — Apr 78

M

The Man Who Broke Purple (Book Review) — Filby — Jan 78
MATHEMATICS
Tell Me I'm Just a Sinobibliophobe — Jul 78
A Matter of Style — Sep 78
A Method of Measuring Negative Intelligence — [redacted] — Oct 78
MICROGRAPHICS
Reduction Ratios in Micrographics — Snow — Oct 78
Back to Square One! — Oct 78
MILITARY
Senior Military Cryptologic Supervisors Course — [redacted] — Feb 78
MINICOMPUTERS
A Computer Scratch Pad at Home or at Work? — Crowell — Jun 78
Minnie's Mini — Kenny — Jun 78
Minnie's Mini — Kenny — Jun 78
More B.S. (Before Spellman) — Butcher — Oct 78
More Beans — Filby — Feb 78
[redacted] — [redacted] — Mar 78
Letter to editor - [redacted] article — Jul 78
[redacted] — Oct 78
MYCROFT
The Joys of Unix — May 78

N, O

NEGATIVE INTELLIGENCE
A Method of Measuring Negative Intelligence — Oct 78
Never Again! — Gurin — Jun 78
Never On My Watch — [redacted] — Nov 78
"No, No, Nanette!" Means Yes? — A.J.S. — Dec 78
No, Winnie, You've Got It Upside Down Too! — A.J.S. — Feb 78
[redacted] — [redacted] — Sep 78
NSA-CROSTIC
NSA-Crostic No. 11 — Williams — Jan 78
NSA-Crostic No. 12 — A.J.S. — Mar 78
NSA-Crostic No. 13 — Williams — Apr 78
NSA-Crostic No. 14 — Sardonyx — May 78
NSA-Crostic No. 15 — A.J.S. — Jun 78
NSA-Crostic No. 16 — Williams — Jul 78
NSA-Crostic No. 17 — A.J.S. — Sep 78
NSA-Crostic No. 18 — Williams — Oct 78
NSA-Crostic No. 19 — Williams — Nov 78
NSA-Crostic No. 20 — Williams — Dec 78

Overheard in the Burnbag Line — -- — Oct 78

P

PEP
A Little PEP Talk — [redacted] — Apr 78
PLURALS
The Joys and Frustrations of Plural Dropping — Salemme — Jan 78
[redacted] — Jan 78
Thanks for the Attaboy — [redacted] — Jun 78
[redacted]

EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36

DOCID: 4011702 P.L. 86-36

~~SECRET SPOKE~~ EO 1.4.(c) P.L. 86-36

PROFESSIONALIZATION
Continuing Professionalization — [redacted] — Oct 78
PROGRAMMING
Formatting PL/1 Source Code — Nov 78
[redacted] — Sep 78
Project UTENSIL: The DDO Data Dictionary/Directory — May 78
PROJECT MANAGEMENT
The Bucky Balance — Jul 78
PROMOTION
A Proposed Cure for the "Performance Syndrome" — Mar 78
Some Tips on Getting Promoted — Dec 78
A Proposed Cure for the "Performance Syndrome" — Mar 78
PURPLE
The Man Who Broke Purple (Book Review) — Filby — Jan 78
PUZZLES
Three Holes — -- — Feb 78
Answer to Three Holes — -- — Mar 78
Prizewinners in Three Holes — -- — Apr 78
¿Conoces Bien la Geografía? — Apr 78
Who and Whom? — Oct 78
Know Your Geography — Oct 78

R

RAGPIE
By Why Do We Do It? — Jan 78
RECONSTRUCTION
Linguistics and the Code Reconstructor — Buck — Nov 78
Reduction Ratios in Micrographics — Snow — Oct 78
Remedial Software Engineering — Caron — Apr 78
REMOTING
An Early NSA Proposal for Satellite Remoting — [redacted] Nolte — Jan 78
REPORTING
A Matter of Style — Kuntz — Sep 78
[redacted] — EO 1.4.(c) P.L. 86-36
I Remember SPELLMAN — Salemme — Jul 78

S

SATELLITES
An Early NSA Proposal for Satellite Remoting — Horn, [redacted] — Jan 78
SCREENWRITER
A Linguist Looks at the "Tube" — Johnson — Mar 78
Letter to editor - Johnson article — [redacted] — Apr 78
[redacted] — Oct 78
Senior Military Cryptologic Supervisors Course — Feb 78
SIGINT
SIGINT Exploitation, 1990 — Apr 78
Cast a Double Shadow: The Trojan Horse of SIGINT — Nov 78
[redacted] — Dec 78
A Small Problem — Nov 78
SOFTWARE
Remedial Software Engineering — Apr 78
SOLIS
How Do You Spell Peking? — [redacted] — Dec 78
Some Background on the C/T Merger — Smith — Mar 78
Some Tips on Getting Promoted — Dec 78
SOVIET
[redacted] — Feb 78

[redacted] — Sep 78
The Soviet General Staff — Jul 78
Soviet COMINT and the Civil War — Sep 78
[redacted] — Sep 78
SPELLMAN
Never Again! — Gurin — Jun 78
I Remember SPELLMAN — Salemme — Jul 78
Letter to editor - Salemme "SPELLMAN" — Williams — Sep 78
More B.S. (Before Spellman) — [redacted] — Oct 78
STANDARDS
NSA Data Standards Center a/k/a Sam — Pattie — Nov 78
[redacted] — Dec 78
[redacted] — Feb 78
STYLE
A Matter of Style — Sep 78

T

T ORGANIZATION
Some Background on the C/T Merger — Smith — Mar 78
T Establishes Human Resource Development Panel — -- — Sep 78
TA
Collection-Support TA Is Not for Everyone — Feb 78
Telephone Problem Here — Apr 78
TA Implications of FCC Proposal — May 78
Unidentified Unit at Unknown Location — Jun 78
[redacted] — Sep 78
A Small Problem — Nov 78
Telephone Problem Here — Apr 78
Tell Me I'm Just a Sinobibliophobe — Jul 78
Thanks for the Attaboy — Jan 78
To Whom It May Concern — Grant — Dec 78
TRANSLATION
Letter of ATA to President Carter — Tinsley — Apr 78
Uncle-a Sam Wantsa You — May 78
Has It Ever Been Translated Before? — Jul 78
TRIGRAPH
Ye Gads! Another Country Trigraph System — Jul 78

U, V

[redacted] — Jun 78
ULTRA
More Beans — Filby — Feb 78
Feeding the Germans Misinformation — Filby — Oct 78
Uncle-a Sam Wantsa You — May 78
UNIX
The Joys of UNIX — May 78
The Unseen Go-Between — Gurin — Feb 78
UTENSIL
Project UTENSIL: The DDO Data Dictionary/Directory — May 78
A VIP Tour Through the Attic of NSOC — Dec 78
VOICE
[redacted] — Feb 78
You Can't Tell the Wheat from the Chaff Without a Program — Gurin — Oct 78

W

WARC 79
Callsigns and WARC 79 — May 78
WEDDING BELLS and that Old Gang of Mine — Nov 78

EO 1.4.(c) P.L. 86-36

~~SECRET SPOKE~~ EO 1.4.(c) P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Authors

(Names in quotation marks are pseudonyms.)

X, Y

[redacted]
Looking at Mr. [redacted] Apr 78
A Dialogue Between Ms. User and Dr. Analysis Nov 78
Ye Gads! Another Country Trigraph System! Jul 78
You Can't Tell the Wheat from the Chaff Without a Program Oct 78

A

[redacted]
Senior Military Cryptologic Supervisors Course Feb 78
[redacted] Mar 78

ANONYMOUS
The Changing Face of NSA Jan 78
Letter to the editor -- appraisal system Nov 78

EO 1.4.(c)

B

[redacted]
Is a Translator a Professional? Jul 78

BARRER, Donald Y.
Letter to the editor -- Gilbertson letter Sep 78

[redacted]
Equipment Maintenance on ABNER Jun 78
[redacted]
The Soviet General Staff Jul 78
[redacted]
And-a You Betta Have Moti-vaysh! Oct 78
[redacted]
The Bucky Balance Jul 78

BUCKLEY, Dan
Letter to the editor -- Pattie "As I Was Saying..." Sep 78
Agency Encourages Summer Language Study Dec 78

[redacted]
More B.S. (Before SPELLMAN) Oct 78

P.L. 86-36

C

[redacted] Sep 78
[redacted]
Remedial Software Engineering Apr 78
[redacted] Feb 78
[redacted]
A Little PEP Talk Apr 78
A Dialogue Between Ms. User and Dr. Analysis Nov 78
[redacted]
Letter to the editor -- [redacted] NSA-Crostic No. 16 Oct 78

CROWELL, Bill
A Computer Scratch Pad at Home or at Work? Jun 78

D

[redacted]
The Joys of UNIX May 78

P.L. 86-36

F

[redacted]
Letter to the editor -- [redacted] article Nov 78

"FENNWATCHER, Hy"
Letter to the editor -- [redacted] article Apr 78

FILBY, P. W.
The Man Who Broke Purple (Book Review) Feb 78
Feeding the Germans Misinformation (Book Review) Oct 78

FILBY, Vera
More Beans Feb 78
Letter to the editor -- Williams NSA-Crostic No. 16 Oct 78

G

[redacted]
Thanks for the Attaboy Jan 78
Uncle-a Sam Wantsa You! May 78

GILBERTSON, Eugene A.
Letter to the editor -- [redacted] "COPES" Jun 78

[redacted]
Ye Gads! Another Country Trigraph System! Jul 78

[redacted]
Letter to the editor -- Appraisal system Nov 78

GRANT, Lou
To Whom It May Concern Dec 78

GURIN, J.
Never Again! Jun 78
Letter to the editor -- [redacted] article Jul 78
You Can't Tell the Wheat from the Chaff Oct 78

H

[redacted]
Soviet COMINT and the Civil War Sep 78
[redacted]
How Do You Spell Peking? Dec 78
[redacted] Dec 78
[redacted] Jun 78

EO 1.4.(c)
P.L. 86-36

HORN, Joseph E., and NOLTE, William M.
An Early NSA Proposal for Satellite Remoting Jan 78
[redacted]
SIGINT Exploitation, 1990 Apr 78
[redacted]
But Why Do We Do It? Jan 78
A Donkey in Your WHAT? Mar 78

P.L. 86-36

I, J

[redacted]
Looking at Mr. [redacted] Apr 78
[redacted] Dec 78
Some Tips on Getting Promoted
[redacted]
A Linguist Looks at the "Tube" Mar 78
[redacted]
[redacted] Dec 78

K, L

EO 1.4.(c)
P.L. 86-36

[redacted]
A Method of Measuring Negative Intelligence Oct 78

KENNY, Minnie
Minnie's Mini Jun 78
[redacted] Sep 78
[redacted]
Letter to the editor -- [redacted] article Jul 78
[redacted]
A Matter of Style Sep 78
[redacted]
Back to Square One! Oct 78

LUTWINIAK, William
The Future of Cryptanalysis May 78

P.L. 86-36

M

[redacted]
Bodyguard of Lies (Book Review) — Jan 78

[redacted]
¿Conoces Bien la Geografía? — Apr 78
Know Your Geography — Oct 78

[redacted]
Callsigns and WARC 79 — May 78

[redacted]
a/k/a Sam — Dec 78

MILLER, Doris E.
An Idea for an Article — Mar 78

[redacted]
Looking at Mr. [redacted] — Apr 78

MOLLICK, JOHN J.
By-Lines Don't Cost -- They Pay — Feb 78

[redacted]
Celtic Languages Today — Jun 78

MYERS, L. S.
[redacted] — Jun 78

N,O

EO 1.4.(c)
P.L. 86-36

[redacted]
Never on My Watch — Nov 78

[redacted]
Accentuate the Negative — Apr 78

NOLTE, William M., and HORN, Joseph E.
An Early NSA Proposal for Satellite Remoting — Jan 78

[redacted]
A Proposed Cure for the "Performance Syndrome" — Mar 78

[redacted]
Collection-Support TA Is Not for Everyone — Feb 78
Continuing Professionalization — Oct 78

P,R

P.L. 86-36

PATTIE, Mark T., Jr.
As I Was Saying Two Years Ago. . . — Jun 78
Letter to the editor -- [redacted] article — Oct 78
NSA Data Standards Center — Nov 78

[redacted]
What's in a Non-Name? — Sep 78

[redacted]
Letter to the editor -- [redacted] 1977 article — Mar 78

[redacted]
Who and Whom? — Oct 78

[redacted]
[redacted] — Feb 78

S

SALEMME, A. J.
The Joys and Frustrations of Plural Dropping — Jan 78
No, Winnie, You've Got It Upside-Down Too — Feb 78
NSA-Crostic No. 12 — Mar 78
NSA-Crostic No. 15 — Jun 78
I Remember SPELLMAN — Jul 78
NSA-Crostic No. 17 — Sep 78
"No, No, Nanette!" Means Yes? — Dec 78

"SARDONYX"
NSA-Crostic No. 14 — May 78

[redacted]
WEDDING BELLS and That Old Gang of Mine — Nov 78

[redacted]
[redacted] — Feb 78

-----, and [redacted]
The Soviet General Staff — Jul 78

[redacted]
First Lady of Naval Cryptology — Feb 78

[redacted]
Formatting PL/1 Source Code — Nov 78

[redacted]
Has It Ever Been Translated Before? — Jul 78

SMITH, Frank
Some Background on the C/T Merger — Mar 78

SNOW, Don
Reduction Ratios in Micrographics — Oct 78

[redacted]
COMINT, COMSEC, and Hilbert's Tenth — Jan 78
Tell Me I'm Just a Sinobibliophobe — Jul 78

[redacted]
A VIP Tour Through the Attic of NSOC — Dec 78

[redacted]
CAA News — Jan-Nov 78
What Ever Happened to COPES? — Jan 78
Letter to the editor -- [redacted] "Whither SRA?" — Jan 78
The Hand Is Not Quicker Than the Eye — Mar 78
Telephone Problem Here — Apr 78
TA Implications of FCC Proposal — May 78
[redacted] — Sep 78
A Small Problem — Nov 78

EO 1.4.(c)
P.L. 86-36

T,V,W

P.L. 86-36

[redacted]
Will It Really Do the Job? — Oct 78

[redacted]
[redacted] — Oct 78

TINSLEY, Royal L., ATA President
ATA Letter to President Carter — Apr 78

[redacted]
Data Security and Human Error — Oct 78

[redacted]
Cast a Double Shadow: The Trojan Horse of SIGINT — Nov 78

WILLIAMS, David H.
NSA-Crostic No. 11 — Jan 78
NSA-Crostic No. 13 — Apr 78
NSA-Crostic No. 16 — Jul 78
Letter to the editor -- Salemme "SPELLMAN" — Sep 78
NSA-Crostic No. 18 — Oct 78
NSA-Crostic No. 19 — Nov 78
NSA-Crostic No. 20 — Dec 78

[redacted]
Project UTENSIL: The DDO Data Dictionary/Directory — May 78

~~(SC)~~

?¿ Ask ~~Alma~~ Art

Dear ~~Alma~~ Art:
I'm depressed. My symptoms are: apathy, boredom, fatigue and lustlessness. And the cure? Please don't tell me to get a job. I don't need the money. — Fenton, Mo.

Dear Fenton:
Have you thought of subscribing to CRYPTOLOG? A lot of people say it has done wonders for curing their apathy, boredom, fatigue and lustlessness.

Dear ~~Alma~~ Art:
My husband is almost 40 and is obsessed with keeping his body young. In addition to working very hard, each day he jogs five to 10 miles and lifts weights. Also, he has eliminated alcohol from his diet and stopped smoking.
All this healthy virtue is driving me bananas. The exercise knocks him out by 10 every night. He sleeps like a baby and I am lonely and sexually frustrated. — Help!

EO 1.4.(c)
P.L. 86-36

Dear Help:
Have you thought of writing an article for CRYPTOLOG? A lot of people say it has done wonders for curing their loneliness and all kinds of frustration.

HAVE A PROBLEM at home or at the office? Write to ~~ASK ALMA, P.O. BOX 40, Closter, N.J. 07624~~ and watch for the answer in this column.

ASK ART, CRYPTOLOG, P1

(U)

P.L. 86-36

DOCID: 4011702

Reader Survey

Well, there's good news and -- I think -- bad news. The good news is that, of the 83 people listed in the 1978 Index, 50 contributed to CRYPTOLOG for the first time and 33 are recidivists. That seems to indicate that we're getting the message across that (1) just about anyone with anything operational to discuss can have his or her say in CRYPTOLOG, (2) it doesn't cost a penny to have the item published; and (3) it might even help you (see [redacted] article in this issue, in which she recommends that you list your publications in your Personnel Summary).

The -- I think -- bad news is that, of the same 83 contributors, 71 are men, 11 are women, and one is unaccounted for (the writer of the anonymous letter in November). Even if we put the unaccounted one in with the women, it still looks bad. Shouldn't more women be contributing to CRYPTOLOG? Or are they all sending their stuff to Brand X?

Why not a survey to ask that question and, while we're at it, a couple of other questions to see what CRYPTOLOG readers think of it.

If you feel like it, answer the following questions (add more paper if needed) and send your comments to: CRYPTOLOG, P1. You don't have to sign your name.

P.L. 86-36

1. In my opinion, the reason why there were so few women contributors to CRYPTOLOG in 1978 was:

2. Of all the titles listed in the 1978 Index, the one I thought most worth reading was:

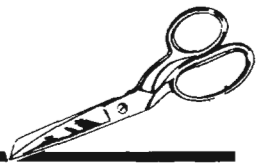
3. Of all the titles listed in the 1978 Index, the one I thought least worth reading was:

4. Of all the things that have ever appeared in CRYPTOLOG, the one that was most beneficial to me (by helping me to solve an operational problem, think out something more clearly, etc.) was:

5. I would like to see CRYPTOLOG authors devote more attention to:

6. I would like to see CRYPTOLOG authors devote less attention to:

7. Not only that, but. . .



Sample NSA-crostic

Here's a little NSA-crostic to show you how easy they are to do. Rules: The first letters of the WORDS, read vertically, spell out the name of the NSAer author and the title of the work. All the letters of the words are scrambled and fitted into the diagram, which contains a quotation from the work. (Black spaces mark ends of words; words do not read up and down in diagram.) The NSA-crostic has been started for you -- now you finish it!

Words

A. "--, shucks!" (Wallace Beery) — 5 16

B. Tom and ----- — 1 43 29 48 22

C. "---- Lake" — S W A N / 3 44 47 11

D. Hansel and ------ — G L / 28 34 7 41 39 26

E. Sleigh-puller — P / 38 2 32 15 9 23 19

F. Orient — E A S T / 33 26 18 14

G. "Lend an ---" — R / 12 40 21

H. Plaything — O / 4 27 45

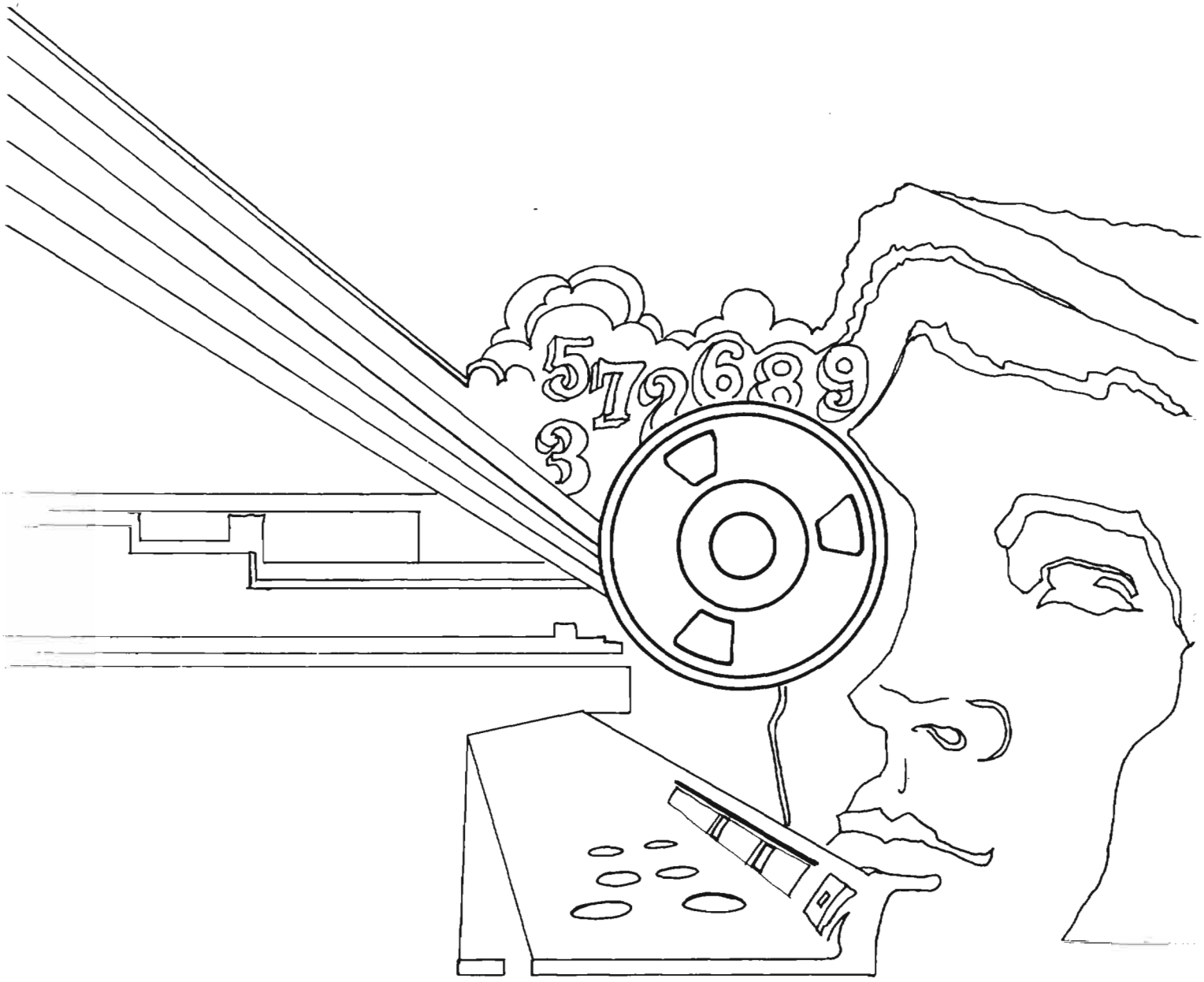
I. Snow and --- — G / 10 20 46

J. Sleigh-puller's feature — 42 25 13 30

K. "---- of the Magi" — T / 37 17 6 24

L. "I --- Mommy..." — 35 31 8

1 Б	2 E	3 C S	4 H	■	5 A	■	6 K	7 D	8 L	■ 9 E
10 I	11 C N	12 G	13 J	■	14 F T	15 E	■	16 A	17 K	18 F S 19 E
■	20 I C	21 G R	22 B	23 E P	24 K T	25 J	26 D L	27 H O	28 D G	■ 29 B
30 J	31 L	32 E	33 F E	34 D	35 L	■	36 A A	■	37 K	38 E 39 D
40 G	41 D	■	42 J	43 B	44 C W	■	45 H	46 I	47 C A	48 B ■ AJS


5 7 9 6 8 9
3

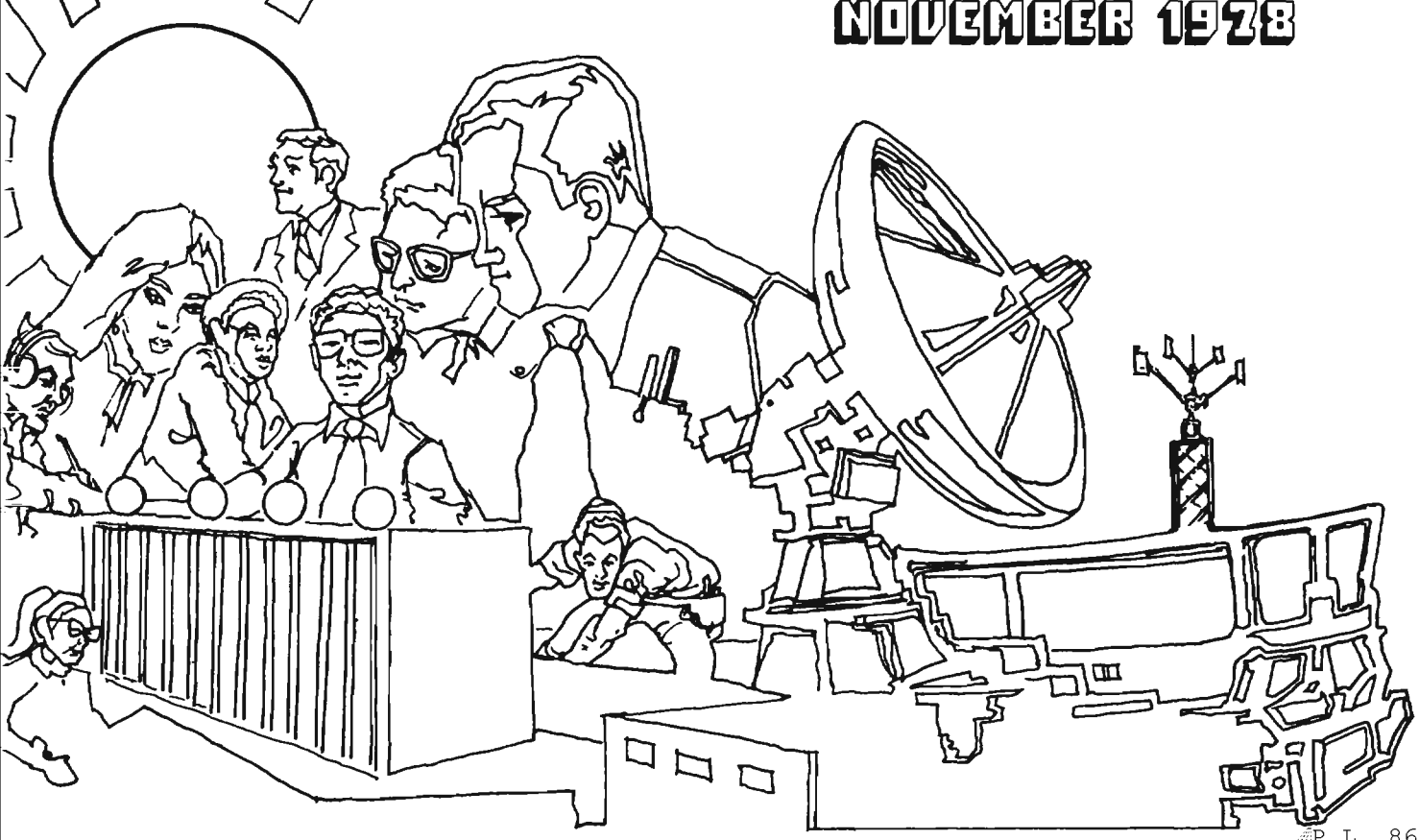
DOCID: 4009817

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

NOVEMBER 1978



P.L. 86-36

WEDDING BELLS AND THAT OLD GANG OF MINE...E. Leigh Sawyer.....1
A SMALL PROBLEM.....[redacted].....2
NSA DATA STANDARDS CENTER.....Mark T. Pattie, Jr.....3
LINGUISTICS AND THE CODE RECONSTRUCTOR....Stuart H. Buck.....6
DIALOGUE BETWEEN MS. USER AND DR. ANALYSIS:..[redacted].....9
CAST A DOUBLE SHADOW: TROJAN HORSE OF SIGINT..[redacted].....11
FORMATTING PL/1 SOURCE CODE.....[redacted].....13
NSA-CROSTIC NO. 19.....David H. Williams.....16
NEVER ON MY WATCH.....[redacted].....18
LETTERS TO THE EDITOR.....[redacted] Anon..19
C.A.A. NEWS.....21

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009817

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. V, NO. 11 NOVEMBER 1978

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5236s)

Collection..... [redacted] (8955s) P.L. 86-36

Cryptanalysis..... [redacted] (4902s)

Cryptolinguistics..... [redacted] (5981s)

Language..... [redacted] (8161s)

Machine Support..... [redacted] (5303s)

Mathematics..... [redacted] (8518s)

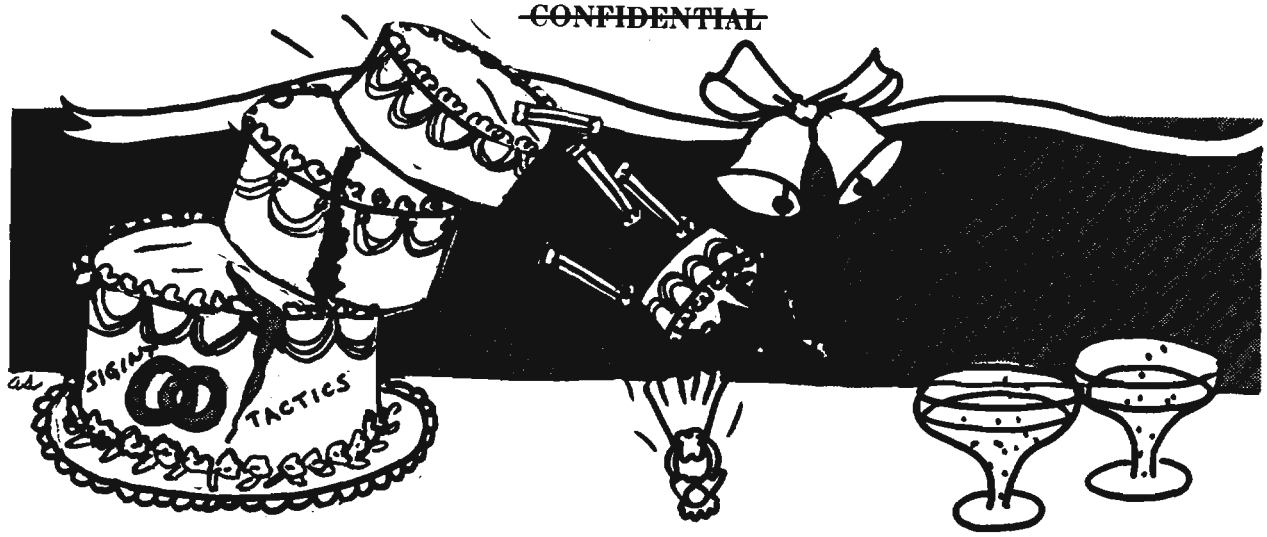
Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Taurone (3573s)

Production Manager.....Harry Goff (5236s)

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4009817



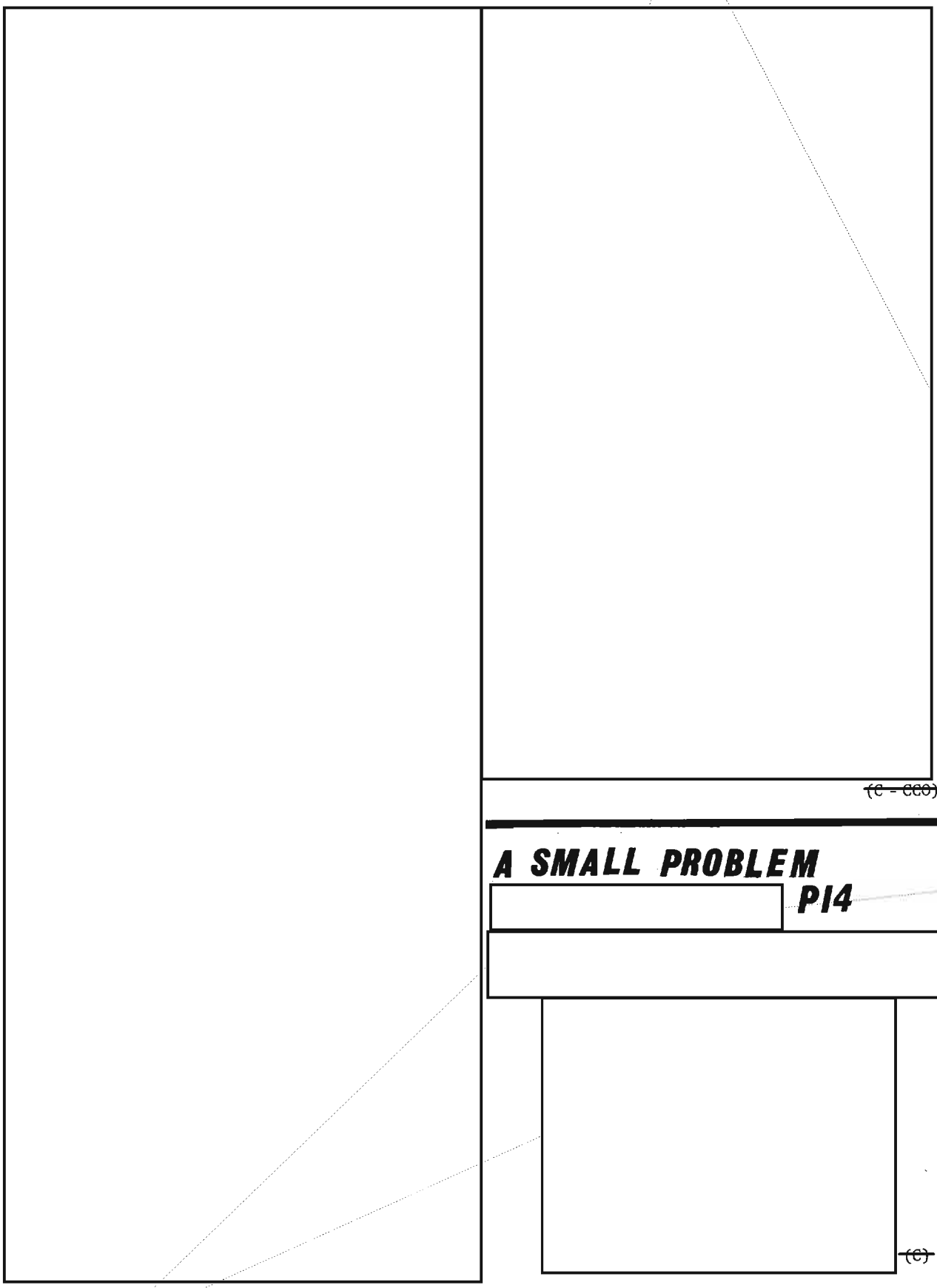
Wedding Bells and That Old Gang of Mine

E. LEIGH SAWYER, B4

E.O. 1.4.(c)
P.L. 86-36

~~CONFIDENTIAL~~

EO 1.4.(c)
P.L. 86-36



~~(C - CCO)~~

A SMALL PROBLEM

P14

P.L. 86-36

~~(C)~~

EO 1.4.(c)
P.L. 86-36

~~CONFIDENTIAL~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4009817

YES, CRYPTOLOG READERS, N.S.A. DOES HAVE A

DATA STANDARDS CENTER

Mark T. Pattie, Jr., P13D (NDSC)

Before I tell you what the NSA Data Standards Center (NDSC) does, perhaps I should explain why we do it. One very good reason is that a previous director, VADM Noel Gayler, established the NDSC by direction on 1 January 1971. This was later formalized by the reissuance in May 1972 of NSA Regulation 80-9, the NSA Program for Standardization of Data Elements and Related Features.

That would be reason enough to have a Center, of course, but there is more. The NDSC is really the element responsible for the Agency portion of the Department of Defense Data Standards Program, which had its beginnings in DoD Directive 5000.11 when that document was published on 7 December 1964. We also work closely with the National Bureau of Standards, which, under Executive Order 11717 of 9 May 1973, is responsible for government-wide automatic data processing standards. By "work closely" I mean that NDSC personnel are often in touch with people from the DoD and other government agencies on data standards matters and they take part in interagency committees and working groups as the NSA representatives to their meetings. All of this comes under NSA Regulation 80-9, which names the NDSC as the Agency point of contact for federal, DoD, and other external programs or efforts for data standardization. One example of our committee work is our participation on the Data Standards Panel of the Intelligence Information Handling Committee of NFIB.

But even if we did not have the official reasons for establishing an NSA Data Standards Centers, there would still be the practical reasons for it. It must make good sense to have data standards instead of Babel and it even saves money. Let me illustrate:

$$x + y = 7 \qquad \pi r^2 \qquad a^2 + b^2 = c^2$$

Would it make any difference in working with these elements if I were in Germany instead of the United States? Or in Italy? Or in Sweden? No, for everyone recognizes that these are mathematical symbols, which are standard around the world.

How about another example?

Speed Limit 50

Well, right away I suspect some readers will be uneasy. Here it does make a difference, for we have to know if speed is measured in miles, in kilometers, or whatever.

And so it goes. In order to communicate with one another, we have to use terms that are mutually understandable. That holds true whether we are talking about listening to a foreign language broadcast or trying to read a technical journal for which we have no background. In the various sciences there is much that is mutually understandable between scientists of different nationalities even with their language differences, whereas laymen within the same country would be at a loss to understand what is said or written.

Incidentally, I do not know whether any of you are aware of it, but some of those who are to all intents and purposes the most handicapped in the art of communication -- those who cannot hear or speak -- have the least trouble with the foreign-language barrier. They use symbols -- hand signs -- which are international standards and they can make themselves understood in any country where sign language is practiced. The hand signs are, in fact, data standards which have the same meaning, for the most part, in the language of whatever country they happen to be in or from. Of course, they might have trouble spelling words that are foreign to them but they are still better off than most of us who claim to have all our faculties.

A certain amount of data standardization is taking place around us all the time. I am referring to expressions that once were unique to particular parts of the United States at one time but which are now becoming rare. Those who make studies of such things were able to pinpoint the birthplace of almost anyone just by asking that person to pronounce about ten different words or to provide the words or terms used for certain objects or actions. For example, how do you pronounce the following words when you are "back home": BUSH/PUSH, HOG, GREASY, MERRY/MARY/MARRY.

Or what do you cook your breakfast eggs in? A FRYING PAN/FRY PAN, SKILLET, or SPIDER? And what's that big piece of furniture in your LIVING ROOM/PARLOR? -- a SOFA, COUCH, DIVAN, or DAVENPORT? How do you pronounce PARK YOUR CAR if you're from the Boston area? How do you say WATER, wherever you're from?

Such regional differences are largely falling by the wayside, perhaps because of the omnipresent TV screen and the nationwide distribution of TV programs. Or it might be

DOCID: 4009817

because people no longer live out their years in the areas where they were born: we are a mobile nation.

Whatever the cause, data standardization seems to be with us, whether we like it or not. It is a fact of life. I'll admit that I look upon this leveling of the American idiom with a certain amount of regret. We are losing some of our rich heritage in language and I think we will be the poorer for it.

But the NDSC is not as concerned with the exchange of information between individuals as it is with the exchange of information between machines or between a machine and a terminal. Here standardization should be a way of life but it is not. There are just too many examples of Agency elements blithely going their own ways regardless of the fact that they are duplicating the work of another element, or, what is worse, establishing their own standards when Agency standards already exist.

Perhaps I should define the term "data standards." Although some readers may know what the term means, I suspect that many do not. By "data standards" we mean consistent, agreed-upon names, descriptions, and codes for categories of data that will ensure unambiguous understanding in data processing and data interchange.

Note two things in that definition. I did not use the word "cryptologic" and I ended with the words "date processing and data interchange." The NDSC is concerned with data standards in *all* fields, both cryptologic and noncryptologic. And, basically, we are trying to come to agreements about definitions that will make data machine-insertable and machine-extractable.

The latter point is essentially what distinguishes data-standards work from that in SIGINT terminology, for which the NDSC is also responsible. In SIGINT terminology we seek to build a SIGINT Terminology Data Base (STDB) and glossaries for each cryptologic field. These will contain terms that are defined in such a manner that they show the currently accepted meanings. One way of making the distinction between standard terminology and data standards is to say that the definitions for the latter are more precise than those for standard glossaries. People have less trouble interpreting nuances in meaning than do machines.

Let me give you a simple example of what we mean about the difference between the two. If we were going to put in a definition for DATE, we could use a definition from a general desk dictionary for our terminology data base.

> "DATE: 1. A statement or formula affixed that specifies the time of execution or making (as *a letter bearing the date 3 January 1856*).
>
> 2. The point of time at which a transaction or event takes place or is scheduled to take place."
> (*Webster's Third New International Dictionary*)

Our Data Standards description is from the *NSA Manual of Standard Data Elements and Related Features* (Annex A to USSID 412):

> "00012
>
> "DATE: The years, months and days of the Gregorian calendar.
>
> DATA ITEMS: Represented by 6 digits, unspaced, left to right: 2 for year, 2 for month (01-12), 2 for day (01-31). (E.g., 15 January 1969 would be 690115)."

You will note that the Data Standards description has measurable factors while the Terminology definition does not.

The NDSC is not an ivory tower where we "do our thing" away and apart from the rest of the NSA world. No, we work very closely with other people. For instance, every major component of the Agency has a representative who works with the NDSC staff in identifying, researching, and approving data standards and SIGINT terms. The Senior Data Representatives and Senior Terminology Representatives, in turn, work with other contacts at lower echelons in their own organizations in the proposing and coordinating phases. We may meet with the SDRs or the STRs as a group or as individuals, depending on the problem of the

The name "Data Standards Center" itself is something of a misnomer, for the NDSC is deeply involved in more than just data standards for machine processing of information. In the terminology program, people working on the development of the SIGINT Terminology Data Base provide guidance on the development and use of terms for SIGINT concepts and their accompanying definitions, maintain a central collection of reference materials on SIGINT terms, and develop a common glossary format for SIGINT glossaries published as appendices to USSID 412. Our SIGINT terminology program is unique within the Intelligence Community.

In the creation of SIGINT glossaries the NDSC terminology people work closely with the appropriate terminology panels to develop the necessary documentation. The Center, working with the Traffic Analysis Terminology Panel, developed a draft TA Glossary which is now being coordinated with certain elements and our people are working with the Signals Collection Terminology Panel on a draft glossary for that field. Terminology personnel are also working with T personnel on a Telecommunications Glossary and with the TEBAC people on a Telemetry Analysis Glossary. In the near future we plan to start work on a Data Processing Glossary, while those for other cryptologic fields and an interdisciplinary glossary will be developed as time and resources permit.

One person concentrates on Multiple Use standards -- those that are essentially non-cryptologic, like personnel or budget standards. The work involves coordination and many meetings with people outside the Agency -- from the Civil Service Commission and the U.S. Air Force, for example. Inside NSA our Multiple Use expert works mostly with personnel from E, L, M, N, or T, but the problems may be of such a nature that they concern the entire Agency.

The NSA Data Standards Center has developed a centralized file of data elements/data field definitions. This file, [redacted] serves as a repository of all the published standards for SIGINT activities [redacted] plus other data elements that are being used in DDO files and elsewhere without being standards. This file will help us to identify data elements that are eligible to be proposed as SIGINT data standards.

[redacted] may eventually become a part of Project UTENSIL, the DDO Data Dictionary/Directory that was envisioned by DDO managers in 1976. A task force, created under the leadership of the NDSC, drew up a charter for a dictionary that was to contain data elements and their meanings; the directory was to give control functions, file names, etc. In the meantime, several DDO elements have proceeded to develop their own Data Dictionaries, unfortunately with little regard for standardization, so their terms are quite often incompatible with those for another DDO dictionary and some times even with their own particular group.

[redacted]

In 1972 Harold Shaklee, then Chief of the NSA Data Standards Center, and George Hicken, COINS Project Manager, met and agreed that the NSA Air Movements files in COINS would be standardized. On 7 September 1972 Mr. Shaklee convoked a meeting of a Working Group of 22 people, most of whom represented the various Agency elements concerned with the appropriate files.

[redacted]

It is unfortunate that those developing the [redacted] files in the early days did not take the time to look into the work of others before building their own unique files. The trouble with that statement is that I know that exclusive files are being created right at this moment and the lesson learned when the COINS users tried to query the [redacted] files seems to have been wasted. Some of those files are being built right within the same organization. P.L. 86-36 EO 1.4.(c)

And even the limited progress we have seen in getting the [redacted] files in COINS standardized for NSA is tempered by the knowledge that many other NSA files need work and we still have not attacked the problem of standardization across the Community. In a 1976

[redacted] P.L. 86-36

In Vol. II of the same study, on page 47, types of user problems are cited:

> "a. They must use different codes, acronyms and abbreviations for referencing like fields of information in different files. They experience frustration both in framing interrogations and in interpreting answers.
>
> "b. Users must cope with more than one set of data item codes for a common data element.
>
> "c. They must have access to a variety of working aids in preparing interrogations or in translating answers into meaningful information."

EO 1.4.(c) P.L. 86-36

In closing, I would just like to say that although the NSA Data Standards Center can be justifiably proud of its accomplishments in standardizing Data Elements within the Agency, we are all too aware of the fact that we have barely scratched the surface.

The second point I would like to leave with you is that we covet your cooperation. If you don't work closely with us in the effort to reduce the data maze in the Agency, all our attempts to improve data standards will become little more than a treadmill operation -- no progress, but a lot of work just to keep abreast of the problem.

DOCID: 4009817

LINGUISTICS AND THE CODE RECONSTRUCTOR

STUART H. BUCK, P16 (Retired)

Let me hasten to point out that I make no pretensions to more than a very limited knowledge of modern linguistic theory. It was my fate to be born several decades too soon. By the time I entered college, language majors were expected to delve deeply into literature and history, but that was about it. Philology, as it was called then, was regarded as a field for specialists, not as a requirement for an AB in Romance Languages. I remember once suggesting, rather timidly, that I would like to take a one-semester course in phonetics. My tutor knocked that one down quickly. Such an aberration, he pointed out, would conflict with a course on Voltaire, which would stay with me longer. He made it sound like a steak dinner. And so the advent of Bloomfield and his disciples caught me preoccupied, first with Voltaire, and then with the Great Depression, when it didn't seem to make any difference what kind of linguist you were -- everyone suffered equally. I can make one small claim to fame, however. Carl Darling Buck, the great philologist, and I are distantly related. Moreover, Carl Buck was Leonard Bloomfield's teacher. That ought to count for something. I wish that I could settle for that, but total candor compels me to reveal that my learned relative and I share a common ancestor, one Colonel Jonathan Buck, who is reputed to have burned a witch back in the 18th century. So much for name-dropping. . .

I have mentioned all of this in order to explain why I was such a late-bloomer in the field of linguistics. It wasn't until I arrived at Arlington Hall over 30 years ago that I realized something was going on that I knew very little about. After the war, I received some free benefits when my older brother decided to get his PhD in linguistics. He not only tested each theory on me, but passed on many of his textbooks, hoping that they would do me some good. In self-defense, I began to read through them. I started with Bloomfield -- and discovered that there was a whole new world waiting out there. Then I read Bloch and Trager, and found them informative, but not likeable. While this sort of desultory reading was going on, I became deeply involved in book-breaking -- or, to use a term that I prefer, *code reconstruction*. Before I retired in 1973, I had worked on a great variety of codes,

EO 1.4.(c)
P.L. 86-36

I know that this sounds boastful, so I shall hasten to add that I still consider myself a novice in the field. I have seen a lot, but not all, of the elephant, so give me credit for being aware of that gloomy fact. One result of all this knocking around was that I acquired a compulsion to talk and write about my experiences, remembering that when I started out, no one told me anything. Not a word was uttered in my presence regarding tools, techniques, or standards. The implication was that either you could do it or you couldn't -- it was just as simple as that.

Plopped into My First Assignment

Throughout most of my career, I have been a loner. On the few occasions when I have worked with another bookbreaker, I have discovered a curious reluctance on his or her part to talk about methodology. Usually it was a case of "That's what it means because I say so" or "If you challenge my results, you attack me

Stu Buck retired from NSA in 1973 but returned to P16 several days a month as a reemployed annuitant to work on a special project requiring his unique qualifications. When he was finally debriefed at the conclusion of that project in October 1977, he handed over to a few coworkers copies of papers they might still find useful. Among those papers was the text of a talk Stu had given in September 1974, which is published here as sound words of advice for the next generation of people to carry out what Stu calls "one of the basic missions of the Agency."

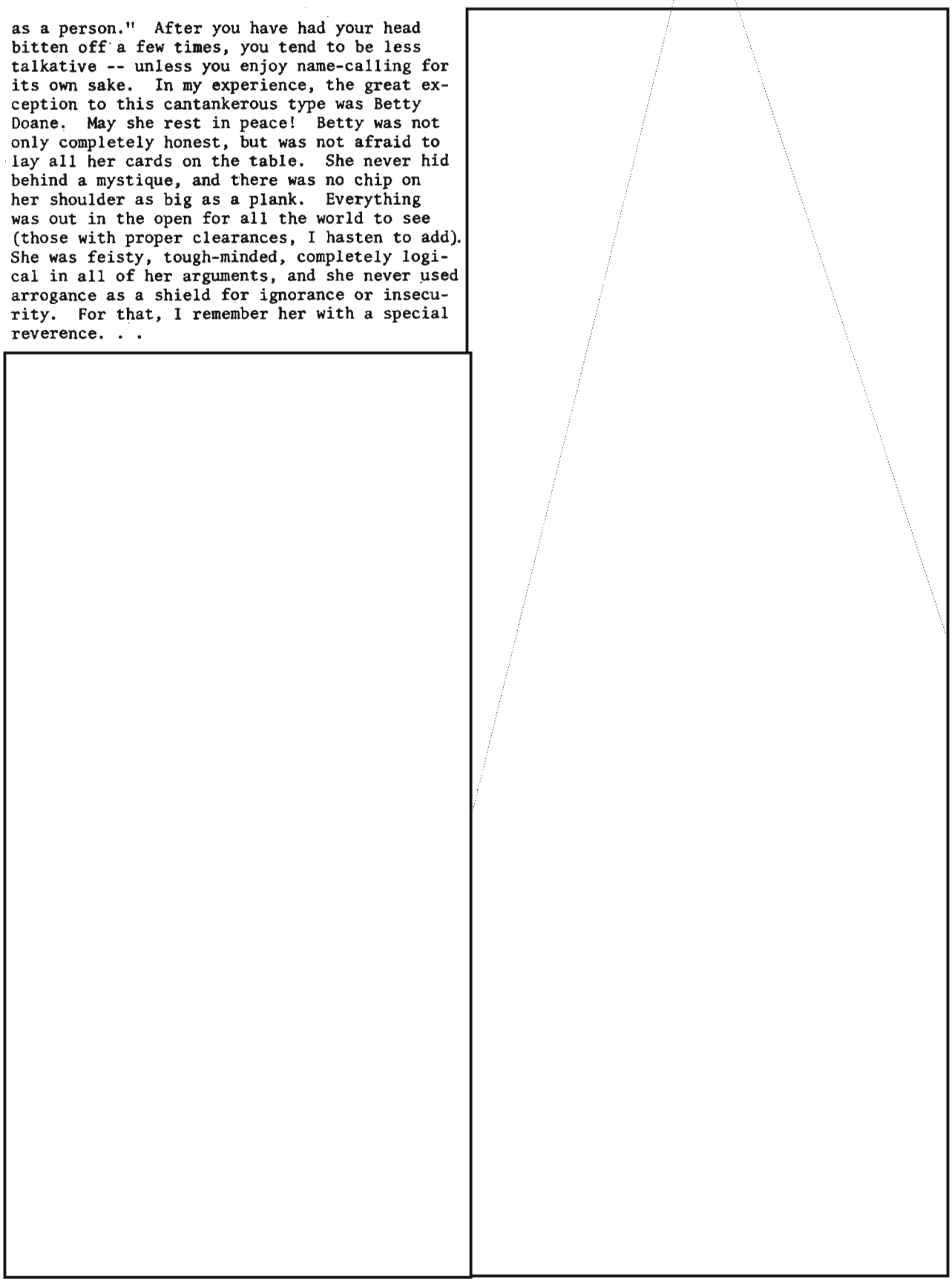
Ed.

EO 1.4.(c)
P.L. 86-36

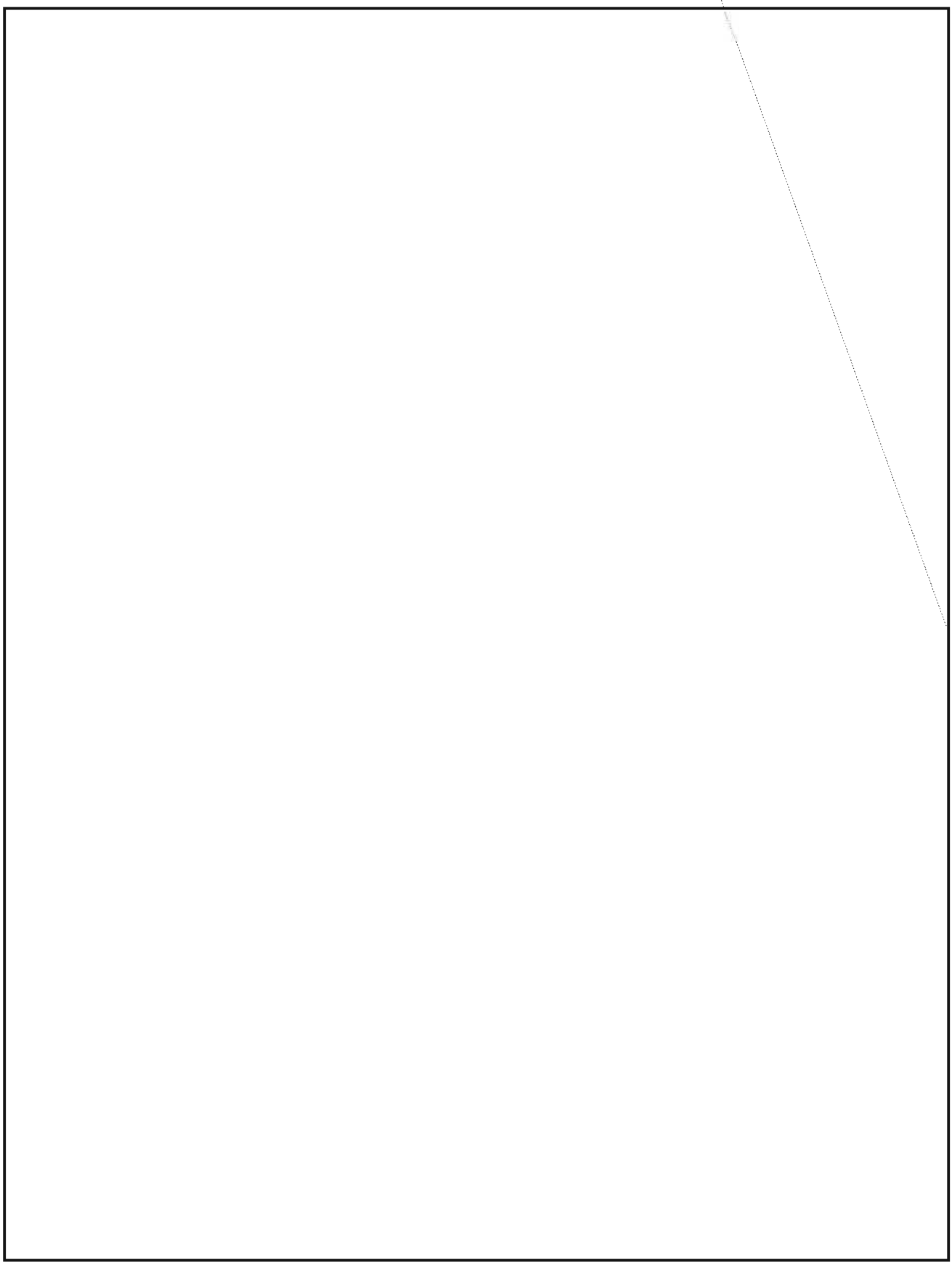
DOCID: 4009817

EO 1.4.(c)
P.L. 86-36

as a person." After you have had your head bitten off a few times, you tend to be less talkative -- unless you enjoy name-calling for its own sake. In my experience, the great exception to this cantankerous type was Betty Doane. May she rest in peace! Betty was not only completely honest, but was not afraid to lay all her cards on the table. She never hid behind a mystique, and there was no chip on her shoulder as big as a plank. Everything was out in the open for all the world to see (those with proper clearances, I hasten to add). She was feisty, tough-minded, completely logical in all of her arguments, and she never used arrogance as a shield for ignorance or insecurity. For that, I remember her with a special reverence. . .



EO 1.4.(c)
P.L. 86-36



DOCID: 4009817

P.L. 86-36

Q&A:

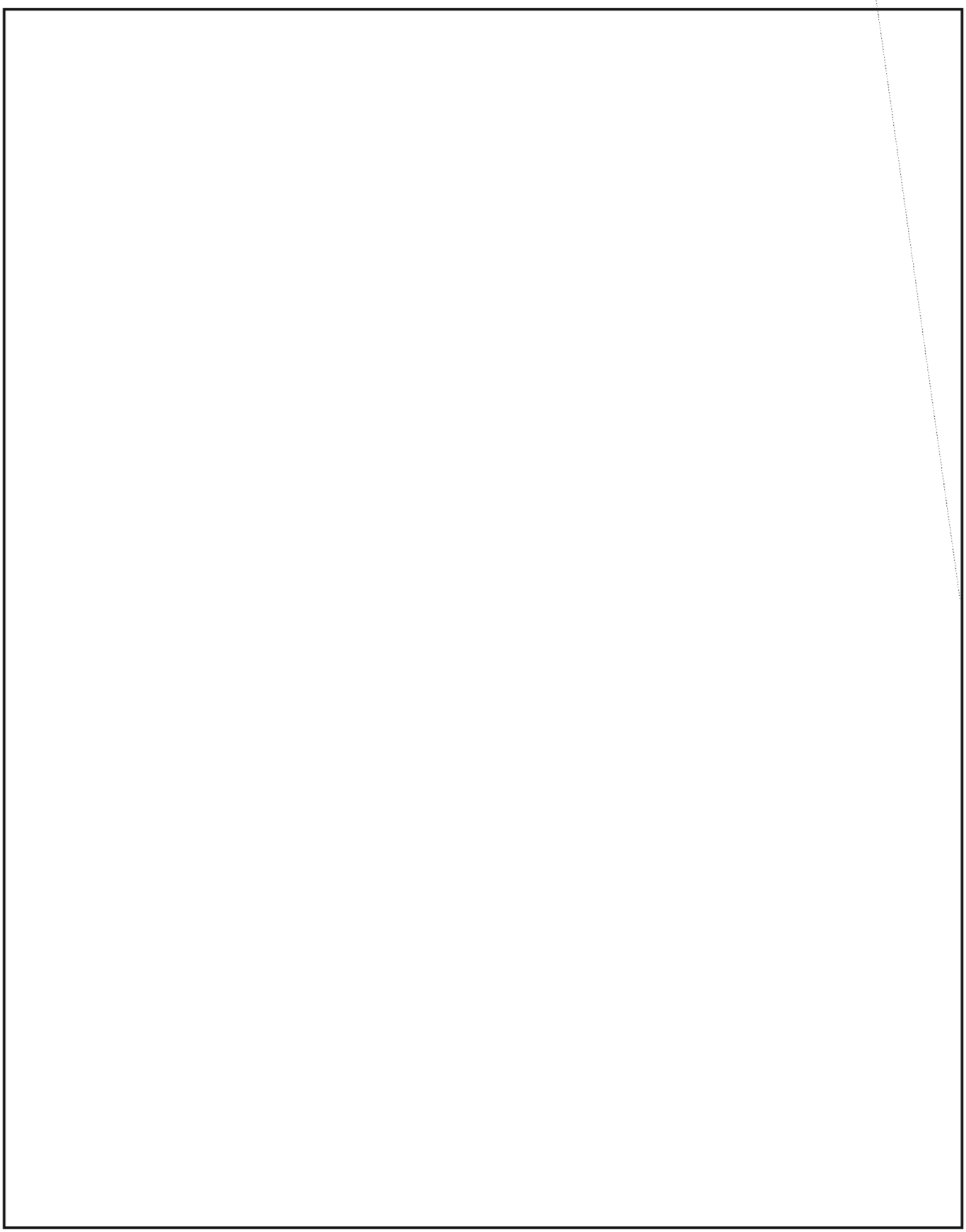
A DIALOGUE BETWEEN MS. USER AND DR. ANALYSIS

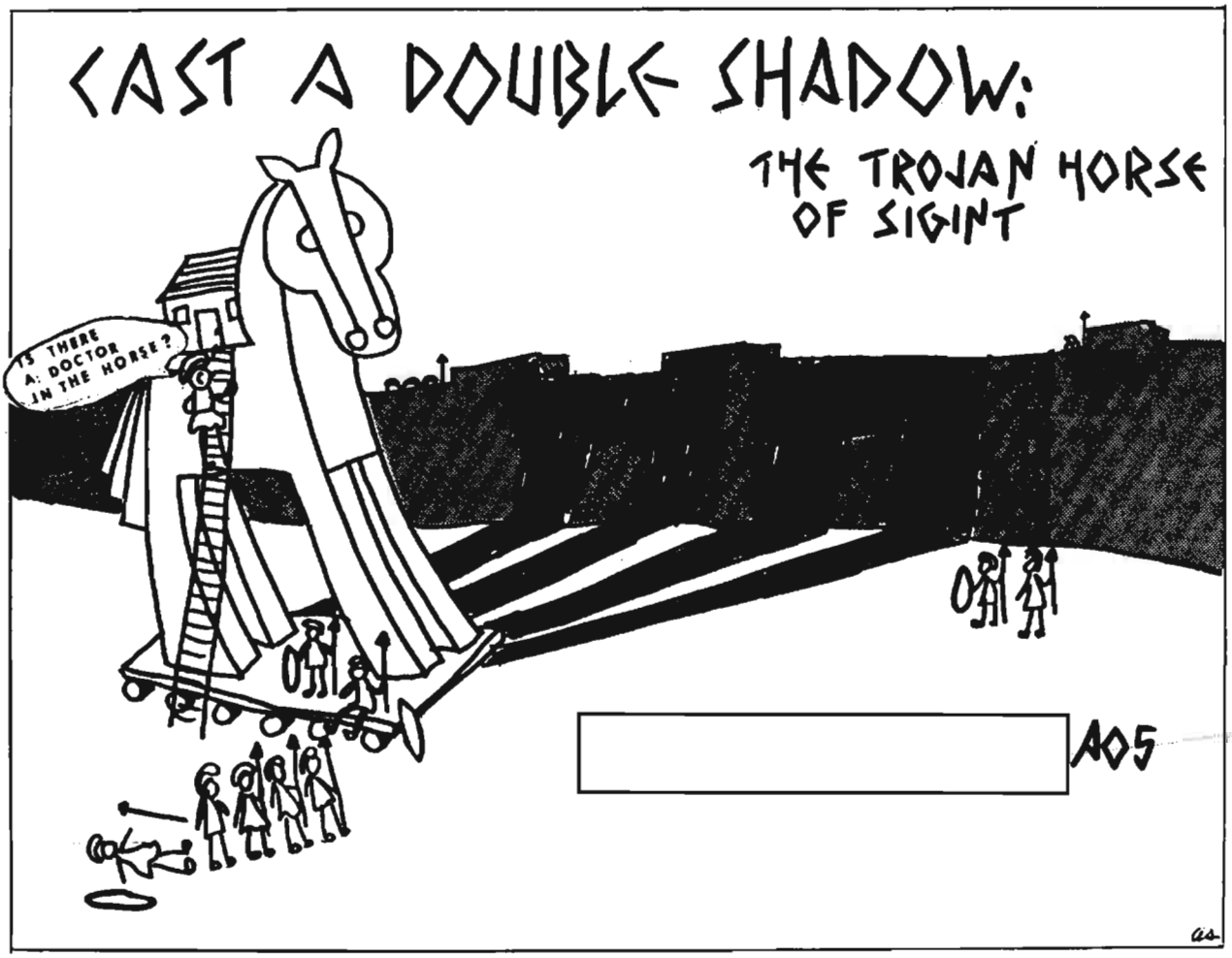
[redacted] **R51**

[redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36





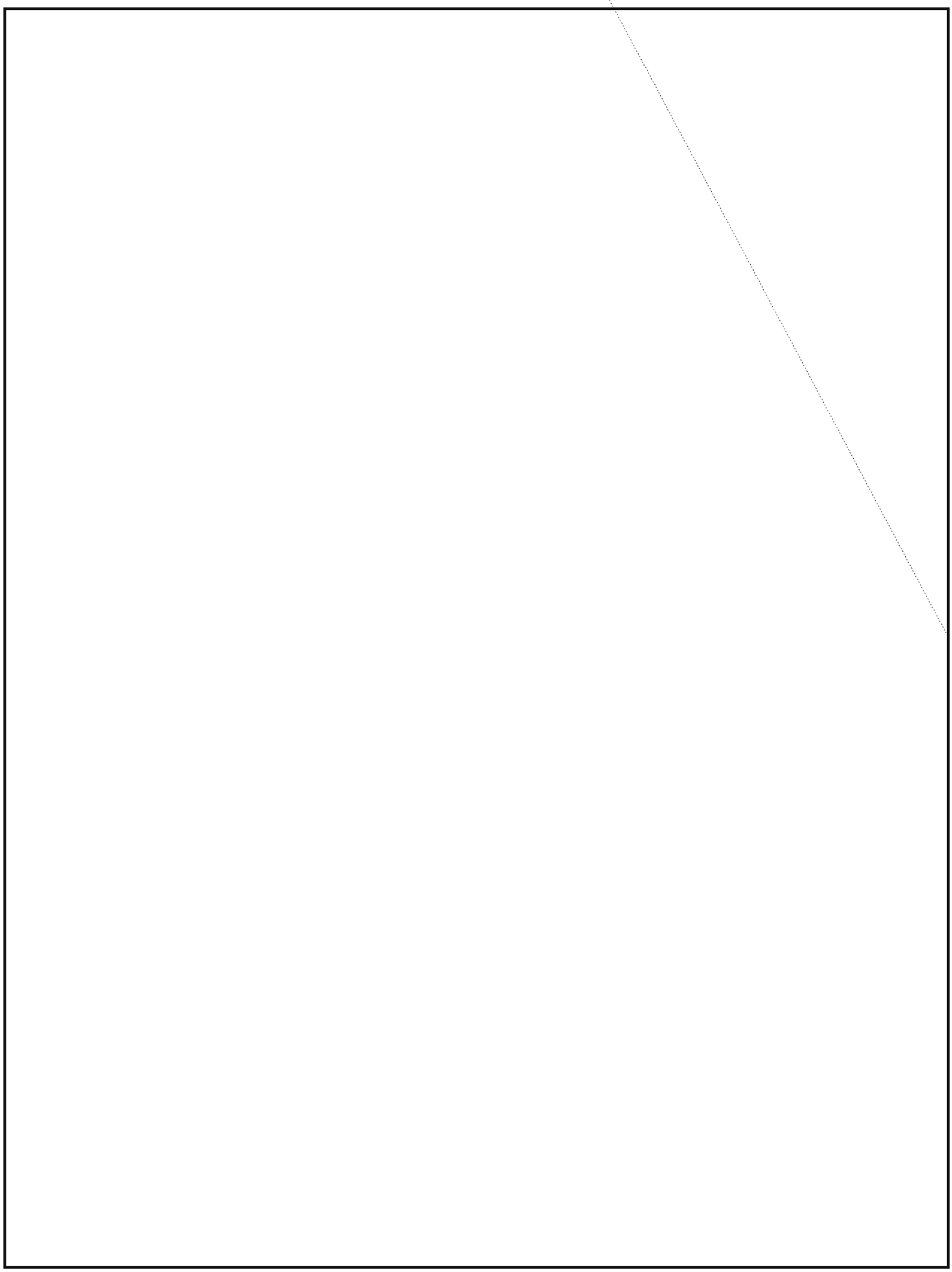
Among the leading attributes of COMINT, according to its past and present practitioners, are the dual qualities of timeliness and authenticity. SIGINT support to tactical military commanders is contingent on these two characteristics, while a wealth of combat and peacetime applications have borne out this unique dependency on the intelligence source known in the open literature as "intercepts." Only recently, in the works of Kahn, Winterbotham, and Brown, has the public been told the story of the central, critical role played both by COMINT and by radio strategems in World War II and in the Allied victory. In fact, so consummately has this story been told that it is now necessary to revise history in light of information only recently made available to scholars. Here we see journalists, and a former SSO, in the role of historical revisionists -- not a new role for journalists, but certainly a new role for SSOs, at least in the open literature.

Dependency on SIGINT's timeliness, authenticity, and -- oft-times -- uniqueness is unsettling. The quality of "believability" or creditability -- the much sought Al source -- is fraught with potential disaster, as Brown's *Bodyguard of Lies* convincingly demonstrates, even to the most skeptical reader. Creditability is everywhere and at once a two-edged sword.

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

EO 1.4.(c)
P.L. 86-36



~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4009817

FORMATTING PL/I SOURCE CODE

[redacted] P16 P.L. 86-36

IBM's Programming Language One (PL/I) is an extremely large and complex higher-level language, even by the standards of programming languages being designed today. To the novice this language is presented either in a watered-down version, sort of a "new style" of FORTRAN, or in such detail that the novice is quite easily overwhelmed. One would expect (as in fact is the case) that the compilers which process this complex source are themselves complex and they, too, are often presented in the same two extremes to the inexperienced user. Either one uses with faith a set of mysterious "JCL" which has been passed around the office and takes for granted that this JCL is in some now-unknown sense optimal, or one obtains one of the compiler guides and attempts to wade through the wealth of information presented there. To aid the PL/I programmer, two catalogued procedures have been developed which allow the programmer to maximize the amount of useful information on the job listing and to have that information arranged and formatted in a highly readable way. These procedures have also been designed to be easily used: each requires only one JCL card.

The PL/I Compilers

Unlike most other higher-level languages, PL/I is supported by two distinct compilers. One compiler, the Checkout compiler, provides very detailed and elaborate diagnostics in addition to, in some sense, acting as a PL/I interpreter. It is not too incorrect to consider that the Checkout compiler interprets PL/I code, while checking subscript bounds for array references, string ranges for substring operators, the attempted use of uninitialized variables, etc., in addition to "trapping" many system-level errors (e.g., overflow or underflow, transmission errors, etc.) and providing diagnostic information before the standard system action is taken. The facilities of the Checkout compiler can be invaluable for program development.

The user, however, "pays" for the extensive checking and debugging aids of the Checkout compiler in increased execution time. For this reason another compiler, the Optimizing compiler, is used for the final compilation before the program is used in production. This compiler attempts to optimize (either time-optimize or space-optimize) the resulting object module by eliminating both common and redundant expressions, replacing in-line code for library function calls, and analyzing DO groups to allow for optimal object coding for some special cases. The Optimizing compiler can substantially reduce the execution time of a PL/I program compared to the old PL/I(F) compiler and, as was stated earlier, the Checkout compiler. It will not, however, check for certain types of user errors such as the use of uninitialized variables. It is precisely these types of errors that can return to haunt the programmer, or, more probably, the person now in charge of maintaining someone else's old program with an unexplained abnormal termination after months of successful production use. The use of the Checkout compiler in program development can reduce the occurrence of such errors.

KENSPL1 and KURTSPL1

A large number of compilation options exist for each compiler. These options vary from those that govern the amount and type of information on the job listing to those that determine the amount of optimization to be done or debugging aids to be included. The proper use of these options will allow the user to get the most out of any particular debug run, or will allow the programmer who has to modify some old source code to understand the program logic as easily as possible. The catalogued procedure KENSPL1[1] does a PL/I compile, link-edit and execution using the Optimizing compiler, and KURTSPL1[2] does the same thing with the Checkout compiler. Both these procedures have been designed to be used by the novice, so that the following JCL is all that is required:

```
//name JOB      (standard JOB card)
//  EXEC KENSPL1   (or KURTSPL1)

          [PL/I SOURCE]

//
```

So, in essence, the user need remember only one JCL card, the EXEC statement.

KENSPL1[3] formats the PL/I source using the standard PL/I format conventions, e.g., DO groups and the THEN and ELSE clauses of IF ... THEN ... ELSE statements are indented, statement labels are highlighted, etc. Comments can be formatted in three different styles, all under the control of the individual programmer. The formatting of the entire source is done in a 100-column-wide section of the listing, allowing for complex PL/I statements to be listed in one line. The block and DO-group nesting level prefaces each statement. Commonly used PL/I abbreviations (E.G., DCL, PROC, PTR, DEF,

[1]KENSPL1 is named in honor of [redacted] a former Agency employee. P.L. 86-36

[2]Guess!

[3]Since both KENSPL1 and KURTSPL1 produce the same output, only KENSPL1 will be discussed from this point on.

etc.) are expanded for greater readability. The equal sign, when used as an assignment operator, is separated from the target and source variable by a blank. In addition one can use imbedded listing control statements (e.g., %SKIP, %NOPRINT, etc.). (Here, "imbedded" means occurring in the same source record as a regular PL/I statement.) Without KENSPL1 this feature is not supported by the Optimizing compiler.

This automatic formatting allows the logic of the program to be seen more easily both by the program designer and, more importantly, the programmer in charge of program maintenance. It also frees the designer from the work of "hand-formatting" a source file and the person in charge of maintenance from the errors of any incorrect "hand-formatting." When this automatic formatting is used in conjunction with the DO levels, the correct location of missing or misplaced END statements can be quickly determined as well as some common program-design errors.

An alphabetical list of all variables used in the program follows the source listing. For each variable, this list contains all the attributes of the variable, whether declared or assumed by default, and a list of each statement (by statement number) where this variable is referenced. In addition a table of all the arrays and structures used in the program is listed along with information concerning the number of dimensions, size and alignment in storage. To aid in debugging and hand-optimization, KURTSPL1 also produces a table listing the number of times each statement in the source was executed. An example showing the output of KENSPL1 vs. the standard IBM procedure, PLIXCLG, is shown in Figs. 1a and 1b.

```
PL/I CHECKOUT COMPILER  FIGURE_1_FOR_CRYPTOLOG:

                    FORMATTED SOURCE LISTING

STMT LEV NT

 1      Ø FIGURE_1_FOR_CRYPTOLOG:
          PROCEDURE OPTIONS(MAIN) REORDER;

            /*                                                                    */
            /*          THE  LISTING OF THIS PROCEDURE SHOWS  SOME OF THE MAIN FEATURES OF KENSPL1  */
            /*          AND   KURTSPL1.   THIS PARTICULAR   COMMENT IS AN EXAMPLE OF A  FORMATTED,  */
            /*          CENTERED  COMMENT.  THIS TYPE OF  COMMENT IS MEANT TO BE USED FOR  GLOBAL,  */
            /*          MAJOR COMMENTS.                                           */
            /*                                                                    */

 2    1  Ø   DECLARE
              INPUT_RECORD CHAR (8Ø),
              OUTPUT_RECORD CHAR (1ØØ),
              EOF BIT (1) INITIAL('1'B),
              SPECIAL_CHARACTERS CHAR (2) INITIAL ('Ø?');
 3    1  Ø   DECLARE
              DUPL EXTERNAL ENTRY ( CHAR (*) VARYING, FIXED BINARY (31,Ø)) RETURNS ( CHAR (1Ø) VARYING);
 4    1  Ø   DECLARE
              LARGE FILE RECORD OUTPUT SEQUENTIAL ENVIRONMENT ( FB RECSIZE(1ØØ) BLKSIZE(1ØØØ) );

 5    1  Ø      ON ENDFILE (SYSIN)
                 EOF = 'Ø'B;

 6    1  Ø GET_RECORD:
              DO WHILE (EOF);
 7    1  1         READ FILE(SYSIN) INTO (INPUT_RECORD);/* THIS IS A COMMENT INTENDED ONLY FOR THIS
                                                          PARTICULAR LINE. NOTICE THAT IT IS FORMATTED TO APPEAR TO
                                                          THE RIGHT OF THE PL/1 STATEMENT. */

 8    1  1         IF (SUBSTR(INPUT_RECORD,1,1) = ' ' | SUBSTR(INPUT_RECORD,8Ø,1) = '+') THEN
                    DO;
 9    1  2            OUTPUT_RECORD = INPUT_RECORD || DUPL(SPECIAL_CHARACTERS,9) || '&' || ' ';
1Ø    1  2            SUBSTR(SPECIAL_CHARACTERS,2,1) = SUBSTR(INPUT_RECORD,2Ø,1);
11    1  2            WRITE FILE(LARGE) FROM (OUTPUT_RECORD);
12    1  2            END;
13    1  1         ELSE
                    LEAVE GET_RECORD;
14    1  1      END GET_RECORD;

            /* 'EOF' WILL BE "1" ONLY IF THE "LEAVE" STATEMENT WAS EXECUTED. THIS IS THE THIRD TYPE OF COMMENT
            FORMATTING. */
15    1  Ø      IF EOF THEN
                 CALL ERROR_ON_INPUT_FROM_SYSIN;


16    1  Ø   END FIGURE_1_FOR_CRYPTOLOG;
```

Fig. 1a. Source listing using KENSPL1

DOCID: 4009817


```
PL/I OPTIMIZING COMPILER          FIGURE_1_FOR_CRYPTOLOG:

                  SOURCE LISTING
  STMT

    1    FIGURE_1_FOR_CRYPTOLOG:
         PROC OPTIONS(MAIN)    REORDER;

         /*                                                              */
         /*  THE LISTING OF THIS PROCEDURE SHOWS SOME OF THE MAIN FEATURES OF   */
         /* KENSPL1 AND KURTSPL1.  THIS PARTICULAR COMMENT IS AN EXAMPLE OF A   */
         /*    FORMATTED,    CENTERED COMMENT.  THIS TYPE OF COMMENT IS MEANT TO BE  */
         /*          USED FOR GLOBAL, MAJOR COMMENTS.                      */
         /*                                                              */

    2    DCL INPUT_RECORD CHAR (80), OUTPUT_RECORD CHAR (100),
              EOF BIT (1) INIT('1'B),
         SPECIAL_CHARACTERS CHAR (2) INIT ('*?');
    3    DCL DUPL EXTERNAL ENTRY ( CHAR (*) VARYING, FIXED BIN (31,0)) RETURNS
             ( CHAR (10) VARYING);
    4    DCL LARGE FILE RECORD OUTPUT SEQUENTIAL ENVIRONMENT
           ( FB RECSIZE(100) BLKSIZE(1000) );

    5    ON ENDFILE (SYSIN) EOF = '0'B;

    6    GET_RECORD:    DO WHILE (EOF);
    7              READ FILE(SYSIN) INTO (INPUT_RECORD);  /*  THIS IS A COMMENT INTENDED
         ONLY FOR THIS PARTICULAR LINE.  NOTICE THAT IT IS FORMATTED TO APPEAR TO THE
          RIGHT OF THE PL/I STATEMENT.  */

    8    IF (SUBSTR(INPUT_RECORD,1,1) = ' ' | SUBSTR(INPUT_RECORD,80,1) = '+')
              THEN    DO;
    9    OUTPUT_RECORD=INPUT_RECORD || DUPL(SPECIAL_CHARACTERS,9)
          || 'G' || ' ';
   10    SUBSTR(SPECIAL_CHARACTERS,2,1) =
         SUBSTR(INPUT_RECORD,20,1);
   11    WRITE FILE(LARGE) FROM (OUTPUT_RECORD);          END;
   12   ELSE LEAVE GET_RECORD;  END GET_RECORD;

         /*  'EOF' WILL BE "1" ONLY IF THE "LEAVE" STATEMENT WAS
         EXECUTED.  THIS IS THE THIRD TYPE OF COMMENT FORMATTING.  */
   13    IF EOF THEN CALL ERROR_ON_INPUT_FROM_SYSIN;


   14    END FIGURE_1_FOR_CRYPTOLOG;
```

Fig. 1b. Source listing using PLIXCLG

In the link-edit step KENSPL1 also frees the user from concern about details that are almost always unimportant to the user. Subroutine calls to any of Nolan's Extended String Functions[4] or the Integrated Graphics Software (IGS) are automatically resolved without the special inclusion of any additional system library data definition ("DD") cards. In addition the link-edit cross-reference table is deleted from the listing. It is felt that this table provides little, if any, information to even experienced application programmers and in general "clutters up" the listing.

As with the extra facilities of the Checkout compiler, the features of KENSPL1 do not come free to the user. Table 1 gives an indication of the additional amount of CPU time required for KENSPL1 vs. PLIXCLG. While these figures can be used as a rough guide, the actual time for any given execution depends on the number of formatted comments, the number of instances of keywords to be expanded, the number of listing control statements, etc. This amount of extra machine processing is more than compensated for by shorter development time and easier program maintenance.

Table 1

Source description	*Extra CPU time using KENSPL1 rather than PLIXCLG**
FIGURE_1_FOR_CRYPTOLOG	1.45 sec
Medium-sized source (about 300 statements; extensive use of comment formatting)	5.46 sec
Large source (more than 700 statements; extensive use of all features)	8.27 sec

* Based on a sample of five runs for each procedure.

[redacted] *Extended String Functions for PL1*, R51/PROG-NOTE/04/77, 13 July 1977.

DOCID: 4009817

NSA-crostic No. 19

By David H. Williams, P16

The quotation on the next page was taken from the published work of an NSAer. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS

A. Central character in "Tobacco Road" (2 wds)

B. Real name of Sweden's greatest gift to American movies (2 wds)

C. Was (3 wds)

D. Giving of new life

E. Followed by word W, what Word B claims she *really* said (5 wds)

F. Poisonous plant which yields a heart medicine

G. Most fortunate

H. Deprive of possession

I. The Lone Ranger's great-grandnephew, Britt Reid (3 wds)

J. Having the gift of finding valuable things not sought for

K. Called, named (archaic)

L. Card game; cheat

M. Abou Ben -----

N. Illness characterized by inflammation or pain of the joints and muscles

O. One (Japanese)

P. Kipling's first poem (4 wds)

Q. Corporate name which might result from the merger of Fairchild and Honeywell ((2 wds)

R. "Pressed into service means pressed out -------." Frost, "The Self-Seeker," 1914 (2 wds)

WORDS

208 223 12 237 41 137 71 25 168 203 193 83

156 23 57 231 10 27 78 188 115 50 175 101 43

96 219

209 7 102 112 46 22 194 146

37 127 119 3 139 154 77 54 110 91 187 28 73

67

234 44 227 87 211 21 72 39 30 196 180 158

75 33 161 117 221 107 130 86 70 63

4 92 109 74 144 166 178 191

165 58 36 9 65 147 32 184 16 133 131

80 159 232 235 103 122 113 26 179 149 141 17 214

200

116 238 121 229 155 182 138 213 197 8 94 106 163

169 98 220 162 84

69 6 224 222 215 135

48 128 201 120 51

228 85 152 124 60 216 88 45 172 15

177 150 192 160

11 236 31 40 111 226 143 93 217 13 59 126 199

181 104 53 82 153

49 108 218 239 142 151 62 125 186 38 34 195 64

20 81 225 99 136

173 18 207 176 157 164 100

DOCID: 4009817

S. Correct

T. Capet, Herbert, or Downs

U. Adjective for Uriah Heep

V. Xylophonist's nonhostile stance, profile to the audience: "with ----------" (3 wds)

W. See Word E

X. Flagrantly wicked or impious

Y. Send

56 206 35 89 1

47 170 185 134

66 42 97 5 68

95 19 183 233 140 171 123 230 105 129 55 148 167

114 212 29 198

118 145 76 132 90

190 205 174 202 79 52 2 14 210

24 204 189 61

1 S	2 X		3 D	4 G	5 U	6 L	7 C	8 J	9 H	10 B	11 P	12 A		13 P	14 X
15 N	16 H	17 I		18 R	19 V	20 Q	21 E	22 C	23 B	24 Y		25 A	26 I	27 B	28 D
29 V	30 E	31 P	32 H	33 F	34 Q	35 S		36 H	37 D	38 Q	39 E	40 P	41 A	42 U	43 B
	44 E	45 N	46 C	47 T		48 M		49 Q	50 B	51 M	52 X	53 P	54 D	55 V	56 S
	57 B	58 H	59 P	60 N	61 Y	62 Q	63 F		64 Q	65 H	66 U		67 D	68 U	69 L
70 F		71 A	72 E	73 D	74 E		75 F	76 W		77 D	78 B	79 X	80 I	81 Q	82 P
83 A		84 K	85 N	86 F	87 E		88 N	89 S	90 W		91 D	92 G	93 P	94 J	95 V
96 B	97 U	98 K	99 Q	100 R		101 B	102 C	103 I	104 P	105 V	106 J	107 F		108 Q	109 G
110 D	111 P	112 C	113 I	114 V	115 B	116 J		117 F	118 W	119 D	120 M		121 J	122 I	123 V
124 N	125 Q	126 P	127 D	128 M		129 V	130 F	131 H	132 W		133 H	134 T	135 L		136 Q
137 A	138 J	139 D	140 V	141 I		142 Q	143 P	144 G	145 W	146 C		147 H	148 V	149 I	150 O
151 Q	152 N	153 P	154 D	155 J	156 B		157 R	158 E		159 I	160 O	161 F	162 K		163 J
164 R	165 H	166 G	167 V		168 A	169 K	170 T	171 V	172 N		173 R	174 X	175 B		176 R
177 O	178 G		179 I	180 E	181 P	182 J	183 V	184 H	185 T	186 Q	187 D	188 B		189 Y	190 X
	191 G	192 O	193 A		194 C	195 Q	196 E	197 J	198 V	199 P		200 I	201 M	202 X	203 A
	204 Y	205 X		206 S	207 R		208 A	209 C	210 X	211 E		212 V	213 J	214 I	215 L
216 N	217 P	218 Q	219 B	220 K		221 F	222 L	223 A		224 L	225 Q	226 P	227 E	228 N	229 J
230 V	231 B	232 I		233 V	234 E	235 I	236 P	237 A	238 J	239 Q					D.H.W.

(Solution next month)

DOCID: 4009817

NOT ONLY "NOT ON MY WATCH," MR. GURIN, BUT NEVER ON MY WATCH, IF I CAN HELP IT!

P.L. 86-36

[redacted]
NSA Archivist

There are few people in the Agency who read Mr. Gurin's article, "Never Again!" (CRYPTOLOG, June 1978) who are more in sympathy than I with his rage at learning that his "only-one-of-its-kind" file on an important processing experiment had been thrown out and then getting an explanation that "proved to be, essentially, 'It didn't happen on *my* watch!'" In fact, my unhappiness is probably even greater than his, because, unlike Mr. Gurin, whose responsibilities for their care officially ended when the papers in question were of no further foreseeable operational value, *my* responsibilities now *start* at that point. The discarded valuable records were destined to be *my* records, and I grieve for them as only an Archivist who has also had 25 years of operational cryptologic experience can.

I must, however, set the record straight, Mr. Gurin. You may have thought that you were sending your papers to NSA's Archives (and you spelled it with a capital A in paragraph 4, implying "The NSA/CSS Archives"), but you didn't. You sent them to "a records storage center." NSA didn't have any Archives in September 1967. In fact, it didn't have any Archives in September 1977 either. Only *now* does it have an Archives -- the Archival Holding Area (AHA) -- with internal NSA approval on 1 March 1978 and official National Archives and Records Service (NARS) approval following soon thereafter.

To all you readers who may be inclined to heed Mr. Gurin's warning about checking the safety of your stored materials -- we (the AHA) agree. Do so! And after you have done this and have reevaluated your holdings, if you still feel that they are "documents," a "collection," or "papers"[1] of enduring value, please send them to the NSA/CSS Archival Holding Area.

What guarantees can we give you that your precious file won't have the same unhappy fate of Mr. Gurin's? As with all things in life, there can never be any absolute guarantees. But we can and do offer the guarantee that the NSA/CSS Archives will be a *thoughtfully* and *carefully* run operation, with as many controls as possible to preclude such unfortunate and irreversible occurrences. Unlike records storage areas, we will not be dealing with masses of items that are unknown and uncared for save by an arbitrary finding number. We are not just box custodians. The primary interests and reponsibilities of the AHA are for what is *inside* the boxes. As we acquire and access documents or collections that merit permanent retention (the National Archives and Records Service says that only 3 percent of all Federal records generated really fall into that category), we will be recording *who* sent them. Subsequently, we will follow the archival principles of "respect des fonds" and provenance and will record, as well as scrupulously comply with, any and all restrictions the donors may place on them. The skilled personnel of the AHA will examine all items received with a view to selecting those of permanent importance, and will, upon request, return whatever appears to be inappropriate. Once accessioned, items will be studied, described, entered into a finding-aid system tied to a source-content descriptive system, labeled, and stored in archival storage boxes on shelves in the AHA. Temporarily the AHA will be in SAB 2 (the old IRC Building). Ultimately, in the 1983-1984 time frame, it will be a part of a newly constructed SAB 5, in a separate, environmentally controlled facility designed for complete and permanent protective storage.

I hope that Mr. Gurin will forgive me for rewriting the very last sentence of his article, but I think that if he had been fully aware of the newly established AHA and its mission, aims, and potential for undoing the chaotic old system (that is, *non*system) for protecting valuable documents, he might even have made the change himself:

> "And, dear reader, if you have anything stored in archives[2], you would be wise to check right now and, if it really is of archival significance, send it to the NSA/CSS Archival Holding Area (c/o [redacted] FANX II, A1A26, 8297s)."

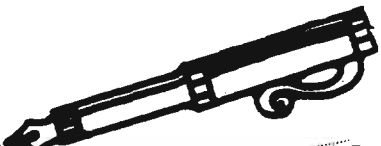
P.L. 86-36

[1] Each of these terms has a special meaning to archivists, but the AHA encourages people to just send whatever they have and let us determine the proper category.

[2] Note the "archives" with a small "a," which equates to "a records storage facility."

~~CONFIDENTIAL~~

Letters to the Editor



P.L. 86-36

To the Editor, CRYPTOLOG:

I wish to expand upon a point touched upon rather briefly in [redacted] informative article on technical translations ("Has It Ever Been Translated Before?", [redacted] CRYPTOLOG, July-August 1978), i.e. the W31 translation effort. W31 publishes contract translations of technical articles and books (or portions thereof), the latter comprising the majority of W31 material translated. The program is aimed to satisfy the interests of W Group and the other NSA organizations. Selection criteria are based on W31 knowledge of cryptologic and other SIGINT interests to NSA elements (inputs solicited), as well as requests from organizations outside of W31. In contrast, translations by JPRS, FSTC, and FTD are performed only to satisfy specific analyst requirements.

[redacted]

Regarding the STINFO system, two copies of all W31 translations are sent for retention to the Technical Library in addition to the key words, abstracts, and publication information. An index of all NSA translations of this type (1962-1978) is available from W31 (3463s).

[redacted] W31

~~(C GCO)~~

To the Editor, CRYPTOLOG:

It's only fitting that my first letter to the editor of anything should be of the bitch-and-moan variety, but then they're the only kind that anybody reads. Whatever, after being told repeatedly for about 10 years that the old annual performance appraisal doesn't mean a damned thing, I'm finally inclined to agree to the point where I really think that the whole thing should just be scrapped. It'd save time, money, and energy, and nobody'd be likely to miss it. It doesn't work and it can't be made to.

This conclusion didn't come to me overnight. At first glance it looks like the shortcomings of the present appraisal system could be overcome. This system, as applied by A2 (and, for all I know, elsewhere), is designed to let an employee and his or her employers know what sort of work the employee has done over the past year. It doesn't do this, for the following reasons:

- It operates on a quota system. This means that you can't recognize more than a certain percentage of the people in a given grade in a given organization as doing outstanding work, no matter how many are actually doing such work. The results are misleading and counterproductive.
- It's a seven-level categorization sloppily modified so that only five levels may be used. Levels 2 and 6 are considered not to exist, but no compensation is made for their absence. (Actually, they're not even absent -- they're right there on the form but you pretend they're not there.) Supposedly, excessive use of Level 6 was being made by supervisors. The remaining five levels really only describe three types of performance: very bad, mediocre, and very good. Consequently, the work of most employees is categorized as mediocre, and that is a real morale-booster in a place that supposedly employs a lot of pretty sharp people.
- It's directly attached to the promotion system. This really circles back to the first reason. If your branch quota for a certain grade level is one Level 7 appraisal, and you've got someone in this grade level up for promotion, then this person has to be your 7. Otherwise someone's going to want to know just what the hell he's doing up for promotion with a crummy Level 5. There's no reason why one person's performance appraisal should be affected by someone else's eligibility for promotion.

So does this mean that the system still can't be revised and made to work? Right! it can't! Even if you remove the quotas and the attachments to promotion, and establish a whole new set of performance levels and criteria, the

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

system is still dependent on the frequently subjective opinions of frequently unqualified supervisors. Supervisors are, in turn, encumbered by inconsistent and often conflicting managerial policies. The system was also designed to encompass too broad an area to accurately assess individual performance. The assessment of an employee's work can be done best within, at most, his own branch. Nevertheless, approval of a Level 7 appraisal must be done at such a high managerial level that often the person giving final approval has never met the person being approved.

To wrap this up, my final argument for dumping the system is that it's unnecessary. Step increases are given to acknowledge satisfactory work. QSIs, SSWPs, and, supposedly, promotions are given to acknowledge outstanding or superior work. Performance appraisals don't acknowledge much of anything and, as a supervisor, I'd much rather forgo the embarrassment of explaining to someone that, while I personally think he or she is doing excellent work, this worthless form says that the person "occasionally exceeds performance norms." Fortunately, nobody takes performance appraisals seriously enough to interpret this as an insult.

[redacted]

(U)

Editor's note: It is generally the rule that CRYPTOLOG publishes anonymous contributions only if the writer's identity is known to the publisher or editor. It is felt, however, that an exception ought to be made for the following completely anonymous letter.

To the Editor, CRYPTOLOG:

I have just received word that another key employee has joined the ranks of the Agency resignees. I couldn't help thinking what might have been the underlying cause of his (not to mention countless others) decision to leave. I hunted for a past issue of CRYPTOLOG (November 1977, to be precise) to find an appropriate article I had run across a few months back. Perhaps the words of wisdom in that article should be revitalized.

Nine months have elapsed since [redacted] interesting and factual article entitled "A Proposed Cure for the Time-in-Grade Syndrome" appeared in CRYPTOLOG. It has obviously not been forgotten by many, such as myself, who firmly believe something ought to be done about the infectious time-in-grade disease rampant throughout the Agency. It appears to have been ignored by the Agency ruling class, however.

One point I feel [redacted] should have elaborated on, though, concerns the archaic ritual of giving yearly performance appraisals. I was led to believe these "psychological strokes" were designed to inform employees of their progress in their present job. In actuality, they seem to be used as a major factor by the "time-in-grade-loving" supervisors/panels in determining which old timer should receive his or her "pay raise" first. Notice that I did not call it a "promotion."

The performance appraisal, under normal circumstances, should be a very good indicator of an individual's performance. I say "should" rather than "is" because I, for one, do not believe it is an accurate way of determining just how well an employee executes his or her job. The way the performance appraisal is set up at present, it is impossible to judge an individual's true progress. For instance, where on the current form does it allow a supervisor to praise an individual for his or her initiative? I've had supervisors in the past completely ignore certain talents and skills I had acquired that I felt were significant towards successfully and efficiently executing my duties. I've also had other supervisors rate me according to a set of duties that some nameless individual in M Group dictated as fulfilling my particular job description, but which, in fact, I never did. And imagine my shock when a previous supervisor once announced, "I'm giving you a low rating on your appraisal this year since you've just been promoted, and we want to give others at your previous grade level a stab at a promotion." How do you think that would have looked on the personnel records if an individual, recently promoted (supposedly equivalent to a Level 7 rating), only received a Level 3 for that year? Since the past 3 years' performance ratings are often included when a supervisor prepares a Promotion Recommendation, do you honestly feel this is a fair system?

P.L. 86-36

We employees (to quote [redacted] have the responsibility for qualifying for promotion, and these qualifications (excluding time in grade) should be judged by an impartial panel, composed of upper management individuals from various elements, who will make their recommendations on the basis of an individual's initiative, drive, willingness, and experience (whether the experience was gained from working inside or outside the Agency), as well as current job performance.

Until a new system for recognizing and rewarding bright employees is established, I'm afraid we shall hear of more key people joining the ranks of the resigned.

"Wish to remain anonymous
due to impending resignation,"
F8353

(U)

[redacted]

P.L. 86-36

C.A.A. NEWS

- Do you like to play games and call it work?
- Are you using cryptanalytic principles and techniques while analyzing your traffic?
- Would you like to be the one to solve that new callsign, frequency, or procedure system?
- Do you already solve complex systems before lunch and sneer at those who need brunch to keep up?
- Would you like to know more about many of the crypto-TA principles used routinely on all TA PQEs?

If you answered yes to two or more of these questions, there is a Special Interest Group (SIG) within the CAA for you. In an effort to appeal to crypto-TA enthusiasts on all levels, the Crypto-TA SIG is now reorganizing to do the following things:

- Search out current practioners of crypto-TA and ask them to make formal presentations to the SIG;
- Try to reach case analysts to give them the necessary tools to recognize pertinent situations where crypto-TA principles could be applied;
- Upgrade the skill of TA professionalization aspirants through study groups, tutoring sessions, problem-solving guidance, etc.;
- Publish crypto-TA brain teasers in CRYPTOLOG every month.

For additional information concerning the Crypto-TA SIG, contact one of the following:

[redacted] 4466s
5372s
8356s
Paul McCormick 5845s

Communications Analysis Association:		
President	David Gaddy	3247
President-elect	Frank Porrino	5879
Secretary		8025
Treasurer		3791
Board members		4935
		5991
		3573
		3369

~~(C)~~

Solution to NSA-crostic No. 18

(CRYPTOLOG, October 1978)

[redacted] "[A] CRYPTOLOG Interview," CRYPTOLOG, December 1976:

"Now it's possible to include in an NSA report a statement like 'this could be an indication that country X is planning an attack on country Y,' whereas previously a report containing that statement would be difficult to get out of the building. There would have been too many doubting Thomases." (U)

"I said, 'Hender hoke!'"

MILITARY LINGUISTS

Military linguists who pass NSA's Language Proficiency Test (LPT) will receive a Certificate of Achievement from the Agency's Language Career Panel. Effective 1 October 1978, anyone who scores more than 130 points on the LPT will be awarded the certificate. Those who score 140 points or higher with get the certificate "With Honors." The passing rate from 1 July 1977 to 1 July 1978 was 40 percent. The awarding of the certificate is intended to recognize the extra effort that military linguists have expended to improve their professional skills. (U)

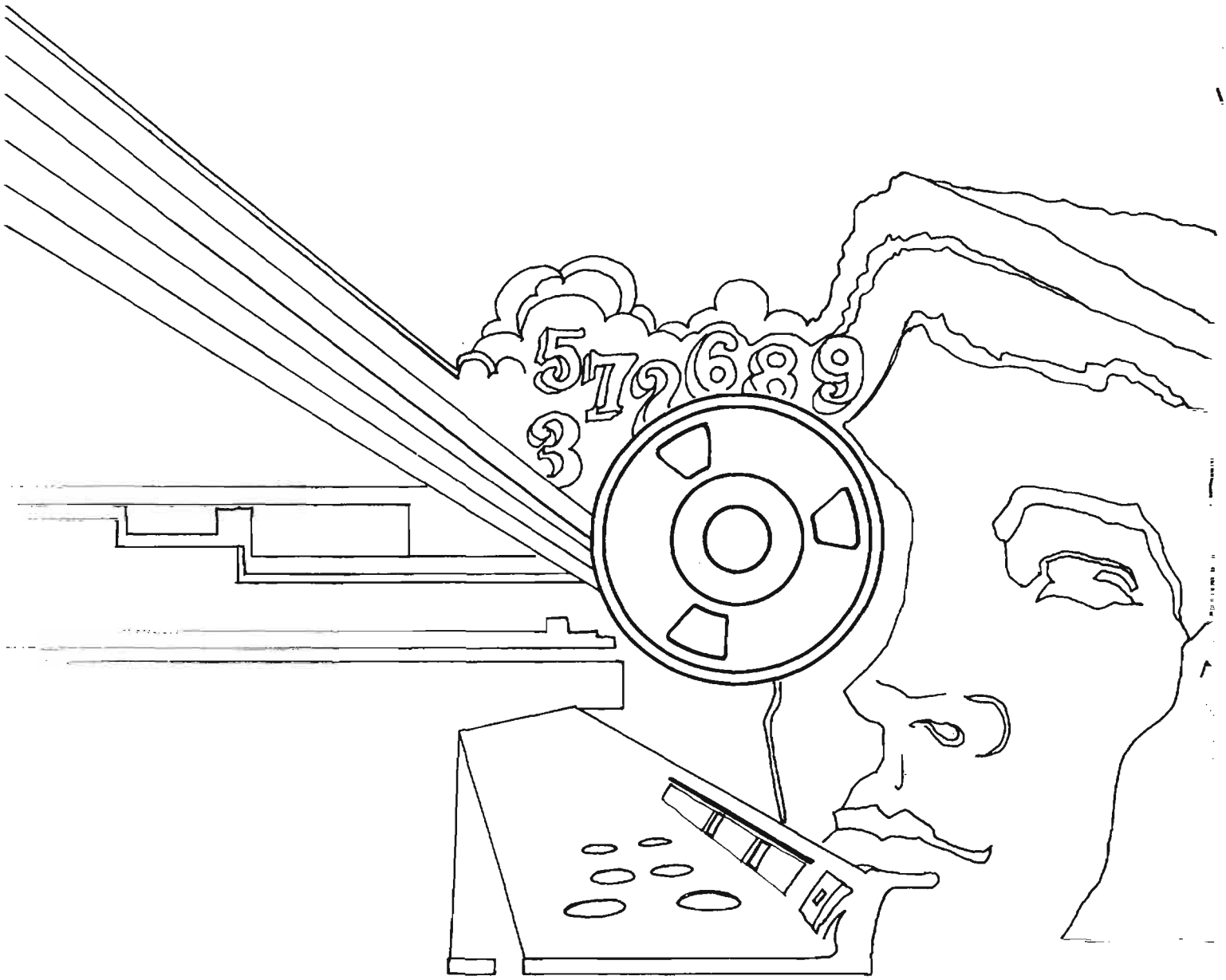
CORREZIONE!

P.L. 86-36

Now THAT'S Italian!

The spelling T-A-U-R-O-N-E, that is. As the editor of a publication that prides itself on being 100-percent free of typographical errors and misspellings (if you can prove otherwise, you may qualify to be an honorary proofreader for a month's issue of your choice), I am embarrassed to report that, as a result of a transcription error, the name of our new TA editor was Irishized in the past two issues. So please note that it's not "Don Tyrone" who's going to give aid and encouragement to traffic analysts who want to have their say in CRYPTOLOG, but Don *Taurone*, on 3573s. (U)

~~TOP SECRET~~



DOCID: 4009815

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

OCTOBER 1978

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

DATA SECURITY AND HUMAN ERROR	[redacted]	1
[redacted]	[redacted]	5
CONTINUING PROFESSIONALIZATION	[redacted]	7
METHOD OF MEASURING NEGATIVE INTELLIGENCE	[redacted]	9
CAN'T TELL WHEAT FROM CHAFF	J. Gurin	11
REDUCTION RATIOS IN MICROGRAPHICS	Don Snow	12
BACK TO SQUARE ONE!	[redacted]	13
FEEDING THE GERMANS MISINFORMATION	P. W. Filby	14
AND-A YOU BETTA HAVE MOTI-VAYSH!	[redacted]	15
NEWS OF COMMUNICATIONS ANALYSIS ASSOCIATION	W.E.S	16
MORE B. S. (BEFORE SPELLMAN)	[redacted]	17
LETTERS TO EDITOR	Pattie, Filby, [redacted]	19
NSA-CROSTIC NO. 18	David H. Williams	20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009815

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. V, No. 10 OCTOBER 1978

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5236s)

Collection..... [redacted] (8555s)

Cryptanalysis..... [redacted] (4902s)

Cryptolinguistics..... [redacted] (5981s)

Language..... [redacted] (8161s)

Machine Support..... [redacted] (5804s)

Mathematics..... [redacted] (8518s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis..... Don Taurone (3573s)

Production Manager.....Harry Goff (5236s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4009815

DATA SECURITY AND HUMAN ERROR

T321

P.L. 86-36

Illustrations by the author

People are not perfect: they make mistakes. In the computer world, they make mistakes in operating machines, entering data, writing programs, and designing systems. In this article I will discuss some of the ways in which people's mistakes -- most of them caused by simple carelessness -- can cause major security violations to data in a computer-system environment.

The term "data security" refers to protection of data against persons, against modifications, or against destruction. An understanding of the number of personnel and other resources having access to information is vital to estimating exposure probability. You must also understand *how* personnel can access information. From the security point of view, a prime concern related to the data-preparation and data-control department is to protect the large quantities of data they handle from destruction and tampering of any kind.

Not only is there concern with the security of the data, but also with the validity of the data. Harm can be inflicted in several ways, such as destroying or modifying other users' data; reading or copying another user's data without knowing it; and/or degrading the service another user gets, e.g., using up all the disk space or getting more than a fair share of the processing time. An extreme case is an accident which crashes the system. This might be considered the ultimate degradation.

The security of information inside a computer system has been dealt with by several authors, who have considered the problem from a number of different points of view, ranging from privacy to government security. All those authors stress the importance of *people* in maintaining proper security. Certain people will have access to the system by virtue of their position. These include the computer operator, programmers, maintenance engineers, users, and certain management personnel. Normally these people will be able to read, modify, or copy files and programs. But all of them, being *people*, can be careless and commit serious errors. Let's look at some of them.

Keypunch Errors

Keypunch errors can cause the loss of single records and modification of records. To even the most trained eye, incorrectly punched cards look the same as punched cards containing legitimate transactions. But an error in keypunching can lead to destruction of data in a file. Keypunch errors can occur when a programmar rushes to get one last run in before the end of the day. In hurrying, he dupes a card incorrectly, throws the correct card away, and adds the incorrect card to his deck (Fig. 1).

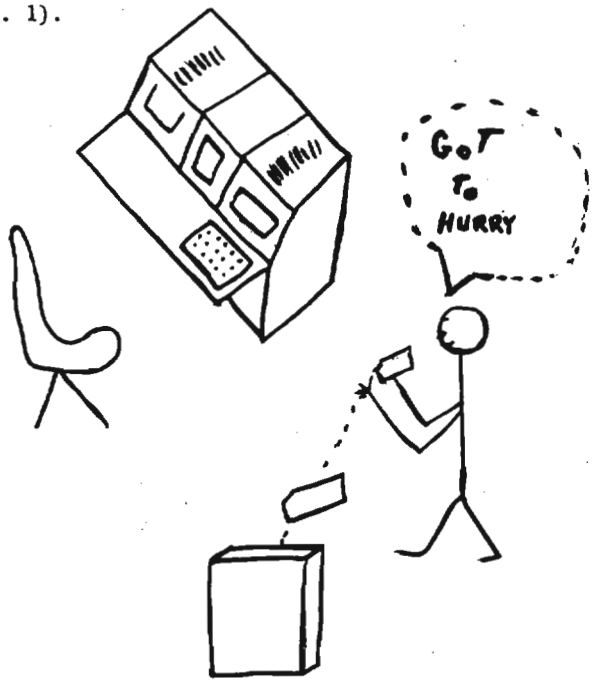


Fig. 1

Other keypunch errors occur when the computer operator is tasked to repunch cards that were destroyed by the card reader (Fig. 2).

Programmers and operators should take great care in examining the newly punched cards before entering them into the computer system.

Terminal Operator Input Errors

A user at a terminal accessing a file can cause loss of single records and modification of records.

Data preparation errors can cause a loss of data or permit erroneous data to enter the data file. When a file is initially created, the user of the file has unlimited access, to perform any of a number of operations on the file. These operations might include, for example,

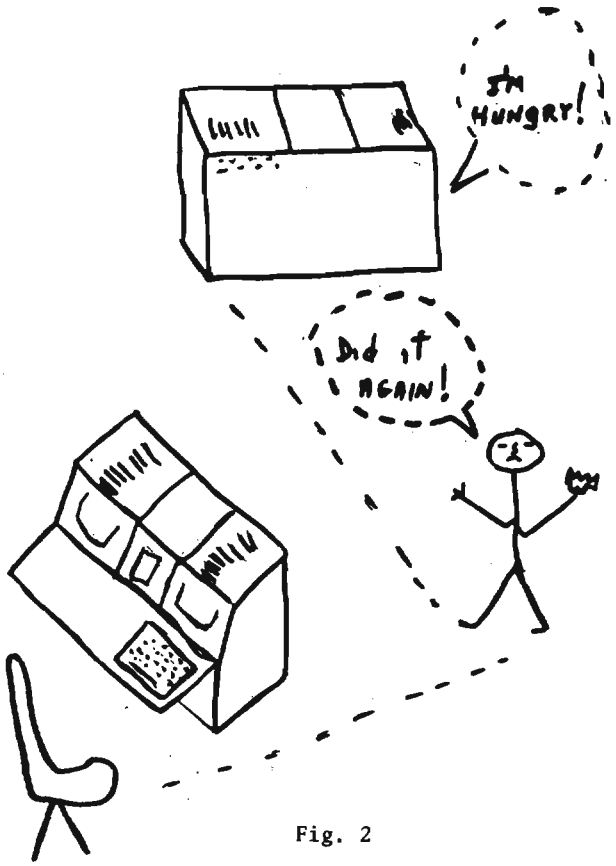


Fig. 2

reading the file, writing, emptying, renumbering, truncating (deallocating unused disk space), and renaming files (Fig. 3).

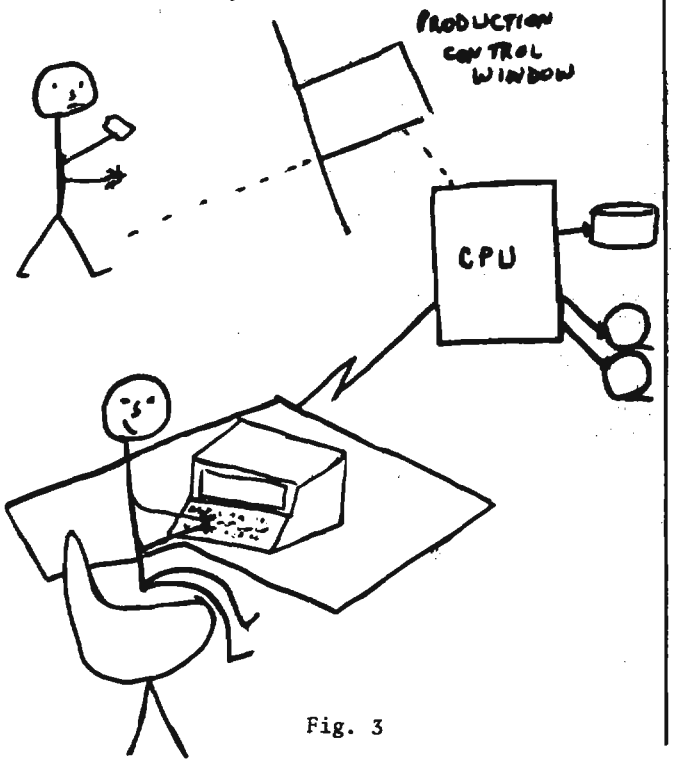


Fig. 3

Data can be destroyed in a file and replaced with inaccurate results, leaving the user with a situation where it may take considerable time to realize that he no longer has the correct data.

The user is responsible for his share of the security problem and should restrict his terminal and batch processing of files to authorized and competent personnel only.

Program Errors

Without a doubt the most common, embarrassing, and expensive software loss is program error. A not fully debugged program, coexisting with other programs, might as well be regarded as having been written by a malicious enemy -- even if all the programs have the same author. Program bugs originate because of errors in system design, errors in logic, errors in coding, errors in problem definition, or sometimes just incomplete definition. Program errors or bugs often do not show up until some *rare* combination of circumstances reveals them. They are so common that there is a regular mythology of program error (often attributed to the computer instead of the program). In some systems, a few residual bugs do not matter too much; in others they can be catastrophic.

Programs should be designed so that a user cannot alter the program. If programs are permitted to be altered, shared programs could be in a constant state of flux and this would lead to inconsistent results.

The majority of installations still have a real security gap when it comes to preventing insertion of unauthorized routines into programs.

The *Wall Street Journal* reported the Borden Company had announced a $2.8 million "deficiency resulting from what appeared to be an error in switching part of the company accounting system over to computerization two years ago" (Dennis Van Tassel, *Computer Security Management*, p. 54).

At Cape Kennedy a space launching failed because of a program error. The computer symbol equivalent of a comma was inadvertently left out of the program. The omission caused the rocket to go far off course and it had to be destroyed (*Ibid.*, p. 55).

While the impact of these two program errors is larger than most, they illustrate the possible magnitude of the problem.

The prime answer to the problems mentioned is *very* thorough program testing.

Operator Errors

Inexperienced computer operators often ignore console error messages, which can cause loss of single records, modification of records, and/or loss of an entire file (Fig. 4).

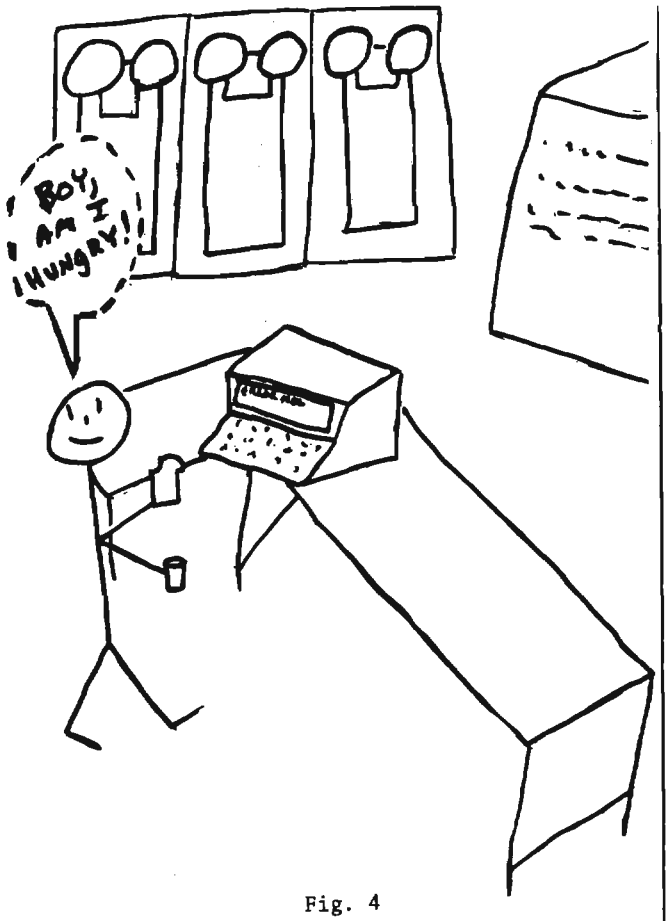


Fig. 4

The mounting of wrong tapes and/or disk packs for updating can cause a loss of entire files and modification of records. Physical damage to tapes or disk packs, such as dropping them on the floor, can cause loss of entire files or loss of single records (Fig. 5).

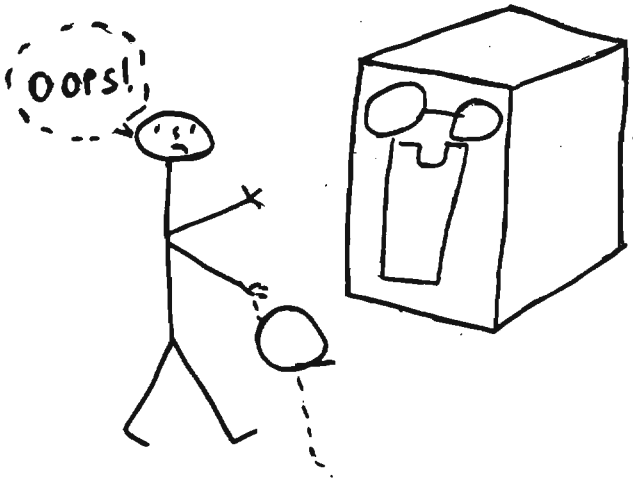


Fig. 5

Operators should be encouraged to strive for care rather than speed in handling tapes and/or disk packs.

An operator may accidentally process updates to a file twice, thus erroneously updating files. Throwing away the latest listing of an update and giving the user/programmer an earlier listing can cause the user and/or programmer to make erroneous changes to a file.

The following is an example of an operator error and what kind of problem it caused.

An operator mounted the wrong day's tapes. The program recognized the error and printed out a message saying so, but the operator ignored the message and pushed the restart button. This error was not discovered until month-end processing was completed, after which much work had to be rerun.

More care should be taken by the computer operator to assure the accuracy and safety of files kept in the computer environment.

Programmer Errors

A programmer updating the wrong version of a program can cause a loss of an entire file and/or modification of records.

A programmer who has access to the computer operations area can run his own jobs and make the same mistake an operator makes, such as mounting wrong tapes, ignoring console error messages, and/or carelessly dropping tapes or disk packs.

The following is an example of a programmer error and the damage it caused.

In August 1971 the French satellite Eole was launched by NASA as part of a cooperative French-American space program. The satellite was designed to gather data from 115 balloons, each carrying an instrument package around the earth at an altitude of 38,000 feet. On command from Eole, the balloons could transmit their information to the satellite, which in turn would relay the data to a computer center for analysis. The balloons all carried explosive charges which could detonate on a command from the satellite. On the 346th orbit of the satellite, a French programmer error caused the "Destruct" command to be sent to the satellite instead of the "Interrogate" command.

The error was discovered quickly, but before the instruction could be rescinded, the satellite had hurtled over the horizon, beyond control. A NASA spokesman said, "I couldn't tell you what happened after that; sort of chaos broke loose in the station." Eole destroyed 72 of the 115 balloons, all of those in its path on that orbit. NASA officials said the mistake resulted in some "procedural changes" at Mission Control and the possible demise of "one dumb computer programmer" (James Martin, *Security, Accuracy, and Privacy in Computer Systems*, p. 10).

Maintenance/System Errors

No system can be regarded as secure unless both the hardware and the systems programs are

designed for security.

The purpose of system controls is to prevent unacceptable data from being processed and to detect it if it does enter the system. System errors, either hardware or software, can cause a failure of one or more of the protective features. The system should be designed to log all attempts to access data files that failed due to a loss of the proper permission or password.

Conclusion

Security is only as strong as its weakest link, and the weakest link in the security chain is people. The weakness arises partly from the fact that people tend to evade or ignore the standards, and partly from the fact that people tend to concentrate on only one thing at a time. When there is pressure on the data processing department -- projects going live, last-minute modifications, emergency maintenance -- observance of standards falls off.

The value of data which is processed on computers, such as social security records and confidential information, is immeasurable. Consequently, protecting equipment and data from unauthorized or inadvertent acts of destruction, alteration, or misuse is a matter of inestimable importance.

Data processing security is a means of safeguarding hardware, software, and data against loss from accidental disclosure of data and/or modification of data.

The control of data-base vulnerability is a significant problem in many computer systems.

There is no method available for measuring the quantity or quality of security that may be adequate for a computer.

In many cases too little attention and too little money is allotted for computer security.

The effectiveness of a security system depends on the interaction of people within the data processing system. The implementation of proper procedures can help to regulate the interaction of personnel and the computer system, thus improving the security of the system.

Maintenance of security demands competence, loyalty, and integrity from all personnel connected with the system. In addition, it requires continuous training for them, both in operating procedures and in security measures. The purpose of this training is to ensure that each individual recognizes his or her vital role in security practices and does not, through familiarity with the system, become careless.

It is my opinion that each individual who is exposed to the computer environment, at periodic intervals, should familiarize himself or herself with the procedures established by management. It is up to management to see that the procedures are followed by all.

I also feel that if everyone would take more care and have more *pride* in his or her work, fewer mistakes would be made.

[redacted] *has prepared a bibliography on the topic discussed in this article. To obtain a copy, write to: CRYPTOLOG, P1, or call the editor on 5236s.* P.L. 86-36

(U)

WHO & WHOM?

By [redacted] P16 P.L. 86-36

& Nobody Else

Some people's last names have become such household words that we may forget that they have -- or had -- first names. This is especially true when two or more names get strung together. It's much easier to talk about "Lunt & Fontanne" than to throw in their first names too.

We have listed ten famous pairs on the left below and, over on the right, there are two columns of first names. In each case, the names in Column A are those of the first member in each pair, and those in Column B are those of the second member. (If we included Lunt & Fontanne "Alfred" would be in Column A and "Lynn" in Column B.)

You will note that all three columns are in alphabetical order, so, just by coincidence, a few names are in the right place. But we won't tell you how many or which ones.

	Column A	Column B
1. Barnum & Bailey	Charles	Adam W.
2. Currier & Ives	Isaac K.	Alva C.
3. Dun & Bradstreet	Merriwether	Arthur S.
4. Funk & Wagnalls	Nathaniel	Fred A. (Jr.)
5. Gilbert & Sullivan	Phineas T.	James A.
6. Lewis & Clark	Richard L.	James M.
7. Mason - Dixon	Richard W.	Jeremiah
8. Sears & Roebuck	Robert A.	John M.
9. Simon & Schuster	Robert G.	Max L.
10. Taft - Hartley	William S.	William

(Answer on page 18)

(U)

[redacted]

EO 1.4.(c)
P.L. 86-36

[redacted]

P.L. 86-36

[redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

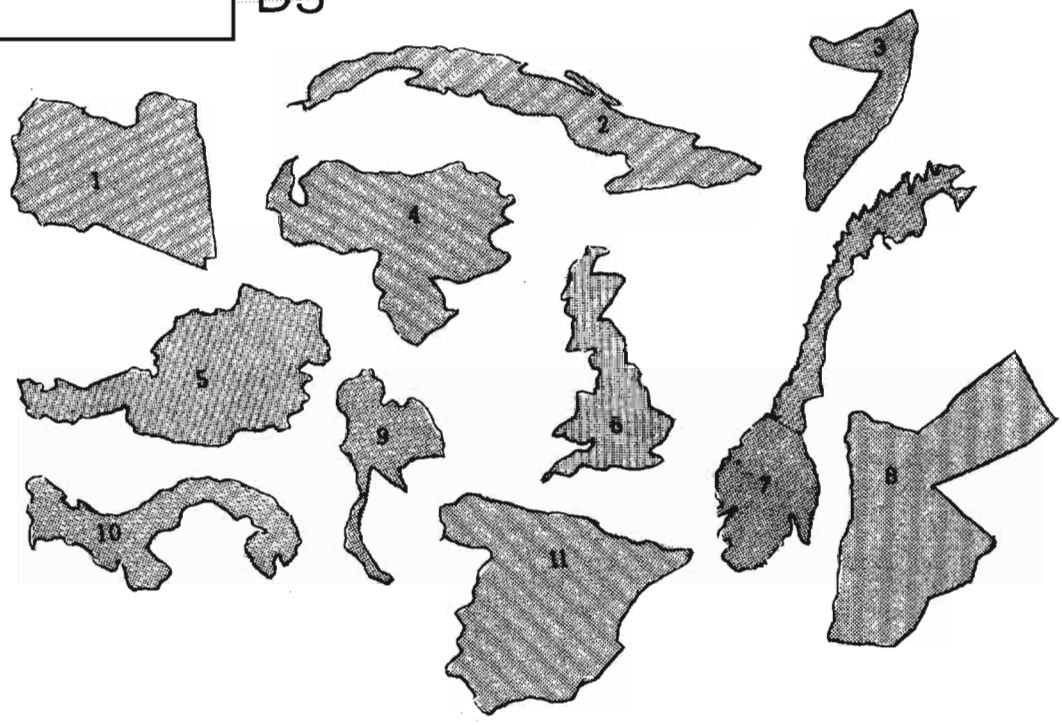
[redacted]

~~(TSC)~~

KNOW YOUR GEOGRAPHY

[redacted] D5

P.L. 86-36



Most countries are difficult to recognize when looked at in isolation. How many of the countries shown, which are regularly in the news, can you recognize? (Countries are not drawn to scale.) If you can get more than five correct, consider yourself at the head of the class.

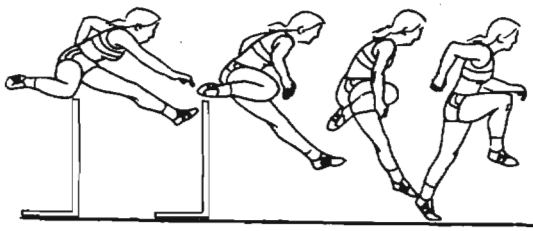
1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____

(Answers on page 19)

(U)

DOCID: 4009815

CONTINUING PROFESSIONALIZATION



P.L. 86-36

The prospect of a postprofessionalization program seems to loom in the future. A viable alternative would be to create a "continuing" system that included all people within a given career field. It would mean starting anew and rethinking the scope, purpose, and objectives of the present system. Since most of us now have a stake in the present system we might tend to deem any new system as threatening. Thus, any changes to the present professionalization program will undoubtedly be gradual and incremental with little likelihood of any radical departure from what exists now. A revolution in professionalization cannot occur, however, unless someone makes the leap to begin the struggle for change. The following is my rationale for a "continuing" system.

All current professionalization programs at NSA have varying types of requirements with assigned point values given to them. Secondly, all have a target point at which that final hurdle is completed and professionalization is yours. Following professionalization, your records are returned to you and you become a statistic. There are few pressures on you either to maintain or to improve yourself within your career field from self-motivation and a certain amount of organizational peer pressure.

It is the view of this writer that all professionalization programs should have no final hurdles. The scope of these programs should be large enough so as to include all people who choose to call themselves a professional. There should be requirements within the system to make it necessary for everyone within the field to both maintain and improve their skills. The assumption here is that there is always more to learn and time to improve, no matter how much you have distinguished yourself within a particular career field. Secondly, professionalization should serve as a measure of a person's skill and worth -- at least from a technical point of view. Professionalization should guide people toward achievement and increase their motivation throughout their career. All work would then follow the path of the high achievers, if the professionalization requirements are skillfully and fairly established and maintained.

Professionalization panels should be people-oriented and serve more as the employee "union" representative vis-a-vis organizational prerogatives. Secondly, the panels should get out of all forms of testing and leave this function in the hands of the Training School. Within guidelines, panels should determine the curriculum necessary for professionalization and then help people achieve their goals. With the functional control of their profession, the panels could then provide an organization with professional help as needed and remove them when necessary. NSA would then become task-oriented. The panels should also provide the lateral input to organizations so as to ensure equal career development opportunity.

Career panels with a larger scope and purpose could ensure functional equality within a given career field and thereby largely eliminate the promotional aspect of "being in the right place at the right time." Unfortunately, it is now possible for people within the same career field to be hurt more by their timing than by their ability. A person with half the ability, half the experience, and half the whatever-is-required, can now be promoted ahead of someone in the same career field who is twice as qualified. A more powerful panel would be better able to prevent such inequity.

A "continuing" professionalization program which included all people within a particular profession would better help managers to quantify people's strengths and weaknesses. It would also enable the Agency to measure statistically the professionalization programs and its people from year to year or whenever necessary. Presently, no one can quantify the statistical worth of each profession to say whether it is improving or declining in expertise. Comparisons should be possible, to provide more effective help in recruiting and career self-monitoring. Now the process is basically subjective in respect to the quality of people within a given career field. It is time for the Agency to become more scientific in its approach to professionalization and increase the level of functional inputs which could help to increase organizational output.

In order to remove any reader's fear of what a "continuing" professionalization process would involve, a hypothetical work sheet for evaluating aspirants is presented on the next page:

DOCID: 4009815

REQUIREMENTS FOR CERTIFICATION
BY PROFESSIONALIZATION PANEL "X"

John Doe
(NAME OF ASPIRANT)

	REFERENCE LEVELS OF EXPERTISE IN "RELATED" CATEGORIES, WITH NUMBER OF POINTS REQUIRED						PANEL AWARDS IN "NON-RELATED" CATEGORIES
	1 750	2 1600	3 2400	4 3300	5 4300	6 5200	
WORK EXPERIENCE	400	800	1200	1600	2000	2400	200
TRAINING	100	200	300	400	500	600	50
EDUCATION	50	150	250	400	600	750	25
PERFORMANCE	100	200	300	400	500	600	150
DOCUMENTATION	100	250	350	500	700	850	0
TOTAL POINTS ACCUMULATED BY ASPIRANT.....			2250				+ 425 = 2675

ASPIRANT CERTIFIABLE AT LEVEL 3

Professionalization awards would be given when a person has accumulated the required number of points for the particular level of expertise. For example, in the hypothetical instance above, 2400 points would be required for professionalization at level 3. (The point values given here are, of course, arbitrary; in the real-life situation, the point values would be assigned by the Panel and would perhaps be approved by an ad-hoc "Panel Comparability Board").

A person would be able to accumulate the required number of points from various reference levels of expertise in categories related to his field of specialization, and also from points awarded for categories pertaining to work experience, etc. which is not related to his field of specialization. The Panel awards for nonrelated categories should be assigned point values and be standard for all aspirants. For example, a person working in Special Research should be given more points for a college course in international relations than for a course in mathematics. The reverse would be true for a Mathematician. Education points should be fitted to the professional discipline.

The reference levels of expertise would help supervisors and aspirants to realize the areas of needed improvement. Each person's assets are different, and each person's professional advancement takes a different route. One person may be long on experience and short on education, and another person may be just the reverse. A glance at the chart would show the supervisor and aspirant that, if the person wants to develop his capabilities to the next higher level of expertise, he should try to bring up his totals in categories with low totals. Otherwise he might prove to be "top-heavy" in one category to the detriment of his overall career development.

In the sample work sheet above, the aspirant's accumulated points indicate that he is long on work experience and should probably try to bring up his total points in the area of education and documentation. A promotion board looking at this work sheet might wonder why, with all his experience, the person has not documented his labors for other people's benefit. Since a person's reference level of expertise as his career progresses should, ideally, be as close to the "vertical" as possible, this work sheet might indicate a reordering of some career priorities. The problem may rest with the individual or the organization. For example, the organization may not have allowed the person enough time to document his work. Alternatively, the person may not write well and may be hesitant to document his work. In that case, the supervisor could suggest that the person take a technical writing course before zeroing in on his documentation task.

The advantages of a "continuing" professionalization system are:

- It is intended as a method of quantifying a person's career from the beginning to to the end;
- There are no "final hurdles" which artificially handicap a person;
- A person could be better identified according to his expertise in different career fields. For example, a person might be a level-1 Collection Operations Officer, a level-2 Special Research Analyst, and a level-3 Traffic Analyst;
- The system would provide for complete quantification of skill levels within a career field. This would aid management by increasing the efficiency in recruiting, staffing, transferring, and promoting people; and
- People would be more motivated to improve their professional skills.

The greatest disadvantage of the proposed scheme is that it makes the present professionalization system obsolete. This would be the largest of all hurdles to overcome. To this writer, however, the concept of "continuing" professionalization is vastly superior to any program of postprofessionalization.

DOCID: 4009815

P.L. 86-36

A METHOD OF MEASURING [redacted] INTELLIGENCE

[redacted] EX-W322

When the author of this article submitted it to CRYPTOLOG in April, he stated that he had deliberately omitted much of the more technical detail, such as how the probability figures are derived, but offered to answer any questions that the published article might engender. Unfortunately, that offer no longer applies, since the author resigned in late June 1978. Questions may, however, be directed to his former associates in W322, on 3764s.

[redacted]
Collection Editor

[redacted] article in the April 1978 CRYPTOLOG ("We Gotta Accentuate the Negative") pointed out the problems that exist with intelligence efforts that yield negative results. The challenge is to make the most of such results and produce negative, but useful, intelligence. This article will attempt to describe a method developed by [redacted]

[redacted]

[redacted]

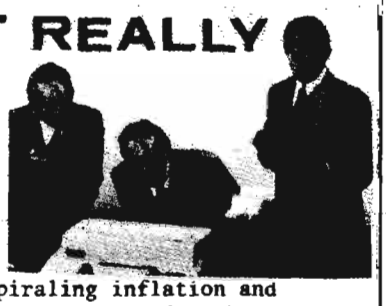
[redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~HANDLE VIA COMINT CHANNELS ONLY~~

WILL IT REALLY DO THE JOB?



T2141

In a day of spiraling inflation and spiraling computer-related technology, the staid method of selecting the best equipment may be impractical. If we select an equipment only for its ability to perform, we will more than likely ignore several other crucial criteria. If criteria such as those I have in mind are ignored, our future operations may be seriously hampered.

It was once said that he who has not learned from his past mistakes is condemned to relive them. And relive them he will, unless flexibility of technology is one prime consideration in selecting an equipment. What degree of flexibility is built into the technology of a contemplated purchase? The knowledge of built-in flexibility would certainly be a comforting thought when -- and it is is inevitable -- the accelerating spiral of technology catches up. At this time one must either put the equipment to new visionary use or plan for a new purchase.

On the other hand, what we buy we must support. Several questions should surface in this area. These questions center around the contractor's ability and willingness to furnish a constant stream of technical support for an equipment he wants to sell. So we ask, does the contractor have a maintenance team available? Can we easily identify and obtain replacement parts? Are good technical manuals available, including logic drawings and technical changes? Does the contractor give training courses on his equipment? Does he have both the ability and the willingness to develop software and drawings specifically for our needs? P.L. 86-36

It is this type of thinking that conveys to the contractor the message that the equipment he sells in June, he must support in December.

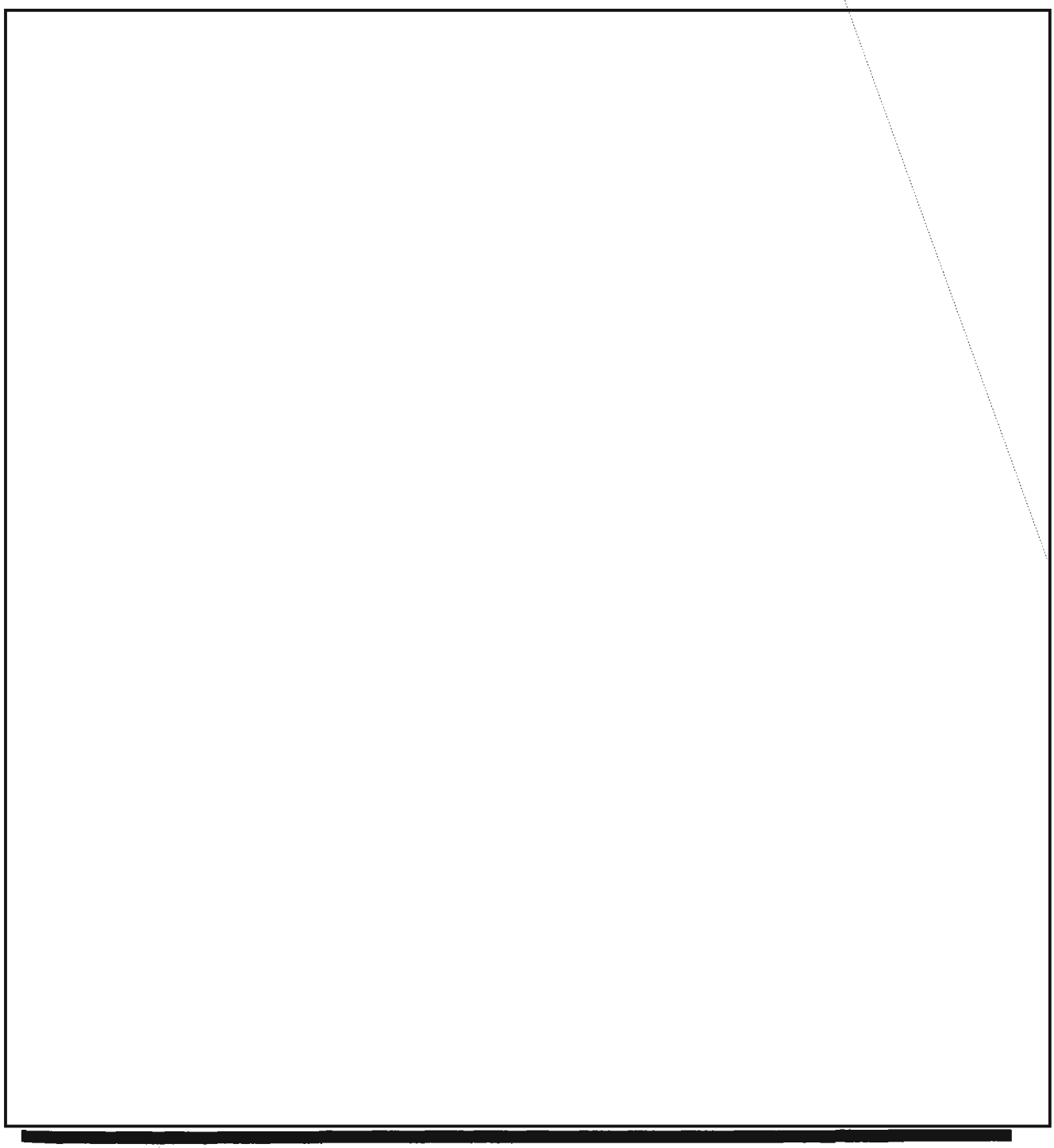
It is needless to say that all these considerations are necessary during the preliminary planning stages. Otherwise we may abruptly discover that the ideal equipment may fall far short for extended use and be doomed to a very short life cycle. (U)

DOCID: 4009815

EO 1.4.(c)
P.L. 86-36

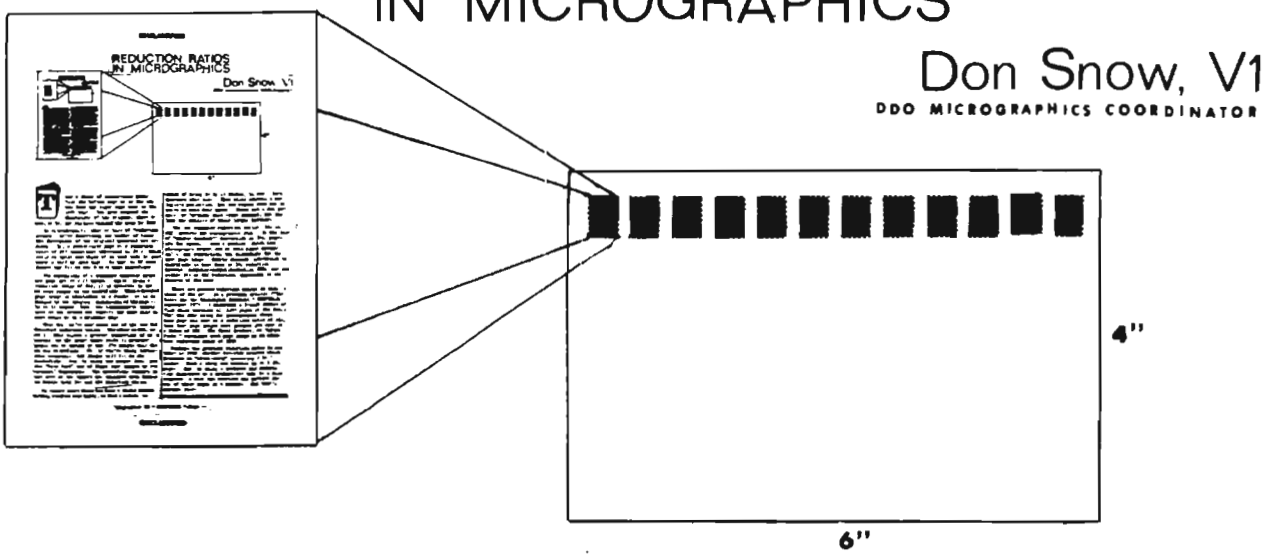
YOU CAN'T TELL THE WHEAT FROM THE CHAFF WITHOUT A PROGRAM

J. Gurin, R5



REDUCTION RATIOS IN MICROGRAPHICS

Don Snow, V1
DDO MICROGRAPHICS COORDINATOR



Take a sheet of letter-size paper. Fold the bottom edge up to the top. Now fold the right edge over to the left edge. You have reduced the *dimensions* of the original sheet by two, or 2X; but you have reduced the *area* by four.

In micrographics, when we talk of "reduction ratios," we're describing the number of times the *dimensions* of the original material are reduced. So, a letter-size page at a reduction ratio of 24X (sometimes expressed as 24:1) would yield an image one-third of an inch wide by just under a half an inch high. As many as 98 such images can fit on one 4-by-6 inch microfiche.

The dimensions of a standard computer printout page are 14 x 11 inches. Again, using a reduction ratio of 24X, it is possible to put 63 such images on one microfiche. When a desired page image is positioned in a reader, it is enlarged to the original dimensions of the page -- 14 by 11 inches; thus, the alphanumeric characters on the screen are exactly the same size as they would be on a printout page.

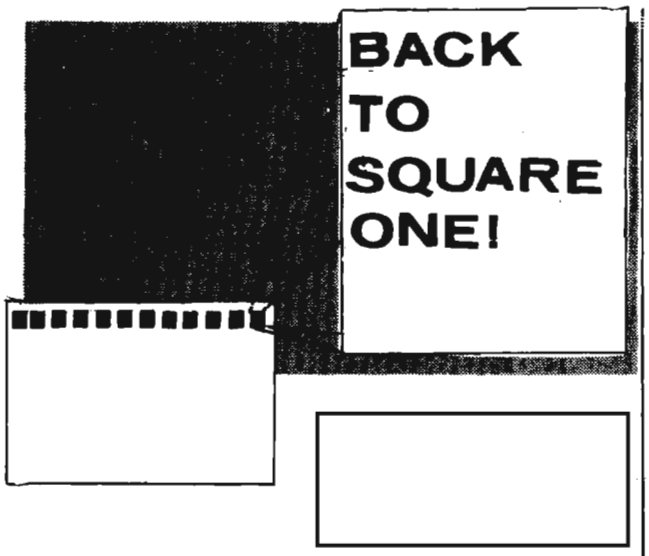
Thus far, we've mentioned one of the two DoD standard reduction ratios. The other is 48X, or 48:1. This allows a greater compaction of material, to the point where 14-by-11 printout pages can be shrunk so that 270 images will fit on one microfiche. Or, if you're using letter-size originals, 420 images will fit on one microfiche. And, by using the proper lens, you can "blow back" one of those tiny images to its original dimensions. The microfiche readers in use here at the Agency are equipped with lenses to handle both 24X and 48X reduction ratios.

In recent years there has been a trend toward making readers less bulky, so that a screen, instead of being 14 by 11 inches, is about three-quarters that size. That still affords a very legible projection, but the reader does not require as much desk space. There are a few portable, or "attaché case"-type readers, but they lack the quality of their larger brothers.

The two standard reduction ratios, 24X and 48X, involve one photographic step. In the case of "source document" conversion at 24X, pages are fed manually into a machine, which then photographs either one or both sides automatically, and repositions the microfiche for the next page image. Source document conversion to microfiche is best done at 24X reduction; however, computer-output-microfilm (COM) may use either 24X or 48X reduction, depending on the desires of the user.

There are greater reduction ratios in today's state of the art. In a previous article ("The Bible and the Washington Monument," CRYPTOLOG, September 1976), I described a 2-inch square of film which contains all 1245 pages of the Bible. That was done using *two* photographic steps: each page was shot at a reduction ratio of 15X; then four page images were grouped and shot at a ratio of 10X. The final product, or "ultrafiche," contained each page image at an effective reduction ratio of 150X.

Perhaps the greatest reduction ratio in use today is 210X, another two-step process which produces an "ultra-strip" measuring 1 by 7 inches. Such a strip can contain up to 2,000 pages! And, by using a keyboard and information displayed on a cathode-ray tube by a minicomputer, a user can retrieve and project any one of those pages in 4 seconds. But that's another story!



The trend toward microforms in all categories of publications seems to be facing a setback. The publishers of the *American Journal of Computational Linguistics*, which has been sponsored since 1974 by the Association for Computational Linguistics in a 20X microfiche format, have recently polled the membership about format preferences. Although previous membership samples have indicated support for the compact format, this latest request for direction from the membership is couched as an appeal for a change to a more traditional format such as used by the *Communications of the ACM* and the various *IEEE Transactions*. The reason? To increase the readership and consequently the rate of submission of technical articles. Production costs would approximate those currently sustained, and it would even be possible to produce the microfiche too for very little more.

P.L. 86-36

Whatever the eventual outcome for *AJCL*, the apparent low readership seems to be attributable to the alien format. Much as I have supported the use of microforms for active files and other uses, I must confess my own response to *AJCL* microfiches has been lukewarm. Although I like being able to keep a complete set of copies in a 4x6" card file, I just can't curl up in an easy chair with a microfiche reader for an evening of professional enlightenment. Is there a solution that the human factors engineers have missed?

(U)

OVERHEARD WHILE STANDING IN THE BURN-BAG LINE

On two days in a row [redacted] submitted to the editor a quote that had been "overheard while standing in the burn-bag line." If that isn't enough reason for initiating a new CRYPTOLOG department, I don't know what is!

The quotes are:

"If they *really* want that many linguists around here, why doesn't the Director hold his staff meetings in Russian?"

"Working all day long on that scope isn't as bad as I thought. I keep a book nearby and whenever the system goes down, there isn't anything to do, so I read. It's all very uplifting. I'm going to read *War and Peace*. The guy beside me is studying law. . ."

Have you overheard anything interesting while standing in the burn-bag line? If so, send it along to this department. Sign your name or keep it anonymous -- it's up to you.

(Hint to would-be authors: Keeping an ear open while you're standing in the line yourself, or keeping an eye open while reading this department might give you an idea for a CRYPTOLOG article -- such as "Is Down-Time Excessive?")

P.L. 86-36

(U)

DOCID: 4009815

FEEDING THE GERMANS MISINFORMATION

P. W. FILBY

Review of: *Beyond Top Secret Ultra*, by Ewen Montagu. Coward, McCann & Geoghegan, 192 pp., $7.95.

Sir John Masterman in his *The Double Cross System in the War of 1939 to 1945*, published in 1972, told how German spies were captured and then used to feed false information to the Germans. At that time the existence of the cipher systems classified Ultra, which were broken by the British at Bletchley, were still under wraps, and Sir John had to use only information which came from other sources. Now Ewen Montagu, a distinguished judge, has produced the complement to Sir John's book in his recollection of double-cross and the manner in which, through Ultra, success or failure could be judged. Some who worked at Bletchley deplore the publication of Winterbotham's *The Ultra Secret**, but readers will be enchanted by Ewen Montagu's book because he is able to use all the secret intelligence gained through Ultra.

Many readers will remember the startling story written by Montagu called *The Man Who Never Was*, about floating a body bearing war plans into Spain (Operation Mincemeat). At the time Montagu could not tell his public that the fact that the Germans bit the whole deception was ascertained from Ultra messages. Now he treats his readers to a tour-de-force on the way the Germans were fed with much misinformation through German spies who were "turned round." He names agents and tells how, when caught, they accepted the role of double agent and played supremely well and fairly on the Allies' behalf. Moreover, through Ultra the British could check on the manner in which the Germans accepted the information and whether an agent had been "blown." Montagu recounts several astonishing and exciting stories of narrow escapes and surprisingly records that in spite of the steps needed to get false information to the Germans the stories were accepted without much question, and one or two star agents were awarded the Iron Cross! Perhaps the most astonishing statement is that throughout the war every agent was caught within a few days of arrival, probably because of England's being a "tight little island."

Ewen Montagu had been called to the bar in 1924. When war broke out he joined the Navy and was assigned to low-level intelligence, but such was his brilliance that he soon became one of the handlers of much of the highest-level intelligence of the war. He tells without bitterness how his meteoric rise was not matched with corresponding promotion, and he remained a Lieutenant Commander for the whole of the war. (Being missed out for promotion was the fate of many cryptanalysts also!) With his wife in the United States he was still forbidden to stay one day over the week demanded by his discussions with his American opposite numbers in Washington.

Readers might also like to picture security in those days. Montagu had to travel between departments with top secret papers and he reports that this put him in a dilemma. He writes, "This problem I solved by fixing a large metal basket-type carrier to the front of the cycle. To this I chained the brief-case when it was parked. There was some doubt about the security of the operation for such 'hot' documents, but I managed to get permission to adopt it as long as I always wore a shoulder-holster and automatic pistol."

Montagu became one of the very few to be let in on Ultra; he attended the famous XX Committee, which met weekly to decide on deceptions to be tried, and therefore needed the information. He had two roles: supplier of information to the Services and producer of "chicken feed" or misinformation to the enemy. He tells story after story, all with undoubted authenticity. Because of Operation Mincemeat Hitler kept forces in the wrong place for over a year while Italy was being invaded, still believing that the main thrust would be on the west coast of Greece and Sardinia. When the invasion of Normandy was imminent the Germans had to defend the Pas de Calais long after the Allies had a firm hold in France, simply because Montagu's team had reported a great build-up in the Dover area. He had trouble when there was a moral issue. Should he report to the Germans that the U-boat commanders, the German Navy's heroes, were traitors? No. But when flying bombs fell in London, should he get the Germans to believe they were overshooting? Yes, because fewer lives would be lost to bombs falling short of densely populated London.

One might wonder how the Germans were tricked so often. Well, not all the information was wrong. Quite often the Allies released perfectly valid information -- just a little too late for any great value to be gained, but the Germans could prove the information correct and the agent therefore reliable.

In this book Ewen Montagu has produced the most exciting of all the Ultra revelations to appear so far.

During World War II the author was an officer in Military Intelligence at Bletchley.

*See CRYPTOLOG, December 1975: "Winterbotham's 'The Ultra Secret' -- Three Views": "A Personal Comment," by Brigadier John H. Tiltman; "Ultra Was Secret Weapon That Helped Defeat Nazis," by P. W. Filby; and "Mum's *Still* the Word!", by Paul R. Hutchinson.

[redacted] said,

P.L. 86-36

[redacted] adds,

...AND-A YOU BETTA HAVE MOTI-VAYSH!

OK., CRYPTOLOG, you finally got my attention! At the risk of falling for a belated cryptologic April Fool's gag, I really have to comment on [redacted] article "Uncle-a Sam Wantsa You!" (CRYPTOLOG, May 1978).

At the end of his article [redacted] offers the opinion that, when recruiting linguists, high ambition in the applicant should be viewed as a criterion for *non*selection. He goes on to state that the problem with highly motivated people is that they expect (and emotionally require) high productivity to be rewarded, and government service is not set up to give rewards for productivity. [redacted] then offers us a formula for recruiting linguists: "If the object is to recruit career linguists, no more than a moderate amount of ambition or motivation should be allowed in a recruit."

Assuming [redacted] is really serious (and I applaud his motivation in undertaking this ambitious article) I strongly differ with his viewpoint. From time to time in the past we've been through this "hire the poor and keep 'em without shoes" syndrome at NSA. The problem is that people's aspirations change as they mature and after they have satisfied their basic needs (get a job and eat regularly). Inevitably some percent of the supposedly unmotivated work force begins to show "dangerous" inclinations toward greater responsibility, take new and nonstandard approaches to their jobs, and (horrors!) begin sinfully lusting after positions where they can influence how and why things are done, rather than to gratefully accept their designated place in the "system." When you think about it, Thomas Edison turned out to have been a pretty poor selection when he was hired as a newsboy. True, he eventually revolutionized communications rather than just delivering them, but you can bet that the guys down at the newspaper's recruiting department didn't see it that way, and redoubled their efforts to find a replacement who would be satisfied with just delivering the damn newspapers.

Let's face it, our future key people will not have been hired in response to a want-ad for "Key People Wanted," but will come from among us, perhaps even to include a maverick linguist or two (to the eternal anguish of those who recruited them as linguists). With a little luck they'll have the moxie to solve the "linguist problem" that has eluded the rest of us for so long.

I also question the validity of [redacted] contention that" government service is not set up to give rewards for productivity." In my view that depends on one's perception of "rewards," and in addition to the bucks involved in rewarding people (important), there are other intangibles which weigh heavily in job satisfaction and the resulting work force stability.

Since I'm apparently the only person in the cryptologic community not previously embroiled in the "linguist issue," here's my two cents' worth:

- Hire the most motivated, most ambitious linguists you can find.
- Tell them *up front* about the problems of day-to-day language work and the riptide of opinion that prevails on how to acquire and keep a linguistic work force.
- Challenge them to solve our problems.
- Listen to what they say after they have some experience.
- Enrich their jobs, encouraging them to stay in the field. Pay them fairly.
- Disregard all they say upon entry about being satisfied doing the exact job they're hired to do.

My theory is that, at recruitment interviews, people tend to tell us what they think we want to hear.

Interviewer: "And do you think you'll like the work?"

Applicant: "Actually, ever since I was a small child I've had an insatiable desire to sit at a desk and translate all day. When all my friends were out playing, I used to translate the labels off of olive-oil cans."

Virtually all will profess a love of doing the job we have in mind for them, vowing no

DOCID: 4009815

aspirations for other things. Once hired, however, a bunch of them will begin their private guerrilla campaign for the Directorate, and, for them, their entry job is only a first step. Great!

To hire unambitious workers as a matter of policy, as [redacted] suggests, is to give validity to the claim that we have in fact become a true old-line bureaucracy and are proud of it.

Our goal has got to be to make our linguists' work more interesting, rewarding, and challenging, and to make an NSA linguistic career a desirable profession rather than a feudal system where the linguist vassals gratefully accept their piecework assignments.

From the symptoms evident to me (a non-linguist), it seems that we have not managed our language people (among others) and their tasks in a way that works both for linguists and management. The danger is that we will default to a mode of the self-fulfilling prophecy, where we hire unambitious people who will then indeed rise to the challenge and become and remain truly mediocre.

P.L. 86-36

P.S. Since writing the above, I have had second thoughts about a work force composed of unmotivated, unambitious people. I have been able to locate several linguists who seem to meet [redacted] standards for low motivation and lack of ambition and would make ideal experimental subjects to test his thesis. Unfortunately, I have been unable to get them to take the initiative and get their applications in for consideration. (U)

News of the Communications Analysis Association

By W.E.S.

If you have ever recovered a frequency rota, or broken an authenticator system, or figured out how an address table works, then you have been *doing* Crypto-TA, whether you realized it or not.

Most analysts need to understand enough about this subject so they can (1) solve their own simple problems as they come across them, and (2) recognize when they need "specialist" help. And there are a few people around who have the interest and ability to get deeper into the "specialist" aspects of the subject. If either of these descriptions seems to fit you, then you ought to get in touch with the CTASIG (Crypto-TA Special Interest Group) and find out what they can do for you. Among the people you might contact are: [redacted], and Fred Mason.

~~(C)~~

A follow-up discussion on the subject "Interstellar SIGINT" was conducted on 14 August 1978 for some 20 CAA members. [redacted] Chief, W16, gave a short recap of the presentation he had given in the NSA Auditorium on 28 June 1978 and then entertained questions. The session lasted about one hour -- members present came prepared with very interesting questions. A transcript of the 28 June talk is now being edited for publication in a future issue of CRYPTOLOG.

(U)

Meet our Program Chairman!

[redacted] has been in the cryptologic business since 1947. After 5 years with the Naval Security element in Washington, D. C. as a Communications Technician, he converted to civilian status in February 1952 and went to work at Arlington Hall Station. Hired as a *Communications Clerk, he performed traffic* analysis on [redacted] (printer and Morse) and served as a section reporter through November 1956. He joined the Office of Training as a TA Instructor for a two-year tour and stayed 13 years. After teaching Basic Radio Communications and Traffic Analysis for some 4 years, he then developed and taught Traffic Analysis, Technical Reporting, and SIGINT Reporting courses. He served as the Training advisor to the TA Career Panel when it was first formed and was selected to serve as the NSA Pacific Staff Training Representative. Prior to his departure for the overseas assignment in the summer of 1967, he served as the Executive for an ad-hoc group charged with determining whether or not Education and Training should be considered a career field with criteria for professionalization established. Earl was instrumental in establishing that set of criteria before leaving for the NSAPAC job. After 2 years in Japan with many trips throughout the Far East, he returned to the NCS (National Cryptologic School) Staff at Fort Meade and was assigned to investigate the possibility of setting up a training course for troopers on their way to Korea, similar to the TA operational training given to troops on their way to Vietnam.

He then assumed the responsiblity as Chief of the TA Training Department of NCS for approximately one year before accepting the appointment as Executive to the TA Career Panel in May 1970. His term expired in May 1973 but was extended for one year. In May 1974 he transferred to R221, "HF Systems Architecture" Project Management. In July 1976 he was appointed TA Executive again and currently serves in that capacity. ~~(S - CCO)~~

EO 1.4.(c)
P.L. 86-36

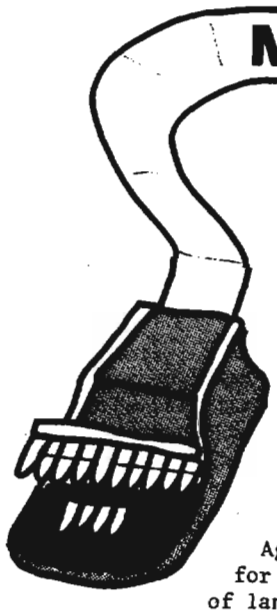
P.L. 86-36

DOCID: 4009815

P.L. 86-36

MORE B.S. (Before SPELLMAN)

[redacted] G03



Another "remembrance of projects past," prompted by Jack Gurin's "Never Again!" (CRYPTOLOG, June 1978) and A. Salemme's follow-up to it, "I Remember SPELLMAN" (CRYPTOLOG, July-August 1978).

Once upon a time (1956) a tender soul (me) was employed by the Agency, which was looking for someone with knowledge of languages, area studies, and intelligence background other than COMINT. And so I became a minion in the TNG (Training) fiefdom of the late lamented Shelby P., where books on desks had to be aligned by size (and not by content) from left to right, where suit coats had to be worn anytime you left your desk for a trip to the you-know-what, and where everything, including thoughts, was hierarchically structured.

But times were changing and even Camelot looked outwards. And one day someone decided that the Agency should look into "management theory." So, soon TNG hired a couple of fellows who would dream up management courses. Their room was next to mine, in fact their entrance was through my office, so I overheard many of the surmisings that eventually found their way into the first trial and proto-seminars -- we, next door, laughed at the absurdity of most of their notions, but of course such endeavors have long since been anointed as the Holy Grail and are believed in by people who look askance at ESP, flying saucers, and all of Serendip. About that time the concept of "brainstorming" was trying out its wings in the world, and of course the management people picked up on that gimmick.

Thus is came to pass in the TNG fiefdom that the Grand Vizier (about that same time Lambros Callimahos took upon himself the title of Guru) promulgated an edict to the effect that on Friday mornings assembled his minions would brainstorm in his presence. His minion of the Irish persuasion soon asked for support from his own subminions, so, mightily did [redacted] myself, and others come up with seed ideas and other things for brainstorming input.

One of these ideas for the brainstorming sessions had to do with -- would you believe? -- stenotypy and possible ways of having transcription done by people with less than the five years' experience with spoken Russian that is required to do professional-level transcription. Whether that idea was ever thrown into the Friday brainstorming hopper or not, I do not know. But herewith is the exegesis of that particular ploy.

In 1949-1950 I had been an English-language teacher at the Lycée Henri IV in Paris. One of my students there was also studying stenotypy at the Grandjean (?Grand Jean) Institute, or was it the Grandjean system? I don't recall. Anyway, that student and a couple of other stenotypy students asked me to help them -- they needed American speech they could practice their stenotypy on. I obliged. One of the students was French-born but the child of Polish refugees. She knew French, Polish, some German, and was perfecting her English. Students of the Grandjean system in Paris were of very diverse backgrounds, coming from all over Europe and from the various French colonies. Therefore, by design, the Grandjean system as taught there was deeply influenced by phonological theory. My little Polish student found it easy to use her stenotype machine to record Polish and English as well as French.

But back to Camelot! During my early years with NSA I lived at Hartnett Hall, where we had a TV room. At 6 p.m. every night two of the Hartnett Hall residents, one of whom was taking stenotypy at some local school, would take their seats, stenotype machines in hand, and practice transcribing the news broadcasts. One night there was possibly up to a minute's worth of foreign language on the news (probably De Gaulle), and I noted that one of the stenotypists continued to stenotype without a break. After the news broadcast was over, I remarked to him that I didn't know that he knew French and his reply was that he didn't -- he was just practicing the sounds he heard. He ran through his roll of tape until he found the proper spot and then pronounced what he had on paper. I could understand it, but he couldn't. It was sort of like the old gimmick of asking a French speaker to read aloud the nonsense phrase "pas de leur Rhône que nous!" in front

P.L. 86-36

of nonspeakers of French, and have the latter burst forth in laughter while the French speaker is totally nonplussed, since the phrase makes no sense -- after all, he is filtering the words and sounds through the French phonemic pattern and doesn't realize that his audience is filtering the sounds through the English phonemic pattern and is hearing "Paddle your own canoe!" Q.E.D., I had learned that it is possible for a person to transcribe a little bit of a foreign language he doesn't even know (Note: This was a highly trained stenotypist who was already working for the D. C. court system).

As a person with a degree in Chinese from Harvard and a Master's in French from Middlebury, plus experience as an announcer in Spanish and Portuguese on WLW short wave in Cincinnati, and an immediate background as an interrogator in German for the USAREUR Intelligence Center, I should have known that my first major assignment at the Agency would be the teaching of Polish. That meant that we hired the Georgetown University Polish instructor as a contract employee of the Sanz School of Languages to get my feet wet and bring me up to speed to take courses from him at Georgetown. The environment at the Georgetown School of Languages and Linguistics, plus the heady atmosphere of the PATA (Promotion and Training Agreement) Program in TNG, in which the students were introduced to the concepts of linguistics (using the Gleason textbook), soon got me into formal linguistics.

And thus the stage was set. Then came brainstorming.

The concept as I came up with it was as follows. Some high-school students would take typing and steno*graphy*. It should be possible to select some people from that population who have an aptitude for language and teach them steno*typy* and drill them in the sounds of phonology (as taught in beginning college courses in Phonetics and Phonemics, using the texts of the Summer Institute of Linguistics or other such materials). Afterwards they would be taught the sounds of Russian.

The second step would be to take a number of open-minded Russian linguists and teach *them* stenotypy. The purpose was not to turn the Russian linguists into stenotypists, but to enable them to read the stenotype tapes made by the non-Russian-speaking clerical specialists. Back in 1956 we had a Russian-language manpower shortage (we still have one, except that now it probably ought to be called a "personpower shortage") -- remember that it takes a degree in Russian and then up to 5 years' experience to become a truly professional transcriber -- but the stenotypy concept could possibly train people in 6 months or so to put onto stenotype tape information which a skilled linguist could scan for relevance and importance. Then the decision could be made to turn the tape over to a transcriber. In other words, my concept was that this was a method of making it possible to scan a far larger volume of material by eye than can be done on a 1 : 1 basis by ear.

The key and salient points of this two-step concept were:

- the careful selection of highly motivated *clerical people* and the training of them first in stenotypy and general phonology, and then specifically in the phonology of Russian; and
- the providing of hand-in-hand training in stenotypy to some *senior Russian linguists* for scanning purposes.

Never did I say that G.I.'s selected in the military manner to learn Russian at a 6-month course in Monterey should simultaneously be taught stenotypy and become stenotypy transcribers; nor that a Cyrillic keyboard would be needed; nor that this could be an input into machine translation. So you can imagine my surprise one day in 1960 when I learned what was being asked of [redacted] I stated to her then and there that it sounded like my original concept of a few years earlier, but one which had been brainstormed and confounded until there was no possible way it could succeed.

If "they" do want to try again with the stenotypy concept some day, I'd like to implore "them" to please-oh-please do it right! This means the proper selection of two types of individuals; the proper in-depth linguistic training of the stenotypists; and matched, paired stenotypy training of the clerical people and of the scanner linguists. And also, have at least one of the monitors and developers of the program be a scientific linguist with the requisite knowledge of the possible pitfalls and difficulties. I am still convinced that a proper trial could well have positive results.

~~(C)~~

ANSWER TO "WHO & WHOM?"

(PAGE 4)

1.	Phineas T. BARNUM	&	James A. BAILEY
2.	Nathaniel CURRIER	&	James M. IVES
3.	Robert C. DUN	&	John M. BRADSTREET
4.	Isaac K. FUNK	&	Adam W. WAGNALLS
5.	William S. GILBERT	&	Arthur S. SULLIVAN
6.	Merriwether LEWIS	&	William CLARK
7.	Charles MASON	&	*Jeremiah DIXON
8.	Richard W. SEARS	&	Alva C. ROEBUCK
9.	Richard L. SIMON	&	*Max L. SCHUSTER
10.	Robert A. TAFT	&	Fred A. HARTLEY, Jr.

* The only two names in the right row.

And Harry says, "If you don't believe me, you can look it up in your Isaac K. & Adam W.!"

(U)

DOCID: 4009815

EO 1.4.(c)
P.L. 86-36

Letters to the Editor

P.L. 86-36

To the Editor, CRYPTOLOG:

[redacted] article in the July-August CRYPTOLOG ("Ye Gads! *Another* Country Trigraph System!") ends by asking if there isn't someone who can solve the problem he brings up -- proliferation of country trigraphs. I suspect that he is already aware that such a group already exists -- the NSA Data Standards Center (P13D). What he may not be aware of is that our group has no teeth, so we cannot force anyone to follow our lead.

The data standards problem that Jack brings out is actually only one of the many that plague this agency, as well as the whole U.S. government. As things stand now, we are not really in a position to know of many such problems until they are full-blown. Even the Senior Data Representatives, who are supposed to see all jobs before they are processed, too often find that they have been bypassed. Data files and data bases are designed and established long before we are brought into the picture and any attempts we make to correct errors are either ignored or circumvented. We have no power to make them change and they know that.

As the NDSC was first conceived it was supposed to have the capability for monitoring and investigating jobs to see if they varied from the norm. The NDSC would also have had the authority to take appropriate action if the initiator failed to conform to standards. For example, we would have been able to order the processing to be discontinued, or we could have denied access to computer systems to those programmers who were habitual offenders.

Yes, Jack, there *is* a standards center, but until we are authorized to deny computer use to those who refuse to accept Agency standards we can have little effect.

Mark T. Pattie, Jr.
Chief, NSA Data Standards Center

~~(FOUO)~~

To the Editor, CRYPTOLOG:

Dave Williams' NSA-Crostic No. 16 in the July-August 1978 CRYPTOLOG reminded me of the question I meant to ask when I read [redacted] Letter to the Editor in the July 1977 CRYPTOLOG, from which the puzzle quotation was taken. The quotation included the observation [redacted] I wondered then and still would like to know about the frequency in [redacted] of references to male traffic analysts. Perhaps some scholar has made a study?

Vera Filby, E41

(U)

To the Editor, CRYPTOLOG:

After several long hours of struggling to complete the July-August NSA-Crostic, distributed across many lunch periods, I was somewhat disappointed when I finally read the text that I had recovered.

Innocent as it may have seemed to Mr. Williams, I found it to be in extremely poor taste to perpetuate through this puzzle a bit of humor regarding female Traffic Analysts.

Although I now work as a Computer Systems Analyst, I have also worked as a Traffic Analyst and still consider myself to be a member of that profession. The quotation in the crostic is the type of statement that promotes basic prejudices that still exist in the Agency because they exist in our society.

I will laugh at jokes about female Traffic Analysts only when the opportunities for professional women are the same as they are for men, and when the rate of women promoted is equal to that of men promoted, and when the number of women in management positions is proportionate to the number of men in management positions.

Furthermore, until that time, the CRYPTOLOG will be doing an injustice to its professional quality by publishing such backhanded affronts to female employees.

[redacted] T323

(U)

ANSWERS TO **KNOW YOUR GEOGRAPHY** *(p. 6)*

1. *Libya*
2. *Cuba*
3. *Somalia*
4. *Venezuela*
5. *Austria*
6. *United Kingdom*
7. *Norway*
8. *Jordan*
9. *Thailand*
10. *Panama*
11. *Spain*

(U)

Solution to NSA-Crostic No. 17

By A.J.S. (CRYPTOLOG, September 1978)

[redacted] "[The] NSA Intern Program," *NSA Cryptologic Spectrum*, Fall 1977, Vol. 7, No. 4.

"The intern program was begun to provide an accelerated system through which new college graduates and in some instances experienced employees were trained to meet professional-level manning requirements."

(U)

P.L. 86-36

DOCID: 4009815

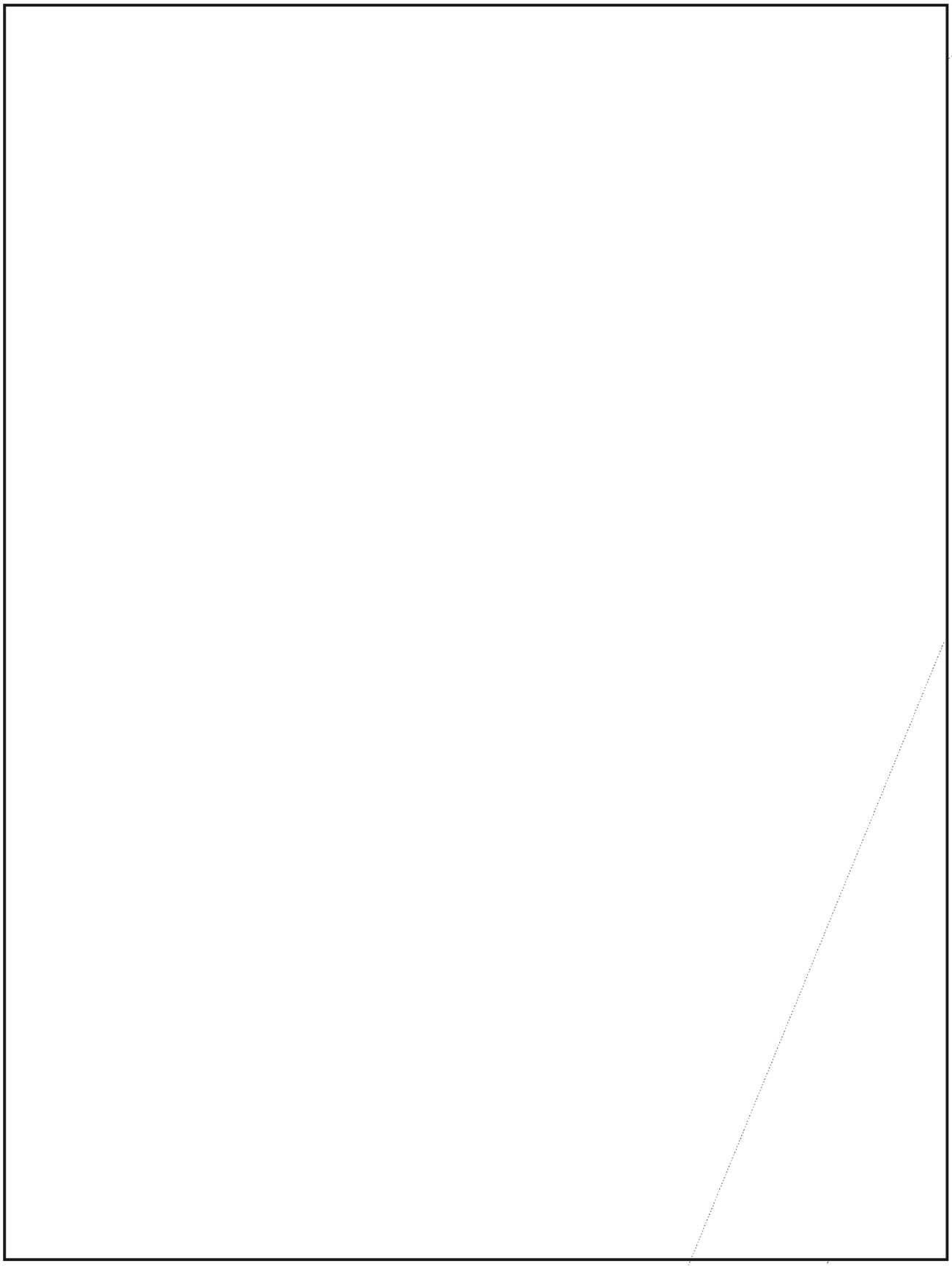
NSA-crostic No. 18

By guest NSA-crostician
David H. Williams, P16

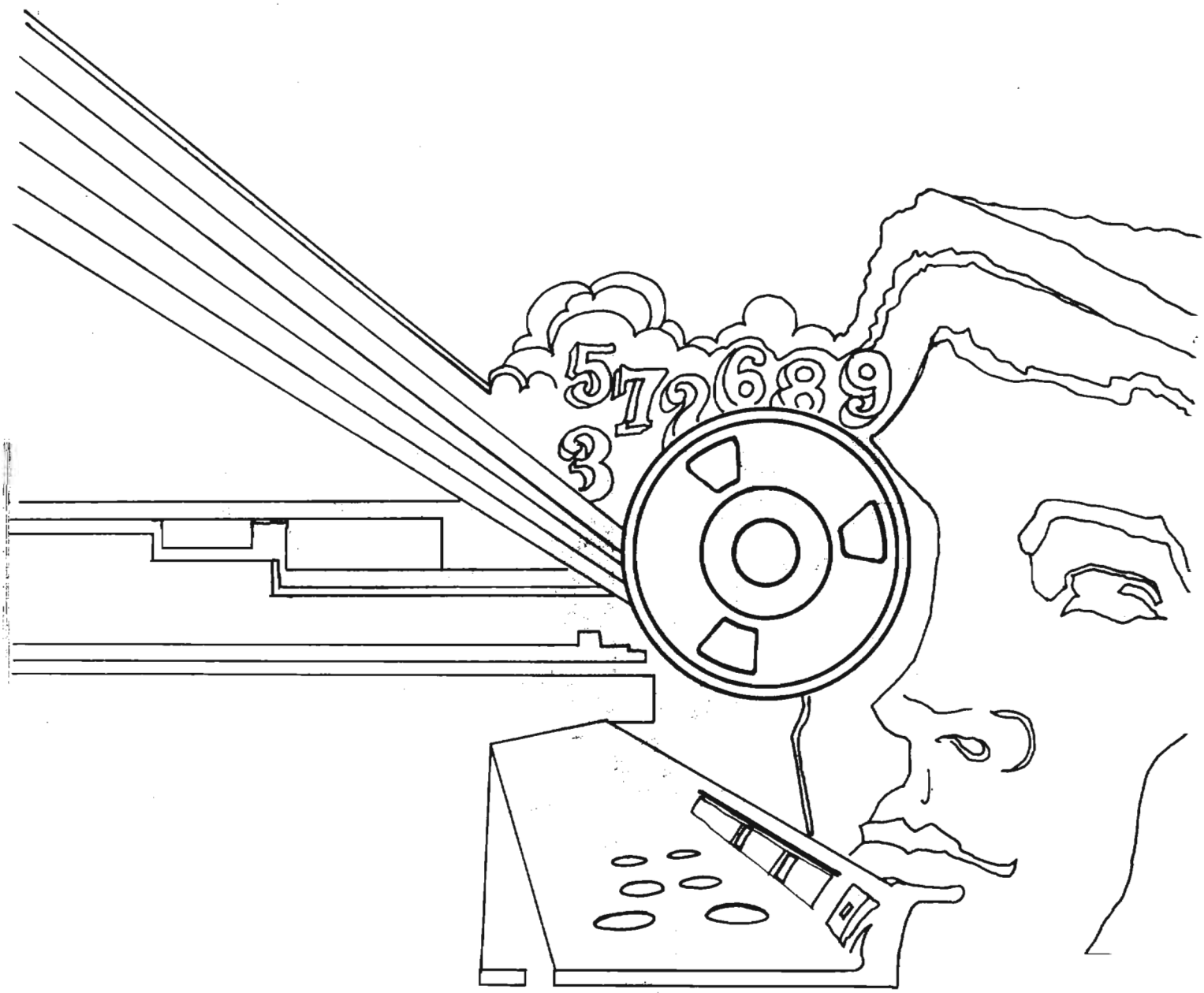
The quotation on the next page was taken from the published work of an NSAer. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS

WORDS



P.L. 86-36


5726893

DOCID: 4019726

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

EO 1.4.(c)
P.L. 86-36

SEPTEMBER 1978

P.L. 86-36

[redacted] ..... [redacted] 1
LETTERS TO THE EDITOR ..... D. Barrer, D. Williams .. 3
[redacted] ..... [redacted] 4
NEWS OF THE CRYPTO-LINGUISTIC ASSOCIATION 8
[redacted] ..... [redacted] 9
A MATTER OF STYLE ..... [redacted] 10
NEWS OF THE COMMUNICATIONS ANALYSIS ASSOCIATION 11
SOVIET COMINT AND THE CIVIL WAR ..... [redacted] 12
WHAT'S IN A NON-NAME? ..... [redacted] 16
LETTERS TO THE EDITOR ..... D. Buckley, M. Pattie .. 17
HUMAN RESOURCE DEVELOPMENT PANEL 19
NSA-CROSTIC NO. 17 ..... A.J.S 20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019726

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. V, NO. 9 SEPTEMBER 1978

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5236s)

Collection.....[redacted] (8955s) P.L. 86-36

Cryptanalysis.....[redacted] (4902s)

Cryptolinguistics.....[redacted] (5981s)

Language.....[redacted] (8161s)

Machine Support.....[redacted] (5303s)

Mathematics.....[redacted] (8518s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....[redacted] (3573s)

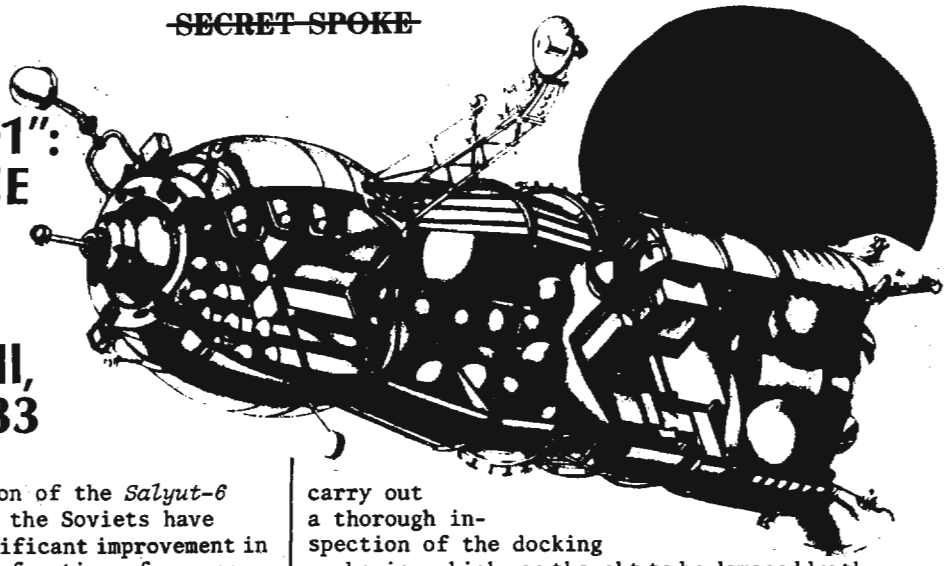
Production Manager.....Harry Goff (5236s)

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4019726

"PROGRESS-1": SOVIET SPACE STATION REFUELING

John Cahill, A433



With the creation of the *Salyut-6* space station, the Soviets have achieved a significant improvement in the design and function of a space vehicle's propulsion system. There are two types of engines on the *Salyut* station: huge, powerful thrusters for raising the station to a higher orbit and for making orbital corrections; and smaller engines for station orientation on the earth or sun. On all previous stations (and on all *Soyuz* spacecraft) the power for each of these engine types was different. The large thrusters worked on a dual-component fuel and had their own separate tanks for fuel and oxidizer. The small thrusters, on the other hand, used a single-component fuel and likewise had their own separate storage tanks.

The *Salyut-6* station, however, has a single dual-component fuel for both its large and small thrusters and fuel tanks for these engines. This new consolidated propulsion system, which can now be refueled by a "tanker" spacecraft, and thus the *Salyut* space station can remain in orbit for longer and longer periods of time. Soviet cosmonauts have

with the successful refueling of *Salyut-6*, the has become a reality and ensures continuous manning by Soviet cosmonauts.

The *Soyuz-26* crew, Commander Lieutenant Colonel Yurij Romanenko and Flight Engineer Georgij Grechko, had successfully docked at the aft end of the orbiting *Salyut-6* space station on 11 December 1977. After transfer into the station, the cosmonauts checked out and activated the onboard equipment. Several days later, Flight Engineer Grechko exited the station through the transfer hatch at the forward end of the station, in a special space suit, to carry out a thorough inspection of the docking mechanism which was thought to be damaged by the *Soyuz-25* crew. *Soyuz-25* cosmonauts, Commander Lieutenant Colonel Vladimir Kovalenok and Flight Engineer Valerij Ryumin, had maneuvering difficulties during the approach and docking phase of their flight and on 10 October 1977 had to abort their mission after three unsuccessful attempts for a "hard dock" onto the station. The *Soyuz-26* cosmonauts had docked their spacecraft at the station's second or aft docking port -- a totally new concept in Soviet space station design. All previous stations had only one docking port at the forward end of the station.

After about 30 days on board the station, the *Soyuz-26* crew was visited by the crew of *Soyuz-27* under the command of Lieutenant Colonel Vladimir Dzhanibekov and Flight Engineer Oleg Makarov. The *Soyuz-27* spacecraft successfully docked at the forward docking port (which, it turned out, had not been damaged by the *Soyuz-25* crew's abortive docking attempts), and now, for the first time, a *Salyut* space station had spacecraft docked at both ends and was manned simultaneously by two separate crews. After five days together, the *Soyuz-27* crew departed the station and returned to earth, not in their own *Soyuz-27* spacecraft but in the *Soyuz-26* craft. This was yet another "first" for Soviet cosmonautics.

The now vacant aft docking port was soon occupied by a modified *Soyuz*-type spacecraft called *Progress-1*. This new vehicle brought needed supplies for the station's crew and also tanks loaded with fuel and oxidizer to replenish the *Salyut*'s own fuel tanks.

E.O 1.4.(c)
P.L. 86-36

The spacecraft can carry up to 1,300 kilograms

This article represents, for the most part, a compilation of information from open-source Soviet space literature. The overall classification of the article, however, is SECRET SPOKE

J.C.

DOCID: 4019726

P.L. 86-36
EO 1.4.(c)

of dry cargo (including water in containers) and up to one ton of fuel components and compressed gas. Its net load is around 33 percent of the gross weight of the spacecraft.

There are three compartments in *Progress-1*: a cargo compartment, a compartment housing the station-refueling tanks, and an instrument-assembly compartment. The cargo compartment is [redacted] of a *Soyuz* and is 6.6 cubic meters in size. Special racks were created to house the various "cargo" needed for resupplying the station's crew. Cargo includes sets of clothing, film cassettes, magnetic tapes, new medical and scientific-research instruments, and such large and heavy items as new air regenerators. The compartment itself is pressurized with a usual atmospheric pressure of 760 mm of mercury and a temperature of 3° to +30° C. On the outside of this compartment are the main fuel lines which are fed into the docking assembly. These fuel lines are similar to those on *Soyuz* spacecraft, but they have, in addition, two hermetically sealed connectors which enable the pumping over of fuel from the refueling tanks in the "tanker" spacecraft's "refueling" compartment after docking with the station.

[redacted] this compartment does not need life-support systems, powerful radiation and heat shielding, or a parachute system (since no part of the *Progress-1* was to be returned to the earth).

The final compartment -- the instrument-assembly compartment -- has three sections: a nonpressurized section where part of the mooring and orientation engine system and the fuel tanks for this system are located; a pressurized instrument section; and an assemblies section with the approach and correction propulsion system found on all *Soyuz*-type spacecraft.

The *Progress-1* cargo spacecraft is launched by the same boosters used to launch all *Soyuz* spacecraft. After orbital insertion, radar antennas of the approach and docking system (installed on the cargo and instrument-assembly compartments) are deployed. The Flight Control Center monitors the spacecraft's orientation via two television cameras installed on the outer hull of the cargo compartment. One of the cameras shows the space station during the approach maneuver, so that the ground can follow the approach and docking procedures if necessary. The *Salyut* station's crew can view the approaching cargo spacecraft via the station's stern-mounted television camera. Special lights on *Progress-1* aid the crew in determining the spacecraft's position relative to the station on both the day and night side of the planet. These lights are uniquely arranged on retractable rods mounted on the outside of the "cargo compartment." One light is in front, with two lights behind it on the sides. When the approach and docking is going normally, the lights appear to be in a straight line. If there are any contingencies during this procedure, the crew can stop the docking process.

Progress-1 successfully docked with the station on 22 January 1978, but the actual fuel transfer did not occur until 2 February.

Within the docking mechanism of the *Progress* vehicle (as in all *Soyuz*-type spacecraft) there are both electrical and hydraulic lines which automatically connect with the station after docking. [redacted]

DOCID: 4019726

valves the fuel is moving to the engines. There are numerous buttons on the control panel for sending the required commands to move the fuel.

After the *Progress-1* docked with the *Salyut-6* station, the two fueling lines -- one for oxidizer, the other for fuel -- were connected to the station; the hermetic seal of the lines was checked for leaks; and the pressure in the station's tanks was lowered. First the fuel and then the oxidizer was pumped from the "refueling" compartment into the station's tanks. After the refueling operation was completed, the fueling lines were purged and vacuum-evaporated with the use of the compressed nitrogen gas.

Besides fuel replenishment, the station's atmosphere was renewed with air from tanks in *Progress*'s "refueling" compartment. This operation was necessary to replenish air lost during the earlier EVA (extra-vehicular activity) and because some air is lost during various garbage-dump operations performed by the crew through a special airlock.

[redacted]

Progress-1 was also used as the first "space tug." Its own propulsion engines were switched on and the spacecraft was used to boost the *Salyut-6* station into a higher orbit.

One final experiment was conducted with *Progress-1* before it was allowed to burn up in the earth's atmosphere. After undocking, a test check of the spacecraft's own reserve automatic search and approach system was made. The test was successful and on 8 February 1978 *Progress-1* disintegrated as it reentered the earth's atmosphere.

~~(SC)~~

LETTERS TO THE EDITOR

To the Editor, CRYPTOLOG:

The following letter was prompted by Eugene A. Gilbertson's letter to the editor (CRYPTOLOG, June 1978) with regard to [redacted] earlier article "What Ever Happened to COPES?" (CRYPTOLOG, January 1978).

Now that COPES has been with us for a number of years I shall make again an observation which originally was a theoretical warning (properly discounted, since in many people's minds "theoretical" is synonymous with "most likely wrong") but which is now capable of observation and verification.

I accept the fact that COPES has had an influence on distribution of effort and resources. How sure are we that it has provided a reasonably objective base for such allocation decisions? My concern stems from admissions made privately and off the record that when COPES objective satisfaction is low we change the objectives so that the rate of satisfaction looks better, and when things look too good we add objectives to preclude a cut in resources. This should not be surprising; it is a natural response and could have been anticipated (theoretically) as the way people react. If this is indeed taking place, consciously or unconsciously, the rate of objective satisfaction is more a measure of how well we have adjusted our objectives to some acceptable norm than a basis for collection resource allocation decisions.

I am not a strong opponent of COPES. It does give us a much better understanding of what collection is doing that we had in pre-COPES days. We must, however, be very careful as to how we use such data.

Donald Y. Barrer, P1

(U)

P.L. 86-36

To the Editor, CRYPTOLOG:

I enjoyed your overlong [redacted] member SPELLMAN" (CRYPTOLOG, Jul P.L. 86-36), concerning the long-defunct Agency project which EO 1.4.(c) had the twin aims of training people [redacted] The first half of the task is no less preposterous today than it was when proposed 20 years ago. The second half, however, is, on the surface at least, a reasonable one, which was nevertheless ultimately abandoned as being beyond the capabilities of the persons involved. This resolution of the problem, you might be interested to know, was not limited to the NSA task group.

In the article from the 1957 Soviet encyclopedia quoted in your article, Stenotypy is treated as a major office-skills advance, and several advantages over "ordinary stenography" are cited: shorter training time, absence of distortion at high transcription speeds, reduced fatigue for the transcriber, etc. Altogether an upbeat view.

Contrast this with the parallel piece in the 1976 edition of the same encyclopedia. In a much briefer article, Stenotypy is succinctly described, then evaluated with this final comment:

> "Stenographic machines have not been widely accepted. Because of the development of magnetic sound-recording technology, in particular the Dictaphone, their production was dropped in the 1950s."

So cheer up. You're in good company.

David H. Williams, P16

~~(S-CCO)~~

DOCID: 4019726

P.L. 86-36

NONSECRET ENCRYPTION (Public Key Cryptosystems)

[redacted]

"We stand today on the brink of a revolution in cryptography." So begins a paper entitled "New Directions in Cryptography" which appeared in the November 1976 issue of the *Transactions on Information Theory* journal published by the Institute of Electrical and Electronics Engineers (IEEE).

We shall examine the developments to which the authors of that paper refer, discuss the potential for cryptographic revolution, and mention some effects which may be felt at NSA.

As early as 1969, mathematicians at GCHQ were considering the possibility of secure encipherment without the necessity of a key being held commonly between sender and recipient. To do this the mathematical properties of "finite fields" were to be employed. It turns out that in finite fields, which are much the same as the real numbers but which are better adapted for computer use and for key production, it is easy, given a and x, to calculate the expression a^x. However, the problem of recovering x when given a and a^x is extremely difficult to solve. One's intuition suggests that, as in the reals, an approximate solution might be satisfactory but the finiteness of the field precludes this. We see here a pair of "inverse" tasks, one of which (exponentiation) is easily performed while the other (solving the equation $y = a^x$ for x means taking the "logarithm" of y) is very difficult.

The idea, first announced by J. H. Ellis in a GCHQ paper, is to create a system in which the cryptographer may use only "easy" algorithms while the analyst is obliged to solve a "hard" problem. Suppose that we wish to send a message to a friend but we have no mutual cryptovariable. Suppose further that we have a small computer capable of performing finite field exponentiation. We may "randomly" select an integer x_1 and calculate a^{x_1} for some a which is fixed and known both to our ally and to the enemy. We transmit $y_1 = a^{x_1}$ (as a string of bits) across an insecure channel, so that both our ally and the enemy may be assumed to be in possession of y_1. The only secret we have is x_1 and even our ally doesn't know x_1.

At the other end our friend receives our bit stream and prepares himself for communication by choosing randomly another integer x_2, calculating $y_2 = a^{x_2}$, and transmitting the corresponding bit stream to us. We assume that the enemy also acquires knowledge of y_2. Now we are ready to determine the key which will be used for encipherment: we calculate ${y_2}^{x_1} = a^{x_1 x_2}$ and use the corresponding bit stream as key. Our friend is able to calculate the same key, using ${y_1}^{x_2}$. But the enemy, who knows a, y_1, and y_2, has no convenient way to calculate $a^{x_1 x_2}$ unless he can, for example, determine x_1 as the logarithm of y.

This novel method, called nonsecret encryption by Ellis, received scant attention in the intelligence community because there was no recognized application for such a system. One advantage of this system is that there is no need for key distribution; on the other hand, there are several problems of implementation. First, there is the matter of selection of the "randomly chosen" integers: maybe certain choices are weaker than others. Certainly the choice $x = 1$ would be totally insecure and one should consider the possibility that the product $x_1 x_2$ will be a weak choice even though x_1 and x_2 are not weak. Then there is the problem of errors in channel transmission. To ensure that the enemy cannot solve our system by brute force, the "finite field" must be very large (allowing a large range of inequivalent choices for x_1 and x_2) and so the bit streams y_1 and y_2 are very long. For successful communication, both y_1 and y_2 must be received with complete accuracy. At the very least this may require some error-correcting capability and the capacity of the channel must be considered, as well as the capability of the computer at each end of the link. The fact that a great deal of computation must be performed will also limit the bit rate at which transmission can be effected. Finally, there is a serious problem with authentication: since the enemy knows our system, he will be able to establish communications with us (just be sending some $y_3 = a^{x_3}$) unless we can check on his identity.

We in the intelligence community have become accustomed to holding a monopoly on useful advanced cryptologic knowledge, so it is with surprise and apprehension that we have witnessed in recent years an increasing interest in cryptology on the part of American academicians*. With the advent of digital technology in the storage and transmission of vast quantities of data, it was inevitable that security questions would arise. Engineers, mathematicians, and computer scientists see in this area a relatively uncharted

[redacted]

Charles Sullivan,

[redacted]

P.L. 86-36
EO 1.4.(c)

DOCID: 4019726

field in which new and important results may be available without the obligation to assimilate enormous bodies of information. Efforts to find and analyze better algorithms could easily lead to rapid advancement and recognition for academic-based researchers.

One of the first opportunities for scholarship arose with the development of the Data Encryption Standard (DES). Several papers have been written both by university researchers and by Bell Laboratories personnel, which are critical of the algorithm or of the size of the cryptovariable. The authors express their anxiety about the (classified) principles underlying some of the design. While the published analyses are not of the quality one would expect to find from experienced crypto-knowledgeable analysts, the intelligence and perception of the authors is easily recognized.

Foremost among the investigators is Martin Hellman, a bright young associate professor of electrical engineering at Stanford University. Widely known among information theorists for his scholarship, Hellman has published several recent articles on cryptology. With his student Whitfield Diffie he published "An Exhaustive Cryptanalysis of the NBS [National Bureau of Standards] Data Encryption Standard" in *Computer* magazine, extending an earlier "Results of an Initial Attempt to Cryptanalyze the NBS Data Encryption Standard" which they and five others published at Stanford. It was the Hellman-Diffie duo which, in *New Directions in Cryptography*, introduced to the public the notion of a "trapdoor function." Hellman's ability to attract press coverage has caused their ideas to receive considerable attention. Last year an episode of a popular television series featured a "code expert" who spoke knowingly of trapdoor functions.

The interest of Hellman and Diffie in criticizing DES is clear. If they were able to destroy the confidence of industry in the DES algorithm, then perhaps their own ideas would gain recognition as an effective security scheme, with a resulting financial windfall. Already Hellman, Diffie, and another Stanford graduate student, Ralph Merkle, have applied for a patent on a device based upon their publication. Taking advantage of the reluctance of NBS (and NSA) to discuss the strengths of DES and the weaknesses of the new approach, articles have appeared which strongly suggest that the Hellman-Diffie algorithms are "unbreakable for all practical purposes" and that the DES has "fatal flaws" which allow a successful attack to be mounted for between $20 and $5000 per message, with an elapsed time of "anywhere from six minutes to 12 hours." One of the more sensational of the articles alleged that "what is beyond dispute is the fact that any system employing the same key both for encoding and decoding is just too awkward for everyday use" (Robert C. Cowen, in *Technology Review*, December 1977).

A public key cryptosystem (this is the name given by Hellman and Diffie to the concept which we know as nonsecret encryption) is envisioned as a convenient communication scheme for a large loose network. Potential users would be financial and industrial organizations. We may think of a nationwide net of banks and brokerage houses, any pair of which may at some time have a desire to communicate securely. Each user K will have a pair of algorithms, E_K for encryption, D_K for decryption, such that, for any message m, $D_K E_K m = m$. Furthermore, D_K and E_K are algorithms which may be accomplished quickly, but it must be that knowledge of one of the algorithms does not allow the other to be deduced. Such a system is really a set of "trapdoor one-way functions," in the sense that it is computationally infeasible to find D_K given E_K. The algorithms E_K are made public. Thus anyone desiring to transmit a message to K may look up the enciphering algorithm and send the message $E_K m$. Only user K will be able to decrypt the message because only user K is in possession of the algorithm D_K.

Immediately one is forced to do something about authentication, since the receiver has no way to verify the identity of the transmitter of a message. Fortunately, there is a neat solution. Suppose that, for all K, the algorithms D_K and E_K also enjoy the property that $E_K D_K m = m$ for all m. Then if A desires to send a message m to B, he first applies the secret decryption algorithm D_A followed by the public algorithm E_B. When B receives the message $E_B D_A m$, he first applies his secret decryption algorithm D_B followed by the public algorithm E_A. The result is $E_A D_B E_B D_A m$. Since $D_B E_B x = x$ for all x, this simplifies to $E_A D_A m = m$, so that the intended recipient can indeed recover the message. Only he can decipher the transmission $E_B D_A m$, for only he has the secret algorithm D_B. Additionally, when he has recovered m, he knows that it was indeed A who sent the message, for only A has the secret algorithm D_A which must have been used (unless by chance some other algorithm could convert m to $D_A m$; this can occur, but with small probability, one would expect).

For this attractive and simple concept to succeed we shall require the existence of a suitable family of trapdoor functions. Several candidates have been proferred and an intensive search is underway to find others. The first to attract national attention was embodied in an MIT paper, "On Digital Signatures and Public-Key Cryptosystems," by Ron Rivest, Adi Shamir, and Len Adleman, which appeared in April 1977. In Martin Gardner's popular "Mathematical Games" column in *Scientific American*, August 1977, appeared a "challenge cipher" based on the MIT paper. A prize of $100 has been offered to the first solver of the cipher. The family of trapdoor functions is based on the difficulty of factoring large numbers and will be detailed below.

On the heels of these advances, the IEEE scheduled an international symposium on information theory, to include two sessions on cryptography, at Cornell University in October 1977. Interest was heightened when the organizers of the symposium received a letter from an NSA employee which suggested that the symposium might be in violation of laws. This letter and the responses of Hellman and others were publicized in the widely read *Science* magazine. The sessions on cryptology were well attended, especially the presentations of Hellman and Rivest. Three NSA employees attended these sessions. Two Stanford graduate students, Merkle and Stephen Pohlig, did not present their work for fear of legal action. At one of these sessions, Hellman remarked that he and his associates would like to analyze (and publish the analysis of) some of the "classical" cryptographic systems. He specifically mentioned rotor devices and "Hagelin." Both Hellman and Rivest have presented their ideas at meetings of scholars throughout the country. NSA employees have attended a talk by Hellman at Catholic University and a presentation by Rivest at the Applied Physics Laboratory. We should expect that considerable research effort will be devoted to cryptology in the next few years.

Computational complexity is the area of mathematics which is most intimately involved in the search for trapdoor algorithms. It is an area which has blossomed with the development of high-speed computing equipment. The difficulty of a problem can be measured by the time required to solve the problem. In general, this will depend upon some parameter associated with the problem. For example, we can consider the time required to invert a square matrix of size n, where n is a positive integer. Naturally the time required will increase as n increases, but how fast does it increase? We say informally that a problem is in class P if there exists an algorithm to solve the problem such that the maximum time required to execute the algorithm is a polynomial function of the parameter. A precise statement would involve the notion of a Turing machine, which we choose not to introduce. A problem is in class NP (nondeterministic polynomial) if an algorithm exists, with time which is a polynomial function of the parameter, to solve the problem using a computer with an unlimited degree of parallelism. The class NP includes the class P but it is not known if there is indeed a problem in class NP which is not in class P. There is a large class of problems, known as NP-complete, which share the property that if any one of them is in class P, then $NP = P$. It would be very surprising if the equality $NP = P$ could be shown. At the moment the problems which are NP-complete are regarded as sufficiently difficult to resist solution if the parameter is chosen large enough.

The goal of the theoretical cryptologist, then, is to create a system so strong that to break the system the enemy analyst must solve a problem which is NP-complete. It must be realized that this is not an assurance of a secure system. There is, until a proof that $NP \neq P$ is found, a possibility that a fast algorithm exists to solve an NP-problem. Even if this is not the case, recall that the definition of class P was a "worst case" definition and it is conceivable that although no fast algorithm exists to solve the problem for all cryptovariables, perhaps a fast algorithm can be found which often, or sometimes, solves the problem.

For a curious example of the distinction between class P and class NP, consider the problem of assigning compatible roommates, given a group of people together with their lists of satisfactory partners. If two roommates are to be assigned to each room, a clever algorithm given by Jack Edmonds of the University of Waterloo will accomplish the pairing in polynomial time, but the same task when three are to share each room is known to be NP-complete.

Suppose that a traveling salesman who must visit n cities wishes to schedule his itinerary so as to minimize the mileage driven. This problem is NP-complete but there exists a fast algorithm to find a good, but not always optimal, route.

One NP-complete problem which has been suggested in connection with cryptographic schemes is known in some circles as the knapsack problem. A pertinent paper is by Merkle and Hellman, "Hiding Information and Receipts in Trap Door Knapsacks." Suppose that you publish a list of, say, 200 very large integers $a_1, a_2, \ldots a_{200}$ and accept communications as follows. I write out my message as a streams of 1's and 0's and break it up into groups of 200. I encipher each block by adding together the a_i which correspond to 1's in my message. Upon receipt of my message, you immediately decipher the text but the enemy cryptanalyst who intercepts the message is unable to decipher it. How is this possible? It seems that both you and the enemy have the same information: the sum of certain ones of a known set of numbers.

The secret behind this method of encryption lies in the choice of the 200 numbers a_i. Suppose that another set of 200 positive integers b_i has the property that for each $i > 1$ the number b_i is bigger than the sum $b_1 + b_2 + b_3 + \ldots b_{i-1}$ of all the preceding numbers. It would be very easy to decipher a message sent using these numbers to encipher: if the message is larger than b_{200} then the 200th bit of the message was 1, otherwise 0; if a 1, subtract b_{200} from the message and repeat with b_{199}, etc. In this case no security is afforded by the encryption procedure. The principle behind the knapsack scheme is for you to transform a

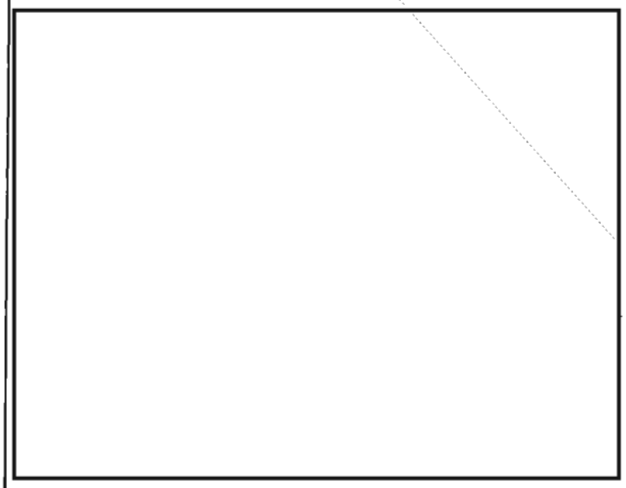
DOCID: 4019726

P.L. 86-36
EO 1.4.(c)

simple case into a difficult case in such a way that only you know how to reconvert the difficult case into the simple case which readily yields a solution. As an example, suppose you select the five integers 171, 196, 457, 1191, and 2410. These numbers satisfy the criterion for simplicity. Now you choose as your cryptovariable the numbers 3950 and 8443 (in a real-life example, the numbers would be much longer). We require that the two numbers be relatively prime and that the second be at least twice as large as the largest of the previously chosen integers. It is easy to find a number x such that $3950x \equiv 1 \bmod 8443$; $x = 2550$. Multiplying our five integers by 2550 and reducing modulo 8443 we obtain the a_i: 5457, 1663, 216, 6013, and 7439. If I wish to transmit the message 11001 I just add 5457 + 1663 + 7439 = 14559 and send that number. Upon receipt, you multiply 14559 by 3950 and reduce mod 8443 to get 2777 which is easily deciphered in your simple scheme. The enemy analyst, not knowing the cryptovariables, faces the task of exhausting over all 2^{200} possibilities: or is there a better approach?

The proposed trapdoor function which has received the most attention is the MIT scheme which was featured in the *Scientific American* article and upon which the "challenge cipher" is based. Two positive integers s and r are published, with r large. To encrypt a digital message, it must first be broken into segments with each segment having fewer digits than r. To encipher a segment x the number $x^s \bmod r$ is computed; this is easily done using current technology. To decipher, only one cryptovariable is needed: an integer t such that $x^{st} \equiv x \bmod r$ for every x. For example, if r is prime, the condition is that st should be 1 modulo r-1, and t is easily determined if s has no factors in common with r-1. Because of the ease of determining t in this case, it is not good to allow r to be a prime. It is also weak to select an r with small factors. The most promising choice seems to be $r = pq$, the product of two large primes which are not close together and which enjoy certain other interrelationships. It is easy to find pairs of appropriate primes. If it should happen that x has a factor in common with r, the decryption algorithm may need modification. The strength of the method rests on the inability of the enemy cryptanalyst to factor r into its factors p and q.

Algorithms to factor integers have been developed recently which are substantially faster than those known before this decade, but the factoring of integers of, say, 100 digits is still well beyond the capability of current computers and known algorithms. It seems that a major (and quite unexpected) breakthrough would be required to factor a typical r of 100 digits in a reasonable time. If this is the best attack on the MIT algorithm then it may be regarded as secure under present conditions. It is not clear that this is the case. If the primes p and q are poorly chosen, special approaches, which would not do in general, may succeed. It is not the case that the time taken to factor is a function solely of the size of the factors.



There are a great many problems still to be solved before public key cryptosystems find widespread usage. We have already mentioned the low rate of transmission and the need for error-correction capabilities. Let us consider an application for which the scheme was intended: a large-scale financial network. The ability of any member of the net to communicate securely with any other is very difficult to realize using conventional cryptologic equipment, but it seems to be a requirement that each user have a computer with the capability of performing the necessary arithmetic operations and with the ability to acquire the public encryption data readily; reliability may be a problem. A central facility may be necessary for the storage of the data; this would introduce additional security considerations. Some provision must be made for the possibility of a compromised decryption algorithm and the ensuing loss of authentication for that user. It is conceivable that a user might intentionally allow his private decryption algorithm to become known so that he may subsequently disavow an unfortunate purchase or sale to which he had agreed. If electronic means are used for transactions, how can the recipient be prevented from making unauthorized copies of, say, stock certificates? For the authentication scheme which is used to guarantee signatures to be wholly satisfactory, legal precedents must be established and penalties specified.

When two algorithms are to be applied consecutively, it may well happen that two different moduli are involved. The message is blocked to allow the application of the first algorithm but it may happen that the integers which result are larger than the second modulus. Solutions to this problem have been proposed but are not entirely satisfactory; perhaps others will be forthcoming. Probably the

~~SECRET~~

EO 1.4.(c)
P.L. 86-36

[redacted]

[redacted]

While public key cryptosystems are not likely to have a significant impact on American military communications in the foreseeable future, we must stay abreast of developments in the area. If implementation can be effected in inexpensive and reliable components, nonsecret encryption may provide secure communication in carefully chosen situations. [redacted]

P.L. 86-36
EO 1.4.(c)

One application for which these algorithms seem well suited is the verification of identification or credit card data. The capture of one of the decrypting boxes by criminals would not allow the preparation of bogus cards with correctly coded data, as would have been the case if the decryption algorithm were identical with the encryption algorithm.

[redacted]

~~(S - CCO)~~

P.L. 86-36
EO 1.4.(c)

NEWS OF THE CRYPTO-LINGUISTIC ASSOCIATION

P.L. 86-36

On 18 May 1978 a large number of CLA members and their guests attended the annual banquet, which was held this year at the Sheraton-Silver Spring Motor Inn. CLA President Donald G. Lasley introduced those seated on the dais. They included the CLA officers and their wives; Joseph P. Burke, Commandant, National Cryptologic School; past CLA President Dr. James R. Nielson; Mrs. Annette Jaffe; and the evening's guest speaker, Dr. Robert T. Meyer. Dr. Meyer, a scholar of international renown in the field of Celtic studies, is currently Professor of Celtic and Comparative Philology at Catholic University, as well as Consultant on Celtic for the Library of Congress He gave an informative and witty talk on "Linguistic Exploration in West Kerry, Ireland."

1978 Jaffe Award

The Crypto-Linguistic Association's highest recognition of exceptional achievements in the field of language, the Sydney Jaffe Award, was given to [redacted] G9, with the presentation of an engraved plaque by Mrs. Annette Jaffe. Previous winners of the award, which was established in 1972 in memory of the CLA's founder, have been:

1973 - Frances Blank and Dr. Mary Roberta Irwin
1974 - Norman Wild
1975 - [redacted]
1976 - John D. Murphy
1977 - [redacted]

1978 CLA Essay Contest

[redacted] awarded the following prizes to winners in this year's Annual CLA Essay Context:

1st Prize ($100) - [redacted] "The Iron Thumb" (CRYPTOLOG, March 1978)

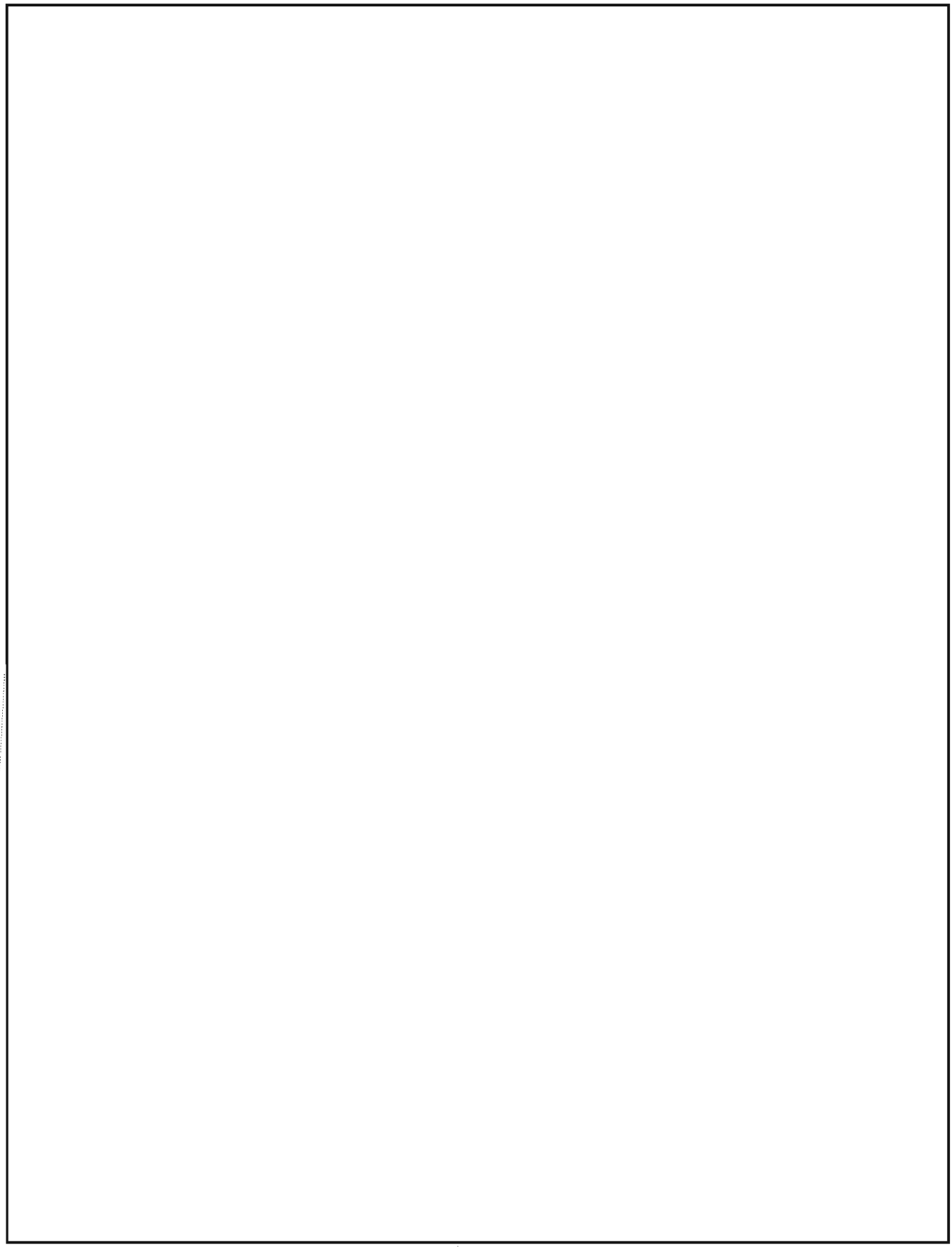
2nd Prize ($50) - Jacob Gurin, "Words and the Intelligence Value of Conversations" (to be published in *NSA Technical Journal* and *NSA Cryptologic Spectrum*)

3rd Prize ($25) - A. J. Salemme, "A Linguist's Suggested Solution for the 'Language Problem'" (*NSA Cryptologic Spectrum*, Winter 1977, Vol. 7, No. 1)

Judges in this year's Essay Contest were: [redacted] Shirley Shamp, and Dr. [redacted]

(U)

P.L. 86-36

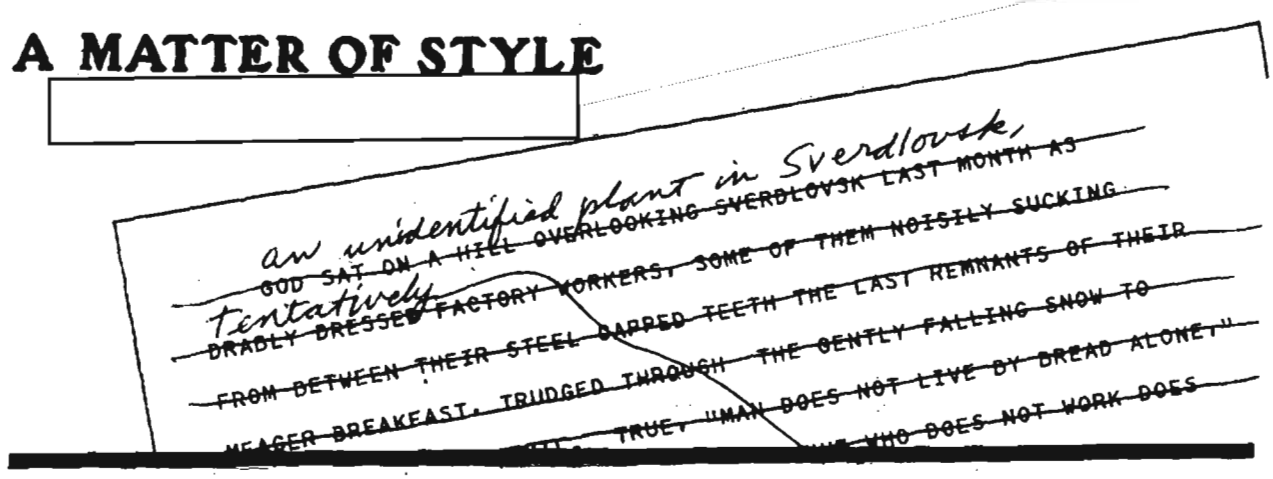


EO 1.4.(c)
P.L. 86-36

DOCID: 4019726

P.L. 86-36

A MATTER OF STYLE



"No passion in the world, no love or hate, is equal to the passion to alter someone else's draft."

H.G. WELLS

The idea for this article came about as the result of sending in a note to CRYPTOLOG, asking to have my name added to the distribution list. The editor, in replying to my request, added the postscript, "I like your style! Why don't *you* send in an article?" A nice compliment, taken at face value, but what exactly is meant by "style"? A quick look at Webster's yields this definition:

> "*style* a: mode of expressing thought in language, esp: a manner of expression characteristic of an individual, period, school or nation; b: manner or tone assumed in discourse; c: the custom or plan followed in spelling, capitalization, punctuation, and typographic arrangement and display."

This is not altogether helpful. There is an excess of verbiage contained in the definition but the reader remains essentially unenlightened. It is obvious that everyone is able to express thought in language, hence everyone has style. Granted, the method of expression by some leaves much to be desired, yet they still have style.

Of course, more is meant than just expressing thought in language. It should be done logically and progressively so that the reader can get from point A to point B without getting lost in a tangle of words. It must follow that NSA condones certain styles while rejecting others. Discovering the acceptable course is usually by trial and error, IS-250 and other courses notwithstanding. Even if a report has been prepared in the acceptable "style," there is always someone along the line willing and eager to change your report -- *your* report! -- in some manner. Since all of us are prone to error, some of these changes are warranted. Others are inexplicable.

USSID 300, that faithful old standby, does give the writer a better idea of what is expected. Hence, one finds on page 13 of the latest edition some guidelines listed after the word "Clarity":

> "Write product in a style that clearly and simply conveys the foreign intelligence information to the reader."

Here, at least, is some sense of what is wanted, i.e., a logically written report. To continue with the definition:

> "Be consistent in style, mechanics and grammar."

There's that word "style" again! If one assumes the "a" definition from Webster's, then a writer's style should never change at a given time, although it may change gradually through the course of his writing career. In a sense, we are back where we started. This being the case, let us press on:

> "Be specific in facts, background and analysis."

Good advice but, obviously, if you didn't write clearly and simply, this advice would be spurious.

> "Use short, plain, concrete words. Avoid passive verb phase."

Here we come to the crux of the matter. Here is the *style* (I use the word too) the Agency is looking for. It can allow for precisely what is needed -- a clear, concise, and logical report.

Unfortunately, there is one pitfall underlying these instructions. It allows all of us to fall into a set, lackluster form of writing. In essence, many product reports which leave this Agency read the same. The only real differences are the time of the activity and the entity involved. This kind of

DOCID: 4019726

writing requires no creativity, but only the analyst's ability to fill in the blanks. Before irate report writers come storming in to protest, let me emphasize that this is not always the case. However, it does happen, and frequently.

All of us like to think we write well. Most of us can, given the chance. I know of analysts who deliberately pattern their writing with their editors in mind. What they have written is not necessarily their own but an aping of what the editor wants. Their own writing, not always bad, has been edited so often that they change their *style* of writing in self-defense. When a new editor appears and begins enforcing his or her interpretations about what a good report should sound like, the report writer simply apes the new style, again through trial and error. There is no pride in writing. It is simply a matter of getting the job done and moving on to something else.

It should be the job of all of us to encourage creative writing as far as possible under the guidelines established in USSID 300. All of us have an affinity for certain words. We should, however, resist the urge to emend another's report simply to replace their words with ours. Editing of reports is a required function and, done properly, can be used as a teaching experience for new writers. Emendations for the sake of preference, rather than improvement, are counterproductive. In such cases, the writer has three courses open to him. He can argue his case with the editor and try to get his wording restored; he can continue a silent war with the editor by continuing to submit his own textual preferences in the hope of slipping one by; or he can change his use of words, whether he agrees with the change or not. It is important to remember that the prime task of the editor is to strive for precision and clarity. If a report must be changed for reasons of clarity or "excess verbiage," the editor should try to discuss these changes with the writer whenever possible. Both will benefit from the experience.

(U)

SOLUTION TO NSA-CROSTIC No. 16, by David H. Williams, P16 (CRYPTOLOG, June 1978):

[redacted]

"Letter to the Editor," CRYPTOLOG, July 1977:

"My point was not to malign the fine women of our Agency or propose a process in violation of any . . . regulation, [redacted] However, the times are changing. . ."

(U)

News of the Communications Analysis Association

[redacted] P14

P.L. 86-36

Dues

Yes, dues. (*"Here he goes again, George, talking about money again!"*) You can be a member of CAA for just one dollar a year. (*"Hey, I'm a dollar-a-year man, Ethel!" "I'm too young to remember what that means, George."*) The dollar brings you all the CAA news, and minutes of meetings, and announcements of various events. If you heard about CAA events too late to attend, you're probably not on our mailing list. And you're not on the mailing list because. . . that's right! . . . because you haven't become a member.

If you used to get our announcements but you haven't seen one lately, you're an *ex*-member. (*"He means you haven't paid your dues lately, George."*) Call our treasurer, [redacted] or one of the other board members and get them to mail you an application card. Then mail it, with the dollar, to Tim. (*"Hand me a dollar, Ethel."*)

(U)

P.L. 86-36

CAA Presentations

[redacted] did stir up a lot of people with his analysis of the "Outer Space" SIGINT problem, which he gave as the June CAA presentation. Does that problem exist? Who are "*they*"? Who do they think *we* are? Protein, *indeed!*

Maybe we should consider a follow-up (discussion? series?) to Clint's talk. By the time you read this, we may have already begun, but only those on our mailing list will know *for sure*. (And, of course, "*they*" will know too, won't they?)

September presentation: Have you ever tried to use a crystal ball? [redacted] will tell you how he uses his. Watch for the announcements.

(U)

Board of Governors, CAA:

President	David Gaddy	3247
President-elect	Frank Porrino	5879
Secretary	[redacted]	8025
Treasurer	Tim Murphy	3791
Board members	[redacted]	4935
		5991
		3575
		3369

P.L. 86-36

(U)

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4019726

P.L. 86-36

SOVIET COMINT & THE CIVIL WAR [1918-1921]

Translator's note: The following is a translation of the article "The Organization and Combat Use of Radio Intelligence During the Civil War," by Lt. Col. Yu. Ural'skij in Voenno-istoricheskij zhurnal (Journal of Military History), Moscow, No. 11, 1972. The article gives a rare glimpse into the early operations of Soviet COMINT and the importance that the top leadership gave to it from the very beginning of the Soviet regime. Footnotes citing Soviet archival records have been eliminated, and a few explanatory footnotes, enclosed in brackets, have been added.

When setting up control agencies, units, and subdivisions of the communications troops of the Red Army that was being created to defend the Soviet authority, the Revvoensovet [Revolutionary Military Council] of the Republic (RSVR)[1] attached great importance to the use of radio as a means of communication among the troops and to its application in the interests of intelligence[2].

During the period of the civil war, the radio situation that had developed on all fronts favored the organization of radio intelligence by the Red Army, since the combat actions encompassed a large territory of Soviet Russia and were of a mobile nature. The interventionists and White Guardists made rather broad communications use of fixed and mobile (field) radio sets, which were supplied to the headquarters of their armies, corps, and divisions, as well as to naval vessels and merchant ships that were carrying troops, arms, ammunition, and other military supplies to the White Armies of the Entente[3]. Attached to the headquarters of Kolchak, Denikin, and Vrangel' were military-diplomatic missions from the Entente countries with a staff of military advisors who had radio sets at their disposal. They maintained contact with London, Paris, Warsaw, Athens, Constantinople, and other cities.

The interventionists and the internal counterrevolutionaries carried out radio communications in the range of 250-3500 meters, with wave lengths from 290 to 740 meters being used for field communications. The White Guardists had at their disposal the radio sets of the former Russian Army, as well as American, British, and French equipment that had been supplied by the Entente. For example, Kolchak's headquarters in Omsk had a radio set with a power of 30 kilowatts, which was used to set up communications along the lines: Omsk-Arkhangel'sk-London and Omsk-Nikolaev-Constantinople-Paris. The fixed radio sets had a power of 3-30 kilowatts, and the field and shipboard radio sets, respectively, 0.5 and 3 kilowatts; this made it possible, on medium and long waves, to cover rather considerable distances either directly or by way of intermediate radio sets. At the same time this allowed radio intelligence to monitor the enemy's radio transmissions from a considerable distance.

There was almost no observance of communications security or discipline among the White forces. Operational summaries concerning combat operations at the fronts, and sometimes even combat orders, were transmitted by radio in the clear. Sometimes the addresses in the radio messages were not encrypted, for example: "Urgent. Operational [summary] No. 3. Via Krinichnaya by radio to General Shkuro. . ." The radio data [callsigns, frequencies, etc.] of field radio sets were not changed for long periods of time. It was possible to determine who the radio sets belonged to by their callsigns, for example: PGL -- *poezd generala Vrangelya* (General Vrangel's train]; ALM -- cruiser *Almaz*; ZhA -- destroyer *Zharkij*; ShI -- submarine *Shipka*; GRV -- *Gur'ev*; etc. The grouping of enemy troops and the deployment and movements of headquarters could be learned from radio messages; from radio direction-finding information, from conversations in the clear between officials, or, indirectly, when the field radio set ceased operating and then started broadcasting again, but with reduced audibility.

Thus, the White and interventionist radio communications were a priceless source of information for the Red Army radio intelligence service concerning the enemy.

When, in the course of the civil war, Soviet Russia proved to be surrounded by a fiery ring of fronts, telegraphic communication with the Western European countries was cut off, and the delivery of foreign newspapers and magazines stopped, there was a sharp limitation in the amount of incoming information concerning international life. However, as during the years of World War I, the international radio stations (Paris, Lyon, Nauen, Carnarvon,

[1] [The RSVR was set up on 2 September 1918 to unify all military control at the fronts and in the rear during the civil war period.]

[2] Radio intelligence had sprung up and had received its organizational formulation during World War I.

[3] [It appears that the Soviet use of the term "Entente" includes all the non-Russian interventionist forces, rather than just the World War I Allies.]

DOCID: 4019726

Corsi, Rome) continued to transmit regularly (within the wave-length band of 600 to 1500 meters) newspaper reports concerning the international and military situation. The reports submitted by the foreign correspondents accredited to the headquarters of the White armies traveled along these channels. All this was of interest and enabled the RSVR, and the Red Army headquarters and troops, to intercept that information and to be informed concerning the international and military events, and to obtain valuable information about the enemy.

For the Petrograd Telegraph Agency (PTA) and subsequently the Russian Telegraph Agency (ROSTA), the interception of foreign reports was carried out at the Moscow, Tver', and Tsarskoe Selo radio stations, which had been constructed in 1914 for the purpose of linking the Russian Army's General Staff with the front-line staffs and with the Allies. In April 1918 these and other radio stations in the War Department were transfered, by decree of the Council of People's Commissars, to the People's Commissariat for Mail and Telegraph. In order to increase the amount of information, in the facilities occupied by ROSTA, its own radio station was set up in 1919; that radio station received reports from the correspondents at the civil war fronts, and also intercepted foreign telegrams. They were used in *Pravda* and *Izvestiya*, which regularly printed surveys of military operations at the fronts, and, in addition, provided special "pages for the Red Army man." A similar radio station was located at the People's Commissariat for Foreign Affairs.

The organization of a radio intelligence service in the Red Army dates from the beginning of 1919. However, attempts to carry out radio intelligence and to intercept enemy radio messages had been undertaken earlier by Red Army units. For example, during the second half of 1918, the interception of foreign reports was organized at radio stations 504, 600, 601, and 602 of the Western Sector of the screen detachments which had been intended for operational communications. This was carried out by radiotelegraph operators who were familiar with radio intelligence from having served in the old Russian army. During the period from July to October 1918, they intercepted 1576 radio messages. In July 1918, radio station 504 carried out surveillance and interception of the radio messages from the field radio stations of the Krasnov troops which were operating in the Don area. The necessity of organizing not only radio intelligence, but also radio counterintelligence, was recognized by the front headquarters. For example, the Board for the Administration of the Military Telegraph Communications of the Northern Front, in a report to the military commissar of the Northern Front in November 1918, noted, ". . . in order to detect and to provide warnings concerning the possible operation of enemy radio stations in the rear of our armies, and also in order to obtain information concerning the location and operation of radio stations attached to enemy military units, it is necessary to set up radio direction-finding stations and to organize radio monitoring on the front. . ."

The formation of radio intelligence subdivisions began in January 1919. Every front and army headquarters was supposed to have one intercept station (*priemo-informatsionnaya stantsiya*) and a radio direction-finding station. The former was intended for the reception of ROSTA summaries beginning with the words "to all Soviet deputies, to all editorial offices, to all propaganda points," and for the interception of of foreign newspaper reports and radio messages transmitted by the enemy's field radio sets. It was manned by eight persons and had one or two radio receivers with a vacuum-tube amplifier. The latter was supposed to detect enemy radio stations and get bearings on them. The staff at the radio direction-finding station consisted of 19 persons. In January 1919, for the purpose of supporting the Field Staff of the RVSR with intelligence information, a radio intercept station manned by 22 persons was set up at Serpukhovo.

Radio intelligence tasks were frequently assigned also to the field radio stations of troop staffs. But that was caused by an acute shortage of radio facilities and radiotelegraph operators working in the intelligence field.

The radio apparatus used for radio intelligence consisted of old models and was produced both by foreign companies and in the shops of the Navy Department. For the most part, they were detection receivers with a wave length range of 240 to 5100 meters. With the aid of changeable circuits, the limit of the range was extended to 15,000 meters. In order to increase the sensitivity of the radio receivers, three-cascade amplifiers operating on radio tubes were used.

Because of the shortage of radio direction-finding stations, an engineer at the Communications Directorate of the Red Army, V. I. Bazhenov, invented a special antenna. This antenna made it possible to adapt for purposes of direction-finding the ordinary field radio sets[4].

Organizationally speaking, the radio intercept and radio direction-finding stations were part of the radiotelegraph battalions of fronts and armies.

The overall management of the radio intelligence service was carried out by the radio

[4]See *Instruktsiya po prisposobleniyu polevykh radiostantsij k radiopelengovaniyu po sposobu inzhenera Bazhenova* (Instruction Manual for Adapting Field Radio Sets to Radio Direction-Finding by Engineer Bazhenov's Method), Moscow, 1922.

department of the Communications Directorate of the Red Army, and, at the fronts, by radio-communications and radio-intelligence sections of the communications directorates of the fronts and armies. The sections summarized the radio-intercept data, and drew up informational documents -- daily radio-intelligence summaries and diagrams showing enemy radio communications as they had reconstructed it. These materials were intended for the Field Headquarters of the RVSR and for the intelligence sections of the appropriate staffs. The most important information was immediately transmitted by telegraph to the Field Headquarters of the RSVR and to other interested headquarters.

It should, however, be noted that the possibility of organizing and making combat use of Red Army radio intelligence at the fronts was limited because of the shortage of radio equipment and specialists. As a result of this circumstance, on all fronts except the Caucasian Front it was impossible to carry out completely the radio direction-finding of enemy radio sets.

During the civil war years, the radio-intercept stations intercepted a large quantity of radio reports issued by foreign telegraph agencies. During 1919-1921, approximately 1000 intelligence summaries were issued solely on the basis of materials intercepted by just one radio station, attached to the RVSR (translated from English, French, German, and Italian). Summaries of radio-intercept materials from the foreign press were reported to V. I. Lenin. They were also regularly provided to members of the RVSR, People's Commissar for Foreign Affairs G. V. Chicherin, the Moscow Oblast' Committee of the RKP(b), the VChK[5], ROSTA, and the directorates and departments of the RVSR Field Headquarters on matters pertaining to their areas of responsibility.

The communiques transmitted by foreign radio stations contained important political, economic, and military information. For example, a radio message intercepted early in 1919 revealed Kolchak's overall strategic plan for the 1919 spring offensive. In a statement made by Kolchak in Omsk, it was stated, "We will attempt to establish contact with Arkhangel'sk, and as soon as we succeed in occupying a line on the Volga, we shall establish contact with the south and General Denikin, after which we will change over to the offensive and advance on Moscow. Seizing Moscow is our primary goal . . ."

In his article "How the Bourgeoisie Uses Renegades," V. I. Lenin emphasized the value of foreign radio communiques. "Our radio stations," he wrote, "intercept radio messages from Carnarvon (England), Paris, and other European centers. Paris is now the center of the worldwide alliance of imperialists, and therefore its radio messages are frequently of particular interest."[6]

The radio waves were the first to carry across the front line the information that the Entente was preparing a new campaign against Soviet Russia (the chief reliance being placed on bourgeois Poland and Vrangel').

During the period of Red Army combat operations against Kolchak in 1918-1919, the radio intelligence service on the Eastern Front successfully monitored the radio communications of Kolchak's Siberian, Western, and Urals White Cossack armies, was well as White Guard radio stations in the Astrakhan', Gur'ev, Krasnovodsk, and Baku areas. Kolchak's radio contact with the Entente was also established. Radio messages and radio conversations in the clear made it possible to establish the location of the headquarters of Kolchak, Denikin, the Caspian Front, the Caucasian and Don Armies, the Astrakhan' Detachment, and the group of forces in the Northern Caucasus.

In the summer of 1919, in combat engagements against the White Cossack Urals Army, the enemy's radio communications were monitored not only by the radio-intercept stations at the headquarters of the Turkestan Front and the I and IV Armies, but also by radio station 529 at the headquarters of the 3rd Cavalry Division, 596 at the 24th Rifle Division, and 530 at the 25th Rifle Division.

On the Southern and Southeastern Fronts in 1919, radio stations 504, 522, 518, and others monitored the field radio stations of Denikin's army and the fixed stations situated on the coast of the Black Sea (Nikolaev, Odessa, Sevastopol'). On the basis of radio messages and radio conversations in the clear, the radio intelligence service on the Southern Front in May 1919 succeeded in revealing rather precisely a grouping of Denikin troops in the south and in noting a concentration of the Volunteer Army in the Azov-Donetsk sector, the III Don Army in the Lugansk sector, the II Don Army on the Northern Donets, the I Don Army to the south of the Don, in the Tsaritsyn sector, and General Vrangel's Caucasian Army in the Northern Caucasus, and also succeeded in establishing the deployment of many of the White Guard troop headquarters.

On 5 October 1919 a radio intercept station at the IX Army headquarters intercepted and decrypted radiogram 04118, which contained a a combat order issued by the Commander of the Voronezh Group, General-Lieutenant Shkuro. The order assigned tasks to the units of Shkuro's cavalry corps after its seizure of Voronezh. The information received was immediately transmitted to the headquarters of the Southeastern Front.

The radio intelligence service of the Red Army operated more successfully against

[5][Secret police; predecessor of KGB.]

[6]V. I. Lenin, *Poln. sobr. soch.* (Complete Collected Works), Vol. 39, p. 182.

DOCID: 4019726

Vrangel' in the concluding phase of the civil war. Factors that contributed to this were the experience that had been accumulated in the combat use of radio facilities for purposes of intelligence, and the improvement in the supplying of technical equipment to radio battalions.

During the Red Army's combat actions against the Vrangel' forces, many of the intercepted radio messages dealt with enemy groupings, the redeployment of headquarters, and the headlong flight of the White Guardists from the Crimea. For example, in one radio intelligence summary issued by the headquarters of the Southern Front it was indicated, "From radio messages intercepted by the chief front [station] from radio stations 6ZhT, 7ZY, and 5PY, one can make the following conclusion: radio station 5PY, attached to the 2nd Don Cavalry Division, approximately between 29 September and 1 October, was transferred, together with the division, to the area to the north of Volkovakha; previously that radio station had been in the Aleksandrovka area." The data obtained was subsequently confirmed by tactical reconnaissance.

Beginning on 8 August 1920 the radio stations on the Caucasian Front noted an exceptionally large amount of radio traffic in the Sea of Azov area. The possibility of a landing operation was raised. And, indeed, on 14 August, under the command of General Ulagay, a landing was made in the Akhtarsk area. Front-line radio intelligence continuously monitored the enemy's radio communications, intercepting radio messages and official conversations. The information thus received contributed to the defeat of this landing.

On 16 October a radio intercept station of the Caucasian Front headquarters intercepted an order from the Commander of the II Army, General Abramov, which had been sent in the clear. That order concerned the changeover on 17 October to the offensive against the Red Army units on the Kakhovka bridgehead. Knowledge of the enemy's plan of operations helped the headquarters of the Southern Front -- to whom the intercepted White order was forwarded -- to destroy the Vrangel' forces at Kakhovka.

In the final stage of the Red Army's combat actions in the fight for the Crimea, the White Guardists did not have enough time to encrypt their combat documents, and the radio traffic was sent in the clear. The radio messages contained information concerning the withdrawal of units, their evacuation from the Crimea. For example, changes in the enemy's groupings were mentioned in the 25 October 1920 radio-intelligence summary issued by the Southern Front: ". . . radio station OCh, attached to I Army headquarters, was removed, for transfer to a new location. Apparently the enemy has begun evacuating Melitopol'. Radio station 81T, which serves the headquarters of the troops operating in the Nikolaev area, also has been removed for transfer to a new location. During the past few days we have observed almost no activity by the enemy's field radio stations. One can assume that the headquarters of the divisions and corps to which the field stations are attached are being redeployed."

Radio communications also provided information about the course of the evacuation of Vrangel's troops from the Crimea. For example, General Kutepov reported to the fleet commander that he had 6500 officers and men on board a steamship, and there was absolutely no water or bread. He also reported that "the LAZAR, which was being towed by it," had sunk as a result of a leak. The KRONSHTADT reported to Constantinople that it had absolutely no coal or food supplies, it had 5000 passengers on board, and was towing the ZVONKIJ.

On the basis of the radio intercept information, the Commander of the Southern Front, M. V. Frunze, in an order dated 15 November 1920, demanded the "development of the most energetic efforts on the part of submarines and the liquidation of the enemy's attempts to use the sea to escape the blows being dealt by our armies."[7]

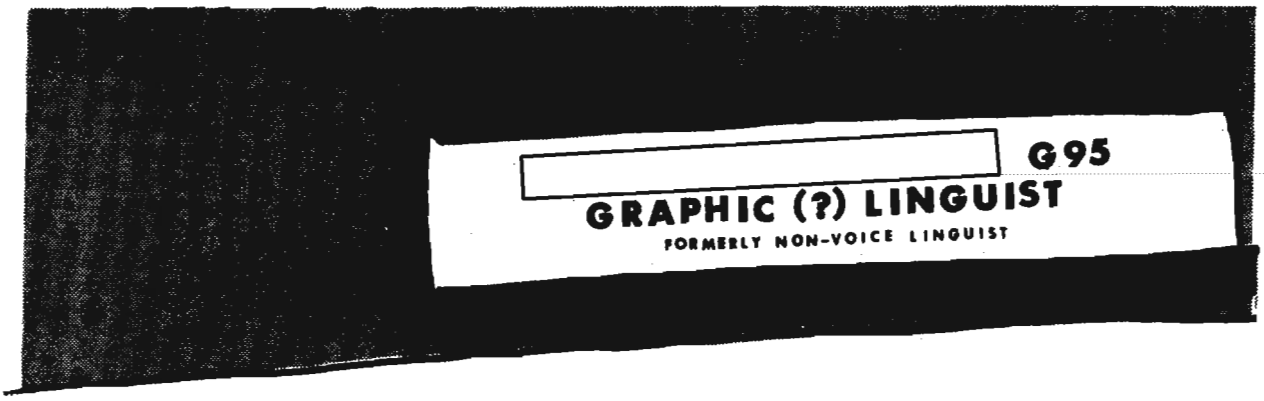
Thus, it follows from what has been stated that during the years of the civil war the Red Army's radio facilities were used successfully for intelligence purposes against the enemy.

At a conference of front-level chiefs of communications troops that was held in 1921, the activities of radio intelligence were rated highly. The radio intelligence service that had been created in our Armed Forces "completely justified its purpose and provided the Red Army with valuable material concerning the enemy, thus helping the Red Army to achieve victory." The role and importance of communications troops, including the role and importance of the radio facilities, were also given their proper credit by the Revolutionary Military Council of the Republic, which, in recognition of the valorous and extremely valuable work for the benefit of Soviet Russia, expressed its appreciation to the entire complement of commissars, commanders, and Red Army men in the Red Army communications troops.

The combat experience of using radio equipment for intelligence purposes during the years of the civil war was used for the further development of the radio intelligence service in the Red Army.

[7] *M. V. Frunze na frontakh grazhdanskoj vojny* (M. V. Frunze on the Civil War Fronts). Collection of articles, Moscow, 1941, p. 448. Unfortunately, the submarine forces could not execute this order. The two submarines in the Black Sea -- the AG-23 and the AG-24 -- were not ready for operations in the open sea.

DOCID: 4019726



P.L. 86-36

For some unknown reason, it seems that persons writing or talking about language skills, functions, and work loads have been unable to find an appropriate descriptive or general heading for the world of the translator. In contrast, the world of the transcriber presents no apparent difficulty, for it is neatly and effectively packaged and labeled as "voice." We speak, hear, read, and write about the "voice problem," a "voice linguist" (can this be a transcriber?), "voice traffic," "voice skills," the "voice language technician," and the "voice language analyst." As for that other world, however, no such overall descriptive has been discovered or devised.

At some point, someone decided to adopt a binary approach in resolving this problem. In our daily routine, we are constantly involved in situations where we are faced with a choice or condition of two alternatives, such as on-off, yes-no, 0-1. It follows, therefore, that if the one world is "voice," what can be more simple than to call the other world "non-voice"? This term has gained acceptability and respectability and is now virtually official NSAese.

When one carefully examines the word "non-voice," one can only conclude that it is a "nonword." It is vague and imprecise. The rejoinder to this might be, "Well, you know what it means from context." True enough. Yet, one could also understand the connotation of the term "non-transcriber" if it were used as a substitute for "translator" in the proper context. Fortunately, no one has suggested the use of the expression "non-voice language analyst" or "non-voice language technician" as career occupational titles, although such an eventuality is not unreasonable to imagine.

In seeking an alternative to "non-voice," I thought it would be helpful to scan the NSA Basic Cryptologic Glossary of June 1971, which the Director in his foreword urged all of us "to consult and be guided by . . . in the preparation of briefings, technical reports, and other documents." I was in for quite a surprise! If a linguist wants to give his or her tender sensibilities a real working over, he or she should review the 20 main categories of cryptology listed on page 47 of the glossary. Neither "language" nor "linguistics" nor "cryptolinguistics" made the honor roll (although "cryptolinguistics does appear as an entry). It is interesting to note that the entries "transcript" and "transcription" appear under the category "Collection (Interception)"! It is evident that the compilers must have wrestled with the placement of the entry "cryptolinguistics" because it is listed -- along with "scanning," "gist," "kana," "Cyrillic alphabet" -- under the category "General"! In effect, although this glossary represents the codification of the highly specialized vocabulary of cryptology, the few terms from the world of the linguist are lumped together as "General."

As for the cryptologic dramatis personae, a "traffic analyst" is defined as "a person versed in the art of traffic analysis," and a "cryptanalyst" is, of course, "a person versed in the art of cryptanalysis or the science of cryptanalytics." A "bookbreaker" is "a cryptanalyst who specializes in the recovery of plain text values in a code." One can only assume that the compilers of the glossary would have referred those who inquired about the definition of a linguist to Webster's dictionary. The Webster's *Third International Dictionary* defines a linguist as "1: a person accomplished in languages and especially in living languages: one who is facile in several languages. 2: a student of or expert in linguistics." The merits and demerits or validity of this definition in the cryptologic context could undoubtedly provide a stimulating subject for discussion among the practitioners of the linguistic art.

The next official source I consulted was the textbook "Radio Traffic Analysis," vintage 1964, which contains a "Glossary of Traffic Analysis Terminology." Although "transcription" and "voice" appear in this glossary, my search for other language-related terms was in vain. And then the trail led to the earlier edition (1955) of "Radio Traffic Analysis" and its glossary. There, for all the world to see, is the entry "linguist." Instead of providing a

DOCID: 4019726

definition at that point, the glossary advises one to "See LINGUISTIC PERSONNEL." For "linguistic personnel," the glossary explains, "In cryptology, those persons skilled in language." The glossary adds what it calls "the specific categories of linguistic personnel engaged in cryptologic work." Would you believe 11 categories? They are:

- identifier,
- interpreter,
- language specialist,
- linguist ("one who has expert knowledge of a foreign language"),
- listener,
- reader (for those who may be puzzled by this, a reader is "a language specialist who deals with a foreign language in its written form"),
- scanner,
- spotter (not one who locates enemy targets or a civilian who watches for approaching airplanes or one who removes spots, but rather "a reader who sorts traffic by means of key terms"),
- transcriber,
- translator, and
- voice translator ("a listener who translates recorded language voice transmissions into written English).

How did the compilers of this glossary overlook the "non-voice translator"?

From the context in which "non-voice" is used, it presumably refers to a foreign language in its written or printed form, although one may make a good case for including Morse code, semaphore, smoke signals, or even intelligible drumbeats. If this presumption is correct, then why not use the term "graphic," defined by Webster's as "of or relating to the written or printed word or the symbols or devices used in writing or printing to represent sound or convey meaning"? In combination forms it may even offer some euphonious possibilities -- "graphic traffic," anyone? In fact, "paper linguist" has been occasionally used as a synonym for translator. However, it comes too close to "paper tiger" and our local humorists have enough material already.

I have been using the term "graphic" in the language context for some time now without having elicited any noticeable confusion, discomfort, or demurral on the part of readers or listeners. Notwithstanding the fact that the "age of verbal permissiveness" is upon us and almost anything goes, I offer it as an effective substitute for "non-voice."

Years ago there was a popular song, written by the late Johnny Mercer, that contained some relevant sound advice in its opening lines: "You got to accentuate the positive, eliminate the negative, latch on to the affirmative, don't mess with Mr. In-between." ~~(C GCO)~~

LETTERS TO THE EDITOR

To the Editor, CRYPTOLOG:

This letter is in response to two articles by Mr. Mark Pattie, "What Language Problem?" (CRYPTOLOG, May 1976) and "As I Was Saying Two Years Ago..." (CRYPTOLOG, June 1978).

You were wrong in 1976, Mr. Pattie, and you are wrong again. Worse, your attempt, or any attempt, to prove that there is a high-level Agency-wide conspiracy against linguists is doomed to failure because no such conspiracy exists. Nor has it ever existed. Individual inequities -- probably, but no more in the ranks of linguists than in any other cryptologic area.

There are some fatal flaws in your articles that ought not to be there, if for no other reason than because of your cryptanalytic background. For example, the current group of GG-15s in the SR, Language, CA, and TA fields breaks down to one SRA, nine "linguists," 11 CA, and one TA. Using your analytic methodology the "linguists" are in pretty good shape in the cryptologic skills area. In fact, we might deduce that they don't do badly when measured against the CA field, and that they are 9 times better off than the SRAs and TAs.

We might make that deduction, but we had better not because those numbers don't tell us anything at all except that there are a certain number of people at a certain grade in a particular group of COSCs. In short, they don't tell us any more than your numbers did. If we took a further look, we would find that the nine "linguists" are in fact almost all division chiefs, research linguists, or language coordinators rather than language analysts or voice language analysts. And that is who we are talking about, isn't it? We must get that straight at the beginning. If we are going to talk about language analysts and voice language analysts at the 13 or higher grade levels, we are not talking about language people at the technician level. Your second fatal flaw, then, I believe, was to put all language people into the same pot. Surely you are aware that the terminal grade for language techs is GG-12 and since that job has requirement for only a level-2 language proficiency, GG-12 seems quite generous to me. I should point out that in the technician arena, in grades GG-5 through GG-12, language people enjoy a promotion rate and an attrition rate that is nearly identical to that of the other cryptologic skills.

But I digress. We are not supposed to be talking about technician-level language people, but rather professionals. You made a big thing out of the statistic that said linguists got 4

percent of promotions in the 13-18 range, while engineers captured 19 percent of the total. That rate is just not strange when you also consider that all professional-level language jobs throughout the Agency constitute only 3 percent of the authorized work force while engineer and computer scientist professional-level jobs constitute 17 percent of that same work force. Now if you want to argue that there should be more professional-level jobs in the language field, that's a different ballgame. But you would probably get a lot of argument there too. The fact is that an awful lot of our current authorized level-3 (professional) jobs are being done by level-2 (technician) people. In some areas the professionalization rate is under 25 percent, meaning that 75 percent and more of the people on the job are not even qualified for consideration to promotion beyond grade 12.

But aside from all of this, I recognize that the gut issue, in your mind, is that we get what we pay for. Not always, Mr. Pattie, not always. Sometimes we have to pay for what we get, though, and we do not operate in a vacuum. We know what professional engineers (and linguists) are paid outside the Agency, so we must be competitive. If that means extra pay and more rapid advancement for engineers and computer scientists at the professional level, then it is so because of a real-world situation -- that is, it is so because it is what we must do to accomplish the mission. You ought not to confuse ideological truths with reality: everybody has an opportunity to become Deputy Director, but not everyone will. The career structure allows for movement in the language field up to GG-18, but there are no real jobs at that level. That's the way it is.

Whoever told you that hiring high school kids was "*the* latest solution to the language problem" lied. Nobody associated with the program that I know believes that. The facts are that we are hiring very sharp high school kids as trainees (in Russian only at this point) because that's where the requirement is. We are also hiring Russian majors, other language majors as trainees, ex-military (many of whom were high schoolers, incidentally), and anybody else who can qualify as a language technician or trainee. The point is that we are hiring people against requirements as trainees only when we cannot get already trained people. We are doing it in language, collection, signals conversion, and soon we will do it in the computer field.

You asked, "Why don't we hire high school graduates to be trained as engineers or mathematicians?" I know you were once assigned to the National Cryptologic School so I expect that you know we aren't equipped to train either from scratch. We are, however, well equipped to train language people from the ground up with one of the best damn language teaching staffs and faculties anywhere in the world. The attrition in those classes is under 10 percent, and that would be a miracle, except that it has been accomplished by outstanding recruiting, teaching, staffing, supporting, and plain hard work by the students themselves.

Another mistake I suspect is that you are confusing the importance of the mission with the difficulty of accomplishing it. We cannot realistically use "job importance" to set pay scales -- who's going to decide whether it is more critical to collect, decrypt, translate, transcribe, analyze, or transmit?

Finally, solutions that cannot be carried out are not solutions. About $20 million and 1000 more people would probably solve all our problems, but neither the $20 million nor the 1000 people are available. If you can figure a way around that, you should immediately pass it on to the "senior managers" you think are involved in the conspiracy. I am sure you would enjoy their unending gratitude.

Dan Buckley, M03

~~(C GCO)~~

Mr. Pattie replies:

My goodness! I must certainly have struck a nerve in Mr. Buckley. His letter flays me up, down, and sideways. Could it be that his role in the high school program has made him a bit sensitive to any criticism?

After reading his scathing letter I thought I had better reread my articles to see if I had said anything about a "high-level Agency-wide conspiracy against linguists." I never brought up the possibility of such a "conspiracy," but since he did, maybe it does exist. Methinks he doth protest too much.

I suppose someone could construe my comments about senior officials and their attitudes toward language work as implying "conspiracy." If anyone took it that way, I apologize. However, I do stick by my statements about individual seniors and their attitudes. Although I suspect that there would be staunch denials, some have definitely expressed low opinions about linguists and language work.

Mr. Buckley uses flamboyant language in castigating me and I feel reasonably sure that if he had thought about it a bit more he might well have toned down his letter. For one thing, I believe he could have made his first "fatal flaws" paragraph more comprehensible. I don't know what he meant by "current group of GG-15s" and I don't really care, for I thought I was comparing linguist *promotions* with those of engineers.

Then, to take me to task for not recognizing that there is a language-technician level is raising another "fatal flaw" to no purpose. Did any other reader believe I was talking about nonprofessional linguists? All of that particular argument is a red herring having nothing to do with the issue I tried to raise.

As for professionalization itself, there is no question in my mind that it is far easier

DOCID: 4019726

to become professionalized as an electronic engineer than as a linguist. Can you deny that, Mr. Buckley? This is so because the Agency has determined that to be a professional linguist one must pass a series of very difficult tests, along with other requirements. That in itself goes a long way towards explaining why so many level-3 language jobs are being handled by level-2 people. Engineers have a far less stringent professionalization program.

The tone of Mr. Buckley's letter is most unfortunate, for he seems determined to read the riot act to me even when he states what I have already said in my articles. Of course I recognize that the Agency must compete with the outside world in hiring. The difference is that the Agency is willing to pay more to hire engineers than linguists. Since he is so close to all of the facts and figures, perhaps Mr. Buckley could tell us how many engineers and how many linguists have been hired directly at the GGD-13 level or higher over the past few years or so.

And, of course, the statement that there are no real jobs in the language field at the higher grades is a fact that we all recognize. But isn't that one of the things I was complaining about? His "That's the way it is" implies that that is the way it will always be, and I fear he is right.

Then, there is the matter of the high school program, for which he berates me so soundly. I would still like to hear someone give facts and figures on the retention rate of the previous high school program. If his office cannot find this data, I suspect that some of the operational areas would be able to fill in the gap.

Incidentally, this "one of the best damn language teaching staffs and faculties" he refers to is composed of contract instructors (many of whom have not had a raise in years) and people on loan from operational elements, in addition to those who are assigned to billets in the NCS. It is a real hodgepodge. I do not have access to any pay records but my best guess would be that the Agency is getting this instruction at bargain rates. It should also be noted that the contract instructors, being only partially cleared, can only carry the students so far before their lack of knowledge about our business brings a halt to their usefulness.

I do not understand the accusation that I am "confusing the importance of the mission with the difficulty of accomplishing it." What does that really mean?

Then, finally, the statement that "we cannot realistically use 'job importance' to set pay scales" does not ring true. Someone does, or should look at Agency mission and function statements when determining hiring needs and tables of distribution. The statement runs contrary to his previous points about hiring and career structure. Yes, someone has decided that pay scales for engineers are higher than those for linguists. Is that a conspiracy? I'll let you decide.

I'll end with one final point -- all the best engineers in the world cannot issue one piece of end product. Linguists can and they ought to be paid well for it.

Mark T. Pattie, Jr., P13D

~~(FOUO)~~

Do you HATE TO WAIT?

Do you hate it when only one or two copies of CRYPTOLOG are circulating in your work area and you have to wait and wait to read the latest issue until after everyone else has read and discussed the provocative ideas expressed in it? Worse yet, do you hate to wait to see the latest CRYPTOLOG, only to find that all the puzzles have already been done? -- *and in ink!* Well, then, why don't you just ask to be put on the distribution list to receive your own personal copy of CRYPTOLOG? Just send your name and organizational designation to: CRYPTOLOG, P1. You don't have to type up a fancy-looking memo -- a scrap of paper will do it. Or you could telephone the editor, on 5236s. That's riskier, however -- while he's got you on the phone, he might try to coax you into writing one of those discussion-provoking articles yourself.

(U)

T ANNOUNCES ESTABLISHMENT OF HUMAN RESOURCE DEVELOPMENT PANEL

Telecommunications and Computer Services (T) announces the establishment of a Human Resource Development Panel. The Panel's two primary functions are to assist T employees in career planning and to advise DDT in areas of human resources development, career planning, and utilization. Information about the operation of the Panel may be obtained from the Chairman, Mrs. [redacted] T432, Room 6A126, x3091s.

P.L. 86-36

(U)

DOCID: 4019726

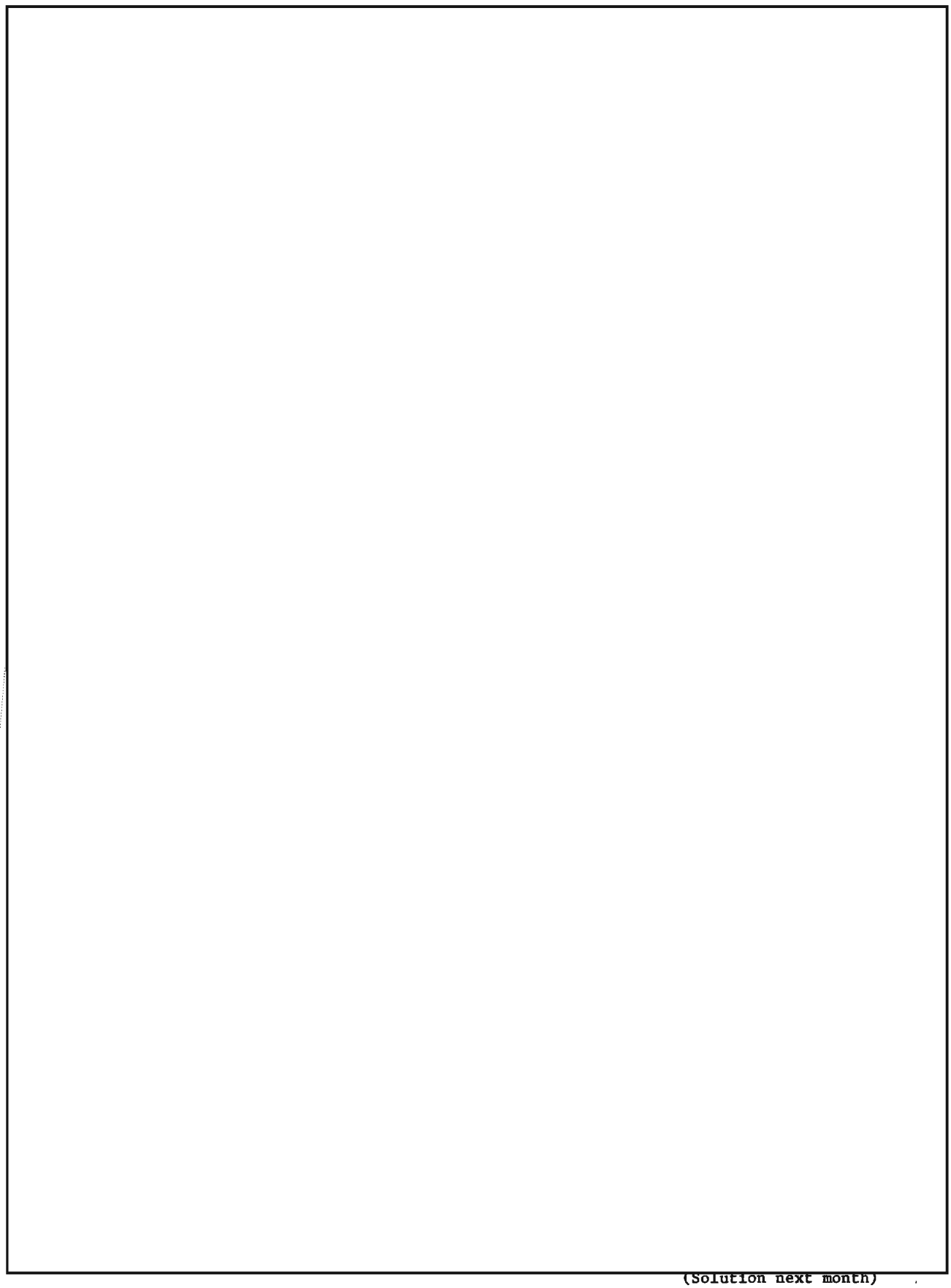
NSA-crostic No. 17

by A.J.S.

The quotation on the next page was taken from the published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS *WORDS*

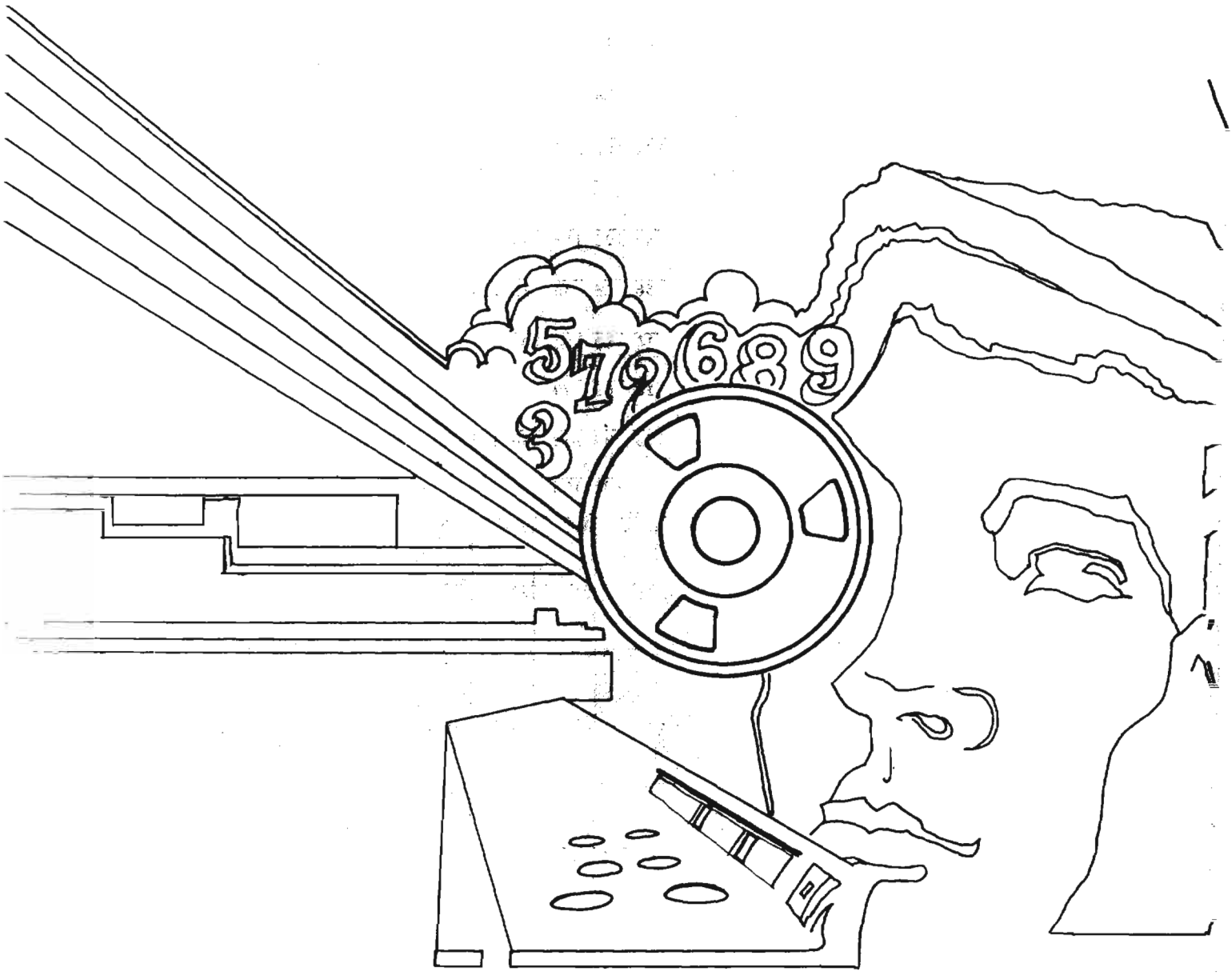
DOCID: 4019726



(Solution next month)

P.L. 86-36

P1-JUL 78-S3-26571


5796893

DOCID: 4019651

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JULY–AUGUST 1978

P.L. 86-36

THE SOVIET GENERAL STAFF..... [redacted] ...1
HAS IT EVER BEEN TRANSLATED BEFORE?..... [redacted] 5
ANOTHER COUNTRY TRIGRAPH SYSTEM..... [redacted] 10
IS A TRANSLATOR A PROFESSIONAL?..... [redacted] .11
THE BUCKY BALANCE..... [redacted] 13
TELL ME I'M JUST A SINOBIBLIOPHOBE!..... [redacted] 16
NSA-CROSTIC NO. 16.....David H. Williams.....18
NEWS OF THE COMMUNICATIONS ANALYSIS ASSOCIATION.....20
I REMEMBER SPELLMAN.....A. J. Salemme.....21
NEW BOARD MEMBERS; NO MORE MISPELLINGS.....28
LETTERS TO THE EDITOR..... [redacted] Gurin, [redacted] .29

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. V, Nos. 7-8 JULY-AUGUST 1978

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5236s)

Collection..... [redacted] (8955s) P.L. 86-36

Cryptanalysis..... [redacted] (4902s)

Cryptolinguistics..... [redacted] (5981s)

Language..... [redacted] (8161s)

Machine Support..... [redacted] (5303s)

Mathematics..... [redacted] (8518s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Tyrone (3573s)

Production Manager.....Harry Goff (5236s)

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

"The General Staff is the main organ of control of the armed forces of the state in peace and wartime." That is the first sentence of the article on the General Staff in *Sovetskaya voennaya ehntsiklopediya* (Soviet Military Encyclopedia), published in 1976. The article was written by General of the Army V. G. Kulikov during his tenure as Chief of the General Staff (September 1971 to January 1977). Kulikov has been reassigned to the position of Commander-in-Chief of the Combined Armed Forces of the Warsaw Pact and promoted to Marshal of the Soviet Union. His successor as Chief of the General Staff is N. V. Ogarkov, who was also promoted to Marshal of the Soviet Union.

In this article we shall examine the role of the Soviet General Staff

[2]Italics are used throughout this article to indicate Russian abbreviations and words.

EO 1.4.(c)
P.L. 86-36

Encyclopedia Article

The translation of the pertinent portion of the encyclopedia article follows:

The first main military organ in the history of the Soviet state which led the formation, equipment and instruction of the troops of the Soviet Army, and also the working out of all questions connected with defense of the Republic was the All-Russian Main Staff, which was established in May 1918. A council consisting of a Chief and two military commissars, which until 6 September 1918 was subordinate to the People's Military Commissars (*Narkomvoen*) and then to the Revolutionary Military Council (*Revvoensovet*) of the Republic, headed the Staff. Chiefs of the All-Russian Main Staff were:

. N. N. Stogov	May 1918 - Jun 1918
. A. A. Svechin	Aug 1918 - Oct 1918
. N. I. Rattehl'	Oct 1918 - Jun 1920
. A. A. Somojlo	Jun 1920 - Feb 1921

In connection with the fact that the organ of operational leadership from 6 September 1918 had become the Staff of the Revolutionary Military Council of the Republic (8 November 1918 renamed Field Staff of the Revolutionary Military Council of the Republic), the functions and composition of the All-Russian Main Staff were changed. Chiefs of Staff (the Field Staff) of the Revolutionary Military Council of the Republic were:

. N. I. Rattehl'	Sep 1918 - Oct 1918
. V. F. Kostyaev	Oct 1918 - Jun 1919
. M. D. Bonch-Bruevich	Jun 1919 - Jul 1919
. P. P. Lebedev	Jul 1919 - Feb 1921

In February 1921, for purposes of establishing a single organ of control of the Armed Forces of the RSFSR, the All-Russian Main Staff and the Field Staff were combined into the Staff of the *RKKA* (Workers and Peasants Red Army), the Chief of which from February 1921 until April 1924 was P. P. Lebedev. Subsequently, in conducting the military reforms of 1924-1925 the position and role of the Staff of the *RKKA* in leading the Soviet Armed Forces became determined more clearly. M. V. Frunze (Chief of the Staff of the *RKKA* from April 1924 until January 1925) emphasized that "this operational staff must become not only the brains of the Red Army, but must also become the military brains of our entire Soviet state." The Staff of the *RKKA* actively participated in the preparation of the country and armed forces of the USSR for military defense against imperialistic aggression. It was charged with the working out of operational and mobilization plans, keeping in mind the political, economic, and military resources of the Soviet state, the conducting of activities on questions of organizing the equipping of the army, aviation, and navy, the operational use in war of the services of the armed forces, arms of service, and special troops and their further development. The Staff became the center for studying and summarizing the combat experience of World War I and the Civil War. After M. V. Frunze, the Staff of the *RKKA* was headed by:

. S. S. Kamenev	Feb 1925 - Nov 1925*
. M. N. Tukhachevskij	Nov 1925 - May 1928
. B. M. Shaposhnikov	May 1928 - Jun 1931
. A. I. Egorov	Jul 1931 - Sep 1935

*After leaving his position as Inspector of the *RKKA*

In the 1930s the tasks of strengthening the defense of the country demanded further perfection of the organs of higher military control. In June 1934 the Revolutionary Military Council of the USSR was abolished by the *TsIK* (Central Executive Committee) of the USSR and the People's Commissariat for Military and Naval Affairs was renamed the People's Commissariat of Defense of the USSR. The Staff the *RKKA*, by decision of the *SNK* (Council of People's Commissars) of the USSR, dated 22 September 1935, was transformed into the General Staff of the *RKKA*. It was composed of the following directorates:

DOCID: 4019651

- . operations,
- . intelligence,
- . organizational,
- . mobilization,
- . military-topographic,
- . military transportion,
- . organization of the rear, and
- . a number of other directorates and departments.

In the prewar years the General Staff was occupied with strategic and operational planning for the utilization of the USSR armed forces in war and operations, the studying of the preparation of the theaters of military operations, perfecting of the organizational structure of forces, mobilization questions, material-technical support and plans for orders of armaments and equipment from industry, directing of operational training of the higher command complement and operations staff, and the working out of questions of Soviet military theory. A major task of the General Staff was supporting a high level of combat readiness of forces and staffs. The development of centers of conflict and the emergence of a direct threat of attack on the USSR demanded that the Communist Party and the Soviet government hasten the carrying out of a number of major measures connected with strengthening the nation's defense capability. A great role in the organization and leadership of these measures was played by the General Staff. Prewar Chiefs of the General Staff were:

. Marshal of the Soviet Union	
A. I. Egorov	Sep 1935 - May 1937
. Marshal of the Soviet Union	
B. M. Shaposhnikov	May 1937 - Aug 1940
. General of the Army	
K. A. Meretskov	Aug 1940 - Jan 1941
. General of the Army	
G. K. Zhukov	Feb 1941 - Jul 1941

At the beginning of the Great Patriotic War [World War II] the General Staff was subordinated to the Supreme High Commander and was a principal operational working organ of the *Stavka* (Headquarters) of the Supreme High Command for strategic planning and directing of the armed forces at the fronts. The General Staff:

- . carried out the collection and analysis of data about the situation at the fronts;
- . prepared conclusions and proposals to the *Stavka;*
- . on the basis of decisions made by the *Stavka*, worked out plans for campaigns and strategic operations;
- . organized strategic interaction of the services of the armed forces and fronts;
- . monitored the working out of plans of frontal operations;
- . informed the troops of decisions, orders, and directives of the Supreme High Command, and checked on their fulfillment;
- . directed military intelligence;
- . organized and checked on the operational transportation of troops;
- . monitored the formation of reserves and the timeliness of their utilization in accordance with decisions of the *Stavka;*
- . looked after the condition, support, and combat readiness of the troops;
- . generalized the experience of the war and informed the troops of it;
- . together with other organs of the People's Commissariat of Defense, worked out and submitted requisitions for the output of military production in accordance with the strategic plans outlined by the *Stavka*; and
- . decided many other questions connected with the conducting of the war.

Particular attention in the work of the General Staff was given to maintaining constant communications with the commanders of forces of the fronts, commanders of fleets and their staffs, and also organizing checks on the fulfillment by the troops of directives and orders issued by the Supreme High Command. Representatives of the General Staff often traveled to the fronts for purposes of rendering assistance to the troops. In the combat Army, from division to the front staff inclusive, there were constantly officers of the General Staff, who checked on the position and condition of the troops, their supply situation, training of troops for operations, and their carrying out of combat missions in the course of military operations, and reported about this to the General Staff.

The work of the General Staff in generalizing the experience of combat operations was of great importance. For this purpose a Department for Utilization of the War Experience was established within the General Staff. In the autumn of 1942 the first "Collection of Materials Concerning the Study of the War Experience" was published. In March 1944 the department was expanded into a directorate, which, along with the earlier publications, organized publication of "Information Bulletins" and "Collections of Tactical Examples." The publishing in 1944 alone of approximately 600,000 copies of various publications on these questions testifies to the scope of the work done by the General Staff in generalizing and utilizing the experience of the war. The preparation of proposals, reports, and materials on all military questions discussed in the course of governmental meetings and international conferences of the nations forming the anti-Hitler coalition, became one of the responsibilities of the General Staff in the course of the war. The General Staff was staffed with officers and generals who knew well the nature of contemporary warafare, the potentialities of the services of the armed forces and the arms of service, mastered skills of planning contemporary operations, possessed broad operational vision, flexible operational thinking, and high military efficiency, as well as a large amount of combat experience. After General of the Army G. K. Zhukov, the Chiefs of the General Staff during the war years were:

DOCID: 4019651

. Marshal of the Soviet Union
B. M. Shaposhnikov — Jul 1941 - May 1942
. General Colonel, from 18 January 1943 General of the Army, from 16 February 1943 Marshal of the Soviet Union
A. M. Vasilevskij — May 1942 - Feb 1945
. General of the Army
A. I. Antonov — Feb 1945 [to end of war]

After the end of the Great Patriotic War a reorganization of the higher organs of military control was conducted in accordance with the conditions of peacetime. The General Staff was subordinated to the Ministry of Defense. Beginning in June 1946, it began to be called the General Staff of the USSR Armed Forces. Chiefs of the General Staff after the Great Patriotic War were:

. General of the Army
A. I. Antonov — [1945] - Mar 1946
. Marshal of the Soviet Union
A. M. Vasilevskij — Mar 1946 - Nov 1948
. General of the Army
S. M. Shtemenko — Nov 1948 - Jun 1950

In 1950 the USSR Ministry of the Armed Forces was renamed the USSR Military Ministry, and the USSR Naval Ministry was formed. As a result, from 1950 to 1953 the Naval General Staff functioned, and the General Staff of the Armed Forces was renamed the General Staff of the Soviet Army in 1950. The General Staff of the Soviet Army was headed by:

. General of the Army
Shtemenko — Jun 1950 - Jun 1952
. Marshal of the Soviet Union
V. D. Sokolovskij — Jun 1952 - Sep 1955

In September 1955 the General Staff of the Soviet Army was reorganized into the General Staff of the USSR Armed Forces, Chiefs of which were:

. Marshal of the Soviet Union
V. D. Sokolovskij — Sep 1955 - Apr 1960
. Marshal of the Soviet Union
M. V. Zakharov — Apr 1960 - Mar 1963
. Marshal of the Soviet Union
S. S. Biryuzov — Mar 1963 - Oct 1964
. Marshal of the Soviet Union
M. V. Zakharov — Nov 1964 - Sep 1971

Since 1971 the General Staff has been headed by General of the Army V. G. Kulikov. Since March 1973 the Chief of the General Staff is simultaneously a First Deputy Minister of Defense of the USSR.

In the postwar period the General Staff has been perfecting its organizational structure and work methods, ensuring the coordinated work of the Main Staffs of the services of the armed forces, the Staff of the Rear, the Staff of USSR Civil Defense, Chief and Central Directorates of the Ministry of Defense, Staffs of Military Districts, Groups of Forces, Air Defense Districts, and Fleets. The subsequent development of science and technology, and fundamental changes in the means, nature, and methods of conducting contemporary warfare have advanced the role of the General Staff in ensuring the reliable defense of the Soviet state, and have expanded and complicated the substance of its missions. The General Staff comprehensively analyzes and evaluates the military-political situation taking shape, determines the tendencies of development of the means of conducting warfare and the methods of their application, organizes training of the armed forces and execution of measures necessary for ensuring their high combat readiness to repulse any potential aggression. The further development of military theory occupies an important place in the activities of the General Staff. It directs military-scientific work, prepares major documents that prescribe regulations and deal with vital problems of Soviet military science, and inculcates its achievements in the practice of operational and combat training of troops and staffs. The combination of the restored centralization of leadership with regard for the initiatives of the subordinate organs of control, a high degree of readiness in the face of the necessity to switch over immediately to fulfilling wartime functions, and the scientific validity of the proposals and prepared decisions, are characteristic of the work of the General Staff. The widespread adoption of scientific organization of labor and of mathematical methods in the work of the General Staff, and the development of automated systems for controlling weapons and troops, permit the General Staff to resolve more effectively the complex problems involved in directing the armed forces in peace and wartime.

The General Staffs (or organs corresponding to them) of other socialist countries play an important role in the direction of the armed forces. Unlike the General Staffs of the imperialistic states, which are instruments of reactionary aggressive policy, the General Staffs of the socialist countries stand on guard, protecting the socialist achievements of their people. As in the USSR, they are organizationally a part of the Ministries of Defense (National Defense). The structure, role, and place of the General Staff in the system of military control ensure effective solution of all tasks concerning the training of national armed forces and permit directing their military operations in repulsing potential imperialistic aggression. For coordination of the activities of the Combined Armed Forces of the member states of the Warsaw Pact, a Staff of the Combined Armed Forces of those states has been established. (U)

(Translated text within double lines, unclassified; introductory analysis, ~~TSC~~)

HAS IT EVER BEEN TRANSLATED BEFORE?

(TRACKING DOWN TECHNICAL TRANSLATIONS)

[redacted]

H218

What would you do if you had what seemed to be an important book or magazine article in a language you couldn't read? How would you find out whether the book or article had been translated into English, and, if it had been, where you could get a copy of the translation?

Foreign-language books and articles contain a great deal of information important to the NSA researcher or analyst. Regular research and state-of-the-art questions can often be answered by reading reports by scientists and engineers working in other countries. [redacted] Since no one person can hope to be able to deal with all the languages in which valuable information might be published, translations are an important research source at NSA.

Who to Call at NSA

Now, then, how *do* you find a translation? Within the Agency, the major point of contact is T1213 -- the STINFO (Scientific-Technical Information) Services work center of the Library (Room 2N090, 5759s). This is the element responsible for locating a translation, if one exists. The Reference Collection in the Main Library, T1212/R (Room 2C051, 4169s) has some sources, such as commercial publications of indexing and abstracting services, and microfiche of the material translated by the U. S. Joint Publications Research Service (JPRS) and the Foreign Broadcast Information Service (FBIS). The Collateral Management and Product Repository, T124 (Room 2E040, 5669s) can often supply a document if the document serial number is known, [redacted]

Even if a translator or translation service is immediately available, getting a book or magazine article translated can often be very time-consuming. Moreover, it can also be very expensive. One author estimates that a translation can cost up to 100 times the price of obtaining the original. A reason for this is

ST. JEROME IN HIS STUDY, an engraving by the German artist Albrecht Dürer. Jerome, a biblical scholar of the fourth and fifth centuries, translated the Bible into Latin. His version, known as the Vulgate, is based on earlier Latin translations and on Greek and Hebrew sources. The lion is Jerome's symbol.

that the translator must be skilled in the subject matter of the document being translated, as well as skilled both in the "source" language (the original, or "from") language and the "target" (the desired, or "into") language. Because of the high cost, and because of the time and effort involved, no one wants to translate something that has already been translated.

Who Translates Foreign Literature?

Many organizations translate. JPRS is one of the major translation services in the U.S. government. It provides translations in many different languages and subject fields, and its products are well indexed. The translations are unclassified, although some are for government use only. The Air Force's Foreign Technology Division (FTD) translates in the scientific and technical realm. Plenum Publishing Corporation, Allerton Press, and Scripta Technica, Inc. are three commercial U.S. firms involved in translations. The American Institute of Physics does a number of translations of journals, as does the Optical Society of America.

Some translation agencies, whether U. S. government or commercial, publish cover-to-cover

EO 1.4.(c)
P.L. 86-36

translations of each issue of certain foreign scientific-technical journals. Other translation agencies, including commercial ones listed in the yellow pages all around the country, translate, on a contract basis, individual monographs, individual issues of a journal, individual articles, etc.

Strictly speaking, however, it is not the "translation agencies" that do the translating, but translators -- human beings. Some U. S. government and commercial agencies keep a small staff of permanent, "in-house" translators, but most of them rely heavily upon part-time, "contract" translators who provide translations as needed. Most in-house or contract translators are anonymous, but there is also a large number of "free-lance" translators, listed in various directories by their country of residence and by the foreign languages and technical areas they are competent in.

With the large number of government and commercial translation agencies, and the large number of translators, it is easy to see that the field is big and confused. And bibliographic control, or having things organized so that you can find what you're looking for, is far from perfect. In fact, it is hardly adequate. But there are some approaches to the problem.

Cover-to-Cover Translations

For the purpose of looking for a translation of a particular article, translations can be divided into two groups: ad hoc and cover-to-cover. Many articles are translated on an ad-hoc basis. That is, they are translated when someone wants a translation of just that particular foreign-language article. For some of the more important foreign scientific journals, however, there is a different approach. About 200 of these journals, mostly Soviet, are translated in entirety each time they are issued. These are the "cover-to-cover" translations. NSA subscribes to a number of the translations (as well as the foreign-language originals). Some are translated by commercial firms, and others are sponsored by professional organizations. Some are commercially viable, and others are heavily subsidized by the U. S. government. As a rule, the translated journals have the same date and volume and issue numbers as the original, which makes matching the original with its translation easier. The main problem with cover-to-cover translations is the time lag between the publication of the original and the appearance of the English translation: the lag can be anywhere from several months to more than a year.

There are several different ways to find out if a particular foreign journal is one of those translated cover-to-cover. The specialized indexing and abstracting services list journals included in their publications, and several of these lists, like those in *Mathematical Reviews* or *Science Abstracts*, indicate which journals are translated and what the English title is. Also, various lists of cover-to-cover translations are available. Since the field is so fluid, with translations beginning and ending all the time, these lists go out of date quickly. The International Translation Centre, which will be mentioned again later, regularly publishes a book called *Translations Journals* that includes this cover-to-cover information. *Translations Journals* also lists periodicals that have translations of articles from more than one source, and those periodicals that are originally published in various language editions. The book is available in the P16 Language Library (Room 3W076).

A somewhat less useful source of information on cover-to-cover translations is *Ulrich's International Periodicals Directory*. Ulrich's lists the source title in the case of a journal that is a translation, but there is no cross reference from the foreign-source title to the title of the cover-to-cover translations. A copy of Ulrich's is available in T1211 (Room B5113, FANX-III), and is also available in the Main Library (Room 2C051).

Ad Hoc Translations

Except for the time lag, articles that are published in journals translated cover-to-cover are no problem to track down. If you wait, the translation will eventually appear. The ad hoc translations -- those articles that were translated because someone wanted only them, rather than the entire journal -- are a completely different matter. They have to be tracked down, and the searcher usually isn't sure that what he's looking for even exists: maybe the article never *was* translated. We have several places here in the Agency where we can check, however, and they cover most of the possibilities.

One source of translation information that is available to government agencies is the Consolidated Translation Survey (CTS), housed at FBIS. CTS is a file of information on translations which are over five pages long and which were produced by U.S. government agencies and some commercial firms. The file includes all JPRS translations, limited distribution or not, that are over five pages long. The CTS coverage of other organizations depends on what they choose to report, although FBIS personnel say they seem to report most of what they translate. In the case of long translations, like books, CTS also lists things that are in process. This can prevent someone's starting a long and expensive translation of something that another agency might have close to completion. Items in the file are retrievable by author and original source title. FBIS doesn't stock copies of the documents, but will tell the requester how to get one. For security reasons, NSA doesn't input translations to CTS.

Commercial indexing and abstracting services are another access point for some translations. Most specialized indexing and abstracting services include items from foreign journals. The abstracts are usually in English, no matter what language the original

article was in, and in many cases the entry for a particular article notes the availability of translations or summaries in English. Sometimes a researcher doesn't actually need to read the translation of a whole article. Depending on how detailed it is, a summary or the abstract itself may contain enough information for the researcher. To make the lookup process easier, many abstracting services are now available as files in commercial on-line computer systems. NSA subscribes to one such system, Lockheed's DIALOG. The records are usually retrievable by author, source title, and subject, although specific details vary from one file to another.

In addition to the commercial abstracting services, DIALOG has another file that includes some translations. This is the National Technical Information Service (NTIS) file. NTIS is a clearinghouse for unclassified government reports and publications releasable to the general public. The translations listed include JPRS material. The same information can also be found in the hard-copy *Government Reports Announcements and Index* (GRA&I). The machine file available through DIALOG goes back to 1964.

Another data base NSA can access is CIRC II, which replaced a system called CIRCOL. CIRC (Central Information Retrieval and Control) is located at Wright-Patterson AFB, Ohio, and is a file of intelligence information that meets the needs of:

- the Air Force's Foreign Technology Division (FTD);
- the Army's Foreign Science and Technology Center (FSTC);
- the Naval Intelligence Support Center (NISC);
- the Medical Intelligence Information Agency (MIIA); and
- the Missile Intelligence Agency (MIA).

CIRC II emphasizes science and technology.

[redacted]

One of the files available through CIRC II -- XLAX -- is devoted exclusively to scientific-technical (S&T) translations. According to the CIRC manual, the primary use of XLAX is to determine whether a particular document has been translated.

Yet another on-line indexing system we can use is the Defense Research, Development, Test and Evaluation On-Line System of the Defense Documentation Center (DDC). DDC stores research and development information prepared and submitted by contractors working on Defense Department-related projects. There is also a hard-copy index to this material, the *Technical Abstract Bulletin* (TAB). The machine system has the same information as is listed in TAB. The documents in the DDC indexes, both the machine system and the hard-copy TAB, can be classified up through SECRET.

[redacted]

These machine systems -- DIALOG, CIRC II, and STINFO -- are all accessible through STINFO Services (Room 2N090, 5759s). The hard-copy indexes, for systems that have them, are also there.

So far we have dealt primarily with translations of journal articles, and of course the Agency is very interested in journal articles. New developments appear in journals first; it may be several years before a book is published on the subject. But journal articles aren't the only things that are translated.

Translations of Books

Books are often translated. One way we have to find information on translations of books is through the Ohio College Library Center (OCLC). OCLC is a data base of shared library cataloging information accessible through T1211. Translations entered into the system include the source title and are often accessible by way of both the original title and the translated title. The data base can also be queried with an author/title combination and, during certain hours, by author's name only.

The *National Union Catalog* (NUC), which is also available in T1211, is another source of information on translations of books. The NUC contains catalog entries of books and some other items processed by the Library of Congress and other major U.S. libraries. NUC entries, like the OCLC entries, mention the source title. Since neither OCLC nor the NUC is specifically designed as a source of information on translations, access is not as direct as might be desired. But the scope of these two sources is much more extensive than any others, and they are thus more likely to have information on translations of books than other sources.

In addition to OCLC and the NUC, translations of books are often included in the sources that concentrate on journal articles.

Translations of Newspaper Articles

Newspaper articles are also sometimes translated. FBIS publishes the *FBIS Daily Report*, which includes translations from foreign news-

papers and radio broadcasts. Some *Daily Report* translations -- those three pages or longer -- are entered into CTS. The print in the *Daily Report* is so small that the five-page limit usually imposed on CTS entries is waived. The *Daily Reports* for the USSR and the PRC are indexed quarterly in publications by NewsBank, Inc.: *Index to Daily Report: Soviet Union* and *Index to Daily Report: People's Republic of China.* These volumes are available in the Reference section of the Main Library. To search for possible translations in the *Daily Reports* for other areas, about the only method is to limit the search by area and date, and then scan tables of contents in appropriate issues.

In-House Translation Efforts

[redacted]

[redacted]

Machine Translation

One method of translation that received considerable publicity in the 1950s and 1960s

is machine translation. Machine translation is actually having a computer prepare a translation. There was to have been no difference in quality or style between a translation done by a machine and one done by a person. Georgetown University was very active in the field for some time. Progress wasn't as easy and rapid as had been anticipated, however, and in 1966 the Automatic Language Processing Advisory Committee published a report recommending that research along machine-translation lines be cut back. This report sharply curtailed federal funding. There is still, however, research being done both here and abroad, and there are several machine-translation systems that claim to be operational. One is the METEO project in Canada, which developed a system that translates weather reports from English into French. CULT (Chinese University Language Translator) in Hong Kong translates two periodicals into English. And a system was developed by a U.S. company for FTD and was adapted for use by NASA during the Apollo-Soyuz Test Project. These systems differ a great deal in their approach and in the amount of pre-editing and postediting that is necessary, but all are true machine-translation efforts.

At present, NSA has a rather limited machine-translation effort.

[redacted]

As machine translation stands today, we haven't reached the stage where we can feed a "source" (foreign-language) text into a computer and produce a text in the "target" (in our case, English) language which is as good as the human product, not without extensive pre-editing or postediting. But in the science and technology world, current machine translation has a place. Some scientists prefer it to the human product. To begin with, the machine product can be made much more quickly than the human product, and the time factor is very important in certain fields. Also, although machine translation is more difficult to read because of peculiar word choice and sentence structure, the translation is consistent. If a word is translated wrong, it will always be translated wrong, and the reader can make allowances. A human translator is liable to change his translation for a particular word, thus causing confusion. Of course, machines have difficulty distinguishing the different meanings a word can have in different contexts. It is difficult to program judgment or background experience into a computer.

National and International Cooperative Efforts

The realm of translation is indeed confusing and confused. There are too many people doing translations for too many reasons to make indexing easy. There have been attempts, however, to organize some of this chaos.

An unofficial agency in the United States is the National Translation Center (NTC), housed at the John Crerar Library in Chicago. It is the national depository for unpublished translations. These translations are produced by industry, government agencies, and universities. Until 1973, the NTC was supported with National Science Foundation funds. NTC produces an index to its holdings, called *Translations Register - Index*. At one time NSA subscribed to this publication, but we no longer receive it. It reported mostly ad-hoc translations that were rather dated and on subjects NSA is not concerned with. The people at this Agency who referred to it didn't find it useful.

There has also been some effort on an international level. The International Translations Centre (ITC), originally established in 1961 and called the European Translations Centre until recently, has this as one of its aims. The ITC, based in the Netherlands, collects information on translations from national centers and thus can refer requesters to the producer of a translation. ITC also keeps some translations itself, and will reproduce copies of these for a small fee. It produces an announcement of translations that are brought to its attention -- the *World Index of Scientific Translations*. NSA does not subscribe to the *World Index* for the same reasons mentioned with regard to the *Translations Register - Index*. The people who input to the CIRC II system, however, scan a number of publications for science and technology translations to be included in XLAX, and the *World Index* is one of these publications. To introduce some order into the cover-to-cover translation area, ITC also publishes *Translations Journals*, which was mentioned before. At present, ITC is limited to translations from eastern European and Asian languages into western European languages, primarily French, German, and English. ITC also concentrates on the science and technology field, but hopes to expand both field and languages before too long.

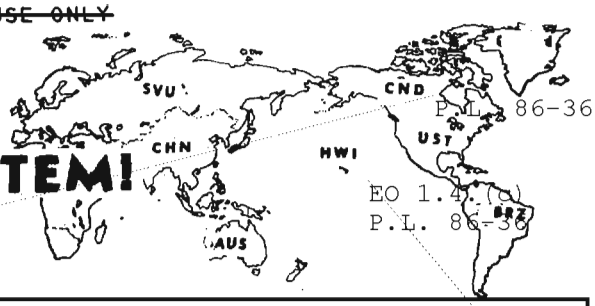
EO 1.4.(c) P.L. 86-36

Translations are indeed an important part of the collateral scene. They allow access to publications and documents that would otherwise be unusable, and they can therefore be very valuable. Since preparing translations is costly in both money and time, users of translations do not want to duplicate anyone else's efforts. This field is a prime one for cooperation. Of course, cooperation demands reference tools that allow access to what has been done, and, so far, the tools available in the translation realm are far from perfect. Translations are indexed along with other things; there are few sources devoted specifically to them. This can make searching for a particular translation frustrating. But the resources saved when a translation is found and thus not retranslated make the effort worthwhile.

~~FOR OFFICIAL USE ONLY~~

YE GADS! ANOTHER COUNTRY TRIGRAPH SYSTEM!

[redacted] T1221



P.L. 86-36
EO 1.4.(c)
P.L. 86-36

While working in the PLATFORM Network Information Center, we became aware of a need for a tool which would enable PLATFORM users to find out which files on the network might contain the information they sought. We identified three elements that such a tool should contain, based on the format "Someone/something from somewhere did something in some way to someone/something from somewhere at some place at some time":

Geographic
Subject/topic
Action/event

For example, "On 15 April 1978 the United States agreed to supply F-16 aircraft to Israel":

Geographic: U.S., Israel
Subject/topic: Aircraft
Action/event: Sales or supplying

Before being assigned to my current job, I had little experience with collateral or product, so I thought that all of NSA used the Country, Area, and Organization Digraphs in USSID 315. But as we began to pull NSA information together, we found that different NSA elements use a variety of geographic codes. Moreover, as we began to extend our search to find out what information was available elsewhere in the Intelligence Community,

[redacted]

At first we thought that it would be very easy to identify the geographic element -- isn't a country a country? The Content Control Code (CCC) trigraph seemed to be better than the Topic and Area Guide (TAG) digraph, as it added the information on the continental location of the country. As we considered how countries might be referenced, we also came up with the following classifications:

Aspect	*Example*
Physical	Middle East, Eastern Europe, etc.
Religious	Islamic, Hindu, etc.
Political	Communist, nonaligned, etc.
Economic	European Economic Community, Council for Mutual Economic Assistance, etc.
Military	NATO, Warsaw Pact, etc.

[redacted]

P.L. 86-36
EO 1.4.(c)

[redacted]

For many months I had been "thinking about" writing for CRYPTOLOG readers an article on the difficulties that the multiplicity of geographic and topical codes was causing the PLATFORM Network Information Center, but reading the words about [redacted] new "system" made me grab for my pen. I realize that NSA's individualism can be a great thing, as one person's exasperated statement that something is "impossible" becomes a challenge to another person, who then goes out and *does* the impossible. But that individualism can be harmful when it leads to a multiplicity of systems, some "official," some "semiofficial," and some "informal." One fine day we will have a computer network and will be able to use other people's files. As we input our machine queries for "China," how will we do it? By using CCH? Or CH only? Or CC or PRC? Or all of them? Or "none of the above," but something else that is being invented as I write these words?

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Frankly, any digraph or trigraph is all right for me, as long as it gives me the highest probability of finding the information I seek. Friends tell me it took the CONUS Group two years to agree on a standardized date form (out of an astronomic number of possibilities, such as 80731, 31JL78, 310778, 07318, etc.), so I should not be very optimistic about agreement on standardization of machinable codings to represent countries.

Does this have to be true? I hope not. Otherwise we are creating an intelligence Tower of Babel.

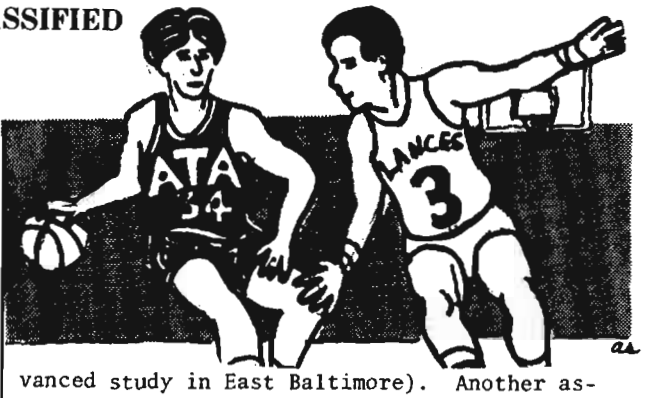
General Allen is alleged to have committed NSA/CSS to FIPS-10 codes within 5 years. I understand this has been retracted. Isn't there someone (or some group of people) who can start solving this problem now, before it reaches the "impossible" state? I think the "smarts" exist here to do it.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019651

IS A TRANSLATOR A PROFESSIONAL?

G53



Is a translator merely someone whose father or mother was born in the "old country"? Can a graduate of, say, a six-month intensive course in a language gain enough proficiency in the mechanics of that language to take upon himself the title of "professional"? Or is a university-trained linguist, for considerations of depth and duration of study, the only claimant to that title?

These and other associated questions were considered in the open forum "Definition of Translation As a Profession," at the convention of the American Translators Association (ATA). The participants were of a widely varied "professional" background:

- free-lance translators, clearly the dominant group in number, who work with texts running the gamut from children's stories to the applied sciences;
- "in-house" technical translators from U.S. and foreign industry, the most heavily represented being engineering firms and oil companies;
- a French/Italian translator from the World Bank;
- university professors and researchers, primarily involved with Russian, German, and the principal Romance languages;
- foreign-language dictionary and glossary publishers; and
- one Romanian intern from NSA.

Revelation: The National Security Agency is *not* the real world! We at NSA who are styled "linguists" (another title suggested for us has been "languagers") know our place. The terms "certified," "level three," "professional "linguist" mean something. The role of the NSA linguist is known to everyone here, at least in broad terms, so that no explanations are required. But out in the real, cash-on-the-barrelhead world of free-lance translation, the translator must at times deal with a special problem. His clients in American industry who, with the rapid onset of multinationalism, are only now beginning to rely routinely on translation services on an appreciable scale, are often ignorant of just who or what a translator really is. A common assumption on their part is that, if a person can translate Polish, he must *be* Polish (or at least have done advanced study in East Baltimore). Another assumption is that, if the translator understands English and a certain foreign language, he can easily put into that foreign language anything the client can say, no matter how technical. Free-lancers at the open forum gave examples such as the one in which an oilman with a knowledge of what "pump down and wireline" technology is all about, assumed that the translator would have a simple task in "making it say that in Yoruba." The fact that the oilman's African customers might be bemused to find, upon reading the contract in their own language, that American oilmen routinely stuff a "dog" (an actual piece of pump-down hardware in the lexicon of some U.S. companies) into an oil pipeline to open or close a valve is of no concern to the employer: it's the translator's problem. "Well, if it doesn't translate, then just describe it." Unfortunately, all the other companies dealing with the apparatus are also describing it, and everyone is probably doing so in a different way.

A National Certifying Agency for Translators?

It is clear that some vehicle to present the translator's case, some method to publicize his usefulness, to proselytize a little if need be, and to clarify his role to the consuming public does have its attractions. A monolithic agency (of the American Bar Association type) to set standards, guard ethics, and enfranchise practitioners would seem to be a ready answer. This proposition, in fact, became the core issue of "Definition of Translation as a Profession." Assuming that ATA, which already administers examinations in a number of languages at its conventions and enjoys representative membership in many areas of the field of translation, would be the proper body to manage the "profession" as such, the task then becomes to fix a title on a linguist that lucidly conveys something about competence, prestige, relative standing, etc. This, of course, has many ramifications -- "grandfathering" of a group to confer the title initially; prerequisites; effect of the title on salary; etc. NSA, with its structured certification system, has attacked the professionalization problem in a reasonably coherent way. In the unstructured world of the free-lance translator, however, a clear-cut definition of "professional" is appreciably more elusive. At the ATA forum it was the free-lancer, both in the role of proponent and of opponent, who proved the most vocal on this subject.

Report on an open forum entitled "Definition of Translation As a Profession," which was held at the 1977 annual convention of the American Translators Association, in Pittsburgh, Pennsylvania. The report was presented at NSA Fort Meade in December 1977 as part of a program jointly sponsored by the CLA's Special Interest Group on Translation (SIGTRAN) and the Special Interest Group on Lexicography (SIGLEX).

"Professional" Like a Basketball Player?

A free-lancer is, in the truest sense, a capitalist, an entrepreneur whose standard of living is directly proportionate to his linguistic competence, marketing aplomb, and, by no means least, his audacity in fee-setting. It is an intensely competitive field in which the individual must make it on his own. Successful translation over many years in scientific and technical fields may serve to enhance a reputation and facilitate the finding of profitable employment. One fundamental error in the translation of a valuable contract, however, can wreck a career. It was not in the least surprising, then, that the veteran free-lancers at the ATA forum, who had survived and prospered over the years without benefit of any sort of badge of professional standing to aid them in the market, reacted the most negatively to the concept of formal "professional" status for translators. Their "professionalism," they felt, is evident from their bank accounts. Just as a "professional" athlete (as distinct from an amateur) is one who derives his principal income from being an athlete, they feel, admittedly simplistically, that a "professional" translator is simply a person who derives his principal income from the act of translating. It must be pointed out that these experienced translators at the ATA forum were by no means playing semantical games with the term "professional." The same considerations that have often been expressed within NSA on the distinction between "technical" and "professional" levels (echoing the blue collar vs. white collar tension of the world at large) underlay their debate.

Reasons Why Novices Want Certification

By contrast, the novices in this same group, for the most part recent university graduates just entering the market, were the most outspoken in their support of an orderly system to identify and certify "professional" translators. Lured by the promises of independence, variety, and remuneration linked directly to skill and diligence, they were more than willing to submit to testing or any other form of objective comparison in order to dull the competitive edge of their more established colleagues. Success in a one-shot showdown of this sort was perceived of as an attractive circumvention of the protracted process of developing a "professional" reputation over many years. Show the certificate and the world will beat a path to your door!

Reasons Why Senior Free-Lancers Don't

The response of the senior free-lancers was simply to attack the entire proposal as presumptuous. The title "professional" itself, as applied in common parlance, is the privilege of, for example, a physician, one who has studied for long years to achieve his universally recognized occupational and social status. His years of study were the solitary route to his respected position. Such a title seems distinctly inapplicable to one who has acquired his skill through no more than an accident of birth. Doctors are not born, but a linguist may well be.

The veteran free-lancers also felt that the fruits of a formal certification program would simply not be commensurate with the effort required to put it into operation. They were understandably concerned with the inevitable pressure for tailored examinations to evaluate equitably both the translator of fairy tales and the translator of engineering specifications, and all those who fall in between them. They wished to know if professionalization would be based solely on testing. Would recalcitrants who shun participation be in some respect blackballed? Would a professionalization system make any earthly difference if the consumers of translations services are not persuaded to give it any credence, but instead choose to ignore the titles and other paraphernalia and continue to employ translators whom they have come to know and trust over a period of time?

Conclusion Drawn by Forum Participants

The conclusion of the forum was that there could be no conclusion. Beyond a feeling that one who lives by translation must be something like a professional already, the experienced translators participating did not foresee professional certification in the offing. The less experienced desired it earnestly. So far, at least, supply and demand has adequately served to advance the skilled and eliminate the rest. Professional standing at present is rooted in peer esteem, customer retention, and plain economics.

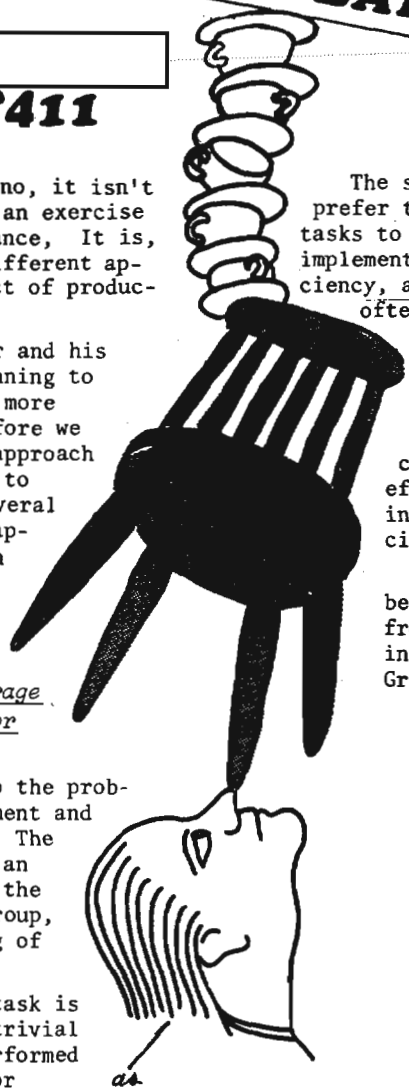
These senior translators, who represent the highest state of their art, needing no external endorsement to aid them and perhaps a little unwilling to risk besmirching a reputation by failing, as some must invariably fail, to qualify in an "objective" testing of the skills that have been their stock in trade for a lifetime, predictably resist. In their free-market environment, there is no practical way to impose certification. The novices, on the other hand, lack the clout necessary to force the issue. Many of them, experience has shown, will not be in the field for very long in any case, as attrition takes its toll. This is hardly the basis for a ground swell. Since the free-lancers are such a large group among all translators, both numerically and in influence, any certification system undertaken which ignores their specific needs is doomed to failure at the outset. Neither could it hope to secure the support of the consuming nontranslator public whose acceptance or rejection of the translator as a professional must, in the end, be determinative.

DOCID: 4019651

THE BUCKY BALANCE

P.L. 86-36

T411



The Bucky Balance -- no, it isn't a balancing act, or an exercise program, or a new dance, It is, however, a little different approach to the subject of productivity.

With the coming of Metzger and his design concepts, we are beginning to see the benefits of spending more time defining the project before we implement the system. This approach is very applicable to large- to medium-size projects with several people involved. This team approach has not, however, been applied to the smaller projects that have traditionally been assigned to one individual.

What Can Be Done for the Average Worker in the Small Project or Task Area?

This paper is addressed to the problem of small projects management and help for the average worker. The success of small projects in an organization is important to the overall achievement of the group, in addition to the well-being of each worker.

Definition: A project or task is a unit of nontrivial work to be performed by one, two, or more workers.

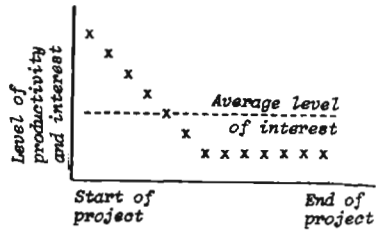
I suggest that within organizations there exist two distinct subgroups of workers.

Individuals in the first group are known as Project Starters. The Project Starter prefers to be given general guidelines for a project, then left alone to do his own design effort. The Project Starter's interest level is highest at the beginning of the project and declines as the major project decisions have been made. Graph 1 shows the interest level plotted against time spent. It is also felt that a worker's productivity is directly related to his interest in what he is doing. His interest centers around planning and designing how the task should be done. He is always trying new and sometimes farfetched ideas.

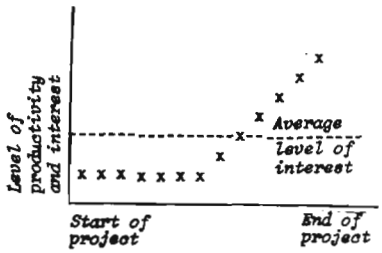
This paper was presented at the 1977 Spring Conference of NSA's Computer and Information Sciences Institute (CISI), where its author won Third Place in the Conference Awards.

The second group, the Project Finishers, prefer to be given specific, well-defined tasks to perform. Their interests involve implementation techniques, operation, efficiency, and testing. The Project Finisher often has problems getting started but, with a little help, usually makes a strong finish. Graph 2 shows the interest and productivity of a Project Finisher plotted against the degree of completion of a project. Of course, there are some workers who are efficient at both starting and finishing, and probably a few who are efficient at neither.

Traditionally, the entire project has been assigned to an individual to do from start to finish. His productivity/interest level will resemble either Graph 1 or Graph 2.



Graph 1



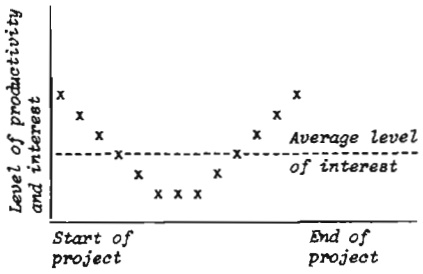
Graph 2

Theorem: The average level of productivity on a given project can be improved by pairing a Project Starter with a Project Finisher, using a division of labor. This pairing is called complementary couplet.

Graph 3 shows the productivity/interest levels of a complementary couplet plotted against the degree of completion of a project.

In order for the complementary couplet theory to be effective, the manager must be able to identify the Project Starters and Project Finishers in his group. There must also be well-

defined procedures for transferring a project from a Starter to a Finisher.



Graph 3

How to Distinguish a Project Starter from a Project Finisher

Helpful hint: The best way to spot a Project Starter or a Project Finisher is to observe the person's working habits closely.

Theorem: The Project Starter is *interrupt-driven.*

The Project Starter will begin work on Task 1. When given Task 2 to do, he immediately drops Task 1 by putting it in his hold tray or dropping it in his bottom drawer. He then starts Task 2. If he is interrupted with another job, Task 3, he pushes Task 2 onto his hold stack and starts Task 3. If uninterrupted for a sufficient length of time, he may actually complete Task 3. He will then pop-up Task 2 from the stack and resume work on it. If interrupted with Task 4, back to the stack for Task 2, and so on. Every task that he is assigned gets a higher priority than the one before. He operates on a last-in-first-out basis. Most Project Starters have at least one uncompleted project stashed in the bottom drawer that has been sitting there since they came into the office.

Theorem: The Project Finisher functions as a *first-in-first-out* queue.

The Project Finisher prefers to work on a one-task-at-a-time basis. The Project Finisher will not start Task 2 until Task 2 is completed. His hold tray is empty but tasks to be done are piling up in his in-basket. He will get to each task as soon as the previous task is complete. Every task that enters his queue comes in at the lowest priority. He takes his task in first-in-first-out order.

General Characteristics

You would be more likely to find a Project Starter organizing meetings or planning sessions. He is usually outspoken and advocates change.

Project Finishers are much better at documentation. They probably have authored many office bulletins describing how to use their completed projects. In programming projects, their software has been tested better and is more bug-free than comparable software written by Project Starters. Project Finishers are more concerned with details and prefer the status-quo methods to new techniques.

How to Get a Project from a Project Starter to a Project Finisher

One of the most important aspects of the Bucky Balance is an orderly, well-defined procedure for transference of a project from a Starter to a Finisher.

Definition: A project is in a suspend state when it is not being worked on actively.

The status of a project should always be recorded and filed in the Project Status Record before the project is suspended. For example, the Project Status Record for a programming project should minimally include current listings of:

- programs,
- run streams,
- reference documents,
- problem specifications,
- narrative documentation, and
- data-flow analysis.

It is very important that the Project Starter and the Project Finisher come to an agreement on project conventions when work begins. Project conventions on a programming project might include what language to program in, whether to use structured design and programming techniques, or which system to use for the project. Some of these decisions may be dictated by the specification of the project itself. However, when convention decisions are made that will affect the way the entire project has to be done, then this decision should be a joint one between the Starter and the Finisher.

The Project Status Record is the link between the Starter and the Finisher. For a programming project, the specification should include the requirements, a general concepts paper, and a detailed design, as well as general test procedures. Often the testing ideas are conceived during the design stage but, unfortunately, are not documented. Thus by the time they are needed, they have been forgotten and must be thought out again. Including ideas on testing in the Project Status Record will benefit the Finisher when he implements the testing package.

Having current listings of programs and run streams are common sense as well as good procedure. It's difficult enough to take over a program from another worker without the additional problem of searching for the latest updates or patches.

The reference documents are important also. Sometimes the Finisher needs more information than is provided in the Problem Specification. The reference documents or manuals provide the basis of general information concerning the project.

The narrative documentation should reflect the Starter's design philosophy, as well as specific technical information. This has been a brief description of the Project Status Record for a programming project. The Project Status Record would be somewhat different for a hardware acquisition project or an educational course set-up project.

Theorem: A suspended project can efficiently be restarted by a Project Starter or a Project Finisher if the Project Status Record is well-defined.

Note: A project need not be suspended before it can be transferred. It is necessary, however, for the Project Status record to be current.

Use of the Project Status Record can also help the Project Starter when he picks up the job that has been in his stack for a long time.

Here is a short quiz. The answer choices are neither right nor wrong, but do illustrate the difference in attitude between the Project Starter and the Project Finisher. The "a" answers reflect the Finisher's point of view, while the "b" responses reflect the Starter's preferences.

QUIZ

1. You are given a new project to do. You would rather:

   a [] Do it the same way you've always done your projects. Even though it's tedious, you know it works. Punching your program on cards that you can keep with you is safer than using a scope.

   b [] Try the new structured programming in the nude approach you've been reading about that might save time or be a better way. At least in the summer it would be cooler.

2. Given a new task to do:

   a [] You'd rather do anything than make an important decision. If you didn't make the decision, then you can't be blamed if it doesn't work.

   b [] You want to make all the decisions, from what language to use to what color cards to punch your program on.

3. You receive a phone call from a grumbling user, stating that option Q on your dandy list program isn't working. What do you do?

   a [] You tell him to submit it in writing with two box tops from his favorite cereal and you will get around to looking at it when you are finished doing the three other tasks you have been assigned. That should be 3 weeks from next Tuesday.

   b [] You tell him to bring the dump down immediately. So what if the project you are currently working on has a deadline of yesterday? This new problem sounds more interesting.

How to Motivate Project Starters and Project Finishers

Theorem: Project Starters are *challenge-motivated.*

The Project Starter is excited by the new and unknown aspects of the project. He is determined to conquer the problem and all obstacles in his path. The challenge lies in determining just how all the pieces will work together, rather than in seeing it actually perform as designed. The Project Starter enjoys learning new things and does best on projects that offer this kind of challenge.

Theorem: Project Finishers are *satisfaction-motivated.*

The Project Finisher takes pride in a job well done. He enjoys working on the details. He needs to be appreciated for his efforts and gets satisfaction from seeing all the pieces perform optimally.

The Project Finisher is procedure-oriented and would prefer to use established methods and already acquired skills to perform his tasks.

How to Manage Project Starters and Project Finishers

A manager has certain responsibilities for the well-being of all his workers. He should try to uphold the worker's "Bill of Rights," which include the following:

visibility - Project Starters and Project Finishers both have the right to visibility to their immediate supervisor as well as higher-level management on at least one project they are assigned to. The Project Status Record can help bring achievements and progress to the attention of management.

worthwhile assignments - Project Starters and Project Finishers have the right to feel that the work they are doing is productive and useful and, in general, worth doing.

praise - Project Starters and Project Finishers have the right to be praised and noticed for jobs well done.

constructive criticism - Project Starters and Project Finishers have the right to be constructively criticized and advised about their performance by an informed manager.

project review - Project Starters and Project Finishers both have the right for periodic reviews of on-going projects to reevaluate priorities and progress. Review of the Project Status Record can be an aid to the worker as well as to the manager.

In addition to supporting the above "Rights," the manager must also be a sounding board to his Starters and a guiding light to his Finishers.

The manager should listen to the many ideas of the Project Starter -- helping him to select the better ones and to reject the unworkable ones. He should guide the Project Finishers and help point them in the right direction, making sure that each Project Finisher knows exactly what is expected of him and all that the task entails.

Managers should realize the difference in Project Starters and Project Finishers and use this difference to the good advantage of the project. Job performance evaluations should also take into consideration whether a Starter or Finisher is being evaluated, and criteria for evaluation should be developed for each.

The success of small projects in an office contributes significantly to the overall office morale. The productivity level of the workers can be increased by pairing a Project Starter and a Project Finisher on the same project. I hope that some trial projects will be monitored using the Bucky Balance approach so that the validity of my theorems can be proven.

Being a Project Starter myself, it has been very difficult to finish this paper. So in conclusion. . .

(U)

TELL ME I'M JUST A SINOBIBLIO-PHOBE!

R51

P.L. 86-36

Afraid of a *book?* Who could be afraid of a book? Why, even the dictionary definition of "bibliophobia," which one might expect to be "fear of books," turns out to be "strong dislike of books." No one is frightened by a book!

Except me! I've just been looking through a Chinese mathematics textbook that was published in Peking in 1976. It's a two-volume paperback edition (about 300 pages per volume), the translated title of which is *Fundamentals of Engineering Mathematics*. The book was written by an unnamed group of authors. In the preface they cite various works by what would appear at first glance to be two people with the same last name (both names are spelled with the same three Chinese characters). But the first one soon proves to be Karl Marx, and the other one, the person whom the authors have chosen as their pedagogical model, would appear to be Robert W. Marks.

The NSA Main Library has a copy of Robert W. Marks' book *The New Mathematics Dictionary and Handbook* (call number QA5: M34). To quote from the Preface to the Marks book,

> "The keynote of this text is clarity -- without sacrifice of authority and definitional precision. All definitions are simple and stand as independent units of explanation. They are meaningful to every reader of average background whether or not he has had prior experience with any form of mathematics beyond the elementary level."

The Chinese text goes beyond Marks in several directions. At the low end, it begins at an ultra-elementary level. Its first theorem (p. 7) asserts that the sum of the interior angles of a triangle equal 180°. Only a few pages later it gives the basic arithmetic properties, i.e., commutativity, transitivity,

and distributivity. Two pages later it defines "coefficients" (by underlining the two relevant Chinese characters). Throughout the two volumes a goodly portion of each page is taken by illustrations (charts, graphs, drawings) and detailed implementation of calculations for the numerous examples. As promised in the Preface, each of the fourteen chapters begins with an outline of its contents and ends with a brief concluding statement.

This latter promise, ending the second of the Preface's five paragraphs, is preceded by an offhand remark that the arrangement of the text is designed for the convenience, and ease of comprehension, of the worker-peasant-soldier student in his *self-study* (i.e., teacherless) attack on the material. It was at this point that I began to feel frightened. If any significant number of those worker-peasant-soldier students self-studied their way through that 1976 textbook, the present technological advantage of the United States (and of the USSR) might not remain so overwhelming all through the foreseeable future.

To give just the flavor of the textbook, let me list the titles of the fourteen chapters and the two annexes. I mention in passing that each chapter contains several "problem-exercise sections," the "solution-answers" to which are printed at the end of the volume in which the chapter appears. Also, each chapter ends with its labeled Postscript. Here I furnish just the titles of the fourteen chapters and the two annexes (with their first-page numbers in the Chinese text):

Volume I

Chapter		Page
1	Basic Information on Forms and Numbers	1
2	First-Degree Equations; Direct and Inverse Proportion	28
3	Trigonometric Ratio (Side, Angle) Calculations	87
4	Algebraic Operations	134
5	Curves and Quadratic Equations	188
6	Functions	237
7	Derivatives and Definite Integrals	263
Answers		313

Volume II

Chapter		
8	Exponential and Logarithm Functions	1
9	Trigonometric Functions	31
10	Differential Calculus	81
11	Integral Calculus	143
12	Differential Equations	194
13	Series	229
14	Algorithmic Language Introduction	281
Annex		
I	Complex Numbers	335
II	Matrices and Simultaneous Linear Equations	354
Answers		402

A few footnotes to the foregoing. The first ten pages of Chapter 14 only introduce the subject of an algorithmic language (avowedly derived from ALGOL-60) after broaching, in some detail, the question of electronic digital computers, very major attention being given to the [IBM] 709 computer (vintage 1957) and the domestic mainland-Chinese TQ-16 (48-bit word, 32K memory, what looks like punched paper tape for input-output operations). About half the problems for Chapter 14 (answered on pp. 418-421) are answered by ALGOL-like responses. Moreover, the last subsection of Annex II is devoted to a listing, with adequate exegesis, of a computer procedure for implementation of the Seidel simple iterative method of solving simultaneous linear equations.

That second annex begins with determinants and ends with simultaneous linear equations. In between, of course, are matrices (pp. 362-376). The compilers of the textbook, in introducing matrices, hark back in Chinese history to the first-century "Nine Chapters of Arithmetic," where, according to the twentieth-century Chinese historian Ch'ien Pao-ts'ung, matrix methods were first used in solving simultaneous linear equations. In his book, the translated title of which is *The History of Mathematics in China* (call number AQ 27.C5: CY3), any cryptologic mathematician, however lacking in Chinese literacy, can follow, on pp. 52-54, the solution process with the attendant abacus-like notation.

Please let me know if I shouldn't feel frightened. (U)

Solution to NSA-crostic No. 15

By A.J.S. (CRYPTOLOG, June 1978)

Sydney Fairbanks, "Editorial Comment," *NSA Technical Journal*, October 1957. Reprinted in *Collected Editorials of Sydney Fairbanks [1956-1959]*, *NSA Technical Journal* Special Issue, December 1966.

"If we were one having authority, saying to one man Spell, and he spelleth, and to another Punctuate, and he punctuateth, we would issue a decree that no sentence could start with 'however' or 'therefore', -- and then sit back and listen in grim glee while the typewriters stopped and silence settled in the corridors." (U)

DOCID: 4019651

NSA-crostic No. 16

by guest NSA-crostician
David H. Williams, P16

The quotation on the next page was taken from a published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS

A. ---- Capp

B. Band leader's first name; comedian's last name

C. Followed by Word D, why the keeper, carrying a sack of sea birds he intended to feed the zoo's dolphins as an aphrodisiac, was arrested by a federal agent as he stepped over Tarzan and Jane (the zoo's mascots, completedly tame, sedate jungle cats), who were sleeping on the steps (9 wds)

D. See Word C (6 wds)

E. The novel Steinbeck never wrote about the venetian blind industry (4 wds)

F. NSA career field (2 wds)

G. Fertile, green; drunkard

H. Professional tennis star (full name)

I. Tossed

J. French acknowledgement of a hit

K. Displayed clearly

L. Amend; improve

M. Regis ------

N. "Are you ---?" (antepunchline)

O. Thirst quencher in Boston: "a boddle-a -----"

WORDS

218	6	143	44										
88	102	63	27	96									
100	176	189	180	89	127	144	209	109	162	155	39	80	133
26	76	10	205	110	198	152	193	68	29	14	136	22	
46	113	167	60	3	34	214	13	220	37	95	18	52	
141	202	41	134	101	90	75	170	165	181	221	86	11	117
74	4	184	148	91	16	45	38	128	164	50	168	158	
55	30	70	212	28	197								
196	153	150	130	138	83	47	105	61	199	187	163	17	7
217													
161	142	9	186	25	5	216	54	129	108	173	194	135	19
151													
82	126	160	206										
211	104	36	33	191	92	40	157	12	67	213	20	120	87
223	172	185	200	114	53	77							
156	147	204	207	8									
183	73	121	43	107	112								
132	64	154	21	58	32	145							
103	79	35	166	93	1								
97	15	51	115	94	131								
98	72	215											
123	116	171	85	140									

DOCID: 4019651

P. "Tales of --------"

124 57 119 177 31 192 149 222

Q. Produce a picture or design by chemical action

59 106 146 111

R. Palindromic body part

182 159 203

S. "The ----- Dozen"

175 62 56 208 2

T. Poem by Kipling

65 137

U. Delicious; attractive

84 125 99 118 23 195 66 179 139

V. External

71 81 169 24 48

W. "Retain our men"

78 201 210 174 219 178 122 190 69 188 49 42

1 L	2 S		3 C	4 D	5 F	6 A	7 E		8 I	9 F	10 C		11 D	12 H	13 C
	14 C	15 M		16 D	17 E	18 C	19 F	20 H	21 K		22 C	23 U	24 V		25 F
26 C	27 B	28 D		29 C	30 D	31 D	32 K	33 H		34 C	35 L		36 H	37 C	38 D
	39 C	40 H	41 D	42 W	43 J	44 A		45 D	46 C		47 E	48 V	49 W	50 D	51 M
52 C	53 H		54 F		55 D	56 S	57 P	58 K	59 Q	60 C	61 E		62 S	63 B	
64 K	65 T	66 U	67 H	68 C	69 W	70 D	71 V	72 N		73 J	74 D		75 D	76 C	77 H
	78 W	79 L	80 C	81 V	82 G	83 E	84 U	85 O	86 D	87 H		88 B	89 C	90 D	
91 D	92 H	93 L	94 M	95 C	96 B		97 M	98 N		99 U	100 C	101 D	102 B	103 L	104 H
105 E		106 Q	107 J	108 F	109 C		110 C	111 Q	112 J		113 C	114 H	115 M	116 D	117 D
118 U		119 P	120 H	121 J	122 W		123 O	124 P	125 U	126 G	127 C	128 D	129 F	130 E	
131 M	132 K	133 C	134 D	135 F		136 C	137 T		138 E	139 U	140 O	141 D	142 F	143 A	144 C
145 K		146 Q	147 I	148 D	149 P	150 E	151 F	152 C		153 E	154 K	155 C	156 I	157 H	158 D
159 R		160 G	161 F	162 C	163 E	164 D		165 D	166 L		167 C	168 D	169 V		170 D
171 O	172 H	173 F	174 W	175 S	176 C		177 P	178 W	179 U	180 C	181 D	182 R		183 J	184 D
185 H	186 F	187 E	188 W	189 C		190 W	191 H	192 P	193 C	194 F	195 U	196 E	197 D		198 C
199 E	200 H	201 W	202 D	203 R	204 I		205 C	206 G	207 I		208 S	209 C	210 W	211 H	212 D
	213 H	214 C	215 N		216 F	217 E	218 A	219 W	220 C	221 D	222 P	223 H			D.H.W

(Solution next month)

DOCID: 4019651

News of the Communications Analysis Association

Our able CAA correspondent, [redacted] (P14), was wending his way through "the field" when this month's CRYPTOLOG was put to bed. Wayne is, among other things, spreading copies of CRYPTOLOG and information on the CAA among our field colleagues, a la Johnny Appleseed, in the hope that readership and interest in the activities of the CAA will flourish. He has reluctantly consented to yield his pen this month to Dave Gaddy.

(U)

The Compleat Analyst

Over the past year the CAA leadership has been exploring ways in which the Association might assist in developing a new breed, tentatively known as a "communications analyst." The germ of the idea lay in the perception that the challenge facing us today and in the foreseeable future is not one for the "conventional" disciplines of past decades, but one in which traditional distinctions have become blurred. A more versatile, better-trained analyst is required. The same sort of motivation has led to a reconsideration of NSA's COSC structure and to a reexamination of workforce development on the part of DDM. The main question is, what, if anything, CAA can usefully do through -- and for -- its membership.

Some of us (including the Director, it would seem) believe that CAA does have a role. One of our goals is professional growth. Our span encompasses the broad field of "communications analysis," both SIGINT and COMSEC. Our membership comprises some first-class craftsmen (craftspersons?). We can't avoid being concerned. But what can we do?

One suggestion centers on professionalization: for example, offering voluntary assistance on the part of CAA members to aspirants in the related career fields. Is "the compleat analyst" a multiprofessionalized analyst -- necessarily? Is full professionalization of the analytical workforce desirable? Is "the compleat analyst" a stage beyond even multi-ticket professionalization? Is it a "postgraduate" accomplishment? "What's in it for me" in terms of promotion or advancement? Is it a personal thing, or is it a recognized "plus" for the record?

That one suggestion illustrates the complexity of the problem (or is it the fuzziness of the objective?).

Our former president, [redacted] continues to be interested in this subject, as are [redacted] Dan Buckley (M). They, or, for that matter, the Board members individually or as a group, would welcome your views on the subject.

~~(C-CCO)~~

Branching Out

P.L. 86-36

One of our objectives for this year is to bring more military analysts into CAA, which, in turn, leads to finding ways of making CAA more useful to them. The Agency's senior enlisted man [redacted] met with the Board of Governors in March, and, at the request of his successor, [redacted], the CAA president met with the Senior Enlisted Advisory Council in May to explain the purpose and goals of the Association.

In a related vein, we have received several proposals for field chapters, perhaps at the SCA headquarters, regional offices and installations. We will be considering ways in which we can support field activities and welcome additional views on the subject.

~~(TSUSI)~~

CAA Programs

The Special Interest Group on Cryptologic History spent a delightful time with P. William (Bill) Filby, reminiscing on "Bletchley in the Steam Days." A highlight for the year was the Director's May address in the Auditorium, "Is There a Future for the CAA?" (The answer associated the goals of the CAA with the future needs of the U.S. SIGINT System as seen by its Chief.) Our June speaker is Dr. Clint Brooks of W, with the mind-stretching subject "Interstellar SIGINT."

~~(C-CCO)~~

Meet the Treasurer. . . Please!

[redacted], our treasurer, also spends a considerable amount of time as a Cryptologic Staff Officer on the B Group Operations Staff. Tim earned his BA in English (1960) and his MA in International Relations (1970) at Georgetown University.

Tim started his cryptologic career with the Communications Intelligence Officer Course at Goodfellow AFB in 1962, followed by the CY-100 course at NSA. He served a tour with the Air Force in Germany, followed by a year in Saigon and a year in Washington on the Air Staff. He started his career at NSA in 1968, and has been with B Group since then, except for one year with the Army at Vint Hill Farms Station. He is certified as a Traffic Analyst, Research Analyst, and Collection Management Officer.

P.S. If you haven't joined CAA, Tim will also gladly exchange your worn and tattered dollar bill for a nice, new membership card.

~~(TSUSI)~~

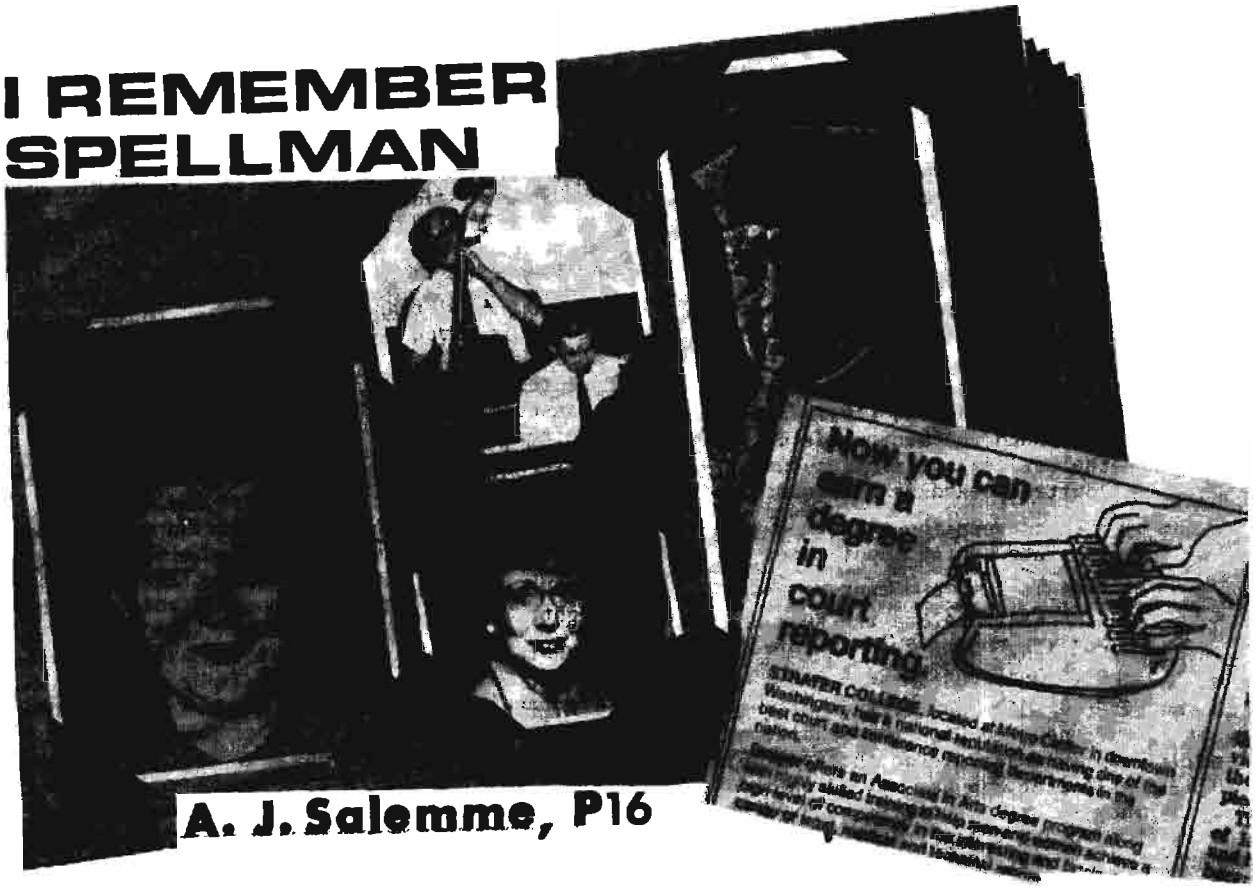
Board of Governors, CAA:

President	David Gaddy	3247
President-elect	Frank Porrino	5879
Secretary	[redacted]	8025
Treasurer		3791
Board members		4935
		5991
		3575
		3369

 P.L. 86-36

DOCID: 4019651

I REMEMBER SPELLMAN



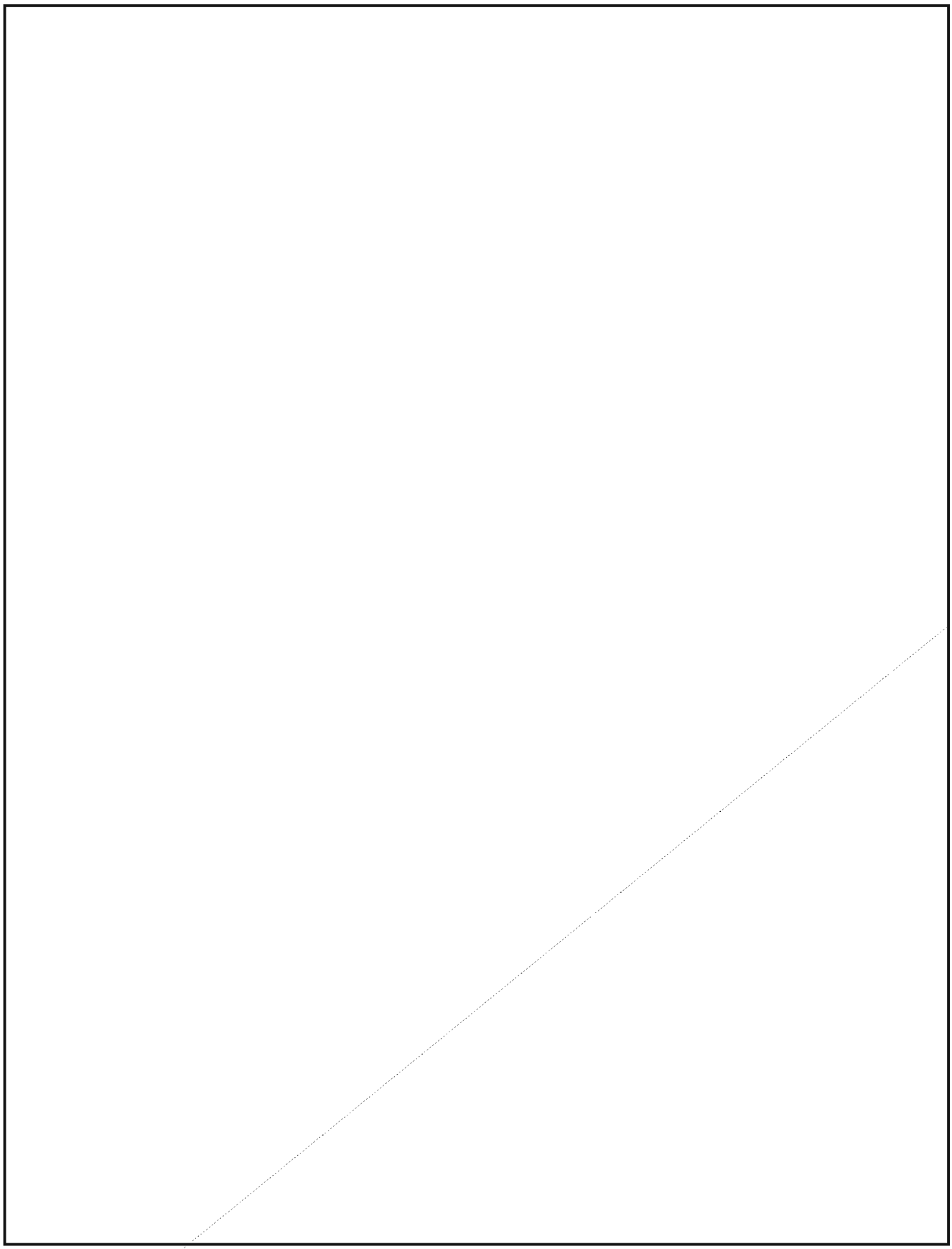
A. J. Salemme, P16

Yes, I remember SPELLMAN! Not Congresswoman Gladys Noon Spellman, of Maryland's 5th District -- her I've never met. Nor do I mean the late William Cardinal Spellman -- *him I never met either*, although I often wished I had, if only to ask him if he indeed began wearing a large S under his vestments when he learned that Japanese press reports of his visits to U.S. troops during the *Korean War* spelled his name, in Romanized form, "Superuman." No, what I mean is *Project* SPELLMAN! It was the project that Jack Gurin referred to in last month's CRYPTOLOG when he said, "I had a file of papers, the only one of its kind, relating to an experiment which had been conducted in an attempt to improve our processing techniques." Jack went on to say that, despite his best efforts to preserve all the information pertaining to that experiment, it had all been thrown away. Well, I was one of the people involved in one phase of that experiment, and I still have strong impressions of it, more than 17 years later. I feel that the best way to reconstitute the general impression about the project (if not the specific details, such as how many hours Student A spent on such and such a day copying Tape 1) is to ask the various participants to tell their version of the story. It could be a kind of "NSA Rashomon," like the movie, based on a traditional Japanese folk tale, in which the same event is described separately, and oh how differently, by each participant -- the husband, the wife, the bandit chief, the casual passerby, etc.

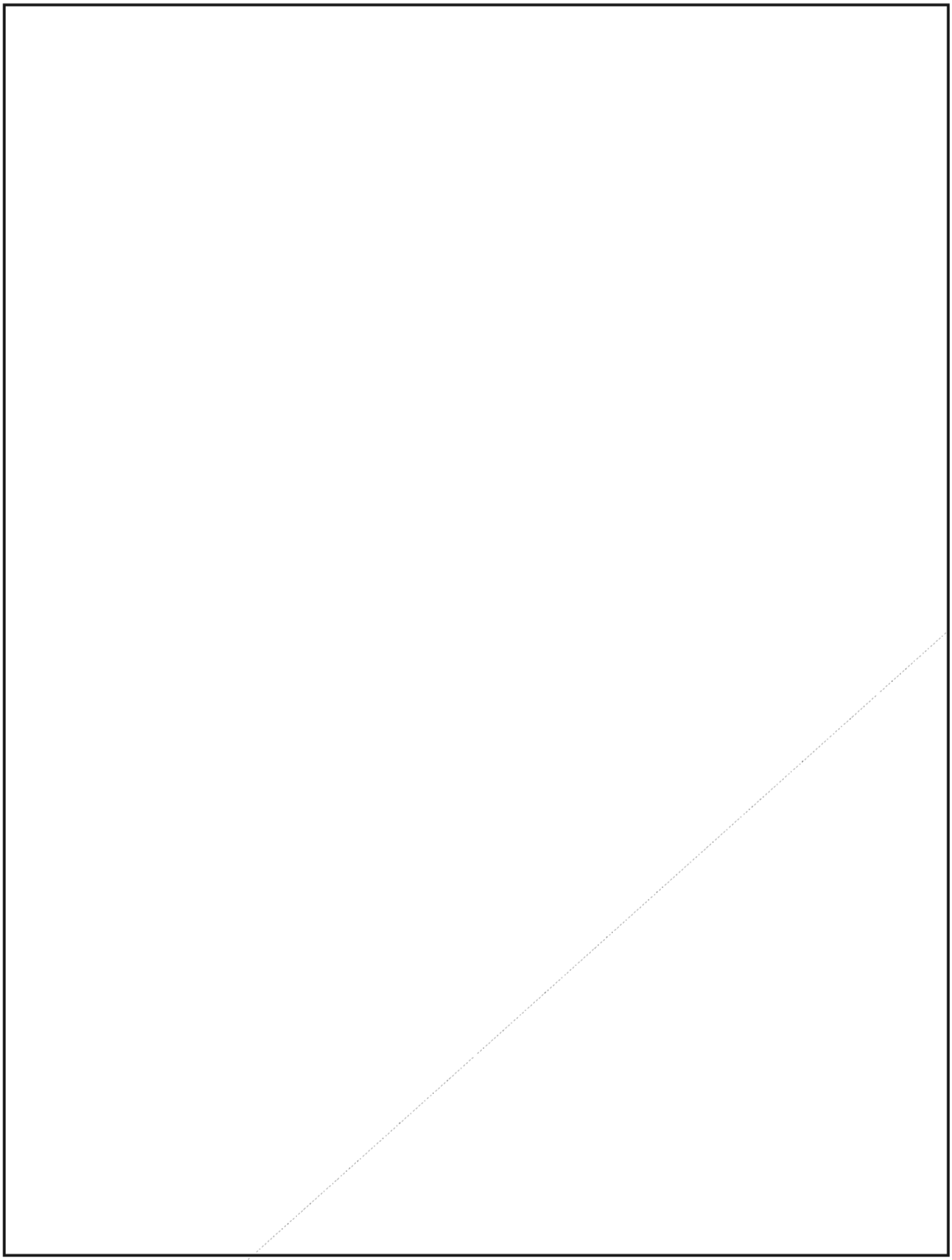
So, professor, a little samisen music, if you please. . .

EO 1.4.(c)
P.L. 86-36

~~HANDLE VIA COMINT CHANNELS ONLY~~

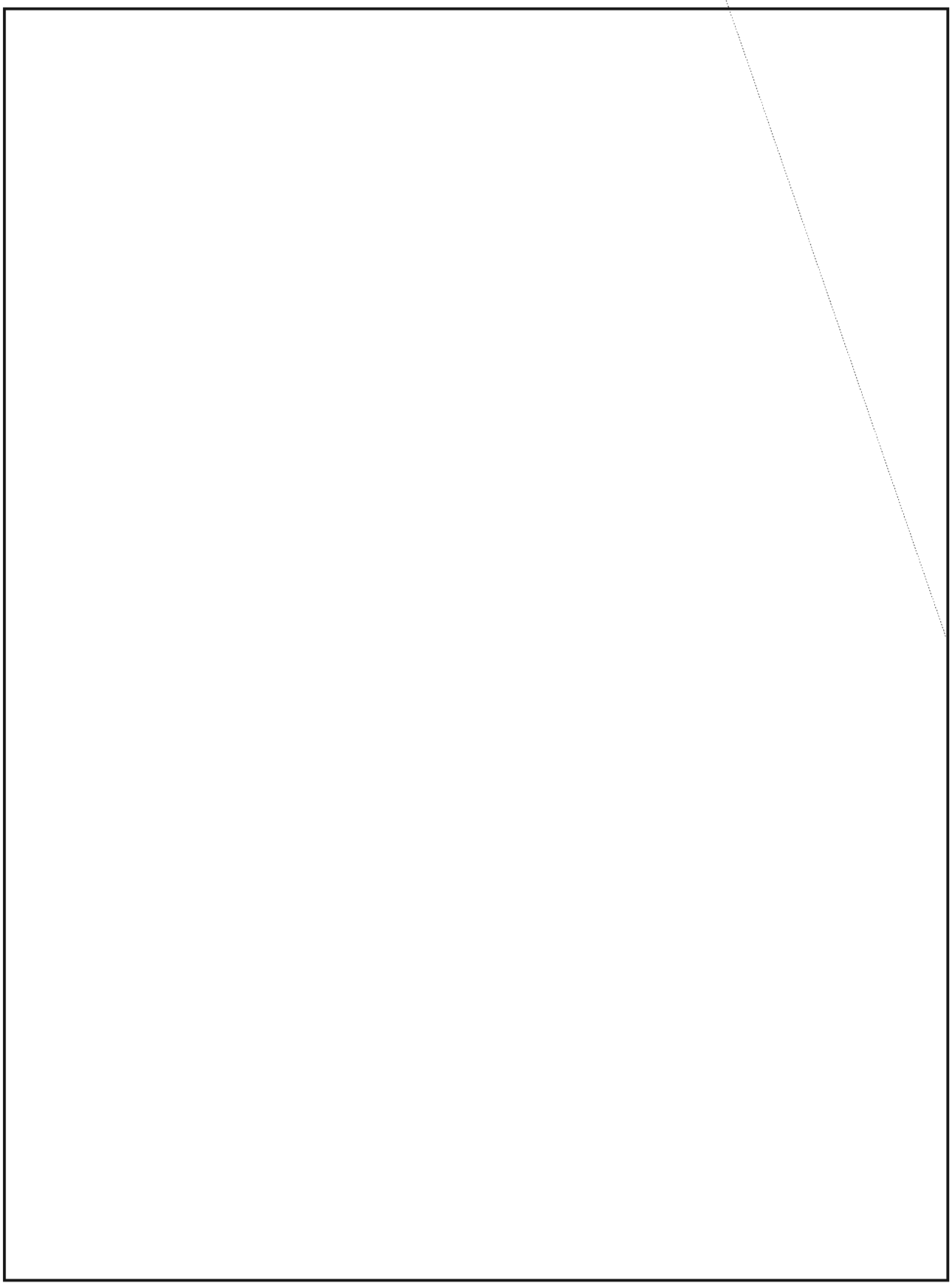


EO 1.4.(c)
P.L. 86-36



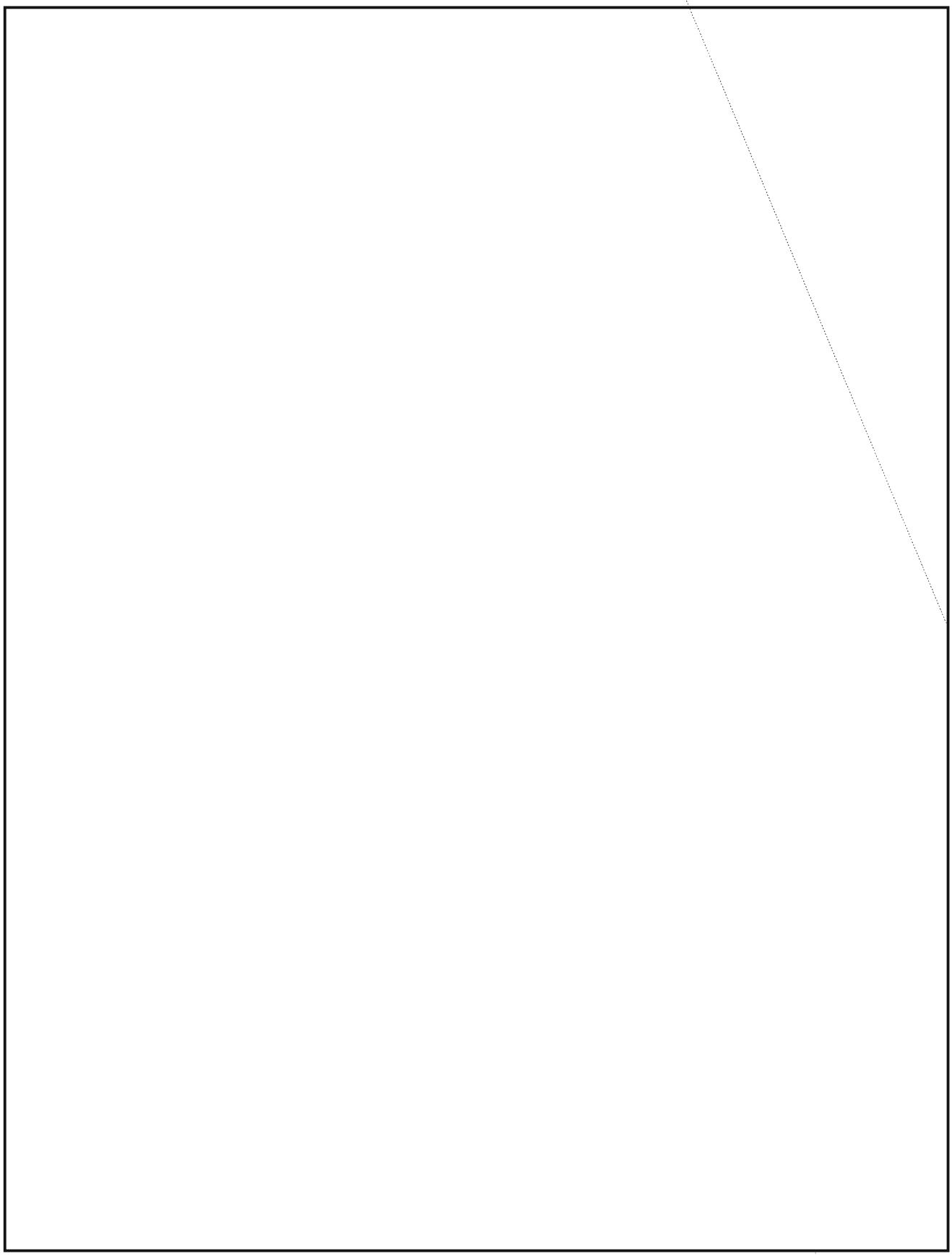
EO 1.4.(c)
P.L. 86-36

E0 1.4.(c)
P.L. 86-36



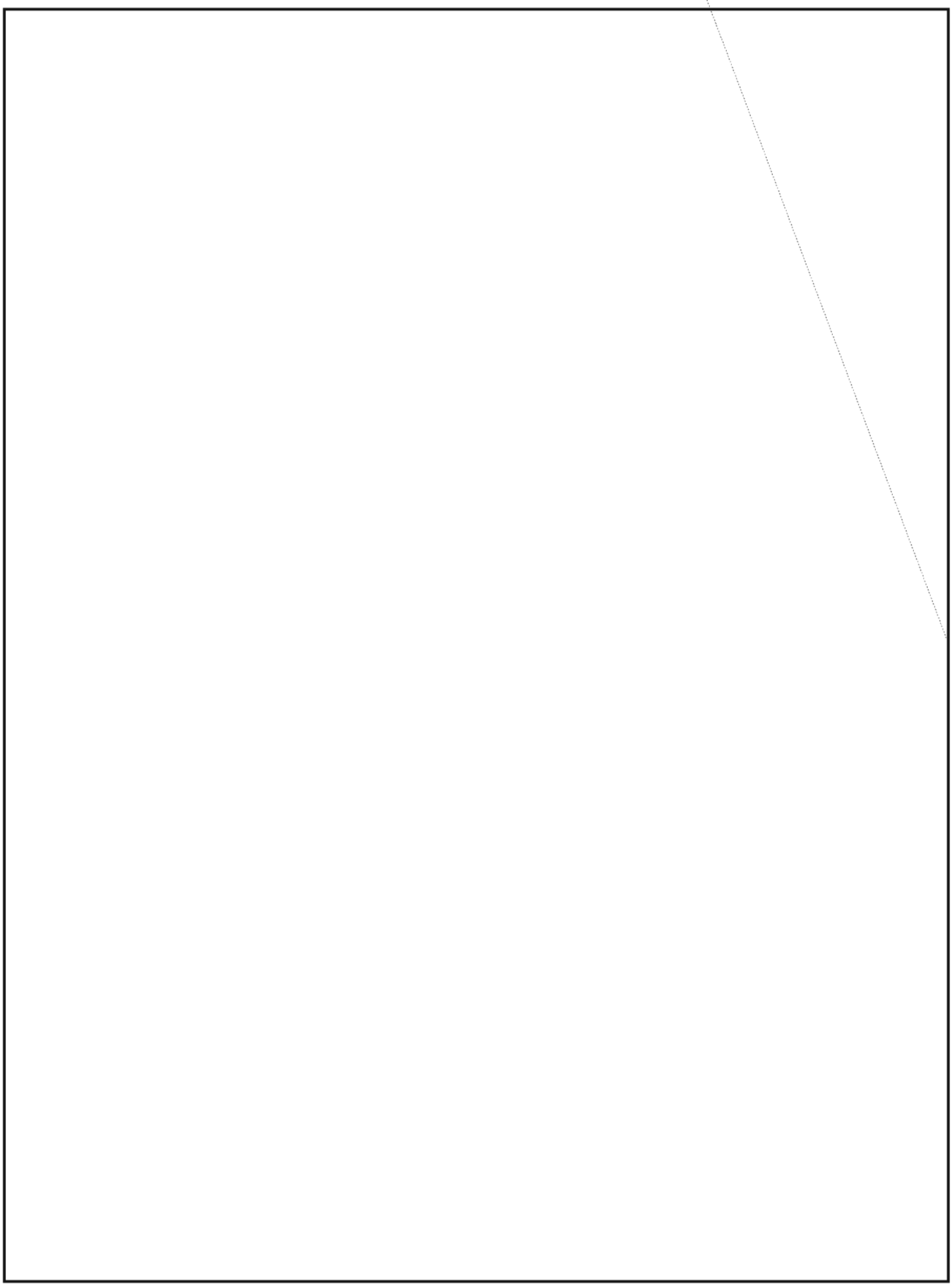
DOCID: 4019651

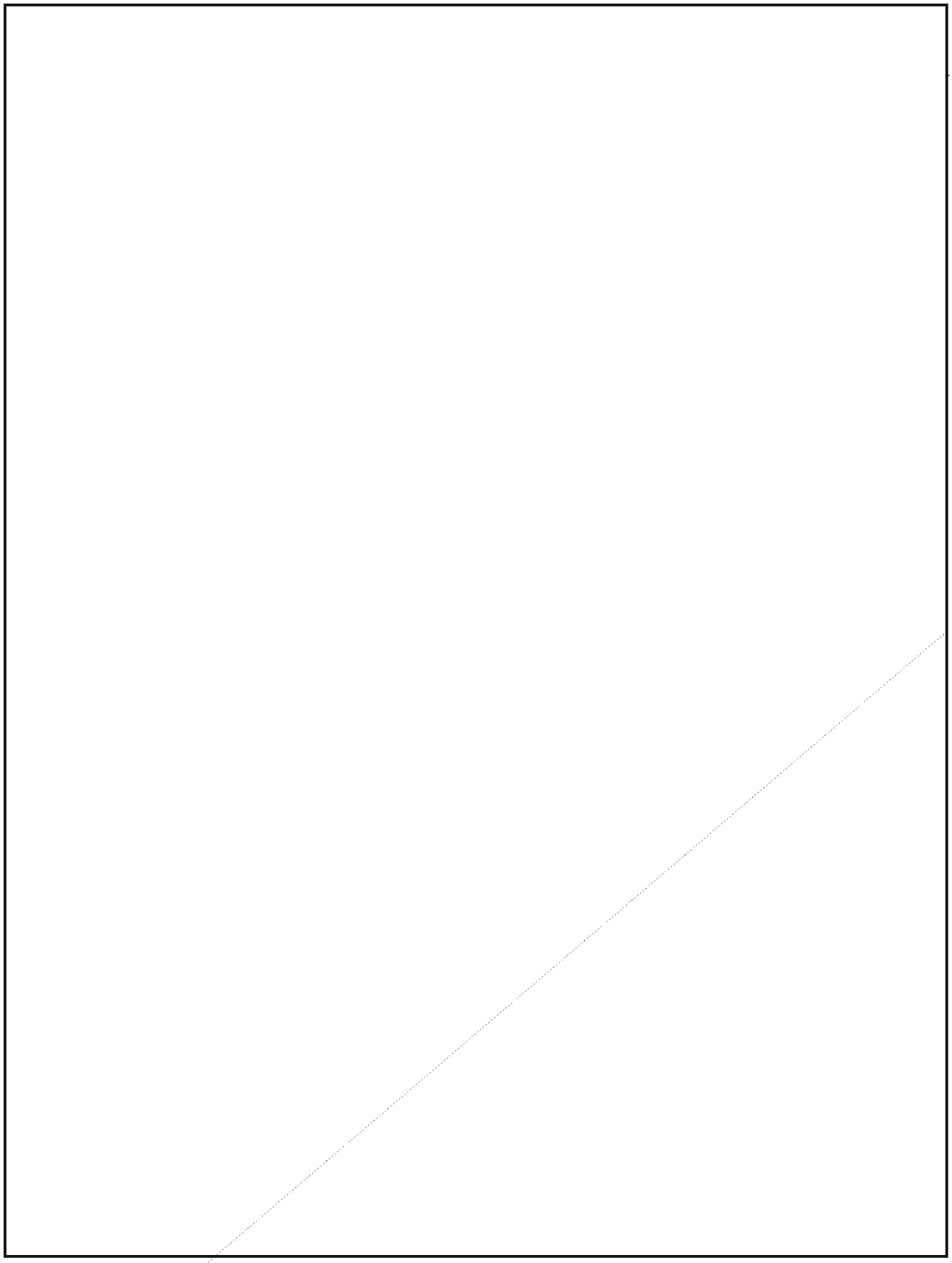
EO 1.4.(c)
P.L. 86-36



DOCID: 4019651

EO 1.4.(c)
P.L. 86-36





EO 1.4.(c)
P.L. 86-36

THE PUBLISHER WELCOMES:

NEW BOARD MEMBERS

With this issue we make a few changes in the makeup of the Board of Editors. Reed Dawson, Mathematics Editor, and [redacted] Traffic Analysis Editor, have completed their tour on the Board. We extend our thanks to them for a job well done. We also welcome three new members to the Board: [redacted] R51, Mathematics Editor [redacted] H115, Traffic Analysis Editor; and [redacted] G931, editor of a new CRYPTOLOG department -- Cryptolinguistics. Ed, Don, and Amelia have promised to carry on the CRYPTOLOG tradition of asking each and every colleague to "write it up for CRYPTOLOG."

I would like to use this opportunity to remind our readers that CRYPTOLOG is intended as a vehicle for the informal, timely exchange of views on the specialist-to-specialist, analyst-to-analyst level. So, if you have anything that you want to say, don't be shy! Write it up for CRYPTOLOG! If you need any kind of help in putting your ideas on paper, ask any of the Board members. Their job is to make it easier for you to present your views to your coworkers.

William Lutwiniak,
Publisher

(U)

THE EDITOR PROMISES:

NO MORE MISPELLINGS!

As the person who would have won the city-wide Boston Spelling Bee in 1937 if it hadn't been for the word "atrophied" (I've been waiting 41 years to use that word so that I could spell it correctly!), your CRYPTOLOG editor/typist/compositor likes to think he's a pretty good speller. Therefore it is always exasperating to hear from an eagle-eyed reader that, despite numerous proofreadings by the e/t/c, the author, and assorted last-minute checkers, a typographical error has snuck into an otherwise perfect issue of CRYPTOLOG. Whenever a new issue comes out, I *know* that the first phone call will be not to tell me how much the person liked So-and-so's article, but to report a typo! So I have finally decided to propose a deal like the one agreed on by the group of buddies who liked to spend two weeks each year fishing in Maine, but all of whom hated to cook (the joke with the punchline ". . . but *good!*"). The *next person* who even *mentions* the words "typographical error" thereby agrees to do all the proofreading for the next issue of CRYPTOLOG being prepared for press. All right? Okay, then, I defy anyone to find the next mispelling!

Art,

(For your dialing convenience: x5236s) (U)

~~(S - CCO)~~

EO 1.4.(c)
P.L. 86-36

Letters to the Editor

EO 1.4.(c)
P.L. 86-36

To the Editor, CRYPTOLOG:

[redacted]

[redacted] G91

~~(SC)~~

To the Editor, CRYPTOLOG:

Delighted to see the lead article in the April 1978 CRYPTOLOG, "SIGINT Exploitation, 1990," by [redacted] I couldn't agree more with Mr. Hunt in his concern that we devise ways to improve our efficiency in handling huge increases provided by increased collection facilities. We in R5 are not only concerned -- in R54 it is seen as their task to come up with sound, workable ideas on how to get on top of the problem of huge quantities of intercepted voice. P.L. 86-36

But I would like to draw attention to another problem in the area of SIGINT exploitation, only lightly touched on by [redacted] This is the impact of increasing volumes of *exploited* SIGINT that inundate our customers. We cannot shrug our shoulders and say, "That's *their* problem. Ours is to get the worthwhile material published and distributed." That is like officials of the Ford Motor Company saying that the fact that the public wasn't buying their lovely Edsel was the public's problem. If we produce large quantities of lovely SIGINT that nobody has time to read, we're committing a sin. And we're committing a sin if we allow any lovely SIGINT to bloom unseen in stacks of unprocessed material. So what's to be done?

We must devise better ways to get SIGINT information to appropriate customers, keeping in mind that their processing shops worry about other sources as well, and are usually quite small. It's up to us to use our technology and smart ideas to avoid the two major sins of SIGINT exploitation -- publishing too much (beyond our customers' absorption limit) and failing to publish material that we have and they need. In pursuing a solution to this problem, we may have to trample on some cherished notions of how end-product is produced and disseminated.

Jack Gurin, R5

~~(C)~~

To the Editor, CRYPTOLOG:

How could the guy who translated your Latin-American geography quiz (CRIPTÓLOGO, abril de 1978) be so dumb as to say "el.página 21"? Even *I* know that "page" is feminine, so it should be "*la* página 21."

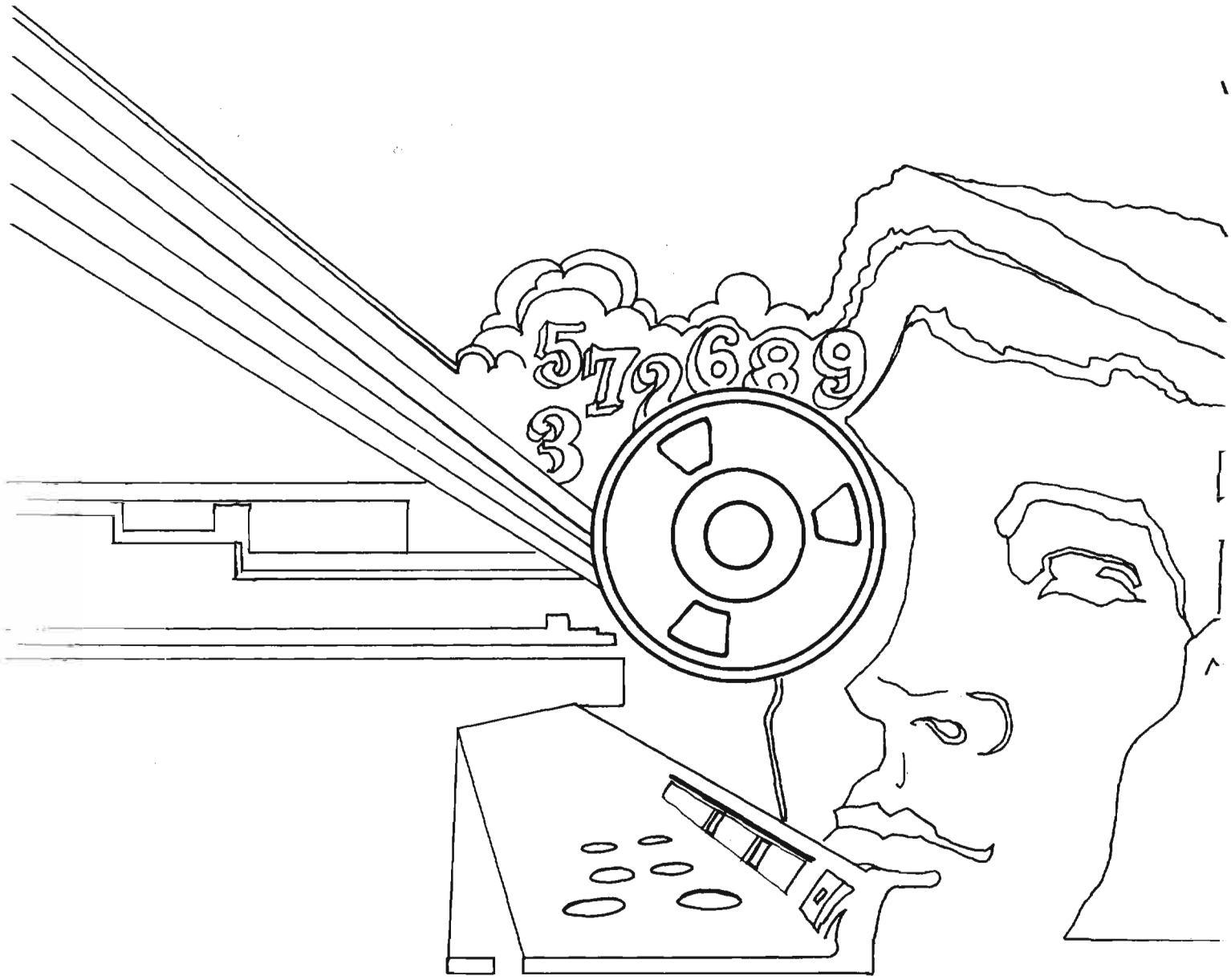
[redacted] P16 P.L. 86-36

Editor's comment:

Just a typo! In other words, it wasn't "the dumb translator" (*tú*). It was "the dumb typist" (*yo*).

(U)

P1-JUL 78-83-26493


5 7 2 6 8 9
3

DOCID: 4019650

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JUNE 1978

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

[redacted] ..... [redacted] 1
BOOKBREAKERS FORUM ON MACHINE AIDS ..... [redacted] 6
EQUIPMENT MAINTENANCE ON ABNER ..... [redacted] 7
GOLDEN OLDIE: UNKNOWN LOCATION OF U/I UNIT 8
NEVER AGAIN! ..... Jack Gurin 9
COMPUTER SCRATCH PAD: AT HOME OR AT WORK? .. Bill Crowell 10
MINNIE'S MINI ..... Minnie M. Kenny 11
NSA-CROSTIC NO. 15 ..... A.J.S 12
AS I WAS SAYING TWO YEARS AGO. . . .. Mark T. Pattie, Jr. 14
[redacted] ..... [redacted] 15
CELTIC LANGUAGES TODAY ..... [redacted] 17
LETTER TO THE EDITOR ..... E. A. Gilbertson 20
C.A.A. NEWS ..... [redacted] 21

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019650

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. V, NO. 6 JUNE 1978

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5236s)

Collection.....[redacted] (8955s)

Cryptanalysis.....[redacted] (4902s)

Language.....[redacted] (5236s)

Machine Support.....[redacted] (5303s)

Mathematics.....Reed Dawson (3957s)

Special Research.....Vera Filby (7119s)

Traffic Analysis.....[redacted] (4477s)

Production Manager.....Harry Goff (4998s)

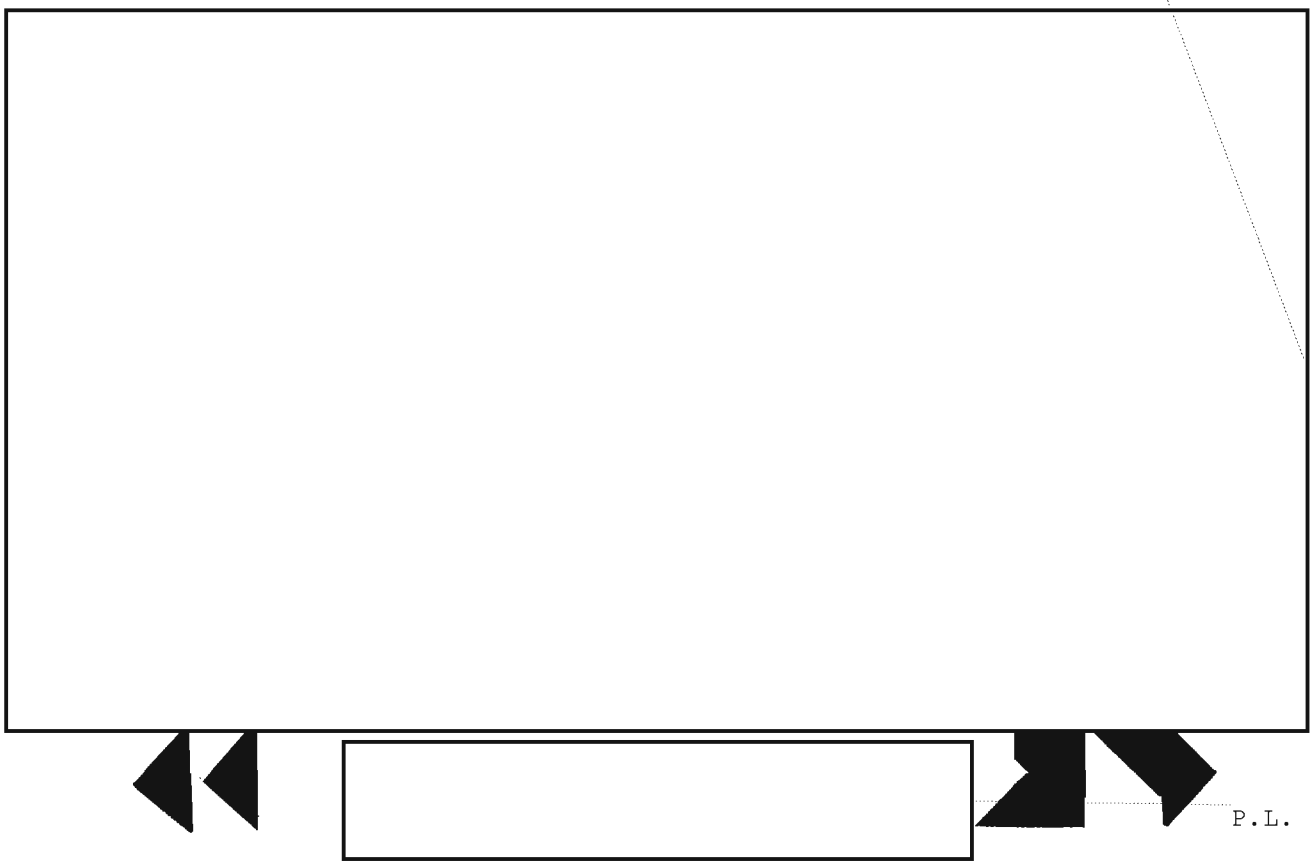
P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

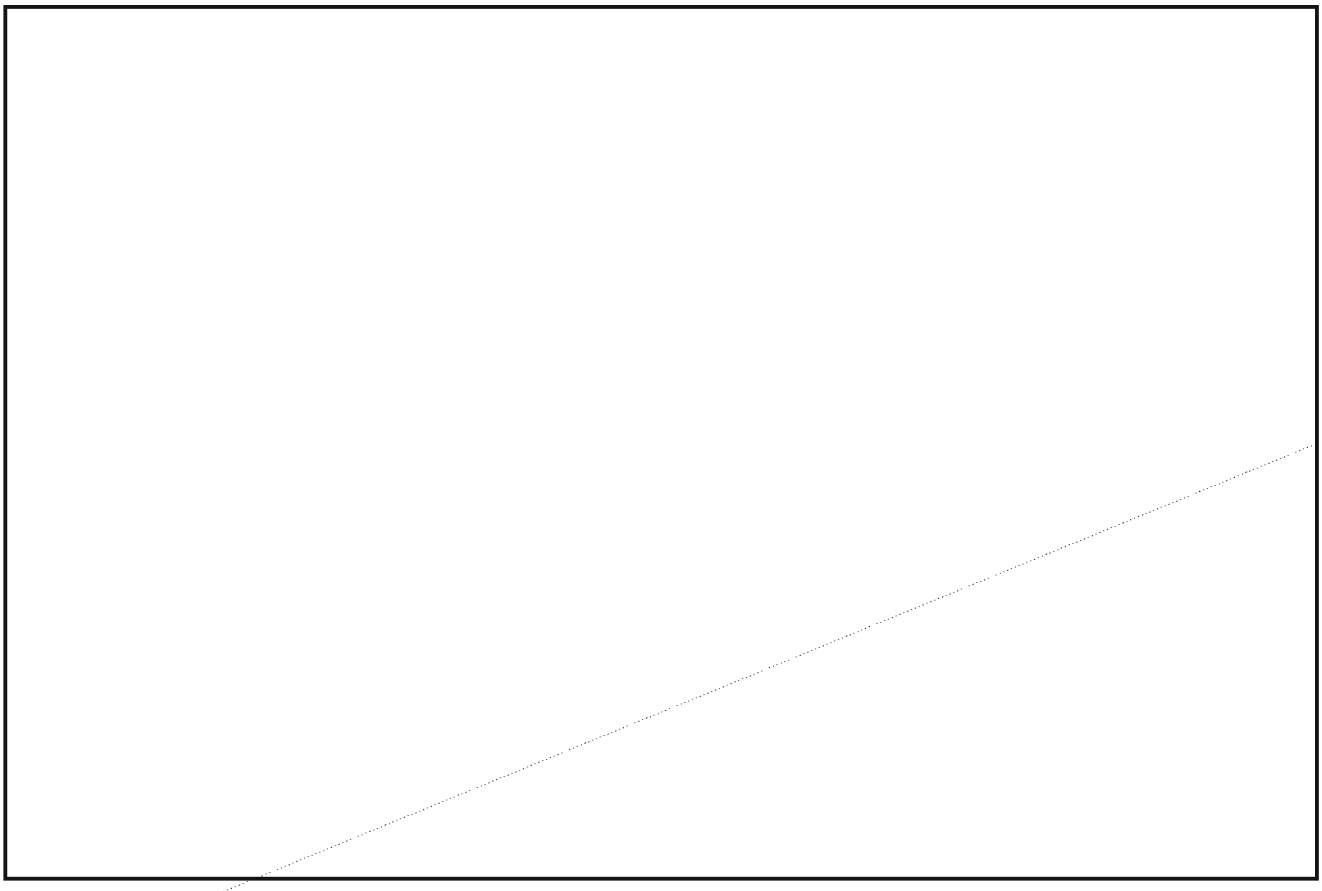
~~TOP SECRET~~

EO 1.4.(c)
P.L. 86-36

~~TOP SECRET UMBRA~~

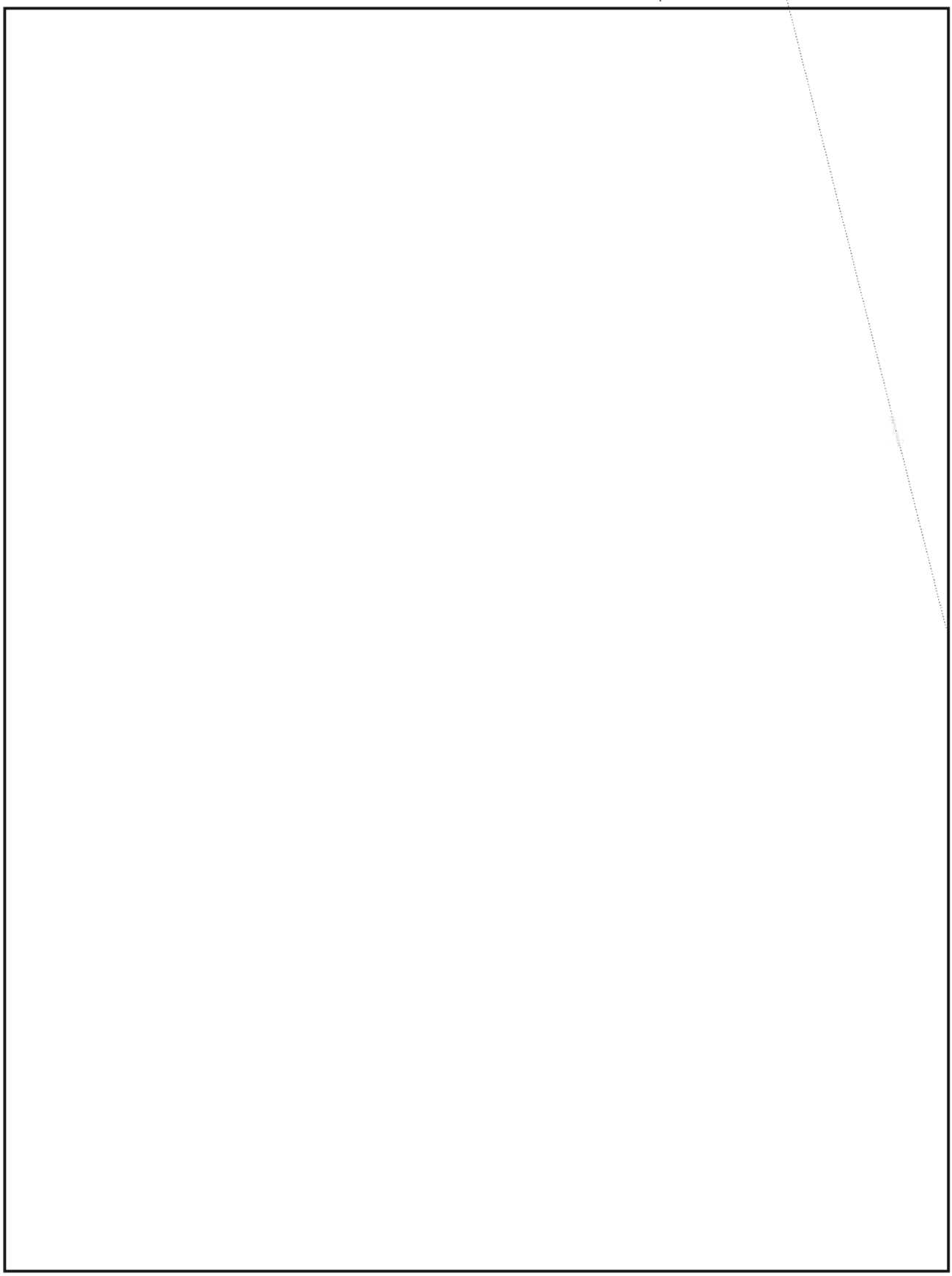


P.L. 86-36

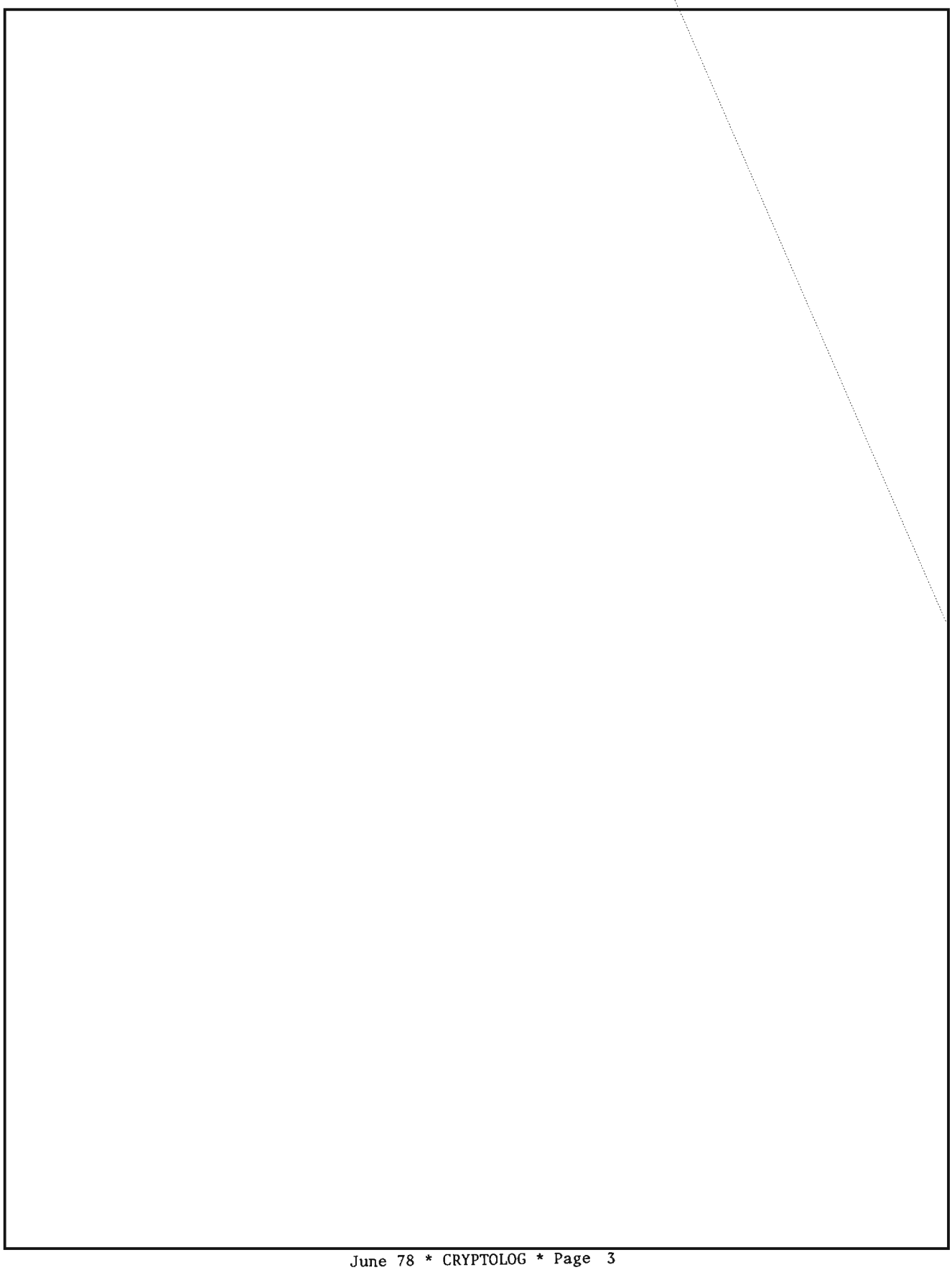


EO 1.4.(c)
P.L. 86-36

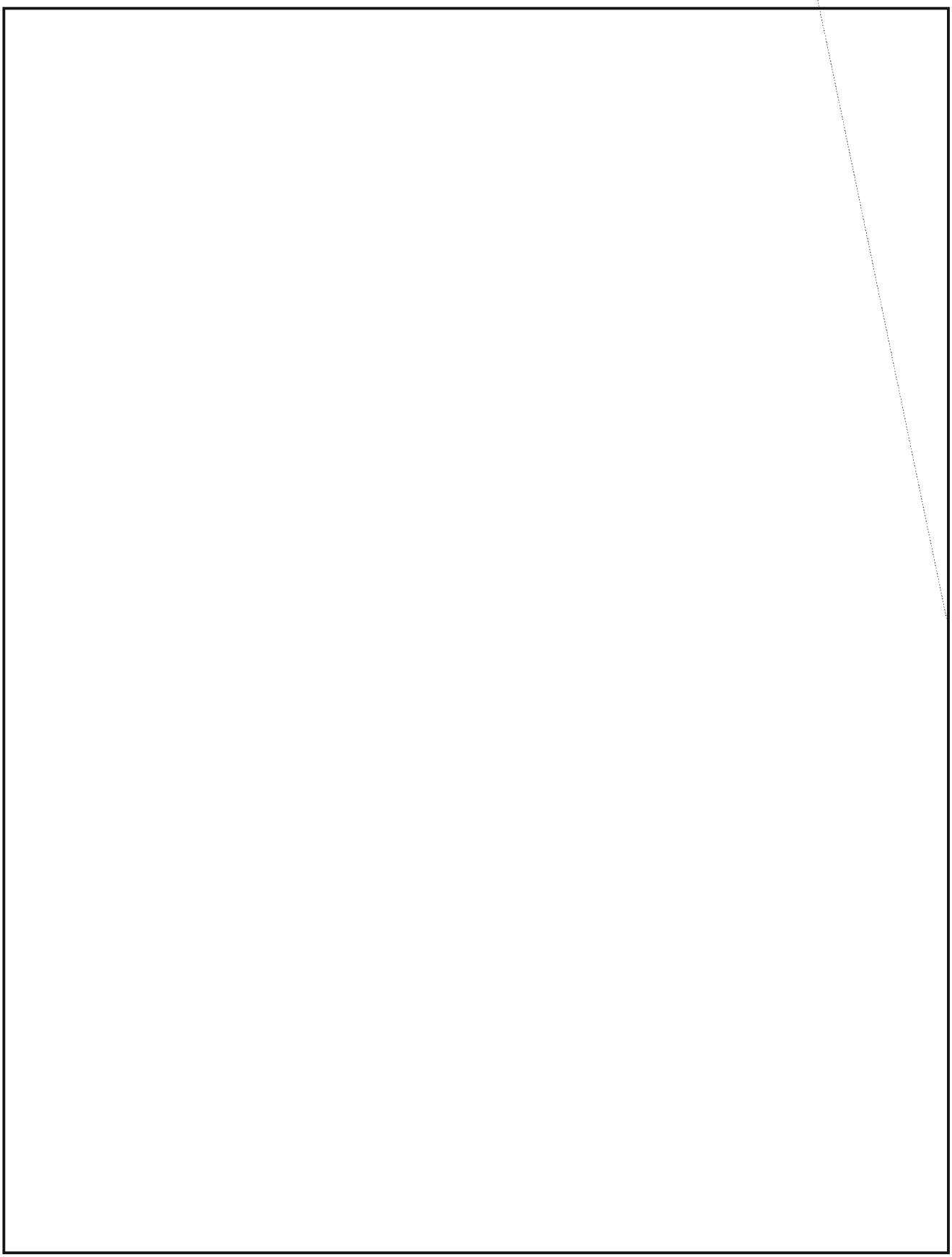
EO 1.4.(c)
P.L. 86-36

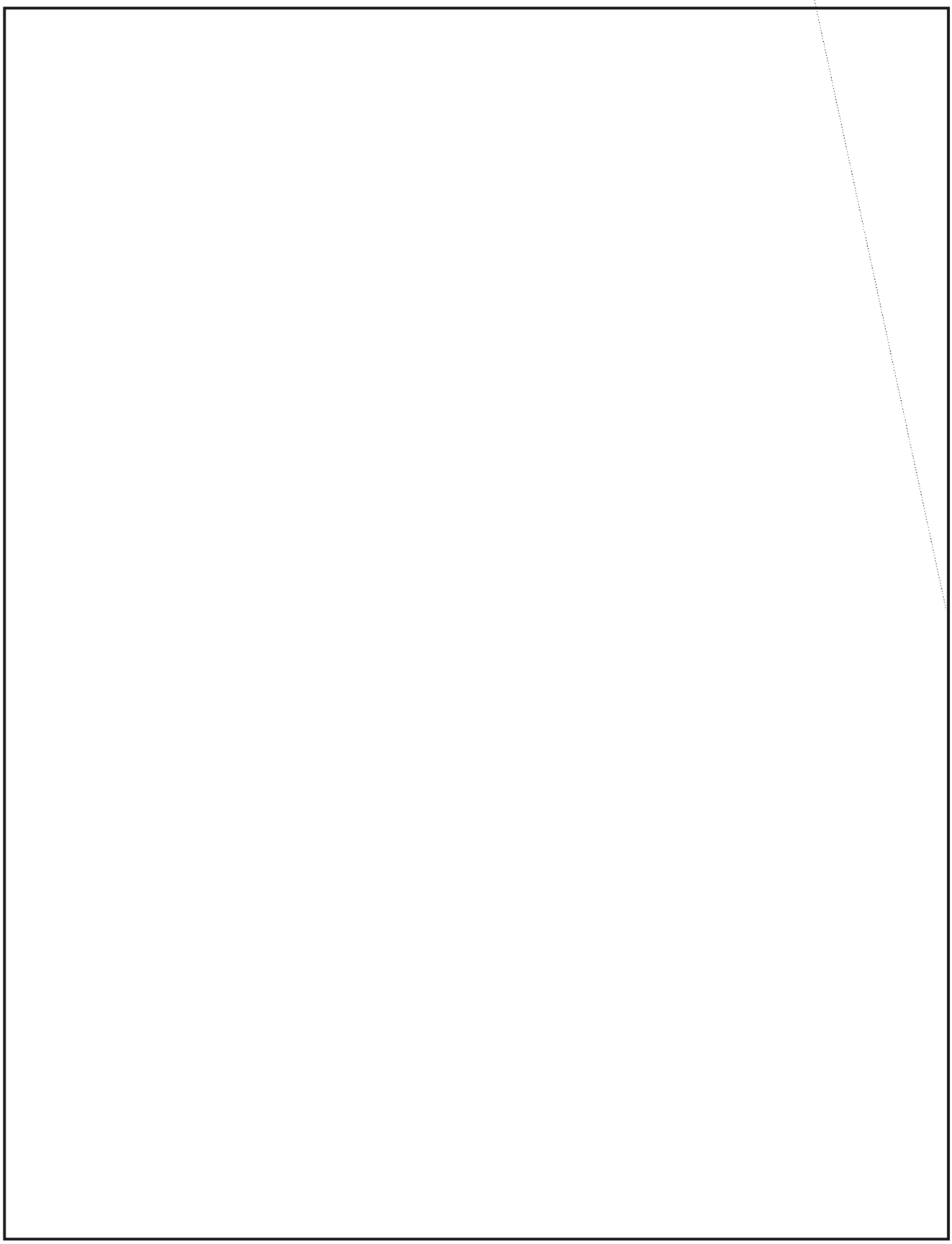


EO 1.4.(c)
P.L. 86-36



P.L. 86-36
EO 1.4.(c)





EO 1.4.(c)
P.L. 86-36

[redacted]

~~(TSC)~~

BOOKBREAKERS FORUM ON MACHINE AIDS

Do you know...

...that the Bookbreakers Forum is currently developing a new set of bookbreaking runs?

EO 1.4.(c)
P.L. 86-36

In the 10 years since the present Bookbreakers Package was designed, there have been remarkable advances in computer technology.

[redacted]

If you have any ideas that you would like to see incorporated in the new set of bookbreaking runs being developed, get in touch with: Bookbreakers Forum, [redacted] Chairman, P16, 5642s, Room 2N039.

~~(C CCO)~~

Solution to NSA-crostic No. 14

by "Sardonyx" (CRYPTOLOG, May 1978)

[redacted] "Freedom in Translation," *NSA Technical Journal*, Vol. XXI, No. 3, Summer 1976:

"Testing and checking always seem to create a climate where conservative attitudes prevail. Setting standards in anything, by its very nature, focuses on the minimum which is required to do the job rather than on excellence of performance."

(U)

P.L. 86-36

DOCID: 4019650

~~FOR OFFICIAL USE ONLY~~

EQUIPMENT MAINTENANCE ON ABNER

[redacted] D/Chief, R7

The article by [redacted] in the August 1977 CRYPTOLOG provided an excellent perspective of how the programmers viewed ABNER. [redacted] followup letter in the November 1977 CRYPTOLOG provided additional insights on the construction of the equipment. I believe it would be remiss not to cover at least a few points concerning some aspects of the equipment maintenance on the ABNER Serial 1 system.

When AFSA, NSA's predecessor at Arlington Hall Station, first determined in the very early 1950s that it was getting into the electronic computer arena, it was readily determined that there was no source of qualified engineering or electronic computer-maintenance personnel to be enticed into service at the Agency. In addition to hiring a few civilian electronic engineers and technicians, it was decided to attempt to get some expertise in this area by seeking military officers. A survey indicated that the training that came closest to meeting the Agency's requirements was given at the Ground Electronics (Radar) School at Keesler Air Force Base. A levy was placed on the USAF/AFSA for one officer in the top third of each of ten succeeding graduating classes. I was "fortunate" enough to be selected as the first officer from the first class. Upon arrival at Arlington Hall, I was assigned to the computer maintenance for ABNER. People like [redacted] now Chief T2 (as well as [redacted] all of whom are still at NSA), were old hands at ABNER maintenance, having already spent about 6 months working side by side with the development engineers and programmers in anticipation of the computer's becoming operational.

ABNER I, Serial 1, the first NSA application of "serial dynamic logic" circuitry, presented new problems for isolating malfunctions. The computer, including the consoles and peripherals, came close to being a maintenance nightmare. All of the electronic D.C. power supplies were of the laboratory type, with variable voltages. They were not overly stable and they generated a tremendous amount of heat. Electrosonic mercury delay lines were used for the 1024 words of memory (512 words per cabinet, or 64 delay lines per cabinet). The only pluggable components in the whole machine were the diode/resistor gates (there were 25,000 1N34 diodes) and the 6AN5 vacuum tubes that were used for digital pulse amplifiers. There were about 1500 6AN5s, all being used close to their design rating, and they had an MTBF that did not endear them to the maintenance personnel. More importantly, all the digital pulses were processed through various lengths of electronic delay lines. The latter were all wire-bound on very delicate metallic-plated fiberglass rods and hard-wired into the system. Likewise, all the pulse transformers were hard-wired into the system and when we were so fortunate as to locate a faulty delay line, pulse transformer, or diode isolating/gating circuitry, it took at least a half-hour or more to replace the suspect component if it was not a tube or a plug-in gate.

Perhaps more important than the hardware replacement problem was the fact that there were almost no electrical or software diagnostics for the machine. The R&D programmers had developed a few "exercise" routines, but the usual "maintenance" technique was to attempt to run an operational program and, when it didn't work, Maintenance was called in to see if we could find the trouble. This was the standard practice in other "computer laboratories" in the United States during this early computer era. Over a period of time, of course, we did develop some diagnostics. Many problems, however, occurred with the electromechanical input and output equipment and with the operations console itself. These faults would, of course, bring everything to a grinding halt, since then we could not even get data into or out of the machine. We were also hampered because the response time of the oscilloscopes was so slow that it was difficult to "see" some of the pulse trains, and delayed-sweep oscilloscopes were not yet in use.

P.L. 86-36

When production operations started in 1952 there was no time allocated for preventive maintenance. All the maintenance time we were allowed was that necessary to correct faults. In general the machine was used during the day shift by the R&D personnel who were continuing to develop some facets of the equipment and, in some cases, to improve reliability.* During the evening shifts it was used by the programmers who were just developing some of the initial programs [redacted] was among the best of these) and the attempt was made during the midnight shift to run on an operational basis the few programs that worked. All three of these "customers" (the R&D engineers and programmers; the operational programmers; and the operators) provided a unique technical as well as human-relations challenge to the maintenance crew.

As time went on, things of course improved. The maintenance people still thought the

~~FOR OFFICIAL USE ONLY~~

equipment was poorly designed; the programmers were probably the happiest of the lot; the R&D engineers were glad to get on to newer things; and the operations people suffered through with all of us. As Art Salemme wrote in the October 1977 *NSA Newsletter*, most of us lived in the Buckingham area and it was not uncommon to work on the machine for several hours at a time, come home and get something to eat (with logic equations and microseconds still going through our brains), and wander back down to work to see if we could try one more idea in the attempt to fix the machine. Maintenance down times of 4 to 8 hours were very common and on occasions lasted up to 4 or 5 days. This was not so much a reflection on the quality of maintenance personnel (I would like to think), as a reflection of the complexity of the design, the newness of the whole concept, and the absence of statistically reliable preventive maintenance procedures and software diagnostics. In many cases, whenever we were sure the input and output equipment and console were working, we would write down our own diagnostics to try and locate a sticky logic problem in the machine. As each new computer application program was written, it was not uncommon to find logic errors in either concept or wiring, even after the first year or two of operation.

After approximately a year of such interesting endeavors, I was considered qualified to become the maintenance chief on a special-purpose machine, DELLA, being constructed by R&D using the same type of digital logic and components (albeit with many more plug-in components used), that was expected to come into operations. DELLA was to be located at Nebraska Avenue and I soon began the joys of carpooling from Arlington to NSS and lost contact with ABNER just as it came into its own as a highly productive piece of computing/analytical equipment.

~~(FOUO)~~

DEPARTMENT OF GOLDEN OLDIES

EXISTENCE OF UNIDENTIFIED UNIT TENTATIVELY ASSUMED AT UNKNOWN LOCATION

One of our regular contributors recently came across the following item in his files. It was written immediately after some directive came down about not publishing anything that sounded like a snap judgement. It was circulated widely at Arlington Hall Station (see the reference to the originating sub[13]element within AFSA-242) and originally bore the fake classification "Top Secret Blurb."

Ed.

U/I Unit, possibly behind "Iron Curtain"[6]

AFSA-242c3b5d4j7s45x(Ø)[7]
(date garbled)
(X groups missing)

Traffic analysis evidence of a very tenuous nature faintly suggests the remote possibility that an unidentified unit, of undetermined echelon or type, may, in some manner, exist somewhere within Soviet Russia, or in that general vicinity.

The tentative existence of this headquarters, possibly a unit of undetermined echelon or type, is suggested by what is believed to be

5 - Intercept date garbled.

6 - Meaning not clear.

7 - Unlocated.

~~(C - CCO)~~

EO 1.4.(c)
P.L. 86-36

NEVER AGAIN!

JACK GURIN, R5

I'm not easily angered, and on those occasions when my face reddens and my hands tremble with the realization that something stupid, ridiculous, and unfair has occurred, I cool off rather quickly. But something happened more than a year ago, and even now, whenever I think of it, my face gets flushed and I find myself searching out appropriate epithets (to mutter to myself, of course).

You see, I believed in the system. I trusted it, even though I knew that many around me, although good and loyal members of the establishment, smiled condescendingly when I claimed that it was better to obey the letter and spirit of the regulations than to ignore them. Their condescension clearly conveyed the notion that they were too canny, too experienced in the ways of bureaucracy, to be taken in. A few came out and said that what I proposed to do was a mistake and that I would rue the day. Others merely shrugged their shoulders and said pityingly, "You'll see."

I had a file of papers, the only one of its kind, relating to an experiment which had been conducted in an attempt to improve our processing techniques. Without debating the merits of the original idea or of the experiment itself, which involved not only NSA, but ASA and AFSS as well, let me state that a lot of hard work went into it. After several years of research, training courses, TDY trips, field trials, and interagency correspondence, it was decided to call the experiment off. The records ended up in my safekeeping, and I felt certain that at some time in the future the issue would be revived.

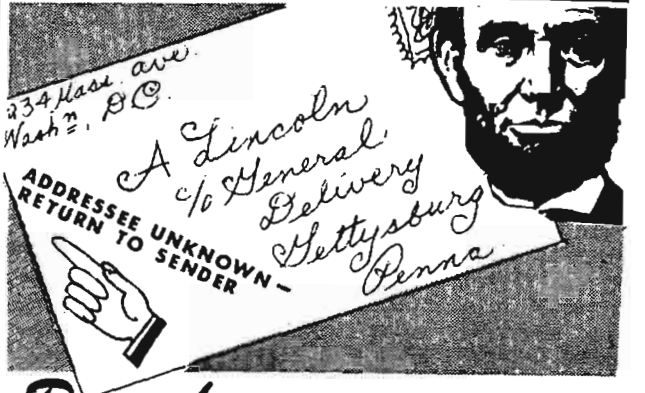
I have always been aware of the heavy cost of filing cabinets and floor space, and I agreed that, if a safe alternative existed, I should not use files in my office to store this material. Besides, I might not be around when the files would be needed again. So I followed the rules and, in September 1967, entrusted the files to NSA's Archives, after carefully noting the contents, and marked them for "Indefinite Retention." I made certain that I had the receipt, which gave the accession number and even the box or shelf number at the storage location. I was *assured* that I could retrieve the file when it would be needed.

Almost 10 years later, in April 1977 (you've already guessed, I'm sure), the subject did come up again, at high levels both within and outside the Agency, and so I proudly pulled out my receipt and called for the file. To my horror, I find that *the entire file has been destroyed!* It seems that "management" became concerned about the amount of material being kept in Indefinite Retention, and in 1971 (while I serving an overseas assignment) a group was charged with examining all the files, discarding any which seemed to have no further value. But nobody had the courtesy (or the courage) to ask me whether the file was worth retaining, even though my name was associated with it. Or maybe it was because it was too much trouble to get in touch with me.

Unable to restore all the data that had been destroyed, I could at least register my rage and warn fellow NSA-ers, so I wrote a letter to "Action Line," in the *NSA Newsletter*. That letter was almost word-for-word what I have described to this point. The "Action Line" editor sent it to the appropriate operational area in the Agency for response, and, when that response proved to be, essentially, "It didn't happen on *my* watch!", my letter was returned to me as inappropriate for publication in "Action Line" (I'll admit it doesn't deal with parking spaces or with people who smoke in no-smoking areas).

But I *do* want to register my rage and warn my fellow NSA-ers. And I still am mad, a year after learning that the material was destroyed. I've learned my lesson: Never again, do you hear, never again, will I trust the system to keep something for me, despite any assurances that the material will be found and returned "in a day or two." And, dear reader, if you have anything stored in archives, you would be wise to check right now to see whether it is still there or has been destroyed.

(U)



Do we have your correct address?

If not, please send the correct one to: CRYPTOLOG, P1.

A piece of paper with information such as the following will suffice:

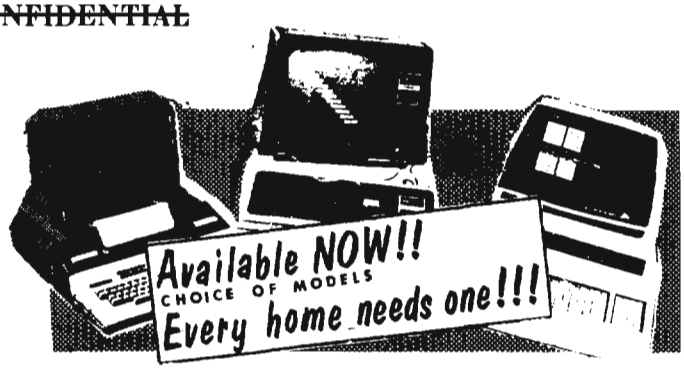
Label reads		Should read
B43		T123

(U)

DOCID: 4019650

WHICH WILL WE SEE FIRST...

A COMPUTER SCRATCH PAD AT HOME OR AT WORK?



BILL CROWELL, A204

Something caught my eye in the March issue of CRYPTOLOG. It was [redacted] article "The Hand Is Not Quicker Than the Eye." What Wayne describes is a dilemma shared by a large number of analysts not only at NSA, but also in businesses and in other government agencies: "How can we best use computers to support the human part of the analytic process?" All of us are familiar with the vast capabilities of big computers to crunch numbers, sort data, and print mountains of listings, but do these approaches really support the "personal" aspects of the human analytic process? The type of analysis that Wayne describes involves *insight* into a problem. The type of analysis best solved by the computer support we currently have is the algorithm, a finite solution based on human insight. Essentially, all of the solutions now on computer are the result of off-line analytic processes that are largely unsupported by computer.

Don't get me wrong! Computers *do* support the analyst. They give him data to work on, and they can be programmed to give him that data in myriad ways, including many of the ways that [redacted] described. But I contend that most of the truly analytic processes go unsupported by our computer complex.

Why? Well, there are at least two contributing factors. One was touched on by Wayne: "... we gain analytic insight by doing it ourselves. Logging brings us in contact -- a kind of slow motion contact -- with the material we are studying." His article attests to the fact that, with our current computer support approaches, *contact is lost*. The other fact is that *analysis* is an iterative heuristic process -- trying solutions or parts of solutions until you find one that works or almost works, and then applying those learned lessons in adaptive iteration until a solution is found. Computers are not easily programmed to do this kind of work -- at least not yet. In most cases today, the analyst not only must be able to do analysis but he must also be able to describe to a programmer the process or analysis or ways of achieving *insight* if he wants computer support for his analytic needs. It is difficult enough to do this for his *data* requirements and get what he wants -- and describing data ought to be a hell-of-a-sight easier than describing an analytic process. This is no slap at the programmer -- or at the analyst. If anything, it is just recognition of the limitations of language as a means of conveying quickly a complex analytic process that may have many blind alleys.

P.L. 86-36

Is there a solution to this dilemma? I believe there is, at least to the specific questions that Wayne raised, and perhaps to facilitating all types of analysis. The solution I suggest is not a panacea nor is it new, but perhaps its time has finally come.

The Analyst's Scratch Pad

Almost unnoticed at NSA, the outside world has undergone a revolution in their approach to computer support. The day of the microcomputer has arrived. Not only have thousands of very small businesses begun using them, but -- heaven forbid -- even individuals are buying them, using them, and rapidly creating new applications on them. Oh, you say, these are all engineers and data systems people who want to take their work home with them as a hobby? Not so! None of the people I know who already have a personal computer or have ordered one is an engineer or a data systems professional. One of them is 72 years old and never programmed before -- he is creating a program to analyze the genetics of his cattle herd, and he doesn't think it's too late to learn to use computers.

Why is this happening? There are probably numerous reasons, among them the fact that very capable computers are becoming available at low cost (less than $800). But another reason relates to the desire expressed by Wayne -- to have *contact* with the material they are studying. These new computerists are really analysts who have discovered a powerful new scratch pad for their analytic wanderings. Their ranks are swelling at an incredible rate. So is the product of their labor.

Can any of this analytic-scratch-pad technology be applied to the problem described in Wayne's article? You bet it can! Computerists have found that the instantaneous nature of the computer can be very inhibiting to human beings -- so they created timing loops that simulate human response. They found that endless listings of data befuddled humans -- so they created graphic presentations of the same data so that visual processes can be applied to problems. They encountered problems in handling mistakes made in coding programs -- and created text and word processors to allow the easy manipulation of such data, much in the manner than a callsign analyst would love to be able to do.

DOCID: 4019650

Does NSA plan to provide such a capability to their analysts? No! At least not soon and perhaps not until most NSA analysts have a more useful capability at home than they have at work. This is one case where the bureaucratic process has developed a life cycle that far exceeds the cycle of development of new systems and capabilities and costs outside NSA. The budget for FY-80 is being built now and it will have us buying more of the large computer systems available last year or the year before. There is money for collection and for processing, but not for analytic support -- at least not the type of support Wayne and other analysts want!

Emotional response? Yes, it is emotional, but only because I think NSA is missing an opportunity. We have led the way in the design and application of computers to the analysis of seemingly unsolvable problems of cryptology. Now the rest of the world has caught fire with enthusiasm in extending the computer's usefulness. We ought to take advantage of this new impetus to extending human analytic capabilities.

~~(C)~~

MINNIE'S MINI:

FIVE YEARS LATER AND I STILL WANT IT!

Minnie M. Kenny
Chief, P16

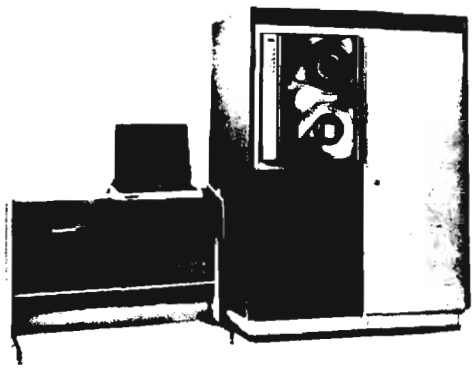
My, my, how the years roll by! In the preceding article, Bill Crowell says that he would like to see personal-sized computers used at NSA. In the December 1973 issue of the B Group publication DRAGON SEEDS, of which she was the founding editor, Minnie M. Kenny said the same thing. That 1973 article is reproduced below, with a brief introductory word by Mrs. Kenny.

Ed.

I definitely agree with Mr. Crowell, as my article in DRAGON SEEDS indicates. Mr. Crowell's article expressed very succintly two points I tried to make to the ALBRECHT Group -- that an analyst must have contact with the materials he is studying and that the personal-sized minicomputers can be used as "powerful new scratch pads" and serve as catalysts for the development of new techniques and applications across the whole vista of cryptologic disciplines. Imagine! Desktop scopes with programmable keyboards and split-screen and scrolling capabilities! They're the answer to a SIGINT maiden's prayers.

It seems like ages ago when it all began. We were still at FANX and had just experienced the nine hundred and ninety-ninth power outage. No COPE, no RYE, no 6700, no *nothing!!!* To top it all off, it wasn't even raining. Now what kind of Providence was that?

We came up with an idea: why not hang a tape drive on that modified PDP-8 called the COPE terminal, boosting its memory by 4K, and declare our independence from Central Control? No way!! We got bottled up in channels and buried under paperwork.



That's when I began dreaming of desk-top terminals for CA applications. Can't you imagine a user-controlled system of minicomputers, say one master and three slaves with an interchangeable hierarchy (to eliminate service interruption when there's a malfunction), and a terminal on each analyst's desk? Why, you'd hardly need cross-section paper and pencils!

One day I stumbled across several idle CRTs. I was nosing around down in C at the time. I *had* to have them. Hooked up to one of the general processors, they'd make an adequate substitute for my dream system. I lost out again. I could pirate the terminals but I couldn't "bootleg" the hook-ups.

About this time, R came on the scene touting minicomputers with blisters. They were developing interactive CA applications. And they wooed me with the promise of the realization of my dream. We formed a committee which formed a study group which formed into teams which inspected CA processes in B. The results were published in a huge compendium called the ALBRECHT Study, but. . . *I still want a mini!*

~~(C)~~

NSA-crostic No. 15

By A.J.S.

The quotation on the next page was taken from a published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS / *WORDS*

A. Escort — 121 21 43 52 95 107 137 163

B. "---------- of Texas" (2 wds) — 29 37 54 101 130 145 211 22 105 122

C. Loathed — 48 4 33 79 134 152 210 247

D. Born — 60 229

E. Genus of snakes comprising the anaconda — 8 86 123 156 228 57 226 230

F. "If I hadda knowed that you'da wanted to of went, I'da seed that ----------" (cited in H. L. Mencken's *The American Language*) (6 wds) — 26 34 72 109 108 186 215 232 67 99 32 179 199 164 243 17 144

G. It sometimes takes people a long time to learn that there's no such thing as --------- (2 wds) — 2 155 182 218 225 19 87 173 200

H. Ballet by Word L (2 wds) — 13 42 204 220 234 28 88 142 169 175 227 250 71 151 24 126 190

I. Bury — 1 47 214 241 23

J. "Alice's ----------" — 7 53 168 202 172 106 70 77 162 233

K. American revolutionary figure (1741-1801) (2 wds) — 171 6 16 56 82 103 127 138 161 207 221 248 44 61

L. American composer (1900-) (2 wds) — 39 64 149 150 176 242 35 85 132 80 183 102

M. Lizard-like animal, found in water or damp places — 10 97 139 209

N. Capital of one of the Soviet republics — 174 30 104 153 246 65 114 147

O. Beloved — 213 3 50 93 135 195 148 117 244 25

P. Civil War general; commanded Confederate left in Battle of Gettysburg — 110 5 125 45 191

Q. Decrease — 236 98 237 31 219 178 11

R. Clumsy — 224 185 113 217 239

S. Type of roof — 141 12 59 75 129 116

T. Get the better of — 158 90 181 206 140 170

U. Extend — 249 160 81 166 194

V. In children's games, the player whom the other players oppose — 188 20

W. The Indian who brought the first electric power line to his tribe's communal outhouse was the first person ever to wire ---------- (5 wds) — 18 49 69 91 133 157 9 112 136 187 192 223 235 245 14 46 124 196 63 167

X. Ballet set to music by Chopin (2 wds)

Y. G. K. ---------- (1874-1936)

Z. Excel

Z_1. Great quantity

Z_2. "Creme de ------"

Z_3. Interrogatory interjection

Z_4. "Blue ---"

Z_5. Teased good-naturedly

55 84 180 212 203 197 216 143 15 222 128 51

111 68 205 27 94 231 159 115 120 40

66 131 92 41 58 208 36 198

189 100 74 83

38 193 73 89 165 146

154 240

119 76 238

78 96 184 62 118 201 177

1 I	2 G		3 O	4 C		5 P	6 K	7 J	8 E		9 W	10 M	11 Q		12 S									
13 H	14 W	15 X	16 K	17 F		18 W	19 G	20 V	21 A	22 B	23 I	24 H	25 O	26 F										
27 Y	28 H	29 B	30 N	31 Q	32 F		33 C	34 F		35 L	36 Z	37 B		38 Z_2	39 L									
40 Y		41 Z	42 H	43 A	44 K	45 P		46 W	47 I	48 C		49 W	50 O		51 X									
52 A	53 J	54 B	55 X	56 K	57 E	58 Z		59 S	60 D	61 K		62 Z_5	63 W		64 L									
65 N	66 Z	67 F	68 Y	69 W	70 J		71 H	72 F	73 Z_2	74 Z_1	75 S	76 Z_4	77 J	78 Z_5	79 c									
	80 L	81 U	82 K		83 Z_1	84 X		85 L	86 E	87 G	88 H	89 Z_2	90 T	91 W	92 Z									
93 O	94 Y	95 A		96 Z_5	97 M		98 Q	99 F	100 Z_1	101 B	102 L		103 K	104 N	105 B									
106 J	107 A		108 F		109 F	110 P	111 Y	112 W	113 R	114 N		115 Y	116 S	117 O	118 Z_5									
	119 Z_4	120 Y		121 A	122 B	123 E	124 W	125 P	126 H	127 K	128 X		129 S	130 B	131 Z									
132 L	133 W		134 C	135 O	136 W	137 A	138 K		139 M	140 T	141 S	142 H		143 X	144 F									
145 B	146 Z_2	147 N	148 O	149 L		150 L	151 H		152 C	153 N	154 Z_3	155 G	156 E	157 W	158 T									
159 Y	160 U		161 K	162 J	163 A		164 F	165 Z_2	166 U	167 W		168 J	169 H	170 T										
171 K	172 J	173 G	174 N		175 H	176 L	177 Z_5		178 Q	179 F	180 X	181 T	182 G	183 L										
184 Z_5	185 R		186 F	187 W	188 V	189 Z_1		190 H	191 P	192 W	193 Z_2		194 U	195 O	196 W									
197 X	198 Z		199 F	200 G	201 Z_5		202 J	203 X	204 H	205 Y	206 T	207 K	208 Z	209 M	210 C									
211 B	212 X		213 O	214 I	215 F	216 X	217 R	218 G	219 Q		220 H	221 K	222 X		223 W									
224 R	225 G	226 E	227 H	228 E	229 D		230 E	231 Y	232 F	233 J	234 H	235 W	236 Q		237 Q									
238 Z_4		239 R	240 Z_3	241 I		242 L	243 F	244 O	245 W	246 N	247 C	248 K	249 U	250 H										

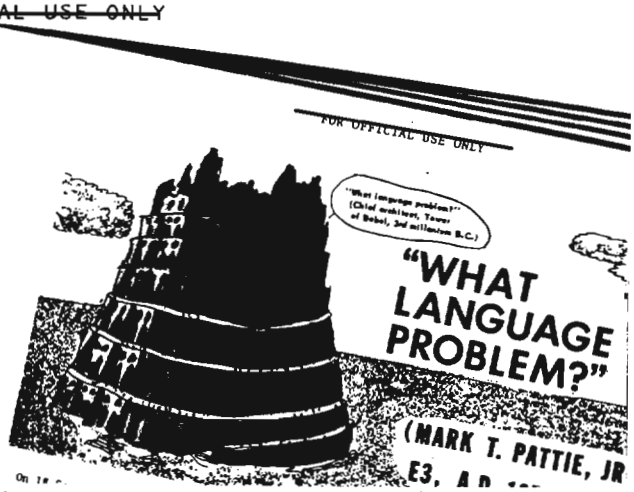
A.J.S.

(Solution next month)

DOCID: 4019650

AS I WAS SAYING TWO YEARS AGO...

Mark T. Pattie, Jr.



Never underestimate the power of the press, even if it only has a negative effect. In the May 1976 issue of CRYPTOLOG I had an article on the "language problem" within NSA and, if I had known then what I know now, I would not have submitted it, for matters have now gone from bad to worse.

In the article I suggested that the language problem might well be solved if Agency powers-that-be would see fit to reward good linguists with tangible items like promotions. Evidently the article struck a nerve, for disparity between linguist promotions and those for others, such as electronic engineers, has increased.

But what about the latest solution to the "language problem" -- hiring high school graduates to be trained as linguists? It will be quite some time before the results of this move can be evaluated, so I am in no position to state positively that it will not work. Still, I find it difficult to be optimistic, for I have been around long enough to remember the similar experiment with high school students back in the 1960s. Surely M3 has figures showing how many were trained and what became of them. If memory serves me right, there were few who completed the program and I have no way of knowing how many, if any, are still with the Agency and in language work.

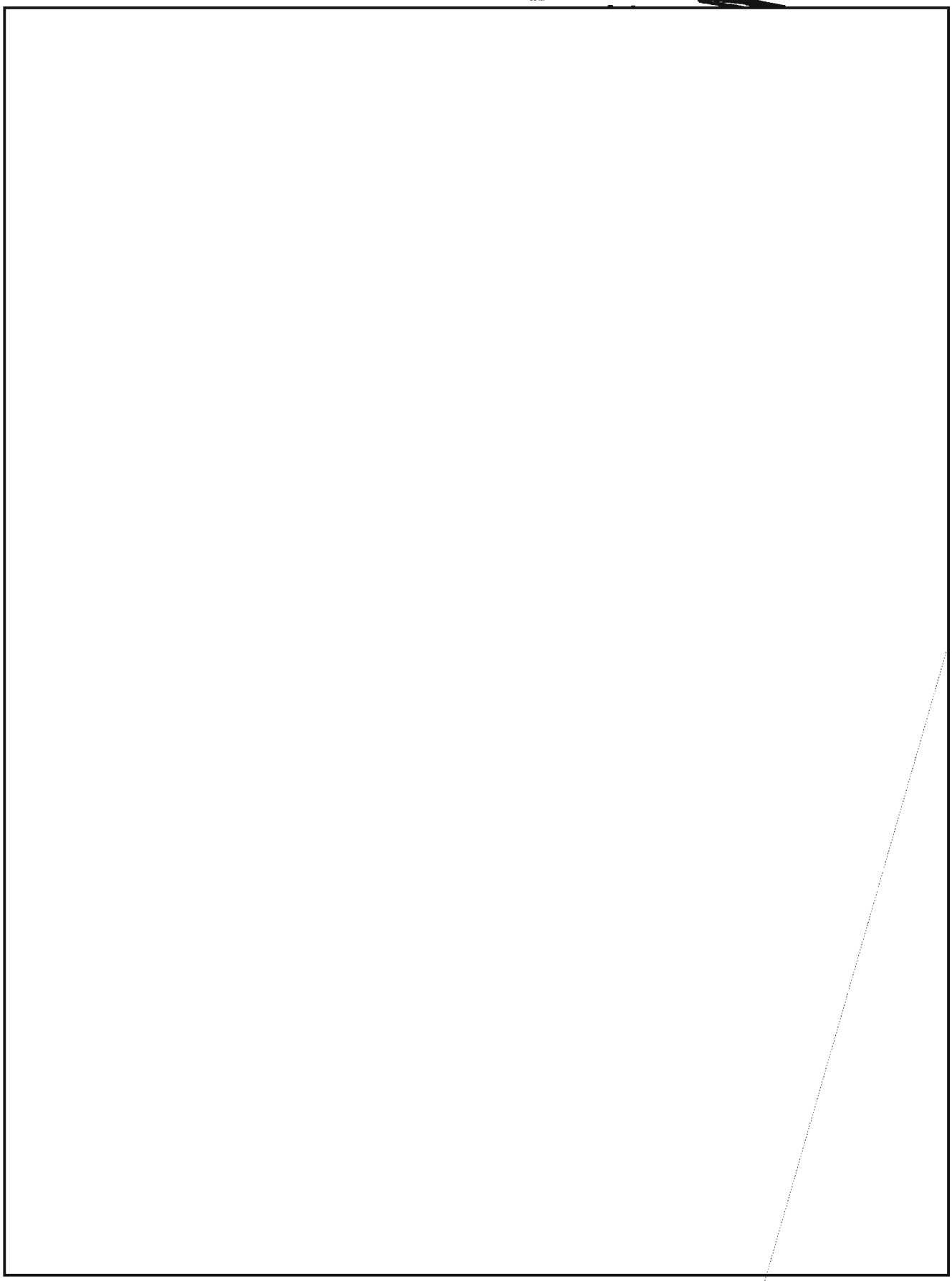
Still, let us assume that the exercise will be completely successful. Then, why don't we hire high school graduates to be trained as engineers or mathematicians? After all, if it would work for one skill, it ought to work for all. Somehow I doubt that those who hire mathematicians and engineers would allow that to happen.

So, how did it happen for linguists? I can only suspect that what I said in the earlier article continues to hold. Those who make decisions about linguistic capability are not linguists and they remain convinced that it takes little to become one. I would think that the fiasco of President Carter's interpreter in Poland might disabuse them of that notion.

P.L. 86-36

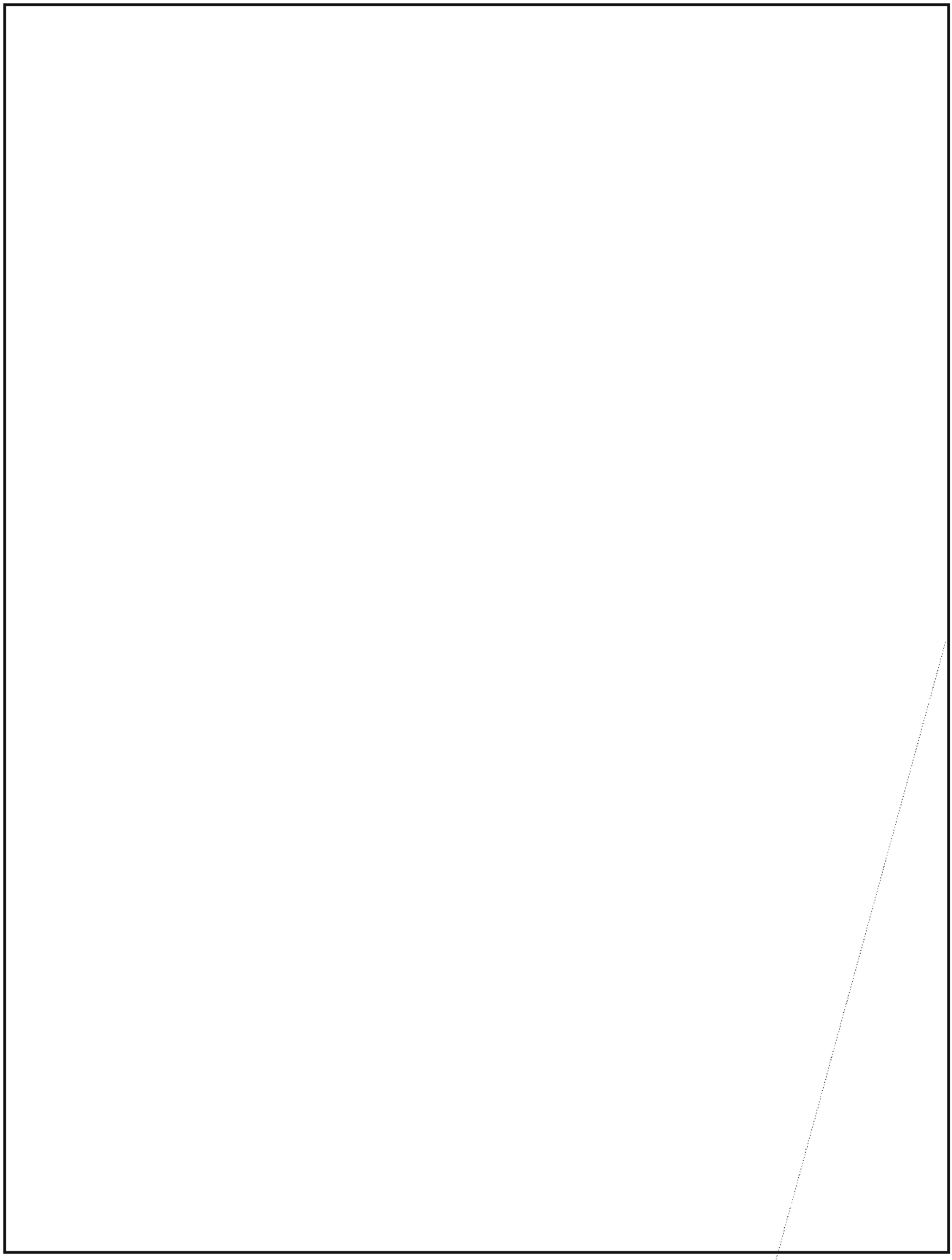
There is an old cliche, "You get what you pay for." For years those who make decisions about hiring for the Agency have managed to use that cliche as a lever to have engineers and scientific personnel hired at higher grades or at higher levels within grades. Now, to use another cliche, "The rich will get richer and the poor will get poorer." Linguists will enter at the lowest possible grades and will be competing with those who are being hired many grades above them, with little -- actually, no -- hope of ever catching up. This will be a self-perpetuating situation, for the time will come when only engineers and scientists will have high enough grades to be considered for appointment to senior management positions and they will continue to make the decisions affecting linguists.

If I sound bitter, it is only because I am. Our product, so dependent upon the efforts of linguists, is bound to suffer as senior linguists leave, and I do not see anything but a downhill trend in the years ahead if the present policies remain unchanged. You *do* get what you pay for!



P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

~~SECRET SPOKE~~



P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

DOCID: 4019650

CELTIC LANGUAGES TODAY

(A LOOK AT WELSH AND GAELIC)

P.L. 86-36

Llanfairpwllgwyngyllgogerychwyrndrobwll-llantysiliogogogoch. It is undoubtedly the longest place name in the world, and it hangs over the train station of this village in Anglesey, North Wales, only a few miles distant from the village of Llanfairfechan, where I stayed in the summer of 1977. The name means "St. Mary's Church, in a hollow of white hazel, close to a rapid whirlpool and St. Tysilio's Church, and near a red cave." (It is usually mercifully abbreviated to Llanfair P. G.)

I had come to Wales to learn more about the Welsh language and to collect materials in that language. Later I would go north to Scotland and try to do the same with Gaelic. The events that led to this pilgrimage, and what I discovered there, are the topic of this article.

Before discussing the difficulties that a student of Welsh encounters (using words of more manageable length than the one above), I would like to say a few words about Celtic in general.

We have witnessed a revival of interest in Celtic (pronounced "*K*el-tick," not "*S*el-tick" -- there is no *c* pronounced as *s* in any Celtic language) studies in recent years. As I looked for the reasons behind this upsurge in interest, I came up with several possible ones:

- the *Roots* search, not limited to blacks, but involving people of all ethnic groups;
- increased publicity. In May 1977 *National Geographic* published a beautifully illustrated article on the Celts by Merle Severy, including a map of Celtic Europe. The map shows that there were Celtic settlements as remote as present-day Turkey, where the Galatians lived. (St. Paul wrote an epistle to the Galatians and it eventually became part of the New Testament.)

  There is also a greater awareness of Celtic language (and mythology) because of the tremendous success of J. R. R. Tolkien's books. *The Hobbitt*, *The Lord of the Rings*, and, more recently, *The Silmarillion* draw upon the wellspring of Icelandic and Celtic lore. Tolkien liked Welsh better than any other language, and used it as a basis for many of the words in his artificial languages. As people became aware of his sources, their own interests in these subjects were stimulated.
- Another reason for the revival of interest is that the field has not been overworked. There is still plenty to do. In my own field of Hebrew -- especially in the area of the Bible -- scholars have gone over the same ground many times with a fine-toothed comb. But with Celtic the situation is just the opposite. Dr. Robert Meyer of Catholic University, in Washington, once said that every time he "puts down his spade," as it were, he comes up with something new.
- Last but not least, one may mention the conflict in Northern Ireland, which has called attention to all things Irish.

My own interest in Celtic languages can be traced at least in part to a chance remark made by Agency linguist John Murphy. He pointed out that in many ways Irish resembles Hebrew and the other Semitic languages in its structure. Some scholars had actually gone so far as to suggest

Based on a talk given in September 1977 to SIGTRAN (the Crypto-Linguistics Association's Special Interest Group on Translation).

that the insular Celtic languages had been influenced by some Afro-Asiatic substratum. John Murphy referred to such features as a "construct state" and conjugated prepositions. Later on, when I took Dr. Meyer's course in Old Irish, I was able to spot more similarities, in addition to the ones John Murphy had mentioned. Here are some examples, taken from the "Scela Mucce Meic Datho" (The Story of Mac Datho's Pig):

Construct State

Old Irish: *"Ailbe ainm in chon."* "Ailbe was the name of the dog," lit. "Ailbe name the dog," exactly parallel to "Ailbe shem ha-kelev" if we were to translate it into Hebrew.

Verb-Subject-Object Word Order

Old Irish: *"Imdīched in cú Laigniu huili."* "The dog defended all Leinster," lit. "Defended the dog Leinster all-of-it." In classical Hebrew one would say, "Vayagen ha-kelev ʿal Leinster kullah," preserving the same word order. Such an order is unusual in a European language.

Conjugated Prepositions

The Old Irish word for "with" is *la*. Conjugated with pronominal suffixes, this becomes *lem, lat, leiss*, etc. In Hebrew and Arabic, most prepositions can likewise be conjugated.

Anticipatory construction for genitive

This feature is shared by both Old Irish and Aramaic. (Late Hebrew has it as a result of Aramaic influence.) Old Irish: *"Ba lán Hériu dia airdircus in chon."* "Ireland was full of the fame of the dog," lit. "Was full Ireland of-his fame of the dog." Cf. Modern Hebrew: "Kalbō šel ha-ʾīš," lit. "his-dog of the man," = "the dog of the man," "the man's dog."

Yet, from a lexical standpoint, the theory that insular Celtic had some kind of Semitic influence -- say, from the Phoenicians -- finds no support. Aside from a few chance resemblances, there is no trace of it. One thinks readily of the Arabic loan-words in Spanish, Turkish, or Persian; the Spanish words in Basque; or the enormous influence exerted on English by Norse (from which even our third person *th-* pronouns were borrowed). The fact that nothing like this can be seen in Celtic makes its connection with Hebrew very doubtful.

I should now like to give an overview of the Celtic languages, both living and extinct, before concentrating on Welsh and Gaelic to "take their pulse," as it were, to determine where they are healthy and where not, and what is being done to keep them alive.

The Celtic languages can be divided into two groups: insular and continental (see Fig. 1). The continental Celtic languages were once very widespread over the European continent, but little is known about them. Caesar wrote about the Gauls, and there are some Gaulic inscriptions, but little else remains.

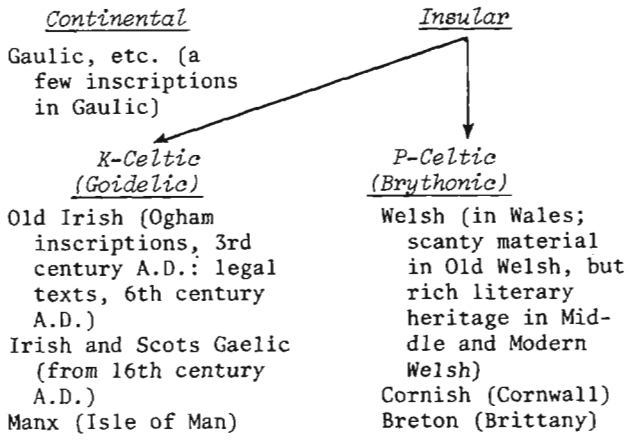


Fig. 1

The insular branch is divided into K-Celtic (Q-Celtic) and P-Celtic because of a split that occurred from the Indo-European consonant **kw-*. In Irish the labialization was lost, so that only the *k* sound remained; cf. the Irish word for "head," *ceann*, as in the name Kennedy, which literally means "ugly head." In Welsh, on the other hand, the word for "head" is *pen* as in "penguin," which literally means "white head."

Both Manx and Cornish are extinct. The last Cornish speaker is reported to have been a fisherwoman named Dolly Pantreath of Mousehole (pronounced *mōōsə'l*), who died in 1789. Another researcher, however, has claimed that its last speakers were Cornish miners who took part in the California gold rush of 1849.

As for Manx, there were still four persons alive in 1954 who spoke that language, and they were very elderly at the time, so we may safely assume that Manx too is by now a dead language.

Turning to Gaelic, we find a living language, but you may have to go out of your way to hear it spoken.

In Edinburgh I attended a Gaelic church service on a Sunday afternoon at the Highland Tolbooth St. John's Church. The people were most friendly; they bade me "a hundred thousand welcomes," or *"Ceud mile failte,"* as they say in Gaelic, and I made the acquaintance of a kilted gentleman and his wife who put me in touch with the right organizations and publishing houses, so that I could acquire more Gaelic materials. The chap had even studied a bit of Hebrew, as it turned out, so we found that we had some other common ground and hit it off very nicely right from the start.

At his recommendation I visited the School of Scottish Studies at the University of Edinburgh. School was out for the summer and they were operating on a skeleton crew, but the visit turned out to be worthwhile nonetheless. I learned that they had recorded thousands of

DOCID: 4019650

hours of Gaelic speech on tape and that they publish an attractive bilingual magazine, *Tocher* (Dowry). It appears 3 times a year and costs only 40 p an issue. Here you can find stories, songs, and traditions from the school's archives.

There is also a publishing house called *"Gairm"* (Word) which prints books and manuals in and about Gaelic (see bibliography).

A complete Gaelic course is available on tape from National Extension College in Cambridge, England, for about $50.00, and a number of other tuitional aids are available on both disks and cassettes (see bibliography).

But to hear Gaelic spoken freely and naturally, one must go to the islands, to a place such as Harris on the Isle of Lewis, so far north that it never gets dark in the summertime, and where people are not subjected to as much English influence. Even television has not made great inroads among the people as yet, for the reception is poor in this region. A great deal of linguistic and sociological research is being conducted on these people. For example, a book was published in 1977 by Kenneth MacKinnon, *Language, Education and Social Processes in a Gaelic Community*. If you are interested in such minute details as the percentage of male Gaelic speakers using the formal second-person pronoun *sibh* to their wives (p. 19) or a poll that asks of the Harris community, "Do girls tend to keep their Gaelic in use better than boys?" (p. 163), then this is the place to turn to.

But in many ways Gaelic is losing ground. Gaelic broadcasting, already infrequent, has recently been cut back even more by the BBC, causing an uproar among Gaelic supporters. An appeal was made to the BBC and a final decision is pending.

Welsh

When we turn our attention to Welsh, the picture has a rosier, healthier look about it. Here we are dealing with a much larger number of speakers -- perhaps around 2 million -- and their firm resolve to keep the language going. Welsh is also easier than Gaelic in that it is more "phonetic" (it is pronounced just about as it is written, while Gaelic is like English in that its spelling includes silent letters, etc.). Radio and TV programs abound; I was able to tape a number of broadcasts during my stay in Wales.

But there is a difficulty in learning Welsh: the initial mutations. Most languages with which we are familiar introduce changes at the *end* of the word (the declensions and conjugations of Latin or Russian, for example). Now imagine a language in which the word changes at the *beginning*. How would you ever find it in the dictionary? You couldn't, of course, unless you knew something about the grammar! There is an excellent example of this in the name of the village where I stayed -- Llanfairfechan. Now, Llanfairfechan means literally "Little Church of St. Mary's." *Llan* is "church" or "parish," a feminine noun. *Fair* is really *Mair* (Mary), but after *llan* the *m* changes to *f*. And the word *fechan* can be found in the dictionary only under its masculine form *bychan*, "small." This is known as the *soft mutation*.

Besides the soft mutation there is a *nasal mutation* involving six consonants:

	Labials	*Dentals*	*Velars*
Voiced	b → m	d → n	g → ng
Unvoiced	p → mh	t → nh	c → ngh

This generally happens after the words *fy* ("my") and *yn* ("in"). Thus, *pen*, "head," but *fy mhen*, "my head."

Finally, there is a *spirant mutation* affecting the consonants *c*, *p*, and *t*. This occurs after the word for "her," *ei*, e. g. *ei phen* = "her head." (To use an English example, "peasant" would become "her pheasant"!)

But aside from this difficulty there is really no problem. The English loan words abound, and the imprint of English is profound in other respects as well; once, in a child's story, I came across the words *Oedd Pwll mewn picil*, "Pwyll was in a pickle," describing one of the characters (Pwyll, hero of the First Branch of the Mabinogion) who had gotten himself into some difficulty. This is hardly the sort of thing that one would expect to find in the original Mabinogion, or in any other writing true to the Welsh spirit!

There are also several Welsh newspapers (such as *Y Herald Cymraeg*), indicating that here again the situation is healthier than for Gaelic, which only has an occasional page or column in an English-language newspaper published in the Hebrides.

It is also easier to find Welsh books. There is, for example, a set of Welsh comic books, designed to teach the language and make it seem like fun; and, though some of the humor is ribald and one senses that beer-drinking must be an important part of the culture, the comic books are nonetheless an effective medium for the acquisition of the colloquial language. There are also graded readers to help one along after he has mastered the rudiments of the language (see bibliography). I was even able to pick up attractive children's books such as *Alice in Wonderland* and *Snow White and the Seven Dwarfs*. The story of Snow White with its Disneyesque illustrations takes place between the Welsh village of Llanfair y Lli and Llanfair y Llwyn. It was also possible to pick up an excellent Welsh dictionary at a very reasonable price, in contrast to the Gaelic one which cost £8 and which I therefore decided to postpone buying.

As one travels the motorways, one sees Welsh signs everywhere. In the June 25, 1977

DOCID: 4019650

issue of *The Economist* in an article entitled "How Bilingual Was My Valley," we are told that the government is spending £10 million to cover Wales with bilingual signs. The article goes on to say:

> "The Welsh Language Society's long efforts at direct action -- raids on television transmitters, bonfires of English-language documents and sit-ins -- have resulted in the Welsh population receiving dual-language versions of all kinds of official forms, from driver's licenses to telephone bills, with even the *p* for pence translated into *c* for *ceiniogau*."

So it appears that an all-out effort is being made for Welsh. In contrast to a tiny corner devoted to Gaelic books at a Scottish book seller's, one finds entire shops in Wales that specialize in Welsh books. In one such shop in Caernarvon the owner, Mr. Eric Jones, told me that after all the tourists go home at the end of August, one hardly hears a word of English spoken in the town until they return in April.

Here, then, is a field that has much to offer the language student. Whether one delves into the medieval or modern phase of Celtic, there is a wealth of interesting literature. It is a field that is not overcrowded and in which much basic work remains to be done. But when one looks at those universities in the United States that offer Celtic languages, one finds that there are only two American universities that have Celtic departments: Harvard University and Catholic University (Dr. Robert T. Meyer, of Catholic, is the only Professor Emeritus of Celtic languages in the country). Elsewhere, Celtic languages are offered within the departments of English or Modern Languages, as is the case at the University of Texas, for example.

Catholic University has an outstanding Celtic collection, having absorbed the libraries of Professor Joseph Dunn and Major William B. S. Smith. These include a complete set of the *Revue celtique* and the rare *Annales de Bretagne*. But the department has remained small due to the shortage of money (they have a $50,000 endowment fund, the annual interest from which comes to only $3000 or so.) People are attracted to the course for a variety of reasons -- some are medievalists or majors in English or linguistics. A small number are actually majoring in Celtic. And then there are people like myself -- people already established in some field who, through a series of circumstances, have caught the Celtic fever and enjoy the subject as a pleasant and rewarding pastime.

Readers who would like to receive a copy of the bibliography prepared by [redacted] *can get one by writing to: CRYPTOLOG, P1, or by calling the editor on 5236s.* (U)

Letter to the Editor

To the Editor, CRYPTOLOG:

I am sure there are many opinions on the questions posed by [redacted] in his article "What Ever Happened to COPES?" (CRYPTOLOG, January 1978). Perhaps the questions that should be answered is: What has COPES done for *us*? Have we increased our understanding of the target? Has output level been maintained with less collection resources? Is collection management easier? I believe the middle managers (some of whom must have been workers in early days of COPES) would have "taken hold of COPES and made it their own" if it had demonstrated its utility.

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

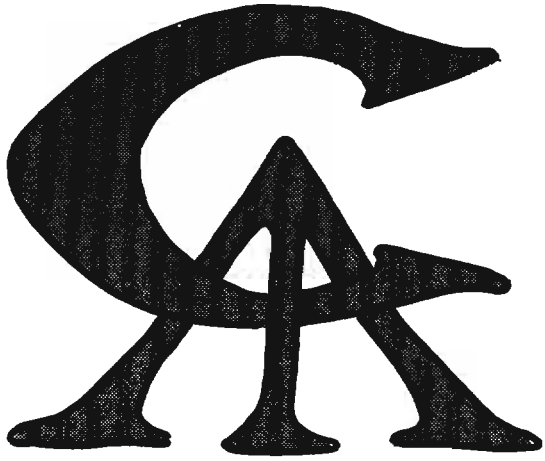
[redacted]

Eugene A. Gilbertson,
[redacted] ~~(C - CCO)~~

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4019650



News of the Communications Analysis Association

By [redacted] P14

P.L. 86-36

How do you like our new logo? As mentioned in last month's News of the CAA, the winning entry was sent in by [redacted] We had hoped to have a professionally drawn version of it for this month's issue, but we were late in asking Graphics to do it for us. In the meantime, to appease your curiosity, here it is, in a version based on the winner's original sketch. In case you don't know why you like it so much, Hugh explains that "The design is the basic monogram based on Classic Roman Capitals, arranged to give an impression of breadth and upward motion."

(U)

Monthly Meetings

The CAA is on the move again, in all its breadth and upward motion! Our board meets once a month, usually around the end of the month, but the exact time and room change from one month to another. But the meetings are open to all, members or others. If you want to come try and look us over before deciding whether to associate with the likes of us, please do so. We won't even swear you to secrecy about all the wild things that go on at the meetings. If you're afraid to come alone, bring a friend. Where and when? To tell you the truth, as I write this (in April) I don't really know. But as you *read* this (in June), you can find out. Just check with your nearest CAA member, or with any of the CAA Board members listed below. Or, if you're already a member, watch for the notices arriving in your in-basket.

(U)

[redacted]

~~(SC)~~

CAA Program Committee

Our Program Committee, chaired by [redacted] has been busy, too. The committee includes:

[redacted] 5617s
8379s
3505s
4226s

In addition to the monthly meetings of the Board, bimonthly meetings of the Special Interest Group on Cryptologic History, and operational briefs, the Program Committee has lined up the following speakers:

28 June [redacted]

(?September?)

Any ideas for other presentations or other speakers? Let the committee know.

(U)

Meet the CAA Secretary!

[redacted] more generally known as Betty, P.L. 86-36 is currently Secretary of the CAA. She came to an early predecessor of NSA as a French linguist but was shunted to cryptanalysis, where she has dwelt happily ever since. Her assignments have covered problems that are now handled in A, B, and G; she has held technical management positions at section, branch, division, and office staff levels; and she now heads the Cryptanalysis Division in the National Cryptologic School. She is a member of the Crypto-Linguistics Association and of the CAA Special Interest Group on Cryptologic History. She is also an EEO Counselor, President of the Patuxent Business and Professional Women's Club and editor of its Newsletter; the former editor of the WIN (Women in NSA) *Newsletter;* former Cryptanalysis Editor of CRYPTOLOG, and Rewrite Editor of its predecessor *Dragon Seeds*.

(U)

Communications Analysis Association:

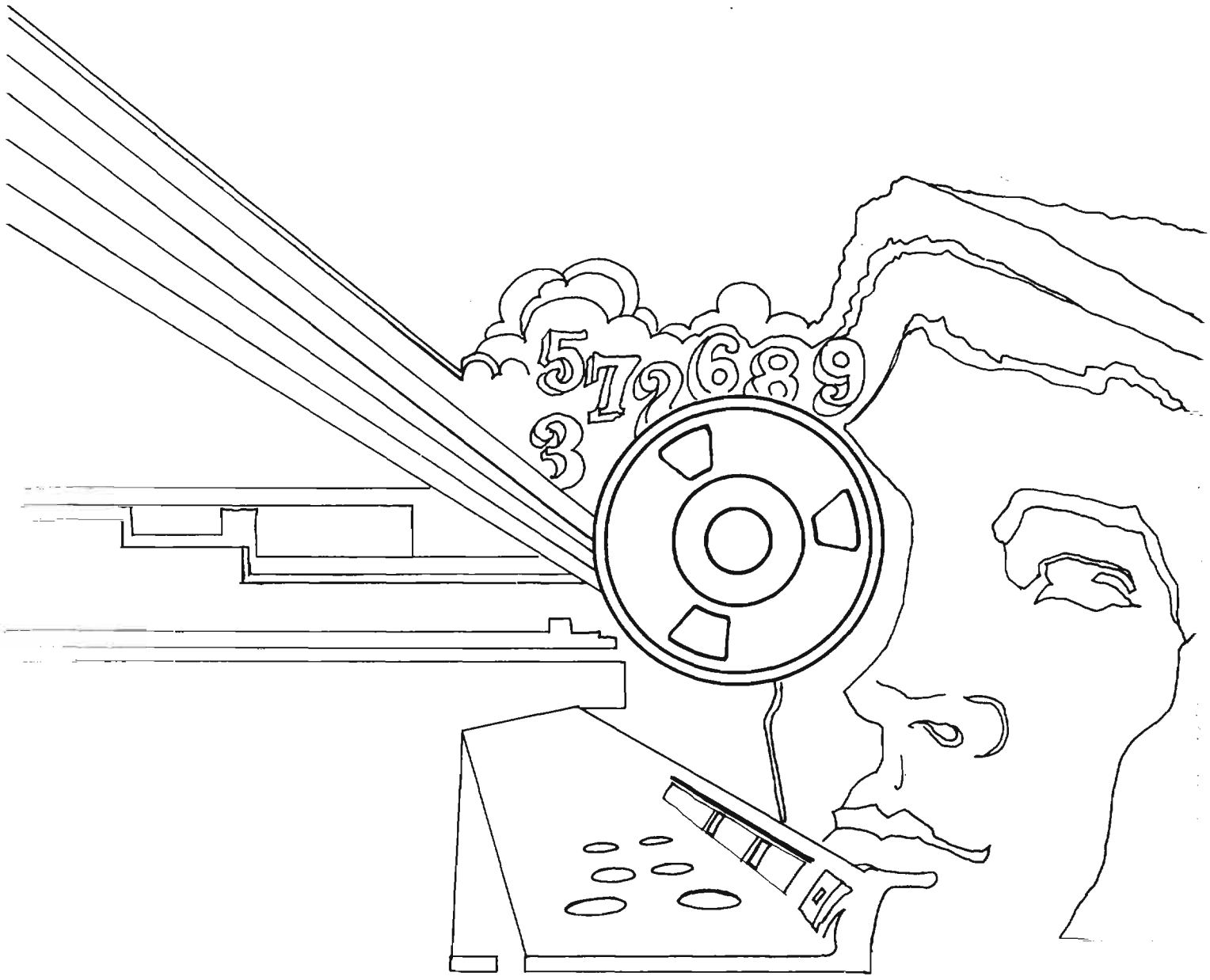
President	David Gaddy	3247
President-elect	Frank Porrino	5879
Secretary	[redacted]	8025
Treasurer	Tim Murphy	3791
Board members	[redacted]	4935
		5991
		3573
		3369

P.L. 86-36

P.L. 86-36
EO 1.4.(C)

P.L. 86-36

P1-MAY 78-S3-26425


5 7 9 6 8 9
3

DOCID: 4009811

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MAY 1978

THE FUTURE OF CRYPTANALYSIS.....William Lutwiniak....1
CALLSIGNS AND W.A.R.C. 79.....[redacted].....4
T.A. IMPLICATIONS OF F.C.C. PROPOSAL.....[redacted].....7
PROJECT UTENSIL: DATA DICTIONARY/DIRECTORY..[redacted].....9
UNCLE-A SAM WANTSA YOU!.....[redacted].....13
C.A.A. NEWS.....W.E.S.....14
THE JOYS OF UNIX.....[redacted].....15
THE EDITOR'S PAGE.....19
NSA-CROSTIC NO. 14.....Sardonyx".....20

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009811

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. V, No. 5 MAY 1978

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5642s)
Collection.....[redacted] (8955s)
Cryptanalysis.....[redacted] (4902s)
Language.....[redacted] (5236s)
Machine Support.....[redacted] (5303s)
Mathematics.....Reed Dawson (3957s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....[redacted] (4477s)

Production Manager.....Harry Goff (4998s)

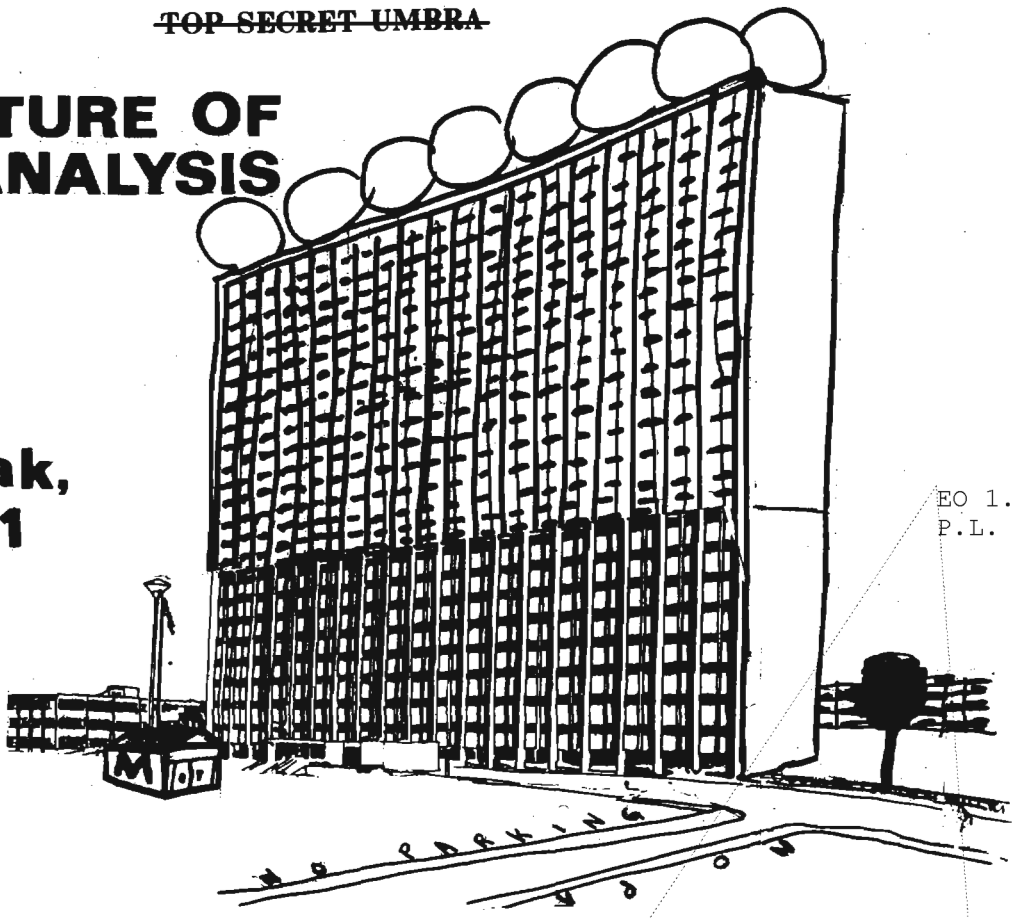
P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4009811

THE FUTURE OF CRYPTANALYSIS

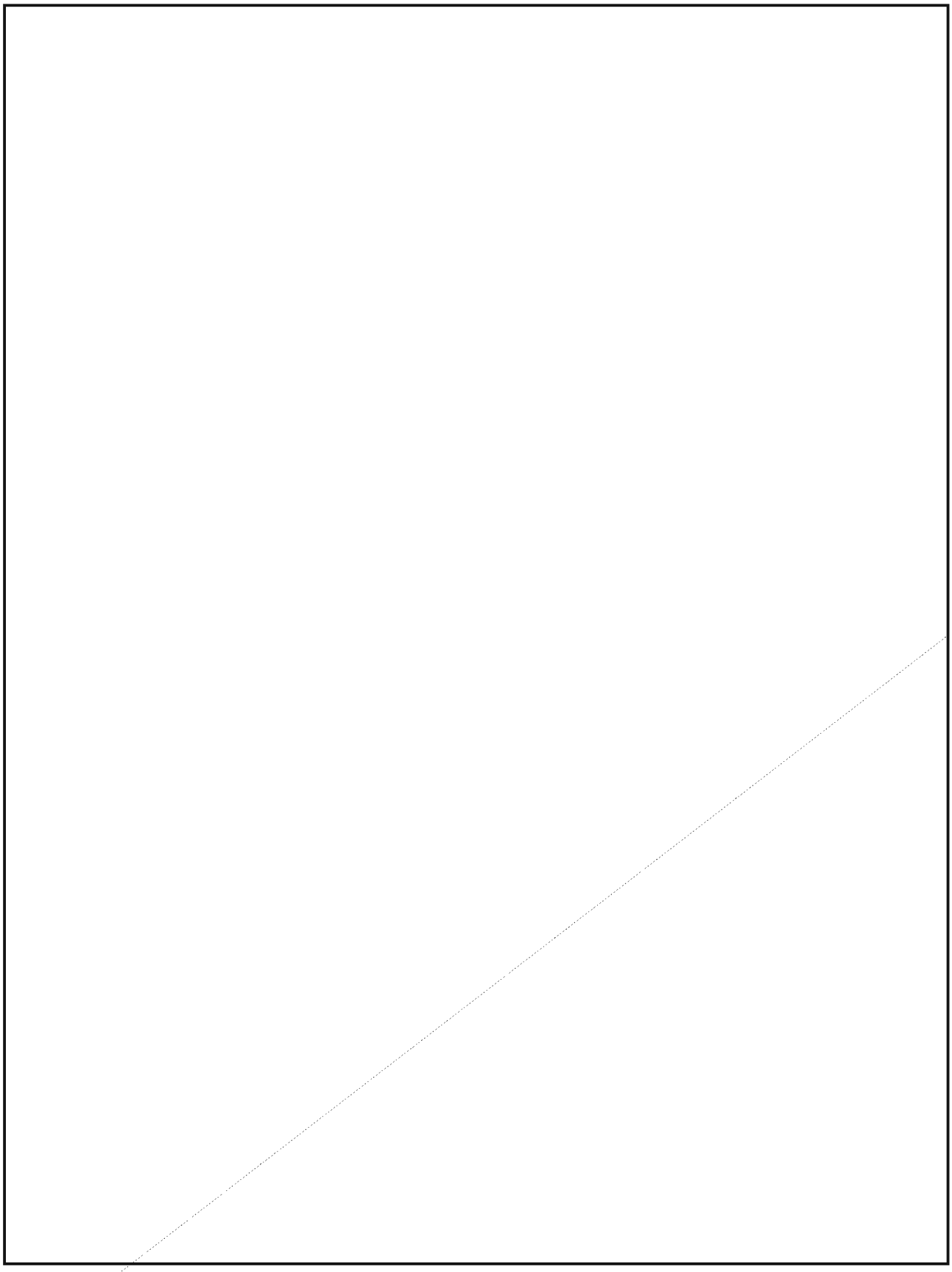
William Lutwiniak, Chief, P1



EO 1.4.(c)
P.L. 86-36

The second most frequent question I'm asked (the first concerns promotions) is "Does the cryptanalyst *have* a future?" Predicting is a risky business. Did you happen to catch, in all the school closures and cancellations announced on the radio on that snowy Friday last week, the postponement of the meeting of the Clairvoyants Society?. . .

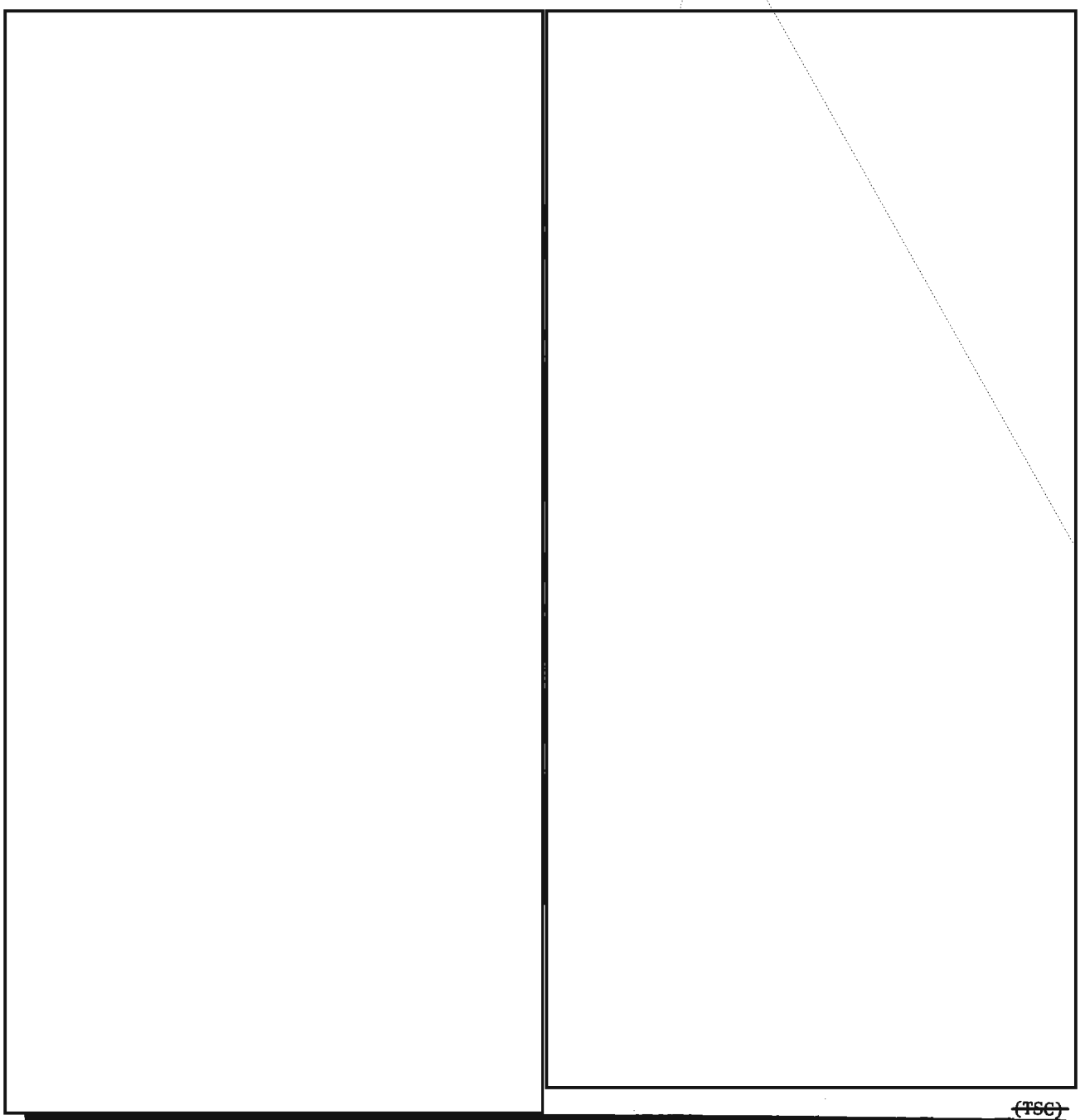
Complete text of the keynote address delivered by Mr. Lutwiniak on 24 January 1978 to the third annual seminar-workshop series "Cryptanalysis: Contemporary Issues." The series is offered as a course (CA-305) by the Cryptanalysis Division of the National Cryptologic School. Other papers presented during the 1978 series will appear in future issues of CRYPTOLOG.



EO 1.4.(c)
P.L. 86-36

DOCID: 4009811

EO 1.4.(c)
P.L. 86-36



~~(TSC)~~

Do you want to attend next year's seminar?

The seminar-workshop "Cryptanalysis: Contemporary Issues" is offered every winter by the Cryptanalysis Division of the National Cryptologic School. It is designed to bring SIGINT and COMSEC cryptanalysts, cryptologic mathematicians, and other interested persons up to date in the status and trends in the current practice of cryptanalysis. Speakers from various parts of the Agency make presentations covering cryptanalysis and related fields.

Usually the seminar lasts three days. It consists of the keynote address (delivered in the Friedman Auditorium) and 15 smaller presentations. Each presentation is given twice. To receive credit, participants must attend the keynote address and five presentations.

The seminar, which changes every year, attracts participants from throughout the Agency. If you are interested in attending the 1979 seminar, look for the course announcement in December 1978. If you haven't seen it by Christmas time, check with your training coordinator. Distribution may have slipped up. J.E.D. (U)

CALLSIGNS AND WARC 79 [redacted] P13

747 Table of Allocation of International

The Federal Communications Commission (FCC) has proposed a significant change in radio callsigns for WARC 79 (World Administrative Radio Conference, Geneva, 1979), namely, that callsigns be *unique* and capable of fully *automatic* monitoring. FCC also proposes that such unique callsigns be applied to every transmitter or transmission "which *could* propagate" (italics added) beyond the boundaries of the country to which they belong. The FCC also wants to drop from the radio regulations the exemption for military transmitters. This scheme, if it is presented as the U.S. position at WARC 79, could have a marked effect on SIGINT and COMSEC of many countries, and hence deserves notice.

The unique callsign scheme was presented by the FCC in its Fifth Notice of Inquiry (NOI) for WARC 79, published in *Federal Register*, 31 May 1977. The specific language appears in Appendix 3 as proposed changes to the *Radio Regulations* of the International Telecommunication Union (ITU) and as Resolution G-C.

Resolution G-C, "Relating to Automatic Identification," states, in part:

> "The General World Administrative Radio Conference, Geneva, 1979, considering
>
> a) the state of the art in respect to identification
> b) the need for unique identification
> c) the possibility of inadvertent operator error
> d) the ever increasing number of active transmitters not only within existing administrations but also noting the ongoing assignments of new call sign and selective calling systems
> e) the economics of presently available equipment which is directly applicable to automatic identification
> f) the possibilities for use of automatic, faster message transmission service in conjunction with automatic identification equipment
> g) the increased ease of resolving cases of harmful interference and of ensuring compliance with the provisions of the Convention and the Radio Regulations
>
> resolves
>
> 1. that administrations shall implement automatic identification as provided in Article 19 MOD [= *mod*ification -- see below] *at the earliest possible time*, and
> 2. that automatic means of identification should be adopted by *all* administrations." (Italics added.)

The FCC then proposes substantial changes to *Radio Regulations* Article 19, "Identification of Stations." It proposes replacing the current (1976) No. 735 with MOD 735, as follows:

Current 735 "Transmissions without identification or with false identifications are prohibited."

MOD 735 "Transmissions and *transmitting stations* shall be *uniquely identified*. Administrations shall make every effort at the earliest possible time to introduce and use automatic identification. On frequencies assigned for international use, means recommended by CCIR [International Radio Consultative Committee, of the ITU] shall be utilized." (Italics added.)

The FCC then proposes the suppression of the current Nos. 736 and 737A of the *Radio Regulations*, in order to remove exceptions to the modified No. 735. No. 736 currently provides an exemption for survival craft and emergency radio beacons; the FCC would eliminate this exemption in favor of callsigns that satisfy MOD 735. No. 737A currently provides an exemption for some space stations (e.g. satellites), which exemption would also be eliminated. No. 737A specifies various acceptable kinds of callsigns, station identifications, or selective call numbers -- which the FCC would accept.

No. 738 would remain unchanged. It specifies regular identification signals, at least hourly, and ends with the statement that ". . .administrations are *urged* to ensure that wherever practicable, superimposed identification methods be employed in accordance with CCIR Recommendations." (Italics added.)

Nos. 739, 740, and 741 would be suppressed. No. 739 states that the identifying signal shall be transmitted by methods which "do *not* require the use of special terminal equipment for reception." (Italics added.) Nos. 740 and 741 also conflict with the automatic monitoring and uniqueness requirements.

The FCC gives as its reason for suppression of Nos. 736 and 737A, "To provide universal, unique, and automated identification." Its reason for suppression of Nos. 739, 740, and 741 is "Consequential to above proposals."

The FCC then proposes that No. 742, which allows each ITU member to establish "its own measures for identifying its stations used for national defence," be suppressed. The FCC gives as its reason for this proposed suppression, "Unnecessary to incorporate Convention

provisions in the Radio Regulations" (that is, the general authority for national defense stations is given in Article 38 of the Convention). However, the deletion of No. 742 is clearly intended to encourage and facilitate the unique identification of military transmitters and transmissions. The treatment of No. 742 at WARC 79 could produce interesting alignments of countries.

The clearly stated aim of all this would be to allow automatic monitoring of all radio stations by causing them to transmit unique callsigns or identification numbers in an automatic and standardized way. The adoption of this regulation would affect millions of stations -- fixed and mobile, CB, radio-amateur, and earth satellite -- which currently are not required (47CFR 25.206) to identify themselves in the United States and in 150 other countries. It would completely change the economics and practical aspects of radio monitoring, interference notifications, and regulatory enforcement in developed countries where there are numerous radio transmitters. It would also have a marked effect in the ITU allocations and statistical studies of the HF spectrum. Although millions of transmitters which already use callsigns would be affected, the FCC proposal does not stop there.

"Harmful Interference" vs. Capability to "Propagate Internationally"

In Section II, "Allocation of International Series, and Assignment of Call Signs," of Article 19, the FCC further proposes a significant regulatory change which would markedly increase the number of stations to be assigned unique international callsigns. No. 743 now reads,

> "All stations open to the international public correspondence service, all amateur stations, and other stations which are capable of causing *harmful interference* beyond the boundaries of the country to which they belong, shall have call signs from the international series allocated to each country as given in the Table of Allocation of Call Sign Series in No. 747." (Italics added.)

Here the deciding criterion of "other stations" is that of "harmful interference," which is defined in Annex 2 of the 1973 ITC (TIAS 8572) as

> "any emission, radiation or induction which *endangers* the functioning of a radionavigation service or of other safety services, or *seriously degrades*, obstructs or repeatedly interrupts a radio communication service operating in accordance with the Radio Regulations." (Italics added.)

This is a stringent criterion which requires the occurrence of sustained severe interference. Hence most stations are not required to use international callsigns, and the burden falls on the victim to prove the harm and identify the station exerting the "harmful interference."

The modified language the FCC proposes is quite different, namely:

> **MOD 743** "Each station whose signal *could propagate* internationally shall uniquely identify itself such as by a call sign formed pursuant to No. 747. Identification shall preferably be by automated means using the applicable Recommendations of the CCIR. (See Resolution G-C)." (Italics added.)

This is clearly a completely different criterion, for "harmful interference" does not have to manifestly occur. Instead, the criterion is merely the technical *capability* for detectable propagation across a national border, into the international ocean areas, or into international space, particularly the equatorial geostationary satellite orbit, which is becoming crowded.

The effect of MOD 743 would be to require that a much larger population of transmitters, all over the world, send unique identifications in a manner that could be automatically monitored. Tens of millions of transmitters, particularly mobile stations, would be affected by this.

Considered in a U.S. context, virtually all mobile and CB transmitters which *could* propagate across national borders would be affected. Earth satellite stations and even radio relay stations near borders would be affected. The modified language of 743 also requires that each station "shall uniquely identify itself," while the existing language only requires that it "shall have" a callsign. This imposes a requirement for automatic identification whenever a transmitter comes on the air, rather than at the operator's discretion, and the use of improvised or changing callsigns, as in CB, would not satisfy the new regulatory language. The FCC has been trying for some years to get automatic identification features into mobile and CB radio (e.g., Docket 2437) and this has been fought by the radio industry. But if WARC 79 adopts such a provision, then Regulation 47 USC 303(R) will make that new Radio Regulation applicable to the United States, and FCC-type approval can exclude all new transmitters which do not satisfy this requirement.

Considered in a foreign context, the adoption of such regulations not only will affect internal radio operations and monitoring, but will also produce a great increase in radio negotiations between countries and in the reports to the ITU, IFRB, and CCIR as countries attempt to reduce the interference their stations cause or suffer. Automatic monitoring, with computer analysis

DOCID: 4009811

EO 1.4.(c)
P.L. 86-36

and accounting, will lead to much more complete models of propagation. Morever, it will provide a great deal of data about radio traffic activity.

One other proposed FCC modification -- to Article 16, "Reports of Infringement," reads,

> "If an administration has information of an infringement of the Convention or Radio Regulations, committed by a station *over which it may exercise authority*, it shall ascertain the facts, fix the responsibility and take the necessary action." (Italics as in text.)

The FCC states that this change is "To permit action against possibly unauthorized stations committing infringements." This closes a legal loophole by which a country could ignore violations by a transmitter in its territory by claiming it had *not authorized* the station.

Aggregate Effect of FCC Proposals

The aggregate effect of the modifications to Articles 16 and 19 and of Resolution G-C would be to establish a framework for global automatic monitoring and much tighter enforcement of radio laws and regulations. If these proposals, or something like them, are adopted at WARC 79, the global radio spectrum will be a much more tightly managed resource, and international engineering of radio systems will become a standard phenomenon, rather than a rare one. The Soviet delegate to CCIR, Sviridenko, favors such central planning, management, and engineering of the radio spectrum, using computer propagation models (largely developed by the United States). At present the "priority rights" of current spectrum users, especially in HF and space systems, are defended by the industrial nations because radical changes in allocations and radio links would produce unpredictable effects. With global automatic monitoring made economical and practical, much more intensive use of the spectrum could be undertaken and propagation effects predicted. Interference, or any infringements, could be quickly identified, and corrections demanded under Article 16. All this would produce a great deal of change in radio usage and data about radio traffic over the next 25 years, particularly in the congested regions of the spectrum.

Effect on U.S. and Foreign COMINT and COMSEC

The unresolved questions is how this will affect U.S. SIGINT and COMSEC, and corresponding foreign SIGINT and COMSEC.

HISTORICAL NOTE ON MILITARY CALLSIGNS

J. A. Meyer

Since the first international radio treaty in 1906, nations have always reserved complete freedom for their military and naval stations, opposing international regulation except with regard to distress messages and interference. This is expressed in Article 38 of the 1973 International Telecommunications Convention (TIAS 8572). The United States has always maintained this same reservation. Section 303(o) of the Communications Act of 1934 states that the FCC shall "have authority to designate call letters of *all* stations" (italics added). Section 305(a) of the same Act provides an exemption for government-owned stations, as follows:

> "Radio stations belonging to and operated by the United States shall not be subject to the provisions of sections 301 and 303 of this Act."

But then the exemption is reduced for *callsigns* by Section 305(c), which states:

> "All stations owned and operated by the United States, except mobile stations of the Army of the United States, and all other stations on land and sea, shall have special call letters designated by the [Federal Communications] Commission.
>
> (Note that the word "except" pertains only to "mobile stations of the Army of the United States.")

Therefore the removal of No. 742 would reinforce the authority of the FCC to assign callsigns to U.S. military stations under 47 USC 303(c). Even the basic concept of freedom for national defense stations, as declared in Article 38 of the ITC was challenged by the USSR in 1932 when that government was first invited to the ITC in Madrid. The Russians proposed that military stations be regulated by the same rules as nonmilitary stations, and although that proposal was defeated, the challenge might be resurrected at WARC 79, where the USSR could expect greater political support than in 1932. If No. 742 is deleted at WARC 79, as the FCC proposes, a considerable effort by U.S. COMSEC to get U.S. military stations to use changing callsigns would be undermined. Hence the FCC proposal would affect U.S. security unless 47 USC 305(c) is amended to compensate for this.

~~(FOUO)~~

EO 1.4.(c)
P.L. 86-36

[redacted]

The FCC, in issuing these proposals on 31 May 1977, invited comments. At that time the Office of Telecommunications Policy (OTP), a White House staff group established in 1970, was the official organ for coordinating and presenting the comments of the government to the FCC. The deadline for the comments on this fifth NOI has passed, and the next NOI is expected in early 1978. The OTP is being disestablished, and it is not clear where the coordination function for NOI responses will eventually land. The Department of Defense, as the largest user of international telecommunications in the world, has a special status and in 1973 was a member of the U.S. delegation to the Plenipotentiary Conference of the ITU. Other government departments respond directly to the NOIs, and the Department of Defense could also reply directly, particularly where national security considerations apply.

The FCC proposal for unique, fixed, automatically recognizable callsigns, having been presented as the public position of the U.S. government in the *Federal Register*, will be widely read around the world and may be introduced and supported by other countries at WARC-79, whether or not the United States presents it.

The FCC proposal represents a consolidation of ideas which have been emerging and finding application -- especially in aeronautical mobile and maritime mobile radio communications -- for some years. Selective calling systems and automatic monitoring equipment, as the FCC notes, are already in service and have proved their value. These facts will be noted at WARC 79. The FCC proposal is a logical generalization of existing practices and a recognition that automatic monitoring -- and the automatic identification of practically *all* transmitters -- is an essential condition for radio planning and management for the next 20 years and beyond.

Effect on Agency's Mission

[redacted]

~~(C - CCO)~~

T.A. IMPLICATIONS OF F.C.C. PROPOSAL

P.L. 86-36

P14

[redacted]

~~(S - CCO)~~

EO 1.4.(c)

DOCID: 4009811

~~SECRET~~

EO 1.4.(c)
P.L. 86-36

[redacted]

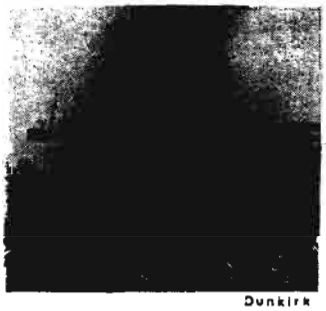
[redacted]

~~(S-CCO)~~

Solution to NSA-crostic No. 13

By [redacted]

(CRYPTOLOG, April 1978)



Dunkirk

P. [William] Filby, "ULTRA [Was] Secret Weapon [That Helped Defeat Nazis]," CRYPTOLOG, December 1975 (U).

"Unhappily, it was not unusual for holders of the German [decrypts] to have to forgo using them for fear of compromising the cypher break. One such occasion was the bombing of poor Coventry; enemy plans were known beforehand, but to defend the city would have aroused German suspicions."

(U)

Answer to "Telephone Problem II"

By [redacted]

(CRYPTOLOG, April 1978)

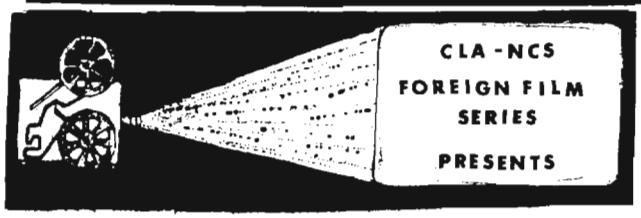
P.L. 86-36

The upper right-hand corner of the covername allocation is:

OVAL	ROWBOAT	-	ADAGE	-	FIGHTER
ALBUM	COMPRESS	-	LACEWING	-	SCHOOLBOY
	PESO	SEEDLING	TONIC	APEMAN	COUNTRY
			GERUND	LOUVER	PLODDER
				TYPHOON	BARRETTE
					MESA

Once you recover the method of generation, can you deduce the *source* of the covernames?

(U)



The Crypto-Linguistics Association and the National Cryptologic School will present

in May: "The Shop on Main Street" (in Czech, with English subtitles)

Friday, 5 May, 0930

in June: "Heroes of Shipka" (in Russian, with English subtitles)

Thursday, 8 June, 0930

Both films will be shown in the Friedman Auditorium. All are welcome.

Announcements with details about the films will be mailed to CLA members and will be posted throughout the Agency. Look for them. We'll see you in the Auditorium! B.Y.O.P.C.

(U)

~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4009811

P.L. 86-36

PROJECT UTENSIL:
The DDO Data Dictionary/Directory

P13

What *is* a data dictionary/directory? Just as an ordinary dictionary contains information about words, a data dictionary contains information about data. It does not contain the actual data that forms the data files, but contains pertinent information about that data, its attributes, and relationships. There are many definitions in the commercial world, but what the dictionary contains is information in two forms:

- the "what" information -- the *data dictionary* (description of the data elements); and
- the "where" information -- the *data directory* (the location and use of the data elements and their relationships to other data elements, records, files, procedures, etc.).

Why Combine the Two?

By combining the dictionary and the directory into a single "data dictionary/directory" we have the ability to provide:

- coordination and control in systems development;
- assistance in search for relevant data during design;
- a means of identifying and reducing data redundancy;
- an increased data-transfer capability between systems;
- data standardization;
- administrative support;
- documentation support;
- data-definition support.

Thus, the system provides a versatile tool for managing the DDO data resource.

Brief History of Data Dictionaries

Data dictionaries are not new, either in the commercial world or within the government. Their existence is related to, and probably can be entirely attributed to, the Data Base Management Systems (DBMS) and many are an integral part of a DBMS. The National Bureau of Standards has published an extensive report on seven of the commercial dictionaries and eleven government-agency systems.

Slightly edited version of a talk given in 1977 at two meetings of CISI's Special Interest Group on Information Processing Systems (SIG/IPS).

The National Bureau of Standards also sponsored a Federal Information Processing Standards (FIPS) task group -- TG-17 -- specifically to address guidelines for establishing data dictionary/directory systems. That task group published its report in late 1977.

NSA also has several data dictionary efforts in various stages of development. They are:

- TEDS, in W, which uses a data dictionary on the M-204 computer system that has been operational for some time;
- an effort in A to utilize the TEDS experience in developing a dictionary for STEPSTONE on the M-204;
- HOLLYHOCK, a project to support L, M, N, and E, which will use a data dictionary developed on the M-204 by T33;
- INLAND, a project to maintain continuity on R tasks, which uses a data dictionary developed in R;
- an IBM data dictionary that is being used on a system developed for a field site by T; and
- the most recent addition, the Cullinane Data Dictionary, which was purchased by T for use with the IDMS Data Base Management System, and which is currently being evaluated.

DDO's Need for a Data Dictionary/Directory

Why does DDO need a data dictionary/directory? If you have ever attempted to solve a problem that required you to find all the possible files, manual or machine, that might contain information about your particular subject, you know one reason why we need a data dictionary. For those of you who have never made that attempt, I have an example of such a situation. About 2 years ago I was asked to help locate all the data files containing geographic coordinates, grids, and/or other means of identifying a point on a map. The requester also wanted to know if there was any associated software to process the geographic information for selecting records by area. I found no means to locate either the files or the software without surveying each organization. How, then, do managers answer questions from auditors, customers, and the Director if there is no means to assure that they have all the information?

Other questions that a data dictionary/directory system might answer are:

- How many programs in the COBOL language are there on each machine?
- How many A files are resident on the IBM 370/168 system?
- Is there a standard for aircraft type?
- What files contain aircraft types associated with the Bulgarian or Hungarian air forces?
- How many B FORTRAN programs are there for the IBM 370/158 system?
- What computers are on the NSA Network (PLATFORM)?

Another illustration of a dictionary's use comes from [redacted] presentation on the G project, GEISHA, in which he discussed their current operations and the problems that G has encountered. He explained that one of the problems is the existence of many individual processes carrying out similar functions. Elimination of duplication and related ills requires a coordinated effort to create a single G system.

Think of DDO as being similar to what Mr. [redacted] reported about G processes. Many individual processes? Similar functions? Duplication? . . . The fact is that there is a system for A, a system for B, a system for G, a system for V, and a system for W. I do not propose that we design a single system for DDO as a whole, but a data dictionary containing descriptions of all the systems in common terms would eliminate many problems, or, at the very least, would help us to recognize problems where they exist.

Let's take a look at ourselves in DDO and diagnose the situation. The DDO organization contains several Groups with similar functions, such as TA and CA. This results in similar computer processes because the analysts' needs are similar. Therefore, it follows that data bases to support these functions will be nearly identical in structure. Well, similar or nearly identical, but not necessarily recognized as being such, because DDO is organized by *area*, and, since each is supported by different computer experts, the design of similar data bases would be different. Add to that the different terms used by analysts in each area and discipline, along with the use of acronyms and abbreviations, and it would be impossible to recognize the similiarities between data bases unless you carried out a thorough study. Therefore we need to agree upon common names and definitions for common fields of information.

Another situation is the result of the size of the Agency and the number of files required to support its functions. PLATFORM, a project to link computers, will make access from one computer to another a reality. I contend that having access to one or more machines doesn't give me any capabilities I don't already have, unless I have an inventory of what is available on those computers. Just having an inventory isn't enough, either, if you don't know how to identify or access a file. You also need to know more about the file if you plan to use it.

Take the following hypothetical example. For some research reason you would like to know the number of current NSA male employees with blond hair, born in New York City, who were hired by the Agency between 1956 and 1970. You want to be sure you have looked in all files which could possibly have information to answer your query. But you do not want to search files which wouldn't possibly have the proper information. With a data dictionary/directory data base containing pertinent information about all the available files, you could narrow your search to only those files which contain information about Agency employees, city of birth, date of hire, and color of hair. The system would then provide from the contents of the data dictionary/directory data base all the information available either on how to extract the information yourself or who to contact to get what you are looking for. This example isn't a typical DDO problem, but it enables me to add that the system would not allow you information about files if you do not have need-to-know or proper credentials. You would have, at minimum, identification of all files which could help you get your answer. P.L. 86-36

So the solution to our data-management problem is to to have a DDO Data Dictionary/Directory. With that dictionary/directory we would no longer have the situation in which the same data, used in two data bases, would be described differently.

Yes, the DDO Data Dictionary/Directory can be the solution, but only if the contents and the data base are current and accurate and if they represent all facets of the DDO data resource. Descriptions of our data elements, data fields, records, files, and data bases are required to build the Dictionary/Directory data base. The following are two examples of descriptions of *data elements*:

DATA ELEMENTS

Name	Social security identification
Abbreviation	SSN
Synonym(s)	Social security account number
Definition	A unique indication of an individual and his Social Security account
Date approved	710701
NDSC identification	NI-0003
(Etc.)	

DOCID: 4009811

Name	Sex
Abbreviation	-
Synonym(s)	-
Definition	The division of human beings into groups based on physiological characteristics
Date approved	710225
NDSC identification	00056
(Etc.)	

The following is an example of a *record*, which can consist of one or more data elements:

RECORD

Name	Personnel record
Abbreviation	PERS RCD
Synonym(s)	-
Definition	The record of a specifi NSA employee
Field 1:	
Name of data element:	Social security number.
Length:	9
Configuration:	Numeric
Update authority:	M3
(Etc.)	
Field 2:	
Name of data element:	Sex
Length:	1
Configuration:	Alphabetic
Update authority	M3
(Etc.)	

What information, then, should we collect for inclusion in the Dictionary/Directory data base? What are the data elements? What are their defintiions. Where are the data elements used? The document "Data Standards for SIGINT Activities," promulgated as Annex A of USSID 414, is the only centrally documented source of data elements with definitions. A Computer Record Format File documents some computer jobs with field names. Except for the published standard Data Elements, these field names -- which are arbitrarily assigned -- are subject to the problems referred to earlier: different terminology and ideas about similar fields. Therefore, we have different fields represented in several files under the same name, and the same field represented in several fields under different names. To use everyday examples, assume that one file contains information on "STOCK" (in the sense of "livestock," with data pertaining to sheep, cattle, hogs, etc.) and another file contains information on "STOCK" (in the sense of "shares", with data pertaining to IBM, General Motors, etc.). If you sit down at the terminal and ask for "STOCK INFORMATION," you will get information you want, plus information you *don't* want:

```
"HOGS       14678 . . .
 IBM        2/3478/87.62/. . .
 SHEEP      12345 . . .
 CATTLE     98362 . . .
 GEN MTRS   4/9231/93.46/. . ."
```

Conversely, if you sit down at the terminal and request information on "CARS" manufactured in the United States, and get the response "REQUESTED DATA NOT FOUND - CARS = 0", it could be because File 1 contains information on "AUTOMOBILES, etc. (Foreign)" and File 2 contains information on "VEHICLES, etc. (U.S. manufactured").

So you can see that a lot of hard thinking goes into getting the terminology right, instead of just dumping all the information into the data base and causing retrieval problems later. Another consideration is that the contents of the data base for the Dictionary/Directory must have amplification information concerning every level that is to be described (see Fig. 1).

DATA LEVELS

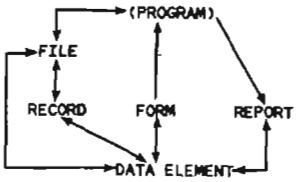


Fig. 1

In order to have reference terms with which we can relate, we shall refer to specific data levels as *entities*. Entities will be distinguished from one another by *attributes* -- descriptors that identify or characterize entities and help to establish relationships within the entity or among entities). The following are some of the attributes:

Identification

- Name
- Abbreviation
- Synonym(s)
- Reference(s)

Description

- Narrative
  - Purpose
  - Scope
- Physical
  - Sequence
  - Size
- Organizations
  - Responsible organization(s)
  - User organization(s)
- Dates
  - Implementation
  - Change
  - Other

(Etc.)

Fig. 2 illustrates some of the entities and their hierarchical relationships. The data

DOCID: 4009811

entities include "data base/file," "record," "data element," etc., which describe storage information. All entities above the data levels are the functional or management entities and, you might say, provide the reasons why each data element exists. By that I mean that there is a functional reason -- or should be -- for each data element, and that requirement is dictated by one of the entities above the data levels. Attributes form the actual contents of the Data Dictionary/Directory data base. We therefore would have attributes for every entity used by DDO to accomplish its data processing.

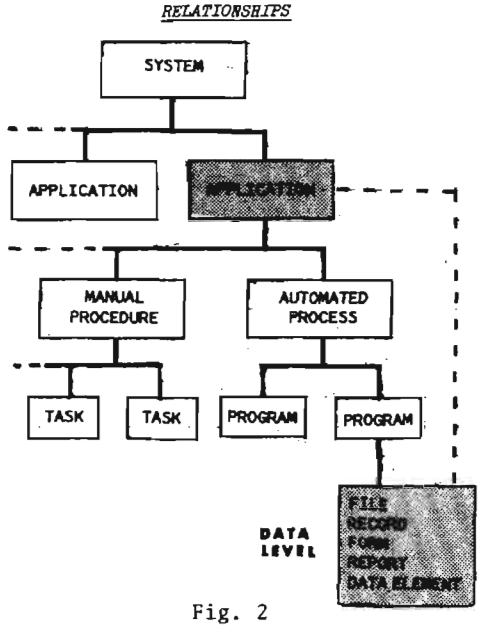


Fig. 2

Fig. 3 is a representation of the dictionary/directory data base -- not how it is actually constructed, but how we visualize it functionally. The

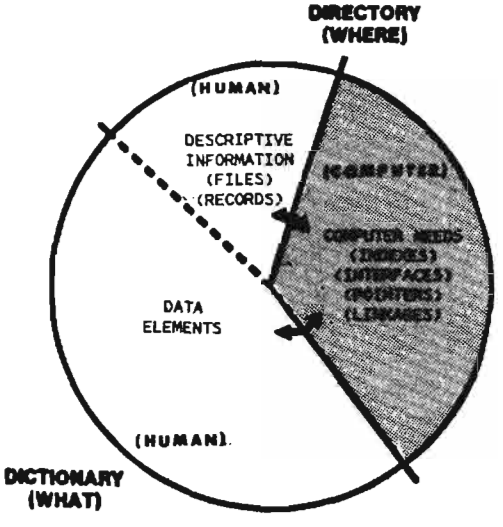


Fig. 3

"what" information is made up of the attributes describing the data elements, and the "where" information" is made up of the attributes describing the records, file, etc. The human aspects I refer to are those descriptions and definitions which are input or used by individuals in a form they can understand. And, finally, the figure shows the machine needs for the computer to maintain the system and the relationships among the entities. The arrows going in both directions indicate that the software uses information *from* the user, as well as providing information *to* him.

Project UTENSIL

I've covered the description of a data dictionary and a few of the uses that DDO could make of such a system. Now I should give you some background on Project UTENSIL. A task force was established by DDO in July 1976 as a result of an A memorandum suggesting the creation of a Data Dictionary/Directory for DDO. The task force forwarded a statement of requirements to C (now T) in February 1977. The project is currently in the fact-gathering and problem-specification stage.

The potential of a DDO Data Dictionary/Directory as a tool is limited only by the degree of commitment to the concept that data is a resource to be managed like people, money, or any other resource. Initially, the DDO system at minimum will be aimed at providing a central computerized resource of information about DDO data. It will provide a capability to show data relationships to all levels contained in the data base, with retrieval capabilities. As with most online systems, there will be input and update capabilities to maintain a current file.

The design of the system must be such that new capabilities can be added without affecting those incorporated in the original design. Therefore, I believe we have to make a careful evaluation of the full potential of a data dictionary/directory for DDO to assure that we design the initial system to be flexible enough to allow for any possibility. The fact that we already have several dictionaries available in the Agency proves that dictionaries are feasible, but at the same time it demonstrates that, given the lack of central management, each dictionary has its own merits and shortcomings. What we need is clear, concise direction from management concerning its goals with regard to managing data. Then we can clearly plan not just the short-term goals of a dictionary, but also the data dictionary/directory system as a tool for the long term.

The data dictionary/directory can be just a glossary of terms used by only a few technicians, or, with good planning, it can develop into a tool to be used at all echelons. The uses of a data dictionary/directory system and its data base will be limited only by the ingenuity of its users.

DOCID: 4009811

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

[redacted]

G51

Every time someone defines a "bigamist" as what an Italian calls a dense fog, I am reminded of the article by Robert E. Gould in the December 1975 CRYPTOLOG ("Linguists from the Melting Pot"). The author's main point was that the Agency's dream of recruiting successful translators from ethnic neighborhoods was being frustrated because the aspirants were not working out. Using examples taken from English as spoken by Italian immigrants, he claimed that "anglicisms" had polluted the applicants' *foreign* language so badly that they did not have a chance of succeeding. What he asked those potential translators from ethnic neighborhoods, in effect, was not "What'sa matter? You no spicka da English?", but, rather, "What'sa matter? You no spicka you owna language?"

That idea struck me funny at the time because I could think of no real reason why a person from an ethnic neighborhood should not be able to do well in the Agency. It certainly was not because the applicant would not know the special vocabulary found in Agency work. The Portuguese I had learned in Brazil as a missionary was very different [redacted] and yet I somehow passed the proficiency test. Surely a child growing up in an ethnic neighborhood would learn the *patterns* and many of the idioms of the "foreign" language. With a mastery of those patterns and idioms, the new hire with an exotic surname could be given a glossary of special terms and be expected to do well, no? Apparently not. But why?

A year after reading the article I discovered the reason why the Agency shouldn't be able to find a rich source of good translators in ethnic neighborhoods. For technical reasons I was left for a while without much to translate, and I finally decided to go to the Learning Center for something more to do (besides, the people there are very nice). I found a course (EG 421) entitled "Effective Writing" and started watching television. To my delight the heart of the 6-hour course explained how to edit and unscramble gobbledygook. That was precisely what I needed.

[redacted]

The impact of taking the course was that, although I hadn't been able to do much translating since failing my first attempt at Part II of the PQE, I passed on the second try. EG 421 was the only visible influence that could have made the difference.

So what does EG 421 have in common with hiring linguists? Well, the prerequisite for the course was that anyone wanting the course was supposed to have job duties requiring extensive writing. It hadn't dawned on me that I was doing a lot of writing; after all, my work was to reduce material written by someone else into English. I had not been doing any composition per se, just translating. No wonder I had failed the PQE! I finally passed it when I began to think of myself as a technical writer whose material is usually dictated by, but sometimes only inspired by, the Portuguese it represents. I rarely had trouble understanding Portuguese; my problem was writing English! (The people who edit my translations insist I still have lots of problems.)

My point is that *writing English is the major portion of a translator's job*: the foreign language is secondary. There are lots of good translators in this Agency whose command of their job-related foreign language is far from native, or even that of a college graduate. This means that if an applicant with a childhood foreign-language background doesn't do well, it is not because his neighborhood was polluted with anglicisms; it is because his English was polluted (or in some other way deficient, like mine). In other words, "*That'sa* matter! He no write-a da *English*!"

Having diagnosed the problem, it's now time to prescribe the remedy. If the Agency ever needs to recruit translators again (I specify translator, a person who writes English -- very different from a transcriber, a person who writes some other language -- it was a sad mistake to confuse the two and mislabel them both "linguists"), it should stop restricting the search to language majors. The ideal recruit really might be a Journalism or English major with a Language minor, and some course work in International Economics and Political Science.

My degree is in Economics. Because of that, no one ever asked me if I wanted to go to the D.C. area as a GS-7 and use my Portuguese. No one asked my roommate, who spoke German, to come to NSA either; he was a chemistry major. I knew lots of people who never took college courses in

EO 1.4.(c)
P.L. 86-36

the foreign languages they spoke fluently (Indonesian, Japanese, or Korean, in addition to French, German, Italian, or Spanish) because they felt they could never make a living with their language and went into other fields; and because they were not language majors, they were not interviewed by NSA. People like this should be talked to by Agency recruiters who are searching for translators. Perhaps recruiters could find people like this with ads in campus papers saying something like "If you got an 'A' in Freshman English and know a foreign language, Uncle Sam wants you!"

An additional thought on recruiting linguists: high ambition in an applicant should be viewed as a criterion for *non*selection. This view contrasts sharply with the one expressed by Daniel G. Buckley in another Agency publication ("Can A Linguist Development Program for High School Graduates Work at NSA?", *Cryptologic Spectrum*, Winter 1977). The problem with highly ambitious or highly motivated people, whether college degree holders or Agency-trained high school graduates, is that they expect (and emotionally require) high productivity to be rewarded, and government service is not set up to give rewards for productivity. The result is that highly motivated linguists begin to look outside the Agency for advancement when they see little opportunity for promotion inside. If the object is to recruit career linguists, no more than a moderate amount of ambition or motivation should be allowed in a recruit.

A word of warning is in order. Due to the accelerated decline in the number of college graduates who can actually write well in English, the Agency may find itself in a position with translators similar to the one it is in now with programmers and engineers: as the general demand for good writers increases in the economy, translators will gain more outward mobility, not for their ability to understand foreign languages, but for their ability to write plain English. Then the Agency may have a "language problem" that will make today's situation pale in comparison.

~~(C)~~

NEWS OF THE C.A.A.
(Communications Analysis Association)

By W.E.S.

Busy Week in March

CAA had a busy week in March. On Wednesday, 1 March, [redacted] spoke in the Auditorium, drawing upon her years of experience in the White House Situation Room.

On Thursday morning, 2 March, the CAA Operational Briefing series featured [redacted]

On Thursday afternoon, the CAA Board held its monthly meeting (by the way, we're back to monthly-changing rooms again), and we spent a large part of our time talking with Sergeant [redacted] and Dan Buckley (M09) about how the CAA might assist and encourage professionalization among civilians and military.

Then, on Friday, 3 March, the CAA's Special Interest Group on Cryptologic History had a session on "Oral History," featuring Dave Goodman (former NCS History Fellow) and Art Zobelein. The presentation included an introduction to the principles and techniques of oral history, and a description of the oral history program here at NSA. ~~(C-CCO)~~

P.L. 86-36

Winner in Logo Contest

It was grueling work, but the board knows its oats. After much animated discussion about the wide variety represented in the entries, the CAA Board finally made up its mind. Out of the sixty-plus entries in the CAA Logo Contest, the winning entry came from [redacted] A645, who will receive a book of his choice. (More about the winning entry next month.) (U)

P.L. 86-36

CAA Presentations

Our Program Committee, chaired by [redacted] has been busy too. The committee has lined up the following speakers:

10 May Admiral Inman
21 June [redacted] (subject: Interstellar SIGINT)
(?September?) [redacted] N1

If you have any ideas for other presentations, let Earl know. (U)

P.L. 86-36
EO 1.4.(c)

Meet Linda!

The newest CAA Board Member is [redacted] a COMSEC Analyst in S1. She earned an AB in Psychology at Gettysburg College and came to work here at NSA in 1966.

P.L. 86-36

Her cryptologic experience has included assignments on the staff of the National Cryptologic School, where she was involved with CY-001 and CY-300; in B Group, where she was associated with the [redacted] and in S, where she became a COMSEC Intern.

EO 1.4.(c)
P.L. 86-36

She is certified in Traffic Analysis and COMSEC. (Inside tip: Ask her about collies.) ~~(C-CCO)~~

CAA Board:

President	David Gaddy	3247
President-elect	Frank Porrino	5879
Secretary	[redacted]	8025
Treasurer	Tim Murphy	3791
Board members:	[redacted]	4935
		5991
		3573
		3369

(U)

Four Easy Steps for Joining the CAA:

1. Get a membership card from any of the members of the CAA Board.
2. Fill it out.
3. Attach $1.00 ("Is *that* all it costs?" "Yes, Fred, that's all it costs!")
4. Mail card and money to Tim Murphy, B09.

(U)

P.L. 86-36

DOCID: 4009811

The Joys of UNIX

[redacted] P13/R53

P.L. 86-36

For the last 6 months or so, I have been experiencing a new and (in my jaded and cynical mind) totally unexpected turn of events in working with computers. I have actually been enjoying the process of using a computer system: the R53 MYCROFT (PDP 11/70 under the UNIX operating system). After several years of being turned off by discouraging encounters with various computer systems, some involving on-line terminals, I find UNIX, and in particular the RAND editor, restoring much of my lost faith in the value and promise of computers.

I have found myself choosing to do at the terminal more and more things that I would once have done with pencil and paper, with a typewriter, or with cumbersome POGOL procedures on the IBM 370. Even more important, I have chosen to undertake many things that I would hardly have considered before; the convenience and accessibility of UNIX makes new things, or old things done in newer ways, seem pleasant, challenging, and possible rather than prohibitively painful, burdensome, and remote. I have been so struck by the dramatic contrast between my former feelings of disgust and discouragement and my present optimistic and positive feelings about UNIX (and, by extension, about computer technology in general, and the tasks I perform with its aid), that I have spent some time in considering which specific features give UNIX its remarkable value for me as a user.

I felt that some informal comments on this topic -- ways to make a computer system more supportive and hospitable to its day-to-day users -- might be of general interest. Our Agency is becoming more and more committed to on-line, interactive systems. Larger and larger numbers of users will soon be attempting to accomplish an increasingly broad and heterogeneous set of tasks on an ever-growing spider web of intersecting networks. The question of how to design and maintain a "friendly" user interface linking a wide range of users to a wide range of computing facilities is becoming increasingly crucial. For one set of users with varied needs, UNIX appears to have provided one good answer.

First Joy

I would like to set the stage with a bit of history -- a rapid glance back over my own experience with computers as an applications programmer since 1951. I am sure many readers will recognize some of the stages of computer usage at NSA that I mention in passing, and will perhaps also recall similar reactions to them (though many will not, perhaps, have been bothered or pleased by the same developments that bothered or pleased me).

When I first began programming on ATLAS I, I felt that programming was a supremely enjoyable and challenging activity. Debugging was done on the computer, in octal; commands were numbers, as were all addresses in memory, and addresses were fixed. Programmers were also operators, and learned as much as possible about the hardware of the computer, since we had to demonstrate and prove each hardware error to the maintenance men before they would fix it. Input and output were on punched paper tape, printed out on a teletypewriter, corrected with sticky tape and a hand punch. Programmers could understand and get at everything, and we could carry out every step of coding, debugging, and running our programs at our own pace and on our own terms, using simple equipment directly accessible to us. Given a chance to vote on whether we wanted an assembler language for ATLAS I, we voted it down. The "manual," consisting of two mimeographed 8 x 11 inch sheets, was a miracle of clarity and succinctness which I have never since seen equaled: it simply listed exactly what each command did with each bit in each register. In any case, we all knew most of it by heart. Who needed an assembler?

As successive "new" computers came and went, things necessarily got more and more complicated. Assemblers, compilers, and subroutine libraries came along, and operating systems began to assume increasing importance. Addresses became relative or relocatable (so we had to add a base address to everything before we could read our octal dumps), and magnetic tape replaced paper tape for input and output. Programmers were banished from the machine area to the outside of a counter, and a new hierarchy of operators and systems specialists reigned supreme "backstage." Computers rose on the horizon and fell away to make way for still newer ones -- 704, 705, 709, 7090, DCS (to name those which which I myself became most familiar). Still, until the advent of IBM's "third generation" -- the 360s and 370s -- and time-sharing, the changes involved primarily a slow accretion of added features which programmers could assimilate a step at a time. I myself still felt that I understood DCS hardware and software almost as well as I did for the earlier machines, and I still felt that it was worthwhile trying to do so (reading and studying maintenance and software reference manuals to learn as much as possible).

Joy Abating

With the coming of the 360s, there seemed to

DOCID: 4009811

be an abrupt discontinuity. Suddenly the "manuals" a programmer needed to study if he really aspired to understand the system had stretched out to fill a rack 10 feet long. The workings of the complex agglomeration of hardware components and peripheral devices in ever-varying configurations were all buried under endless layers of software comprehensible only to "the IBM men" and a very small number of others who chose to specialize full-time in these arcane matters. For programmers whose interest and knowledge were centered around an application rather than programming as such, the effects of this sudden increase in complexity, coupled with a loss of understanding and control, could not fail to be discouraging.

Against this changing background, my own experience was, for the most part, one of growth to accommodate the added complexity. Up until and including DCS (again, in the IBM computer series that I know best), most of the changes seemed to bring improved capabilities without too much of a sacrifice for the user in terms of convenience and control over what was happening. After the 360s arrived, however, my experience began to be one of progressive deterioration in my ability to get what I wanted out of "the system" (the hardware, the software, and, no less important, the "fleshware" -- the people behind the computer installation and their ways of dealing with me as a user).

I became, in fact, less and less of a programmer at all, and more and more simply a procedure-writer who tacked together canned routines or previously debugged POGOL steps to do dull things in a dull way. Since it invariably took me 2 or 3 days just to catch up with all the control-card and rule changes (transgression of which invariably resulted in a canceled run accompanied by little or no helpful information), correct JCL errors, achieve the necessary two valid POGOL listings (a compile and a "go" listing), and cope with all the other things that usually went wrong with FILE cards to keep me from reading my input tape and getting an output tape, it hardly ever seemed worthwhile to try anything the least bit conceptually challenging. I was just glad to get a job done, any way I could!

To sum up this quick sketch of my own view of the trends in NSA computer technology as seen through the eyes of a day-to-day user, I recall an early period of maximum accessibility, complete control and understanding of the computer by the programmer. This was followed by a period in which hardware, software, and the human procedures within which these were embedded became increasingly complex; while many features were removed from the programmer's direct control, the added power and conceptual richness of the facilities at my disposal more than balanced these losses. For me, at least (and, to judge by many comments I have heard, for many others as well), the coming of the 360s upset the balance of power greatly to my disadvantage. There was a lot of computing power available, and POGOL, in particular, was always a convenient, useful tool for accomplishing the data processing functions I needed. Unfortunately, so many people were trying to do so many things with the system (some of them apparently mutually incompatible at times!) that some of us were unable to get much out of it. Thus, for me, the time during which I used the IBM 360 and 370 systems was a very discouraging nadir in my interaction with computers.

Joy Regained

It was at this point that I had the good fortune to discover MYCROFT, UNIX, and the RAND editor. Now, suddenly, I have the best of both worlds -- the illusion of having the computing resources all to myself at the terminal (though many others are enjoying the same experience at the same time), with all the power and richness of a modern computer. Once again I have a chance to understand some of what is going on "under the cover" if I wish to make a reasonable effort to do so; in the office where I work there are helpful and patient people who understand the system and can aid me when the documentation is not enough. I can call on a wide variety of programming languages, and I can also call up generalized functions (sort, select, dedupe, translate or convert, spelling check for English words, and several report generators), all in a very simple and flexible manner. I can create new files and execute my own programs or generalized functions on them directly and easily. The whole system is consistent and unified so that I can quickly learn to use it at my terminal. If I have been able to use and enjoy this system, I am certain that anyone else could do so at least twice as quickly (since I have always had a very hard time learning any new programming language and usually require a long time to feel at all comfortable with it).

The key feature of the MYCROFT system for me, and probably for many other users, is the RAND editor. With the editor, I can write a program, jot down rough notes, or draft a report, placing it in a UNIX file. I can then immediately attempt to compile and execute the program, find the errors, go right back into the editor to make changes, rerun the changed program, re-enter the editor, and so forth, until I have either checked out the program or else decide to leave my terminal (to search for food or water or to satisfy some other basic need). In fact, I have once gain the same ideal debugging situation I enjoyed back in the days of ATLAS I. When I do leave the terminal in the middle of this process, I can rest assured that my files will usually be safe, and will reappear when I log on again just as I left them (a certainty that I never had with the other on-line system I tried). After roughing out a report or some initial jottings (an outline, for example), I can come back to the terminal and rapidly reshape and refine the draft, or fill in the outline as easily as I could with pencil and paper, and

more effectively.

Many readers may be taking issue with me, somewhat as follows: "Aren't these just the things anybody can do with a system like LODESTAR, TSO, or CANDE? What's so special?" I am certain that these systems have many advantages, and would like to see an informal write-up on their good points, seen strictly from the applications-oriented user's point of view. It should be remembered, however, that UNIX operates on a "minicomputer," in contrast to the large-scale systems mentioned above. UNIX provides a remarkable amount of power, coupled with an outstanding user interface, all within a computer systems which costs less than $300,000 -- about as much, I am told, as the disc storage alone of the big IBM, CDC, or Burroughs systems.

I would like to describe for the interested reader some features of UNIX which I find most helpful. First and foremost, the RAND editor is beautifully designed from a human-factors point of view. No other software tool that I have ever used or studied can equal it in this respect. Most other editors are "line editors," requiring that editing be carried out on lines specified by number, as was usual with card-oriented file-update procedures. These line editors also require that some set of commands ("REPLACE," "FIND," "DELETE," "MODIFY") be keyed into the terminal, with the necessary strings to specify the sought string, the replacement string, and so forth. These commands, also, have syntax rules which must be learned and which are easily transgressed. Transgressing the rules brings upon the user the need to rewrite the command (edit the command to the editor!) and try again.

In contrast to this line-oriented, programming-language-like type of editor, the RAND editor allows the user to do most things by pressing a single key. Pressing a special "ARG" key permits the next integer or character string to be fed as a parameter to the function designated by any of the other keys. Thus, a user can accomplish many complex actions by simply pressing "ARG," keying in a number or a string of letters depending on the action desired, and then pressing the single key that stands for the action. This is all the "syntax" that has to be learned, and it is consistent over the whole set of actions provided by the editor. In fact, I can guess at what will happen with a set of key presses I have not tried before, simply by extrapolating from the editor's behavior after the key presses I already know. In many instances of guessing the results of key sequences, I have never so far been disappointed. I cannot think of *any* other programming tool I have seen which can be counted on to behave so transparently, so logically, and so sensibly.

In addition to being designed to behave as a user expects it to behave, the editor even achieves sensible behavior when the user goofs. For example, if I press "ARG," then make a mistake while keying the integer or string parameter, I get a crisp and clear warning and can start over again by simply pressing "ARG" again. Often the user can recover from a mistake by repeating a few simple key strokes. In any case, the mistake and its correction do not spoil or interfere with the text on the screen or the previous correct actions. I remember well how pleased I was when, having written down to the last line of the screen without noticing and then having pressed "CARRIAGE RETURN" to get a new line, I saw the editor obediently roll the window down to display a new page for me to write on, having apparently read my mind.

How It Works

In order to gain a more vivid picture of the editor, let us imagine a user -- me -- sitting down at the terminal to write a report. I have some ideas of what I want to say, but nothing written down yet. I log on (a matter of typing two tiny character strings devoid of "syntax" and in response to two simple prompts). Having decided to call my paper "report," I key in "re report," that is, I call for "re," the RAND editor, to work for me on a file called "report." Since this is a new file which I am about to create, the editor displays a polite message telling me to press a "USE" key to cause the file to be set up. Immediately, the editor then provides me with a "window" labeled with the name "report" and all ready for me to begin writing.

I tab over to a preset margin (which I can change if I wish), and set tabs for indentation or tables if I need them, with a few easy key strokes. Then, since I am in early stages of planning my paper, I begin an outline. I start out:

"1. Introduction
2. Essentials of the problem
3. A summary of past solutions"

At this point, I decide that I want another heading between 2 and 3. I position the cursor anywhere on line 3, and press the "OPEN" key. The editor moves line 3 down one line, and I am all ready to write in the new line 3, then change the old 3 to a 4. After I finish my rough outline, and wish to write in subheadings, I can open up space and squeeze any number of them in with ease. Then, when I am satisfied with the outline, I can write the text in after each heading in the same way. No muss, no fuss, no scratch paper, and the copy I see on my scope is always clean and well formatted, without crossouts or strike-overs.

Suppose I am writing along on a line, and inadvertently continue writing past the right border of the window. A flashing message, and, on some terminals also a beeper, demands my attention, and I see a right-pointing arrowhead warning me of the overflow. I move the cursor back to where I meant to end the line, press

the "DELETE CHARACTER" key, and hold it down while the overflow letters are neatly gobbled up and disappear. If I decide, after I have typed a few words, that I want to leave one out in the middle, I can press the "DELETE CHARACTER" key to squeeze out the unwanted word. To squeeze in some words, I press the "INSERT MODE" key and type them in. Material to the right on the line moves over to accommodate them.

Now, suppose that I wish to incorporate a paragraph from another report, already on a UNIX file in my work space, into this new report. By positioning the cursor along the left margin, pressing "ARG," then keying the name of the old file, and then pressing "CONTROL" and "Z," I can split the screen into two horizontal windows (I can have up to ten windows) and call for the old report to be displayed in the second window while I keep the new one in the first window. I know that the paragraph I want starts with the words" It is obvious that," so I press "ARG," then type in these words, just as I expect them to appear in the text. Then I press "+SCH"; the editor finds the phrase and displays it with its surrounding text in the second window. I count 12 lines in the paragraph; by pressing "ARG," then "12," then "PICK," I copy the entire paragraph into a buffer -- the "pick buffer." I press "CONTROL" and "C" to move the cursor back to my new file in the first window, position the cursor where the paragraph is to be inserted, and press "PUT" -- the paragraph magically appears, and I am ready to go on writing. (This feature is a delight in writing programs: one need only code one version of a routine, then "PICK" it and "PUT" it over and over again wherever a similar routine is desired, changing the details later.) Once I have set up windows and filled them with files, I can switch from file to file in each window, and move the cursor from window to window, with a few quick keystrokes.

Nothing Lost When System Crashes

Now, let us imagine that I have been working at the terminal for about an hour, and suddenly the system crashes. I have not been saving my file as I went along, so I fear that I have lost an hour's work -- work that I might have trouble duplicating from memory. The editor has automatically saved a backup version of my file, "report," as it was before I began the latest editing session, in a file called "report.bak." But that is no help with the changes I have made during the session. With most editors, I would be in a very annoying fix; the RAND editor, however, saves a record of every keystroke I have made during the current session. By keying in a simple sequence of commands, I can call this record in and execute it on the "report.bak" file," so that every motion I made is duplicated until the cursor stops at just the point where it was when the system went down, and I am ready to go again. It is very amusing to watch the cursor scooting around, lines, words, and paragraphs jumping in and out, appearing and disappearing, all untouched by human hands. In fact, the "keystroke file" saved by the editor to produce this re-run of my session is just like any other UNIX file, so that I could get it into a window and edit it with the RAND editor to change sequences of key strokes and thus rewrite the history of my own editing session if I wanted to!

As if this were not enough, there is a "macro" facility in a special form of the RAND editor. This facility permits the user to perform sequences of key strokes and then treat them like little programs; he can designate an entire sequence by one key (for example, "X"), then position the cursor wherever he wants to and press "X" to execute the entire sequence. This would be convenient, for example, in reformatting a fielded file; a "macro" could be defined to accomplish reformatting of a page, then executed for each page.

Summary

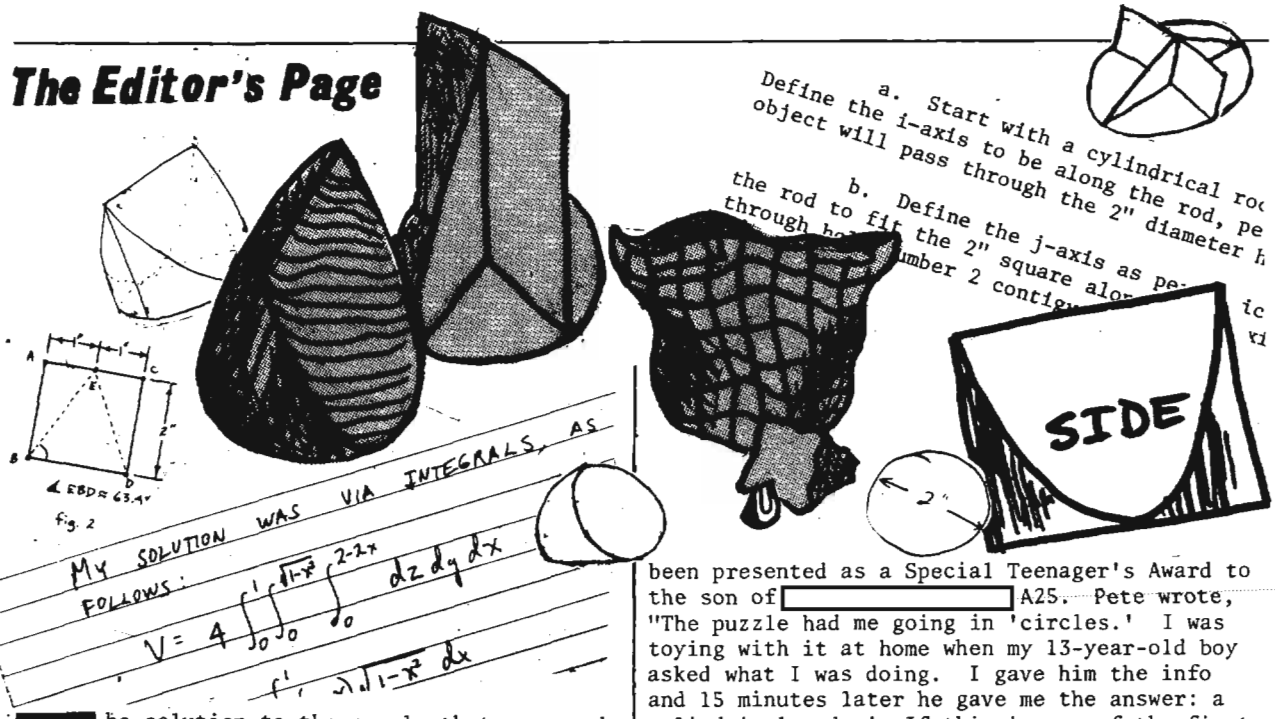
While the features described above are those that have proven most useful to me, UNIX provides many other advantages for more sophisticated users. For the benefit of readers who may be interested, I will quote a summary of UNIX strengths from a technical report prepared for RS3 by a contractor:

> "In general the UNIX world view appears ready-made for user-controllable, multiprocessor systems. The capabilities that make UNIX attractive include process creation (forking), process intercommunication (piping), file directories and referencing via a MULTICS-like tree addressing scheme, the shell concept, command language elegance, the equivalent treatment of system and user procedures, and the user extensible command language."
>
> (Charles Kellogg, "Alternative Architectures for Deductively Augmented Data Management System," TM-6005/000/00 Draft, Systems Development Corporation, December 1977)

I hope that the previous paragraphs have conveyed some of the ease and pleasure of using MYCROFT with UNIX and the RAND editor. I find that I can get much more work done, with far less trouble and effort, using this facility as contrasted to what I could do with other computing systems or with pencil and paper. The RAND editor became familiar to users of the ELROND computer under Programmer's Workbench, and it is available on the KEPLER facility in R17. It is also a part of STEPSTONE II on PLATFORM, and will undoubtedly become a valued tool of many NSA employees. In closing, I would like to emphasize the importance of the "user-friendly" design of the RAND editor, and urge that software designers use it as a model for future systems. With tools like UNIX and the RAND editor, computers can come into their own at last as real aids to human performance.

DOCID: 4009811

The Editor's Page



The solution to the puzzle that appeared in the February issue of CRYPTOLOG was printed in the March issue. Because of print-shop deadlines, this is the first opportunity we have to print the names of the winners.

The response to the puzzle was tremendous -- 48 correct answers were mailed in, carried in, or telephoned in (telephone solutions were accepted if the person could explain what he or she had in mind, even without the use of hands). Other than the drawn solutions, representing the easy-to-make version (the three pieces of cardboard), or a cone with a square plane intersecting it vertically, or a piece of a cylinder with two facets shaved off, the editorial office received some "look-alike" descriptions: a vacuum cleaner attachment, a washing machine agitator, etc. We also received some three-dimensional models: an actual piece of a wooden dowel with facets shaved off it (the woodworking equipment to make it must have cost hundreds of dollars); a shaved piece of a pencil eraser; a cut piece of a pencil; a raggedly cut (chewed?) piece of artgum eraser; a piece of graph paper sort of squished into what was an honest attempt at the right answer. And, finally, we got two *offers* of models that never materialized, including an appropriately cut wedge of salami.

The following is an alphabetic list of the first ten persons to provide the correct solution:

David H. Williams, P16.

Flimsy gold-papered cardboard trophies have been sent to the ten winners. Another one has been presented as a Special Teenager's Award to the son of [redacted] A25. Pete wrote, "The puzzle had me going in 'circles.' I was toying with it at home when my 13-year-old boy asked what I was doing. I gave him the info and 15 minutes later he gave me the answer: a cylindrical wedge! If this is one of the first ten, I would like for him to have the trophy." Although the solution was not among the first ten, we are pleased to make this award as a sign of appreciation for spreading the name and fame of CRYPTOLOG.

P.L. 86-36

P.L. 86-36

Other CRYPTOLOG readers who provided the correct solution, but too late to win a trophy (it's a cheap old thing, anyway!), are:

[redacted]

Here it is!

When some of the contest winners showed up in the Editorial Office (that's what I call this mess), I would ask, "Now that you see how easy it is to contribute to CRYPTOLOG, why don't you contribute an article?" Almost invariably, the answer would be, "I might someday, when I get a round TUIT." Okay, then, here's a round TUIT! If anyone -- contest winner or just a casual reader -- is thinking of submitting an article to CRYPTOLOG, cut out the TUIT, fasten it to your article, and send everything to: CRYPTOLOG, P1, Room 2N039. *(Offer void where prohibited)*

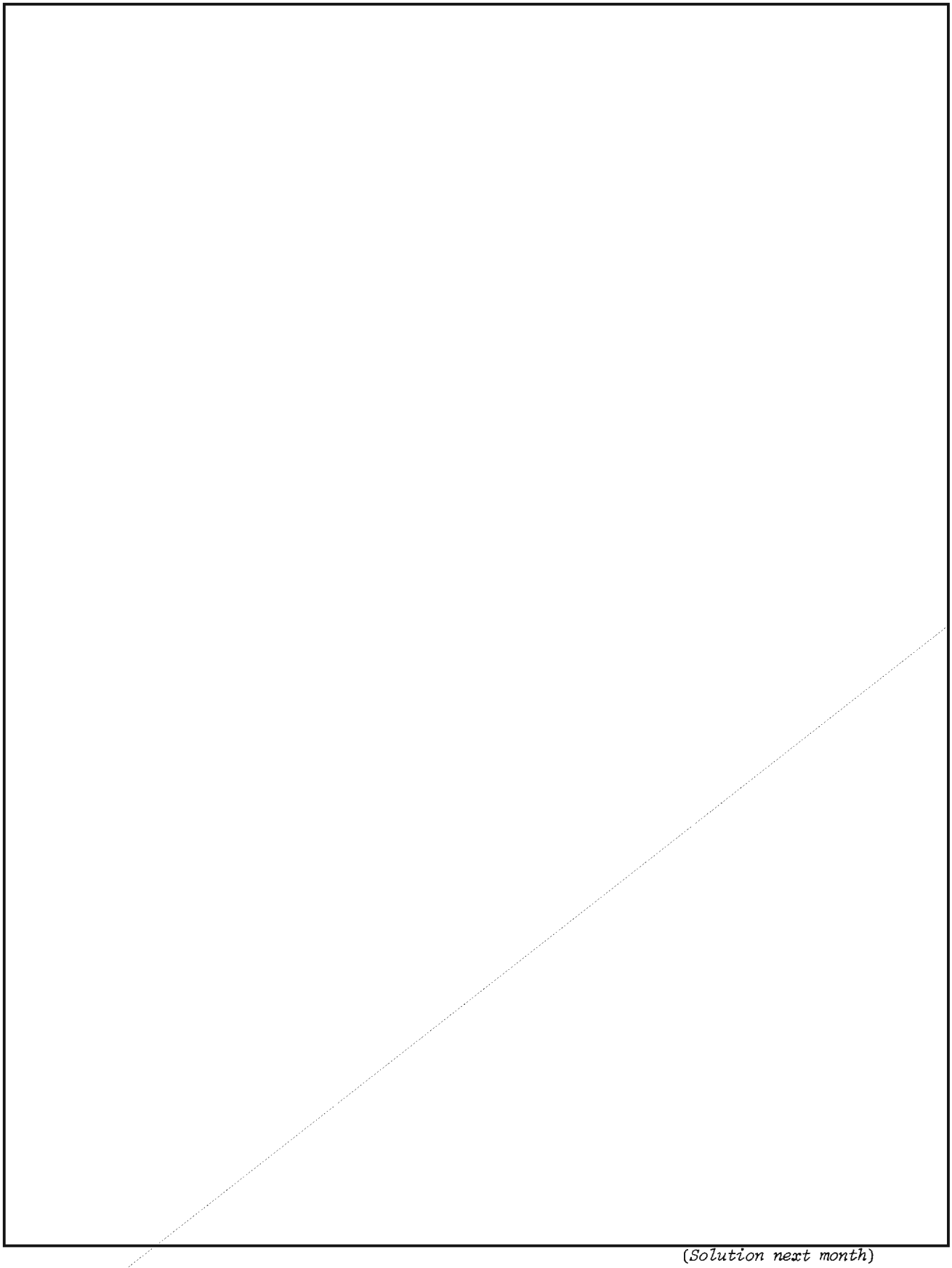
P.L. 86-36

NSA-crostic No. 14

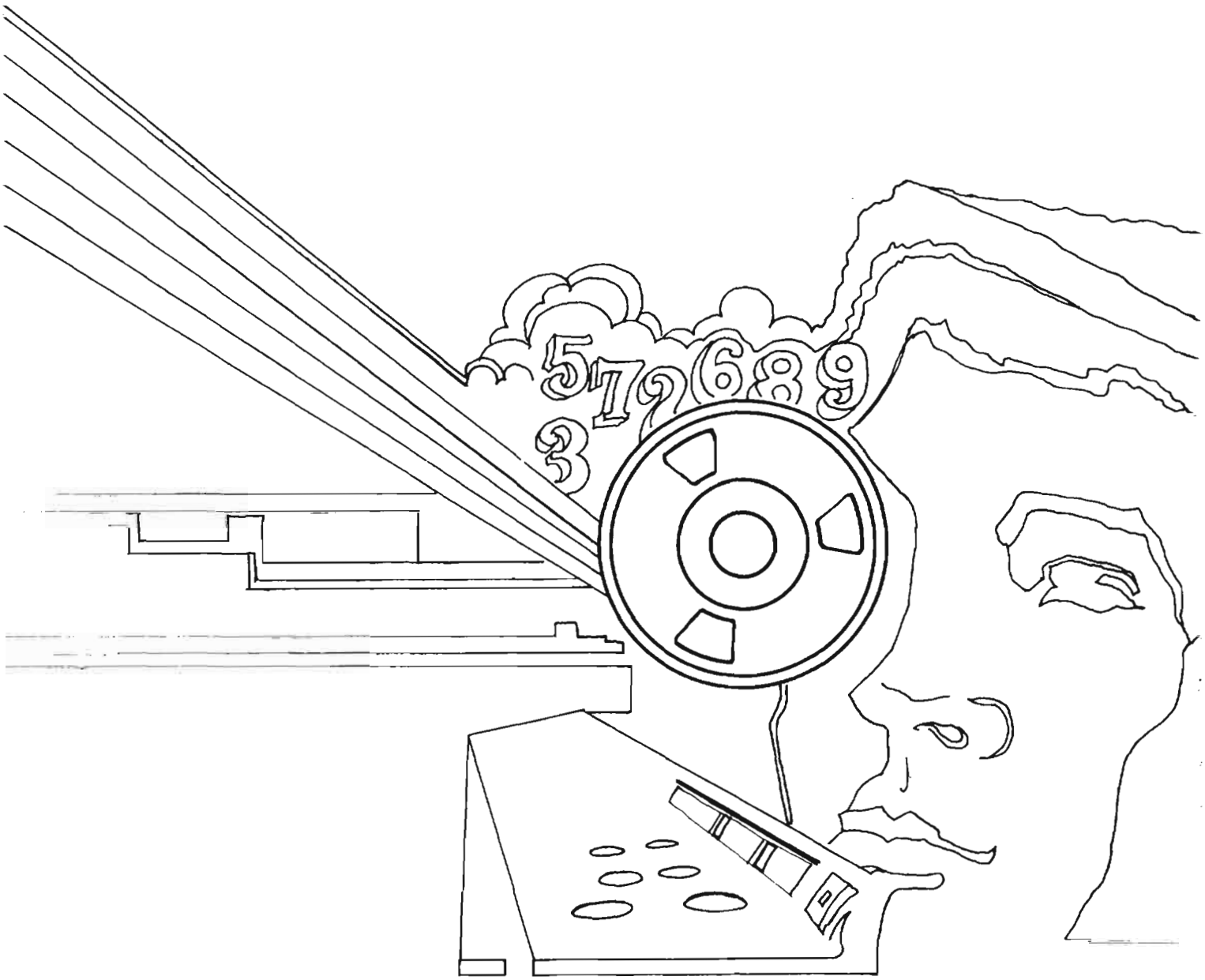
by guest NSA-crostician "Sardonyx"

The quotation on the next page was taken from the published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS *WORDS*



(Solution next month)


5 7 2 6 8 9
3

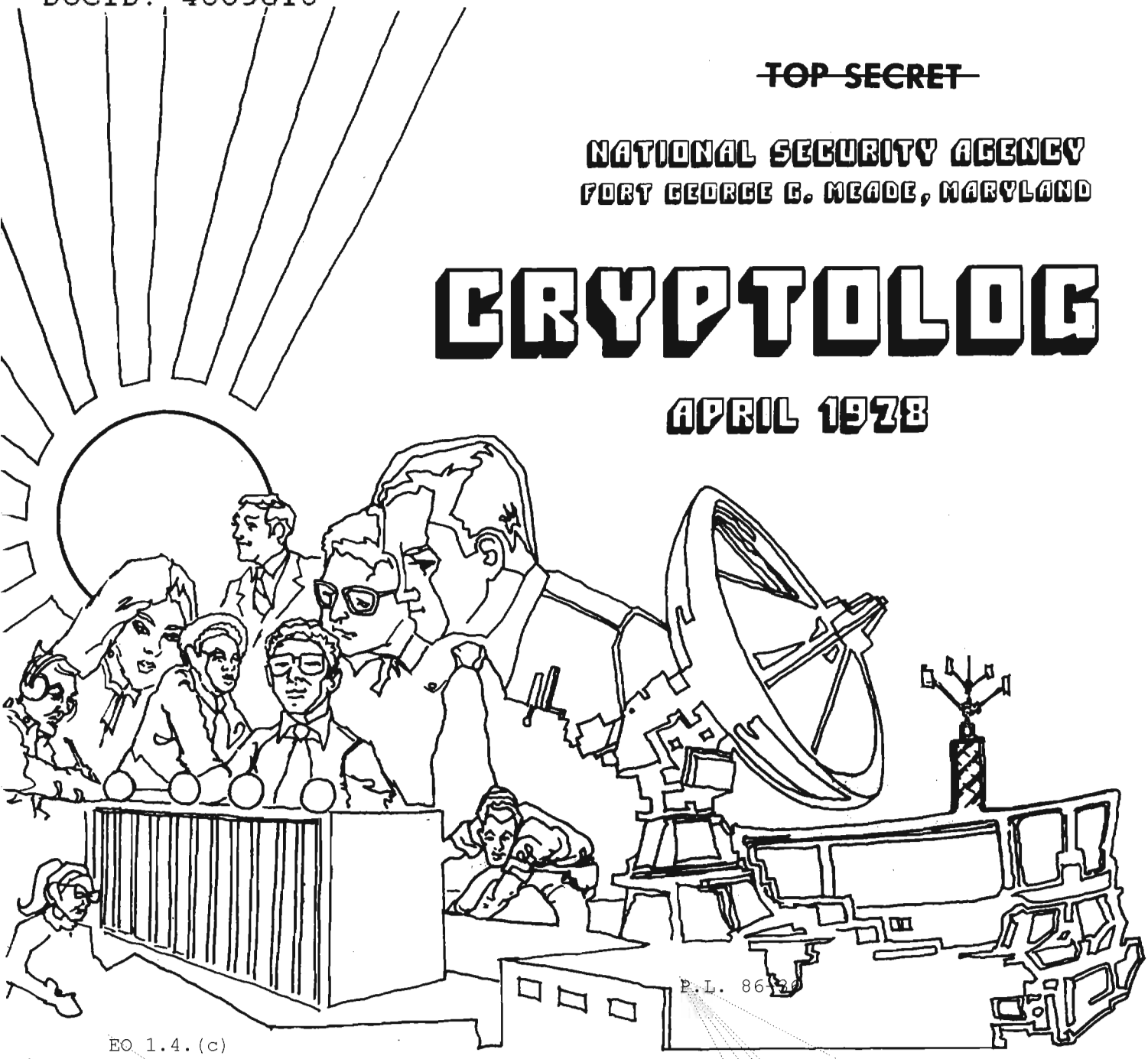
DOCID: 4009810

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

APRIL 1978



P.L. 86-2

EO 1.4.(c)
P.L. 86-36

SIGINT EXPLOITATION, 1990	Robert L. Hunt	1
LOOKING AT MR. [redacted]	[redacted]	2
A LITTLE PEP TALK	[redacted]	4
ACCENTUATE THE NEGATIVE	[redacted]	6
REMEDIAL SOFTWARE ENGINEERING	[redacted]	7
TELEPHONE PROBLEM HERE!	[redacted]	13
NSA-CROSTIC NO. 13	David H. Williams	14
¿CONOCES BIEN LA GEOGRAFÍA?	[redacted]	16
C.A.A. NEWS	W.E.S.	17
A.T.A. LETTER TO PRESIDENT		18
LETTERS TO EDITOR		21

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009810

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. V, NO. 4 APRIL 1978

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5236s)

Collection.....[redacted] (8955s)

Cryptanalysis.....[redacted] (4902s)

Language.....[redacted] (5236s)

Machine Support.....[redacted] 5303s)

Mathematics.....Reed Dawson (3957s)

Special Research.....Vera Filby (7119s)

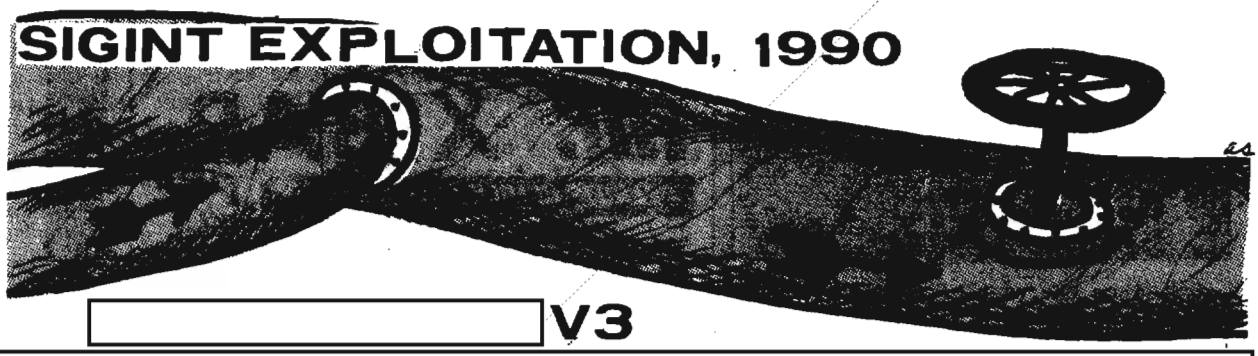
Traffic Analysis.....[redacted] (4477s)

Production Manager.....Harry Goff (4998s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

SIGINT EXPLOITATION, 1990



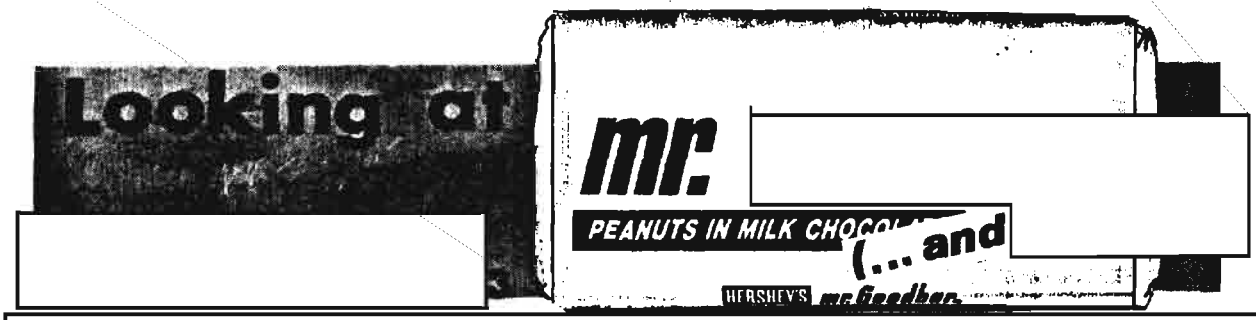
[redacted] V3

[redacted]

EO 1.4.(c)
P.L. 86-36

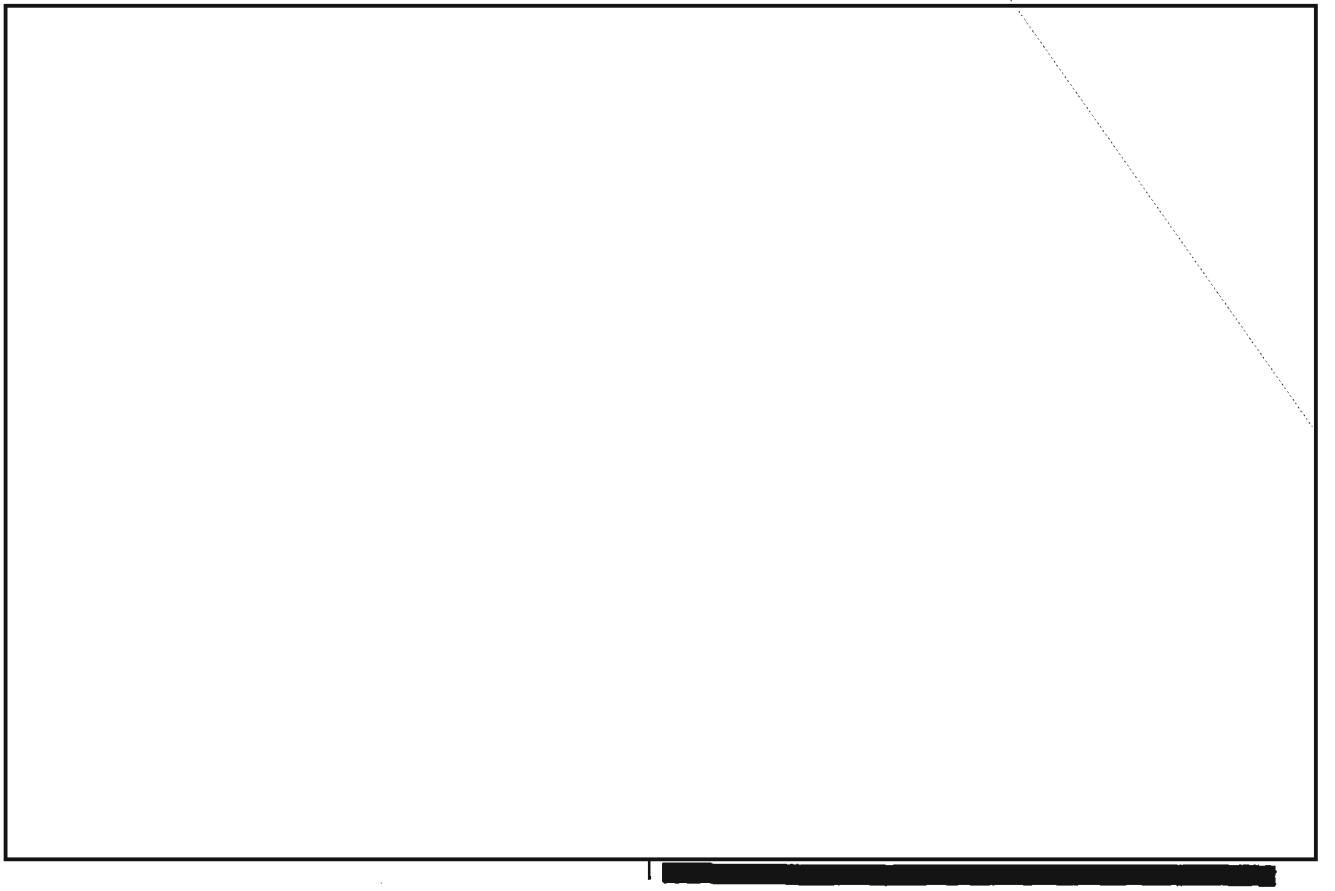
DOCID:4009810
P.L. 86-36

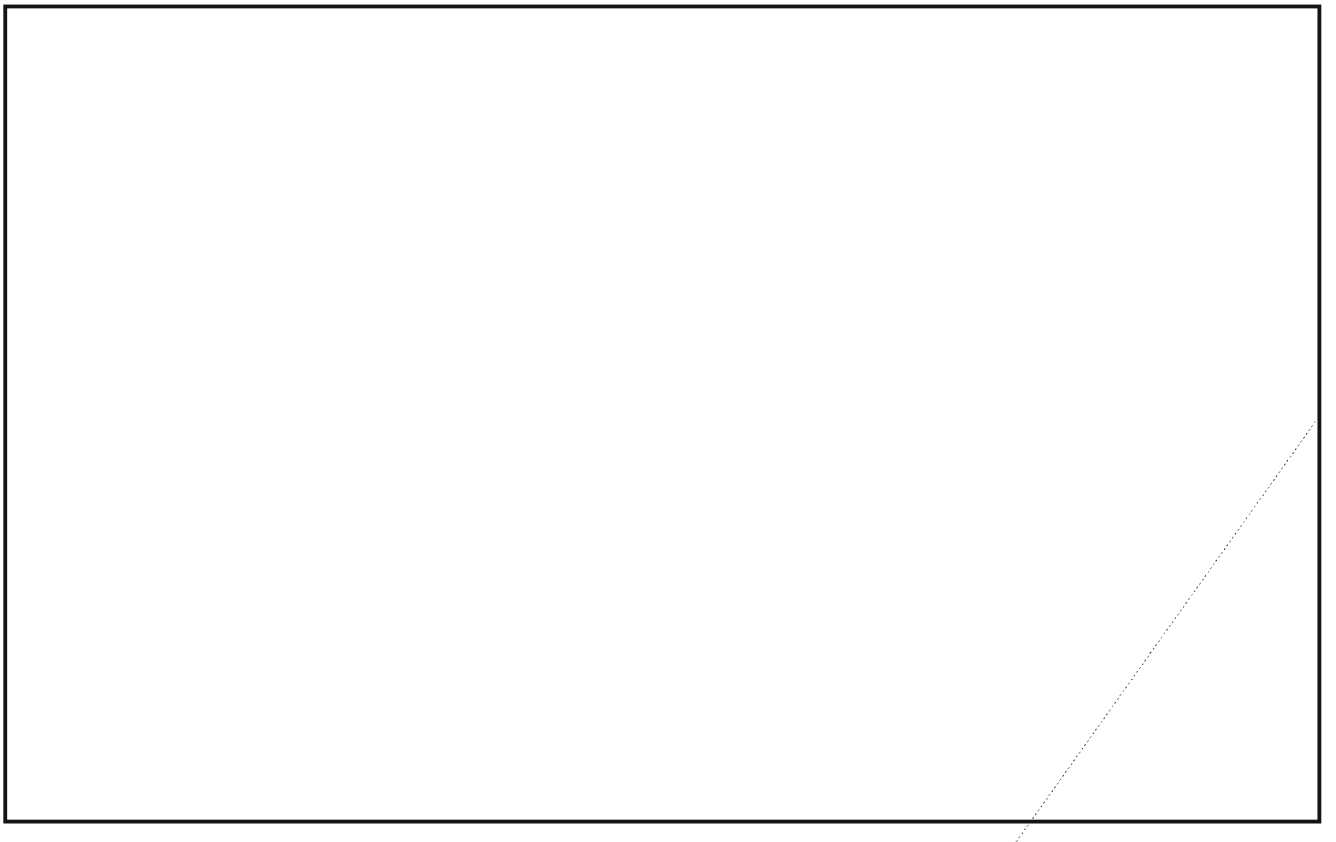
EO 1.4.(c)
P.L. 86-36



P.L. 86-36
EO 1.4.(c)

EO 1.4.(c)
P.L. 86-36





P.L. 86-36
EO 1.4.(c)

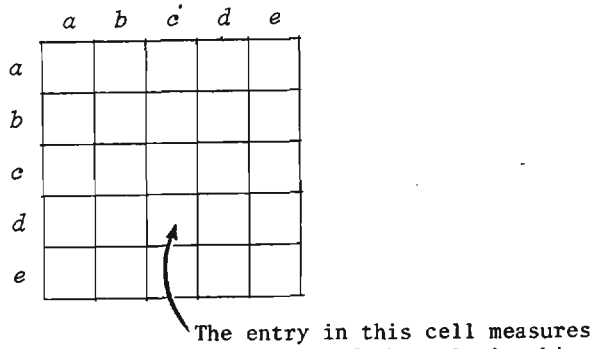
A LITTLE PEP TALK

R51

Over the past couple of years R51/CADRE has been experimenting with computer software for cluster analysis. Six programs, implementing nine clustering algorithms, have been acquired from outside the Agency and modified for use on CDC 6600/7600 computers.

These clustering methods are data-dependent, i.e, the model most suitable for a specific data set will depend on the form and nature of the data. The intent of the analyst must also be a consideration. (For example, does the investigator wish to find natural groupings in the data or to partition the data base into a predetermined number of categories?) It may be necessary to try several clustering methods on the same data to determine the most appropriate algorithm.

PEP-1 (*P*robability *E*valuated *P*artitions, version *1*) is one of the six clustering programs that R51 has adapted for Agency use. PEP-1 converts a set of input vectors into a matrix of pairwise similarities (or dissimilarities) (see Fig. 1). The choice of similarity (or dissimilarity) measure is an option of the program. The user may select any of the following measures: cross I.C. values, dot products, normalized dot products, Euclidean distances, and city block distances. The choice of measure must be guided by the nature of the real-world problem and the intent of the investigator. For example, does the analyst wish to match peaks and valleys in the vector profiles or, instead, match numerical values in corresponding components?



The entry in this cell measures the strength of the relationship between objects *d* and *c*. For similarity data, the higher the value, the stronger the association. For dissimilarity data, the lower the value, the stronger the association.

Fig. 1 Similarity Matrix on Five Objects

It should be mentioned that the analyst may construct his own similarity (or dissimilarity) matrix and then input the result into PEP-1.

PEP-1 orders the matrix entries from highest to lowest and replaces the numerical value in each cell with its rank order. (Tied entries receive the same rank order.) The PEP-1 algorithm can best be understood by regarding the entities to be clustered as vertices of a complete graph (i.e., an edge joins every pair of vertices) (see Fig. 2). The edge connecting any two vertices is identified with the entry in the similarity matrix which measures the strength of the association between those entities.

P.L. 86-36

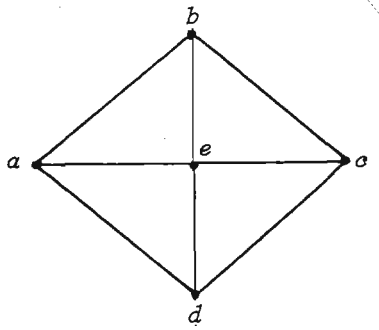


Fig. 2 A Complete Graph on Five Vertices

PEP-1 sequentially deletes edges from the complete graph according to the rank order of the entries in the similiarity matrix (the edge corresponding to the weakest association is removed at each step of the algorithm/ multiple edges are ridded in the case of ties)

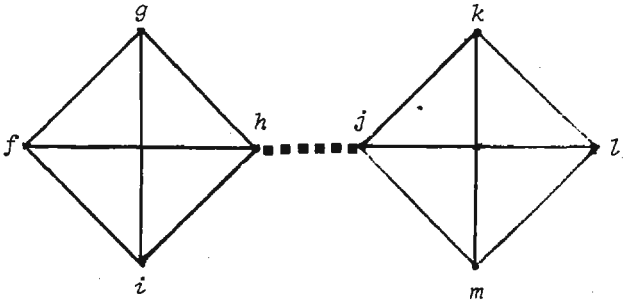


Fig. 3 Removal of the edge joining *h* and *j* produces a disconnected graph consisting of two clusters

until a disconnected graph is produced. At this point PEP-1 publishes the two partitions, the similarity (dissimilarity) value where the split occurs, the rank order of this value, and a "probability" that the disconnection could happen at random. The PEP-1 probability is merely an estimate (the true combinatorial probability is very complicated to compute) and is to be used only as an analytic aid to give a general impression of cluster validity. PEP-1 then reapplies the algorithm to each partition until the number of entities in a partition or subpartition is less than six.

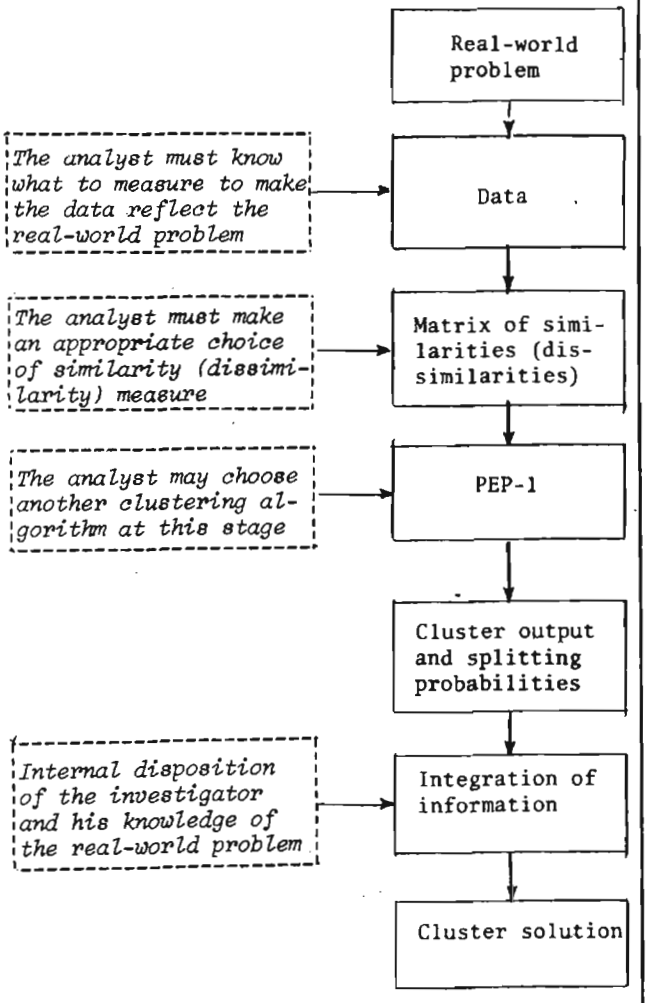


Fig. 4 The Clustering Process, Showing the Interaction (in Italics) of the Analyst and his Algorithm

It should be emphasized that the analyst is unable to prescribe in advance the number of clusters to be found by PEP-1 or the threshold levels at which the splittings occur.

PEP-1 is a reasonable choice for a clustering algorithm if the following conditions are satisfied:

- the analyst wishes to cluster a similarity (dissimilarity) matrix of his own construction or feels that he can select an appropriate measure to derive similarity (dissimilarity) data from vector input;
- the analyst seeks to determine natural clusters in his similarity (dissimilarity) data matrix;
- the analyst requires some numerical indication of the quality of the clustering produced by an algorithm;
- the analyst wishes only the rank order information in his similarity (dissimilarity) matrix and not the numerical values themselves to determine cluster structure;
- the analyst is aware that PEP clusters are not necessarily compact and may, in fact, be serpentine or sausage-shaped (see Fig. 5);
- the analyst wants an algorithm that will *not* be harmed by the presence of outliers (deviant observations) in the data;
- the analyst wishes to cluster fewer than 100 entries (fewer than 128 on the IBM 370/65).

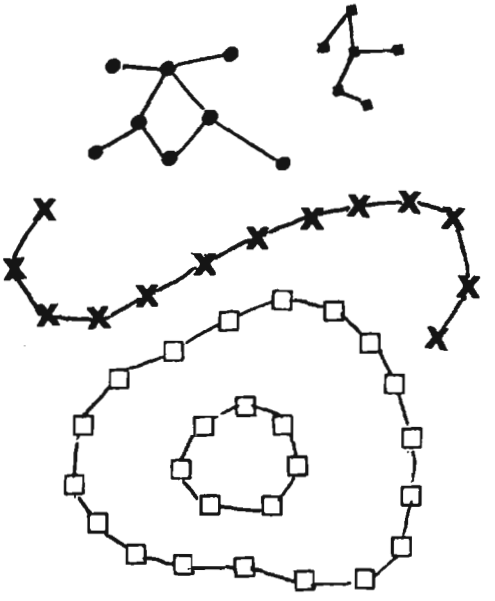


Fig. 5 PEP-1 clusters may assume a variety of shapes

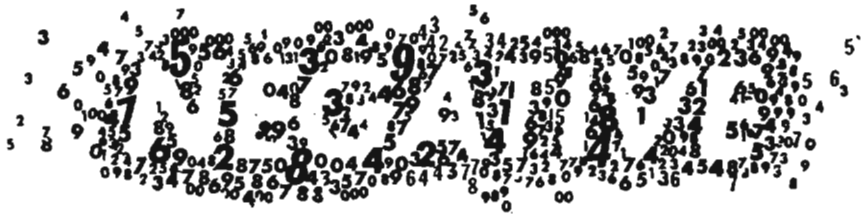
If you have any questions about cluster analysis or about the possibility of applying clustering techniques to your operational problem, please contact either [redacted] (Chief, R51, 8518s) or [redacted] (R51, 8626s). (U)

[redacted]

P.L. 86-36

We gotta...

ACCENTUATE THE



P.L. 86-36

For some time now, the subelement manager has been engaged in a battle to defend his resources against reductions initiated for a number of reasons. Managers at all levels have been barraged by a series of statistics designed to aid in making resources-reduction decisions, to show the efficiency of collection resources, to determine the cost of product reporting, and to allocate the resource expenditures for each function within the subelement of interest. The usefulness of statistics as a tool for making these types of decisions has been widely accepted. The accuracy of the statistics is rarely questioned and many decisions are based solely on this data.

The current period of dwindling resources and rising inflation, with the concurrent review of intelligence expenditures, has created an increased dependence on statistical methods as a means of determining efficiencies of operation. Aided by a myriad of computers providing a capability to count and measure that was never before possible, statistics have emerged as the guardian of our expenditures, the protector of our resources, and the practically omnipotent champion of efficiency. Savings have been made and some very necessary trimming of fat has resulted. These are significant accomplishments and speak well of the systems we have created.

Statistics, by definition, is a branch of mathematics dealing with the collection, analysis, interpretation, and presentation of masses of numerical data. The compilation of statistics requires a collection of quantifiable data. Only those things which can be measured or otherwise quantified can be considered when constructing statistics. In measuring SIGINT production, the statistician must therefore look at such things as the number of COPES objectives satisfied, the number of minutes of copy by case, the number of products produced, the number of intelligence requirements satisfied, or some other similar quantifiable data.

This has caused great difficulties for some subelement managers when defending their resources and has caused us to overlook one of our greatest intelligence contributions, which I call *negative intelligence*. Negative intelligence is the intelligence gained from knowing that a target unit is performing normally or is perhaps inactive.

Statistics, as most statisticians will admit, can be used to show whatever the statistician desires. Remember the old "Figures don't lie, but liars figure" adage? To guard against this, in our very important resources area, it is necessary to temper statistically suggested resource reallocations with considerations of the negative intelligence not reflected in the statisticians' figures or to devise a method of measuring negative intelligence contributions. Until we can do that, we must rely on the analysts to provide qualitative judgments through the subelement manager. The importance of these qualitative judgments cannot be overemphasized and they must be considered along with the statistical inputs. Granted this makes assessments subjective to a point and renders decision-making more difficult, since decisions cannot be made solely on a quantitative basis, these assessments nonetheless can provide the information necessary to protect that important negative intelligence data which may be irretrievably lost in a primarily quantitative evaluation. Remember that what we *don't* get is also important. In many cases we must accentuate the negative.

E.O. 1.4.(c)
P.L. 86-36

DOCID: 4009810

P.L. 86-36

UNCLASSIFIED

REMEDIAL SOFTWARE ENGINEERING

[redacted] T3214

Reprinted from *Proceedings: CISI Spring Conference, 23-26 May 1977* (Computer and Information Sciences Institute, National Security Agency: May 1977), S-217-661, 217 pp., SC. [redacted] paper was awarded First Place among the Conference Awards presented by Mr. Kermith H. Speierman, Assistant Deputy Director, Telecommunications and Computer Services, in the Friedman Auditorium on 23 June 1977.

This paper will describe Remedial Software Engineering, a systematic approach to identifying design deficiencies in software systems and implementing improved systems economically. I will combine ideas previously published by Yourdon, Metzger, and other authors to produce a methodology for dealing effectively with "problem" systems. I will give no detailed explanation of software design methodologies but will assume that the reader either is familiar with them or will consult the references for clarification where necessary.

Peter Prescription #36 asserts that rational action must be based on answering three questions:

1. Where am I?
2. Where do I want to be?
3. How do I know I am getting there?[1]

This paper will explain how to use proven tools and techniques of software design and project management to answer these three questions. It is based on my experience with some small- to medium-sized NSA systems where these principles have been applied successfully. I leave it to the reader to decide whether or not Remedial Software Engineering might be applied beneficially to very large projects.

I chose the term "Remedial Software Engineering' (RSE) for three reasons. First, to imply that its application would be to a system for which some pieces have already been created, but which needs further work to be made useful. Secondly, to distinguish it from any particular software design or project management methodology. And, thirdly, to imply some measure of orderliness in the craft of rescuing systems from disaster. Equally suitable titles for the discipline described below might have been "Creative Software Salvage" or "What to Do When Disaster Overtakes Your Software Development Project."

How Did I Get Here?

The premise of this paper is that the answer to Peter's first question, "Where am I?", is, "In charge of a software development project which is in deep trouble." A quick review of some basic causes of project failure will lay the foundation for the RSE methodology.

One major source of trouble is the lack of any system design. If nobody understands what is being built, then it follows that nobody will be very successful in trying to build it. Another source of trouble is a design that will not satisfy the real requirements. In this case, the implementers know precisely what they are building. What they don't know is that their product will never perform useful functions for the customer without major remedial action.

A second cause of disaster has to do with the project plan rather than the system design. The system design is a detailed blueprint of all the elements of the system being built and their interrelationships. The project plan, on the other hand, is a step-by-step description of how the pieces of the system will be assembled, unit-tested, integrated, and tested as a system. Where the system design specifies precisely *what* will be built, the project plan details *how* it will be built. If a project plan is missing or if it omits key considerations, serious problems will result and will frequently manifest themselves as apparent hardware or software design problems. If a house-building plan calls for installing the roof before laying the foundation, it is almost inevitable that the house design itself will be attacked by the carpenters as being unworkable. The plan and the design will then be modified on an *ad hoc* basis to make possible the immediate tasks at hand. Usually there will be no distinction made between the plan and the design.

A third class of problems results from failure to follow the plan. For example, the system in trouble might have the wrong amount or the wrong kind of staffing even though the plan spells out exactly what staffing is required. Assigning 25 troglodytes to build a condominium is unlikely to produce a livable structure even though the cavemen are handed a set of detailed blueprints and an hour-by-hour description of the thousands of subtasks required. Assigning 4000 architects to the project, again with perfect design and planning documentation, might yield similar results.

Although Remedial Software Engineering is called for when development efforts run into trouble, there are other times when the application of the same principles might be beneficial. For example, if a functioning system is about to be upgraded to incorporate new hardware or software such as microprocessors, data base management systems, etc., the methodology detailed below might be an excellent preparation for the conversion. Similarly, a system may be producing acceptable results but only at an excessive software-maintenance cost; RSE could help reduce the costs. In short, use Remedial Software Engineering whenever the pain associated with your current software efforts seems to be unbearable.

In these introductory paragraphs I have

[1] Laurence J. Peter, *The Peter Prescription* (New York: Bantam Books, 1972), p. 159.

UNCLASSIFIED

defined Remedial Software Engineering, stated its purpose, and suggested when its use would be appropriate. In summary, I quote the author of *Patterns of Problem Solving*, who said, "The most common difficulty in problem solving is not lack of information, but rather the failure to use information that the problem solver has."[2] The remainder of this paper details three phases of making systematic use of the information on hand to answer the three questions of Peter Prescription #36 and convert incipient software disaster into a productive system.

Where Am I?

First, gather the current requirements for the system you are seeking to build or modify, and design an "ideal" system against those requirements. Ignore for the moment the pieces of software you already have, even if they are "unit tested" and function perfectly. Use any structured design methodology of your choice and apply it rigorously. Various groups, some at NSA, have applied HIPO, Transform Analysis, Transaction Center Analysis, and Jackson Design methodology[3] with success. It appears as though the particular tool used is not as important as the fact that some technique is applied uniformly and rigorously across the whole system.

Fig. 1 is an abbreviated structure chart of a segment of a hypothetical system which must gather some data and display it on a terminal, among other things. Note that all functions are broken down into the smallest possible component parts and that all data flow and control are explicit. You can trace the flow of solid arrows to see where the data goes and how it gets changed along the way. Each module has a single function. The modules may be combined together in-line to form a single program, they might be a mix of separate programs and subroutines, or they might even be a mix of hardware, firmware, and software. The point is, the structure chart ignores all those considerations and concentrates on the elements of the problem solution only. Once they are understood, then intelligent decisions can be made separately about how to package the modules.

You may have to resist a great deal of pressure to skip this step. There are still some people lurking about NSA who will try to persuade you that time spent drawing pictures is wasted. (I suspect such characters pervade many institutions in the private sector, too, although I only deduce this from the work delivered by some contractors to NSA.) These people advise that we start attacking the problems directly, even though some symptoms may be half-recognized. Indeed it seems as though each of us tends to have a deep-seated urge to

[2]Moshe F. Rubinstein, *Patterns of Problem Solving* (Englewood Cliffs: Prentice-Hall Inc., 1975), p. 8.

[3]See: Edward Yourdon and Larry L. Constantine, *Structured Design* (New York: Yourdon Inc., 1975) for a discussion of the first three methodologies. See also: *The Jackson Design Methodology*, Infotech International Handbook (Pasadena, 1977).

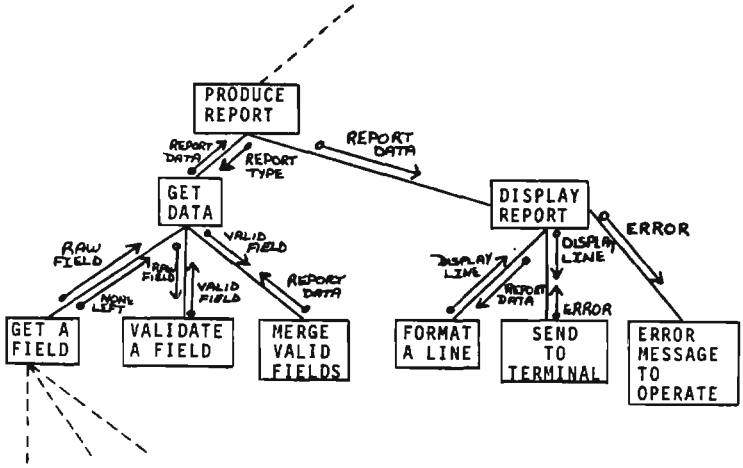


Fig. 1*

* This paper will use several of the Yourdon definitions and conventions. Among them are:

Solid-tailed arrows represent data.
Hollow-tailed arrows represent flags.
A box represents a module.
Arrows into a box interior indicate data flow into the middle of a module as opposed to through the module's entry point.
A module is any lexically contiguous set of computer instructions.
Atomic modules are the lowest-level modules.
A straight line represents one module invoking another module. The higher invokes the lower unless otherwise noted.

DOCID: 4009810

start modifying code too soon.

Just remember that design is cheaper than fabrication. It is an abstraction which can be manipulated easily without intervening distractions such as the hardware peculiarities, operating system vagaries, or programming-language oddities. If done properly, the structure of the design will very closely depict the structure of the actual problem to be solved. You will probably find that someone who has not had a hand in creating the mess you are correcting will be extremely helpful during this design phase. Being uncorrupted by the faults of the existing software design, he can give a more objective opinion of the "fit" between your "ideal" system design and the problem to be solved. The trick is to keep yourself and your team from corrupting him!

You must now document the existing system design using the same notation you used for the design of the ideal system. If you cannot document the design of the existing system, then you should decide to replace it in its entirety. In this case, you might be able to salvage some code from the old system modules as described below. This activity can be very dangerous, however, since you might preserve some of the major causes of your troubles. By saving only atomic modules and resisting the temptation to add code to them, you can protect yourself in most cases.

Now that you have two system designs, the old and ideal, lay them side by side and compare them. You should look for correspondence between the two designs. You might even have some modules from the old design that have already been coded and can be kept as is because they match the ideal design perfectly.

You are likely to have some modules that should be replaced because they are "corrupt" in design. The lack of correspondence will be seen as confused flow of control and inconsistent interfaces with various superordinate modules. The modules will also mix several functions without justifiable purpose.

Fig. 2 shows a possible representation of the existing design documented using the same conventions as the ideal design in Fig. 1. Notice that the data display portion of the system consists of a single module with the functions hopelessly entwined. This characteristic probably was due to a bad system design before the software implementation began, or perhaps the design was not understood or followed. When confronted with hopelessly corrupt modules such as the data gathering/displaying one in Fig. 2, you should salvage whatever atomic modules you can and then throw the remainder of the code away.

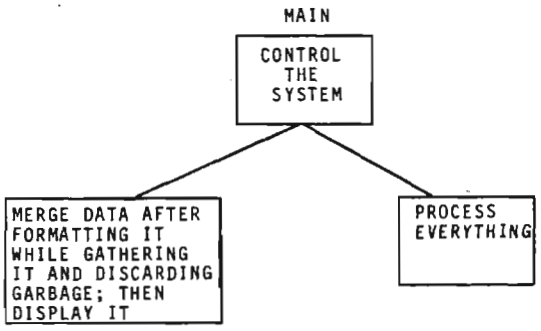


Fig. 2

Fig. 3 depicts how you might be able to extract the coding to construct your ideal "Send to Terminal" and "Format a Line" modules from the existing mess. Very likely, all the other functions are so dispersed and mixed up that you will be able to salvage nothing else.

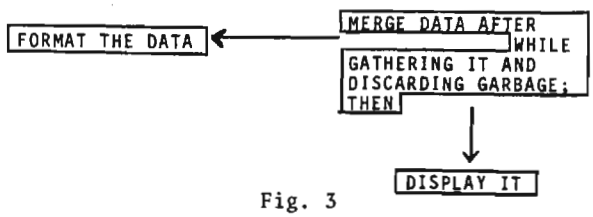


Fig. 3

You might also find some modules in the existing system that are moderately corrupt but have been performing satisfactorily for some time. These represent a real problem, particularly if you find yourself in the same tight resources situation as the rest of the world. You will be tempted to keep them and thus corrupt your ideal system design. Indeed, you might have no choice but to keep at least some of them because of the lack of time, money, or people.

Where Do I Want to Be?

You have already documented where you would like to be in a utopian world when you designed an "ideal" system. But now you must reconcile your ambitions with the reality of limited resources. You must answer Mr. Peter's second question by defining revisions to the software system that make the best possible use of the software already implemented as well as new software to produce a reliable and useful system.

If you keep any poorly-designed modules, you must recognize that you are doing so and realize the possible consequences. The cost of maintaining those modules will be excessive for the life of the system. They might contaminate the rest of your system if you do not take positive steps to prevent it. They might not even be functioning as well as you think; perhaps they just have not yet had sufficient opportunity to fail. They might come back to haunt you at a critical point in the project.

A more subtle danger in using admittedly corrupt modules is that members of your team might perceive a lower set of standards for the software project than you intend. Actions

speak louder than words. If you retain substandard modules from the old system, make sure that every member of your team understands that you know they are substandard, that you have weighed the risks, and that you kept the modules for very specific reasons. Emphasize that the modules are substandard and that you will accept no new modules of similar quality.

You should insulate all substandard modules from the rest of the system with interim interfaces that conform to all the standards of good system design. Figs. 4 and 5 show how this can be done. Module 3 is typical of modules that can be found in many systems. It has multiple entry points; its logic depends on internal flags set by external modules; it gets its data inserted into it by external modules; and it returns its results by placing data directly into the middle of the invoking modules. Let us suppose that module 3 has been stable for a considerable length of time under extremely severe testing conditions and further suppose that to replace module 3 would take 12 man-months. Let us also suppose that you want to replace module 2, a one man-month job, and retain modules 1 and 3.

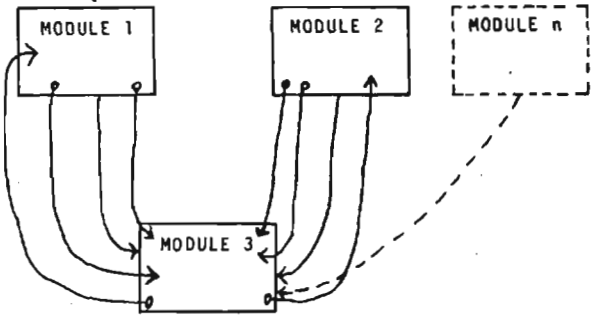


Fig. 4

Fig. 5 depicts the proper way to insulate modules 1 and 3 from the rest of your system. The interim interface module has single entry and exit points, and conducts its external communications (data and control) explicitly. Note that the new version of module 2 uses the interface and follows all the rules of proper intermodule communication, but that modules 1 and 3 are unchanged. You are now in a position to redesign at your leisure module 1 and any other modules which invoke module 1. You can also deploy new modules which invoke module 3 through the interface without compromising their design because of deficiencies in module 3.

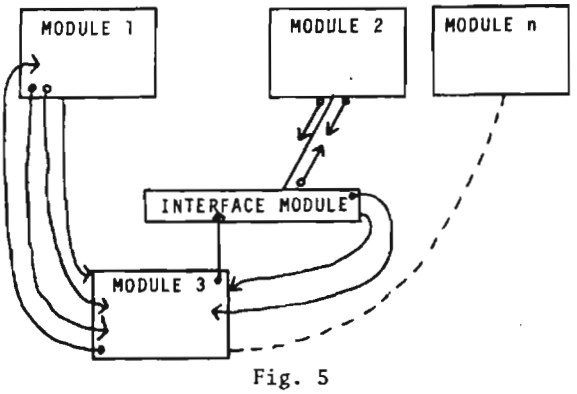


Fig. 5

After all the invoking modules have been converted, then module 3 itself can be reconstructed. Fig. 6 depicts this last step. The interface module has become permanent with the assumption of controlling functions. An array of subordinate modules has been created with each submodule performing exactly one of the functions from the original module 3.

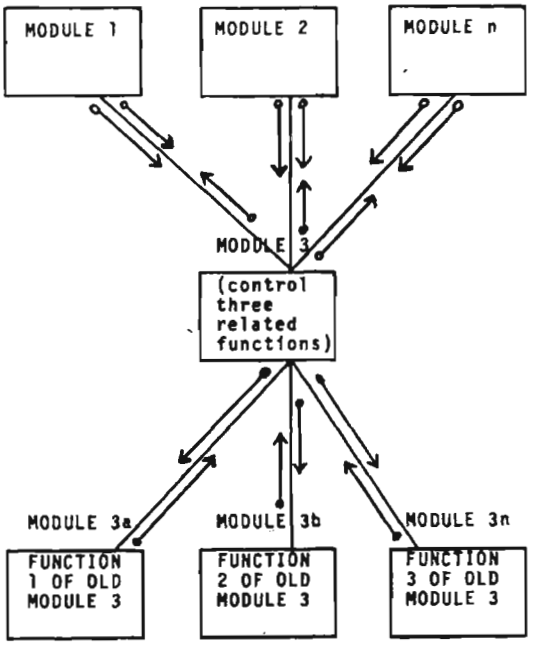


Fig. 6

Another activity of designing is to incorporate the best commercially available products wherever possible, rather than reinventing the wheel. If a portion of your system design calls for modules to manage data, consider using a commercially available data base management system. There are now several on the market which have given many customers satisfactory results[4]. By using one of them, you can concentrate your own personnel on solving the customer problems rather than the computer problems. Consider also some of the newer hardware technology that is available. For example, some of your modules might be best implemented on microprocessors. When you complete step 2 of your remedial software engineering, you will have a complete design plan for your system including how each module will be implemented.

[4]See: Herbert L. Gepner, "User Ratings of Software Packages, *Datamation* (December 1976), p. 108.

How Do I Know I Am Getting There?

You have compared the existing design to an "ideal" system based on the current requirements and devised a design for the system you will implement. Now you must plan the implementation effort and continually compare the actual progress to the plan to answer the last of Peter's questions.

Managing a Programming Project[5] is an excellent reference for use in the project-planning phase and I will not repeat in this paper everything Metzger says in his book. Several points deserve special emphasis, however, and Metzger touches on them only lightly.

It is essential to match your resources to the task or vice versa. Remember the cave dwellers building the house? Assign the right number of people with the appropriate skills to the remedial software effort. Consider augmenting your work force by contracting some pieces of the system to the private sector if you have a surplus of money and a shortage of people, or if some particular skills are unavailable to you directly. I know of one project, not at NSA, where the configuration management function was contracted successfully.

If you cannot staff your effort properly, then scale down your ambitions and undertake to deploy a more limited system. If it is impossible to undertake less and still produce a useful and reliable system, then you should cancel the project. To do otherwise would be a waste of taxpayer dollars. One project manager at NSA recently mused as he stood in the shambles of an overly ambitious and understaffed project, "If you are not big enough to take the bull by the horns, then the best you can possibly hope for is to stay a few steps ahead of the beast as you run in circles around the ring." He was right, only if you accept his assumptions that his size and boldness were the only variables. But the bull could have been either trimmed down in size or eliminated. Shrinking the bull would increase the project manager's relative size and executing the bull would allow the manager to tidy up in a leisurely manner before regrouping for the next fray.

Having achieved the right match-up between the project size and staffing, make sure you provide your workers with all the tools they need. Dick Brandon, president of ACT-Brandon, recently said, "I am amazed today that we are working with 1975 hardware, using 1971 software, and managing as though it is 1960 -- and that we are trying to automate an organization with a structure designed in 1944."[6] Mr. Brandon could have been studying NSA when he said that.

Some of the tools that some managers give too little emphasis to are training, testing mechanisms, and standards. It is unfair to everyone involved to ask a newly hired college graduate or recently transferred computer operator to design, code, and test a piece of software for a computer he has never seen, in a language he knows nothing about, to solve a problem he only vaguely understands. Instead, he should be trained in the language he is to use; he should be handed a copy of the standards his documentation, software, and test plans are expected to adhere to; and he should understand the system design and project plan documentation. He should be working from a detailed functional description of the module or modules he is to produce. The functional description will include detailed descriptions of all interfaces between his software and the rest of the system. The system should have built-in trace and audit trail features to facilitate debugging and testing. Given these tools, you can safely leave the detailed design, coding, debug, and unit testing to the individual's programming team.

One last point I would like to add to Metzger's discussion of planning the project is to consider carefully your system implementation strategy. Harlan Mills of IBM has made some thought-provoking points about the working relationship between computer people and their customers.[7] He suggests that rather than disappearing for several months of coding and testing as soon as you have gotten the customer to sign a detailed requirements document, you should demonstrate another real piece of the system at least once a month. This would greatly reduce the understanding gap that frequently widens between the customer and the system implementers on many software development projects. It will help insure that misunderstandings which occurred during the requirements definition phase are surfaced early, before the whole system is coded and tested. Mr. Mills' arguments tend to be reinforced by my experience with several NSA projects and they suggest some guidelines for your implementation efforts.

Getting There

You have done your homework and rolled up your sleeves to begin the real work. Since your system design has been thoroughly tested in the abstract and you have a detailed project plan and you have even scattered all the right tools about your workers' domain, not much can possibly go wrong. Right?

Wrong!

---

[5]Philip W. Metzger, *Managing a Programming Project* (Englewood Cliffs: Prentice-Hall Inc., 1973).

[6]"The Computer As Villain," *Datamation* (April 1976), p. 14.

[7]Robert L. Patrick, "Software Engineering and Life Cycle Planning, *Datamation* (December 1976), p. 79.

Remember, you are beginning your remedial software engineering effort at a low point on the project. Everyone has been working for 3 years and seems to be no closer to putting a system into production now than when they started. Morale was low before you walked in, but now the requests for transfer are outnumbered only by the volume of help-wanted ads being clipped from the newspaper. You will have to manage the remedial project better than any other project you have worked on.

Metzger covers most aspects of managing the remedial software effort in his chapter, "The Programming Phase."[8] If you heed his advice on organizing your effort, dealing with changes, monitoring and controlling the work, and carrying the water for your subordinates, you will be in pretty good shape. Since the premise of this paper is that the project is already in the middle of the programming phase (or even the test phase) a few additional points should be made.

First, you are likely to encounter great resistance to change. You will find that some optimistic members of the project team are caught up in the "light at the end of the tunnel" syndrome. They will insist that the successful completion of the system is in sight; just a few more corrections and a little extra effort will save the system. Of course, they have been saying this for months and have been reporting the system as 95% complete for about 50% of the elapsed project time. They are expending all of their energies on trying to make whatever code they have work. They never stop to seriously consider that their system design might be unworkable, either from basic flaws present from the outset or because the design has been seriously corrupted during the implementation.

The trick is to convince them that things are really as bad as you know they are. Sometimes a suspension of coding/debugging/testing and the assignment of a design analysis task culminating in a written report will do the trick. Some people will even see the light if you brief them on your own analysis of the existing design. Sometimes, though, you might have to simply pull rank on the individuals and direct them to abandon their design in favor of your revisions. The result could be subordinates who are convinced that you sabotaged their good efforts just as they were about to bear fruit. You will not have their commitment to the revised system and their support will be less than enthusiastic. It would probably be better to transfer to another project anyone who has such an enormous emotional investment in the unworkable design that he refuses to listen to reason.

You may also find that many of your programmers have become obsessed with creating "sophisticated" code to the detriment of the system. This is a common problem, stemming in part from historical pressures to use every possible trick to cram many functions into the fewest memory locations possible. It might also stem from individual recognition that the current system design will never work and the "part of a successful team" reward will never materialize. The individual then internalizes his rewards by challenging himself to be even more clever in his production of code that will run faster in less core and do more work. The trouble is that nobody, including the original creator, will be able to understand the code in 3 months when it has to be modified to allow for a requirements change.

The solution to this problem is twofold. Orient every member of your team to the project objectives and build commitment from all to the development of a system that works. Also establish and enforce programming standards for the project. By ensuring that each individual understands the long-term benefits of never using part of an executable instruction as a constant, never using self-relative arithmetic, never hard-coding variables, avoiding GOTO's, etc., it will become easier for you to enforce the standards. Be sure to reward those who produce quality code as well as redirecting those who spend forever making a seldom-executed subroutine run faster, violating standards in the process.

Remedial Software Engineering: Summary

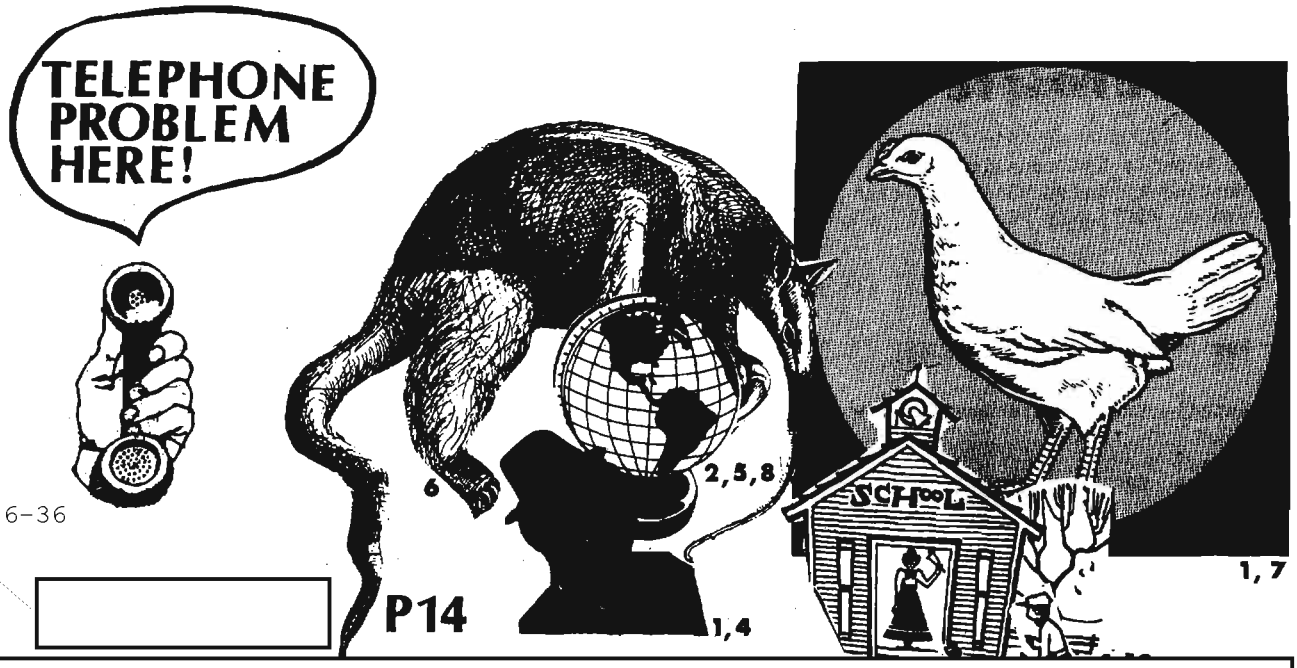
Remedial software Engineering is the systematic application of the best available software design and project management techniques to bring about desirable changes in software systems. RSE uses readily available information to analyze the current state of the system and implement an improved system.

First, the remedial software engineer designs an "ideal" system to satisfy the requirements of the customers and documents the design of the existing system with the same design notation. Next he compares the two designs and evaluates discrepancies between them. Then he resolves the discrepancies by designing a revised system which combines elements of the existing system, new elements, and some temporary elements. Lastly, he manages the remedial project paying particular attention to the "people problems."

By using a Remedial Software Engineering approach to problem systems, the project manager will make rational choices among explicit alternatives, lay the groundwork for productive team efforts, and bring the expectations of management, programmers, and customers into harmony with reality. He will have the management tools required to produce a quality product in a reasonable time.

[8]Metzger, pp. 69-112.

~~CONFIDENTIAL~~



P.L. 86-36

~~CONFIDENTIAL~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36

NSA-crostic No. 13

The quotation on the next page was taken from an NSA publication. The first letters of the WORDS spell out the author's name and the title of the work.

This month's NSA-crostic was submitted by guest NSA-crostician David H. Williams, P16

DEFINITIONS	*WORDS*
A. Feels clumsily	141 160 126 53
B. Intellectual nourishment (3 wds)	76 229 118 204 189 133 176 150 38 86 212 65 103 52
C. Russian man in the street	69 58 127 112 61 207
D. Inside scoop	8 55 163 46 186 200 95
E. Line from film by Word R, cited in Bartlett's Quotations, 14th ed. (5 wds)	172 214 20 203 109 205 88 217 32 159 134 153 121 40 105 4 51 188
F. Industrial city in NE Ohio	9 142 223 221 71 21 60 26 12 168
G. Emphasizes	183 149 31 177 165 231 119 16 78 74 93
H. Pressure group	24 139 106 135 50
I. "To be ------- is some danger," *Hamlet*, Act III, Sc. iv (2 wds)	11 83 77 132 115 224 199
J. "... of their appointed ------"	64 90 1 161 192 34
K. Prolific motion picture director (2 wds)	44 30 79 218 39 181 73 94 17 227 56 100 146 48 110
L. Reinforcing	213 37 144 173 230 138 129 98 208 171 123 2 96
M. Erases	131 84 36 13 120 155 222
N. Another line by Word R cited in Bartlett's Quotations	196 175 91 104 18 5 209 137 187 68 164 41 219 47 122 201 75 148 193 10 156 99
O. Gemstone	107 67 182 152
P. Eluder	195 14 116 206 102 166 33
Q. Word K's fiftieth film, 1966 (2 wds)	54 143 210 125 85 22 42 185 57 226 180
R. Star of eleven films ("Every Day's a Holiday," "Night after Night," etc.), author of eight of them (1893-)	170 80 162 97
S. Vicinity	113 45 147 92 82 63 15 128

DOCID: 4009810

T. Question asked of the cook at the monastery's fish-and-chip stand (5 wds)

U. Process of producing images by reaction of light

V. Intermittently (3 wds)

W. Answer to query in Word T (5 wds)

220	49	59	101	211	202	72	28	108	62	136	114	3	174
	89	228	23	151									
6	194	66	198	111	216	27	81	158	130	157			
35	140	25	179	154	215	169	191						
70	124	7	43	184	117	190	145	178	197	225	87	29	19
						167							

1 J	2 L	3 T	4 E	5 N	6 U	7 W	8 D	9 F		10 N	11 I		12 F	13 M	14 P
	15 S	16 G	17 K		18 N	19 W	20 E	21 F	22 Q	23 T	24 N		25 V	26 F	27 U
	28 T	29 W	30 K	31 G	32 E	33 P	34 J		35 V	36 M		37 L	38 B	39 K	
40 E	41 N	42 Q	43 W	44 K	45 S		46 D	47 N	48 K	49 T	50 H	51 E	52 B	53 A	
54 Q	55 D		56 K	57 Q	58 C	59 T		60 F	61 C		62 T	63 S	64 J	65 B	66 U
	67 O	68 N	69 C	70 W	71 F		72 T	73 K	74 G	75 N		76 B	77 I	78 G	
79 K	80 R	81 U	82 S		83 I	84 M		85 Q	86 B	87 W	88 E	89 T	90 J	91 N	92 S
93 G	94 K	95 D	96 L		97 R	98 L	99 N		100 K	101 T	102 P	103 B	104 N	105 E	
106 H	107 O	108 T	109 E	110 K		111 U	112 C	113 S		114 T	115 I	116 P	117 W		118 B
119 G	120 M	121 E	122 N	123 L	124 W	125 Q		126 A	127 C	128 S		129 L	130 U	131 M	
132 I	133 B	134 E	135 H	136 T	137 N	138 L		139 H	140 V		141 A	142 F	143 Q	144 L	
145 W	146 K	147 S	148 N	149 G	150 B	151 T	152 O		153 E	154 V	155 M	156 N	157 U		158 U
159 E	160 A	161 J	162 R		163 D	164 N	165 G	166 P		167 W	168 F	169 V	170 R	171 L	
172 E	173 L	174 T	175 N	176 B	177 G	178 W	179 V	180 Q	181 K		182 O	183 G	184 W		185 Q
186 D		187 N	188 E	189 B	190 W	191 V	192 J		193 N	194 U	195 P		196 N	197 W	198 U
199 I		200 D	201 N	202 T	203 E	204 B		205 E	206 P	207 C	208 L		209 N	210 Q	211 T
212 B	213 L	214 E	215 V		216 U	217 E	218 K	219 N	220 T	221 F		222 M	223 F	224 I	225 W
226 Q	227 K	228 T	229 B	230 L	231 G										D.H.W.

(Solution next month)

DOCID: 4009810

¿CONOCES BIEN LA GEOGRAFÍA?

Tony Melzer, D5*

Esta vez queremos que tu dés no sólo el nombre de cada país sino el de su capital también.

	País	Capital
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		

Las respuestas se hallarán en el página 21.

Tanteo	
0-8	¡Muy malo!
9-12	Talcualillo
13-15	Bastante bueno
16-17	¡Muy bueno!

* Cartógrafo y autor del texto en inglés; traducido en español por Esteban Vermás.

C.A.A. NEWS By W.E.S.

May 1978 Presentation Planned

As of this writing (February 1978), it *looks* pretty firm that our featured speaker for May will be our #1 Member (see reproduced membership card). Watch for announcements about day and time.

COMMUNICATIONS ANALYSIS ASSOCIATION
THIS IS TO CERTIFY THAT
VADM B. R. Inman, USN
is a member in good standing of this association for the year ending 31 December 19 *78*
1 '78 President

(U)

What to do for members on PCS?

CAA members who transfer to overseas jobs are continued on our membership rolls "free" (no dues) for the duration of their PCS tour overseas. One of the things the CAA Board will be wrestling with this year is how we can extend the aims and goals and benefits of the CAA to people who are "off campus." We want to talk with those of you who have ideas about this. Have you been overseas and "out of touch"? What do you think the CAA can do to help people who are now in the situation you were in? (U)

Meet our new president!

Our new president is David W. Gaddy, a Cryptologist in D5. He earned his BA in U.S. History at the University of North Carolina and an MS in International Affairs at George Washington University.

His cryptologic experience has included assignments as linguist, bookbreaker, reporter, and supervisor on a wide variety of problems and targets in Southeast Asia. He was selected for the Armed Forces Staff College, Norfolk, Virginia, in 1967, and for the National War College in 1971.

Since his return from the War College, he has held various senior planning positions, including a tour at the Pentagon (NCR Defense). He is currently Deputy Chief, Intelligence Community Affairs (D5).

He is certified as a Linguist and Special Research Analyst. ~~(C CCO)~~

. . .and our new president-elect!

Our new president-elect is Francis X. Porrino, Chief of A1, Office of Operations and Control. He has served in the cryptologic community since 1951, first as an enlisted man in the Air Force Security Service, then in several capacities as a civilian (since 1955).

He has performed at all levels of management through Office Chief.

has attended the National War College, has served on the staff of the NCRDEF, and has served as Chief, A1. Also, over the course of his NSA career, he has completed studies at the University of Maryland, earning a BA degree in Government and Politics, and has served overseas in the Office He has also been awarded the Civilian Meritorious Service Award. EO 1.4.(c) P.L. 86-36

He is certified in TA and SR and has been a member of the SR Career Panel. ~~(C CCO)~~

How to become a member

CAA dues are $1.00 per year. You can get membership applications from any of the people mentioned in these CAA news items. Send the completed application and $1.00 to Tim Murphy, B09, 3W114. Then just sit back and watch your in-basket fill up with news bulletins and announcements about all the many and varied activities and programs of CAA. (U) P.L. 86-36

Communications Analysis Association:		
President	David Gaddy	3247
President-elect	Frank Porrino	5879
Secretary		
Treasurer	Tim Murphy	3791
Board members		

I'm running out of space! I wanted to give a biographical sketch on our newest CAA Board member, and mention our Program Committee chaired by Can't wedge them in. I'll try next month!

~~CONFIDENTIAL~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4009810

ata american translators association

Dear President Carter:

September 14, 1977

The following letter was sent on September 14, 1977 to the President of the United States by Royal L. Tinsley, Jr., President of the American Translators Association.

Dear Mr. President:

Please accept my congratulations and sincere appreciation for your encouraging attitude toward the study of foreign languages and cultures as expressed in your letter of 29 June 1977 to Congressman Dante Fascell concerning the Helsinki Final Act. Let us hope that the foreign-language teaching profession has learned its lesson from the 1960s and will make better use of future support by the Federal Government. I am a dedicated teacher of German (and sometime Russian teacher), but it is not as a teacher of foreign languages that I am writing this letter; you will no doubt receive enough letters from my colleagues in the profession.

Rather, as President of the American Translators Association I am deeply concerned about the future of the translating profession in this country. Although the study of foreign languages is critically important for the welfare of the U.S., no one can learn more than a few languages, and most will do well to acquire minimal competence in even one foreign language. Anything the individual learns about all the other cultures must ultimately be learned through the medium of translation.

You are more aware than most Americans, I am sure, that the United States is no longer the world leader in several scientific and technical fields. This is no catastrophe, in itself, for surely every nation should have the right to excel at something. I think you will agree, however, that unless our American scientists and technicians can keep abreast of the latest developments in their respective specialties there is, at the very least, undesirable duplication of effort and waste of time, energy, and money. Translation provides the only feasible means by which we can keep up with developments in all areas of the world.

In recent years there has been much duplication and waste even in the vital area of technical translation. Cover-to-cover translations of foreign technical journals often provide translation of worthless material along with the crucially important. There should be a screening process for each discipline whereby leading experts in the field would select important articles and books for translation by competently trained translators.

The latest developments in science and technology are now being published in more than 70 languages of some 100 countries. Even though English still accounts for about 45% of this material, and another 35% is published in Russian, German, and French, some 20% appears in the less-well-known languages. The information value of Japanese publications has increased remarkably over the past few years, while Hungarian has become very important for electroninc, Swedish for metallurgy, power engineering, and communications systems, and Finnish for woodworking, pulp and paper technology, icebreaker construction, etc. Polish, Czech, Bulgarian, and Rumanian technical literature is also becoming important, as is Spanish and Portuguese. When an agreement is finally reached that will permit us access to the technical literature of the People's Republic of China we shall have several decades of development to study, and there is less than a handful of people in the United States today who are competent to translate technical Chinese.

The number of translators in the Federal Government has been steadily reduced over the past several years. The shocking state of affairs in government translation was described by Richard S. Relac in a report in *The Federal Linguist*, Vol. 6, No. 1-2 (Summer 1974). In what was presumably intended as an economy measure, government translators were progressively phased out by elimination of jobs and by refusal to replace personnel lost through death or retirement. Many simply resigned because they were given GS ratings below those specified for the positions and were denied promotions. Government translation needs were supplied to an increasing degree by contractors who received the work on a low-bid basis. Despite claims to the contrary by government

Reprinted by permission of "The ATA Chronicle," newsletter of the American Translators Association, P.O. Box 129, Croton-on-Hudson, N. Y. 10520.

DOCID: 4009810

procurement officers it can be documented that this procedure resulted in an incredible waste of money for a large number of marginally useful or completely worthless translations. Most professional translators either refused to work for the ridiculously low rates paid by the contractors or, in some few cases of which we are ashamed, they simply did not spend the time and effort necessary to do a professional job. The contractors were forced to recruit students, immigrants, war brides, etc., in order to meet their commitments. Some of these people did indeed become competent translators in time, but at a staggering cost to the taxpayers!

Mr. Lester C. Benefeld, Jr., Director of the Foreign Language Research Branch of the U.S. Army Foreign Science and Technology Center, was questioned during a meeting at Georgetown University in 1975 about the quality of this contract translation. Mr. Benefeld answered that most of these translations would never be used, and that it was sufficient, in any case, if the Army's scientists and technicians could deduce from the equations, tables, and graphs what the article was about! One wonders why the government should have paid even low rates for translation that apparently was not needed.

"Shocking state of affairs in government translation."

In July of this year an official of the U.S. Bureau of Reclamation in Denver stated that there are government scientists and technicians who honestly believe that their Russian and German counterparts are incapable of writing understandable reports of their own experiments because every translation these American technicians have tried to use has been virtually incomprehensible! Competent professional translators do not turn Russian and German technical writing into incomprehensible English, and the Bureau of Reclamation asked the American Translators Association to hold a workshop for translators so that the Bureau could explain the types of materials it needed translated. Through this workshop the Bureau found several professional translators who could provide competent translation services for reasonable compensation.

This false economy move of the Federal Government has also had its negative effects on foreign-language education in the colleges and, especially, in the high schools of this nation. Granted that the foreign-language teachers were slow to respond to the desire of students to learn foreign languages for practical use rather than as an entrée into the literature of these languages, government policies must also share a large part of the blame for the decline in foreign-language study in this country during the past few years. Back in 1973 President Nixon's budget wiped out support by the National Defense Education Act of some 4500 courses in more than 80 languages and in all foreign areas -- at a savings of less than the cost of one F-111 fighter-bomber! [Marshall D. Schulman, *The New York Times*, April 6, 1973, p. 39.] With the Federal Government eliminating career opportunities and foreign-language programs in the schools, indicating by its own example that foreign-language study was of little or no importance, is it any wonder that young Americans have no desire to study foreign languages?

The United States is unique among the large industrial nations of the world in its attitude toward translation. There is practically no training available for translators in this country. Most of our professional translators are either self-trained through years of trial and error, or they received training in European schools for translators and interpreters. According to the Relac Report, there were no more than a half dozen translator trainees in the entire U.S. Civil Service in 1974. Prior to 1970 the only training programs were at Georgetown University and at the Monterey Istitute of Foreign Studies. Since then some 25 or 30 colleges and universities have initiated one or more courses in translation techniques, but the only viable, comprehensive training programs that have been added for technical translators are those at the University of California at Santa Barbara (French, German, Spanish), Carnegie-Mellon University (French, German, Russian, Spanish), Stanford University (German), the University of Puerto Rico (Spanish), St.-Mary-of-the-Woods College (French, Spanish), and the Rose Hulman Institute of Technology (German, Russian).

"No reliable statistics exist for the amount of translation in the United States."

Moreover, most of the students in these programs (all of them at the Rose Hulman Institutute) are not training to become translators -- they are future scientists and engineers who want to learn how to read foreign research in their own fields. (They will still be able to read only one or two foreign languages, however.) Of a total 162 students enrolled in 5 of these programs as of October 1976, approximately 60 hoped to become translators. The same 5 programs graduated 12 students in 1975, at least 10 of whom were employed in non-translation jobs or in positions where their language skills were of only minor importance.

In contrast, Canada has 8 training institutions for translators and interpreters, and Western Europe has over 40. There is already a critical shortage of competent technical translators in this country, and if the Bilingual Courts Act ever becomes law there will be utter chaos with every Spanish-speaking janitor pressed into service as a court-interpreter. In a courtroom situation where property, freedom, and even lives may depend upon

---

"A national disgrace"

---

accurate translation of not only words but of culturally significant gestures, tones of voice, facial expression, etc., we cannot afford to have untrained people acting as interpreters. Translating and interpreting require training and experience, NOT just bilinguality.

No reliable, comprehensive statistics exist for the amount of translation performed annually in the United States, the amount spent for translation, the relative importance of various language combinations and of the different scientific and technical fields that use translations, the number of full-time and part-time translators in the country, etc., etc., etc. On the other hand, periodic surveys of almost every other aspect of business provide current statistics on how many hamburgers are consumed annually in Kalamazoo or how many pickles one can expect to sell in Atlanta. Since 1970 I have contacted the Bureau of the Census, Department of Commerce, Congressmen, Senators -- anyone and everyone I thought might persuade the Federal Government to collect such data along with the myriad other statistics they are compiling continuously -- all to no avail. How can we plan training programs intelligently, how can we predict how many translators will be needed in 10 years, for example, and in which languages and technical fields, without reliable data concerning the present state of the profession? The American Translators Association simply does not have sufficient funds to gather such statistics.

The Soviet Union has these vital statistics. The All-Union Center for Translation of Scientific and Technical Literature and Documentation in Moscow reports that its translation output doubled between 1970 and 1973, that it increased by 150% between 1973 and 1975, and that the 1976 output was 30% greater than in 1975, totally some 350 million words. The All-Union Center is only one of several agencies in the Soviet Union. The Chambers of Commerce and Industry translated 230 million words in 1975, Intourist translates about 17 million words annually, and the Central Research Institute for Patent Information a little over 7 million words. This was a total of more than 500 million words in 1975, and other, smaller departments, agencies, and research institutions in the Soviet Union are reported to have translated several times that amount. [V. N. Gerasimov, *Translation News*, Vol. 7, No. 1 (April/May 1977), pp. 1-11.]

Moreover, since 1975 all translations in the Soviet Union have been registered. We have a National Translations Center at the John Crerar Library in Chicago that makes a valiant effort to eliminate duplication and reduce costs by making existing translations available for approximately the cost of duplication, or by directing requestors to the proper source for the desired translation. Unfortunately, National Science Foundation funds for the NTC were cut off a few years ago and the NTC staff was reduced from 11 to 4. Over the past four-and-a-half years the NTC has deposited or reported availability of 85,891 technical translations, but even more were deposited with or reported to the NTC -- the staff of four simply could not process any more. The NTC estimates that no more than half the technical translations made in the U.S. (and probably considerably less than half) are reported to them, due at least in part to lack of funds and staff to make the existence of the NTC known to everyone involved in the production and utilization of translations. This, Mr. President, is a national disgrace.

Although I have concentrated on technical translation because that is the critical field, commercial translation (banking reports, correspondence, contracts, bills of lading, etc.) is playing an increasingly important role as American business tries to compete in the world marketplace. Nor should we forget the importance of translation in making literature and drama from other cultures available to the American public. The only training program for literary translators in the U.S. at this time is at the State University of New York at Binghamton.

In your efforts to encourage the study of foreign language and cultures I hope you will also remember the neglected but very important role of the translators of America -- in science and technology, in business and commerce, and in the humanities. In closing I would like to offer my services as an individual and the cooperation of the American Translators Association to the Commission proposed by Congressman Simon.

Respectfully,

Royal L. Tinsley, Jr.
President of ATA
Associate Professor of German
University of Arizona
Tucson, Arizona 85721

DOCID: 4009810

P.L. 86-36

Letters to the Editor

To the Editor, CRYPTOLOG:

The note at the end of [redacted] article "A Linguist Looks at the 'Tube'" (CRYPTOLOG, March 1978) states that the article was "untouched by human hands." Whenever I read or hear such statements, I start looking for human intervention. I remember, for example, machine-translation output that used to be advertised as "completely un-postedited" that would prove to have hyphens appearing mysteriously (but correctly!), or to have proper names output in capital letters (such as EYZENKHAUER) even though the names had been "unrecognized" by the computer.

From reading the article, I get the impression that the right-hand justification is done by adjusting the spaces between the words in each line, without bothering to use any complicated hyphenation rules. But I see (last line, left column, page 11) "organi-" and (line 6, right column, page 11) "justifi-." Who put in those hyphens and when?

Hy Fennwatcher

The author of the article replies:

The word processing system used for my article accomplishes right-margin justification by inserting a maximum of two spaces between words and works best on normal lines of 60 to 80 characters.

Because of CRYPTOLOG's short lines, the word processor occasionally was unable fully to perform its right justification on my article and, in fact, left a very ragged margin in the paragraph that Hy Fennwatcher mentioned.

Therefore, to improve the appearance of the paragraph, my helper interactively (i.e. on the CRT screen) hyphenated "organization" and let the computer realign the rest of the paragraph. Seeing that the results were acceptable except for the last three lines, she then hyphenated "justification" in the third-from-last line and let the computer redo the last two lines.

This intervention would not have been necessary for a page of standard width, but it is a good example of the ease with which text can be revised on a CRT-based text handling system. The alterations did not require retyping of the article or even a page.

[redacted] G92

(U)

To the Editor, CRYPTOLOG:

Yes, Art, CRYPTOLOG ads *do* get results. In a quarter-page filler in the January 1978 issue I listed some "new and improved aids for bookbreaking." Within a week after the issue hit the streets, the persons listed as contact points were bombarded with requests for information or copies of the programs. It pays to advertise in CRYPTOLOG!

An unsolicited testimonial from a satisfied subscriber -- V. V. (Bookbreaking and Cryptolinguistics Coordinator, P16) (U)

Solution to NSA-crostic No. 12

(*CRYPTOLOG*, March 1977)

Sam[uel S.] Snyder, "[*Influence of U.S. Cryptologic Organizations on the Digital] Computer Industry*, National Security Agency, Fort George G. Meade, Maryland, May 1977, 36 pp., S-217,130, (U).

"One of the earliest commercial high-speed line printers came about because of NSA support, based at least partly on experimentation and initiatives by Agency engineers. Likewise, one of the first practical character-sensing machines received early [contract] encouragement from NSA."

(U)

Solución a "¿Conoces Bien la Geografía?"

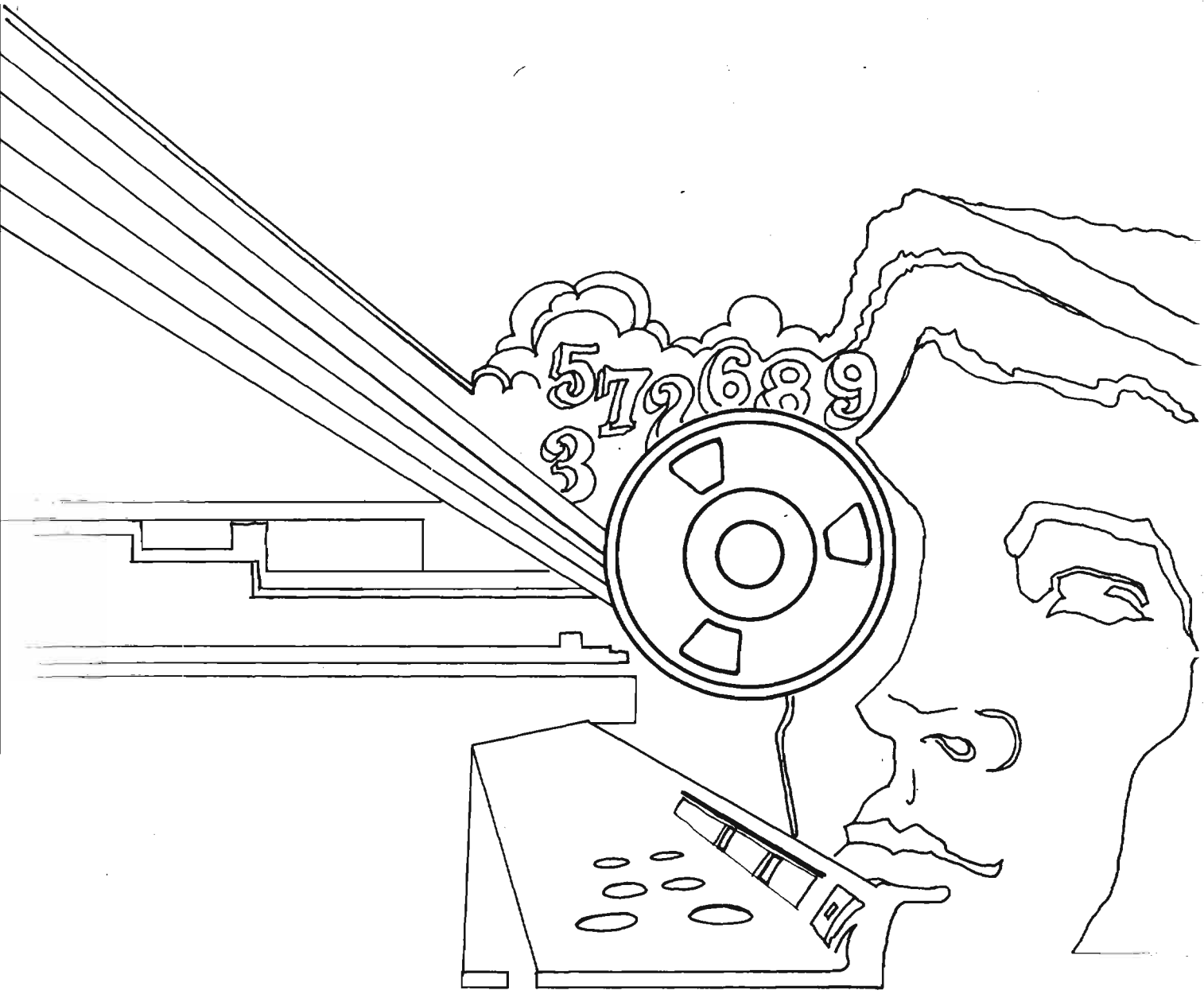
(p. 18)

1. Honduras	Tegucigalpa
2. Nicaragua	Managua
3. Costa Rica	San José
4. Panamá	Panamá (Panama City)
5. Colombia	Bogotá
6. Venezuela	Caracas
7. Guayana (Guyana)	Georgetown
8. Surinam	Paramaribo
9. Guayana francesa (French Guiana)	Cayena (Cayenne)
10. Ecuador	Quito
11. Perú	Lima
12. Brasil (Brazil)	Brasilia
13. Bolivia	La Paz/Sucre
14. Paraguay	Asunción
15. Chile	Santiago
16. Argentina	Buenos Aires
17. Uruguay	Montevideo

(U)

P1-MAR 78-S3-26295

P.L. 86-36


5726893

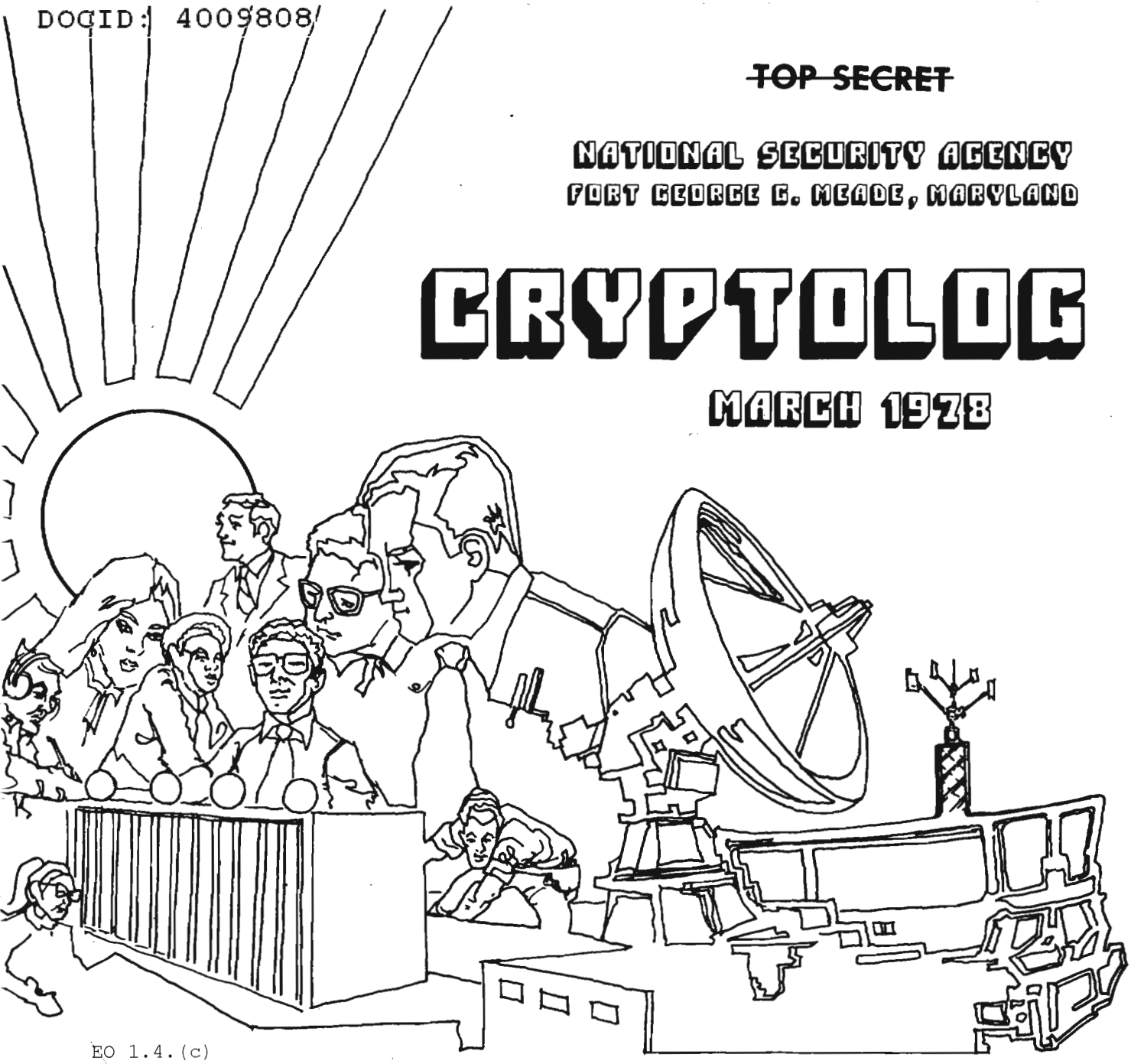
DOCID: 4009808

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MARCH 1978



EO 1.4.(c)

SOME BACKGROUND ON THE C/T MERGER....Frank Smith.....1
HAND IS NOT QUICKER THAN THE EYE....[redacted].....9
A DONKEY IN YOUR WHAT?.....[redacted].....10
A LINGUIST LOOKS AT THE "TUBE".....[redacted].....11
LETTERS TO THE EDITOR.....13
AN IDEA FOR AN ARTICLE.....Doris E. Miller.....14
WORD-SEEK.....[redacted].....15
NSA-CROSTIC NO. 12.....A.J.S.....16
C.L.A. NEWS: C.A.A. NEWS.....18
[redacted].....[redacted].....19
CURE FOR "PERFORMANCE SYNDROME".....[redacted].....29

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009808

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. V, NO. 3 MARCH 1978

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5642s)
Collection.....[redacted] (8955s)
Cryptanalysis.....[redacted] (4902s)
Language.....[redacted] (5236s)
Machine Support.....[redacted] (5303s)
Mathematics.....Reed Dawson (3957s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....[redacted] (4477s)

Production Manager.....Harry Goff (4998s)

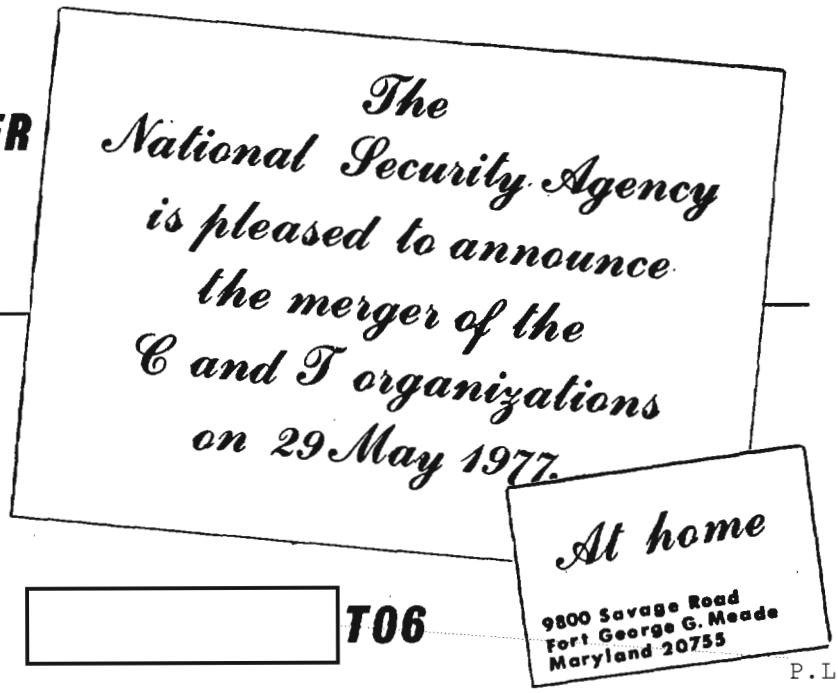
P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4009808

~~FOR OFFICIAL USE ONLY~~

SOME BACKGROUND ON THE C/T MERGER



P.L. 86-36

On 25 March 1977 the Director published a memorandum directing the "Consolidation of Automatic Data Processing and Communications." On 29 May the C and T organizations combined to form the Telecommunications and Computer Services Organization (T) under the Deputy Director for Telecommunications and Computer Services (DDT). It is my purpose this morning to review with you some of the background to this decision. Please note that the title is "Some Background." I know there are many different opinions about something as significant as the C/T merger. This is especially so when people feel -- as the people in C Group and TCOM felt -- that they were generally satisfied with the way things were.

It is not my intent to discuss the new organization itself, but to concentrate on some of the events which led to the C/T merger. In other words, to explore what many believe to be an increasing convergence of the disciplines of data processing and telecommunications which indicates that they should be combined.

Closely related to this convergence is the problem of how to organize automatic data processing (ADP). The problem of how to organize is not unique to us or to the federal government. In the fall of 1976 the American Management Association began sponsoring a series of 3-day study sessions on "The Crisis in EDP Organization," primarily for the business community. These study sessions -- which deal with the organization of such equipment and functions as "Data Networks," "Data Bases," "Micros," "Minis," "Virtual Memory," "Distributed Systems," "Stand-Alone Minicomputers," "Minicomputer Networks," and "Small Business Computers" -- have been well attended, I understand.

Basic Principles of Organization

It might be well for us to refresh our memory about how this subject of "organization" fits into the management function. Ernest Dale, in his *Management Theory and Practice*, lists the following management functions:

- Planning,
- Organizing,
- Staffing,
- Direction,
- Control,
- Innovation.

You will note that "organizing" is of a very high order in top management's consideration.

In his 1964 book *Managing for Results*, Peter Drucker outlines how knowledge is the essential ingredient. He cites IBM as an example. IBM bills for equipment; that was more true in 1964 when he made the statement than it is today. But both IBM and the customer know that knowledge is the essential thing, and that the customer buys service rather than product. Indeed, it is this awareness on both sides that explains why IBM, starting late and with reluctance, took the leadership in the computer field away from companies that had started earlier and that seemed to possess much greater technical competence. In his later and very provocative book, *The Unseen Revolution*, in 1976, Drucker discusses the fact that more and more jobs are "knowledge" jobs in our society. The number of "knowledge" jobs is growing rapidly while the number in manufacturing has shrunk sharply. Yet little has been done about the productivity of the so-called knowledge worker. The principles that apply to making manual work pro-

Complete transcript of a talk given to CISI (NSA Computer & Information Sciences Institute) in September 1977. Excerpts of the talk were printed in Field Information Letter 1-78.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009808

P.L. 86-36

ductive also apply to knowledge work. He then outlines the need for analyzing and organizing the tasks of "knowledge" jobs to improve productivity.

"Challenge to SIGINT: Change or Die" (1969)

By way of introduction to this subject in NSA, I would like to make a digression from the C/T merger and quote from an article that you may remember from the first issue of the *Cryptologic Spectrum* in 1969. The article, "Challenge to SIGINT: Change or Die," was written by [redacted] a recognized authority in the scientific community and a member of the NSA Scientific Advisory Board. In that article [redacted] pointed out that SIGINT activities, obviously, would continue to be important for NSA's future, but the ever-increasing speed of technological advances was threatening to put us out of business, unless we could exploit the other changes that opened new doors. If we can't move with the new technologies that help us, [redacted] said, the ones that make our job harder will bury us. By "change" he did not mean something simple, like replacing vacuum tubes with transistors and continuing to perform the same old functions. He meant changes in strategies, tactics, tools, organizational structures, resource allocations, and personnel. He said that the right way of doing the job would change in elusive ways.

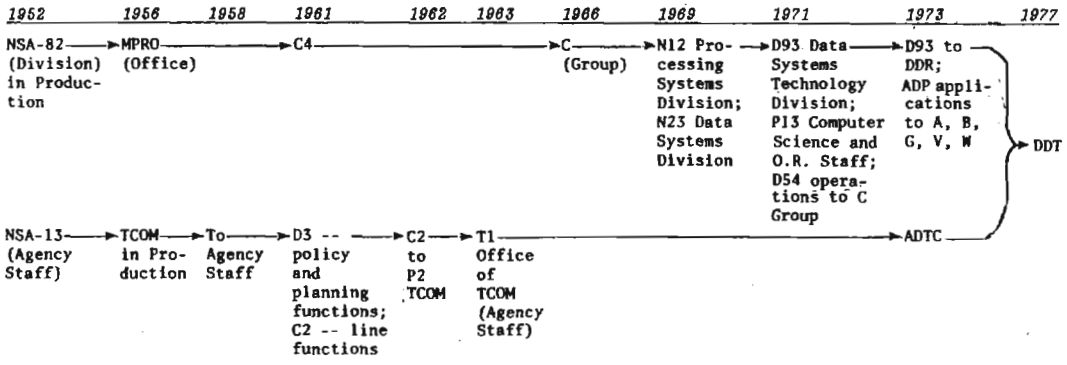
[redacted] further pointed out that in the "poor world," where over two-thirds of the world's population live, the population growth rate was 3 percent per year or more, while in the "rich world," where we live, the rate was dropping. We can expect, he said, to be attacked (verbally and physically) over the next few decades by larger numbers of dissatisfied people. We cannot expect to bring more people into our military defense; we must move forward in labor-saving tools so that we can do more work with fewer people. The number of governments in the world to whose intentions the United States must keep alert was growing, and even when [redacted] wrote these words in 1969, was well over 100. While only a small number of nations threatened us in 1969 with military force, there was little to suggest that the number could not increase dramatically within the coming years. We would have to be on the lookout in all directions simultaneously. Meanwhile, the communication of information from point to point was becoming incredibly less costly. There was promise, [redacted] said, that those costs would fall by a factor of 5 or 10 within a few years after he wrote his article.

[redacted] warned that although many of the early contributions to the arts of automatic computing had their origin within NSA and its predecessors, the commercial world appeared to be outstripping us in the application of computer systems. As the cost of output from computers continued to drop, we had an opportunity, he said, to do more and more work with the help of these amazing machines. So this was the challenge that [redacted] saw in 1969, and it continues to pertain today: Don't try to stick too long with obsolete means. Press forward with vigor and stay flexible. Try to achieve that nice distinction between the visionary and the tried-and-true.

History of C & T Organizations

In briefly reviewing the history of the C and T organizations, we can get a better understanding of what has happened to both ADP and Telecommunications by comparing their organizational development over the 25 years since the Agency was created.

History of C & T Organizations (1952-1977)



DOCID: 4009808

As one can see from the chart, ADP has remained within the Production organization, except that certain staff functions have been assigned to Agency staffs and DDR. In 1971 the N12 and N23 functions went to D9, the Assistant Directorship for Science and Technology. You will note that in 1961 the ADP function was C4. At that time TCOM was C2 -- the two functions were both under Group C as co-support functions within the Production organization. The idea at that time was much as it is today -- to achieve an integrated systems approach to the design and flow of materials in the overall NSA production system.

In the case of telecommunications there were some complications which did not appear in the ADP field until later. TCOM functions within NSA were always more closely aligned to other elements of the government than was ADP. This became more pronounced in the early planning of CRITICOMM, when the Chief, TCOM, wherever he was, was working closely with the J6, JCS, and DCS. There was a need for "the emphasis and prestige that the Agency desired to place on TCOM functions and the channels of communications desired between the Director and his principal TCOM executive."

Consolidation of ADP and Communications Outside of NSA

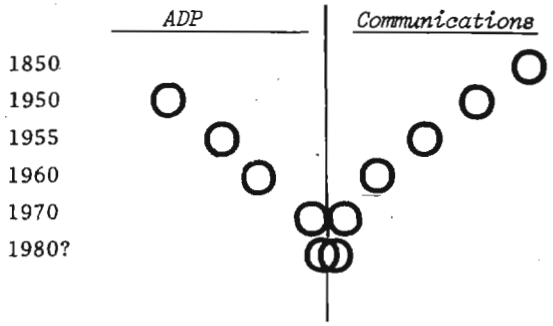
I would like now to review, briefly of course, what has been recommended and what is being done about ADP and telecommunications organizations outside of NSA.

A Blue Ribbon Defense Panel Report, in July 1970, found that "indications are that most computers will be on-line with teleprocessing capability by 1980." The report continued with the statement:

> "Present assignment of policy responsibility for ADP in OSD takes inadequate cognizance of the close technical and cost relationship of communications and ADP management. As a consequence, the interface between ADP and communications is inadequate, and will become increasingly inadequate as digital communications technology increases."

The House Committee on Appropriations, in its report on the FY-71 DoD Appropriation Bill, expressed concern with the Panel's recommendation that all responsibility for Defense ADP should be placed under the supervision of the Office of Special Assistant to the Secretary of Defense for Telecommunications. The committee was pleased with progress being made in improving the management of communications and ADP, but saw them as two distinct and separate operational activities which should have separate management.

A number of NSA people -- and I was one of them -- attended a symposium on computer/communications sponsored by the National Communications System in October 1970. The theme of the symposium was "The Growing Interrelationship Between ... ADP and Communications." That interrelationship, with the tendency toward convergence, can be seen from the following diagram.



This symposium followed the logic of the Blue Ribbon Panel and created considerable impetus for consideration of ADP and telecommunication mergers throughout the federal government. Perhaps I can best summarize the thrust of the symposium by quoting from its program:

> "Teleprocessing is a new technology, resulting from the marriage of automatic data processing and telecommunications techniques, providing a tool to extend information processing, storage, retrieval, transfer, and recording capabilities for more effectively directing and controlling organizations and systems. Typically, while teleprocessing retains certain characteristics of its parents, this new technology possesses features that are both different and unique."

The push toward closer coordination between ADP and telecommunications in the federal government continued through the early 1970s.

Interagency and DoD Conferences (1976)

Mr. Terril J. Steichen, from the Office of Telecommunications Policy, Executive Office of the President, spoke to the Interagency and Planning Conference in early 1976 on the challenge of the converging technologies and the crossing of disciplines. He expressed concern that the convergence of these two formerly separate technologies has spawned a very top-heavy dual staff organization that is perhaps beginning to cause more problem than it solves.

Later, as a part of the Department of Defense ADP Management Improvement Conference held on 12 January 1976, several issues affecting the DoD Automation Objectives were identified. One of these was AUTODIN II. The presentation and discussion for this item centered around the theme that a cooperative effort between the ADP and telecommunications communities is all-important.

The Honorable Terence E. McClary, ASD (Comptroller) concluded the conference with some pertinent comments:

DOCID: 4009808

- Congressional direction to the Air Force relative to centralizing all ADP resources will be executed, unless absolutely impossible.

- GSA is reaching out with leadership plans in the ADP arena; the DoD community should react with the view that if we cannot change GSA, then we must learn to live with the situation.

- The DoD ADP group is characterized by emotion and outrage. This attitude may require correction. There is a need to back off and look at the reasons why GSA and the Office of Federal Procurement Policy thrusts in ADP are taking place. We may be wise to adjust more to the public policy. Positive leadership by the DoD ADP executive may be more important than ever before.

Survey of Communications Organization and Structure

Gilbert Held, Acting Chief of Teleprocessing for the U.S. Civil Service Commission, conducted a survey of the communications organization and structure at eight government agencies and industrial firms. His June 1977 report uncovered a characteristic common to the majority: lack of organization.

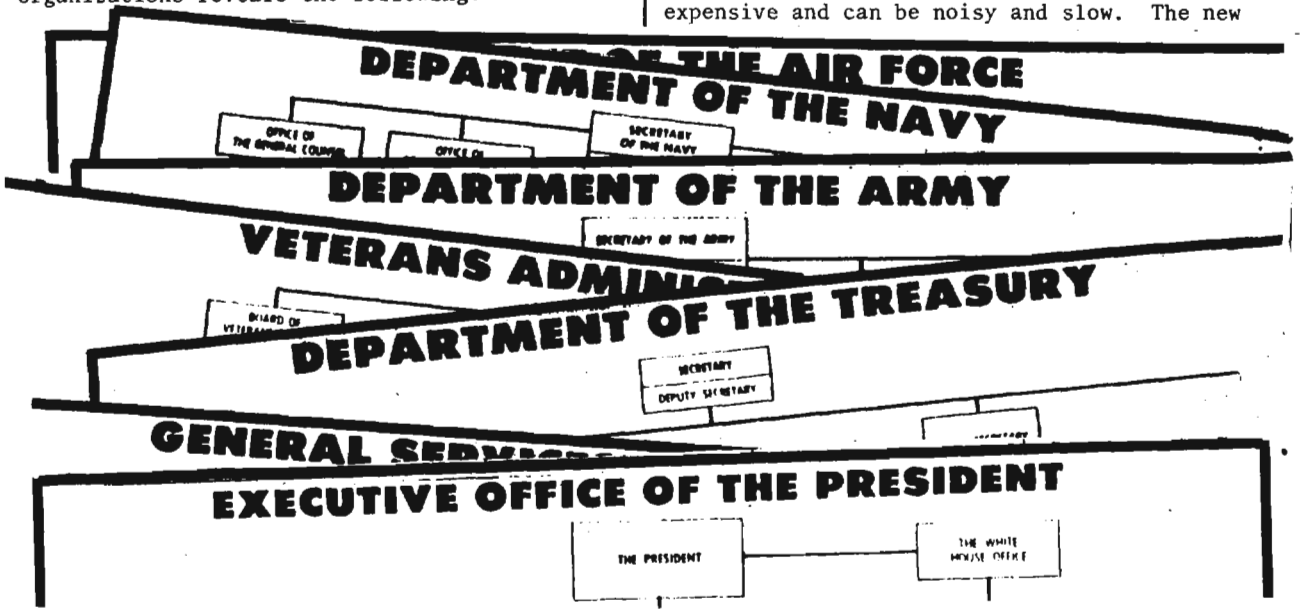
Perhaps this can best be demonstrated by taking a look at several major government organizations to see where ADP and communications fit into the overall scheme. A thorough examination of the organizational charts for those organizations reveals the following:

- *Executive Office of the President* has an Office of Telecommunications Policy, but nothing on ADP;
- *GSA* has a Commissioner of Automated Data and Telecommunications Services. As you know, GSA was probably the first major element of government to combine these services;
- *Treasury* has an Office of Computer Sciences, but nothing on communications;
- *Veterans Administration* has a Department of Data Management, and under that department is an Office of Telecommunications Service;
- *Army* has a Communications Command, but you can't find ADP;
- *Navy* has a Naval Telecommunications Command, but no ADP;
- *Air Force* has an Assistant Chief of Staff for Communications and Computer Services. As I mentioned earlier, the merger was done by Congressional direction.

Situation in Private Industry

At the present time, only three companies -- RCA, Western Union, and Comsat General -- own complete satellite systems. In January 1977, though, the Federal Communications Commission took a momentous step by admitting IBM to the satellite business, and with it the first system that will push the technology to some of its logical conclusions. Five or six years from now, if all goes according to plan, large corporations and government agencies will have private networks using a total of at least 375 earth stations.

The current satellite facilities, for the most part, all transmit to a relatively few, large earth satellites, which then send the message to customers over land lines that are expensive and can be noisy and slow. The new



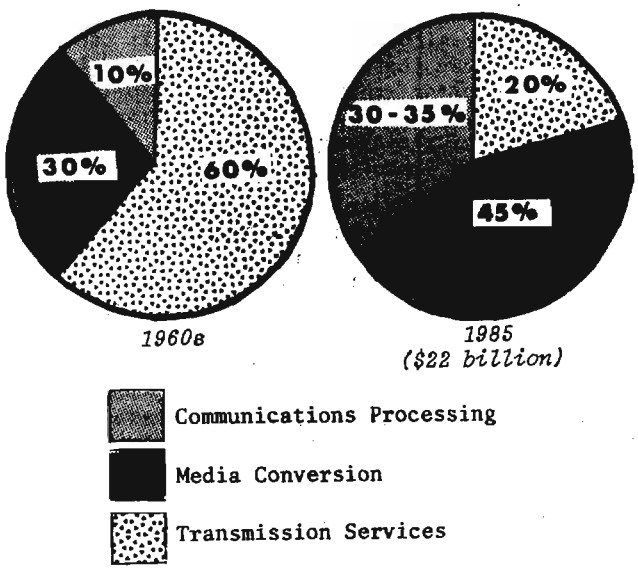
system will bypass this mire by broadcasting directly to antennas small enough to fit into a two-car garage. They will typically be on the roof of a building or in a parking lot. At an average production cost of $345,000 each, the earth stations will be cheap enough for a corporation to lease a dozen or two and forge direct celestial links among its offices and plants across the country.

For those of you who haven't read the book *The Waves of Change*, by Charles P. Lecht, which has been published in *Computerworld* in installments, you will find some interesting thoughts. In his discussion of future system architecture in the commercial field, he sees a vast expansion in on-line, communications-oriented, transaction-oriented, and real-time systems in the 1979-1984 period. But he sees this growth restricted by AT&T communications tariffs and line inefficiencies until AT&T can fully implement digital networks, or until IBM communications satellites and private branch exchanges become operational.

Lecht sees IBM and AT&T pursuing strategies which suggest major competitive confrontations by the end of the 1970s. Both want to supply a total end-to-end service. A key challenge is to define the relative meaning of "data processing" in such a way as to arrive at some workable consensus on the meaning and roles of "message switching," "transmission," "circuit switching," and other interdependent terms and concepts. This issue is currently being hotly debated by the Federal Communications Commission.

However, the shape of the data communications "revenue pie" is changing dramatically. The change in the relative shape of the pie slices is primarily a result of technological changes. Clearly, AT&T does not want to participate solely in the transmission-services aspect of the business, given that segment's expected relative shrinkage to a 20% share of the 1985 market configuration.

The Changing Dollar Distribution in Data Communications



NSA Studies and Recommendations on Organization

I now want to outline the NSA studies that eventually led to the merger of C and T in the summer of 1977. I am sure you will agree it was not a hasty decision.

In March 1972 the Director, VADM Gaylor, directed that a study be conducted to examine the possibility of merging the Agency's ADP and telecommunications functions. An *ad hoc* committee, with membership from most of the key components, was appointed to conduct the study and was chaired by Mr. Neil Carson from PROD.

The Carson committee identified the following 12 problems in two categories -- *planning* and *operations* -- and, for each of them, attempted to answer the question: Would the merger of the ADP and telecommunications functions facilitate the solution of the problem?

Problem	*Would merger facilitate the solution?*
Planning:	
1. Difficulty in obtaining realistic, well-coordinated long-range requirements for telecommunications and ADP	Probably not. This is primarily a problem for P in developing requirements which encompass those of A, B, G, and W. There might be a slight advantage in having a single technical interface for C and T1.
2. Many requirements are *ad hoc*, necessitating quick reaction to a specific, unpredictable situation	Not directly. Combining functions could facilitate some.
3. Lack of integrated planning for ADP in the telecommunications area	Yes.
4. Omissions in plans	Yes, the merger would facilitate but not guarantee a solution to this problem.
5. Imbalances in programming for telecommunications vs. ADP and other CCP areas	Yes, although many other factors also influence the balance.

DOCID: 4009808

6. Complexity of external coordination and relationships in telecommunications planning, roles of DCA and the military services	No. On the contrary, the present status of T1 in the organizational structure makes it easier to deal with this complexity.
7. Incompatibilities between terminal equipment at field sites and internal NSA processing system	Possibly. But this is more related to other problems already mentioned. A strengthened role of a combined C and T1 would help some.
8. Lack of total systems automation for computer networks	Yes. The combination of ADP/COMM functions into one organization should accelerate developments in this and related fields.

Operations:

1. Coordination of telecommunications operations involving computers	Yes.
2. Trouble-shooting, i.e., the difficulty in determining whether a computer problem is due to computer hardware, executive software, lines terminal equipment, or worker software	Probably, in that there would be a greater probability that those involved would learn to speak the same language.
3. Time and red tape involved in accomplishing relatively simple operations, e. g. moving a computer terminal	Yes, potentially. Delay of work requests could be alleviated.
4. Lack of consistency in availability of C8 and T1 maintenance personnel	Yes. A single key element could more easily adjust resources to balance the situation

The Study Group attempted to anticipate major factors in the future and considered the following in some detail:

- Computer netting;
- Software conversion;
- Integration of ADP into analysis; and
- Dynamic resource allocation.

I shall not go into the details of their deliberation, but simply state their conclusion that combining C and T would alleviate these problems. Regardless of the organization, they saw a great need to have better definition of the interfaces between C, T, and SIGINT processing.

The majority of the Study Group concluded that most of the Agency's automatic data processing and telecommunications functions, especially the planning, software development, and maintenance, should be integrated. The Group believed that the two disciplines would rapidly merge into one as technology advanced in the 10 years following their 1972 study.

The Group also believed that the ADP component must become a central Agency utility of hardware, systems software, and data bases, with applications software increasingly the province of the user. Because of the complexities of the ADP effort and of the external relationship in the telecommunications area, the group considered it necessary to accomplish the merger in the following two stages:

- C Group to be removed from the Production organization, reorganized, and given a strengthened mission statement as the central NSA/CSS authority for automatic data processing systems. C and the P Staff, with a third party chairing the working group, to be charged with completing a plan for separation and reorganization within 6 months;
- While this action was under way, C and T1 to be charged with preparing a plan for merging the ADP and telecommunications functions. Such a plan to be completed within 12 months.

There were two minority views to this report (two of seven members, plus the chairman). One minority view agreed that an organizational merger could become the solution at some point in the future, but major surgery was not recommended at the time. What was recommended at the time was an exchange of skilled ADP and communications personnel.

The other minority view was that it had not been shown that the activities would be conducted better, that economies in dollars, space, or manpower would result, or that the efficiency of the Agency's operation would be significantly improved.

[redacted] USN, who had been chief of NSA Telecommunications for several years, studied the Carson report and commented, on 14 June 1972, that he believed "that the long-range trend is toward consolidation." He was very concerned that such a merger be done carefully. P.L. 86-36

Because the findings of the group were not conclusive, the Deputy Director reported to the Director on 24 May 1972, ". . .the group is now exploring alternative courses of action which might also achieve the objective of compatible system design without actual organizational merger."

DOCID: 4009808

The Ware Report (1973)

In 1965-1966 Dr. Willis Ware had been tasked by the Director, LTG Carter, with preparing a study of the Agency's computer center. The study was to review capabilities and capacity planning. In 1971 Admiral Gayler authorized a review of that earlier study, but asked that additional factors such as centralization and the advancement of communications be considered.

In May 1973 the second Ware Study Group published its report. That group, of course, had the Carson study as additional background. The only recommendation in the second Ware which bears on the present subject is:

> "Relocate the Agency computing facility organizationally so that it has high management visibility, is the property of the entire Agency and not only of the analytic groups, and is under the direct purview of the Director."

The rationale for that relocation was:

- It would give the Director better visibility of a resource that consumes a substantial fraction of the budget;
- It would give him a larger personnel base over which to exercise the man-machine trade-offs of operational costs;
- It would put the allocation of a scarce resource in view at Agency level, where things can be selectively controlled;
- It would be more responsive to the broad needs of the Agency; and
- Since computing and communications were becoming interrelated technogically, combining these two functions would be advantageous. Should this occur, it would be more appropriate for them to be an independent organization responsible to the Director.

The 1973 Ware report also recognized that not all computer-trained personnel should be located in one organization. The analytical groups -- A, B, G, V, and W -- undertake problem-solving efforts involving computers and should have "applications programmers" assigned. As you will recall, all applications programmers in C Group who were directly supporting one of the analytical elements were transferred out of C in July 1973.)

The OSD Audit of ADP (1975)

An OSD audit of NSA's ADP equipment maintenance, dated 7 July 1975, recommended consolidation of ADP equipment maintenance and supply support responsibilities in order to achieve cost savings.

The audit found that:

- Maintenance personnel trained to work on the same ADP equipment were assigned to various elements -- operations, R&E, and telecommunications;
- More control was needed over repair parts inventories;
- Improved procedures were needed to review and monitor contract maintenance support to ensure that contractors were satisfying contractual commitments.

The audit recommended that activities involving the maintenance of ADP equipment be consolidated under the management of C Group.

The Tordella Study (1976)

On 23 October 1975 the Director, LTG Allen, asked Dr. Tordella to look into the current functioning of T and of C. Dr. Tordella submitted his report on 15 March 1976. He recommended the establishment of a new Assistant Director for Communications and ADP. He considered it a sound solution and suggested that, if not implemented at that time, it would recommend itself at such time as any major reorganization of NSA could be accomplished.

He also expressed a major concern stated by DDO that removal of C from PROD would decrease the ADP responsiveness to DDO analysts. DDO argued, with great logic, that the reorganization proposal risked damage to the relationship between ADP and operations to achieve improvement in what could be the narrower relationship between ADP and communications. If the C/T organization were merged outside of DDO, the C experts could become more ingrown and systems-oriented and less responsive to DDO analyst needs.

Of course, one possibility was to merge C and T within DDO. TCOM had been in PROD, as I outlined earlier, but the thought of resubordinating TCOM to PROD was rejected because many of the goals of combining C and T would be negated. Dr. Tordella concluded that the *status quo* was clearly the least disruptive choice, but even if that were chosen in the short run, he recommended that a merger be planned for an early date.

As we know, the Director considered the matter for about a year and selected an appropriate time to direct the merger.

A Look at the Record

I have talked at some length now about the expected acceleration of the convergence of data processing and communications. Now I would like to look at the record of the past to see what has been happening here at NSA.

[redacted] I really hate to gloss over this period and the outstanding work that was done by the people in both the old C Group and TCOM. The advances during this period have been dramatic and have provided the technical base for the accelerated growth of the future.

P.L. 86-36

Improvements Expected from C/T Merger

During the several months of 1976 and 1977 that General Allen considered the relative merits of merging C and T into a single organization, his staff helped him develop a list of improvements to be expected from such a merger. Those expected improvements -- which really constitute the "bottom line" of the merger -- are:

- enhanced visibility of a more direct management focus on the Agency's computing resources;
- creation of a central point for long-range planning/systems development involving computers for communications and processing;
- greater effectiveness and efficiency in application and management of computing resources;
- consolidation of computer maintenance activities;
- central control of support planning for computer facilities;
- clearer definitions of interface between Agency customers (P, R, S, T, M, N, field, etc.) and supplier of computing services;
- possibility of development of standards across the board, rather than only within projects;
- centralization of control of policy and procedures for communication and computer systems/services;
- possibility of better career development.

"United We Stand"

In conclusion, all of us who work in the new T organization have a major challenge and responsibility. Communications and computer services have been fused into one and organizationally placed under a Deputy Director in an attempt to achieve the improvements I have just outlined. It is up to us as individual members to insure that it becomes a real fusion of the two types of services and the two technologies, not simply a combination of two things under a common management. There is a great reluctance for organizations to change. We must be especially attentive to the risk that the merger be only a half-one.

[redacted]

~~CONFIDENTIAL~~

THE HAND IS NOT QUICKER THAN THE EYE

Many years ago I was told that "a good analyst" does his own logging, counting, and tallying. While at first I admit I thought I was being set up to do all the menial labor (my son calls it "the donkey work"), it wasn't long before I saw that the senior people around me *did* do their own logs, and counts, and tallies -- not always, but much of the time.

I can remember more than one callsign problem when the callsigns had been extracted (by hand) from some sort of generating matrix and inscribed (again, by hand) into pages. Often the makers of the pages would begin in an attempt to be very "random" but boredom and inattentiveness quickly set in and both processes, extraction and inscription, slowly became more orderly and regular. Near the end, as fatigue set in, the processes became virtually mechanical. Such "handwriting" patterns -- top to bottom, left to right -- are sometimes so strong that one can convert pages from arbitrary to true base on this feature alone. On a problem like this, one can deal with the problem on a statistical basis -- one can even convince one's statistically/mathematically minded friends of the truth of one's solution -- but the acid test is to sit down with pencil and cross-section paper and, by hand, duplicate the process, callsign by callsign. If your solution is right, you'll see it and you'll *feel* it intuitively.

In both of these processes, we gain analytic insight by doing it ourselves. Logging brings us into contact -- a kind of slow-motion contact -- with the material we are studying. I don't know about you, but I know that I have *discovered* more things while logging, or counting, or tallying, or some other donkey work than I have while sitting there looking at the results of the logging/counting/tallying. Especially the discoveries that were unexpected -- outside the range of what I *thought* I was going to find. In the extraction/inscription kind of problem, the insight comes as my hand follows the hand of the enemy signal officer. Why did he stop just there? What made him jump over (or away from) that callsign?

Nowadays we are told that the computers are going to do all things for us. But what happens to that intimate contact with the material when the original traffic -- if you can call it that anymore -- is deep inside a computer somewhere and all you've got to look at is some computer output? Well, some of us still find a way to do some hand-logging. And not just because we can't get responsive software support (that's a subject for a separate article). We *want* to log! It helps us touch the material. It's like buying a piece of land and not being satisfied with topographic charts -- you have to go out and walk all over it. Then you begin to *know* the land.

I have always had the notion that someday interactive computers with *screens* might begin to meet this "touching" need of the analysts.

[redacted]

[redacted]

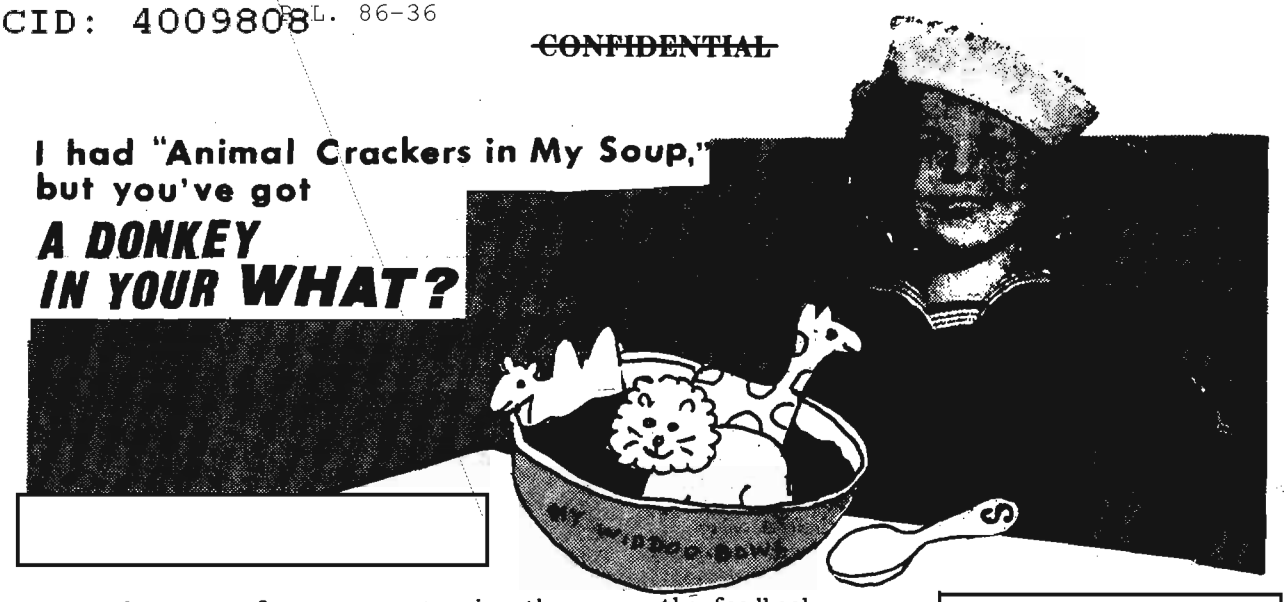
[redacted]

Has anybody done this sort of thing or ever seen it done? If it works, I'd sure like to stop all this logging!

[redacted]

DOCID: 4009808 P.L. 86-36

I had "Animal Crackers in My Soup," but you've got A DONKEY IN YOUR WHAT?



The group of mayors was touring the water quality-control facility at a municipal reservoir. Their tour guide, a young engineer, repeatedly extolled the virtues of the equipment they were about to see. They entered the operations room and beheld an entire wall of gauges, dials, lights, and buzzers, all sensing the pulse of the hundreds of acres of water outside the building. Fully a dozen technicians moved purposefully back and forth among the dials and gauges, stopping to record their readings on the forms attached to their clipboards.

"Gentlemen," intoned the proud tour guide, "this facility and its equipment represent the absolute state of the art in municipal water supply quality control. From this one room, staffed by only 12 men per shift, the health of over eight million people is guarded against disease. From here we monitor numerous hazards. We scan the salinity, the coliform level, and the chlorine concentration. We check for algae growth and a host of industrial contaminants and agricultural pollutants. To put it succinctly, we're on top of it."

Following a polite round of applause and a few parting oohs and aahs, the mayors headed back to their bus for the return to their hotel, convinced to a man that they would request funds for a similar facility in their next budget.

As they walked across the dam, they saw a sight that caused their jaws to drop. There, lying on the shore of the reservoir, half in and half out of the water, was the bloated carcass of a dead donkey. It had not affected the salinity; nor had it made any contribution to the algae concentration; and so, it had gone undetected despite "the absolute state of the art" in sophisticated equipment.

The story, of course, is apocryphal, but it illustrates a lesson which, while always important, becomes increasingly so in the age of computers and staff meetings.

A host of "bugs" raise their ugly little heads when machine processing intervenes in the feedback process.

All over this agency are managers who scan performance-oriented printouts with a frequency ranging from daily to monthly. They rely heavily on the reports they review to give them what they need in order to fulfill their role. Many will not discover, until a "dead donkey" of some sort shows up in their shop, that statistics, as useful as they can be, are not meant to be the end-all. Their purpose is to indicate, hint, or suggest that a problem *might* exist. They may highlight a known problem or aid a manager in distinguishing between a symptom and an underlying cause. At that point the computerized report has done as much as it can ever do.

The other pitfall comes about when an individual rises within an organization to the level at which the role is to manage *managers* (as opposed to a first-line supervisor, who manages the people who actually perform the tasks). Meeting with subordinates then becomes the primary mechanism through which the manager acquires data on the system for which he is responsible.

Heaven help the manager whose knowledge of his organization is limited to that provided in staff meetings by subordinates who, in turn, rely too heavily on statistics. That constitutes double jeopardy.

The cure for "managerial myopia" is prevention. For every half-hour spent reviewing statistics, a like period should be devoted to visiting part or all of your empire. It prevents "dead donkeys" in your reservoir.

EO 1.4.(c)
P.L. 86-36

DOCID: 4009808

P.L. 86-36

A LINGUIST LOOKS AT THE "TUBE"

THE TUBE IS COMING

Computer systems which use video, or CRT (cathode ray tube), terminals distributed to work areas are on the increase at NSA, and we linguists can take heart that the "tube," plus a good text manipulation system, can be an ideal tool for the translator.

THE TUBE AND THE NEWS MEDIA

The fact that video terminals are widely employed by the news media is evidence of their usefulness to those whose job is writing. The major wire services and, according to the NEW YORK TIMES, more than 300 newspapers have installed computer systems which permit reporters to type their stories on the screens of CRT terminals, then move their drafts to other terminals for editing, proofreading, and computerized layout and typesetting. As long ago as 1970, UPI let a contract for such a system, and in 1971 AP reporters were already writing stories on the screens of a trial system.

This item from a recent issue of U.S. NEWS AND WORLD REPORT tells of that publication's system:

> "Instead of a typewriter, the editors use a video-display terminal, or VDT. It is simply a keyboard attached to a television screen. Letters appear on the screen when the keys are struck. A computer to which the set is connected allows writers to drop words with the push of a button, or insert full sentences without retyping old copy. Entire paragraphs can be transposed by striking other keys. This saves time spent erasing, striking over, shuffling paper and typing clean drafts.
>
> "The VDT was viewed with skepticism by many newsmen steeped in traditions of a business that has used typewriters for generations. 'It seemed like a hell of a lot of trouble to go to to write a story,' says Associate Editor Frank Diggs. 'But you get hooked to the point that you come in in the morning with a smile on your face to sit down with it.'"

A more detailed description of a typical text-oriented terminal comes from this COMPUTERWORLD news item:

> "Designed exclusively for ,organizations like newspapers, publishing houses and other communications firms, the [Delta 4300] terminal provides text manipulation features that include automatic word wrap, automatic ragged right sentence and paragraph justification and automatic justification of new insertions, the firm said.
>
> "In addition, four automatic search modes are possible including searching text for a specific word or word string; search and replace each occurrence in text with a new word or word string; search and replace upon request; and search and delete each occurrence in text of a specific word or word string.
>
> "Other features include the ability to move/copy/delete any defined text from the terminal's memory."

The similarity between news media operations and NSA translating and reporting makes us ask whether we Agency linguists might profit from the use of technology which the news industry finds so effective. Businesses also are stepping up use of computerized "word processing" equipment, including video screens, to produce letters and documents.

THE TUBE AND TRANSLATION

We can never translate at computer speed, but a computerized tool which removes our dependence on paper can make us much more productive. Surely everyone who has worked at translating a foreign language has felt frustration at the slowness inherent in the conversion of foreign words to an English translation on paper. A typewriter may be a little better than longhand for some linguists, but the medium is still paper, where small corrections are time-consuming and revisions require recopying by the translator or someone else.

The feature of the video terminal which I find most attractive is the worksheet nature of the screen. I can type as fast as possible, knowing that any correction, insertion, or deletion can be made instantaneously. I can transpose whole sentences in a moment -- a marvellous time-saver when sentences in the

DOCID: 4009808
EO 1.4.(c)

original text are long and convoluted. After I have made all needed changes, my draft is actually the finished copy. In a total system, a button push would flash my translation to the terminal of the checker and then to the releaser. I could print a copy for local reference if needed. An EXPERT data form could be displayed on the screen, and data elements not recoverable automatically from an associated data base could be entered quickly.

From my experimentation with a CRT terminal for translating texts for product, I estimate that I at least double the productivity of the time I devote directly to translating. The amount of time saved will of course vary by person, language, and subject matter, but any linguist should expect to make his valuable language skills more effective.

Although it is the experienced linguist who will profit most from the use of a video terminal, the work of the less experienced will also be speeded up. The worksheet nature of the display screen makes alterations easy for him or the reviewer without the need for retyping.

If a translator uses a dictation system, [redacted] the transcriber will be the one who uses the video terminal, with the same advantages of rapid correction and revision and the capability to transmit completed texts for checking and disposition at a button push.

There are, to be sure, conditions for the success of a translator's video terminal system. The first is up to the linguist, and the rest are the responsibility of management:

1. The linguist must be able to type. This is not an unreasonable requirement in a high-technology agency. A typing course is available in the learning center for any who need it.

2. There must be a terminal at the linguist's desk and a printer nearby.

3. Text manipulation on the screen must be flexible and fast.

4. The system must be dependable. Nothing will discourage the linguists's use of the terminal more than a few lost translations.

5. The lighting and physical arrangement of the terminal must be suitable for constant use.

THE TUBE AND A TOTAL SYSTEM

Although my immediate purpose here has been to extol the value of the CRT terminal to the translator, the total benefit of an on-line, intercept-to-product system should be kept in view.

We should not only help the translator to be more productive, we should capture the first key stroke of his translation on the computer terminal and pass it on electronically to the end user without copying from paper. Record copies on paper undoubtedly will be wanted at some points in the flow, but paper must not be the medium of transmission. Time and money are wasted, and errors introduced, by the retyping required in the present process.

In G Group, for example, [redacted] If a text editing system is then available on those terminals and there is a direct connection to NSA's product release and distribution system, the translator will be able to perform his work as an integral part of an overall system.

[redacted]

Segments of the total system principle are already in use or on the way, but they are limited either to a part of the Agency or to a part of the process. To make the [redacted] concept a reality, we await a total on-line system, hopefully one with text-handling features which will allow us who are linguists to be as productive as technology will allow.

EO 1.4.(c)
P.L. 86-36

THE TUBE AND THE TRANSLATOR -- "I DO"

Both linguists and managers have a part in arranging the marriage of the translator and the video terminal. We who translate must be willing to accept and master the use of tools which will make our language knowledge more valuable to the Agency. For its part, management must ensure that new on-line systems have flexible, fast text-handling capabilities plus suitable physical environment and that the translator's role is not merely an afterthought. Agency efforts to recruit and keep good linguists should be matched by the determination that they will have modern equipment for their part in SIGINT production.

(This article was typed and revised on the screen of a computerized word processing system. It was produced in the form of a single column to fit the CRYPTOLOG format. With the exception of the human labor involved in cutting and pasting these columns onto the page masters, the article was "untouched by human hands.")

~~(TSC)~~

LETTERS

To the Editor, CRYPTOLOG:

As a twenty-six-plus-year veteran of NSA and its predecessor, AFSA, I just cannot resist commenting on the article "How Not to Make an OB" (CRYPTOLOG, December 1977). Although I have never been a traffic analyst or special research analyst, I am nonetheless motivated to make the following comments.

The intent of the article is obvious, i. e., to hopefully eradicate to some degree the lethargy that may have crept into some of our analysts' daily work habits. I hope that the article is a gross exaggeration; however, I have made the assumption that occurrences similar to the one pantomimed in the article have taken place at NSA with sufficient frequency to prompt the writing of this article. I am appalled at the very thought. If this assumption is correct, we are indeed in a sorry state. Can someone allay my fears and reassure me that we are more professional in these endeavors?

P.S. If some of our consumers read this article, what would be their thinking in terms of the validity of our product?

[redacted] K31

The author of the article replies:

As a twenty-*seven*-plus-year veteran of NSA and its predecessor, I can assure [redacted] that the article was based on a real-life incident. It was slightly exaggerated and the names were changed to protect the guilty.

However, [redacted] fears may be allayed somewhat by the following facts:

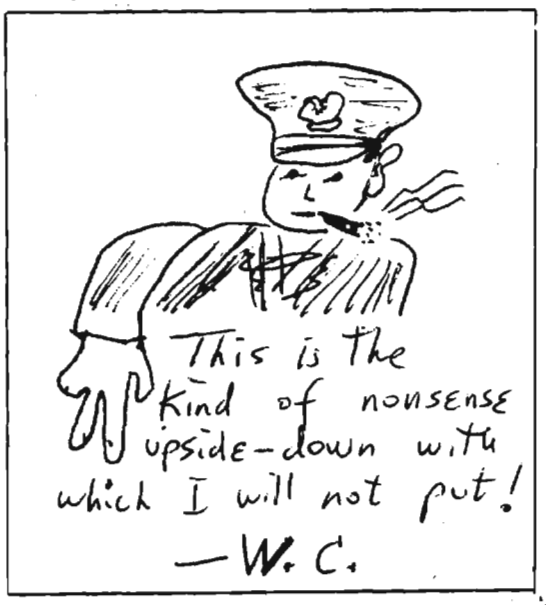
1) The incident happened many years ago -- about 15, as a I recall -- and most of the people involved are no longer involved in Agency reporting.
2) All the sloppy practices described did not involve the listing of just one "Obscenian" officer. The story was a composite with many mistakes being thrown into one OB entry. It's the sort of thing they do on TV when they want to show mismanagement in hospitals. Rather than clutter up the story with a whole lot of characters, they come up with one patient who is suffering from high blood pressure, low blood pressure, prostate trouble, pregnancy complications, chills, fever, and a few other symptoms.
3) The OB in question did not get issued, thanks to the efforts of the checker (but my natural modesty prevents me from telling you who he was).

[redacted] P16 P.L. 86-36

(U)

Editor's note:

The following communication, attached to the article "No, Winnie, You've Got It Upside-Down Too!" (CRYPTOLOG, February 1978), appeared recently on the Editor's desk:



(U)

P.L. 86-36

DOCID: 4009808

The Editor's' Page

AN IDEA FOR AN ARTICLE

Doris E. Miller, P16 (RETIRED)

I had to move the apostrophe this month because we're printing something sent in from retirement paradise by our founding editor, Doris E. Miller.

From time to time we send Doris unclassified clippings from CRYPTOLOG, just to let her see how her baby is getting along. Sometimes it's only the picture on the title page of the article, plus the author's name. But occasionally we can send Doris a treat -- a completely unclassified item.

Recently our clippings to Doris included the unclassified letter to the editor that was sent in by [redacted] *and was printed in the January 1978 issue. It prompted Doris to send me the following letter, with a suggestion for a definitive article (How's this for proof that you can take the girl out of the Agency, but you can't take the Agency out of the girl?). I'm too busy editoring to take her up on her suggestion. Instead, I'll just print her letter here and hope that some CRYPTOLOG reader will seize the opportunity. In a way, I feel like Mikey's brothers, pushing the new cereal back and forth, each saying, "No, you try it!" Won't I be pleasantly surprised when someone really "LIKES it!" and does something about it. (Assuming, of course, that the person sends it in to CRYPTOLOG for publication!)*

Ed.

[redacted] letter about the relationship between TA and IRA (CRYPTOLOG, January 1978) reminds me of an article I once started to write, called "What Is a Cryptolinguist?" It was in the months just before I retired and I had so many passionate thoughts I wanted to put on paper about the work of the cryptolinguist, and so little time to do it, and I would write at home, far, far into the night, using substitute words and leaving spaces, etc., trying to get it down in shape so that I could work it up finally at the building. Well, it was not to be. I piled up an enormous amount of stuff, some of it very good, I thought, on the whole concept, techniques, philosophy, and ethics of "special intelligence" -- trying to fight through the wilderness we have got lost in and get back to some kind of common sense approach to the work. I had something like 50 pages in varying degrees of eloquence and incoherence when D-Day Eve came around and I simply had to scrap it.

One part of it, though, that I regret not having passed on to you, or somebody, retraced the evolution of the cryptolinguist, that is, our present conception of him (in which I include her, who they mostly is) using as indicators of the various stages the different job titles.

When I came into the Agency you were either a CA or a TA. I was quite astonished at being dubbed a cryptanalyst on the strength of a couple of Dilly's courses, but soon learned that at that time, because the nature of the systems being used, the linguist either picked up some CA or the CA picked up some language: the real distinction was whether you worked with the message externals or internals. Then the systems became more and more mathematical and the solutions more and more independent of linguistic aid; also, when some of the big, big systems broke, lots of linguists were brought in, as a second wave, so to speak, who had no part in breaking them, and they just "exploited" them. Then the Agency began reporting its own scoops, and the linguist became a research analyst. Then the research analysis was separated out (how do you like that for redundancy?) and the linguist became just plain linguists, except that that didn't seem quite right, either, so they became cryptolinguists. (I still remember the State Department interpreter who was so amused at that word -- "cryptolinguist." "What is a cryptolinguist? Is it something like a pseudoliberal?")

P.L. 86-36

So the chronological sequence went something like: Cryptanalyst, Cryptanalyst F/L, Research Analyst F/L, Linguist or Cryptolinguist. This is a steady diminution of the role of the linguist, who is now considered to be neither a cryptologist nor an intelligence analyst, but a kind of simulated translation machine.

P.L. 86-36

This shows a frightening lack of comprehension as to what the linguist actually does, how much nonlinguistic work he does, how much is left to his judgment and discretion that never comes to the attention of other "disciplines" (because the linguist makes the live-or-die decision in his scanning) or is slanted by the linguist's rendition of it, of which the SRA is frequently unable to make an independent judgment. . . Well, here I go again.

I think Agency linguists have made a mistake in emphasizing the intricacies and difficulties of the *languages* (who cares?) and not bringing out the tremendous power the

linguist has in the early (and sometimes the late) stages of processing -- power which is sometimes put into the hands of people who are totally unprepared for it.

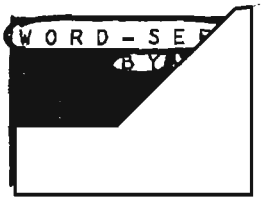
Linguists should emphasize their role in producing *intelligence*, not their virtuosity at one -- or 21 -- languages. If they would present it from that angle, which is the only one that butters any parsnips for the Agency, anyway, they might get a better hearing.

Be that as it may, it might make an interesting article. No, I'm sure it would! It might be possible to write -- or get someone to write -- a historical account of the process by which the originally simple dichotomy (always wanted to use that word) of "CA and TA" has been elaborated into our present jungle of specialties.

Where one would find the material, I don't know. Job auditors? People's own personnel files? Position papers?

Wayne's remarks are very much along my line of thinking. He could probably produce a large chunk of such an article. If the idea appeals to you, you can take it from there.

(U)



[redacted] A254 asks you to find the World War II phonetic alphabet in the Word-Seek below. (*Solution next month.*)

O	H	C	E	R	N	W	O	H	E	M
E	O	E	L	B	A	G	N	I	K	A
M	T	R	C	E	N	G	T	E	I	I
O	E	O	N	Q	V	E	U	F	M	L
R	L	P	U	I	M	O	E	S	O	L
I	X	E	C	H	A	R	L	I	E	I
P	E	T	E	R	A	G	O	D	R	W
N	O	I	S	T	R	E	K	A	B	Q
R	E	G	O	R	B	K	Y	S	A	E
A	I	X	O	F	E	O	B	O	E	N
J	A	P	A	P	Z	Y	A	R	X	K

(U)

SLOW NEWS DAY IN MOSCOW

For the past 60 years, foreign correspondents have always had a dispatch that they could count on whenever there wasn't really anything to report, or whenever it was too cold to go out and take a picture of the old peasant women sweeping up the streets. The dispatch deals with "English words in Russian." The latest in this genre filled a whole column in a recent *New York Times*. The following snippets give you the general idea.

By CRAIG R. WHITNEY
Special to The New York Times

MOSCOW, Sept. 26—The Soviet Union may have resisted ideological contamination from the West so far, but its leaders apparently fear that the Russian language is not doing so well.

There has been so much linguistic "infiltratsiya," according to the cultural editor of the official Soviet youth daily Komsomolskaya Pravda, that the richness of Russian speech is in danger of giving way to facelessness and "standartizatsiya."

"Lenin said that we mar the Russian language by using foreign words unnecessarily," Vladimir V. Vasilyev wrote in a recent issue of the paper. "Isn't it high time to declare war on the torture of Russian tongue?"

they have been for centuries, Russ are fascinated by countries beyond borders, yet at the same time y suspicious and distrustful of all influences—including linguistic

yet "sportsmen" play pretty for "khokkei" these days, maybe be their goalkipers are so good. At bas too, their dribbling is remarkable. uropean futbol (soccer) they have en relegated to outsider the world chemnionat, situatsiya has become kriticho

SEPT. 27, '77

(Slow day in CRYPTOLOG art department: Ever notice how, whenever there's an odd space to fill, it's always a news clipping on Russian?)

(U)

Answer to puzzle

(See CRYPTOLOG, February 1978)

The problem was to think of what solid figure (not a squeezable material) could be passed through each of the holes (a circle 2" in diameter, a 2" square, and a triangle with a 2" base and 2" height). At each pass-through, it was to make a completely contiguous fit.

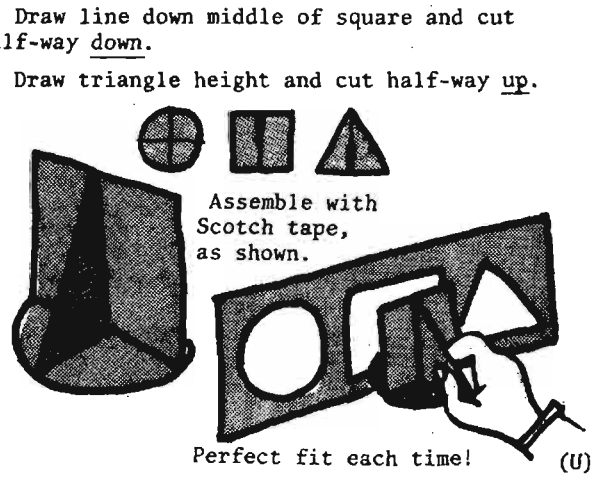
Here's the solution:

Cut the appropriate circle, square, and triangle out of light cardboard.

Draw perpendicular diameters on the circle.

Draw line down middle of square and cut half-way down.

Draw triangle height and cut half-way up.



Assemble with Scotch tape, as shown.

Perfect fit each time!

(U)

DOCID: 4009808

NSA-crostic No. 12

By A.J.S.

The quotation on the next page was taken from the published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS — *WORDS*

A. Kind of English earthenware (mantlepiece spaniels, etc.) — 31 120 81 65 5 73 46 113 181 27 136 100 39

B. Head of a monastery — 174 76 53 210 44

C. Songwriter's summary of "Hamlet": "When a ghost and a prince meet, And everyone ends as ----------." — 188 118 43 131 58 233 14 205 167

D. When her three boys bought a cattle ranch, she suggested they name it "Focus," because that's where the ---------- (3 wds) — 69 1 137 184 164 49 192 161 9 226 45 85 107

E. What Sir Francis Drake was looking for (2 wds) — 66 94 196 105 173 146 51 15 212 40 89 195 235 111 29 182

F. Affirmative (colloq) — 208 123 32

G. Vessel abandoned on the high seas — 203 149 180 129 36 108 59 6

H. Spin — 204 193 187 12 114 62 30

I. Attempt to vomit — 74 133 16 169 156

J. When told that this was a person's favorite phonograph record, the other person said, "Oh, I didn't know that Ol' Blue Eyes had such a fancy first name!" (3 wds) — 23 33 78 189 41 154 90 170 2 177 144 86 64 186 127 216 119

K. Vegetable — 153 110 143 54 134

L. Person in charge of entertainment (3 wds) — 102 10 141 229 179 213 150 158 17 138 175 199 50 220 38 147 194 47

M. Lastest period of the Tertiary (2 wds) — 71 83 28 232 209 3 95 63 34 98 18 219 191

N. Not torn asunder — 70 115 22 37 122 103 211

O. South American lake, highest in the world; fifth-grade geography teachers hate to mention it because the rest of the class hour is nothing but giggles and smirks — 82 116 91 13 190 60 215 165

P. Ancient sculptures taken from Athens to England in 1806; now in British Museum (the Greeks want 'em back!) (2 wds) — 139 92 224 121 151 19 77 11 125 142 96 67

Q. Vegetable melange — 231 223 178 214 117 4 55 185 171 207 84

R. Wild goat of Europe and Asia

159 57 217 97

S. Refusal

130 109 228 25 48 166 8 88 87 106 218 172 197

T. One helluva good poet (2 wds)

35 236 112 162 145 176 26 200 135 7 168 227 206

42

U. Large indeterminate number

221 20 163 75 202 79 104

V. Fiddle-maker

124 155 222 52 80 101 201 68 160 24 61 148

W. Make lukewarm

56 99 72 225 230 126

X. Last nine years (1811-1820) of the reign of George III

140 157 128 152 234 198 93

Y. Oriental monetary unit

132 21 183

1 D	2 J	3 M		4 Q	5 A		6 G	7 T	8 S		9 D	10 L	11 P	12 H	13 O
14 C	15 E	16 I		17 L	18 M	19 P	20 U	21 Y	22 N	23 J	24 V	25 S	26 T		27 A
28 M	29 E	30 H	—	31 A	32 F	33 J	34 M	35 T		36 G	37 N	38 L	39 A		40 E
41 J	42 T	43 C	44 B	45 D	46 A	47 L		48 S	49 D	50 L	51 E		52 V	53 B	54 K
55 Q	56 W		57 R	58 C	59 G	60 O	61 V	62 H	63 M		64 J	65 A		66 E	67 P
68 V		69 D	70 N	71 M	72 W	73 A	74 I	75 U		76 B	77 P	78 J	79 U	80 V	
81 A	82 O		83 M	84 Q	85 D	86 J	87 S		88 S	89 E	90 J	91 O	92 P	93 X	
94 E	95 M		96 P	97 R	98 M	99 W	100 A	101 V	102 L	103 N	104 U	105 E	106 S	107 D	108 G
109 S	110 K		111 E	112 T	113 A		114 H	115 N	116 O	117 Q	118 C	119 J	120 A	121 P	122 N
123 F	124 V		125 P	126 W		127J	128 X	129 G	130 S	131 C	132 Y		133 I	134 K	135 T
136 A	137 D	138 L	139 P	140 X	141 L		142 P	143 K	144 J	145 T	146 E	147 L	148 V	149 G	
150 L	151 P	152 X		153 K	154 J		155 V	156 I	157 X		158 L	159 R	160 V	161 D	162 T
	163 U	164 D	165 O	166 S	167 C	168 T	169 I	170 J	171 Q		172 S	173 E	174 B	175 L	176 T
177 J	178 Q	179 L	180 G	—	181 A	182 E	183 Y	184 D	185 Q	186 J	187 H		188 C	189 J	190 O
191 M	192 D	193 H	194 L	195 E		196 E	197 S	198 X	199 L	200 T	201 V	202 U	203 G		204 H
205 C	206 T	207 Q	208 F		209 M	210 B	211 N	212 E	213 L	214 Q	215 O	216 J		217 R	218 S
219 M	220 L	221 U	222 V	223 Q	224 P	225 W	226 D	227 T	228 S	229 L		230 W	231 Q	232 M	233 C
	234 X	235 E	236 T												A.J.S.

(Solution next month.)

DOCID: 4009808

News of the Crypto-Linguistic Association

☑ Yes

☐ No

Yes, Jack Gurin, R5, is obviously the winner in CLA's informal "Think of the Longest Title for Your CLA Lecture, Just So Long as You Give the Lecture!" contest. The title is:

"I Was Just a Middle-Aged Polyglot Until I Discovered Transformational Grammar: Or, A Layman!s Guide to the Mysteries of Linguistics."

Time and place: Wednesday, 22 March 1978
0930 hours, Friedman Auditorium

All are welcome! (U)

News of the Communications Analysis Association

☐ Yes

☑ No

No, you don't *have* to be a member of CAA, but it makes it easier for you to get the word.

Like, did you get to hear [redacted] briefing on that [redacted] system, how they got into the solution, and what great things the solution has done for the problem? You say you didn't get the word?

How about the CAA's Special Interest Group on Cryptologic History? Does that tickle your fancy? Are you an older hand who just wants to get it all down on paper and set the record straight? Have you just read *The ULTRA Secret* and are you just burning to write a classified rebuttal to appear in CRYPTOLOG? Or are you one of the younger ones who's tired of hearing about the "good old days" and who wants to go look for yourself at what *really* happened? Well, the meetings of the Special Interest Group are open to everyone, but. . .

Maybe you've heard a rumor that the CAA is working on a proposal for a Communications Analyst, but you're having trouble tracking down who, when, where, so you can go and give them your two cents' worth.

Or you might have an idea for a different kind of Special Interest Group, but you don't know who to see or how to get it started. If it crosses skill/discipline lines (and don't they all anymore?), maybe you're thinking about asking the CAA for help, but you never seem to know who we are, which of us is interested in what, and where we hang our hats.

Yes, Penelope, there *is* a CAA and it has a lot of things going on -- all aimed at promoting growth and professionalism among communications analysts. But the reason you're not hearing about these things until too late is that you're not on our mailing list. And the reason for *that* is, you haven't joined. And if you have been sitting there smiling, saying, "I'm OK, I'm already a member!", you better check your membership card. If it says "1977," then I'm talking to you too. EO 1.4.(c) P.L. 86-36

Wait a minute! What does *my* card say? Hmmm! Can somebody lend me a dollar?

W.E.S. ~~(SC)~~ P.L. 86-36

Communications Analysis Association:

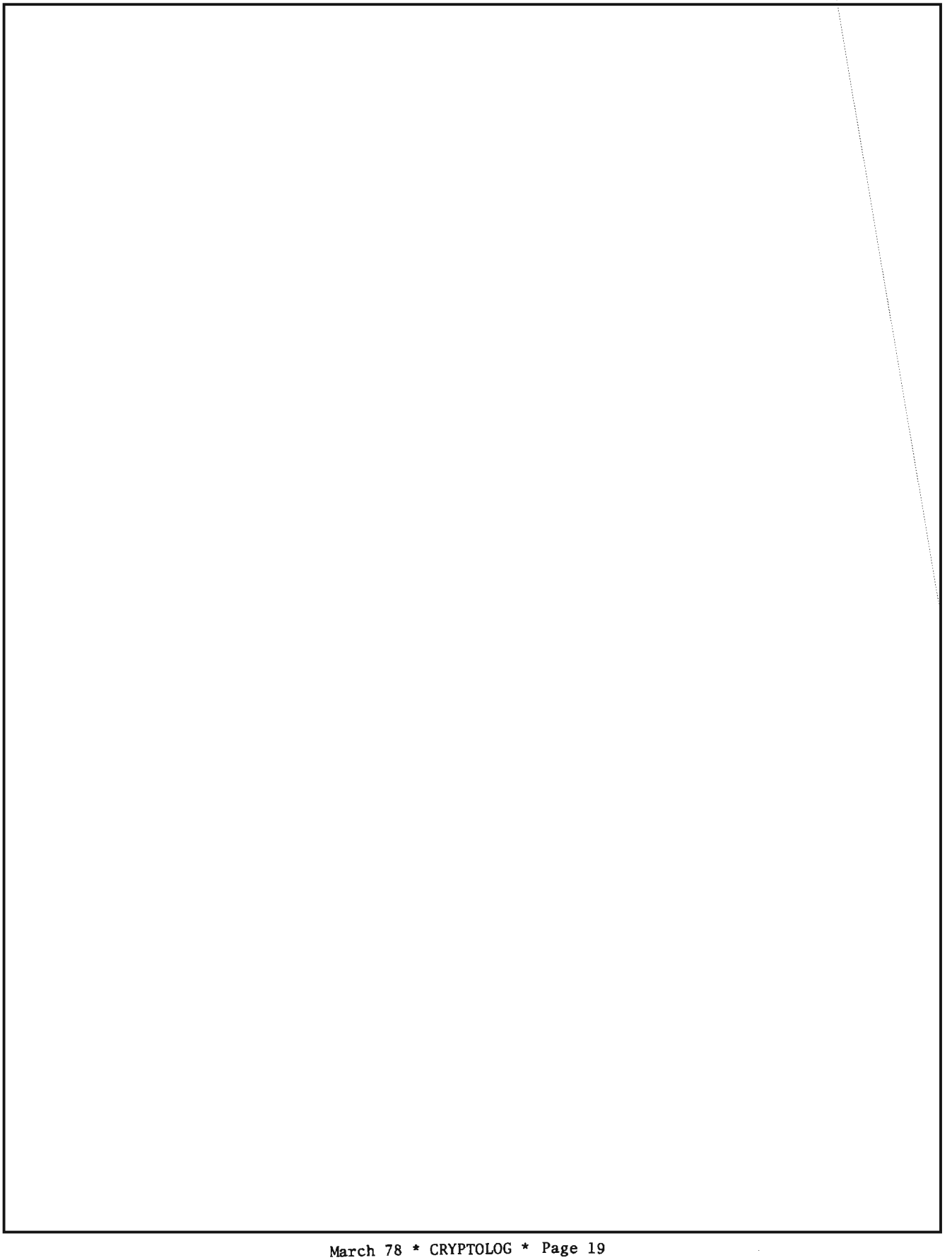
David Gaddy, President	3247s
[redacted]	1139s
Timothy Murphy	3791s
[redacted]	8025s
	5991s
	3573s
	3369s
	3500s

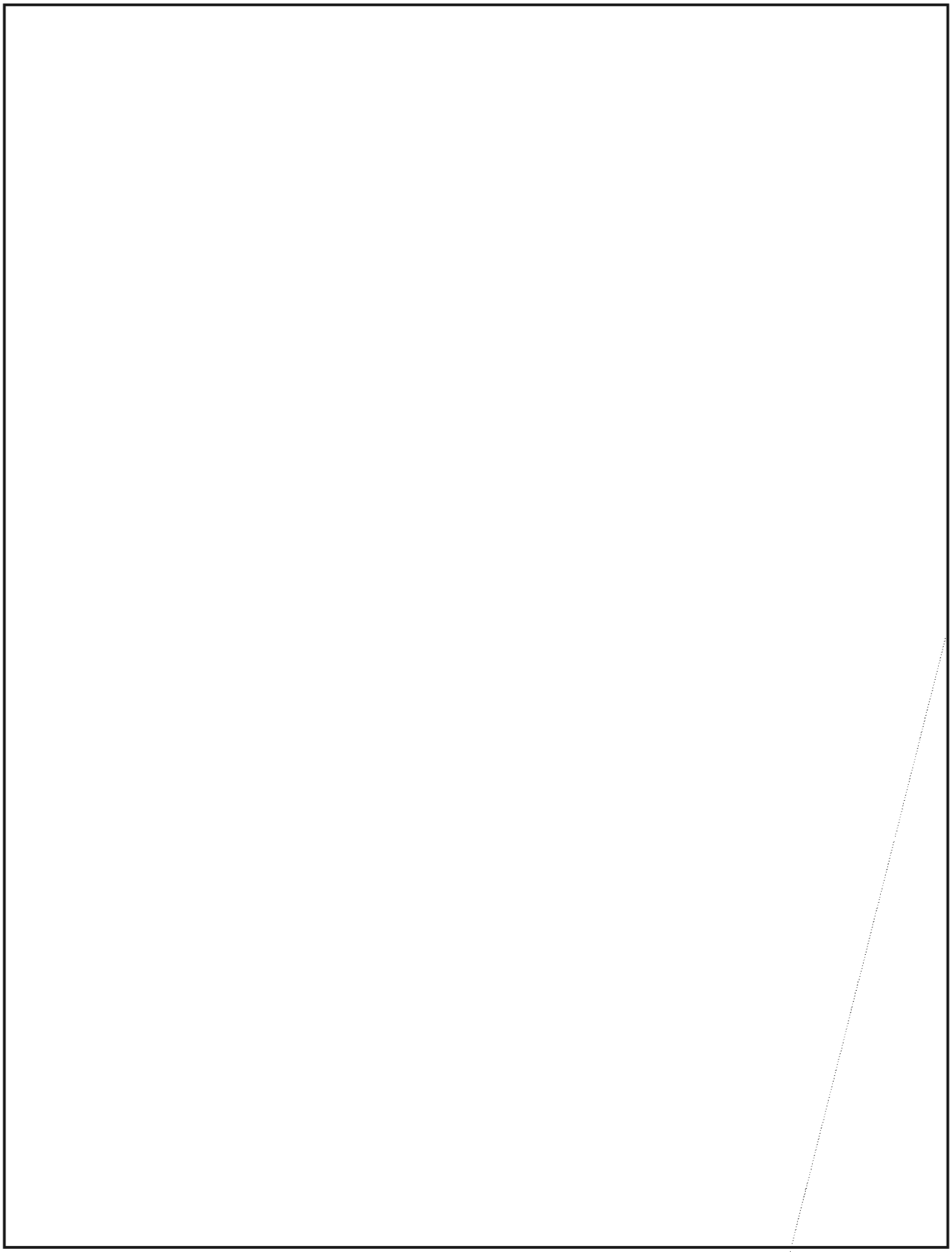
[1]Appointed to serve for the remainder of the term of [redacted] USN, who has resigned as Board Member.
[2]New appointment (U)

✱ Space reserved for CAA logo (see CRYPTOLOG, January 1978, p. 7)

P.L. 86-36
EO 1.4.(c)

~~SECRET SPOKE~~

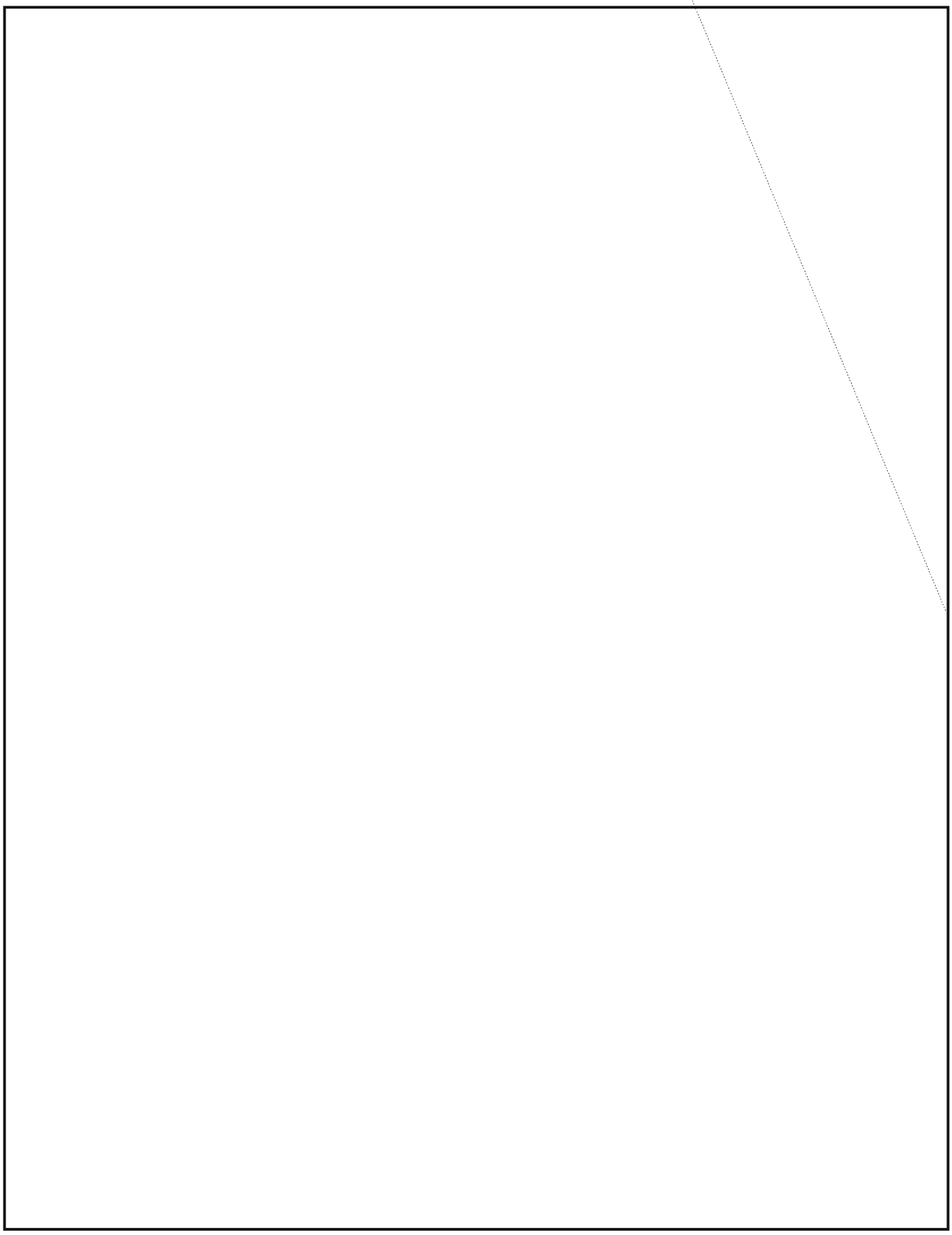




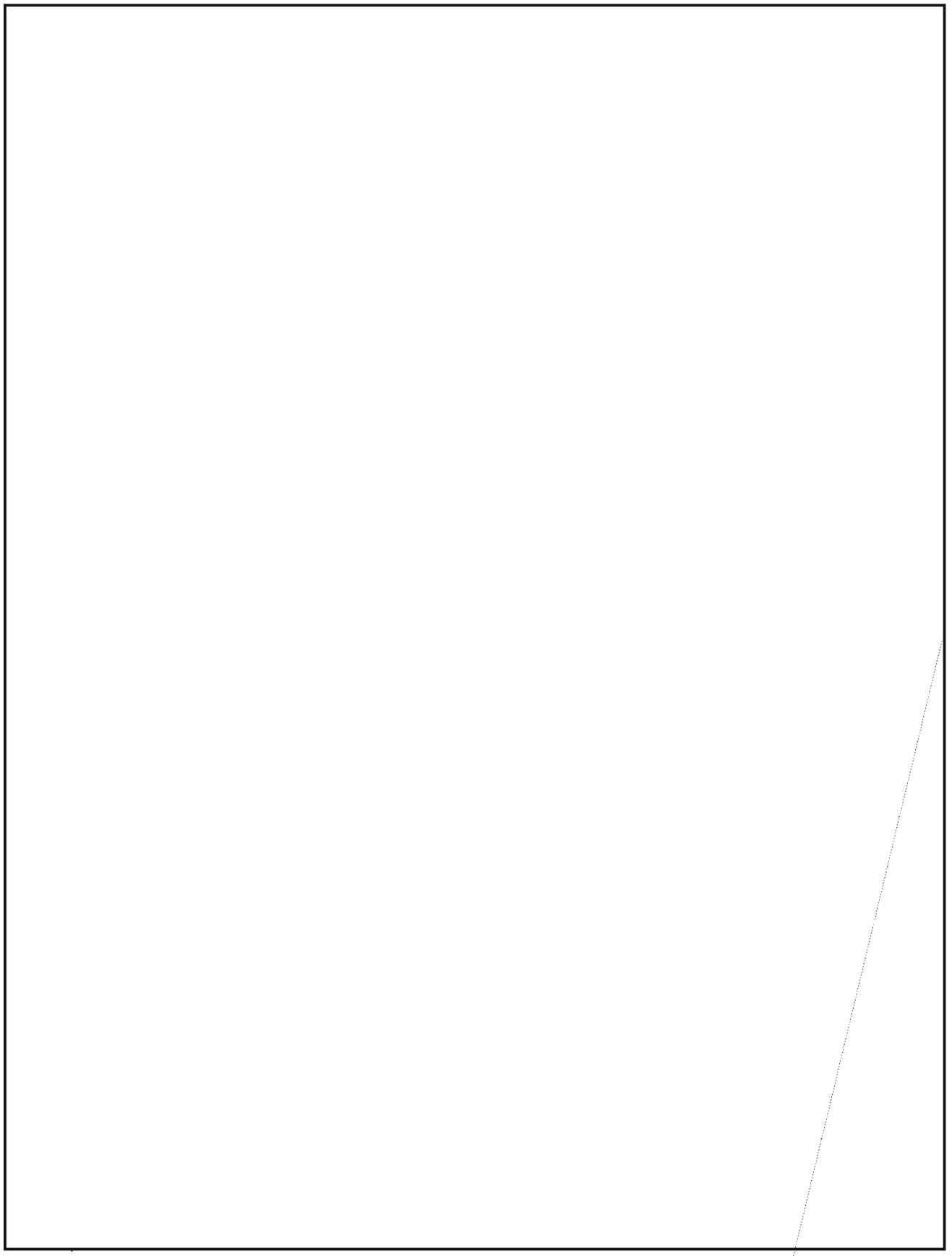
EO 1.4.(c)
P.L. 86-36

DOCID: 4009808

EO 1.4.(c)
P.L. 86-36



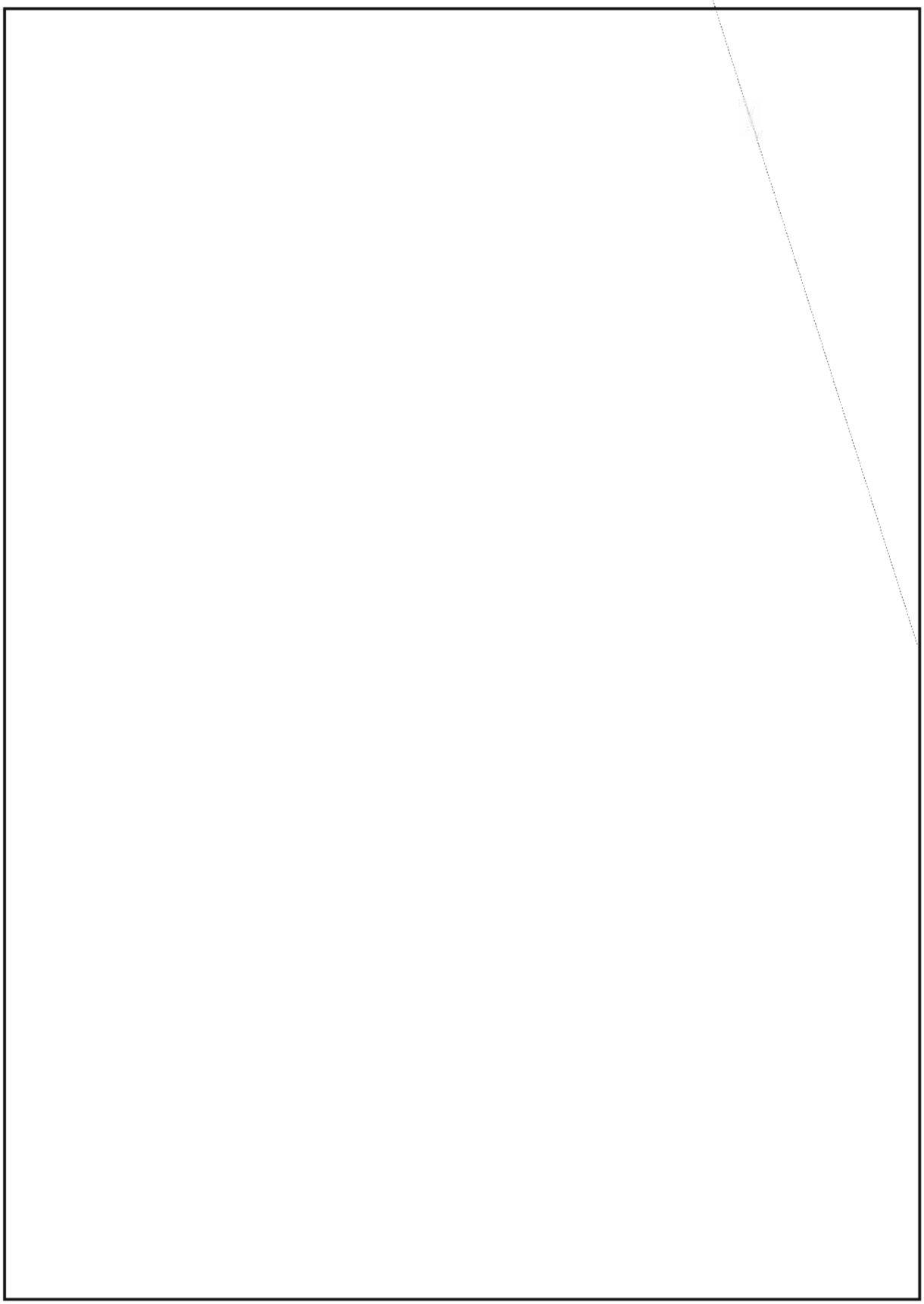
DOCID: 4009808



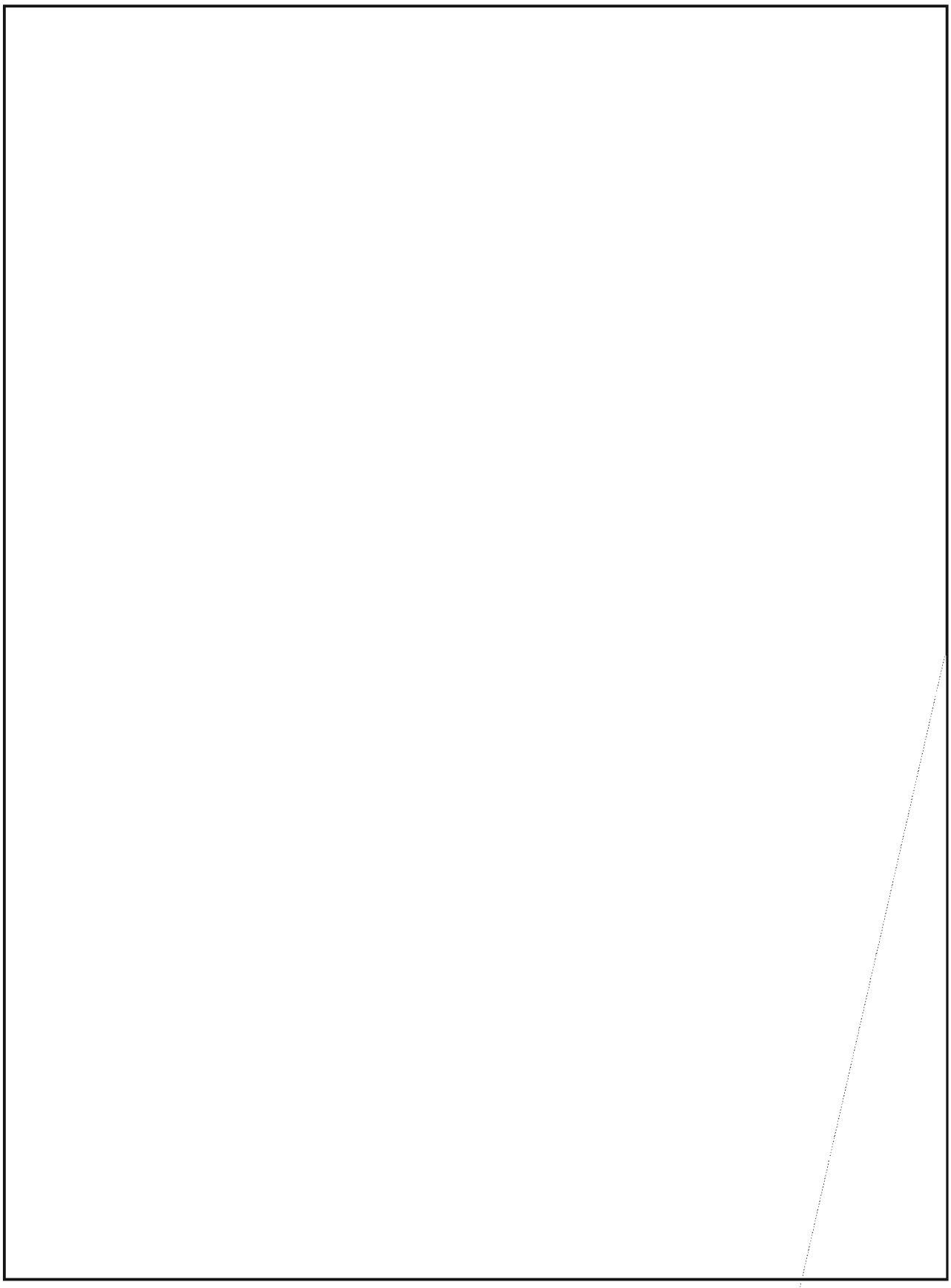
EO 1.4.(c)
P.L. 86-36

DOCID: 4009808

EO 1.4.(c)
P.L. 86-36



~~SECRET SPOKE~~

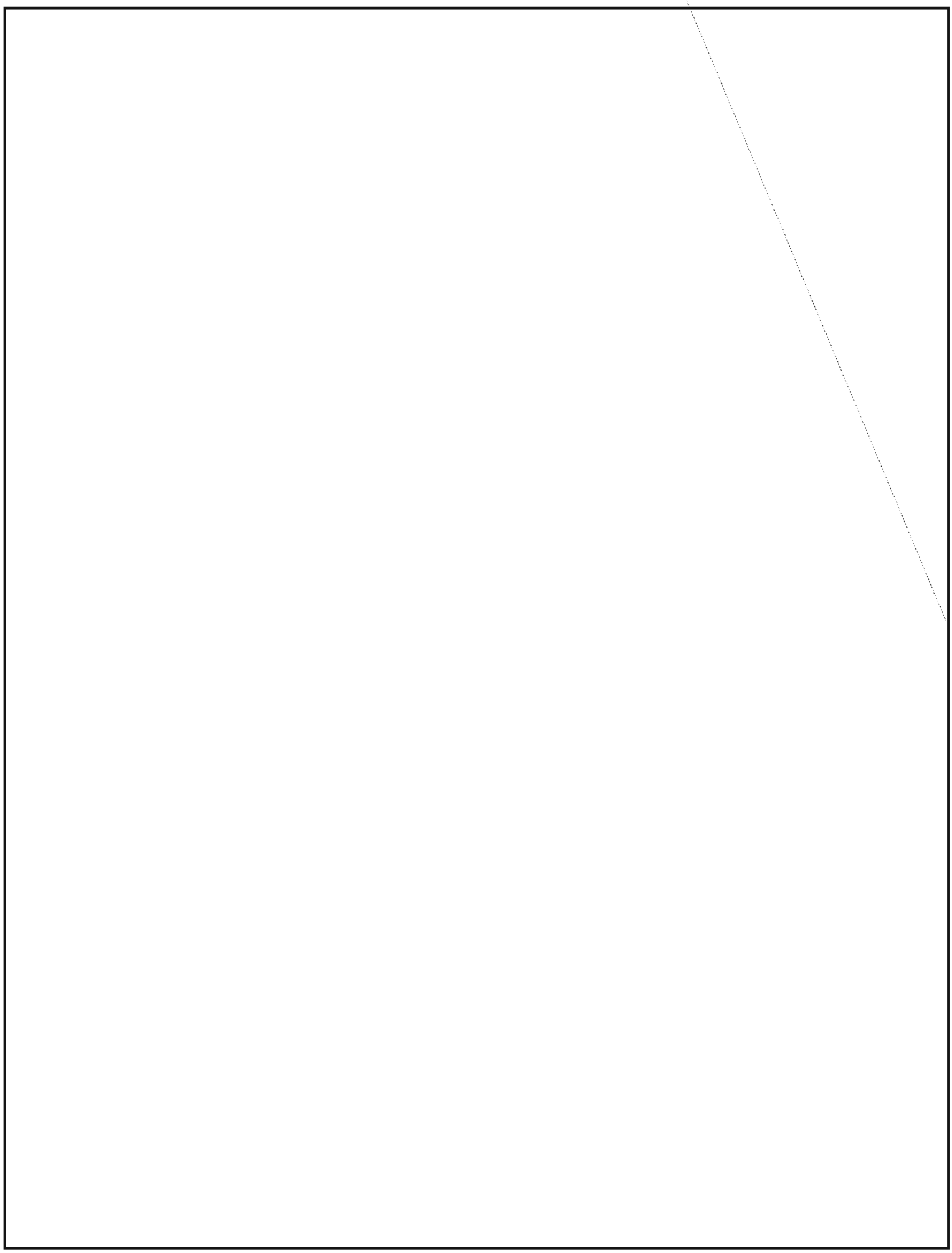


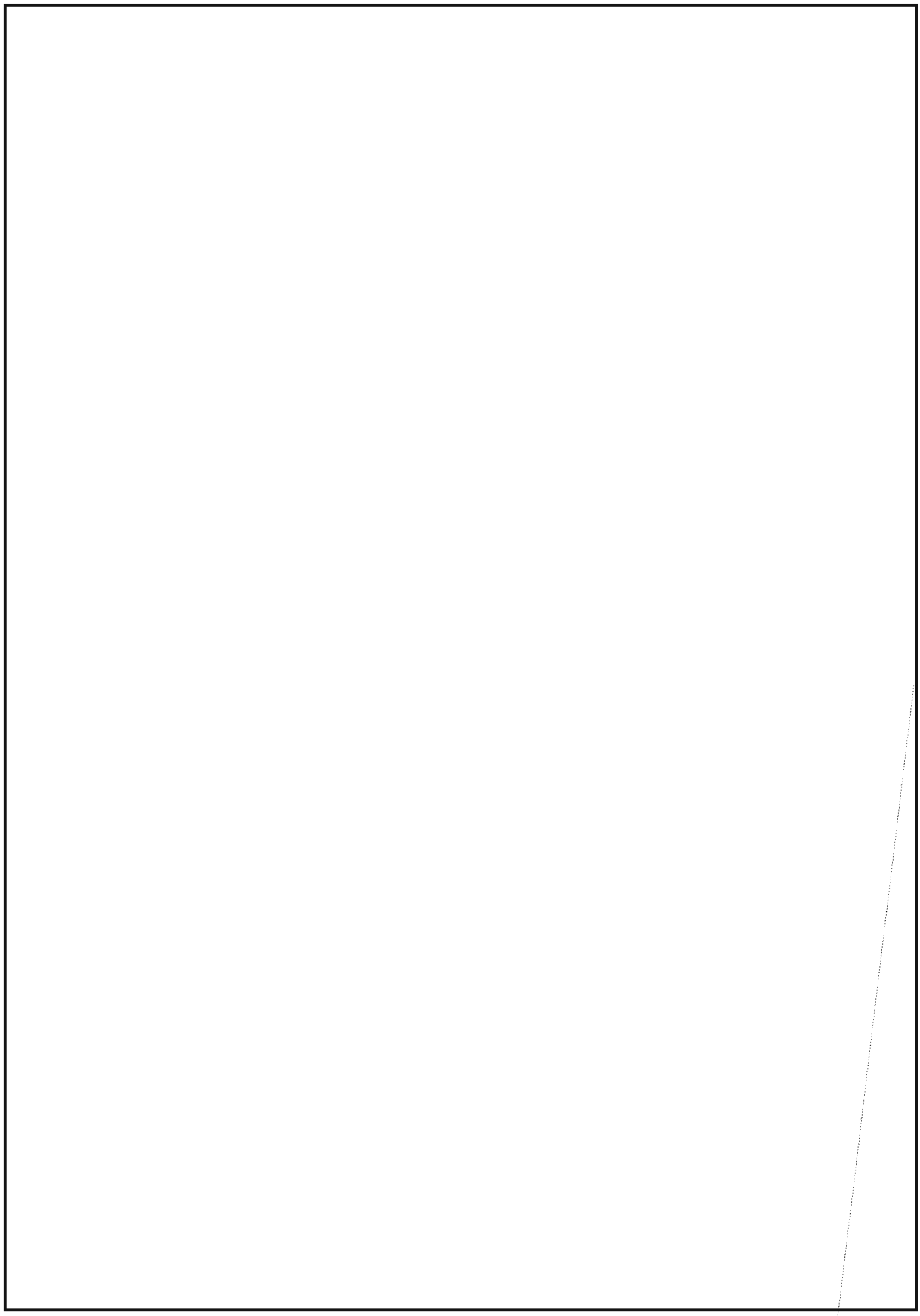
~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36

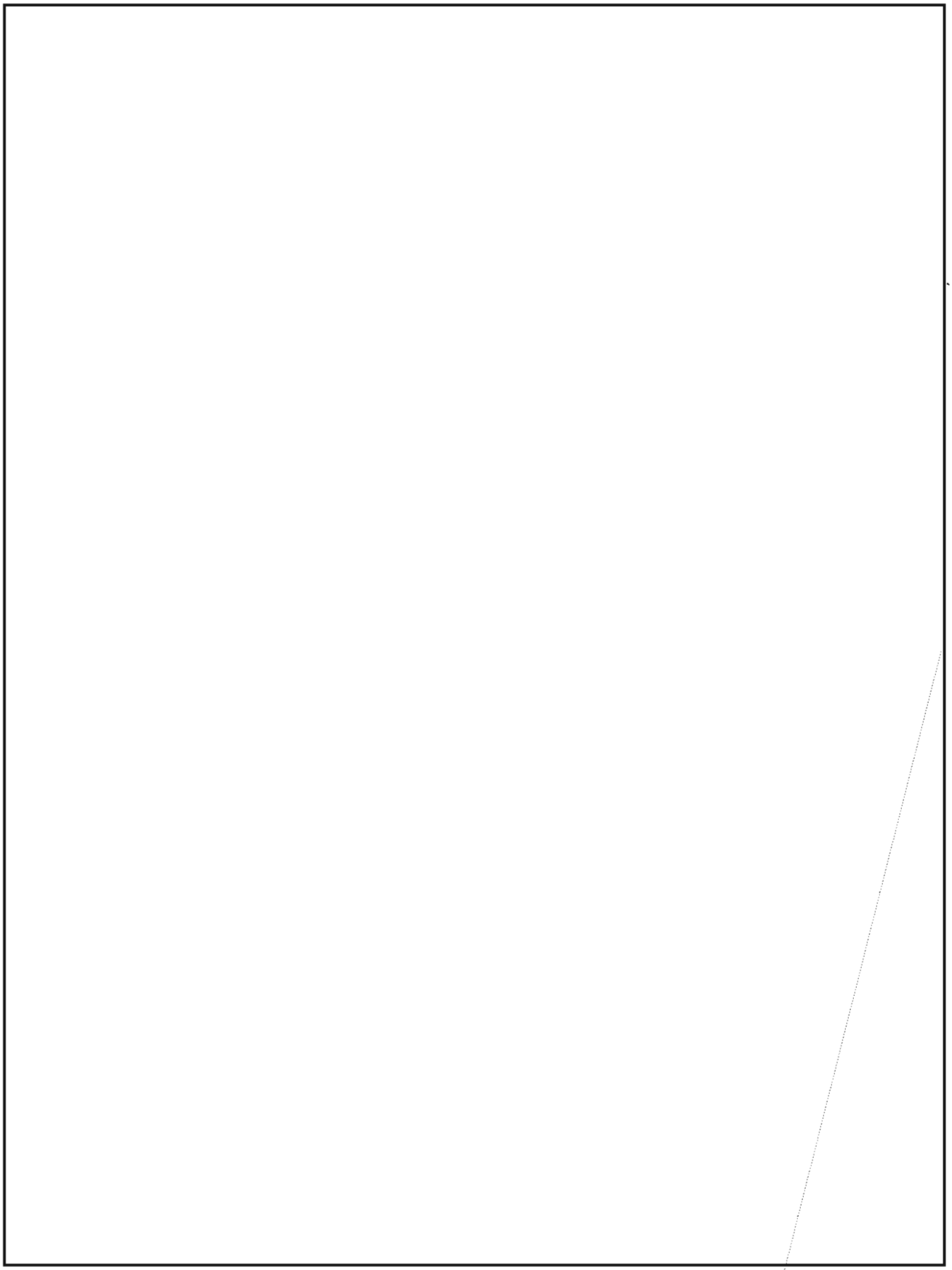
DOCID: 4009808

EO 1.4.(c)
P.L. 86-36



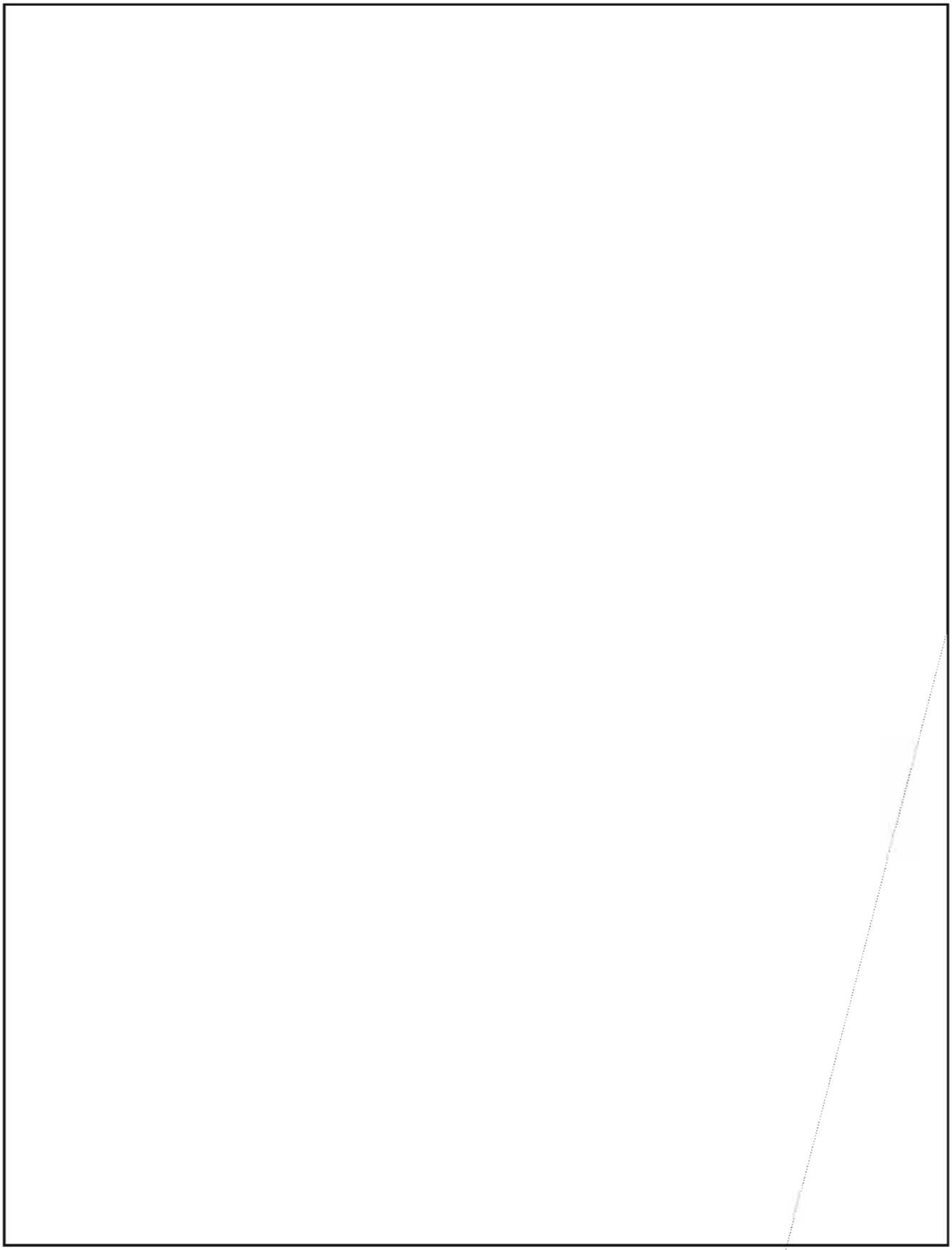


EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

DOCID: 4009808



EO 1.4.(c)
P.L. 86-36

~~(SC)~~

A PROPOSED CURE FOR THE "PERFORMANCE SYNDROME"

The following is submitted in rebuttal to [redacted] article, "A Proposed Cure for the Time-in-Grade Syndrome" (CRYPTOLOG, November 1977). To paraphrase the article, [redacted] suggested that too much attention is paid to an employee's time in grade, that the primary factors for promotion should be performance and capability to perform at the next level (potential), and that, to offset charges of discrimination, promotion boards should not be given employee's names, but only arbitrary numbers. He further suggested that jobs not be limited to certain grades, but geared to performance/potential.

Well, I find [redacted] article a mixture of fact and fancy. The fact part is based on his own experiences and the fancy is based on what sounds like extracts from a book on labor relations. It has been my own experience that each manager has his own pet criteria for promotions. If he has had to wait a long time for a promotion, he probably favors time in grade. If he has gotten his promotions fairly fast, he probably favors performance. If he has been held up for a promotion because of professionalization, he probably thinks the program is a waste of time. If his boss doesn't believe in giving outstandings, he probably doesn't want performance to count too much. If his boss has a forceful personality and likes him, he probably does want performance to count. If he doesn't have a degree himself, he probably has a low opinion of the value of a college education. People with several degrees are sometimes called "professional students"; people with several professionalizations are often referred to as "jack of all trades"; people with a lot of experience in several areas must always reestablish themselves in each new area.

The reason so many views are possible is that NSA does not have a definitive (prioritized and objective) set of criteria for promotions. Without such objectively measurable criteria, "performance" has often become a personality contest, a case of who-you-know, who-you-like, and not a real test of a person's productivity. Time-in-grade advocates are that way only because the performance advocates have abused the system.

Finally, it may surprise [redacted] to know I fully accept his "cure" for the time-in-grade syndrome; it is the same cure that is needed for the current performance syndrome. That is, I fully accept promotion boards being required to judge a candidate on the basis of the records and not on how well they personally know the person or how forceful their supervisor is, compared to others present. It may also surprise [redacted] when he finds most of the objectors to this plan are performance advocates.

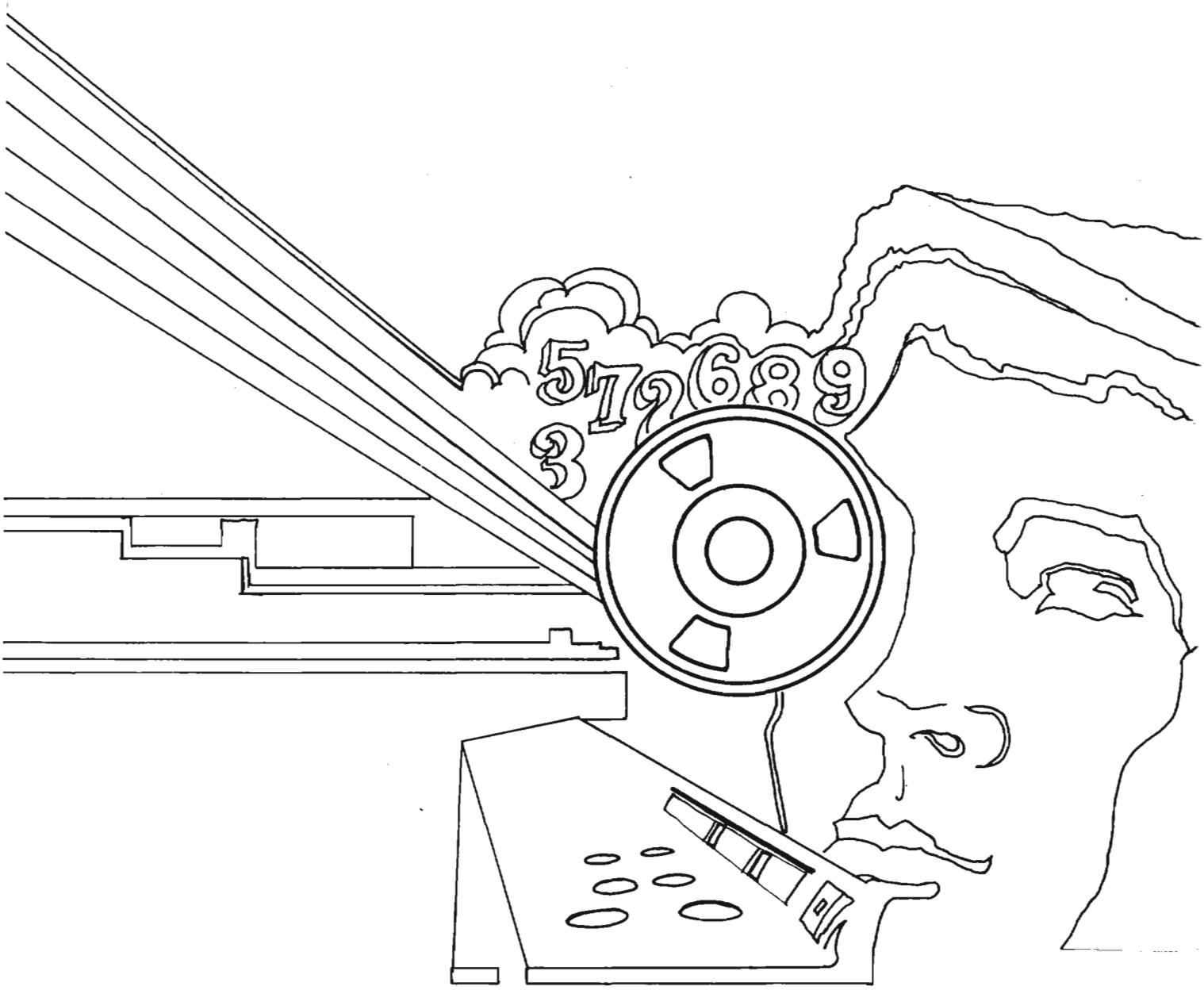
P.L. 86-36

By the way. . . Hi, George! This is

[redacted]

G943

(U)


5726893

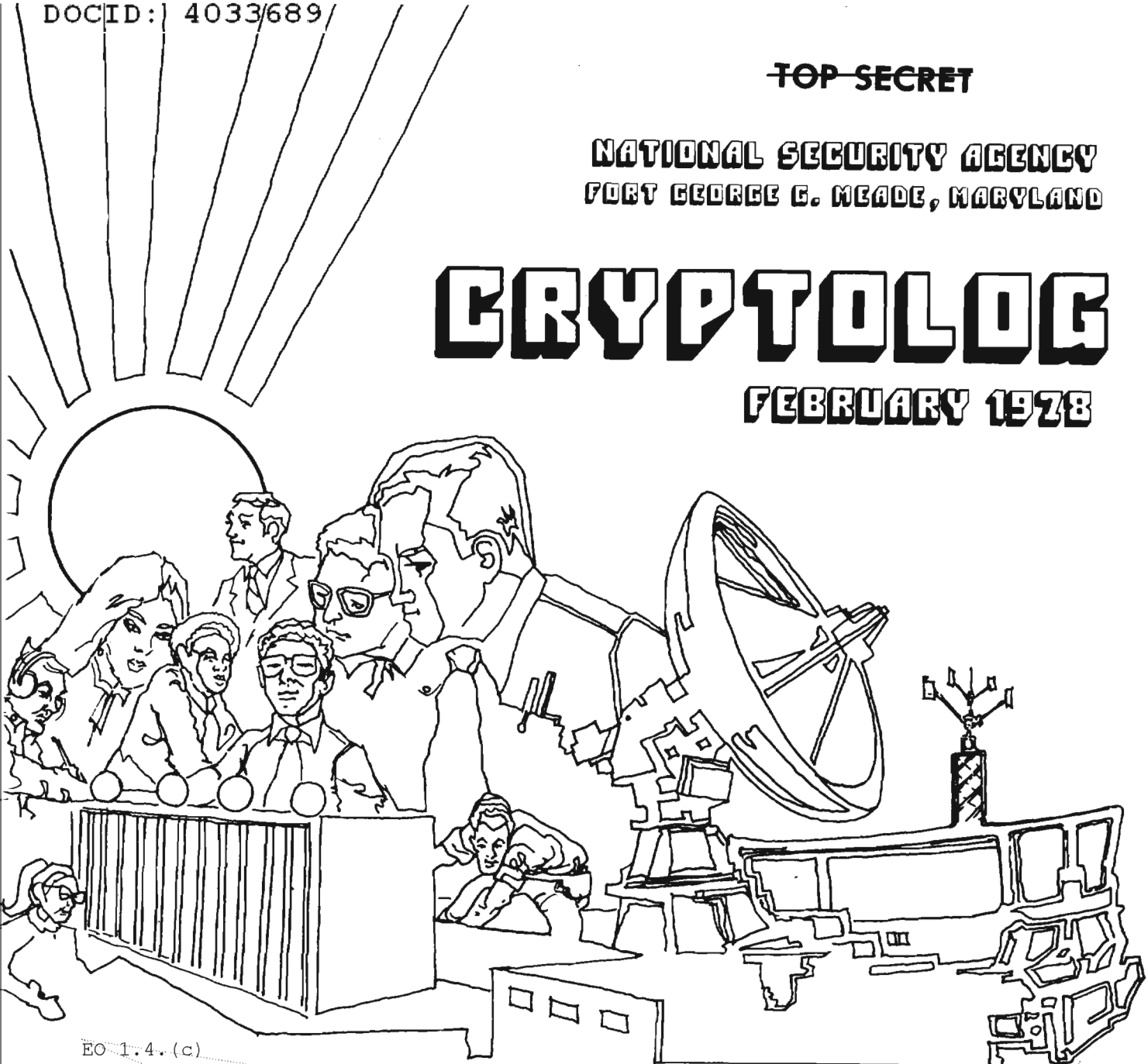
DOCID: 4033689

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

FEBRUARY 1978



EO 1.4.(c)

P.L. 86-36

[redacted] . [redacted] 1
COLLECTION-SUPPORT T.A. IS NOT FOR EVERYONE [redacted] 7
UNSEEN GO-BETWEEN: CONFERENCE INTERPRETER...J. Gurin.....9
[redacted] ..... [redacted] ...11
FIRST LADY OF NAVAL CRYPTOLOGY..... [redacted] ...14
C.A.A. NEWS.....14
MILITARY CRYPTOLOGIC SUPERVISORS COURSE.... [redacted] ..15
MORE BEANS.....Vera Ruth Filby.....17
BY-LINES DON'T COST -- THEY PAY!.....John J. Mollick.....19
"NO, WINNIE, YOU'VE GOT IT UPSIDE-DOWN!"....A.J.S.....20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4033689

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. V, NO. 2 FEBRUARY 1978

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5236s)

Collection..... [redacted] (8955s) P.L. 86-36

Cryptanalysis..... [redacted] (4902s)

Language..... [redacted] (5236s)

Machine Support..... [redacted] (5303s)

Mathematics.....Reed Dawson (3957s)

Special Research.....Vera Filby (7119s)

Traffic Analysis..... [redacted] (4477s)

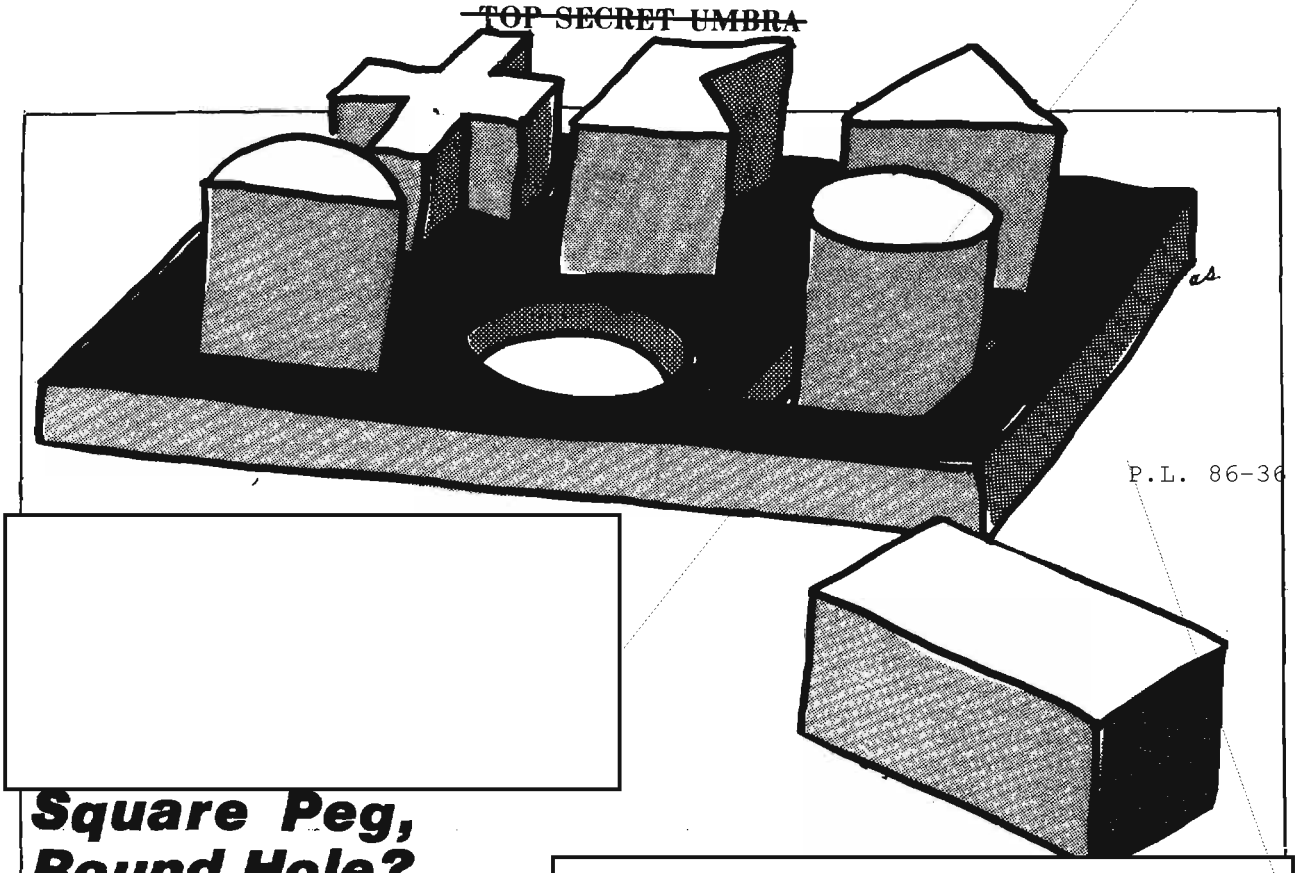
Production Manager.....Harry Goff (4998s)

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4033689

EO 1.4.(c)
P.L. 86-36

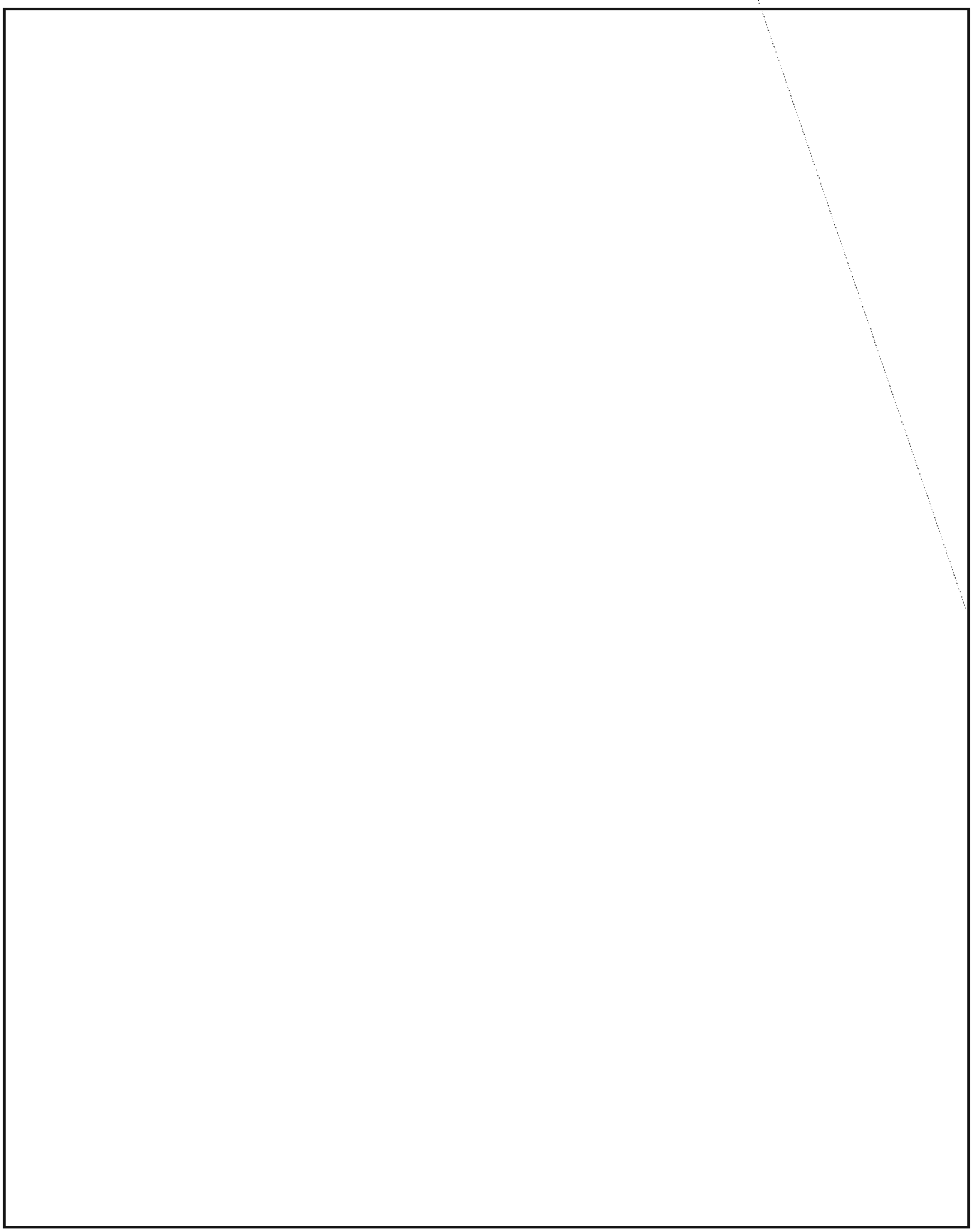


P.L. 86-36

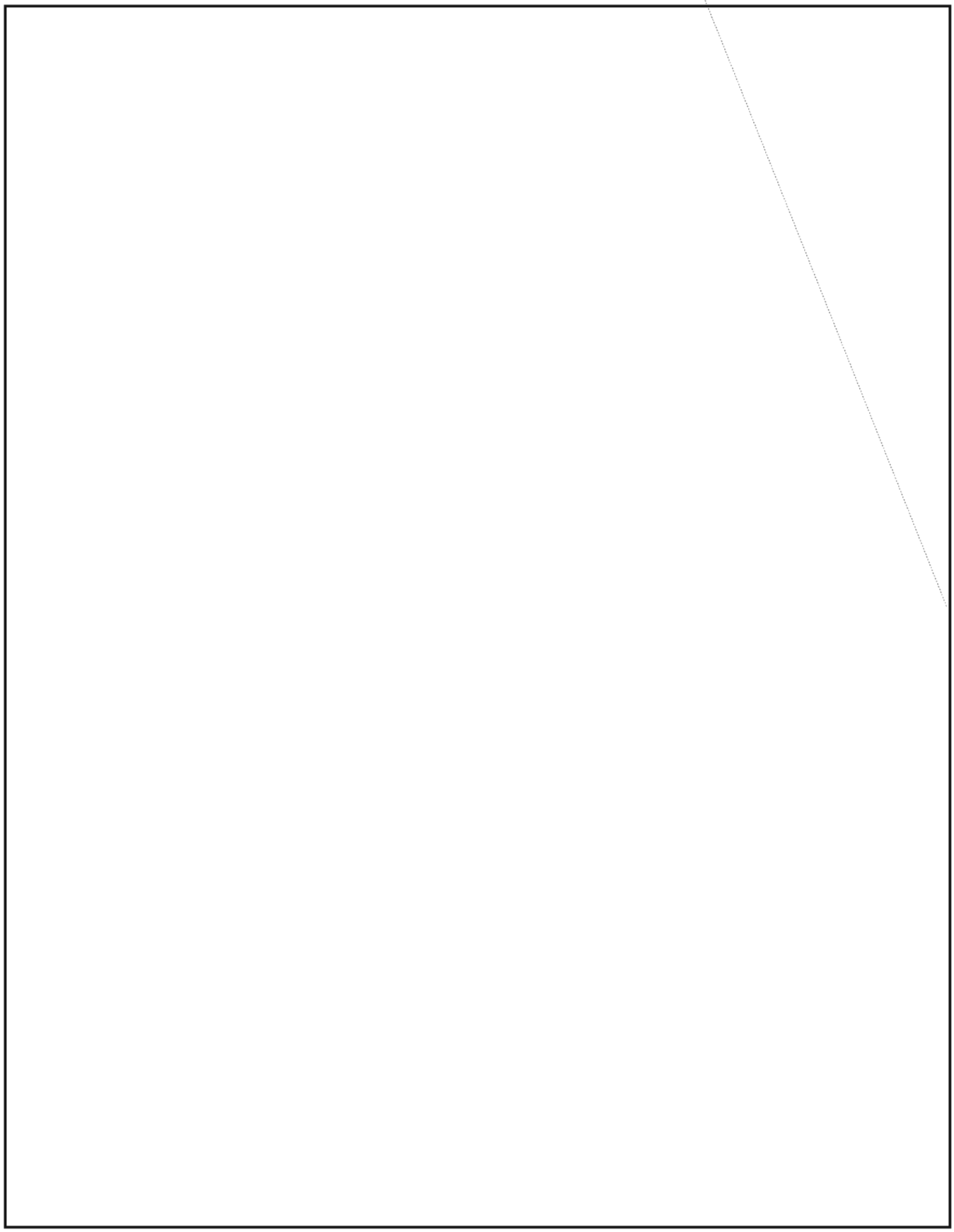
Square Peg, Round Hole?

EO 1.4.(c)
P.L. 86-36

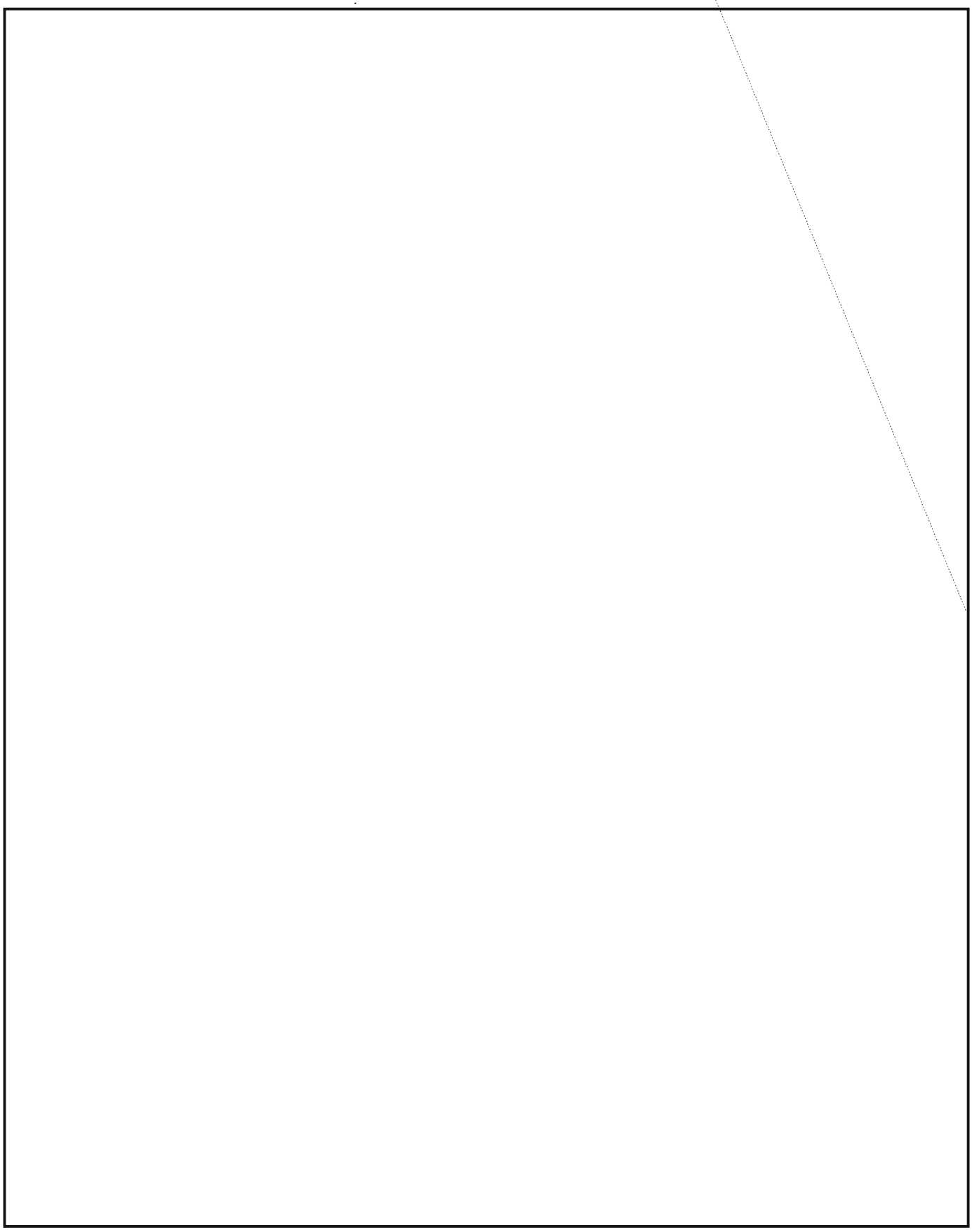
EO 1.4.(c)
P.L. 86-36



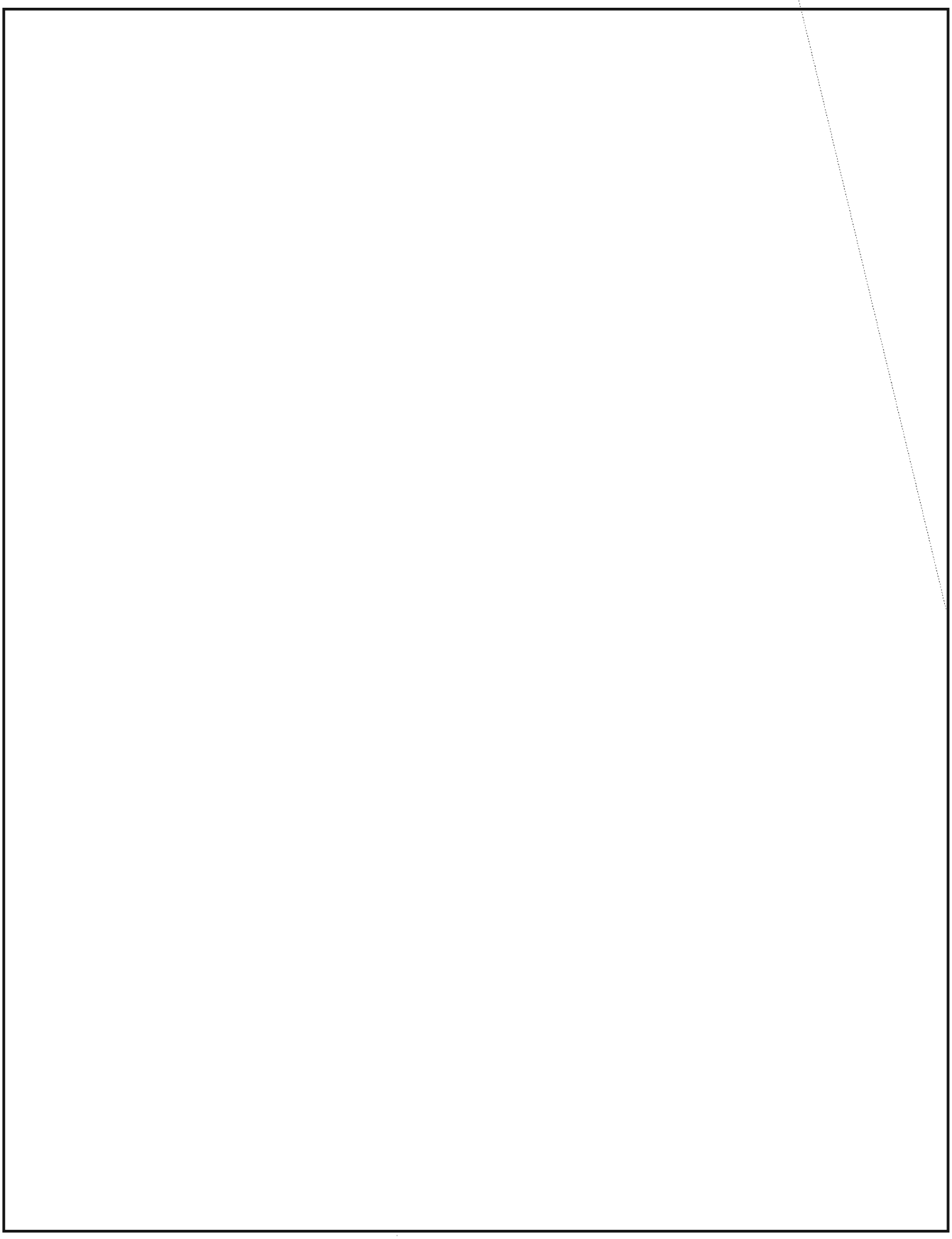
EO 1.4.(c)
P.L. 86-36



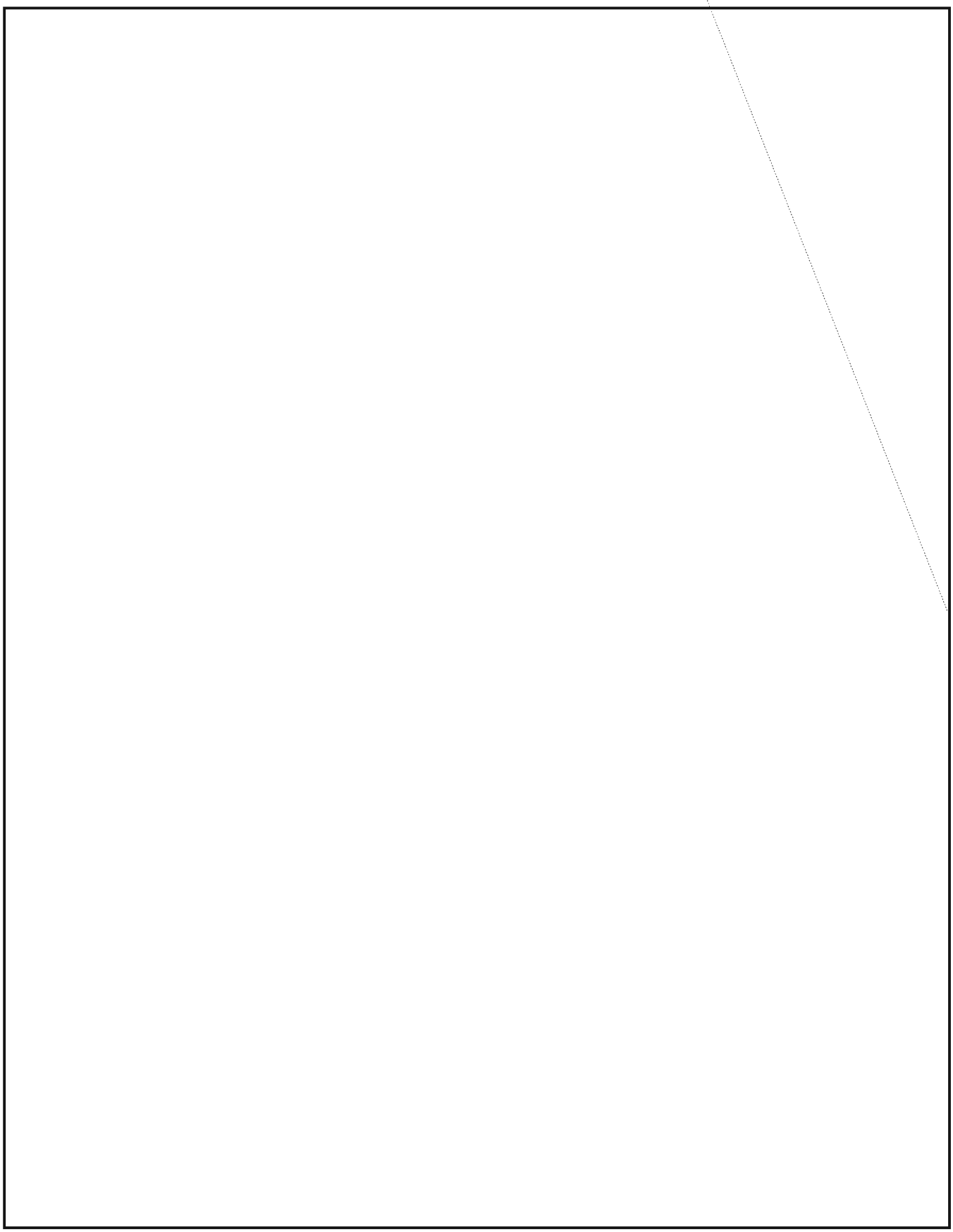
EO 1.4.(c)
P.L. 86-36



E.O. 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36



DOCID: 4033689

COLLECTION-SUPPORT TA IS NOT FOR EVERYONE

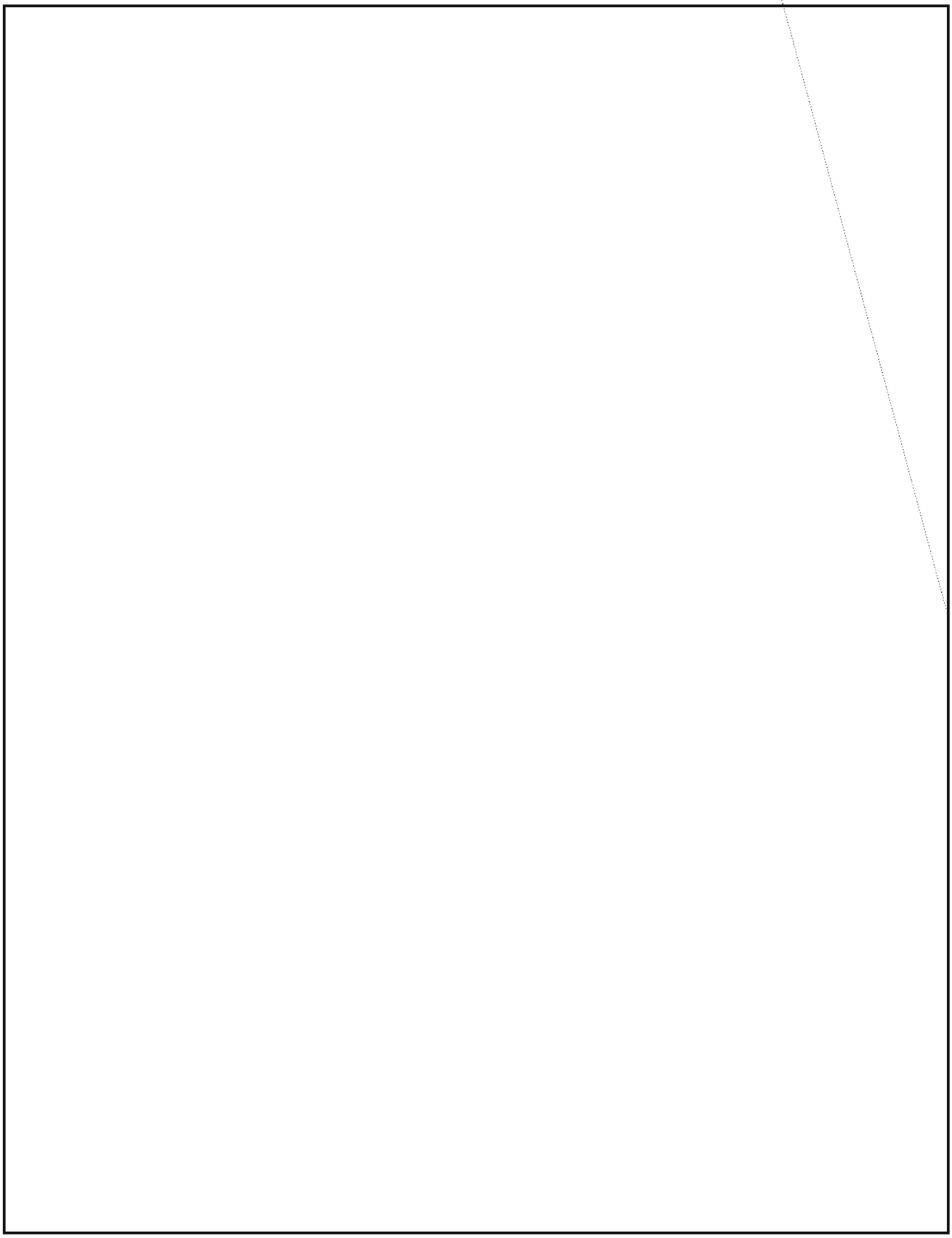
P.L. 86-36

It is often said that the traffic analyst working in a collection-operations area isn't doing traffic analysis. This is because very little in-depth analysis is being performed. Better termed, the work could be called "collection-support analysis." It is a special type of traffic analysis for which not all traffic analysts are well-suited. In fact, it is so different that some might suggest it be considered as a unique career specialty.

Recruitment of individuals with an aptitude for collection-support analysis, in my opinion, should be better defined. Too often, there seems to have been a willingness to accept any traffic analyst willing to work rotating shifts or perhaps willing to take a field-station tour of duty. Unfortunately, the skills needed to be a good traffic analyst do not necessarily transfer into making a good collection-support analyst (CSA). A certain mental persuasion is needed in order to be a competent CSA/TA in a collection-support analysis environment. This person plays a vital role in the collection cycle. He should be the oil and grease in the input, output, and feedback process of the collection cycle. This article will identify the role of the collection-support analyst and attempt to identify what his mental persuasion should be toward his job.

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



DOCID: 4033689

THE UNSEEN GO-BETWEEN: THE CONFERENCE INTERPRETER

J. Gurin, R5

Conference interpreting, without which there could be little communication among conferees from different countries, speaking different languages, is a young art. Before World War I, it was recognized and accepted that international conferences would be conducted in French, and no diplomat could expect to follow the course of action at such a meeting or be invited to participate actively if he did not possess a respectable command of that language. But during World War I, things changed drastically, and meetings between high-ranking French and British (and, later, American) officers required the services of interpreters.

At a recent NATO symposium on interpreting, it was my good fortune to meet and hear Dr. Jean Herbert, now of Geneva, who is the grand old man of conference interpreting. He has been performing that function for more than 60 years, beginning as a young officer in the French Army who happened to speak fluent English. He told of the Armistice Commissions, at which interpreters did the best they could at consecutive interpretation in French and English around the conference table. By the time of the Peace Conference, held exclusively in French and English, there were about a dozen interpreters who could take down and translate speeches verbatim. Consecutive interpretation was the rule throughout the life of the League of Nations, and it wasn't until World War II that simultaneous interpretation was introduced. For a long time it was not trusted because the speaker's delegation could not check the translation and because the performance left much to be desired. As a result, consecutive interpretation continued for a number of years in meetings of the United Nations. With the increase in the number of languages used, however, simultaneous interpretation finally won over, and with the availability of competent, professional interpreters, it is now fully accepted.

It is almost inevitable that, in a discussion of highly demanding interpreting tasks, the subject of bilingualism, or the degree of fluency in more than one language, should come up. While they still may argue among themselves about the precise meanings of the term, the professional interpreters rate themselves for their languages as follows: A - mother-tongue proficiency; B - fluent, active proficiency; C - excellent passive knowledge. It seems to be generally accepted that bilingualism means two mother tongues, a rare event even among the interpreters. Dr. Christopher Thiery, who teaches interpreting at the University of Paris, and who demonstrated for us in the course of the conference the skill of a consecutive interpreter of the first rank, maintained that trilingualism, i.e., three mother tongues, was virtually an impossibility. He himself could pass for an Englishman in England and a

Frenchman in France and never make a single slip. He admitted that several professional interpreters listed three Level-A languages against their names, but said that, in his opinion, only one might qualify as a true trilingual. This man, a former Spanish aristocrat, had learned his English and French from governesses in his childhood.

In recent years, the role of the conference interpreter, his specific professional task, the skills needed for its execution, and the material conditions permitting optimal permance have been analyzed and even codified with respect to working conditions. It is now recognized that good interpreter training aims not only at teaching the techniques of simultaneous and consecutive interpretation, but also preparing the mind of the interpreter for cross-cultural communication. One need only think of the way Khrushchev used to flavor his speeches with Russian proverbs to appreciate the need for the interpreter to be sensitive to the subtleties of meaning in both cultures. The program for training conference interpreters at the Polytechnic of Central London, for example, is geared to developing a triple awareness: of the cultural and social mores that motivate the speaker; of how his speech can best be expressed by the interpreter without altering the message; and of the socially and culturally heterogeneous audience to whom the message must be clearly conveyed. On this last point, English is particularly sensitive, for it is the language to which many listen whose mother tongues are extremely diverse. For example, the interpreter may be called upon to render into English a speech whose subtleties are to be understood clearly by Japanese, Danish, and Pakistani listeners, as well as Americans and British. What else should be expected of the interpreter? An analytical mind, phenomenal short-term memory, tireless powers of concentration, and good health. To this list one might add the requirement for the right kind of psychological and physical makeup to permit sharing a tiny booth with another interpreter, sometimes for many hours on end, and the requirement to be able to lose one's own identity in order to play the role of the speaker being interpreted.

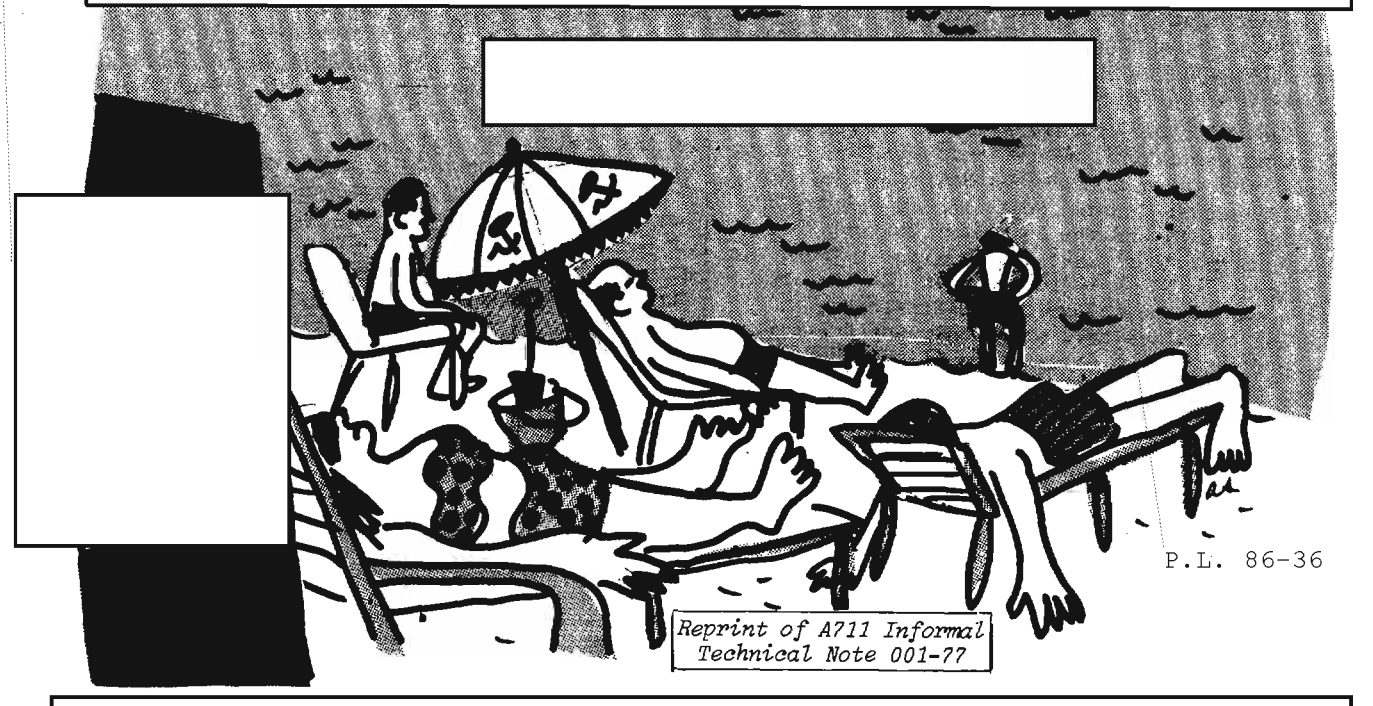
Of course there has been recognition of interpreting as an innate skill, and of the widespread phenomenon of natural translation, defined as "the bilingual translation done in everyday circumstances by people who have no special training for it." This condition is especially prevalent in bilingual countries like Canada and Belgium, where people from many walks of life, and of all ages, are frequently called upon to act informally as translators or interpreters. Studies have been made of very young children, under 3 years of age in some cases, who fall naturally into an interpreter role. In a different context, there is the repeated phenomenon of a child acting as interpreter for another child whose speech is difficult for an adult to understand.

For many of those who are seeking to comprehend the nature of the linguistic process, the professional interpreter, engaged in either simultaneous or consecutive interpretation, has provided an ideal subject for research and speculation. Synchronous recordings of debates at international meetings and of their simultaneous interpretation have stimulated investigations leading to the detection of units of meaning, or chunks of language, contained in the listener's short-term memory. This unit of meaning can be defined as the smallest group of symbols required for making sense, the minimum for translating a message or a portion thereof. Some regard the translation act as consisting of two distinct processes: the translation of the input discourse into an internal cognitive representation, and the transformation of this representation into output discourse. Here again, the unit of meaning would play an important role.

Much of the research evidence suggests that the bilingual's two languages are learned as separate systems and function as such thereafter. This raises questions regarding the "switching" mechanism and how it functions. Relevant research also suggests that the bilingual's two linguistic systems feed into and draw from some common supralinguistic background which seems to be independent of any language. Far from resenting this intrusion into their mental processes, the interpreters seemed as interested as the psychologists in discovering how they do what they do so well.

Conference interpreting, which had started so informally, has now been institutionalized. Many of the old-time pros are refugees of one sort or another from World War II, who capitalized on their usually accidental knowledge of several languages. New entries into the field are a different breed, and are normally the product of one of a number of training institutions that prepare students for this specific application of linguistic skills. The market for conference interpreters is greatest in Europe, especially for Common Market activities in Brussels, and there are several excellent schools on the continent. There is one graduate-level institution in the United States that has a program designed to produce professional conference interpreters; the Monterey Institute of Foreign Studies. Courses are given there in Chinese, English, French, German, Russian, and Spanish.

It takes a special kind of person to be successful in the field of conference interpreting, and when one watches a highly skilled, experienced interpreter in action, it is an impressive display of how the human intelligence can be called upon for near-miracles of performance.

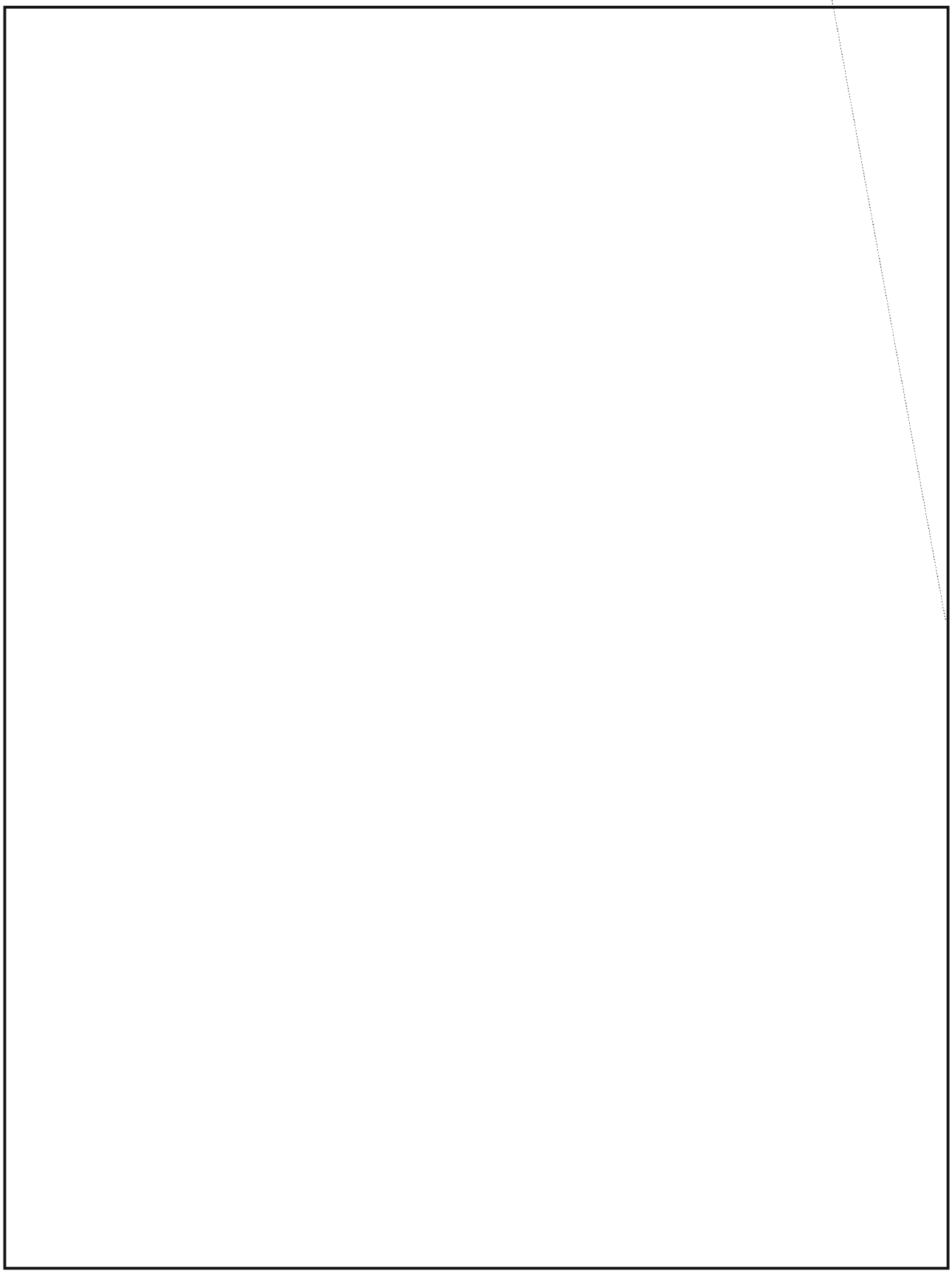


P.L. 86-36

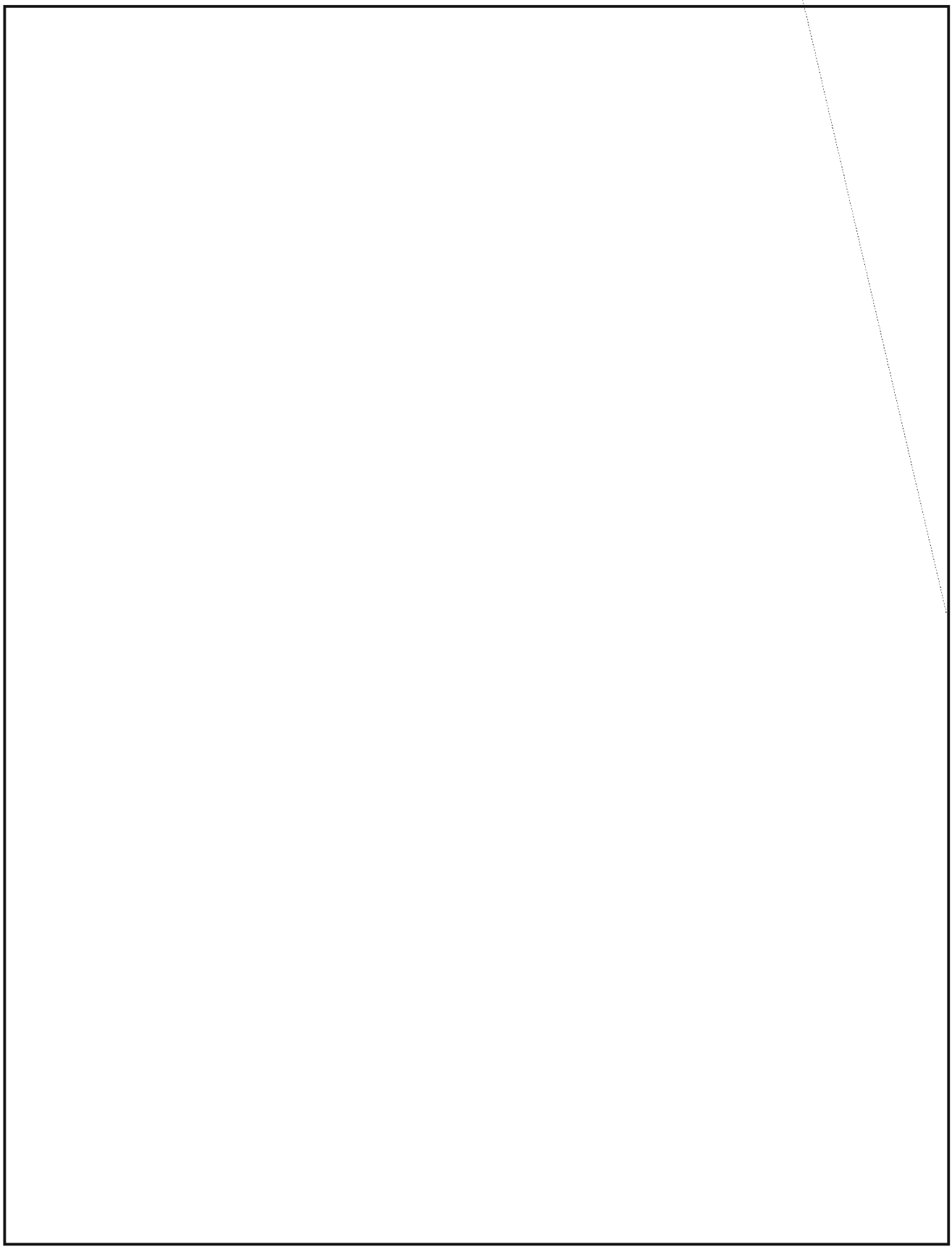
Reprint of A711 Informal Technical Note 001-77

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36



DOCID: 4033689

First Lady of Naval Cryptology

RAYMOND P. SCHMIDT,
NSG Historian

Reprinted, with permission, from the *NAVSECGRU Bulletin.*

Mrs. Agnes May (Meyer) Driscoll must have been a welcome person at Main Navy Building on Constitution Avenue in Washington, D.C. during the late 1920s and 1930s. She helped train Navy officers and civilians in the art of cryptanalysis (including the late Captain Laurance F. Safford, who first assumed direction of the "Research Desk" of the Code and Signal Section in OPNAV). After World War II, Mrs. Driscoll achieved recognition as a "principal cryptanalyst" for the Navy. She served in that capacity until December 1949, when she accepted a transfer to the Armed Forces Security Agency. She retired from active federal service on 31 July 1959.

Miss Agnes May Meyer entered the Naval Reserve in June 1918. In July 1919 she accepted a job as a stenographer for the Director of Naval Communications in the Code and Signal Section at $1400 annual salary. Working up to the position of clerk by 1920, she subsequently resigned in 1923 to evaluate a new electric cipher machine for Mr. Edward Hebern. She "solved" a message in his "unbreakable cipher" and was on her way to becoming a code and cipher expert.

On 1 August 1924 Miss Meyer returned to the Department of the Navy; she never again left government employment until her retirement. A Government Accounting Office memorandum of 6 May 1925 shows her as a cryptanalyst earning $1860 annually. In the mid-1930s she testified before the Senate Naval Affairs Committee that she had assisted the late William F. Gresham in developing a secure cipher machine for the Navy. The Senate appears to have believed her and awarded $15,000 to her and Gresham's widow. Not only was she qualified as a cryptanalyst, but also she obviously had skill as a cryptographer.

Agnes Meyer had earned an undergraduate degree from Ohio State University in 1911. As a first-generation American citizen, she took obvious pride in her naval service during the "Great War." One of her personal data sheets lists special qualifications in physics, engineering mathematics, statistics, auditing, bookkeeping, typing, and clerical work. She also possessed musical talent, having served as Director of Music in a small Texas school from 1912 to 1915. Then she became head of the mathematics department of an Amarillo, Texas high school until enlisting in the Naval Reserve during the war. It is interesting to note that she qualified in four languages -- German, French, Latin, and Japanese.

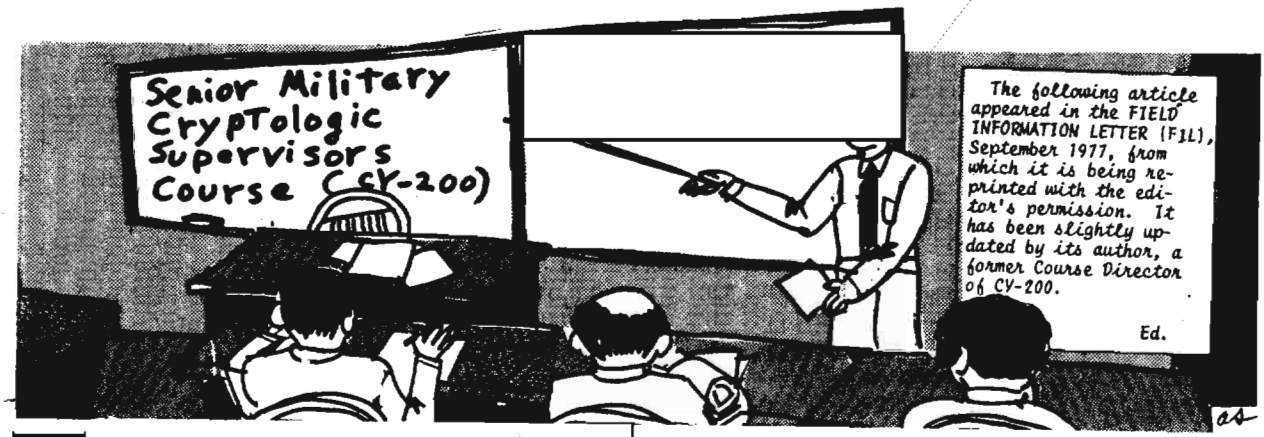
Agnes Driscoll deserves recognition as a "plank owner" in the naval cryptologic organization. Her abilities and skills as a cryptologist were widely respected by several generations of naval and NSA colleagues. Although her technical contributions to the United States have not been reclaimed from historical records, they obviously deserve far more space than permitted in this article. It is characteristic of her cheerful modesty that she described her job simply as one involving "scientific duties."

It would be sad, indeed, if Mrs. Agnes May Meyer Driscoll were to be forgotten by the present generation of cryptologists. We may very well owe her a professional debt that can only be repaid by continuing her rather awesome legacy of devotion and technical competence.

C.A.A. NEWS

The Communications Analysis Association's Winter Social was a great success, and why not? After all -- let's face it -- *free* parties are not that common around here. Of course, if you weren't a member, it did cost you something to get in. But *I* got in free and so did every other CAA member. Hope you got a chance to chat with the Director. (W.E.S.)

News from the CAA Special Interest Group on Cryptologic History: The group had its first meeting in November, and its first activity -- a tour of the P1 Cryptologic Collection -- in January. In December, members of the group received a copy of Dr. Harold Deutsch's article "The Historical Impact of Revealing the ULTRA Secret." Nonmembers of the group did not. Anyone -- CAA member or not -- who would like a copy can call Bill Nolte, 4087s, who can also explain the group's elaborate initiation rites. Future activities: In February or March (date to be announced): a session on oral history. (W.M.N.)



Twice a year, the National Cryptologic School (NCS) conducts the Senior Military Cryptologic Supervisors Course, Course CY-200. This course is for the senior NCOs/petty officers and warrant officers who are "going places" -- that is, those middle-level managers who will eventually be moving into jobs requiring a wider range of cryptologic knowledge. The objectives of the course are to:

- increase the student's understanding of the relationships and functions of the cryptologic community within the national intelligence community and the U.S. government structure;
- demonstrate the impact of increased requirements, decreased resources, and increasingly sophisticated targets on the cryptologic community;
- illustrate the responsiveness of the cryptologic community to the National Command Authority in times of peace, crisis, and war;
- bring the student up to date on the latest developments in cryptologic technology, operations, policies, and plans; and
- further develop and prepare the student for positions of added responsibility by exposing him to a variety of subjects outside his own area of specialization.

CY-200 is open to personnel from all four military services, grades E-7 to W-4 inclusive. Additionally, the NCS may grant waivers for highly qualified E-6s. Students must have at least 8 years of cryptologic experience, preferably in operations (as opposed to maintenance, communications, personnel, and other support specialties). To insure maximum utilization after graduation, NSA policy is to give priority in selection to personnel in their thirteenth or fourteenth year of service.

The course lasts 7 weeks and is conducted at Friendship Annex (FANX). It is designed in modular fashion, with each module covering a different subject area, as shown below in the schedule for Class 12 (summer of 1977):

Module	*Some of the topics covered*
Management Seminar	Contemporary management concepts, practices, and practical applications; problem-solving and decision-making; the planning and communicating process
U.S. Intelligence Community	Intelligence community organization and NSA's interface with it; role of the Director of Central Intelligence; Defense Intelligence Agency; Central Intelligence Agency; NSA support to national policy makers; national cryptologic security policy
SIGINT Resource Management System	National planning, programming, and budgeting; Consolidated Cryptologic Program; information management; economic analysis; resource management in the intelligence community; cryptologic planning
SIGINT Operational Process	

EO 1.4.(c)
P.L. 86-36

DOCID: 4033689
P.L. 86 36

[redacted]

Support Activities and Area Studies

Role of the SCAs and SIGINT Support to Military Commanders

Communications Security

gives an introduction to the U.S. worldwide photographic-reconnaissance program. At NSA's Headquarters complex, students have the opportunity to tour various spaces, including NSOC, DEFSMAC, AROF, BROF, and GROF, various research and development projects, and COMSEC facilities.

Throughout the course, student participation is encouraged through the use of seminars, panel discussions, and student presentations. Students are able to talk to and interact with experts from many fields.

Senior officials of NSA/CSS and other agencies in the intelligence community regularly brief each class. SCA commanders and senior enlisted advisors are also frequent visitors to the CY-200 classroom. At the end of the course, students have seminars with the Commandant of the National Cryptologic School and Director, NSA/Chief, CSS.

Students are selected for CY-200 by a simple procedure. Three to four months before the next course begins, the National Cryptologic School sends course announcements to the military services and SCAs. The announcements give course dates and student quotas (class size is usually 45), and solicit nominees. The services then submit the names of persons nominated for attendance.

If you are interested in attending CY-200, contact the appropriate organization as indicated below, depending upon your branch of service:

Service	*Point of Contact*	*AUTOVON Number*
Army	MILPERCEN:	
	(Enlisted: DAPC-EPL-M)	221-0070/0254/0329
	(Warrants: DAPC-OPW-AI)	221-7842
Navy	HQ NSGC (G131)	292-0757
Marine Corps	HQ Marine Corps (INT-S)	224-1208
Air Force	HQ USAFSS (DPXP)	945-2641

Since the first class in 1971, 316 students have been graduated from CY-200. Excellent comments on the value of the course have been received from the graduates to date. The distinguished graduates of the course include [redacted] who is now the senior enlisted advisor to DIRNSA. So who knows what CY-200 will do for you? If you think that this course might further your military career and you would like more information about it, contact either the course director, [redacted] USAF, E61, on 8043s/796-6181, or the NCS Registrar's Office, on 8041s/796-6417. You're too late to be graduate No. 317 (Class 13 began in January), but there are still a lot of good numbers to come!

P.L. 86-36

P.L. 86-36

In addition to the lecture modules, the class also goes on a number of field trips. At the Pentagon, students visit the Defense Intelligence Agency, the National Military Intelligence Center, and the military services' operations centers, and receive briefings on the missions and functions of DIA and the Strategic Warning Staff. While touring the Central Intelligence Agency in Langley, Virginia, students learn about the CIA's role within the intelligence community, its SIGINT operations, and its production of intelligence for national-level customers. The class also makes a trip to the National Photographic Interpretation Center, where the NPIC staff

DOCID: 4033689

MORE BEANS

NET WT. 16 OZS. (1 LB.)

Town House

Vera Ruth Filby, E41

Full text of all the papers presented at the ULTRA seminar will appear in a forthcoming issue of Cryptologic Spectrum.

We may as well get used to it -- used to hearing terms like "signal intelligence," "HFDF," and "traffic analysis" in public places, used to feeling exposed and unprotected at moments when our accustomed and familiar anonymity seems to be snatched away. Like most of us, no doubt, I had hoped that our "time of indecent exposure," as I have heard it expressed, might be nearly over, but a rainy October evening and foggy morning in Annapolis have persuaded me that we have seen only the beginning. Now that a few of our bean-counters' beans have been spilled, packs of hungry animals of various breeds, having caught the scent, are out there gnawing at the foundations of the storehouses, sniffing and rooting for more beans.

The occasion in Annapolis was the Third Naval History Symposium at the U. S. Naval Academy, 27-28 October 1977, specifically the Friday morning program on "Naval Intelligence in the Second World War." There, filling a tall, tiered lecture room in Rickover Hall, more than 200 people sat rapt for nearly 3 hours, without even a break, listening to presentations on "ULTRA and the Battle of the Atlantic." There it was easy to sense the appetite of the gathered historians for facts and more facts, their desire for truth and all the truth; and surely we can understand and appreciate that. The hunger -- even lust -- for information was evident even at the vast cocktail party the evening before, in the eagerness, for example, of a young historian snapping up a remark that there might be unreleased ULTRA information to be pursued. ("You mean," he asked, almost licking his chops, "there's lots more to come?") But influences other than scholarly questing for knowledge are present too, as I suddenly realized at the same party when an equally eager young historian, responding to a comment about inaccuracies in F. W. Winterbotham's *The ULTRA Secret*, retorted, "Yes, but it made him a million pounds."

Chairman of the Friday morning meeting was Harold C. Deutsch of the U.S. Army War College, and the speakers included:

- Patrick Beesly, former Deputy Chief, Submarine Plotting Room, the Admiralty;
- Jurgen Rohwer, Library of Contemporary History, Stuttgart;
- Kenneth A. Knowles, former Head, Atlantic Section, Combat Intelligence, COMINCH; and
- an unexpected bonus -- Vice-Admiral Sir Norman Denning, Naval Intelligence Division.

In his urbane and interesting introduction Dr. Deutsch remarked that many in the audience had been occupying themselves with the significance of ULTRA and said that although "tremendous euphoria" had following the publication of *The ULTRA Secret* in 1974, savage reviews had sent the tendency in the other direction. (Incidentally, despite critics' attacks, there are some who, while deploring the publication of the book at all, consider the charges of technical incompetence too harsh. Winterbotham was not a technician and never said he was; he was the vastly experienced intelligence officer who served as liaison between the producers of Special Intelligence and the highest echelon of users.)

On introducing Commander Beesly, Dr. Deutsch showed advance copies of Beesly's book on *Very Special Intelligence*, being published in England and scheduled for publication in this country in March 1978. Commander Beesly opened his masterful presentation by defining terms. He pointed out that that the term the Admiralty always used was Special Intelligence, that there is almost no mention of ULTRA in British naval records, that ULTRA was a classification, not a cipher title, although the term has taken on that meaning as a result of the Winterbotham book. Commander Beesly said that it is impossible to overstate the value of SI, but he stressed that it was only one of many sources. The information from the triumphs at Bletchley Park went to the Operational Intelligence Centre (OIC), which was a "full and true" intelligence center. Even when most complete, SI needs the genius of a few experienced analysts to piece it all together. Even at its best, SI is useless if the users do not understand and accept it, and Commander Beesley told horror stories of events when commanders refused to accept SI conclusions. Both he and the following speaker provided extensive examples of the use of ULTRA results in protecting convoys against German submarines, and he noted that German operations against the east coast of the United States were detected in advance by OIC. He summarized the state of success

at various phases of cipher recovery and the need during "blackouts" to fall back on HFDF (both he and the German speaker pronounced it "huffduff") and to try to read Admiral Doenitz' mind. Despite efforts at communications security, signaling remained necessary. U-boats had to report and to receive instructions, but later in the war the U-boat commanders were given more control and signaling became less frequent. At the time the Allies finally changed their codes in June 1943, both sides were reading each other's traffic without either being aware of the other's success. Concerning his sources for research on his book, Commander Beesly said that the British records were not complete but that many fascinating files were available from OIC and even from Bletchley. The most revealing were the weekly reports to the First Sea Lord, written by Beesly's chief, Captain Rodger Winn. The reports made by the tracking room were based mostly on SI. In estimating the value of SI, Commander Beesly said that its contribution was enormous in planning evasive routing and in concentrating naval forces, that without it victory would have come much later and at much greater human and material cost. SI, with the use OIC and the U.S. Navy's OP-22-G made of it, was a war-winner -- but not the only one. The real heroes were those who risked their lives and often had to pay a fatal price for other people's mistakes.

After an enthusiastic ovation for Commander Beesly, Jurgen Rohwer continued the story from the German side. He began by noting that TV and the other public media have given the public the idea that the Allies knew every German move in advance. If that had been the case the Battle of the Atlantic would have been over much sooner. He explained that ENIGMA was the codename for several cipher machines made by a private firm, and he described ENIGMA with slides showing rotors and other details. The German assumption was that the time needed to break an ENIGMA cipher would be so long that the results would be useless, and indeed the British did need the Polish and French reconstructions as a basis for their success. With a series of plotting charts on slides he showed the sequence of events at the time when both the Bletchley and B-Dienst cryptanalysts were reading each other's naval traffic and both sides were using radio intelligence, as he called it, in deploying and redeploying their submarines and convoys, in moves and countermoves based on current decrypts. In evaluating the German use of ENIGMA, he said that there were mistakes, there was carelessness, that full use was not made of the machines' capabilities. By the end of the war, however, the German Navy was using up to 40 different ciphers, so that Bletchley had to set priorities for attacking and exploiting them. In summarizing the role of naval intelligence, he listed in priority order radio intelligence, DF, and traffic analysis. Radio intelligence had much greater influence on decisions on the Allied side than on the German. The turning point would not have come, as it did, in May 1943 without radio intelligence, and Normandy would have come much later. In a final, startling statement, he said the end might have come with the dropping of an atomic bomb on Berlin.

Dr. Rohwer's speech was a tour-de-force, and it too received a long ovation. It was an interesting experience to see these two representatives of the great opposing forces complementing each other's presentations and helping each other by pointing out the movements depicted on the slides.

An American followed -- Kenneth A. Knowles, wartime Head of Atlantic Intelligence, Chief of the Intelligence Staff of the 10th Fleet. Captain Knowles had come from his retirement home in Florida and had written his talk on his boat in Chesapeake Bay, depending entirely on his memory of events 35 years ago, without any recourse to official records. He opened by commenting that World War II had brought technical achievements of the highest order and that transcending all was the breaking of ULTRA. The Americans, he said, were more selective for need-to-know than the British, and only three persons actually dealt with ULTRA at Headquarters "in a former girls' school in Washington." At the communications center there, traffic included ULTRA results, HFDF telefax, and radio-fingerprinting reports. ULTRA results were, with one exception, never used without such backup as aircraft sightings, DF, or other cover sources. The one exception, the one risk taken, was against the U-boat "milk cows" in the South Atlantic, and the ULTRA-based action against them brought results, in Captain Winn's words, "too true to be good." The Allies recovered U-boat ciphers, grid location charts, and a new acoustic device. Historians, he said, have considered the turning point in the Battle of the Atlantic to be the summer of 1943, after the sinking of 90 U-boats. But the Germans were making technical improvements -- flash transmissions, an acoustic torpedo, 10-cm radar, new designs for U-boats -- so it was necessary to crush the Germans before these improvement began to have effect. In evaluating ULTRA, Captain Knowles pointed out that it was used for defensive as well as offensive operations. He judged that in its use the British were more clever and the Americans more daring, and said that the teamwork between them was superb. He commented on the value to cryptanalysts of the sheer volume of traffic stemming from Doenitz' insistence on direct control. No such volume would have been available without it, but then, he pointed out, Doenitz' methods almost worked.

The final speaker, not on the original program, was Sir Norman Denning, of British Naval Intelligence. In his opening remarks he made it clear that, although he did not condemn

DOCID: 4033689

The ULTRA Secret, Winterbotham was the first person to break the oath of silence taken in 1940 when a select few signed their names to a document which forbade them ever to divulge ULTRA. He commented that surely ULTRA was the best kept secret in world history. He described early efforts to recover material to help in attacking the ciphers, the partial successes from, among other methods, capture of a weather ship, then recoveries from submarine U-110, after which Bletchley could read continental W/T traffic. But cryptanalysis is not the end of the job, he emphasized. Detailed analysis must follow; and he quoted from memory a comment referring to the World War I successes of Room 40, that "the information received has to be refined in the crucible of intellect and experience before it can be considered intelligence." In evaluating the results of SI, he said that only SCHARNHORST was a direct victim of its use. Sir Norman was in a reminiscent mood, and he spoke of Churchill in the anteroom of the war room just after the victory. "I see you're still celebrating," said the Prime Minister. "Can I join you?" And he turned to (then Commander) Denning and said, as Denning remembered it, "When I was a naval person we sometimes rang on the middle watch together in the dungeons of the Admiralty . . . You were the young officer who told me that total war required total intelligence, and without full commitment we might lose the war." After more Churchill stories, the applause of the listeners demonstrated how fully they had entered into the mood of nostalgia he had evoked.

During the too-brief question time which followed, the questions showed the intense interest of the audience, an interest which is certain, it seems to me, not to slacken. Earlier in the program, Dr. Deutsch had announced that a TV program was being produced at the Army War College at Carlisle Barracks on the Battle of the Atlantic, to be made available to government agencies and perhaps the public, and he urged his Army and Air Force colleagues to do what they could to sponsor similar programs on ULTRA as it affected ground and air operations. The range of sponsors for the Navy conference -- including the Army War College, the Smithsonian, the National Archives, the Eisenhower Foundation, and the Naval Academy -- would suggest that more such conferences are altogether likely. This listener noted particularly the rather coy references to a certain "agency of the Department of Defense" which had been consulted about the symposium and the expressed hope that more information for scholars would be forthcoming. It is unmistakably evident that even military historians, who should understand the purposes of military security, will be exerting continuing pressure.

(U)

BY-LINES DON'T COST — THEY PAY!

JOHN J. MOLLICK, B41

There has been a lot of talk recently about revamping procedures within the intelligence community to get bigger bangs from increasingly fewer bucks. That being the case, it appears the time has come to seriously consider instituting a relatively minor change in Agency reporting which I believe could greatly enhance the quality of our product, profoundly improve morale, and tremendously stimulate professional pride among the Agency's analysts and translators. And it wouldn't cost the National Security Agency one (pardon the expression) red cent!

My simple proposal is that NSA should begin putting the names of analysts and translators on the items they publish. This is no radical concept that has never been tried before. A number of sister agencies have long attached the names of their analysts to their products. As a matter of fact, by-lines on collateral items have several times served as my introduction to fellow analysts and have been responsible for my initiating mutually beneficial communications with those individuals.

Now that promotions seem to be farther and farther apart, new methods of increasing psychic income should be especially welcomed by those managers who are concerned with morale in their organizations. As an analyst, I can think of no source of psychic income more rewarding than to see my name on a piece of intelligence I have done my best to produce. No analyst or translator worthy of the title can help but take increased pride in, and care with, his work if his name is there for the intelligence world to see.

Within modern society as a whole, and certainly in modern government, there seems to be an increasingly dangerous tendency to shy away from fixing responsibility. Perhaps the most apparent truism of this age is the recognition that lack of responsibility breeds mediocrity. In addition to boosting morale, by-lines fix responsibility for the quality of our product. When names are attached to their work, professionals are bound to do their best all the time, and neophytes are compelled to improve rapidly by the most exacting of taskmasters -- their own developing reputations.

It is high time each analyst and translator is able to say to his peers, "This is my product. My name on it proves that I stand behind it. If it is accurate, don't hesitate to contact me, and perhaps we can help one another even more. If it contains error, tell me, and I'll try to improve. In any case, I proudly accept full responsibility for my work." The way to begin fixing responsibility, and giving credit where it is due, is by giving by-lines to live up to. The time to begin is now.

~~(FOUO)~~

DOCID: 4033689

"NO, WINNIE, YOU'VE GOT IT UPSIDE-DOWN TOO!"

The Editor's Page-and-a-half

Whenever I make up an NSA-Crostic, I give an advance copy to the person whose published work I'm quoting from. I don't give any hint about who wrote it, and the person usually tells me what a surprise it was to have his own words jumping off the page at him. Therefore, when guest NSA-crostician David H, Williams asked me to preview NSA-Crostic No. 11, I was surprised to see the following text emerge:

> [A. J.] Salemme, [*Guide to Russian*] *Technical Translation,* NSA, November 1974, 189 pp. (U):
>
> "The translator must . . . determine the precise type of [rotary-wing] aircraft . . . being referred to in Russian as . . . ВЕРТОЛЕТ so that his rendition will conform to precise English usage. He must not . . . avoid the issue by translating it in formal context as 'eggbeater' or 'chopper.'"

All the time I was solving the puzzle, I was chortling at the way that Dave had used Latin letters in the WORDS to represent Russian letters in the word ВЕРТОЛЕТ: the B in "This beets them all" suddenly turned into a Russian B (which is really pronounced V); the P in "Christopher Robin" turned into a Russian P (which is an R); etc. But what, I asked myself, was Dave going to do with the Л? The very last letter I put in the puzzle was in his "What *f* equals in a basic physics formula (3 wds)" -- "RECIPROCAL OF __." I don't know from physics, so I said, "That son-of-a-gun must be using a Greek lambda!" so I wrote in λ in both places in the puzzle. When I phoned him and congratulated him on his tour-de-force, he said that my guess had been right: *f* (frequency) is indeed the reciprocal of λ ([wave] length).

And so NSA-Crostic No. 11 was typed up for printing in the January issue. But, as is another practice of mine, I handed out some advance copies to a crew of people who like to do NSA-crostics critically, so that they can correct any typographical errors (178 instead of 187) or tighten up any definitions, etc. I was flabbergasted to learn that not one of them knew what to do with the letter in box 92. Here are the results:

Previewer	*"Words"*	*In text*
E.W., Russian linguist	"reciprocal of L"	ВЕРТОЛЕТ

Dialog:

A.S.: "All the other letters are Cyrillic -- where'd you get the Latin L from?"
E.W.: "I thought of it as a Russian L, but wrote a Latin one."

E.S., mathematician, knows "some Russian"	"reciprocal of F"	ВЕРТОФЕТ

Dialog:

E.S.: "The definition's wrong -- it should be 'f^{-1}'."
A.S.: "I don't know about that but I know that there isn't any Russian word with a Latin F in it."

G.E., Mongolian linguist (Mongolian has lots of borrowings from Russian and an alphabet based on Russian)	"reciprocal of ?"	ВЕРТО ЕТ

Dialog:

A.S.: "What does the ? stand for?"
G.E.: "How do *I* know? It's a Russian word!"
A.S.: "Why didn't you look it up?
G.E.: "I don't look up Russian words to do puzzles."

T.L., mathematician	"reciprocal of ?"	ВЕРТОЈЕТ

Dialog:

T.L.: "It's a Russian letter, but I don't know Russian."
A.S.: "Then where'd the J come from?"
T.L.: "I figured it was a kind of airplane."

With this preliminary showing (four wrong answers from four smart people), I figured out that somewhat was awry with the puzzle. I asked Dave if I could edit it in such a way that any ordinary CRYPTOLOG reader (with no knowledge of Russian, or physics, or nothing!) could make his or her hand make the correct letter and then stick it in box 92. The thing I came up with was to shuffle some of the letters around and come up with a definition:

N	O	I	S	I	Λ
119	44	182	164	63	92

("a ------")
his head for 20 years
saw after standing on
What the Hindu holy man

Back to a new group of previewers!

Previewer	*"Words"*	*In text*
C.G.	NOISIΛ	BEPTO ET

Dialog:

A.S.: "Why is box 92 blank?"
C.G.: "Charlie [C.G.'s husband] says it's Russian, but the puzzle's 'too damned cute' for him."

G.T.	NOISIΛ	BEPTOVET

Dialog:

A.S.: "You had the V upside-down in the words -- why did you turn it right-side-up in box 92?"
G.T.: "I didn't know I could put it in upside-down."

A.S.^{d}	NOISIΛ	BEPTOΛET

Dialog:

A.S.: "Yippee! You got it right! Why'd you put it in upside-down?"
A.S.^{d}: "I figured it must be a Russian letter that looks like an upside-down V. But I don't know how to pronounce it."*

Having finally got one person with no knowledge of Russian (and no prompting from me) to write an upside-down V and place it in box 92 in that same attitude (is it coincidental that that person is my daughter Anne?), I figured that the puzzle was ready for the average CRYPTOLOG reader. With Dave's blessing and with E.S.'s fear that the definition might offend any Hindu holy men who might get to see the puzzle, we went to press.

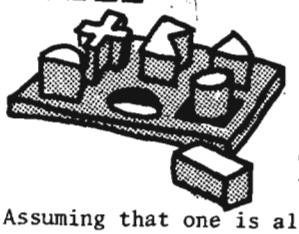
May I respectfully ask any CRYPTOLOG readers who did the puzzle, "What did you put in box 92? L? F? J? V? Λ? Or something else?" Or did you agree with Charlie, "It's too damned cute for me."

*Well, this is how you pronounce it. (First E is pronounced "ye" as in "yet"; second E is pronounced "yo" as in "yonder.")

B	E	P	T	O	Λ	E	T
v	ye	r	t	o	l	yó	t

Now say it -- "vyertoLYOT!" (Oops, I forgot to tell you to roll that R.) Try it again -- "vyer-r-r-rtoLYOT!" But you *still* don't know whether to translate it as "helicopter," "autogyro," "rotary-wing aircraft," "VTOL," or whatever. For guidance, see *Guide to Russian Technical Translation*.

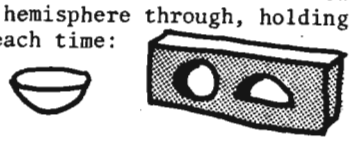
PUZZLE



Getting back to that psychological test on page 1, where the cylindrical peg *does* fit into a square hole, here's a little puzzle you CRYPTOLOG readers can work on.

Assuming that one is allowed to use only solid figures (rather than squeezable ones) which have to fit completely contiguously inside the cut-out hole, one could pass several different objects through a two-inch hole in a board. For example, a two-inch sphere, a cylinder with a two-inch diameter, a cone with a two-inch base:

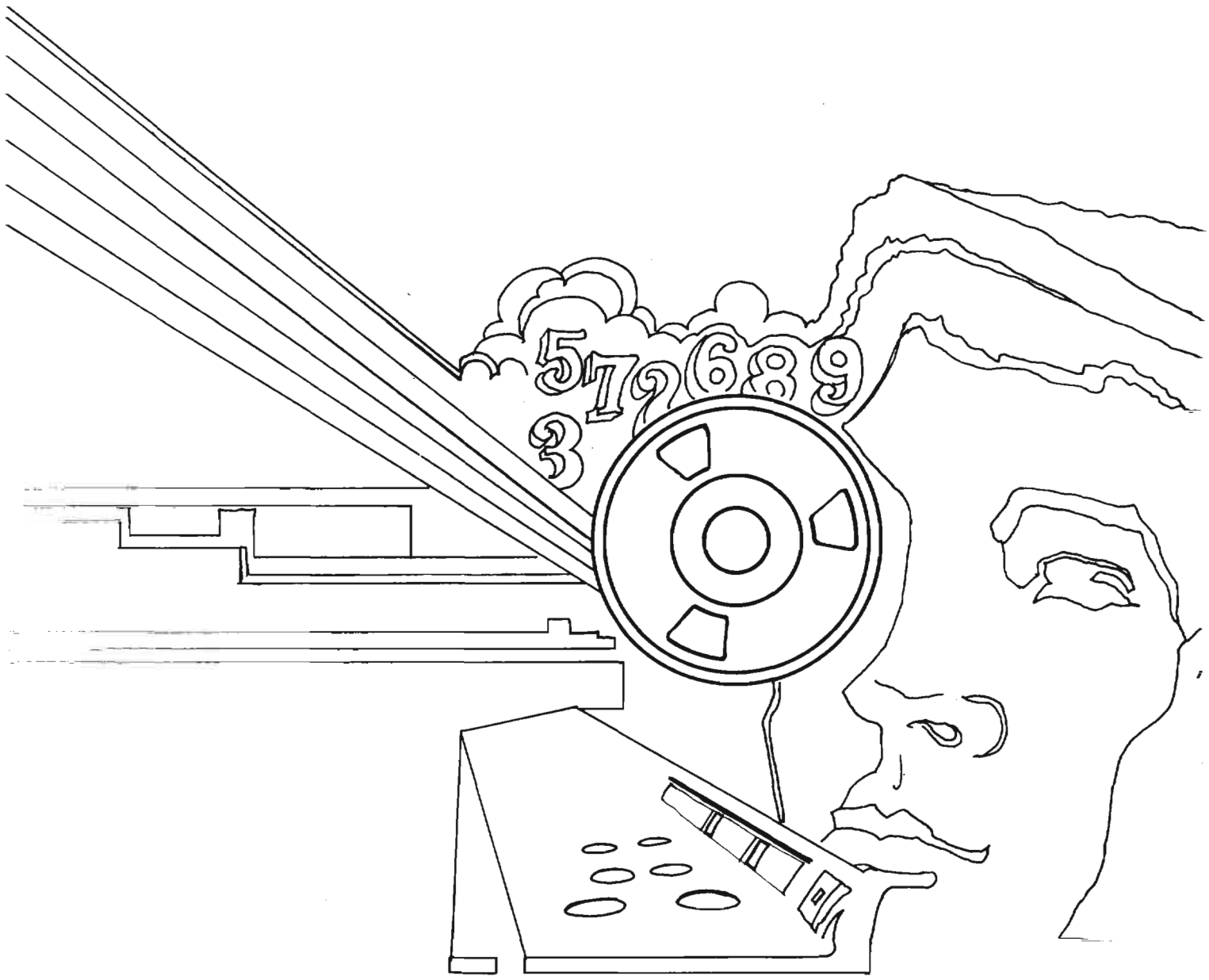
If you wanted to pass an object through *two* holes and have a completely contiguous fit each time, you could do that too. For example, if you had a board like the one shown below, you could pass a hemisphere through, holding it differently each time:



Now, then, the puzzle: Imagine a board like the one shown below. What *single object* can be passed through each of the three holes in turn, with a completely contiguous fit each time?

1 - 2" diameter
2 - 2" square
3 - 2" base, 2" height

A beautifully hand-crafted model of the object will be awarded to the first ten readers to send in the correct answer. (Answer will appear in next month's issue.)


5726893

DOCID: 4009806

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JANUARY 1978

P.L. 86-36

EO 1.4.(c)

EARLY PROPOSAL FOR SATELLITE REMOTING..... Joseph E. Horn..... 1
COMINT, COMSEC, AND HILBERT'S TENTH..... [redacted]..... 5
THE CHANGING FACE OF N.S.A..... 8
[redacted]..... [redacted]..... 8
BUT WHY DO WE DO IT?..... [redacted]..... 9
THANKS FOR THE ATTABOY!..... [redacted]..... 11
WHAT EVER HAPPENED TO COPES?..... [redacted]..... 12
"THE MAN WHO BROKE PURPLE"..... P. William Filby..... 13
A. C. BROWN'S "BODYGUARD OF LIES"..... [redacted]..... 14
NSA-CROSTIC NO. 11..... David H. Williams..... 16
C.A.A. NEWS..... 18
JOYS AND FRUSTRATIONS OF PLURAL-DROPPING.... A.J.S..... 19
LETTER TO THE EDITOR..... [redacted]..... 21

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009806

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. V, NO. 1 JANUARY 1978

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5236s)
Collection.....[redacted] (8955s)
Cryptanalysis.....[redacted] (4902s)
Language.....[redacted] (5236s)
Machine Support.....[redacted] (5303s)
Mathematics.....Reed Dawson (3957s)
Special Research.....Vera Filby (7119s)
Traffic Analysis.....[redacted] (4477s)
Production Manager.....Harry Goff (4998s)

P.L. 86-36

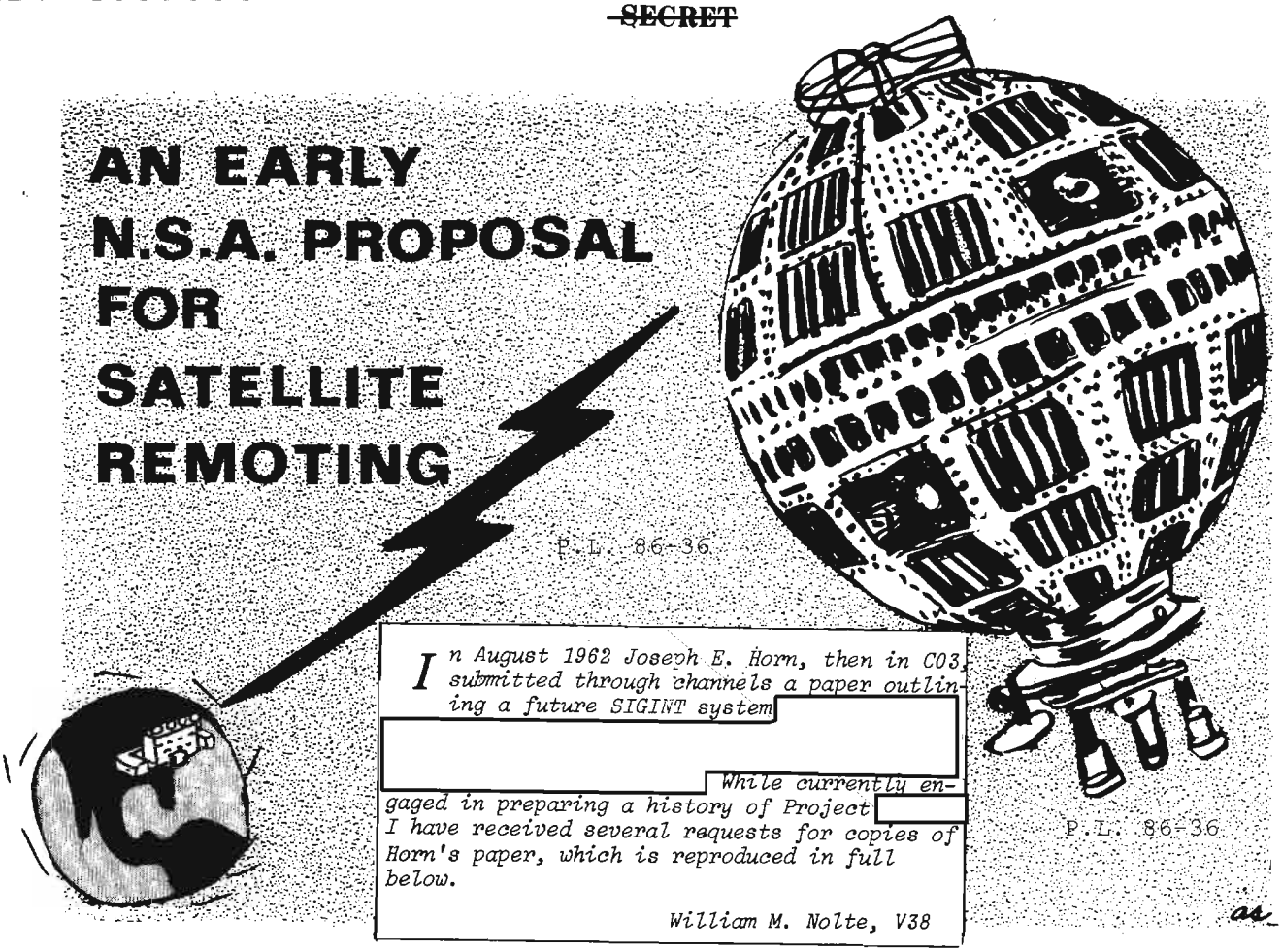
For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4009806

~~SECRET~~

AN EARLY N.S.A. PROPOSAL FOR SATELLITE REMOTING



P.L. 86-36

In August 1962 Joseph E. Horn, then in C03, submitted through channels a paper outlining a future SIGINT system [redacted] *While currently engaged in preparing a history of Project* [redacted] *I have received several requests for copies of Horn's paper, which is reproduced in full below.*

William M. Nolte, V38

P.L. 86-36

DISPOSITION FORM

File No. C03/085/62, 19 September 1962

The attached paper is submitted, as a think piece, not a proposal. The devotion of time to considering the statements made in the inclosure was motivated by the day-to-day pressures on SIGINT activities and the feeling that NSA should have a long range plan which steps beyond the many SIGINT development plans of varying scope that are prevalent today throughout the SIGINT Community. As far as known, the idea as presented is different from any current development plans.

JOSEPH E. HORN
C03

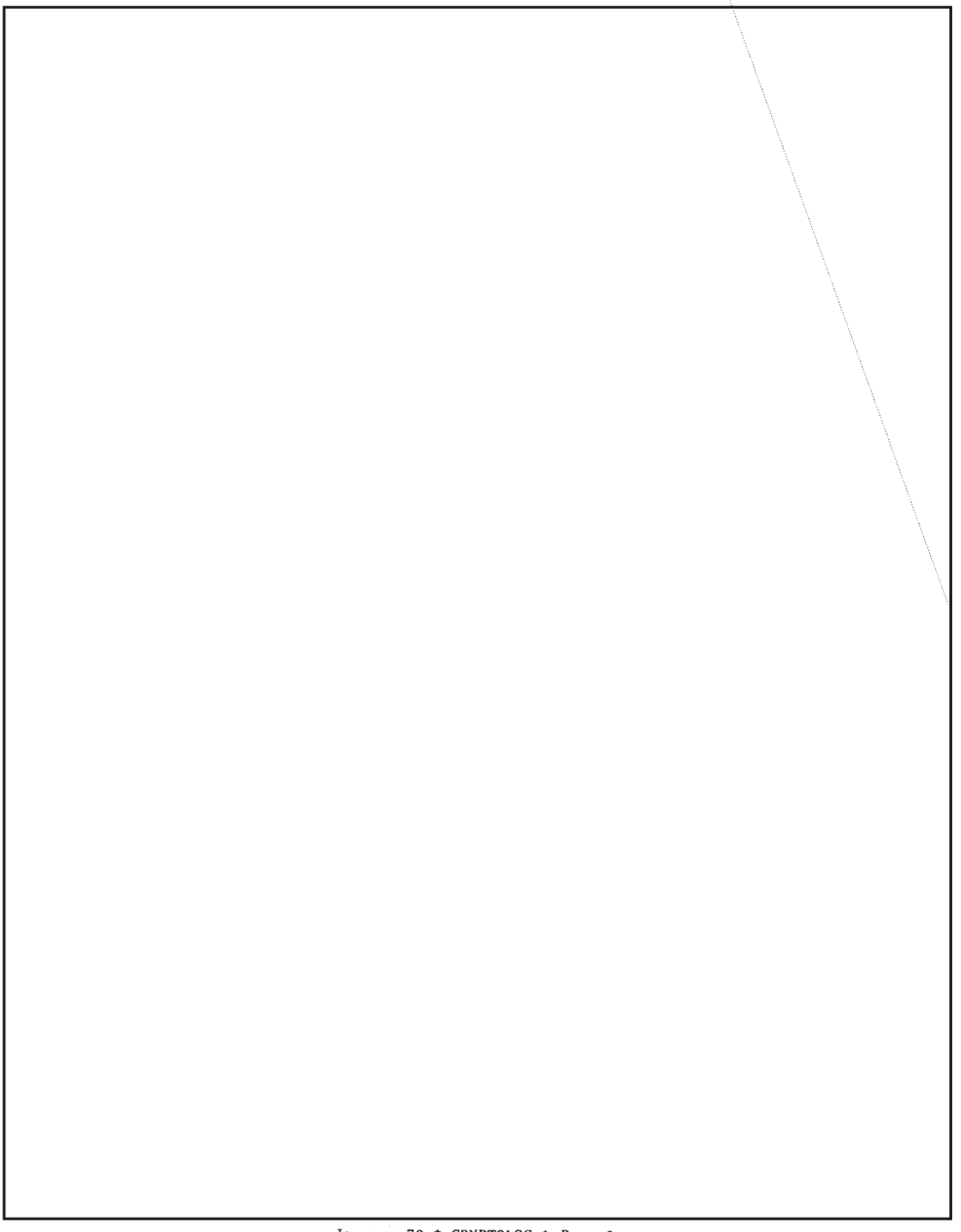
29 August 1962
JOSEPH E. HORN/Ext. 3723/C03

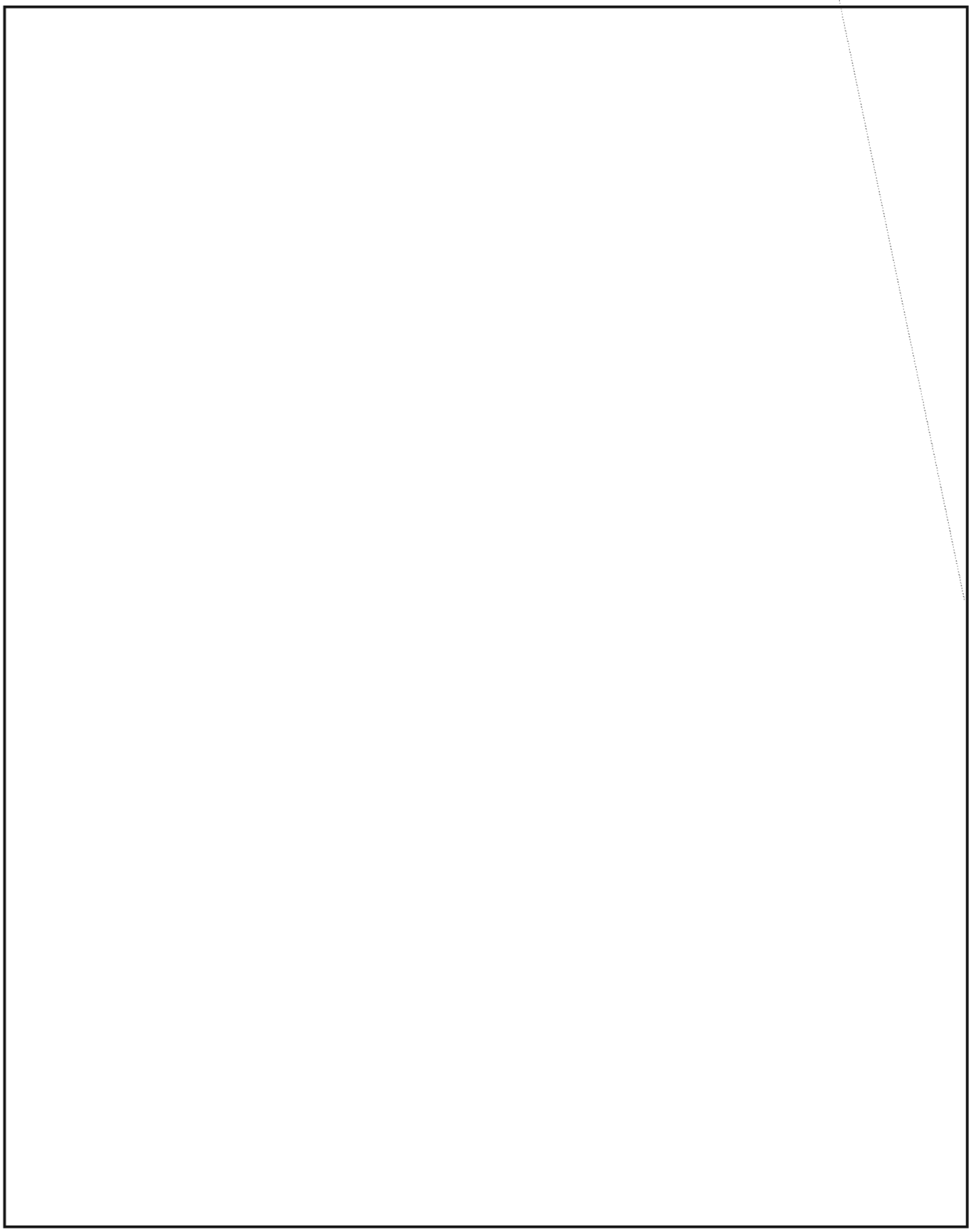
EO 1.4.(c)
P.L. 86-36

~~SECRET~~

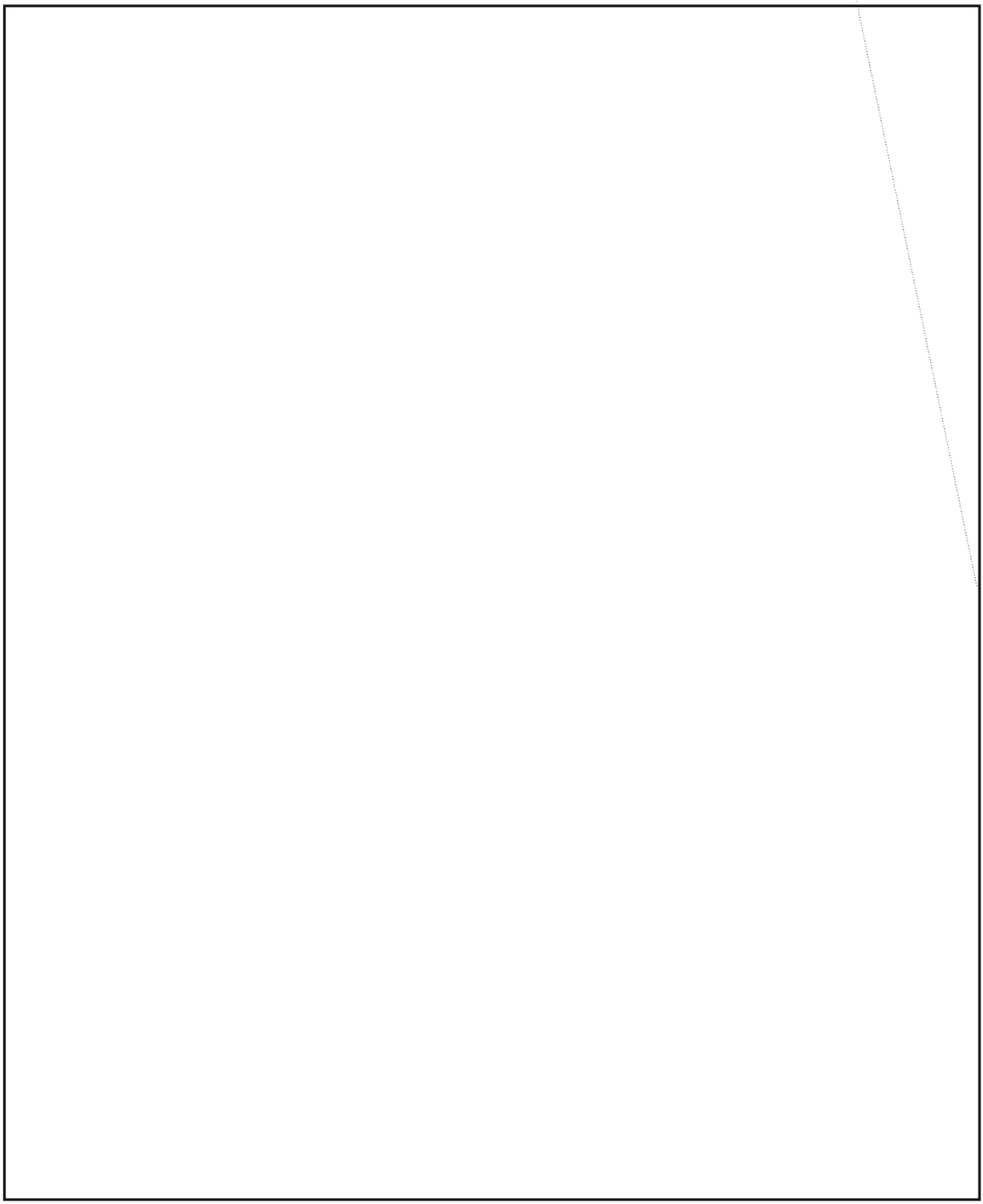
~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36





EO 1.4.(c)
P.L. 86-36



DOCID: 4009806

EO 1.4.(c)
P.L. 86-36

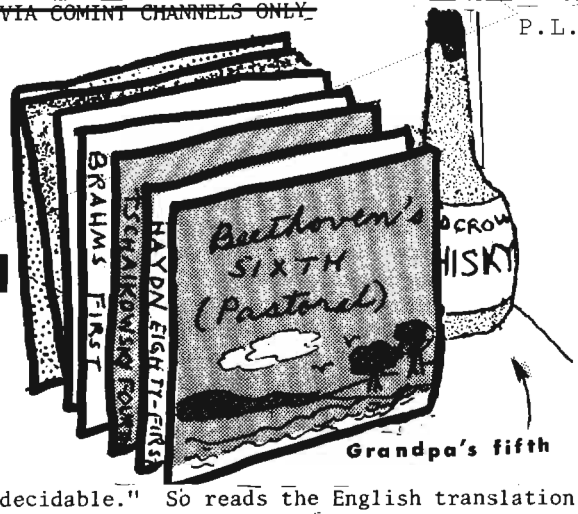
~~SECRET~~

~~(S CCO)~~

~~CONFIDENTIAL - HANDLE VIA COMINT CHANNELS ONLY~~

COMINT, COMSEC, AND HILBERT'S TENTH

P.L. 86-36



R51

The great German mathematician David Hilbert died in 1943 after a long and highly productive career. He was well into that career in 1900 when he delivered a paper in Paris which engaged the attention and energies of mathematicians for many subsequent years. That paper[1] listed 23 problems which, in Hilbert's opinion, the mathematical community should endeavor to solve forthwith.

One by one, the 23 problems were solved, except for problem No. 10. Finally, in 1970, even that holdout gave out (or gave in). Several important blows had been delivered earlier, but the coup de grace was delivered by a 23-year-old native of Leningrad, Yu. V. Matiyasevich*.

The American mathematician Martin Davis, who had delivered, in 1953[2], one of the earlier blows, had pointed out[3] that the tenth problem was the only one of Hilbert's 23 which, in today's terminology, could be classed as a "decision" problem. Indeed the M solution[4] asserts that Hilbert's tenth problem is "algorithmically undecidable." So reads the English translation of his first Russian paper[5] on his solution. In what I assume is his own English-language paper[6], delivered at the Nice International Congress of 1970, he simply calls Hilbert's tenth problem "unsolvable." Unfortunately for those who translate from Russian to English, the English words "undecidable" and "unsolvable" are translations of the same Russian word *nereshimyj*, which is related to the Russian word *reshenie*, and that word can be rendered correctly into English, depending upon context, as "decision," "determination," "judgment," "decree," "verdict," "solution," "answer," "conclusion," etc.[7]

Of possible interest [redacted] is *not* Hilbert's tenth problem, per se, or its final alleged solution, per se. What *is*, or might be, of interest is one of the ancillary conclusions tossed off by M, first in a parenthetical note in his first paper, then in its own sentence in his 1970 paper: "For example, the set of all prime numbers coincides with the set of all positive values of some polynomial with integer coefficients!" (M's!)

EO 1.4.(c)
P.L. 86-36

*Russian spelling Ю. В. Матиясевич (pronounced "mah-tee-yah-*SEH*-vitch," with the sole stress on the fourth syllable. The name appears in the literature in the "international" transliterated form: Ju. V. Matijasevič. Henceforth I will refer to that bright kid (now an over-the-hill 30-year-older) as M.

~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4009806

It's been established that a polynomial in *one* variable will never generate all the prime numbers. M, however, is not talking about polynomials on one variable. His first paper gives a step-by-step *construction* of the polynomial which generates all, and nothing but, the primes (as its *positive* values). That polynomial, says M in his third paper, would have a hundred variables. By the second paper, the claim is for some 25 variables. Finally, the third paper gives the *construction* of a polynomial of 37th degree in 24 variables. That was in the first sentence of the original paper. In the addendum (added in the translation to English[8]), M is down to a polynomial of degree 21 in 21 variables. In that same paper, M goes on to say that "The number of variables may be reduced even more, but the author has been able to do this only at the expense of an essential increase in the degree of the polynomial."

[redacted]

Way back in November 1976, Whitfield Diffie and Martin E. Hellman (henceforth referred to as D-H) wrote an invited paper, "New Directions in Cryptography."[9] The ideas of these two Stanford University professors were discussed by Martin Gardner in the Mathematical Games department of the August 1977 issue of *Scientific American*. Gardner notes that the D-H thesis has been "improved" by the three M.I.T. workers Ronald Rivest, Adi Shamir, and Leonard Adleman. The nub of their improvement was the utilization of *prime numbers*. Almost simultaneously, the computer-encryption waters were further muddied by the outpourings of Gina Bari Kolata in the July 29, 1977 issue of *Science* (Vol. *197*, No. 4302), writing, in the "News and Comments" section, on "Computer Encryption and the National Security Agency Connection."

[redacted]

Annotated Bibliography

[1]D. Hilbert, *Gesammelte Abhandlungen*, Band 3, Berlin (1935). In the NSA library, the call number is: QAS, H54, 1970, V.1. See pp. 290-329 (particularly p. 310).

[2]Martin Davis, "Arithmetical Problems and Recursively Enumerable Predicates," *Journal of Symbolic Logic, 18*, 33-41 (1953). The NSA file of this journal goes back only 20 years, but our library's [redacted] can (and already has been able to) borrow the Library of Congress copy. P.L. 86-36

[3]Martin Davis, *Computability and Unsolvability*, Wiley, New York (1958). In the NSA library, the call number is: QA 248.5, D29.

[4]Yu. V. Matiyasevich, "Diofantovost' perechislimykh mnozhestv" (The Diophantine Nature of Enumerable Sets), in *Doklady AN SSSR* (Papers of the USSR Academy of Sciences), *191*, 2, 279-282 (1970). Not in NSA Library. M's own abstract can be found in review 7A80 in *Referativnyj zhurnal: Matematika* (Abstracts Journal: Mathematics), in the R5 library -- see [redacted]

[5]Ju. V. Matijasevič, "Enumerable Sets Are Diophantine," *Soviet Math. Dokl., 11*, No. 2, 354-358 (1970). English version of [4]. In NSA Library, look under "Soviet Mathematics." EO 1.4.(c) P.L. 86-36

[6]Ju. V. Matijasevič, "Diophantine Representation of Recursively Enumerable Predicates," *Actes, Congrès intern. math.*, 1, 235-238, Paris (1971). NSA Library call number for the first volume of proceedings of the 1970 Nice Congress is QA1, In 8, 1970, V.1.

[7]*Russian-English Dictionary* (chief compiler A. I. Smirnitsky), Moscow (1958). There are later editions -- this is the one on my desk.

[8]Ju. V. Matiyasevich, "Diophantine Representation of the Set of Prime Numbers," *Soviet Math. Dokl., 12*, No. 1, 249-254 (1971). In NSA Library, look under "Soviet Mathematics."

[9]Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory, IT-22*, 6, 644-654 (1976).

M has published frequently, almost always in Russian, since 1967. For an Englishman's reviews of the Russian originals of [4] and [8], as well as M's detailed proof of his thesis (in *Izv. AN SSSR* (News of the USSR Academy of Sciences, *35*, 3-30 (1970)), see three reviews by J. W. S. Cassels, Cambridge, England, all in our *Mathematical Reviews (MR)*, in the NSA Library: EO 1.4.(c) P.L. 86-36

MR 41, review 3390 (1971)
MR 43, review 54 (1972)
MR 43, review 1921 (1972).

M's initial paper received a favorable review by one of the Americans he cited, Martin Davis, in *MR 50*, review 6820 (1975), and M has coauthored two papers with another American he cited, Julia Robinson. The relevant reviews are: *MR 52*, review 8033 (1976) and *MR 53*, review 10566 (1977).

~~(C - CCO)~~

*Addendum

UNCLASSIFIED

The text of my original paper, as submitted to CRYPTOLOG on 28 September, ended at this point. Three weeks later, [redacted] another -- and far more competent -- R51 mathematician, brought to my attention (i.e., showed me) a 1976 P.L. 86-36

article[10] which actually contained a prime-representing polynomial. This polynomial is of degree 25 in 26 variables. The four authors assert that, "When nonnegative values are substituted for the variables, the positive values of (1) coincide exactly with the set of all prime numbers. . . [It] also takes on negative values, e.g. -76."

To assuage the reader's curiosity, I include here polynomial (1) from that paper:

$$(1)\quad (k+2)\{1-[wz+h+j-q]^2-[(gk+2g+k+1)\cdot(h+j)+h-z]^2-[2n+p+q+z-e]^2$$
$$-[16(k+1)^3\cdot(k+2)\cdot(n+1)^2+1-f^2]^2-[e^3\cdot(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2$$
$$-[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)\cdot(n+4dy)^2+1-(x+cu)^2]^2-[n+l+v-y]^2$$
$$-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2$$
$$-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}$$

[10]James P. Jones, Daihachiro Sato, Hideo Wada, and Douglas Wiens, "Diophantine Representation of the Set of Prime Numbers," *The American Mathematical Monthly, 83,* 6, 449-464 (1976). (U)

Addendum$_2$

A few remarks about *the* polynomial -- call it P(a,b,...z), since it is a function of those 26 variables. Notice that P can be written in the form $(2 + k)\cdot(1 - S)$, where S is a function (of those same 26 variables) taking the very specific form of a sum of 14 perfect squares, i.e.,

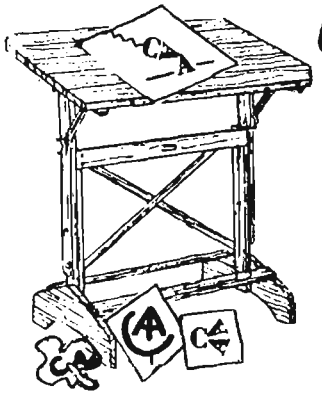
$$S = \sum_{\alpha=1}^{14} T_\alpha^2,$$

with each of the 14 T_α being a sum, difference, or product of integer variables, each occasionally raised to a low power. Since each of the T_α is an integer (whether negative or positive), its square (T_α^2) is necessarily positive (or just zero). Hence S, being the sum of squares, is either zero (if all 14 terms are themselves zero) or positive.

The product of the necessarily positive factor $(2 + k)$ by $(1 - S)$ is itself either zero, if $S = 1$, or equals $2 + k$, if $S = 0$, or is negative. Since we are to ignore all *negative* values of polynomial P, and we're quite indifferent to its zero values, we must remain indifferent to *all* values of S except $S = 0$. Variable k, being free to roam all the positive integers, starting with zero, can certainly be zero, giving the smallest prime 2 + 0 = 2, or can equal one, giving the lowest odd prime 2 + 1 = 3 and, thereafter, must be some, by no means just any, odd number (while 2 + 3 = 5, a prime, and 2 + 5 = 7, another prime, 2 + 7 = 9, which is hardly prime). *That* k, in conjunction with the other 25 variables, must somehow serve to provide a zero value to all 14 of the terms T_α, in order for P's value to be a prime. I remind at least some of my readers that an algebraic equation with integer coefficients all of whose solutions (if any) are integers is called a Diophantine equation since they afforded such entertainment to that ancient Greek mathematician Diophantus. (U)

E.S.S.

(Any more addenda? Last chance!. . All right, then, to press! -- *Ed.*)



C.A.A. Logo Contest

The Communications Analysis Association (CAA) is looking for a logo -- a symbol or emblem which is simple yet symbolic of the goals and purposes of the Association. We've tried a few ideas of our own, but aren't particularly pleased with anything we've come up with to date.

In order to benefit from the vast amount of creative talent available throughout the Agency, we've devised a contest to find a suitable logo.

Anyone may enter. The rules are simple:

1. Art work is not important. The concept or idea is what we're seeking.

P.L. 86-36

2. All entries must be submitted (one entry per page) to the contest chairman, [redacted] D5, Room 9A181, not later than 1 March 1978. Any individual may submit more than one entry.

3. Each entry must have the name, organization, and phone number of the submitter on the back.

4. Judging will be by the Executive Board of the CAA. The judges' decision is final (naturally).

5. No submissions will be returned.

The first (and only) prize will be a gift of a book of the winner's choice, and, of course, public recognition.

(U)

DOCID: 4009806

P.L. 86-36

THE CHANGING FACE OF N.S.A.

One of our constant readers (and almost as constant contributors) is also a pack rat. He has saved, for example, all the back issues of the Agency's *Quarterly Management Review*. Recently he compared the issue for the fourth quarter of FY73 and the issue for the second quarter of FY77, and came up with some interesting figures that he wants to submit without comment. *Ed.*

How many people are there in your COSC field today, and how has that number changed over the last 4 years? The following figures were taken from two issues (4 years apart) of the *Quarterly Management Review*. Only fields with 100 or more civilians *assigned* to them are shown.

~~(C - CCO)~~

~~(S - CCO)~~

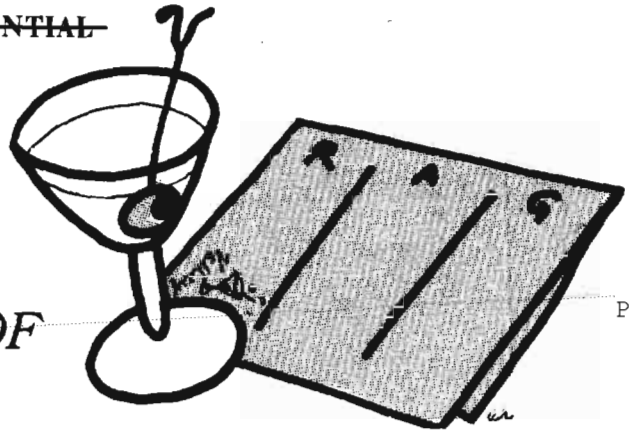
EO 1.4.(c)
P.L. 86-36

P.L. 86-36
EO 1.4.(c)

DOCID: 4009806

BUT WHY DO WE DO IT?

[redacted] GROF



P.L. 86-36

Every couple of months you open your copy of CRYPTOLOG and come across a piece which has as its subject matter a topic which, you proclaim to all within earshot, "everybody knows anyway." This is the January article of that species.

The purpose of this article is to point out an existing problem, briefly explore its symptoms and underlying cause, and present one means of reducing its incidence.

Picture, if you will, the following scenes:

Scene 1: George Allen and Billy Kilmer are discussing the team's faltering fortunes (or, if team loyalty will not permit it, picture Ted Marchibroda and Bert Jones). The team has just lost its eighth straight game; the QB has not completed a single pass. "But, Coach, I'm *throwing* the ball," the QB protests.

Scene 2: You enter your doctor's office for a postoperative examination; you feel just as poorly as you did before the surgery. "I've done all that I can do, Mr. Smedley; I *made* the incision," your physician says.

Scene 3: You've loaned your beautiful new 1977 Belchfire V8 to your neighbor. An hour later, you watch in horror as a tow truck returns a twisted pile of useless metal to your driveway. "It's not my fault, Harry; I *looked* both ways!"

Put you in the coach's place and you'd sack the quarterback quicker than a defensive end would. If that was your doctor, you would protest his bill, in court if need be. And, as for your neighbor, you'd probably force-feed the hood ornament to him.

But what, you ask, does all of that have to do with NSA? Those were contrived, exaggerated examples, weren't they? Yes, somewhat. But how about these:

"Don't look at me; I *sent* that tasking message."

"It's not my fault he's not here; I *called* him."

"We're covered on that; I *posted* the notice on the bulletin board myself."

"The blame lies elsewhere; I *informed* that office months ago."

"I can't help it if your in-grade is late; I *mailed* the personnel action weeks ago."

"I'm sorry the tape is blank, but I *recorded* the signal."

Do they hit a little closer to home than the first three? You bet they do! And, if anything, statements such as these are getting to be an increasingly commonplace occurrence.

The root cause of the problem is not unique to NSA, or to the federal government for that matter. It is pervasive in our society (remember the last time you spoke to the billing department at Sears?). A sociologist might point to "the attempt by an organism to adapt to an environment of increasing complexity" as the reason behind the problem. In management terms, however, the problem is due to a confusion of activities and goals.

A glance back at the scenes will highlight the problem. All the emphasized words are verbs, things that we *do*.

"I'm *throwing* the ball," "I *made* the incision," "I *looked* both ways," "I *sent* that tasking message," "I *called* him," . . .

But two self-evident statements might be made here:

Self-evident statement No. 1:

The words "doing" and "done" are *not* the same word.

Self-evident statement No. 2:

Just because someone performs an activity does *not* mean that a goal has been achieved, that the job is completed, or that that person's responsibilities have been fulfilled. The activity might have had nothing whatsoever to do with the goal. The activity may, in fact, have been *counter*productive, leaving the organization even farther from the goal than before.

What needs to be understood, then, is the difference between a *goal* and an *activity*.

A goal (or "objective," if you prefer), as generally accepted, is a state of being. It is a point or phase which is achieved or reached.

An activity, on the other hand, is something that is done in order to achieve the goal.

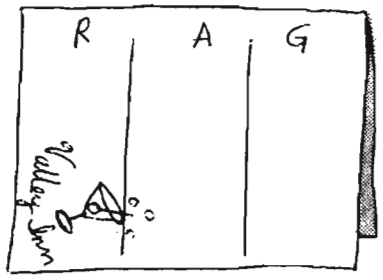
We have now come to the "so what?" point in this article. But there are actually two levels of this question -- "so what?" and SO WHAT?" -- and I'll treat them in that order.

The "so what?" is the one that you mentally utter to yourself during all meetings, briefings, tours, and conferences. While the speaker drones interminably on, listing the electronic wizardry which his organization is capable of performing or his shop's latest analytical coup, you repeat "So what?" to yourself.

At the conclusion of the gathering, and if your "so what?" has not been answered to your satisfaction, that is the time to exclaim, aloud (preferably in private conversation), "SO WHAT?"

Finally, you'll need a framework for listening to, gisting, and recalling the meeting. As with most other organizational matters, simplest is best.

The simplest model of which I am aware* is one which was developed on a cocktail napkin at the Valley Inn in Fallston, Maryland. Like another, more famous document, written on an envelope during a train ride to Gettysburg, this one retains its ability to describe many conditions while maintaining its simplicity. It is reproduced in miniature below:



R = Resources
A = Activities
G = Goals

So, during the meeting, while others are taking notes in the standard format, or merely listening, you jot down the key words in the proper cell or cells. Items such as people, equipment, time, real estate, and dollars go into the "Resources" (R) cell. Anything that will be done, such as collecting, analyzing, processing, storing, disseminating, etc., you will place in the "Activities" (A) cell. Hopefully, you will also have some "Goals" (G) to enter:

"Ten percent fewer poking errors,"

"To know the target's complete Basic Station Designator system,"

"The same hours of coverage for 22% fewer dollars,"

"A completely safe and uneventful evacuation of the crisis spot."

A simple extension of the matrix will help cover situations wherein "Time" plays a role for which you will have to account. This alteration is pictured below:

	R	A	G
P			
I			
E			

P = Planning
I = Implementation
E = Evaluation

Thus, you may:

- see if the *planned* activities were actually *implemented* later on;
- determine what percentage of the *resources* were expended;
- find out if the *planned* goals, as *implemented*, were at all realistic;
- and a host of other questions (some of which may even be pertinent).

If you will enlarge the following "Program Matrix" to 8x10½" format, your division's Xerox machine will provide you enough RAGPIE matrices for a lifetime of meetings:

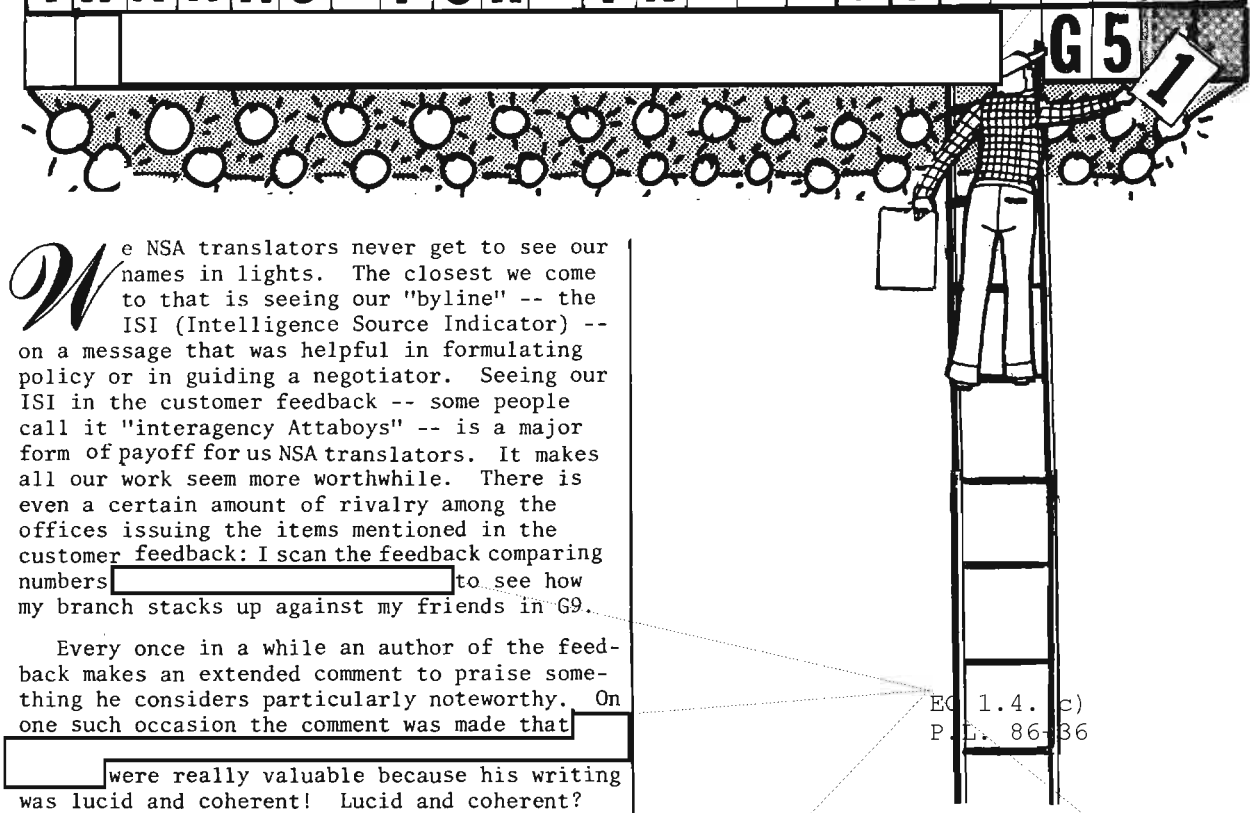
PROGRAM MATRIX	*Resources*	*Activities*	*Goals*
Plan			
Imple-ment			
Evalu-ate			

*J. J. Dempsey and J. A. Grant, "Viewing Program Evaluation as a Component of the Administrative Process: The RAGPIE Model," *Perspectives in Maternal and Child Health, Series B, Program Evaluation.* No. 4, September 1971.

DOCID: 4009806

P.L. 86-36

THANKS FOR THE ATTABOY!



We NSA translators never get to see our names in lights. The closest we come to that is seeing our "byline" -- the ISI (Intelligence Source Indicator) -- on a message that was helpful in formulating policy or in guiding a negotiator. Seeing our ISI in the customer feedback -- some people call it "interagency Attaboys" -- is a major form of payoff for us NSA translators. It makes all our work seem more worthwhile. There is even a certain amount of rivalry among the offices issuing the items mentioned in the customer feedback: I scan the feedback comparing numbers to see how my branch stacks up against my friends in G9.

Every once in a while an author of the feedback makes an extended comment to praise something he considers particularly noteworthy. On one such occasion the comment was made that were really valuable because his writing was lucid and coherent! Lucid and coherent? We had always thought he was just a pain in the neck!

Then it struck me: this comment was at least as much a tribute to the skill of the translators and the checking team I ought to give a brief description of the checking process, since it represents the pinnacle of the Agency's language skill -- checkers are operationally responsible for the Agency's looking good in print.

G51 Checking Process

One very successful, efficient, and productive system for checking translations involves two stages. In the first stage, one person reads the translation aloud while a second person follows along in the original, foreign-language text. Whenever the translation differs from the meaning in the initial text, the second checker interrupts the first and gives a sight translation of that portion of the text. The two people then resolve the differences until both are satisfied. Sometimes the resolution requires considerable delving into dictionaries and glossaries and the use of a thesaurus in both languages. Occasionally it requires brainstorming with other checkers and senior translators. When a decision is finally made, the checkers may record the finding in their glossary for future reference, and resume reading the English translation.

EO 1.4. c)
P.L. 86-36

The second stage of the process is to turn the corrected translation over to a third checker who edits the English Surprisingly, this two-stage process is actually more efficient than having the three checkers work separately, and far more likely to catch errors and accurately represent the intent of the original author. The dialogue between the checkers that the process requires also satisfies the social needs of the checkers and upgrades their job satisfaction. The editing process is so important and demanding that if the Agency ever decides to solve its "language problem" by promoting operational linguists to higher grades, my vote is to promote the checkers first!

Clear to Whom?

Let's return to the business of being lucid. When an author is lucid, his meaning is completely clear. He uses grammatical constructions, figures

of speech, historical and literary allusions, etc. that he knows his reader will be familiar with. But translating a foreign text that is completely clear to the *foreign reader* does not always result in something that is completely obvious to the *English-speaking reader*. It is hard enough for the translator to make the meaning completely clear to *his* reader when a foreign word has no direct one-for-one English synonym -- if a foreign word means either "son-in-law" or "grandson," does the translator flip a coin, or put in one of those footnotes that nontranslators hate, or what? Yes, that's hard enough, but when a metaphor creates an image, the problem is sometimes compounded exponentially because the image itself is unfamiliar to Americans.

[redacted]

Challenging images like these can be exasperating, but the silver lining is that the possibility and unpredictability of their occurrence means that no computer will ever fully take over my job.

[redacted]

The absence of any one of them can leave a translator wishing that the next issue of the *NSA Newsletter* would come so that he could at least spend the government's time solving the puzzle. Since none of the three can be controlled by the translator, there is a constant threat that some change will eliminate the job of even the most skilled and dedicated professional.

EO 1.4.(c)
P.L. 86-36

Perhaps that is why the "interagency Attaboys" are so welcome. Even if people in other agencies do not have a good feel for what it takes for a diplomat to be lucid and coherent, it is very reassuring to know that somebody else values our work.

~~(TSC)~~

~~CONFIDENTIAL - HANDLE VIA COMINT CHANNELS ONLY~~

P.L. 86-36

Never mind what ever happened to Baby Jane, or even to the CAA!

P14 asks: What Ever Happened to COPES?

[redacted]

EO 1.4.(c)
P.L. 86-36

[redacted]

~~(C - CCO)~~

UNCLASSIFIED

EO 1.4.(c)
P.L. 86-36

THE MAN WHO BROKE PURPLE

REVIEWED BY **P. William Filby**

The following review appeared originally in the Baltimore Sunday Sun, October 16, 1977, under the title "Teaching Purple to Talk Saved Thousands." Its author, P. William Filby, is already known to our readers as the author of "Ultra Was Secret Weapon That Helped Defeat Nazis" (CRYPTOLOG, December 1975) and as the husband of CRYPTOLOG SRA Editor, Vera Filby.

Ed.

The Man Who Broke Purple. By Ronald Clark. 271 pages. Little, Brown. $8.95.

By virtue of recent books on cryptography, starting with "The Ultra Secret," British biographer Ronald Clark felt that the story of William Friedman, grand old man of American cryptography, should be told. It was a daunting task because the British law permitting release of certain classified information after 30 years is not matched in the United States. No doubt there were many on both sides of the Atlantic who felt that Wing Commander Winterbotham's story of the breaking of Hitler's command cipher in "The Ultra Secret" was unwise, but since the documents were 30 years old nothing could be done about the publication.

Winterbotham opened up a Pandora's box, and it was not long before we had "Bodyguard of Lies" and "A Man Called Intrepid" -- and now "The Man Who Broke Purple." The chief difficulty with all these authors is that none was actually involved in cipher work and therefore their treatment of cipher breaking is second-hand. Since those who were involved are unable (and unwilling) to assist the writers, errors were unavoidable. These books can be faulted heavily on this score, but since some of Friedman's work is public knowledge through Senate and other hearings at the time of Pearl Harbor, Ronald Clark had masses of information to use, and he make a great effort to interview those who knew Colonel Friedman. The reviewer well remembers a dinner with Mr. Clark, fresh from his triumph as the biographer of Einstein, where it was impossible to fill in any of the gaps vital to the story. But it was possible

to give some insight into Friedman as a person through a friendship which started in November 1942 and continued until his death in 1969.

Readers will be a trifle disappointed if they expect startling disclosures, but the author has done all he could to write of the man -- his many successes, his few failures, and his psychological sufferings and frequent depressions. Because of Russian pogroms, the Friedman family fled to America when William was only 3. Clark tells of his early life with its setbacks, but we find him as a young geneticist at Cornell University and later working for one Colonel Fabyan, who had a team at his Riverbank Laboratories in Illinois attempting to prove that Bacon and not Shakespeare had written the plays. All manner of tests were made on the First Folios and other Shakespearean works, but in 1957 Mr. and Mrs. Friedman exploded the whole theory in a book "The Shakespeare Ciphers Examined." Bill and Elizebeth -- she was also and still is an expert cryptographer -- made fun of all the Shakespeare cipher theories, and in fact with one system developed by a Fabyan worker Bill "proved" that he had himself written the plays.

But if Fabyan was an eccentric, he was nevertheless the cause of the two meeting and forming easily the world's finest husband and wife cryptographic team. While Friedman was with the Army, Elizebeth was with the Navy, Coast Guard and Treasury, both on similar though separate tasks and no doubt similarly successful. Certainly their later collaboration on the Shakespeare book was a brilliant achievement.

When World War II started, the Army Department quickly called upon Friedman to create a team, and through superhuman efforts the Japanese main cipher known as "Purple" was solved and in fact was being read at the time of Pearl Harbor. Purple was the name given to the diplomatic cipher system used by the Japanese Foreign Office for the most secret communications with its ambassadors abroad, and its decipherment makes exciting reading. If the reader wonders why even with Purple the Pearl Harbor defenses were unready he should study Roberta Wohlstetter's "Pearl Harbor" to realize the confusion which existed at that time. The breaking of Purple has been public property for over 30 years. With these records and with the Friedman papers in the George C. Marshall Research Foundation and invaluable help from Elizebeth Friedman, Clark tells a fine story, and even those close to William Friedman for many years will learn facts hitherto unknown to them.

Clark has given a sympathetic and penetrating study of America's outstanding cryptographer (*pace* Major Herbert Yardley and his "American Black Chamber"). Tyros will enjoy the succinct descriptions of the ciphers and their breaking since they are presented in clear, nontechnical language and no doubt were vetted by Elizebeth Friedman.

Unfortunately such men as Friedman are sworn to everlasting secrecy and their fame comes, if ever, after their death. Though he was awarded America's top civilian honors, the reasons could not be spelled out, and in fact the actual ceremonies were generally held out of the reach of the press.

Various writers have averred that the reading of Ultra and Purple and other ciphers actually won the war. There are many who will dispute this, but Clark's book will leave the reader with the certainty that even if the outcome had been the same, victory would have taken much longer to achieve without the knowledge derived from the breaking of the ciphers.

Mr. Filby is director of the Maryland Historical Society; he served in British Intelligence in World War II.

(U)

The following book review appeared originally in the Agency's COMSEC Intern Review, Vol. I, No. 1, September 1976. That publication, which is issued quarterly by the COMSEC Intern Organization, is entirely produced and managed by the interns toward whom it is oriented. In his first editorial, the founding editor, [redacted] *stated that the publication is intended as a "vehicle [of instruction] not only for the interns, but also for those in the larger COMSEC community who care about the principles, techniques, theory, and applications of COMSEC. A primary purpose of the Review, therefore, is to provide an educational tool of general COMSEC interest." For further information about the COMSEC Intern Review, call the current editor,* [redacted] *1LT USA; S02, x2445s.*

Ed.

A.C. Brown's "BODYGUARD OF LIES"

REVIEWED BY [redacted] S02

Bodyguard of Lies is called "the most important work on World War II in a quarter century" by the Army historian Charles B. MacDonald. It is a master work on strategic thinking and planning and it will surely become a recognized classic on the art of stratagem. No less than Barton Whaley, that other master of stratagem, author Anthony Cave Brown demonstrates decisively that static security measures contribute little to effective protection. Where Whaley consciously and statistically

points to this conclusion, Brown achieves more by an organized recounting of events, plans, and programs.

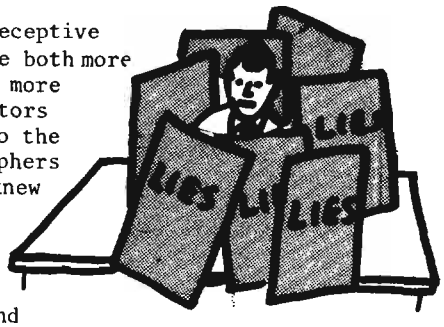
Besides the elaborate orchestrations of BODYGUARD and FORTITUDE, the operations and programs surrounding El Alamein are of particular interest to the COMSEC strategist and tactician. As is ever the case, the COMSEC lesson was only learned after a series of staggering military reverses, and then only after the capture of a German "wireless intelligence post." When the sources of Rommel's "brilliance" were demonstrated to be poor American and British radio security, the Allies at last reacted with swiftness and imagination. Cryptosystems were both changed and used for deception. "New disciplines were imposed for the use of radio telephones, call signs, cryptographic procedures, voice codes, wireless silences for units on the move. . . The British formed new companies to monitor the security procedures of their own troops and severe disciplinary action was taken against offenders." One of the greatest COMSEC actions against Rommel, however, was the destruction by the British of his entire experienced radio intercept organization. The new inexperienced organization was "very vulnerable to wireless deception." Not only did the British exploit this weakness by Manipulative Communications Deception (MCD), but they also reconstituted a captured German espionage net and used this fiction to pass deceptive intelligence to Rommel. All the fabrications were carefully supported by camouflage feints and leaks of material. With a fine eye for essential detail Brown relates how the "Desert Fox" was systematically turned into a dunce and carefully maneuvered into a trap.

A large portion of the book is devoted to COMSEC -- practices, systems, successes, and failures. The authoritative voice of Ultra is consistently heard throughout the work. It is the final authority on all German plans, beliefs, and intentions. This constant unfailing source of intelligence brings the weighty and cumulative conviction that this COMSEC disaster was one of the primary causes of Germany's downfall.

In sharp contrast to this strategic failure of COMSEC is the painstaking use by the British of a one-time pad to transmit the whole BODYGUARD plan, a mile long, to Moscow.

While Brown does not blanch at revealing many of the subtleties of Allied deceptive practices, he does not give cryptographic system details to any substantial degree in the methods by which cryptographic systems were broken. Some measure of this book's concern with COMSEC is indicated on page 912 in the index, where more than a full column is devoted to codes/ciphers and cryptanalysis.

One of the most fascinating chapters of the book is entitled the "Wireless Game." As D-Day approached, deceptive gambles became both more elaborate and more risky. Operators were sent into the field with ciphers "the British knew the Germans would be able to decrypt." The British would then send "normal" traffic to their operators and thereby feed the Germans deceptive information. Sometimes this program compromised numbers of agents. Brown pursues this labyrinthine aspect of stratagem. He scrutinizes its effectiveness, raises the ethical considerations, pursues the official inquiries and their muddied conclusions. The human difficulties with such operations are painfully illustrated. The decisions were made indeed, but were they as ruthless in their use of human life as some thought? He gives the benefit of doubt if such is warranted. In all he shows that men did not risk other men's lives lightly. Whether it was Churchill's decision about alerting Coventry and sacrificing ULTRA or SOE's game with Princess Khan, the ends did not easily justify the means.



In summary, *Bodyguard of Lies* is often carefully researched and entertainingly written. It is a monumental and unforgettable volume. It contains both conceptual strategic sweep and finely chosen detail. The subjects of strategy, stratagem, and COMSEC are treated in a balanced and integrated manner. It is a necessary volume for the serious COMSEC professional.

(U)

(U)

DOCID: 4009806

NSA-crostic No. 11

by guest NSA-crostician
David H. Williams

The quotation on the next page was taken from the published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS	*WORDS*
A. U.S. state capital (2 wds)	198 204 7 150 175 59 69
B. Testify	83 74 17 93 173 37
C. "--- Angeles"	136 91 103
D. Avid	40 99 143 26 43
E. Prepare potatoes; popular TV program	14 197 86 28
F. See Word L	147 206 195 76 129 96
G. Glowing coal	19 187 167 29 70
H. Laugh nervously	124 157 1 97 88 5
I. First pocket watch (ca. 1500) -- "Nuremberg ---"	3 52 200
J. "Point ----------"	190 152 148 172 27 105 186 214 12 130 64 94
K. Pester	145 53 71 127 48
L. Followed by Word F, Word A's state	192 166 113
M. Pertaining to a stomach ailment	24 183 107 137 179 194 131 181 110 155 32
N. Character in A. A. Milne's books (2 wds)	33 139 66 50 81 4 118 89 211 132 57 104 185 202 177 25
O. Star (prefix)	142 95 45 216 125
P. Second line of Burma-Shave jingle beginning "You know your onions..." (2 wds)	116 203 11 176 165 117 72 138 15 30 39 41 80 21
Q. Third line of jingle (4 wds)	205 98 82 141 87 67 36 60 163 169 101 215 23 85 115 9
R. Mutually existing, shared	207 128 56 108 213 13 121 210 188 174
S. Selected at random and without reason	6 170 61 114 90 31 58 22 168
T. (What the Hindu holy man saw after standing on his head for 20 years ("a ------")	119 44 182 164 63 92

DOCID: 4009806

U. Last line of jingle (5 wds)

V. Swiss adventurer who "initiated Peter the Great into the pleasures of debauchery and became his best friend"

W. Fix

X. Miserly

Y. Set aflame

Z. Extemporaneous

Z_1. David Brinkley

8 191 73 111 178 196 20 79 55 51 34 126 38

212 140 122 134 156 16 199

189 133 42 75 47 159

171 78 209 46 151 201 62

109 162 135 160 100 68 54 35 193 144 18

102 65 77 180 153 161

208 184 120 2 10 112 158

106 146 49 149 123 154 84

1 H	2 Z	3 I		4 N	5 H	6 S	7 A	8 U	9 Q	10 Z	11 P	12 J	13 R		14 E
15 P	16 U	17 B		18 X	19 G	20 U	21 P	22 S	23 Q	24 M	25 N	26 D		27 J	28 E
29 G		30 P	31 S	32 M	33 N	34 U	35 X	36 Q		37 B	38 U	39 P	40 D		41 P
42 V		43 D	44 T	45 O	46 W	47 V	48 K	—	49 Z_1	50 N	51 U	52 I		53 K	54 X
55 U	56 R	57 N	58 S	59 A	60 Q		61 S	62 W	63 T	64 J	65 Y		66 N	67 Q	68 X
69 A	70 G	71 K	72 P	73 U		74 B	75 V		76 F	77 Y		78 W	79 U	80 P	81 N
82 Q	83 B	84 Z_1		85 Q	86 E		87 Q	88 H	89 N	90 S	91 C	92 T	93 B	94 J	
95 O	96 F		97 H	98 Q	99 D	100 X		101 Q	102 Y	103 C		104 N	105 J	106 Z_1	107 M
108 R	109 X	110 M	111 U	112 Z		113 L	114 S	115 Q	116 P		117 P	118 N	119 T	120 Z	121 R
122 U	123 Z_1		124 H	125 O		126 U	127 K	128 R	129 F	130 J	131 M	132 N		133 V	134 U
135 X	136 C	137 M	138 P	139 N		140 U	141 Q	142 O	143 D	144 X		145 K	146 Z_1		147 F
148 J	149 Z_1	150 A		151 W	152 J	153 Y		154 Z_1	155 M	156 U	157 H	158 Z		159 V	160 X
161 Y		162 X	163 Q	164 T	165 P	166 L		167 G	168 S		169 Q	170 S	171 W	172 J	173 B
174 R	175 A	176 P	177 N	178 U	179 M		180 Y	181 M		182 T	183 M		184 Z	185 N	186 J
187 G	188 R	189 V		190 J	191 U	192 L	193 X	194 M	195 F	196 U		197 E	198 A		199 U
200 I	201 W	202 N	203 P	204 A	205 Q	206 F	207 R		208 Z	209 W		210 R	211 N	212 U	213 R
214 J	215 Q	216 O													D.H.W.

(Solution next month)

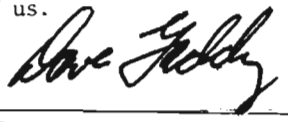
[redacted] C.A.A. NEWS [redacted]

President's Letter

CAA is on the move again, energized by the deepfelt concern of its membership -- including new members, who saw in the Association the potential to meet a real need. "Professional growth" has been the objective since our by-laws were first adopted. It should be a personal objective for each of us. Under [redacted] inspired leadership this past year, the Association continued the attempt to realize that objective. Why CAA? Because, of the various groupings and mechanisms available to us, CAA is pan-discipline in its orientation. (Even collectors, who wanted a home of their own and are off to a great start with Bill Hunt and the newly formed Collection Association, continue to have a role in CAA.)

Tom has given us a vision and a challenge. As incoming President, my aim will be to further the accomplishments of this past year. Extend an invitation to your coworkers to join with us. Make a special effort to enlist professionally motivated military specialists. Attend our open Board meetings -- make your views known and lend us your support. Promote the CAA. Help us to continue our contacts with our people in field service.

An alma mater of fond memory adopted some years ago a slogan which I'd like to borrow for CAA: "Emphasis on Excellence." Let's keep that thought in front of us.



Hurry, hurry, hurry!

(A few choice memberships still available!)

In the past few issues of CRYPTOLOG, [redacted] provided the CRYPTOLOG reader with some incisive, and often witty, perspectives into the "new" Communications Analysis Association (CAA) and the underlying philosophy that governs it.

But what exactly is the CAA? The CAA was established to promote professional growth and outstanding accomplishments in the career fields involved in communications analysis, e.g. traffic analysis (TA), special research (SR), signals collections, cryptanalysis (CA), and communications security (COMSEC). Using its interdisciplinary membership, the CAA would promote active dialogue or an exchange of ideas in an effort to stimulate the U.S. cryptologic community with new concepts in the application of communications analysis to cryptologic problems. Such an exchange of ideas is manifested in the fine lecture series sponsored by the CAA, e. g., Whitney Reed's [redacted] The CAA also sponsors technical briefings for smaller audiences and special interest groups.

Equally important to the CAA, however, is the contribution it can make to *your* professional development. The CAA is not only interested in those who have been professionalized but also those who aspire for professionalization in the career fields mentioned above. In an effort to augment existing structures within NSA, the CAA is working on an approach to "career development" for both categories of members. For the aspirant, we hope to draw on our most important asset -- our cadre of experienced, knowledgeable individuals within each discipline. We feel strongly about helping aspirants toward career professionalization. This help could be in the form of work/study groups prior to PQEs (what to look for, etc.) or more individualized tutoring, etc. For the professional, the CAA is currently thinking about and talking (with M and others) about a post-professionalization program. We envision a program that would encourage professionalized individuals to broaden themselves so that they could function more effectively within an interdisciplinary environment. Such a program could include NCS courses, university-level courses, and special training that would provide the opportunity to achieve this broad, interdisciplinary perspective.

P.L. 86-36

So, you see, the CAA is concerned about you and can provide something for you in the form of its stimulating lecture series, its special interest groups, and its real concern for your "career development program." All the CAA wants in return is to have as members concerned, dedicated individuals like yourself.

So how about it? Why not join the CAA today? Call any of the following individuals for an application form or for more information:

David Gaddy, President, 3247s

[redacted]

P.L. 86-36

[redacted]
Chairman, Membership Committee
~~(C)~~

New, new, new!

A Special Interest Group on Cryptologic History. [redacted] (4087s) is the organizer of this group, which will have had its first organizing meeting by the time you read this. If you missed that meeting, but are interested, call Bill for the latest on this new SIG.

Logo Contest

For information, see page 7.

DOCID: 4009806

The Editor's Page: THE JOYS AND FRUSTRATIONS OF PLURAL-DROPPING By A.J.S.

One of the easier chores of the CRYPTOLOG editor is making minor changes in the text automatically, changing, for example, "this phenomena is" to "this phenomenon is." Or changing "these antennae are" to "these antennas are."

Sometimes the original author doesn't like the change, and if, for example, he or she doesn't like my version, "these media are," we usually come to a compromise. A few months ago I automatically changed the statement "you may find these data in technical reports" to "you may find this data in technical reports." After checking the proof sheets, the author[2] told me, "I've been insisting for years that 'data' is plural, and if you print it this way, it will look as though I've finally knuckled under." So, what the heck, I changed it back to "these data," and that's how it appeared in print. (Did anyone notice, one way or the other?)

The following article, written soon after the unveiling of the mosaic NSA seal in 1968, has been awaiting the proper publication moment since then. Having recently corrected the straw that broke the editor's back, I now ordain that that moment has come.

The article contains a couple of references to since-departed Beautiful People, and at first I thought of updating the references. But then I decided that that would be a form of tampering similar to the kind that ruins old songs, as when Pearl Bailey sings, "A-washin' an' a-scrubbin' don't make me look like no movie star!" instead of "Don't make me look like no Hedy Lamarr!" Why don't we just assume that everyone knows who Hedy, and Ari, and Maria are?

Some people enjoy name-dropping, saying things like "When I was on Ari's yacht a couple of years ago, I thought Maria looked a bit peevish." Others enjoy placename-dropping. "If you think that *this* is deep snow," they say, "you should have seen the snow in Garmisch-Partenkirchen the year of the big snowslide on the Zugspitze." Still others -- it takes all kinds -- prefer plural-dropping. The plural-dropper looks up from what he is reading -- perhaps the newspaper, the *NSA Newsletter*, or an important, or at least important-looking, report -- and says, "Oh?" Having attracted the attention of those around him, he reads a phrase from the text, preferably in a colorless tone that disguises what's biting him. One of those in earshot asks, say, "What's wrong with 'This is the most important media of expression'?" The plural-dropper says simply, "Well, 'media' is plural -- 'medium' is the singular, remember?" Then he shuts up, while the others get into an emotional discussion bringing in everything from whether to say "None of them is" or "None of them are" to completely ad-hominen (fancy way of saying "Your-mother-wears-army-boots") remarks such as, "Well, maybe in your part of the country they say that, but in cultivated English we don't usually say it that way."

Well, today, I -- or, rather, a certain plural-dropper I know -- was able to read aloud one sentence from the *NSA Newsletter*, and get two with one blow. "Byzantine smalti," the sentence read, "considered the king of mosaics, is still being used to decorate modern building facades, and the NSA insignia was made with smalti in much the same way that mosaics were made when Michelangelo was painting the Sistine Chapel." "What's wrong with that?" came the nibble, "they probably don't have a cedilla to put under the 'c' in 'facades.'" "No, I was referring to 'smalti' -- pieces of glass used in making mosaics -- that's plural. 'Smalto' is the singular, remember? And, oh, by the way, 'insignia' is a plural word meaning the distinguishing signs. 'Insigne' is the singular, remember?" Then, since I have been convinced that everything happens in threes, I began to read each and every item in the *Newsletter*, looking for the third boo-boo involving singular or plural number. Twelve pages later, I found it. The item on the Fort Meade nursery said that "Parents may leave their offsprings for periods of an hour or more. Is it conceivable that someone does not know that, while "bedspring" has a plural, as in "People may leave their bedsprings to be retied," "offspring" in the sense of "progeny" is singular and collective?

Elated or not, any plural-dropper who finds three examples in a single publication is morally obligated to write an article on the problems of handling singular and plural nouns in English. Even if, ignoring the current NSA trend of using a cute title to signify a discussion of a complex and potentially dull topic, he decides not to call it "Are It Singular or Are It Plural?", he still has to mention a couple of linguistic facts of life.

[1] Well, maybe a wee bit more than a page!

[2] I have deliberately used the words "the author" instead of the appropriate "he" or she," in order to protect the author's identity. Norma would kill me otherwise.

DOCID: 4009806

One such fact is that there's no logical reason why English, or any other language, or any old speaker, for that matter, thinks of something as being singular or collective, rather than plural. In English we say, "Her hair is blond," but in French, German, and Russian they say "Her hairs (*cheveux, Haare, volosy*) are blond" -- dumb foreigners! Scissors are plural in English (except when people refer to "a scissor," obviously thinking of it/them as a single gadget), French (*ciseaux*), and Russian (*nozhnitsy*), but singular in German (*Schere*). Eyeglasses? Plural in Russian (*ochki*), but singular in French (*binocle*) and German (*Brille*). And ink is plural in Russian (*chernila*)!

So, if there is no logical reason why some things are thought of, in various languages, as being singular or plural, are we surprised that American kids, talking everyday English, sometimes use "wrong" forms? But are they "wrong"? Actually, sentences like "Jimmy and me's going to the movies" make perfect sense to one-half of an inseparable pair of pals. It isn't until many years later that some mean old English teacher splits up the pair by putting the two halves on opposite sides of the room and makes them say dumb (that is, "correct") things like "Jimmy and I -- or, better yet, *James* and I -- are going to the movies -- or, better yet, motion-picture theater." Teachers like this have convinced so many kids that there's something nasty about saying "Jimmy and me is" that, to this day, we hear and read statements like "I want to thank you gentlemen for taking the trouble to come to the airport to meet Mrs. Smith and I in this terrible weather." (A gracious statement, but, goodness gracious, the grammar!) They have also given a lot of people the idea that there's no difference between "no one" (as in "No one is perfect") and "none" (as in "None of us are perfect"). Why, anyone can see and hear that they're different and that "no one" is singular and "none" is plural (except when it's singular).

Or are we surprised that American kids also make mistakes recognizing plural suffixes? Perhaps the boy who showed the remains of his broken yo-yo and called it "a yo" was make-believe (it sounds just like Dennis the Menace and therefore is suspect). But I can attest to two real incidents from my own experience. When our daughter and a friend of hers were both five and were eating lunch together at our house, my wife gave them each a sandwich (cut in quarters -- without crusts, naturally), carrot sticks, and a slice of American cheese cut in strips. The little friend particularly liked the latter and asked what they were (must have been culturally deprived). "Cheese," she was told. Well, then, she asked, "May I have another chee?" (Culturally deprived, but talked polite.) Another ordinary English noun suffix tricked a nephew of mine when he was about four, many moons ago when we all went on a family picnic that included the girl destined to become his Aunt Gerry. Pointing to a plate of cherries, he asked his mother, "Can I have one of those things?" (Another one culturally deprived!) His mother said, "They're Gerry's." He said, "Well, then, can I have one of those gerries?"

Impossible, you say? Then how to you explain that the very word "cherry" itself is a mistake? When the Normans introduced the fruit to the Anglo-Saxons, the singular noun "cherise" (modern French "cerise"), meaning "one of them little red things," was misunderstood as "a lot of them little red things," since the last consonant sounded an awful lot like a plural English ending. Well, it's too late to do anything about it now. So don't go around saying, "Some joker says that we're supposed to say 'These cherrieses taste sour.'"

And look at the language now! It has words from all kinds of languages in it -- Latin, Greek, French, Russian, Italian, Indonesian. How are we supposed to know what the words really meant in the original language? Ah, that's where the plural-dropper comes in! Just as there is always a Greek expert waiting for someone to say "the hoi polloi" so that he can explain that "hoi polloi" means "the people" and, thus, "the hoi polloi" means "the the people," there are all kinds of experts telling good, solid, tax-payin' Amurricans what to do with Latin and Greek nouns in English. "You can't say 'This data seems to be correct' -- 'data' is a plural noun in Latin. Singular is 'datum,' remember?" You can argue yourself blue in the face that "data" seems to behave in two different ways. When the word means specific, isolated items of information, in scientific context, it wants to be plural: "The basic data are pressure, temperature, and humidity." But when it is used in a collective sense as a body of information, it wants to be singular: "This data was furnished by the Mayor's office." A lot of people, having talked themselves blue in the face, will avoid the issue and just say "This information was furnished by the Mayor's office." But if there is, somewhere in this country, someone who wants to fight it out to the death, like a mongoose and a cobra, here's a fact he can use: English has other nouns which, although plural in Latin, are singular in English, dammit, and nothing *but* singular. Even people who know that "opera" is the plural of "opus" do not say, "My favorite opera are 'Carmen.'" Nor do they say, "the agenda have been approved."

But there are still a few people who learned all that Latin and they're not going to let us forget it. So they write personnel regulations concerning "annual-leave maxima" ("What's the matter, 'maximums' isn't good enough for them?"). And they carefully write "these media, these

theses, these bases." Sometimes their readers figure out that those words are the plural forms of "medium, thesis, basis." Sometimes they don't. Sometimes the careful writers themselves get so careful about their pronunciation that they carry it to the point of referring to "air bases" [pronounced "base-ease"] in Western Europe." Sometimes careless readers and careless listeners pick up a catchy word but botch the ending ("This is an important media of communication," or "These are important medias of communication"). Who's going to straighten out all these bums (or is it "ba")? Why, the plural-dropper!

Formal written English being what it is, the reading plural-dropper usually pounces on a Latin word. Only an infrequent Greek boner like "this phenomena" will catch his eye. The best that he can hope for in a conversational environment is to insinuate the word "stigma" into the discussion, and wait for his partner to feed back the plural "stigmas," affording him a chance to ask, "Stigmas? Oh, I guess you mean 'stigmata?'"

As for the nonclassical languages, they are rarely encountered in contexts where one can amass a considerable number of oneupmanship points. What is he supposed to do? Tell his hostess, "These spaghetti are delicious -- 'spaghetto' is the singular of a diminutive of the noun 'spago.'" Or tell a wedding guest on the church steps after the young couple has driven away, "You have a confetto stuck onto your cheek -- 'confetti' is a plural form, you know." Or is he supposed to point to the sign on the cafeteria counter that reads "Lasagna - 70 cents" and ask the server, "Certainly that can't be right? 'Lasagna' is the Italian word meaning '*a* noodle.' Certainly we get more than '*a*' noodle for 70 cents? Is it conceivable that it's a misspelling for 'lasagne,' the proper plural form?" What's he supposed to do when he sees a recipe in the newspaper for "pirozhki" that -- in addition to leaving out the mushrooms! -- says, "Each *pirozhki* should be bite-size"? Should he write a nasty letter to the editor, signing it Paul E. Glott or some other silly name, and say, "Anyone with a modicum of knowledge of Russian haute cuisine should be aware of the fact that the singular of 'pirozhki' is 'pirozhok.'"

Certainly he's supposed to do none of these things. He's supposed to *avoid the issue*, like a chicken mongoose. (Not a mongoose that eats chickens -- they're brave -- but a mongoose who won't fight a cobra -- they're chicken!) He's supposed to smile understandingly at other people's mistakes and make sure that when he uses such words himself, they can be interpreted either in the singular or the plural. He would, in a *Newsletter* item, for example, say, "Smalti can be used in such-and-such a way," rather than "Smalti is used" or "Smalti are used." In effect, he ideally should write just like the zoo owner ordering two mongooses. "'Please send me two mongooses.' No, strike that out -- make it 'two mongeese.' No, strike *that* out. Make it, 'Please send me one mongoose as soon as possible. And, oh, by the way, while you're at it, send me another one."

(U)

Letter to the Editor

To the Editor, CRYPTOLOG:

In reply to [redacted] article, "Whither the SRA?" (CRYPTOLOG, September 1977), I would like to say that some of my best friends were SRAs (whatever *that* is)! Back in the PCP days (pre-career panel), the relationship between TA and IRA (as it was then called) was quite clear: if you were below a certain grade (I think it was GS-9), you were TA, and if you were above that grade, you were IRA. We thought of IRA as professional (with a small p) and TA as preprofessional and that was the way the job auditors titled the jobs. Then one day the career panels were formed, and when the dust cleared, behold -- TA and IRA were two separate fields!

We (in that early TACP) studied the situation at great length and found, among other things, that it was then standard practice for job auditors to classify a job as IRA if the incumbent produced *any* reports and TA if he or she didn't. As I recall, we did not care for that at all, since it was our view that *all* traffic analysis efforts should be aimed ultimately at the production of results in writing, i.e., reports. And, after some negotiation, the job auditors' guidelines were adjusted.

Last, but clearly not least, the two career panels were directed to investigate the problem of "defining the boundary line" between them. After some 6 months of discussion, it was concluded that the boundary was indeed a problem. What we finally committed to paper said, in effect, that at one end of the spectrum there were jobs that were clearly TA, and at the other end there were easily recognizable IRA jobs, but that all along the line between those two extremes there was overlap between the two fields.

My own view is that reporting (to consumers) can be a very specialized business and undoubtedly is a cryptologic skill but it is really more of an *overlay* skill, like supervision. The field seems to have drawn most of its people from the language and traffic analysis fields (many of the better reporters I've known began either as a linguist or as a traffic analyst).

Finally, what traffic analysis is all about is producing intelligence -- by reconstructing the network, by recovering the signal plan, by watching the target day after day to see what it is doing and how today's behavior differs from yesterday's.

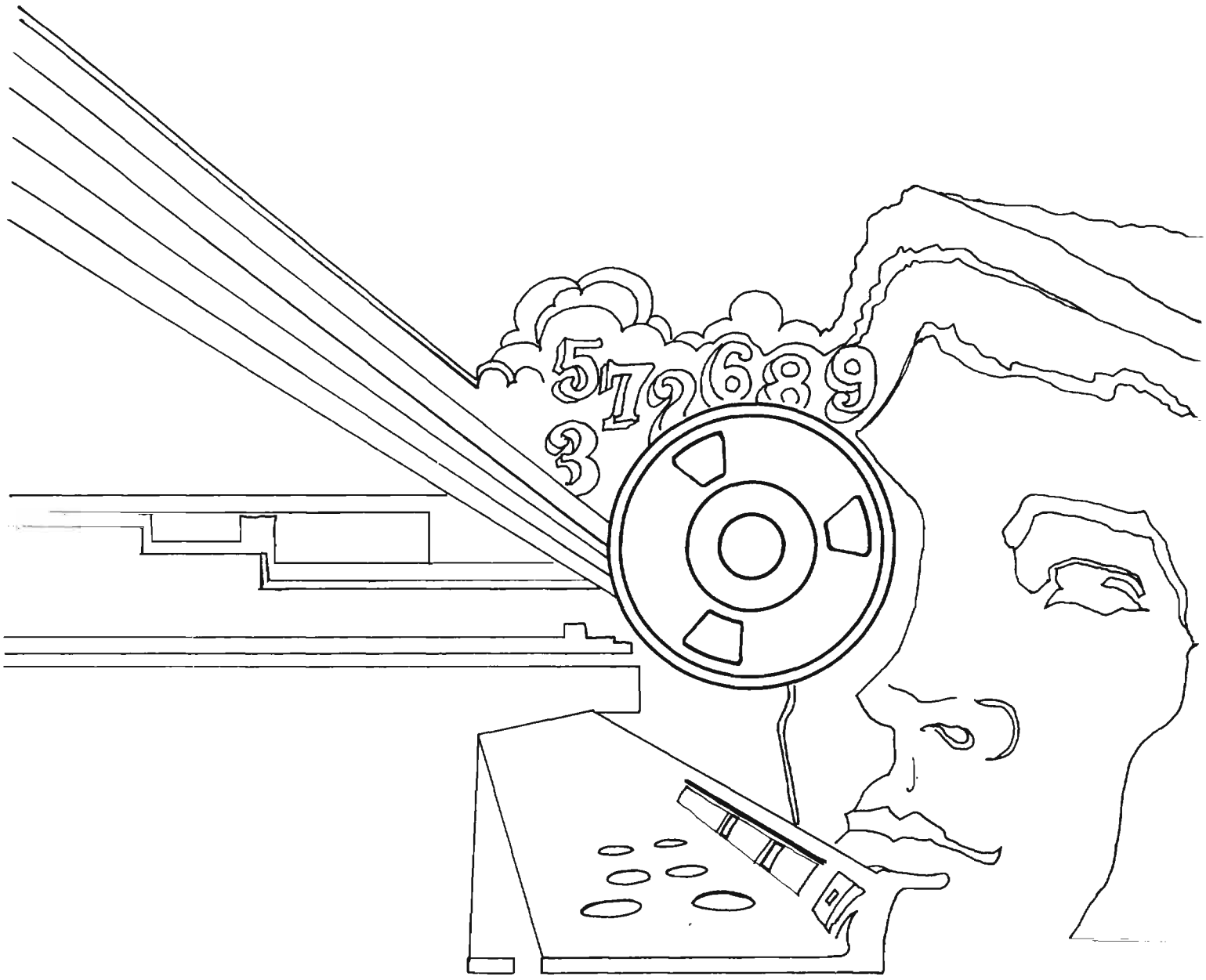
[redacted] Chief, Traffic Analysis
Office of Techniques and Standards (U)

P1-DEC 77-S3-26140

P.L. 86-36

UNCLASSIFIED

~~TOP SECRET~~



DOCID: 4009805

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

DECEMBER 1977

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

[redacted].....[redacted].....1
CONVERSATION WITH A MICROGRAPHICS PIONEER...Don Wigglesworth.....4
WHAT MADE THEM DO IT?.....[redacted].....5
C.A.A. MESSAGE AND NEWS.....[redacted].....9
[redacted].....[redacted].....10
WHAT IS PATTERN RECOGNITION?.....[redacted].....15
LETTER TO THE EDITOR.....[redacted].....16
1977 CRYPTOLOG INDEX.....17

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526,MDR Case # 54778

DOCID: 4009805

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. IV, NO. 12 DECEMBER 1977

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5236s)

Collection.....[redacted] (8955s)

Cryptanalysis.....[redacted] (4902s)

Language.....[redacted] (5236s)

Machine Support.....[redacted] (5303s)

Mathematics.....Reed Dawson (3957s)

Special Research.....Vera Filby (7119s)

Traffic Analysis.....[redacted] (4477s)

Production Manager.....Harry Goff (4998s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

EO 1.4.(c)
P.L. 86-36

DOCID: 4009805

[redacted]

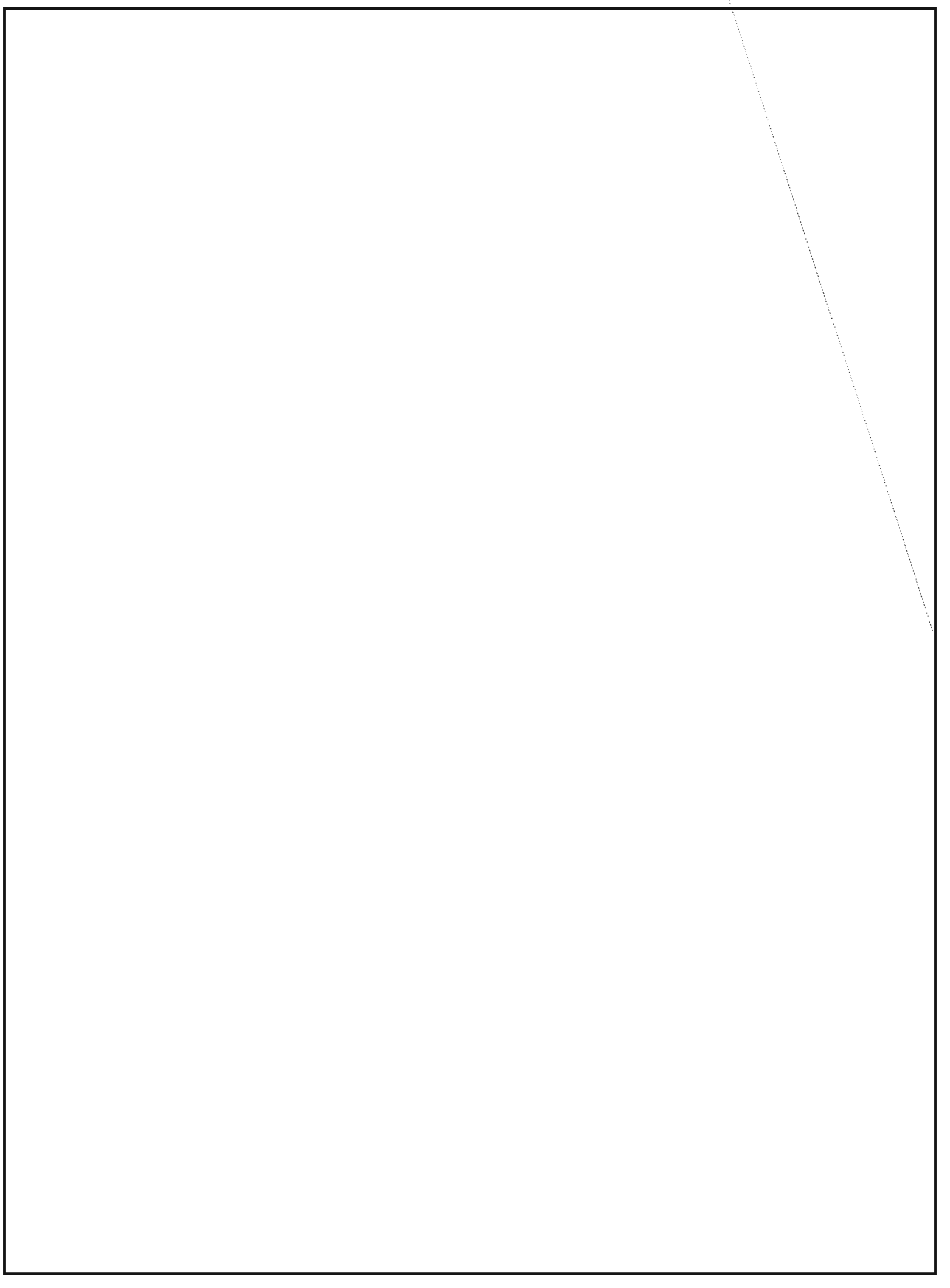
[redacted] G422 P.L. 86-36

t

[redacted]

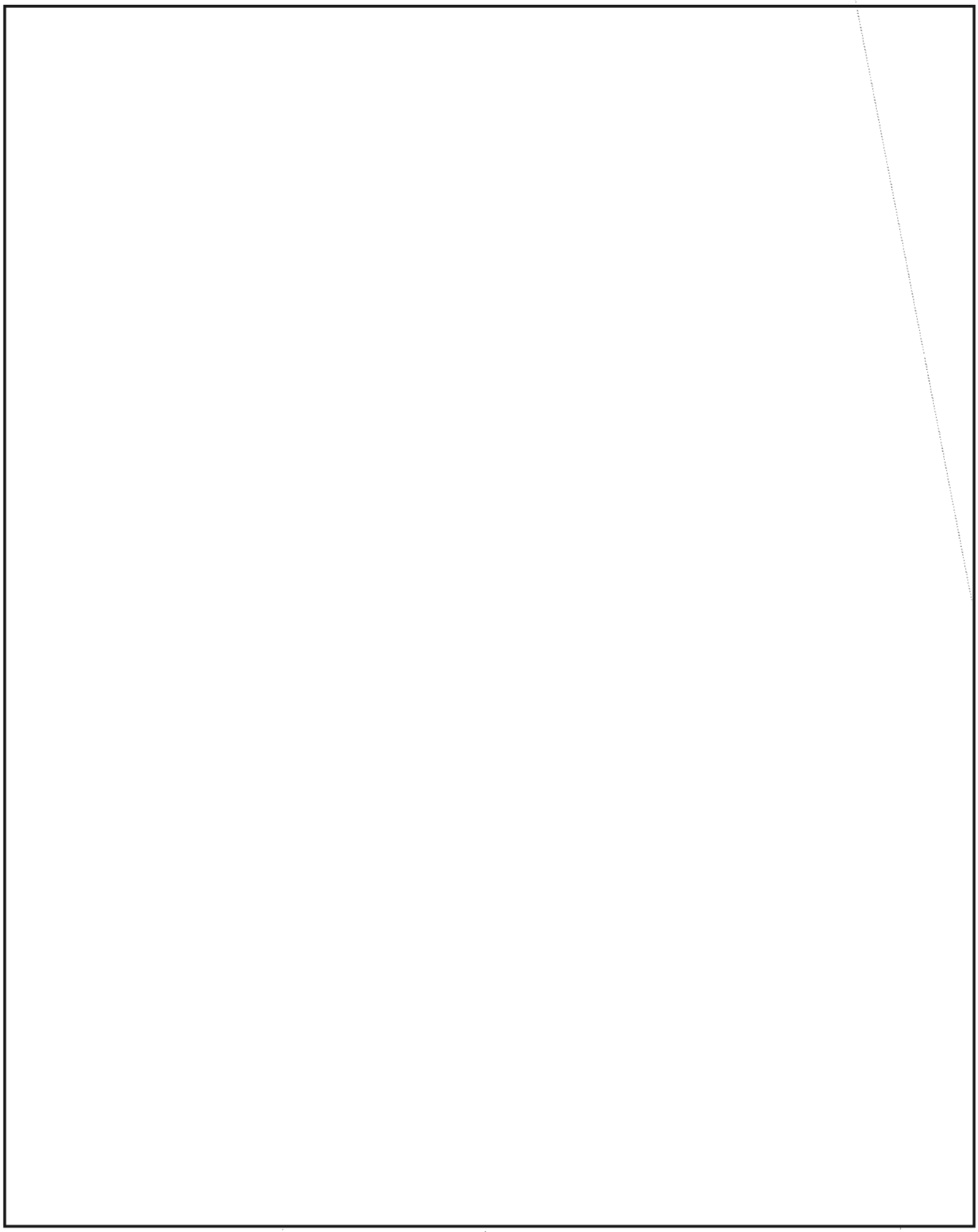
EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



DOCID: 4009805

EO 1.4.(c)
P.L. 86-36



DOCID: 4009805

CONVERSATION WITH A MICROGRAPHICS PIONEER

Don Wigglesworth, N33

One frigid day last January the Federal Government Micrographics Council (FGMC) sponsored an "Introduction to Micrographics" program at the National Archives Theater at 19th and Pennsylvania. As the host, representing the FGMC, I had the job of introducing the speaker, Mr. Richard W. Batchelder, and, later, accompanying him to lunch.

In the course of our pleasant conversation during a much too heavy meal, I learned that Mr. Batchelder had spent the better part of his life in some phase of micrographics development both in the government and in private industry. Even though retired, he still participates from time to time in promoting this long-used information medium (it was first used for intelligence purposes in the Franco-Prussian War of 1870). But what particularly interested me was that I was talking to one who actually participated in the R&D of an information system which was of great intelligence value during WW II and which we at NSA still depend upon for information management and fast retrieval. Further, Mr. Batchelder's efforts during WW II took place only a floor or two above the theater in the Archives Building in which that day's program was unfolding.

The story is a repeat of the axiom "Necessity is the mother of invention." The "necessity" in this case was a requirement for a photographic data file on enemy countries that was critically needed for military operational purposes: pictures of geographical details, bridges, factories, rail yards, seaport facilities, the whole bit. Lacking Congressional appropriations for significant intelligence efforts during the pacifistic 1930s, the United States was at a disadvantage came the Pearl Harbor attack. U.S. intelligence services had only months to accomplish what the enemy had developed over the previous decade. "Wild Bill" Donovan's OSS was conceived to help do some fast catching up.

The OSS task included a crash effort to meet this particular need and this job was assigned to the Pictorial Records Division of OSS. In the summer of 1942 Mr. John F. Langan was made chief of this division and told to get on with the monumental task.

To establish a pictorial data base of sites of potential military importance, Langan issued a call to various government components and to Americans in general to send him photographs of any place in an enemy or enemy-occupied country. And, as you would expect, Americans responded with gusto. Langan was inundated with about a half a million pictures of, say, Aunt Suzie standing on the Remagen Bridge, or Cousin Chester at the docks at St. Nazaire, or Grandma enjoying the view from a dike on the Zuider Zee. Langan's staff had these photos stacked all over the place in the Archives Building while they were being sorted -- wheat from the chaff, that is. From the pile of 500,000 pictures they selected about 100,000 considered useful. But that was still a good pile to index and effectively access and constantly update as OSS agents began to send in new photos and as the daily demands of the intelligence consumers increased. As time passed, the demands on the hand system reached some 250,000 photos to be processed each month. The manual system simply couldn't hack it. Pure and simple, the problem was how to add to, subtract from, and sort the pictures on a timely basis.

Before the war Langan had been working on developing a better system to file and retrieve stock films for the movie industry. To solve the critical problem in the OSS Pictorial Records Division, he drew on his earlier efforts by experimenting with the possibility of using a tabulating card. The idea was to cut a rectangular hole in a free area of the card and to mount a microfilm of one photo in the hole. My lunch colleague, Mr. Batchelder, was assigned the then very difficult and tedious task of hand-cutting the rectangles in the Hollerith cards and trying to mount the microfilm in the "aperture." The real test came when they tried to run the cards through the sorter -- crossing their fingers that the cards wouldn't jam. But they did, regardless of the adhesive used to hold the film in place. One day, while in the basement of the Archives Building, Langan noted some sheets of plastic adhesive which was used for document preservation. He had this adhesive used to secure the film in the aperture and again the cards were tested in the sorter. And they shuffled quite nicely, thank you.

Langan also developed the machine-coding system to be punched in the card to permit sorting the micro photos by, say, longitude, latitude, geographic location, etc. With the help of the at first nonbelieving crowd from Endicott (they shuffled a bunch of Mr. Batchelder's handmade aperture cards in their own sorters before they would believe the idea would work), a massive effort was started to microfilm the thousands of photographs, to hand-mount them to the tabulating cards, and to index the cards via keypunch. By 1943 the first "aperture card" system was in operation in OSS. By a fast sorting of the cards, photos of a potential landing site in southern France, or a river crossing on the Rhine, or a rail yard at Dresden could be retrieved from the pile without waiting weeks or months for the pictures to be located.

Langan's cards with Mr. Batchelder's apertures are still with us and still effectively serving data needs in the intelligence business.

If it wasn't the devil, WHAT MADE THEM DO IT?

(Study languages on their own, that is?)

P.L. 86-36

CRYPTOLOG's language editor, [redacted] asked four of the Agency's recognized multilinguists to talk about their experiences in studying foreign languages on their own. [redacted] John D. Murphy, and [redacted] all of P16, met with him and the following article is the result of their discussions.

What foreign languages have you studied on your own? Why did you select these languages?

[redacted] It's hard to remember which I've done myself and which I had in courses. I was in a graduate course at NYU where you got an entire family of languages at once. That gave me the background, as a matter of fact, for all the self-study I've done since. Of the 38 ancient and modern languages that I claim at least a reading and translation capability in, I'd guess that I've done half on my own and the other half with instruction of some sort.

Murphy: That's a difficult question. I've studied many languages, but a large number of those only in a casual way. But with intensity perhaps you might say Luganda, Albanian, Thai, Burmese, Bengali, Tamil, and Romanian.

[redacted] I'll try to stick just to those languages that I did learn on my own. I began with classical Greek when I was about 9 or 10. I switched to Russian by the time I got to prep school, because that was the thing to do. After Russian -- really simultaneously with Russian -- I took a crack at Japanese. I got to the point where I could actually do some reading in all of those, but I was hardly fluent in any of them.

Later on, upon my arrival at NSA, I studied languages for a different purpose. The first one I studied solely on my own was Indonesian. I am mainly self-taught in Czech and Turkish as well.

[redacted] The only one that I've done from scratch up through passing the PQE is Hungarian. I've done a lot of self-study in Russian, but that was after some formal classes at the beginning. Recently I've started looking at some books on Arabic and Chinese.

Is it important that you pick the language, i.e., from a psychological point of view is it better for self-study purposes that the language not be one someone told you to do?

Murphy: Even a language nut or language buff does not have an interest in certain languages. Sometimes you're told this is the language you are going to study. I have an aversion to neo-Indic languages like Bengali. But I was told that that was what I was going to do. So you construct an interest, you fake an interest for that period.

But some languages are more interesting than others. Everybody has a favorite. I like the highly agglutinated languages.

[redacted] I don't care for Persian at all.

[redacted] If there's one thing I have no desire to even look at, it's Korean. But I really like Hungarian. I think I'd like Turkish. I think enthusiasm is especially important for self-study.

[redacted] I've been lucky in that I've never yet encountered a language that I was completely unwilling to learn. But certainly I agree that some are a lot more interesting than others.

What sort of materials did you use? What do you look for in a textbook or recordings? Can you rely on a series, such as the Teach Yourself books?

[redacted] It certainly depends a great deal on what you want to accomplish. I have just been looking at a number of beginning Chinese books. Some were given entirely in romanization. Maybe that would fulfill entirely what somebody wanted to learn. If what they were after was speaking with comprehension, that would do. I don't like it myself, but that is possible.

[redacted] In my case many of the languages I've had to learn on my own in the last 11 years I've been here were learned simply for the purpose of teaching them to others. That certainly colors your outlook right from the start. For one thing, that means that I'm going to want to be able to use a book that I can teach from.

In some languages the choice of books is dependent simply on what if anything you can find. For example, in ancient Egyptian there is Gardiner, a couple of ancient things by Budge if you can find them, and a perfectly foul little thing

P.L. 86-36

P.L. 86-36

by Mercer. In some there is not enough of a choice to make a choice.

[redacted] Of course it depends on the purpose. I've always been guided by one of two purposes: first, the excitement and thrill of learning a new language in order to get at the literature and culture or the structure of the language; secondly, to master a tool.

Depending on which of these things I wanted to do, I would choose a particular reference grammar. Some reference grammars, or student grammars for that matter, are excellent at getting you to a point in Russian, let's say, where you can work on your own. Others are much better for purposes of historical reconstruction or literary aspects of the language.

Jack [Murphy] and I both like the pony technique for learning a language, and that will get you into the literature much more quickly. You have a valid English translation and learn as you go[1].

Murphy: I've been on Susu for a spell and you take the two or three things that exist. As far as the types of books are concerned, I like to hit a language from several points of view. And that brings to my mind the problem of the reader. I think that the most useless type of reader on earth is the chrestomathy, where you get a mass of texts with nothing else. If a person is capable of reading that, he doesn't need a course. It's much better to have a tiny amount of text annotated to within an inch of its life and glossarized. The Lund-Humphrey series is brilliant on that score. In Arabic, the Rabin reader in the Lund-Humphrey series is beautiful.

There is a great abundance now, compared to 1938, when the only thing that dominated the market was the Otto-Gaspé-Sauer series. The USAFI series, as a series, is the greatest thing that has been done. During World War II they made 21 of them, and with all the big guns in American linguistics. Bloomfield did the Dutch, Lukoff did the Hindi, Hockett the Chinese, Carleton Hodge the Serbo-Croatian.

The Teach Yourself series does not require any standardization from its authors and they bypass some very important languages. The one in Swahili is a model for learning to read the language; Bengali is an abomination. The one in Icelandic is magnificent as a reference grammar. It introduces 17 irregular verbs to the student in complete conjugation in one of the early lessons, before the student has even approached the regular verbs. Welsh is excellent and Irish is horrible. And the Finnish is a shambles.

[redacted] For beginning students in several languages I use the Teach Yourself series as a classroom text. Generally they range from fairly good to excellent. There are only a couple of bad ones. They are filling in the gaps in the series. They did finally come out with a Romanian. The one in modern Persian is very good for a rank beginner. The Samoan is lousy.

[redacted] Some of those in the Otto-Gaspé-Sauer series were excellent. The Turkish reader in the Indiana University Uralic-Altaic series is first rate, a super production, the best I've seen. On the other hand, the Turkish job in the Teach Yourself series is weak. I tried to teach from it no less than four times, with very meager results.

[redacted] One of the nice things about studying more than one language is that you can often find good books in a language you've studied already[2]. There are a lot of good books in German and Russian, I know.

Do you aim for a specific level of proficiency? Do you start with a certain application or goal in mind? Does that determine the level and type of proficiency you try for?

[redacted] I aim for Level 3 myself, regardless of the application, and hope that ultimately I can make Level 4, i.e., that I can read anything that an educated native speaker could read, without translating it in my own mind.

These readers that we were discussing will get you certainly, if you master them, to Level 2, which corresponds to the placement level of the NSA linguist. How far you can actually get with the best type of reader is a moot point. Whether it's possible to get to Level 3 or Level 4 is difficult to say.

Another point I would like to make is that there is always a trade-off involved: if you're going to be in a position where you have to get to Level 2 or 2+ in a lot of languages, you've got to give up the notion of getting to Level 3 or 4 global proficiency in five or six languages. You do one or you do the other, but you don't do it all.

What kinds of language proficiency can you get from self-study? Is it limited to reading proficiency, or can proficiency in aural comprehension, writing, and speaking be learned in this fashion too?

Murphy: If you use cassettes and tapes to a great degree, you can get aural comprehension. An interesting thing happened to me the other night in an English class for Spanish speakers. The native Spanish speakers I've met all have a horrible accent when speaking English. One girl

---

[1] In his article "Backing into Language Acquisition" (CRYPTOLOG, November 1977), [redacted] tells mathematicians how easy it is to learn foreign languages by already knowing the mathematical principles being discussed.

[2] For a discussion of how to use the knowledge of one foreign language to acquire another, see "Tool Languages," by John D. Murphy, CRYPTOLOG, July 1977.

in the class had a beautiful American English accent, much better than the others, though her educational level was not and I wondered why. She told me later that she had listened to tapes hour after hour during her English language course. To me that would be tedium to the ultimate, but it really helped her.

We must also distinguish between languages which are foreign to the first power and those which are foreign to the second power. French, Spanish -- the West European languages -- are not foreign in the sense that Burmese is foreign. And it takes a lot of chutzpah for an American to sit down and write a piece of text in Japanese, or Bhutanese, or Chinese. The Japanese and Hindis do this in English and they come to grief.

[redacted] I think it's much easier to say that you can learn more than just a reading knowledge via self-study, now that we have all these tapes and cassettes.

The only fault with that, of course, like TV instruction, is that the teacher can't stop and correct you when you do something wrong. You can't ask it a question that it isn't programmed to answer. The single question I encounter most often in my language classes is after I've said "That's the right answer," a student will ask "Could it also be done this way?" A key will never solve that.

[redacted] I aim for usable reading proficiency. That's just a personal taste and I don't think it's the same for everybody. People have said a great deal too much about the one correct way to do things. I think it's different for everyone.

[redacted] I think the interesting point here is that we're talking about the passive skills as far as self-study is concerned. Now I'm almost certain that you can't learn to speak a foreign language through self-study, and I'm quite sure that you can't learn to write either. There has to be someone who says "yea" or "nay" to what you're producing, whether written or spoken, and you're immediately out of the self-study mode.

How far can you go on your own before you do need help of some sort? Who do you turn to?

[redacted] Something I have come to believe in a great deal is making a lot of notes, even for languages like Hungarian or Russian which are supposedly well documented. If you write down enough sentences with snags of the same sort, if you can get a half-dozen or so examples of the same thing, it usually comes to mind what it must mean. This is a sort of window-index approach. Then also, if you are able to get the help of a native speaker, it's certainly a great deal better than trying to remember what you wanted to ask him.

I realize what heresy this is supposed to be, but I am not sold on the alleged sacredness of the native speaker. You do have to get a good one. Many people think you can talk to just any native. They are not professional teachers, they're not trained grammarians, and some of them have never thought about their own language. I think it makes a great deal of difference which native speaker you get help from.

Murphy: In the case of Luganda I worked alone for a long while before we hired a native. I had gone through the morphology and syntax and that was no problem. I could take a given piece of text and know the grammatical structure of each paragraph, and know the meaning of every single word and yet not know one damned thing they were talking about. This because of the complicated phraseology -- Luganda is a folk language and folk languages are highly poetic.

P.L. 86-36

[redacted] I would say that you can go an awfully long way on your own, perhaps all the way insofar as reading comprehension is concerned, if you are talking about West European languages. If you're talking about relatively badly documented languages, even languages like Turkish, you run out of aids eventually. You get difficult, complicated texts in these languages and there are no reference materials to cover them. That means turning to a native speaker because there's no other recourse.

[redacted] In many cases with the lower-density or minor languages you run out of aids at the point where you need them most, or even before that. I think it's just largely a combination of luck and how good your teaching aids are. Sooner or later you're going to ask a question that your teaching aid doesn't have an answer for. If you're lucky it's going to be later. If you're unlucky, it's going to be page one, lesson one.

How long does it take, approximately, to achieve a Level 2 reading proficiency in a foreign language? How much time per day or week do you spend studying a language? Is there an optimum amount of time to spend on self-study?

Murphy: Continuity is extremely important. It's much better, I think, if you have a limited amount of time, to spend a little bit of time every day rather than 3 hours on Sunday and then forget it.

On occasion I have had to study languages with extreme intensity. For example, Burmese: during a 9-month period I spent many hours eating, living, breathing, sleeping Burmese. Then I dropped it after having spent many, many hours on it. After 5 years had passed I remembered French and Spanish, which I studied on a much more leisurely basis, much better.

The curse of languages, though, is the fact that they have so many words and phrases. There's the matter of learning a mass of words. And it is not pleasant.

DOCID: 4009805
P.L. 86-36

P.L. 86-36

[redacted] I'm studying Sanskrit now on my own. The grammar offers me no great problem, for I feel that I am at least a pseudo-Indo-Europeanist, if not a full-fledged one. The writing system, on the other hand, requires a kind of visual memorization and association that I do not possess. I must put in 2 hours a day continually for 2-3 weeks before I feel I've made any progress.

I do think that there is probably a limit. A point of diminishing returns sets in, so that you can overdo it. But I think a couple of hours a day every day, over an extended period of time, is necessary. In fact, it's the only thing that will get you to where you want to go.

When you get to a certain point as a linguist, you can make very rapid progress in achieving Level 2, and then perhaps on to Level 3 in the grammatical structures. I feel today that I could take on any new language as far as its morphological and syntactic components are concerned. But learning that bloody vocabulary in one language after another is something I am increasingly less able to do as I grow older. It becomes exhausting.

[redacted] I would say that any consistent amount of daily study is worth 10 times the same amount of time in oddly assorted lumps, one week here, one week there. Even if it's only 15-20 minutes a day, that's better than 3 hours once a month.

How long it takes to get to Level 2 reading proficiency depends on the language and student. After the first 10 languages, they get easier. It sounds like a bad joke, but it's true.

[redacted] You get so you know what your own best pace is. But if you're starting in on self-study, it might be a good idea to avoid making arrogant announcements. If you don't tell your friends you're going to whip Japanese in 6 weeks, you won't have to tell them later that you didn't.

Is self-study a practical method of learning a foreign language? In the case of an African language it may be the only way, but should someone study French or German that way when classroom instruction is so readily available?

[redacted] Self-study is practical. In many instances it is really the only practical way. Let us suppose that one of us wants to acquire some reading knowledge, particularly to acquire a tool language such as Czech. More and more, very interesting information is coming out in the Czech language on a multitude of subjects. So he decides to learn Czech. A Czech course is going to involve months and months of going through baby drills and not very interesting exercises, whereas the learner knows just how he wants to learn the language and for what particular purpose. So it is intensively practical for a person to teach himself, and it is highly impractical to go and study at the feet of a native speaker.

A linguist should have a reading knowledge of French and/or German. That's a moral commitment. What we're talking about here goes a little beyond the question of self-study, but rather learning a tool language one way or another. That need is absolutely essential.

Murphy: It depends on the student's temperament. Some people learn best from courses. You've heard people say that they don't have the discipline. The only reason they take a course is for discipline.

You sign up for a course, you pay the university a rather substantial sum, and you spend night after night traveling. You can solve this problem by getting a good book and just turning to page one.

Do you think the Agency should place more emphasis on self-study of foreign languages? Should it promote it? If so, how?

[redacted] You might expect me to answer the question in the negative, because I wouldn't want to put myself out of a job teaching. But in the ultimate analysis, even in the classroom it is self-study. A teacher can't somehow infuse the knowledge into the student. The student has got to learn it himself. It's just self-study with a little more help than the textbook.

I think that paying people a bonus for acquiring a solid knowledge of a new language, upon passing a test at a certain level, is a good idea. It would certainly be a powerful incentive.

[redacted] I think so.

EO 1.4.(c)
P.L. 86-36

Murphy: Especially now that we have a good testing system where we can prove whether or not they've learned the language.

[redacted] We certainly should put more emphasis on self-study, if for no other reason than we can't always tailor schedules either in our own school or somewhere else so that instructor X is going to be on hand at a particular time when it is advantageous for student Y to begin studying the language.

Absolutely, we should pay people for acquiring new languages. [redacted] They overextended themselves to include the most commonly taught languages, so people began using it as a gravy train and they had to stop.

[redacted] Another thing I think the Agency should do that would hardly cost anything is advertise the fact that self-studiers should make a point of taking an Agency test in a language they've studied, whenever they feel ready to take it. It's very important to get your new proficiency on record. Supervisors can't give you credit for studying they don't know you've done.

What are the rewards -- personal and/or professional -- that you have experienced as a result of studying a foreign language on your own?

[redacted] In the first place, it's fun.

P.L. 86-36

P.L. 86-36

[redacted] I love it.

Murphy: Because it's there.

[redacted] I think we would all continue to study languages even if we weren't making a living at it.

Have you got your next language picked out?

[redacted] I'm doing Sanskrit now. My next one is Ge'ez (classical Ethiopic) -- my next and last!

[redacted] My next one is going to be a review. I'm going to brush up on Swahili.

[redacted] I'd like to try Arabic or Chinese.

Murphy: I've started Shona. That's going to be a winner, I hope. It has whistling fricatives. That's something you can't hardly get nowadays!

~~(C)~~

We've Caught a Glimpse of All That We Could Be

P.L. 86-36

[redacted]

We'll just say that we've been to the mountain,
And caught a glimpse of all that we could be.
We will know that a new day is dawning,
With a morning sun for all of us to see.

—From a folk hymn

Now that my term as President of the Communications Analysis Association (CAA) is over, I guess I can admit to you that what I have been trying to do during the past year was to start a minor revolution. The CAA Board of Governors and I, more or less deliberately, set out a year ago to change to some small degree the things we thought were bad for NSA by trying to restore a measure of excitement to the SIGINT business. We consciously sought to bring into the CAA younger, more vigorous people who would take *de facto* control and move the organization forward and make it an instrument of change. Our goal was to improve the people in NSA in mind and psyche stretching, making them more nearly complete SIGINTers (in accordance with our charter of cross-discipline actions). That we were less than totally successful is no failure; to have made a promising start was an achievement.

In the same spirit of confession, I can tell you too that we deliberately chose controversial speakers on controversial subjects, aiming at disturbing the apathetic. Cecil Phillips told us about our foolishness in expecting computers to think. Dave Gaddy drew parallels between our behavior and that of our counterparts of more than a century ago. Whit Reed talked about our common sense and the lack of it in living with remoting systems. [redacted] made us see that the future is now. Through our parties, we tried to show that zaniness and camaraderie have a place in professional life. And in our efforts to establish a program for the Communications Analyst, our work reached its more nearly crystalline form. The response to each of these moves was good, and our membership doubled during the year.

It was a good year and a satisfying experience for me. I've been accused from time to time of management-by-inspiration, and at least as far as CAA is concerned, I plead guilty. For to me the CAA represents a fertile field for creativity and innovation, for forward movement, for excellence. To the degree that CAA or any other learned organization fails to exploit new knowledge and to move forward in keeping NSA vital and alive, it has failed to execute its most important mission. With Dave Gaddy, a man of wisdom and wit, taking over CAA's presidency, I leave office comfortable that the future offers more promise than the past.

I don't often have a chance to say thank you in public. So this time I plan to make the most of it. Thanks to the entire Board of Governors for hard work, innovative thinking, and the wry maturity to keep me out of trouble. Thanks to Dave Gaddy and [redacted] for the constant streams of vigorous ideas. Thanks to Tim Murphy for his sober, good-natured hard work in keeping CAA solvent. Thanks to Dan Buckley and [redacted] for their brainstorming in drawing up a program for the Communications Analyst. And thanks too to all the program chairpersons -- too many to name -- for their work in setting programs for CAA. Thanks to all the members whose enthusiasm kept us going. And, most of all, thanks to the hardest worker of all, [redacted] who had to live with our hardy foolishness and carry out our ideas almost single-handedly.

Do you have the feeling that somebody is watching you? Maybe it's our Nominating Committee! They've been out scouting the countryside, looking for a slate of officers and board members for 1978.

Just one dollar a year. That's all it takes for you to become a member of CAA. Well, not quite all! You *do* have to fill out a membership card (call any officer or board member to get one) and then send the card and your dollar to the treasurer.

Coming soon-in January

The CAA General Meeting -- Election of the 1978 Board. Be there!

CAA Board:

President [redacted]
President-Elect David Gaddy, 3247s
Treasurer Timothy Murphy, 3701s
Secretary [redacted]
Board Members [redacted]

(U)

P.L. 86-36

DOCID: 4009805

HOW NOT TO MAKE AN O.B.

TITLE: ~~The Military Career of Lt. Doorn~~

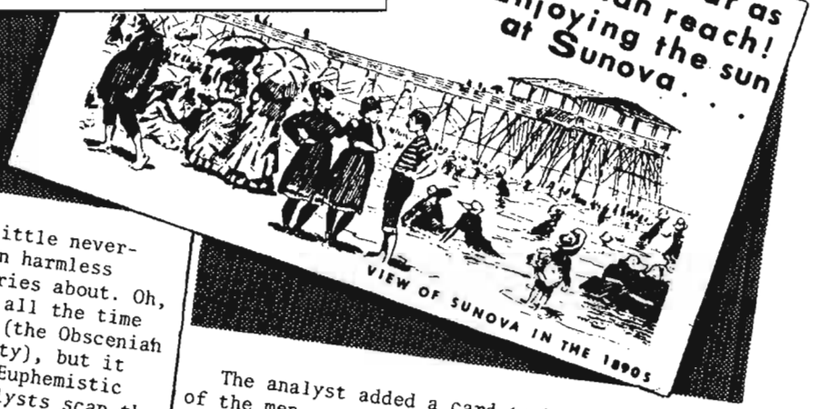
AUTHOR: Harry H. G. Rosenbluh

ORGN: P16

PUBLICATION: CRYPTOLOG ~~CommAND~~

DATE: ~~Feb 74~~ Dec 77

The following article appeared originally in the February 1974 issue of CommAnD (The Communications Analysts' Digest), a P1 publication no longer issued. A complete file of CommAND is available in the P1 Cryptologic library, Room 3W076. For information, call Mrs. Dorothy Rittenhouse, 4998s.



Euphemisia is a pleasant little never-never land which a certain harmless Pedantian SIGINT unit worries about. Oh, they don't worry about it all the time and it isn't their greatest worry (the Obscenian problem is their number one priority), but it rates fairly high, especially the Euphemistic military forces. Two or three analysts scan the traffic when there is any -- and intercept is sporadic -- keeping files of names and units.

After several years of such reading and file-making, one of the analysts decided that the section had enough Euphemistic traffic on hand to put out an Order of Battle (OB) for Euphemesia and proceeded to do so. Of course, he went about it all wrong, and that is why this article is written: in the hope that if a reader sees any practices that match those described here, he or she will try to change those practices.

If this were a movie, we would now have a flashback showing the section in the 1960s, scanning and filing Euphemistic army, navy, and air force messages. One item in the batch is this one:

FROM WEST SNAFU TO CQ 20 JUNE 1962

THE FOLLOWING CADETS HAVE BEEN GRADUATED FROM THE EUPHEMISTIC MILITARY ACADEMY IN WEST SNAFU WITH THE RANK OF SECOND LIEUTENANT IN THE ARMY OF EUPHEMISIA:

BLANK, BLANKETY
BLEU, SACRE
CARAMBA, AY
DARN, GOL
(and eight more names)

The message was signed by the Army Chief of Staff.

The analyst added a card to his file for each of the men, and we will keep an eye on the file of one of them, newly commissioned Lt. Gol Darn.

LAST NAME	DARN
FIRST NAME	GOL
MIDDLE NAME	—
RANK:	2ND LT.
UNIT:	EUPHEMISTIC MIL ACADEMY
LOCATION:	WEST SNAFU
POSITION:	UNK
REMARKS:	P/T MSG LISTING 12 GRADVATES
DATE:	20 JN 62

There's one mistake! Once he graduated from the Academy, that shouldn't be listed as his unit unless he is being kept on as an instructor, and there was nothing in the message to suggest that.

About a week later, there was a large volume of traffic reflecting transfers and assignments, and 10 of the 12 academy graduates were noted, including Lt. Darn, who was sent to the 3rd Messkit Repair Unit in Dag, Nabit (Nabit in a state in northwestern Euphemisia, and Dag is its capital). The first card was removed and a new one was added:

~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4009805

LAST NAME	FIRST NAME	MIDDLE NAME
DARN	GOL	—

RANK: 2ND LT.

UNIT: 3RD MESSKIT REPAIR UNIT

LOCATION: DAG, NABIT

POSITION: UNK

REMARKS: P/T

DATE: 28 JN 62

Except for a few personal cables to his parents, Lt. Darn didn't pop up in traffic for almost a year when his signature appeared on a message to the Chief Motor Pool Officer at Third Division Headquarters in Istenem (to which 3rd Messkit Repair was subordinated), requesting a large number of tires and batteries for jeeps. The analyst changed the card to read:

LAST NAME	FIRST NAME	MIDDLE NAME
DARN	GOL	—

RANK: 2ND LT.

UNIT: 3RD MESSKIT REPAIR UNIT

LOCATION: DAG, NABIT

POSITION: ~~UNK~~ MOTOR POOL OFFICER

REMARKS: P/T RQSTG 26 TIRES & 9 BATTERIES

DATE: ~~28 JN 62~~ 13 MY 63

Just as sleeping in a stable doesn't make you a horse, so asking a motor pool officer for tires and batteries doesn't make you a motor pool officer. It seems like a logical assumption, but should be given a validity indicator (C% and D%), or "POSS," or something to show that the title wasn't included in the message of 10 May.

It so happened that Lt. Darn was the Assistant Motor Pool Officer, as was proved 3 days later when the Chief Motor Pool Officer at division headquarters cabled back:

FM ISTENEM TO DAGNABIT 13 MAY 63

LT GOL DARN, ASST MPO 3MKRU

PER YR REQ 10 MAY, SENDING 13 TIRES, 5 BTRIES

MAJ DONNER WETTER, CMPO 3 DIV

The card was then changed to:

LAST NAME	FIRST NAME	MIDDLE NAME
DARN	GOL	—

RANK: 2ND LT.

UNIT: 3RD MESSKIT REPAIR UNIT

LOCATION: DAG, NABIT

POSITION: ~~UNK~~ ASST MOTOR POOL OFFICER

REMARKS: P/T ~~RQSTG~~ ABOUT ~~26~~ TIRES & ~~9~~ BATTERIES

DATE: ~~28 JN 62~~ ~~13~~ MY 63

This would have been a good time to make a new card. That word "ASST" could easily get missed and that "3" written over the zero in the date is pretty hard to read. No doubt the analyst was in one of his lazy moods, changing the information about the request to cover the subject matter of the 13 May reply, but the card should have shown the fact that the message was addressed to "Lt. Gol Darn, Asst MPO."

There was a routine personnel message on 5 June 1963 from 3rd Messkit Repair to Army Finance in Euphemisia City asking that the beneficiary for Lt. Darn's army insurance be changed because on 10 June he would marry Miss Gosh Amighty and henceforth the beneficiary was to be his wife rather than his mother. If the analyst saw this, he ignored it because an officer's marital status wasn't necessary information.

But on 12 June Lt. Darn sent a cable to his parents:

FM SUNOVA TO CHORT 12 JUN 63

MR AND MRS O. H. DARN, 69 DRAT STREET, CHORT

GOSH AND I ARE VERY HAPPY IN OUR HONEYMOON COTTAGE STOP LOVE FROM US BOTH

LT GOSH DARN

He signed the cable with his rank and full name because he could send it cheaper that way, but that signature caught the analyst's eye, and he noted that Lt. Darn was no longer in Dag, Nabit, so he reasoned that the 3rd Messkit Repair Unit must have moved, and he changed the card:

LAST NAME	FIRST NAME	MIDDLE NAME
DARN	GOL	—

RANK: 2ND LT.

UNIT: 3RD MESSKIT REPAIR UNIT

LOCATION: ~~DAG, NABIT~~ SUNOVA

POSITION: ~~UNK~~ ASST MOTOR POOL OFFICER

REMARKS: P/T ~~RQSTG~~ ABOUT ~~26~~ ~~TIRES & 9 BATTERIES~~

DATE: ~~28 JN 62~~ ~~13 MY 63~~ 12 JN 63

~~SECRET~~

The analyst should not have assumed a move of the unit on the basis of an unofficial message. Units go to other areas for maneuvers, but the reason that this message was sent from Sunova is that it's Euphemisia's most famous summer resort and the place where many Euphemists go on their honeymoons. A week later he was back on the job, and our analyst had to change the card back:

LAST NAME	FIRST NAME	MIDDLE NAME
DARN	GOL	—

RANK: 2ND LT.

UNIT: 3RD MESSKIT REPAIR UNIT

LOCATION: ~~DAG, NABIT~~ ~~SUNOVA~~ DAG, NABIT

POSITION: ~~UNK~~ ASST MOTOR POOL OFFICER

REMARKS: P/T ~~REQTS~~ ~~ABOUT~~ ABOUT AUTO PARTS ~~TIRES & W~~ ~~BATTERIES~~

DATE: ~~8 JN 62~~ ~~19 MY 63~~ 19 JN 63

There was still some room left on the card, but the analyst decided to be neat when the lieutenant got promoted, so a new card appeared:

LAST NAME	FIRST NAME	MIDDLE NAME
DARN	GOL	—

RANK: 1ST LT.

UNIT: 3RD MESSKIT REPAIR UNIT

LOCATION: DAG, NABIT

POSITION: ASST MOTOR POOL OFFICER

REMARKS: P/T MSG FROM CHIEF OF STAFF

DATE: 1 JAN 65

And about a month later, still using his army signature because it was cheaper, he cabled his parents:

FM HECK TO CHORT 3 FEB 65

MR AND MRS O. H. DARN, 69 DRAT STREET, CHORT

HAVE BEEN TRANSFERRED STOP OUR NEW ADDRESS IS 123 GOTOBLAZES STREET, HECK. GOSH SENDS LOVE

LT GOL DARN

The analyst changed the record to show:

LAST NAME	FIRST NAME	MIDDLE NAME
DARN	GOL	—

RANK: 1ST LT.

UNIT: 3RD MESSKIT REPAIR UNIT

LOCATION: ~~DAG, NABIT~~ HECK

POSITION: ASST MOTOR POOL OFFICER

REMARKS: PERSONAL MSG TO HIS FAMILY ~~P/T MSG FROM CHIEF OF STAFF~~

DATE: ~~1 JAN 65~~ 3 FEB 65

The only trouble was that he was not still assistant motor pool officer of the 3rd MKRU. He was now assistant supply officer of the 678th Infantry Battalion in Heck. The official message announcing his transfer was not intercepted. He moved to Heck because he had a new job in a new unit, but the card doesn't reflect that.

Two years later his name appeared on another promotion list, with his first name misspelled as GOLL. The analyst assumed that the second L was a middle initial and made a new card:

LAST NAME	FIRST NAME	MIDDLE NAME
DARN	GOL	L

RANK: CAPT.

UNIT: 3RD MKRU

LOCATION: HECK

POSITION: ASST MOTOR POOL OFFICER

REMARKS: OFFICIAL PROMOTION LIST

DATE: 1 JN 67

The spotty intercept didn't yield much more about him for 2 more years, when a personal message from him to his parents announced:

FM HECK TO CHORT 1 JUN 69

MR AND MRS. O H DARN, 69 DRAT ST, CHORT

TODAY I GOT PROMOTED TO MAJOR STOP YOUR LOVING SON

GOL

Apparently majors can affort to pay the higher rate because he didn't use his rank and

~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

full name, but the analyst spotted the message, checked the name, and found a Capt. Gol Darn. It turned out to be a valid assumption, but you'd be surprised how many Latin American second lieutenants are named José Jiménez, or how many German captains are named Heinrich Mueller, or how many American officers yclept George Smith there are. A personal message is not nearly as valid as an official promotion list. The Gol Darn example is better than average since he signed his cable to Mr. and Mrs. Darn as "your loving son," implying that his last name is also Darn; the captain in question has previously sent messages to the Darns on Drat Street; and Captain Darn was in Heck. But Pedantian analysts have been known to have conflicting entries in their files because there are two or more individuals with the same name.

Well, a month later, Major Darn received a cable from his parents:

FROM CHORT TO BLAST 1 JUL 69

MAJOR AND MRS GOL DARN 222 DANG STREET, BLAST

OUR LOVE TO YOU IN YOUR NEW HOME AND BEST WISHES TO OUR SON AS HE ASSUMES HIS FIRST COMMAND

YOUR PARENTS

This warranted making out a new card.

LAST NAME	FIRST NAME	MIDDLE NAME
DARN	GOL	L

RANK: MAJOR

UNIT: 3RD MKRU

LOCATION: BLAST

POSITION: CO

REMARKS: PERSONAL MSG

DATE: 1 JUL 69

Notice that he's still being carried as being in the 3rd MKRU -- and by this time there's probably a new analyst on the problem who doesn't have the slightest idea what that abbreviation expands to -- although Darn hasn't been in the 3rd MKRU for years. He's commanding officer of something, but the analysts never got traffic mentioning his unit in the interim.

Over the next year or so, there were occasional messages to units and individuals, all signed "DARN CO," as well as personal messages to his wife and parents. The analyst changed the last two lines on the card to show the type of message and the date that his name was last seen.

In 1972 the section decided to put out an Order of Battle for Euphemisia, so the analyst dug out his cards, ruled off some paper into columns, and proceeded to transfer the information. When he reached the card for DARN, the analyst wrote:

LAST NAME	RANK	FIRST NAME	MIDDLE NAME
DARN	MAJOR	GOL	L.

POSITION	UNIT	LOCATION	DATE LAST SEEN IN TFC
CO.	3RD MKRU	BLAST	4 JAN 72

Just then a new batch of traffic came in and one of the messages was:

FM SUNOVA TO CHORT 12 JUN 72

MR AND MRS O.H. DARN, 69 DRAT ST, CHORT

CAME BACK HERE TO CELEBRATE OUR NINTH ANNIVERSARY STOP OUR KIDS REALLY LIKE IT AND SEND THEIR LOVE TO GRANDMA AND GRANDPA

GOL AND GOSH

Recognizing a familiar name, the analyst changed the entry in the last column to "12 Jun 72" and went on with his order of battle, blissfully unaware that he was compiling quite a bit of false information.

Fortunately, a checker came across the entry and thought that major was an awfully high rank for the CO of a messkit repair unit. He checked with the analyst, who, fortunately, had saved all the traffic and they discovered that the messkit repair unit hadn't been mentioned since 1962. A similar check on that middle initial revealed that it hadn't been seen since that original garble in 1967. The only thing that was dated 12 June 1972 was the fact that there was somebody named Gol Darn in Euphemisia.

The checker suggested that the dates of each bit of information be shown to give the recipients a more honest picture. The DARN entry would then be:

~~SECRET~~

LAST NAME	RANK	FIRST NAME	MIDDLE NAME	POSITION	UNIT	LOCATION	DATE LAST SEEN IN TFC
DARN	MAJOR	GOL	L.	CO	3RD MKRU	BLAST	12 JUN 72
12 JUN 72	1 JUN 69	12 JUN 72	1 JUN 67	1 JUN 69	13 MAY 63	1 JUN 69	

The analyst blew a fuse. This would take a million years to check out and write in, and none of the recipents would look at the dates anyhow, etc., etc. Well, suggested the checker, how about a note with that last-seen date, explaining how much of the entry it verified (in this case, just the name), and again the analyst objected, "Then the user will doubt all the rest of it and all the rest isn't necessarily wrong!" The checker asked if any attempt had been made to check with the Central Library to see if they had any information that could fill in some of the gaps, to which the analyst replied, "This is supposed to be an all-COMINT OB! We don't want any collateral in it!" The checker explained that it could still be a COMINT-based OB with collateral being used to fill in the gaps. Collateral isn't all bad! The analyst seemed unconvinced, and so did the branch chief.

The checker resigned himself to putting out an all-COMINT (and largely erroneous) OB. His suggestion about validity indicators on each entry --

(A% DARN) (A% Major) (A% Gol) (D% L)
(B% CO) (D% 3rd MKRU) (B% Blast) 12 Jun 72

-- was also vetoed.

When the checker found the entry

DURN 1st Lt Gol ____ ____ 678 Inf Bn Heck 10 Mar 65

he was struck by the similarity of names, so he asked the analyst if DARN and DURN might be the same person. The traffic file on 1st Lt. Gol Durn consisted of one piece of paper:

FM EUPHEMISIA CITY TO HECK 10 MAR 65

CO, 678 INF BN

TELL 1ST LT GOL DURN OF YOUR BN THAT MONTHLY SUBMISSION OF USED FLYPAPER REPORT NO LONGER REQUIRED

CHIEF G4

The analyst couldn't prove whether DARN and DURN were the same person, but he also couldn't prove that they weren't. So, despite the dictum of "no collateral in all-COMINT OB," the checker called the Central Library to see if they had any further information about 1st Lt. Gol Durn, explaining that he thought it might be a garbled reference to the man who was now Major Gol Darn. . . and as long as he was on the phone, he also asked if they had any information about what unit Major Darn was CO of.

The Library analyst replied:

(1) that there was no trace of anybody named GOL DURN in any of their Euphemisia files;

(2) that among the items in those files was the official Euphemistic Army Officers List for 1 June 1972, which went all the way down to second lieutenant and the cadets in the military academy who would soon be second lieutenants;

(3) that this list gave the name, rank, date of rank, position, and location of every officer in the Euphemistic Army; and

(4) that, as of 1 June 1972, Major Gol Darn was a lieutenant colonel, assigned to the West Snafu Military Academy as Deputy Assistant Commandant.

The analyst thought that this was cheating. He insisted that he wanted an all-COMINT order of battle and the checker had no right trying to get collateral. The fact that this wasn't ordinary old run-of-the-mill collateral, but was an official document from the Euphemistic Defense Department put out for their own use, so he could be sure of its accuracy, didn't seem to impress him. He was still convinced that COMINT was better. However, even the branch chief had to admit that it would look pretty silly putting out an OB that conflicted with such a document. The Euphemistic Order of Battle project was allowed to die, but the analyst was urged to keep making files just in case those Euphemists ever stopped giving that Officers List to the Pedantian military attache.

[redacted]

DOCID: 4009805

WHAT IS PATTERN RECOGNITION?

[redacted] R51

Pattern recognition is concerned with answering the following two questions:

- How does one describe a pattern so that a machine can recognize it?, and
- How does one design a machine so that it can recognize a pattern?

The word "recognition" as used here means either classification or description, or both. Classification is the identification of the pattern with one of several predetermined classes. It may sometimes happen that the pattern is associated with more than one class (this is called multimembership data) or the pattern item may be regarded as an "outlier," a nonmember of any of the classes. The classification process involves deriving a decision rule from a set of samples of known class membership (this is the learning or training phase) and then evaluating the rule on another set of samples of known class membership (this is the testing phase).

The input to a pattern recognition system may be any of the following:

- vectors of measurements,
- one-dimensional time waveforms,
- two-dimensional images.

There are two basic models for a pattern recognition system:

- decision-theoretic,
- syntactic-structural (sometimes called linguistic or grammatical).

Hybrid models are, of course, possible.

In the decision-theoretic model, *features* or distinguishing characteristics are derived from the input. This process is called *feature extraction*. The number of features should be relatively small and carefully chosen to separate members of the different classes. Each vector of features is then identified with one of several predetermined classes via a prescribed decision rule.

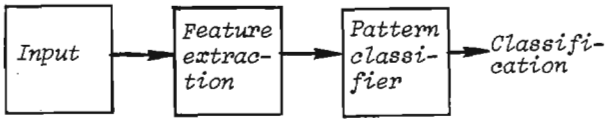


Fig. 1. Schematic of a decision-theoretic pattern recognition system

As a simple example of a decision rule, consider the data structure depicted below.

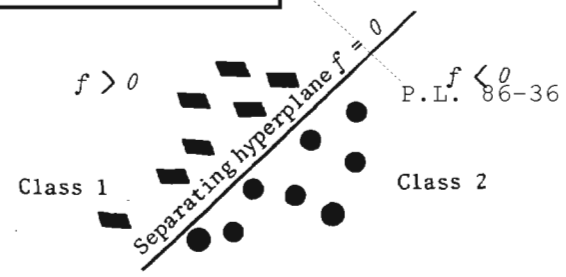


Fig. 2. Linearly separable classes in two-dimensional feature space

The two classes may be separated perfectly by a linear function $f(x_1,x_2) = w_1x_1 + w_2x_2$, where (x_1,x_2) is a feature vector to be classified and w_1 and w_2 are parameters that define the classifier.

The decision rule is as follows:

- if $f(x_1,x_2) > 0$, identify (x_1,x_2) with Class 1,
- if $f(x_1,x_2) < 0$, identify (x_1,x_2) with Class 2,
- if $f(x_1,x_2) = 0$, make no identification.

The most commonly used decision rules in pattern recognition are:

- minimum distance classifiers,
- nearest neighbor classifiers,
- maximum discriminant function classifiers.

[redacted]

EO 1.4.(c)
P.L. 86-36

In the syntactic-structural model, the objective is pattern description as well as classification. The input is represented by a language-like structure (e.g., a string of symbols or a graph) in terms of relations among subpatterns called *primitives*. The syntax analyzer then decides whether or not the pattern belongs to the class described by a given grammar. If the pattern is syntactically correct with respect to

EO 1.4.(c)
P.L. 86-36

that grammar, it usually may be described in terms of a parse or parsing tree. Otherwise the pattern is either excluded from further consideration or is analyzed with respect to other given grammars (each describing a different class).

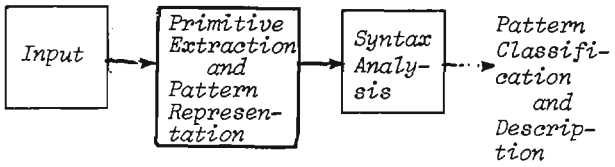


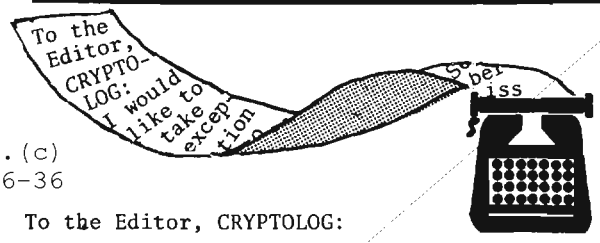
Fig. 3. Schematic of a syntactic pattern recognition system

[redacted]

If you have any questions about these approaches or about the possibility of applying these techniques to your operational problem, please contact either [redacted] (R51, 3461s) or [redacted] (R51, 5228s).

P.L. 86-36

~~(S)~~



P.L. 86-36

EO 1.4.(c)
P.L. 86-36

To the Editor, CRYPTOLOG:

I would like to take exception to some remarks made by [redacted] in the September issue [redacted] As a linguist/analyst/reporter who daily uses the [redacted] program, I believe that I am qualified to discuss the system.

[redacted]

[redacted] B41

~~(SC)~~

P.L. 86-36
EO 1.4.(c)

P.L. 86-36

DOCID: 4009805

1977 INDEX

The following index of the articles published in Volume IV, 1977, of CRYPTOLOG should be used in conjunction with the separately published CUMULATIVE INDEX (Vols. I through III, 1974-1976). The next cumulative index will be published next year.

The index below adheres to the format of the Cumulative Index, which was computer-produced using the Super Bee CRT/Tycom typewriter terminal on the B6700 and programs written by George P. Wood, P16.

The index is in two parts. The first part is an index of titles, listed alphabetically (1) by title and (2) by keyword in the title. A few titles have also been assigned, by human intervention, keywords that do not appear in the titles. The second part is an index of authors. In both parts, multiple entries are listed in chronological order.

Items appearing in the January-February double issue are indicated by "Jan 77."

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Titles

P.L. 86-36

A

ABNER
Early Days in NSA Computing — [redacted] — Aug 77

AFRICA
How Many African Countries Can You Spot? — [redacted] — Nov 77

AG-22/IATS
The Last Word on IATS — Phillips — Apr 77
A View from the Bridge — [redacted] — Jun 77
Another Last Word on IATS — [redacted] — Sep 77

AI
Another Controversial Book on Artificial Intelligence — [redacted] — May 77
The Doctor Is In(capable of Diagnosing) — [redacted] — Sep 77
[redacted] — [redacted] — Nov 77

ANALYST, ANALYSTS
What Is an Information Research Analyst? — [redacted] — Aug 77

Analyzation of Data — [redacted] — Oct 77

Another Controversial Book on Artificial Intelligence — [redacted] — May 77

ARTIFICIAL INTELLIGENCE
Another Controversial Book on Artificial Intelligence — [redacted] — May 77
The Doctor Is In(capable of Diagnosing) — [redacted] — Sep 77
[redacted] — [redacted] — Sep 77

B

Backing into Language Acquisition — [redacted] — Nov 77

BALLONI
[redacted] Editor — A.J.S. — Sep 77
[redacted] — [redacted] — Mar 77
[redacted] — Buck — Jul 77
[redacted] — [redacted] — Jul 77

BUDGETING
ZBB? What in the World Is That? — [redacted] — Jul 77

C

CAA
CAA News: What Ever Happened to the CAA? — [redacted] — Jul 77
CAA News: What Are They Up to Anyway? — [redacted] — Aug 77
CAA News: Whom? — [redacted] — Sep 77
CAA News — [redacted] — Oct 77
CAA News — [redacted] — Nov 77
CAA Message and News — [redacted] — Dec 77

[redacted] — [redacted] — Mar 77

CALLIMAHOS, L. D.
Tribute to the Guru — Class 32 — Sep 77

CHINESE
Backing into Language Acquisition — [redacted] — Nov 77
Choose Ye! — [redacted] — May 77

CIPHER
Old Russian Manuscript Ciphers — [redacted] — Jun 77

CLASSIFICATION
Classification Corner — [redacted] — Jul 77
Classification Corner: XGDS-2 — [redacted] — Sep 77
Classification: A Bigger Picture — [redacted] — Oct 77
Classification Corner: Who Said? — [redacted] — Oct 77

C-LINERS
Letter to editor -- C-LINERS article — "Appalled" — Mar 77

COLLECTION
Objective Satisfication Score; Collection Performance — [redacted] — Nov 77

COMPUTER, COMPUTERS
A View of the Central Computer Complex in the Late 1970s and Early 1980s — Phillips — Mar 77
Contemplating Computing — [redacted] — Apr 77
Early Days in NSA Computing — [redacted] — Aug 77
Contemplating Computing — [redacted] — Apr 77
Conversation with a Micrographics Pioneer — Wigglesworth — Dec 77

[redacted] — [redacted] — Mar 77
Which Tape Has the Intelligence: Project [redacted] — Gurin — Jul 77

CRYPTANALYSIS, CRYPTANALYSTS
[redacted] — [redacted] — Dec 77

CRYPTOGRAMS, CRYPTOGRAPHIC
Want to Play with a Pickfair Square? . . . — [redacted] — Aug 77

D

DATA
DIALOG Available at NSA . . . — [redacted] — Aug 77

Dating Game — [redacted] — Jul 77

[redacted] — [redacted] — Sep 77

DIALOG Available at NSA . . . — [redacted] — Aug 77

Director's Memorandum: [redacted] Guidance" — DIRNSA — Nov 77

DOCUMENTATION
Is There a Doctor in the House? — [redacted] — Sep 77
The Doctor Is In(capable of Diagnosing) — [redacted] — Sep 77

E

Early Days in NSA Computing — [redacted] — Aug 77

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

DOCID: 4009805

EO 1.4.(c)
P.L. 86-36

~~TOP SECRET UMBRA~~

P.L. 86-36

ENGLISH
Choose Ye! [redacted] May 77
Plain English [redacted] May 77
Vich Iss R-r-right? A.J.S. Jun 77
What Ever Does "However" Mean? [redacted] Nov 77
[redacted] Dec 77
Executive Order 11652 "Leiner" Jan 77
Expletives Deleted? Salemme Aug 77

F

A Few Thoughts on the NSA Linguist Anon. Mar 77
FIELD
K1 -- SCA Field Management and Evaluation [redacted] Oct 77
Flash! 115th SRI Located! Salemme Apr 77
[redacted] [redacted] Oct 77

G

GERMAN
Backing into Language Acquisition [redacted] Nov 77
GOLDEN OLDIES
GOLDEN OLDIE: A Medal for Horatius [redacted] Jan 77
GOLDEN OLDIE: Analyzation of Data [redacted] Oct 77

H

[redacted] [redacted] Dec 77
How Many African Countries Can You Spot? [redacted] Nov 77
[redacted] Dec 77
Human Factors and Systems Design -- An Estranged Relationship? Jun 77
Human Factors in the Use of Microfiche Readers at NSA Oct 77

I

The "Ice Age" and International Security [redacted] Apr 77
INFORMATION
What Is an Information Research Analyst? Aug 77
INKSTAND
SIGINT Welcomes INKSTAND Jun 77
IRA
What Is an Information Research Analyst? Aug 77
Is There a Doctor in the House? Sep 77
"It's Got to Get Out Today!" Apr 77

J

JAPANESE
The Transcription Skill: Concepts and Teaching Methodologies [redacted] Jul 77
JPRS Language Reference Aids Sep 77

K

KEYWORD
Letter to editor -- Keyword spotting Gurin Mar 77
KILOMETER
Vich Iss R-r-right? A.J.S. Jun 77
Knowledge Resource Management at NSA [redacted] Sep 77
K-1 -- SCA Field Management and Evaluation Oct 77

L

LANGUAGE
"It's Got to Get Out Today!" [redacted] Apr 77
[redacted] Buck Jul 77
Tool Languages Murphy Jul 77
JPRS Language Reference Aids [redacted] Sep 77
The [redacted] Seminar Program Sep 77
Backing Into Language Acquisition [redacted] Nov 77
Language Processing Forum Nov 77
What Made Them Do It? (Language Self-Study) Dec 77
The Last Word on IATS? Phillips Apr 77
Let Me Repeat -- And Make Myself Perfectly Clear Jenks Aug 77
LETTERS TO EDITOR
Letter to editor -- "Firebrand" letter [redacted] Jan 77
Letter to editor -- [redacted] article Jan 77
Letter to editor -- Mason article Jan 77
Letter to editor -- Use of term "compartmented" Jan 77
Letter to editor -- [redacted] interview Mar 77
Letter to editor -- [redacted] article Mar 77
Letter to editor -- C-LINERS article "Appalled" Mar 77
Letter to editor -- Keyword spotting [redacted] Mar 77
Letter to editor -- [redacted] article Apr 77
Letter to editor -- [redacted] article Newton Apr 77
Letter to editor -- [redacted] letter Tetrault Apr 77
Letter to editor -- Mason article Apr 77
Letter to editor -- Mason article Apr 77
Letter to editor -- Mason article Apr 77
Letter to editor -- "Horatius" May 77
Letter to editor -- Buckley letter Jun 77
Letter to editor -- [redacted] article Jun 77
Letter to editor -- Mason article Jun 77
Letter to editor -- [redacted] article Jul 77
Letter to editor -- [redacted] article Jul 77
Letter to editor -- Subscription Jul 77
Letter to editor -- [redacted] article Jul 77
Letter to editor -- [redacted] article "Weeson" Aug 77
Letter to editor -- Subscription "Mouse" Aug 77
Letter to editor -- [redacted] letter [redacted] Sep 77
Letter to editor -- [redacted] "Reader" Oct 77
Letter to editor -- [redacted] "Early Days...Computing" [redacted] Nov 77
Letter to editor -- Salemme "Expletives Deleted?" [redacted] Nov 77
Letter to editor -- Salemme "Expletives Deleted?" [redacted] Nov 77
Letter to editor -- [redacted] article [redacted] Dec 77
[redacted] Buck Jul 77
LINGUIST
What If the Linguists Disappeared? [redacted] Jan 77
A Few Thoughts on the NSA Linguist Anon. Mar 77
A Little TA Problem [redacted] Nov 77
LOG
Speaking of Logging. . . [redacted] Sep 77

M

MANUAL
Revised Technical SIGINT Manual in Preparation Filby Mar 77
[redacted] Guidance (Director's Memorandum) DIRNSA Nov 77
Match Them Up! [redacted] Jul 77
A Medal for Horatius . . . Jan 77
MICROFICHE
Human Factors in the Use of Microfiche Readers at NSA Snow Oct 77
MICROGRAPHICS
Conversation with a Micrographics Pioneer Wigglesworth Dec 77
[redacted] [redacted] Nov 77
More about More about the NSA SIGINT Summary Boucher Jun 77
More about the NSA SIGINT Summary Friedmann Mar 77

N

New Directions for the U.S. Intelligence Community Gaddy Aug 77
NSA-CROSTIC
NSA-Crostic No. 6 A.J.S. Jan 77
NSA-Crostic No. 7 [redacted] Apr 77

P.L. 86-36

~~TOP SECRET UMBRA~~

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

DOCID: 4009805
EO 1.4.(c)
P.L. 86-36

P.L. 86-36

NSA-Crostic No. 8 — A.J.S. — Jul 77
NSA-Crostic No. 9 — Williams — Sep 77
NSA-Crostic No. 10 — A.J.S. — Nov 77

NUMBERING SYSTEM
Which Numbering System Should We Use — "Asken" — Oct 77

O

Objective Satisfaction Score: Collection Performance — Nov 77
Old Russian Manuscript Ciphers — Jun 77
[redacted] — Dec 77
An Overview of Project [redacted] — Mar 77

P

Partners in the Exciting Future of SIGINT — Oct 77
PATTERN RECOGNITION
What Is Pattern Recognition? — Dec 77
The Perils of Being a State Department Interpreter — Oct 77
Plain English — May 77
[redacted]
An Overview of Project [redacted] — Mar 77

The Polyhedral War — May 77

Postscript to "Dating Game" — Aug 77
PROFESSIONALIZATION
Some Thoughts on the Russian PQE — Apr 77
PROMOTION
A Proposed Cure for the Time-in-Grade Syndrome — Nov 77
A Proposed Cure for the Time-in-Grade Syndrome — Nov 77
PUZZLE
Match Them Up! — Jul 77

R

RESEARCH
What is an Information Research Analyst? — Aug 77
RESOURCE MANAGEMENT
Knowledge Resource Management at NSA — Sep 77
Revised Technical SIGINT Manual in Preparation — Filby — Mar 77
RUSSIAN
Some Thoughts on the Russian PQE — [redacted] — Apr 77
Why Are These People Smiling? — Harrison — May 77
Old Russian Manuscript Ciphers — Jun 77
[redacted] — Sep 77
Backing into Language Acquisition — Nov 77

S

SIGINT
More About the NSA SIGINT Summary — Mar 77
Revised Technical SIGINT Manual in Preparation — Filby — Mar 77
More About More About the NSA SIGINT Summary — Jun 77
SIGINT Welcomes INKSTAND — Jun 77
Partners in the Exciting Future of SIGINT — Rosenblum — Oct 77
"Simonoff Says!" — A.J.S. — Sep 77
Some Thoughts on the Russian PQE — Apr 77
[redacted] — Nov 77
SPANISH
Telling It Like It Is — Santiago-Ortiz — Aug 77
Speaking of Logging. . . — Sep 77
SPECIAL RESEARCH ANALYSIS
Whither the SRA? — Sep 77
SPOTTING
Letter to editor -- Keyword spotting — Gurin — Mar 77

STATE DEPARTMENT
The Perils of Being a State Department Interpreter — . . . — Oct 77
A Story With a Moral — May 77
SYSTEM DESIGN
Human Factors and Systems Design -- An Estranged Relationship? — Jun 77

T

TA
A Story With A Moral — [redacted] — May 77
Which Numbering System Should We Use? — "Asken" — Oct 77
A Little TA Problem — Nov 77
[redacted] — Dec 77
TEACHING
The Transcription Skill: Concepts and Teaching Methodologies — Jul 77
[redacted] — Nov 77
Telling It Like It Is — Santiago-Ortiz — Aug 77
The [redacted] Seminar Program — Sep 77
[redacted] — Buck — Jul 77
Tool Languages — Murphy — Jul 77
TRAFFIC ANALYSIS
[redacted] — Dec 77
A Story With a Moral — May 77
Which Numbering System Should We Use? — "Asken" — Oct 77
A Little TA Problem — Nov 77
The Transcription Skill: Concepts and Teaching Methodologies — Jul 77
TRANSCRIPTION
Why Are These People Smiling? — Harrison — May 77
Which Tape Has the Intelligence: Project [redacted] — Gurin — Jun 77
The Transcription Skill: Concepts and Teaching Methodologies — Jul 77
Telling It Like It Is — Santiago-Ortiz — Aug 77
TRANSLATION, TRANSLATOR
"It's Got to Get Out Today!" — Apr 77
What Ever Does "However" Mean? — Nov 77
Tribute to the Guru — Class 32 — Sep 77

UV

Universes, Galaxies, Stars, Bars, and Other Concepts — Phillips — May 77
[redacted] — Oct 77
Vich Iss R-r-right? — A.J.S. — Jun 77
A View from the Bridge — Jun 77
A View of the Central Computer Complex in the Late 1970s and Early 1980s — Phillips — Mar 77

W

Want to Play with a Pickfair Square? — . . . — Aug 77
What Are They Up To, Anyway? (CAA News) — Aug 77
What If the Linguists Disappeared? — Jan 77
What Is an Information Research Analyst? — Aug 77
What Is Pattern Recognition? — Dec 77
What Ever Does "However" Mean? — Nov 77
What Ever Happened to the CAA? — Jul 77
What Made Them Do It? (Language Self-Study) — Dec 77
Where Were We? — Mason — Jan 77
Which Numbering System Should We Use? — "Asken" — Oct 77
Which Tape Has the Intelligence: Project [redacted] — Gurin — Jul 77

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

Whither the SRA? [redacted] Sep 77
Why Are These People Smiling? Harrison May 77

XYZ

XGDS-2 (Classification Corner) [redacted] Sep 77
ZBB? What In the World Is That? Jul 77

P.L. 86-36

Authors

(Names in quotation marks are pseudonyms.)

A

[redacted]
Letter to the editor -- [redacted] article Jul 77

ANONYMOUS
A Few Thoughts on the NSA Linguist Mar 77

"APPALLED"
Letter to the editor -- C-LINERS article Mar 77

"ASKEN, Jess"
Which Numbering System Should We Use? Oct 77

B

[redacted]
The Transcription Skill: Concepts and Teaching Methodologies Jul 77

BLANK, Frances
"It's Got to Get Out Today!" Apr 77

BOUCHER, Melvin J.
Letter to the editor -- Mason article "Where Were We? Apr 77
More About More About the NSA SIGINT Summary Jun 77

[redacted]
Contemplating Computing Apr 77

BUCK, Stuart H.
[redacted] Jul 77

BUCKLEY, Dan
Letter to the editor -- [redacted] article Mar 77
Letter to the editor -- [redacted] letter Sep 77

[redacted]
What Ever Does "However" Mean? Nov 77

EO 1.4.(c)
P.L. 86-36

C

[redacted]
NSA-Crostic No. 7 Apr 77
Early Days in NSA Computing Aug 77
The Doctor Is In(capable of Diagnosing) Sep 77

[redacted] Oct 77

[redacted]
Some Thoughts on the Russian PQE Apr 77

[redacted]
Letter to the editor -- Use of term "compartmented" Jan 77

[redacted]
Knowledge Resource Management at NSA Sep 77

[redacted] Mar 77
What Is Pattern Recognition? Dec 77

[redacted]
What Made Them Do It? (Language Self-Study) Dec 77

[redacted]
An Overview of Project [redacted] Mar 77

[redacted]
Human Factors and System Design -- An Estranged Relationship: Jun 77

[redacted]
GOLDEN OLDIE -- Analyzation of Data Oct 77

D

[redacted]
The Polyhedral War May 77

[redacted]
Letter to the editor -- [redacted] article Jul 77

P.L. 86-36

[redacted]
Another Controversial Book on Artificial Intelligence May 77

E

[redacted]
KI -- SCA Field Management and Evaluation Oct 77

[redacted]
What Is an Information Research Analyst? Aug 77

[redacted]
SIGINT Welcomes INKSTAND Jun 77

F

FILBY, Vera R.
Revised Technical SIGINT Manual in Preparation Mar 77

[redacted]
Letter to the editor -- Salemme article "Expletives Deleted?" Nov 77

[redacted]
More About the NSA SIGINT Summary Mar 77

G

GADDY, David W.
New Directions for the U.S. Intelligence Community Aug 77

[redacted]
Letter to the editor -- "Firebrand" letter Jan 77

[redacted]
CAA Message and News Dec 77

[redacted]
Letter to the editor -- [redacted] article Dec 77

[redacted]
Letter to the editor -- "Medal for Horatius" May 77
A Story with a Moral May 77
Is There a Doctor in the House? Sep 77

GURIN, Jacob
Letter to the editor -- Keyword spotting Mar 77
Which Tape Has the Intelligence: Project [redacted] Jul 77

H

[redacted]
Old Russian Manuscript Ciphers Jun 77

HARRISON, Mary Ann
Why Are These People Smiling? May 77

[redacted]
Letter to the editor -- Salemme article "Expletives Deleted?" Nov 77

EO 1.4.(c)
P.L. 86-36

I

INMAN, B. R., Director, NSA/Chief, CSS:
Director's memorandum: [redacted] Guidance" Nov 77

J

JENKS, Peter
Let Me Repeat -- and Make Myself Perfectly Clear Aug 77

K

[redacted]
Letter to the editor -- Mason article "Vexing Agency-Wide Problem" Jan 77

[redacted]
Speaking of Logging. . . Sep 77

KENNY, MINNIE
Letter to the editor -- [redacted] article Jan 77

[redacted]
Classification Corner Jul 77
XGDS-2 (Classification Corner) Sep 77
Who Said? (Classification Corner) Oct 77

L

[redacted]
Letter to the editor -- Mason article "Where Were We?" Apr 77

[redacted]
Language Processing Forum Nov 77

[redacted]
Objective Satisfaction Score: Collection Performance Nov 77

P.L. 86-36

P.L. 86-36

DOCID: 4009805
P.L. 86-36

[redacted]
Letter to the editor -- [redacted] article "Ice Age. . ." Jul 77
[redacted]
Letter to the editor -- [redacted] letter Jun 77
"LEINER, Helmut"
Executive Order 11652 Jan 77
[redacted] Nov 77

M

MASON, Frederic O., Jr.
Where Were We? Jan 77
[redacted]
Letter to the editor -- [redacted] article Apr 77
[redacted]
An Overview of Project [redacted] Mar 77
McGRILLIES, James R.
Letter to the editor -- Mason article "Where Were We?" Apr 77
[redacted]
Match Them Up! Jul 77
How Many African Countries Can You Spot? Nov 77
"MOUSE, Ima"
Letter to the editor -- Subscription Aug 77
MURPHY, John D.
Tool Languages Jul 77
[redacted]
What If the Linguists Disappeared? Jan 77

N

[redacted]
A Proposed Cure for the Time-in-Grade Syndrome Nov 77
[redacted]
Letter to the editor -- [redacted] article Apr 77

P

[redacted]
The [redacted] Seminar Program Sep 77
PHILLIPS, Cecil
A View of the Central Computer Complex in the Late 1970s and Early 1980s Mar 77
The Last Word on IATS? Apr 77
Universes, Galazies, Stars, Bars, and Other Concepts May 77
[redacted] Sep 77

R

EO 1.4.(c)
P.L. 86-36

[redacted]
Letter to the editor -- [redacted] interview Mar 77
"READER, Constant"
Letter to the editor -- [redacted] Oct 77
[redacted]
Another Last Word on IATS Sep 77
[redacted] Dec 77
ROSENBLUM, Howard E.
Partners in the Exciting Future of SIGINT Oct 77

S

SALEMME, A. J.
Flash! 115th SRI Located! Apr 77
Vich Iss R-r-right? Jun 77
Expletives Deleted? Aug 77
SANTIAGO-ORTIZ, Ramon A.
Telling It Like It Is Aug 77
[redacted]
Classification: A Bigger Picture Oct 77
-----, and [redacted]
The Polyhedral War May 77
[redacted]
Plain English May 77
[redacted]
Letter to the editor -- Subscription Jul 77
SNOW, Don
Human Factors in the Use of Microfiche Readers at NSA Oct 77
[redacted]
Letter to the editor -- [redacted] article "Early Days. . . Computing" Nov 77
[redacted]
[redacted] Dec 77
[redacted]
Postscript to "Dating Game" Aug 77
JPRS Language Reference Aids Sep 77
Backing Into Language Acquisition Nov 77
[redacted]
Letter to the editor -- Mason article "Where Were We?" Jun 77
[redacted]
What Ever Happened to the CAA? Jul 77
What Are They Up To, Anyway? (CAA News) Aug 77
Whom? (CAA News) Sep 77
CAA News Oct 77
CAA News Nov 77
A Little TA Problem Nov 77
CAA News Dec 77
[redacted]
Letter to the editor -- [redacted] article Jun 77

T

TETRAULT, Emery W.
Letter to the editor -- Buckley letter Apr 77
[redacted]
Choose Ye! May 77
ZBB? What in the World Is That? Jul 77

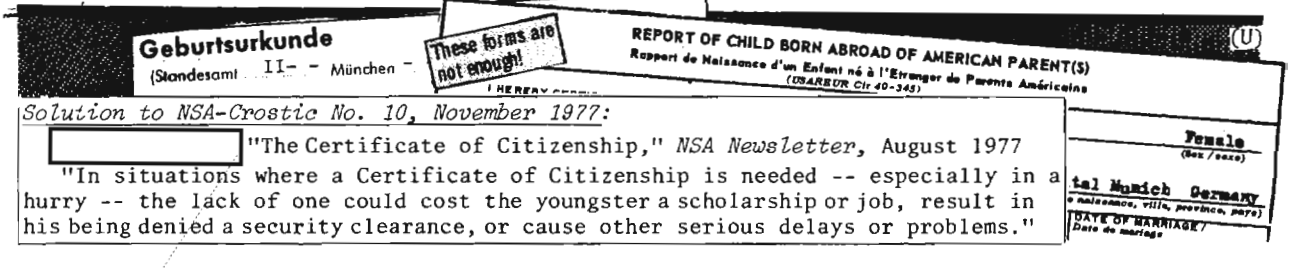
V

EO 1.4.(c)
P.L. 86-36

[redacted]
[redacted] Mar 77
Jul 77

W

"WEESON, Derek"
Letter to the editor -- [redacted] article Aug 77
[redacted]
AG-22/IATS: A View from the Bridge Jun 77
[redacted]
The "Ice Age" and International Security Apr 77
Whither the SRA? Sep 77
WIGGLESWORTH, Don
Conversation with a Micrographics Pioneer Dec 77
WILLIAMS, David H.
Dating Game Jul 77
NSA-Crostic No. 9 Sep 77
[redacted]
Language Processing Forum Nov 77

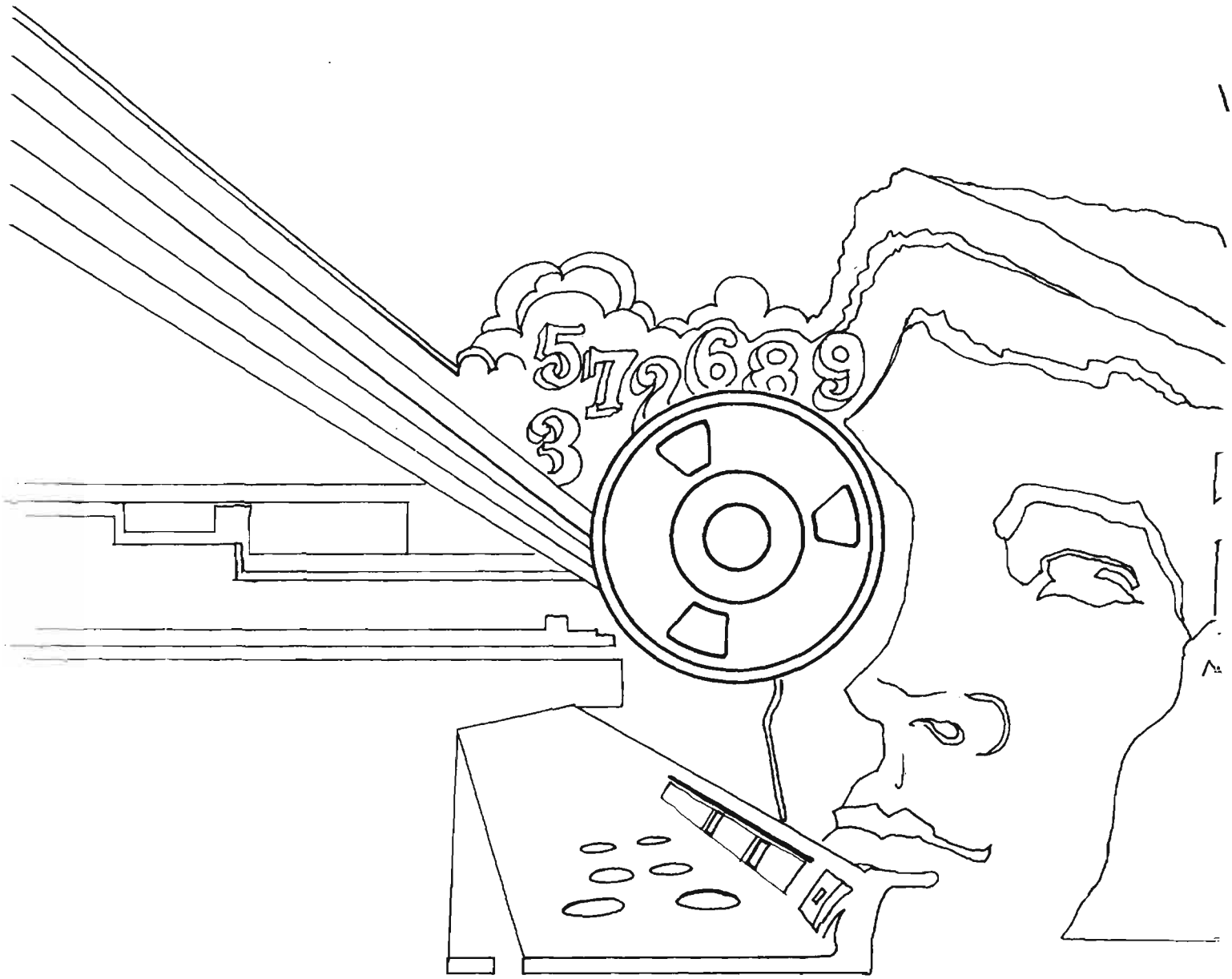


Solution to NSA-Crostic No. 10, November 1977:

[redacted] "The Certificate of Citizenship," *NSA Newsletter*, August 1977

"In situations where a Certificate of Citizenship is needed -- especially in a hurry -- the lack of one could cost the youngster a scholarship or job, result in his being denied a security clearance, or cause other serious delays or problems."

Pl-OCT 77-S32-26042



DOCID: 4009804

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

NOVEMBER 1977

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

[redacted] ..... [redacted] 1
OBJECTIVE SATISFACTION SCORE: COLLECTION ..... [redacted] 2
DIRECTOR'S MEMORANDUM: [redacted] ... Vice Admiral B.R. Inman ... 7
CURE FOR TIME-IN-GRADE SYNDROME ..... [redacted] 9
A LITTLE T.A. PROBLEM ..... [redacted] 10
BACKING INTO LANGUAGE ACQUISITION ..... [redacted] 11
NSA-CROSTIC No. 10 ..... A.J.S. 14
HOW MANY AFRICAN COUNTRIES CAN YOU SPOT? ..... [redacted] 16
LANGUAGE PROCESSING FORUM ..... [redacted] 17
C.A.A. NEWS ..... [redacted] 18
WHAT EVER DOES "HOWEVER" MEAN? ..... [redacted] 19
LETTERS TO THE EDITOR 21

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009804

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. IV, NO. 11 NOVEMBER 1977

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5236s)

Collection.....[redacted] (8955s)

Cryptanalysis.....[redacted] (4902s)

Language.....[redacted] (5236s)

Machine Support.....[redacted] (5303s)

Mathematics.....Reed Dawson (3957s)

Special Research.....Vera Filby (7119s)

Traffic Analysis.....[redacted] (4477s)

Production Manager.....Harry Goff (4998s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

One of the major efforts of the intelligence community has been the monitoring of the development and testing of Soviet missiles. The main sources of data for this purpose are provided by the reception and exploitation of instrumentation test signals that the Soviets transmit to assist their engineers in testing and evaluating these weapon systems. The instrumentation signals, along with beacons and space vehicle command signals, are commonly referred to as telemetry.

The following paragraphs provide information about a new direction in telemetry -- the making of *external* measurements of missile transmissions -- and give some insight into the application of this development in W1, the Office of Space and Missiles.

Background

As a result of the decreasing availability of exploitable telemetry internals (i.e. the data transmitted to monitor critical missile parameters like fluid flow and acceleration) -- either because of encryption of that data or because of low received-signal strength -- the Scientific and Technical Intelligence Community (e. g. MIA, FTD) has been forced to explore the area of externals data. It is of extreme significance that, from the external characteristics of the signal, the community can now recover data on weapon systems that would otherwise not be available.

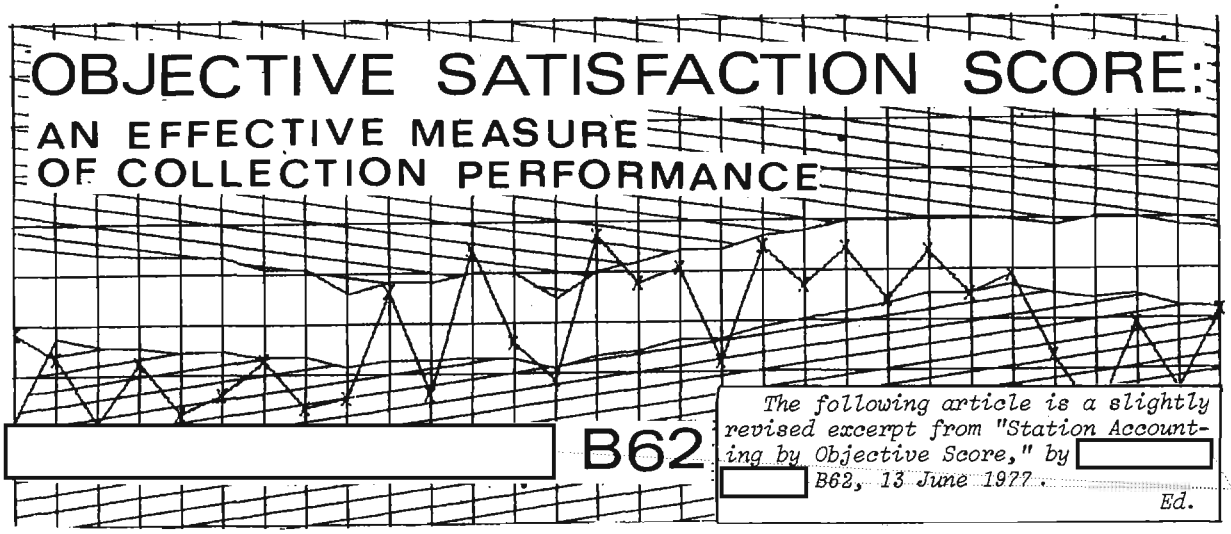
Conclusion

The extraction and uses of externals data require the continued interaction of experienced signal analysts with experienced missile system analysts so that each extracted characteristic can be identified as a parameter of interest or discarded as a byproduct of interference, collection, recording, or processing.

In general, externals telemetry data alone does not permit determination of the missile capabilities. The externals data must be used in conjunction with other data types (e. g., internals, models, simulation programs) to obtain the highest confidence estimates of Soviet missile capabilities.

~~(TSC)~~

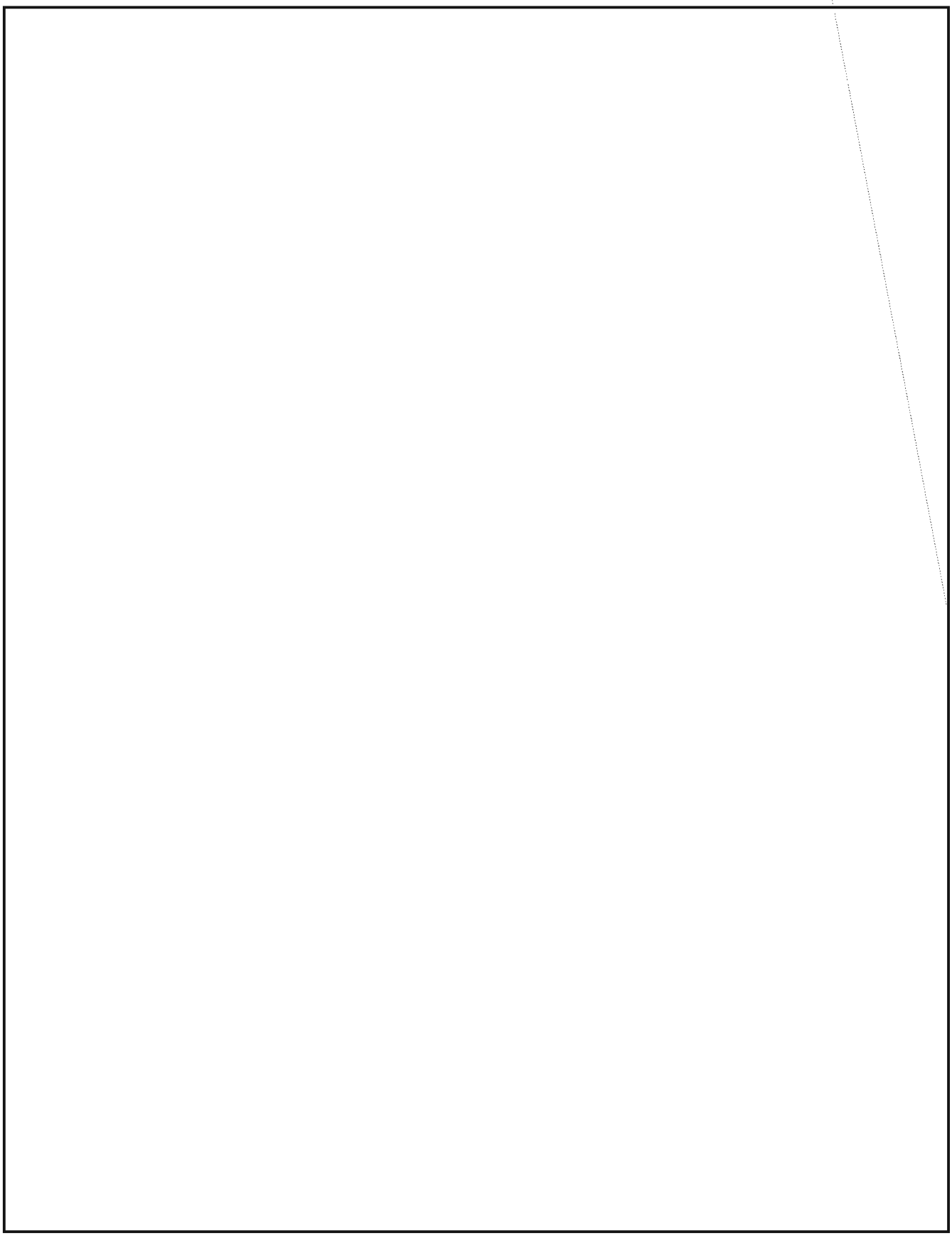
~~(SC)~~



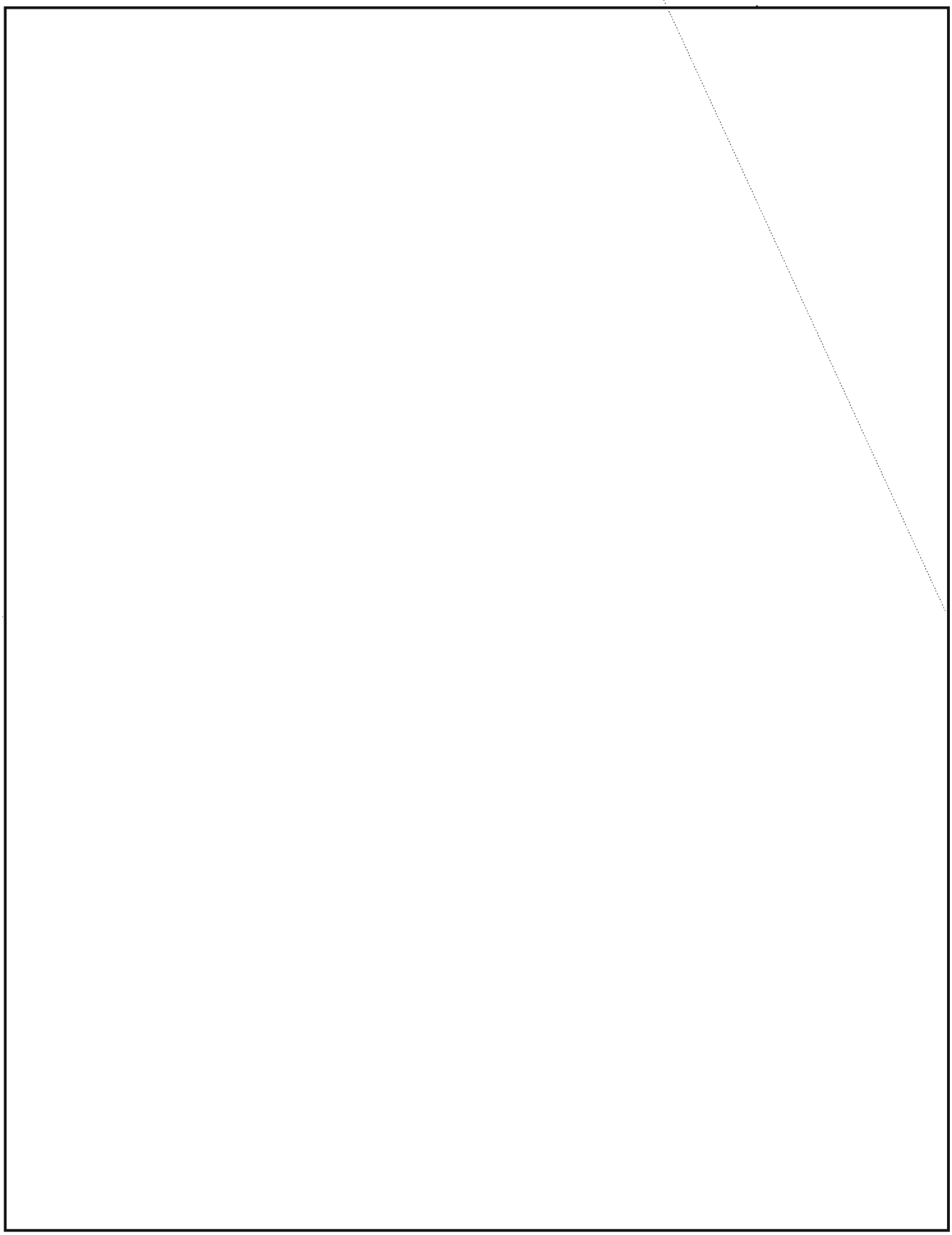
The following article is a slightly revised excerpt from "Station Accounting by Objective Score," by [redacted] *B62, 13 June 1977.*

Ed. P.L. 86-36

EO 1.4.(c)
P.L. 86-36

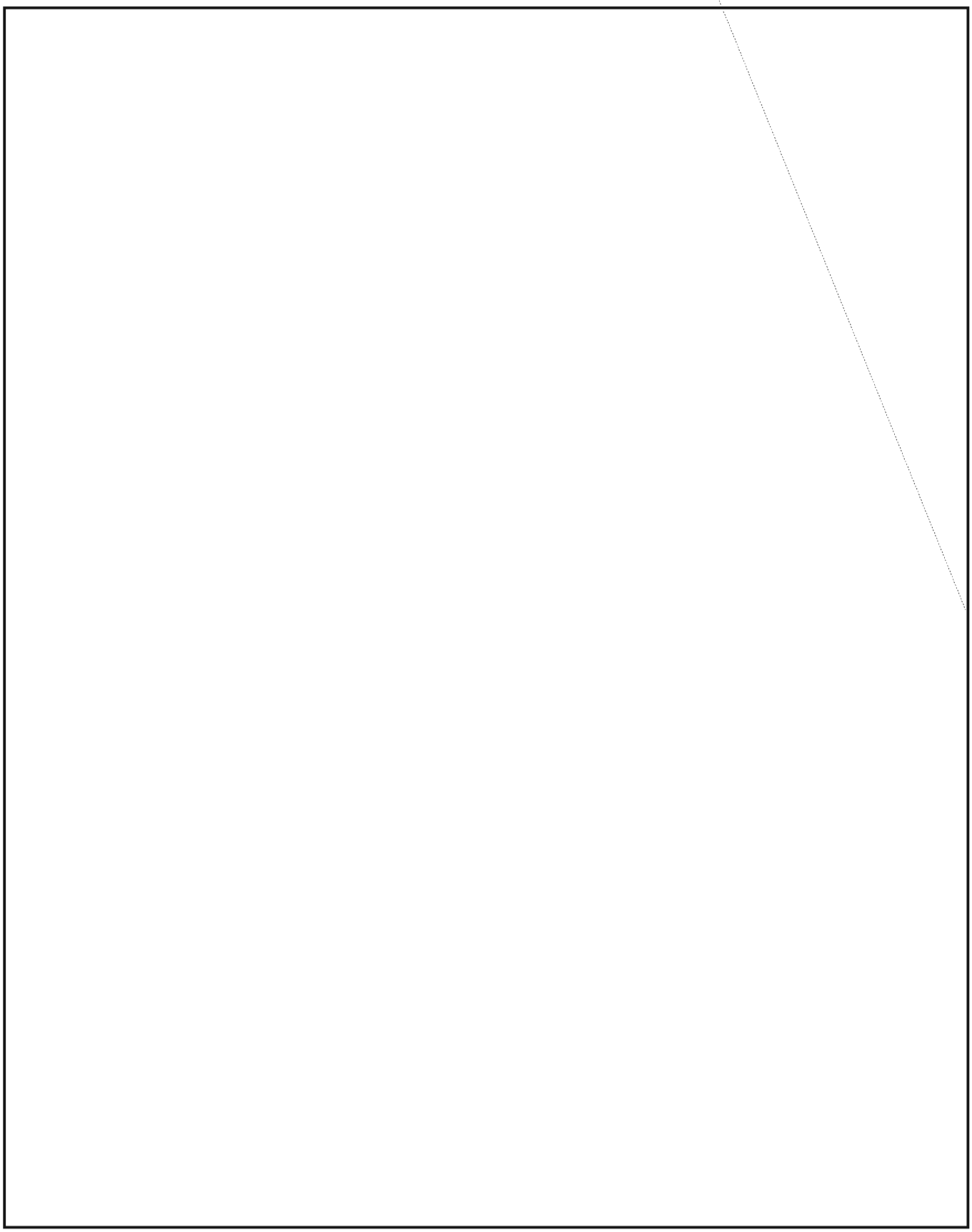


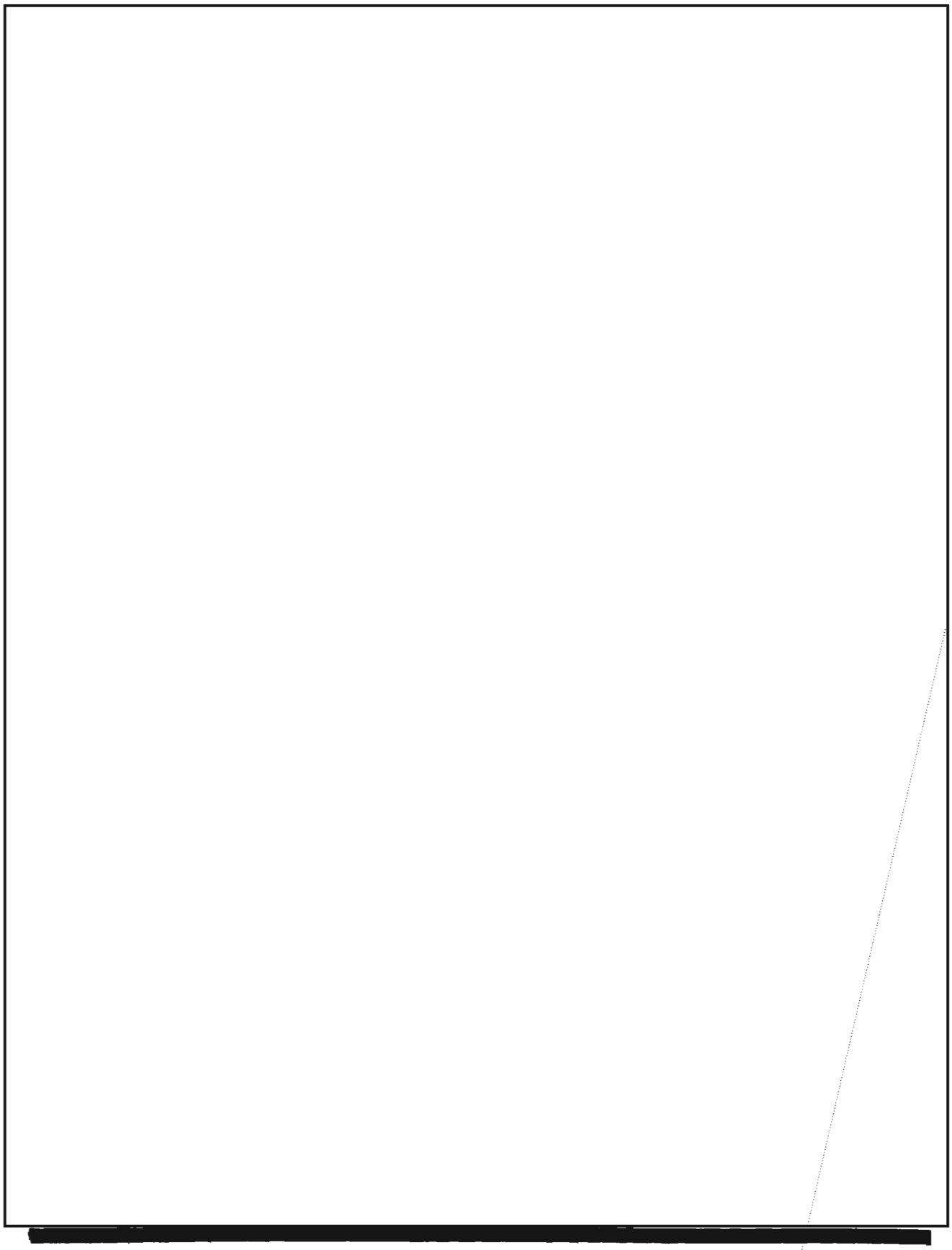
EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~





EO 1.4.(c)
P.L. 86-36

DOCID: 4009804

~~CONFIDENTIAL~~

EO 1.4.(c)
P.L. 86-36

DIRECTOR'S MEMORANDUM: [redacted] GUIDANCE"

Recently I came across a copy of the Director's 4 August 1977 Memorandum and was greatly impressed by its clarity and succinctness. Since a fairly large percentage of the Agency's population is not as well informed as might be desired concerning the objective of [redacted] and the constraints and considerations to be applied to that program, I requested the Director's permission to reproduce the Memorandum in entirety in CRYPTOLOG. In that way, we could inform our readers of what the program will entail. The Director has graciously granted that permission and we are pleased to reproduce the Memorandum in this issue.

[redacted]
Collection Editor

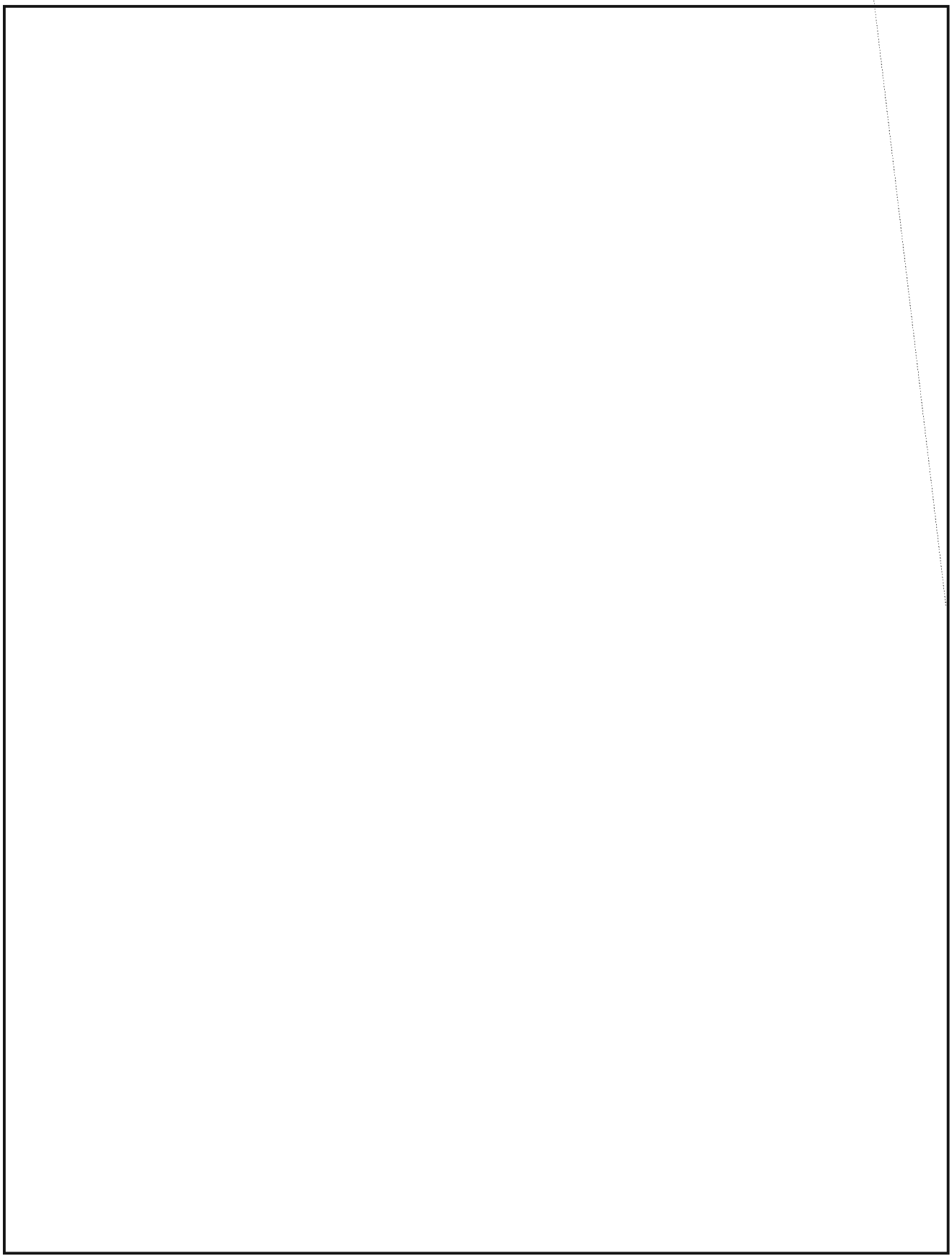
[redacted]

EO 1.4.(c)
P.L. 86-36

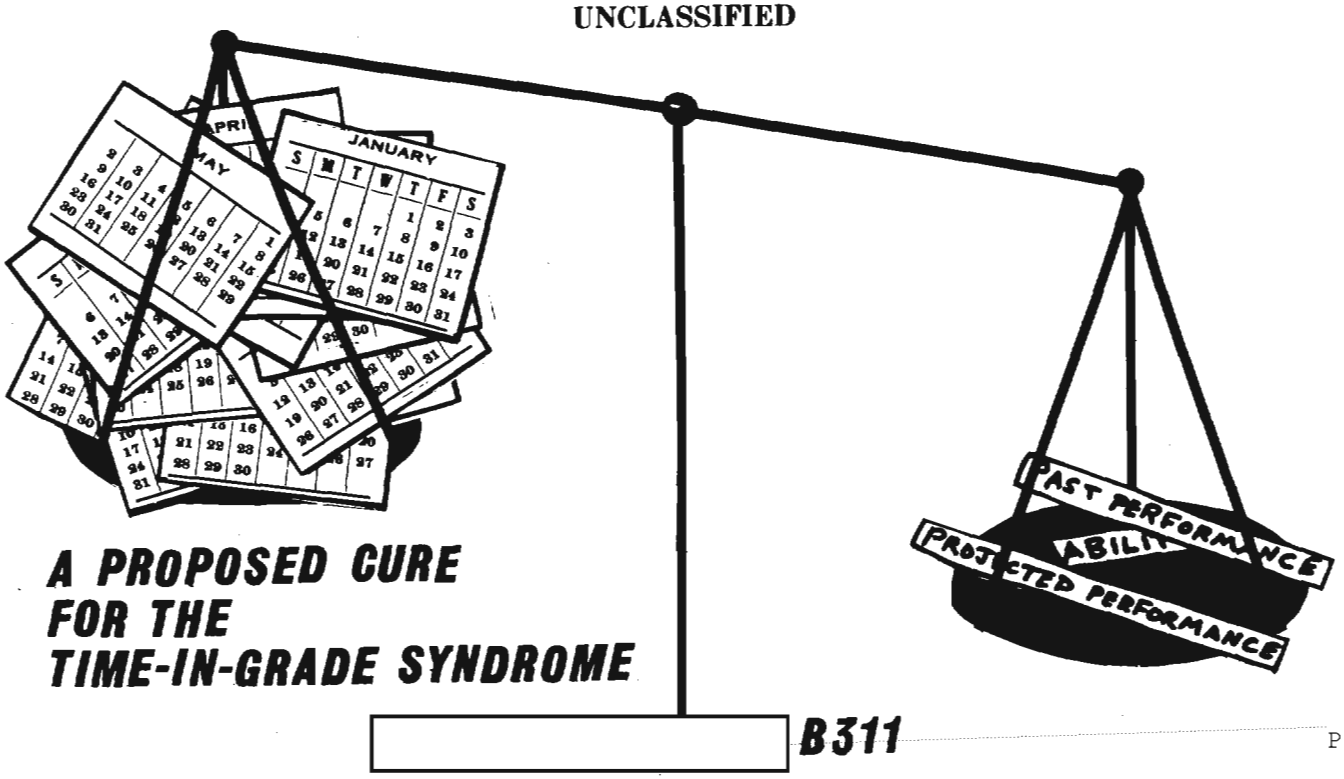
~~CONFIDENTIAL~~

P.L. 86-36

EO 1.4.(c)
P.L. 86-36



DOCID: 4009804



A PROPOSED CURE FOR THE TIME-IN-GRADE SYNDROME

B311

P.L. 86-36

Following a recent promotion ceremony, several employees were overheard discussing the merits of the people who had been promoted. Generally their comments concerned the time in grade of those recently promoted, and how that time in grade compared to that of known contemporaries. There was only an occasional reference to professionalization. But there was absolutely no comment about performance. That conversation was typical of those heard daily in almost any element within the Agency. Invariably, whenever promotions are discussed, the first question concerns how much time in grade the person had. Rarely does performance enter into these discussions. The failure of even employees themselves to consider performance or capabilitity is a widespread problem which I have labeled the "time-in-grade syndrome."

The time-in-grade syndrome permeates NSA, as well as other governmental agencies, and is fostered by promotion and pay policies, job assignment criteria, and the employees within the system. It grew from the once-popular belief, still expounded by American labor unions, that management should reward its employees for long and faithful service. This belief was substantiated by using the argument that experience is necessarily the best teacher and thus was a prerequisite for adequate job performance. In other words, performance was only an outgrowth of experience.

The use of experience as a criterion developed from the primitive societies where invariably the oldest men occupied the highest positions. Our society, although not rigidly following this practice, is partially an "age-graded society" where age, position, and prestige are positively correlated. These practices, ingrained since birth, tend to proliferate and strengthen the time-in-grade syndrome.

Fear of subjective criteria for performance evaluation has also fostered the time-in-grade syndrome since time in grade is a relatively easy criterion to establish and denies charges of favoritism or discrimination. In fact, many still believe that seniority is the only really valid promotion consideration. These people believe that granting promotions to those with extended time in grade is a way of rewarding the employee for loyalty and devotion. No one would deny that loyal service deserves some reward, but no supervisor can get effective results with people if there are limitations in the opportunities to make the best use of subordinates' capabilities.

Advocates of the time-in-grade criteria hold that ability increases with service, especially in the lower-level jobs on the promotional ladder. No doubt this is true in the beginning formative years of an employee's career, but, beyond a certain level, continued length of service at the same level actually *reduces* an employee's ability by producing what is referred to as "a trained incapacity"*. As

* "The employee becomes so inbred with the problems and procedures of his present job that he is unable to adjust to new circumstances and situations. The expert becomes too expert." See: James J. Healy, "The Ability Factor in Labor Relations," *Arbitration Journal*, Vol. X, No. 1 (1955), pp. 3-11.

DOCID: 4009804

Frank Lloyd Wright once said, "An expert is a man who has stopped thinking." In unionized shops the relative importance of seniority has always been greater than in nonunion organizations. Recently there has been new emphasis placed on the importance of ability and compromises even in unionized organizations, with many organizations now using a formula which provides more or less equal consideration to seniority and ability. Many contracts are even being written to allow exceptions for those employees who are "head and shoulders" above their contemporaries in terms of ability.

In general, promotion decisions ultimately determine who will make the key decisions within the organization. At stake is the quality management of the organization. Remedying a mistake in the promotion process is a very difficult and expensive procedure and could result in serious decay or destruction of organizational efficiency. The initiative for promotion must belong to the managers and it is their responsibility to see that worthy personnel are promoted. It is the employees' responsibility to qualify for promotion.

Who to promote should be decided by the manager on the basis of his knowledge of the employee's past performance and, more important, a judgment of the employee's capability to perform in a position of higher responsibility. Promotions should be fairly and capably used to place in each job the most competent and productive employee available. Promotions should be a reward only to encourage those employees who make a successful effort to increase their knowledge and skill, maintain a high level of productivity, and demonstrate a capacity to perform in a job of greater responsibility. It should not be necessary to stress that promotions made on the basis of performance should not concern race, sex, religion, national origin, or age.

The cure is not easy, since the time-in-grade syndrome has been ingrained into the system for so long. It must be made apparent to everyone that performance and capability will be the primary promotion criteria. Peripheral areas which may serve as indicators (such as education, training, and any professionalization certifications obtained) must be considered, but only as an extension of the primary factors of performance and capability. Time in grade should never be considered since an employee should not be nominated for promotion unless he or she has fulfilled the minimum requirements.

To ensure that this system works and to protect the managers against any charges of discrimination, some basic changes in the method of preparing promotion recommendations must be made. When a deserving employee has attained the minimum time in grade to be considered for promotion, a record of that person's previous performance and a statement of his or her projected capability, together with supporting data pertaining to education, training, and professionalization, should be submitted through the existing promotion channels. Each recommendation should be identified by an arbitrary designator, without any references to name, age, color, sex, time of service, or, most important, time in grade. The selection panel would then be able to make their choices solely on the important performance indicators, thus eliminating one of the major causes of the time-in-grade syndrome. Likewise, job assignments should be made on ability, considering grade if necessary, but not eliminating obvious choices simply because of their grade.

Naturally these two changes are going to cause much discussion and certainly some of those ingrained with the time-in-grade syndrome are going to be upset. This is normal when making any change in behavior patterns. In the long run it should improve the Agency's operations and efficiency, with the resultant cure being worth the bitter pill that must be swallowed.

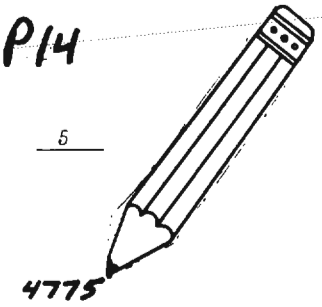
A LITTLE T.A. PROBLEM

These radio frequencies have been recovered on the Third Army network. Recover the system of generation and allocation.

P14

P.L. 86-36

Address	*Unit*	*1*	*2*	*3*	*4*	*5*
518	3rd Army	4716	4051	4796	——	
011	15 Inf.Bde	4691	4116	4876	4281	
176	38 Inf.Bde	4762	4237	5012	4327	
234	420 Arty.Regt.	4898	4303	4023	——	
469	796 Sply.Regt.	5041	4356	4161	4606	
853	562 Inf.Regt.	4085	4505	4305	4750	
503	87 Inf.Regt.	4165	4610	4330	——	
217	149 Inf.Regt.	4241	4686	——	4766	
004	281 Inf.Regt.	4280	4690	4420	4875	
606	356 Inf.Regt.	4370	4805	4620	5055	
180	618 Inf.Regt.	4438	4893	4683	——	



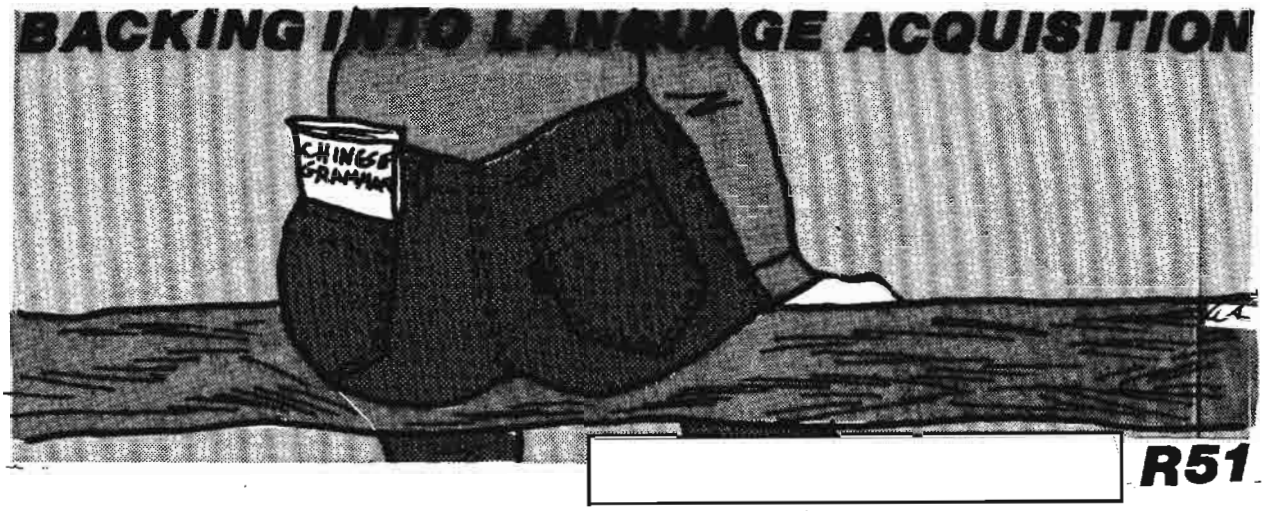
Solution next month.

(U)

DOCID: 4009804

P.L. 86-36

UNCLASSIFIED



In this paper, as in the 5 May 1977 SIGLEX talk on which it is based, I try to illustrate the relative ease for the mathematically literate (in English) to acquire analogous literacy in some foreign (i.e. non-English) language. In mathematics (mostly) and in many (not all) of the so-called "hard" sciences (frequently), the speaker (writer) *must* say a specific something, and the appropriately literate audience (reader) *knows* what that specific something is. This foreknowledge does not remove the necessity of learning the syntactic essentials of the foreign language, but it can facilitate the task to a significant degree. With more and more worthwhile material in mathematics (electronics, physics, biology. . .) appearing in the open literature in such languages as Russian, Chinese, Japanese, and even such has-beens as German, the working mathematician, engineer, etc., might do himself a service in obtaining at least minimal competency in reading the relevant material. Even were it possible -- and inexpensive -- and rapid -- to obtain a relatively good reliable translation of the original material, the translator himself (perhaps "herself," never "itself") would have to be at least minimally competent in mathematics, engineering, etc. I suspect that it's much easier for the ordinary mathematician to learn to read in Russian about mathematics than for the ordinary Russian linguist to learn to read about mathematics in any language.

My few examples are all from an area of elementary mathematics, that of the theory of equations, and , specifically, the mathematical construct called a "polynomial" (see Fig. 1).

$$ax^n + bx^{n-1} + \ldots cx + d$$
(degree n)

$$5x^3 + 2x^2 + 17x + 4$$
(degree 3)

Fig. 1. Polynomial

The word component "-nom-" has the meaning "name" or "term." Hence, "binomial" refers to an expression that has two terms, "trinomial" to one that has three terms, etc. Fig. 2 sketches the etymology, in English, of the word "polynomial" and also shows its equivalent "names" in Russian and Chinese.

*poly*nomial	многочлен	多項式
("*many* terms")	("*many*-term")	("many term expression")

Fig. 2. Etymology of "polynomial"

When two polynomials are multiplied together, as shown in Fig. 3, the result -- another polynomial -- is called the "product" of the first two.

$$(ax^5 + \ldots)(bx^3 + \ldots) = abx^{5+3} = abx^8$$

Fig. 3

A fact, well known to the mathematician, is stated, in Russian, in Fig. 4, mostly to suggest how the Russian handling of the "double negative" can be made more palatable to the mathematician by an example where he *knows* that the *English* sentence has a single negative.

Произведение многочленов, отличных
([the] product) (of polynomials) (different)
от нуля, никогда не будет
(from) (zero) (never) (not) (will be)
равным нулю.
(equal) (to zero)
= "will never be"

Fig. 4

UNCLASSIFIED

Another glance at Fig. 4 might help recall that the degree (largest exponent) of the product of polynomials is equal to the *sum* of the degrees of the polynomials being multiplied. That's precisely what is being said in Figs. 5 and 6, except that Fig. 6 insists that the two polynomials be "non-zero."

Степень	произведения	двух
([the] degree)	(of [the] product)	(of two)
многочленов	равна	сумме
(polynomials)	([is] equal)	(to [the] sum)
степеней	этих	многочленов.
(of [the] degrees)	(of those)	(polynomials)

Fig. 5

两个	非零	多项式	的
(two)	(non-zero)	(polynomial[s])	('s)
积	的次数	等于	
(product)	('s) (degree)	([is] equal to)	
两个	多项式	的次数	
([these] two)	(polynomial[s])	('s)	(degree[s])
的	和.		
('s)	(sum)		

Fig. 6

Having done *some* study of Russian (Chinese) syntax, morphology, lexicology (how to handle a dictionary when the alphabet is different or, respectively, nonexistent), our mathematician may simply be *reinforced* by examples such as the last two. He might be taught something about Chinese syntax in the next example (Fig. 7), precisely because he *knows* what the sentence is saying and, therefore, will learn, albeit the hard way, what a nice relative pronoun is doing in a place like that.

这个	方程	可能	有	
(this)	(equation)	(may)	(have)	
D	E	F	G	
的	有理	根	是	±1, ±3, ...
(which)	(rational)	(root[s])	(are)	
C	A	B	H	

(Letters indicate sequence of translation into English: "Rational roots which this equation may have are. . .")

Fig. 7

Besides examples of syntactic behavior, the mathematician is likely to run into other examples of (foreign) linguistic cavortings where he is almost uniquely equipped to determine the unique exegesis. The German four-letter "abbreviation" (a growing unpleasant phenomenon world-wide) in Fig. 8 presented some difficulty until the German clues (nouns begin with capital letters) combined with the translator's knowledge of what mathematicians *always* say in such instances. Fig. 9 shows the standard (and idiosyncratically mathematical) renderings in English, Russian, and Chinese, plus some additional hints of "morphological" behavior in the four languages at issue.

Sei o.B.d.A. m = 1.
(let) (?)

Fig. 8

ohne	Beschränkung	der	Allgemein|heit
(without)	(limitation)	(of)	(general-ity)
не	ограничивая		общ|ности
(not)	(limiting)		(general-ity)
不	失	一般	|性
(no)	(lose)	(general	-ity)

"with no loss of generality"

Fig. 9

Another way in which mathematicians can back into language acquisition is by recognizing, in a foreign transliteration, names that they are already familiar with. For example, the name of the French mathematician Hadamard (b. 1865) is spelled in Russian as **Адамар** because neither the H nor the D is pronounced in the original name[1]. The transliteration of Western

[1]The rules for transliterating words and names from 18 languages into Russian are given in the book: **Р. С. Гиляревский, Г. А. Старостин, Иностранные имена и названия в русском тексте** (Foreign Names and Designations in Russian Text), a copy of which is available in the P1 Language Library, Room 3W076.

DOCID: 4009804

words and names into Chinese is complicated by the fact that the process involves characters which can be interpreted either according to their *meaning* or according to their *sound*. Fig. 10 shows this two-faced comportment of the character 馬 ("horse"). Note that the Chinese also drop the R from Hadamard's name.

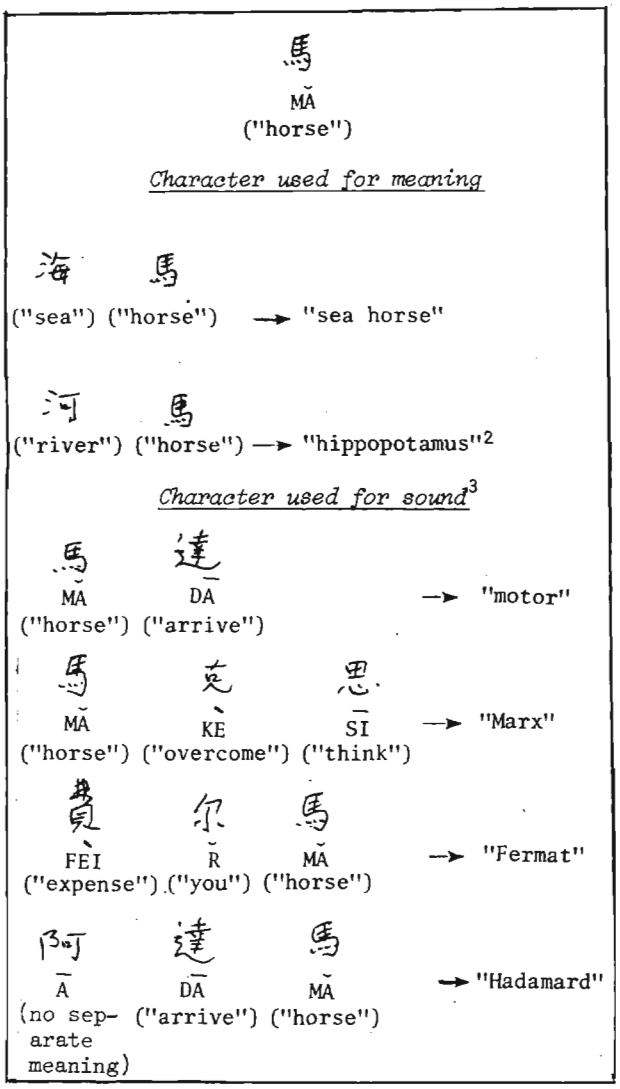


Fig. 10

Finally, Fig. 11 exhibits another frequent trick in modern languages, the neologism obtained by concatenating the original characters (sometimes syllables) of consecutive words. To reconstruct the original string of words, one needs to know that neologisms are sometimes formed this way, one needs to be knowledgeable in the field in question, and, occasionally, one has to be lucky.

[2]Which, strangely enough, is derived from Greek words meaning "river horse."

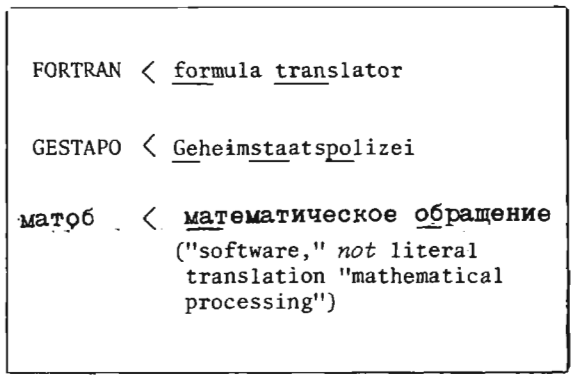


Fig. 11

Certainly, acquiring proficiency in reading any foreign language is not easy. However, it may be easier than you think. It may also be more necessary than you think. It might also be fun.

[3]Sometimes, when transliterating a foreign word or name, a particular Chinese character will be selected for its sound *and also* its meaning or connotation. Hence, the character 馬 would be particularly appropriate in transliterating, say, the name of a British cavalry officer. In Pl's *Quarterly Review for Linguists* (February 1972) [redacted] said, "It was recently brought to my attention by a British friend, [redacted] that the Chinese term for that venerable cocktail, the martini 馬提尼 could have been more imaginatively written as 馬踢你 (also pronounced MA-TI-NI, but meaning 'horse-kick-you')." Actually, although the Chinese transliteration is standard, some Chinese do appreciate the "horse-kick-you" pun. There is at least one other transliterated foreign word in which the *sound* of a syllable got confused with the *meaning* of the Chinese character used to represent it. According to *Aspects of Chinese Sociolinguistics: Essays by Yuen Ren Chao* (Stanford University Press, Stanford, 1976, p. 398), "In the Shanghai tramway system the cars did not run all night and passengers going out nights would naturally be interested in the last cars on various lines. . . But the penultimate car was also of practical importance." According to the essayist, the folks in Shanghai transliterated the British pronunciation of "last car" by three Chinese characters, roughly pronounced, in Shanghai, LA SI KA. Since the middle character, in addition to having the sound SI, also has the meaning "four," and the number before four is "three" (the Chinese character for which is pronounced SAN), the obvious move, at least in Shanghai, was to list both the last car (LA SI KA) and the next-to-last car (LA SAN KA).

P.L. 86-36

P.L. 86-36

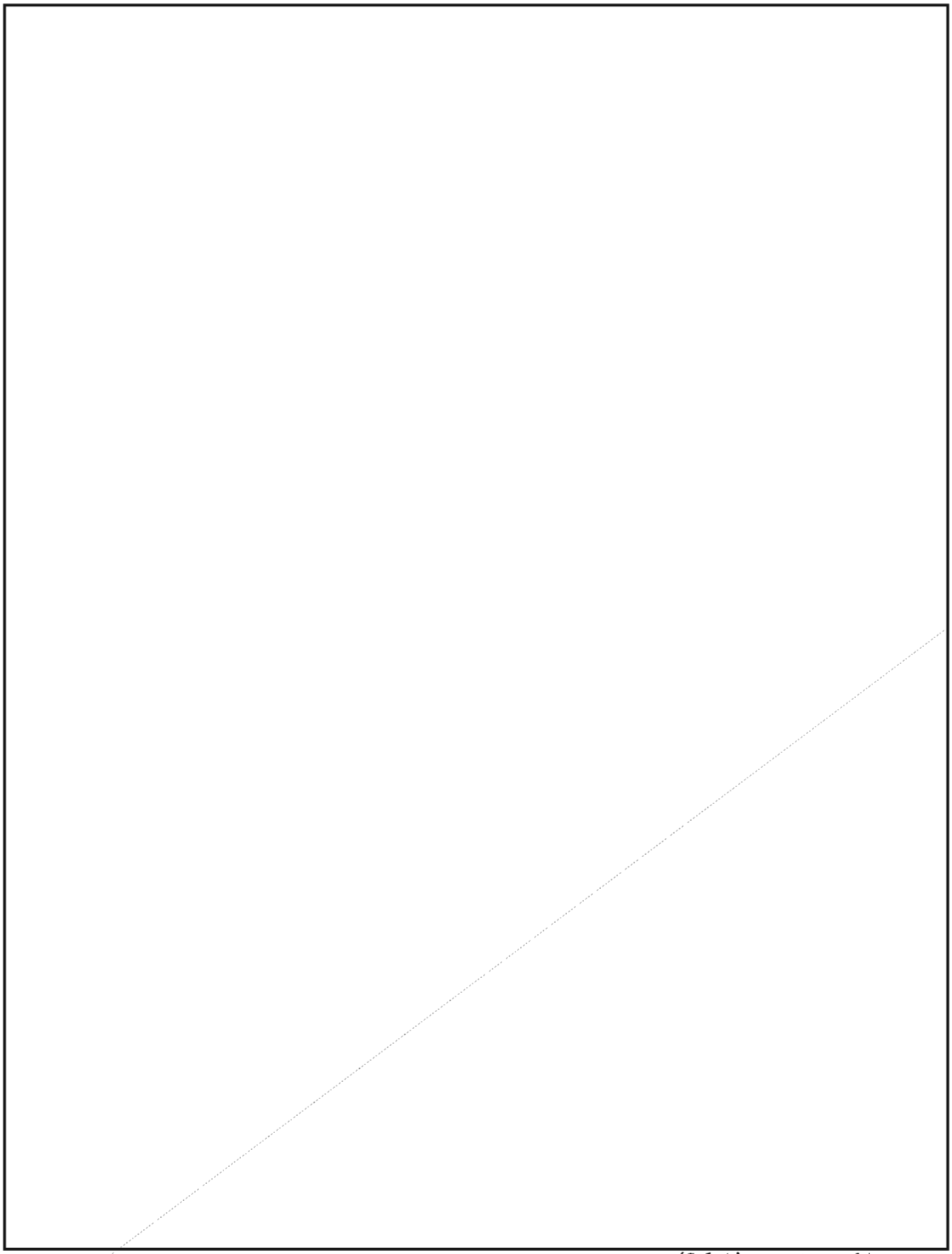
NSA-crostic No.10

By A.J.S.

The quotation on the next page was taken from the published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS *WORDS*

DOCID: 4009804



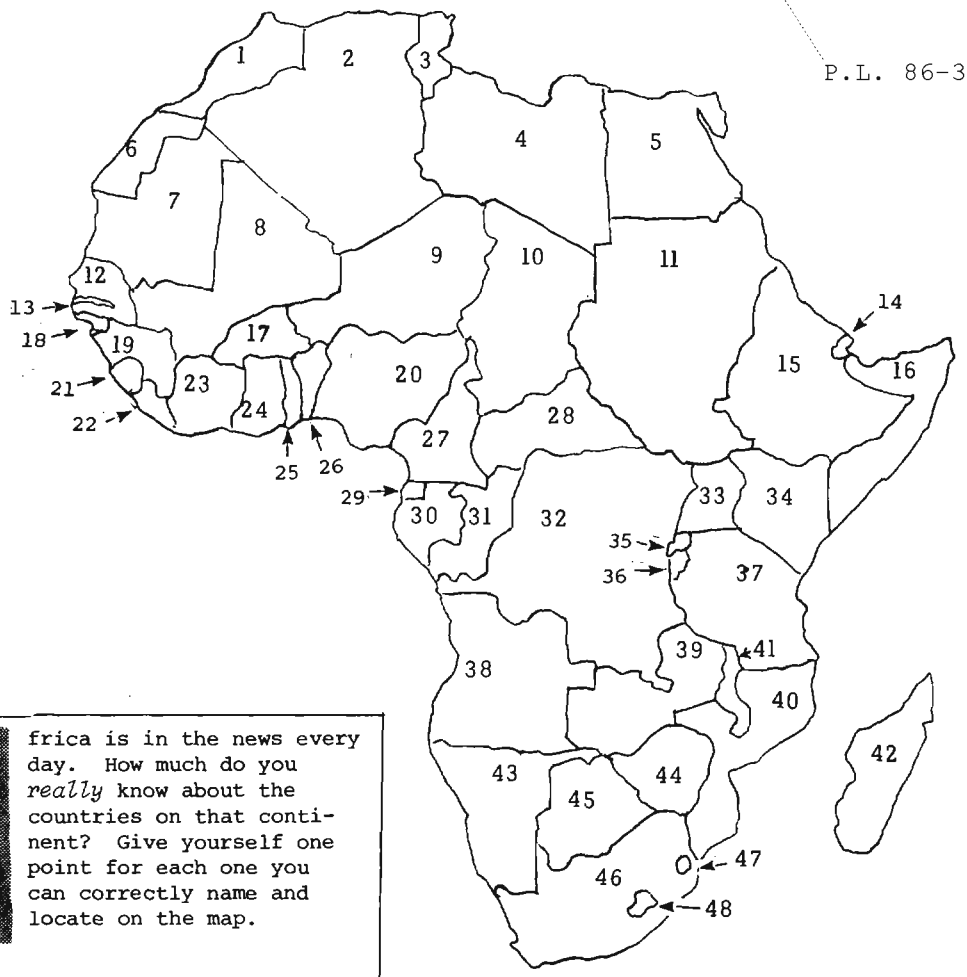
(Solution next month)

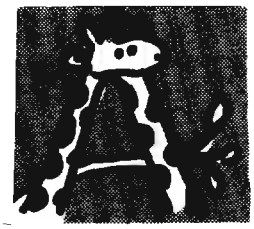
P.L. 86-36

HOW MANY AFRICAN COUNTRIES CAN YOU SPOT?

D5

P.L. 86-36





frica is in the news every day. How much do you *really* know about the countries on that continent? Give yourself one point for each one you can correctly name and locate on the map.

0-8	Very poor!
8-12	Not too bad
12-16	Getting better
17-20	Excellent
Over 20	If you didn't cheat, you're in the genius category!

(Answers on page 20)

DOCID: 4009804

P.L. 86-36

LANGVAGE PROCESSING FORVM

[redacted] Pxvi
[redacted] Pxvi

Language processing has undergone many changes at NSA as a result of such varied pressures as reorganizations, increases and decreases in personnel, and the influences of data-processing procedures. Changes in technology and target-country practices, as well as shifting policies and priorities, have placed requirements for flexibility upon a discipline which by its nature responds slowly to change (language acquisition is a time-consuming process).

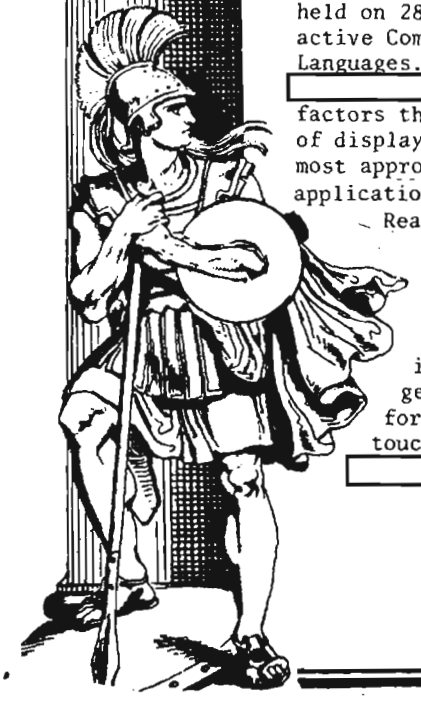
In order to keep pace with rapidly changing demands, good communication is essential. To provide a central focus for persons in various elements, P1 has inaugurated a LANGUAGE PROCESSING FORUM. Meetings of this forum feature speakers and discussion on a focus topic. Audience participation is encouraged in order to obtain views, opinions, and information about successes and failures from a broad sample of persons actively engaged in language processing.

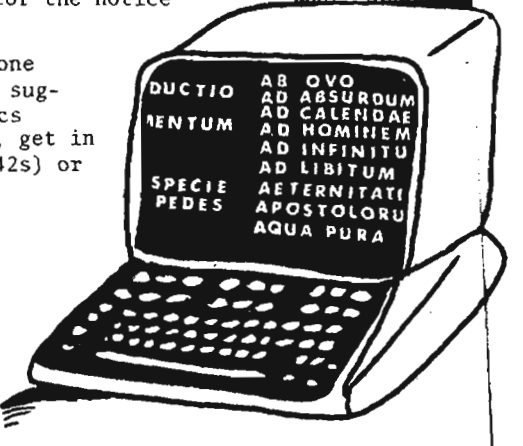
Minutes of each forum meeting, including suggestions, recommendations, criticisms expressed, and language-processing requirements resulting therefrom, will be distributed to a mailing list of interested persons and to all managers of elements having potential interest in the topic discussed.

The impact of CRT (cathode-ray tube) technology upon language processing provides the content of at least the first two meetings. The first of these, which was held on 28 October, was titled "The Impact of Interactive Computer Graphics on the Processing of Ideographic Languages." A panel consisting of [redacted] led a discussion focusing on factors that must be considered in choosing which type of display system (full-graphics or alphanumeric) is most appropriate for a given [redacted] processing application. The second program, "Is an Interactive CRT Really the Answer (And, If So, What Was the Question)?", is planned for late November or early December. Look for the notice giving time and place.

Attendance is open to anyone interested in the issue. To suggest language-processing topics for consideration by the forum, get in touch with [redacted] (P16, x5642s) or [redacted] (P16, x4032s).

P.L. 86-36





C.A.A. NEWS

P14

COMMUNICATIONS ANALYSIS ASSOCIATION

CAA Board:

President:
President-elect: David Gaddy, 324/s
Treasurer:
Secretary:
Board members:

November presentation:

All you ever wanted to know about [redacted] what's *really* happening [redacted] (and revealed by [redacted] will be re-
Watch for the notices.

"So here I am a professional! Now what? Where do I go from here?" That's a good question. [redacted] mentioned postprofessional development in his letter, published here last month. What do you think about it? What should we be doing about it? Or do you care, one way or the other? The CAA Board is beginning to think about maybe having a round table discussion about postprofessional development, sometime after the first of the year. Are you interested? If you are, then send a note or call a board member and tell us what you think.

P.L. 86-36

Membership drive:

Some of you folks out there have always wanted to be a member of the CAA but you just haven't known how to go about joining -- isn't that right? Well, anyway, *now* is the time to join. Come to one of our presentations a few minutes early. Or call one of the board members. If you don't have a phone -- write (to me). Dues are $1.00 per year.

Did you attend the September presentation by Whitney Reed ("Doing It Remotely"), which described his experiences in developing and managing the B Remote Operating Facility? If you did, did you remember to sign up for that special tour of BROF?

It rhymes with "tickle"

I hardly know where to start. The Five-Foot Shelf of Great Cryptologic Literature (abbreviated FFSGCL and pronounced "foffs-gickle," for all those who *have* to pronounce abbreviations) actually exists. A large box arrived in my office not long ago, containing two large notebooks chock full of interesting reading about COMSEC -- courtesy of Harry Daniels and [redacted] These books contain a series of lectures on COMSEC by David G. Boak, as well as surveys and examples of current systems and equipment, and lots of other interesting goodies. You can find these books (as soon as *I* finish reading them) on the *shelf* in the Cryptologic Collection of the P1 Technical Library, Room 3W076. [redacted] 4017s, can help you find the shelf. Among the books that have been suggested by other people are: Sinkov, *Cryptanalysis;* Kahn, *Codebreakers;* Blair, *Silent Victory;* Pratt, *Secret and Urgent;* H. F. Gaines, *Cryptanalysis* (Dover); L. D. Smith, *Cryptography* (Dover); Winterbotham, *Ultra Secret.*

The point of the shelf, you will remember, is that each item describes the activities of a skill field to people *outside* that skill field (i.e., in other cryptologic skill fields).

Not everyone agrees about what should be on the shelf. Some people are themselves aggressive seekers of information about what's going on in other people's territories, and these people were quick to share with me where they find their information (Project Management Directives, journals and periodicals of the services and the SCAs, DDT's *TeleCOMMENTS,* etc.). But far too many people in our business spend most of their energy just keeping up with what's happening in their *own* field. Reaching *this* audience when writing about some *other* field isn't easy -- I don't think it happens nearly as often as many authors think it does. Most cryptologic writing, unfortunately, is aimed at "insiders" -- not just people inside cryptology, but, rather, the people inside the writer's skill field.

"Can you tell me a little more about what you do?" "Didn't you read my article/report/paper? It's all there in black and white!" "Yes, I read it. That's why I'm calling. . ."

Think back over what cryptologic writing you can remember that made an impression upon you, where the subject was outside your own field or pet project areas. How many different writers (or articles/reports/papers) can you recall?

It's not easy to write about your favorite subject in such a way that an "outsider" will completely understand you and sense your enthusiasm. If you take this statement as a personal challenge, try doing it and send in your article to CRYPTOLOG. It's just the sort of thing that CRYPTOLOG was set up to publish.

By the way, Dave Gaddy now claims that the five-foot shelf wasn't his idea after all! (I think he just doesn't want to find out how we will pronounce DGFFSGCL!)

WHAT EVER DOES "HOWEVER" MEAN?

G03

English adverbials are poorly understood by most writers, whether they be innovative writers, report writers, or translators. The difficulty is greatly enhanced for translators if they tend to look upon lexical items in a foreign language as having one-for-one "word" correspondences in English, i.e., they have a once-a-word-always-a-word mentality. The function of the word is oftentimes more important than its gloss -- its so-called meaning or equivalent.

As an example, let us take the English lexical item "however." Writers and translators have great difficulty with this word. They have been exposed to teachers or books maintaining that "but" cannot initiate a sentence, much less a paragraph, and must be replaced by the more elegant "however." Then, too, their sources stress that words such as "however," "nevertheless," etc. must be set off by commas. But see page 49a of *Webster's Third New International Dictionary* for usage of the comma with transitional words and expressions (i.e. adverbials):

> "4.1.3. Commas set off transitional words and expressions (as *on the contrary, on the other hand, consequently, furthermore, moreover, nevertheless, therefore*) whenever they are or would be spoken with the adjacent rising or sustained pauses that indicate subordinate matter. 'The question, however, remains unsettled.' 'Nevertheless, we shall go.' 'On the contrary, under the rules a vote is in order.'
>
> "4.1.3.1. Such expressions may occur in context so as to be spoken without significant pauses and may likewise require no punctuation. 'We shall therefore proceed with the operation.' 'The weaklings will consequently be forced to drop out.' 'A clear-cut decision is on the other hand too much to expect.'"

The translator has the added difficulty of the fact that oftentimes a number of words in the foreign language can be translated as "however" in English. But oftentimes the dictionaries label the foreign word as some given part of speech in that language and then give English glosses which are not the same part of speech in English, and this does become confusing!

So, let's take a look at this English word "however." What part of speech *is* it? It's a conjunction, a concessive conjunct, and an interrogative. In each function its placement in a clause or sentence and its punctuation are fixed. As a conjunction, "however" is a simple subordinating conjunction. It is also one of the so-called *wh*-elements which are initial markers of subordination in interrogative *wh*-clauses, in relative *wh*-clauses, and in conditional-concessive *wh*-clauses (i.e. *who/whom/whose, which, where, when, whether, how, what, why, whoever, whomever, which ever, wherever, whenever, whatever, however*). "However" is also a concessive conjunct, i. e., it is an adverbial that occurs peripherally in clause structures but is primarily connective in function. Adverbials as a class can occur in four positions in the declarative form of a clause:

- I - initial position (i.e., before the subject)
- M1 - medial position #1:
  - (a) immediately before the operator (DO, etc.), or
  - (b) between two auxiliaries.
- M2 - medial position #2:
  - (a) immediately before the verb, or
  - (b) before the complement in intensive BE-clauses, e. g. "He is soon to be transferred."
- E - end position:
  - (a) after an intransitive verb, or
  - (b) after an object or complement.

Concessive conjuncts are contrastive, i.e., they signal the unexpected, surprising nature of what is being said in view of what was said just before:

> "He has been in office for only a few months. He has, *however*, achieved more than any of his predecessors."

But note that when "however" is positioned initially it is sometimes used in conversation to indicate that the speaker wishes to change the subject:

> "I think you had no right to speak to him in that way. *However*, I really wanted to let you know what I think about your recent letters to me."

Conjuncts also occur as correlatives reinforcing particular subordinators: "however" is one of eight conjuncts (*yet, still, however, nevertheless, nonetheless, notwithstanding, anyway, anyhow*) that can occur after five concessive subordinators (*although, [even] though, while, granted [that], even if*). "However" as a conjunct (along with the antithetic "then" and "though") can also be linked to a preceding clause by the coordinator "but"*. "However"

* In the article "The Legendary William F. Friedman" (*NSA Cryptologic Spectrum*, Winter 1974, Vol. 4, No. 1), Lambros Callimahos mentions that a code message that Mr. Friedman broke started with the words "But though. . ."

does not follow the "but" immediately; i.e., it cannot be initial unless there is no conjunction in front of it:

> "You can phone the doctor if you like, *but* I very much doubt, *however*, whether he'll come out on a Saturday night."
>
> "You can phone the doctor if you like. *However*, I very much doubt whether he'll come out on a Saturday night."

As a subordinator, "however" can occur in a nominal clause:

Subject:	"*However the election goes* will depend on the situation."
Direct object:	"I can't imagine *however he got into that situation*"; "I can't imagine *how he ever got into that situation.*"
Subject complement:	"The question is not *however it came up* but who will solve it."
Appositive:	"My original question, *however will he go to the Middle East this time*, has not been answered."
Adverbial complement:	"I wasn't certain *however long he'd been here.*"
Prepositional complement:	"No one was consulted *in however small a way.*"

But "however" more usually occurs as an adverbial clause:

> "He is welcome *however he comes.*"
> "*However much advice he gets*, he does exactly as he sees fit."

Note that in restricted circumstances (namely, with an abstract noun-phrase subject of a subject-verb-complement clause), the verb BE can be omitted from a universal conditional-concessive clause:

> "*However great the pitfalls (are)*, we must do out best to succeed."

This particular type of clause can also be treated as an optative subjunctive or as front-placing of the main verb:

> "*However that may be*, he will do his best";
> "*Be that as it may*, he will do his best."

"However" is also one of a group of informal intensificatory question-words (*whoever, whatever, whichever, whenever, wherever, however*) but these words are usually spelled as two separate words and thus distinguished from the subordinating *wh*-words. There are various ways of intensifying the emotive effect of a *wh*-question, however:

> "*How ever* did you think of that?"; "*However* did you think of that!"; "*How in heaven's name* did you think of that?"; etc.

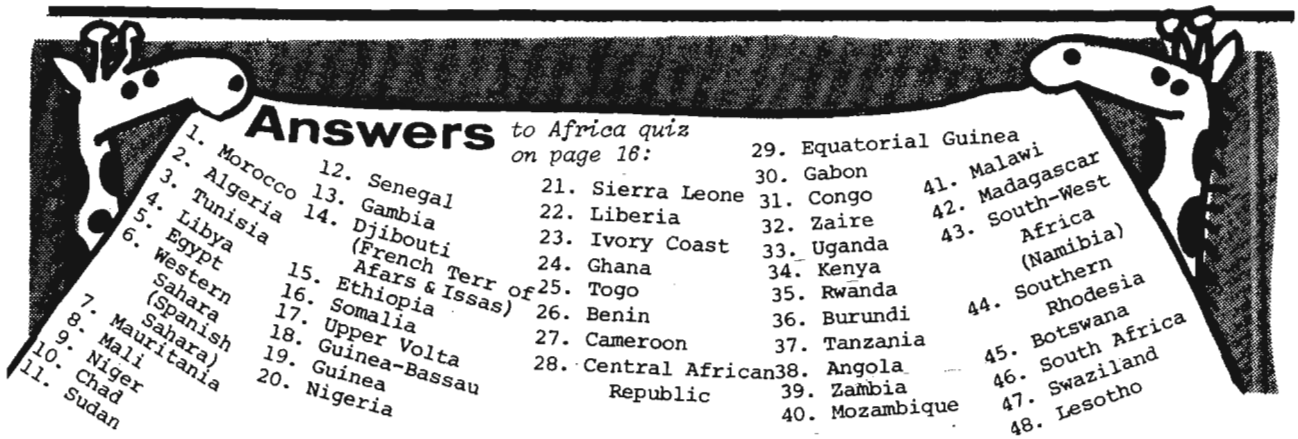
Another use of "however" is for premodification of a maximizer (*fully, thoroughly, totally, completely, perfectly, entirely, utterly, extremely, absolutely*) to form the opening of a dependent adverbial clause:

> "*However* totally they believed in the leader's integrity, they were prepared to examine his actions dispassionately."

Conjuncts in initial position extend the scope of the adverbial to subsequent clauses:

> "David doesn't have any money of his own. *However*, he can ask his parents for some, and he might be able to borrow a small amount from his sister."

This small excursus into the syntax and semantics of "however" is a slight indication of the complexity of adverbials in English and is illustrative of the insights to be gained from a linguistically sound analysis of English. Now, all that remains is to do a similar analysis of the words in some one foreign language that can be glossed as "however"; and, then, do a comparative syntactic and semantic linguistic analysis of this lexical item which is "however" in English and which, in translation from a foreign language, can at times be glossed as "however."



DOCID: 4009804

LETTERS

[redacted] *recently received the following letter in response to his article "Early Days in NSA Computing" (CRYPTOLOG, August 1977).*

Russ:

Congratulations on your fine article "Early Days in NSA Computing." Since I consider myself one of the parents of ABNER, it was especially interesting to me.

It's too bad we don't often get the chance to mention names of people in some of the things we write for publication. An example is the enclosed article "Influence of U.S. Cryptologic Organizations on the Digital Computer Industry," which you may have seen. In case you haven't, I've inscribed this copy. I originally had a long list of names for the acknowledgements paragraph. But since it was written for distribution outside (yes, many things we used to consider classified may now be said out loud!), I was told it would be safer and give less annoyance to those named if we left off the list of names. Some copies have already been distributed, and it's expected the article will eventually have its impact on students of computer history. So I note that you mention [redacted] who indeed did contribute brilliant work on ABNER. Too bad you didn't also recognize Ray Bowman and [redacted] who were really the ones in charge of the engineering. But that's the way with naming names; one doesn't know where to leave off, for fear of leaving somebody out!

As a re-employed retiree, I am working for D4, the people in charge of answering requests under the Freedom of Information Act. My extension is 4656s or, at FANX-III, 8214s. I am starting work on an article about early machines including special-purpose ones (pre-computer), provided the story can be written for uncleared readers. It will be like walking a tightrope, so I'm not sure what good the result will be.

Thanks again for a nice job on ABNER and the 701, etc.

[redacted] D4

Editor's note:

The Introduction to [redacted] "Influence of U.S. Cryptologic Organizations on the Digital Computer Industry" (National Security Agency, May 1977, ii + 36 pp., Unclassified) contains the following statement:

> "An unfortunate aspect of . . . historical accounts of computer lore is the omission (conspicuously, to some of us) of mention of the National Security Agency, or of the contributions by that Agency which helped in laying the foundation of the computer industry. The NSA over the years has been required to observe a policy of anonymity, and with good reason. But, in this age of maturing appreciation of the role of computers in nearly all civilized endeavors, it is time for acknowledging that NSA, too, uses computers. In fact, that Agency's contributions to the computer industry have been outstanding. This article relates for the first time some of the details behind the NSA computer story."

P.L. 86-36

[redacted] has told us that he has several extra copies of his article available, and that any CRYPTOLOG reader who would like to have one can contact either him (on 4656s or 8214s) or [redacted] T1213, Room 2N090, 5801s. (U)

In addition to [redacted] letter, which wasn't even addressed to us, we received two genuine Letters to the Editor. Both of them -- hereinunder abridged for reasons of mock modesty -- would like to correct errors of fact.

To the Editor, CRYPTOLOG:

In the article "Expletives Deleted?" (CRYPTOLOG, August 1977), your reference to *sh-/sk-* pairs in English is slightly misleading. It is true that the Greek *skatos* is etymologically related to the appropriate *sh-/sk-* pair in English. However, the true origin of these pairs lies in the Old Norse contributions to English, dating from the period of the Viking invasions of Britain. Typically, in these pairs, such as *skoot/shoot* or *skirl/shrill*, the *sk-* word comes from Old Norse and the *sh-* comes from its cousin in Anglo-Saxon.

[redacted] A542

To the Editor, CRYPTOLOG:

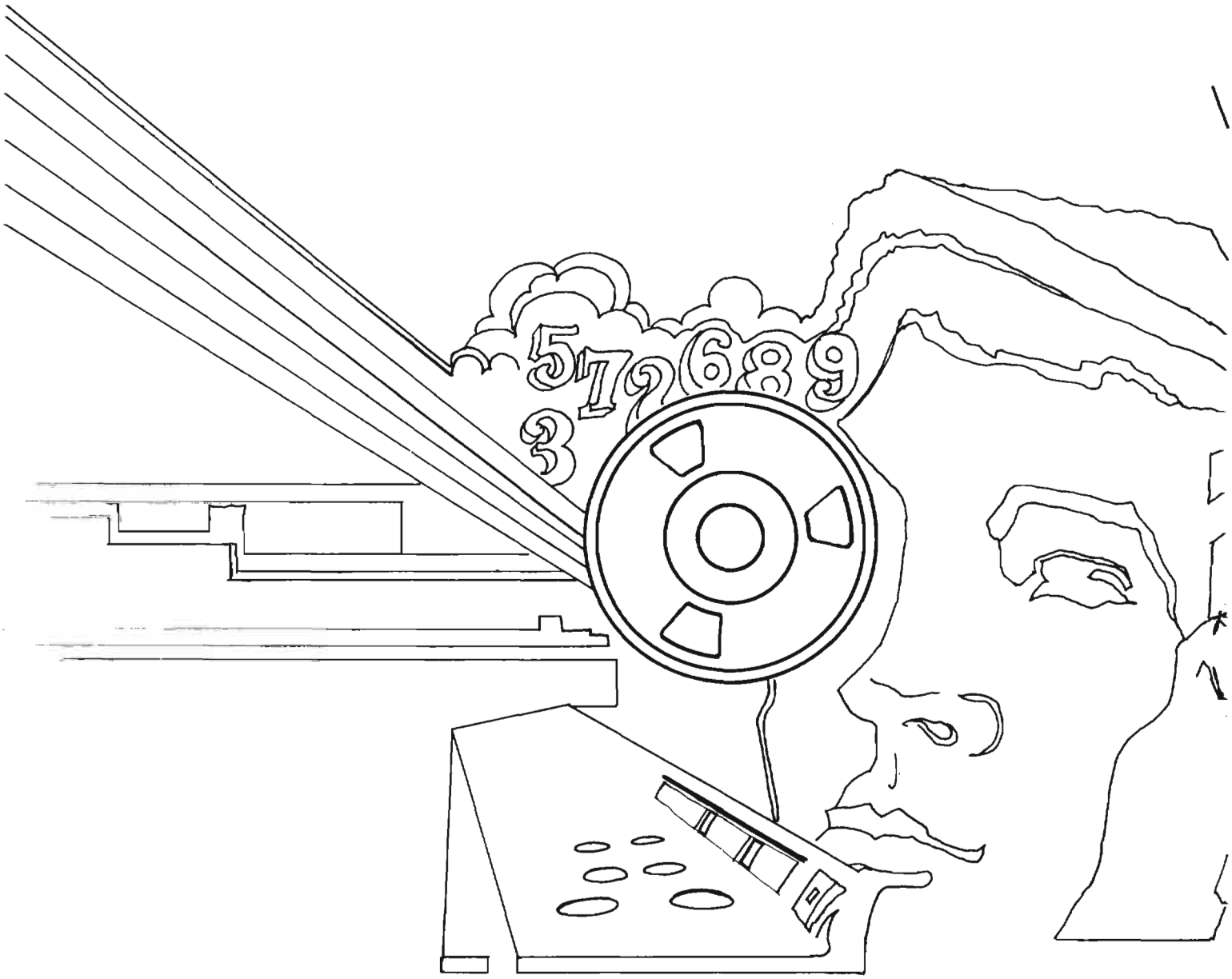
Your contention, in "Expletives Deleted?", that Ferdinand de Lesseps was "creator" of the Panama Canal requires some clarification. Isthmus be realized that this statement is not entirely accurate. If we study canal roots, we find that, although Monsieur's company was successful in developing the Suez Canal, it failed in Panama. (It finally took Yankee ingenuity to "create" it; among those who know canals best, that's alimentary.) De Lesseps these **bleep!** inaccuracies, the better.

Howard C. Heron, S14

Editor's reply:

I'm always pleased to publicize my own mistakes (as I tell my kids, "It proves I'm human!"). I really don't mind these two clarifications at all! Now, if someone had challenged my etymology of the term "raspberry," I would have been completely deflated. (U)

P1-Nov 77-S3-25567


5 7 2 6 8 9
3

DOCID: 4009803

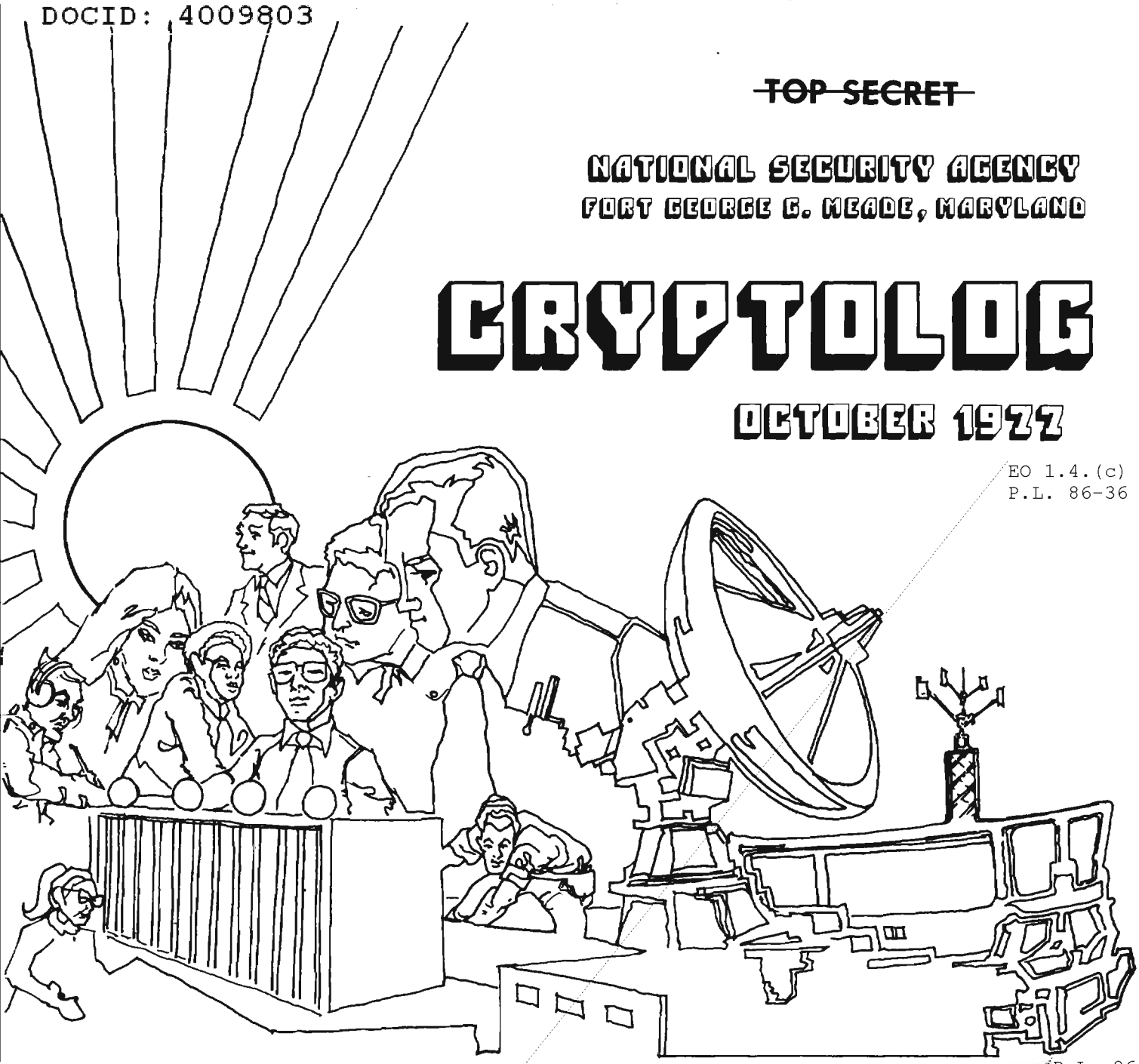
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

OCTOBER 1977

EO 1.4.(c)
P.L. 86-36



P.L. 86-36

PARTNERS IN THE EXCITING FUTURE OF SIGINT... Howard E. Rosenblum.....1
CLASSIFICATION CORNER: WHO SAID?..... [redacted].....3
HUMAN FACTORS WITH MICROFICHE READERS.... Don Snow.....4
[redacted]..... [redacted].....7
WHICH NUMBERING SYSTEM SHOULD WE USE?.....Jess Asken.....12
CLASSIFICATION: A BIGGER PICTURE..... [redacted].....13
K1 - SCA FIELD MANAGEMENT AND EVALUATION.... [redacted].....15
PERILS OF A STATE DEPARTMENT INTERPRETER..... [redacted].....17
CAA NEWS..... [redacted].....19
GOLDEN OLDIE: ANALYZATION OF DATA..... [redacted].....20
LETTER TO THE EDITOR.....21

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009803

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. IV, No. 10 OCTOBER 1977

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

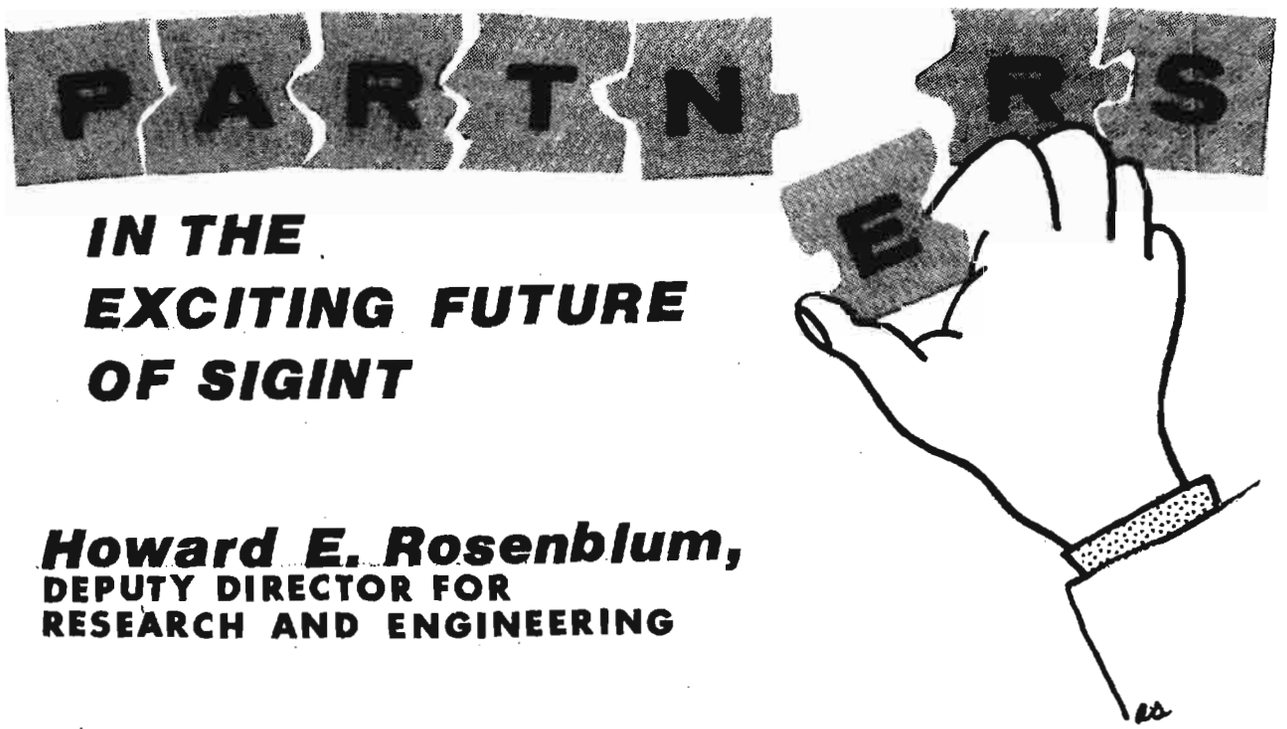
Editor in Chief.....Arthur J. Salemme (5642s)
Collection.....[redacted] (8955s)
Cryptanalysis.....[redacted] (4902s)
Language.....[redacted] (5236s)
Machine Support.....[redacted] (5303s)
Mathematics.....Reed Dawson (3957s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....[redacted] (4477s)

Production Manager.....Harry Goff (4998s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4009803



IN THE EXCITING FUTURE OF SIGINT

Howard E. Rosenblum,
DEPUTY DIRECTOR FOR RESEARCH AND ENGINEERING

Mr. Howard E. Rosenblum, Deputy Director for Research and Engineering, was the guest speaker at the April 1977 graduation ceremony for the National Senior Cryptologic Course CY-600. We considered his perceptive remarks to be of value for a much wider audience than the graduating class and asked Mr. Rosenblum for permission to publish them in CRYPTOLOG. He has kindly granted that permission, and we are now pleased to publish his talk, in a form slightly abbreviated and modified for written rather than spoken presentation.

Ed.

Distinguished guests and members of the CY-600 graduation class: I am delighted to represent Mr. Buffham, our Deputy Director, and address you at the conclusion of your 7 weeks in CY-600. I trust this course has been stimulating, that it has demonstrated the complexities of the SIGINT business, and that it related SIGINT to the Intelligence Community.

Before we get to the graduation ceremony itself, I would like to spend a few minutes with you sharing CY-600 experience and seeking some perspective. You see, I'm a graduate of CY-600 too. I attended the first course given, a pilot course, more than 10 years ago.

I have studied the current CY-600 schedule and I can see that you have covered a lot of ground. You have received tutorial background on SIGINT disciplines, presentations on NSA management, and background on the Intelligence Community. You have seen SIGINT product worldwide. You have toured CIA, NPIC, and even NSA. You have had seminars with NSA seniors and with Intelligence Community seniors. You have had slick "best of all possible worlds" types of presentations, and also some incomplete ramblings that left you uneasy and unsatisfied. You have tried to sift both types, to locate their warts and dimples. It has surely been a broad-based, mind-boggling (and spine-boggling) experience! I have also examined your roster and I see that CY-600 attendance is also broad-based. About 50 percent of you are from non-NSA organizations.

How was my CY-600 course of 10 years ago? I'll cite only the major differences. I am impressed by these differences because I believe that the differences between the first CY-600 course and the current course reflect a change in the National Security Agency and a change in the Intelligence Community, and those changes attest to the responsible maturing of both.

Comparing this course with the pilot course of 10 years ago, we see that that first course had:

- a makeshift, crowded facility,
- an all-NSA student body,
- no speakers from CIA,
- no speakers from DIA,
- no tour of CIA,
- no speakers from the Intelligence Community staff,
- no tour of NPIC,
- no seminar with DIRNSA,
- no seminar with seniors outside of NSA,
- no inputs on military support.

It's obvious that the course has come a long way!

What perspective can one gain by examining the differences between the first and the current course? The differences are not accidental: The CY-600 course has evolved under pressure from its managerial environment. NSA has become less parochial. It recognizes a "community," the Intelligence Community, and the need to be a cooperative contributing member of it. On its part, the Intelligence Community also has become less parochial: it sends students to CY-600 and participates in course presentations. The Intelligence Community thus recognizes a need to understand and cooperate with NSA. NSA and the Community recognize the need for its new wave of leaders not just to be *aware of*, but also to be a *part of* a cooperative, interactive Intelligence Community.

This is what is happening now! The Intelligence Community is slowly growing together. NSA/CSS is a real factor now. Support to military commanders has a genuine thrust. SIGINT is having an impact on tactics. There is less parochialism: "mine" is stressed less and less often, and "ours" is stressed more and more. More and more frequently, tough decisions are being made with a consideration of overall intelligence needs, rather than narrow element needs. CIA, DIA, and NSA actually talk to one another! Cooperative endeavors are under way, with joint review of research and development programs and joint projects. [redacted] The Intelligence Community structure has become ecumenical, with broad Community participation and impact.

So it *is* happening, and the changes I have noted in CY-600 are *not* accidental. The perspective of the course, its objective, is *community*. NSA and the Intelligence Community recognize and depend on each other. All of you graduates of this course -- whether students from NSA, or students from the Service Cryptologic Agencies, CIA, DIA, FBI, DOD, or the military departments -- had a two-fold purpose in participating in it: the purpose of educating yourselves as individuals, and also the purpose of building *Community teams*. As all of you got to know one another during these 7 weeks, you have learned that you are *partners*. Yes, we are all partners in our Intelligence Community future. And what a future we face together!

"May you live in exciting times!" I am told that that expression was a curse in old China, where change and excitement were to be feared. I am also told that in Turkey the same expression was a toast, a challenge given in confidence that change meant opportunity for those with ability. The Intelligence Community is living in exciting times. The world -- the balance of power -- is changing at a bewildering pace. The gathering, reporting, and use of intelligence are taking on critical importance. The Intelligence Community, using American technology, has some amazing tools: satellites for photography, for surveillance, and for communications and control; computers for selection, analysis, editing, and reporting; and technology for [redacted] intercept and analysis. We use the leading edge of semiconductor technology, cryogenics, optics, computing. . . What an exciting array!

And we have a new President, who wants to reorganize. We have a new SECDEF, who wants to reorganize. We have a new ASD C^3I, and a new DDR&E. We have more publicity, and also more controls on us. We have more requirements and fewer resources. These are exciting times indeed, with many changes, with problems and opportunities for all of us. So "live in exciting times!" and make full use of the knowledge that the National Senior Cryptologic Course has given you.

A few weeks ago I had the privilege of attending the swearing-in ceremony for the new Director of Central Intelligence. President Carter was there and addressed the group. Let me paraphrase some of his remarks. The President observed that he had been told of the Intelligence Community, but this was his first opportunity to understand its complexity. (He had just met and spoken individually with the dozen or so heads of the Community components.) He commented on how difficult it must be to ensure that such a complex is coordinated, responsive, and correct. By the way, President Carter said that he expected mistakes, just as he would make mistakes as a new President, but he stressed that they not be concealed mistakes. The President described the Intelligence Community as "damaged" -- damaged by hiding mistakes, by Watergate, by adverse publicity. He resolved to undo the damage. He said he needed good intelligence and wanted to help the Intelligence Community restore its self-confidence and, just as important, restore the confidence of the people of the United States in a Community of needed, professional, productive experts.

So intelligence -- your product, our product -- is needed at the highest level, and that need is recognized by the President, the Cabinet, economic and military planners, and military commanders. Intelligence contributes to arms limitations agreements; formulation of foreign policy; Government options early in a situation; force-structure decisions; warning; tactics and strategy development; countermeasures development; and military decisions during conflict. This range of intelligence has gotten more important to our country as our country has gotten weaker with respect to the rest of the world. Our job is to get intelligence, to protect our means and sources of getting it, and to secure our communications that carry it. And we must do it openly. We must make as much information as possible available to the news media, because our open society so dictates, and we must conduct intelligence operations on American principles, hence more open to the public than intelligence activities of other nations, yet closed enough to protect sources and methods. This process arouses wonder in our foreign

DOCID: 4009803

associates as to our openness, and arouses concern among some Americans that we still must keep some information secret.

This, then, is the challenge: Make the complex Intelligence Community work. Make it efficient. Make it responsive. Make it accurate. Keep it clean and open. We must work as a team to make this happen. CY-600 today is designed to help. My CY-600 of yesterday was not.

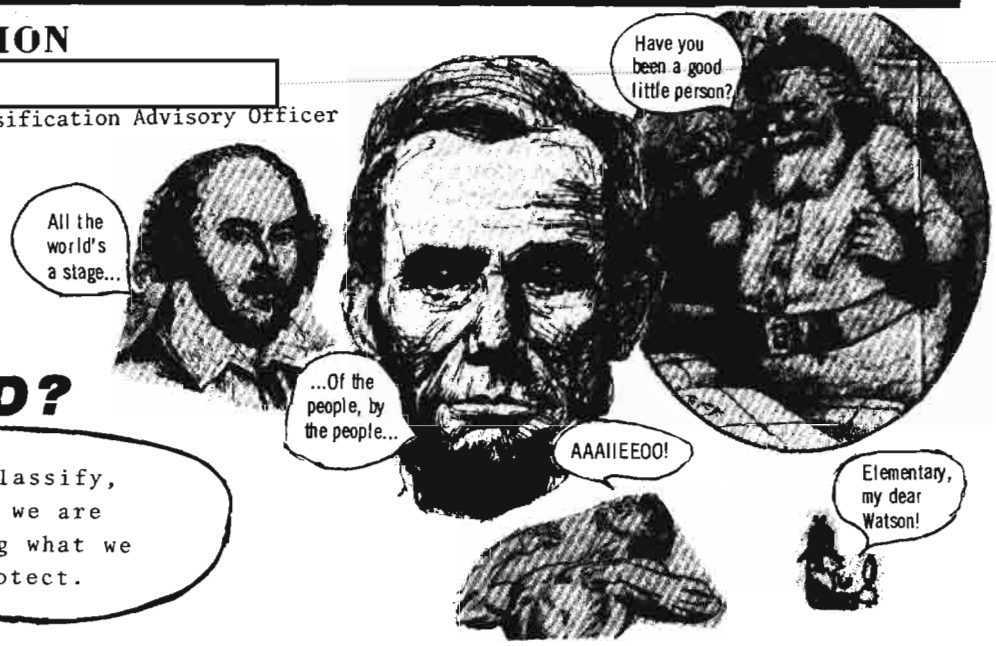
The work that goes on at NSA and throughout the Cryptologic Community is important. It reflects the technical and intellectual talents of many people. It reflects our need to function in an open society. It also reflects the courage and integrity expected of professionals in the intelligence business. The things we are doing in the future will provide American policy-makers and military commanders with critical information and reasoned assessments about the complex foreign political, economic, and military challenges to our national security and welfare. The output from our Agency, our Community, is designed to achieve and to live in peace, rather than only to protect us in time of war. What we do has become an important and permanent element of our national foreign policy and military structure.

~~(S - CCO)~~

CLASSIFICATION CORNER

By [redacted]
DDO Classification Advisory Officer

P.L. 86-36



WHO SAID?

"The less we classify, the better off we are in protecting what we have to protect."

The person who said this also believes that too much secrecy makes it harder to keep the significant secrets. This thought should be well taken by those in NSA who classify papers they originate. The problem of overclassification is real. Although the originator feels safe when he affixes a SECRET stamp on a memo that really needs only CONFIDENTIAL protection, he is only compounding a problem situation that has existed here for a long time.

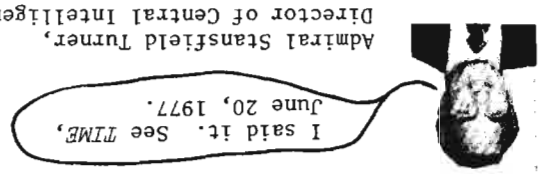
Here's a test for you. Go to a file cabinet in your work area and check the classification of the first ten folders you see. I did, and these were the results:

SECRET - CCO	6
SECRET	1
CONFIDENTIAL - CCO	2
UNCLASSIFIED	1

The higher classification wins every time.

When assigning a classification to a paper that you have originated, remember that DoD Directive 5200.IR, the NSA Classification Manual, and USSID 525 all state that, when doubt exists as to what level of classification is appropriate, or as to whether certain information should be classified at all, the resolution should favor the less restrictive treatment. That is, if you have to choose between SECRET and CONFIDENTIAL, choose CONFIDENTIAL. And if you have to choose betwen CONFIDENTIAL and UNCLASSIFIED, choose UNCLASSIFIED.

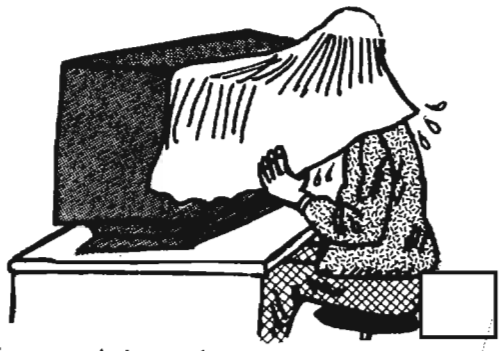
Answer:



(U)

DOCID: 4009803

HUMAN FACTORS IN THE USE OF MICROFICHE READERS AT N.S.A.



Don Snow, V1
DDO Micrographics Coordinator

The success of an applied micrographics program depends on its acceptance by the user. That acceptance may be slow or fast, and there are a number of factors which will influence it. But one very important factor -- the "user" or "human" factor -- has received scant attention until recently.

The June 1977 issue of CRYPTOLOG began with an excellent article by [redacted] on "Human Factors and Systems Design." Although he was not specific about what kind of system design or designs might be under consideration, Doug seemed to be talking about electronic data-handling systems involving, say, terminals in an analytic area, which are hooked up to a computer, and operated by the user according to instructions developed for the specific type or model of terminal.

A few days after reading Doug's article, I came across another one in the May/June 1977 issue of the *Journal of Micrographics*. This one, by Dr. Robert M. Landau (a sometime consultant to NSA) is entitled "Microfiche Reader Human Factors." In that very detailed paper, Dr. Landau sets his stage by saying,

> "The subject of human-information system interface has been studied and reported on by thousands of people. The physical, psychological and intellectual interface problems of the three major media: paper (hardcopy), micrographic (viewer screen), and electronic (TV or video screen) have been studied extensively. Almost all of the studies have related to the use of electronic (TV/video) media. Less than 100 studies have been directed to the micrographic medium; only a small number of those have been directed to the specific human factors involved in microfiche readers. . ."

That is true, at least in the formal, documented sense. However, we at NSA and our counterparts in the Intelligence Community who are involved in designing and applying micrographic systems have almost automatically included "human factors" in those applications. The reason is simple: we wanted the application to succeed. And it would really succeed only if the user or users accepted it.

Many of the factors discussed below are included in Dr. Landau's article. The main difference lies in the fact that he was addressing a readership comprising *makers* as well as users; and, among the users, people in the world of business and commerce as well as government. My article is aimed at those readers of CRYPTOLOG who are, or may become, users of microfiche and microfiche readers.

P.L. 86-36

FICHE-RELATED FACTORS

Film thickness

First-generation (i.e., "master" or "from the camera") silver halide film is usually 4 mil or 5 mil thick (.004" or .005"), regardless of whether it came from a source-document camera or from a computer-output-microfilm (COM) camera. If additional copies are required from that "master," diazo film stock is used. Diazo microfiche are 7 mil (0.007") thick, making them a bit stiffer and more durable than the silver halide "master." It is important to note that smudges or fingerprints on silver film are permanent, while such blemishes can be carefully wiped from the surface of diazo film. For that reason we always recommend that first-generation silver halide film be used as "record" or "later duplication" copy, and diazo duplicates be used as "working" copies.

Polarity

First-generation film comes from the camera in the *negative* mode -- clear characters on a dark background. Diazo duplicates retain that negative polarity; this is another "human factor" we use here. It creates far less eyestrain to look at a page of information on a reader screen if the characters are clear and the rest of the "page area" is dark, than vice versa. Admittedly, the user must become accustomed to that switch; for example, right now, you're reading this article as black words on a white page, which most hardcopy readers are used to. But the frequent user of microfiche soon appreciates the negative polarity when looking at a reader screen.

PHYSICAL CHARACTERISTICS OF READER

Controls (type and position)

This is not much of a problem at NSA, since we have standardized on one or two types of fiche readers. Remember, this article is limited to fiche readers and does not address the area of reader/printers. For the most part, at NSA we see a considerable number of W.S.I.

(Washington Scientific Industries, Inc.) Mini-Cat Model 1114D readers (Fig. 1). (The model

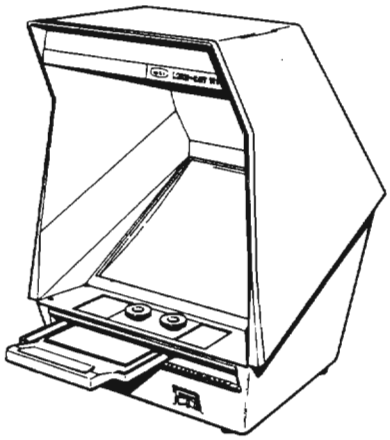


Fig. 1

number reflects the dimensions of the screen -- 11" high by 14" wide, and the "D" indicates dual lenses.) These models are hooded, with a front-projection system reflecting the image onto a screen tilted about 60° from the vertical. (That feature is a boon to people with bifocal glasses -- still another "human factor" of importance to at least *some* of us!) The fiche carrier is free-floating under the lens in use; it moves in the *opposite* direction from the sequence of pages on the fiche. Column coordinates are etched on the front edge of the carrier traverse area, and row coordinates are etched on the left and right edges of the carrier itself.

The other model is made by Realist Inc., in their VANTAGE line (Fig. 2); depending on how long or short a time the user has had it, it could be a Model I, II, X-II, COM-IV, or IV. They have the following features in common: rear projection onto a vertical screen; a free-floating carrier with a pointer attached to it (the pointer points to the particular grid area, on a

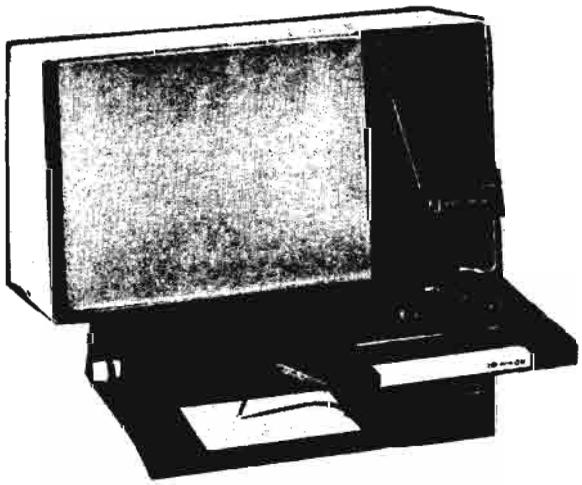


Fig. 2

fiche-size printed card, which is being projected onto the screen). The carrier moves in the *same* direction as the sequence of pages. By moving the rear of the reader body in and out, the user can increase the magnification of the lens used by as much as 25 percent, thus projecting a portion of a page in larger-than-original size.

Fiche insertion and removal

To the novice, this is always a problem. With all the fiche readers on the market, each having its own "special" optics system, the beginning user is not sure how to insert the microfiche into the carrier. Fortunately for us, the problem has been resolved. In the W.S.I. Mini-Cat model, the fiche is inserted into the carrier with the title area *face up* and toward the user. In the VANTAGE line, the fiche is inserted with the title area *face down* and toward the user. There are decals (Fig. 3) which can be applied to the

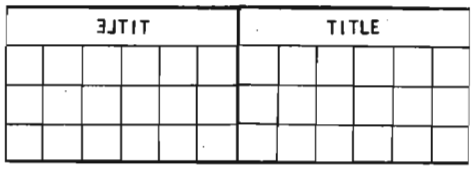


Fig. 3

carrier frame of each model, to serve as a guide for the proper insertion of the fiche the first time. *One reminder:* When placing the fiche between the glass plates of the carrier, be sure that you put it as far *right* and as far *away* from you as the carrier will accept. That will ensure that the grid coordinates will give you the desired page image. (Another "human factor" suggestion!)

Screen hood

As noted earlier, the Mini-Cat has a hood as part of its design. The VANTAGE series of models, however, have a front-mounted vertical screen. If your work area has windows, the placement of your reader is important because of ambient light. The screen should *not* face a window area; if it did, the brightness of the image on the screen would be considerably lowered by the light coming in through we window. (We have found this to be particularly true during daytime hours; moonlight doesn't seem to have nearly so much effect on screen luminance.)

If you want to maintain the brightness of the image on a VANTAGE reader, either sit so that *you* face the window, or tape a cardboard hood around the top and sides of your reader. A hood of about 4 inches should cut off most ambient light.

Screen size

Both the Mini-Cat and the VANTAGE lines have screens that are horizontally oriented. As noted earlier, the dimensions of the Mini-Cat screen are 11" high by 14" wide (the dimen-

DOCID: 4009803

sions of a regular computer print-out page). Those of the VANTAGE line are 10" high by 14" wide; however, the optics system will still project a full page-image of computer print-out information. Both models have a thin black reference strip across the middle of the screen.

Size of reader

Both readers discussed in this article are big. This is a "human factor" which the equipment makers are only now beginning to realize. There is practically a void between the bulky, desk-top readers and the "available light" hand-held viewers. The next 3 or 4 years, in my judgment, will see the development of compact, less bulky, and yet high-quality readers. (Admittedly, there are a few "attache case" types of readers on the market, but they're far from perfect, as far as human factors here at NSA are concerned.)

OTHER FACTORS

Reader availability to user

This is a tricky one, since it depends on a number of variables. The following examples are only a few of the variables:

- the number of people in a work area (section or branch), and, among those people, the number who have to refer to material on microfilm;
- the proportion of information on microform to information in hard copy;
- the number of times a day (or week) a person has to refer to microform information.

Ideally (this is currently in effect in some work areas in B Group), each analyst should have his or her own reader. Then the question of availability to the user is answered. Not only is there no competition, but the user does not have to get up and go to the reader -- it's right there on his or her desk.

All is not lost, though, if you don't find yourself in that ideal situation. A good micrographics-system designer should be able to recommend the appropriate number of readers for a work area, after taking into account the variables mentioned above, along with work patterns, schedules, deadlines, and the other things the SIGINT flesh is heir to.

Security

While it is true that information on microfiche is the same as information on hard copy (and thus subject to the same handling and storage precautions), there is one important distinction: the physical dimensions and bulk of a sheet of microfiche are far *less* (by about 98 percent) than the hard-copy version it represents. A few examples: A source-document report of over 90 pages will fit onto a single 4x6" microfiche at a 24X reduction; a computer print-out of 270 pages will also go onto a single microfiche at a 48X reduction.

When a person finishes with that report or that print-out in its hard-copy form, he or she knows that it has to be returned to its proper place in the files. If it were left on top of the desk, it would be very noticeable. Consider, though, the single microfiche version of either of those. The user must put it into a reader, in order to peruse any portion of it. When the user is finished -- *if that user is careful* -- he or she will remove it from the reader and replace it in its proper place in the microfiche files.

To help in this regard, and to make life more pleasant for the user, the Marine guards, and the char force, we have a SECURED card (Fig. 4),

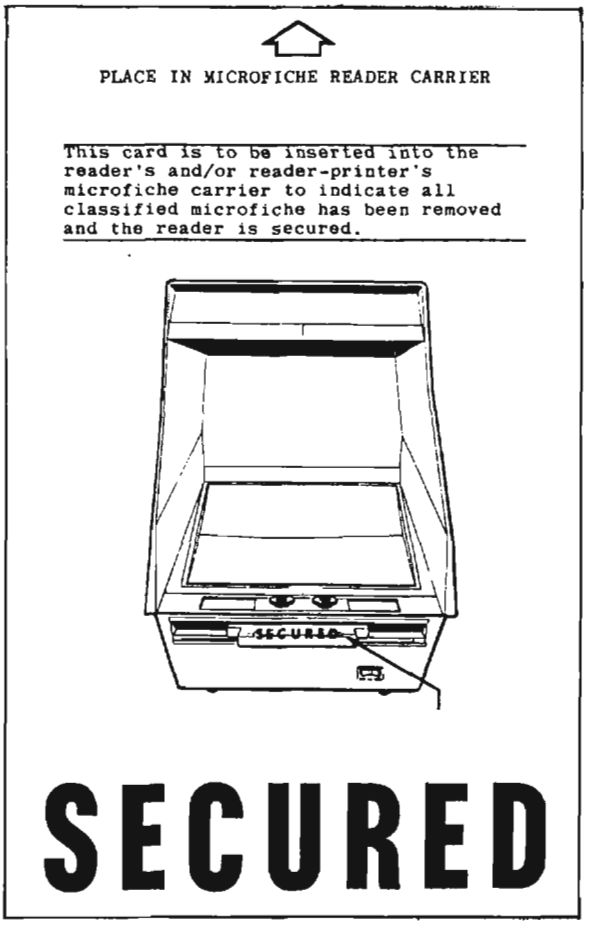


Fig. 4

which fits between the glass plates of the carrier, and indicates that ". . . classified microfiche has been removed and the reader is secured."

Summary

This article has discussed only a few of the "human factors" involved in the acceptance and effective use of microfiche readers. There are many others which -- perhaps together with a discussion of reader/printers -- will be treated in a subsequent article.

Reprints of this article available from Harry Goff, 3W076, 4998(s).

EO 1.4.(c)
P.L. 86-36

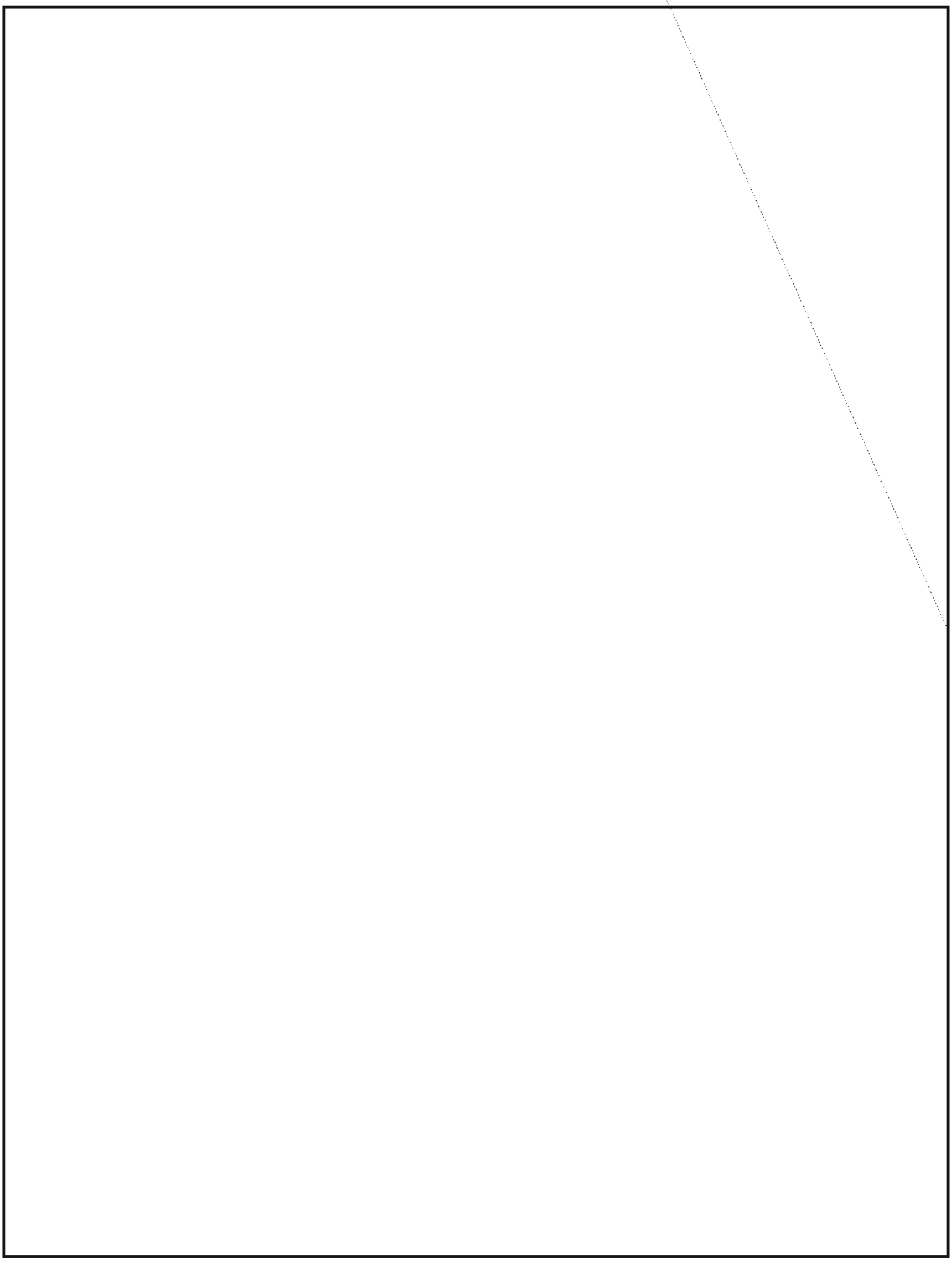
~~SECRET~~

P.L. 86-36

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

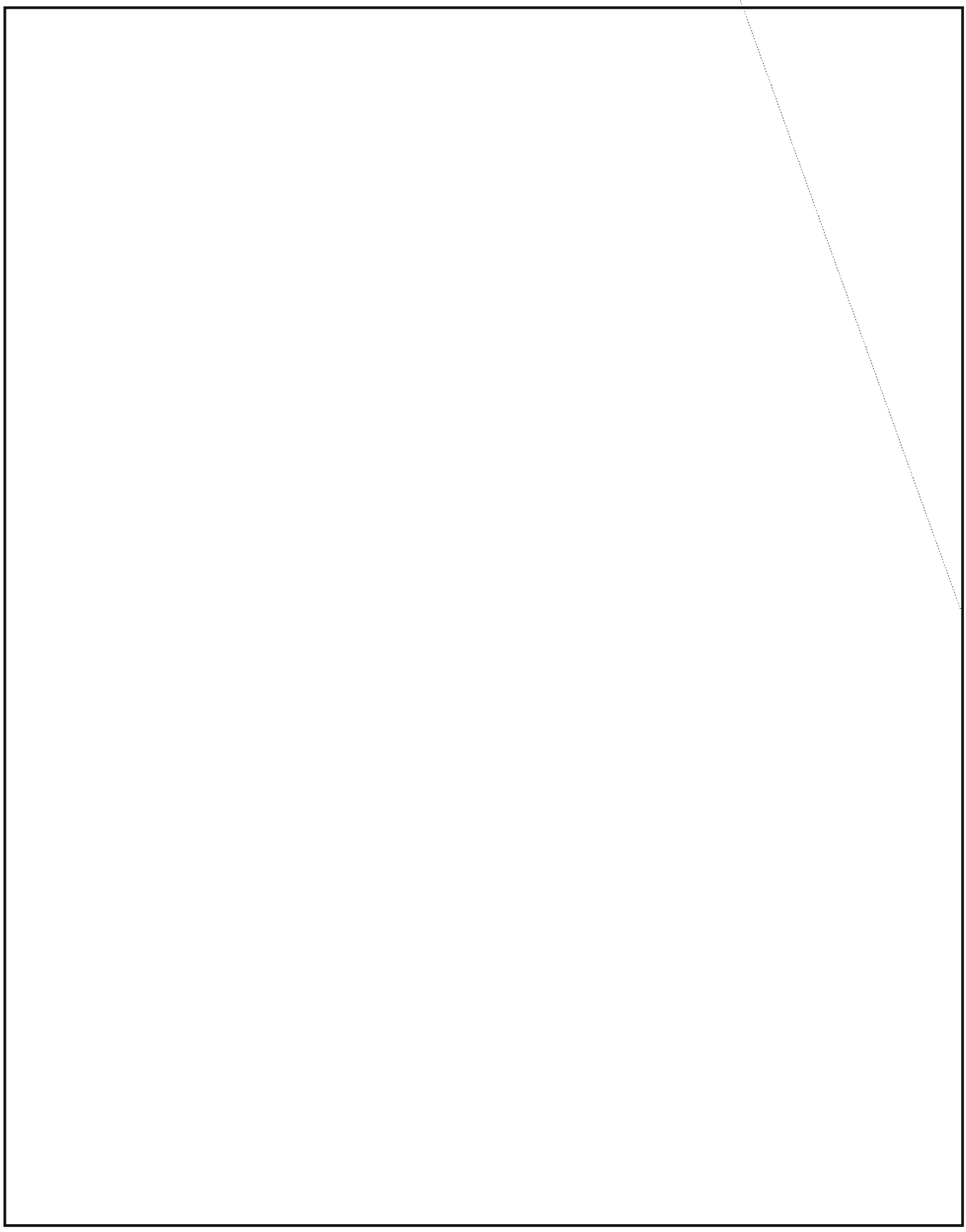
P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

~~SECRET~~



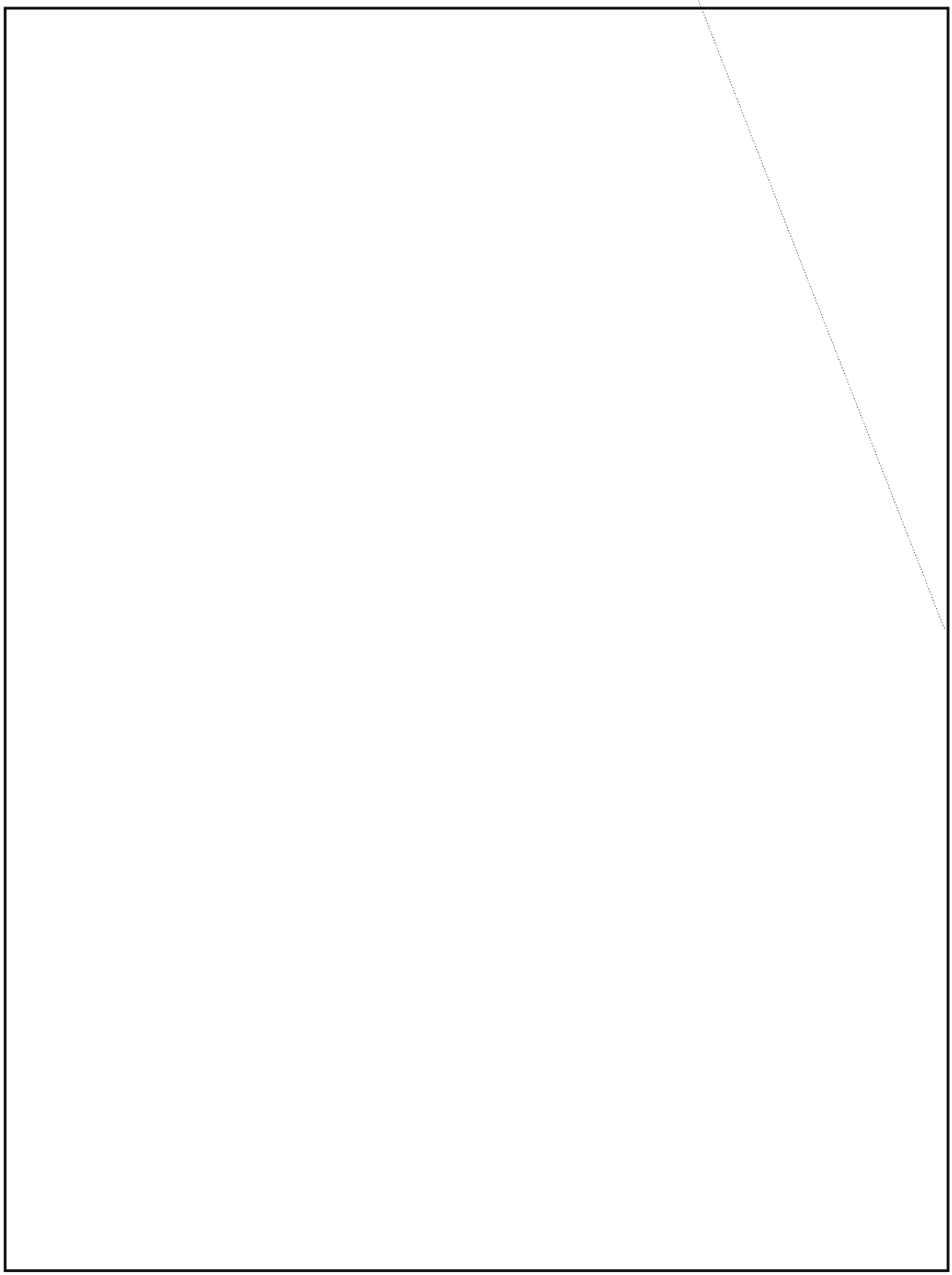
DOCID: 4009803

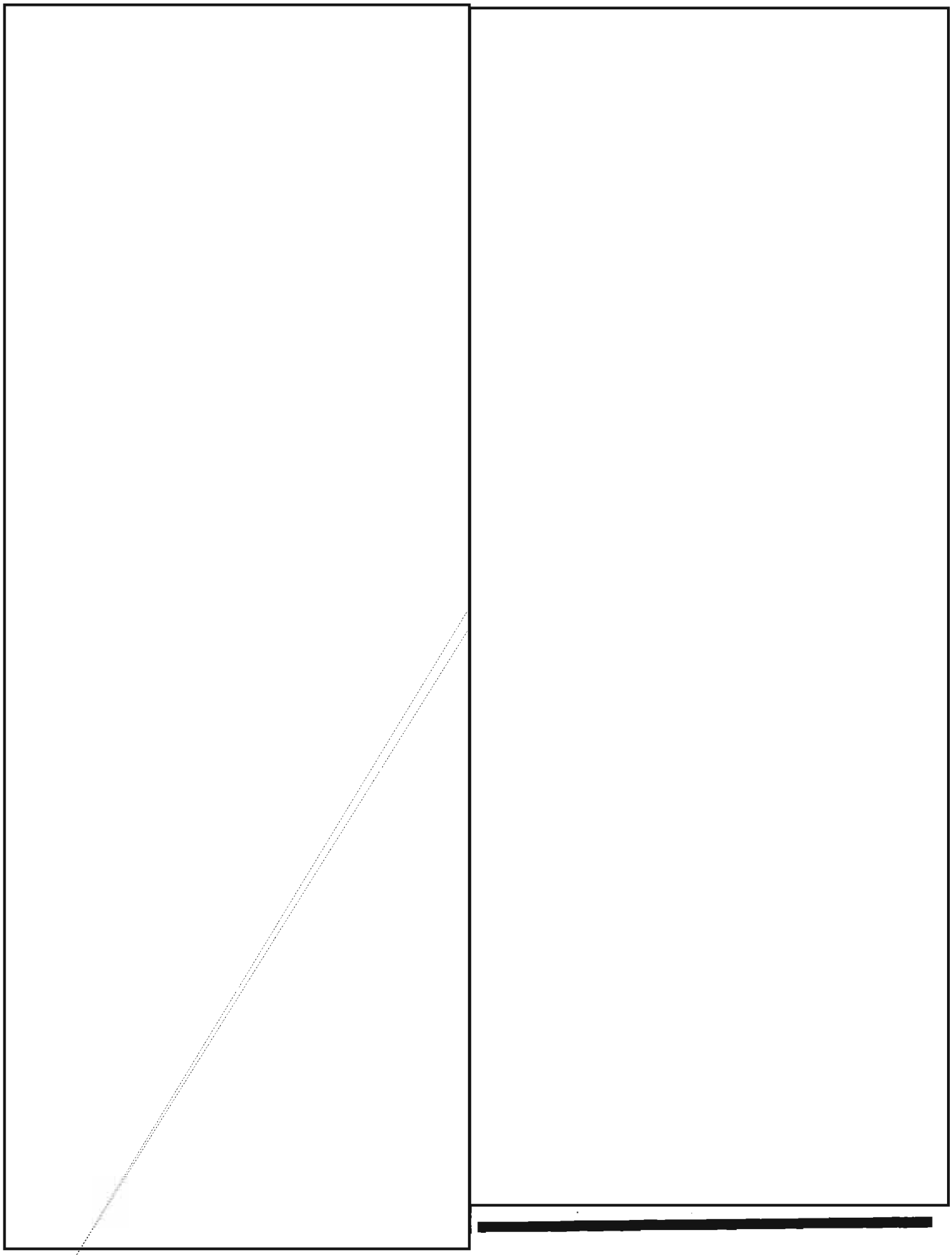
P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)



P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

~~SECRET~~





P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

DOCID: 4009803

WHICH NUMBERING SYSTEM SHOULD WE USE?

By Jess Asken

Interoffice Memorandum (Informal)

Subject: Decisions

Just a quick note to fill you in. I know you're just getting settled in, but some matters are pressing and we need to make some decisions rather quickly. I've taken the liberty of jotting down some questions and "thinking out loud" to give you some background.

We are setting up this communications center and we need to decide now what records should be kept, so that all the instructions can be written out, double-checked, and then issued to all parties concerned. What sort of numbering systems should we use? We need to decide very soon.

First of all, there's the radio station. I think we're going to need the strictest kind of control over messages coming into the station so that nothing gets lost. Radio operators can get so involved with their schedules and frequencies and transmitter adjustments that they forget all about the messages they are supposed to send. (I'm sure the Signal Officer will send down another one of those complicated signal plans he likes so much. He never seems to appreciate simplicity.)

We'll have to decide what system to use. Sometimes the simplest serial system is the best -- like a single log book for every message. Everything gets logged in the same place in the same way. That way, everything coming in gets a number and is controlled. Of course, if there is a lot of traffic, we may have to keep several logs and maybe split the traffic into "up-echelon" and "down-echelon." (Which log should contain the lateral stuff?) I wonder what sort of status reports the Staff will want from us? If they are going to require message volumes by subject matter, maybe we should organize the log books that way -- one log book for each subject. Then all we will need to do to get the volumes is pick off the last number used. Of course, if we get a batch of inexperienced people coming in, they will make a mess out of anything that isn't very simple. What do you think?

Circular messages go to more people, so they are probably subject to more queries -- maybe they should be logged separately. Servicing can get to be a headache whenever we start handling lots of messages. The busier we are, the more errors we'll make. We *could* give each message a unique date and time of file and then only accept servicing queries if they reference the file date and time; but if the messages pile up at certain heavy times of the day (such as at close of business), the file times would get pretty artificial and we wouldn't be able to measure how long it took messages to get out. The alternative is to use a date/time stamp as the message come in and, if two messages come in together and get the same date and time, don't worry about it -- they can be distinguished by their serial numbers. We need to decide which system to use.

Most servicing queries come in because the recipient can't break out the message. Maybe we need a master log in the crypto center so that servicing queries can go right in to the cipher people. I wonder whether we need a master log in the crypto center, or one log for each system. (If we use different logs for different systems, maybe each log should have a unique numbering range, so there could be no confusion about which system/log book was being referred to.)

What do you think about requiring each message writer to use some serial number system, maybe with his own organizational designator as a prefix, on all the *outgoing* messages? Then it would be a lot easier to distribute *incoming* messages that begin with "Reference your number . . ." to the *right* people. (Some people get irritated when they don't get their incoming messages.) Should we set up a standard system or let everybody set up their own?

Whatever we use, I suppose the Signal Staff will insist that all our serial numbers be enciphered. I think we need to fight that, unless they come up with more people for us. Maybe we ought to start a study *now* on the extra work load that would cause us.

We need to develop some thoughts on how often the log books will have to be replaced. If the radio station log books are replaced *daily*, we can get each day's operations reviewed the very next day for whatever corrective action is needed -- that ought to keep them sharp! Of course, the logs in the crypto center ought to stay there for a while, at least until the bulk of the servicing is over. Maybe monthly or yearly.

Maybe what we need is a master log in the message center. . .

DOCID: 4009803

CLASSIFICATION: A BIGGER PICTURE

P.L. 86-36

By [redacted] P16

Before one delves into the many specifics present in the subject of classification here at NSA, it might be useful to step back and examine the world of classification in the large. Often because of one's particular job at NSA, or even in the Intelligence Community, this global view of how the various classifications relate to each other is lost in the myriad of detail needed to perform that job adequately.

In so far as the cryptologic community is concerned, the world of classification can be described at its most absolute level by Fig. 1. This diagram takes into account the National Level classification, while also showing *the* three compartments with their interrelationships. The National Level classifications are represented by the area of the rectangle outside the three circles, which themselves represent the individual compartments.

It may be surprising to hear that there are only three compartments. The colloquial use of that word in the shop talk at NSA is often imprecise and leads one to draw erroneous conclusions. A compartment is a special control structure in the Intelligence Community controlled by a National Level agency. Access to the information contained in the compartment requires an oath to abide by its special controls and an indoctrination. Compartments have unique codewords with which to protect the specific information, along with a "channel." This is most notably seen in the "Handle via ---- channels only" and "Appended documents contain codeword material" caveats.

This is as opposed to special access briefings used to control information to very specific

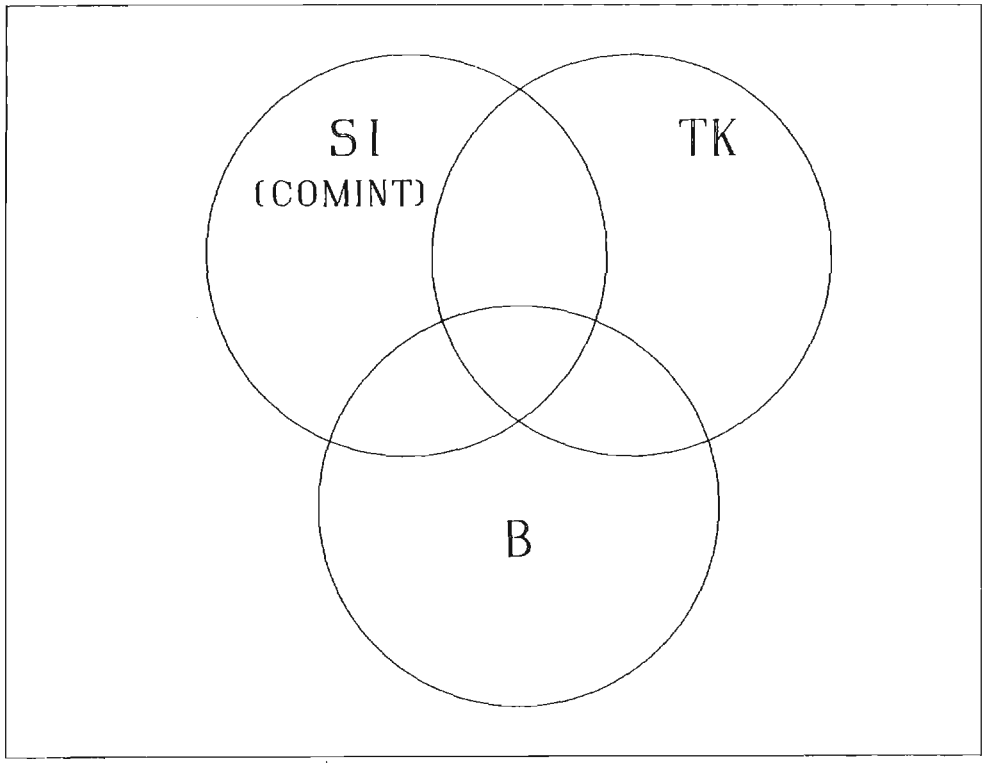


Fig. 1. The Classification World

DOCID: 4009803

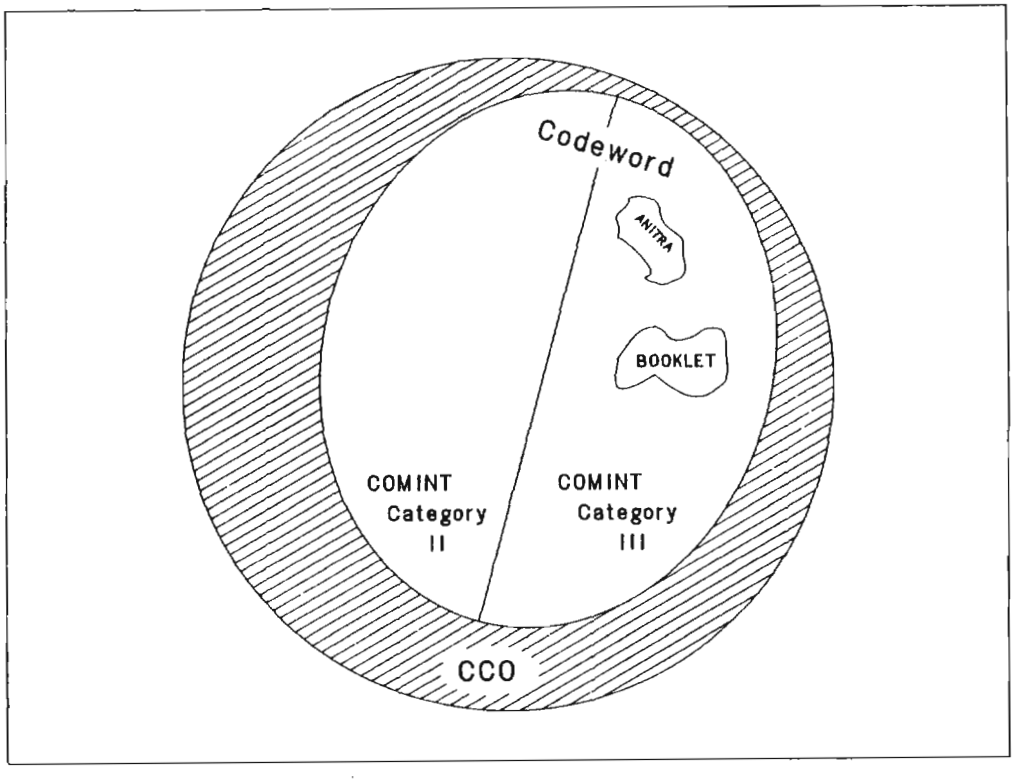


Fig. 2. COMINT Classification

projects, unlike the very broad nature of the information controlled by a compartment. Special access briefings are controlled by the office involved in the project. These accesses do not have codewords but merely append the name of the special access clearance to the appropriate classification following any necessary codewords. Hence we might have a classification "TOP SECRET UMBRA DESKTOP" if there was a project which required access to the material controlled by a special access named DESKTOP.

The three compartments of interest to the cryptologic community are COMINT (referred to as Special Intelligence by those outside this compartment), TK, and B. Each can be easily distinguished by the type of codeword used. COMINT codewords always have five letters (e.g., UMBRA, SPOKE, GLINT): TK codewords have four; and B codewords, six. Each has its own special channel and National-Level OPI. It often happens, however, that some specific project or piece of intelligence falls under more than one of these compartments. For this reason, the circles in Fig. 1 are mutually overlapping. Such a piece of information would have to bear the caveat: "Handle via ----- and ***** channels jointly." The names used for special access, however, follow no similar clear-cut rule and appear to be randomly chosen.

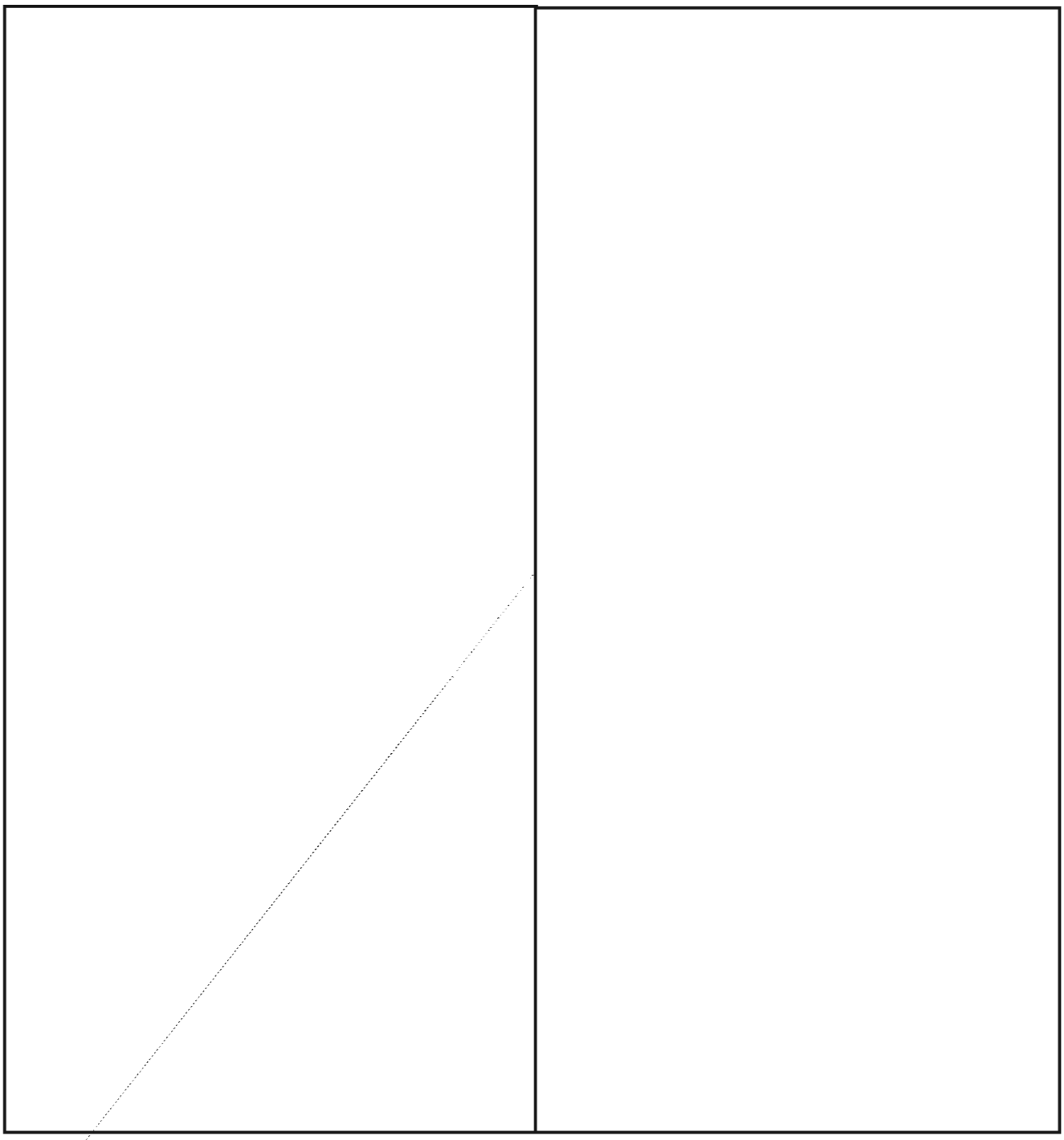
The COMINT compartment also has a substructure. The next level of detail is shown in Fig. 2. Information which falls between the two circles (the shaded region) requires COMINT channel handling but no further protection. More sensitive material is protected by a codeword. Hence "TOP SECRET UMBRA" implies the additional caveat "Handle via COMINT channels only." The classification "TOP SECRET CODEWORD," while in itself not so specific, is, however, used only for COMINT materials. Within the COMINT Category III codeword section are the various special access restructions.

Working at an agency like NSA, where almost all personnel are cleared for access to one of these compartments, one can lose sight of the very restricted nature of the information one has access to. It can be quite a shock to work with other people in the Intelligence Community or the military who are cleared up to the national secret or top secret level but who do not have access to COMINT. This shock strongly reinforces one's appreciation of the sensitivity of the work being carried out at NSA.

~~CONFIDENTIAL~~

K1- "S.C.A. FIELD MANAGEMENT AND EVALUATION"

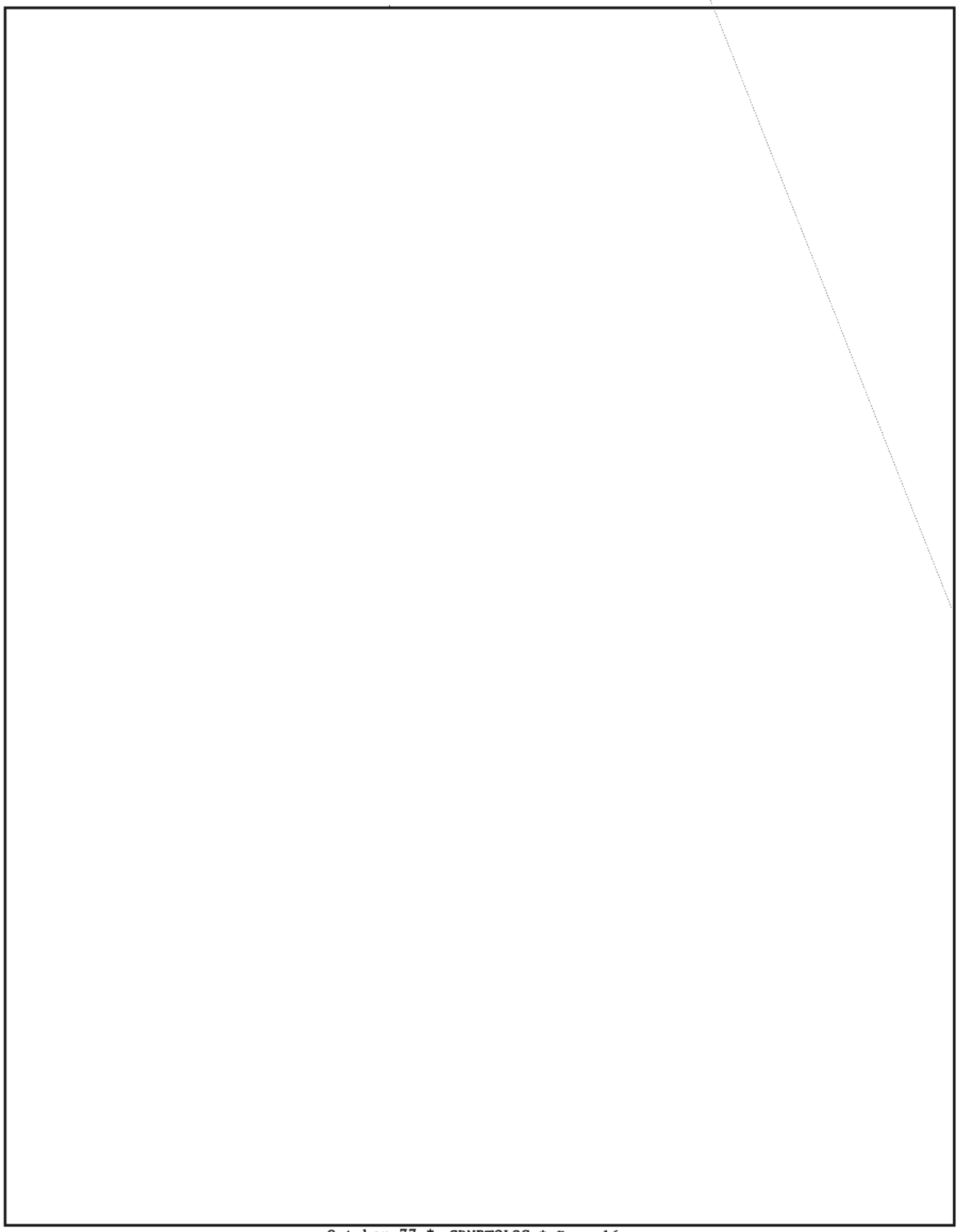
K1 P.L. 86-36



EO 1.4.(c)
P.L. 86-36

P.L. 86-36
EO 1.4.(c)

~~CONFIDENTIAL~~



DOCID: 4009803

The Perils of Being a State Department Interpreter

Reprinted from the Department of State Newsletter, June 1977.

On his very first assignment as a State Department interpreter, Theodore E. Herrera faced a most difficult challenge. He was called on to interpret a joke.

The setting was a table for three at an elegant restaurant in New York. Mr. Herrera sat between the rector of a South American university -- a guest of the United States -- and an official of an American foundation engaged in educational projects.

"Now this guy walks into the saloon," the American said, as the interpreter rendered his words into Spanish.

"He says to the bartender, 'Blindfold me and pour me any drink in the house. I'll tell you the brand.'

"So the bartender pours him a few, and each time this guy not only calls out the brand, but he also gives the proof and how old the whiskey is.

"The bartender figures to himself, 'I'll fix this wise guy.' So he pours some water into a shot glass and says, 'O.K. Tell me this one!'

"The guy sips it and lets it go down slowly. He thinks a minute and then he says, 'I don't know the brand, but I'll tell you one thing -- it's never going to sell.'"

The South American had been listening with a polite smile. When the punch line came, he wasn't aware of it. He merely looked on with the same smile and waited patiently for the next sentence -- as silence descended.

"After that," Mr. Herrera recalled in a recent *Department of State Newsletter* interview, "I promised myself I would always give notice to the other party that a joke was on the way. This becomes the cue for a courtesy laugh, at least, and after that, things tend to go very well."

Mr. Herrera is one of 18 full-time interpreters in the Department's Language Services Division. Each of them has to develop techniques for meeting the challenges of their profession whether they are acting as simultaneous interpreters, with earphones, at international conferences; sitting in on important negotiations like the SALT talks; working on the joint Apollo-Soyuz space project with the Soviets; or escorting foreign VIPs on tours of the United States.

Nora M. Lejins has a way of using her eyes to encourage principals to speak to each other, rather than to her. "I was in the Oval Office at the White House once," she related, "interpreting for the President and a high German official. The conversation got very animated.

"Then I noticed that each party, after making his statement, paused to look at me. It got to the point where both of them seemed to be talking to me, as if I were the one who was giving the argument on each side.

"This became disconcerting for me, and I thought it was wrong. I felt they couldn't be communicating very effectively if they spent so much time watching me instead of sizing up each other.

"So as one looked at me, I sort of took hold of his eyes with my eyes and then, by moving my head, led his eyes over to the other principal. Then I did the same thing with the second party when the reply came.

"It worked. After a while, they weren't noticing me any more, and they were speaking directly to each other. I've found it necessary since then to use this technique from time to time."

"It sometimes might look to others like a game of Ping Pong," Mr. Herrera said, "but interpreting is not so simple a matter as an interpreter merely paddling words back and forth.

"Your mind has to do several things all at once while the conversation is going on. You

DOCID: 4009803

have to listen and you have to speak, but of course what you say is not what you hear.

"I don't mean just the switch from one language and vocabulary to another, and then the reverse. It's really the ideas that you are trying to communicate, not a word-for-word statement.

"What you have to do is transmit the real meaning in the spirit in which it is being said, and this often means being an actor -- without making it obvious.

"You are handed a script on the spot -- what one of the parties is saying -- and then you have to perform that script, faithfully and convincingly, in the other language.

"I'll give you an example. I was escorting a Latin American official in this country who was invited to address a joint session of a state legislature. He was a very emotional speaker -- an accomplished orator.

"I sensed that I could not do him justice as an interpreter unless I worked myself into his mood. So when he shook his fist, I shook my fist. And it went on like that. I was able to do most of it with intonations and inflections, but I had to use some of his gestures as well.

"When the speech was over, one of the state legislators came up to me and said, 'With a voice like yours, you should be in politics.' I knew then that I had succeeded in putting the principal across, and I felt very good about it."

"All of that is true, but up to a point," said Theodore H. Leon, head of the Language Services Division. "We don't go as far as the interpreter at the United Nations who found his principal pounding the table, so he pounded the table -- and then, when the principal knocked his water glass off the table and smashed it, so did the interpreter.

"I tell our own people, 'Don't go so far as to knock down the glass. If the speaker wants to do it, that's his privilege. But it's not your privilege.'"

Mr. Leon continued, "I can tell you, after 32 years here at State, that this can be a very tricky business. On the one hand, you're supposed to interpret for the speaker by saying only what he says -- without trying to improve on it or knock it down, or otherwise change it.

"If he repeats himself, for instance, then you're supposed to repeat yourself. If he exaggerates, you exaggerate. If he discounts something, then you do so too.

"But, on the other hand, word-for-word interpreting can lead you into a trap, and sometimes you can see it coming, but you might not be quick enough to escape it.

"What comes to mind is an international conference we had once on the spawning grounds of fish. The speaker was British and, speaking an English that was perfectly proper, he said, 'Just put yourself in the mackerel's place. Now what would *you* do if *you* were a mackerel?"

"The interpreter repeated this in French. When he came to the word 'mackerel,' he plunged right ahead. The audience reacted immediately, breaking up with laughter.

"The British speaker was surprised and embarrassed because he had been discoursing with great seriousness and had had no intention of being funny. What he didn't realize, of course, was that mackerel in French has a second meaning -- denoting a very unsavory individual."

Ms. Lejins said, "One way the interpreter could have got around that would have been by saying something like this: 'What would *you* do if *you* were that species of fish?' That would have been neutral. He could have skipped the word 'mackerel.'

"But, while we're on that point, let me say that an interpreter is lucky sometimes if she can keep up with the speaker on a word-for-word basis. Usually we can't. That's why we often have to take notes.

"I was taking notes furiously one time when a West German cabinet minister came here to confer with our Secretary of the Treasury. The German was very, very loquacious, and he had already worn out the German interpreter he had brought with him. That was in the morning, and she asked me to take over in the afternoon.

"The cabinet minister, once he got going, would speak sometimes for 20 minutes without stopping. Now, of course, I'm not a stenotypist, but that's not the kind of skill that was needed in this situation anyway.

"The idea was to get the sense -- accurately -- of what the cabinet minister was saying and then, when he was finished, to recount it in English.

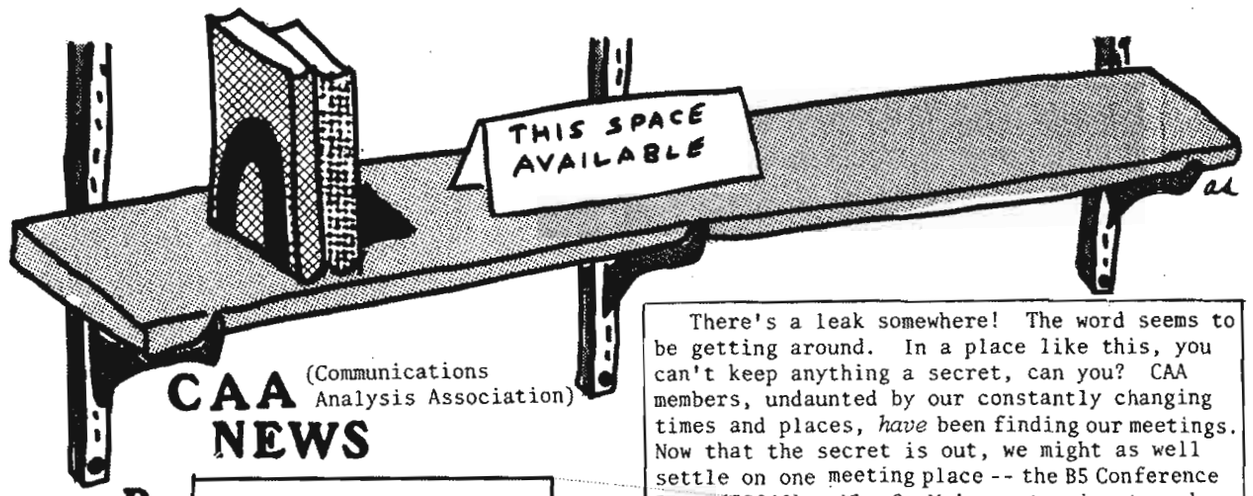
"The reason for taking notes was to make sure I would leave nothing out. But you can imagine the pressure an interpreter is under in a case like this. If the principal has spoken for 20 minutes, then you also have to speak for 20 minutes when your turn comes.

"It just wouldn't do to abbreviate. You can't take liberties like than when you're interpreting."

(Editor's note: Mr. Herrera was born in New Jersey; his mother had come here from Spain and his father from Puerto Rico. Ms. Lejins was born in Germany and came here as a child; she majored in the Romance languages in school but also studied German. Mr. Leon was born in West Virginia; his first "and most difficult job," he says, was teaching freshman English to American college students; he came to the Department as a translator.)

DOCID: 4009803

~~CONFIDENTIAL~~



CAA (Communications Analysis Association) NEWS

By [redacted] P14

What's black and white and red all over -- and has five feet? Or, to ask it another way: Suppose you were asked to explain what your particular corner of the cryptologic garden is really like, to someone who is "in the business" but not in your skill field. How can, say, a cryptanalyst explain to someone who isn't (and probably isn't going to be) just what goes on in the life and work of a cryppie? It seems to me that over the years one of the most difficult communication problems we have had is getting one skill group to really understand what a neighboring one does. If I am never going to *be* a collector (and I'm not), then how can you get your viewpoint through to me, by answering such questions as: "What is it like to be a collector? What things turn you on? What things represent excellence in work to your peers? When you've had a good day, what made it so? How do *you* spot a "pro" in your field when you see one?"

Dave Gaddy came up with an idea about this and what the CAA might do to encourage such communication between disciplines. Imagine, if you will, a Five-Foot Shelf of Great Cryptologic Literature -- but with this proviso: that every book or article on the shelf is aimed at people *outside* the field described. What would you choose?

I've asked several people, and have gotten rather different answers. At the outset, I frankly wasn't thinking about an actual shelf, but more like a bibliography. However, I have been offered (and have accepted) some collections of documents and papers on various subjects.

Do you have any favorites you want to see on the shelf?

Membership Drive: Our Annual October Membership Drive is now under way. If you join now, your dues will be fully paid through the end of next year. That's 15 months for the price of 12, folks!

There's a leak somewhere! The word seems to be getting around. In a place like this, you can't keep anything a secret, can you? CAA members, undaunted by our constantly changing times and places, *have* been finding our meetings. Now that the secret is out, we might as well settle on one meeting place -- the B5 Conference Room (3S040). When? We're not going to make it *that* easy for you. There will usually be a secret clue, in the minutes of each board meeting, about the time and place of the next one. See if you can find it!

P.L. 86-36

At a recent Board meeting, [redacted] President of CAA, submitted a note that contained the following statement that, I think, deserves wider publicity:

"I would like to see us doing things that aid people to grow in their work. Personal growth (that is, becoming better people and better NSA employees, not just getting promoted) is to me a key objective, and, given the cross-disciplinary orientation of CAA, we are in an ideal position to help. Post-professionalization (and even professionalization) is one place where we can get into things like this. Nor do I think we should limit ourselves by a strict interpretation of the limitations of our charter or fear of impinging on management's prerogatives. If we can improve the quality of people at NSA, we have done a service for all."

OCTOBER presentation:

Mike Tilley [redacted]

P.L. 86-36
EO 1.4.(c)

NOVEMBER presentation:

The following are clues concerning the CAA November presentation. Can you match them up? Each number matches up with one of the letters.

1.	[redacted]	A. Found in some homes
2.		B. Found in the Orient
3.		C. Found in some homes
4.		D. Found in the Orient
5.		E. Found in some homes
6.		F. None of the above

For additional clues, watch for the announcement of our November presentation. (CAA members: Check your mailboxes for the announcement.)

P.L. 86-36

For information, call [redacted] President, 1193s, or [redacted] Board Member, 3369s. CAA Board listed in September CRYPTOLOG.

P.L. 86-36

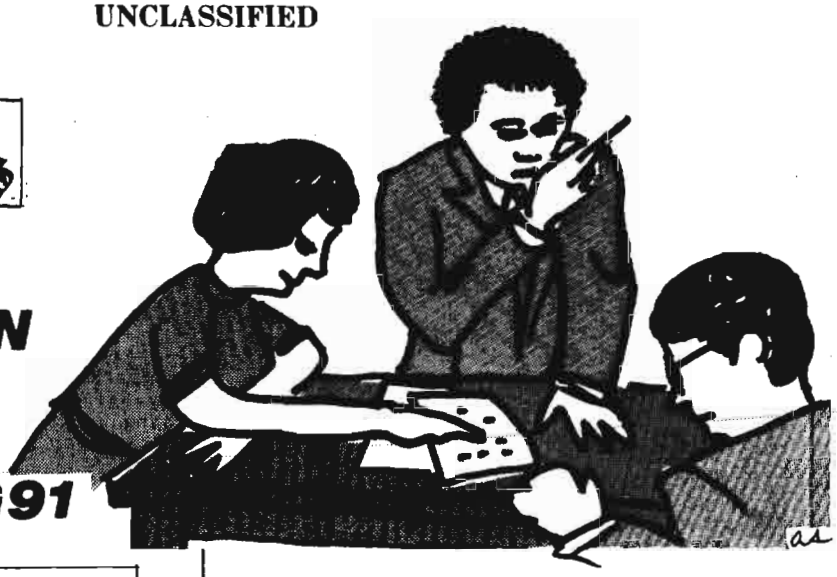
~~CONFIDENTIAL~~

DOCID: 4009803

Department of
GOLDEN OLDIES

ANALYZATION OF DATA

G91



P.L. 86-36

The following article appeared in the September 1971 issue of DRAGON SEEDS, an informal B Group publication that has since been discontinued. The article was followed by an editor's note saying "We will have further comment on this article in the December issue of DRAGON SEEDS."

And there was further comment on it -- some of it vehement -- even before the December issue of DRAGON SEEDS appeared. CRYPTOLOG readers who are not familiar with the article might like to figure out what all the ruckus was about. But CRYPTOLOG readers who already know are asked to keep silent, thus letting a whole new group of readers enjoy this classic fully.

Explanatory comments can be obtained by writing to: CRYPTOLOG, P1.

Ed.

An analyst should first study data in its original form looking for obvious or significant points. By all standards it is most important that an analyst look for virtually any and all signs of unusual conditions which could occur in any form, in any data.

Customarily a thorough analysis is a primary goal but prior to any thorough analytic study, much can follow from initial scanning of data looking for virtually any important sign or signs. Do this first! From this point, particularly having run out of initial scanning of data, an analyst who works with traffic should dirty his hands by actually handling and sorting traffic in its original hard copy form.

Going through traffic, occasionally voluminous amounts of traffic, is a duty of all analysts. Having to do this has its applications to follow-on analysis. In this follow-on analysis many sound conclusions may solidify by improving facts first found during initialization. Just to avoid confusion, analysis is not sorting traffic -- it is a logical accounting for all individual parts of a main body of data.

Knowing functions and limits of said individual parts is important. Looking at all parts individually and as a group is always most important. Missing parts could focus on basic primary origins of data. Non-association of parts could add support to analysis also.

Odd or unusual conditions should aid in producing a working copy of an original body from which your data was forthcoming. Primarily, in addition to analysis of data, an analyst must list all significant facts for historical background information. Quick logical drawback of this information is an important point in analyzation. Random approach to drawback of data is not satisfactory in most situations.

Should various arts and skills apply, an analyst must vary his attack accordingly. This is a sign of a good analyst -- pliability or adaptability to situations and changing conditions. Until an analyst displays this quality in his analysis, an analyst is not functioning at a maximum standard.

Vital to all analysis is a thinking analyst, with ability to occupy his mind with various and sundry points. Which point to disavow or disclaim and which to follow up is not always obvious. X-ray vision would aid any analyst, in both scanning of data and looking into goals of tomorrow.

You, as an analyst, occupy a vital position in an analytic community -- much of your analysis is original with no duplication by co-analysts, thus your analysis is primary to analytic community goals and missions. Z-groups and A-groups should aid cryptanalysts in locating indicator or discriminant groups and in turn aid in important cryptologic findings.

(Did you do any analysis of *this* data?)

Letter

[redacted]

(C ~~CCO~~)

Solution to NSA-crostic No. 9

(*CRYPTOLOG*, September 1977), by David H. Williams

P.L. 86-36

[redacted] "[The] Uses of Elegant English" (*CRYPTOLOG*, November 1976):

"It was Engelbert Humperdinck, I think, who sang a song recently, whose lyrics are the epitome of originality and poetic imagery of which today's songwriters can be so proud. 'I'm yours,' sang Mr. Humperdinck, 'till the stars fall from the sky, for you and I.'"

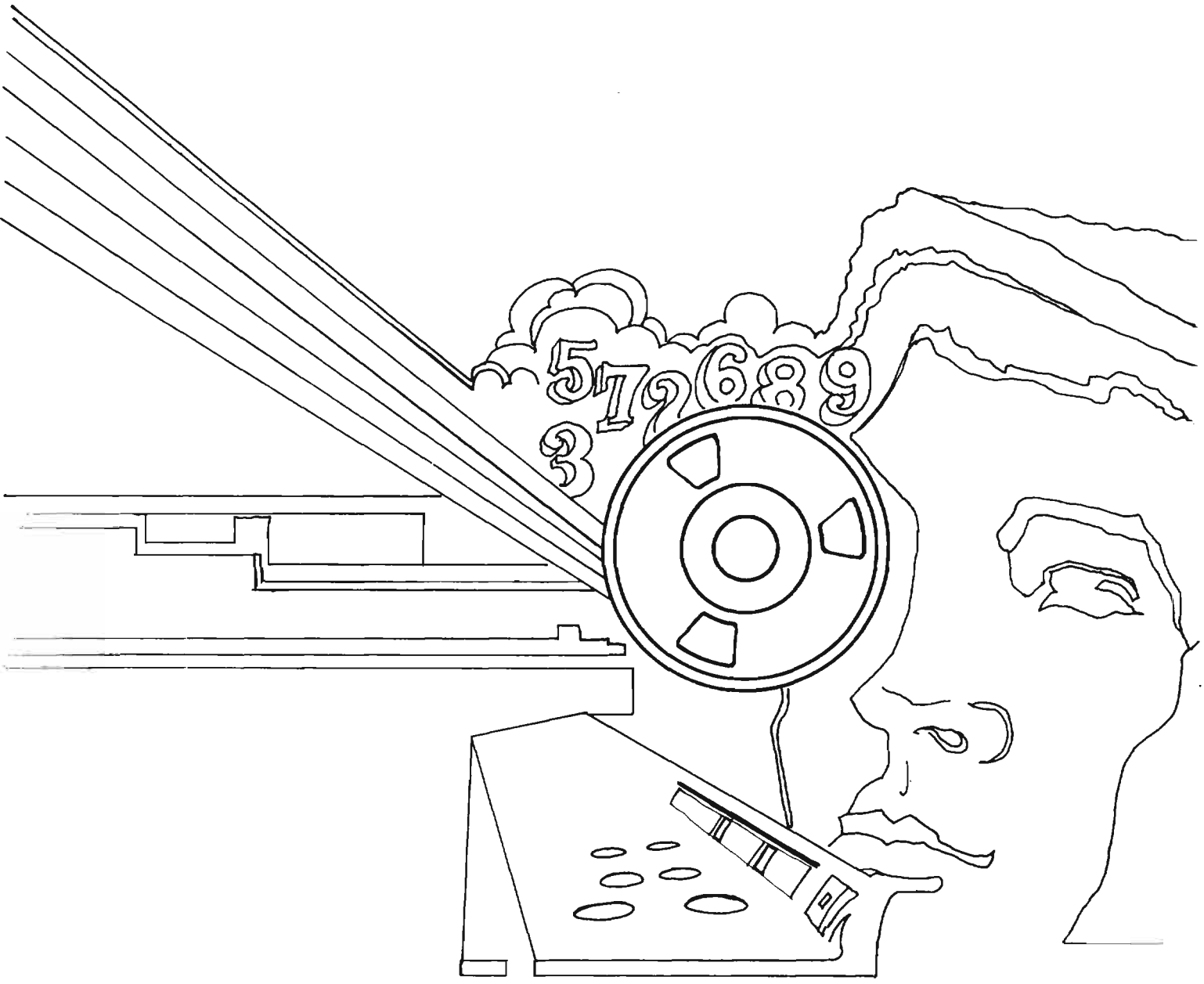
Engelbert HUMPERDINCK
COMPOSER
(Hansel and Gretel)

(U)

[redacted]

EO 1.4.(c)
P.L. 86-36

P1-SEPT 77-S3-25519


5 7 7 6 8 9
3

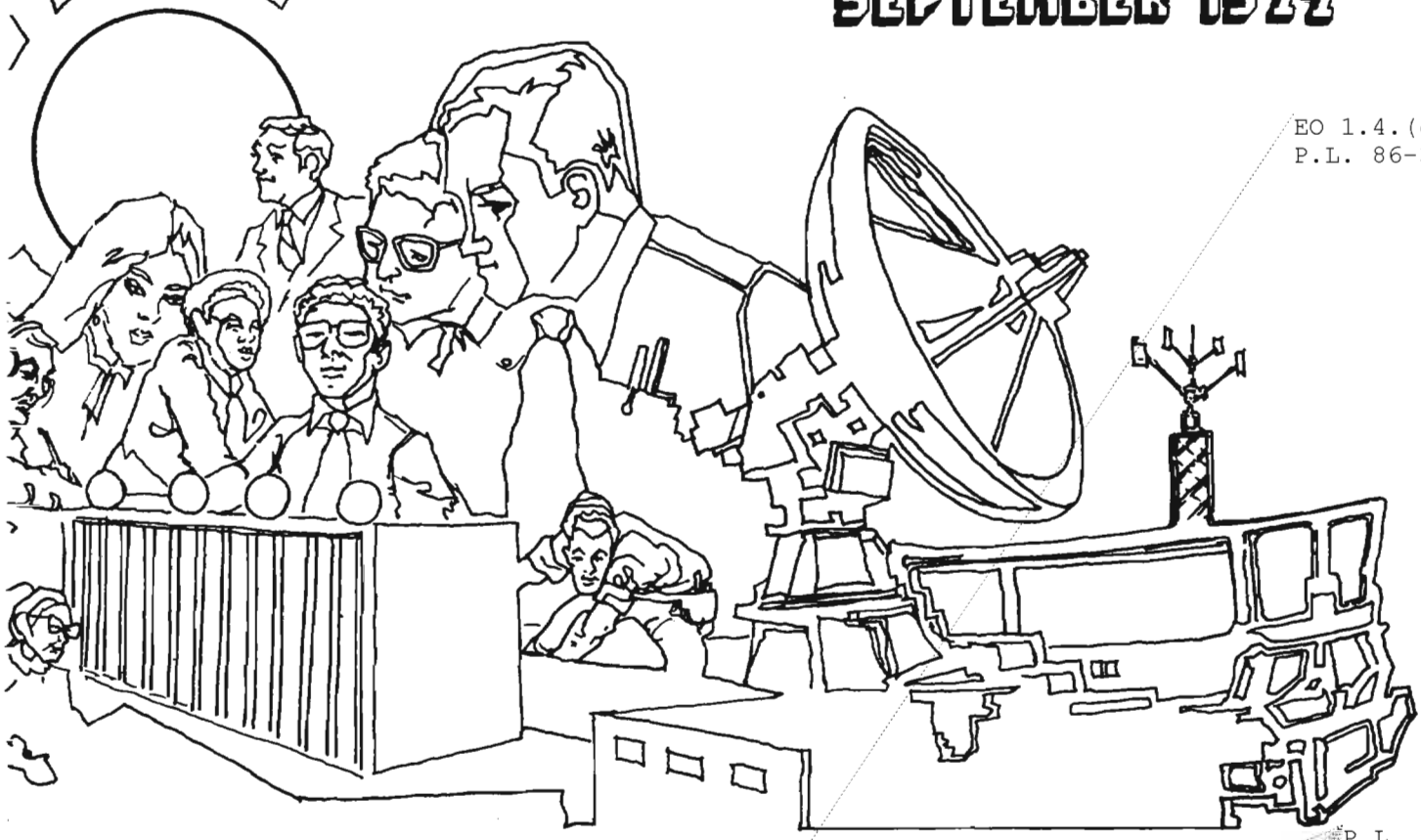
DOCID: 4009801

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

SEPTEMBER 1977



EO 1.4.(c)
P.L. 86-36

ANOTHER LAST WORD ON I.A.T.S. . . . . [redacted] 1
DOCTOR IS IN(CAPABLE OF DIAGNOSING) . . . . Russell Chauvenet 4
[redacted] . . . . [redacted] 5
KNOWLEDGE RESOURCE MANAGEMENT AT N.S.A. . . . [redacted] 8
"IS THERE A DOCTOR IN THE HOUSE?" . . . . . [redacted] 9
TRIBUTE TO THE GURU. . . . . CA-400 Class 32. 11
CLASSIFICATION CORNER: XGDS-2. . . . . [redacted] 19
WHITHER THE S.R.A.? . . . . . [redacted] 19
SPEAKING OF LOGGING. . . . . [redacted] 21
NSA-CROSTIC NO. 9. . . . . David H. Williams. 22
THE THAI SEMINAR PROGRAM. . . . . [redacted] 24
J.P.R.S. LANGUAGE REFERENCE AIDS. 25
C.A.A. NEWS. . . . . [redacted] 27
LETTER TO THE EDITOR. . . . . Dan Buckley. 28
"SIMONOFF SAYS!". 29

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009801

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. IV, NO. 9 SEPTEMBER 1977

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5236s)

Collection..... (8955s)

Cryptanalysis..... (4902s)

Language..... (5236s)

Machine Support..... (5303s)

Mathematics.....Reed Dawson (3997s)

Special Research.....Vera Filby (7119s)

Traffic Analysis..... (4477s)

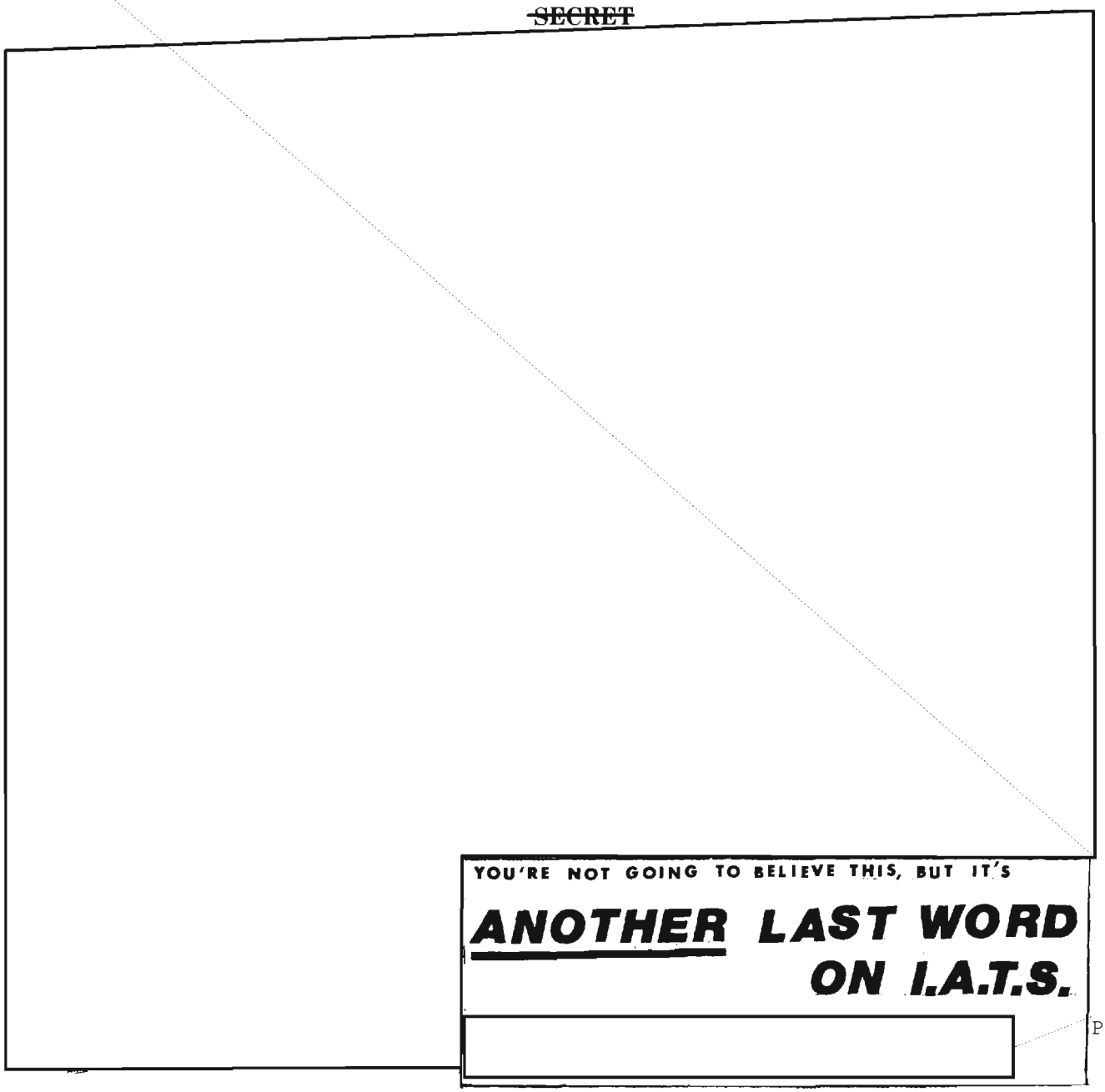
Production Manager.....Harry Goff (4998s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

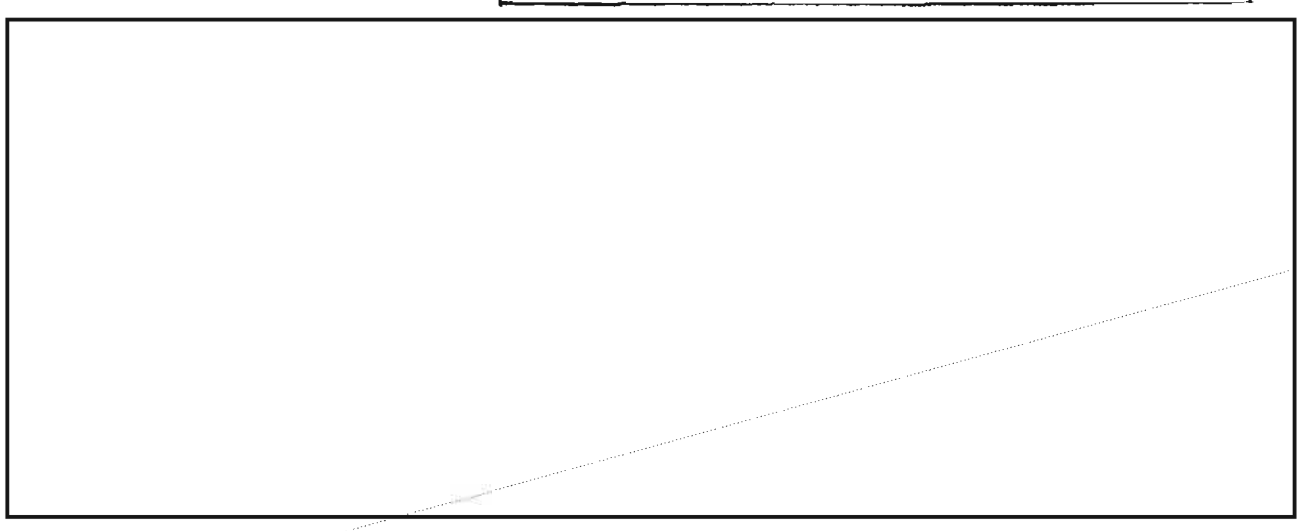
EO 1.4.(c)
P.L. 86-36
DOCID: 4009801



YOU'RE NOT GOING TO BELIEVE THIS, BUT IT'S

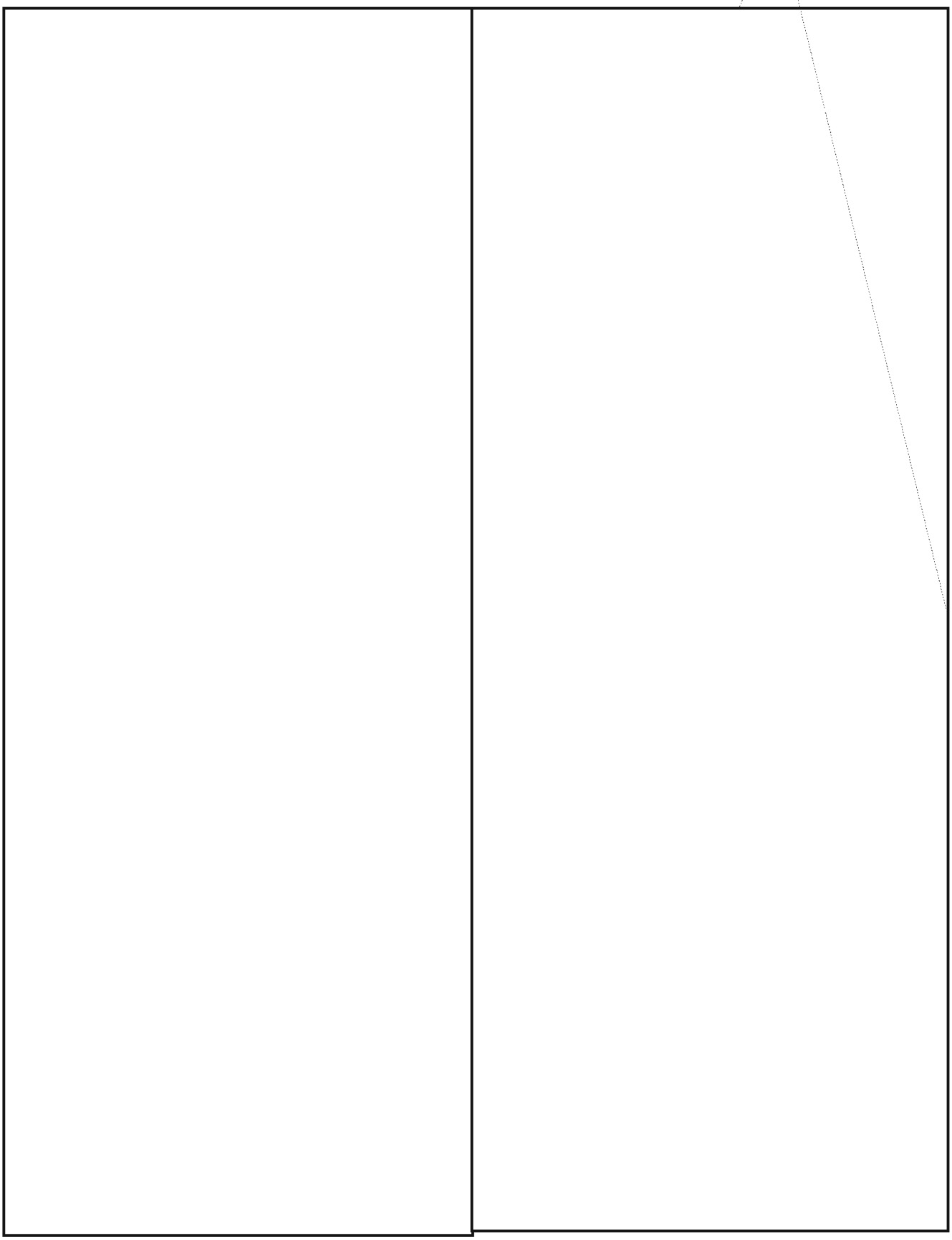
ANOTHER LAST WORD ON I.A.T.S.

P.L. 86-36

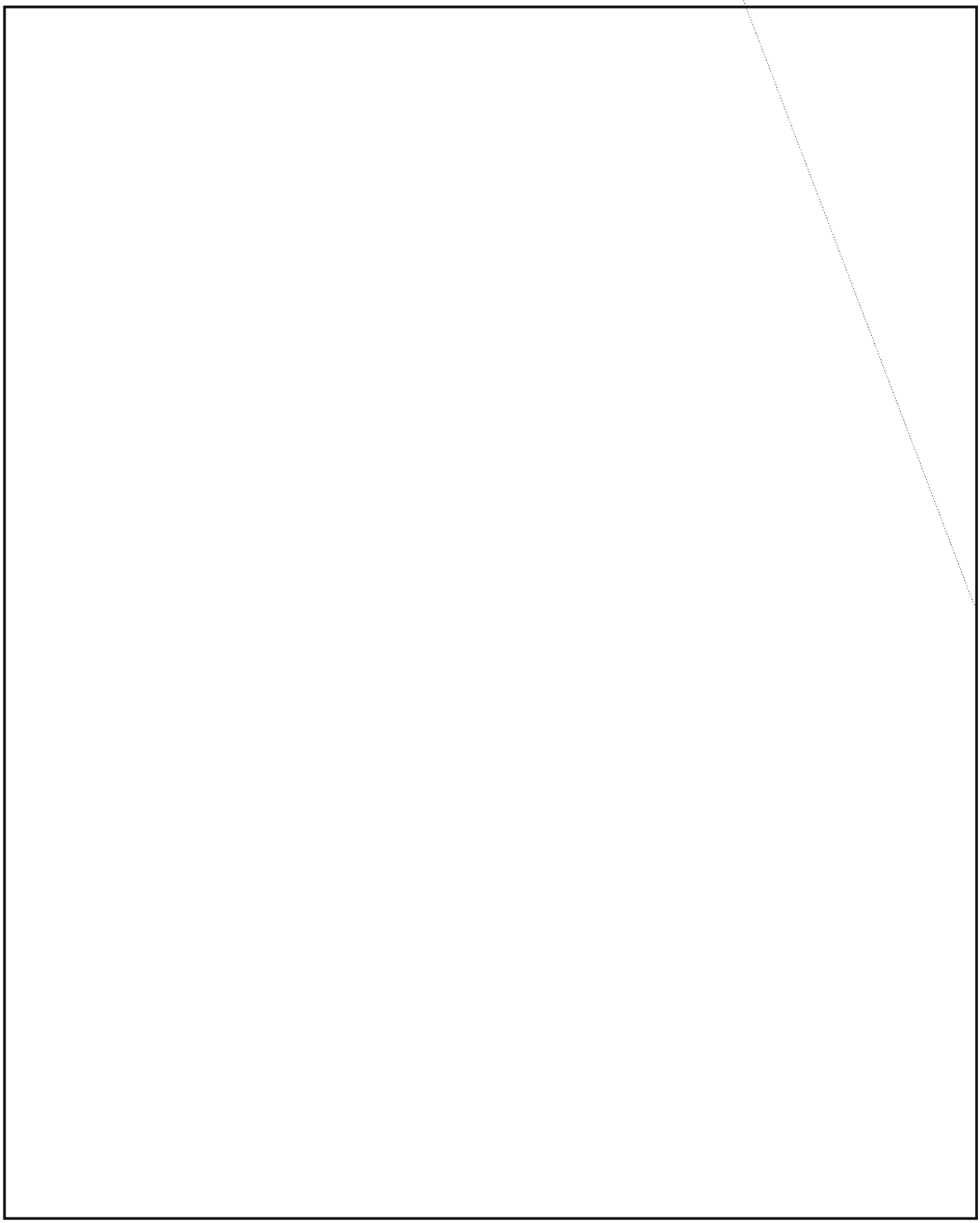


EO 1.4.(c)
P.L. 86-36

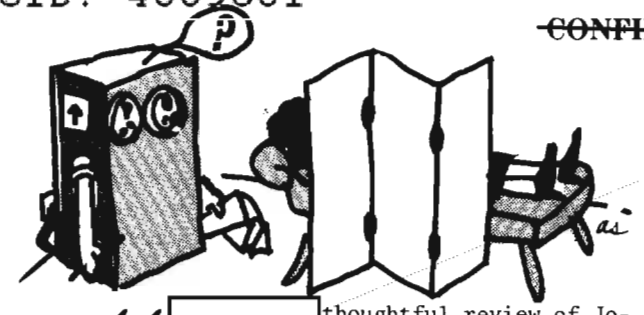
~~HANDLE VIA COMINT CHANNELS ONLY~~



EO 1.4.(c)
P.L. 86-36



DOCID: 4009801



THE DOCTOR IS IN(CAPABLE OF DIAGNOSING)

Russell Chauvenet, P12

[redacted] thoughtful review of Joseph Weizenbaum's *Computer Power and Human Thought* (see "Another Controversial Book on Artificial Intelligence," CRYPTOLOG, May 1977) is an outstanding contribution which merits both praise and attention.

It is easy to agree with Weizenbaum that proponents of Artificial Intelligence (AI) have made unsubstantiated claims. I am doubtful about the merits of his proposition that some things computers could do are morally wrong, and should not be programmed. As an example, Weizenbaum equates treatment of mental disorders by prefrontal lobotomy, a drastic and somewhat discredited surgical procedure, with treatment of the same by a computer program. He says "machine-administered psychotherapy would induce an image of what it means to be human that would be prohibitively costly to human culture." In so saying, Weizenbaum shows that he is still suffering from cultural shock induced by his secretary's asking him to leave the room while she was "talking" to his ELIZA computer program running in DOCTOR mode.

It is likely Weizenbaum missed the real significance of the incident. The nature of DOCTOR is to reflect the user's thoughts, when supplied as input, back to the user. Like any other computer program, it manipulates data but originates nothing. When the user inputs personal items, the DOCTOR program returns them in various noncommital formats which often stimulate the user to further thoughts. The user need not have a "demeaning image of what it means to be human" to use DOCTOR in this manner, and if the input includes personal and confidential material, an instinct for privacy is natural.

As a crude analogy, a tennis player practicing against a wall finds all shots being returned by the wall in various patterns. The dialogue with the wall may help perfect the player's technique. If the player is not an expert, a desire to practice in privacy without spectators is only natural. DOCTOR is a more clever construct than a wall but it serves an analogous purpose under the proper circumstances, when used seriously and not for laughs. In neither case is the wall or program contributing any original values to the physical or mental exchanges taking place.

This brings us to the basic impasse in AI work. You can describe a problem or, even better, a situation, and ask a person, "What do you think about it?" To ask the same question of an AI computer program is an almost meaningless gesture. At best the program may have been provided with means to print out "Insufficient data" when not specifically assigned any task recognizable to the program.

Consider the practical problem of diagnosing some traffic received in a new crypto system. The human analyst looks over the material and develops from experience and judgment some feeling for what kinds of systems might be involved. A set of statistical diagnostic routines is specifically selected by the analyst. Each routine accepts the given data and returns the specific analysis requested, within parameter limits the analyst has chosen. The results are considered and other tests are made, and if a hypothesis occurs to the analyst for which no ready-made program exists, then the needed program is created for the job.

But if an AI program were to be attempted, the lack of motivation, judgment, and original thinking provides built-in limitations to the project. We can think of the "AI Diagnostic Program" as a main routine having access to all the known diagnostic subroutines, but if we intend to submit batches of unknown traffic and ask for a report on the system underlying it, we have to supply all the "motivation" ourselves. The main program can be told to try various subroutines, but if we forget to put in an instruction to call the δ I.C. routine, the "AI program" is not going to notice the omission and remember to call the subroutine we didn't tell it to use. Nor is it easy to imagine the "AI" routine digesting the results of the subroutines used so far, deciding that some new test is needed, and creating the routine to do that test. The coding may exist in "AI" to accept, for example, our instructions to create a δ I.C. routine, but *we* have to supply the rules and, if we make a mistake, "AI" will probably not know the difference.

The drift of this argument is not that it is wrong to work towards AI, as Weizenbaum seems to think, but it is generally unproductive. The neurons in human brain cells are not off-on flipflops or +/- magnetized spots. We do not think in binary arithmetic. Weizenbaum is probably right in feeling that an attempt to make computers simulate human thinking is singularly futile when we don't really understand the processes involved in human thought.

The moral is, then, not that AI is wrong, but that it is unrewarding. We can get more for our money by using computer programs as our tools, discarding (for at least some time to come) the fanciful AI concept.

DOCID: 4009801

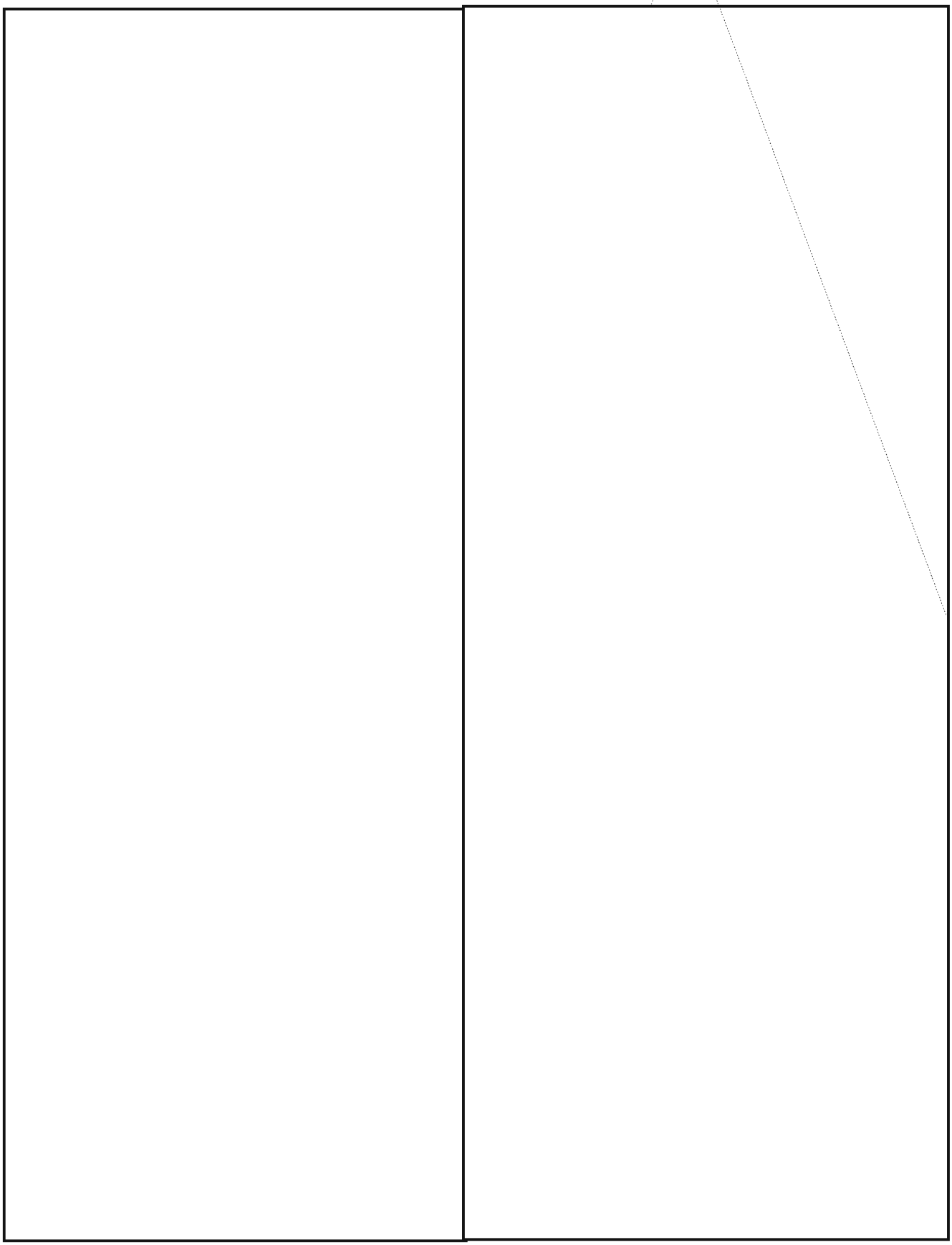
EO 1.4.(c)
P.L. 86-36

P.L. 86-36

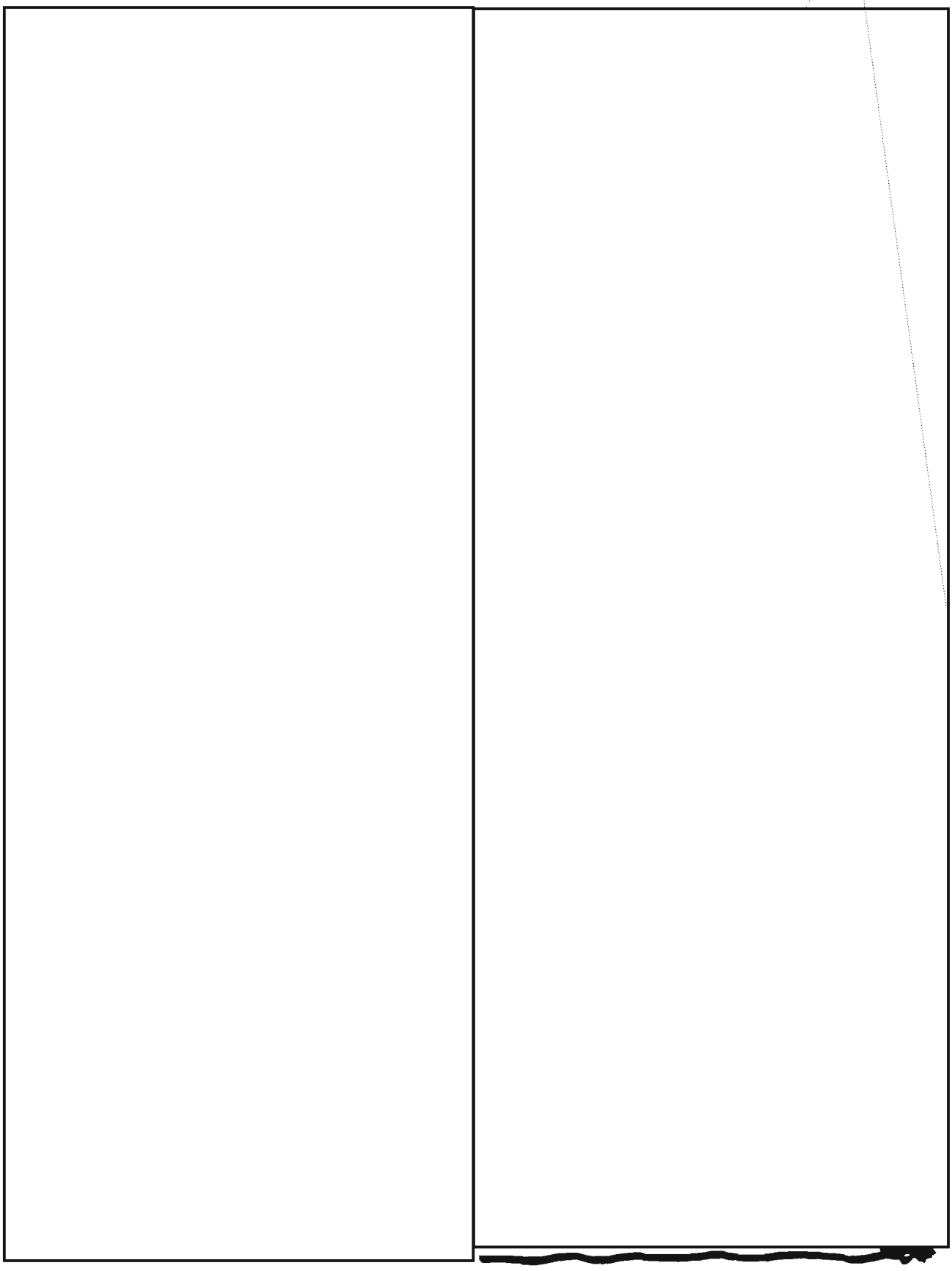
P16

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



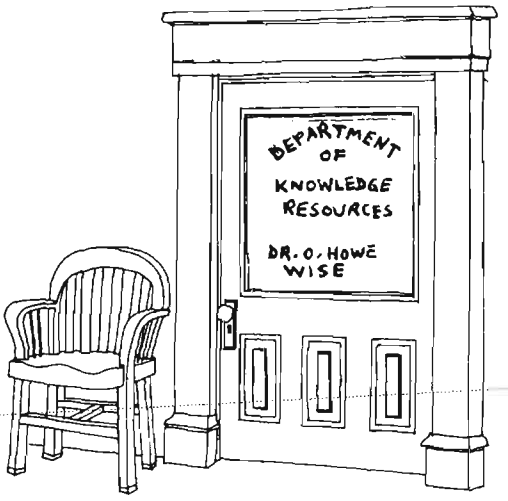
EO 1.4.(c)
P.L. 86-36



DOCID: 4009801

KNOWLEDGE RESOURCE MANAGEMENT AT N.S.A.

[redacted] R532



P.L. 86-36

A recent R5 Technical Report* proposes the concept that knowledge is a basic resource of the National Security Agency, and computerized systems can play a key role in preserving and manipulating much of this valuable resource in a process called Knowledge Resource Management. The paper

- identifies several problems with the current mode of operations;
- presents a theory of knowledge and argues why knowledge should be treated as a basic resource;
- introduces some new technology and identifies some areas where further research is required; and
- proposes a system architecture for implementing knowledge management in a distributed heterogeneous computer network environment.

The knowledge-related problems which are addressed in the paper include:

- the increasing costs associated with producing intelligence information;
- sharing data in a heterogeneous computer network, requiring analysts to master a large variety of user interfaces (essentially, one for each data base and file);
- inadequate problem-solving support from our computer resources;
- the continued loss of analytic expertise through attrition; and
- the need to preserve more of the knowledge acquired by these analysts for the use of those left behind.

The knowledge-theory section presents a taxonomy of knowledge which identifies and distinguishes among factual, procedural, and judgmental knowledge in order to define what constitutes the Agency's knowledge which is to managed.

Factual knowledge deals with facts (or data) and their interrelationships. *Procedural knowledge* includes the algorithms and heuristic methods which our analysts use to solve problems employing this data. *Judgmental knowledge* involves the constraints and goals which are used to direct the Agency's problem-solving behavior. A basic tenet of knowledge resource management is that these various forms of knowledge should be maintained independent of one another to effect knowledge sharing, to improve manageability, and to reduce costly duplication.

The theory of knowledge resource management relies heavily on the basic concepts of data-base management, but attempts to extend these concepts to include more than just managing data. The three-schema view of ANSI/SPARC (internal, external, and conceptual schemas) is investigated and the human roles of applications administrators, data-base administrators, and an enterprise administrator are examined. A new technology called Knowledge-Based Systems is introduced, which may provide some of the problem-solving support needed by our analysts. A set of user interfaces is also presented and explained.

The paper suggests a methodology for managing knowledge as a basic resource. The methodology includes an architectural model for knowledge management which defines a role for existing software technology such as data-base management systems, knowledge-based systems, applications programs, and user interfaces. Finally, some on-going and planned research activities in the realm of knowledge management are described.

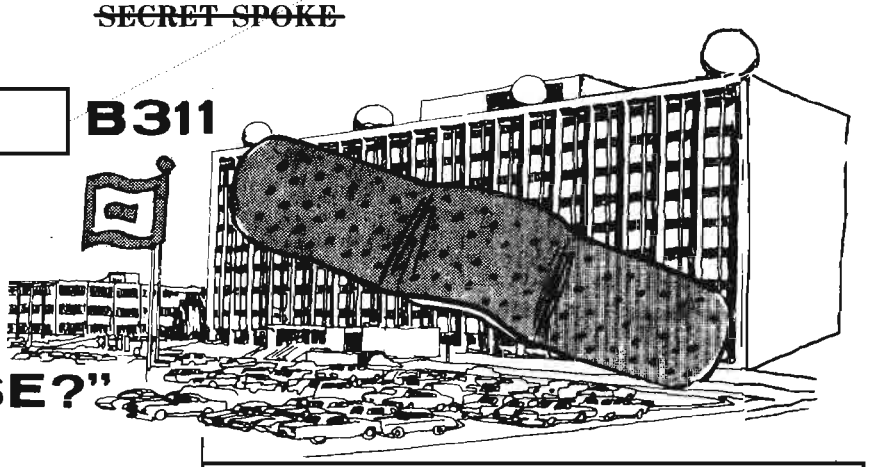
Several contractual efforts are currently underway to evaluate the knowledge-resource concept and the proposed architecture, to develop some of the advanced user interfaces, to investigate the application of knowledge-based systems to NSA problems, and to develop a canonical representation for data which can be used to facilitate data sharing among different data bases.

Copies of the report have been widely circulated throughout the Agency. Additional copies may be obtained from R53, x5504s.

*Managing Knowledge as an Agency Resource, R53/08/76, November 1976, S-215,904 (TSC).

DOCID: 4009801

[redacted] B311 asks



"IS THERE A DOCTOR IN THE HOUSE?"

Have you heard the latest rumor? There is a terrible miasma seeping through the corridors of NSA, infiltrating, where it can, all the elements of PROD, creeping under doors, insidiously attacking all who cross its path. Do you care? You should, because it's probably affecting you even as you read this. Let me say I don't think it's just a rumor. It goes under the name "Technical Documentation Syndrome," and its constant companion is "Apathy."

For some time now I have been concerned with the lack of technical reporting and documentation, and if the examples I use appear to have

[redacted]

We have all heard, ad nauseum, that "Product is our bread and butter," and without it we'd be out of business. Now, I wholeheartedly agree with this. However, which comes first, the chicken or the egg?

In order to write the product, someone has to perform some analysis. In many cases it's easy for the problem-wise analysts to recognize unusual activity and to issue appropriate product, but the job shouldn't stop there, although, all too often, that's just where it does stop.

When it does, inevitably, back come the questions:

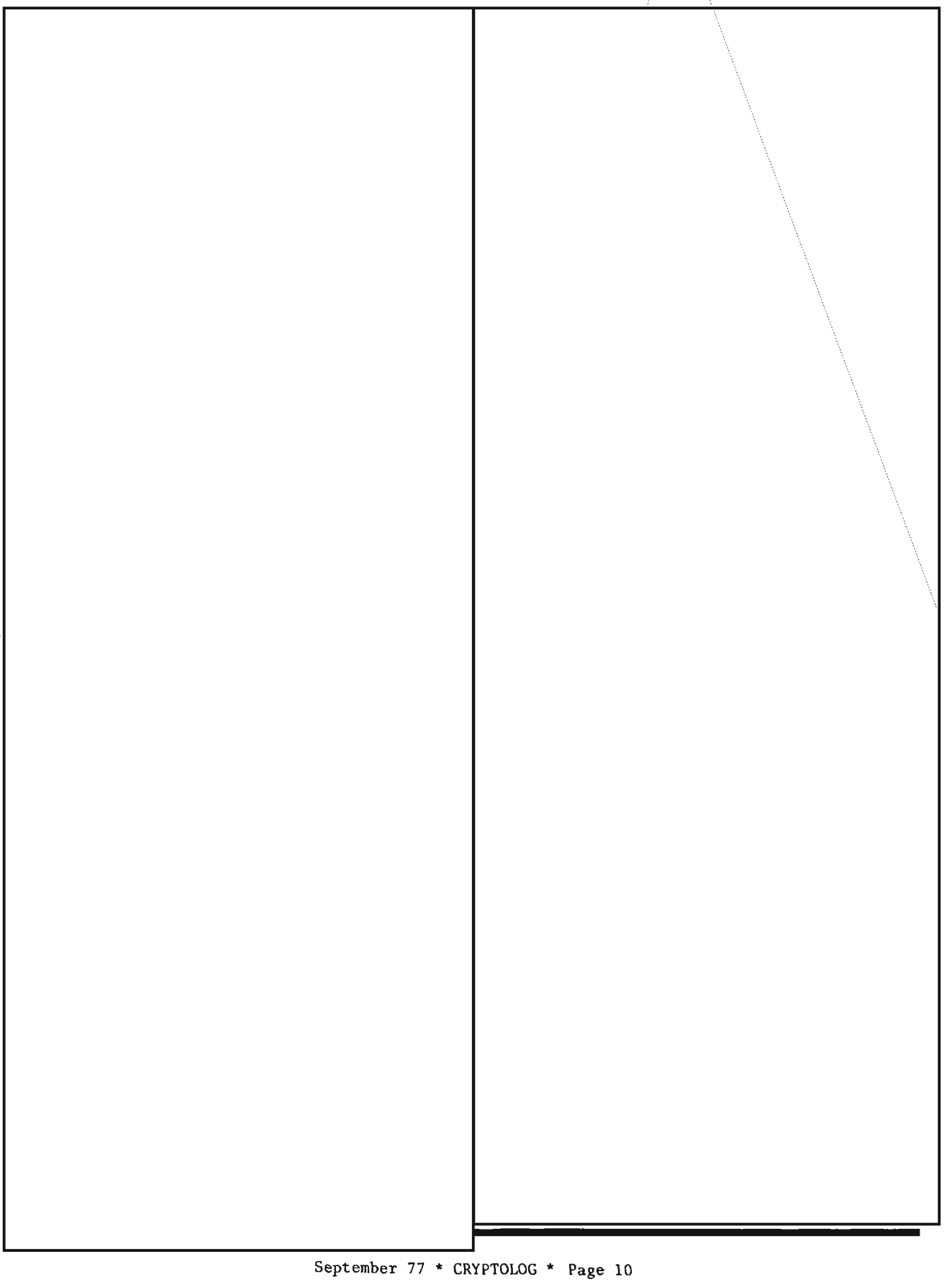
[redacted]

[redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~



DOCID: 4009801

TRIBUTE TO THE GURU

In 1956 Lambros D. Callimahos originated, and began teaching, course CA-400, "Intensive Study Program in General Cryptanalysis." Since that time there have been 32 classes -- all taught by the Guru (or Spiritual Leader) himself -- with 271 graduates (30.3% female). A complete tabulation of the graduates who are no longer with us (because of retirement, resignation, military reassignment, etc.) shows a remarkably low attrition rate during the 22-year period -- 26.2%, or 1.2% per year.

It has been suggested that the cement that binds together the graduates of Course CA-400 is the Dundee Society, which was founded in 1968. That society (named after the Dundee Marmalade jar in which the Guru keeps his pencils) consists of graduates of the course, who meet annually to salute the graduates of the current course. Each year, also, the society inducts an honored personage as an honorary member. At the June 1977 graduation luncheon, Admiral Stansfield Turner, USN, Director of Central Intelligence, was inducted into the society while the graduates of Class 32 sang, to the tune of the well-known Gilbert and Sullivan air, "And Now He is Director of the C-I-A!"

The graduates of Class 32 also prepared, for presentation to Mr. Callimahos, a "monograph" in which they recorded their many hours of hard work and hard fun, and their affection for the Guru and their Guru-ji (or Deputy Spiritual Leader) [redacted]. The following pages contain a few excerpts and drawings from that "monograph."

Ed.

Monograph Dedication

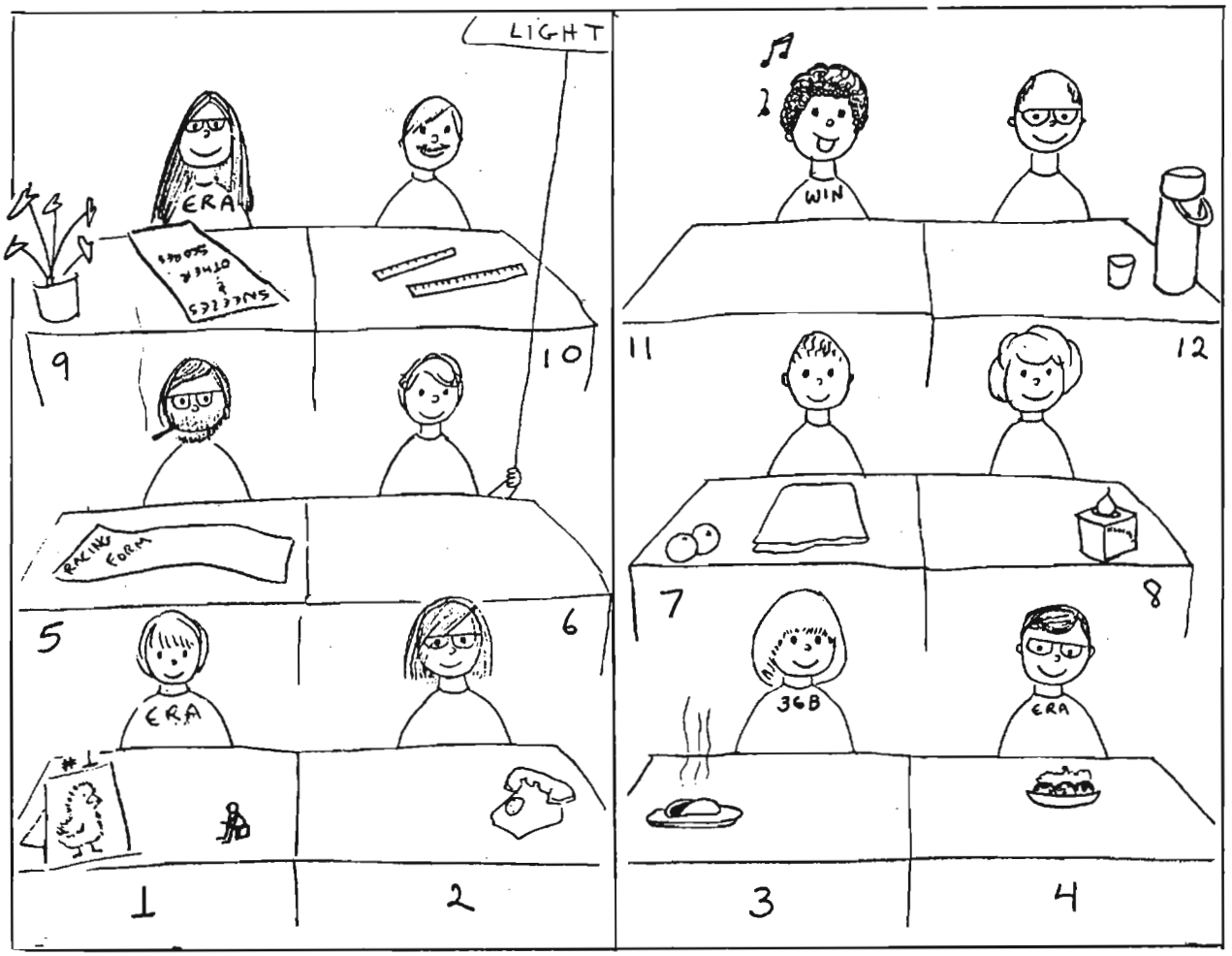
This monograph has a two-fold purpose. It is intended not only as an item of memorabilia for Class 32, the Great One, and the Near-Great One, but also to illustrate the qualifications of this nonpareil class to serve as a paragon for future Dundee aspirants in their pursuit of cerebral enlightenment, cultivation of raunchiness and bad puns, and kissing habits.

[redacted]

The monograph is dedicated of course to our Guru and Guru-ji, who inspired us to greatness.

Class 32

P.L. 86-36



On 7 February 1977 Class 32 of the much-heralded CA-400 class began. Handpicked by none other than the Guru and Caudillo himself (otherwise known as Lambros D. Callimahos) the class commenced an effort to prove itself worthy of membership in the elite Dundee Society.

In an attempt to document the many and varied accomplishments and experiences of Class 32, this document has been produced to emblazon forever in the annals of cryptologic literature the "rising to the task" and completion of the rigorous CA-400 course.

Prior to revealing the many unique and wondrous talents and attributes of the class and its unique individuals, some demographic data pertaining to the class as a whole will be provided for those with a statistical inclination (or interest, as the case may be). Note that the class roster is included as Appendix 1 for reference and further details.

Category	*Statistics*
Age	Total - 395; mean - 32.91; range -- 30-48
Grade	Total - 127; mean - 10.5; range - 9-13
Marital status	Married - 9; single 3; range -- none to twice
Sex	Yes, 6 male, 6 female (Note 1: WIN proponents please excuse this category.) (Note 2: Class members claiming other than "male" or "female" were considered "liberal"; however, for purposes of this document, they were placed in either male or female categories based on physical appearance, style of dress, or other identifying characteristics. Range - no comment.
Children	Total - 12; mean - 1, 8 boys, 4 girls; range 0-4
Education	Total years in school - 180; mean - 3 years of college; range - high school graduate to Master's Degree
Certification	Total - 13; mean - 1.08; range - E/T-C/A

DOCID: 4009801

Years of NSA service	Total - 117; mean - 9.75; range - 5-22.
Parent state (place of birth)	Maryland - 5; Texas, 1; Colorado - 1; New Jersey, 1; Oregon - 1; Virginia - 1; West Virginia - 1; Pennsylvania - 1.
Political philosophy	Liberal - 3; conservative - 4; moderate - 4; abstains - 1.

Enough dry statistics!!

As previously mentioned, certain characteristics were identified with class members and thus set them apart as a unique entity within a unique entity. Although not mentioned by name, correlation of the following information with other data and the pictures contained in this document will reveal the person's identity. (Concomitantly, match letters with numbers appearing in Appendix 1.)

Mystery letter	*Characteristic(s)*
A	a singer? and lyricist? and official raspberry
B	dog, newspaper, oranges (has a lot of a "peel")
C	sends (Playtex living) support through the mail
D	two rulers and no shoes
E	Grand Marshal Captain Sleaze, the burlesque's squeeze
F	incorruptible, coffee-thermos kid
G	double dipper but hold the cones!!
H	"Sneezy" (allergic to her partner?)
I	the creative caricaturist that has great leggs
J	the mover, and future author of the book *Moving to a New Home and Its Effects on Marriage*
K	winner of award for "receiving most phone calls, or the COMSEC kid
L	red hair, position second to one, polished prose, WHAT??
M	give me liberation, down with Bryant, ban Gallo, save the trees, do you have a headache?
N	the dispenser of knowledge who speaks with white tongue OH!!

Class 32 was also given credit for a number of particularly unique qualities which set the class apart from all others. In the words of the Guru himself, Class 32 was cited for its "unity," "bussing," "raunchiness," and "perhaps not the most entertaining, but certainly not far behind."

Chronological sequence of class: With nose to the grindstone, under the tutelage of the Guru and Guru-ji (otherwise known as Bruce, [redacted] Class 32 galloped through the halls of learning and knowledge, moving right along until finally the Zendian foe was met.

Mobilizing Task Force Pearl (see Appendix 2 for order of battle), under the direction of General [redacted] and Ensign [redacted] the assault on Zendia began, with success finally gained as [redacted] succumbed. Thus concluded the preliminary portion of the CA-400 course. The final week was more than intellectually stimulating and was accomplied with the utmost fervor and zeal (cough!).

As the sun sets on the CA-400 Class 32, the participants return to the Realm of the Unknown to apply the knowledge and many new capabilities which they now possess. With sincere affection and utmost respect the Class 32 members bid the Guru and Guru-ji fond farewell and "nighty-nite!"

Appendix 1

CA-400 Class 32 Roster

1. [redacted]
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

P.L. 86-36

Guru and Caudillo - Lambros D. Callimahos
Guru-ji - [redacted]

Appendix 2

U.S. Task Force Pearl (Every One a Gem)

[redacted]

DOCID: 4009801

Appendix 3

Sneezes, Scores, and Other Pertinent Data

Student number:	1	2	3	4	5	6	7	8
Sneezes:	14	8	0	27	0	0*	1	160**

9	10	11	12	G-I	G-II
32	107	95	14	0	9

Office next door	Other class
2	4

Vampires	Movers
1	4

*But many giggles
**Includes 2 unofficial sneezes in CA exam

Sneezes by location:	Front row	Middle row	Back row	Right side	Left (devil's) side
	49	161*	248	161	297

*Only 1 was not Student #8

Sneezes by day of week:	M	T	W	Th	F
	88	103	121	87	76

Student number:	1	2	3	4	5	6	7	8
Score:	0	-25	-2	-35	-105	0	-90	-15

9	10	11	12	G-I	G-II
+4	-125	0	-5	-5	-16

Note: All scoring is purely objective. Scorekeeper is #9.

Scores are awarded mostly for sexist remarks, and occasionally for general raunchiness.

Other pertinent data:

14 March: 2 bad puns from Guru-ji. Later puns became too numerous to record.

21 March: Student #9 had hiccups.

23 March: Student #7's single recorded sneeze was with potato chips.

31 March: Student #8 had a fit.

7 April: Student #4 applauded for "Uncle Walter's Dog. . ." Student #11 applauded for "Union leaders make good targets. . ."

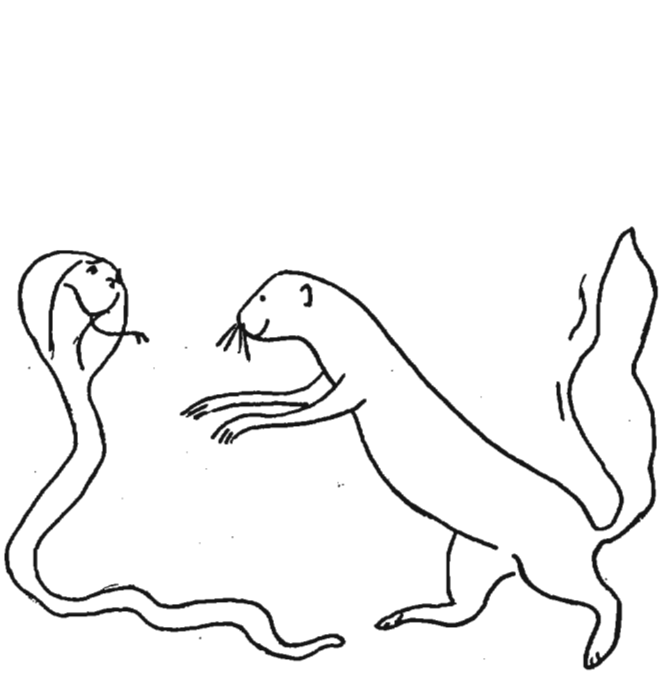
5 May: Student #10 was leading sleaze.

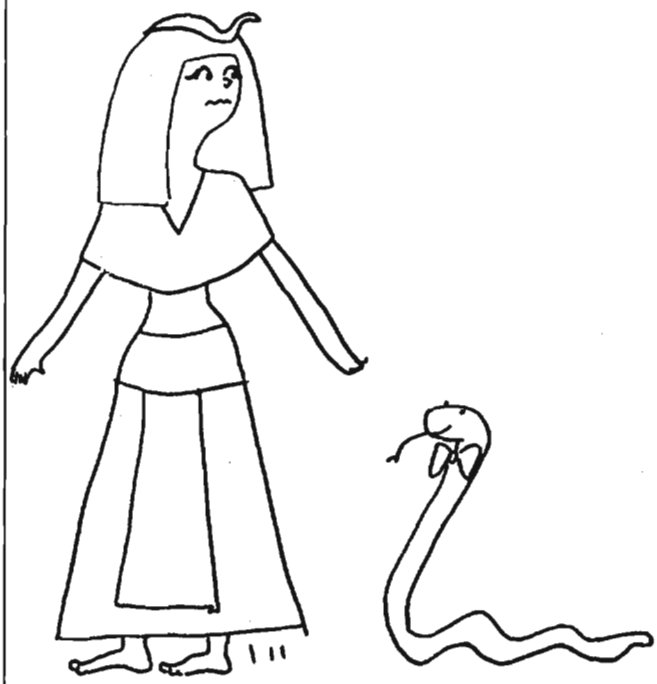
6 May: Guru-ji received -50 for lascivious "Hubba-hubba," but redeemed self by removing his shirt.

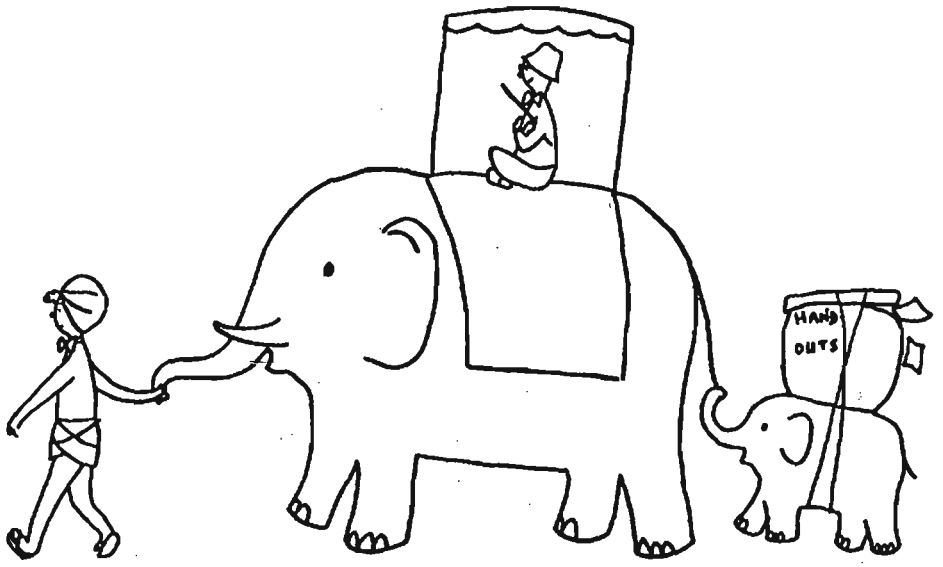
7 May: Student #1 called "Good Cryppie" by Mike What's-His-Name

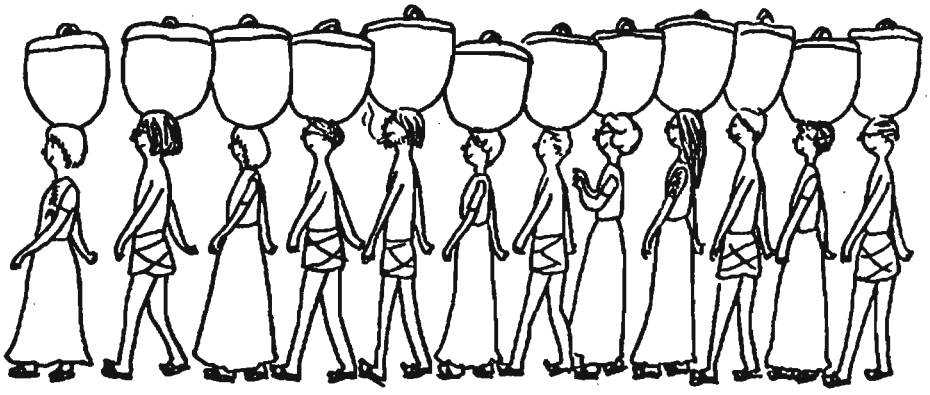
24 May to 6 June: Guru has hiccups.

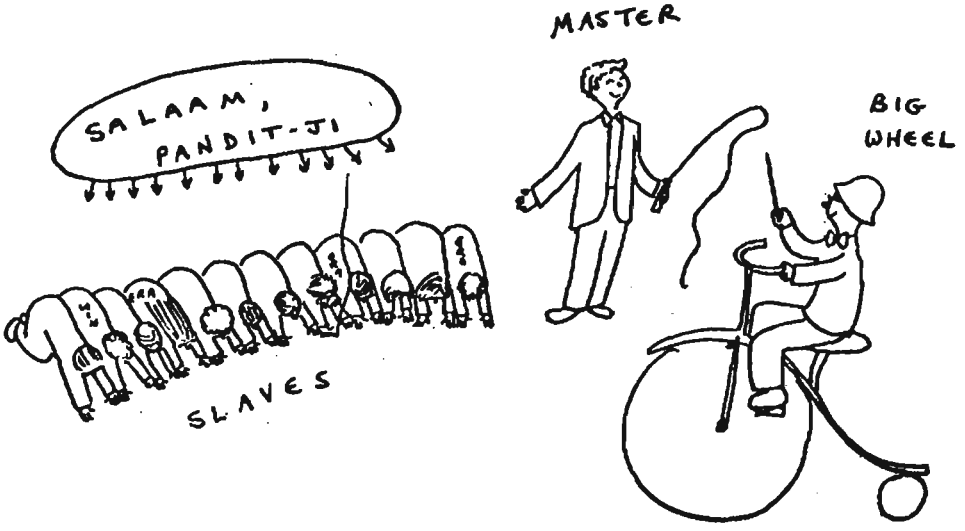
8 June: Guru and Guru-ji unofficially receive -100 points apiece.

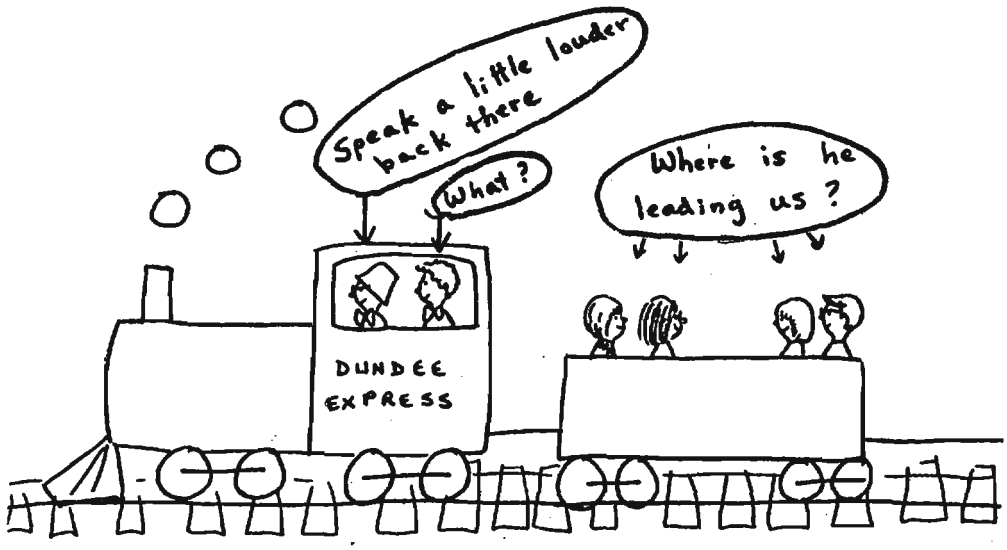


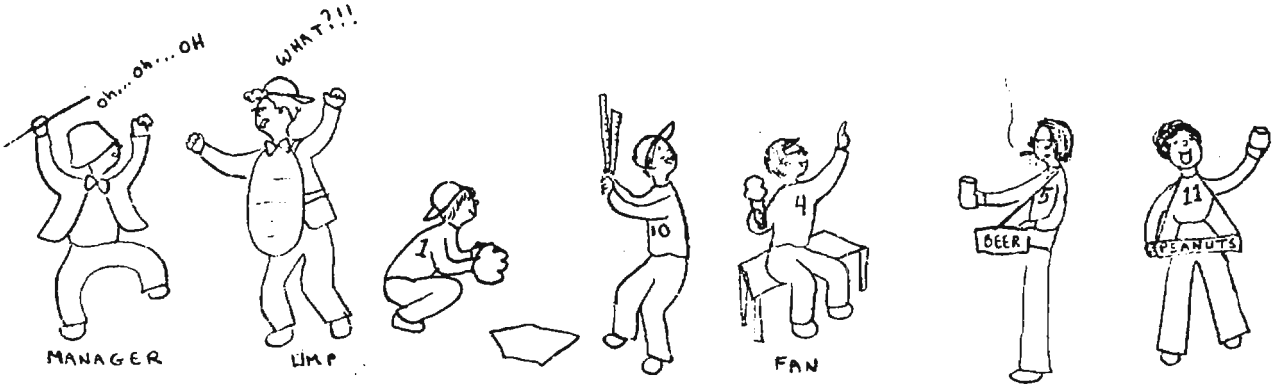



HAND OUTS



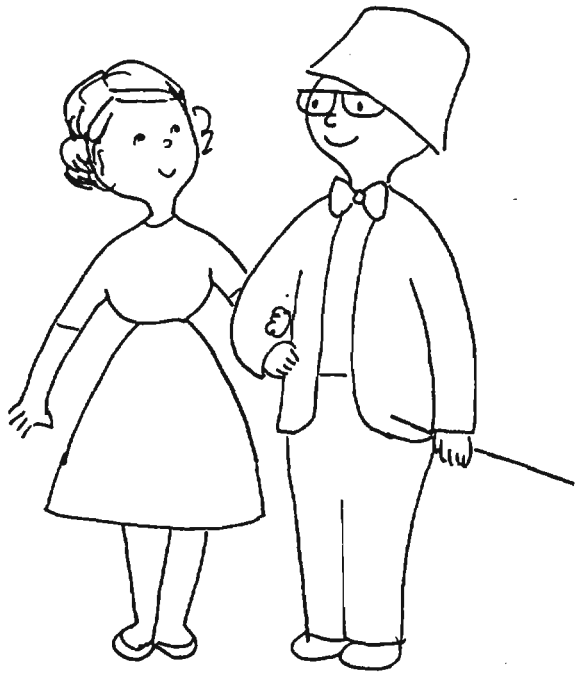

MASTER
SALAAM, PANDIT-JI
BIG WHEEL
SLAVES


Speak a little louder back there
What?
Where is he leading us?
DUNDEE EXPRESS


oh...oh...OH
WHAT?!!
MANAGER
UMP
FAN
BEER
PEANUTS

WHERE IS EVERYONE?
LEVEL 5
HOW THE HECK DID HE GET ALL THE WAY UP THERE?
LEVEL 4
LEVEL 3
LEVEL 2

DOCID: 4009801



Helen, our honorary member of Class 32

The drawings and excerpts from "Monograph 32" which are reproduced on the preceding pages attest to the high professional regard and personal affection that the members of Class 32 feel for Lambros D. Callimahos. Those feelings are shared by 22 years' worth of graduates of CA-400. The following statements by just a few of the 271 graduates show that the members of Class 32 have lots of company in considering Mr. Callimahos to be their Guru.

Ed.

To the Man of Letters, the Flutist, Master Cryptographer, Epicurean, Gourmet, Keeper of the Key to Wisdom, Tutor of the Unlearned, and key to my personal successful career as Cryptanalyst, to my venerated mentor, Mr. Absolute, Lambros D. Callimahos:

Undaunted by my apparent unworthiness, Mr. Callimahos accomplished yet another of his unsung miracles -- he prodded me to the heights. I am one of the select few, a survivor of the tribulations of the "General Study of Communications," the hallmark class of the National Security Agency. Sir, I salute you!

[redacted]
Class 10 (1961)

* * *

CA-400 is an unforgettable experience. One of the fortunate ones, I took CA-400 when the class size was still very small. Only three other students and I shared a unique and uniquely qualified instructor for 4 hectic, glorious months.

The whole world of cryptanalysis opened up before us, past and present. We sensed continuity with history and tradition, yet felt the stimulus of new horizons and modern challenges. The wealth of cryptanalytic experiences and skills presented to us would have taken years to acquire on the job. Mind and imagination were pushed almost to the limit. We were encouraged daily to work harder and quicker, to accomplish more in less time than we would have believed possible.

All of this for an instructor who was always several steps ahead of the student -- however clever that student thought he might be -- and who combined teaching with a friendship with his students that endures long after the class has graduated.

CA-400 is one of my most treasured memories. I shall never forget it -- or the extraordinary man who taught it.

[redacted]
Class 14 (1962-1963)

* * *

Of the many and varied courses to relating to cryptanalysis, that teach principles of cryptography and techniques of analysis, none provides a philosophy of the art comparable to that of CA-400.

It is certainly true that, with a variety of systems and techniques an analyst becomes familiar with, the broader his outlook becomes as he applies them to the real world. Thus, with the personality of Mr. Callimahos to provide the philosophy, one should be successful in any analytic endeavor.

For me personally, what successes I have had as a cryptanalyst can be attributed directly to CA-400. This was, I believe, due to a feeling I developed about the particular system.

I have been back in the Training Department for 2 years as a cryptanalytic instructor. I am now better able to impart to a class, in some small way, this idea of a philosophy. Even though most or all of my students will never be cryptanalysts, the subject does provide a vehicle to form a way of thinking that can be applied to any science. I feel assured this philosophy that I can relate to others will never be outdated by technology or time.

C. E. Morrell
Class 25 (1970)

* * *

Cryptanalytics taught by the Guru is an exhilarating experience, one that I shall never forget. I am convinced that those who share this same feeling have been strengthened by his teaching.

Lambros D. Callimahos gave me a confidence when I most needed it. He helped to sharpen my analytic skills, and the wisdom imparted by him will forever remain with me.

[redacted]
Class 10 (1961)

* * *

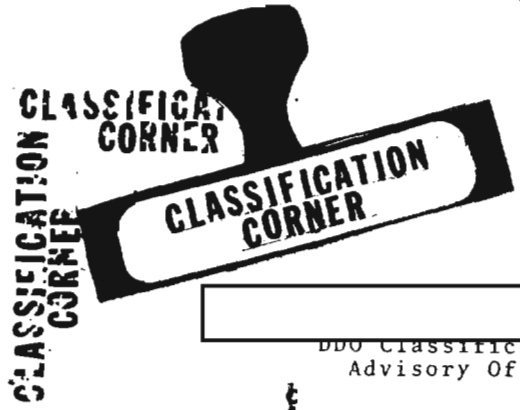
We were the Guru's first class to consist of 12 students. We became known as "Naughty 17," and until this very year enjoyed the Guru's recognition as "raunchiest class" (this year that distinction was won by Class 32). The heterogeneity of our demographic data certainly equaled that of Class 32 as described in its "monograph," and perhaps even excelled it.

The Guru taught us many things we had not even heard of before, including the correct names for various sizes of wine bottles. Together we explored the corridors of the "new" Training School, which had previously been the Fort Meade Hospital. Surely, Class 17 set a record for number of graduation parties which will stand for the ages, attributable to a certain natural sociability inherent in some class members and the air of camaraderie quickly established by our Leader.

Above all, the Guru gave us a crash course in how to use our brains, in how to derive pleasure from hard work, and how to feel true joy from technical success in our chosen profession.

[redacted]
Class 17 (1963-1964)

DOCID: 4009801



[redacted]
DDO Classification Advisory Officer

XGDS-2

EXEMPT FROM THE GENERAL DECLASSIFICATION SCHEDULE CATEGORY

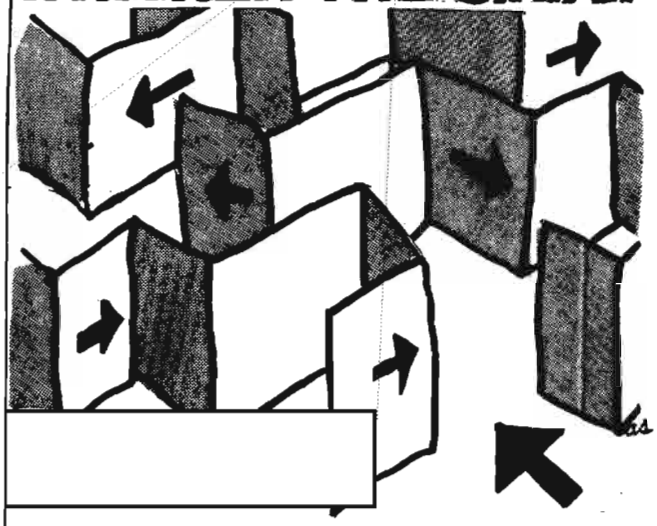
Executive Order 11652 requires that all classified information be considered for downgrading and declassification at the earliest possible time. It includes a General Declassification Schedule (GDS) which allows for downgrading of TS to S in 2 years, S to C in 2 years, and C to U in 6 years. The GDS states that all classified information will be so downgraded/declassified unless it falls in one or more of the following categories:

1. Information was furnished by foreign governments or international organizations;
2. Information is specifically covered by statute (for example, Restricted Data or Formerly Restricted Data) or is information pertaining to cryptography or disclosing intelligence sources or methods.
3. Downgrading/declassification would disclose a system, plan, installation, project, or specific foreign-relations matter the continuing protection of which is essential to national security.
4. Disclosure would place a person in immediate jeopardy.

The exemption category 2 is most widely used by NSA and is generally construed to mean all COMINT Channels, codeword, ELINT, TELINT, and SIGINT related information. XGDS-2 is the abbreviated version of "Classified by DIRNSA/CHCSS (NSA/CSSM 123-2), Exempt from GDS, EO 11652, Category 2, Declassify Upon Notification by the Originator."

~~(C--CCO)~~

WHITHER THE S.R.A?



[redacted]

The following article represents the personal and professional opinions of the author and should not be interpreted as an official statement on the part of the Panel.

J.T.W.

This is a short paper ambitiously aimed at resolving a controversial question: To what end does the Special Research Analyst (SRA) serve in the U.S. SIGINT system? There are more SRA people in the U.S. SIGINT organization than in any other single SIGINT career field, and the question of what constitutes the substance of their work is surrounded by a sometimes vigorous debate. An official definition exists, but does not seem to have taken hold. It somehow appears easier to define what a linguist does or should be expected to do -- or to describe the duties of a traffic analyst, cryptanalyst, telecommunicator, engineer, etc. -- and get a general agreement. Still, whither the SRA?

Being the military member of the SR and IS (Information Science) Panel and working at an SR assignment in A7 (Office of Operational and Strategic Studies) has motivated me to try to come to grips with what it is that SRAs are bent towards. The idea is to get at the function by trying to get at the results: what is the SRA supposed to produce? Regrettably, convictions of those who are certain they know what an SRA is differ from others who are like-minded. This is distressing in its administrative ramifications. What follows is a contribution, rather than a fixed proposal -- one which could further confuse the issue. In part it is aimed at the person who aspires to be an SRA, or who believes he or she already is one.

The SRA *produces* intelligence by *analysis* and by one or more forms of *reporting*, of which the end product is but one. As in the case of

EO 1.4.(c)
P.L. 86-36

a person suspected of a crime, the SRA must be shown to have motive, means, and opportunity. Analysis and reporting is the means and the opportunity.

I hope that these brief reflections are helpful. This is my own view, which does not necessarily represent the position of any authority in the Agency, and I would not want it construed as such. I am merely trying to get a handle on the nature of the SRA's work by linking SRA motives with SRA means, opportunities, and products (reconstructions).

DOCID: 4009801

CRYPTOLOG LOG Name of author	Organ	Title of article	Date rcvd	Accepted? Yes	Accepted? No	Page proof	Author's OK	Publication Issue
	G521	SPEAKING OF LOGGING...	31 May	✓		28 Jun	1 Jul	Sept 77

P.L. 86-36

I make this proposal and not at all in jest. I feel it would rectify a glaring inefficiency in the System as we now know it, and serve to raise Intelligence to heights never before imagined.

Throughout the Agency one notes a multiplicity and marvelous diversity of logs. Logs are to be found for every purpose and occasion. There are logs of messages, both incoming and outgoing; logs of security check; logs of lanes; logs of telephone calls; and so forth. In our quest for Order and Knowledge, logs have assumed an all-important role as a vital tool to organize and recall the myriad of information pouring into the Agency. There is not a single section that would not flounder within hours or even minutes were its logs not kept up to date. Logs provide an excellent management tool for compiling statistics of Output, Input, Production, Numbers of Messages, Workers, Logs, Hours, etc. It may be said that the power to log is the power to destroy. The integrity of logs is of utmost importance to the System and therefore to Intelligence. We must have logs and we must have the best logs.

Currently, in the Agency, all logs are decentralized and subject neither to a common administrative body nor a quality control. This is potentially a disastrous situation. Thus far we have been lucky. Imagine, though, the havoc one perverted secretary could wreak in a branch by subtly subverting its logs. Imagine the utter chaos a minor conspiracy of such degenerates would create in no time at all. Or, alternatively, imagine a fire raging out of control, consuming a division's logs before it could be extinguished. This threat is real. There is currently more wood, dead and otherwise, in the form of paper stored in the bowels of NSA than forest fires consumed last year. The hazard is astounding. One careless cigarette, one thoughtlessly placed Thermit bomb, and all could be lost.

It is to prevent such a disaster or disasters that the following measures must be instituted.

A well-defined career field of log-keepers must be formulated and introduced into the System. This should be a very tight group of chosen individuals -- hand-picked for their dedication and unswerving reliability and honesty. These will doubtless have to be found outside the Agency. This log-keeping career field should be organized as a guild, with apprentice log-keepers, progressing through journeymen and several degrees of master, up to guildmaster, who would hold rank equal to a Deputy DIRNSA. Special uniforms, oaths, and initiation rites would be phased in as the Guild became fully operational. The Guild would have jurisdiction over all Agency logs. No one except a Guild member would be allowed to log anything. Suitable punishments for illicit logging would be instituted to act as deterrents against tampering, sabotage, or other wanton acts against the System by non-Guild members. Coupled with the Guild would be a Standard Agency Log and Uniform System of Logging. All logs would be bound in a suitable material demanding respect, e. g. leather and gold, and be of a standard size. The Uniform System of Logging would ensure orthodoxy among all Keepers of Logs and members of the Agency. But, more than that, it would stand as a Guardian of Truth, inviolate and unyielding before the tempests of heresy. All logs could thus be kept pure.

The second phase is perhaps the most crucial. It involves the creation of THE MASTER LOG. When in full operation, THE MASTER LOG would contain all -- I repeat, all -- entries made in any approved logs in the entire Agency. Central control would thus be assured and DIRNSA would have total access to all knowledge logged in the System through the inviolate person of the Guild Master Keeper of THE MASTER LOG. It is not important whether the system is mechanical or electronic, although I must admit the reassuring effect paper and pen have on lay people. Division-level and group-level Master Logs would be kept prior to full implementation of the Agency Master Log and maintained thereafter in supportive roles to ensure quality in THE MASTER LOG.

THE MASTER LOG, as the total repository of log entries in the Agency, would naturally require increased security of the highest order. Black cloths, perhaps with gilt edging, could provide a great deal of protection from saboteurs (the magical powers of black cloths have been amply demonstrated Agency-wide in the past in the countless espionage attempts that have been foiled by them). Contingents of guards from each service in equal strength -- 8 Army, 5 Air Force, 5 Navy, 1 Marine -- would serve to physically thwart intrusion by any malefactors.

This is a concept late in coming. Its potential is universal. It could ultimately be applied nationwide, perhaps worldwide: A tool for Uniformity, Orthodoxy, and Peace.

NSA-crostic No. 9

The following NSA-crostic was submitted by guest NSA-crostician David H. Williams, P16.

The quotation on the next page was taken from an article in an NSA publication. The first letters of the WORDS spell out the author's name and the title of the article.

DEFINITIONS — *WORDS*

A. With Word L, one of the wives of Henry VIII — 24 36 169 108 158 79 96 120 102

B. Agreement, conformity; Honda — 84 163 129 138 146 21

C. Fashionably elegant — 128 107 174 23 164 190

D. Ladies' apparel — 134 189 166 64 2 172

E. Moslem prayer leader — 29 17 63 152

F. Advice to a patron in a Nairobi restaurant to try the intoxicated jungle beast (5 wds) — 160 200 150 126 135 48 66 33 6 176 183 165 27 / 19 91 180 80 105 198

G. Caesar's surprised comment upon hearing that his friend had also had dinner (4 wds) — 104 119 155 12 49 87 113 144 132 137 16 173 94

H. Escorts inside (2 wds) — 139 117 170 187 182 147 86 90

I. How Mark Spitz departs (2 wds) — 188 3 161 74 40 76 181 191

J. Enlighten — 69 114 1 77 88

K. Shanty — 35 186 130 46 31

L. See Word A (2 wds) — 41 177 197 59 4 38 54 30

M. Device to cause a light to operate intermittently; MHMH's grandfather — 106 85 89 62 15 47 103

N. Abrasive powder — 171 156 75 193 58

O. Flaccid — 179 26 142 70

P. Small whirlpool — 9 140 199 194

Q. Pickles — 81 28 68 127 25 71 162 118

R. Preempting, confiscating; usurping — 178 18 157 123 78 136 175 109 115 72 60 7 101

S. Dozes — 37 39 92 148

T. Small-caliber rifle or pistol (comp) — 14 52 65 83 112 51 185 122 73

U. Chinese hors d'oeuvre — 56 8 43 44 93 10 57

V. Less wide

$\overline{42}$ $\overline{100}$ $\overline{159}$ $\overline{20}$ $\overline{192}$ $\overline{32}$ $\overline{45}$ $\overline{13}$

W. Spectral

$\overline{151}$ $\overline{67}$ $\overline{34}$ $\overline{55}$ $\overline{125}$ $\overline{168}$ $\overline{116}$

X. Drawback; debt

$\overline{50}$ $\overline{22}$ $\overline{149}$ $\overline{11}$ $\overline{124}$ $\overline{167}$ $\overline{98}$ $\overline{95}$ $\overline{143}$

Y. Unit of linear measure

$\overline{141}$ $\overline{131}$ $\overline{110}$ $\overline{53}$

Z. Season

$\overline{5}$ $\overline{196}$ $\overline{99}$ $\overline{184}$ $\overline{133}$ $\overline{153}$

Z_1. Spasmodic inbreathing accompanied by a characteristic sound

$\overline{154}$ $\overline{82}$ $\overline{97}$ $\overline{61}$ $\overline{195}$ $\overline{145}$ $\overline{121}$ $\overline{111}$

1 J	2 D		3 I	4 L	5 Z		6 F	7 R	8 U	9 P	10 U	11 X	12 G	13 V	14 T
	15 M	16 G	17 E	18 R	19 F	20 V	21 B	22 X	23 C	24 A	25 Q		26 O		27 F
28 Q	29 E	30 L	31 K		32 V	33 F	34 W		35 K	36 A	37 S	38 L		39 S	
40 I	41 L	42 V	43 U		44 U	45 V	46 K	47 M	48 F	49 G	50 X	51 T		52 T	53 Y
54 L	55 W	56 U		57 U	58 N	59 L	60 R	61 Z_1	62 M		63 E	64 D	65 T		66 F
67 W	68 Q		69 J	70 O	71 Q	72 R	73 T	74 I	75 N		76 I	77 J		78 R	79 A
80 F	81 Q	82 Z_1	83 T	84 B	85 M	86 H	87 G	88 J		89 M	90 H	91 F		92 S	93 U
94 G	95 X	96 A	97 Z_1		98 X	99 Z	100 V	101 R	102 A	103 M	104 G		105 F	106 M	
107 C	108 A	109 R	110 Y	111 Z_1		112 T	113 G	114 J	115 R	116 W	117 H		118 Q	119 G	120 A
121 Z_1	122 T	123 R	124 X	125 W	126 F	127 Q	128 C		129 B	130 K	131 Y		132 G	133 Z	
134 D	135 F		136 R	137 G	138 B	139 H	140 P		141 Y	142 O		143 X	144 G	145 Z_1	146 B
147 H		148 S	149 X	150 F	151 W		152 E	153 Z		154 Z_1	155 G	156 N	157 R	158 A	159 V
160 F	161 I	162 Q	163 B	164 C		165 F	166 D	167 X	168 W		169 A	170 H	171 N		172 D
173 G	174 C	175 R	176 F		177 L	178 R	179 O	180 F		181 I	182 H	183 F	184 Z		185 T
186 K	187 H		188 I	189 D	190 C		191 I	192 V	193 N		194 P	195 Z_1	196 Z		197 L
198 F	199 P		200 F												D.H.W.

(Solution next month)

THE THAI SEMINAR PROGRAM

P.L. 86-36

G92

A new training program in Thai language for preprofessional and postprofessional NSA linguists may provide a useful model for similar training in other languages. Although it has been in existence only since September 1976, three courses have already been conducted, and planning is underway to set up an Indonesian program along the same lines. In addition, one Thai seminar participant whose current assignment involves French (and who is under pressure to attain certification in French) declared, "This is exactly the type of course we need in French!" So there may be a French version soon, as well.

The purpose of the Thai program is to provide opportunities for preprofessional and postprofessional Thai linguists to participate once each year in a continuing education program, to grow in the language, to increase their knowledge of Thai cultural background, to discuss language problems which may be bothering them, and to receive periodic professional stimulation through immersion in the Thai language.

The program is designed to offer intermediate and advance training as a follow-up to the Thai Basic Course. Currently eight seminar-type courses -- two intermediate and six advanced -- are available. However, one advanced seminar on current affairs may be taken repeatedly, since the study material is always different.

Seminar sessions are held once a week for 12 weeks at a remote facility with a native instructor. Each session lasts 4 hours, during which all discussion is in Thai language.

Required reading assignments on Thai cultural subjects (sometimes supplemented by additional reading materials) are given one week in advance. Each student is assigned responsibility for making an oral report to seminar participants on a portion of the required reading. Everyone may discuss the oral reports, describe language problems they have encountered, and ask questions or contribute experiences related to the subject.

Instructors are native Thai speakers. Their job is to:

- offer criticism or correction when students misspeak;
- answer student questions regarding either subject matter or language;
- moderate the seminar; and
- stimulate discussion if conversation lags.

Because the amount of discussion generated by different topics varies considerably, other teaching techniques are used to supplement discussion, such as having students read aloud or transcribe from dictation.

J.P.R.S. LANGUAGE REFERENCE AIDS OFFERED TO N.S.A. LINGUISTS

After his lecture on 23 May 1977 in the Friedman Auditorium, [redacted] Chief of the U.S. Joint Publications Research Service (JPRS), turned over to his host, SIGTRAN Chairman [redacted] a multipage list of JPRS-produced aids for the translator. He stated that some of the aids are now out of print; others are still in print and may be obtained, at cost, through normal, time-consuming channels. But [redacted] kindly offered to send [redacted] informally, and gratis, as many copies as he requests of those aids that are still available.

Mr. Spiegelthal would like to consolidate his requests for the aids, and offers CRYPTOLOG readers this opportunity to obtain copies by cutting out this page and sending it, by 30 September 1977, to:

P.L. 86-36

[redacted] R51

	Title	Number of copies desired
	WORLDWIDE	
01	*Handbook for Contractors*, Nov 75, 51 pp.	
02	*Directory of JPRS Serial Publications 1957-1972*, JPRS 58118, Jan 73, 42 pp.	
03	*Directory of JPRS Ad Hoc Publications Jan-Dec 1972*, JPRS 58548, Mar 73, 78 pp.	
04	*Directory of JPRS Ad Hoc Publications Jan-Dec 1973*, JPRS 61363, Mar 74, 87 pp.	
05	*Directory of JPRS Ad Hoc Publications Jan-Dec 1974*, JPRS 64000, Jan 75, 69 pp.	
06	*Directory of JPRS Ad Hoc Publications Jan-Dec 1975*, JPRS L/5602, 5 Feb 75, 74 pp.	
07	*Selected Press Agencies of the World*, unnumbered, Jan 76, 9 pp.	
08	*Glossary of Narcotic Terms*, JPRS 60386, Oct 73, 58 pp.	
09	*Notes on the Language of Communism*, unnumbered, undated, 19 pp.	
	USSR	
100	*Glossary of Selected Russian Terminology*, unnumbered, Jun 69, 152 pp.	
101	*A Short Dictionary of Fishery Terms (Russian-English)*, JPRS 44072, Jan 68, 67 pp.	
102	*Russian-English Glossary of Motor-Transport and Related Terms*, JPRS 19600, Jun 63, 77 pp.	
103	*Recommended Radio Terms*, JPRS 55957, May 72, 17 pp.	
104	*Glossary of Russian Abbreviations and Acronyms*, Library of Congress/ATD, 1967, 806 pp.	
105	*Apollo-Soyuz Test Project Glossary (Russian-English, English-Russian)*, ASTP 20020.1, 3 Feb 75, 364 pp.	
106	*Concise Handbook on Space Biology and Medicine*, Parts I & II, JPRS 61236-1 & 2, Feb 74, 501 pp.	
107	*Drug Products*, JPRS 64908, Jun 75, 275 pp.	
108	*All-Union State Standard GOST 15845-70: Cables, Wiring and Cords, Terms and Definitions*, JPRS 61234, Feb 74, 23 pp.	
109	*Administrative Gazetteer of the USSR - 1974 Edition*, 188 pp.	
110	*Directory of the USSR Academy of Sciences*, JPRS 66592, Jan 76, 167 pp.	
	EASTERN EUROPE	
200	*Glossary of Standard East European Legal Terms*, unnumbered, Oct 68, 8 pp.	
201	*Abbreviations in the Czechoslovak Press*, JPRS 51050, Jul 70, 185 pp.	
202	*Glossary of Special Terms, Acronyms and Abbreviations As Used by East German and Other German Publications*, JPRS 64561, Apr 75, 166 pp.	
203	*Abbreviations in the Hungarian Press*, JPRS 53853, Aug 71, 127 pp.	
204	*Abbreviations in the Polish Press*, JPRS 47870, Apr 69, 161 pp.	
205	*Abbreviations in the Romanian Press*, JPRS 62348, June 74, 72 pp.	
	PEOPLE'S REPUBLIC OF CHINA	
300	*Chinese-English Dictionary of Modern Communist Chinese Use*, JPRS 20904, Feb 65, 845 pp.	

301	*Standard Translation of Chinese Terms*, JPRS 57420, Nov 72, 119 pp.	
302	*Glossary of Chinese Communist Terms and Phrases*, unnumbered, Oct 69, 113 pp.	
303	*Standard Chinese Telecode Book*, unnumbered, Dec 66, 101 pp.	
304	*Chinese-English Concordance to "Quotations from Chairman Mao Tse-tung,"* unnumbered, Jun 71, 167 pp.	
305	*Simplified Handbook on Administrative Division of the People's Republic of China -- 1972*, JPRS L/4379, Jan 73, 152 pp. (GUO control removed 24 Apr 74)	
	ASIA	
400	*Glossary of Terms Used in the Overseas Chinese Press of Southeast Asia*, unnumbered, Jun 72, 88 pp.	
401	*Glossary of Shipping Terms Used by the Chinese in Southeast Asia*, unnumbered, Mar 72, 24 pp.	
402	*Abbreviations in the Cambodian and Lao Press*, JPRS 62295, Jun 74, 50 pp.	
403	*Guide to Translation of Cambodian Press Material*, unnumbered, Jun 74, 28 pp.	
404	*Glossary of Indonesian Abbreviations and Acronyms*, unnumbered, Jun 71, 18 pp.	
405	*Glossary of North Korean Terms*, unnumbered, May 73, 122 pp.	
406	*Standard Translation of North Korean Communist Terms*, JPRS 26237, Sep 64, 95 pp.	
407	*Glossary of Specialized Japanese Terms*, unnumbered, Apr 74, 255 pp.	
408	*Guide to Translation of Lao Press Material*, unnumbered, Mar 71, 16 pp.	
409	*Glossary of Malaysian and English Abbreviations Appearing in the Press of Malaysia and Singapore*, JPRS 56582, Jul 72, 49 pp.	
410	*Abbreviations in the Mongolian Press*, JPRS 57176, Oct 72, 47 pp.	
411	*Vietnamese-English Dictionary*, Vol I (A-L) & Vol II (M-Y), JPRS 37700, Sep 66, 1476 pp.	
412	*Glossary of Terms Used in the North Vietnamese Press*, unnumbered, Sep 71, 93 pp.	
413	*VC/NVA Terminology Glossary*, Vol I (A-M) & Vol II (N-Z), 3d Edition, US MACV, Jul 71, 610 pp.	
	NEAR EAST AND AFRICA	
500	*Abbreviations in the African Press*, JPRS 54371, Nov 71, 121 pp.	
501	*Guide to Translation of Middle East Press Material*, unnumbered, Nov 74, 24 pp.	
502	*Guide to the Transliteration of Algerian Place Names*, JPRS 58041, Jan 73, 63 pp.	
503	*Alphabetical Listing of Cypriot Towns and Villages Transliterated into English from Greek and Turkish Names*, unnumbered, Oct 73, 63 pp.	
504	*Abbreviations, Acronyms and Special Terms in the Press of Greece and Cyprus*, JPRS	
505	*Principal Journalists and Trade Union Leaders in Egypt*, unnumbered, Jan 72, 26 pp.	
506	*Guide to the Transliteration of Moroccan Arabic Place Names*, JPRS 64704, May 75, 45 pp.	
507	*Abbreviations, Acronyms and Special Terms in the Turkish Press*, JPRS 64701, May 75, 68 pp.	
	WESTERN EUROPE AND LATIN AMERICA	
600	*Glossary of Abbreviations, Acronyms and Terms Used in the Western European Press*, JPRS 58963, May 73, 62 pp.	
601	*Abbreviations in the Latin American Press*, JPRS 64152, Feb 75, 192 pp.	
602	*Spanish-English Scientific Glossary*, unnumbered, Jan 72, 332 pp.	
603	*Illustrated List of Common and Scientific Names of Fishes from the Gulf of Mexico in Latin, Spanish, Russian and English*, JPRS 46741, Oct 68, 46 pp.	

TO: [ ] R51

P.L. 86-36

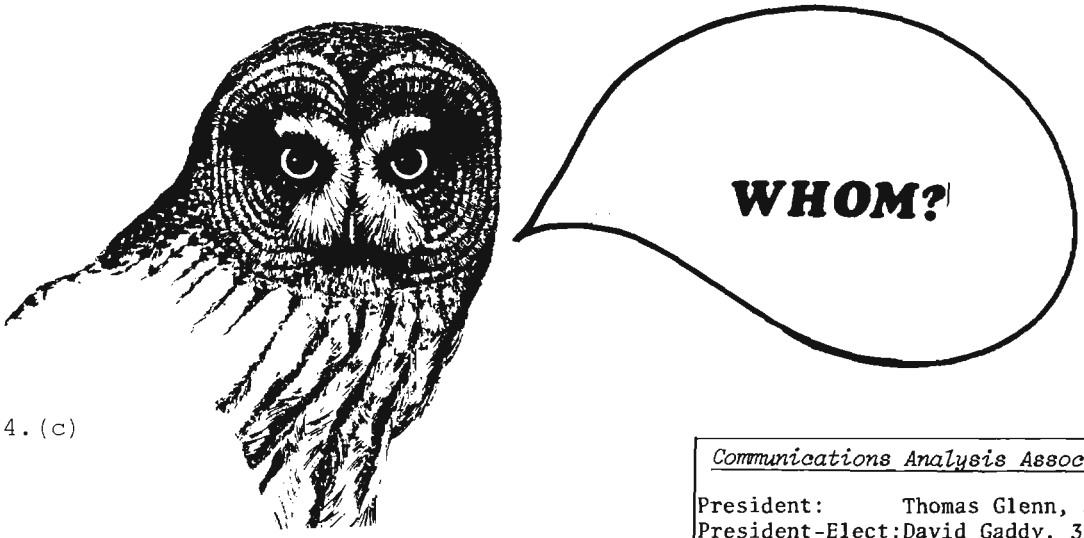
Please order for me the JPRS publications I have indicated on this order blank -- one copy each unless otherwise specified.

I realize that some of these publications may be out of print and unobtainable now.

(Name, printed)

(Organization and room number)

CUT ON LINE. MAIL ENTIRE PAGE.



EO 1.4.(c)

C.A.A. NEWS

by [redacted]

P14

"Whom?" Or, rather, "*Who*?" *Who* belongs to the CAA, anyway? What kind of people are they? Where do they work, and what do they do? And why do they want to be members of the CAA?

A quick look at the membership list [redacted] leaves a person with two distinct impressions:

First, the CAA population is really dispersed throughout the Agency. There are no real pockets or strongholds of members to speak of.

Second, a significant number of the members may well view their association with CAA as a way to keep up with "what's going on" around the Agency.

With this in mind, your fearless CAA Board has launched out in yet another effort to meet the needs of our members: a series of operational briefings, in what we hope will be an informal atmosphere. These briefings are designed to let CAA members "get current" on whether we're gaining on the target or the target is gaining on us.

[redacted]

This is all very experimental. Dennis Chadwick, a TA intern (x4202s), agreed to steer this effort for CAA. The first of this series, held recently, [redacted] If you have an idea for a briefing in this series, see Dennis. If you would like to talk to kindred souls (not kindled soles, Harvey!) about *your* problem (target, that is), see Dennis. If you want to know where and when the next briefing is, join the CAA (members are notified of times and places). Or find a CAA member who will let you read his mail!

~~(C)~~

Communications Analysis Association:

President:	Thomas Glenn, 5973s
President-Elect:	David Gaddy, 3247s
Treasurer:	Timothy Murphy, 3791s
Secretary:	Jane Dunn, 8025s
Board members:	Capt.J.Williamson, USN, 3981s
	Earl Broglie, 3573s
	Wayne Stoffel, 3369s

(U)

UPCOMING EVENTS

September

The presentation by [redacted] that was scheduled for this month has had to be canceled.

A picnic? It's still a gleam in our President's eye at this writing, but the CAA could be having its First Annual Picnic this month.

October

A nominating committee will be appointed to seek out the best slate of candidates for the forthcoming CAA elections at year's end. (No, let's *not* call it Project DIOGENES.) If you want to be involved in this process, either as picker or as pickee, let one of the board members know.

(U)

LOGO WANTED!

"*logo:* n., a clipped form of *logotype*."
"*logotype*: n., a distinctive company signature, trademark, colophon, newspaper nameplate, etc."

The CAA is looking for a logo. We might even start up a contest to find one. Watch for details, or check with a board member.

[redacted]

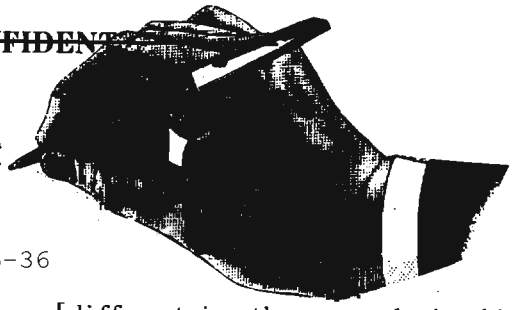
SIGNS BY W.S.

(U)

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Letter to the Editor



To the Editor, CRYPTOLOG:

The letter from [redacted] P.L. 86-36 in your June 1977 issue, responding to my letter in March, was something of a surprise. I anticipated some anger from quarters other than the "desk linguist" (a term which I have never considered derogatory, by the way, rather one that aptly describes the very backbone of the language-reporting effort in the Agency).

But before I get into the various issues raised by [redacted] I will do something I should have done in the beginning, that is, establish some credentials for addressing the problem. I started as a desk linguist at NSA in 1963 and stayed in that job as a translator-transcriber-analyst-reporter, section chief, integrated analyst at three field sites, branch chief, and Group language coordinator until 1977. I was certified by the Language Panel in 1969 and by the Special Research Panel in 1972. I was a member of the [redacted] PQE Committee from 1970 to January 1977 and chaired that committee twice. I was a member of the DDO Language Advisory Committee from July 1975 until February 1977 and I am currently the intern sponsor [redacted] Language Interns. "Ignorance concerning the work that the desk linguist does for the Agency"??? Ignorance indeed, [redacted] Then again, I may have overestimated my infamy.

At any rate, let me get to the real issue. No intelligent person would argue against the idea that "turning foreign sounds or words into English" is a difficult task requiring a great deal of knowledge that is "peripheral" to the skill itself. It is a well-founded rule that you must have some degree of subject-matter knowledge to get those foreign sounds and words into understandable English; you need target knowledge and a raft of other skills -- cryptanalysis, TA, etc, in some cases. And very often for the highly qualified desk linguist, language skill is so intertwined with those other skills that it becomes indistinguishable and we have the guy or gal that I believe to be one of the most valuable resources this Agency will ever see, the "complete SIGINTer."

[redacted]

The "truth" I was trying to get at in my letter was that, even after certification, few people would develop so well as to get much beyond 13, a grade level that starts at close to $25,000 per year. And, hopefully for the last time, let me try to destroy the myth that it is any different in other cryptologic skills: I know few people in the TA, CA, or SR field working on a particular problem who are paid at a rate higher than GG 13. As in the language field, there are precious few billets beyond 13 and the competition for those promotions is fierce -- as I believe it should be.

A few facts:

- Average pay for [redacted] transcribers, who must be excellent in their language and possess the peripheral skills -- GG 11-12.
- Average pay for civilian technicians hired by U.S. companies working abroad -- and, again, they must be near-fluent -- $17,000-20,000 per year, except in the desert oil fields, where it is higher. EO 1.4.(c) P.L. 86-36
- Average pay for simultaneous interpreters at the United Nations (and their language skill would put most of us to shame) -- $19,000-20,000 per year.

There are two points I want to make here: first, the average pay scales are remarkably similar to our own, and, secondly, everybody expects the good linguist to have the peripheral skills when they are getting that much money. P.L. 86-36

New subject: Neither I, nor anyone I know, wants to replace you, or any other good linguist, with "high school graduates at grade level 2." The introduction of the GG-2s [redacted] is driven by three things:

- Average grade structure, which is too high and must be lowered. This is not a problem we dreamed up. It is real and it must be solved. One way to help that is to fill in the bottom of the grade structure.
- [redacted]

P.L. 86-36
EO 1.4.(c)

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

In the meantime, [redacted] please forgive me for quite unintentionally offending you. My background should help to convince you that I could not ever put linguists down without including myself.

Dan Buckley, M03

P.L. 86-36

~~(C — CCO)~~

"Simonoff says!"

The national spirit that created the Potemkin village and Gogol's "Inspector General" apparently lives on in the Soviet Army. Writing in a recent issue of the official organ of the USSR Ministry of Defense, a Soviet Army officer deplores two methods that are used to achieve snappy precision in tactical exercises involving armored personnel carriers. Describing one of these methods, he writes:*

Recently it has become the practice at our exercises, especially tactical exercises, to have none of the issued commands executed until the exercise leader or the subdivision commander has given the code number "222." For example, the company is located in the concentration area. The command is given, "Mount your vehicles!" But everyone continues to carry out his previous duties until he hears the slowly pronounced words, "T-w-o h-u-n-d-r-e-d t-w-e-n-t-y t-w-o!", after which they dash to the combat vehicles. That is how all the subsequent commands are executed: "Take your positions -- 222!", "Start your motors -- 222!", "Form a line of platoon columns -- 222!", and even "Fire a burst from the front -- 222!"

The question arises, "What advantage is to be gained from this innovation?" Probably just one thing: we strive for precision, the simultaneous beginning of command execution, and, especially, beauty. But, on the other hand, we lose an awful lot, particularly time. Because this is modern combat! Under real-life conditions, a single command will be issued. Consequently, it is necessary to strive for rapid reaction to precisely *that* command, rather than to those ridiculous 222's.

The Soviet author says that these "ridiculous 222's" will not be used in real-life combat situations. But who can predict that, in some future engagement, real Soviet troops will not hear some other code number used to tell them "Charge! -- Simonoff says!"

(U)

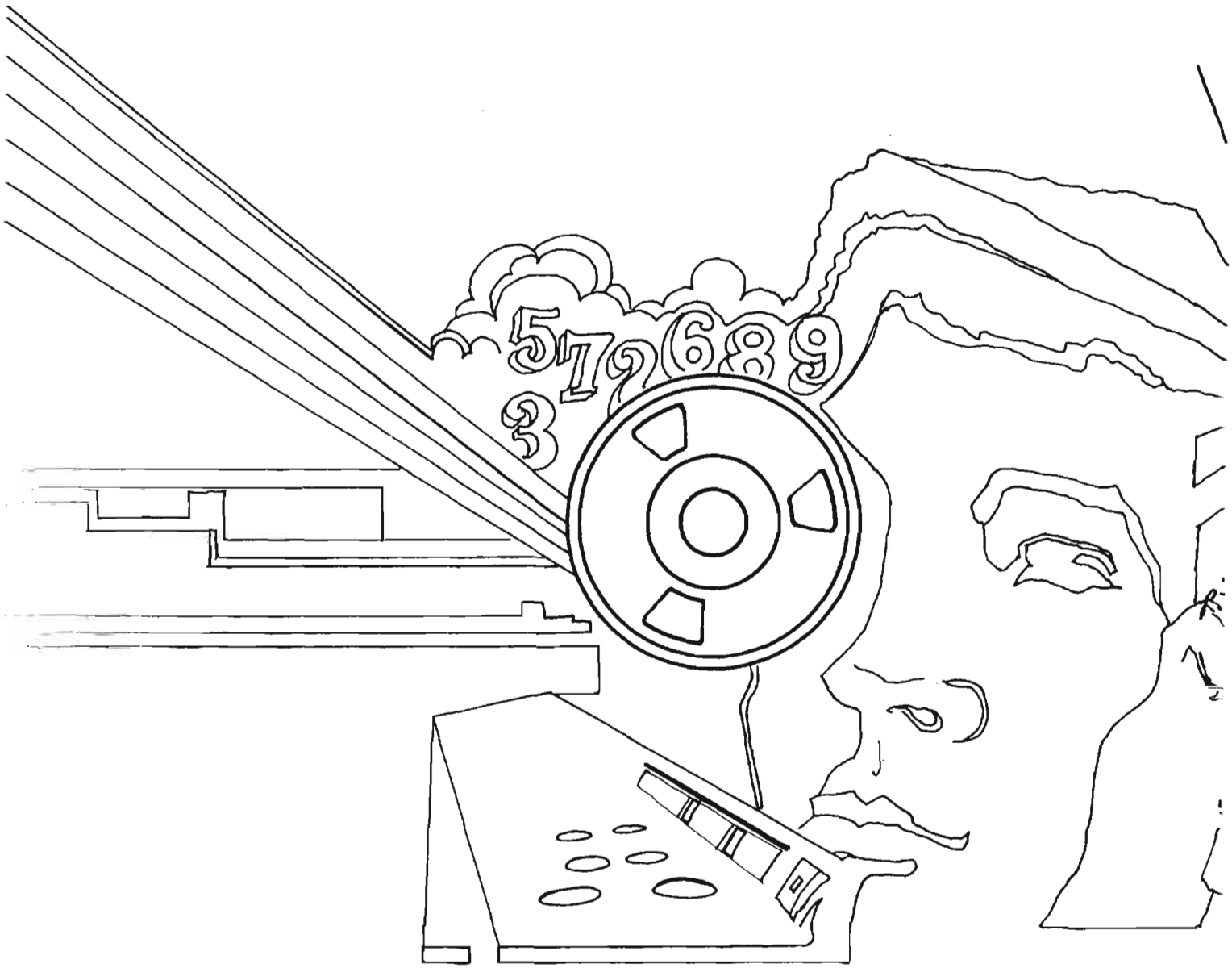
*Senior Lieutenant S. Latush, "Tactics or Parade Precision?", *Voennyj Vestnik* (Military Herald), February 1977, pp. 57-58.

NEW UNSYNDICATED COMIC STRIP WILL APPEAR FROM TIME TO TIME IN "CRYPTOLOG"

Al Balloni, Editor

By A.J.S.

(U)


5 7 2 6 8 9
3

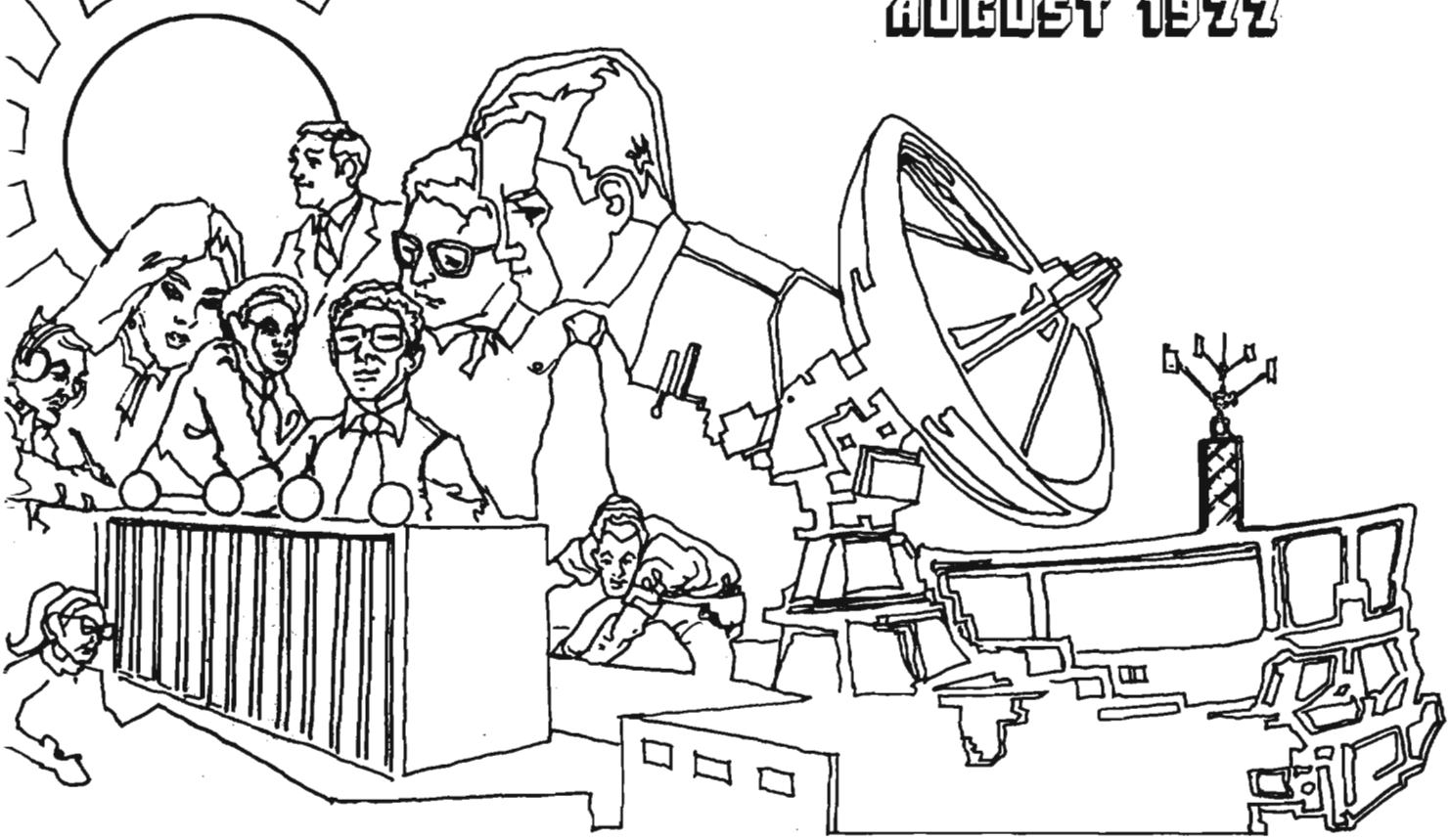
DOCID: 4009800

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

AUGUST 1977



WHAT IS AN INFORMATION RESEARCH ANALYST?. [redacted] 1
"DIALOG" AVAILABLE AT N.S.A.....2
LET ME REPEAT AND MAKE MYSELF CLEAR....Peter Jenks.....3
POSTSCRIPT TO "DATING GAME"..... [redacted] 5
NEW DIRECTIONS IN INTELLIGENCE COMMUNITY.David W. Gaddy.....6
EARLY DAYS IN N.S.A. COMPUTING..... [redacted] 8
TELLING IT LIKE IT IS.....Ramon A. Santiago-Ortiz..11
EXPLETIVES DELETED?.....A. J. Salemme.....13
WHAT ARE THEY UP TO ANYWAY?..... [redacted] 20
LETTERS TO THE EDITOR.....21

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526,MDR Case # 54778

DOCID: 4009800

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. IV, NO. 8 AUGUST 1977

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5642s)
Collection.....[redacted] (8955s)
Cryptanalysis.....[redacted] (4902s)
Language.....[redacted] (5236s)
Machine Support.....[redacted] 4267s)
Mathematics.....Reed Dawson (3957s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....[redacted] (4477s)
Production Manager.....[redacted] (4998s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4009800

WHAT IS AN INFORMATION RESEARCH ANALYST?

[redacted] **T12**

"Information Science is concerned with the recognition, acquisition, orderly storage, maintenance, retrieval, and dissemination of information, data or materials, in support of NSA/CSS analytic and research functions. Information Science is interdisciplinary in nature and draws upon computer science, library science, documentation and other technologies for theory and methods." This quote was taken from the Information Science Intern Manual.

The field of Information Science has not been effectively introduced to NSA/CSS. Certainly this is partially attributable to the lack of a conclusive, widely-known explanation of the discipline. At present, T12 is the only NSA organization which seeks to train such analysts. This restrictive compartmentalization is shortchanging the Agency. It is time to recognize the skills of Information Science Analysts (ISAs) as skills of potential benefit to all organizations.

T12 can and does provide a valuable service to NSA, but it is not used to its greatest potential. Perhaps this is because the services are not advertised enough or that experience has been that the wrong services have been offered. The reaction on the part of the users seems to be to give up. A more productive approach by customers might result in better experiences in the future. Since T12 is a service organization, suggestions by other organizations would be

P.L. 86-36

DOCID: 4009800

welcomed readily and, if feasible, could be instituted.

All organizations should take another look at Information Science Analysts and note the skills and knowledge that well-trained ISAs have.

[redacted]

If that analyst or those offices had an experienced ISA to turn to for help -- right in the same office -- product might improve, and experience with and services from T12 might also improve.

Often, analysts are unsure of whom to consult or even if anyone should be consulted on a particular problem. The in-office ISA could, at least, direct the questioning analyst to the correct T12 service.

Many organizations do long-term research projects and have Special Research Analysts (SRAs) working on them. However, it is my understanding that SRAs are to do day-to-day research and reporting, while ISAs should research the long-term or new efforts. Perhaps a pool of ISAs could be organized for temporary loan to offices for such projects. In fact, such is the situation with IS interns in many cases. Why not continue this practice, extending it to professionalized analysts?

Although I am an intern and my judgment is certainly biased, I think that the IS interns have already proved my proint. When interns go into non-T12 elements and work alongside other analysts, they see how much people do not know about T12's services. They also see where T12 is lacking. The interchange between the interns and their parent organization, T12, is an excellent way to encourage changes which will improve the information services at NSA. A pool of ISAs might enhance the possibilities for continued interchange.

Thus, I make the following proposals:

1. [redacted]
2. T12 should investigate the possibility of establishing a pool of ISAs who can be loaned on a temporary basis to those organizations needing such service.
3. Non-T12 offices should investigate the need for full-time ISAs and include them in their next budget requirements.

~~(CONFIDENTIAL)~~

DIALOG Available at NSA

DIALOG, the on-line data system shown in the illustration on page 1, is one of the newest systems serving the information needs of NSA analysts. The system provides access to more than 40 open-literature data bases dealing with science, technology, business/economics, and the social sciences. Individual files include biology, chemistry, meteorology, oceanography, physics, agriculture, international business forecasts, electronic data processing, patents, computers, energy, metals, education, psychology, etc.

Thousands of periodicals are indexed, ready to help solve your information needs.

To make use of the DIALOG system, and for other information service, call or visit the following organizations:

Organization	*Room*	*Telephone*
T1213	2N090	5759s
T1222	2C053	3258s
T1222	2E029	3189s

(U)

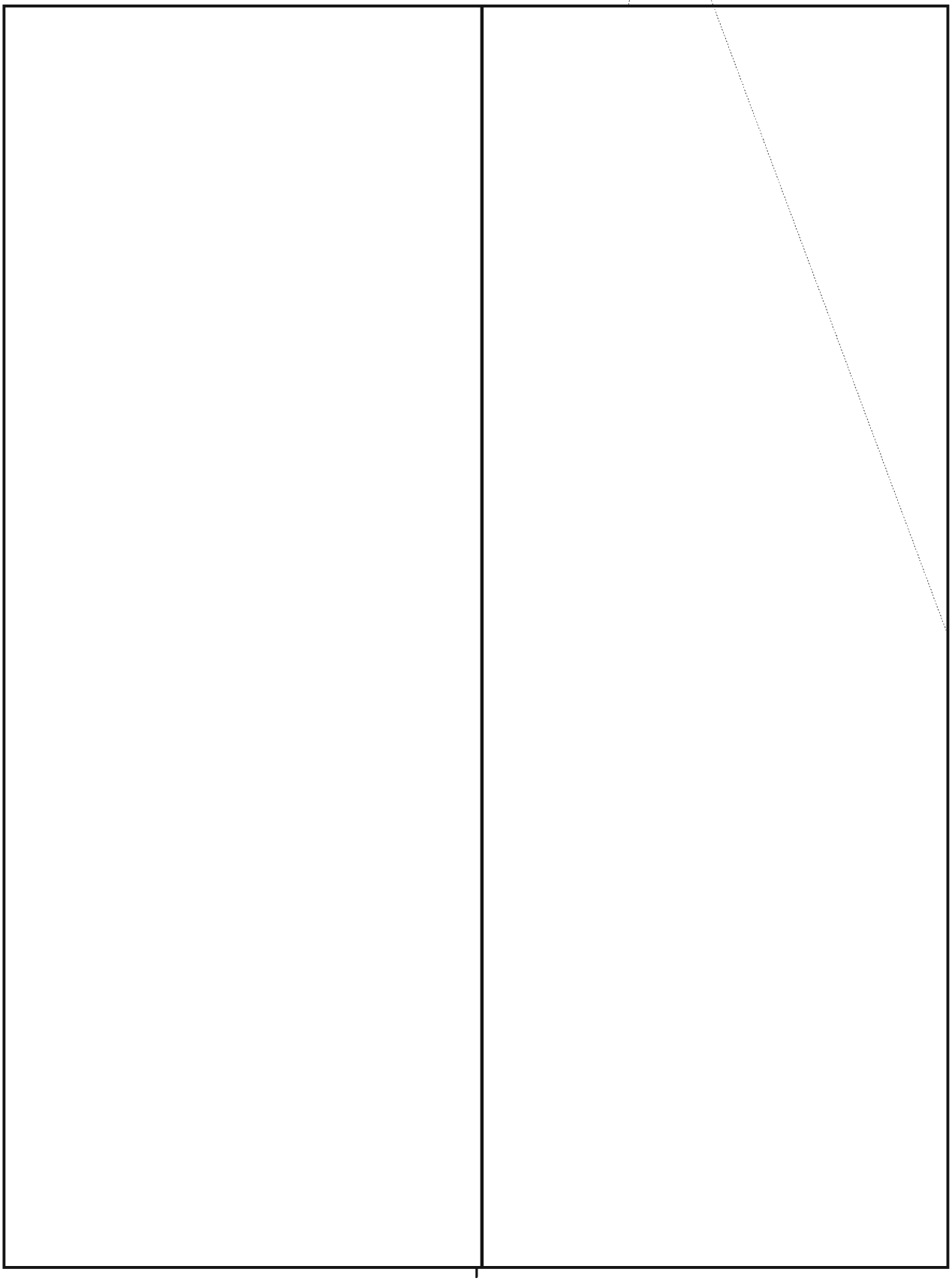
DOCID: 4009800

LET ME REPEAT –
(I say, let me repeat)
AND MAKE MYSELF PERFECTLY CLEAR

Peter Jenks, G

EO 1.4.(c)
P.L. 86-36

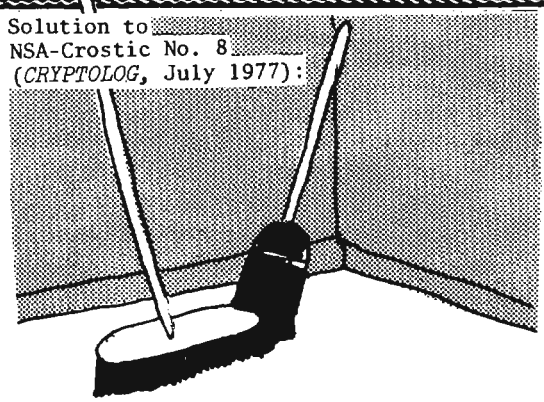
EO 1.4.(c)
P.L. 86-36



DOCID: 4009800 E.O. 1.4.(c)
P.L. 86-36

(TSC)

Solution to NSA-Crostic No. 8 (*CRYPTOLOG*, July 1977):



"Stop the Presses!", *NSA Technical Journal*, Vol. XXI, No. 1 (Twentieth Anniversary Issue), Winter 1976.

"Many [codewords are] vague enough to leave doubt as to their precise interpretation. [One officer told me], "I got a message which directed me to get ready for Operation CLEAN SWEEP. I didn't know whether to run for the broom closet or pack my bags in anticipation of being reassigned."

(U)

POSTSCRIPT TO "DATING GAME"

P.L. 86-36

R51

It's hard to take exception to a formula as simple as Y + L + M + D = N. One can, and I will, add a few complications.

A note at the end of Dave Williams' article, "Dating Game" (CRYPTOLOG, July 1977) specifies: "For dates in the twenty-first century, subtract one from N; for those in the nineteenth century, add 2."

To subsume these two apparently ad-hoc directives under a general rule, valid for all centuries (after the sixteenth, when the calendar reform went into effect): Let C be the *first* two digits of the year (i.e., the *century* digits, but, numerically, one smaller, since we are now in the twentieth century, although C = 19). Like L (Williams' leap-year factor), let $F = \frac{C}{4}$ (ignoring any remainder). Then, the "century correction" to the Williams formula is to add to his N (before finding the remainder after division by 7) the terms

F - 2C + 34

(or, alternatively, F - 2C - 1).

For the nineteenth, twentieth, and twenty-first centuries, the century correction, in tabular form, is:

Century	*C*	*F*	*F - 2C + 34*
19	18	4	+2
20	19	4	0
21	20	5	-1

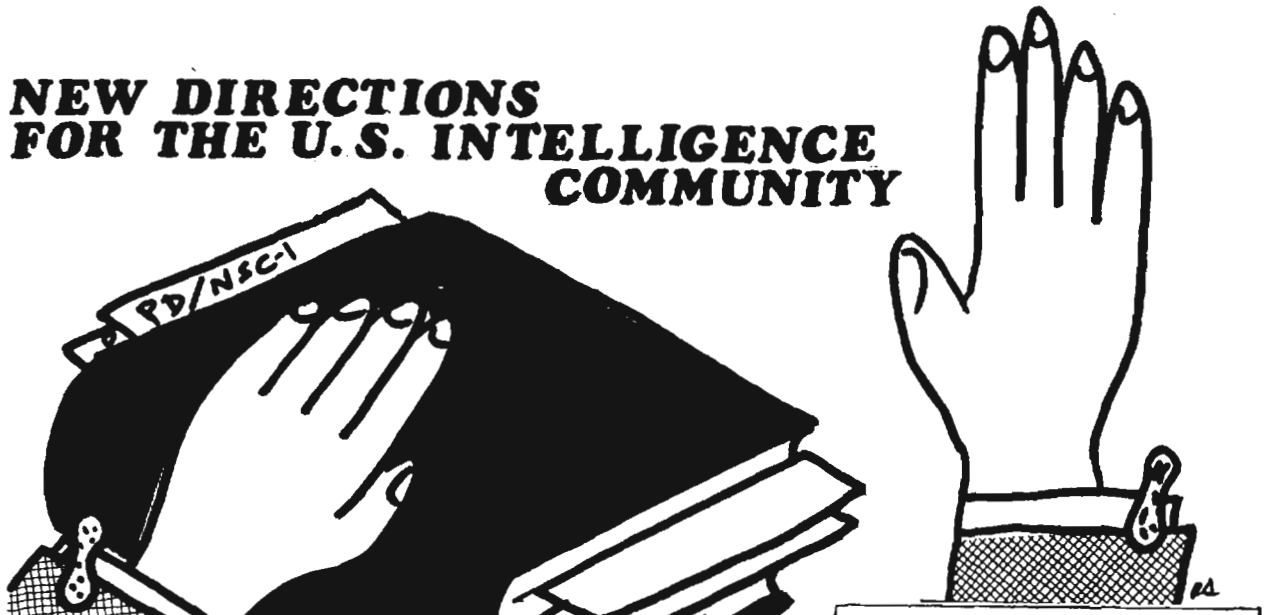
Thus, the "ad-hoc" directives aren't all that ad-hoc. A more detailed treatment can be found on page 209 of *Elementary Number Theory*, Uspensky and Heaslet, Mc-Graw-Hill, New York, 1939 (available in NSA Library, call numbers QA241. Us6).

(UNCLASSIFIED)

P.L. 86-36

DOCID: 4009800

NEW DIRECTIONS FOR THE U.S. INTELLIGENCE COMMUNITY



David W. Gaddy, D5

Reprinted from *Field Information Letter* 4-77, April 1977 with the kind permission of its editor, William Hunt

One of the Inaugural Day acts of the Carter administration was the announcement of a reorganization of the National Security Council. Reflecting the personal touch of the new President, the change was "to place more responsibility in the departments and agencies while assuring that the National Security Council (NSC), with [the] Assistant [to the President] for National Security Affairs, continues to integrate and facilitate foreign and defense policy decisions"[1]. Participation at appropriate NSC meetings was broadened, yet a more flexible concept was evident. The Carter NSC was to be more a mechanism than a structure, a facilitating mechanism to assist the President in analyzing and reaching decisions in matters of foreign, domestic, and intelligence policy.

The concept is most evident in the establishment of just two basic NSC committees, through which all work is to be done:

- the Policy Review Committee (PRC), and
- the Special Coordination Committee (SCC).

Chairmanship of the PRC is designated for each meeting, depending on the subject matter being considered; the Assistant for National Security Affairs (Mr. Brzezinski) chairs the SCC. Both committees are of concern to us. Both impact on the organizational structure announced by President Ford in EO 11905[2].

The PRC is "to develop national security policy for Presidential decision in those cases where the basic responsibilities fall primarily within a given department but where the subject also has important implications for other departments and agencies." Examples are:

- foreign policy issues with significant military or other interagency aspects;
- defense policy issues with international implications;
- coordination of the annual Defense budget with foreign policy objectives;
- preparation of a consolidated national intelligence budget and resource allocation for the Intelligence Community; and
- international economic issues pertinent to U.S. foreign policy and security.

The intelligence function of the PRC thus replaced that of the Committee on Foreign Intelligence (CFI) under EO 11905. True to the "flexible mechanism" idea, when the PRC is performing in the "CFI-like" role, the Director of Central Intelligence (DCI) chairs, and staff support

[1]Presidential Directive/NSC-2, 20 January 1977. PD/NSC-1, also dated 20 January 1977, established the Presidential Directive and the Presidential Review Memorandum (PRM) as instrumentalities to direct the work of the NSC and participating agencies, and to inform the departments and agencies of Presidential directives. They replace the National Security Study Memoranda (NSSM)/National Security Decision Memoranda (NSDM) of the Kissinger era. The PRM series directs that reviews and analyses be undertaken on subjects of interest to the President.

[2]See "Reorganization of United States Intelligence," *Field Information Letter* 8-76, August 1976, pp. 4-8.

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

(especially of the program and budget sort) is provided by the Intelligence Community Staff (ICS). PRC(I) is the shorthand acronym.

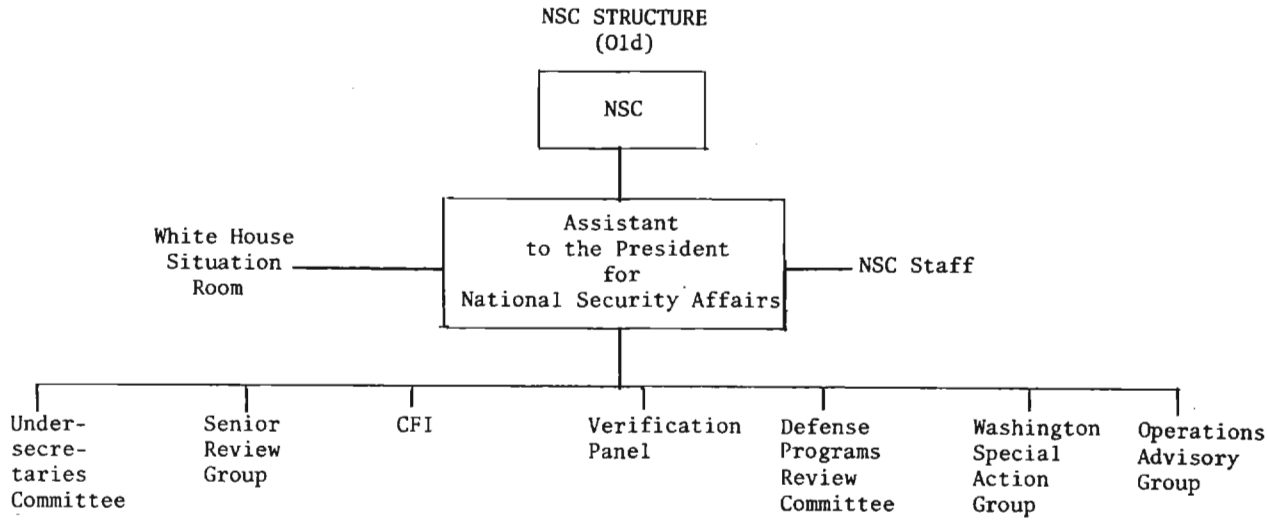
The Intelligence Research and Development Council, shifted from IRAC (the former Intelligence Resources Advisory Committee, the resource counterpart of USIB, the intelligence board) to CFI last go-round, has been resubordinated to the PRC(I).

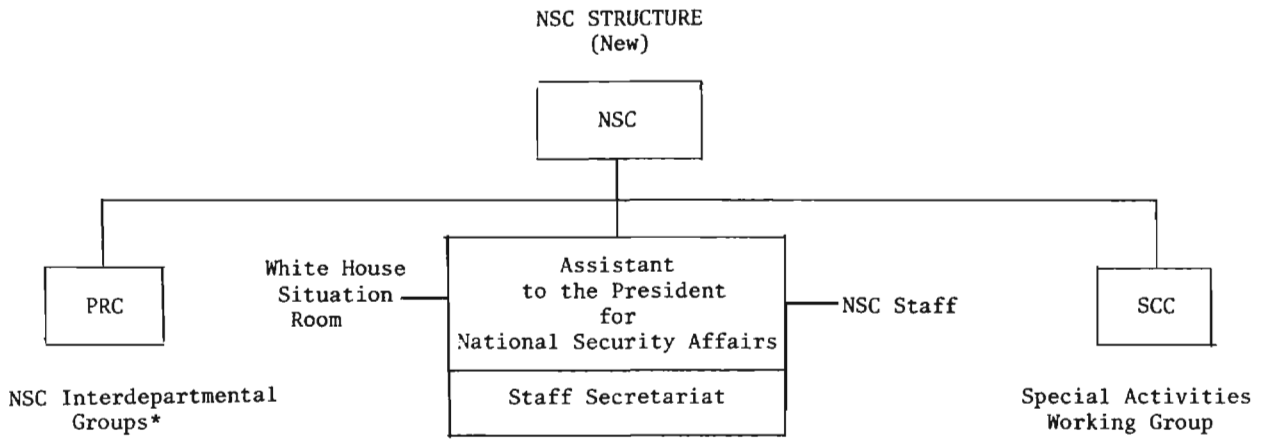
The SCC deals with special cross-cutting issues requiring coordination in the development of options and the implementation of Presidential decisions. This includes such items as oversight of sensitive intelligence activities, arms control evaluation, and assistance to the President in crisis management.

[redacted]

[redacted]

What does all this portend for the substructure? It's too early to tell, but we shouldn't have to wait long. A full-scale "comprehensive review of major foreign intelligence activities and the organizational structure and functioning of the Intelligence Community" has been directed of the SCC by the President in his PRM/NSC-11 of 22 February 1977. Among other considerations, it will specifically address EO 11905 and the interrelationships among the various intelligence agencies. It had a "due date" of June 1977. The Senate, Select Committee has a special interest in the matter of legislative charters. Therefore, Congress will be watching the outcome closely, as will we all.

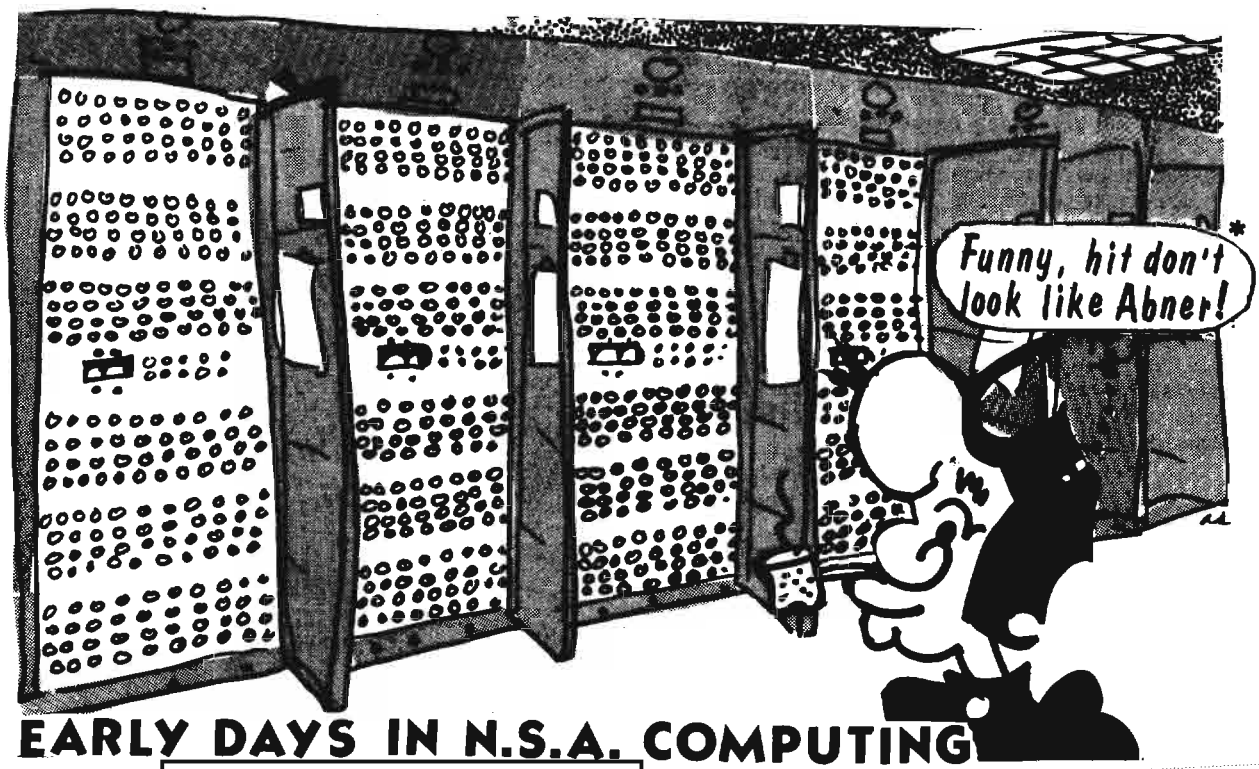




*The five regional and one Politico-Military interdepartmental groups are carry-overs, expected to change. The NSC staff is organized on a regional/functional basis.

~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4009800



EARLY DAYS IN N.S.A. COMPUTING

[redacted] P12

P.L. 86-36

Before the first generation of modern computers became a reality, NSA (even in the fragmented form of early years before officially constituted as such in 1952) realized the enormous possibilities of these devices. No satisfactory model being commercially available, not even from IBM, our staff of engineers at Arlington Hall Station proceeded in 1950 to design and build a computer tailored for NSA problems. This device, which became known as ABNER, was our first real computer, the first means we had, other than such things as primitive IBM card-sorting devices, of relieving analysts from the drudgery of repetitive pencil and paper trials. ABNER's genesis and construction owed much to the abilities of [redacted] of R&D.

The ABNER machine consisted of four logical units with electronic circuitry capable of carrying out arithmetic, control, analytical, and input-output functions, connected to a memory device holding 1024 48-bit words. This memory took the physical form of 128 tubes filled with mercury, each tube equipped at one end with a sound-pulse generator and at the other with a read-out gate which transformed the sound pulses back to electrical signals.

When in operation, each tube contained a train of 384 sound or no-sound pulses, representing the binary digits 1 and 0 in eight computer words of 45 bits apiece, with an additional 3 bits for synchronization. Once a word was read out at the gate, it was immediately available for interpretation by one of the logical units. Either in its original form, or as altered by a logical unit, the word was then sent back to the other end of its tube and once more converted to a train of sound pulses. While traveling through the tube in this form, the word was unavailable for any purpose, and if it was called for by the program during this interval, the computer had to wait until it arrived at the read-out gate. A good deal of the programmer's time was therefore devoted to planning an arrangement of the program orders and the data so that this delay time would be minimized in the execution of the program. This delay time could be anything from 0 to 7 cycles. An ABNER cycle consisted of 48 microseconds.

The first 5 bits of a word defined one of the 32 basic ABNER Operations when the word was interpreted as an Instruction. The succeeding four 10-bit segments were called the α, β, γ, δ ("alpha," "beta," "gamma," "delta") addresses. In the generalized form of an ABNER operation, the machine sent words α and β to the Arithmetic Unit, performed the indicated Operation, stored the result in word γ, and took the next Instruction from word δ.

The power and versatility of ABNER were considerably enhanced by a number of deviations

---

* Wal, hit is! See: *History of NSA General-Purpose Electronic Digital Computers*, by Samuel S. Snyder, Monograph No. 2, NSA Technical Literature Series, 1964 (S-CCO).

DOCID: 4009800

P.L. 86-36
EO 1.4.(c)

from the above scheme which permitted an effective use of more than 32 Operations. Certain of the Operations utilized the α bits to expand the Instruction code. Five analytical orders provided a "Beta Prime" feature whereby an order could be set up to refer to two operands, one at the given β address, the other at the β address plus 512 (mod 1024). An auxiliary order D used before certain other orders modified their functions. It was possible to hold one operand during repetition, or to define any two streams of pentabits as operands in a repetitive process. This facilitated sliding messages against each other in search of depths created by reuse of keys, which was quite a common phenomenon in those relatively innocent days of long ago.

In the four logical units of the ABNER computer, a word was interpreted differently, as follows:

In the	*Interpreted as*	
Arithmetic unit	a number	bits 2^{43} to 2^{0} plus sign
Control unit	an order	δ γ β α OP
Analytical unit	pentabits	eight 5-bit words (5 bits not used)
Input-output unit	characters	nine 5-bit characters

This versatility of interpretation gave ABNER a more powerful computing ability than the modern programmer would assume from its modest memory and limited number of orders.

ABNER was designed to have magnetic tapes, punched cards, paper tape, and an IBM CXCO-1 typewriter as input/output media. In my experience, the latter two were the most widely used. When it proved necessary to write a program which could not fit into the available memory, it often proved practical to organize the job in what we would now call modules, so that after module 1 completed its task, results could be outputted or stored in a small part of the memory, and module 2 could be read in from paper tape, destroying module 1 and data no longer required. In this manner, several steps could be carried out serially, circumventing to a degree the memory limitations.

In the early use of ABNER, pioneer programmers such as [redacted] contributed to the development of the diagnostic programs grouped under the name STETHOSCOPE. These were forerunners of the RYE programs developed much later; these RYE programs remain available today.

As an example of the excellence of ABNER's logical design, consider the P order, nicknamed "Swish." In one operation "Swish" lined up two streams of pentabits, and returned a count of hits, accomplishing thereby what even today takes several orders to do. Modern computers are not logically superior to ABNER: they have merely benefitted from staggering advances in electronic technology. The logical organization of ABNER was not only well in advance of its own era, but in some respects has yet to be equaled by any present computer.

Very few examples of ABNER programs survive today. [redacted] Four other programmers, all individually brighter than myself, had been assigned to do this job as a team. Each said his or her part was OK, but when the four parts were put on ABNER at the same time, distressing things occurred and no solutions appeared. Each was therefore convinced that one of the other three was sadly in error, and an impasse developed. At this point I was called in to give it a try.

In those long-departed days it was considered that analysts should do the thinking, and programmers should do what they were told. So the analyst [redacted] explained to me in great detail the method of attack. It all seemed very clever and complicated, but as a simple-minded person I couldn't help feeling there was an easier way. (As one detail, in recovering a fractionation of the cipher, they tested for an excess of 7s by carefully counting all 10 digits before making the calculation; I merely counted 7s, and not -7s.) With the advantage of a simplified approach and the fact that -- in contrast to the team of four -- my right hand did know what my left hand was doing, I was able to make the VITAMIN program work. This was beneficial to the Agency (and to my career therein), but I don't know that the team of four was altogether ecstatic.

In my opinion, a difficult problem can be effectively tackled by a team of two programmers. It is becoming less and less efficient to add more programmers to the team. Two will correct each other's errors on a reciprocal basis and the project will move ahead smoothly. With more people involved, more anxiety enters the picture. The individual programmer doesn't want to be lost in the crowd and becomes increasingly reluctant to take or give useful criticism. I once knew a programmer who had been hunting for a bug for several days. One day I stopped by his desk to talk about something else and, while waiting for his return, glanced at his program lying face up on his desk. I noticed a certain irregularity in one routine that didn't seem to look right, and on his return asked about it. A great light dawned on him. Yet, ever thereafter, when he saw me coming or he left his desk, he would carefully turn his program sheets face down.

P.L. 86-36

DOCID: 4009800

Another programmer, finally baffled, asked me to look for a bug. Being familiar with all kinds (must I admit, through having made them myself?), I quickly found in 5 minutes of search the places where arabic I had been punched instead of Roman I, which proved indeed to be her trouble. She was stunned that I found the errors so quickly, thanked me faintly, and never asked for my help again! So I think, in the education of programmers, egoless programming is the most important single thing to learn.

Returning to ABNER, it seems fitting to mention that in those days the engineers kept the machine working. The programmers were the operators. You had to know what all the buttons did, and take complete responsibility for loading and running your own program -- there was no one to do it for you.

The decision to move from Arlington Hall to Fort Meade was doom for ABNER. A one-of-a-kind machine, it was never intended to be moved and was not. At the Fort Meade site, the engineers worked on ABNER Model 2 which utilized quartz instead of mercury pools as a medium for the sound pulses. In a technical sense they were successful. Given perfect conditions, ABNER-2 would work. However, the quartz medium was sensitive to minuscule changes in temperature and humidity and was never as reliable as the pools of mercury in ABNER-1's tubes. Then too, advances in electronic technology made the whole concept of sound pulses and 48-microsecond cycles seem quaint and out of date, so ABNER-2 was dismantled and the ABNER concept passed into history.

The arrival of the IBM 701 computer at Arlington Hall, some time before the 1955 move to Fort Meade, brought us into contact with the first generation of commercial computer devices. Navy Lieutenant [redacted] (I hope he has since made admiral) became our outstanding expert on this device, which modern programmers would also consider impossibly quaint. The magnetic tapes did work, but they were not physically strong enough to hold up well. One program I wrote prepared a difference book for use in depth-readings, but it was about a 50-50 proposition as to whether or not the magnetic tape used would break before the run was completed.

A more provoking feature of the 701 for many programmers was the necessity of programming card input-output through the formation of a "card image" in the machine. For the 12 rows of a card to be read, it was necessary to program 12 pairs of Left Copy and Right Copy orders, given at specified time intervals, to copy the left and right halves of the 12 rows of a card into 24 computer words. The information then required an additional routine to convert the punches (binary 1) and blanks (binary 0) into characters or numbers. To output anything, a similar process was needed in reverse. [redacted] and I did a brisk business for a while preparing input/output routines for programmers who found the whole process discouraging. Of course, all programming was in machine language -- if Ø4 was the ADD order, you punched Ø4 and not ADD. No one had heard of FORTRAN as yet, and, as with ABNER, if you wanted to run your program, you became the operator in order to do so. P.L. 86-36

For all its primitive features, the 701 still represented a quantum jump in analytical capacity, and, as everyone knows by now, was followed by the 704, 709, 7090, and the latest 360 and 370 models, with all the associated software and a babel of "higher-level" languages such as FORTRAN, COBOL, ALGOL, PL/1, and the like. No future programmers will ever know what the early days were like. Yet something may still be gleaned from a glimpse of the pioneers and their problems.

~~(SECRET CCO)~~

From: *History of NSA General-Purpose Electronic Digital Computers*, by Samuel S. Snyder

~~SECRET~~

delay lines in the memory was always extremely critical, and the instruments used for measurement and regulation were inadequate. Also, the input-output equipment (IBM collator, Remington-Rand printer, electric typewriter, and Raytheon magnetic-tape drives) were often out of operation; and computation was ineffective or erroneous when input-output errors arose.

However, ABNER design and construction laid the foundation for many important later developments. ABNER was among the first computers in the country to operate successfully magnetic tapes simultaneously with internal computation. Its analytic instructions and other unique features made it extremely efficient for many cryptologic applications. Its Swish instruction was a model for planning DELLA, CICERO, and several other specially-designed equipments in the cryptologic arsenal and was a forerunner of the HARVEST Streaming units. Many programs made good use of the magnetic-tape capabilities, as well as the analytic instructions.

ABNER, Serial 1, cost approximately $600,000. It contained 1500 tubes and 25,000 diodes. ABNER, Serial 2, cost about $750,000.

(SCCO)

DOCID: 4009800

TELLING IT LIKE IT IS

A CRYPTOLOG Interview with Ramon A. Santiago-Ortiz, G612

Mary Ann Harrison tells us that you telephoned her recently to tell her how much you liked her article, "Why Are These People Smiling?", in the May 1977 CRYPTOLOG. She said that your remarks about the status of the Spanish native linguist at NSA deserve much broader dissemination. Would you be willing to share some of your views with CRYPTOLOG readers?

Certainly! The situation that I mentioned to Ms. Harrison has been building up for several years, and I feel that now might be a good time to bring it to the attention of people who might be able to improve it.

EO 1.4.(c)
P.L. 86-36

~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4009800

EO 1.4.(c)
P.L. 86-36

[redacted]

[redacted]

~~(SECRET - CCO)~~

Want to Play with a Pickfair Square?

The following letter appeared in the June 19, 1977 edition of Potomac Magazine (*The Washington Post*):

Cryptographic Challenge

Recent correspondence concerning the cryptogram inspires this letter. Your readers obviously work at it.

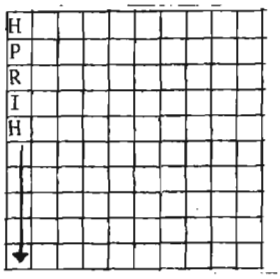
In gathering research for a book I am writing on Douglas Fairbanks and Mary Pickford, I came across a coded message sent to Douglas Fairbanks by his brother, Robert. The few cryptographers I know have been unable to solve it. Naturally, I'd love to know what it says. The word "Wycoff" may possibly appear; it was the brothers' code word for Sylvia, Lady Ashley, with whom Fairbanks was involved at the time. The message, dated June 23, 1933, follows:

HPRIHTOPRT
IERGAGUISN PRNSYCANOH
AIEACFYCHI URDOKWLTWH
ERGCGLIDUOUNIHIWNOYY
IPTNRAYENSYIPERE V (perhaps U) ANR (no spaces in this line—all run together)
WOFERAUITU CTIONS
ROBERT

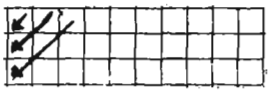
Booton Herndon,
Charlottesville, Virginia.

The next day our Cryptanalysis editor received the following solution from [redacted] G54: P.L. 86-36

Inscribe the first 100 letters in a 10x10 matrix in columns from left to right:



Then pull off letters diagonally, starting in upper left-hand corner:



Note that the questioned letter is actually a V, but there are two other garbles.

P.S. PICKFAIR in the message refers to the Hollywood estate of Mary *Pick*ford and Douglas *Fair*banks.

(UNCLASSIFIED)

DOCID: 4009800

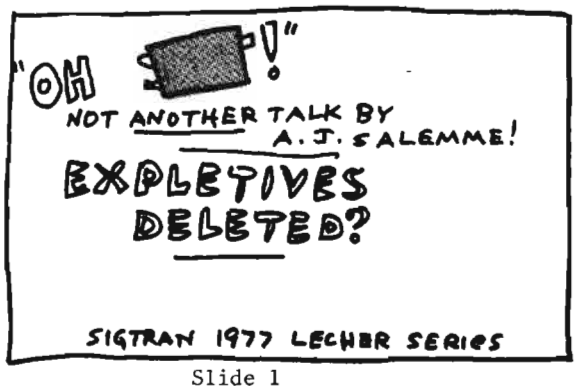
EXPLETIVES DELETED?
HOW TO HANDLE OBSCENITIES IN FOREIGN TEXT

A. J. S[redacted]e, P16

Edited version of a talk given in March 1977 for CLA's Special Interest Group on Translation

Explanatory note: The word bleep in the following text does not indicate that certain words were originally spoken but are now deemed to be unprintable. No! The words were never uttered! On each occurrence, a 30x40" posterboard with that word was held in front of the speaker's face. As for what he thought. . .

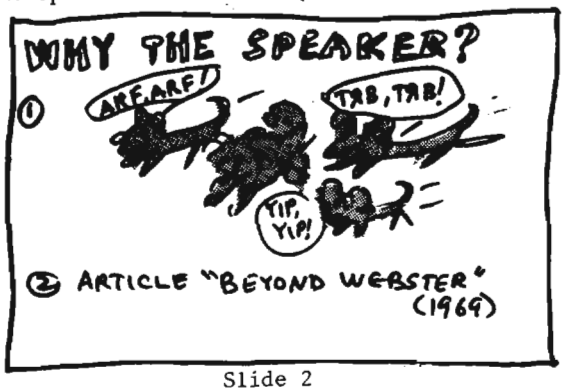
I'm completely aware that half of you people have looked at your watch and are wondering how long it will be before I actually come out and say bleep! so let's get it over with! (Slide 1).



Slide 1

Yes, SIGTRAN has another speaker. But the question might be, "Why the topic?" Well, this is the way the situation developed. The CLA lecture committee had another topic, and a speaker lined up, and the posters were all made up too. The lecture was called "The Flyaway Linguist." Well, he done flew away! When one of the members of the SIGTRAN lecture committee heard that, he said something like, well, "Oh bleep!" Someone else present said, "Say, that would be a good idea for a talk!"

And so, once they got the idea for the talk, the speaker was obvious (Slide 2), because,

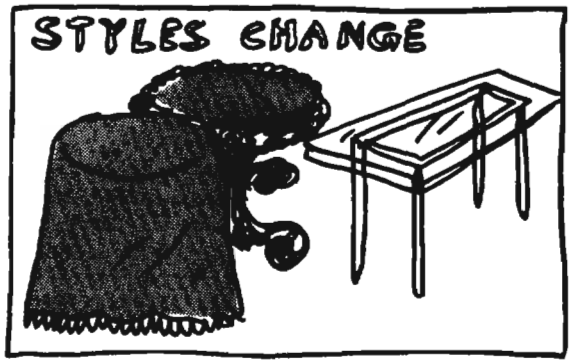


Slide 2

although I don't really have a reputation as bad as Typhoid Mary of the lecture series, if you see my name on a poster as the person who is going to be giving a lecture, you can be pretty sure that the *good* speaker, the one who's going to get paid a fee, who's actually prepared a *written* text and dry-runned it (dry-ran it?), has suddenly got sick or is out of the country and good old Art is like the guy with the trained dog act in the circus who waits for the aerialist to miss the net, whereupon the cry goes out, "Bring 'em out!" So here I am! In a way, I'm also like Ferdinand de Lesseps, the creator of the Panama Canal. You know the palindrome "A man, a plan, a canal -- Panama!" (It reads the same backwards.) I tried to work one out for me too, but the best I could do was "Emmelas -- ecneidua na, cipot a!" It doesn't read as well frontwards, but the idea is there.

I had another reason to be considered, because several years ago I wrote an article for what we could call a sister agency's publication. The article was on this very topic of -- well, some people call them "dirty words," but I call them "unconventional words." In fact, when I heard that the topic was chosen for the talk, I at first thought that Mrs. Kenny was going to give the talk, so I gave her a copy of that article, "Beyond Webster's and All That: Dictionaries of Unconventional Language," to help her out. But she said, "No, Art, *you're* going to give it!" So here I stand.

Before discussing obscenities in foreign languages (Slide 3), we have to know what obscenities are, what nasty language is. Perhaps



Slide 3

a definition of "obscenity" would be fitting here? Well, if the Supreme Court couldn't do it, I'd have to be a pretty dumb bleep! to think that *I* could! Instead, I'm going to say, "You know what an obscenity is. You know what blasphemy is." Because, surprisingly enough, the very words that we use and -- oops! did I say "we"? I mean "you"! The very words that *you* use have been in the English language for

DOCID: 4009800

many, many centuries. Since the words have been kicking around for so long, everyone knows them by now. But, as you know, styles change! And that includes styles in speech. People nowadays can come right out and say, loud and clear, words like [bleep!] And even print words like [bleep!] *People* can, not me! But, really, styles in language are similar to styles in anything. In clothing! The things I see on television, you wouldn't believe it! The things I see in furniture stores! Because you know that a table is a table. People have been making tables for hundreds of years. There's a basic concept for a table: it's a surface with legs on it. Now, if the Victorians wanted to clutter that all up with a lot of gingerbread carving and then cover the whole thing with a tablecloth, that didn't alter the fact that there really were legs under there. But the Victorians couldn't even *talk* about table legs. Because if they talked about table legs, that would make people think, "You must be thinking about human legs!" And if so. . . So the Victorians covered it up. With cloth. And their language covered it all up too. Well, we live different now. We live in the Age of Plastics, the Age of Glass. We don't want to cover the structure of what we're saying. So, if we feel like calling someone a dirty son of a -- oops! that was close! -- and then come out and say it. But a proviso, again -- *we* don't, *they* do!

There are many factors that influence the use of language. They include:

- *style,*
- *taboo and superstition,*
- *word magic,*
- *basic human meanness,*
- *etc.*

If Jackie O says, "Oh, stuff it!," then all her pals will say, "Oh, stuff it!" Just like the way that anyone who wanted to work with or for McNamara had to say "VEET Nam." If he said, "Vi-ET NAHM," he wouldn't have been "in." So language fashions come in and go out.

That applies too to nasty words. Especially since they are involved with word taboo and superstitition. You can't say certain things! You can't say, "Oh, isn't that a cute baby!" because then his hair will fall out. Or if you say that you hope that something nasty will happen to someone, it will really happen. Word magic is very strong. But nevertheless the words stay in the language. Because people are people. Basically, they're no damned good! I mean, *we're* no damned good! So the words have been around for a long time and we use them whenever we feel like it. My wife has been telling my kids for a lifetime, "Well, your father uses those words because he's got a poor vocabulary." On the contrary! I know just when I want to use them. Yes, people are mean. They can remember them for a long time and then use them appropriately. All of you who have kids, maybe, 2, 3, 4, or 5 years old -- you know that if you say one word once, in an odd moment, that kid will store it away and know exactly when to say it. It's when your mother-in-law is visiting. But why is what the kid says so nasty? It all depends on the society in which he lives. You've all heard about the family in a primitive society where the people wore no clothing whatsoever. The only adornment was the bone that married women wore through their nose. One day, seated around the campfire, the kid -- 12 or 13, say -- happened to notice anatomical differences. He tells Paw, "Hey, Paw, Maw don't have a . . ." So, Paw gave the kid the names of all the differences -- no problem! Then the kid said, "But, Paw, there's one thing I'm wondering about. What's that thing that Maw has through her nose?" Paw said, "Goddammit, kid, there are some things that decent people just don't talk about!"

Another example of a sociological aspect of language, and also of basic human meanness, is provided by last names. Most last names, in all languages, are based on the father's name, or the person's occupation, where he lives, how tall he is, etc. Smith, Kuznetsov, and Haddad are all the same name. Johnson, Ivanov, Johannson are the same. Little, Malenkov. . . Baker, Boulanger. . . But there are also, in all languages, names like Shitepoke. We know from history that, in societies where people didn't have last names, people's basic meanness came to the forefront when names were being assigned. Like in the Austro-Hungarian Empire in the time of Maria Theresa, when registry offices were set up to give every Jew a last name, like it or not. You could buy a good name, or, if not, well, your name might not be too appealing. H. L. Mencken mentions the story about the fellow who comes out of the registry office and tells his friend he was given the name "Schweisshund" (Bloodhound). "Why didn't you give him some money and get a good name?" "Are you kidding? It took every pfennig I had just to have him put the W in!"

And those of you who know Turkish know that the same situation prevailed in this very century, after Kemal Ataturk came to power. He said that people would have last names. "Live modern! Get a last name, just like the Europeans have!" And, once again, people got inferior names if they didn't come across with some money, or if they resisted the idea completely. Of course, in any country, then and now, it's possible to get court relief. In old Russia, if you didn't pay the registrar enough to get a good name, you could pay a judge 500 rubles and get it changed. If you got the name Durakov (son of a fool), you could get one letter changed -- Durasov. In old Russia they wouldn't let you change your name so drastically that it would seem that you were hiding from the authorities -- so, if your name were, say, Semizhopov, the best you could hope for was a reduction to, say, Pyatizhopov -- Seven-bottoms, changed to Five-bottoms. Russians really know

DOCID: 4009800

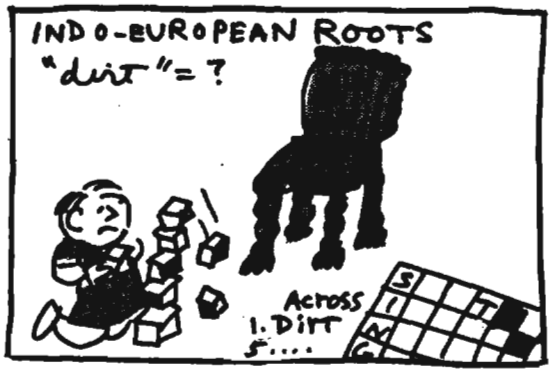
how to change their names. A Soviet pilot defected in Japan several years ago. He's got the name Rastvorov. He wants to disguise his name, so he changes it to Rastovorov! But that's Russians! Americans have a more sensible attitude toward names. Oh yeah? A few months ago, an American judge refused to allow a woman to change her name legally from Cooperman to Cooperperson (see CRYPTOLOG, December 1976). He ruled that, "It would have serious repercussions perhaps throughout the entire country."

In addition to being mean, people are ingenious when it comes to language. If you want to say something nasty, but are afraid to, for fear of getting your mouth washed out with soap, you can say things like, "Jumping Jehosephat!", "Dad nabbit!", "Goldernit!", "Gee dee it!", "Heck!", "Sherbet!", and so on. You can even see these things in print. You can see or say the letters S.O.B., although you can't come out and say the words they stand for. But people know that, when you say "Sherbet!" you're really not thinking sherbet. The wife of a former carpool member of mine grew up in the Texas Bible Belt. Whenever she said, "Heck!", she'd get a good slap across the mouth and her mother would say, "You *said* one thing but you *thought* the other!"

And don't try to fool people! If you say one thing and think another, your listeners will know it. Several years ago my wife and I went on a guided bus tour to Pennsylvania Dutch country. The guide -- Miss Priss we called her -- worn white gloves, to show she was a lady. But she had the dirtiest mind. She made all kinds of funny references to placenames in Pennsylvania Dutch country. When people would sort of snicker, she'd say, "What's so funny? I don't even know what you're *talking* about. Because I'm not that kind of girl." Well, I thought she *was* that kind of a girl, and the white gloves didn't change it. So if I hear people snickering in my audience, I know that you know what I'm talking about, even if I don't come out and say it.

So you can use words that *almost* say it. You can say "Sherbet!" and no one will mind. Or "Phenobarbitol!" You can trick kids sometimes, when they're just starting to pick up nasty language (from the kids in the street!), by saying, "Well, I don't mind what you say, but don't say the worst word there is! No, I'm not going to tell you what it is, or you'll say it! Well, okay, you've wormed it out of me -- it's 'Phenobarbitol!'" So you can trick a kid for maybe a week, to think that that is really the worst possible cuss word. But if you still want to say something nasty, but don't want to fake it by words that sound sort of like it, there's something else you can do. You can use fancy language. English is unusual in that it is a Germanic language, with lots of French vocabulary slapped onto it. Also we can use Latin or Greek when we want to sound extra fancy while saying everyday things. No doctor would say, "You have an infected toenail." That wouldn't be worth $55. He's got a fancier name for it, and you'd better make sure you use it on your hospitalization form!

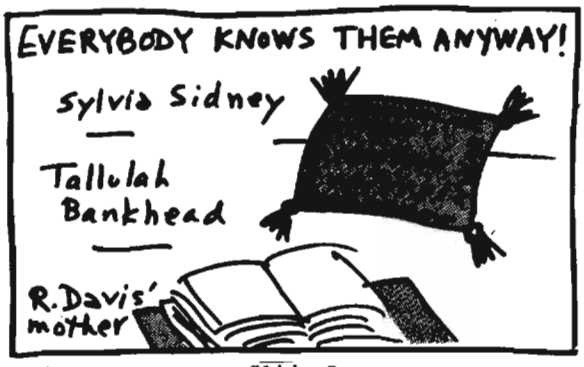
Thus, if you want to say something nasty, you don't have to use nasty Anglo-Saxon words. If a person does use those Anglo-Saxon words, you can say, "He uses scatological language." But is that any better than using the ordinary word? For, it dawned on me a while back, as a linguist, that the word "scatological" is the same as the Modern Greek word "skata," which means -- well, I don't really know how to explain it, except by saying that there are several word pairs in English in which an initial *sh* and *sk* are derived from the same word. For example, the word "skirt" and "shirt" are both derived from the same older word. So look up the word "scatological" in the dictionary, and you might be surprised at its etymology.



Slide 4

Yes, Indo-European roots can reveal a lot! For example, there I was, several years ago, when Peter was only 3 years old and all our friends were saying that he had a speech impediment. Well, he didn't and he doesn't. And so I was rather pleased when he would try to build blocks and, when they fell down, he would say, "Oh, drit!" I'd think, "Good, he can't say it like Dad does!" But then again, years after Peter was grown, it dawned on me. "My God, 'drit' is a metathesis of 'dirt'! I wonder if . . ." Sure enough! It was! And if you go to the dictionary and look up the English word "dirt," you'll be amazed at what it really means. Not only that, but it's same word as the German "Dreck." (As in the inexpensive furniture that furniture salesmen try to push -- furniture which is "Dreck from the factory," to use the Yiddish in-joke.) Yes, "dirt" means bleep! Of course, it's not the only meaning. As the nun in the story learned. The nun, seated in the airplane, doing a crossword puzzle, who asked her companion, "What's a four-letter word meaning 'dirt'?" He answered, "Silt." "Oh dear," she said, "do you have an eraser?"

So what's the fuss? Everyone seems to know the words anyway. Even women! Those soft, cuddly -- no, I shouldn't use sexist terms! -- those *rough, uncuddly* creatures know them. Take, for example, Sylvia Sidney's needlepoint book (Slide 5). You cuddly or uncuddly females can ask yourself, "What's he doing,



Slide 5

reading a needlepoint book?" But I'm going to stay with the example. In that book she has a full-color photograph of a cushion she embroidered for a friend in show biz. It says, "O LORD, give me a BASTARD with TALENT." Why not? Bastard's a word. And Tallulah Bankhead, when she was introduced to Norman Mailer! You recall that in *The Naked and the Dead* Mailer used a commonly used Army word repeatedly, but he spelled it differently -- he put a final *g* on it, instead of the original *ck*. That caused quite a ruckus in the publishing business then. Imagine, using the actual word (sort of), instead of using a dash! So when Tallulah Bankhead was introduced to Mailer at a party, she said, "Oh yes, you're the young man who doesn't know how to spell **bleep!**

Or maybe everybody doesn't know them? [redacted] who used to work here, came from a very cultivated family in San Francisco. Royola once said that, when she or her sister would bring home a new word that they had heard someone use at school, her mother wouldn't say, "That's a nasty word!" Instead, she would say, "Let's look it up in the dictionary and see what it means. Let's see, how do you spell it? F? Then what? Why, it's not even in the dictionary. So I guess it's not a word! Why would anyone want to say words that don't exist?" Well, it was a pretty good trick, but it won't work with current dictionaries.

Thus, we can use various combinations and permutations of trickery to refer to nasty words without actually saying them. We can use phonetic "close ones" ("Fudge!") or fancy terms derived from Latin or Greek ("Coprocephalus"), etc. But if we want to be stylishly deceptive, we can use foreign terms. The problem is that, if we say "Merde!" often enough, our listeners might get the idea that it's a nasty French word, and then we have to disguise *it*. But that's no problem. We can say, "Mer-r-r d'Azov" (that's "Sea of Azov" in French). Or "Mer-r-r Daly of Chicago!" Or even do what the French do -- refer to it as "le mot de Cambronne." Because French General Cambronne was famous for saying it, so it has become "Cambronne's word." Just as "Nuts!" is General McAuliffe's word. Or, rather, just as it ain't! Because, even though much has been written about how McAuliffe told the Germans "Nuts!" when they asked him to capitulate at Bastogne, he didn't really say that. I can see the poor general up there in heaven now, strumming his harp, saying, "Gee dee it! I didn't *say* it!" No, he really didn't say it. He said something else that was *sort of* similar, but a bit more army-ish. To make the story more acceptable to the news services and the delicate readers Stateside, his original five-letter rejoinder was replaced by "Nuts!" (was this the first and only time that a four-letter word was put *in* to clean up the text?).

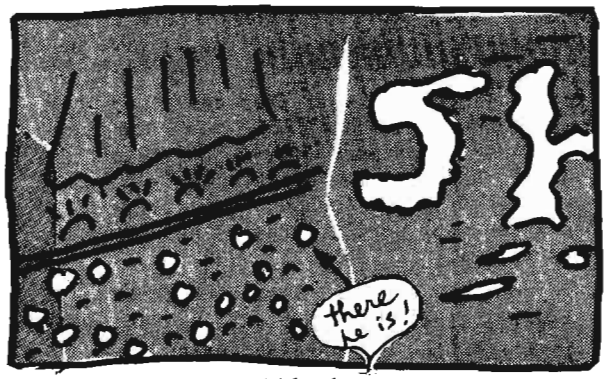
And there are even more ways of concealing what you want to say. You can use a secret language -- in your own family or in your own crowd. Take, for example, Cockney rhyming slang. "Me and the trouble and strife" means "me and the wife." And who are the "God-forbids"? -- why, the kids! After a while, though, everyone else learns the secret language, so you have to introduce refinements. With Cockney rhyming slang, the refinement was to drop the last element -- the rhyming word. So, nowadays, "Run up the apples!" means "Run upstairs!" (it rhymes with "apples [and pears]"). "It's in 'is titfer!" means "It's in 'is 'at!" (rhymes with "titfer [tat]"). All right, then, why is the Bronx cheer ("le mot d'Archie Bunker") defined in *Webster's Third* as "raspberry 3"? And what does the third definition of "raspberry" ("A sound of contempt or derision made by trilling the extended tongue between the protruded lips") have in common with raspberries? *Webster's Third* doesn't say. *Webster's Second* is no help, either -- it only says "[orig. E. slang]." Well, to understand the origin of the expression that so many people use innocently, you have to know Cockney rhyming slang and figure out what rhymes with "raspberry tart."

You can hide meanings in music, too. Often, when people say that the words of a song don't make sense, that they're just "nonsense," that's

P.L. 86-36

when they have a meaning! The songs of the 1930s and 1940s that used to mean "nothing" to us now sound different -- "Want some seafood, Mama!" Seafood! . . Or just listen to "La Cucuracha" -- they've changed the lines in it. What happened to the line "Porque no tiene, porque lo falta marijuana que fumar"? When people find out the secret meanings, the words change. My youngest girl, Mary, plays a song over and over, "Shake your booty!" As many times as she plays it, I cannot actually *hear* the word "booty" -- it sounds like "Shake your trooby!", "Shake your snooty!" "Shake your dooby!" But that's understandable, because language researchers have proven that if the same statement is repeated over and over, the human ear will hear it differently each time. Especially if it is a "nonsense word." But, in real life, "Shake your booty!" does have a meaning, and I'm not going to say what it is. Except to say that once, on television, they had several girls lined up. They asked them, in turn, "Would you shake your booty?" They all answered, "Sure!" Until they got to the black girl. "I ain't gonna shake *my* booty!" (Good for her!)

Until recent years, there have been infrequent instances when nasty words came up in print. (Even medical textbooks would explain things in Latin, rather than come out and call a [bleep] a [bleep!]) Years ago, when H. Allen Smith was writing funny books, he wrote in one of them that his secret desire was to arrange the seating plan on the floor of the Metropolitan Opera on opening night. And he would arrange the bald heads in such a way that they would spell out "a four-letter word, and the dot over the I would be Nicholas Murray Butler," the President of Columbia University at the time (Slide 6).



Slide 6

I've also been told of a book by Philip Wylie, called *The Disappearance*. According to my informant -- I haven't been able to find a copy of the book yet -- God gets dissatisfied with the human race. So He decides to do something about it. To show His displeasure, he has the clouds form the letter S. That catches people's attention. Then they form the letter H. By the time the clouds start to form the letter I, people start to think that it must be some practical joker with a plane up there. But, no, there isn't any plane! So they realize that it is a sign of God's displeasure. He also writes the appropriate word, in Russian, in Cyrillic letters, over Russia, but it doesn't cause any ruckus. Not until He says something about the leadership! How typical! But the question is, Would God talk that way? Well, in my capacity as CRYPTOLOG editor -- forgive the plug -- I recently edited an article that will appear in a future issue. In the article, God created things like a communications terminal, a link, and so on. Then He went on vacation, leaving everything in Control's hands. When He came came back and say how Control had mixed everything up, He said, "What the devil happened?" And Control answered, "That's just it! The devil made me do it!" When the proof sheets (with the "d" in devil duly lower-cased!) were shown to a few people to see if there were any objections, one person wrote, "I object to this strongly. God wouldn't talk this way." I don't know how he knows that. As for me, I do believe that even God can look words up the *Webster's Third*, and might use any of them in the proper context.

Nasty Words at NSA

And so, finally, we come to the real topic of this talk -- nasty words at NSA and how to handle them. If you, as linguists, want to read all the literature on the subject, you won't have much to read. There's that article that I wrote back in 1969. It was submitted to an Agency publication at that time (there was only one), and it was deemed to be unsuitable. So I sent it to the editor of a publication at a sister Agency. Over there in Langley? And they published it. They realized that the article had a point -- "Linguists have to *know* all the nasty words in their foreign language, and should not be embarrassed to ask what any word really means in English." Linguists have the right to know all the words in electronic engineering, don't they? So why not nasty words, too? If two people are talking to one another in a foreign language and one belts the other in the mouth, why did he do it? What did the other guy call him? Come on, now, don't be coy or cute! Tell me, if you know. Did he call him a "son of a camel-driver"? "No, it was worse than that." Well, what was it? "I don't wanna tell you." The article explains why and how the linguist should insist on finding out what everything means in the language he specializes in, even the "unconventional" words.

When [redacted] was at Detachment R, he wrote a dissertation on Russian "taboo" words. Most of the students at Detachment R wrote dissertations like "The Soviet Police System" or "The Role of the Messkit Repair Battalion in the Tactical Situation." So, when Larry said

P.L. 86-36

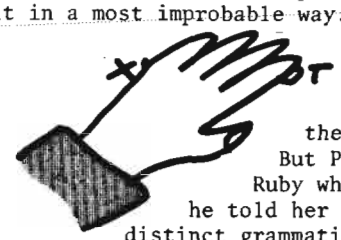
that he wanted to compile a dictionary of "taboo" words, he had a heck of a time getting that dissertation approved. Finally it was approved, with the understanding that the complete printing run would be five (count 'em, five) copies, and Larry would do his own typing of the multilith stencils (we wouldn't want our typists to *see*, much less type, those words, would we?). Larry then went around to the Russian instructors and pumped them for information. They all said the same thing, "I personally have never used these words, but I have heard other people saying them." Larry got all of them, in poems, in songs, in expressions, and, of all things, he gave the English translations of them! That made the dissertation a very unusual dictionary. In fact, about 2 years ago, our librarian said, "Hey, here's a mention in a bookseller's list of a dictionary of Russian obscenities. It was published in Cambridge and it costs $10.00. Should we buy it?" So we bought it. And it turned out to be a pirated edition of Larry's dissertation, with his front page torn off. Someone else had apparently felt that it deserved a bigger printing run.

[redacted] also wrote something for CRYPTOLOG on Soviet prison slang. But, for the most part, if you work in foreign languages at NSA, you won't have any "literature" to read. All you will have -- if you're lucky -- is a list of nasty words in the appropriate language, but without their definitions. It's like telling you, "Here's a list of words that you're not supposed to translate, and you're not even supposed to know why!" As you will see, this really isn't the best way to handle the situation.

Just as English dictionaries have not always listed the nasty words, foreign-language dictionaries produced by the various national lexicographical groups have not always contained those words in the foreign language. Lately, again as in English, the situation has been changing. The Chinese, for example, have been including in their dictionaries, together with English translations, words which previously would have been considered to be unprintable. But dictionaries are not always helpful. The Russian dictionaries that do list "yolki-palki" (which means "Christmas trees and sticks") sometimes limit their definition to the old standby, "Indecent expression not used in polite society." Why don't they come out and say, "Don't use it because the first syllable sounds as though you were going to say something else"?

Since dictionaries used to hedge like that, the Agency's linguists had to muddle through any way that they could. [redacted] many years ago, prepared a list of Russian words which, if they showed up in the language material, indicated that we weren't really interested in it. Since [redacted] had a professorial turn of mind, he thought it might be nice to give the English meanings. No, it was pointed out to him at the time, people didn't have to know what the expressions meant -- all they had to know was that the material wasn't worth looking at. At that time, several people working in that area formulated Rule No. 1 when dealing with Russian text: If you have an expression that you cannot find out the meaning of, and one of the words in it begins with a Cyrillic X, stop trying to find out! It's probably indecent!

That rule should have been kept in mind several years ago when Charlie Pritchard was one of the Russian linguists channeling work to [redacted]. Once he showed her something he had, but he kept his hand over something else. "What are you covering?" she asked. Well, it was a four-word expression in Russian, and one of the words began with an X. (Now, you know that it must have been nasty!) She insisted she had to see what it said, and he insisted that he couldn't show her. To make a long (and classified) story short (and unclassified), when he finally removed his hand, she said, "But that makes sense!" And then proceeded to translate it in a most improbable way. Its real meaning P.L. 86-36



can be given here as "bleep my bleep!" or "verb my noun!", and the verb isn't "kiss." But Pritch couldn't tell Ruby what it meant. Instead he told her the five separate and distinct grammatical reasons why it did not mean what she said it did. She *still* was unconvinced, and he left fuming. When he returned to his desk and told others what had happened, someone suggested, "Well, Pritch, why didn't you tell her what it means?" "No," he said, "it wouldn't have done any good. She would have said, 'Pritch, I asked you a civil question -- the least you could do is give me a civil answer!'"

Can NSA linguists learn from newspapers how to handle obscene expressions? Maybe and maybe not. Because even the same newspaper can't decide how to handle them consistently. Here are a few quotes from *The Washington Post*, just within a two-week period. Dashes and hyphens are as in text."

- "a commonly heard 12-letter epithet";
- "'You m--- f---, you better open the door, or we'll blow your brains out'";
- "'Damn' cost 5 cents. 'Hell' - 10 cents. 'Goddam' was 25. What if I said, '——.' 'That's free'";
- "[Joan Jett,] the band's rhythm guitarist, said, 'We'll give him a raft of s--- as soon as he walks in the door!'";
- [Richard Pryor to tennis opponent Sander Vanocur:] "'I'm gonna whip your a—!'"

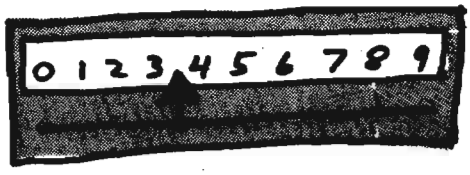
There are a lot of questions to ask here. Such as, if the epithet is that "commonly

heard," why not *print* the mother? And, what is M-plus-three-dashes F-plus-three dashes supposed to mean? -- is it the same as the "commonly heard epithet"? And exactly what word can Robert Mitchum say for free, without putting money in Loretta Young's swear box? In this inflationary age, I'd like to know what I can get for free -- why not tell me? And Richard Pryor's expression -- is "a—" really such a bad word?

Well, maybe it is, because the same *Washington Post* printed, the same week, an article about an FCC ruling concerning "seven commonly-used epithets which range from three letters to 12." But the article didn't list them. So, minutes before I started my talk here, Dave Williams asked me if I could think of any nasty three-letter words. "Yeah, one is A-dash-dash." "Oh, that's not so bad!" "Well, then, how about **bleep!**

What if there aren't enough clues? In our business we tend to measure things, count letters, see how long dashes are, count the dots. What good does it do if we read "m——f————"? ("First dash is too short, second dash is too long!") Or "m---f---"? ("Not enough letters!") Or "you ————————!" ("Is the word really that long, or is it a phrase?").

So, if you have trouble figuring out the nasty words in your own language when not enough clues are given, what do you think it is like when you're dealing with foreign languages? When someone uses an expression that is defined in the foreign dictionary as "An improper expression" and you have no idea why? Or what about when you *do* know what it means, but are advised to treat it in your translation as "[Obscenity]"? What good does that do your reader? It has been suggested that, when it is impossible to give the actual translation of a foreign nasty word, it might be nice to have something like a Richter scale of improper words -- ranging from 1 ("Convivial chuckle") to 9 ("Punch in the mouth"). Perhaps we could call it the Schichter scale? Then, in a translation, instead of saying "[Obscenity]", we could say, "Speaking in Polish [or whatever], he called his conversational partner a Schichter-4." Well, that gives the reader some idea -- at least it wasn't a 9! I realize that any scale won't work all the time. For example, among friends, or in a John Wayne movie, "you cross-eyed sonnovabitch!" might be only a Schichter-1 (if that high), but elsewhere?



In the absence of any hard-and-fast scale, why don't I just give you my own word of advice? From one practicing linguist to another. First,

- UNDERSTAND. Insist on your right, as a linguist, to know every word in your language of specialization. Insist on the need and the right to buy "dirty dictionaries." Don't be embarrassed at the words in them. Everybody knows what a ———— does for a living! Don't guess at the meanings! Did the guy in Arabic say that the other guy was a "dirty son of a camel driver" or did he say that he was doing something to or with a camel? Remember, don't be embarrassed! *You* didn't say it, *he* said it!

Then, having understood what it says, you'll have to

- DECIDE ON THE TREATMENT. You might have to ask your boss for guidance on this. Some bosses don't like to see words like ———— in print. I myself feel funny about saying words like ———— into this mike. So you will have to decide which of the following you want to do:
  - Hem and haw. The traditional treatment, "beating around the bush." Paraphrase. Use "nice words." Don't give the reader any idea what the words meant.
  - Be a tease. Give a minimum amount of clues. Maybe the correct first letter, but a misleading number of dashes. As in, "Everybody knows what a c---- does for a living."
  - Use the correct number of dashes, and hope that your reader gets the idea. "That dirty c---------!" (If the reader gets the idea, that's okay. If he doesn't, he can ask around.)
  - Come right out and say it! If he called the other guy a ————, he called him a ————! So put it down that way! That's what they do in court. The judge tells the witness to say exactly the words that the defendant said, and the court stenographer puts them into the record. They're only words!

Why, then, when giving my "word of advice," did I use the traditional method of handling these words -- hypocrisy? Why, when telling *you* to "come right out and say it," did I use a long dash and not "come out and say it" myself? Was it because "c---------" isn't in *Webster's Third?* Because you can say, or imply, certain words but feel inhibited about seeing them in print? Why, as I try to explain away my hypocrisy, do I have a mental image of Wallace Beery, completely flustered, saying, "Aw-w-w-w, shucks!" I can tell you, and tell myself, not to be embarrassed. That we didn't invent the word. That it has been around for at least 500 years. That everyone knows it anyway. But, aw-w-w-w, shucks!

DOCID: 4009800

WHAT ARE THEY UP TO, ANYWAY?

P.L. 86-36

CAA News by [redacted] P14

It may be the only secret open meeting in the building. Certainly it's the only one I know of. The CAA Board meeting, that is. How can it be secret and open too? Well, sometime ago, the CAA Board decided to open up its meetings to the public and let a little sunshine in. That's the open part. But, since we started this policy, nobody else comes to the meetings to see what we do, or to tell us what we ought to do. That's the secret part. Obviously, the word hasn't gotten around about what wild things happen at CAA Board meetings.

Seriously, though, folks, you are invited to come along and voice your opinions about what the CAA should be doing, what special interest groups ought to be formed, etc. All right, you say, where and when is the next meeting? Funny you should ask, because, as I write this (early June), I don't really know! We usually hire one of the conference rooms on the second or third floor, and the room will vary according to what is available. (Say, maybe that's why nobody comes -- they can't find us!) If you want to know where the next meeting will be held, you can always ask one of the officers. Or, better yet, join CAA and get your very own announcement mailed directly to you. If you're shy, just watch the announcements on the CLO bulletin boards (there are four of them, one in each building).

Maybe our strategy is all wrong. Maybe we should see how long we can keep our string of unattended meetings unbroken. We could have monthly changing times and rooms. Maybe offer a challenge cup to whoever solves our rota and actually shows up at our meeting place. It's a thought. . .

Upcoming CAA events

AUGUST

The opening day ribbon has been cut, all the festivities have died down, and the brand-new remoted system is now operational. The guy who used to give those fancy speeches about what the system was *going* to do has moved on to some other project. What happens now? What is it really like to live with a remoted system day by day? What are the real-life problems that will now be encountered by the people who are responsible for making the system work on a daily, operational basis? Will Mary leave George? Will Fido survive surgery? These and other questions will be discussed when Whitney Reed and B5 give us an inside look at "Life With a Remoted System."

SEPTEMBER

The whole subject of NSA initiatives on support to combat operations, both in Europe and in the Pacific, is scheduled to be explored by [redacted] of V4.

Check your nearest CLO bulletin board for exact dates, places, and times. CAA members will receive notification by mail.

Communications Analysis Association
Board:
President: [redacted]
President-Elect: David Gaddy, 3247s
Treasurer: Timothy Murphy, 3791s
Secretary:
Board members: [redacted]

P.L. 86-36

Letters to the Editor

P.L. 86-36

To the Editor, CRYPTOLOG:

I am writing to congratulate you on an absolutely smashing article in CRYPTOLOG, I refer to "The Polyhedral War," by [redacted] (illustrated by [redacted]. Please pass my "well done" to both of them.

I recognized immediately an old friend in the pentagonal dodecahedron which the author calls a "pitiful polyhedron." The model is a delightful toy and I have spent many enjoyable hours flexing the many dodecahedra made for me and my friends.

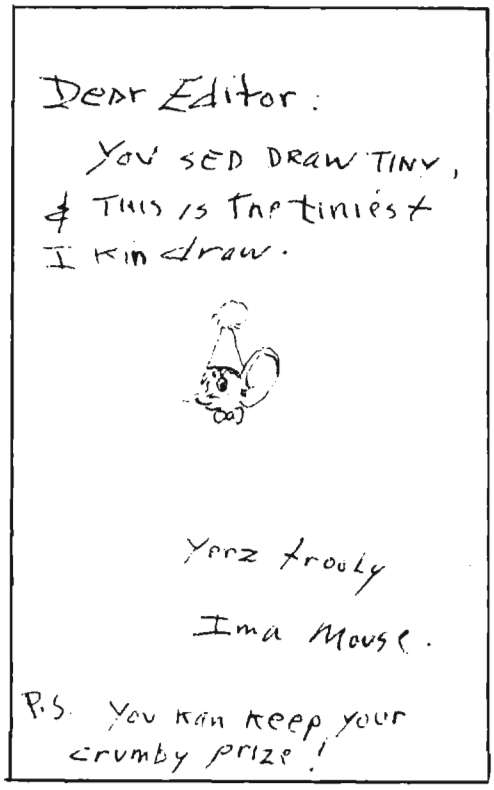
One question: What do the *other* models do?

Derek Weeson

Editor's reply:

Now I know how Ann Landers feels when she has to decide whether she has a real letter or one from "the boys at Yale." Assuming that this is legitimate (big assumption: they haven't used those envelopes in *years*), thank you for your kind remarks. In reply to your question: they do pretty much what the rest of us do -- occupy space.

(U)



Editor's reply:

Your note puts us in rather a quandary. Your entry is *not only* the best one we received this month. It's the only one! In any event, we are required to carry out the terms of our offer and award you a CRYPTOLOG subscription (the "crumby prize" you refer to). Trouble is, we can't find your name in Locator's files. The last Mouse family we knew worked in the sixth wing of B Building at Arlington Hall more than 20 years ago (they used to love those cheese-and-peanut-butter crackers Norman K. would leave in his desk among his galoshes and not quite empty Coke bottles. Any kin?

(U)

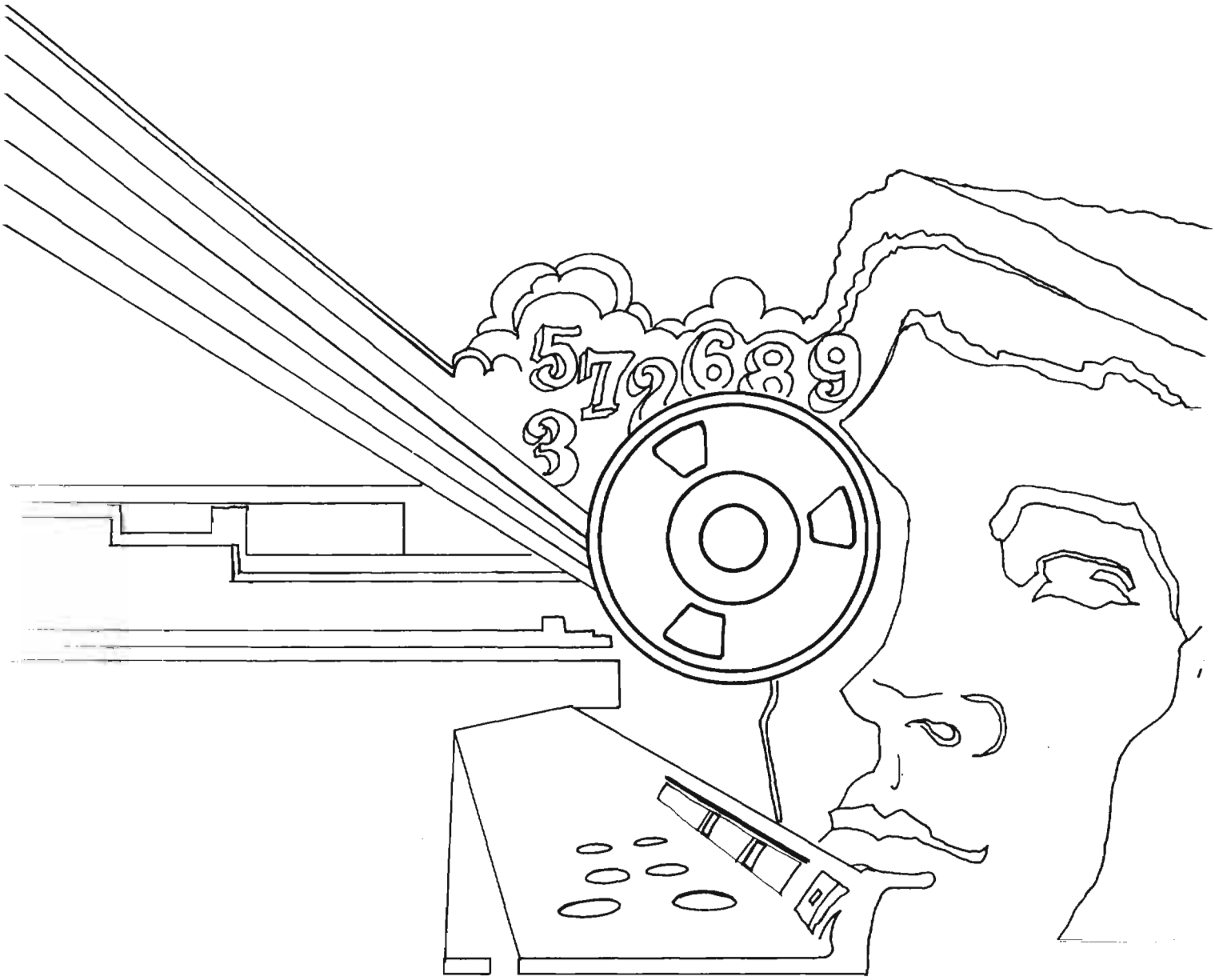
Solution to "Match Them Up!", by Tony Melzer (CRYPTOLOG, June 1977)

1-f	Amin-Uganda
2-d	Asad-Syria
3-T	Bhutto-Pakistan
4-B	Boumediene-Algeria
5-H	Castro-Cuba
6-A	Daoud-Afghanistan
7-L	Desai-India
8-Y	Fahd-Saudi Arabia
9-O	Fukuda-Japan
10-G	Geisel-Brazil
11-K	Giscard-France
12-S	Hassan-Morocco
13-N	Houphouet-Boigny--Ivory Coast
14-R	Lopez Portillo-Mexico
15-V	Marcos-Philippines
16-J	Mengistu-Ethiopia
17-g	Mobutu-Zaire
18-U	Morales Burmudez-Peru
19-C	Neto-Angola
20-c	Numayri-Sudan
21-e	Nyerere-Tanzania
22-P	Qadhafi-Libya
23-M	Rabin-Israel
24-Q	Ramgoolam-Mauritius
25-I	Sadat-Egypt
26-a	Senghor-Somali
27-Z	Siad-Senegal
28-W	Soares-Portugal
29-b	Suarez-Spain
30-X	Smith-Rhodesia
31-F	Tindemans-Belgium
32-D	Videla-Argentina
33-E	Zia Urrahman-Bangladesh

(U)

P1-JUN 77-S3-25371

~~TOP SECRET~~



DOCID: 4009798

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JULY 1977

EO 1.4.(c)
P.L. 86-36

TEACHING THE TRANSCRIPTION SKILL.... [redacted] 1
CHANGES IN MAKEUP OF EDITORIAL BOARD.....6
TOOL LANGUAGES.....John D. Murphy.....7
ZBB? WHAT IN THE WORLD IS THAT?..... [redacted] 10
[redacted] ...Stuart H. Buck.....11
WHICH TAPE HAS THE INTELLIGENCE?.....J. Gurin.....19
DATING GAME.....David H. Williams.....21
NSA-CROSTIC NO. 8.....A.J.S.....22
CLASSIFICATION CORNER..... [redacted] 24
WHAT EVER HAPPENED TO THE C.A.A.?... [redacted] 25
LETTERS TO THE EDITOR.....26
MATCH THEM UP!..... [redacted] 28

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009798

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. IV, NO. 7 JULY 1977

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5236s)

Collection..... [redacted] (8955s) P.L. 86-36

Cryptanalysis..... [redacted] (4902s)

Language..... [redacted] (5236s)

Machine Support..... [redacted] 5303s)

Mathematics.....Reed Dawson (3957s)

Special Research.....Vera Filby (7119s)

Traffic Analysis..... [redacted] (4477s)

Production Manager.....Harry Goff (4998s)

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4009798

THE TRANSCRIPTION SKILL: CONCEPTS AND TEACHING METHODOLOGIES

P.L. 86-36

ACKNOWLEDGEMENTS

The author owes a great deal to her students for their suggestions, which have helped to improve the quality of the transcription course and which have made the classroom activities more effective.

She also wishes to express her gratitude to her many colleagues for their cooperation in answering the questionnaires which provided much of the foundation of the paper, to [redacted] *for their valuable suggestions, and to her supervisor, Harvey Hoffman, for his encouragement and support.*

A special debt of gratitude is owed to [redacted] *for his thoughtful assistance, in both the development and preparation of this manuscript.*

N. B.

The National Cryptologic School (NCS) is currently offering many transcription courses to develop students' ability to listen to recorded tapes and transcribe them. Since the transcription skill is not one of the so-called four skills involved in foreign-language learning (listening, speaking, reading, writing), it appears that no academic institutions have offered courses specifically to develop this skill. Moreover, little research has been done on this subject. Consequently, teachers at NCS are individually experimenting with various methodologies to teach the transcription skill. For these reasons, there is a need to clarify and establish a definition for the skill of transcription, identify the relationship between the skill and the other four skills, describe the level of the transcription skill which the students should attain, and develop an effective methodology to use in teaching the transcription skill.

Problems of Transcription

Transcription involves hearing the sounds and sound patterns of a language, understanding their meanings, and representing the sounds in the written symbols of the language, inferring unheard or inaudible sounds and words. Understanding the meaning of sets or combinations of sounds is absolutely necessary, especially for those languages such as English, French, or Chinese, for which the graphemic representation (the writing system) generally does not correspond to the phonemic structure (the sound system) of the language. For example, the underlined spellings in the words *shot, schist, session, efficiency, cautious* all represent the same sound (all of which can be represented by the IPA symbol [ʃ]). Cases such as this illustrate that English cannot be transcribed without knowledge of the meaning of the sets of sounds of the language.

Even for those languages whose writing systems are largely phonemic, such as Turkish, Spanish, Japanese, or Korean, understanding of the meaning is indispensable to obtain a correct transcription for several reasons. Firstly, any

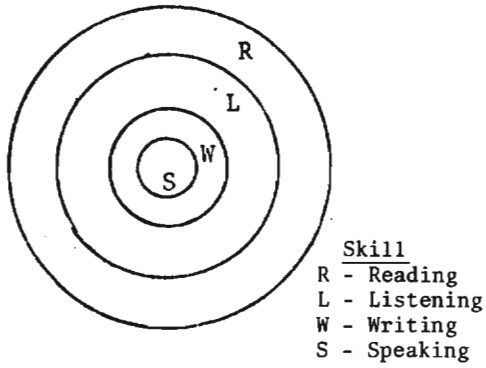
unit of speech sound is articulated differently depending upon its environment. That is, the place and manner of articulation of a consonant will change according to the vowels which accompany it[1]. Secondly, when sounds are articulated in rapid speech or casually, an assimilative tendency[2] to reduce the differences between sounds takes place, and the sounds that a person does utter are the result of a compromise between the assimilative tendency and the minimum differentiation necessary to make himself understood. Thirdly, pronunciation in the spoken form of the language varies, depending upon the social level of the speaker, some group membership, or a personal idiosyncrasy[3]. These allophonic variations are phonetic and do not necessarily signify any change in meaning. However, what seems to be a very small phonetic difference in one's own language may signal a distinct difference in meaning in some other language.

In addition to allophonic difficulties, the listener may not hear clearly everything that is said. This is true even in one's native language. The native speaker, however, can piece together the information from what he does hear because of redundancy[4] in the language and the probabilities of occurrence of certain sequences of sounds. Knowledge of redundancy and probabilities of occurrences of certain linguistic elements built up through experience in the language makes it possible to guess correctly the words that are missing or inaudible. Redundancy in languages is to be found in elements of sound and in morphological and syntactical formations which reinforce each other in the conveying of meaning. The English language, for example, is 50 percent redundant[5]. Without comprehending the meaning, a person cannot take advantage of this redundancy and, consequently, cannot infer missing words.

Relative Skill Ranges

We have found that a significant portion of the transcription skill rests upon the ability to infer missing phonological, morphological, syntactical, and semantic elements as well as to hear the sound patterns of a language and understand and translate the sounds into written symbols. With this in mind we can discuss the relationship of the transcription skill to the other four language skills and analyze the transcription skill range which students should achieve.

When an adult is studying a foreign language, his ideal goal is to achieve the skill range of an educated adult who is native to the language. The relative skill range of an educated native adult may be illustrated as follows:



Relative Skill Ranges of Educated Native Adult

As the diagram suggests, the ranges of reading and listening skills are generally broader than those of writing or speaking. The educated native speaker will be able to recognize and comprehend visually more of the grammatical, lexical, and semantic system of the language than he can recognize and comprehend aurally. Listening requires him to comprehend immediately without deliberation what he has heard. Reading, in contrast, allows for more time to analyze and analogize unfamiliar elements.

Writing requires a more complete and active control of the elements of the language than listening comprehension, and therefore the range of the writing skill of the educated native adult is more limited than the range of listening skill. His writing skill, a productive skill, never surpasses his receptive listening skill ability[6].

The speaking skill, a productive skill, is the most complex skill[7] and therefore is the most limited skill of the educated native adult. Speech requires almost instantaneous interaction between formulations of statements, questions, and replies, while writing is a much slower process which allows more time to deliberate and search for words and forms. Speaking involves thinking of what is to be said while saying what has been thought. Words must be formulated at a rapid rate, with a spacing of about five to ten words ahead of the utterance. In addition, words and patterns must be chosen to fit the right situation or attitude intended.

---

[1]Bertil Malmberg, *Phonetics* (New York: Dover Publications, Inc., 1963), p. 58.

[2]*Ibid.*

[3]Wilga M. Rivers, *Teaching Foreign-Language Skills* (Chicago: The University of Chicago Press, 1968), p. 115.

[4]Claude E. Shannon and Warren Weaver, *The Mathematical Theory of Communication* (Urbana: University of Illinois Press, 1959), p. 104

[5]*Ibid.*

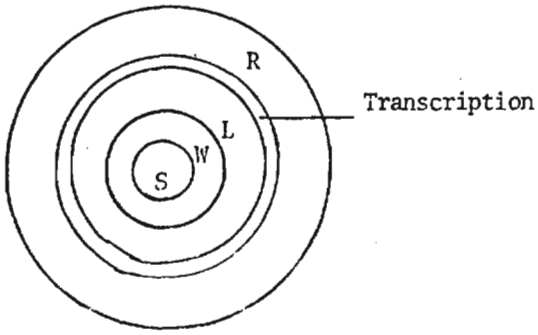
[6]Kenneth Chastain, *The Development of Modern Language Skills: Theory to Practice* (Chicago: Rand McNally and Co., 1971), p. 164.

[7]William Francis Mackey, *Language Teaching* (Bloomington: Indiana University Press, 1967), p. 263.

DOCID: 4009798

This discussion indicates that the native adult can listen to and understand, and read and understand, more vocabulary and structure than he can speak, and he can demonstrate a greater command of the language in writing than he can in speech. The range of the four language skills of an educated native adult may also correspond to the order of difficulty in acquiring these skills. The speaking skill is the most limited skill of all because it is the most difficult skill to acquire, and the reading skill is the broadest skill of all because it is the easiest one to acquire.

Considering the features and the relationships of the four skills in an educated native speaker, and the features of the transcription skill defined above, the transcription skill may be illustrated in the following diagram in terms of the ranges of skills of an educated native adult and in terms of difficulty of acquisition.



Relative Range of Transcription Skill in Terms of the Four Language Skills of the Native Adult

This diagram suggests that transcription is perhaps easier than listening comprehension. Listening requires retention of information from an ongoing series of sounds and immediate or unconscious comprehension of what has been heard. Transcription does not require that information be retained, nor must comprehension of sounds be immediate and unconscious. In fact, it is sometimes possible to recognize words and write down the words without comprehending their meanings. Transcription is more difficult than reading comprehension, however, because transcription involves recognition of sounds, comprehension of their meanings, and recognition of the words to be copied in the writing system of the languge, and inferring of necessary missing elements. Reading, on the other hand, involves only recognition of written symbols and comprehension of their meaning. We suggest, however, that the listening comprehension skill, which is defined as a receptive skill by most language teachers and scholars, as well as the transcription still, is not a purely receptive skill, but a combination of both receptive and productive skills. The listener always anticipates and predicts certain sequences of sounds with high probabilities of occurrence, and through his knowledge of the language and the factors of redundancy in the language, he actively fills in the sequences of sounds that he does not actually hear or distinguish.

Dependence on the Four Skills

If we assume the transcription skill to be a combination of receptive skill and productive skill, what skills should be developed together with the transcription skill? All language skills are closely related and each language skill complements the other. At the same time, the students' passive knowledge of the components of a language, i.e., phonology, morphology, syntax, and semantics, cannot be deepened, reinforced, and internalized without actively and repeatedly exercising the productive oral skills and the productive written skills. Furthermore, the transcription skill is also a receptive-productive oral skill and, therefore, the speaking skill, which is a productive oral skill, must be developed and used as the means to achieve the development and consolidation of the transcription skill.

Desired Transcription Skill Range

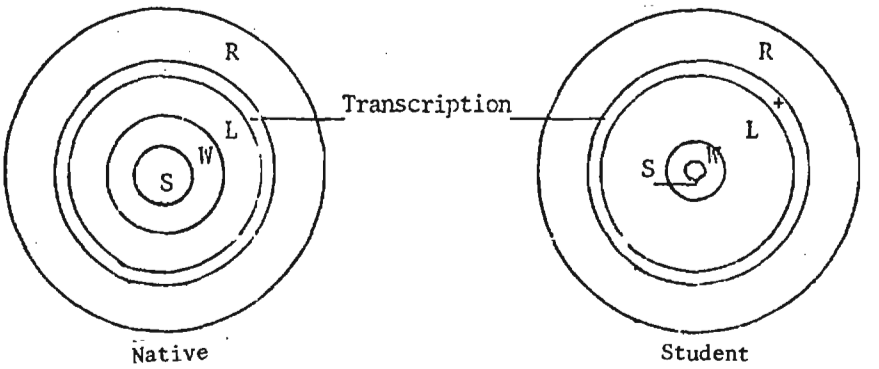
The ideal skill ranges for an adult student to attain in a foreign language are the skill ranges of an educated adult who is native to the language. In the practical situation, however, we recognize that the skill ranges[8] of our students will not correspond to those of a native adult. The students need not acquire as high a level of proficiency in speaking and writing as they do in listening comprehension, transcription, and reading to be able to function satisfactorily in the language. The goal of communication through speaking and writing would be acceptable at a level below that of a native speaker. The minimum skill ranges required in listening comprehension, transcription, and reading, however, are identical to the skill ranges of an educated native adult. The difficulty which the students will experience in acquiring the listening, transcription, and reading skills will therefore be quantitative in nature rather than qualitative. The relative skill abilities of an educated adult who is native to the language and the desired skill ranges of the students are illustrated in the diagram on the next page.

Summary of Concepts

So far, we have discussed the following points:

- Transcription involves hearing the sounds and sound patterns of a language, understanding their meaning, and representing the sounds in the written symbols of the language, while inferring missing linguistic elements;

[8]The concept of different goals for the four different skills originated with Ted Everett.



Relative Skill Ranges of Native Adult
and Desired Skill Ranges of the Student

- The transcription skill is inherently part receptive and part productive;
- The transcription skill should be reinforced by development of the speaking skill, which is a productive oral skill;
- The goal of transcription is to be able to comprehend native speech at normal speed in a real-life nonstereotyped situation. This requires a lengthy period of classroom instruction and on-the-job experience.

Teaching Methods and Techniques

Now that we have discussed the characteristics of the transcription skill, its relationships with the four other language skills, and the desired goal, we will describe methodology and techniques for teaching the transcription skill. In the Korean Department and Japanese Department we have reviewed available information on learning psychology and theories of language teaching, and have adopted the audio-lingual cognitive method (called the "cognitive method" in short) to teach transcription. This method is based upon the assumption that language learning includes a mechanical process and a cognitive process. The idea of the mechanical process of language learning stemmed from the behaviorist theory of stimulus-response learning, particularly as developed in the operant conditioning model of Skinner[9]. This view has been rejected by Chomsky and Lennenberg[10] and other theorists who maintain that there is something more to language learning than the mechanical process of imitation and generalization. They have, instead, emphasized the cognitive aspect of language learning.

We suggest, however, that the process of foreign language learning is built upon both habit formation and the cognitive process and therefore we have incorporated both concepts into five distinct phases of classroom activity. These phases include:

- expository presentation of material;
- analysis of the content through explanation in the native language;
- drills stressing understanding of the content;
- consolidation of those learned patterns through application to new situations; and
- evaluation of the students' level of learning.

The Five Teaching Phases at the 120 Level

- *Presentation*

In this initial stage, students are given written material to study before they listen to recordings. They can study the written text and the accompanying tape before a particular lesson outside of the class if they wish. In the classroom, the teacher first projects the written text on a screen and reads it aloud, alone, as a model. Then the teacher reads it with the students, and/or asks the students to read it in chorus and individually. The objective of this activity is to provide practice in the visual and aural identification of common word groupings, and phonological and structural patterns which are unfamiliar to the students. Memorization of the text, if possible for the student, greatly enhances the students' ability to identify a sequence of sounds and their associated written symbols.

- *Explanation*

After reading the material alound, the teacher and the students analyze grammatical sequences and tenses, modifiers and function words, cliches, expletives, hesitation expressions (which can be ignored as irrelevant to the message), levels of discourse (colloquial or formal), emotional overtones, as well as regional or dialectal variations, and translate them correctly.

Initially, the students at the 120 level usually have little ability in listening and

[9]Rivers, p. 73.
[10]*Ibid.*

speaking and writing, and, therefore, the foreign language utterances strike their ears as a stream of undifferentiated noises. By providing a written text and explaining the meaning thoroughly, we can help the student to assign meaning to these utterances and thereby enable him to transcribe material more efficiently and accurately. The value of this method can be contrasted with the unguided learning situation commonly encountered by immigrants in a foreign land. Lacking explanation of the meaning of sound patterns, immigrants are unable to understand more than a few simple phrases, even after many years of residence. This leads us to assume that aural comprehension must be learned in part through the theoretical framework which is provided by recognition of the meaning of words and phrases.

■ *Manipulation*

After the materials have been visually presented and explained by the teacher, the students listen to and transcribe a recording of the material without benefit of the written text. This drill allows the students to aurally identify a sequence of sounds in meaningful succession and to transcribe them correctly in the writing system of the foreign language, while inferring sounds which they missed or could not identify. Moreover, they utilize the passive knowledge of vocabulary and structure which they have studied and retained from the preceding presentation and explanation activities.

The transcription drill is followed by a drill in which the students read aloud their transcripts in turn and the other students listen to it, correct mistakes, and supply missing sounds and words. At the same time, the teacher helps the students to understand the material by explaining deductively why they made mistakes and what particular phonological, morphological, and syntactical elements are involved.

After the transcriptions are corrected in class, the students listen to the tape recording again and compare their transcript against the sounds on the tape. This exercise reinforces the students' ability to associate sounds, meanings, and written symbols. The students' transcripts are submitted to the teacher after this drill, and the teacher corrects any remaining mistakes. The transcript sheets are returned to the student at the earliest opportunity, on the same day if possible, so that the students will be aware of any mistakes which they missed while correcting their transcripts.

After reviewing the transcript sheets, the class moves on to another drill or drills, such as true-false drills, question-and-answer drills, or reproduction drills. For example, the students are asked to respond "true" or "false" in English to statements which the teacher prepared based upon the text, or the teacher may ask each student to compose a statement and have another student respond "true" or "false." In the question-and-answer drill, the teacher may put questions to the students, the students to the teacher, and/or the students to each other. These drills facilitate the students' ability to recognize word groupings and patterns and to produce them with ease in a sequence and environment which are are slightly different from those in the text.

The various oral drills are indispensable for developing and reinforcing the productive aspect of the transcription skill. Their effectiveness can be easily demonstrated by giving transcription tests. Students with a superior speaking skill and inferior reading skill will perform better than students with an inferior speaking skill and a superior reading skill.

■ *Consolidation*

After the manipulation activities, the students are ready and eager to try their ability at recognizing, understanding, and transcribing vocabulary and structure which they have studied in a totally different context without the use of the prepared written text. The teacher dictates selected material which includes some of the vocabulary and structures which the students have studied. As a challenge, the teacher also includes some unfamiliar vocabulary and structures. The students listen to and transcribe it, and do so with a great sense of achievement when they find that they understand the meaning of what they are transcribing.

A question-and-answer drill follows the dictation drill. This time, the questions and answers are exchanged only among the students. Both form and content are dealt with in the questions and answers. The students at first ask questions about form in order to supply missing words or to correct mistakes. The students then proceed to ask questions concerning the meaning of vocabulary items and then move on to the content of the entire selection. After the question-and-answer drill, each student may be asked to narrate it in his own words.

The teacher's role is kept to a minimum in this activity. He plays the role of consultant, guide, and assistant to the students -- and only when needed. Afterwards, the teacher collects the students' transcription sheets, corrects mistakes, and returns them at the next session in order to advise students of unnoticed or uncorrected mistakes. The teacher may also show the correct transcript on the screen and ask the students to read and translate it for reinforcement.

■ *Evaluation*

After the material has been presented, explained, manipulated, and consolidated, the teacher gives the students a very brief achievement test which covers only what has been taught so far in the course. The test consists of dictation which the teacher presents to the students for transcription, either through the medium of recorded tape or by reading it to

them. The teacher collects the transcription sheets for evaluation and then projects the correct version of the transcription on a scrren. The students are asked to translate this version, and their translations are also collected for evaluation. The transcriptions and translations indicate how much of the material has actually been mastered by the students and serve as the basis for the final grade in the course.

In addition to this type of text, every ten lessons or so the teacher gives a transcription test which does not contain material from the text or which was covered during the consolidation activities, but which is of approximately equal difficulty. The test measures students' growth in the range of their transcription skill since the last such proficiency test. The transcript is corrected by the teacher. It is not used in determining the final grade, however, because the content of the test was not taught to the students.

Course Emphasis

We have discussed the different objectives of the five teaching phases in a 120-level transcription course. The activities of each phase may vary from teacher to teacher or from day to day, but the five teaching and learning phases are distinct and characterize the cognitive method. The five phases are covered each class day, which lasts from 3 to 3½ hours. At the end of the day, the students should be able to transcribe about 200 syllables of dictation with an average of two mistakes. The dictation can be based on material covered in any of the past lessons.

The five phases are emphasized differently for more advanced transcription courses, such as 220 or 320. In general, the higher the course level, the more time is spent on consolidation and evaluation. Emphasis on evaluation activities does not mean that the students are given long tests, but that the students can independently transcribe more material which is unfamiliar in more advanced courses. The 120-level course is fairly tightly controlled by the teacher. The 220 class is an intermediate situation. At the 320 level, the students experience a more unstructured environment which resembles a real-life work situation where totally unfamiliar material must be transcribed every day.

The cognitive method of instruction has so far proven quite successful. Nevertheless, the students are still unable to transcribe all material freely after these courses. The goal of the student is to achieve a transcription skill range which matches that of the native speaker. It must be emphasized that this cannot be successfully achieved without development of the speaking skill, nor can it be achieved without a long period of instruction and on-the-job experience. For example, a recent study of students of Japanese[11] has shown that fluency in the language requires 5 or more years of formal study, including approximately 2 years of residence and study in Japan. The study shows that even after this lengthy period of training, students are still unable to write with ease. An adequate transcription skill range is not easy to achieve, but through the cognitive method and with instruction in the listening comprehension and speaking skills, it is possible to give students the basic tools with which they can achieve the desired transcription skill range.

---

[11]American Council of Learned Societies and the Social Science Research Council, *Japanese Language Studies in the United States: A Report of the Subcommittee on Japanese Language Training Study of the Joint Committee on Japanese Studies* (December 1976), p. 30.

TET, FRED HAND OVER BLUE PENCILS, BRASS KNUCKS

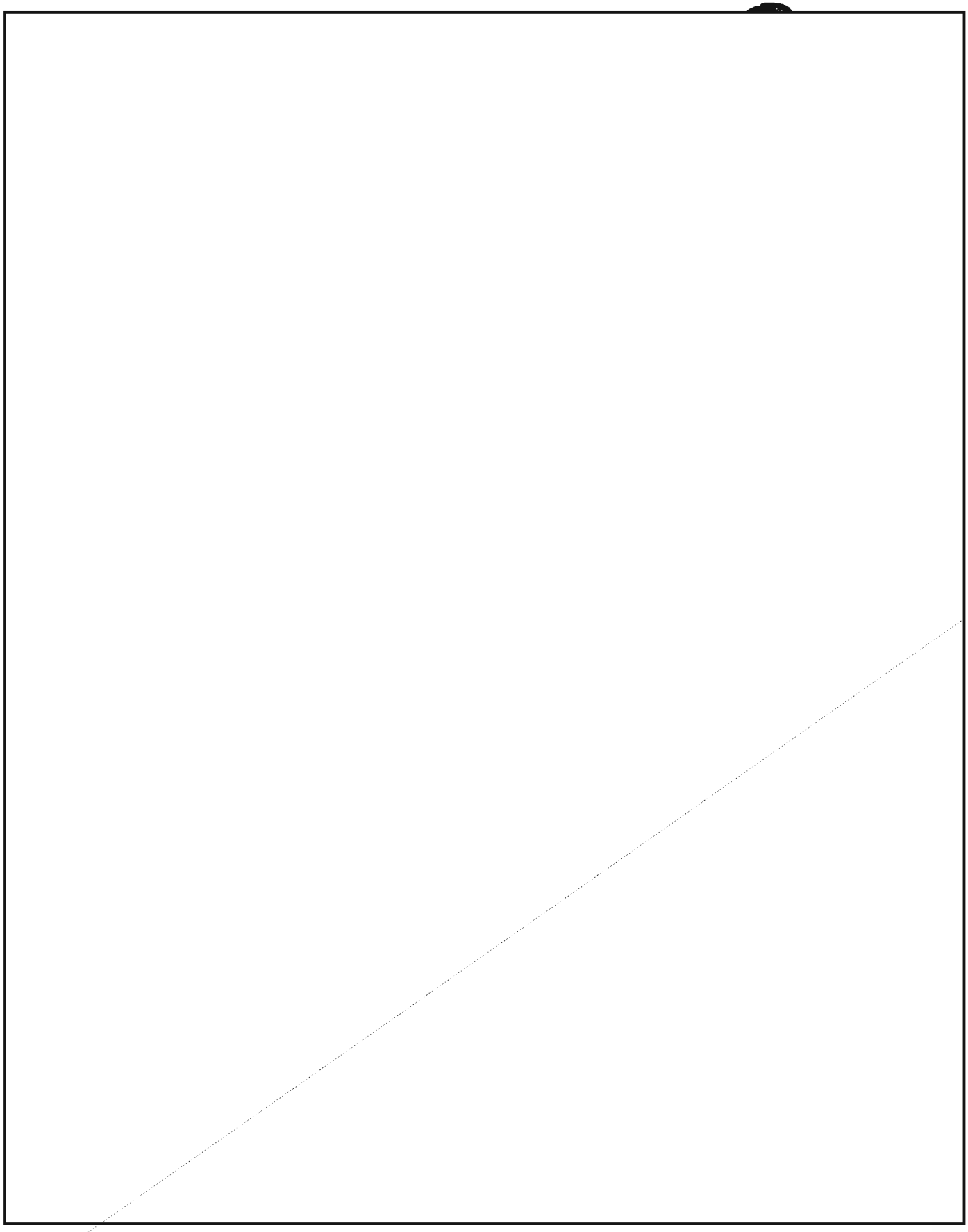
Starting with this issue, there are two changes in the makeup of the Editorial Board: Emery Tetrault (Language Editor since February 1975) and Frederic O. Mason, Jr. (TA Editor since January 1975) have completed tours in which each has made a large contribution to broadening the magazine's readership. In addition to acting as advisor on incoming manuscripts in their respective fields, as well as encouraging and assisting their coworkers to submit articles to CRYPTOLOG, Tet and Fred contributed several articles of their own. Tet wrote "Even a 5-year-Old Child..." (October 1974); cogent letters to the editor (February 1975, April 1977); "Where Does 'Does' Come From?" (June 1975); and "Research in Speech Perception" (August 1976). Fred wrote "TA, Handmaiden of CA" (May 1975); "More on Squaring the Page (A Crypto-TA Function)" (June 1975): "Abdul and His 40 Tanks" (August 1975); "A Vexing Agency-Wide Problem" (November 1976): and "Where Were We?" (January-February 1977).

I've appreciated working with Tet and Fred and know that they will continue to share their ideas with CRYPTOLOG readers. Who knows? Maybe now, with no need to persuade others to write articles, they might find lots of time to write many more of their own.

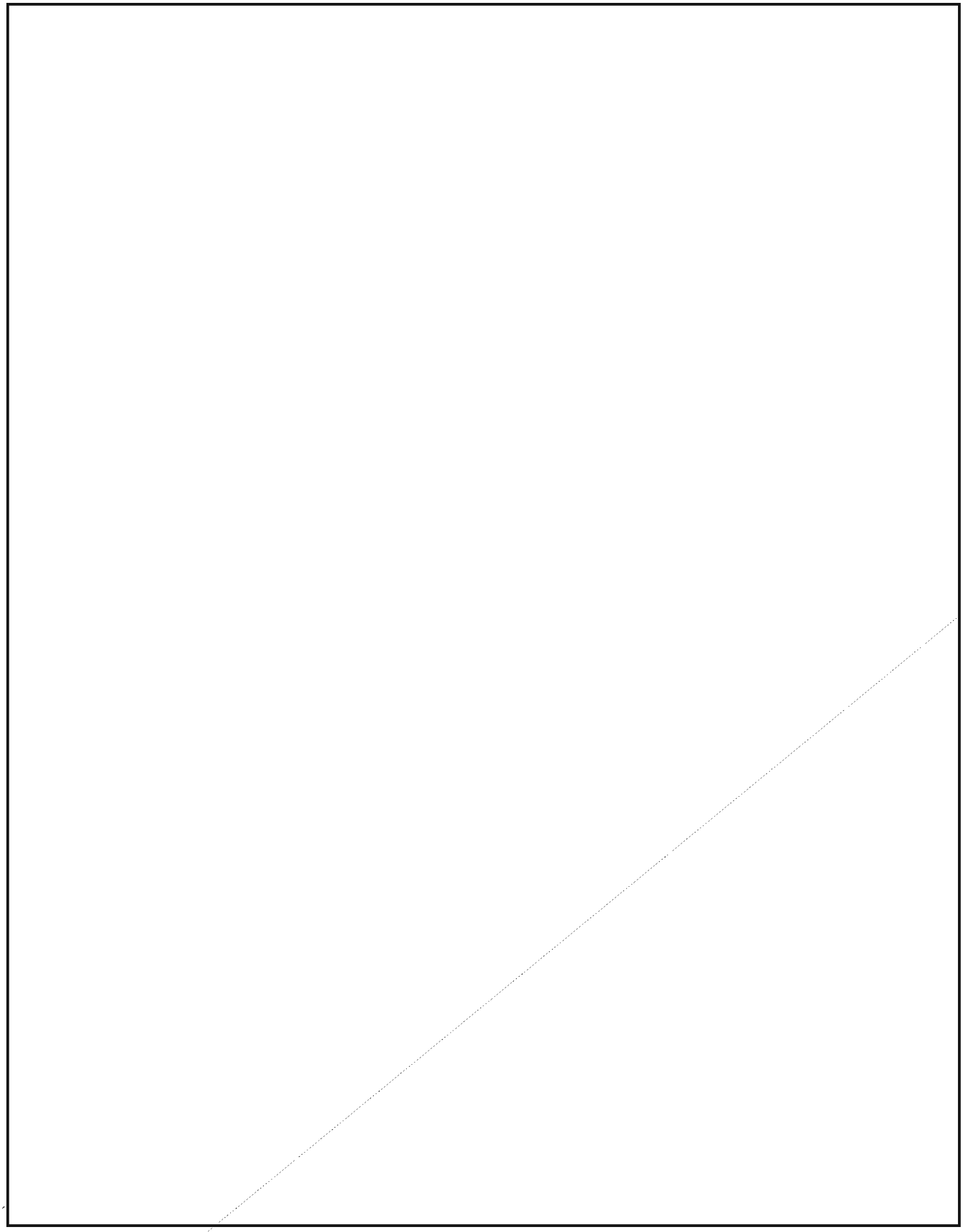
Tet and Fred are being replaced, respectively, by [redacted] have been told that they do not actually have to write articles themselves (although they may, if they want to). But their main job will be to lean on their coworkers and have *them* write about things they know about. So if you linguists and traffic analysts out there hear an increase in occurrences of the exclamation, "Hey, that would make a good article for CRYPTOLOG!", you'll know why.

Ed. (UNCLASSIFIED)

P.L. 86-36



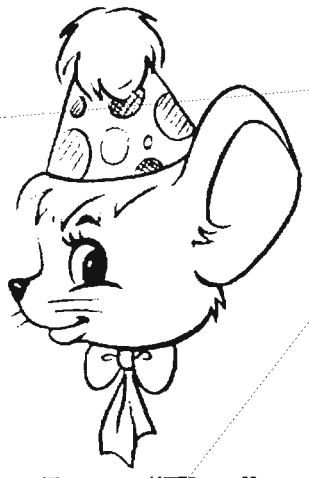
EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

DOCID: 4009798

Less than **$5,000 in prizes**
Awarded Monthly



EO 1.4.(c)
P.L. 86-36

Draw "Tiny"

YES, WE AWARD LESS THAN $5,000 IN PRIZES MONTHLY TO NEW CRYPTOLOG SUBSCRIBERS!!!

Considerably less than $5,000! In fact, we don't award *any* cash prizes monthly! Or *ever*! But you can still win a subscription to CRYPTOLOG.

Draw "Tiny" any size except like a tracing. Use pencil. (Or simply print your name on the coupon below.) Every entrant receives a free unprofessional estimate of his (or her) drawing (or ability to hand-print).

ALL ENTRANTS ARE WINNERS! Winners will receive a subscription to CRYPTOLOG, one of America's leading TSC in-house publications. Our objective is to find prospective readers who appear to be properly motivated and have an appreciation and liking for this sort of publication.

Your entry will be judged in the month received. Prizes will not be awarded for best drawings of various subjects (or best hand-printing specimens) received from any entrants age 14 (or any age). No drawings (or hand-printing specimens) can be returned. Contest winners will not be notified. Send your entry today.

MAIL THIS COUPON TO ENTER CONTEST

To: CRYPTOLOG,
P1

Please enter my drawing in your monthly contest. (PLEASE PRINT)

Name_____
Organization
~~Occupation~~_____ Age_____
Address N/A Apt. N/A
City N/A State N/A
County N/A Zip N/A
Telephone Number N/A

~~(C)~~

(U)

DOCID: 4009798

ZBB? WHAT IN THE WORLD IS THAT?

C263

Early in 1973, at an office meeting, the speaker read the acronym SADPPO, then asked, "What in the world is *that*?" Having just read NSA Regulation 110-2 the day before, I immediately jumped up and unraveled the deep mystery: "Senior ADP Policy Officer!" From that simple statement I was immediately proclaimed the world's foremost authority on SADPPO.

In a way, the same thing happened again recently with the abbreviation ZBB. When I saw it cross my desk for the first time, I was able to jump up mentally and say, "Zero-base budgeting!" Because just a few days earlier, I had read the book by that name (*Zero-Base Budgeting*, by Peter A. Phyrr). Having become, *ipso facto*, the Agency's "ZBB expert," I now feel ready to write an article about it and really establish my field of authorityship.

I'll leave the more intricate details of ZBB to the budget boys, but try to give a glossary-level understanding of the key objectives so that the operational force can find the transition to the new concept easier to take.

I'll purposely avoid using words and phrases such as "decision packages," "ranking, "macro-planning," and "microplanning." It is so easy to become entangled in catch words and phrases, until they become a part of our normal vocabulary even though we are still unable to grasp the main intent of ZBB.

First, ZBB is not just another burden laid on us all, although I have been just told that it is. On the contrary, it is a concept which, if the understanding of it were to filter down to the working level, would ensure that the government gets more for its money. Just as Value Engineering attacks the very premise of our design as possibly not being the best, and Base-Line Management shows us where we are and where we are going (even though we already profess to know), ZBB has as its roots the assumption that there is always an alternative way to solve a problem (even though we doubt it). Dare we admit that there is even the remotest possibility of an alternative to our already perfect plan?

Unlike PERT (Program Evaluation and Review Technique) and CPM (Critical Path Management), which will never concede a need for a slipped date, but only a readjustment of activities or events with slack or float time or alterations to the critical path, ZBB demands that we *do* concede an alternative to our already perfect plan. Years ago, in a Work Simplification course, the professor gave our class a project to cut the time, and thereby the cost, of a simple manufacturing process that had already been "simplified" by three previous classes. It was utterly impossible for us to cut the time any more. Or so it seemed to us, until the professor very humbly suggested an alternative: instead of shortening the process, we could eliminate it completely. We were all very quiet until the next class.

IN ZBB, not only must we concede that there must be alternatives to our plan, but we must further concede that they are cost-related. If we can swallow that much crow, we are ready for Step 2: that someone else will undoubtedly evaluate our alternatives and then, possibly, have the audacity to place our second choice first.

For it is on this tenet that ZBB draws its strength: that there *are* alternatives and that these alternatives must be ranked as to their cost-effectiveness value within the relationship of the total budget which was reached mainly through the workings of PPB (Planning Programming Budgeting). Also, ZBB requires that we point out in each alternative the consequences of not doing something. As programs progress, so do the alternatives. Therefore, industry has found ZBB most useful for budgeting non-production expenses, because of its flexibility.

"What about PPB?" someone may ask. Does ZBB negate PPB, or does it supersede it? Neither! The two concepts work together. We still require top-level, long-range planning. The big difference now involves the low-level, short-range planning, with cost-related alternatives. Except that, with ZBB, we are soliciting our budgeting aid from the grass-roots level.

Does ZBB affect us in our negotiations with the contractor? Absolutely yes, particularly where an RFQ (Request for Quote) is sought. It's back to the crow-eating example. Are we willing to ask our contractor to use his expertise and initiative to devise an alternative to our already perfect task description in the project directive? Remember, he is an expert and the best qualified, or we would not have picked him.

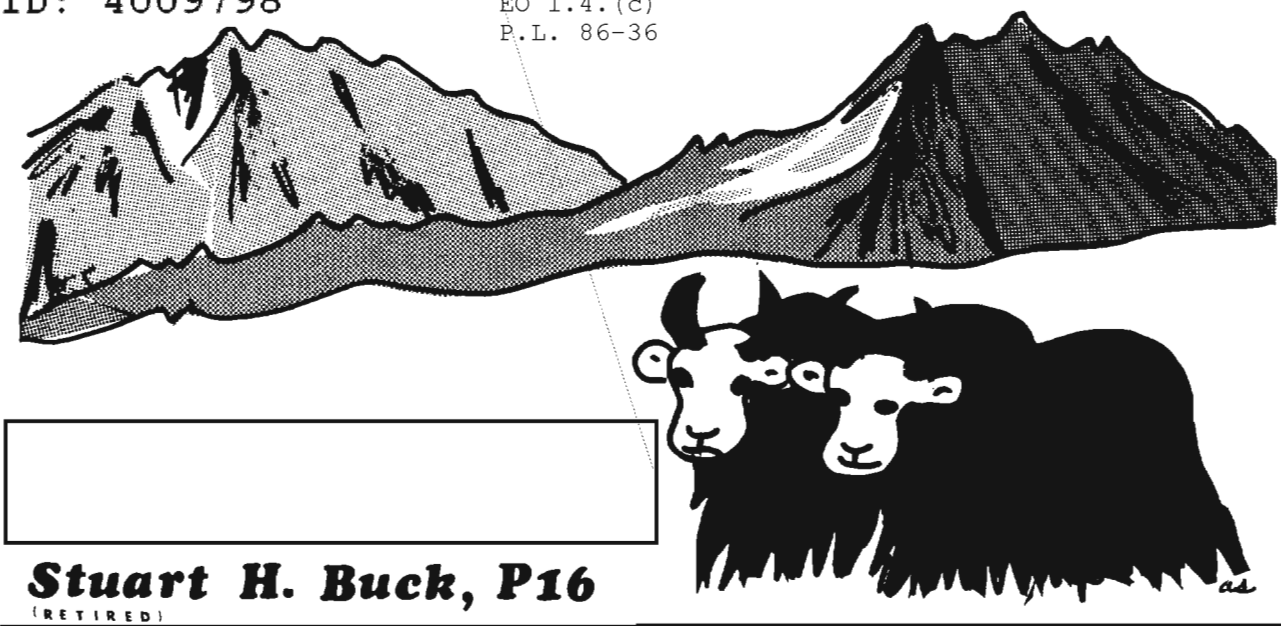
What if we're planning a really big project and we know it's going to cost more than what is available? What do we do? Cry a little and lie a lot? Or plan only enough to get started? It's "none of the above." Instead, we consider the alternatives. And then we look for *more* alternatives.

(Continued on page 20)

P.L. 86-36

DOCID: 4009798

~~TOP SECRET UMBRA~~
EO 1.4.(c)
P.L. 86-36



Stuart H. Buck, P16
(RETIRED)

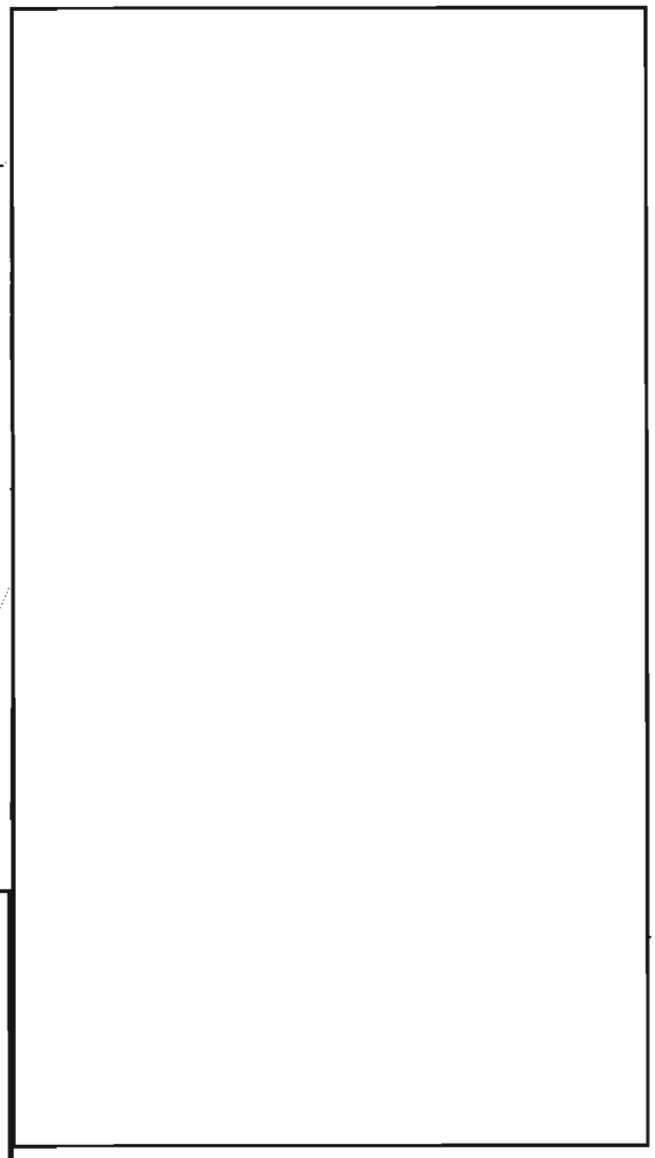
Before dwelling further on this thought, I think it would be advisable to define what we mean by bookbreaking, as used in the context of this talk. This is a ticklish subject, guaranteed to inflame tempers. Bookbreakers, as a group, are much like the blind men and the elephant -- they seem incapable of distinguishing the whole beast from the one small portion that they happen to touch. A common assumption is, "All codes are like the one that I once worked on. . ." Nothing could be farther from the truth. In fact, it is impossible to have a meaningful discussion of bookbreaking without clearing up certain common misconceptions.

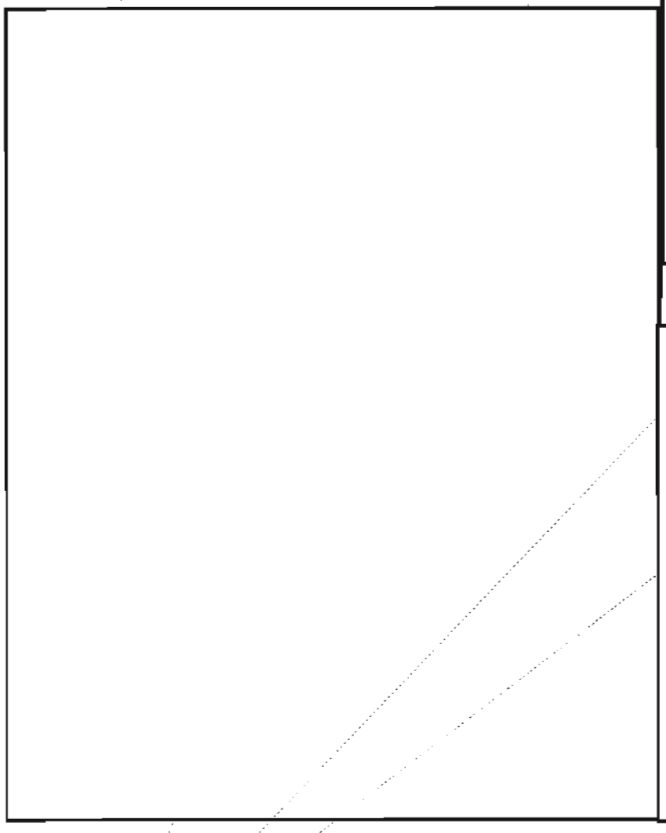
First, we had better settle the whole business of code charts as opposed to code books, the area where most of the misunderstanding begins. It is absolutely vital to understand the difference between these two broad categories; otherwise, our present thesis will make little sense. Generally speaking, code charts are made up of blocks of information or specific categories

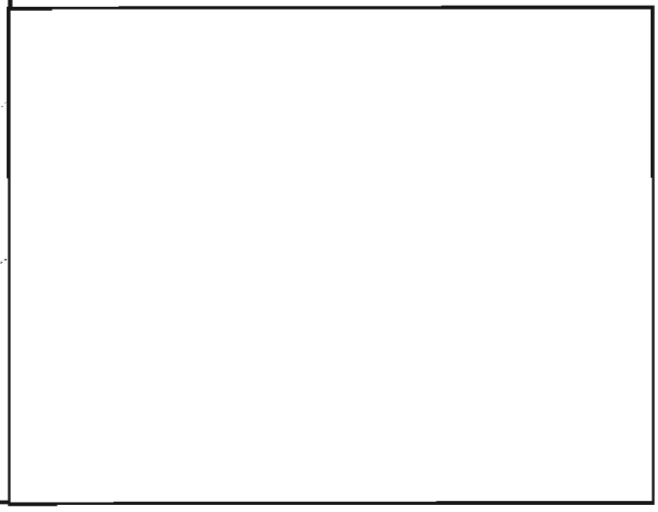
~~TOP SECRET UMBRA~~
EO 1.4.(c)
P.L. 86-36

DOCID: 4009798

that have a definite beginning and ending, each with a built-in logic of its own. In other words, they are *finite*. Common examples are: numbers, the alphabet, a syllabary, years, months, days, time of day, etc. If the chart is intended for the routine operations of a particular organization (as it usually is), it may contain special category blocks, such as types of aircraft, names of vessels, ports, airfields, points of the compass, weather conditions, and so forth. Actual vocabulary included in such charts is limited to the immediate needs of the users. After all, words not on the chart can be easily spelled out, using either the alphabet or the syllabary, or both. Code charts of this type are a cryptanalyst's delight. All you have to do is to break into a category in a couple of places, then generate the rest. Moreover, each chart is subject-oriented to a high degree. Ships don't fly, aircraft don't drop anchor, and the weather, however disagreeable, can do just so many things. You might have to consult with a linguist occasionally to make sure that things are going right, but, for the most part, the problem-solver happily thinks in English -- and usually gets away with it. In the end, he arrives at a total solution, just as in a crossword puzzle. Decrypted messages are then handed over, not to the person who solved the puzzle (because he can't read them), but to a linguist, who, presumably, functions at a lower level.

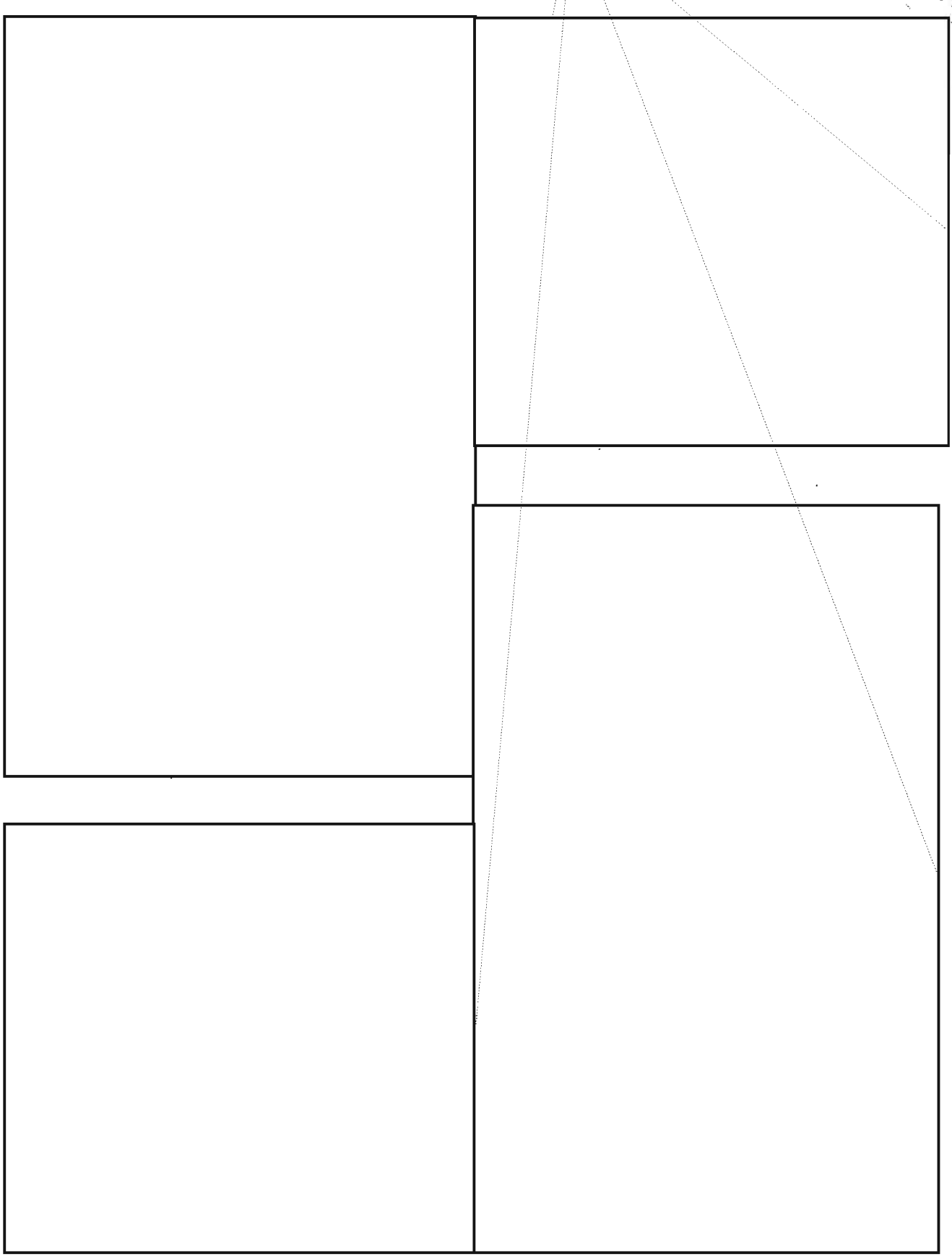


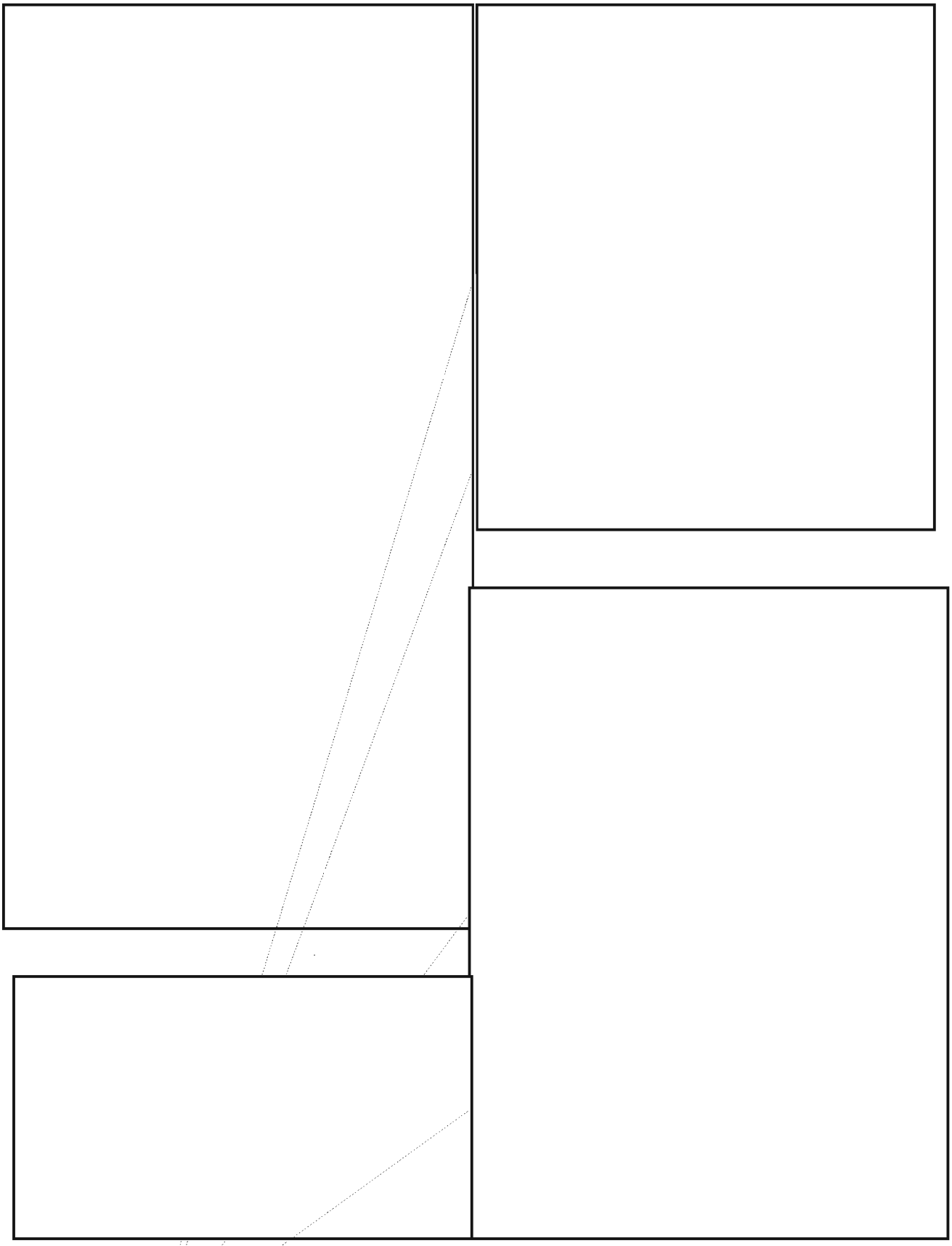




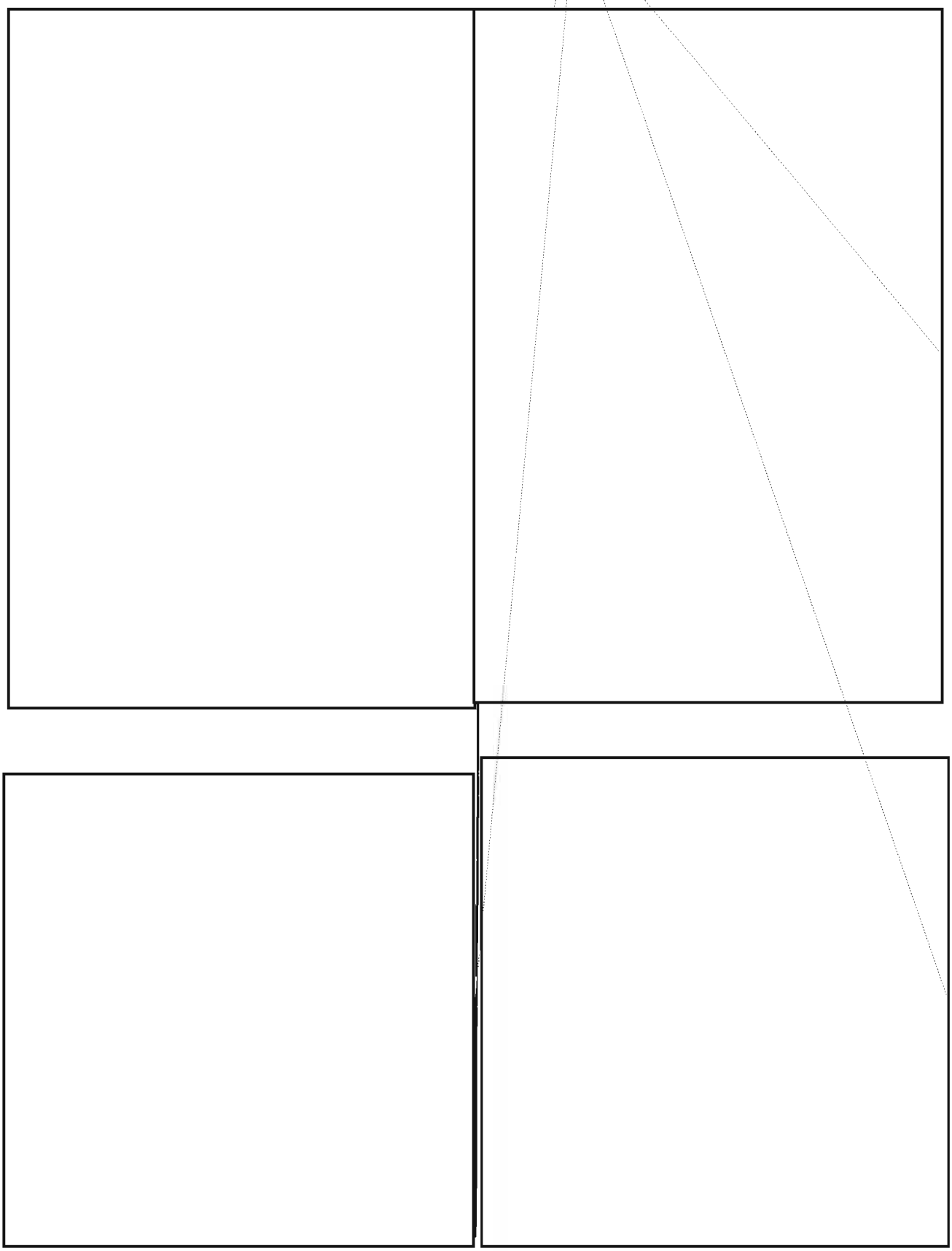
EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

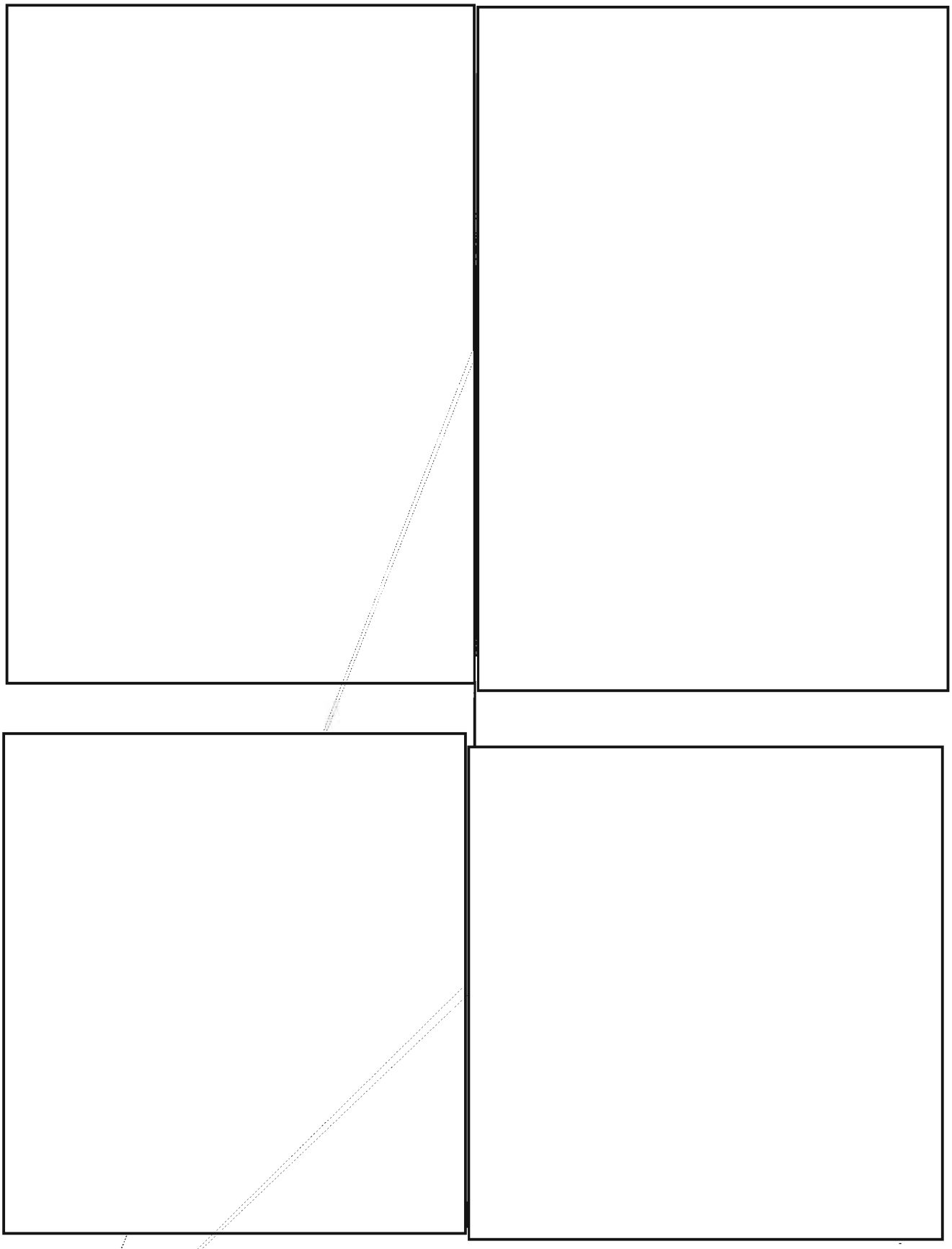




EO 1.4.(c)
P.L. 86-36



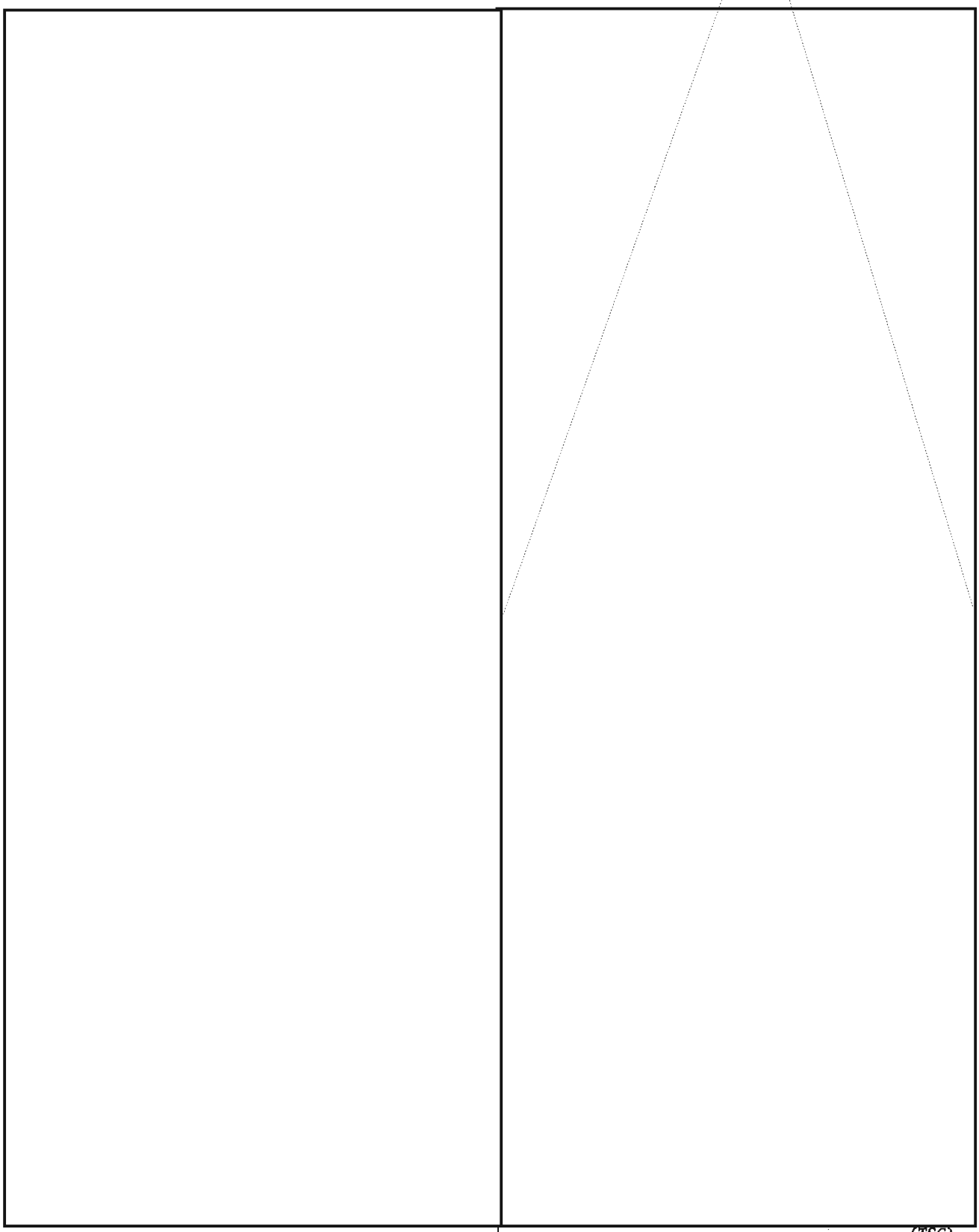
DOCID: 4009798



EO 1.4.(c)
P.L. 86-36

DOCID: 4009798

EO 1.4.(c)
P.L. 86-36



~~(TSC)~~

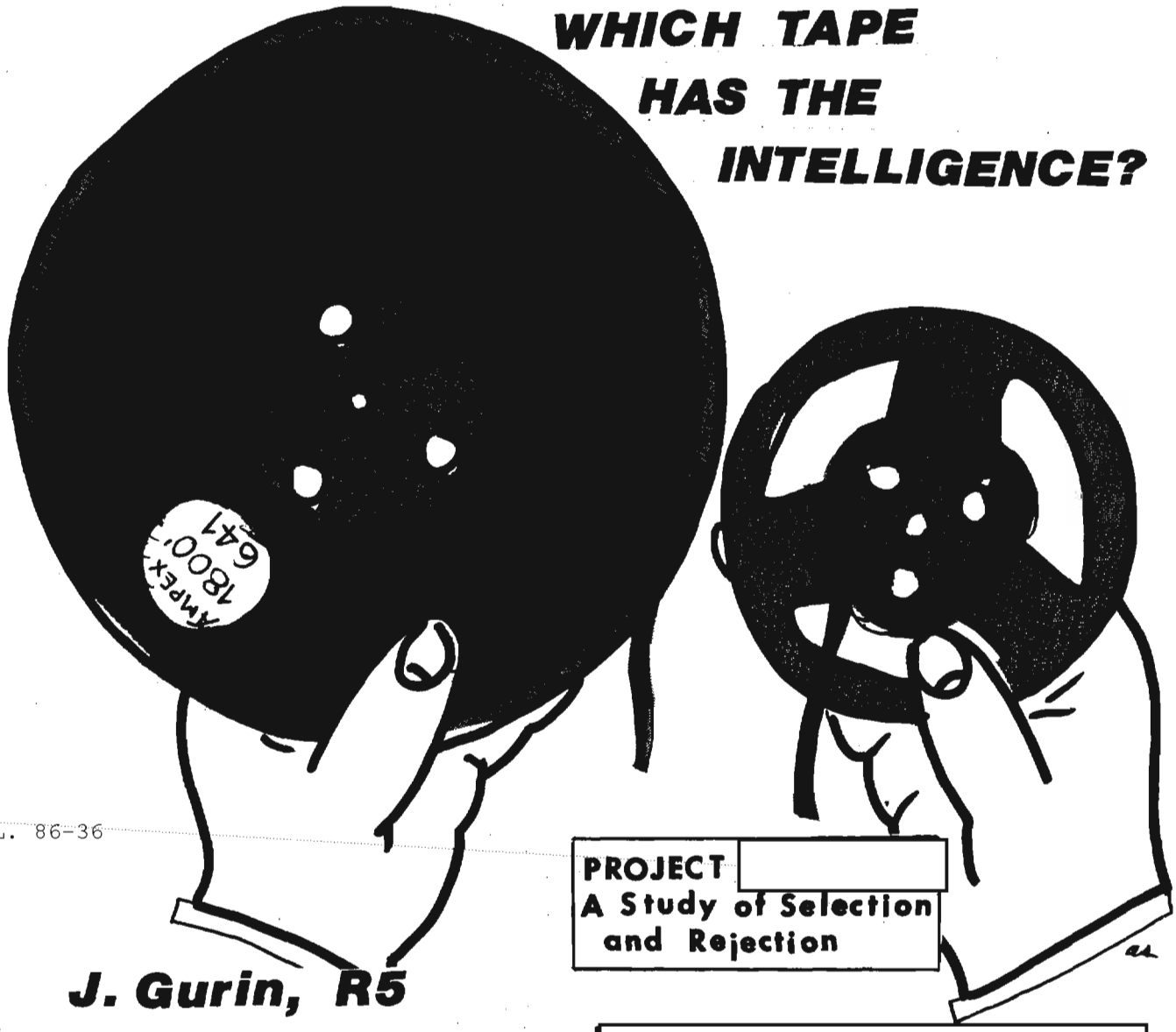
As we saw in the preceding article, Stu Buck accomplished a feat in the tradition of Champollion and Ventris, applying techniques that evolved over centuries of studying ancient texts. Some of the aids Stu referred to were so well described by [redacted] (now retired) that her comments are reproduced below, somewhat abridged for reasons of space. Her unabridged comments are contained in *Bookbreakers Workshop 1970*, the proceedings of a series of 14 sessions sponsored by P1 and chaired by Stu. Copies of the publication (TSC, S-212,800) can be obtained from Harry Goff, P16, 4998 S.

[redacted]
Chairman, Bookbreakers Forum

[redacted]

[redacted]

WHICH TAPE HAS THE INTELLIGENCE?



P.L. 86-36

PROJECT [redacted] A Study of Selection and Rejection

J. Gurin, R5

A certain excitement seems to have been generated by a modest project, devised in the Office of Research (R5) and under way in A6. It purports to discover how decisions are made either to retain or to reject intercepted conversations. No doubt the excitement is related to the desire, or even anxiety, of those who are seeking some way in which the machine may help solve the problem of too much traffic for too few transcribers. Project [redacted] under way for several months, is attempting to pin down the precise factors which enter into the human decision-making act, in the hope that much will be learned that will be of value in the eventual automation of some part of the process.

[redacted]

[redacted]

EO 1.4.(c)
P.L. 86-36

[redacted]

It may seem odd that we have never examined our selection mechanism in this way until now, but perhaps the need was never felt so acutely. Whether we succeed eventually in automating some significant portion of the process or not, we should gain some useful insight into the process and benefit in some other ways as a result of this investigation.

~~(CONFIDENTIAL — CCO)~~

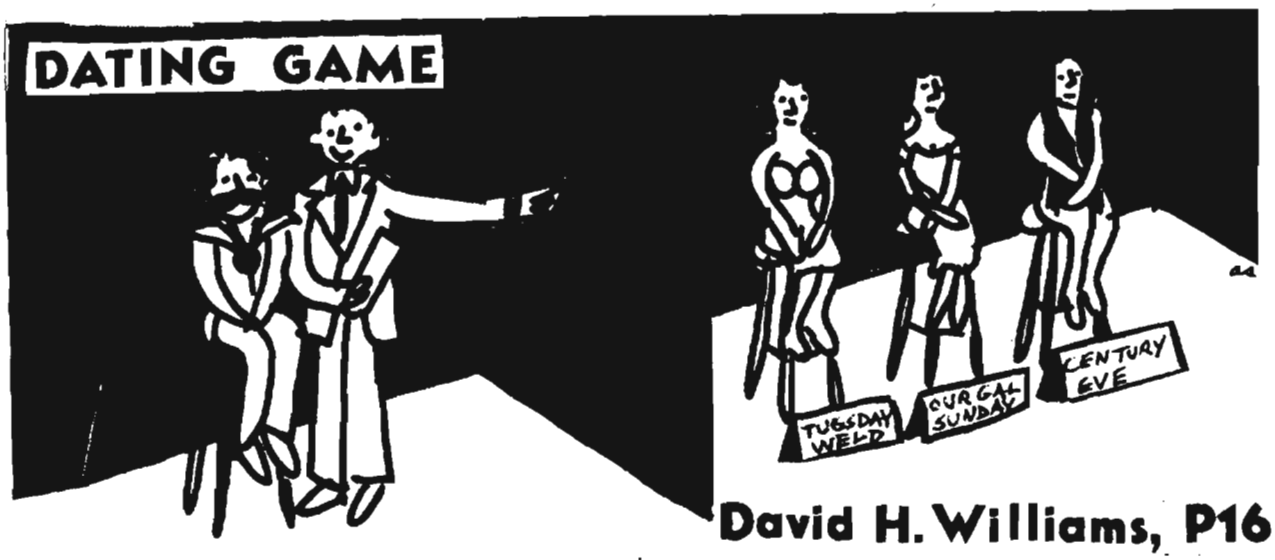
(Continued from page 10)

To imply that this is all there is to ZBB and that it is as simple as this brief introduction might indicate is to discredit ZBB grossly. So don't stop here! Read up on it! There is plenty of good material available at the C5 Library, including the following:

- *Zero-Base Budgeting*, Peter A. Phyrr (HF5550. P99);
- *Zero-Base Budgeting Comes of Age*, Logan Cheek, American Management Association;
- "Annual Overhaul," Lindley H. Clark, Jr., *Wall Street Journal*, 14 March 1977, p. 1;
- White House Memo, dated February 14, 1977, signed by President Jimmy Carter, with attachment by Burt Lance, Director DMB; with working draft of instructions for agencies in designing and implementing their internal zero-base budgeting systems;
- *Planning Programming Budgeting*, Fremont J. Lyden (HJ2052. L98);
- *The Politics and Economics of Public Spending*, Charles L. Schultze (HJ2052. Sch8).

(UNCLASSIFIED)

DOCID: 4009798



David H. Williams, P16

Have you ever found yourself needing to know the day of the week that some date fell on several years ago, and been unable to find a calendar for the proper year? If so, you might be interested in the following method for determining the day of the week by a bit of arithmetic simple enough to do in your head. The system looks more complicated than it actually is. In the course of preparing this article, I taught the system, as an experiment, to a 13-year old. It took 15 minutes.

The formula is quite simple:

$$Y + L + M + D = N,$$

where Y is the last two digits of the year,

L (leap year factor) is $\frac{Y}{4}$ (ignoring any remainder;

M is the month additive;

D is the date; and

N is the day-of-the-week factor.

The month additives are:

JaFeMr	ApMyJn	JlAuSe	OcNoDe
1 4 4	0 2 5	0 3 6	1 4 6

These must be memorized. It helps if you think of the first three triplets as perfect squares.

To determine day of the week, divide the day-of-the-week factor (sum N) by 7, and, ignoring the quotient, convert the *remainder* thus:

1	2	3	4	5	6	0
Su	Mo	Tu	We	Th	Fr	Sa

Examples:

1. What day of the week did December 7, 1941 fall on?

$$Y + L + M + D = N$$
$$41 + 10 + 6 + 7 = 64$$

Answer: $\frac{64}{7}$ yields a remainder of 1, equating to *Sunday*.

2. What day of the week will December 31, 1999 fall on?

$$Y + L + M + D = N$$
$$99 + 24 + 6 + 31 = 160$$

Answer: $\frac{160}{7}$ yields a remainder of 6, equating to *Friday*.

Obviously, with dates late in the month or late in the century, or both, the arithmetic gets a little cumbersome. Since you're shooting for the remainder after dividing by 7, you can simplify the process by eliminating 7s as you go along. That is, if Y or L or D is greater than 7, simply divide it by 7, and use the remainder in the formula. Likewise when your running subtotal (ST) exceeds 7, reduce it similarly. Thus, the Pearl Harbor example becomes:

$$Y \quad L \quad \overline{ST} \quad M \quad \overline{ST} \quad D \quad N$$
$$6 + 3 = \overline{9 \rightarrow 2} + 6 = \overline{8 \rightarrow 1} + 0 = 1 \text{ (Sunday)}$$

And the bulky arithmetic of the Century Eve* example simplifies to:

$$Y \quad L \quad M \quad \overline{ST} \quad D \quad N$$
$$1 + 3 + 6 = \overline{10 \rightarrow 3} + 3 = 6 \text{ (Friday)}$$

Since I've found that about half my usages of this method involve dates in the current year, I always keep the current Y + L subtotal in mind. For 1977 it's 5. Thus, determining, say, what day Christmas falls on is an easy 5 + 6 + 4 = 1 (Sunday).

For January and February of leap years, subtract 1 from N.

For dates in the twenty-first century, subtract 1 from N; for those in the nineteenth century, add 2.

**Editor's note:* I certainly hope that Dave and I are alive on December 31, 1999 so that I can see the incredulous look on his face when I tell him that that date is *not* Century Eve (or even Millenium Eve) and he's a year early with his funny hat and noisemaker.

DOCID: 4009798

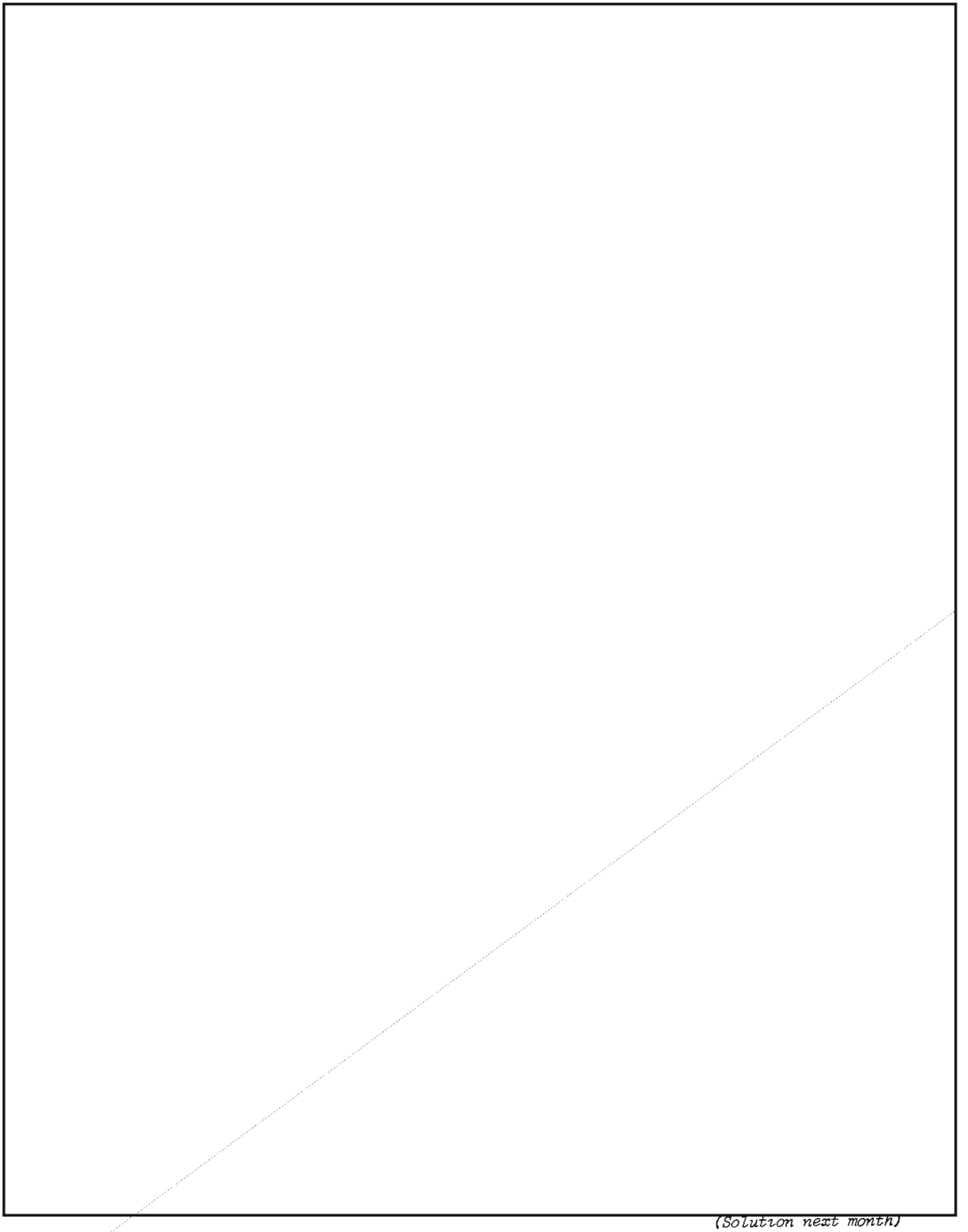
P.L. 86-36

NSA-crostic No. 8

By A.J.S.

The quotation on the next page was taken from a published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS *WORDS*



(Solution next month)

P.L. 86-36

~~CONFIDENTIAL~~

CORNER

[redacted] P.L. 86-36

DDO Classification Advisory Officer

With this issue, CRYPTOLOG is starting a series devoted to improving classification procedures. From time to time we shall print brief articles that are designed to help the reader in maintaining good classification practices while carrying out his or her everyday duties. Readers are invited to send in questions on difficult classification problems that they would like [redacted] to discuss in future issues, or to send in their own brief articles dealing with classification matters to "Classification Corner."

Ed.

Are there standardized abbreviations for classifications, or can people make up their own abbreviations? Nowadays it's a common thing to pick up papers -- messages, memos, correspondence, etc. -- with various classification abbreviations being used to designate individual paragraphs or titles. The information in one report may be SECRET COMINT Category II, and yet one originator uses the abbreviation "(SCW)" as the abbreviation, another uses "(SS)", and a third uses "(SC)". Do all three abbreviations mean the same thing? Can we use any of them interchangeably? Or is only one correct? If so, which one?

What would you do if you had to take the three reports with the different abbreviations and consolidate them into a single memorandum to be sent forward? Could you look somewhere for the correct abbreviation? The answer is, "Yes, in the *NSA Classification Manual*." That manual lists, on page 28a, all the classification abbreviations as standardized for use in NSA/CSS correspondence. They are the following:

[redacted] P.L. 86-36

First letter(s) indicating the National Classification Level:

TS - TOP SECRET
S - SECRET
C - CONFIDENTIAL
U - UNCLASSIFIED

Second letter(s) indicating special handling:

C - COMINT Codeword
CCO - Handle via COMINT Channels Only

These abbreviations are always enclosed by parentheses, e. g., (TS), (U).

When using the letter "C," do not use a hyphen, slash, space, or other separator, e. g., (TSC), (SC).

But *do* use a hyphen with the abbreviation "CCO", e. g., (TS-CCO), (S-CCO).

With all other special-handling caveats, phrases, or instructions, use a space to separate it from the first letter(s). For example:

(S-CCO NOFORN)	(SC FRONTO)
(TS NOFORN)	(TSC ISHTAR)
(S FRONTO)	(TSC GAMMA)

The only instance when a slash is used instead of a space is when using a codeword that is not normally associated with the National Level classification:

(TS/SPOKE)

~~(C-CCO)~~

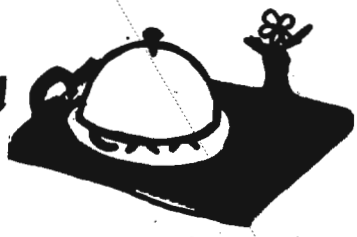
~~CONFIDENTIAL~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4009798

UNCLASSIFIED

EO 1.4.(c)
P.L. 86-36

What Ever Happened to the CAA?



[redacted]

P14

Funny you should ask! In January 1977 a new Board of Directors for CAA was elected:

President: [redacted]
President-Elect: David Gaddy
Treasurer: Timothy Murphy
Secretary:
Board Members: [redacted]

Since then, we have been asking around, "What do you think the CAA should be doing?" Some people answered, "Never heard of the CAA!" Others asked, "What ever happened to the CAA?" Still others said, "I thought the CAA died when I stopped seeing COMMAND." And on and on.

Well, let's begin with basics. What *is* the CAA and what is it *supposed* to be doing? The NSA Communications Analysis Assocation has as its purpose, according to its charter:

What - to promote professional growth and outstanding accomplishments;

Where - throughout the U.S. cryptologic community;

How - stimulate new ideas in the analysis of cryptologic problems;
- promote professional contacts and exchange of ideas between analysts in related career fields;
- encourage writing and publication of significant contributions to communications analysis;
- establish a forum for workshops, special interest groups, lectures, etc.

Who - members of the several fields of communications analysis:

- Traffic Analysis
- Special Research
- Signals Collection
- Signals Analysis
- Cryptanalysis
- Communications Security

So, what has the Board been doing? We meet at least once a month, and the meetings are open. You are invited to come out and see for yourself what is going on. Come and tell us where the CAA should be going and what it should be doing.

- We have been lining up speakers for general sessions in the Auditorium: Dave Gaddy in May, Cecil Phillips in June. (Did you miss them?) Watch for the announcements on who our speakers will be. Better yet, join CAA and let us send you your very own copy of the announcements, so that you won't miss any speakers. Other possible speakers at press time (mid-May) include Dr. Telford Taylor, an expert on World War II cryptology and now a professor at Columbia; [redacted]

- A small Special Interest Group on Crypto-TA problems has been started under the leadership of Fred Mason. Other SIGs could be developed, wherever there is enough interest. The Board has taken the attitude that CAA should serve all members and a wide variety of interdisciplines, even if some of the subjects don't have the broad general appeal of a presentation in the Auditorium. Therefore, if some things are interesting to only a smaller, select audience, we're ready to book a smaller room rather than the Auditorium.

Finally, where does the CAA seem to be headed? That's not so easy to answer. Our crystal ball is a little cloudy. Nevertheless, the Board seems to be moving in the following areas:

- In June (still in the future as of this writing), we will have a social get-together -- a cocktail party for Past President [redacted] (departing for NCPAC). Depending upon the response, we'll have more of this sort of thing.
- We are actively discussing (with DDM and others) just what role the CAA could play in post-certification growth. Since we are an interdisciplinary organization, and most notions about what happens after professionalization lean in the direction of cross-discipline work or study, we are beginning to think the CAA could be useful in this area.
- We will continue to look for opportunities to "light fires by rubbing two skills together." There has always been a need to get analytic people to look beyond their own immediate territories, to see how "what I do" might be connected with "what you do." This need is ever-present, both before and after certification (and some career panels have included in their criteria some form of encouragement for aspirants to "get out and see" how other analytic skills live and work).

We're not proud! We'll accept ideas, suggestions, and criticism from anybody. So, what do you want the CAA to do? Where do you want the CAA to go (figuratively speaking)?

P.L. 86-36

UNCLASSIFIED

DOCID: 4009798

Letters to the Editor

To the Editor, CRYPTOLOG:

I am distressed that the reaction to my article on "Integrated Analysts for Asia: A Cohesive Approach" (CRYPTOLOG, August 1976) has centered on an observation I made regarding the Asian male (not my personal) attitude towards women. "Firebrand" (CRYPTOLOG, October 1976) alleges that I have virtually admitted to sex discrimination in the placement of integrated analysts, and Mr. Newton (CRYPTOLOG, April 1977) states that I discourage "utilizing women as employees," which seems a bit much.

Before I am given the "MCP of the Year" award, or disfigured, or something, let me, once again, state what I was trying to achieve in that article. The point I was trying to make is that I believe we need a cyclical program of development for the very few, highly important, integrated analytic jobs which we support, and such a program may require several years (rather than a few months) of preparation by the selectee before deployment. Further, we should, insofar as possible, try to identify those people who will have the best chance of success with [redacted] counterparts and to do so requires an understanding of the counterpart mores, customs, and attitudes.

EO 1.4.(c)
P.L. 86-36

You might be interested to know that before I submitted my article to CRYPTOLOG I had it reviewed by a senior female employee of the Agency whom I have known and respected for several years. This individual is, herself, very active in insuring equality of rights and opportunity for women in the Agency, [redacted] She found my observations to be neither offensive nor inflammatory in the context of the article since she allowed that, while she personally did not like the Asian male attitude toward woman (and what U.S. woman would?), my portrayal of that attitude was accurate within her experience, and was worth noting. She also felt that any woman considering applying for one of the integrated analytic jobs should be aware of what she would be confronted with, and cognitively be prepared to deal with

EO 1.4.(d)
P.L. 86-36

~~CONFIDENTIAL~~

EO 1.4.(c)
P.L. 86-36

it if she were selected. If would appear, if nothing else, my article has achieved this latter effect; although I would welcome some opinion on the program I proposed beyond the particular point at hand.

[redacted] I must confess that my observations of last summer were somewhat superficial. These people have attitudinal idiosyncracies which I never even started to consider. For example, a left-handed person is considered inferior and parents will expend much time and energy retraining a lefty early in life. Another inferior being is a person who drives his or her own car -- if you can afford the car, you surely can afford a driver! And on it goes.

[redacted]

I hope the above will put to rest any sexist charges still pending against me. My point was not to malign the fine women of our Agency or suggest a process in violation of any Executive Order, Personnel Regulation, etc., [redacted] However, the times are changing...

[redacted]

EO 1.4.(c)
P.L. 86-36 ~~(CONFIDENTIAL)~~

To the Editor, CRYPTOLOG:

At the risk of jumping on the proverbial bandwagon or otherwise blowing a rather innocent article completely out of proportion, I, for one, would like to register a bit of moral support for [redacted] concerning his comments regarding women in Integrated Analyst positions. I know he would like to put the entire matter to rest, but it appears that there are those who either thrive on the art of disagreement or otherwise simply refuse to address facts or face reality, especially a reality over which they have *no control*. That is, after all, the root of this entire discussion.

With no intent of disrespect, either for our President or Director, it is evident that the quoted Executive Order 11478 is a work of naiveté. Our foreign friends (the few that still really like us) more often than not are willing to go along with our American customs and standards for a number of reasons -- usually borne of politeness, economy or fashion. He is extremely naive, however, who thinks that by simply issuing an Executive Order, our friends will buckle under and change native habits and customs [redacted] Some are changing, but it's terribly slow and due to worldwide social development, not the whims and desires of *our* women, *our* President, or *our* Agency. That is fact. That is reality.

[redacted] They are great people and they (the men) love their women deeply, and respect them. In fact, behind the scenes the women are more often than not both the driving and stabilizing force in the man's life. But *in public, at work* it's a man's world. That is fact. That is reality.

Can we follow the Executive Order and select a female for an integrated position? Sure. If she is qualified, why not? Should we select a female? To answer this question and to be reasonable, we must go beyond the Executive Order and the American ideal. If an integrated analyst is going to function and be effective in pursuing the assigned mission, he/she must have the mutual respect and credibility of foreign counterparts. If, however, the counterparts do not wish to share that feeling a female due to their own customs and standards, well, that's *life*, and all the Executive Orders, Lib movements, and the like are not going to change it, at least not in the next few years. If, on the other hand, it can be categorically determined that the moot principle and/or spirit of the Executive Order are more important than lasting foreign friendships and hard-won intelligence relationships so necessary to support our National Mission objectives, then perhaps we should press on with same, regardless of the cost.

That is fact. That is reality, guys and girls. If you (both selectees and selectors) fully understand the rules of the game and still desire to fill a specific Integrated Analyst position, then proceed post haste, albeit not blindly in a bureaucratic fog.

Heaven only knows, 6 months of looking at [redacted] fuzzy beard is about all I can take, and a change of scenery would be most welcome!

[redacted]

~~(CONFIDENTIAL)~~

To the Editor, CRYPTOLOG:

Could you please arrange to send me a copy of your exciting, fast-paced, and informative journal each month?

I have heard that the magazine is free, but if this is not the case, I would be happy to give you a recording of "Georgie, Handle the Cows Well" as sung in the original Romanian by

~~CONFIDENTIAL~~

P.L. 86-36

the Brothers Petreusi, in exchange for a one-year subscription.

Thank you very much.

[redacted]

Editor's reply:

No, thank *you* very much!. . . for those complimentary adjectives. If CRYPTOLOG really is "exciting, fast-paced, and informative," it's because of readers like yourself -- people who are willing to send in their letters and their articles, and thus to share their most valuable possessions -- their ideas, their gripes, their suggestions, their honest accounts of successes achieved and failures experienced. We're always pleased to add new names to our subscription list, but even more pleased when new names appear in the table of contents. So, although we appreciate your offer of that choice recording, we would rather have you send us an article we can print. What have you done lately that you're proud of? Or disappointed in? Or mad about? What would you want to share with other CRYPTOLOG readers? Quick, start writing!

(UNCLASSIFIED)

MATCH THEM UP!

By [redacted] D5

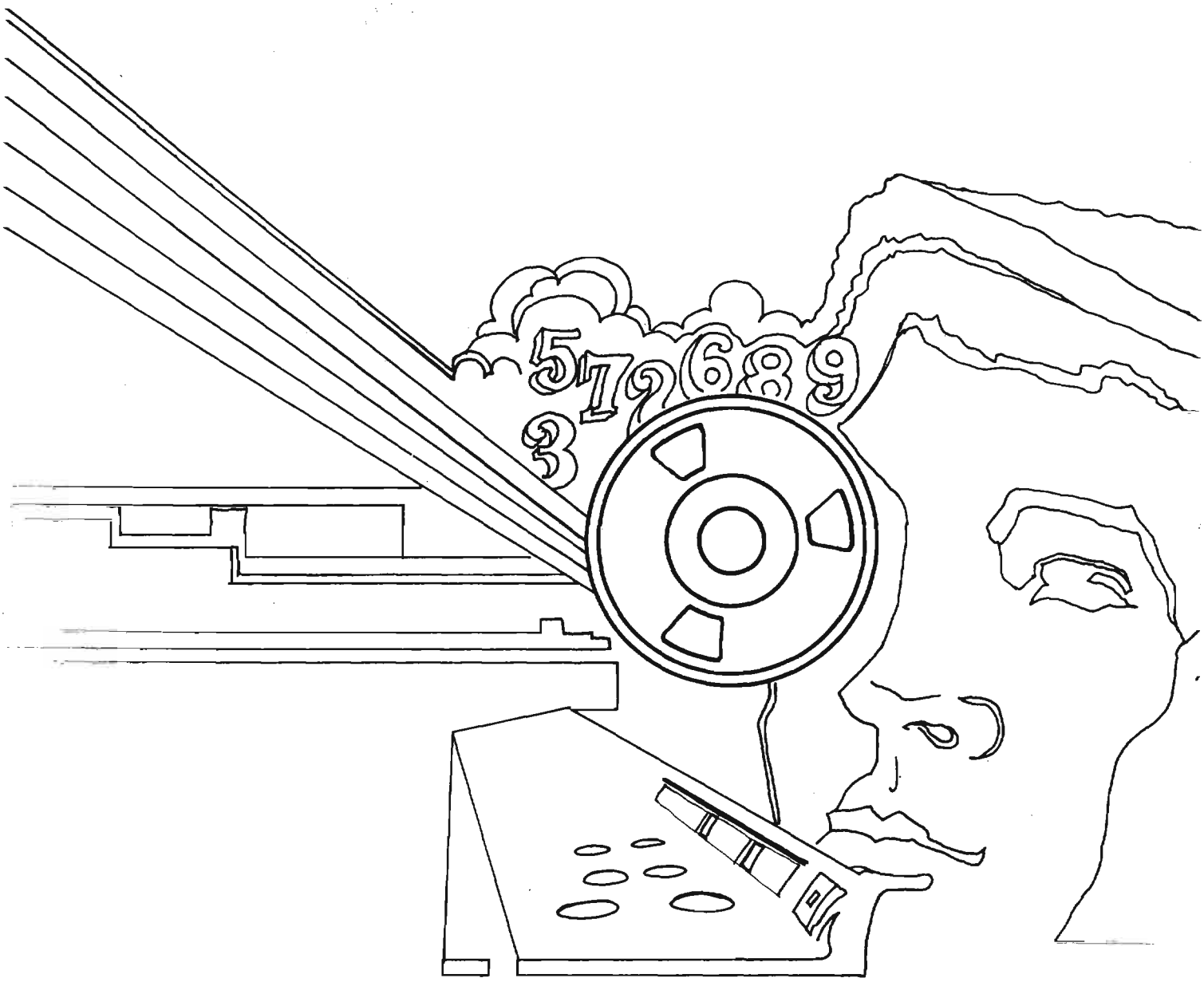
The following Prime Ministers or Heads of State were identified in Intelligence Product during the week of 25 April 1977. Can you associate the names and countries?

1. Amin
2. Asad
3. Bhutto
4. Boumediene
5. Castro
6. Daoud
7. Desai
8. Fahd
9. Fukuda
10. Geisel
11. Giscard
12. Hassan
13. Houphouet-Boigny
14. Lopez Portillo
15. Marcos
16. Mengistu
17. Mobutu
18. Morales Burmudez
19. Neto
20. Numayri
21. Nyerere
22. Qadhafi
23. Rabin
24. Ramgoolam
25. Sadat
26. Senghor
27. Siad
28. Soares
29. Suarez
30. Smith
31. Tindemans
32. Videla
33. Zia Urrahman

A. Afghanistan
B. Algeria
C. Angola
D. Argentina
E. Bangladesh
F. Belgium
G. Brazil
H. Cuba
I. Egypt
J. Ethiopia
K. France
L. India
M. Israel
N. Ivory Coast
O. Japan
P. Libya
Q. Mauritius
R. Mexico
S. Morocco
T. Pakistan
U. Peru
V. Philippines
W. Portugal
X. Rhodesia
Y. Saudi Arabia
Z. Senegal
a. Somalia
b. Spain
c. Sudan
d. Syria
e. Tanzania
f. Uganda
g. Zaire

Answers next month.

~~(CONFIDENTIAL)~~


5726893

DOCID: 4009797

P.L. 86-36

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JUNE 1977

HUMAN FACTORS AND SYSTEMS DESIGN..... [redacted] 1
OLD RUSSIAN MANUSCRIPT CIPHERS..... [redacted] 3
SIGINT WELCOMES INKSTAND..... [redacted] 4
AG-22/IATS: A VIEW FROM THE BRIDGE..... [redacted] 5
VICH ISS R-R-RIGHT?.....A.J.S.....17
LETTERS TO THE EDITOR.....18
CLA ANNOUNCEMENT: ANNUAL BANQUET.....21

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

~~DOCID: 4009797~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. IV, No. 6 JUNE 1977

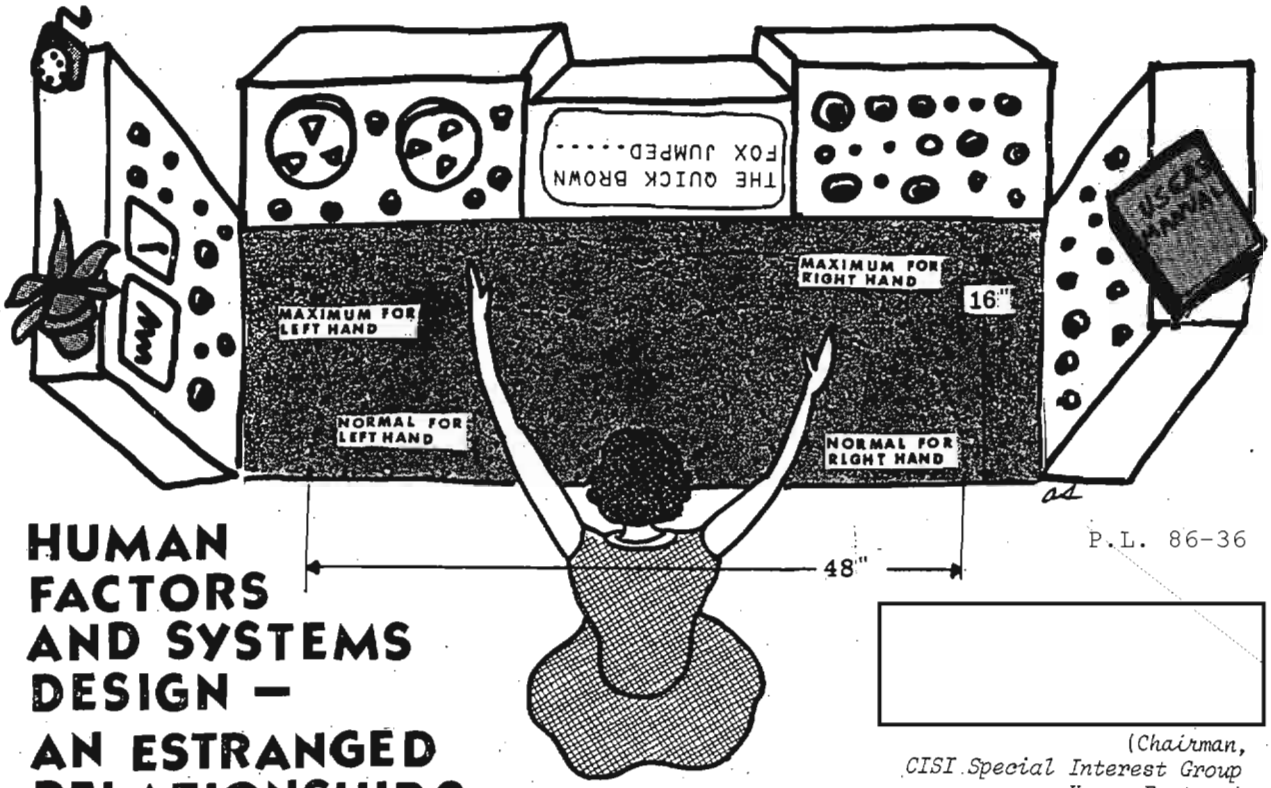
PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5642s)
Collection.....[redacted] (8955s) P.L. 86-36
Cryptanalysis.....[redacted] (4902s)
Language.....Emery W. Tetrault (5236s)
Machine Support.....[redacted] (3321s)
Mathematics.....Reed Dawson (3957s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Frederic O. Mason, Jr. (4142s)
Production Manager.....Harry Goff (4998s)

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4009797



HUMAN FACTORS AND SYSTEMS DESIGN — AN ESTRANGED RELATIONSHIP?

P.L. 86-36

(Chairman,
CISI Special Interest Group on Human Factors)

The process of designing computer systems -- particularly, on-line interactive display systems -- in today's environment presents challenges that summon the very best from a variety of professional disciplines. Those who have survived the experience of specifying, designing, and implementing such systems will no doubt agree that the most difficult task can be that of analyzing and providing useful, viable solutions to problems of the man-machine interface.

In a total systems context, man-machine interfaces are rarely simple. Environmental factors -- such as visual problems caused by glare or distracting reflections, awkward positioning of keyboards and control devices, uncomfortable consoles with sharp edges, lack of storage or writing space, exhaust fans blowing hot air on the operator and causing normal eyes to dry out and eyes with contact lenses to become seriously irritated, etc. -- present a set of problems in themselves. Generally speaking, the "man" part of the system in terms of physical dimensions, visual and auditory sensory systems, sensitivity to heat, cold, noise, vibration, and other environmental factors have been well documented. Knowledge of these is fundamental to systems design and should be part of the skills the professional has acquired through formal courses or independent study. There is simply no excuse for overlooking human physiological characteristics, or basic needs and comforts, when hardware is being designed. But, unfortunately, these are indeed ignored with alarming regularity, and, by the time the end-user discovers what has been done to him, it is usually too late to change. Talk to field station personnel sometime! They could write a book on equipment horror stories.

The man-machine design task is compounded by another set of problems brought on by the complexities of having a human being function as a major working component of the system. The human component, while intelligent, adaptive, clever, and resourceful, is also characterized by serious processing limitations, individual differences, and unpredictable -- sometimes illogical -- behavior. The seemingly infinite number of problems introduced by the human element call for special knowledge and skills. Systems analysts/designers must look to the human-factors profession and related fields (psychology, for example) for guidance. Specifically, it may be desirable to seek direct assistance from human-factors specialists. Since such specialists are not readily available, especially at NSA, an alternative is to research human-factors literature. The latter alternative is difficult and should be approached with caution, respect, and a dash of wisdom. Over the past several years, I have probed the journals and technical papers issued by human-factors societies, searching for answers to a variety of questions. The sobering fact is that such searches have typically yielded little information that could be applied to the real world.

Most laboratory experiments conducted by psychologists (even those boasting of being "applied psychologists") have very limited relevance to practical problems. Lab experiments can select only a few independent variables, and unsuspected interactions in more complex real-life conditions may nullify or reverse conclusions reached in the lab. Only with extreme caution can one generalize from the results of such experiments. This is not to say that experiments cannot be of value. Some very significant work has begun in recent years in the computer industry, the military services, and in major universities in the United States and Europe. Basic studies in the areas of the effects of computer response times on users, display formats, the effectiveness of control devices (light pens, joy sticks, etc.) and techniques for imbedding training subsystems into basic software packages are a few examples. All show promise of helping systems designers.

Sparse as it may be, however, the information that is available contributes to a designer's general store of knowledge brought to bear on real-world problems. Beyond this, designers are pretty much on their own. At this juncture, it seems to me that the most reasonable course of action for the designer is to get down to the basics -- simple, accurate statements of problems in plain English, and commonsense solutions. This means long chats with the end-user of the system to find out what he *really* needs to do his job. It also means reviews (formal and informal) at many points in the system-development process, with strong user participation.

From the very beginning, the user must become actively involved if there is any hope of influencing the system that will show up at the door some day. Systems designers, being finite creatures, can go only so far in interpreting what the user really needs and how the analyst's mental processes might function in the heat of problem-solving.

Much can be done to provide highly responsive generalized system capabilities that will satisfy most of the users most of the time. But where in the system is the point reached where specialized capabilities tailored to critical or frequently executed processes are necessary or justified? What are the most meaningful ways to organize and present data to the analyst? Are traditional manual ways of working the best ways in an interactive computer environment, or is a whole new concept needed? How fast must the system respond to user requests for information? What is the response threshold beyond which user productivity is significantly reduced or problem-solving abilities are rendered ineffective because human short-term memory is disrupted? Many such hard questions must be asked and alternatives must be probed. Systems people and users must rigorously analyze specific tasks, information needs, and work scenarios to identify and specify needed capabilities. It all takes time and a lot of hard work. There is no short cut. If it is done right, the dividends are high.

If there is any conclusion to be drawn from these mental meanderings on the very diverse subject of human factors, I believe it is that, overall, there exists a serious gap between designers and end-users, and human factors are considered either "too little or too late." Closing the gap is a two-way process. Users and designers must both take active, positive steps toward understanding each other's roles in systems development and work closely toward a common objective. The objective should be to deliver useful, productive information-handling tools that take maximum advantage of what computers do best and what people do best, and that bring people and data together with the least resistance and highest productivity.

(UNCLASSIFIED)

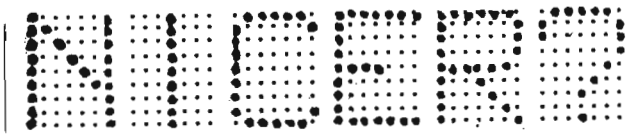
Cheap CRT displays usually mean cheap character fonts. By saving a few bucks, you may be buying high error rates and lowering productivity.

On the low end of the CRT display scale are those El-Cheapo display terminals that draw characters with a 5 x 7 dot matrix. There is just so much you can squeeze out of that matrix: A through Z (capitals only), zero through 9, and a few awkwardly shaped special characters. The whole scene is rather barbaric!

Nevertheless, if your budget is low and your application limited, you may just end up with those kinds of CRTs in front of your analysts (or whoever). Faced with the 5 x 7 option, at least you should be aware of which character sets offered by manufacturers are acceptable from a human engineering standpoint.

Human factors studies have shown three fonts to be superior. These are: Maximum Dot, Maximum Angle, and Lincoln/Mitre. Even the "best" of these (Maximum Dot) has a high percentage of confusion (25%) between certain characters (M, Q, S, U, V, 0, 1, 2, 7, and 8). If your application cannot tolerate this degradation, you should consider a better display terminal with a 7 x 9 dot matrix or even stroke-generated character sets. If you'd like to borrow the referenced studies, call me on 3758s.

[redacted] (U) P.L. 86-36



DOCID: 4009797
P.L. 86-36

OLD RUSSIAN MANUSCRIPT CIPHERS

In the CLA announcement on page ·· of the May issue of CRYPTOLOG, you probably figured out the way that dots and lines equate to numbers in the Maya writing system -- 12 is represented by two lines having a value of 5 each, plus two dots. The following article describes how a similar system of dots and lines was used in ancient Russia to represent not only numbers, but also something else.

Ed.

Translator's note: The following is a translation of an article by V. N. Perets, "Litoreya," in the prerevolutionary Russian *Ehntsiklopedicheskij slovar'* (Encyclopedic Dictionary), by Brockhaus and Efron (St. Petersburg, 1896, Vol. XVIIa, pp. 834-835). A current dictionary defines "litoreya" as "one of the oldest forms of secret writing, which is based on substituting letters of the alphabet for each other."

LITOREYA (from [Latin] "littera), secret writing system, type of enciphered writing used in ancient Russian manuscript literature. Two types of "litoreya" are known: simple [*prostaya*] and complex [*mudraya*]. The simple type, also called gibberish language, lies in the following. The consonants [in the *Russian* alphabetic order] are arranged in two rows [boustrophedonically]:

б в г д ж з к л м н

щ ш ч ц х ф т с р п

When writing the message, the letters in the upper row are replaced by the lower ones, and vice versa; the vowels remain unchanged. For example, лсошарь [sic] = словарь, etc.

Less well known, and less frequently used because of its complexity, is the complex type, the key to which lies in the following: the letters in the *Church Slavic* alphabet which have numerical value were designated by dots, lines, and circles. The values 1 through 10 were designated by dots:

а в г д е ѕ з и ѳ і

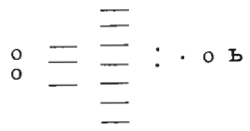
The values 20 through 90 were designated by horizontal lines:

к л м н ξ о п ч

And the values 100 through 900 were designated by circles:

р с т у ф х ѱ ѡ ц

The following letters were not used to designate numbers: б, ж, ъ, ь, ы, ю, я. They remained in place unchanged. Thus, the word словарь written in complex "litoreya" would look like this:



By using this type of secret writing, a person could either create a riddle for his reader, or express his opinion in a manner that protected him from persecution; for example, in a certain ancient Russian manuscript we read the following, which was written in the complex type of "litoreya": "Andrej at the Romanov [monastery] is a knave, and I know that he's a knave; all you priests are thieves." See Vostokov, *Opis. rukop. muzeuma* (1842) and also his *Filologicheskiya nablyudeniya* (1865).

SIGINT WELCOMES INK STAND

[redacted] P.L. 86-36

E12

The intelligence community has come a long way since the days of six-ply paper, MC-88 mills, headsets, and grease pencils in meeting its intelligence objectives. Automated systems now command the field in the collection, processing, displaying, reporting, storing, and management of SIGINT. Systems have been developed that are capable of identifying and exploiting

[redacted]

Each system was developed to contribute to the advance warning of the hostile military "threat" to the United States. We have seen these "project" systems developed, named, *re*developed, *re*named, and then we have seen them meet expectations or, having failed to meet them, be phased out. Yet, through all this, many of us who have had personal contact with these systems have come to cherish them as an exciting experience to be remembered.

There is another automated system in the works which may cause many an old S&WC analyst or reporter to wish it had come along sooner. This new system is known as Project INKSTAND

[redacted]

[redacted]

[1]See: [redacted] "IRONHORSE: A Tactical SIGINT System," *CRYPTOLOG*, October 1975.

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

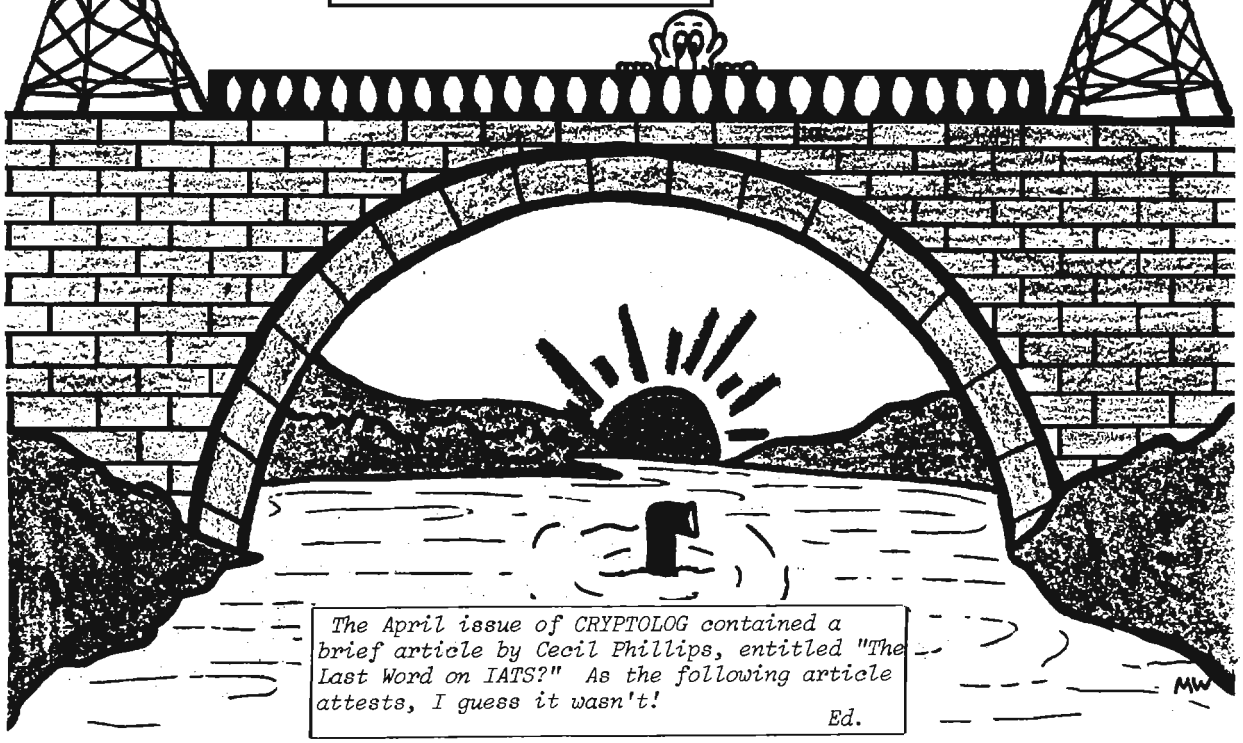
~~SECRET SPOKE~~

AG22/IATS

A VIEW FROM THE BRIDGE

[redacted] G5 ADP

P.L. 86-36



The April issue of CRYPTOLOG contained a brief article by Cecil Phillips, entitled "The Last Word on IATS?" As the following article attests, I guess it wasn't!

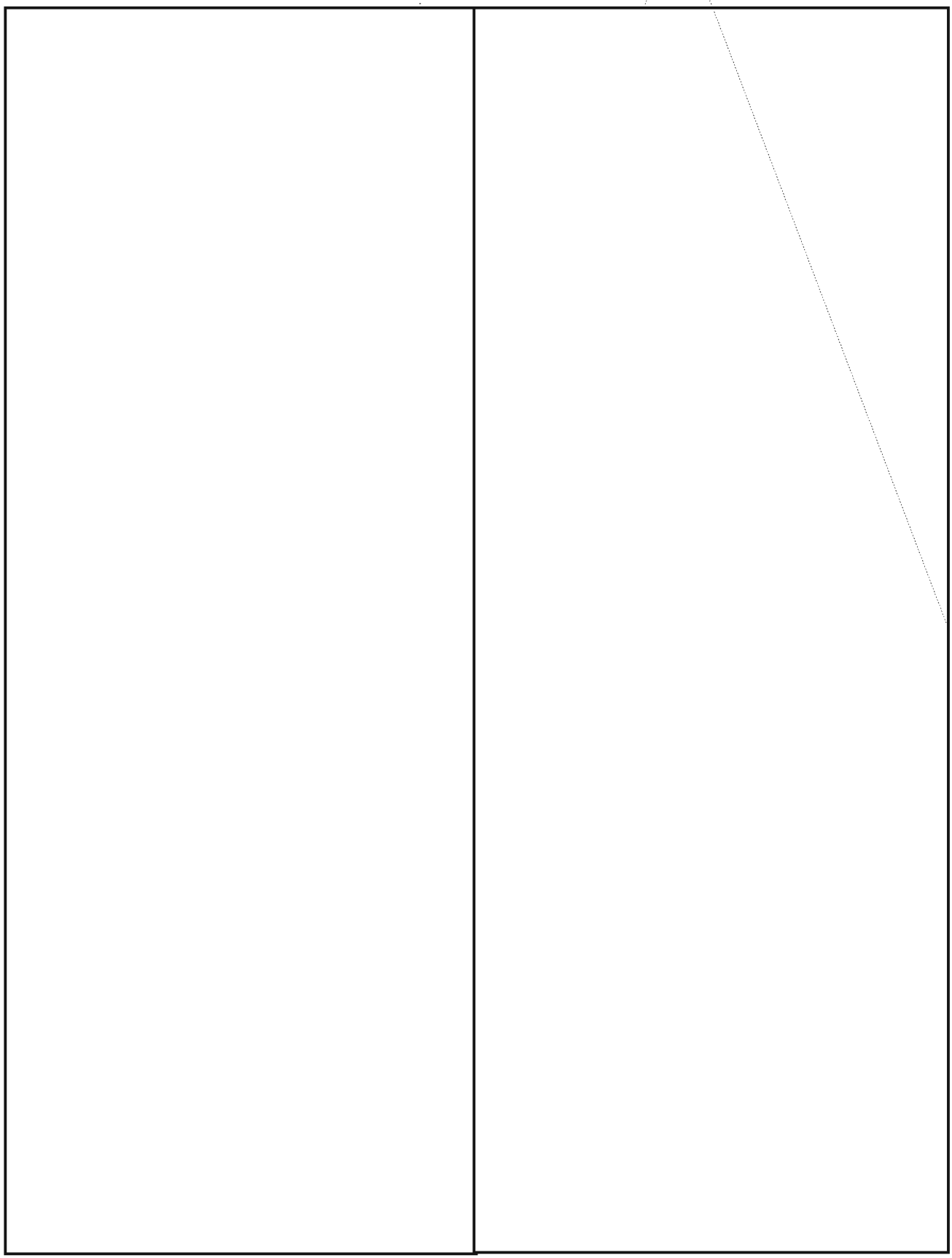
Ed.

~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36

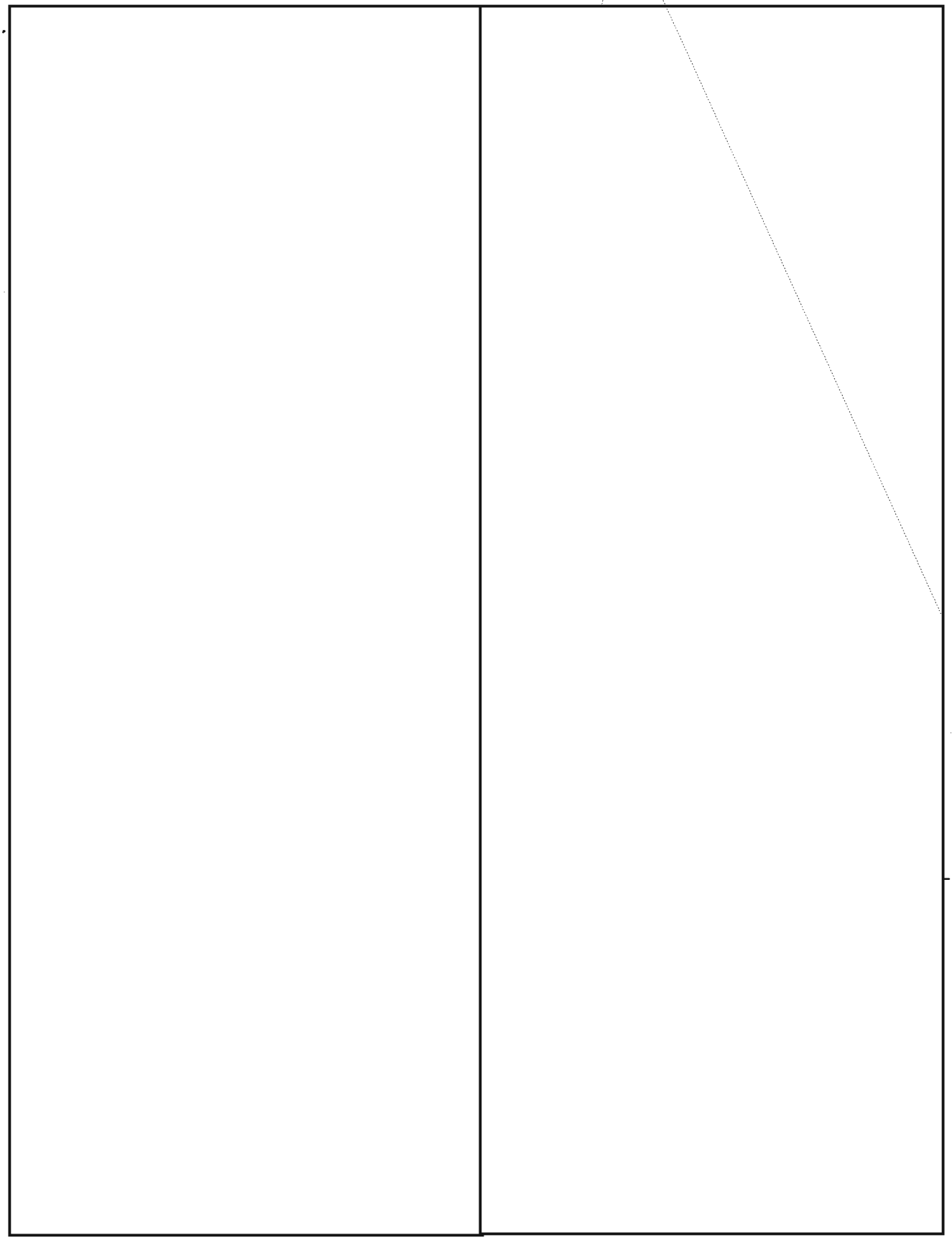
EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~



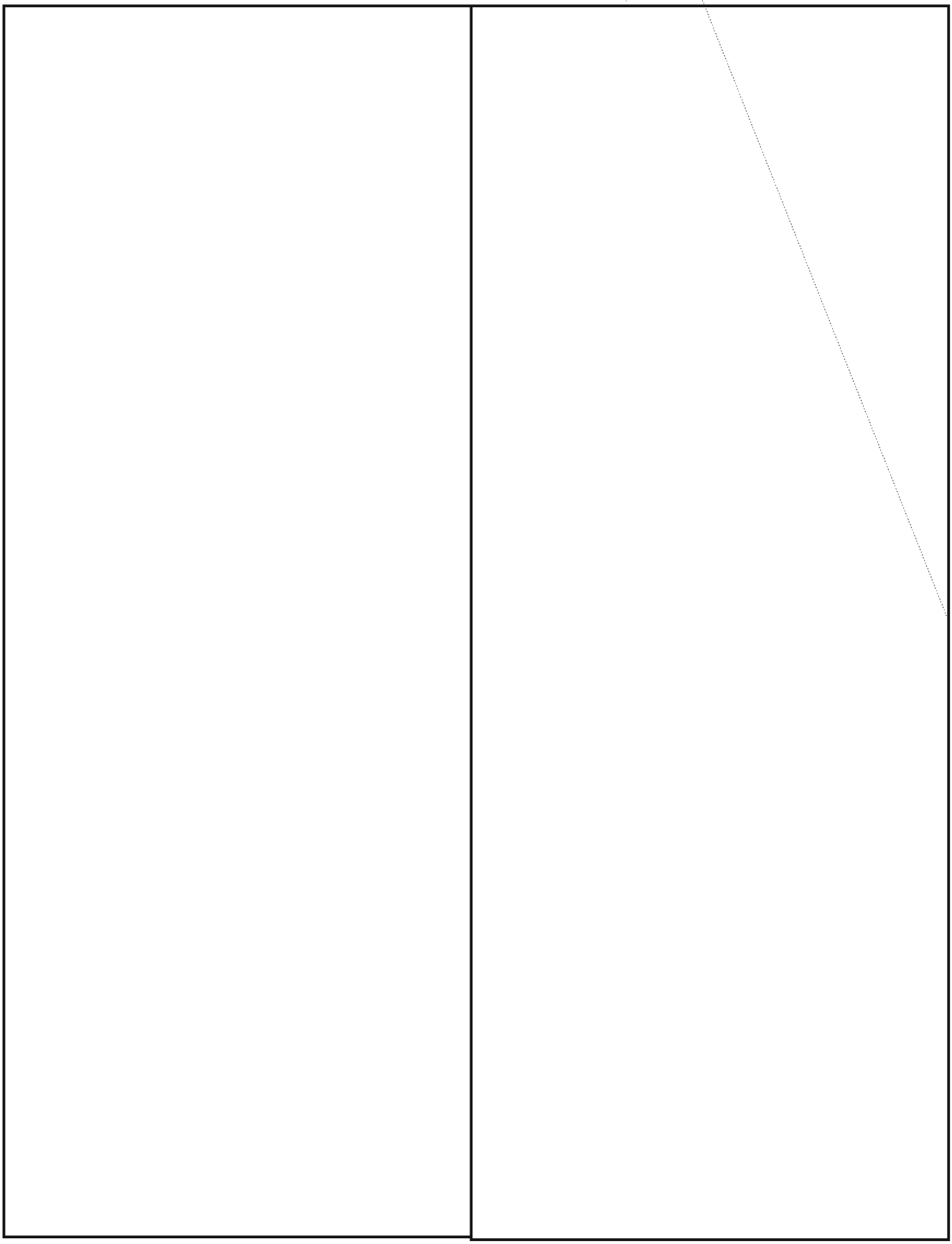
EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~



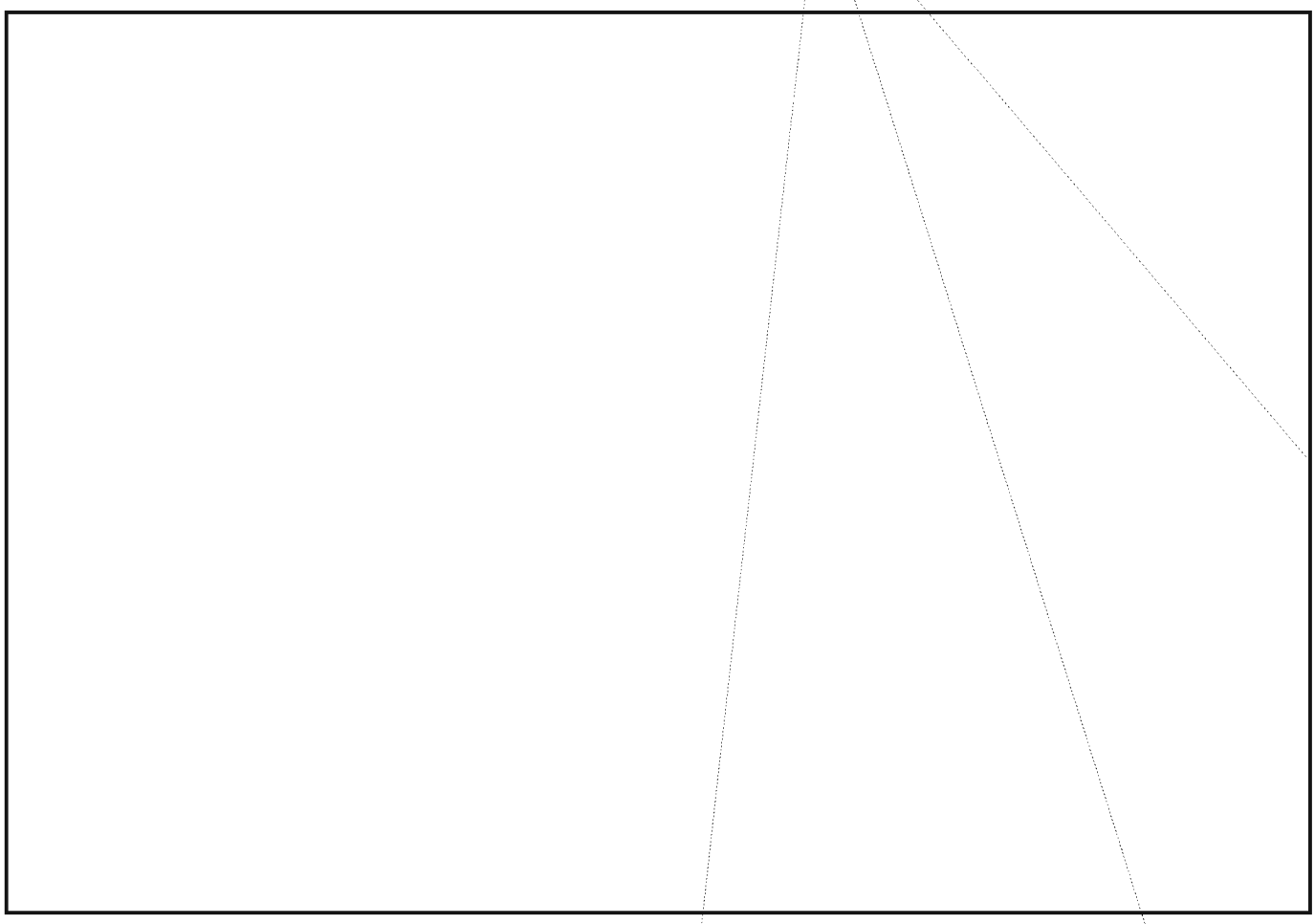
DOCID: 4009797

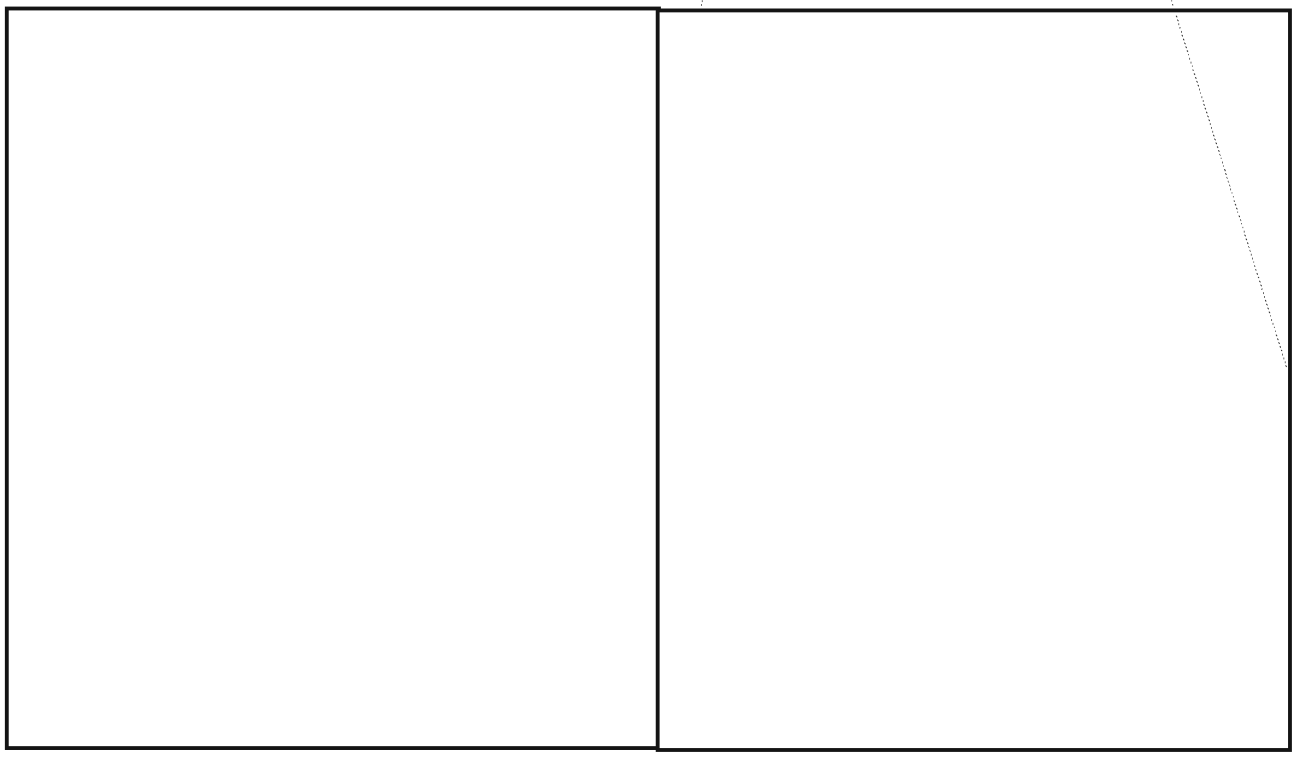
EO 1.4.(c)
P.L. 86-36



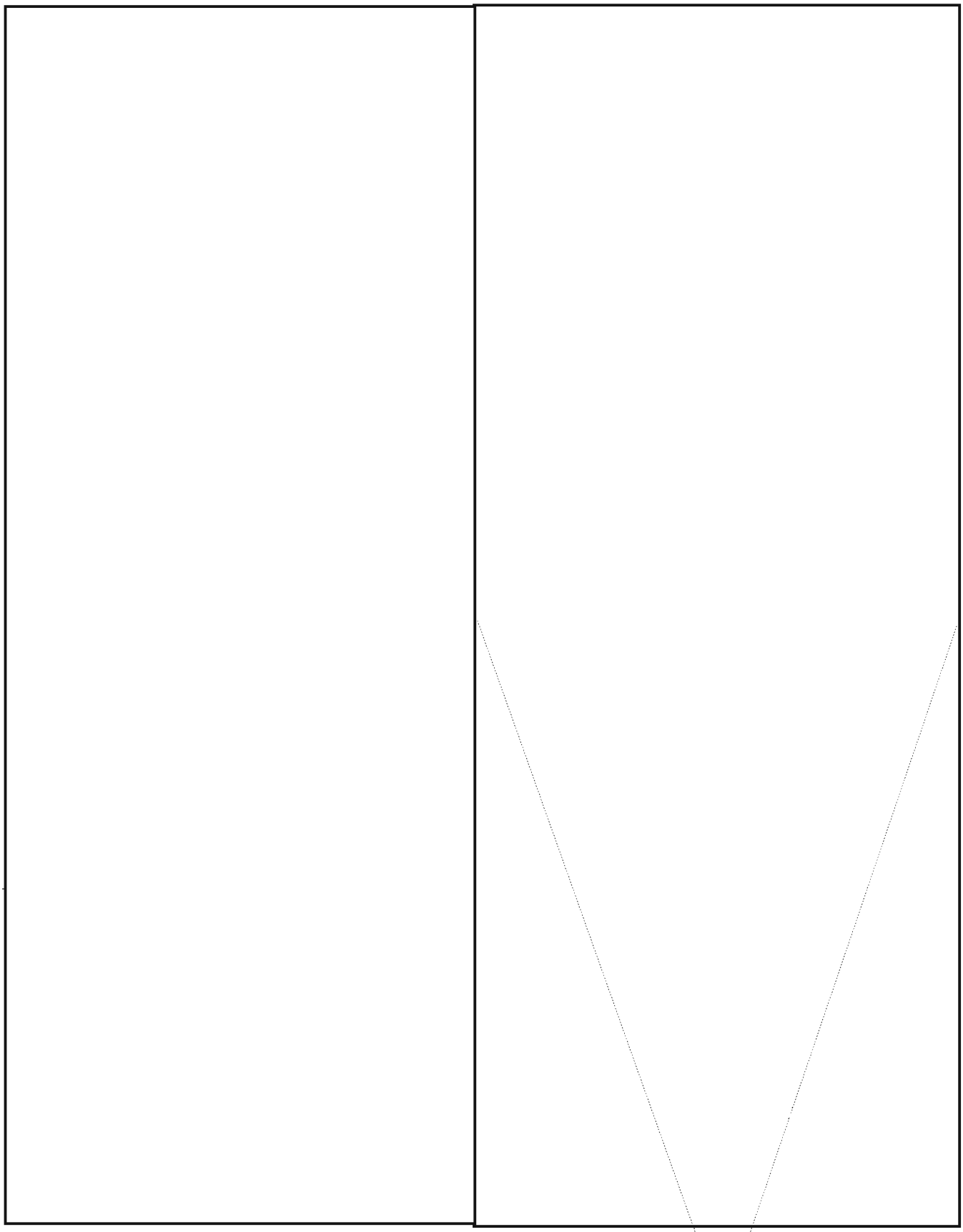
~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36

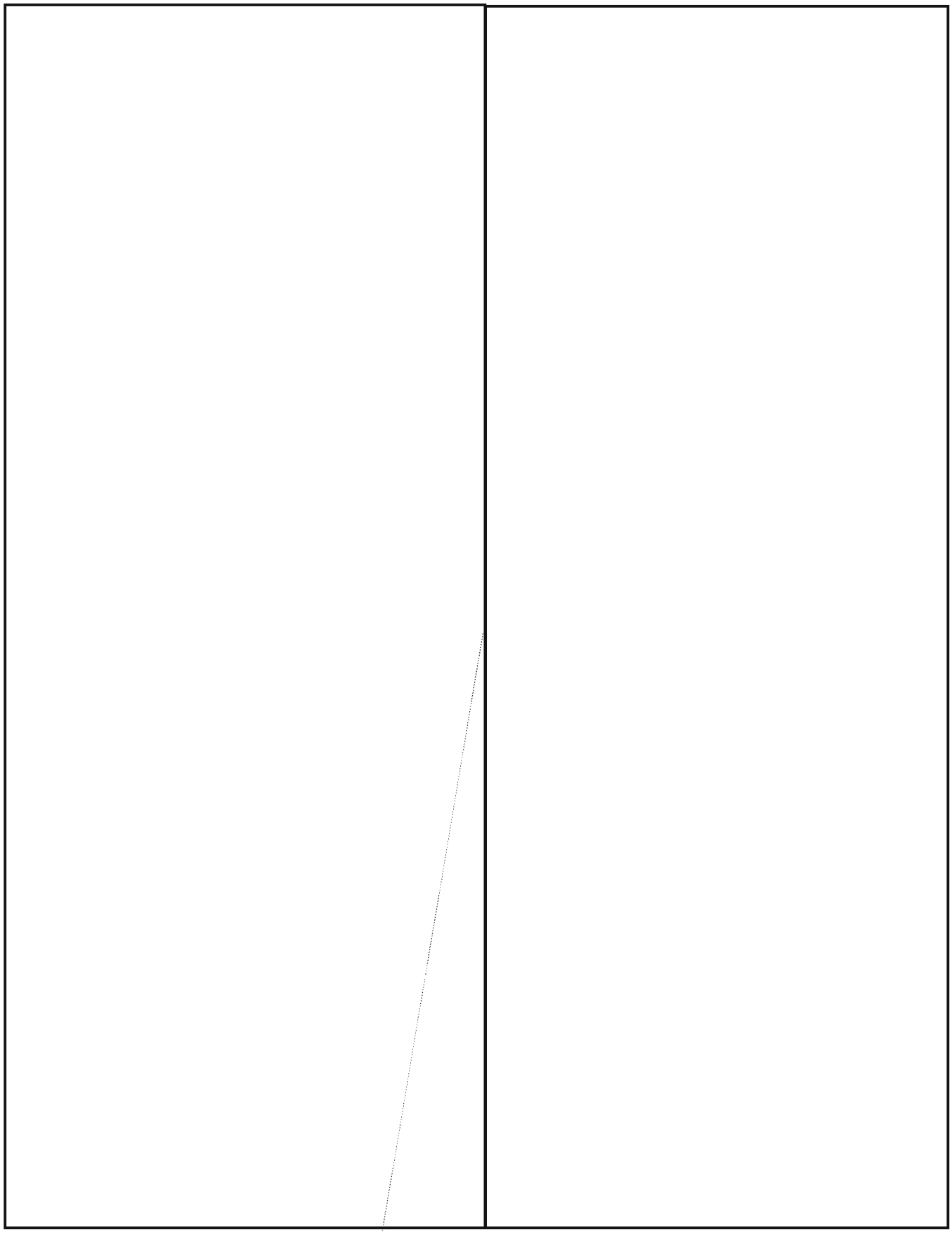




~~SECRET SPOKE~~



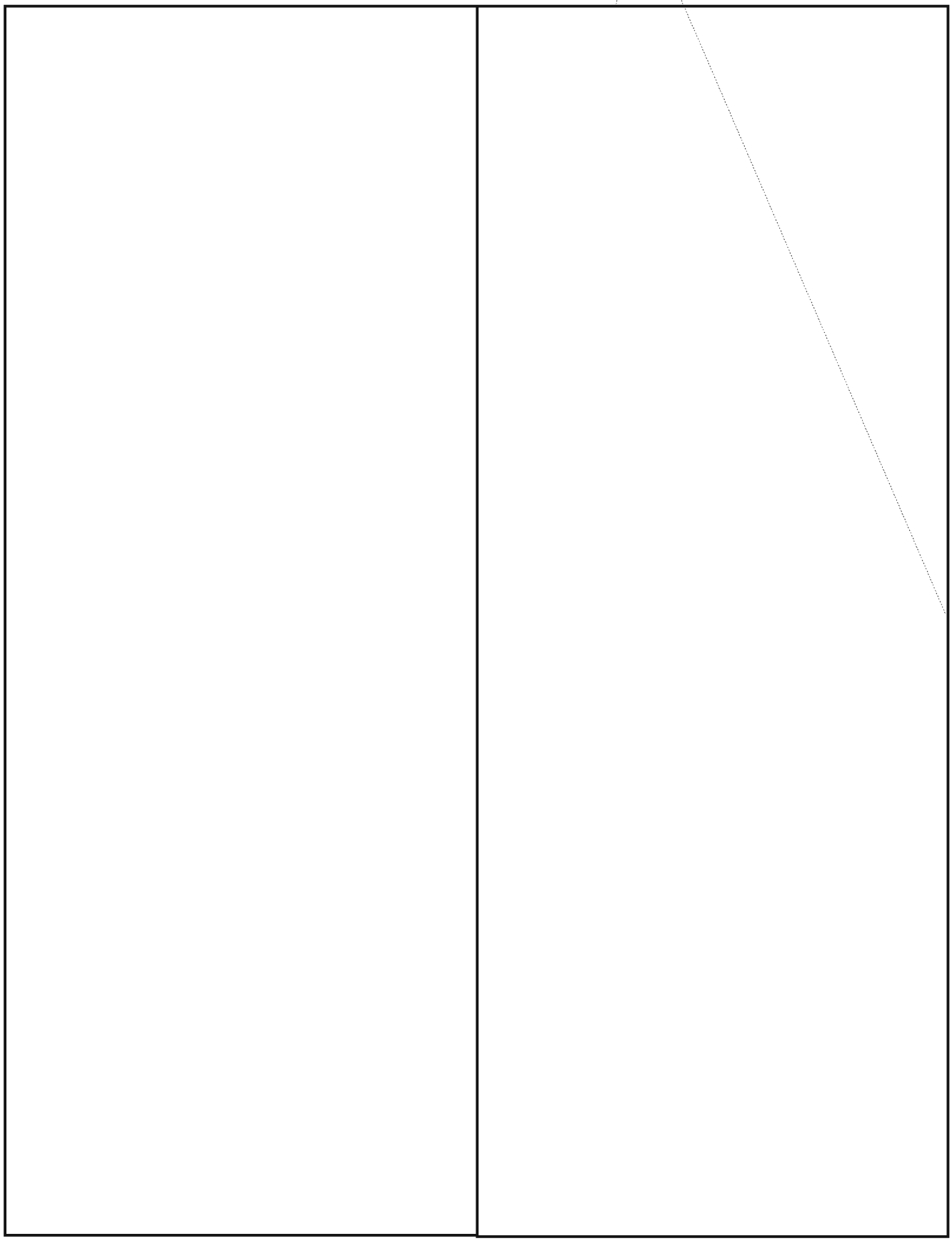
EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

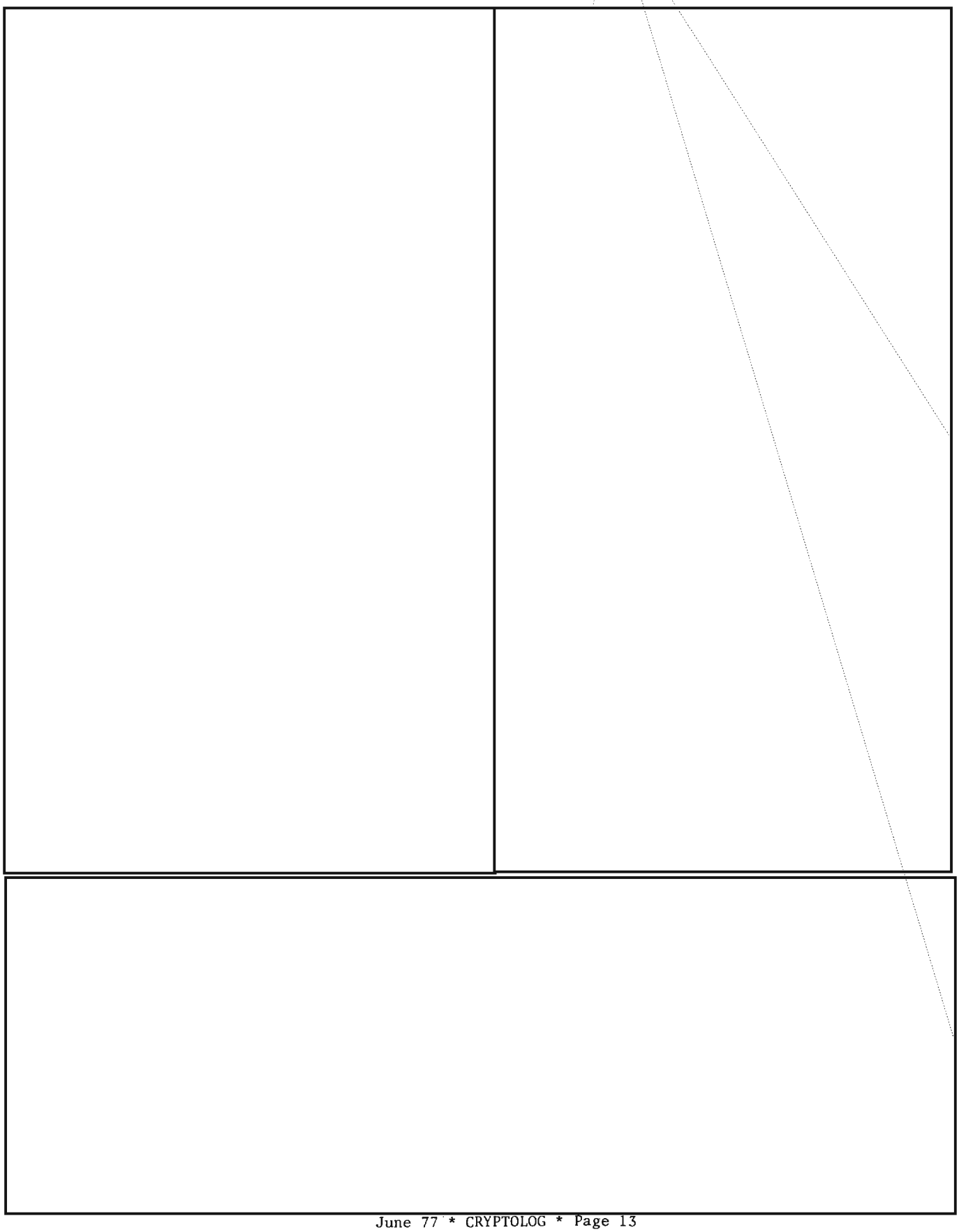
DOCID: 4009797

EO 1.4.(c)
P.L. 86-36

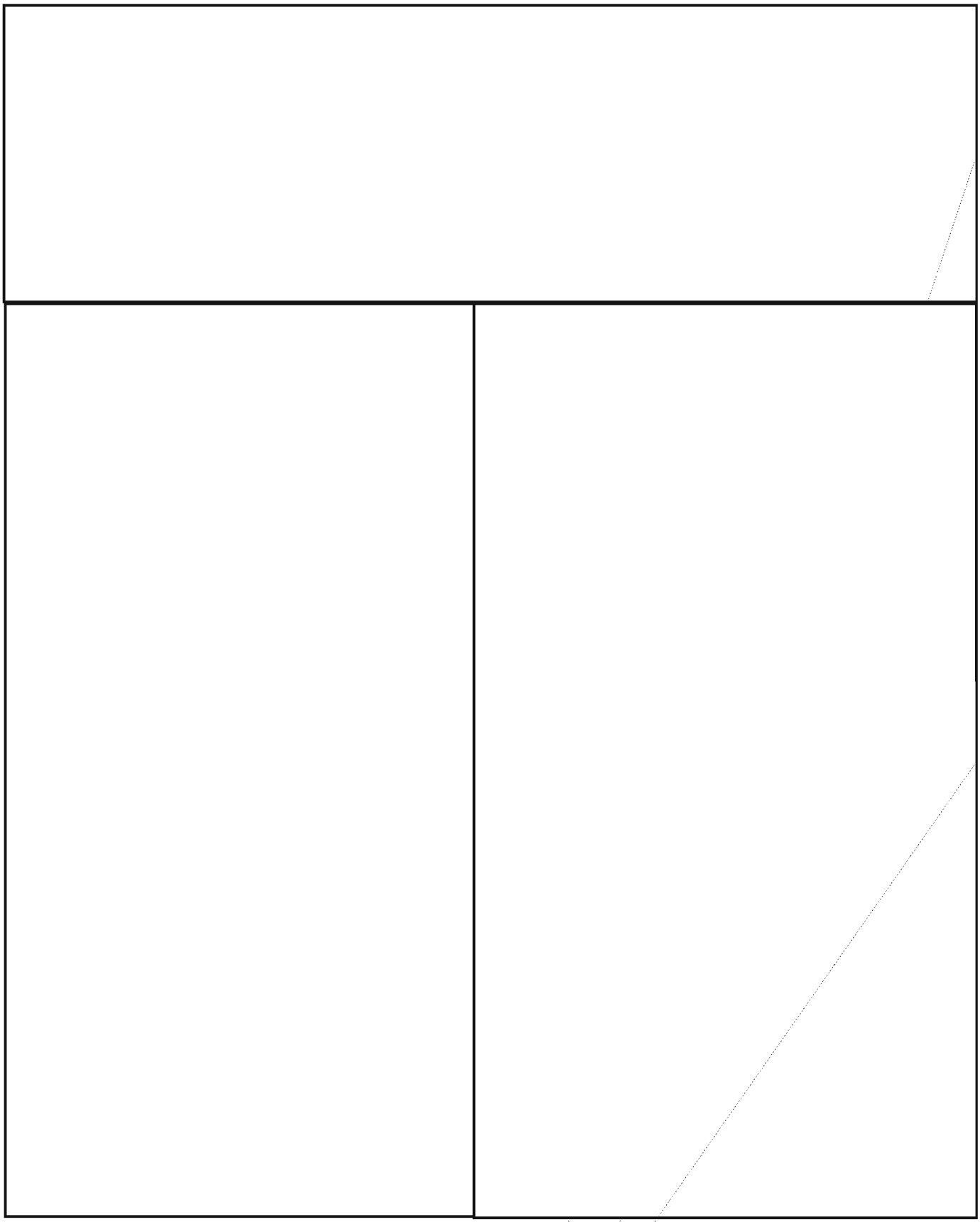


DOCID: 4009797

EO 1.4.(c)
P.L. 86-36



~~SECRET SPOKE~~

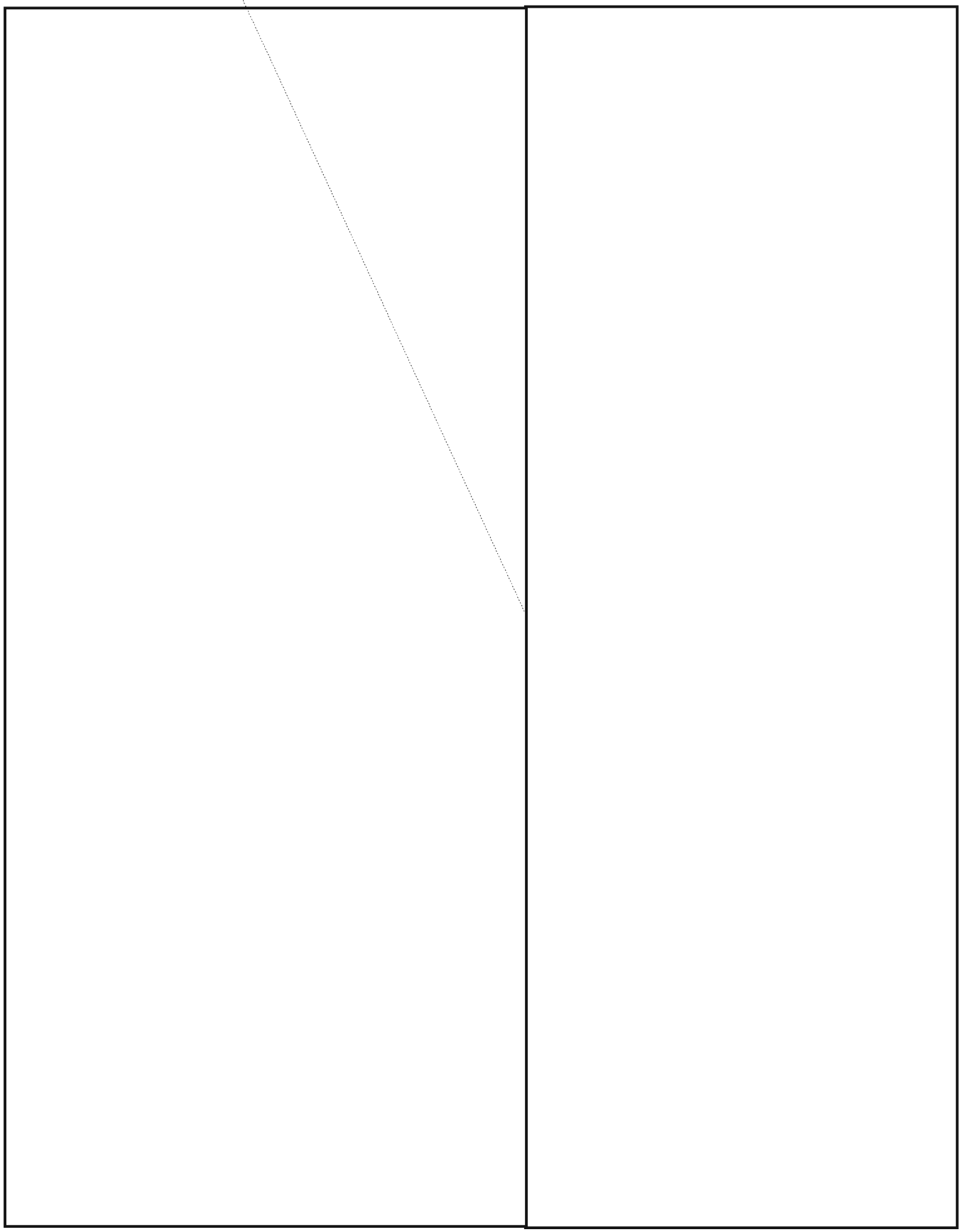


~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4009797



Bibliography (in chronological order)

GAPS Documentation, July 1974.

"More Timely AG-22/IATS ADP Support," AG-22/IATS Processing Study Group, 8 October 1975.

Cecil Phillips, "Musings About the AG-22/IATS." *C-LINERS* (C Group Machine Processing Information Bulletin), Vol. 3, No. 7, August/September/October 1975. Reprinted in *CRYPTOLOG*, March 1976.

[redacted] "What's Wrong with AG-22/IATS?", *C-LINERS*, Vol. 3, No. 8, Winter 1975. Reprinted in *CRYPTOLOG*, May 1976.

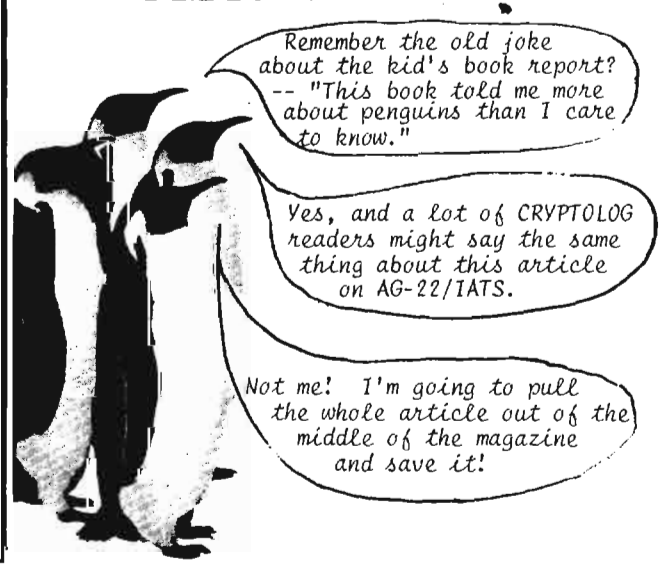
"Comments as Requested (More on the AG-22/IATS)," *CRYPTOLOG*, June-July 1976. Individual comments by [redacted]

[redacted] ". . . And *Still* More Comments! (On the AG-22/IATS Question)," *C-LINERS*, Vol. 3, No. 9, Spring 1976. Reprinted in *CRYPTOLOG*, September 1976.

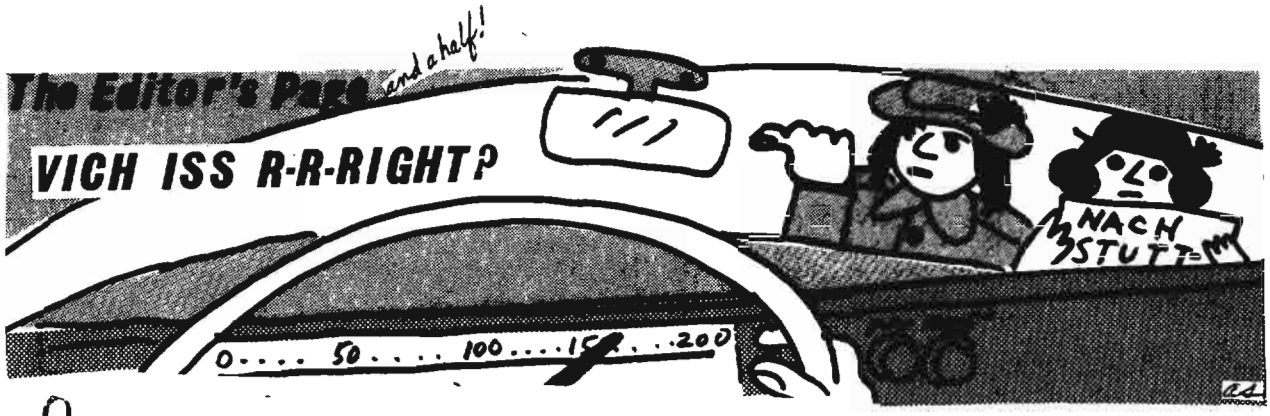
[redacted] "Another Word on AG-22," *CRYPTOLOG*, October 1976.

Cecil Phillips, "The Last Word on IATS?", *CRYPTOLOG*, April 1977.

P.L. 86-36



DOCID: 4009797



Several years ago a friend and I were chit-chatting when another person whom he knew joined the group. After introductions, the three of us carried on some more light banter, during which I noted a quizzical expression on the new person's face several times. The next day my friend told me that, after I left, his friend had said, "You know, for a linguist, that Mr. Salemme really uses atrocious grammar." "Like what?" "Well, he kept saying, 'Don't that beat all!' and 'Ain't that the truth!'"

Well, lately I've been noticing the same expression on people's faces when I used the word *kil*ometer, and I've decided that it's not quizzical but pitying. People used to come right out and say, "The correct pronunciation of the word is ki*lo*meter!" We'd fight about it from various angles, with me contributing wisdom and reasonableness and my opponent contributing non sequiturs like, "But it's ki*lo*metro in Spanish. . ." Then we'd retire to neutral corners and each feel good about being right. But now people just put that pitying look on their faces and don't want to talk about it. So, since I can't defend myself face to face, I'd like to use this means of putting into written form (*Congressional Record* please copy) my views on the *kil*ometer vs. ki*lo*meter controversy.

If language were logical. . .

If language were logical, I'd use the following argument. I'd break the word kilometer into two components. I'd say that in every word with the combining form "kilo-" (meaning "thousand units" in the metric system), the main stress is always on the first syllable (with a secondary stress on the second component of the word). These words include:

*kil*oampere	*kil*ogauss	*kil*oparsec
*kil*obar	*kil*ogram	*kil*oton
*kil*obuck	*kil*ohertz	*kil*ovar
*kil*ocalorie	*kil*ojoule	*kil*ovolt
*kil*ocycle	*kil*oliter	*kil*owatt

Then I'd say that the English words ending in "-meter" fall into three separate and distinct categories according to meaning. They are:

- units of poetic meter (number of metrical feet per line of poetry);
- measurement devices (devices to measure length, height, width, pressure, etc.);
- units of measurement in the metric system.

I'd dispose of the first category cavalierly by saying that *everybody* knows that in such words the stress always falls on the syllable in front of the "-meter." For example,

anapestic *dim*eter
trochaic *trim*eter
dactylic hex*am*eter

I might even mention, in passing, that I'm still looking for a person who *must* exist -- a person named Bickford Pentameter. When he is finally pointed out to me, I'm going to go right up to him and say, "You look just like Bick Pentameter!" and wait for him to reply, "I *am* Bick Pentameter!"

Then, swinging back to the main argument, I'd say that words ending in "-meter" and designating *devices* also have the stress in front of the "-meter." I'd give examples like:

bar*om*eter
ther*mom*eter
spee*dom*eter
sphygomoma*nom*eter
alt*im*eter
*volt*meter
alcoho*lom*eter, alcoho*lim*eter (also *al*coholmeter)

Then I'd say, "Plus innumerable other ones," meaning that I couldn't think of any more. I might, to be intellectually honest, mention as a sort of exception:

drun*kom*eter, *drunk*ometer

but I'd weasel out of that by asking my opponent to just imagine a sheriff in a speedtrap town saying, "Wal, we'll jes' see what our li'l ole drun*kom*eter says about that." Nope, it just don't sound right.

Finally, getting closer to the end of my oh-so-logical argument, I'd say, "But words designating *units of measurement* in the metric system have a primary stress on the first component and a secondary stress on the "-meter." Like:

*cen*timeter	*mil*limeter
*dec*imeter	*mic*rometer

And when I got to *mic*rometer, I'd say, "Gotcha!"

Because, as a unit of measurement (equal to one millionth part of a meter), it's pronounced *mi*crometer, but as a gadget for measuring small tolerances, it's a different word, micr*o*meter!

With my opponent hanging on the ropes, I'd use the ultimate weapon -- sarcasm. I'd say, "You don't *really* mean to tell me that you're using that laissez-faire Webster's *Third* as an authority, do you? With its kilometer-shmilometer attitude toward pronunciation? Just look at the Webster's *Second* (three cheers for the Puritan ethic!), where the pronunciation of kilometer is shown as '*kil*ometer; sometimes ki*lo*meter by false analogy with barometer, etc.' How in the name of Holy Hannah could a person with *your* astuteness make a (snicker, snicker!) 'false analogy' between a *unit* of measurement and a *device* for measurement?"

I would then, ladies and gentlemen of the jury, sum up the argument by saying, "The only sensible pronunciation is *kil*ometer."

But language isn't logical. . .

But language isn't logical, so I think I'd say, "So what if every word beginning in 'kilo-' is stressed on the first syllable -- couldn't ki*lo*meter be an exception?" Sure it could! Who says that life doesn't have exceptions? Couldn't a certain country have 37 varieties of snakes, only one of which is poisonous? Could a person have four brothers, only one of whom has red hair? So why couldn't ki*lo*meter be an exception -- the only word with "kilo-" accented on the *o*? Sure it could!

And so, if you think it sounds "nicer," "more correct," "more European," or just plain like the sound of it because there's a word ki*lo*metro in Spanish, go right ahead and pronounce it ki*lo*meter. I really don't mind. Say it! Ki*lo*meter, ki*lo*meter, ki*lo*meter -- see, I'm not flinching! But although I say it's okay for you to say it your way, please don't try to make me say it your way too.

Back to the neutral corners. . .

I know it's going to be hard for you to accept my sanctimonious understanding of your aberration (cf. *Games People Play*), so why don't we declare a moratorium on the word? Why don't we use a word that every American ever stationed in Germany uses, a word that probably has already, like the expression "No sweat!", entered the German language too. It's the word "click." No American in Germany says, "It's 60 kilometers to Stuttgart." It's always "60 clicks" or "60 K's." Instead of saying ki*lo*meters and looking at me funny when I say *kil*ometers, why don't you just use the word "click"? Think how good you'll feel, using a word correctly even before it's listed in the dictionary! And how stunned you'll be, years from now, when you read in Webster's *Fourth*: "Click; also, by false analogy with kilometer, klick. . ."

(UNCLASSIFIED)

LETTERS

To the Editor, CRYPTOLOG:

In your March 1977 issue you published a letter by Dan Buckley which demonstrated several common misconceptions concerning linguists working at NSA and one misconception in particular -- that linguists simply turn "foreign sounds or words into English sounds or words." Mr. Buckley feels that a "single-language linguist" hardly deserves to be promoted into the supergrades for performing such a simple task. He conveniently places all "highly skilled single-language linguists" into one group and assumes that they all do the same job. He labels them "desk linguists," which reinforces the idea that they are something less than a "real linguist." I cannot speak for all the linguists in the Agency, but I do know that the linguists in A64 should be highly insulted by Mr. Buckley's ignorance concerning the work that the "desk linguist" does for the Agency.

We in A64 are charged with the daily task of, as Mr. Buckley so generously puts it, "turning foreign sounds or words into English sounds or words," a skill so simple that we are going to be replaced by high-school graduates at grade level 2, in Mr. Buckley's opinion. This seems quite silly, considering that most individuals in A64 have at least the equivalent of 4 or more years of formal language education. This often includes a general literary knowledge as well as a special technical knowledge in a particular language. But even this is not enough to step into a "desk linguist's" job in A64. Sometimes it takes as much as 2 years' experience before a "desk linguist" is doing a halfway competent job of turning "foreign sounds or words into English sounds or words."

P.L. 86-36

Mr. Buckley wrote his letter to criticize an article (written by [redacted] and published in the December 1976 CRYPTOLOG) which advocates promotions into the supergrades for linguists. Mr. Butcher was quite specific on why the linguist deserves promotions into the higher grades. However, Mr. Buckley appears to have missed the point, so perhaps I can clarify the situation for him.

Besides having a mastery of the language, the "desk linguist" in A64 often requires a special

DOCID: 4009797 P.L. 86-36
EO 1.4.(c)

and detailed knowledge of a specific target area -- knowledge that is not easily acquired and that can be very technical.

[redacted]

Thus this simple task is not quite as simple as Mr. Buckley would have us believe. It requires a variety of skills, including a great deal of experience. I would venture to say, although there is no way to prove it, that an NSA linguist's job is never as easy as "turning foreign sounds or words into English sounds or words."

But Mr. Buckley will not admit this, and would rather lose these hard-earned skills than promote linguists beyond grade 12 . Unfortunately, it also appears that Agency management agrees with him. Thus, linguists flee to other disciplines in hope of promotions and other rewards, and this results in a significant loss of manpower and skills. Then the Agency scurries to hire more linguists, wondering why it's impossible to keep up with the drain. This method of operation has its costs. Recruiting, hiring, and training new linguists is not cheap. But it seems that the Agency prefers to put money into recruiting new linguists, rather than using that same money to keep experienced ones on the job.

It is also interesting to note that the Agency not only limits the promotions and financial rewards for a linguist but also severely restricts the recognition the "desk linguist" in A64 gets for the work he does. Often his work is highly diluted in the final report. Even the work he sends to the analysts will contain only his initials and the analysts may never bother to recognize the contribution. The linguist may put days of work into turning those foreign sounds or words into English sounds or words and then they may not even be recognizable in the final product, if the linguist ever gets the opportunity to see the final product.

Putting all Agency linguists into one pot is hardly fair. But to insinuate that all a linguist does is "turn foreign sounds or words into English sounds or words" is downright inaccurate. The language problem is seldom that simple and linguists should be paid for their special knowledge and skills, even into the supergrades if that is what it takes to keep them on the job. Furthermore, linguists should fill Mr. Buckley's mailbox with reasons why they should be promoted beyond grade level 12. Perhaps he will come to realize that sinking money into recruiting, hiring, training, and waiting for linguists to gain experience is more expensive than making it worthwhile for experienced people to stay at their jobs -- jobs that are not easily refilled. And that *is* the truth, Mr. Buckley!

[redacted]

~~(CONFIDENTIAL)~~

P.L. 86-36

To the Editor, CRYPTOLOG:

[redacted] article on the Russian PQE (CRYPTOLOG, April 1977) was timely, informative, and thought-provoking for all of NSA's Russian linguists. It is to be hoped that those in a position to effect changes will seriously consider those defects which [redacted] article pointed out. Certainly it is to the Agency's advantage to revise and update any test of the importance of the PQE in order to make it fairer to all.

I would, however, like to correct a mistaken impression which [redacted] obviously received from the NCSch course catalog: RS 220 (Intermediate Russian Transcription) has not been given since 1971, and the NCSch has no plans to conduct such a course in the future. One might well ask, why is it listed in the current course catalog? As a result, this means that there not only is no course to prepare a linguist for Part IIa (classified translation), but there is also no course with which one can prepare for Part IIB (classified transcription). It would be most interesting and enlightening to hear from someone in a responsible position as to why this is the case and what can be done about it.

[redacted]

~~(CONFIDENTIAL)~~

~~CONFIDENTIAL~~

The author of the following letter began it by rewriting the first paragraph and some of the second paragraph of an article that appeared in the March 1977 CRYPTOLOG.
Ed.

To the Editor, CRYPTOLOG:

The ~~May 1976~~ March 1977 issue of CRYPTOLOG contained an article by [redacted] ~~CSA/DDF~~, which described in some detail the ~~functions and purposes of the NSA SIGINT Summary. On the whole it was rather complete and quite interesting.~~ ~~But for the~~ Bill Hunt's period between the inception of the SIGSUM and ~~Bill's~~ association with it ~~was~~ But for the period between the inception of a consolidated NSA current reporting vehicle and Paul's knowledge of the SIGSUM — a period of ~~3 or 4~~ several years -- the article provided ~~virtually~~ no information at all. Having, with some others, devoted a part of those years to the business of ~~conceiving and~~ developing the SIGSUM, I am perhaps in as good a position as any to fill in the gaps. In ~~the process, I will also clarify some statements in~~ leaving such a gap, the article was ~~that are~~ unintentionally misleading, made so simply by the fact that ~~Bill~~ Paul had no part in the conception and early development of the original report and therefore could not be expected to know how it all began.

EO 1.4.(c)
P.L. 86-36

In the early ~~1960s~~ 1950's, a number of events occurred which, taken together, had a far-reaching impact on the role NSA was then playing in the ~~U.S.~~ intelligence community.

P.L. 86-36 ~~CONFIDENTIAL~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

[redacted]

Melville J. Boucher, Vl

~~(CONFIDENTIAL - CCO)~~

To the Editor, CRYPTOLOG:

In the list of U.S. naval radio stations during World War II, a couple of stations were missing. The station located on the southern tip of Greeland was called "GAMMATRON" and I am quite positive that the designator was "G" and the call was NTG.

Also missing on the list was U.S. naval radio station Poyners Hill, N.C., which was located about 20 miles north of Nag's Head on the Outer Banks. Its designator was "P," as Mr. McGrillies indicated and the callsign eludes me for the moment. Poyners Hill was turned over to the Coast Guard just after VE Day in 1945 and has totally vanished except for foundations of buildings.

A reunion of former members who were stationed at Poyners Hill was held in September 1976. Only seven members were located for the reunion but we are planning to hold another if we can get additional names and addresses of former personnel. Anyone having served at Poyners Hill, or knowing the whereabouts of anyone who served there, please call me on 796-6528.

P.L. 86-36

[redacted]

~~(CONFIDENTIAL)~~

AN ENTERTAINING EXCURSION with Charles Lacombe
at the 1977 CLA Banquet..."Does Anyone Here Speak Ancient Mayan?"

The date [illegible]* is drawing near!

That's the date of the CLA's Annual Banquet at:
Sheraton-Silver Spring Motor Inn,
Colesville Road, Silver Spring, Md.

Cash Bar - 6:30 p.m.
Dinner - 7:30 p.m.

Dinner is a lavish buffet (roast beef, chicken, etc.), with salad and dessert courses served at the table.

Price, $9.00 per person.

Reservation deadline, Friday, 17 June 77.

* Remember? "12.18.3.17.16 - 13 Men 13 Zotz," in our calendar, comes out to Thursday,

23 June 1977

For reservations, call any of the following:

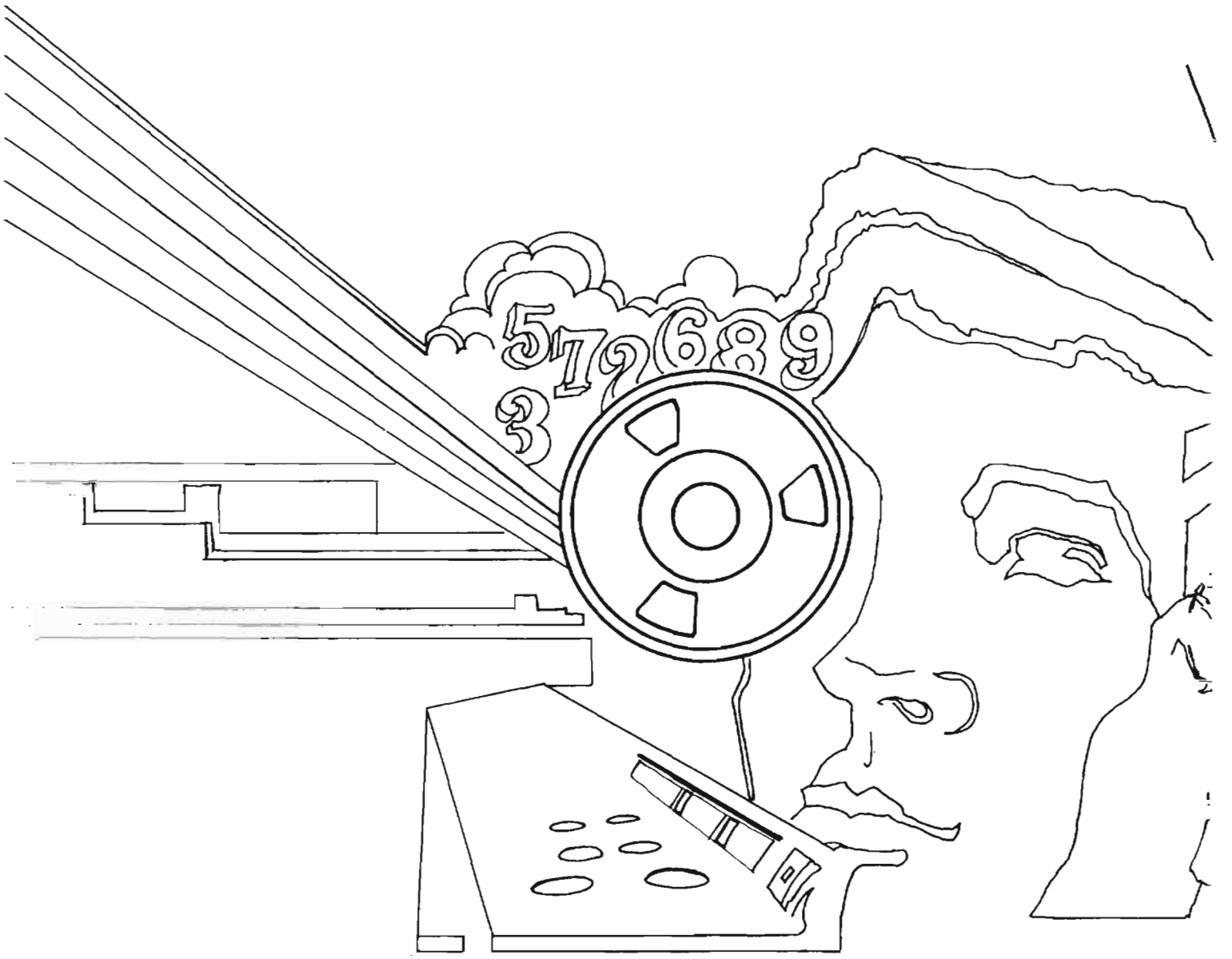
Steve Bladey (Chairman)...5236s
Rose Baruzzi.....4477s

P.L. 86-36

[redacted]...8404s
[redacted]...4966s
[redacted]...4751s

(UNCLASSIFIED)

~~TOP SECRET~~



DOCID: 4009794

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MAY 1977

UNIVERSES, GALAXIES, ETC. (UGSBOC!).....Cecil J. Phillips.....1
SIG/IPS ANNOUNCEMENT.....8
WHY ARE THESE PEOPLE SMILING?.....Mary Ann Harrison.....9
CLA BANQUET ANNOUNCEMENT.....12
CONTROVERSIAL BOOK ON ARTIFICIAL INTELLIGENCE..[redacted]..13
THE POLYHEDRAL WAR.....[redacted]...17
PLAIN ENGLISH.....[redacted]...21
A STORY WITH A MORAL.....[redacted].....22
CHOOSE YE!.....[redacted].....27
LETTER TO THE EDITOR.....28

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009794

P.L. 86-36
E.O. 1.4.(c)

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. IV, NO. 5 MAY 1977

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief..... Arthur J. Salemme (5236s)
Collection..... [redacted] (8955s)
Cryptanalysis..... [redacted] (4902s)
Language..... Emery W. Tetrault (5236s)
Machine Support..... [redacted] (5303s)
Mathematics..... Reed Dawson (3957s)
Special Research..... Vera R. Filby (7119s)
Traffic Analysis..... Frederic O. Mason, Jr. (4142s)
Production Manager..... Harry Goff (4998s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4009794

When I was first asked by the SIGIPS program committee to talk about relationships among systems, projects, etc., I almost laughed out loud, because we had wrestled with a similar request by Admiral Phillips a couple of years ago. What made Admiral Phillips' request impossible to answer was that, I presume, he wanted an official reply -- that is, one which had been coordinated with the several thousand people -- almost everyone in the Agency -- who consider themselves systems designers and the like. I am not sure I remember to whom Admiral Phillips' request was addressed, but it was not addressed to C, so we did not answer it.

All of this is by way of explaining that what I am going to say is pretty much my own opinion and that I hope you understand that there is not a single, simple chart which will relate everything. That is, unless we take the simple approach of creating a new project --

standing for "Universes, Galaxies, etc."

Every one of these items I will discuss is multifaceted -- and many are perceived differently by different viewers. Thus, it is not surprising that one viewer can see a pair of projects as badly interfaced and another viewer can see them as having a satisfactory interface.

One more bit of philosophy before I talk about some of the specific projects. I think that project management has a bad side as well as a good side. On the good side, it probably leads to better-defined projects, bounded projects, and, hopefully, to timely and correct completion of projects. On the bad side, it leads to introspective, parochial views of the world and narrow problem approaches. I believe project management needs a little more tempering -- with some input from disorganized geniuses. Don't ask me how to distinguish geniuses from cranks. I don't know the answer to this, but I think we have a lot of both.

P.L. 86-36
EO 1.4.(c)

~~SECRET~~

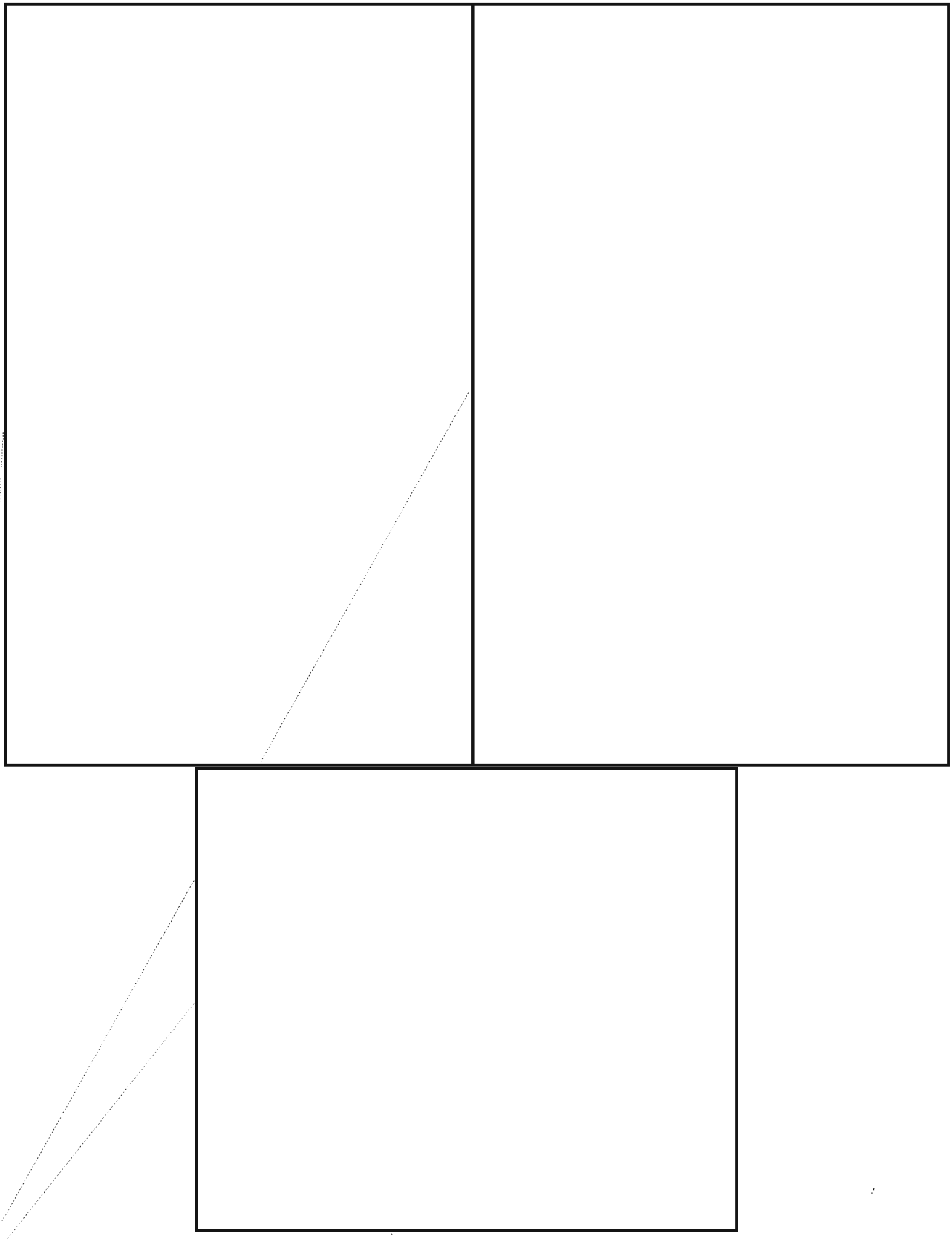
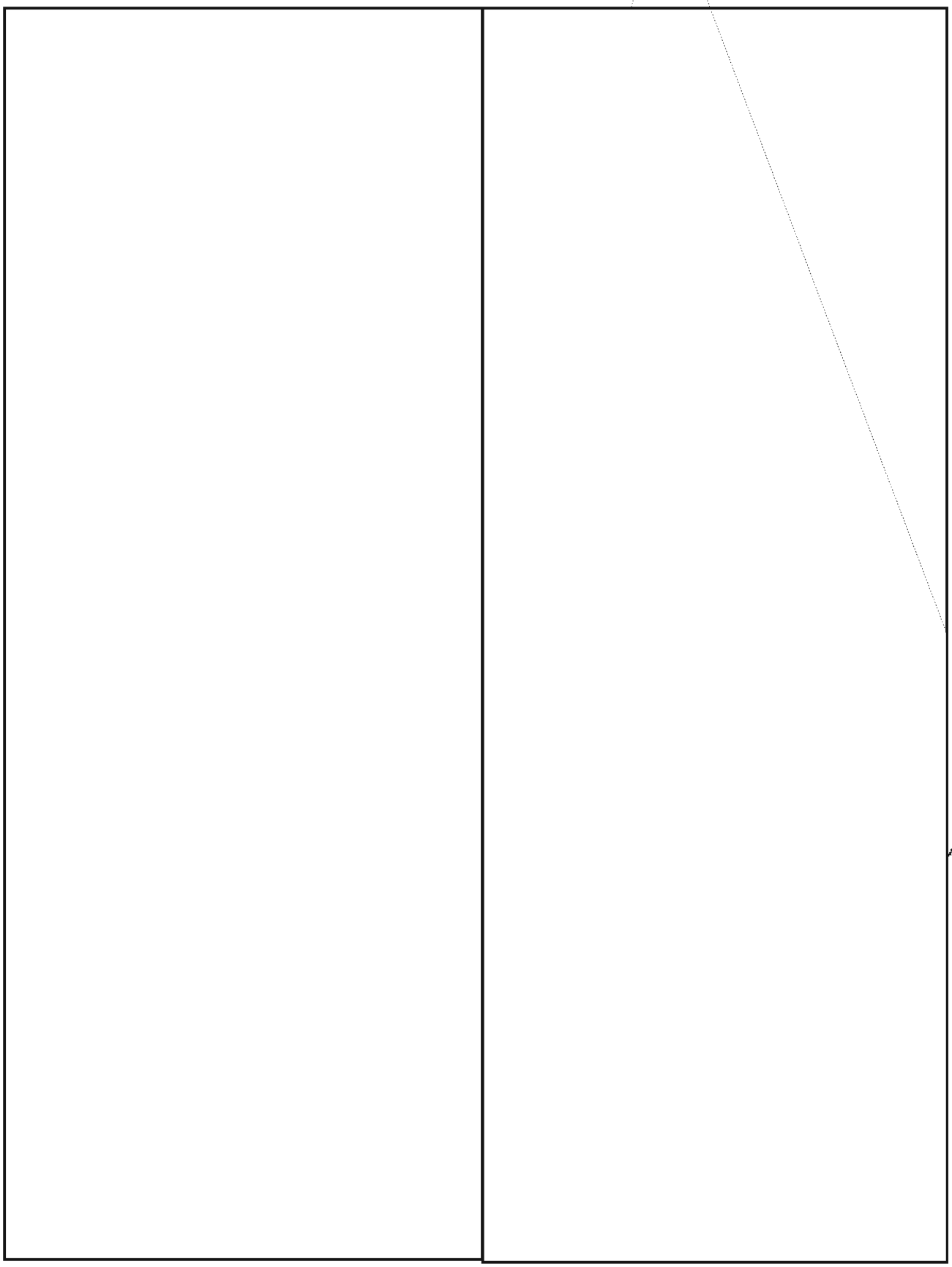


Fig. 2

P.L. 86-36
EO 1.4.(c)

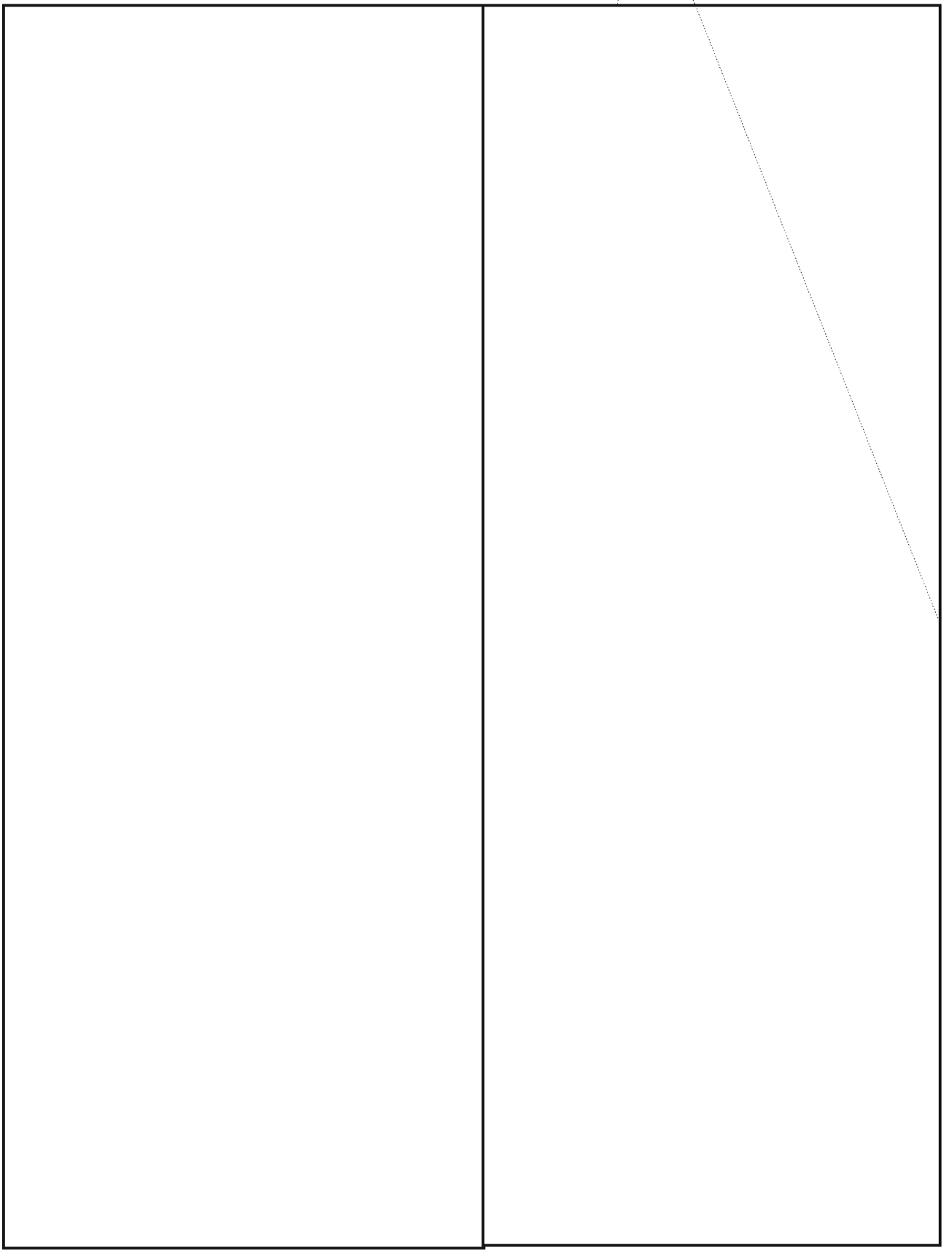
DOCID: 4009794

P.L. 86-36
EO 1.4.(c)



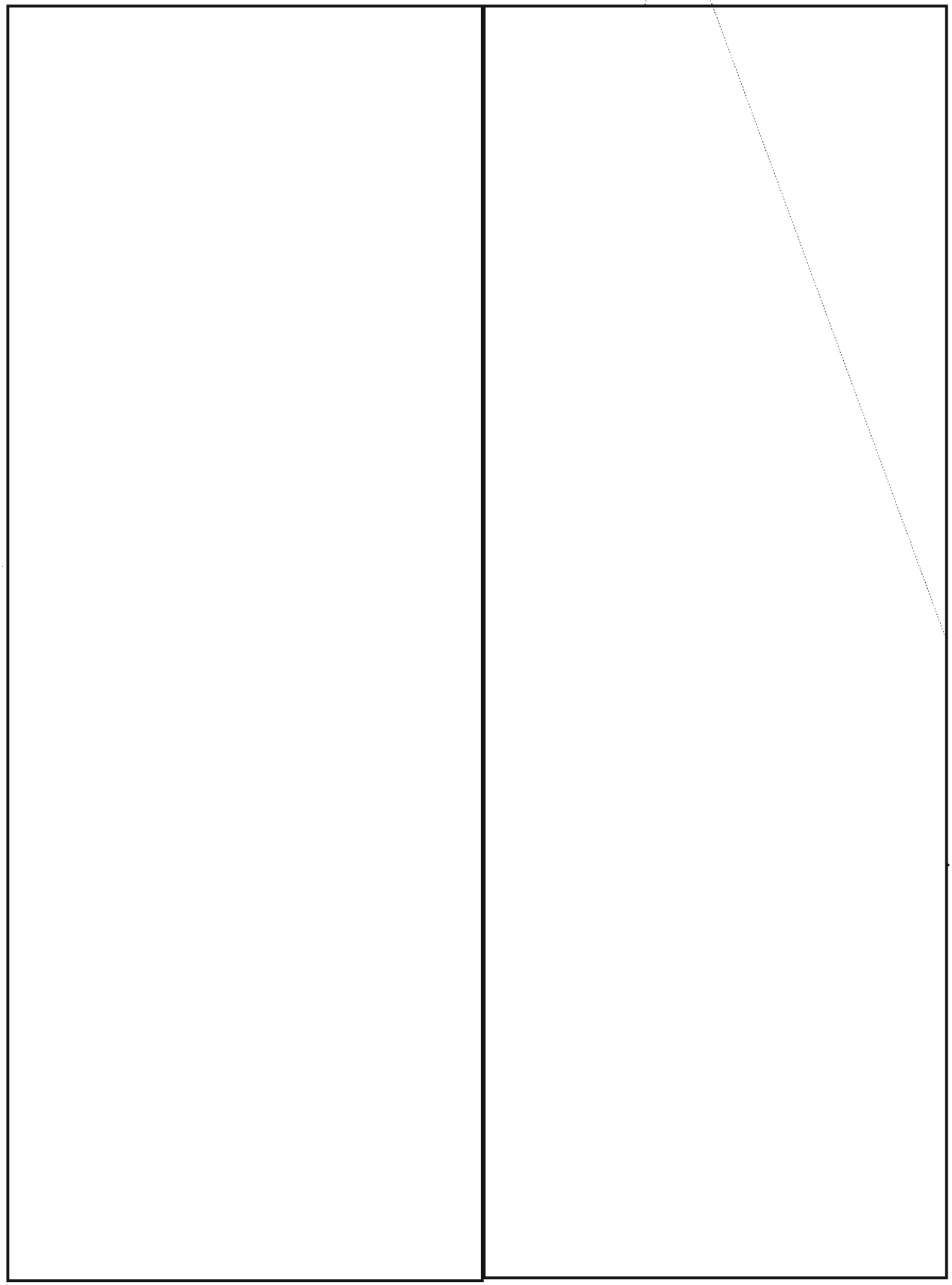
DOCID: 4009794

P.L. 86-36
EO 1.4.(c)



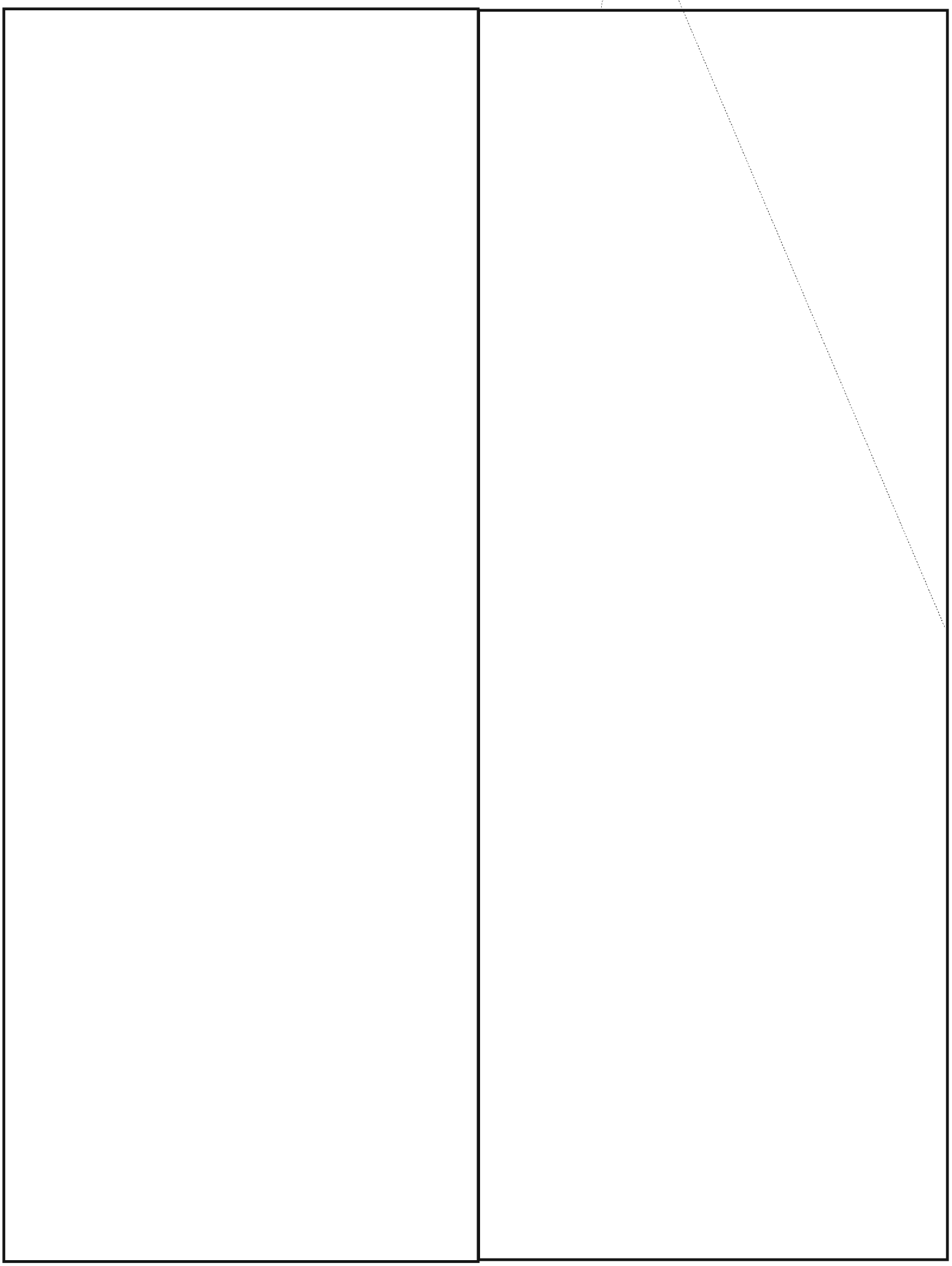
P.L. 86-36
EO 1.4.(c)

~~SECRET~~



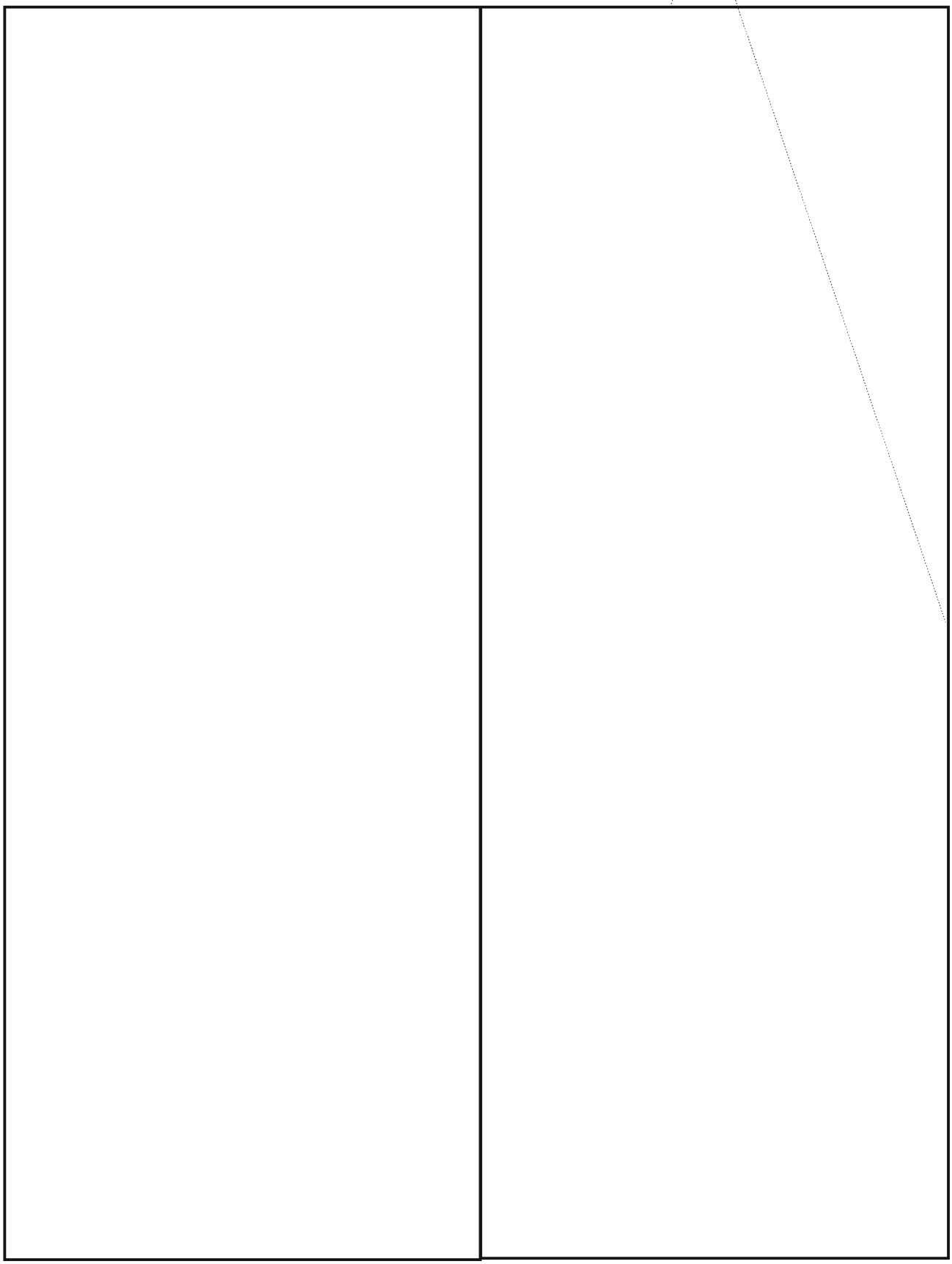
P.L. 86-36
EO 1.4.(c)

~~SECRET~~



DOCID: 4009794

P.L. 86-36
EO 1.4.(c)



~~(SECRET - CCO)~~

NSA CSI

The preceding article is the text of a presentation given by Mr. Phillips to members of the Special Interest Group on Information Processing Systems (SIG/IPS) in August 1976. SIG/IPS is an organization, under the auspices of the NSA Computer and Information Sciences Institute (CISI), which addresses problems and technical developments in the fields of data storage, data processing, and data retrieval.

Mr. Phillips' presentation was one of a series of monthly programs which SIG/IPS sponsors for the benefit of all interested NSA employees. Additional programs include seminars and technical films.

Persons wishing to join SIG/IPS or to suggest topics for programs are invited to contact [redacted] *SIG/IPS Chairman, on x55048.*

(UNCLASSIFIED)

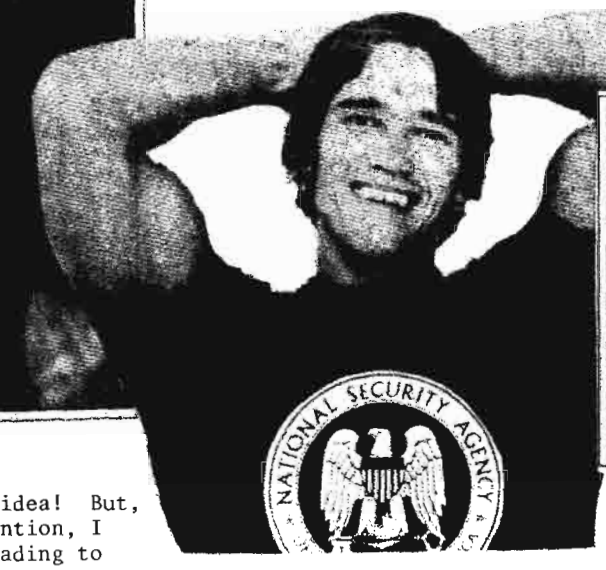
P.L. 86-36

P.L. 86-36
EO 1.4.(c)

DOCID: 4009794

WHY ARE THESE PEOPLE SMILING?

Mary Ann Harrison, A64



Actually, I have no idea! But, now that I have your attention, I hope you will continue reading to find out why certain other people -- the Agency's foreign-language transcribers -- are definitely *not* smiling.

Despite his[1] position as the linchpin in the SIGINT process, the transcriber has for many years been the stepchild of the intelligence-processing family. While most professionals in the SIGINT business acknowledge the importance of transcription, there is widespread lack of understanding and, for that matter, concern about what a transcriber does and what it takes to be a transcriber. Many NSA managers and supervisors, especially those who themselves have no foreign-language training, do not realize how difficult transcription is. In their ignorance they dismiss the work as a purely mechanical function and transcribers as near-automatons.

Unfortunately, this attitude toward transcription is not confined to those in management and supervisory positions. Newly hired linguists are indoctrinated with this negative evaluation of transcription even before they are on the job. It is not unusual to hear recently arrived college-trained linguists say they will quit rather than go into transcription, even before they know what transcription *is*! The anti-transcription virus has apparently spread to recruiting and personnel offices.

Every transcription shop has its own horror stories to illustrate the prevailing ignorance, indifference, and outright hostility to transcribers and transcription. I will not burden you with many of them, but I believe a few excerpts will illustrate my point.

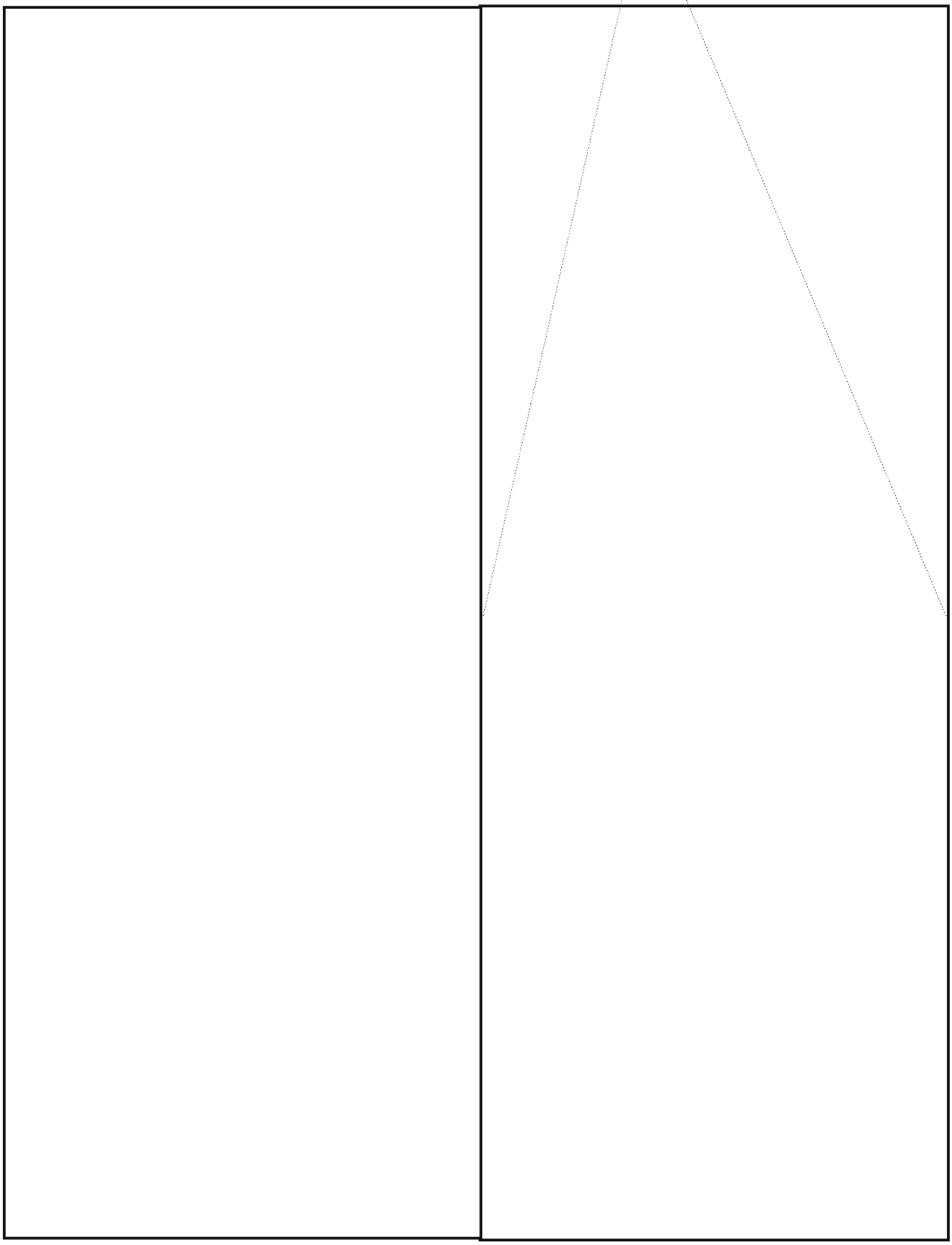
[1] I shall use the masculine forms throughout, in order to avoid the cumbersome "he or she" constructions, and also because the majority of transcribers are, currently at least, men.

EO 1.4.(c)
P.L. 86-36

What other group of NSA professionals has heard themselves described by a senior management official as "plumbers"? The connotation was unmistakable: transcribers are the day-laborers of the intelligence world. Analyst-reporters and others with whom the Russian transcribers work on a daily basis have asked, "Where do you keep your transcribers?" Or have issued instructions to "take these tapes and run 'em through your transcribing machines." There is a real and apparently widespread belief that transcribers do nothing but thread tape through a machine, turn it on, and collect page-print as it pours out the other end. Many of those who understand that a real live human being is involved in the transcription process still fail to appreciate the difficulties of the job. These persons' assessment of transcription is that "any idiot with a dictionary can handle this stuff."

So much for the transcription myth. Now, please allow me to present a thumbnail sketch of who a transcriber is, what he does, and how

EO 1.4.(c)
P.L. 86-36



DOCID: 4009794

EO 1.4.(c)
P.L. 86-36

[redacted]

~~(SECRET GCO)~~

Remember this date!

The date "12.18.3.17.16 - 13 Men 13 Zotz" in the Maya calendar is an important one for those interested in the ancient Maya civilization. On that date Charles Lacombe will make the question "Does Anyone Here Speak Ancient Mayan?" the theme of his speech at the annual banquet of the Crypto-Linguistic Association. Last July, during a visit here from his home base in Miami, Mr. Lacombe, a former NSAer, spoke to a joint meeting of CLA's special interest groups on lexicography (SIGLEX) and translation (SIGTRAN), on computer techniques for decryption of Maya climatic records.

To make your banquet reservation, call Steve Bladey, P16, x5236s.

Oh, incidentally, for those who are a bit rusty on Maya dates, the banquet will be on:

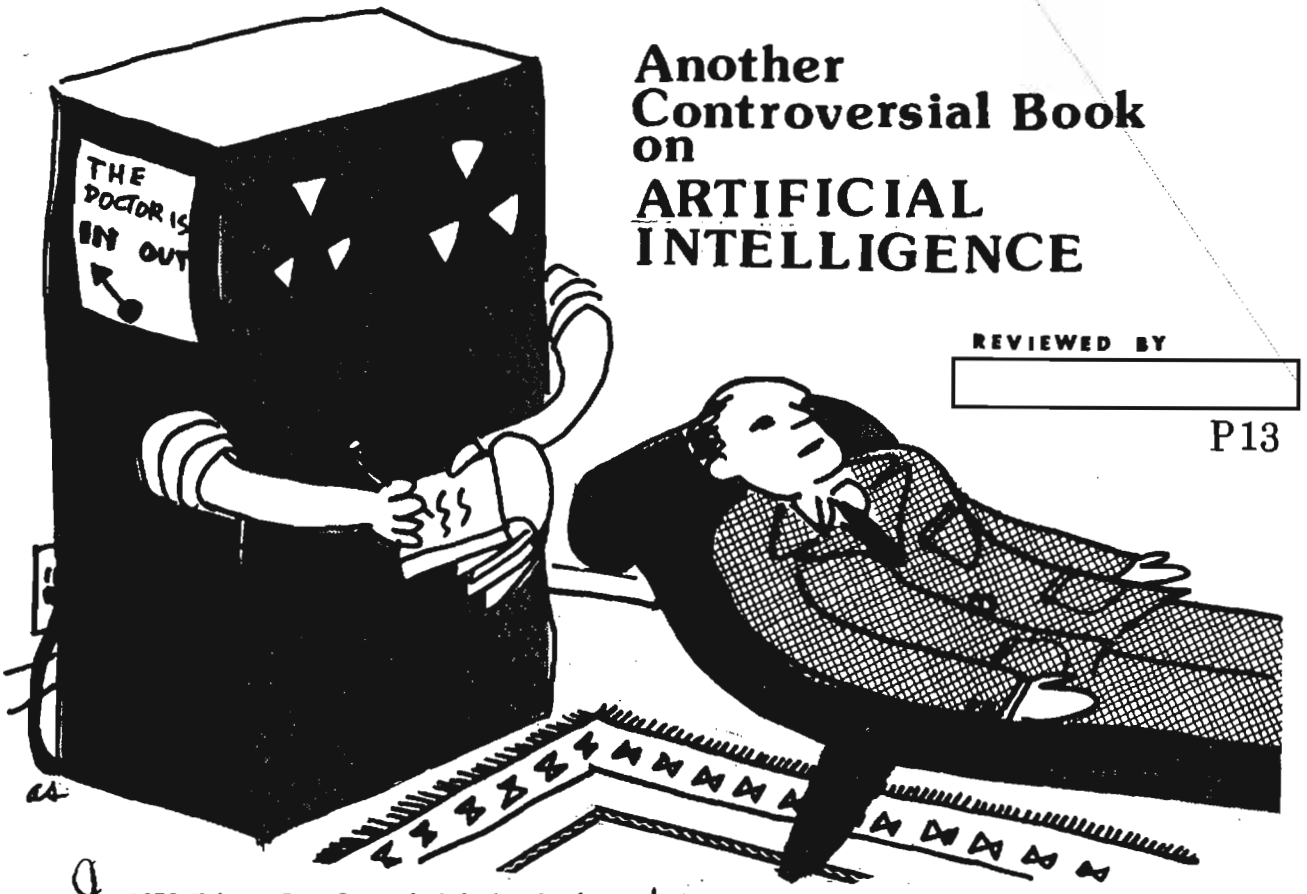
Thursday, 23 JUNE

(UNCLASSIFIED)

DOCID: 4009794

P.L. 86-36

Another Controversial Book on ARTIFICIAL INTELLIGENCE



REVIEWED BY

P13

In 1972 Hubert Dreyfus published a book entitled *What Computers Can't Do* (Dreyfus 1972). This book created somewhat of a stir in computer circles; a number of provocative challenges were made, and considerable healthy and constructive self-examination was stimulated in the minds of many workers in the field of Artificial Intelligence (AI). It seemed that Dreyfus had raised so many basic questions that his book deserved a careful reading by anyone interested in the future of computer science, even if only to strengthen and clarify the grounds for disagreeing with him (see my review, "Machine Intelligence: Promise or Delusion?", CRYPTOLOG, July 1975).

Now we find ourselves challenged again, and this time on even more fundamental and extensive grounds, in a new book, *Computer Power and Human Reason*, by Joseph Weizenbaum of MIT (published by W. H. Freeman and Co., San Francisco, 1976). Dreyfus is a professional philosopher, and his expertise lies entirely outside of computer science; thus, he was assailing the bastions of AI research from an external position. In Weizenbaum, by contrast, we see an insider -- a very highly respected and creative worker in the field of AI research -- breaching the walls of the citadel from within.

Weizenbaum's accomplishments include the development of a useful list-processing computer language called SLIP ("Symmetric List Processor") and various other work centering around the problem of making computers capable of language understanding and other intelligent human activities (cf. Weizenbaum 1963, 1967a, 1967b). Along with his technical work, Weizenbaum has also consistently carried forward an interest in and concern for the social implications of computer technology. Perhaps his best-known AI work was the development of a natural language analysis program called ELIZA, which could carry on a dialog on some preselected topic with a human conversational partner. ELIZA created considerable interest and excitement, and also enjoyed substantial popularity as a demonstration vehicle in computer science centers around the United States, in a version called "DOCTOR," which was programmed to parody the interview of a Rogerian "nondirective" psychotherapist with a new patient.

In his introduction, Weizenbaum sets the stage for the reader by describing his own frame of reference and stating his reasons for writing the book. As a practicing computer scientist, and a teacher of computer science in the great temple of technology which is MIT, Weizenbaum became acutely aware of his students' questions and doubts about the value of what they were learning and doing. On the one hand, they were bending all their efforts toward learning their craft, and many of them were seeking only to increase their dogmatic dependence on and polarization around science and technology. On the other hand, many were aware

DOCID: 4009794

that they were not learning anything that would help them to choose the right questions to ask, or to evaluate the answers they got. Some were rebelling openly "at working on projects that appear to address themselves neither to answering interesting questions of fact nor to solving problems in theory" (p. 11).

In addition to the questions raised in the classroom, Weizenbaum was confronted with a more abrupt and compelling philosophical shock as a result of his work with ELIZA. He saw practicing psychiatrists hailing what was really no more than a technical trick, of parodying one particular interviewing method, as a breakthrough in automated psychotherapy. He was further dismayed to see how quickly and easily people of all walks of life and degrees of education became emotionally involved with ELIZA playing "DOCTOR," accepting it as a therapist, and personifying it to the extent of asking Weizenbaum to leave the room so that they could converse with the "DOCTOR" in private. A third unpleasant surprise emerged when he became aware of a widespread belief that ELIZA represented a general solution to the problem of computer understanding of natural language. These disproportionate overevaluations of his successful but modestly-framed experiment made him realize that most people do not understand anything about computers, and are ready and eager to believe that these magical machines and those who program them can do anything under the sun.

Weizenbaum tells us that he felt himself thus suddenly faced with a terrifying responsibility, that seem to compel him to step back and reconsider in a new light what he had been doing. His book is the result of a 2-year leave of absence from teaching: one year spent at the Stanford Center for Advanced Study in the Behaviorial Sciences, and the other year at Harvard University, both on research grants. His work at these institutions benefited greatly by contacts with many other workers in a variety of fields, some of them well-known authorities, and his manuscript was read and commented upon by these new colleagues.

How have we reached the point where practicing psychiatrists can so overvalue a computer program as a therapeutic breakthrough? What historical process has brought the "man in the street" to the place where he can unquestioningly accept a computer program as an appropriate receptacle for his deepest emotional and personal confidences? Weizenbaum poses these questions and seeks to answer them by tracing the transformations wrought upon human thought and experience through the growth of new tools and techniques that laid the foundations for modern empirical science. He seeks to show that this history, and the particular paths it has taken, have brought us to a scientific outlook that seems to have produced a mechanistic conception of man. We have made ourselves and all our institutions over into the image of the computer. A practicing psychiatrist, under this mechanistic spell, sees nothing amiss in a picture of himself "not as an engaged human being acting as a healer, but as an information processor following rules. . ." (p. 6).

Weizenbaum's trip back into the history of Western thought begins with the clock -- man's first truly "autonomous" machine, capable of running for long periods without human guidance or intervention. He follows Mumford (1963) in stressing the importance of the clock, and its use by medieval monks to time their devotions in the monasteries. With Mumford, Weizenbaum sees the widespread use of clocks and measuring devices producing "pointer readings" and numbers as the cause of a crucial change in man's perception of time and, consequently, of space. The concept of time as disassociated from particular events made possible the creation of "'an independent world of mathematically measurable sequences: the special world of science'" (Mumford's words, quoted by Weizenbaum, p. 23). The clock, as man's first autonomous machine, foreshadowed the programmable computer; both, once started, continue operating "on the basis of an internalized model of some aspect of the real world. Clocks are fundamentally models of the planetary system" (p. 23).

The growth of our dependence on machines of various kinds, and the changes that brought the modern scientific world view into wide acceptance, resulted, Weizenbaum continues, in a wholesale rejection of direct experience. "Gradually at first, then ever more rapidly and, it is fair to say, ever more compulsively, experiences of reality had to be representable as numbers in order to appear legitimate in the eyes of the common wisdom" (p. 25). The value of everything, and especially of human labor, became quantified as money. These developments set the stage for such devout and impassioned statements of the ascetic faith of science as that of Pearson (dating from 1892) which Weizenbaum quotes: "'The scientific man has above all things to strive at self-elimination in his judgements'" (p. 25). This statement, as Weizenbaum points out, urges man to make himself into a disembodied intelligence, a sort of dispassionate, dehumanized machine.

The computer arrived on the scene after the scientific transformation of human thought was essentially complete. Weizenbaum describes the first widespread practical use of computers, automating the great "tab rooms" of business and industry in performing their accounting operations. In this use, the computer took over, essentially unchanged, the work of punched-card accounting machines that sorted, summarized, and printed office records. Then businesses and government agencies found that the very techniques they had developed to study and model their own operations, often motivated by the acquisition of their first computer, could be

DOCID: 4009794

programmed and carried out by means of the new machines. "The crucial transition, from the business computer as a mere substitute for work-horse tab machines to its present status as a versatile information engine, began when the power of the computer was projected onto the framework already established by operations research and systems analysis" (pp. 33-34).

It has become a truism among spokesmen for technology that the computer came along just in time to save our society from breaking down under the strain of population growth and exploding complexity. Weizenbaum, while agreeing that our institutions could not now exist in their present form without the computer, provides a different slant on the matter. He shows how the computer was seized upon by business and government as a God-given means of maintaining the status quo, and sidestepping the creative reshaping of our institutions that might have been called forth by the crises in complexity that threatened after World War II. The bottlenecks and breakdowns that motivated us to "augment or replace the low-internal-speed human organizations with computers, might in some other historical situation have been an incentive for modifying the task to be accomplished, perhaps doing away with it altogether, or for restructuring the human organizations whose inherent limitations were, after all, seen as the root of the trouble" (p. 30). Weizenbaum condemns the choice that was made, and the use that was made of computers as a result of that choice, in words recalling some of Dreyfus' statements: "Of the many paths to social innovation the invention of the computer opened to man, the most fateful was to make it possible for him to eschew all deliberate thought of substantive change. That was the option man chose to exercise" (pp. 31-32). The computer has now become truly indispensable to the survival of our society, *in the present specific form in which the computer itself has helped to freeze and fossilize one way of doing things.*

Weizenbaum devotes several very readable and interesting chapters to an explanation of what computers are, how they work, and whence they gain their unique and awesome power to change our world. His excellent, clear discussion of the Turing machine, the nature of programs and programming, and other computer concepts, are in my opinion worthy of unreserved recommendation to any reader who wants a good insight into the matter. Whatever disagreements one may have with his value judgments, Weizenbaum must certainly be a superlative teacher of computer science.

The computer, Weizenbaum continues, perhaps more than any other tool, has altered Man's concept of his own identity, mind, and experience. An all-pervasive computer metaphor has taken hold of the minds of scientists, many humanists, and the "man in the street." According to this view, man and computer are merely two subspecies of the genus "information processor." Weizenbaum singles out for special attack the Simon and Newell General Problem Solver (GPS) and its "means-end" analysis of human problem-solving behavior. This theory sought to found a new "information processing psychology," based on a hierarchical set of modular actions and tests which described all goal-directed behavior in terms of reducing differences between the object in hand and a desired object (Simon and Newell 1958).

The broad and ambitious general claims made for the GPS theory by its authors are roundly condemned by Weizenbaum, who dismisses it as a limited metaphor and not a scientific theory at all in any proper sense. Its worst consequence in his eyes is the production of an image of Man as a "GPS-like machine." This impoverished metaphor, says Weizenbaum, has made it possible for a psychiatrist to regard his patient as "an object different from the desired object. The therapist's task is to detect the difference, using difference-detecting operators, and then to reduce it, using difference-reducing operators, and so on. That is his 'problem'! And that is how far the computer metaphor has brought some of us" (p. 181).

Weizenbaum points out a number of other consequences of the overenthusiastic and unbalanced application of computer technology. While new tools can open up new horizons for people, he warns us that they can also have the effect of closing off certain possibilities of social action, and distancing us from some domains of data and experience that were previously accessible. "A computing system that permits the asking of only certain kinds of questions, that accepts only certain kinds of 'data,' and that cannot even in principle be understood by those who rely on it. . . has effectively closed many doors that were open before it was installed" (p. 38).

Another important adverse consequence of the modern scientific world view, and especially of its latest manifestation, the computer, is an abdication of individual human autonomy and responsibility, and a new tyranny of technical expertise. Weizenbaum condemns a number of recent theories and research efforts (among them GPS, Forrester's "Limits to Growth" model, and B. F. Skinner's psychological theories), accusing them of distorting and abusing language, advertising easy "scientifically-endorsed" panaceas for every ill, and exploiting the myth of expertise. The language "is mystifying . . . All contact with concrete situations is abstracted away. Then only graphs, data sets, printouts are left. And only 'we,' the experts, can understand them . . . The expert will take care of everything, even of the problems he himself creates" (pp. 253-254).

Weizenbaum presents a provocative viewpoint on science itself, that most sacred of sacred cows. He accuses it of having become, in our present overemphasis and abuse, an "addic-

tive drug" and even a "slow-acting poison," in spite of the admitted benefits we have obtained from some of its accomplishments. Science, directly contrary to the generally accepted belief in its solid foundation in absolute objectivity and the validated work of the past, can only be anchored ultimately on "the shifting sand of fallible human judgment, conjecture, and intuition" (p. 15). The myth of scientific objectivity would have us believe than any clearly demonstrated counter-instance is sufficient to force revision of the most cherished theory. On the contrary, Weizenbaum shows, scientists routinely explain away counter-instances as erroneous or inconsequential, and cling to their pet theories in the hope that they will be rescued by some later discovery. "The man in the street surely believes. . . scientific facts to be as well-established, as well-proven, as his own existence. His certitude is an illusion" (p. 15).

Drawing a trenchant and amusing parallel between the compulsive gambler, the compulsive programmer, and the "mad scientist," Weizenbaum drives home some telling points. All three share these characteristics in common: they are certain they will succeed, regardless of any number of setbacks; they have an invincible faith in their own cleverness; and they are convinced that all of life can be reduced to the terms of their "system," whether it be gambling, programming, or empirical science. All three disciplines are revealed by Weizenbaum as "magical" and "self-validating" belief systems, capable of being unrestrainedly abused by people with an overriding passion for absolute certainty and control over artificial worlds of their own making. "The compulsive programmer is merely the proverbial mad scientist who has been given a theater, the computer, in which he can, and does, play out his fantasies" (p. 126).

In an interesting discussion of theories and models, Weizenbaum contrasts the theory-based application of computers in such successful AI projects as MACSYMA and DENDRAL to the ad hoc, patchwork approach in most other areas where no strong theoretical base exists or has been applied. DENDRAL, at Stanford University, produces descriptions of those molecular structures that can explain a given record from a mass spectrograph. Its competence is as good as, or better than, that of the human postdoctoral chemists who have traditionally performed this task (Buchanan, Sutherland, and Feigenbaum 1969). MACSYMA, at MIT, performs symbolic mathematical manipulations also usually carried out by highly-skilled specialists (Martin and Fateman 1971). "Such theory-based programs," Weizenbaum suggests, "enjoy the enormously important advantage that, when they misbehave, their human monitors can detect that their performance does not correspond to the dictates of their theory and can diagnose the reason for the failure from the theory" (p. 232).

Most existing programs in use by business, industry, and government can be based on no such theory; they are, Weizenbaum maintains, patched and "hacked" together from hit-and-miss strategies that seemed to work for this or that case. Such programs are typically written by large, loose "teams" of programmers, many of whom have left or been reassigned before the program goes into operation. Thus, there is no one around who really knows how the program works; in the absence of any theoretical base, no one can even tell *whether* it is working properly in all cases, let alone correct it when it fails.

Weizenbaum justly devotes considerable attention to Terry Winograd's language-understanding research. This work undoubtedly constitutes one of the most successful and creative recent AI accomplishments, and has been hailed by many as a major breakthrough. I strongly recommend Winograd's report (1970) to any reader interested in gaining an idea of what can be done by computers in the analysis of natural language; it is enjoyable reading and represents a very fine piece of research. Weizenbaum does not see it, however, as a theory-based accomplishment comparable to MACSYMA or DENDRAL. He praises it as an "important achievement," which "shows how a specific view of certain aspects of language can really be filled in with enough detail to provide a working model" (p. 195). Winograd's heuristics, however, according to Weizenbaum, "express no interesting general principles" (p. 197). Winograd's effort shares with GPS and many other AI projects the fault of appearing to present general theories when they really provide only "virtually empty heuristic slogans." They seek to verify these "theories" by constructing models "that do perform some tasks, but in a way that fails to give insight into general principles" (p. 196).

Weizenbaum bases his deeper philosophical objections to such AI research, and to the abuse of computers and of technology in general, on two main grounds. His first argument is an attempt to show that much of human thought is not amenable to formal expression. His second basic position concerns the ways in which man must differ in essence from any machine. In much of what he says on these topics, Weizenbaum comes close to many of Dreyfus' points, but with a rather different emphasis. Human thought and behavior cannot ever be entirely expressed in terms of the "effective procedures: which can be carried out by a Universal Turing Machine. The reasons he presents for this view can be summarized as follows:

● *Much human thought, action, and speech is context-dependent.* It matters quite a lot to us *which* values of "x" and "y" are plugged into an expression. The human participant in a conversation or other social act brings to it a frame of reference that establishes what the talk or action is "about." Weizenbaum maintains that we can never get a sufficiently inclusive "knowledge base" into a computer to permit it to do this for any significant task or context.

(Continued on p. 23)

DOCID: 4009794

From ⬡ to the undrawable...

THE POLYHEDRAL WAR

[redacted] P12

P.L. 86-36

ILLUSTRATED BY [redacted] P12

Some time ago, a model of a polyhedron appeared in the P1 office. For those of you who have forgotten -- or never had -- three-dimensional geometry, a polyhedron is the space-filling analog of the area-filling polygon. A square is a two-dimensional polygon; a cube is its three-dimensional analog, a polyhedron. In their idealized form, polyhedra are examples of some of the most beautiful shapes and can often be seen incorporated into the works of contemporary artists. Yet the model of the polyhedron in the P1 office, a "flexible" dodecahedron (12-faced figure) in basic black, was at the opposite end of the beauty scale (see Fig. 1). It was, in my opinion, one of the most pitiful examples of a polyhedral model I had ever seen. To add insult to injury, in addition to being unaesthetic, it was constructed by using a most inefficient method. Both of these considerations led me to state that I, with my background in geometry and my interest in model-building, could easily build a better polyhedral model, the only criterion of "better" being its aesthetic quality as judged by an unbiased observer.

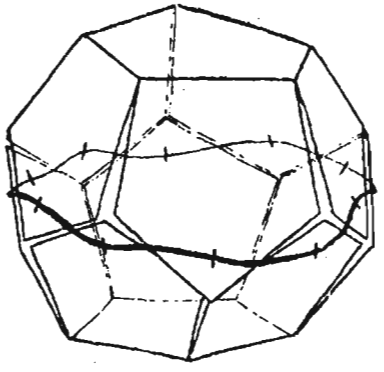


Fig. 1. Pitiful polyhedron

Little did I know that my innocent boast would begin the now-famous Polyhedral War. The same one-upsmanship that led me to build a better model would also lead another young mathematician, the illustrator of this article, [redacted] to do the same. Yet consider the issue about which the War was being waged: the beauty of models of abstract geometric entities. This may serve to show the only real distinction between the outlook of mathematicians and that of others. Often the mathematician is concerned with more abstract things than the general person, yet the manifestation of that concern takes on very familiar, practical forms, e. g. a contest. This contest, the "War," is a good example of this dichotomy between the planes of thought and of action. The War was fought at two levels -- an abstract level with choices of polyhedra or polyhedral combinations, and a practical level with construction methods, materials, colors, and glue.

Michael chose models of interpenetrating polyhedra as the most beautiful. These figures, known since the time of Gauss and Euler, often depict graphically the interrelationships among the five most basic polyhedra, the Platonic solids. These solids are:

- tetrahedron [*tetra* = "four" + *hedron* = "face"],
- cube (figure with six square sides),
- octahedron [*octa* = "eight"],
- dodecahedron [*dodeca* = "twelve"], and
- icosahedron [*icosa* = "twenty"].

They exhibit a surprising degree of interdependence. The cube and the octahedron, for example, are duals, i.e. "mirror images" in a certain sense. More specifically, the cube's six faces, eight vertices, and 12 edges correspond directly to the octahedron's six vertices, eight faces, and 12 edges. Indeed, if you connect the centers of the six square faces of a cube, you obtain an octahedron, and vice versa with the eight triangular faces of the octahedron, as can be seen from Figs. 2a and 2b. These and

DOCID: 4009794

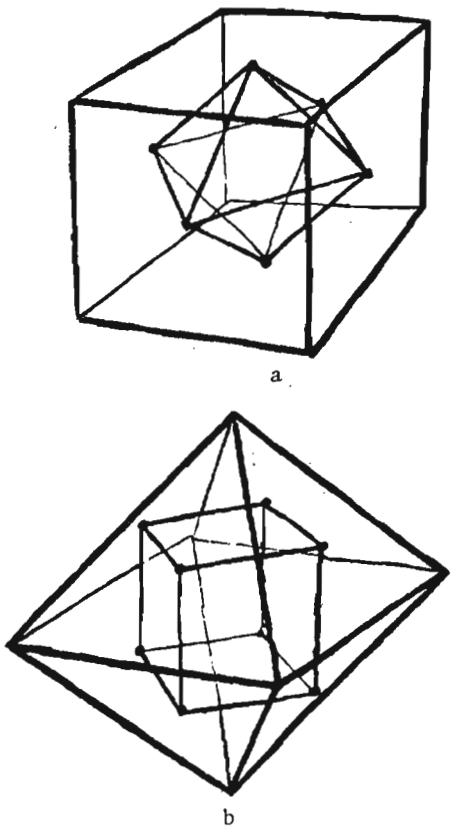


Fig. 2. Duality of cube and octahedron.
a - Octahedron in cube;
b - Cube in octahedron.

other unexpected and unusual properties have fascinated mathematicians and mystics alike, even so far as to have inspired various schools of cosmology into varied and numerous misguided interpretations of the mathematics involved. With this wealth of history behind him, Michael decided to build a model of five intersecting tetrahedra, intersecting in such a way as to outline the largest of the Platonic solids[1], the dodecahedron. This polyhedral configuration is pictured in Fig. 3. After choosing the basic strategy for using these models of interpenetrating polyhedra, Michael worked out the tactics of construction. He chose to use the traditional method of cutting and pasting faces which are especially constructed for the particular model. This method requires extreme exactitude in the preparation of the faces and great patience in the assembly, and is suited only for permanent-display models which represent polyhedra whose geometry has been completely described.

[1]While the dodecahedron has fewer *faces* than the icosahedron, it is "larger" in terms of volume. The ancient Greeks knew this and made balls for their sporting events with 12 pentagonal faces sewn together.

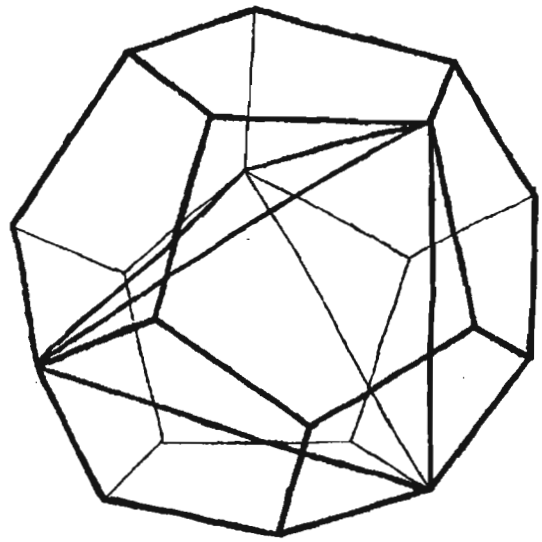


Fig. 3a. One tetrahedron in a dodecahedron

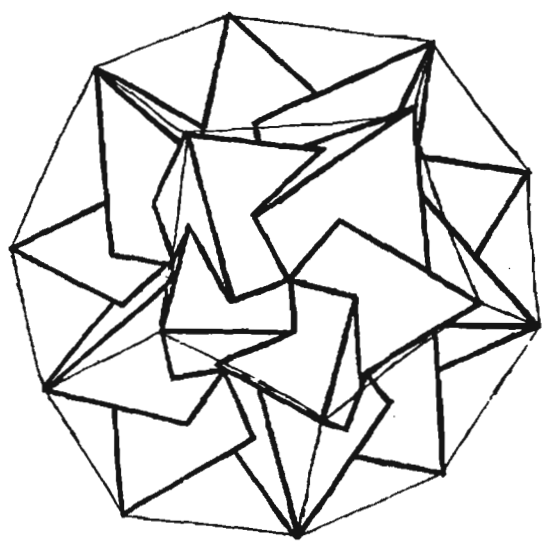


Fig. 3b. Five tetrahedra (visible edges only) in an imaginary dodecahedron

The family of polyhedra I chose, however, is known as the toroids. A toroid is a polyhedron out of which a "polyhedral hole" has been cut. As an example, consider Fig. 4, a square orthobicupola with a cuboctahedron "hole" cut out of its inside. These types of polyhedral combinations show the relationships between the altitudes and angles of the various polyhedra as opposed to the interpenetration figures which tend to reveal the symmetry relationships. Also unlike the interpenetration figures, toroids are relatively new, most having been discovered since 1970. As an example of one of the most aesthetic toroids, I chose a three-holed truncated octahedron. Since this toroid is extremely difficult to visualize from a drawing, Fig. 5 shows how it is constructed, as well as the final result.

DOCID: 4009794

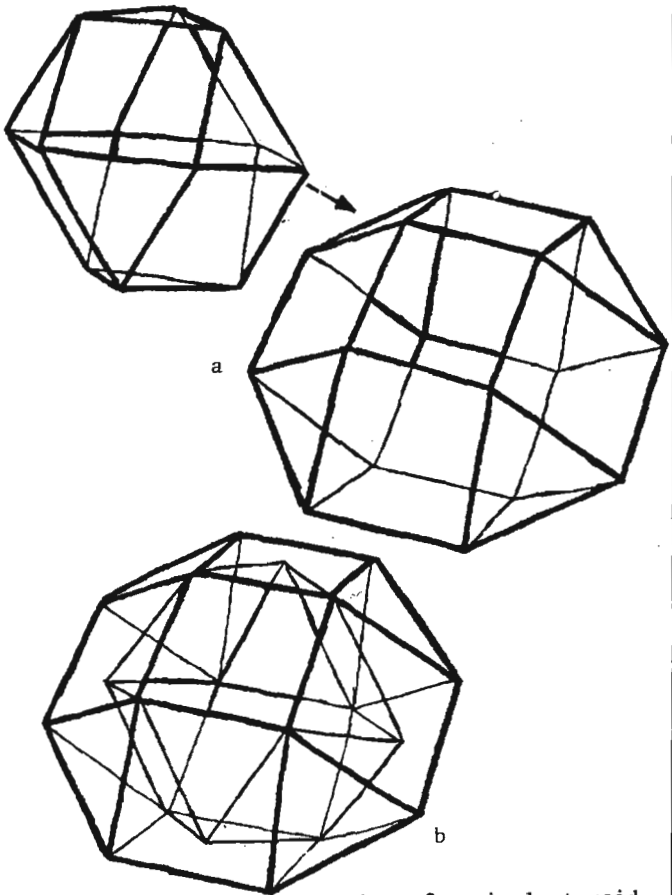


Fig. 4. The construction of a simple toroid.
a - Components; b -- Final result

Toroids, as a group, represent a real challenge to the model-builder. The traditional cut-and-paste method fails in two important areas. The construction of a many-holed toroid, as that depicted in Fig. 5, requires an almost unattainable degree of dexterity and patience. The experience of using this method is so discouraging that some mathematicians have suggested that the lack of an appropriate model-building technique may account for the fact that toroids have been unknown for so long. Also, the cut-and-paste method is totally unsuited for any kind of "exploring." Often it would be nice to build a quick model to assist one in working out the geometry involved in a polyhedron, in a manner comparable to the way in which proofs in high-school geometry are solved with the aid of a rough sketch. One cannot quickly "test out" an idea for a toroid with the cut-and-paste method. In the first place, the inspiration for the idea would probably die before a model could be constructed with this laborious method, and, in the second place, this method requires that the geometry of the polyhedron be entirely determined before building the model. But the model was being built to assist in the working out of the geometry!

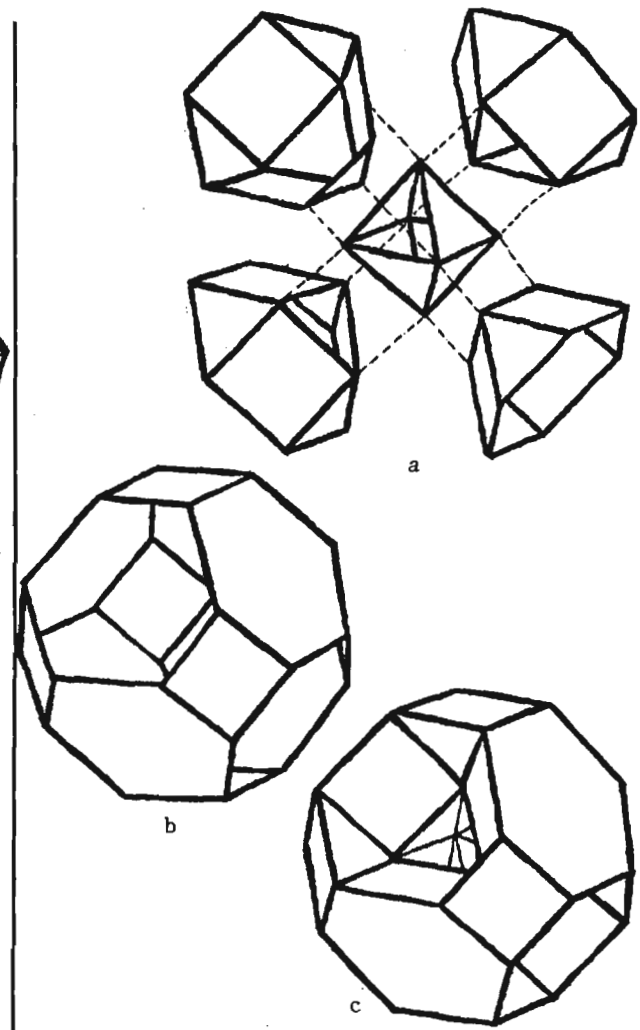


Fig. 5. a - Exploded view of the "hole";
b - "Shell" into which components of "hole" are fitted;
c - Final result -- a three-holed toroid

These weaknesses have led to the so-called cardboard-and-rubberband method. In this method, regular polygons are constructed in great numbers, without having any specific polyhedron in mind. These polygons are appended with flaps on each side. The flaps are bent to be at right angles to the polygon and notched at each vertex. Two such polygons can be joined, in the process of building a polyhedral model, by a rubberband surrounding the flaps, which is caught securely in the notches. While it is true that the resulting models have flaps and rubberbands on the outside, which tend somewhat to highlight the edges and vertices of the polyhedron, they are mainly an aid in construction and are not a part of the idealized, geometric entity. Fig. 6a shows a polyhedral model complete with these flaps and rubberbands. For "explorations" this method yields an unexpected bonus. Models made in

this way may be quickly disassembled and the pieces can then be used, in a mild form of cannibalism, for new models. The effort expended to construct the original polygonal pieces then becomes an investment as the pieces can be re-used. While the ease of use and the economy of effort of the cardboard-and-rubberband method cannot be overemphasized, it must be remarked that the final model lacks the professional appearance of the cut-and-paste models, and also that, unfortunately, rubberbands do not last forever. After a year or so, one can be horrified to find his cherished model as a tangled jumble of polygons and decayed rubberbands. The cardboard-and-rubberband method of construction, along with a lengthy and delightful exploration of the world of toroids, is fully described in Stewart's *Adventures Among the Toroids*.

The toroid in Figs. 6a and 6b, a pentagonal orthobicupola with a pentagonal prism as a hole, reminds us that the War is fought on two levels and not merely on one. For, in reality, Fig. 6

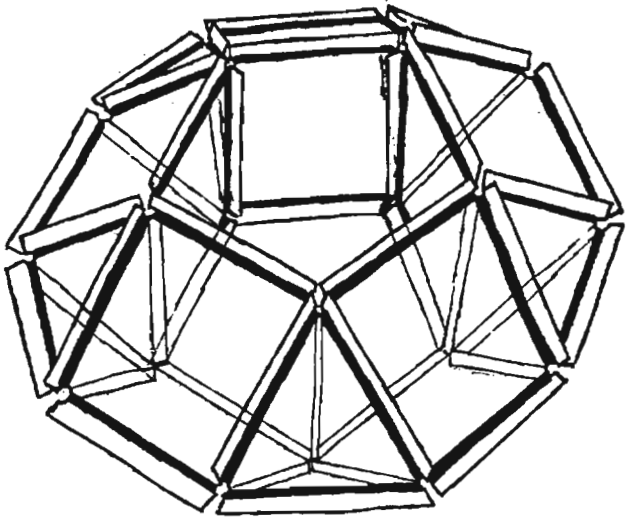


Fig. 6a. Cardboard-and-rubberband model

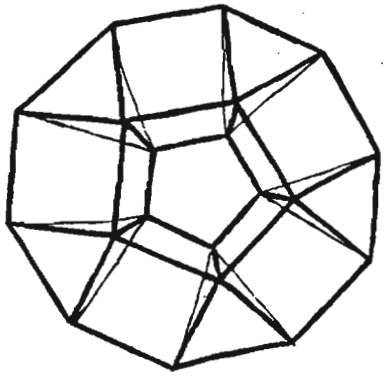


Fig. 6b. Top view of "idealized" cardboard-and-rubberband model (rubberbands and flaps removed)

represents nothing at all! While examination of the figure or even the model itself reveals nothing suspicious, a detailed analysis of the geometry of the model shows us that such a toroid is nonexistent. Assuming an edge length of one for all polygons, the altitude from the parallel pentagonal faces of the bicupola would have to be precisely one for the prism to fit exactly inside. After a small amount of computation, the altitude of the bicupola is found to be:

$$h = \frac{2}{\sqrt{R + 2}},$$

where $R = \frac{1 + \sqrt{5}}{2}$

This yields:

$$1.05 < h < 1.06$$

Thus the idealized pentagonal prism could not possibly fit inside the idealized pentagonal bicupola. The model appears to fit together because there is just enough stretch in the rubberbands so that the distortion is not noticed when the model of the bicupola is compressed. The War requires not only attractive models, but also that the models represent an actual geometric form. Cardboard and rubberbands do not a polyhedron make.

While the tide of the War was decidely in my favor with the submission of the three-holed truncated octahedron built by using the cardboard-and-rubberband method, Michael, after much secretive delay and deception, countered with two flawlessly constructed interpenetration figures. One was the nonsuperimposable mirror image of the five intersecting tetrahedra, and the other (Figs. 7a and 7b) was a model of five intersecting cubes, also intersecting in such a way as to outline the dodecahedron.

At this point, however, because of time and space limitations (the P1 office was beginning

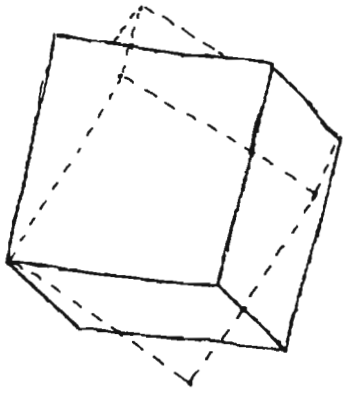


Fig. 7a. One cube (solid lines), with positioning of next cube (dotted lines)

DOCID: 4009794

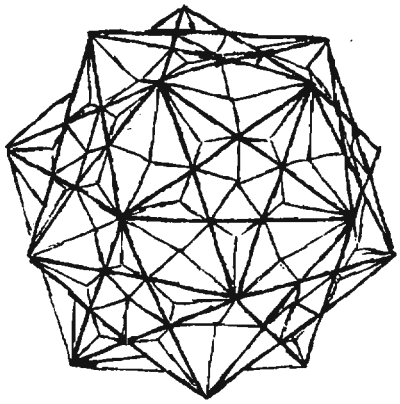


Fig. 7b. Five cubes in a dodecahedron (visible edges only)

to get rather crowded), a truce was declared and the War officially ended by the joint submission[2] of a model of a toroid constructed by the cut-and-paste method. The toroid chosen was Stewart's "Gem of the Expedition," a truncated dodecahedron with 11 holes, constructed of pentagonal cupolas and antiprisms. This gargantuan effort consisting of 260 faces was declared unsurpassable by the unbiased judge of the contest and can now be viewed in the P1 office (Room 3W090). Since a drawing can hardly do justice to a model of such complexity and beauty, none is even attempted here.

Perhaps the average person thinks that the mathematician gets his fun out of standing hip-deep in computer output as he mutters absent-mindedly about some obscure calculation, or by filling in blackboards with theoretical equations, so much so that he is completely unable to enjoy ordinary pleasures. Actually, mathematicians are pretty much like everyone else, and can appreciate a lot of other things too, including beauty wherever they see it. And one of the biggest joys of the mathematician is to use mathematical principles to construct a beautiful object that everyone can enjoy in his or her own way -- the mathematician because it is a "truncated dodecahedron" logically derived from one of the Platonic solids, and the average person just because it "looks absolutely beautiful!"

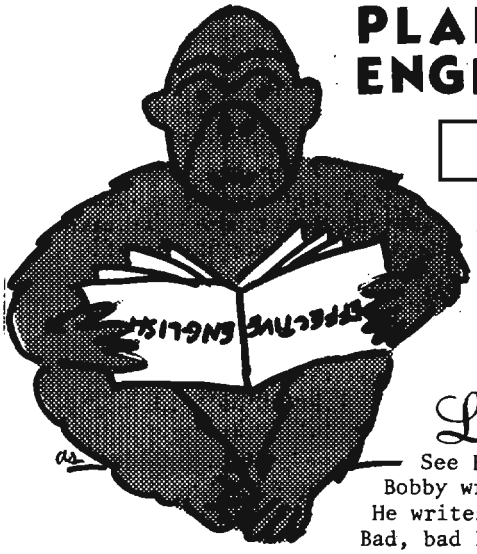
All the models illustrated in this article, plus the undrawable "Gem of the Expedition," will be shown in the Headquarters Building display case (in the passageway toward the Operations Building), from 16 through 31 May.

provided invaluable assistance in the construction of this model.

PLAIN ENGLISH

C22

Reprinted from C-LINERS, Final issue.



Look, Mary.
See Bobby write.
Bobby writes bad.
He writes long words.
Bad, bad Bobby.

See me write. I write good. I write little words. Good, good me. And I am a college graduate.

Daddy paid lots and lots of money so I could speak English good. I was an English major. Now I work. I work at NSA. Now I use APE (Agency Plain English). Now I am good. I even got a letter of appre. . . appri. . . apre . . . I forgot how to spell it.

P.L. 86-36

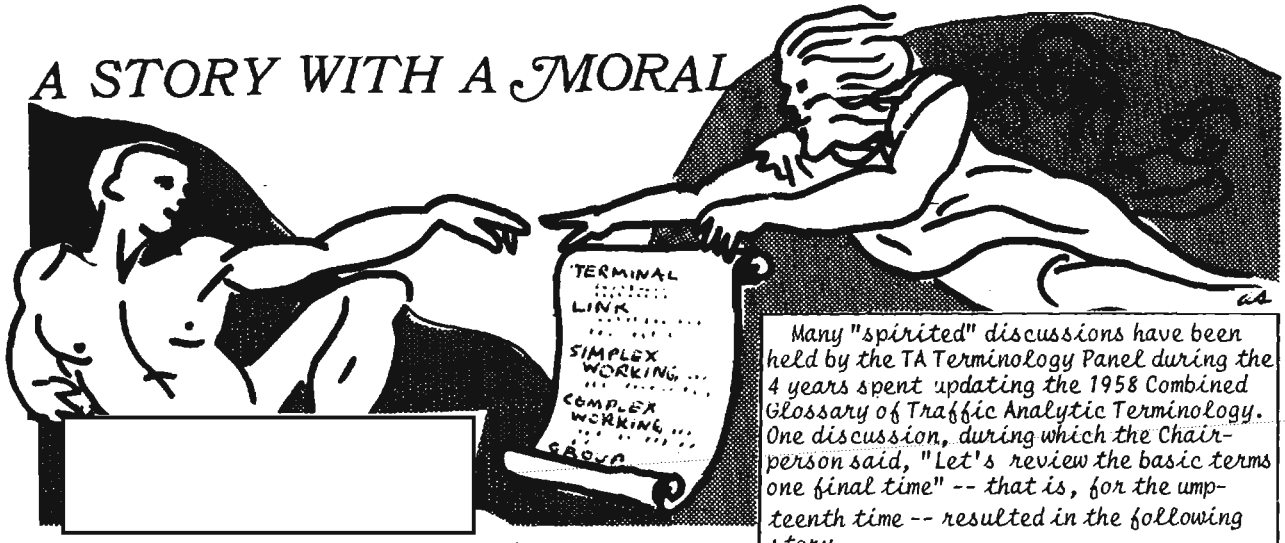
Rubbish. Understand that I am not against plain communication, straightforward communication, where each word must be justified must add a necessary and vital ingredient to the communication. But our nation's universities are horrified at what they have come to call "college-level illiteracy." This year in the California state colleges, nearly 50 percent of the incoming freshman class was required to take mandatory, noncredit, remedial English. Yet at NSA we are encouraged to all but abandon what we used to call the English language. We have actually been told not to worry too much about formal sentence structure. We have been criticized for using a dictionary and thesaurus.

But did it ever occur to anyone that wordy, passive, confusing memos might be a weapon, or, more correctly, a shield? If we want all Agency personnel to speak and write plain English, perhaps we should first teach Agency personnel English. If we want Agency management to write concise, active, decisive memos, perhaps we should first teach Agency management to be concise, active, and decisive.

Let us attack the problem, not just hide the symptom.

DOCID: 4009794

A STORY WITH A MORAL



Many "spirited" discussions have been held by the TA Terminology Panel during the 4 years spent updating the 1958 Combined Glossary of Traffic Analytic Terminology. One discussion, during which the Chairperson said, "Let's review the basic terms one final time" -- that is, for the umpteenth time -- resulted in the following story.

N.G.

P.L. 86-36

To all the members of the TA Terminology Panel:

In the beginning God created a TERMINAL.

For a while this terminal was happy. He had a transmitter and a receiver. He played with the transmitter, sending little signals throughout the ionosphere. But, although he could send, he never received any answers. So the little terminal became unhappy. After much thought, God created another terminal, and He called the two terminals a LINK. Because He was a kind God, He assigned them a single frequency to use for communication, and He called this SIMPLEX WORKING.

Time passed and, as is wont to happen in the best of families, the two little terminals each wanted to claim the frequency for its very own. So God, in His infinite wisdom, gave each terminal its own frequency, and He called this COMPLEX WORKING.

More time passed, and almost nine months later, to the day (give or take a few days), a new terminal appeared. God decided He would call these terminals a GROUP.

Now He knew, from past experience, that trouble could arise, so He made the first terminal CONTROL. And He told Control, "You are the boss of this group, and you tell 'em how it's gonna be!"

And He left on vacation.

Now, Control decided that there was only one way to make everybody happy, so he gave each terminal a different transmitting frequency to use to contact the other terminals, and he called it COMPLEX SENDING.

Additionally, because he had some smarts of his own, Control gave each terminal a different receiving frequency, and all terminals, when sending to a particular terminal, used the frequency allotted to it. And he called it COMPLEX RECEIVING.

Still more time passed and the group grew. More terminals appeared and these terminals all chatted happily together. One day, as happens in all good stories, one of these terminals decided that he wanted to talk to two of his friends simultaneously, and he needed *two* frequencies to do so. Control agreed and called it DUALING.

Now Jealousy reared its ugly head! Another terminal decided he also wanted two frequencies, but he wanted to transmit *different* information simultaneously. Control was shook! But he said okay, and he called it DOUBLE CHANNEL OPERATION.

Two other little terminals, who had been watching all this byplay, decided they too should get into the act. They wanted to simultaneously transmit and receive messages in both directions between themselves, each using his one transmitter and his one receiver. Control began to worry, thinking, "This is getting out of hand!" But he said okay, and he called it DUPLEX OPERATION.

But, he added, just in case it should arise, the normal practice of transmitting and receiving messages between two terminals in either direction alternately would be called HALF DUPLEX OPERATION. And he went home and threw up.

Then God came home.

He looked around. He could not believe what He saw.

He called Control and asked, "What happened?"

Control replied, "The devil made me do it!"

God said, "I thought, when I told you you're the boss, you would have sense enough to use the KISS principle. That's Keep It Simple, Stupid!"

The moral of the story is:

"Terminals, and panels, should not mess with God's creations."

DOCID: 4009794

Artificial Intelligence

(Continued from p. 16)

● *Much human thought is essentially beyond formalization.* Weizenbaum refers to the recent work of Ornstein (1972) and the psychological discoveries concerning differences of function in the left and right hemispheres of the human brain. According to this (still somewhat new and controversial) finding, the left hemisphere specializes in sequential, logical, and verbal thought, while the right specializes in holistic, global, intuitive concepts, and movement in space. We have, thus, at least two major "modes" of thought: the "left-brained" mode produces structures like computer programs and formal descriptions, but the "right-brained" mode so far completely escapes our ability to pin it down in formal terms. We must use our "left-brained" methods to think rationally, and science singles these out as the sole avenues of thought for its purposes. Unfortunately for science and for AI research, human problem-solving and communication require that both "halves" of the brain work together in close cooperation. Dreyfus' distinction between "digital" and "nondigital" modes of thought, and his mention of "fringe consciousness," "insight," and "perspicuous grouping" as nondigital features of human thinking, appear to be closely related concepts.

● *Formal systems and empirical observations are essentially incomplete.* Weizenbaum alludes to Heisenberg's Uncertainty Principle as undermining the basis of emprical observation on which science is founded; further, Gödel's Proof exposed "the shakiness of the foundations of mathematics and logic itself," and proved that they "must necessarily be forever incomplete" (p. 221). Thus, there must always be things that we can never measure accurately, or describe completely.

● *Human beings are embodied.* Here Weizenbaum echoes, in almost the same words, one of Dreyfus' most important and interesting points. "It is not obvious that all human knowledge is encodable in 'information structures,' however complex . . . there are. . . some things humans know by virtue of having a human body. No organism that does not have a human body can know these things in the same way humans know them. Every symbolic representation of them must lose some information that is essential for some human purposes" (pp. 208-209).

● *Human beings are socialized by other humans.* "The human infant. . . is born prematurely, that is, in a state of utter helplessness. . . An infant will die if he is fed and cleaned but not, from the very beginning of his life, fondled and caressed -- if, in other words, he is not treated as a human being by other human beings. . . Thus begins the individual human's imaginative reconstruction of the world. And this world. . . is the repository of his subjectivity, the stimulator of his consciousness, and ultimately the constructor of the apparently external forces he is to confront all his life" (pp. 210-211). By virtue of facing and solving human problems, man's thought is determined in ways forever and essentially alien to the procedures and representations of a computer. "Man is not a machine. . . Computers and men are not species of the same genus" (p.203).

We are faced, as Weizenbaum vividly demonstrates, with a basic epistemological and moral dilemma. Science provides us with tools, in the form of descriptions, algorithms, and computer programs; we have employed these tools to gain an unprecedented degree of apparent control over the physical world. Science also provides us with a seductive and all-encompassing way of perceiving the world in terms of numbers, rules, and formalisms. We are armed with a plethora of instruments and devices, but we have cut out from under ourselves the basis of making value judgments, or for choosing whither we shall direct our armament of techniques. Science rules out by definition all the vast domain of reality that is subjective, that cannot be counted, measured, or proved, and where the bases of human choice truly reside.

Weizenbaum makes repeated use of a metaphor drawn from an old joke involving a drunk who has lost his keys on a dark street at night, but persists in looking for them only under the street lamp because "the light is so much better over here." This is the way science, and indeed all of man's "left-brained" undertakings, must proceed. The trouble comes when the scientist or programmer deliberately and consciously simplifies (and thereby impoverishes and distorts) reality, and then proceeds to accept that distortion as a complete and final picture, claiming to have produced a theory about the world when he has only pulled off a limited technical trick. "Indeed, what is sought can be found only where there is illumination. Sometimes one even finds a new source of light in the circle within which one is searching. Two things matter: the size of the circle of light that is the universe of one's inquiry, and the spirit of one's inquiry. The latter must include an acute awareness that there is an outer darkness, and that there are sources of illumination of which one as yet knows very little" (p. 127).

Since our scientific lamppost has no light to throw on any matter concerned with human values or purposes, we are in the position of the "compulsive programmer" who has forgotten, if he ever cared, what his program was supposed to do in the first place. "He has only technique, not knowledge. He has nothing he can analyze or synthesize; in short, he has nothing to form theories about. His skill is therefore aimless, even disembodied. It is simply not connected with anything other than the instrument on which it may be exercised" (p. 118). Enthroned in the midst of our artificial world

and all our expensive gadgets, "we can count, but we are rapidly forgetting how to say what is worth counting and why" (p. 16).

Weizenbaum anticipates some of the objections that will be raised against his positions. The " technologist" will dismiss his arguments as "merely philosphical," and condemn them as polemical and subjective. Such objections are, essentially, just another way of saying that Weizenbaum's points belong to the world beyond the edges of that circle of light cast by the scientist's lamppost. He makes the only answer he can, repeatedly reminding the technologist that his keys are not where he is looking, however good the light may be there. A common defense of our total reliance on science and technology maintains that the only alternative is chaos, destruction, and mindless irrationality. Weizenbaum counters this argument in a forthright statement: "In fact, I *am* arguing for rationality. But I argue that rationality may not be separated from intuition and feeling. I argue for a rational use of science and technology. . . I urge the introduction of ethical thought into science planning" (pp. 255-256).

The inevitable refusal of those on the opposite side of the debate to accept as legitimate any of the grounds on which he bases his arguments confronts Weizenbaum with an impossible dilemma. "Anyone who wishes to persuade his colleagues to cooperate in imposing some limits on their research. . . risks being excommunicated as a sort of comic fool" (p. 266). Nevertheless, Weizenbaum states three kinds of uses to which he feels, on moral grounds, computer ought not to be applied. These are:

- projects that seek to substitute machines for parts of living animals to create hybrid bionic systems (for example, coupling an animal's brain and visual system to computers). Such projects are "obscene" and represent "an attack on life itself." "One must wonder what conceivable need of man could be fulfilled by such a 'device' at all. . ." (p. 269).

- projects involving the substitution of a computer system for a human social function. The use of computers or machines of any sort to take the place of a human participant in a "function that involves interpersonal respect, understanding, and love" is also "obscene" and ought not to be attempted, Weizenbahum maintains, because "respect, understanding, and love are not technical problems" (pp. 269-270). The obvious example of such projects is the use of computers as psychotherapists.

- projects that may clearly be seen to have unpredictable and irreversible side effects. As an example of this kind of application, Weizenbaum cites the automatic recognition of human speech. "I have no objection to serious scientists studying the psycho-physiology of human speech recognition," he says; the work he objects to is "mere tinkering," aimed ultimately at facilitating electronic snooping and wiretapping. He specifically mentions ARPA-funded speech research as the sort of work he means to condemn (p. 271).

Weizenbaum ends his book with a chapter which honestly and eloquently states his own personal position. Whether or not one agrees with anything he has said in the book, I feel that this frank personal statement deserves the greatest respect. He refers to his work as a teacher, with which he began, and which is obviously of great importance to him, much to his credit. He says that much of his message is directed in particular to teachers of computer science. Such a teacher, "no more nor less than any other faculty member, is in effect constantly inviting his students to become what he himself is. If he views himself as a mere trainer, as a mere applier of 'methods' for achieving ends determined by others, then he does his students two disservices. First, he invites them to become less than fully autonomous persons. . . Second, he robs them of the glimpse of the ideas that alone purchase for computer science a place in the university's curriculum at all" (p. 279). Weizenbaum makes a final strong statement of his position: "The computer is a powerful new metaphor for helping us to understand many aspects of the world, but. . . it enslaves the mind that has no other metaphors and few other resources to call on. . . The teacher must teach more than one metaphor, and he must teach more by the example of his conduct than by what he writes on the blackboard. He must teach the limitations of his tools as well as their power" (p. 277).

What should our reaction be to this book? Admittedly, it is often a polemical, biased, and emotional presentation. On the other hand, many excellent and telling substantive points are raised which merit a serious effort at understanding on their own terms and a reasoned reply based on such an understanding. The clear, well-presented chapters on the nature of computers, programs, theories and models, etc., written by a man who has "paid his dues" through many years of competent and creative computer science research, are in themselves rewarding features for any reader aside from the value judgments elsewhere in the book. Dismissing Weizenbaum's positions out of hand as "New Left" propaganda is not, in my opinion, a justifiable approach to the book's more controversial points. After all, the deeper issue is not the particular computer applications he personally objects to, but rather the fact that he challenges each of us to take up our own stand about how technology should or should not be used, and what kind of a world we want for ourselves and our children.

Several critiques have already been directed at Weizenbaum's book by members of the AI community. In the June 1976 issue of the *SIGART Newsletter* (a publication of the Special Interest Group on Artificial Intelligence in the Association for Computing Machinery), pp. 4-13, there is a highly interesting collection of

reviews and a rebuttal by Weizenbaum, all originally available on the ARPANET on-line communications network linking many major research centers. The first review, by Benjamin Kuipers of the AI Lab at MIT, is entitled, "Reactions to Weizenbaum's Book." It sets a very balanced and restrained tone, and seems open-minded and even sympathetic to many of Weizenbaum's viewpoints. Kuipers clearly seems to understand and acknowledge Weizenbaum's frame of reference, and agrees on the importance of avoiding a narrowly instrumental approach to human reason and scientific undertakings. He claims, however, that AI researchers are already well aware of and engaged with these issues, and he is "puzzled by Weizenbaum's vehement attacks" on the AI community. He also accuses Weizenbaum of obscuring his valid points by "harsh and sometimes shrill accusations" and "personal attacks" (p. 4).

A very long review by John McCarthy of the Stanford University AI Labor, entitled "An Unreasonable Book," takes a much more impatient and hostile attitude (pp. 5-10). McCarthy characterizes the book as "moralistic," "incoherent," and self-contradictory on matters Weizenbaum has not thought through as carefully as he should have. In several places, he raises the interesting point that Weizenbaum's "moralistic" strictures may be twisted and exploited by "activist bureaucrats" or "public interest organizations" as an excuse to stifle scientific freedom or to redirect scientific endeavor. "I am frightened," says McCarthy, "by the book's arguments that certain research should not be done if it is based on or might result in an 'obscene' picture of the world and man. Worse yet, the book's notion of 'obscenity' is vague enough to admit arbitrary interpretations by activist bureaucrats" (p. 5).

It seems to me, in reading McCarthy's comments, that science itself represents an ultimate value source for him, like a religion. He appears to accept it as such unquestioningly, to the point where he is completely unable or unwilling to entertain the suggestion that any other value source might take precedence over science. In support of his overriding respect for science, he presents an uncompromisingly absolute (and emotional!) statement by Andrew D. White, first president of Cornell University: "'In all modern history, interference with science in the supposed interest of religion . . . has resulted in the direst evils both to religion and science, and invariably; and, on the other hand, all untrammelled scientific investigation . . . has invariably resulted in the highest good both of religion and of science'" (p. 9). For McCarthy, evidently, "scientific freedom" is an unquestioned value in itself, which must be preserved as our first priority, and at any cost.

McCarthy takes issue in his review with almost every point that Weizenbaum made; in my opinion, however, he does not come to grips directly with Weizenbaum's essential arguments. He dismisses them *in toto*, much as many AI workers dismissed Dreyfus' earlier work. His approach is purely pragmatist: anything is moral so long as it "works." "Using computer programs as psychotherapists. . . would be moral if it would cure people" (p. 7).

Weizenbaum's response to McCarthy forms the third and final portion of the presentation in the *SIGART Newsletter* (pp. 10-13). He reiterates the main arguments of the book, and defends himself against some of McCarthy's more barbed attacks. He provides a direct rejoinder, for example, to McCarthy's pragmatic justification for computer psychotherapy; this reply can serve to bring into focus the basic gulf between the two viewpoints. "Prefrontal lobotomy 'cures' certain mental disorders. But at what price to the patient, and, I would add, to the surgeon as well? I believe that machine-administered psychotherapy would induce an image of what it means to be human that would be prohibitively costly to human culture."

In closing, I would like to single out three points that seemed most important to me in Weizenbaum's book. These are, at least in part, highly relevant to many of our concerns as employees of a large government organization that uses computers.

- *A solid theory base is crucially important.* The lesson of DENDRAL and MYCIN, pointed out by Weizenbaum, has been presented by others also: the cooperation of one or more specialists who are highly skilled and gifted in the problem area, and, can transfer their knowledge into the program's knowledge base, is a vital prerequisite for a successful application. This means that the problem, the data, the habits of working of human problem-solvers, the function of the automated process within a larger context, etc., must all be intensively studied and deeply understood. Then a model must be developed which is sufficiently detailed and representative of all aspects of the problem situation to satisfy the needs of those who will use the program. And, ultimately, this means more emphasis on learning about the problem, the data, and the man-machine interfaces and less emphasis on instruments and techniques as such: more on the "what" and "why," and less on the "how."

- *Control over the technology or program is essential.* Someone, or some small group of people, must maintain a grasp on how the program or device performs. Someone must be watching to see that the data and the problem situation do not drift away from the program's model. Someone must be able to detect malfunctions and correct them, not with a "patch," but by amending the model and, if necessary, also the theory beneath the model. We must even be willing to junk the model altogether if it breaks down, and build another. All of this, again, forces us to direct constant attention to the problem, the data, and the human users who must work with the program.

DOCID: 4009794

● *Human goals have overriding importance.* We cannot take our values and goals for granted, as if they were somehow part of the package containing our current scientific theories and the state of the art in some technology. We must find a way to choose where to put our effort, which programs to write, which techniques to use, which problems to solve -- a way that does not simply reflect the monetary or political pragmatism of the moment. I am doubtful about the reality of "pure research"; most research gets done because of passing fashions, interests, and demands; simply because a given field is active and "paying off" at the moment; or, even worse, just to get another paper into the literature. I agree with Weizenbaum in wishing that basic human considerations could have a larger part in the motivation of those choices that will, inevitably, be made. Weizenbaum does not tell us how to make better choices, but he has had the courage to tell us how he himself has chosen what he will and will not do with computers.

References

Buchanan, B., Sutherland, G., and Feigenbaum, E. A. "Heuristic DENDRAL: A Program for Generating Explanatory Hypotheses in Organic Chemistry," in Meltzer, B., ed., *Machine Intelligence*. New York: American Elsevier, 1969.

Dreyfus, Hubert L. *What Computers Can't Do*. New York: Harper and Row, 1972.

Martin, W. A., and Fateman, R. J. "The MACSYMA System," in *Proceedings of the Second Symposium on Symbolic and Algebraic Manipulation*. New York: Association for Computing Machinery, 1971.

Mumford, Lewis. *Technics and Civilization*. New York: Harcourt Brace Jovanovich, 1963.

Ornstein, Robert E. *The Psychology of Consciousness*. San Francisco: W. H. Freeman and Co., 1972.

Simon, H. A., and Newell, A. "Heuristic Problem Solving: The Next Advance in Operations Research," in *Operations Research*, Vol. 6 (January-February 1958), pp. 8 ff.

Weizenbaum, Joseph. "Symmetric List Processor." *Communications of the ACM*, Vol. 6, No. 9 (September 1963), pp. 524-525.

-------. "ELIZA -- A Computer Program for the Study of Natural Language Communication Between Man and Machine." *Ibid.*, Vol. 9, No. 1 (January 1967), pp. 36-45.

-------. "Contextual Understanding by Computers." *Ibid.*, Vol. 10, No. 8 (August 1967), pp. 474-480.

Winograd, T., *Procedures as a Representation for Data in a Computer Program for Understanding Natural Language*. PhD Dissertation submitted to the Department of Mathematics, MIT, August 24, 1970.

From Weizenbaum's Preface:

Briefly summarized, I composed a computer program with which one could "converse" in English (by means of a typewriter). . . I chose the name ELIZA for the language analysis program because, like the Eliza of *Pygmalion* fame, it could be taught to "speak" increasingly well. . .

For my first experiment, I gave ELIZA a script designed to permit it to play -- I should really say parody -- the role of a Rogerian psychotherapist engaged in an initial interview with a patient. . . DOCTOR, as ELIZA playing psychiatrist came to be known, soon became famous around the Massachusetts Institute of Technology. . . (and) at other institutions in the United States. The program became nationally known and even, in certain circles, a national plaything.

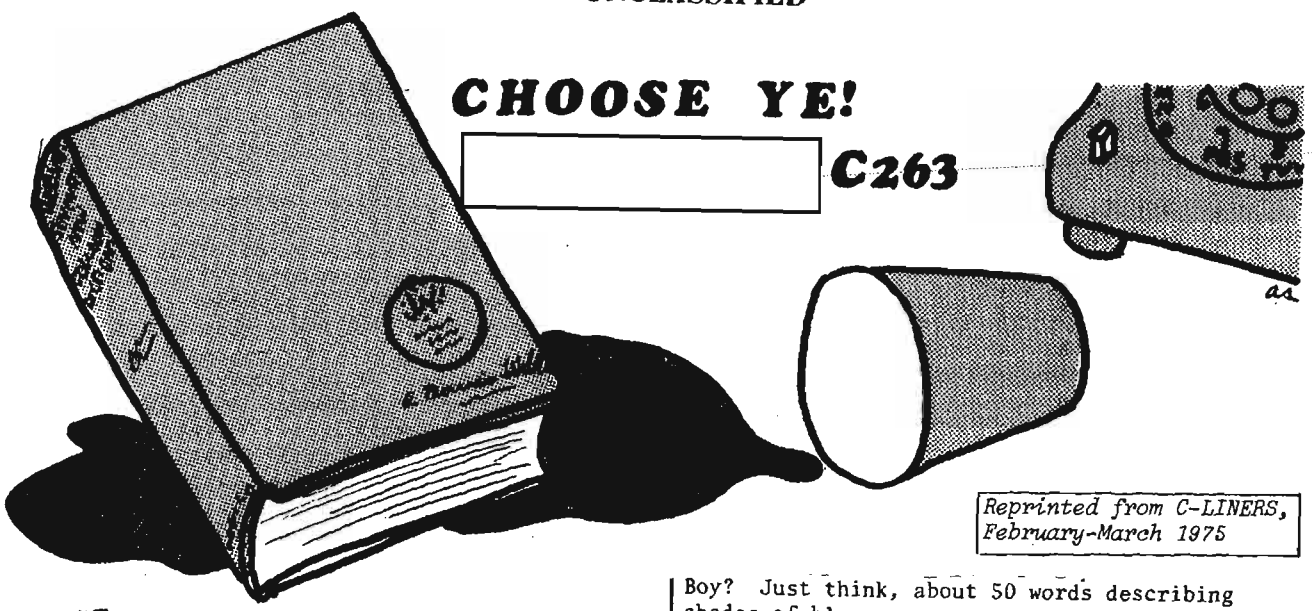
The shocks I experienced, as DOCTOR became widely known and "played," were due principally to three distinct events:

1. A number of practicing psychiatrists seriously believed the DOCTOR computer program to have the potential of growing into a nearly completely automatic form of psychotherapy. . .

2. I was startled to see how quickly and how very deeply people conversing with DOCTOR became emotionally involved with the computer. . . My secretary, who had watched me work on the program for many months and therefore surely knew it to be merely a computer program, started conversing with it. After only a few interchanges with it, she asked me to leave the room . . .

3. Another widespread, and to me surprising, reaction to the ELIZA program was the spread of a belief that it demonstrated a general solution to the problem of computer understanding of natural language. In my paper, I had tried to say that no general solution to the problem was possible, *i.e.*, that language is understood only in contextual frameworks. . .

DOCID: 4009794



Reprinted from C-LINERS, February-March 1975

"This technique will eschew the obfuscation prevailing in the system." When I first read this line, it was Monday morning, and I hadn't had my first coffee. In my excitement fumbling for the phone under emergency conditions, I spilled my coffee. It ran under my Webster on the desk. Still grappling for the phone, I pulled the dictionary deeper into the coffee. In spite of all this, my only thought was to make my call and get rid of the "obfuscation in the system."

The clue was right on my desk. The dictionary was now coffee-soaked. It was as though Old Noah was deliberately maneuvering his book into a position which would prevent my using the phone. But I still didn't catch on.

Wouldn't you know it? The line is busy. Perhaps a fast rereading of the memo would help me to better understand the problem. Yes, this guy was in real trouble. Not only was he plagued by "obfuscation," but he also had a "plethora of common recordings." I wonder why he didn't call me instead of writing a memo. Perhaps he also had a Webster on his desk.

Now this has gone far enough and I apologize to my readers, but I cannot exonerate Webster for his part in this fiasco of communications. In his desire to record our language, Webster unwittingly gave us an overabundance of choices of words. One might say that we have the Midas touch in our lexicon. We, like the king, may starve to death unless we discipline ourselves in the art of choosing.

Further compounding the problems are the many thesauruses lying around unguarded like Pandora's boxes, just waiting for the unwitting to lift the cover. Now, I did it: 300 words to replace "use," but only 50 to replace "possibility," but each, you must remember, is just a shade different from the others. Leonardo would certainly have stopped with finger paints if someone had told him that there are over a hundred shades of brown. Then, what about Gainsborough's Blue Boy? Just think, about 50 words describing shades of blue.

At this point I am about to be accused of, among other things, being against mother love, apple pie, and hot dogs, but really I'm not. I love Mom.

Who except the one trained in chromatography can distinguish between ochre and saffron, both shades of yellow? Possibly he's the same person who can distinguish between "use" and "utilize," or "possible" and "feasible."

Even the job titles of our duties give credence to this attempt to cushion the impact of our communication. What does a "coordinator" do? What is a "focal point"? In the latter title I envision many inputs being channeled through a small opening, sometimes called a lens, sometimes a bottleneck, and emerging inverted, completely reversed, at some secondary destination. Is a focal point a passive position in which the only requirement is to sharpen up the image of a previous input, as does a lens, or can it take independent action and contribute to the output? My apologies to all who must bear up under this label.

It is all too easy to poke fun at ourselves, but it takes a little more thought to find solutions. So, then, why do we choose words for a particular job anyway? There are many reasons: you may or may not agree. One textbook says that we write to direct, inform, or persuade. I have observed that we also write to impress, confuse, stall, or even retaliate. Then there is the neutrality syndrome. Some writing is done, of all things, to communicate. Perhaps you could make a few additions to my list.

If, upon weighing a particular reason for writing, the decision is "to communicate," I believe that there is but one rule in picking the best word: pick the shortest and most common word. Risk being called a square. Make the decision now. Decide whether you would rather "eschew the obfuscation" or "avoid the confusion."

DOCID: 4009794

Solution to NSA-crostic No. 7 (CRYPTOLOG, April 1977), by L. R. Chauvenet, P12.

[redacted] "[The Thrusts and Boggles of] Outrageous Escalation", *NSA Technical Journal*, Vol. XIII, Spring 1968, No. 2:

"Not everything has to be *per se* in order to be real; reasonable deals were rarely mentioned but the old *quid pro quo* was much in evidence; but the true winner in the foreign competition was *vis-a-vis* . . . a beguiling Frenchy sound. . ."

(UNCLASSIFIED)

Letter

To the Editor, CRYPTOLOG:

I must confess that I thoroughly enjoyed -- even found hilarious -- the article in CRYPTOLOG entitled "A Medal for Horatius" (January-February 1977). I see the "colonels' club" was active in those days too! Having had a similar experience in the not too distant past -- trying to justify the awarding of a Legion of Merit decoration to one of my military subordinates, over the objections of various but nameless peoples and boards -- I found it gratifying to realize that inanity can also be humorous. Thanks for the laugh.

[redacted] B311

P.S. Thanks to Regular Army channels, the award finally came through.

(UNCLASSIFIED)

DID YOU GET YOUR INDEX?

The cumulative index (1974 through 1976) of CRYPTOLOG articles and authors' names was distributed in February according to a special distribution list. If you requested a copy but did not receive one, or if you did not request a copy originally but would like to have one anyway, please write to: CRYPTOLOG, P1, or telephone the editor on 5236s.

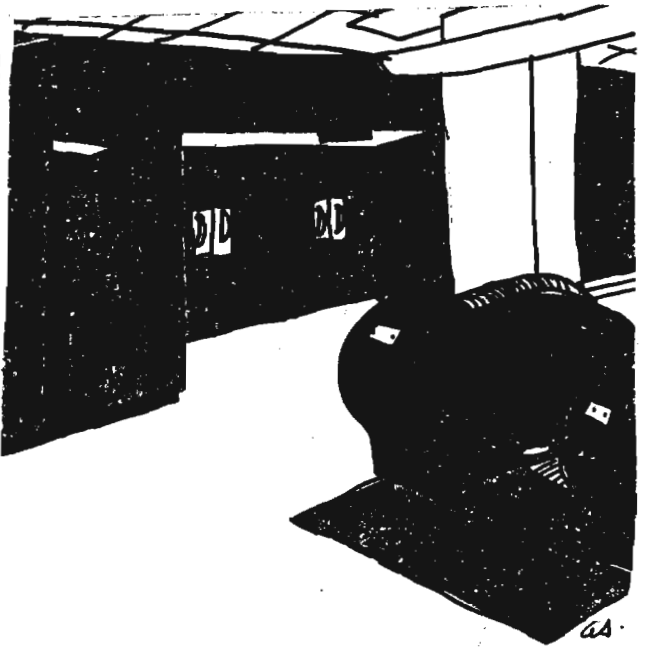
(UNCLASSIFIED)

ANNOUNCEMENT:

P.L. 86-36

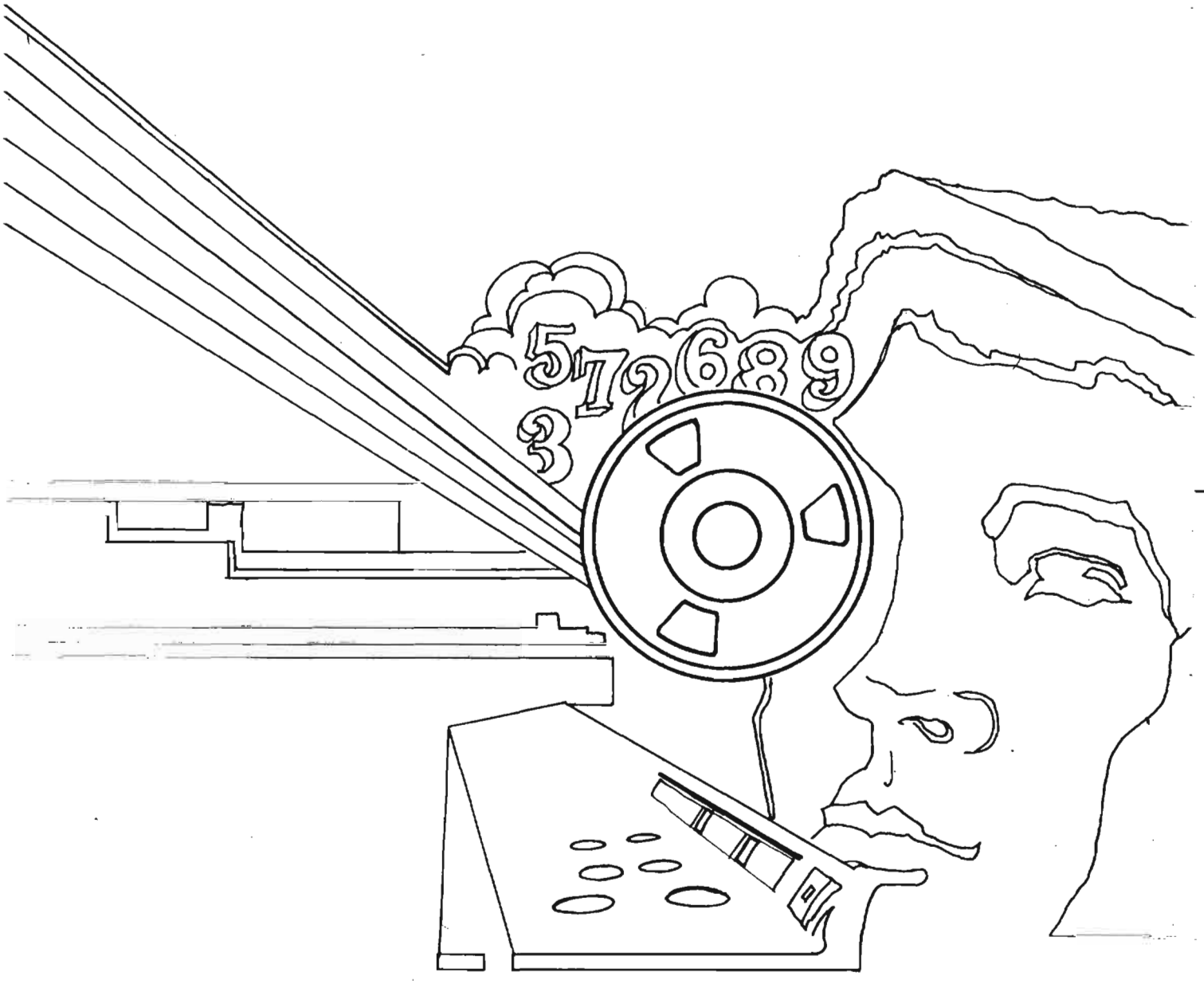
With this issue, [redacted] ends her tour as Cryptanalysis Editor of CRYPTOLOG. Betty has been a member of the Board of Editors since even before the first issue of CRYPTOLOG appeared in August 1974. In addition to contributing articles of her own ("What Should You Expect?, or, The Analysis of Cryptanalysts," August 1974; "Secrets of the Altars -- The Moustier Cryptogram," September 1974; "An October Overlap," October 1975; and "Twenty Years of Transposition," August 1975), Betty has been of invaluable aid in encouraging cryptanalysts, young and old, to write articles for CRYPTOLOG. In her current assignment, however, Betty has fewer opportunities to sniff out good articles, and therefore has asked to give this important job to someone else who has more such opportunities. [redacted] G42, has graciously agreed to become Betty's successor as Cryptanalysis Editor and promises to beat the bushes for good articles in that field. So, Betty, thanks for doing a wonderful job all these years, and, Alice, now it's your turn -- so, go get 'em!

William Lutwiniak,
Publisher



P1-Apr 77-83-25237

~~TOP SECRET~~



DOCID: 4009793

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

APRIL 1977

THE "ICE AGE" AND INTERNATIONAL SECURITY. [redacted] 1
"IT'S GOT TO GET OUT TODAY!".....Frances Blank.....3
CONTEMPLATING COMPUTING..... [redacted] 6
SOME THOUGHTS ON THE RUSSIAN P.Q.E..... [redacted] 7
NSA-CROSTIC No. 7.....L. R. Chauvenet.....10
THE LAST WORD ON I.A.T.S.....Cecil Phillips.....12
SWIFT/OLIVER AID ON CODE RECONSTRUCTION.....12
FLASH! 115TH S.R.I. LOCATED!.....A. J. Salemme.....13
LETTERS TO THE EDITOR.....19

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009793

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. IV, No. 4 APRIL 1977

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5642s)
Collection.....[redacted] (8955s)
Cryptanalysis.....[redacted] (8025s)
Language.....Emery W. Tetrault (5236s)
Machine Support.....[redacted] (3321s)
Mathematics.....Reed Dawson (3957s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Frederic O. Mason, Jr. (4142s)
Production Manager.....Harry Goff (4998s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4009793

During the last year or so, a number of scientific writers have published articles discussing cyclical recurrences of world ice ages, including the possibility of future recurrences. If the winter of 1976-1977 in the greater Washington-Baltimore area is any indicator, the next "cycle" could now be in its formative stage! As this article is being written (early January 1977), the Washington temperature is 13° F., and the chill factor is below zero.

Sometimes we do not appreciate that the Russians, as a whole population, have always lived with wind, ice, snow, fog, and extremely low temperatures throughout a great part of their country, all their lives, and through many generations of Russian peoples. By necessity they have learned to adjust to these severe climatic conditions. The important industrial and port city of Murmansk, for example, has 200,000 inhabitants living and working there year round (and the "greater Murmansk area" -- Murmansk Oblast -- has one million year-round inhabitants). Murmansk itself is located above the Arctic Circle, on the Kola Peninsula, at about 69° north latitude. It is hard for many people to realize that almost all of the state of Alaska is situated *south* of that latitude. The Soviet Union's largest and most potent fleet -- the Northern Fleet -- is headquartered near Murmansk at Severomorsk, and most of its ships operate from home bases located in and around the Kola Peninsula.

Fortunately for the Soviet Navy, the North Atlantic Drift, i.e. the northern reach of the famed Gulf Stream, finds its eventual terminus hard against the Kola coast. By the time it reaches those extreme latitudes, it carries just enough warmth to keep the southern Barents Sea relatively ice-free year round. Even so, the less mobile and less-warmed estuaries and riverine outflows freeze in the winter and have to be kept open through the continuous use of icebreakers. The Soviet Navy and merchant fleet rely heavily on icebreakers, including the new nuclear-powered ARKTIK-class super-icebreaker of 25,000 tons standard displacement. There are 45 icebreakers in the Soviet maritime service, more such units than of any other service-force type found in the Soviet Navy. (Submarine tenders are in second place.) Viewed in the naval context, icebreakers in the Soviet Union account for over 30 percent of the aggregate tonnage of the naval service force and for just over 9 percent of the aggregate displacement of the entire Soviet Navy.

P.L. 86-36

Prevailing winds across almost the whole of the Soviet Union emanate from the north and northwest in July and from the south and southwest in January. Highest actual temperatures in July do not, for the most part, exceed 70° F., and, in January, drop to from -30° to +30° F. Permafrost (perennially frozen ground) occurs extensively in the USSR. This creates extremely adverse financial and technical problems for development: small gains can be made only at great costs. Agriculture is negligible in such areas: there is little or no growing season. Most food supplies, as well as almost all manufactured goods must be imported. Any heat leaking from road surfaces or structures leads to flooding and soil subsidence, with considerable structural damage. Accordingly, public works and human habitability systems require special, costly engineering and cold-weather maintenance.

All of the Soviet Union is affected by only three seasonal climates:

- 80 percent of the country experiences cool summers and cold winters,
- Another 10 percent experiences a full summer and a cold winter, and
- The remaining 10 percent sees only a very short and very cool summer, followed by a very long and very cold winter.

Above 58° (latitude of Labrador) lies nearly half the USSR, where the soil is predominantly the high-latitude *podsols* (soils with acidic, nearly structureless upper layers) or the *andept inceptisols* (soils which contain high amounts of clay, are perennially or seasonally wet, and have little or no horizons of redistributed materials). These soil types are found on high-latitude wastelands, tundra, and ice caps, and millions of acres of coniferous forest, all of which areas are tractless and without access or inhabitation.

Given these adverse conditions, one sees the climatological sense of what appears to be a certain Russian predilection for cruises to warm-water ports, continous naval deployments in the Mediterranean Sea and the Indian Ocean, and sometime voyages to the Caribbean Sea, Philippine Sea, Middle and South Atlantic Oceans, and elsewhere below 40° north latitude. Such rangings of the Soviet Navy and merchant fleet should not be viewed with exclusive respect to their more obvious political, military, and economic dimensions. It does not seem altogether facetious to regard Soviet maritime expansion in a climatic and physiographic light.

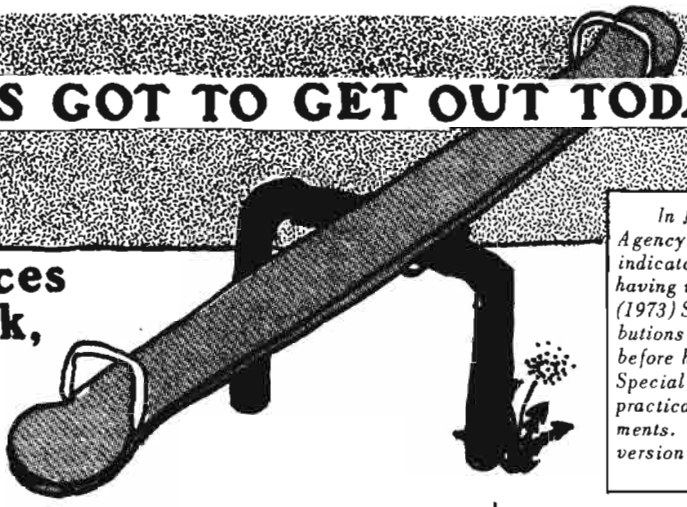
Consider, if only momentarily, the possible consequences for international security (that is, NATO) and U. S. national security of a gradually advancing future "ice age." (Here, there is neither the space nor the rationale to debate the merits of some of the climatologists' arguments.) Assume only that there will be another ice age in the imaginable future. With what increasing covetousness might the Soviets come to regard seaports and habitations below 50° north latitude? On the land, the Middle East, Africa, and South Asia could prove increasingly attractive. A place like Angola with a relatively small native population and an extremely large supply of largely undeveloped minerals and arable soils, seems properly worth a substantial commitment. In 1973, Angola already had the fourth-highest gross national product per capita of the approximately 50 African countries, and produced, *on a largely undeveloped basis*, 750 to 1220 calories per person per day. As early as 1963-1965, iron-ore production at Cuina and Cassinga was large enough to be listed in world economic atlases. Mackerel, sardines, and anchovies inhabit the waters off Angola, Gabon, and southwest Africa. The port of Luanda is well developed for general (dry) cargo transfer; the USSR merchant fleet is heavily specified in general (dry) cargo bottoms. In the Congo, immediately north of Angola, at Tchitondi, is located a fertilizer center which was able, in 1969, to produce 100,000-500,000 metric tons of phosphates annually.

One more point needs to be stated: If there is to be another slowly encroaching "ice age" (and the purpose of this article is not to take one position or another on that question), then the Soviets probably are, or will be, better informed on that subject than any other people in the world. Only Scandinavians, and North Americans -- although in nowhere near the numbers of Russians -- generally live in the high northern latitudes. Continuous Russian polar-research programs predate the October 1917 revolution. The continent of Antarctica was discovered in December 1817 by a Russian naval officer, one Lieutenant Thaddeus von Bellingshausen*, whose voyage, emanating from the Baltic Sea, was specifically tasked to see in what the "other" polar region consisted. Insofar as Soviet nonmilitary technology and research are highly developed, they are most highly developed in arctic-polar matters and in the transportation, exploitation, and industrialized habitation of the extreme latitudes. Their prior commitment to developing such potential as exists in those reaches of geography is driven by historical, geographical, and demographic necessity. On balance, the Russians probably stand to suffer more from a future ice age than do Scandinavians or North Americans -- or Chileans and Argentinians. The thesis of this brief discussion is merely that an advancing northern ice cap, pushing in its path the great ice pack, may have long-range implications for Soviet political, economic, and military expansion -- or may, even now, be a valid consideration not only in the United States and among its allies, but also certainly in the Soviet Union, where much of the cold-weather existence is experimental and delicate and from whence the only direction to move under insurmountable pressure is south.

---

*Editor's note: One reason why Antarctica has international status is because a lot of countries claimed to have "discovered" it around that time, including the United States, on the basis of the official log of an 18-year-old whaling captain from Stonington, Connecticut, whose crew had actually *disembarked onto the continent* and were cavorting around when they heard strange bells coming through the fog. Turns out it was Bellingshausen's ship, and the Russians had a good laugh out of it, saying, "Here we thought we had discovered a continent, even though we haven't seen it yet, and now we see that a young-punk American has beaten us to it!"

"IT'S GOT TO GET OUT TODAY!"



Frances Blank, G52

In January 1977 Frances Blank retired from the Agency after a long and distinguished career. One indicator of her high professional standards is her having won, jointly with [redacted] *the first (1973) Sydney Jaffe Award for Outstanding Contributions to the Language Effort at NSA. Shortly before her retirement, Ms. Blank spoke to the CLA's Special Interest Group on Translation, giving much practical advice based on her operational assignments. The following article is a slightly expanded version of that talk.*

Ed.

P.L. 86-36

Before any discussion of my ideas on translation of end product, a word of warning may not be out of place. I have frequently been told, when I expressed disapproval or amazement at certain procedures in other linguistic areas, "But you don't *understand!* You've always been in an old-line section. You don't know what it's like in other places." This charge is undoubtedly true, but since my views were formed and are colored by by own experiences, I cannot ignore them in discussing translation. So

[redacted]

As for languages, my experience has been largely in Romance, with some Germanic. Moreover, I have worked an unusually high proportion of flaps, swing and graveyard shifts, and holidays. For several years, Saturday or Sunday, or both, have been part of my regular work week. Indeed, the title of this article came to me one Saturday when I was trying to find

[redacted]

care! It's got to go out *today!*"

NSA translation, it has always seemed to me, is marked by three qualities:

- *timeliness,*
- *accuracy,*
- *style.*

I have listed these qualities in what I consider to be their order of importance. I am aware that there are many Agency linguists who would shout out, in outraged chorus, "No! In our work, accuracy is all-important!" Actually, if I were pinned down, I would come near to agreement. I question only the "all" part of it. Accuracy *is* important, but it has to be considered constantly in relation to timeliness.

Timeliness

[redacted]

EO 1.4.(c)
~~TOP SECRET UMBRA~~ P.L. 86-36

EO 1.4.(c)
DOCID: 4009793
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

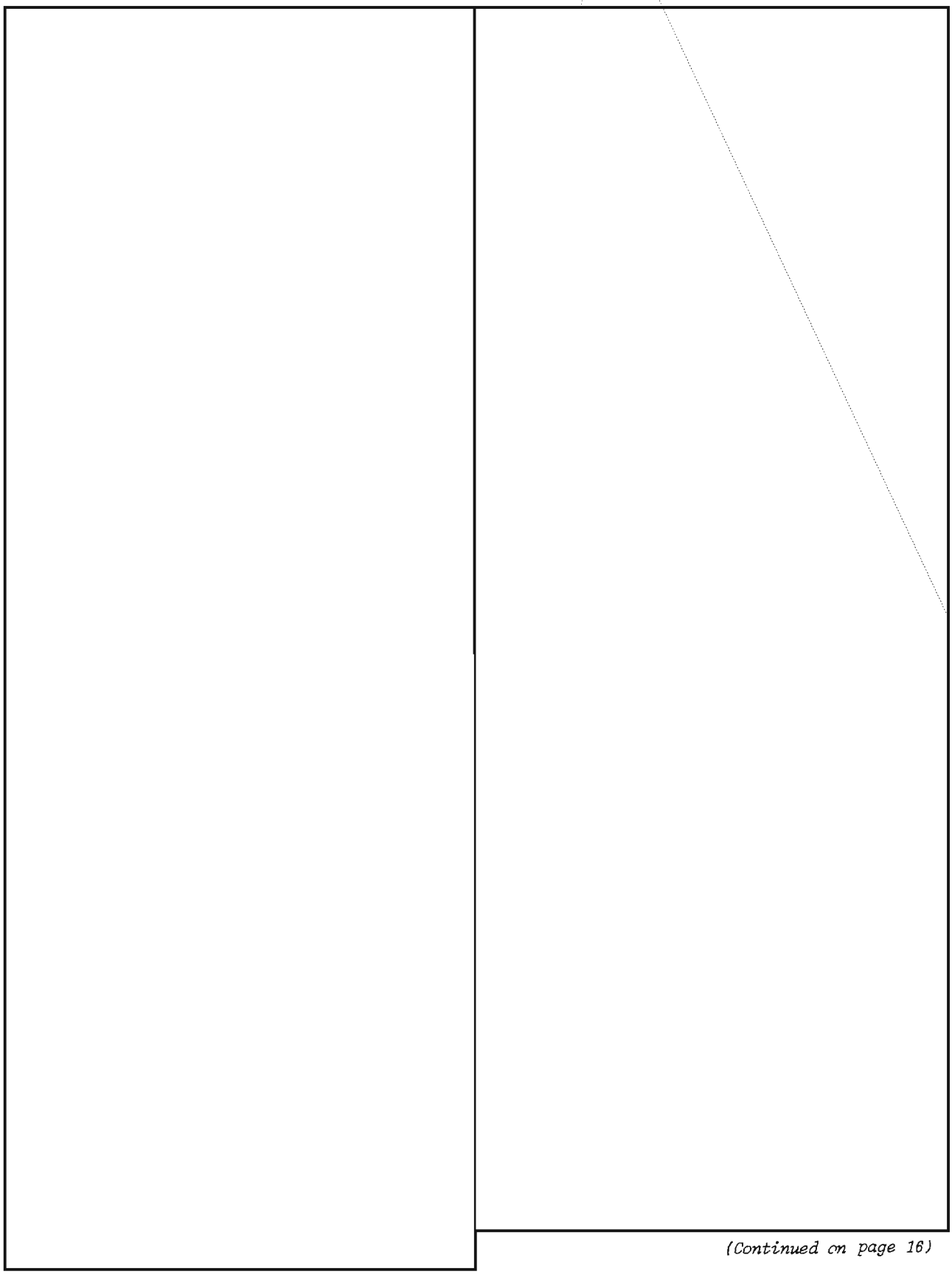
Anyone named Blank understands about sensitivity to names. In fact, when Hecht's first installed its computers and elected to call me Frangert Blank, I protested by letter the first month. Then I marched down to Hecht's the next month and told the lady in Complaints that, much as I valued my Hecht's charge account, I was going to have to cancel it because my ulcer simply would not endure facing Frangert every month. Fortunately, she had a sense of humor.

And what about abbreviations? The translator is instructed to expand them. Yet BP, KLM, and BMW are better known than their expansions. And how many people can expand *fob*, *rif*, or even *a.m.* and *p.m.*? TV hasn't quite reached that point now, but I suspect that in another generation there will be people who do not know the expansion for TV. In the same way, many abbreviations in the traffic, quite exotic to the translator, are old friends to the real customer. Certainly expand them if you can, but do not delay publication, or waste time looking for them. Your customer will know.

EO 1.4.(c)
P.L. 86-36

DOCID: 4009793

EO 1.4.(c)
P.L. 86-36



(Continued on page 16)

CONTEMPLATING COMPUTING

W16

Computer listings and "IBM cards" are such commonplace items in our lives here at NSA that most of us probably take for granted the rather awesome capability that lies within the Agency's high-speed digital processors. Similarly, many of us probably take for granted the computer power that is readily accessible to anyone who can afford even the simplest pocket calculator.

It was not too long ago that the type of calculation that we perform today in fractions of a second had to be done by hand with the aid of logarithm tables. The very tediousness of the operations prevented many problems from being considered. Today, using high-speed computers in combination with mathematical techniques the principles of many of which have been known for a century or more, we are able to perform operations that would have been unbelievable to a nineteenth-century mathematician.

For example, recently Morrison and Brillhart (M. A. Morrison and J. Brillhart, *Math. Comput.* 29, 183, 1975) tackled the problem of discovering the prime factors of $2^{128} + 1$. This is the 39-digit number:

340,282,366,920,938,463,463,374,607,431,768,211,457.

Their answer, determined after about 1 1/2 hours of computer time, is:

5,704,689,200,685,129,054,721

x 59,649,589,127,497,217.

To place this in perspective, let us see what would be involved if we simply approached this problem without an algorithm and tried to work our way up to the smallest factor, starting with 1. There are 31,556,952,000,000 microseconds in our year -- a 14-digit number. Assuming that, in our search for the smaller factor above -- a 17-digit number -- we use a computer capable of performing one operation per microsecond, it could require about 2000 years of our machine time to find this number. By the way, this is not simply an exercise for the fun of it. The factors of $2^{128} + 1$ are of use in designing codes for space communications, and the same type of considerations arise today in carrying out some of NSA's challenging communication tasks.

This capability has arrived during the lifetime of most of us, for the first electronic computer was the University of Pennsylvania's ENIAC, operational in 1946. One might contemplate the implications of the rapid increase in computer speed. The adding speeds for 10-digit numbers are of the order of the following:

		Additions per second
19th, early 20th century	mechanical calculator	4
1960s	medium-speed computer	200,000
today	high-speed computer	200,000,000

Knuth (D. E. Knuth, *Science*, 194, No. 4271, 1236, 1976) compares this acceleration to that of transportation speeds:

	Miles per hour
snail	0.006
man walking	4
U.S. automobile	55
commercial jet plane	600

Even if we add a nominal near-earth satellite, with a speed of 17,400 miles per hour, the ratio of the computation speed of today's computer to mechanical calculator is approximately 11,500 times greater than the speed of our satellite compared to a man walking. When one notes the cultural impact the transportation-speed increase has had on mankind, can one help but wonder what the computer impact ultimately will be?

DOCID: 4009793

Another aspect for contemplation is our growing dependence on computers and calculators In our division, if the computers are down, so is our productivity. This dependence was strikingly called to my attention on a recent airplane flight where two individuals seated next to me were assembling cost figures on their week's sales efforts. When it came time to add up the column of figures, they discovered their pocket calculator was discharged. One then told the other, "I no longer trust myself in adding figures like this since I have grown so used to using my calculator." They put their work away without the final sum.

It was not too long ago that agility in mental arithmetic was widespread. This was particularly true of astronomers, who had numerous dreary calculations to perform. One very well-known American Astronomer who possessed a remarkable mental calculating ability was Truman Henry Safford (1836-1901). Ashbrook (J. Ashbrook, *Sky and Telescope*, November 1976, p. 346) has uncovered some documentation, which there is no evident reason to doubt, illustrating Safford's talents. I repeat several of the anecdotes here.

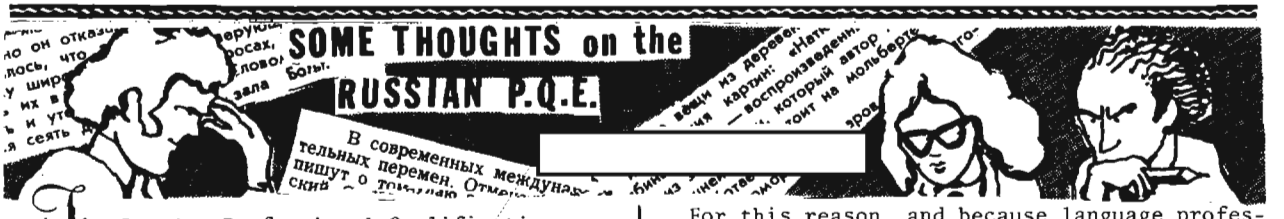
A friend gave Safford the following problem: "Suppose I was born at a certain hour, minute, and second of a certain day of a certain year (where the friend supplied values for the certain), how old would I be, in seconds, at noon today? Safford walked up and down along a blackboard and told him the answer. The friend responded, "No, that is not correct, for I have worked it out and the answer is different." "What was your answer?" asked Safford. When he was told, he retraced his path along the blackboard and then exclaimed, "Oh, you forgot the leap years." Safford was right.

Safford's ability was recognized by the time he was 9 years old. An interviewer asked him, "How many acres are in a circular piece of ground with a circumference of 31.416 miles?" The child flew around the room and in a minute answered, "50,265.6." He was next asked, "What is the entire surface of a regular pyramid whose slant height is 17 feet, the base a pentagon of which each side is 33.5 feet?" In about 2 minutes he replied, "3,354.5538." He could routinely take a column of about 40 numbers with from two to four figures in each number, and in about 5 seconds write down the sum of the squares of these numbers.

Perhaps the most astounding feat was when he was asked to square 365,365,365,365,365,365. It is reported that in less than a minute he gave the answer from left to right:

133,491,850,208,566,925,016,658,299,941,583,225.

It took me considerably more time than this to verify the answer using the calculating tools I have available from my desk. If anyone reading this can do this type of calculations in his or her head, we could use you when the computers go down! (U)



The Russian Professional Qualification Examination (PQE) is a topic guaranteed to stimulate lively discussion among NSA's Russian linguists. And if you want to get into a really heated conversation, spend an hour or so with an aspirant who has failed a portion of the PQE more than once -- he will have a definite opinion on what can be done with the PQE. The frustration, despair, and anger of such an aspirant are understandable for, it seems to him, his career advancement and promotion are inseparably linked with passing the test. To some, particularly those who have been with NSA for only a few years, the PQE becomes the added frustration that makes working at NSA almost unbearable. Unfortunately (perhaps fortunately in some cases), some linguists eventually begin boycotting the tests; others seek job reclassification to pursue a career elsewhere. The loser in such cases is NSA because, usually, large investments in time and money have been made to train the aspirant to become what he will not be if he abandons the language career field.

For this reason, and because language professionalization is a particularly timely topic, I would like to share with CRYPTOLOG readers a sampling of the opinions expressed by discouraged aspirants. Some expressed feelings which are no more than vague complaints about the "unfairness" and "irrelevancy" of the PQE; others have voiced more compelling evaluations and arguments. It is my intention here to note only those valid and reasonable complaints which are, in my opinion, worthy of the Language Career Panel's consideration. The audience I have in mind is those Agency linguists who are receptive to criticism and who are in a position to effect meaningful changes in PQE policy. I also wish to address the aspirants, those who are finding it difficult to pass all parts of the PQE, and those who will soon be taking the tests for the first time, to ask for their forbearance as well as their suggestions, and to reassure them that the "test-makers" are aware of their frustration and are striving to devise better tests.

~~(CONFIDENTIAL - CCO)~~

P.L. 86-36

~~CONFIDENTIAL~~

EO 1.4.(c)
P.L. 86-36

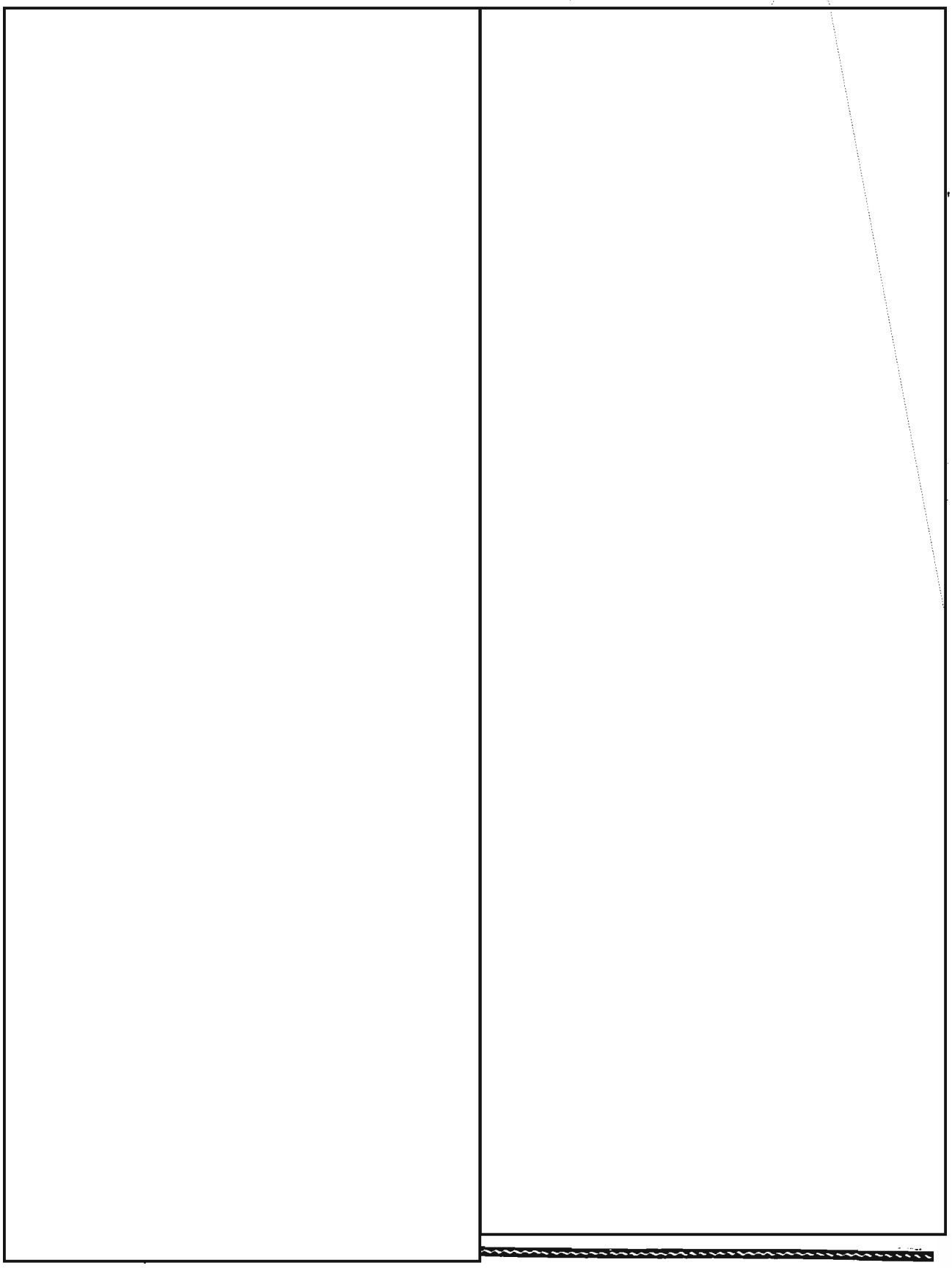
There is clearly a need for a testing program to determine which Agency linguists are of a "professional" caliber. Academic credentials alone are not enough. However, the effectiveness of Parts IIA and IIB in particular in filling this need is clouded by the following factors:

In this light we need to ask ourselves a few searching questions. Such as, does a "pass" on either Part IIA or IIB tell us with any certainty that an aspirant is a professional linguist? Or does it tell us only that the aspirant has finally succeeded in passing the test? And, finally, how many professionalized linguists could pass the test a second time? There are no clear answers to such questions, but, on the basis of the large number of linguists who repeatedly fail, it is obvious that, for many Agency Russian linguists, Parts IIA and IIB in their present form are a formidable, perhaps an unfair, barrier to the professionalization which has become an important criterion for promotion.

~~CONFIDENTIAL~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36

~~CONFIDENTIAL~~



NSA-crostic No.7

The following NSA-crostic was submitted by guest NSA-crostician L. R. Chauvenet, P12.

The quotation on the next page was taken from a published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS

A. Caesar's mother

B. Reflector

C. Deep dish fruit pie

D. If two do it, it may make a to-do (3 wds)

E. Ready

F. Eager

G. A Vermont answer to the question, "Have you lived here all your life?" (2 wds)

H. Part of a ton

I. An opinion of the paleface

J. What the sign carried by the tackle said (4 wds)

K. How a burden might feel to a left-handed man (2 wds)

L. You can do this with flowers

M. Concentrated quarters of a racial minority

N. We sometimes hope retirement will bring us a life of this

O. Yellow green

P. Lacking nourishment

Q. A call to dinner which made the Frenchman suspicious (2 wds)

R. A branch of philosophy

S. "Would she could make of me a saint, or I of her a ------"

T. Common meeting place

U. What the prisoner said when the judge shouted, "Order in the court!" (4 wds)

V. Matter in a state

WORDS

66 15 146 120 89

141 105 37 134 71 7

139 34 75 111 64 162 171

82 145 5 80 165 1 55 127 123

59 84 112 167 21 142 50 106

47 104 154 181

149 178 113 65 110 3

148 119 46 99 73

164 137 14

17 175 31 4 138 87 158 96 72 36 151 41

118 70 163 10 129 100 6 53 157 176

61 126 29 156 102 169 52

13 115 38 69 77 28

143 63 116 131

93 54 11 153 135

85 12 170 103 51

155 2 92 88 24 81 173

25 177 9 79 107 33 101 174 152

44 26 168 108 57 23

109 42 124 117 67 58

160 130 95 97 18 180 60 8 20

40 147 91 98 136 30

W. Confuse

39 83 74 166 172

X. Water conservation expedient (3 wds)

78 179 48 132 45 62 144 121 90

Y. Why my picture might have made it seem I was twins (3 wds)

86 56 43 159 114 150 140

Z. Proprietor

133 94 27 125 32

Z_1. What you might do to alleviate the condition of Word P (2 wds)

68 122 19 161 49 22 35 76 128 16

1 D	2 Q	3 G	■	4 J	5 D	6 K	7 B	8 U	9 R	10 K	11 O	12 P	13 M	■	14 I
15 A	16 Z_1	■	17 J	18 U	■	19 Z_1	20 U	■	21 E	22 Z_1	23 S	■	24 Q	25 R	■
26 S	27 Z	■	28 M	29 L	30 V	31 J	32 Z	■	33 R	34 C	■	35 Z_1	36 J	■	37 B
38 M	39 W	40 V	■	41 J	42 T	43 Y	44 S	45 X	46 H	47 F	48 X	49 Z_1	50 E	■	51 P
52 L	53 K	54 O	55 D	■	56 Y	57 S	58 T	59 E	■	60 U	61 L	62 X	63 N	64 C	65 G
■	66 A	67 T	68 Z_1	69 M	70 K	71 B	72 J	73 H	74 W	■	75 C	76 Z_1	77 M	■	78 X
79 R	80 D	■	81 Q	82 D	83 W	■	84 E	85 P	86 Y	87 J	■	88 Q	89 A	90 X	■
91 V	92 Q	93 O	■	94 Z	95 U	96 J	■	97 U	98 V	99 H	100 K	■	101 R	102 L	■
103 P	104 F	105 B	106 E	107 R	108 S	109 T	110 G	■	111 C	112 E	113 G	■	114 Y	115 M	116 N
■	117 T	118 K	119 H	120 A	■	121 X	122 Z_1	123 D	124 T	125 Z	126 L	■	127 D	128 Z_1	■
129 K	130 U	131 N	■	132 X	133 Z	134 B	135 O	136 V	137 I	138 J	■	139 C	140 Y	141 B	142 E
143 N	144 X	145 D	146 A	147 V	148 H	149 G	■	150 Y	151 J	152 R	■	153 O	154 F	155 Q	■
156 L	■	157 K	158 J	159 Y	■	160 U	■	161 Z_1	162 C	163 K	164 I	165 D	166 W	167 E	168 S
169 L	■	170 P	171 C	172 W	173 Q	174 R	175 J	176 K	■	177 R	178 G	179 X	180 U	181 F	■ L.R.C.

(Solution next month.)

EO 1.4.(c)
P.L. 86-36

THE LAST WORD ON IATS?

CECIL PHILLIPS, C03

[redacted]

~~(CONFIDENTIAL — CCO)~~

Swift/Oliver Aid on Code Reconstruction

The revised edition of *Collected Articles on Code Reconstruction**, compiled by Katharine Swift and [redacted] is now available.

The foreword of the 314-page publication states:

"This collection of articles, most of which have previously appeared in various Agency publications, is a revised version of a collection edited by Katharine Swift which was published in 1973. A demand for more copies after depletion of the supply has necessitated an early revision.

"While it has not been possible to include all pertinent articles in one publication, it is hoped that managers as well as book-breakers and programmers, and senior analysts as well as neophytes, will find material that will help each in making his individual contribution on the job.

[redacted] Editor"

Anyone with a Top Secret Codeword clearance can obtain a copy of the publication by calling Harry Goff, P16, x4998s.

~~(FOUO)~~

*Publication of Cryptanalysis Department, National Cryptologic School, 1976. TSC, CCO, S-212802.

 P.L. 86-36

FLASH! 115th S.R.I. LOCATED!

A. J. Salemme, P16

Now that everyone is writing in to Fred Mason, filling in the gaps in his excellent compilation of radio stations ("Where Were We?", CRYPTOLOG, January-February 1977), it's time for me to add my bit. Where Fred has:

RADIO INTELLIGENCE COMPANIES	
111, 112, 125, 126 under Gen MacArthur in SW Pacific	4 4 2345?
113, 114, 116, 117, 118, 121, 124 129, 137 in Europe	2345?
115, 119, 120, 122, 123, 127, 130-136, 138 unlocated	2345?

I'd like to add:

115th Sig Rad Int Co, Presidio, S. F. 4 3 4 4
115th Sig Rad Int Co, Fort Lewis, Wash. 456

How do I know? Because I was there! And the memories those terse entries evoke!

In the hot summer of 1943, I, a city boy who had never seen a real horse, took my basic training at Fort Riley, Kansas, in what was the last horse-cavalry (the real troopers all called it the "hoss-calvary") unit in the U. S. Army. They tried to teach me, first of all, to ride a hoss. Rule 1: "Take care of your hoss first." We would ride out to the riding-practice area and ride around in a large circle while the drill instructor in the middle would holler, "I said 'Canter!' Who told you to gallop?" I clearly remember one day when I was on the horse one minute and seated on the ground the next, with no recollection of what must have been the majestic flip that made the transition between the two states. ("Who told you to dismount, trooper?") After practice, we'd go back to the stables, rub down and curry the horses, wipe the horse sweat off the gear and saddlesoap it, clean out the horse's hooves, clean the dock, etc. And *then* lead the horse to water. Believe me, he would want to drink! But you had to slow him down. ("You kill that hoss with cold water, trooper, and it'll be statement-of-charges for you!") Put the horse back in the stall and then, only then, could you, the trooper, get a drink of water for yourself. And did that vile-smelling Kansas water coming out of a green-encrusted faucet ever taste good! To this day when, watering the lawn on a hot day, I pause to take a gulp of water from the hose, the taste of the brass nozzle takes me back to Fort Riley.

The second thing they taught me at Fort Riley was Morse code. The Army's idea was to send me, along with other city boys (no one I knew who actually yearned to be in the hoss calvary and wear those distinctive jodphurs and high boots actually made it), to a radio reconnaissance outfit. We practiced our Morse code and practiced establishing radio contact. One guy would send while the other cranked a portable hand generator. Then we would break down the equipment, load it onto our two hosses, and move to the next stop. The concept was to send us poor excuses of hossmen and Morse operators -- would you believe? -- *ahead of* our troops on those steamy South Pacific islands, with our hosses crashing quietly through the underbrush, until we detected some Nips, and then get off our hosses, set up business, and start transmitting the news back to base -- one guy cranking, and the other asking, "Is B dah-dit-dit or dit-dit-dah?"

Sure enough, basic training completed, I was sent to a radio recon outfit in San Rafael, California, which, I suppose, was as close as they could get to simulating the South Pacific jungle conditions. When I arrived, it turned out that they didn't even *have* hosses! They had *vehicles* (pronounced, invariably, "vee-HICK-les"). So forget the canter and gallop! Now the city boy, who had never driven a car yet (we was pore city folks) had to learn driving while double-clutching on a two-and-a-half-ton half-track. (Drill instructor: "Do not scoff at the two-and-a-half-ton half-track, gentlemen! It is a for-MID-able vee-HICK-le!") We would drive up into the California mountains and establish radio contact. "We don't use Morse code. We just stick in these crystals and talk into the mike. But watch what you say, because they're monitoring us!" I remember once, driving through -- what *was* it? steam? fog? what? -- on the top of a mountain. Then it dawned on me. "It's a cloud!" City boy had discovered that clouds aren't solid like mashed potatoes -- they're nothing but fog up high.

In driving through the mountains, Rule 1 (replacing "Take care of your hoss first") was "Always remember to close the farmer's gate." We would open the gate, dismount, close the gate, and then drive up paths that a mountain goat would wince at. I'll never forget the time when the driver (not me!) misjudged the width of the path and that massive two-and-a-half-ton hulk slid sideways, finally resting at a 45-degree angle against one tightly-drawn strand of barbed-wire fence. If I had been brave enough to lean out the window and pluck that strand, the "Bo-o-o-o-ing!" would still be reverberating around the world. Were we worried? Sure! That if the barbed-wire strand broke and we tumbled down that ski slope, vee-HICK-le and all, some farmer would be mighty mad. Not only that, but there'd be a little matter of a statement of charges for the half-track. If I remember the physical and fiscal terror of the situation, why don't I remember how we got out?

We used to simulate maneuvers. I remember one night, long, long after missing evening chow ("You'll get your chow after you find your way back to base!"), being told, "Okay, Salami! [no one ever did get the name right] Contact base and arrange for rendezvous!" Instead of things like dah-dit-dit vs. dit-dit-dah, I had to worry about things like which crystal to use and what's a beat frequency? Plus those daily-changing codewords for locations. One day CUCUMBER would mean "the firehouse in Petaluma" and SPARROW would mean "City Hall in San Rafael," and the next day they'd be something else. I remember one night (my rebellious gastric juices made me do it!) when, in order to resolve an insoluble rendezvous problem, Radio Operator Salami blatted out in the clear, for all the monitoring operators to hear and record, "Where are we supposed to meet, anyway? Is BETTY BOOP the firehouse in Petaluma or the City Hall in San Rafael?" Not only did I not get to crash a hoss through the South Pacific jungle (did *anyone*?), but I didn't get to crash a for-MID-able vee-HICK-le through it either. No, within a couple of months of my arrival in signal reconnaissance, I was transferred to signal intelligence. It was obvious, from my having flunked my "response to crisis" test, that I sure needed some.

And so I arrived, in November 1943, at the 115th Signal Radio Intelligence Company, Presidio of San Francisco, California. For 4 or 5 months, World War II was rugged, I mean to tell you! Every time that the Golden Gate Bridge is flashed on television (and that's pretty frequent, even without the opening credits for "Phyllis"), one of my kids will say, "Yeah, Dad, we know, we know! They used to make you put on full field equipment, march to the middle of the bridge, and then run non-stop to the other end!" (End of "War is hell" reminiscence.)

Since I was supposed to know Morse code, it was easy to teach me a few niceties like the Japanese Morse code (Kana syllabary) and abbreviated numerals, and make me a Japanese intercept operator. Okay, then, a week of the new frills and onto the job! That meant driving up to the highest hill in the Presidio to the intercept station (it was called "Fubar," an acronym meaning something like "Fouled up beyond all recognition"), and trying to pick up Japanese Morse signals. Some nights they were mighty sparse. It had something to do with the Heaviside layer -- I couldn't figure it out. A lot of guys would switch instead to local San Francisco stations, listen all night to the Andrews Sisters (". . . with anyone else but me-e-e-e"), and put "NIL HEARD" in their log. That was risky, though, because there was a central control room from which the trick chief could patch into any receiver and hear what you were listening to. He could talk to the intercept operator and help him adjust his signal. Or he could even send Morse code to him. In fact, he would often do that very thing, in order to dispel his own boredom and to provide training for some Andrews Sisters fan who had twisted his vernier a fraction of a second (they didn't have nanoseconds then) too late. I remember one night when Farley was caught that way. The trick chief started sending, from his control booth, a series of Japanese messages that had been intercepted the night before. Everyone was in on the gag but Farley. We clustered around him, saying, "Hey, everyone! Farley's the only one who's picking up a signal!" Farley would feverishly copy the messages. Occasionally he would say, "Dammit, I missed a group!" Miraculously, the "operator in Tokyo" would repeat that group. "Dammit, he's sending too fast!" Miraculously, the "operator in Tokyo" would slow down. After a couple of hours, Farley was still "copying traffic." The trick chief decided to cut it off by carrying out Farley's every wish in ways that should have made it clear to him that it was all a big hoax. But whatever ridiculous thing he did, or whatever we other guys said, Farley kept "copying traffic." Finally, the trick chief sent a message with an address line reading, not in Japanese Morse code but, unbelievably, in International Morse code, "ATTENTION STUPID AMERICAN FARLEY." Farley jumped up, shouting, "Hey, they're sending this one to the Postmaster General!"

But what if the trick chief didn't enliven the proceedings that way? The nights would really drag as we tried to pick up Tokyo. And how many times can the same joke work? Or the joke of crumbling up a pile of intercept paper and setting it on fire under the hard metal chair of a snoring intercept operator with his hand frozen to the dial as he "searched for a signal"?

If anything went wrong -- such as putting "NIL HEARD" in your log when another operator on the other side of the room heard a signal loud and clear on the same frequency -- you might see your name posted on the "Discrepancy List." I remember one country boy asking, "What does that-there 'discrepancy' mean, anyway?", and a city boy replying, "It means 'you keep up dis-crep-an-see how long you stay in this outfit!'"

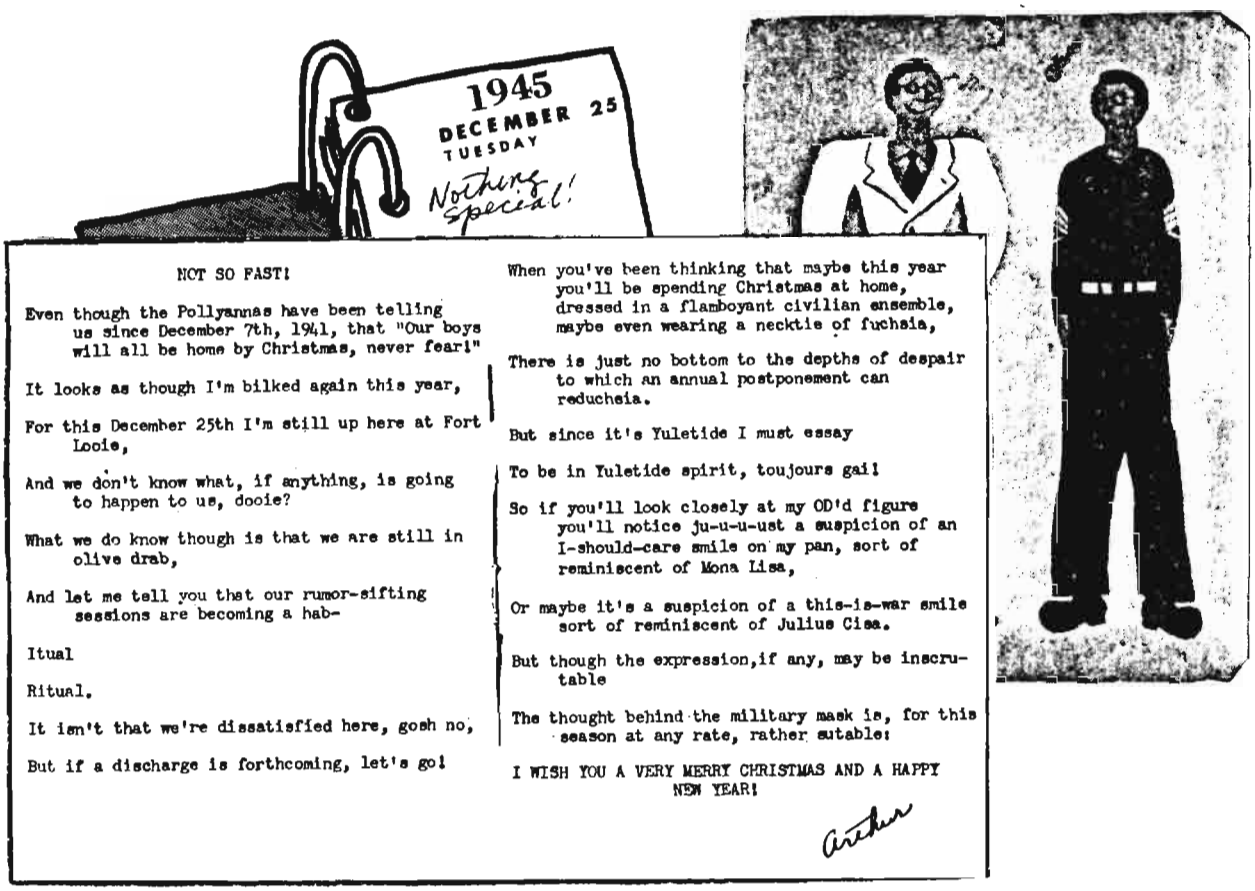
In the spring of 1944 the 115th moved to Fort Lewis, Washington, probably because the audibility was better there. And there I stayed, as a Jap intercept operator and, later, as a Jap traffic analyst (my, that was a prestigious jump!) until my discharge in March 1946. I did have a little TDY interlude, however. After I had been a practicing traffic analyst for more than a year, another fellow and I were sent to Vint Hill to take a 2-month course in Introductory Japanese Traffic Analysis. We joined a group of 20 guys just out of basic training, during which they had learned Morse code ("Is B dit-dah-dit-dit or dit-dit-dah-

DOCID: 4009793

dit?"). When, all by myself (the other guy had taken some leave en route), I showed up in class, 20 guys shouted in unison, "Hey, it's Goldberg!" What do you mean? Well, it seems that this group of New York wisenheimers had invented a twenty-first member of the group -- Goldberg -- so that, each day, one guy could disappear, someone else would respond "Yo!" to Goldberg's name at roll call, and the head count would come out right. (Some of those wisenheimers are probably now writers for "Hogan's Heroes" -- they really knew how to fight a war.)

All I remember from the TA course is the instructor telling us that the time difference between Tokyo and Washington state was so many hours. Maybe ex-hossman Salami couldn't tell a canter from a gallop, and ex-radio operator Salami couldn't tell CUCUMBER from BETTY BOOP, but, dammit, he knew his time differences! He had the temerity to tell the instructor that the computation was an hour off -- we had to consider Pacific Daylight Saving Time. No, says the instructor, "the book says. . ." No matter that I had worked many a long, dull night in that intercept shack and I knew that when I got off duty, it was midnight in Tokyo. No, "the book" won.

TDY over, it was back to Fort Looie, as it was called. The only things I remember about the rest of my tour there include some useless facts that I'll take with me to my grave, such as the routing number for "TOKYO AIR" -- 26907, according to a system in which the fourth digit was always a zero or a 5, and the fifth digit showed the total in noncarrying arithmetic. I also remember the things I did to fight off the boredom during off-duty hours between shifts while stuck in the boondocks. Like trying to tie my extra shoelaces in that funny braided way that only the Regular Army guys could master. Or taking a USAFI (U. S. Armed Forces Institute) correspondence course in Russian ("So *that's* how he started!"). Things like that. The last Christmas there, however, I made a lot of Christmas cards, including in each one a poem I wrote, imitating but not quite approximating Ogden Nash. One of the cards survived the holocaust of World War II and, strange to say, the poem in it was printed recently on the back cover of the Winter 1976 issue of the Phoenix Society's *Phoenician*. The reprint didn't bear a date or any word of explanation, so it looked to the uncritical eye like a "Christmas 1976" message. One NSA-er even asked me a couple of times why I wrote the poem "as though" I was in the Signal Corps in 1945. I'd like to assure him, and anyone else who was confused by the *Phoenician* reprint, that it wasn't "as though" I was in Fort Looie in December of 1945 and until March 1946. I really was! Fred, believe me!



DOCID: 4009793

EO 1.4.(c)
P.L. 86-36

~~TOP SECRET UMBRA~~

"...out today!"

(Continued from p. 3)

research not only delays publication of the message being researched, but all subsequent ones.

One factor that helps timeliness is any kind of background knowledge you happen to have -- in history, literature, the comics. It is amazing how many odd kinds of information come in handy.

[redacted] Within a reasonable period of time I have seen references to:

- the "Gray Eminence" (French history -- the reference puzzled one young translator very much),
- "Adamastor" (Portuguese literature -- I tried hard to ungarble that),
- "Fabius Cunctator" (Roman history),
- Latin phrases -- *obtorto collo, sic rebus stantibus, primus inter pares,*
- "the Prime Minister is required to steer between Scylla and Charybdis" (Greek mythology),
- "These findings, unsatisfactory as they are to a Cartesian mind" (French science),
- "He refuses to go to Canossa" (medieval history -- if the allusion is unknown, finding that Canossa is a small village in the Alps is not very helpful),
- "the Draconian program passed by the Italian Parliament" (Greek history),
- "the sword of Damocles hangs over his head" (Greek mythology),
- "he is a quisling" (modern history),
- "Yalta" (this is *not* Malta, as some younger translators are inclined to ungarble it, while admitting that it makes no sense).

Any or all of these, if not recognized by the translator, may take much of his time to research or, unfortunately, attempt to degarble. Such background information may come, not only from newspapers or collateral, but from paperback novels, science fiction, and, for all I know, from *True Story Magazine*. All of this is grist to a translator's mill.

Style

The word "style" suggests different things to different people. Some authors, translators, and editors -- especially those in the outside world -- think that style is concerned with making the text sound "elegant," with such things as never splitting an infinitive or changing the word "horse" to "equine quadruped." In the field of COMINT translation, however, "style" means just one thing -- translating the foreign text into completely unambiguous English. It is *not* concerned with "elegant variations," and therefore, if a foreign writer, for example, uses the word "section" repeatedly, the translator sticks to it. Because the customer is not always able to ask the translator, "Does the word

[redacted]

"A good translation," my Latin teacher used to say, "is one in which I can see where you got every word, but which reads as though it had been written in English." This is, of course, a goal to strive for, not to be attained. But, even so, in the interest of the readability I mentioned earlier, a translator should make sure that his adverbs clearly modify the right word, his adjective clauses attach to their antecedent nouns ("which" clauses dangling several words after their antecedents are, if not actually ambiguous, at least temporarily confusing). Try to avoid juxtaposing two words which normally go together if, in the passage in question, they do not belong together. True, if given enough time, the reader will work out the ambiguities, but in the intelligence field, time is of the essence. Many years ago I read

> "Lake Leman lies by Chillon's walls.
> A thousand feet in depth below,
> Its massy waters meet and flow;
> Thus much the fathom line was sent
> From Chillon's snow-white battlement
> Which round about the wave enthralls;
> A double dungeon wall and wave
> Have made -- and like a living grave. . ."

It took me 20 years to get that passage parsed and realize that "wave" is not the object of the prepositional phrase "round about," but the subject of the verb "enthralls"; and that "double dungeon" is not a modifier of "wall," but the object of the verb ("wall and wave have made a double dungeon"). NSA's customers should not have to wait 20 years to realize what the translator is saying, nor even have to read a sentence twice.

P.L. 86-36
EO 1.4.(c)

In the above excerpt, the words "dungeon" and "wall" form an unfortunate juxtaposition: they constitute a good concept and *want* to be read together. Poetic license allows the poet to write this way, and allows the reader

[redacted]

~~TOP SECRET UMBRA~~

Every language has its own characteristic translation problems. In Italian the abstract noun and the third-person impersonal subject are very popular. In English the active verb carries much more weight. Train yourself so that when you see, in the foreign text, "There is a tendency on the part of the Germans toward doubt," to make your pencil write "The Germans tend to doubt," without your having to think too much about why or how you are doing it. And don't allow yourself to fall into the habit of writing out a translation on a tablet sheet and then "Englishing" it. It wastes time. If translation into a dictaphone becomes more widespread, the ability to produce a fairly smooth translation first off will be essential. Listen mentally to your proposed translation to catch the awkward spots. "The statement states that the member states will make a statement on the state of their defense."

How to Use a Dictionary

For some time in this discussion I have been wanting to say something about dictionary usage. But I am not sure where is the best place to discuss it, because the dictionary is closely connected with all three essential elements of translation -- as a tool for accuracy and as a guide for style, but also, improperly used, as an enemy of timeliness. Yes, there is a wrong way to use a dictionary, namely, to believe that no word may be used in a translation unless it can be found in a dictionary as equivalent to the foreign word being translated. This erroneous belief leads to "dictionary hopping," the waste of time, and the use of a second- or third-choice word. I am sure that every checker, suggesting a different English word to a novice (or sometimes a not-so-novice) has heard, *ad nauseam*, "I *wanted* to say that, but I couldn't find it in the dictionary," or the opposite, "I know that the English doesn't make sense, but that's what it says in the dictionary!" And yet, even the dictionary compiler is human. I have seen some quaint, if not downright hilarious, English renderings of foreign words in dictionaries, even in the "standard" languages such as Italian, French, Spanish, or German.

To show the impossibility of relying wholly on dictionary synonyms without using critical judgment, I quote from "Teaching English as a Second Language," *Toronto Education Quarterly*, Winter/Spring 1968, as published in *Today's Education -- NEA Journal:*

> "What happens when we consider only the words of a language and not their cultural connotations? One difficulty arose with electronic computers designed to translate from one language to another. The sentence 'The spirit is willing but the flesh is weak' was fed into a computer, translated into Russian, and then back into English. It came back as, 'The liquor is good but the meat is rotten.' The same process was followed with the headline, 'Mary suspended for youthful prank' and it came out as 'Mary hung for juvenile delinquency'. . . 'Out of sight, out of mind' went into Japanese and returned to English as 'invisible, insane.'

I am certain that, if one could have asked the computer, it would have said plaintively in each instance, "But that's what it said in the dictionary!"

The right way to use a dictionary is to consider its range of meaning or meanings (sometimes one word has two apparently unrelated meanings). Try to get a general idea of the root meaning. Look for examples of word usage. A dictionary says that a foreign word means "range." That's all! But is it "range" meaning the span of effectiveness, or "range" meaning a thing you cook on? Or maybe even the place where you fire at targets? What about "pot"? Is it what some people smoke, or what other people boil water in? Or is the place where things go when they fall apart?

No bilingual dictionary (say, an Italian-English dictionary) can list every English word that might be used to translate a foreign word in every conceivable context. Therefore, get used to the idea of referring to a dictionary *in the foreign language*, in which you read the *definition* of the foreign word, as speakers of that language define it, rather than the word's equivalents in English. After getting the *idea* from all the dictionaries available to you, select the English word for that idea out of your own vocabulary to match the context you have. And, if you know the word you want, but no bilingual dictionary gives anything near enough to satisfy you, look in a dictionary going in the opposite direction -- say, English-Italian. Often you will find the very word that you want.

And remember that usage changes. I noticed this particularly because I was away from Italian for several years, and when I first began working on it again, I spent half my time, it seemed, turning to somebody to ask, "Have you seen this word meaning this?" The answer usually was, "Yes. It has been meaning that for the last couple of years." For example, for 30 years *in vista di* regularly meant "in view of." Now, at least half the time, it seems to mean a completely different concept, "with a view to."

Furthermore, be sure you are looking for the right word in the dictionary. Can this verb form be derived from this infinitive? Can this

DOCID: 4009793 P.L. 86-36
EO 1.4.(c)

EO 1.4.(c)
P.L. 86-36

noun be the plural of this one? Is there another dictionary entry from which the form in question could come? In Italian, *testa* (pl. *teste*) means "head," and *testo* (pl. *testi*) means "text." And then, to confuse one thoroughly, there is an adverb *testè*, meaning "just now." True, it has an accent mark in ordinary text, but since accent marks never appear [redacted] this is of no help. The ordinary reader may think that it should be completely obvious to the translator which of these three words was used, but in telegraphic, often garbled, text, things aren't always that easy.

To determine the root word, also consider the adjectives or articles that modify the noun. For example, *La capitale italiana* (feminine) refers to Rome, "the capital city," but *il capitale italiano* (masculine) is money, "Italian capital." *Colpo* means "blow," as in *colpo di stato*, "coup d'etat"; and *colpa* means "fault" or "blame."

[redacted]

At this point I would like to make a gripe. Current foreign-language education (or English education, for that matter) doesn't seem to teach grammar. One translator, to whom I pointed out that the verb was subjunctive, not indicative, and it made a difference (*perchè* followed by indicative means "because"; followed by subjunctive means "in order that"), looked at me wide-eyed and said, "But I haven't studied any French grammar since high school!" And he had been a French major in college. I'd like to know why or how.

Linguist's "Other Duties"?

A major enemy of timeliness is piling everything on the translator. "The buck stops here" currently belongs on the translator's desk, not the President's. I know that it is nice for the administrator to have management information; in fact, it is rather necessary. But in most cases it doesn't require a linguist to supply it. Much has been written, and more said -- frequently blasphemously (by the translator) -- about the EXPERT sheet. The whole subject is currently in flux; while some of the burdens, such as writing "ØØ1" on virtually every translation, have been removed. Others have been added, and a report says that many others are in the offing. At present one major complaint is the effort -- and, usually, rewriting -- required to make the last carbon copy readable. One translator said recently, "I used to like to finish a translation so I could get a new one to start. Now I dread it, and put it off, because I'll have to make the EXPERT sheet."

Apart from the EXPERT sheet, there is the lack of translation sheets with the classification preprinted, and the lack of prenumbered paper for worksheet assignment. No reason that I have heard given for these lacks seems to have any validity. The paper with preprinted classification, I was told, can be used incorrectly. But whether the paper is preprinted by the Agency print shop or the classification is prestamped in the section, the paper frequently has the classification already on it. And even if it doesn't, the translator who, by hand, writes TOP SECRET UMBRA 100 times correctly will frequently write it the hundred and first time, even it is not the correct classification.

"Does It Make Sense?"

Last but not least. "It's got to get out today," but it also has to make sense. If it does not, either it is wrong or you, the translator, are ignorant of some fact involved, and you'd better find out which. I have already said that you can't know everything, but you do know *something* and you should have and use common sense. A message should conform to what you already know and to its own internal logic. If man bites dog, it may be news, but in our business it is much more

[redacted]

This has been basically an attempt to counteract what I feel is an *excessive* emphasis on research, research, and more research. It is not an excuse for sloppy or inaccurate translation. It all comes down to "It's got to get out today" -- or at least it ought to, in the best possible shape.

[redacted]

DOCID: 4009793

P.L. 86-36

LETTERS TO THE EDITOR

To the Editor, CRYPTOLOG:

I'm not sure if it is proper for a member of the editorial board to send a letter to the editor, but I would like to add a few observations of my own to the dialogue between Mr. [redacted] (CRYPTOLOG, December 1976) and Mr. Buckley (CRYPTOLOG, March 1977).

As far as I can see, [redacted] thinks that the NSA overall grade distribution from GG-11 through GG-18 ought to be applied through some sort of affirmative action to the Language Analysis Career Field. Mr. Buckley, on the other hand, believes that no single-language "linguist" (maybe it would be better to say "languist" or "languager") is worth much more than a GG-12 or -13. Without calling a plague down on both their houses, I do believe that a third position is defensible.

All linguists may have been created equal, but they don't remain so for long. A relatively small number of them develop a real personal interest in at least one foreign language and the cultural system in which it serves as a medium of communication. It is no coincidence that these are the same people who, as Mr. [redacted] An equally small number of individuals (and for this we can be thankful) go to the other extreme. They appear to be antagonistic toward the language which is putting food on their tables. They absolutely refuse to have anything to do with it except as it appears in their work. It is often these same people who display a truly abysmal ignorance of their target countries. [redacted] Most of us, however, fall somewhere in between these two extremes.

So what? We seem to be rediscovering nothing more than the bell curve. It should not be surprising that linguists fall into three groups: the dedicated, the indifferent, and the militantly incompetent. Most career fields show the same sort of distribution. What is surprising, however, is the fact that supervisors and managers have so much trouble telling the difference between good and bad linguists.

[redacted] As a result, most working members of the language field remain unconvinced that "pure" language proficiency has any positive effect on their career development. (It is true that there are junctures in a linguist's career where the failure to demonstrate some minimum level of proficiency in a foreign language has an adverse effect on career development.) As long as good, indifferent, and even incompetent linguists are held in the same regard by their supervisors and as long as all linguists are provided roughly the same incentives, regardless of proficiency, we will continue to have a language problem and all the delightful things that go with it. It is not so much a question of a "bigger piece of the pie" for linguists, but rather which linguists should get any pie at all.

P.L. 86-36

E. W. Tetrault, P16
~~(FOR OFFICIAL USE ONLY)~~

To the Editor, CRYPTOLOG:

In reference to [redacted] article, "Integrated Analysts for Asia" (CRYPTOLOG, August 1976), where he discourages utilizing women as employees, and letters to the editor on the same subject (CRYPTOLOG, October 1976 and January-February 1977), D8 reiterates the applicability of Exec Order 11478, the EEO Act of 1972 (P.L. 92-261), and pursuant regulations to all Federal personnel actions, including those which involve overseas assignment of employees as underscored by President Ford's memo of November 20, 1975, to all departments and agencies:

P.L. 86-36

> "In making selections for overseas assignment, the possible exclusionary policies of the country to which the applicant or employee is to be assigned must not be a factor in any part of the selection process of a Federal agency. United States law must be observed and not the policy of the foreign nation. Individuals, therefore, must be considered and selected solely on the basis of merit factors without reference to race, color, religion, national origin, sex or age. Persons must not be selected out at any stage of the selection process because their race, color, religion, national origin, sex or age does not conform to any formal or informal requirements set by a foreign nation."

P.L. 86-36

Director NSA, General Allen, further stressed the adherence to these guidelines in a memo to all NSA/CSS personnel, dated 4 December 1975.

[redacted] Chief, D8
~~(FOR OFFICIAL USE ONLY)~~

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

P.L. 86-36

To the Editor, CRYPTOLOG:

I noted in your January-February 1977 issue a letter from [redacted] As President Ford emphasized in regard to selections for overseas assignments (see January 1977 *WIN Newsletter*), "United States law must be observed and not the policy of the foreign nation." If a woman applicant is the best qualified for a particular position, it is *illegal* to not accept her. [redacted] concern is appreciated, I'm sure, but it is not necessary; there can be only a single standard for rating the performance. Elimination of *double standards* is what Women's Rights is all about.

[redacted] G515
Editor, *WIN Newsletter*

P.S. Anyone wishing to subscribe to the *WIN Newsletter* can call me for information on extension 4235s. Anyone who would like to become a WIN member (membership includes a subscription to the *Newsletter*) can do so by sending $3.00 to Rosalie L'Ecuyer, V362, 2E068, 5773s.

(UNCLASSIFIED)

To the Editor, CRYPTOLOG:

We all owe Fred Mason a vote of thanks for his "Where Were We?" contribution to cryptologic history in the January-February 1977 issue. The centerfold idea makes it a useful desk reference aid (even though it can't compete with Burt Reynolds or Marilyn Monroe).

[redacted]

While the Intercept Station list includes some units without alpha-numeric designators, Part II does not. [redacted] maybe other readers can contribute dates/units to this worthwhile project? Should they send them to you? to P1? to E51?

[redacted] V1

Editor's reply:

Thank you for your word of caution and for your additions to Mr. Mason's compilation, which I have sent to him. Readers who have any more additions, corrections, etc. can send them either to: CRYPTOLOG, P1; or direct to the author: Frederic O. Mason, Jr., P14.

~~(SECRET — CCO)~~

To the Editor, CRYPTOLOG:

Mr. Mason's article lists [redacted]

Walter E. Landi, [redacted]

~~(CONFIDENTIAL)~~

To the Editor, CRYPTOLOG:

Missing from Mr. Mason's list of U.S. Navy stations is Poyner's Hill, N. C. During World War II it was located about 20 miles north of Nag's Head, on the Atlantic coast, east of Currituck Sound. I believe its designator was P. EO 1.4.(c)

Also missing is the Navy station that was lo P.L. 86-36 cated on the southern tip of Greenland during WWII. It lay to the northwest of Julianhaab, near the entrance to a large fjord. I do not recall its name or designator (its callsign was NTG).

I suggest that the Navy station at Bainbridge Island, Wash., was turned over to the Coast Guard well after 1945. I served as an intercept operator there until mid-June 1946.

[redacted]

James R. McGrillies, F9203

~~(CONFIDENTIAL)~~

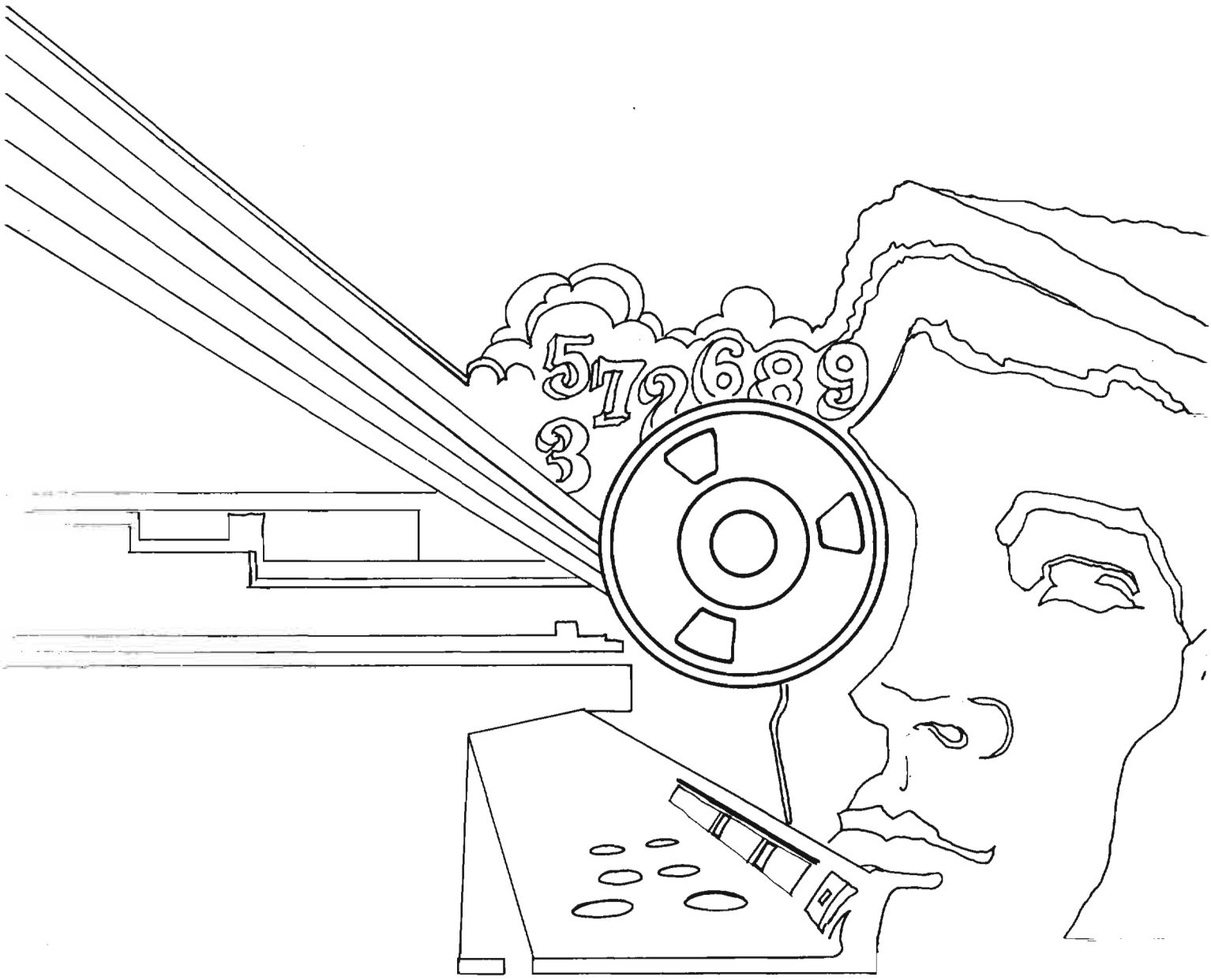
P.L. 86-36

P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

P1-Mar 77-S32-25187

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~


5 7 2 6 8 9
3

DOCID: 4019647

~~TOP SECRET~~

P.L. 86-36

P16

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MARCH 1977

P.L. 86-36

P.L. 86-36

AN OVERVIEW OF PROJECT [redacted].....[redacted].....1
CADRE REVEALS WHAT DATA CONCEALS.....[redacted].....7
SIGINT PUBLICATION MANUAL IN PREPARATION....V. R. Filby.....8
CENTRAL COMPUTER COMPLEX IN 1970-1980s....Cecil Phillips.....9
A FEW THOUGHTS ON THE N.S.A. LINGUIST.....Anon.....15
BOOKBREAKERS FORUM.....[redacted].....16
MORE ABOUT THE N.S.A. SIGINT SUMMARY.....[redacted].....17
LETTERS TO THE EDITOR.....19

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019647

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. IV, No. 3 MARCH 1977

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief..... Arthur J. Salemme (5642s)
Collection..... [redacted] (8955s) P.L. 86-36
Cryptanalysis..... [redacted] (8025s)
Language..... Emery W. Tetrault (5236s)
Machine Support..... [redacted] 3321s)
Mathematics..... Reed Dawson (3957s)
Special Research..... Vera R. Filby (7119s)
Traffic Analysis..... Frederic O. Mason, Jr. (4142s)
Production Manager..... Harry Goff (4998s)

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4019647

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

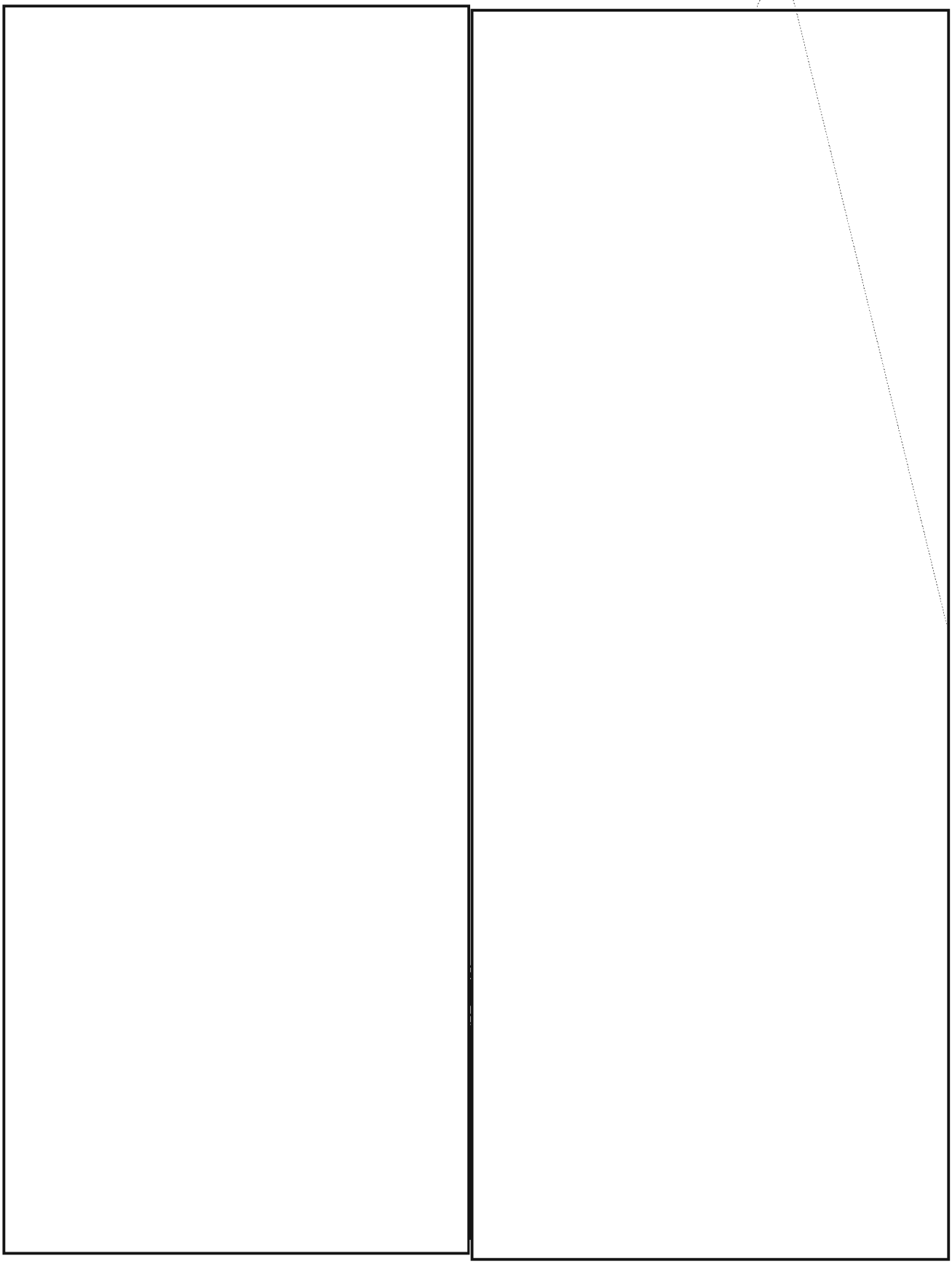
AN OVERVIEW OF PROJECT

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

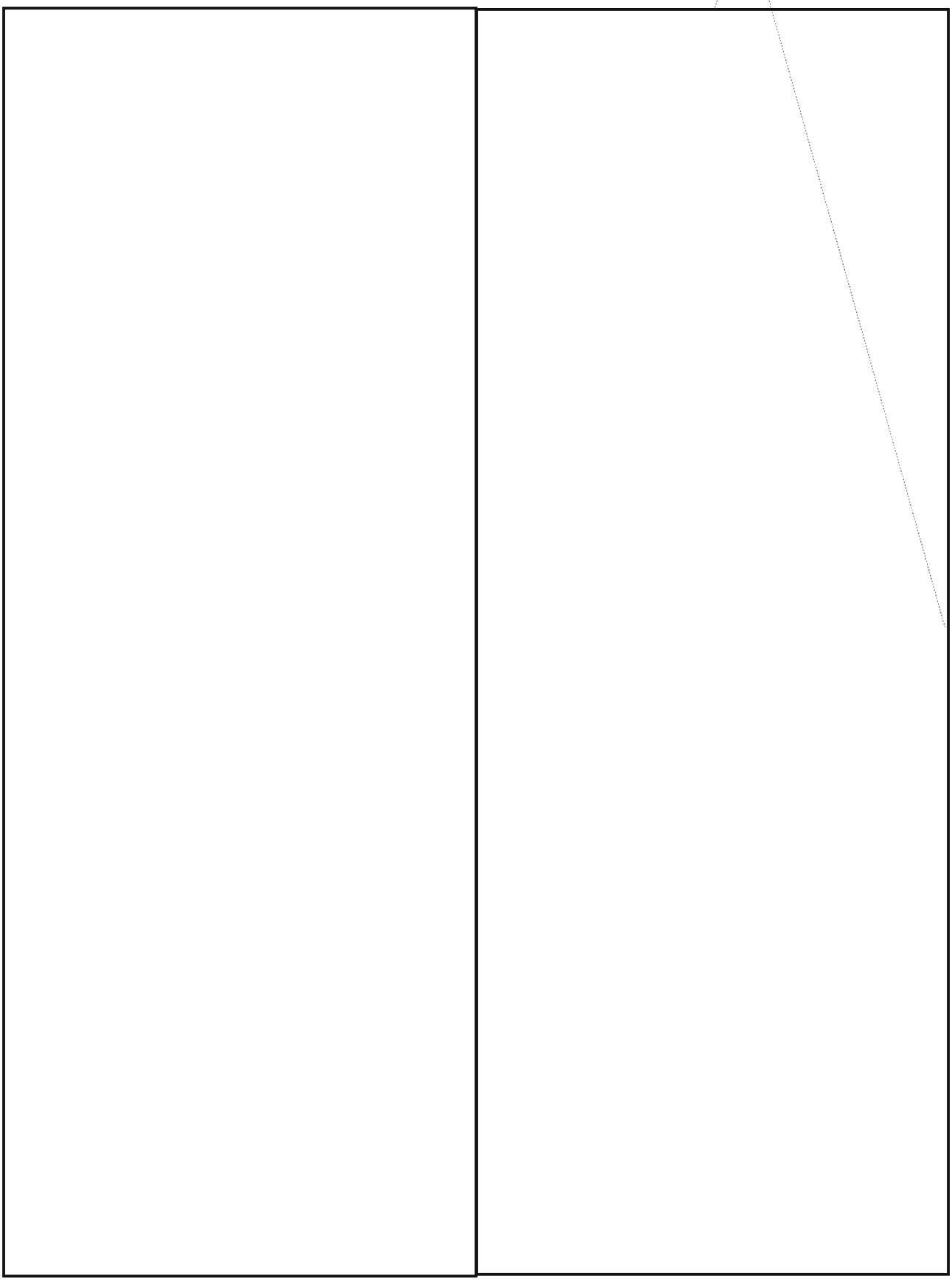
DOCID: 4019647

EO 1.4.(c)
P.L. 86-36



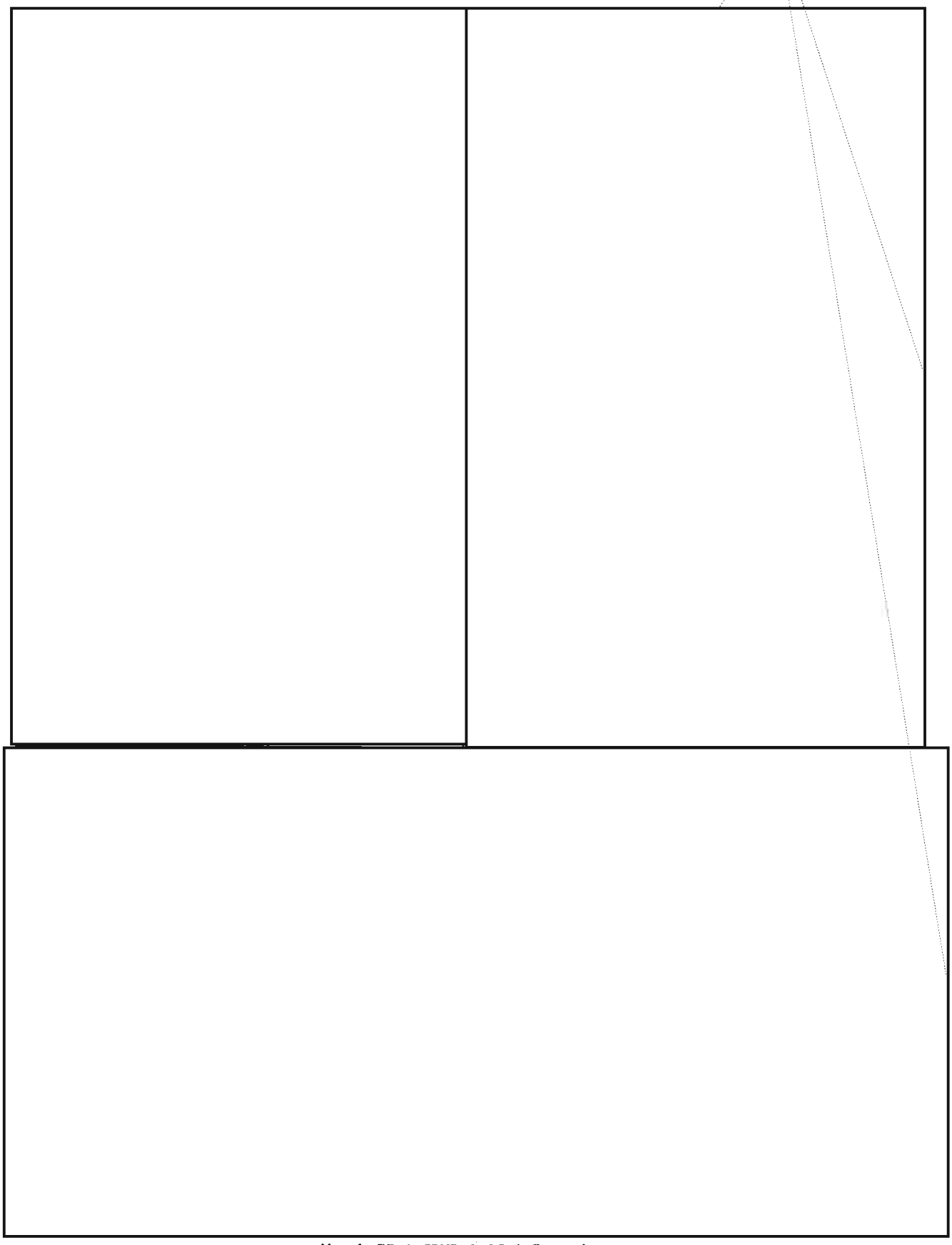
DOCID: 4019647

EO 1.4.(c)
P.L. 86-36



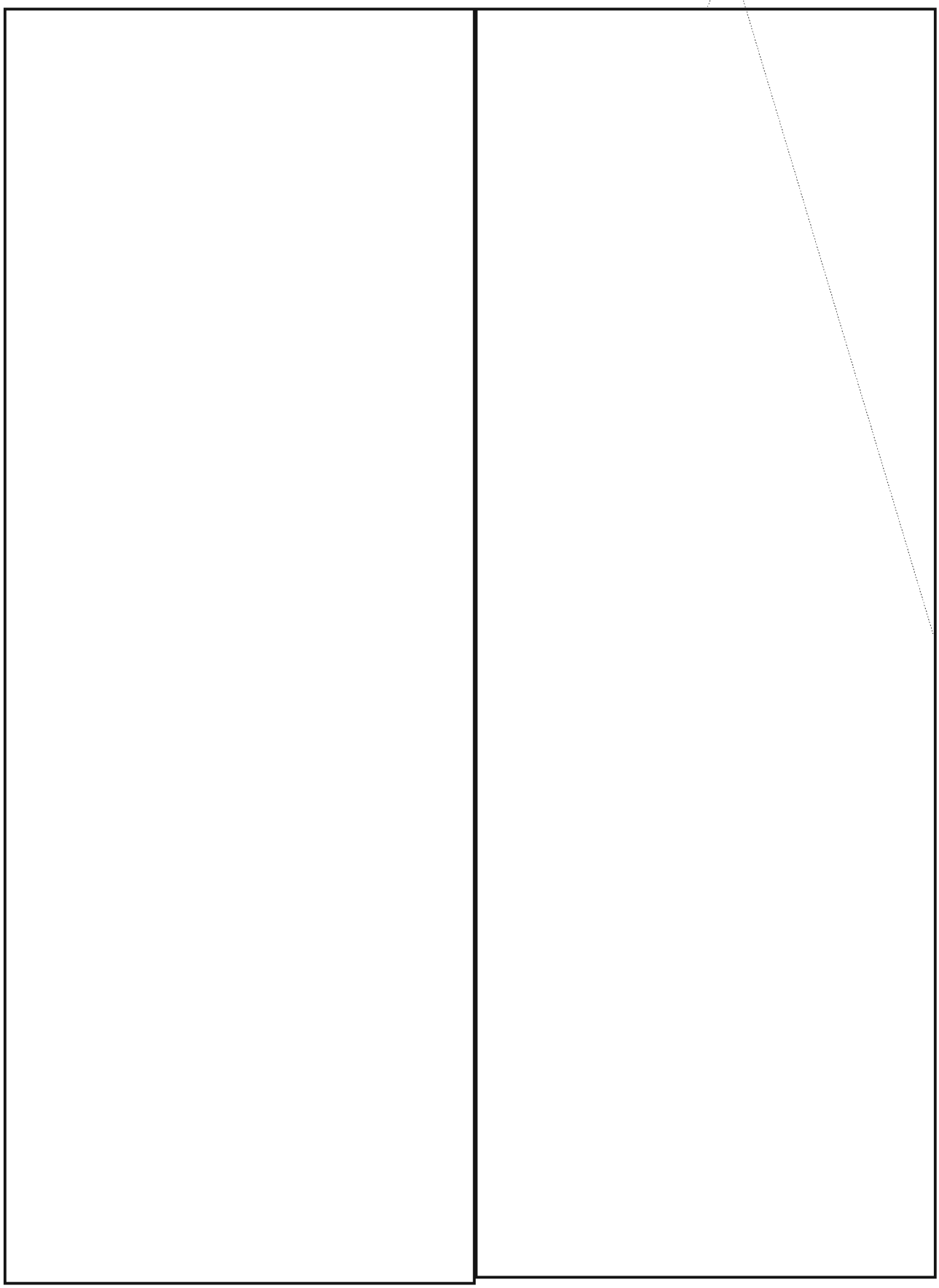
DOCID: 4019647

EO 1.4.(c)
P.L. 86-36



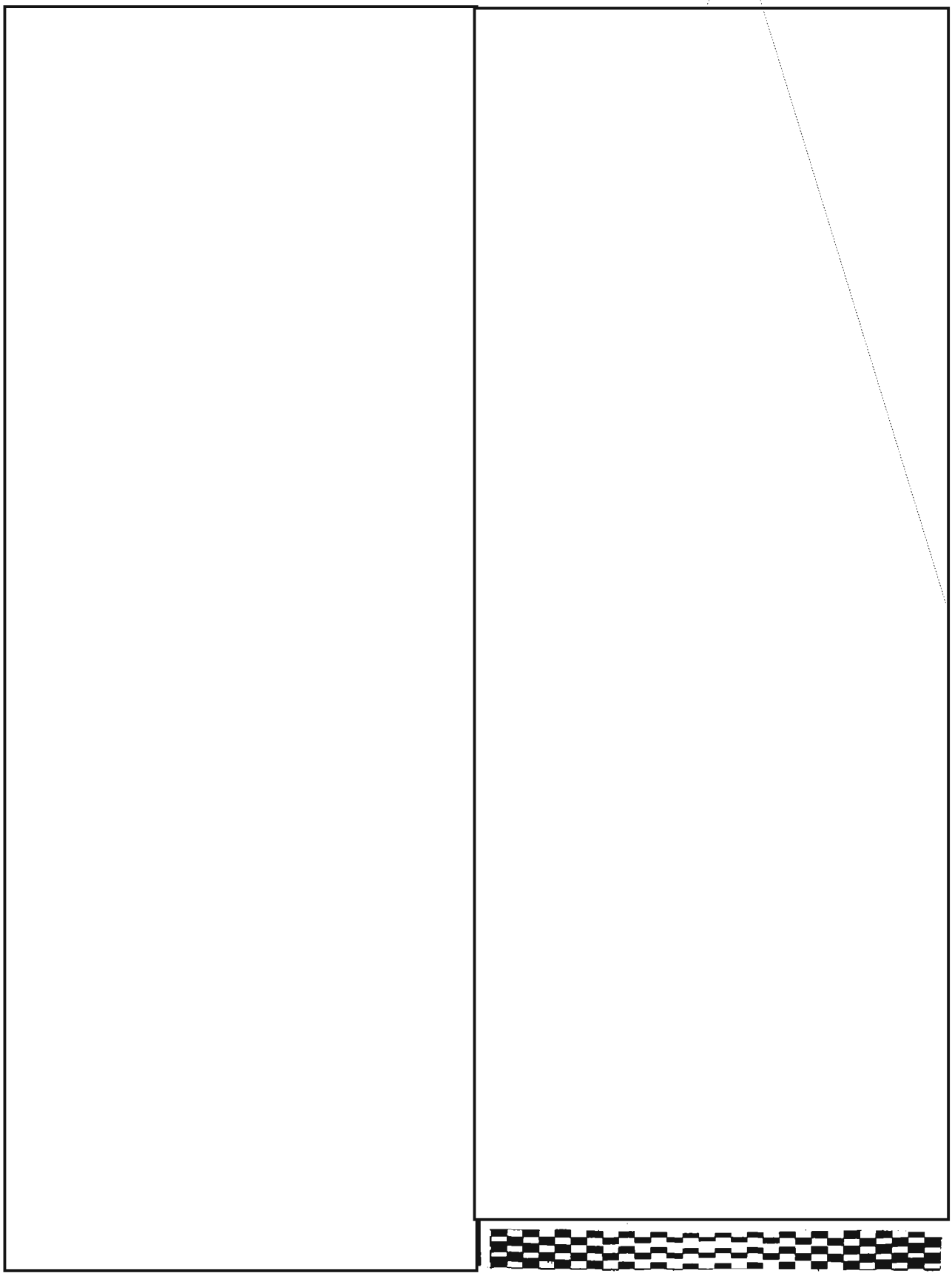
~~SECRET~~

EO 1.4.(c)
P.L. 86-36

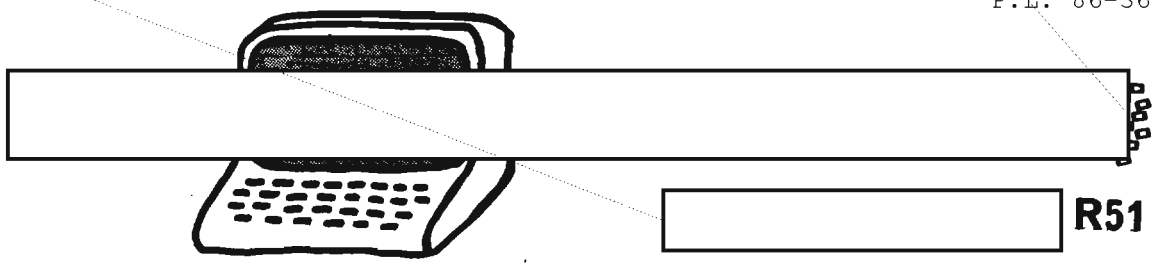


EO 1.4.(c)
P.L. 86-36

~~SECRET~~



~~SECRET~~



R51

P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)

[redacted]

~~(TOP SECRET UMBRA)~~

REVISED TECHNICAL SIGINT PUBLICATION MANUAL IN PREPARATION

V.R. Filby, E12

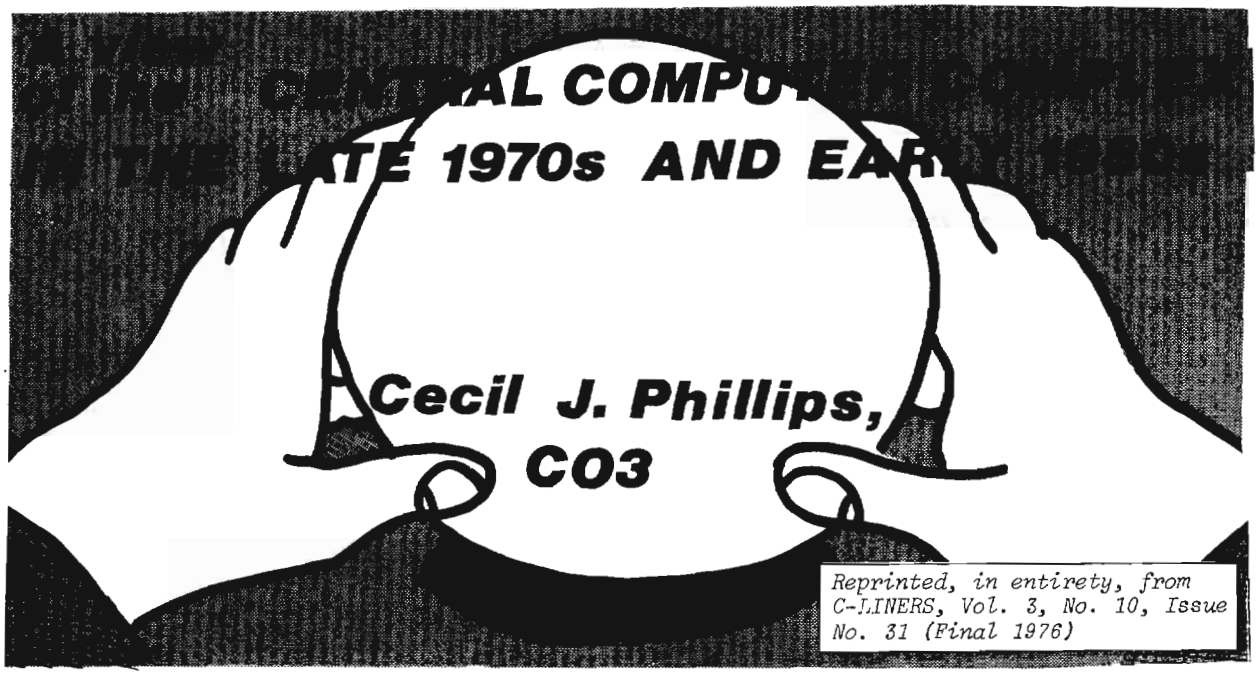
It is well known that not all analysts everywhere get to see the formal instructions and other documents that affect them in their work. For those who may not find out about it through normal channels, here is news of a document all analysts and reporters should take the trouble to get hold of and study. The revised and updated *Technical SIGINT Publication Manual (U)*, to replace the present TSPM dated 19 August 1969, is in final draft form and should be ready for distribution in mid-1977. It will be promulgated by USSID 200.

[redacted]

~~(CONFIDENTIAL — HANDLE VIA COMINT CHANNELS ONLY)~~

EO 1.4.(c)
P.L. 86-36

DOCID: 4019647



Reprinted, in entirety, from C-LINERS, Vol. 3, No. 10, Issue No. 31 (Final 1976)

The most dramatic change in SIGINT computer processing in the next few years is almost certain to come from the much wider development of man-machine interactive processes. This does not necessarily preclude growth in regular batch processing or growth in fully automatic processes, but it certainly means a strong shift of emphasis in the development of computer processing systems. Some of this emphasis comes from a desire to explore the newfound capability of interactive computing but, hopefully, most of it comes from a realization that machines alone are not nearly as effective as man and machine working closely together. These views are presumably not unique to the SIGINT process, since comparable growth in the use and sale of interactive computer terminals is being experienced in all kinds of pursuits.

Interactive computing in the SIGINT case can mean a variety of things. It can mean the ability of an analyst to "adjust" the collection process while it is going on. It can mean the ability to scan some output in real time and adjust it as necessary. Or, in an analytic process, it may give a person the ability to correlate and cross-check new data against the mass of historical information one has collected before; or the ability to prepare reports, gists, and similar inputs to other processes.

It is clear that there are a number of ingredients to a good interactive processing system. One of the most critical of these ingredients is a knowledgeable and well-trained cadre of users. This group is already growing, but more specific action will be necessary in the future to insure that we use the full potential of the systems which are built. At the same time, the central computing service must do everything it can to make user interfaces simpler, rather than assume that every user has some skill and knowledge as a programmer. In addition to making computer systems easier to use, the central computing service must provide a number of capabilities and tools for the users, in much the same sense in which utilities are provided to homes and businesses.

In a practical computer sense we see this utility as:

- an adequate set of computer terminals to serve all users who need access to the system and simplified user procedures;
- on-line mass data storage systems and data management software which will minimize the complexity of the user interface;
- a computer network connecting all SIGINT locations which will enable us to put the required computing power into a connected system and provide user access to any part of the system from any terminal; and
- individual computers and devices and appropriate software which will provide the best computational capability available.

Some of the details of current plans and broad concepts of usage for parts of the system are described below. This detail will be added to and modified as necessary to reflect requirements developed under [redacted]. The overall [redacted] plan, which is basically the plan for the central computing facility and externally connected computer nodes, is due to be completed in draft early in 1977. P.L. 86-36

Computer Terminals and Terminal Access Systems

The largest group of computer terminals for SIGINT operations will consist of alpha-numeric

displays and associated keyboard for analyst interaction with the system. By 1980 or sooner, computer terminal density should have reached the point where there is at least a terminal for every three or four production personnel. This should mean that almost every analyst does part of his work at a computer terminal. A smaller set of terminals will have "full graphics" capability in addition to alpha-numeric capability, that is, they will be able to plot and to produce line drawings through the use of vectors. A still smaller number of remote batch terminals will continue to be used to initiate batch processes and to receive printed output. It is probable that as the use of interactive terminals grows, remote job entry terminals will become more basically "remote job output" terminals, or, simply, remote printers. Softcopy displays, that is, writing output to a computer file for subsequent examination on a terminal screen, will probably replace some print, but it is not too likely that all printing will be replaced. In many cases, line printers will be associated with display terminals so that output can be recorded. Equally, local storage cassettes may be used as safeguards against loss of data during entry and as a way of insuring the ability to input data at all times.

With present technology, and probably within the foreseeable future, the main bulk of the interactive terminals will be attached to minicomputers as terminal concentrators, and, through these, will be attached to the network and will have potential access to all of the system resources attached to the network. The actual access will be limited by absolute security constraints and by need-to-know procedures. These will be effected by both hardware and software means. Hardware controls are certain to be used to limit some terminals and may be used to identify users through badge readers or the like. Software controls will consists of authorization tables and passwords which will control a user's access both to files and to processes.

The total extent of the work to be performed at the terminal level or at the terminal concentrator is not yet determined. However, it seems most likely that, with present terminals, efforts will be made to limit them to "universal" functions. These will amount to data entry and data editing functions dealing with lines or screens full of data and probably to the generation of standard protocols for network entry and access to a specific system. If the terminal "intelligence" (actually storage and processing power) grows a great deal, as most manufacturers predict, then this power may be used to accomplish procedure and data language translations or to provide the capability to do other functions common to a group or class of users.

At the next, or terminal concentrator, level, more advanced functions will be performed than those at the terminal level. With controls and with standard principles applied, software in the concentrator may perform machine editing and automatic formatting, and provide file-browsing capability. Where the primary function is data entry, the concentrator will also serve as a "fail soft" capability to allow data entry to continue until the main system becomes operational again.

Work not done or not possible in the terminals or the concentrators will be done in the main systems, or "hosts." Communication between concentrators and the hosts will be via the computer network described below. To a considerable extent, hosts will be specialized processors as they are now. If network protocols and individual host protocols and language can be simplified for the user by translation and creation in the terminals and concentrators, it may result in even more task specialization by the hosts. Alternative views are that networking of host computers may result in automatic "load leveling" of tasks by automatic distribution of them throughout the network. In the next few years, the latter seems practically attainable only for multiple copies of the same computer within the network. In general, the network will contain multiple copies of hosts for reliability and backup and for achieving the desired processing power.

All of the description above pertains to user-to-computer communications through terminals, concentrators, and computer hosts, natural parts of a man-machine process. A quite separate kind of communication capability will exist within the network to support person-to-person communications. With this capability, analyst-to-analyst discussions such as are now handled by OPSCOMMs would be straightforward. A "mailbox" variation of this capability would permit messages to be left by one analyst for another when direct contact is not possible because of working time differences, etc. By signaling his "mailbox," an analyst receives all his accumulated messages from other analysts or computer generated messages to advise him of the status of some piece of work.

Data Storage and Data Management

In discussing a processing system for SIGINT operations we are certainly talking about a system serving several thousand people -- probably more than 10,000 when the operational aspects of field sites are considered. Even if terminal density is as low as one terminal for each ten members of the operational community, it will clearly be a very large system with many terminal systems and many hosts. In all probability, terminal density will be much higher, particularly so if MAROON SHIELD concepts extend to all sites.

To support such a large community of users from interactive terminals, it will be extremely important to have a large amount (if not all) of the recent data on-line. While it

is not out of the question to have a single large central store for all data, recent experience would seem to indicate that distributed data "collections" are much more likely. Some systems will have much more storage than others because of the historical nature of the kinds of problems handled and because the primary impetus in developing and marketing very large mass store systems is toward IBM systems. Thus, it is likely that we will have "unevenly distributed data," with more than half of the data in a single large collection.

Examples of this uneven nature of data distribution are quite pronounced now and will be greatly exaggerated when the IBM storage system called OAK is added to the present IBM 370/168 complex. With its 169 billion byte storage and "virtual disk" concepts, it is bound to lead to a large imbalance in storage of data throughout the general purpose system.

In spite of the imbalance, there will be a continuing need for large local collections of data on other hosts in the central complex in order to satisfy specific requirements for rapid response and other special requirements. In addition, there will be requirements for data correlation-fusing-updating and other functions inter-host. For this latter case and for inter-host/inter-process operations, a great deal of data management is needed.

We feel that a number of things will be necessary in order to deal with distributed data. First, some kind of data management plan will be desirable so that data will not be distributed helter-skelter over several storage devices. Such a plan should address necessary and unnecessary redundancy. It should also address the software tools which are to be provided to enable users, data base administrators, and others -- as well as programs and computer systems -- to have convenient access to the data. Some work has been done in NSA toward developing a data management plan (DAMAP) but clearly a great deal more work remains to be done, especially if anyone is to make regular use of distributed data bases. To a great extent we will not have very much experience with trying to use distributed data bases until the computer network linking computer hosts is operational.

As far as data base management systems (DBMS) are concerned, these are key "tools" for handling data. Hand in hand with DBMS usage, there must be a growing awareness in user organizations of the need for individuals who know the data base and control its development -- generally referred to as data base administrators. The data base administrator and his management have the potential to make data base operations useful and productive. In their efforts to do so, it is imperative that they achieve standardization of data elements, standardization of data codes, and standardization of files in the sense of requiring basic data elements in there. Data dictionaries and data directories will be key tools for data base administrators and others who face the job of producing and managing the data bases.

In achieving the SIGINT operations processing system, data base management techniques will be guided by a unified systems discipline with a goal of a single data base management system. Standardization will play a much larger role than in the past. Until adequate data standards are developed, existing data management will be continued but its future growth will be limited. The goal is a coherent whole for managing data, supported by a comprehensive set of data management tools.

Experience with networks such as COINS points to the critical need for accelerated work in NSA's data standards, Emphasis should be on NSA or SIGINT data standards, rather than large efforts at meeting non-SIGINT standards. These may be important in some cases, but many of them have little bearing on SIGINT problems. Further, SIGINT data standards work should concentrate on the most frequently used data elements and types, so that the benefits are maximum. Standardizing data elements which are rarely used or used in narrow areas of SIGINT is useful, but it does not contribute as much to the areas of broad use.

A final note on data standardization implementation -- a phase more difficult than developing the standard. This must be vigorously but rationally pursued, with NSA management taking active interest in the arguments and counterarguments. Good standards are usable standards.

Computer Networking

Another key ingredient of a large interactive system such as that required by SIGINT operations is a way of linking computer systems. The scope of SIGINT processing exceeded a single large computer many years ago. In the interim, specific computer-to-computer linking and loose coupling of several large computers through shared storage have helped with the problem. Project [redacted] NSA's computer networking plan, is the generalized solution to linking as many systems as necessary into an integrated processing complex. P.L. 86-36

Project [redacted] may be described as a "railroad," since it provides the basic techniques for linking computers and terminals with standard connection protocols. It does not of itself guarantee standard processes, standard data bases, or any other set of standards except for the basic network protocols. P.L. 86-36

NSA's computer networking is based on technology developed for the Department of Defense Advanced Research Projects Agency (ARPA). It is a packet switched network in which every node is connected to at least two other nodes. This gives additional reliability to inter-host connections. As mentioned above, the use of these

connections is not controlled except by the network protocols, network control programs in the hosts, and the provisions for inter-process communication.

As the network comes into use, some additional controls will come into use. Security will be one of these. Job, process, and message accounting will add another dimension of control. The details of an overall control or management system are yet to be developed, but will be formed from the experience of using the network and from growing user requirements for process control or process management. The requirement for process management by users is developing rapidly in parallel with the ability of processes and processors to be linked together.

Effective use of the network will require extensive user knowledge of computer processes and computer facilities, as well as knowledge of the data mentioned earlier. A network information center is being developed to assist the users in understanding all the capabilities and complexities of the network.

The full development of the computer network [redacted] will take a number of years. Its effective use is a key factor in the development of the Agency's potential to use computers.

The Equipment Complexes

Equipment complexes (or sometimes "computing complexes") is a term which has come into increasing use as we couple two or more pieces of equipment or link equipments through some common peripheral device. The use of equipment complexes for planning and management has been accelerated by the need for operator and maintenance economies, and by the practicalities of consistent operation of identical and related systems.

The principal example of such an equipment complex is the main IBM 370 complex, now called [redacted] By developing the large IBM systems so that they share disk storage, a significant improvement was obtained in the flexibility of the four systems. At the same time, it was possible to reduce the staff necessary to operate the machines. In other cases, we can also reduce maintenance costs by collocation of machines.

The Central Data Processing Complex [redacted]

This complex is the historical successor of more than 40 years of automatic data processing (ADP) which began with IBM punched card machines in the 1930s. As noted earlier, it is the processing area where the most data is stored and where the input and output (at least of traditional data records) greatly exceeds any other set of NSA computers. Because of storage capacity available in this complex, and because of increasing requirements for data correlation, this complex continues to grow at a considerable pace. It is possible that computer networking will reduce the demand ". . . to have everything together," but from a practical point of view this will take some time, perhaps 2 to 3 or more years.

Immediate plans for the large IBM 370 systems are to add a fifth IBM 370/168 to the present four systems and to create one multiprocessor system. It is planned that the multiprocessor will serve needs which demand high reliability or availability. This will include immediate front-end processing of field data arriving from [redacted] and support of critical terminals. The whole 370/168 complex, along with the OAK mass storage system of 169 billion bytes of on-line data, will serve [redacted] and similar functions.

The present IBM 370/158 serving primarily administrative functions will be upgraded to an IBM 370/168 and formed into the larger complex by loose coupling through shared storage and by linkage to the computer network. The present IBM 370/158 used for Information Storage and Retrieval (IS&R) will serve principally as a developmental system and will be used in background mode and in nondevelopmental times for large batch processes. Future large IBM systems (or IBM-based systems such as AMDAHL) which may have to be added as supply capacity will be coupled into the main complex. The linking of more systems as multiprocessors will be dependent on the success of the MP system planned for late 1976. P.L. 86-36

In order to meet DDO's goal by bringing time-critical and batch processes together, the IBM 370 complex will have to be made to respond much more rapidly, so that bulk data can be almost as available as selected data such as [redacted] reports. In fact, it seems likely that [redacted] and the IBM 370s will have to work well together to accomplish this.

The Time Critical Complex

This complex is also expected to continue to grow rapidly. The success of the TIDE system over the last 6 or 7 years has produced the present overload state of the pair of UNIVAC 494s and has led to the development of PREFACE plans.

As planned, the UNIVAC 1110s in [redacted] will be used to relieve [redacted] of processing functions, as distinguished from communications functions. While converting processes from the U 494 to the U 1110, a data base management system (DBMS) will be introduced to provide for more orderly handling of data and to simplify future programming. As the [redacted] development proceeds, it will be necessary to address the broad question of alpha-numeric terminals for NSOC and to begin development of plans for a communications subsystem to replace [redacted]. It is estimated that [redacted] will continue to operate until at least January 1980, and possibly a couple of years after that.

P.L. 86-36

[redacted] which is now slated to serve both full graphics needs and some alpha-numeric needs, will be diverted to full graphics-only usage as [redacted] becomes operational. A careful study of all full graphics needs will be undertaken with a goal of developing a set of requirements for full graphics. While these requirements will ultimately drive the full graphics solution, it is likely that [redacted] will fill most of these needs over the next 2 to 4 years.

The High Compute Complex

This complex of computers is now almost entirely synonymous with cryptanalysis. To some extent this is because the cryptanalysts have carefully guarded it and to some extent it is because the [redacted] set of CDC 6000s preceded the first CDC 6600 for cryptanalysis.

As far as the cryptanalytic side of the problem is concerned, the high-compute-complex plans are described under a C Group concept called HYPERCAN -- for *HI*gh *PER*formance *C*rypt*AN*alysis. Under this concept, four CDC 7600s using the NSA/IDA Operating System will be linked by a 50 megabit data transmission bus. In addition, a new and more advanced super computer [redacted] will be sought to add to the capacity of the complex. We hope to add this new capacity in about 2 years and, thereby, double the straight-compute capacity. Interactive terminals will not be developed at the output for the new system. Instead, access to the new system will be primarily through the CDC 7600s and the 50 megabit network. This is expected to optimize the use of available resources and to minimize the impact on users by retaining the present NSA/IDASYS procedures and languages.

Operating Facilities

The term "operating facility" is being used as a catch-all for the NSA end of remoted collection operations. Presumably, every one of these operations needs some interconnection to the main computer complex. To date, most of the interconnection has been described as a connection to the computer network -- [redacted] with little more specifics than that. Almost without exception, design of these complexes has ignored the necessary and desirable interaction with existing data collections on the central computers. In viewing overall operations processing in the next few years, it seems certain that more complete plans will have to be developed using existing resources as well as the new equipment.

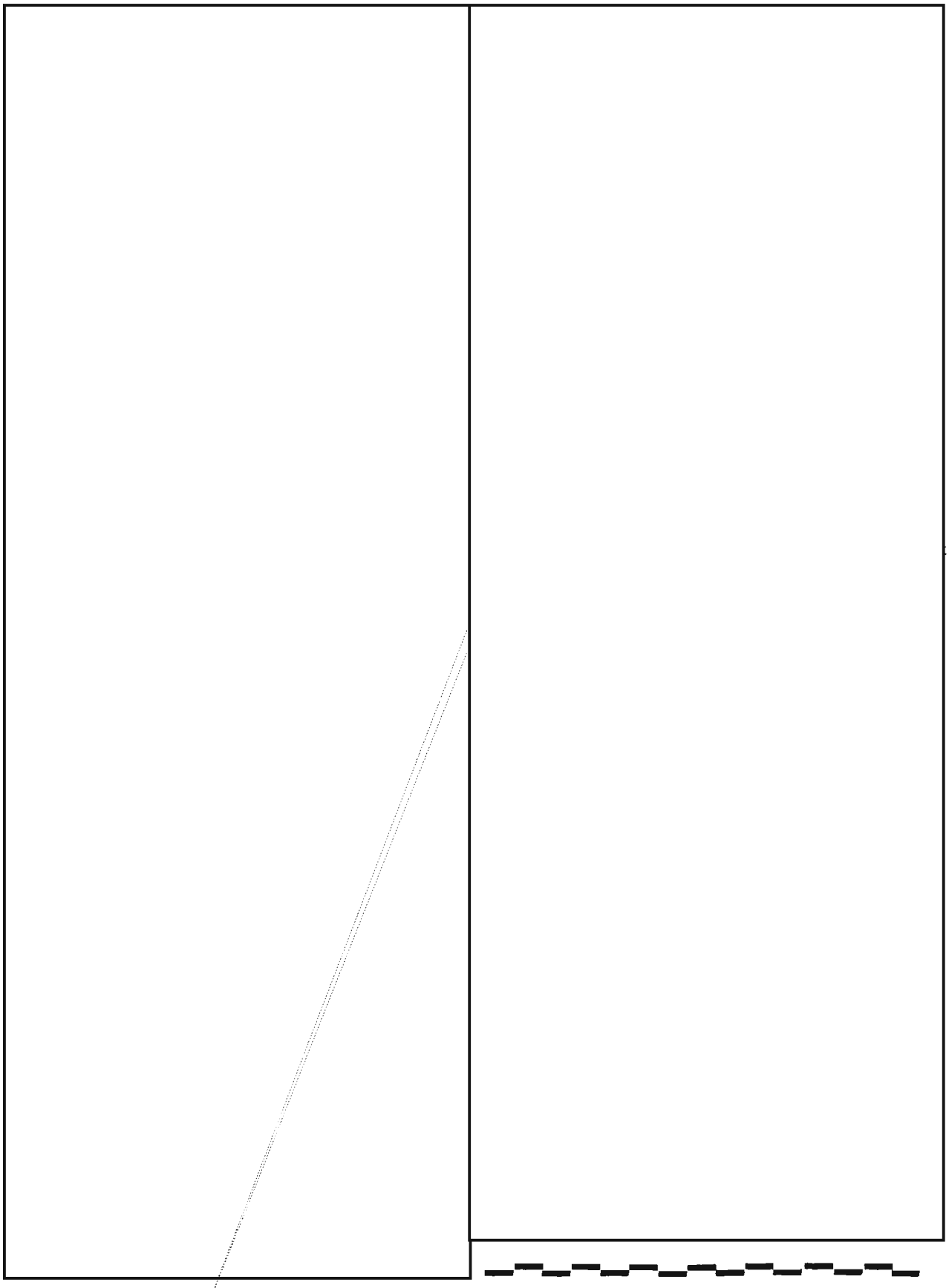
One mode of operation which may emerge is to limit "operating facility" computers to problems requiring extremely quick response and to use the main computing complex (MCC) for basic support. In this mode, the MCC would update basic files in the operating facilities by "downloading" from the central analytic files. In the operating facility, immediate response problems would be dealt with by the local computer and more complex questions could be relayed to the MCC. This mode is already projected in [redacted] applications where the broad functional similarity to Morse collection is almost identical, except for tuning.

The presence of high bit rate signals at operating facilities may dictate the need for a special network or data bus paralleling the [redacted] network. This is under study in R as a part of [redacted] and other projects. It is most likely that [redacted] would be used for control information and that the parallel high-capacity linkage would be reserved for only signals. This would limit the number of required nodes.

More details of these connections to the [redacted] network and the interaction of operating facilities with the Main Computer Complex are emerging as the projects develop. It is reasonable to expect that requirements gathered for [redacted] will provide more understanding of what is needed.

[redacted]

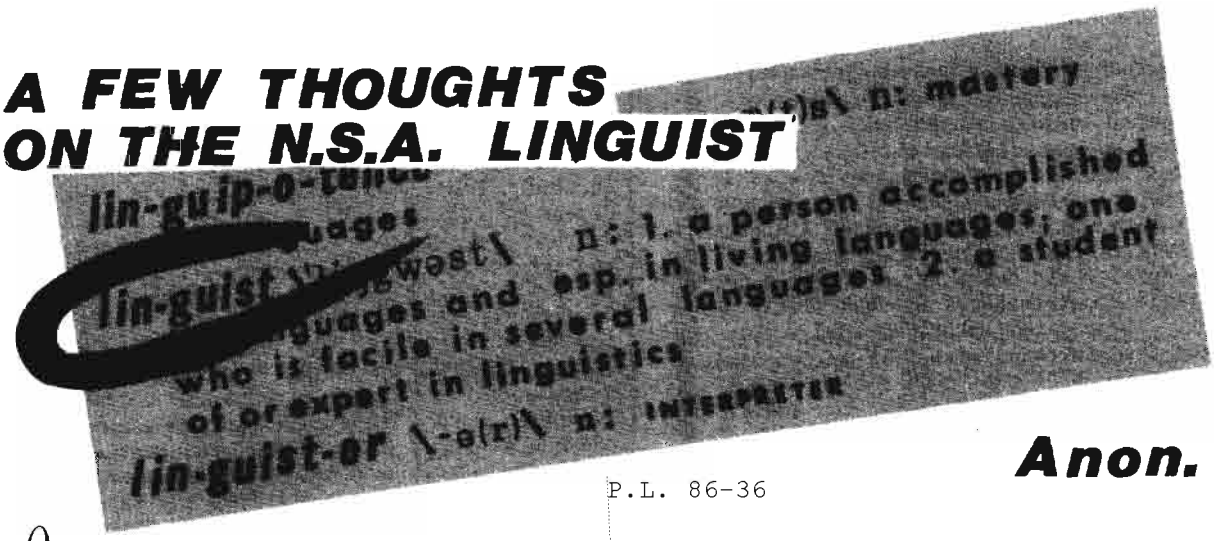
P.L. 86-36
EO 1.4.(c)



P.L. 86-36
EO 1.4.(c)

DOCID: 4019647

A FEW THOUGHTS ON THE N.S.A. LINGUIST



Anon.

P.L. 86-36

I am being somewhat arbitrary in using the term "linguist." What I mean here is an individual who is capable of performing the full range of tasks required at NSA in which knowledge of a foreign language is *primary*. Let's forget all hyphenated job titles in which some degree of language knowledge is coupled with some other skill. You can carry this hyphenation business to the point where it becomes difficult to locate *anyone* who doesn't claim to use a foreign language to some extent in his or her specialty. It sometimes seems that the pretensions of such people are in direct proportion to their ignorance of the language claimed.

Nonlinguists, especially, have a curious tendency to treat language jobs as though we at the Agency were in complete control of inflowing language materials. Thus, a particular language task (in a very low grade, of course) is described as "highly stereotyped, low-level," requiring no more than a minimum language knowledge.

[redacted]

So, what is a linguist expected to know -- everything? It would be a miracle indeed to discover a native of this country who has mastered his own language (including all the words in the dictionary), and, besides that, knows all the subjects that can be discussed in English; in short, a walking encyclopedia of both linguistic and factual information. Obviously, there is no such person. It should come as no surprise, then, that the NSA linguist at any level is apt to run into problems that involve either language or factual knowledge (or both) outside his own experience, not covered in any of his training courses or anticipated by the latest crop of "scientific" linguists -- and not to be found in any reference works available to him. If we agree that it is extremely important in our work to be right [redacted] if you doubt this), what, then, can you reasonably expect of an NSA linguist? What choices do you offer him? Must he confine himself strictly to the level of his job description (and pay), and ignore everything else? Or should he try to cope with everything that flows across his desk, even though many of the problems (linguistic and otherwise) will be beyond his competence?

Backing off for a moment, let's consider again the first question raised: what *is* a linguist, anyway? Is he a person who can provide a precise description of a language, employing all the scientific terminology currently in vogue? Or is he someone who can use the language as an educated native would? Is it realistic to assume that the person who can describe a foreign language can also *use* it in the manner indicated? Probably not. Of the two, which one does the Agency's work -- the "describer" or the "practitioner"?

EO 1.4.(c)
P.L. 86-36

I am reminded here of the never-ending debate over the term "bookbreaker." Is he (or she) the person who "breaks into" a code and provides a tentative description of its size and structure -- with, perhaps, a few hypothetical "recoveries"? Or is the bookbreaker the one who actually *reconstructs* the code book to the point where incoming messages can be decoded and translated upon receipt? I would go

[redacted]

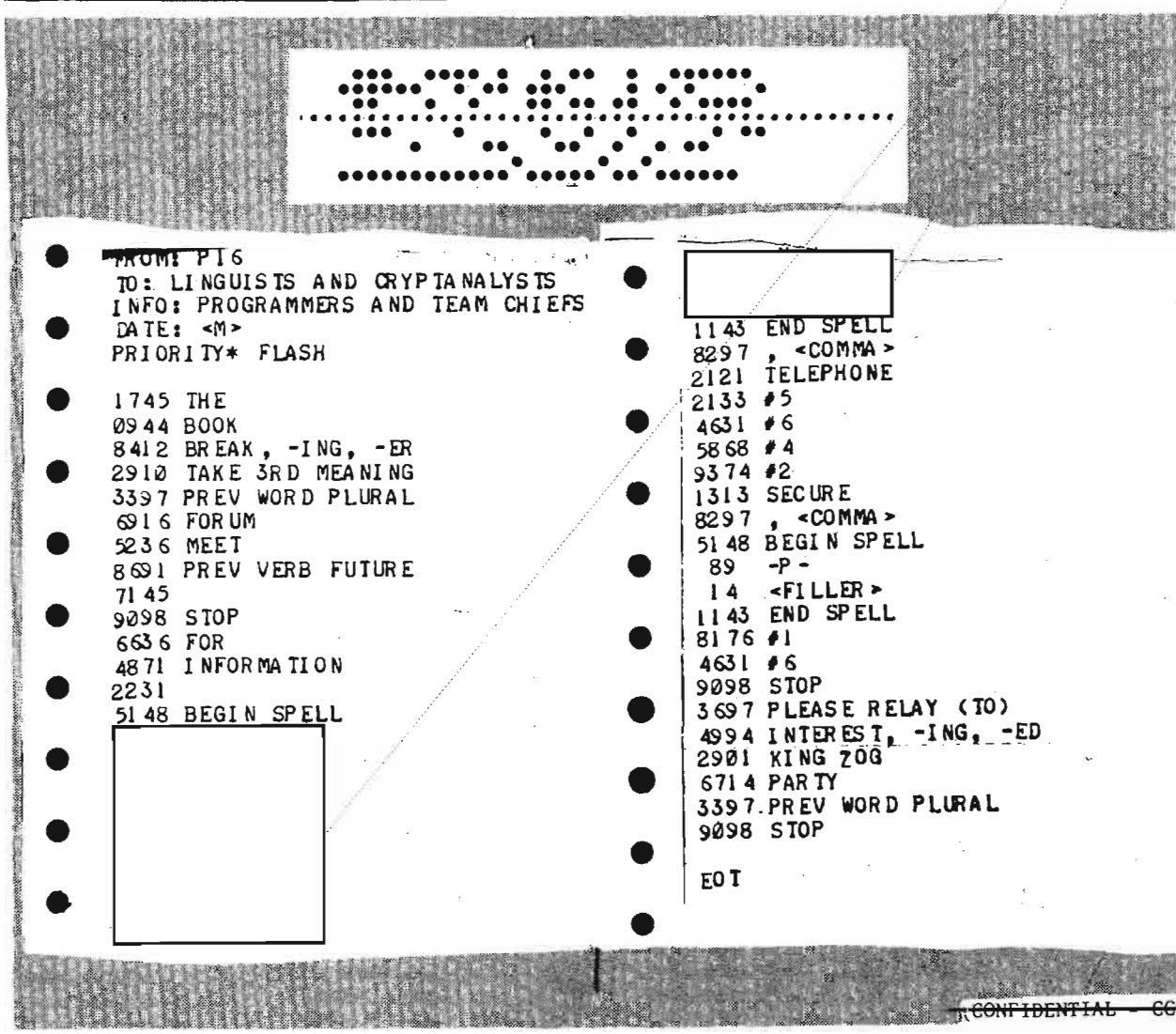
P.L. 86-36

even further and insist that the "reconstructor" should, upon request, be capable of translating any decoded message -- and have his translation survive a language check by the most experienced linguist in the area (who may not be friendly). A demand like this tends to divide analysts into two groups: the "describers" and the "reconstructors." These two groups will disagree forever as to who is more deserving of the title "bookbreaker," but that isn't the point. Their great debate is really more over status than anything else. In my own mind, I expect as much of the "code reconstructor" (the one who meets the standard imposed above) as I would of the true NSA linguist, as defined at the outset. Neither one has the right to assume that the task at hand will be tailored to fit his own limitations or narrow interests. To begin with, both must be literate in the foreign language involved ("literate" as defined in Webster's -- "able to read and write").

Why make such a big thing about mere literacy? Simply to plant our feet firmly on the ground in this whole matter. We shall never get the linguistic paragon who knows all the answers offhand, nor can we afford the risk of depending forever on those who never know enough. The real NSA linguist is the person who is literate to begin with -- and who has an infinite capacity for growth. To quote Will Rogers, "We are all dumb on certain subjects," and this description fits linguists like a glove. But with the ability to read a foreign language at sight, we can overcome our ignorance by searching for the answers in the very places where a native scholar would look, just as we regularly consult standard reference works in English. If we still can't find the answers, the trouble may be that the other fellow's reference sources are better than ours.

P.L. 86-36

~~(CONFIDENTIAL - CCO)~~



FROM: P16
TO: LINGUISTS AND CRYPTANALYSTS
INFO: PROGRAMMERS AND TEAM CHIEFS
DATE: <M>
PRIORITY* FLASH

1745 THE
0944 BOOK
8412 BREAK, -ING, -ER
2910 TAKE 3RD MEANING
3397 PREV WORD PLURAL
6916 FORUM
5236 MEET
8691 PREV VERB FUTURE
7145
9098 STOP
6636 FOR
4871 INFORMATION
2231
5148 BEGIN SPELL
[redacted]
1143 END SPELL
8297 , <COMMA>
2121 TELEPHONE
2133 #5
4631 #6
5868 #4
9374 #2
1313 SECURE
8297 , <COMMA>
5148 BEGIN SPELL
89 -P-
14 <FILLER>
1143 END SPELL
8176 #1
4631 #6
9098 STOP
3697 PLEASE RELAY (TO)
4994 INTEREST, -ING, -ED
2901 KING ZOG
6714 PARTY
3397 PREV WORD PLURAL
9098 STOP

EOT

~~(CONFIDENTIAL - CCO)~~

DOCID: 4019647

MORE ABOUT THE NSA SIGINT SUMMARY

P.L. 86-36

[redacted]

The year, 1965. The place, the NSA SIGINT Command Center. The occasion, the beginning of the NSA SIGINT Summary. And you are there . . . (Sorry, Walter!)

The May 1976 issue of CRYPTOLOG contained an article by William Hunt, SA/DDF, which described in some detail the functions and purposes of the NSA SIGINT Summary. On the whole it was rather complete and quite interesting. But for the period between the inception of the SIGSUM and Bill's association with it -- a period of 8 or so years -- the article provided virtually no information at all. Having, with some others, devoted a part of those years to the business of conceiving and developing the SIGSUM, I am perhaps in as good a position as any to fill in the gaps. In the process, I will also clarify some statements in the article that are unintentionally misleading, made so simply by the fact that Bill had no part in the conception and early development of the report and therefore could not be expected to know how it all began.

In the early 1960s, a number of events occurred which, taken together, had a far-reaching impact on the role NSA was then playing in the U.S. intelligence community. Where prior to that time the role of the SIGINT establishment had been mainly that of collector and processor, from the Cuban missile crisis onward we experienced a marked increase in requirements for end-product reporting of SIGINT developments. Our customers wanted SIGINT information to be put in its true perspective. At the same time, of course, we were reminded to avoid even the appearance of producing "finished intelligence" for which we were not equipped, technically or statutorily. Coincident with the entry of NSA into the reporting business was the establishment of the NSA SIGINT Command Center, successor to the PROD Watch Office and predecessor to our present NSOC. At some point during this time it must have seemed logical to produce a daily summary of SIGINT highlights for our customers and for NSA executives. And so the NSA SIGINT Daily Summary (SDS) -- the immediate predecessor of the NSA SIGINT Summary -- was born.

The SDS was divided into three sections:

- World Highlights (mostly G Group items),
- Red Extract (A Group items), and
- Gold Extract (B Group items).

Items were carried to the Command Center during the morning and early afternoon, edited there, and delivered to the FLEXROOM in the early evening hours for hard-copy and electrical preparation. Later in the evening the electrical version would go out over the wires to a worldwide distribution which is essentially the same as that which the SIGSUM uses today. The hard copy, most of the time, would be delivered to its Washington-area customers early the next morning. (I say "most of the time" because I can recall one or two times when its delivery was not so early and some of our customers let us know about it.)

The SDS had some shortcomings. The quality of the items it printed was, to put it charitably, inconsistent. Items were often submitted in handwritten form and had to be deciphered

". . . the idea was not passionately embraced; at least, not right away."

and typed before they could be edited. Most serious was the virtual absence of any input to the Gold Extract. The reason for that was that [redacted] put out its own daily summary and the SDS was not only competition for it but, since a large percentage of their respective audiences were the same, there was the problem of redundancy. For these reasons, chiefly, the then deputy chief of the Command Center, [redacted], sent me on a mission to each of the PROD Group chiefs to appeal for better support for the SDS. The result of the conversations which then took place was a decision to scrap the SDS in favor of the daily report now called, as it was then, the NSA SIGINT Summary.

P.L. 86-36
EO 1.4.(c)

P.L. 86-36

Contrary to what one might suppose, the idea was not passionately embraced; at least, not right away. [redacted] and some others in the Command Center had reservations about the size of the effort that would be necessary. And there was some concern expressed that we would get flak from CIA, DIA, and State on the ground that we infringing on their prerogatives. But the SIGSUM was clearly an idea whose time had

DOCID: 4019647

come. All the Group chiefs and Chief, P05 were strongly in favor of a first-class daily SIGINT summary report, in fact, had been for some time, and persuaded the then ADP, [redacted], that the time to strike was at hand.

It took about 2 months to do the preliminary planning for the SIGSUM. The original team that was responsible for developing the format and layout consisted of two people -- Dave Cossum and me. Warner Parsons soon joined us as visual-aids coordinator, and [redacted] and [redacted] were the principal artists who developed the cover design and page formats.

At this point it should be made clear that the SIGSUM had no official status as yet; Mr. [redacted] had only given his approval to explore the ways and means of upgrading NSA daily-summary reporting and to prepare a mockup (a printer's dummy) of our proposed publication. He would then decide between two alternatives: seek the Director's approval or shelve the idea. In the course of the exploration some amusing situations developed. The one that I remember most clearly had to do with estimating the number of maps we would have to keep on hand to cover all reasonably projected reporting situations for a given period of time -- 2 months, I think. Our plan was to place the resulting order with a Mr. [redacted] at CIA, with whom we had a "connection." After considerable postulation, speculation, and multiplication, Warner arrived at a number that none of us, including him, believed. Our astonishment was quickly exceeded, however, by the uproarious laughter the number evoked in our "connection," [redacted], then Chief of the Geographic Branch in CREF (now C5). The number was 1,500,000 maps. (Incredible as it may seem, the figure proved to be very near the mark.)

EO 1.4.(c)

[redacted]

At this point I must take issue with Bill on three points he made in his article, and clarify the situation by emphasizing the following true statements:

- the SIGSUM was *not* conceived and designed by the Assistant Director for Production;
- there *was*, indeed, a clear-cut requirement for it which was set forth with admirable clarity and directness by General Carter in a letter to DIRDIA, General Carroll, in early 1966; and
- it *was* fully developed within a year after it first appeared.

The reader might have also concluded, if he has read this far, that it is indeed both possible and -- from my point of view, at least -- desirable "to trace the SIGSUM's growing pains."

By mutual agreement with the Group Chiefs, the SIGSUM was put together every day by an editorial board on which each Group had representation. In addition, a CREF representative, Miss Ruth Schley, provided collateral and scientific and technical information support, and Warner Parsons served as art editor.

The other charter members of the editorial board were [redacted]. Dave Cossum was appointed Editor-in-Chief, and I was designated his alternate. The hard decisions which became the basic operating philosophy of the SIGSUM were hammered out by this group, often in the late hours of the evening. One of the Director's briefers, [redacted] also sat in on the deliberations. This group of people and the others who followed them, particularly Warren Keniston [redacted], deserve an equal share of any credit that is to be given for the SIGSUM. The result of all their efforts was a first-class intelligence report that was widely praised as being a worthy addition to the daily reports that were already available to the government's highest-level decision-makers. Among the many laudatory wires received, I particularly recall those sent by the Secretary of State, CINCSAC, and CINCPAC. We were also told unofficially that it was warmly received at the White House (a number of copies with Walt Rostow's marginal notes very much in evidence were mysteriously returned to us for disposition). Needless to say, we were all both pleased and relieved to have the SIGSUM so highly regarded, especially by some who might have considered it competition with their own daily summaries. The SIGSUM had received its baptism of fire, so to speak, and had come through it unscathed.

P.L. 86-36

> *"Among the many laudatory wires received [after the institution of of the SIGSUM], I particularly recall those sent by the Secretary of State, CINCSAC, and CINCPAC."*

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

Letters to the Editor

To the Editor, CRYPTOLOG:

I had a scare the other day, but it all turned out okay and I thought that you and some of your readers might find amusement and instruction in the tale. While on a brief TDY to [redacted] Washington, with [redacted] we were told informally, by one of the people there, of a technique [redacted] that amazed me. This was the story:

EO 1.4.(c)
P.L. 86-36

[redacted]

doesn't seem to matter.

Had we been missing an obvious bet? How could such a scheme possibly work? We had to find out more about it.

[redacted]

Without denying that this scheme, which has proven to be very successful, is an example of a simple yet ingenious solution to a problem of long standing, I am relieved. If it were possible to train a linguistically naive person to listen to *any* language and hear specific words imbedded in conversations, some basic ideas would have to be changed, and I am too old to start over.

Jack Gurin, R5

~~(SECRET - CCO)~~

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

To the Editor, CRYPTOLOG:

Under normal circumstances I would have exercised my prerogative to ditch C-LINER's "Impure Mathematics" (Final 1976 issue) in the open trash receptacle where it belongs. It clearly has no SIGINT value, no intellectual value, and in my judgment not a modicum of socially redeeming value. No wonder the author chose not to put his name to it.

But I can't do that because the thing was published in an official government document under an official SECRET Codeword classification -- circumstances which could hardly be considered normal. Hence, the burn bag.

I feel reasonably confident that C-LINER, in taking upon itself this one degree of freedom too many, has offended the moral and professional sensitivities of other people around the agency, as it did mine. It is inconceivable that the average mission-oriented NSAer would give assent to the seepage of this type of writing into SIGINT literature. P.L. 86-36

Where is the sorely-needed NSA/CSS voice of authority to say: "Yes. As a society we have indeed mortgaged our self-respect to the likes of Hefner and Guccione. But this is where we draw the line"?

Hopefully, we will not have to wait too long before the Director's voice is heard in this regard.

As for C-LINER itself, all things considered maybe it is just as well that it's now a thing of the past.

"Appalled"
[name withheld at writer's request]

Copy to:
Chief C (Mr. Speierman)
Director NSA/CSS (General Allen)

(UNCLASSIFIED)

Editor's reply

In the final issue of C-LINERS ("the second reincarnation cycle of the C Group Machine Processing Information Bulletin"), its editor, David J. Williams urged potential authors to send their articles to CRYPTOLOG. He also stated, "If you disagree with any of the materials in this issue, you can carry on the fight in CRYPTOLOG, I am sure that Arthur will be happy to carry your rebuttal." I'm pleased that someone took up Dave's second suggestion. Wouldn't it have been nice if someone had taken up his first suggestion that quickly.

Dave explains the lack of an author's name as follows: the item was supposed to have a headline "Tales from the Past" or "Golden Oldie"), but the headline got dropped during page composition. The general feeling was that the item was in the public domain, and might have been written by "someone [redacted] in the early 1950s." Dave says that he is "highly EO 1.4.(c) P.L. 86-36

DOCID: 4019647

amused" at the reaction it evoked from you because, when the C-LINERS editorial board was considering it for publication, they showed it to several professional mathematicians. All felt that it was (a) "cute," (b) "professionally sound," and (c) "definitely worth printing." With a consensus like that, how could Dave have failed to print it?

(UNCLASSIFIED)

To the Editor, CRYPTOLOG:

The [redacted] interview in the December issue of CRYPTOLOG is outstanding! I also think that the interview idea is a brilliant one. There are undoubtedly more than a few of our people at various levels of the management chain and also more than a few of the stalwart experts who would be amenable to sharing their views, experiences, and expertise in this format. The [redacted] interview provided an insight into a story that may never have seen the light of day had it not been for CRYPTOLOG. Truly, SIGINT journalism at its finest!

I am in the process of collecting information for a couple of articles which I promised you some time ago. I hope to surprise you one day and even complete them.

Keep up the outstanding work!

[redacted] G95

Editor's reply

Thanks for the kind words. We're glad you like the interview format, and we hope to use it again soon. Someone else who liked the [redacted] interview, as well as the Kathy Bjorklund article on the SR test, was [redacted] of the SR Career Panel. He requested 50 extra copies of the December issue and intends to give them to current and future SR interns for "mandatory reading" of both items.

(UNCLASSIFIED)

To the Editor, CRYPTOLOG:

In response to [redacted] article "Let's Give Linguists a Bigger Piece of the Pie!" (CRYPTOLOG, December 1976), I say, "No more pie 'til you eat your spinach!"

[redacted] article states or implies the following suggestions:

(a) some sort of quota system should be implemented that would allow the distribution of GG 15-18 personnel in this agency to include *x* desk linguists;

(b) various levels of agency management are unaware of the problem as perceived by [redacted]

(c) an advanced degree in language is *prima facie* evidence that we can expect superior performance as an operational linguist;

(d) we are grossly overpaying linguists at the lower end of the GG scale, while grossly underpaying them at the high end.

Well, sir, that is a most extraordinary group of suggestions, and a group that I mostly disagree with. Let me start at the beginning:

(a) I expect that [redacted] meant to imply some degree of quality in recommending that the desk linguist be included in the 15-18 category. But does he really expect that someone in this agency can or will come up with language analyst billets in that grade range? I don't think so. And I think the rationale behind such a decision would be that "he isn't likely to be worth that much money." Now that's a hard cold look at it, but it's probably closer to the truth than any COSC manual that allows 9-18 as the path of the language analyst. Since [redacted] did not indicate that he was discussing multi-linguists or multi-skilled people, I am assuming that he is including the highly qualified, single-foreign-language, certified language or voice language analyst in his numbers. If he honestly believes that such an analyst is going to make it beyond 12 or 13 without demonstrating a skill beyond turning foreign sounds or words into English sounds or words, using a skill in a single foreign language -- well, I just don't know what measure he is using. P.L. 86-36

(b) A few years ago I would have agreed that the upper levels of agency management were at best unreceptive to the idea of promoting linguists. I no longer believe that. I have seen too many promotions in the last couple of years to the 12-15 range and, while I am certain that there are individual cases of inequity, I would strongly disagree that there are any grounds for a "class action." Our activist language panel would no doubt be offended by the suggestion that it did not know what was going on in the language world. Perhaps [redacted] is not aware that current hiring plans for new agency personnel are almost totally devoted to the acquisition of language technicians.

(c) The issue of advanced degrees in language, I think, has been largely resolved by several developments: a general lack of availability brought about by an overall reduction of language majors at many universities; a requirement to retrain language majors in real-world applications of the language they studied in the academic world -- and all too frequently this training has been at the very basic level, hence expensive; and, last but not least, the "average grade structure" problem which says that we got to hire more people at lower grades, do less promoting above grade 12, and, perhaps most important, keep the language analyst in that job -- the job on which his paycheck is quite likely to depend. Again, I realize that it sounds harsh, but the times are changing. While the agency might like to help the language analyst to move into a different

DOCID: 4019647

field and very often did that in the past, I would expect to see a tightening of the belt as more and more interest is shown in the problems we face. Ironic, isn't it? In the years when those language problems were back-burnered, we always kind of assumed that when the linguist got the spotlight he would just zoom ahead so fast, we wouldn't be able to keep up with him. Now that he is in that spotlight -- and, believe me, he is there -- we are going to see, I expect, more actions similar to the recent personnel decision that dropped the entry level for linguists (and others); higher standards for language professionalization; and tighter controls on the language field in general. FYI, our language-hire program for the next couple of years will probably focus on high-school graduates at grades 2-3.

(d) While I don't have much of a problem finding some underpaid linguists in grades 5-9, I personally am unaware of any who think they are underpaid above those grades. But, here again, we may be discussing two different ideas. [redacted] seems to be suggesting that, as a matter of high agency policy, linguists do not get promoted. I would like to suggest that he look lower. Promotion recommendations come from the divisions and offices and, by and large, they get their recommendations accepted.

One final remark: the linguist who flees the field had better take with him some skills other than language. I don't know many desk analysts, TAs, or CAs who are supergrades. If there is ever to be a group of supergrades in the language field, they will come from the ranks of multi-linguists, linguist/analyst/managers, or other multi-skilled people. And that's the truth.

Dan Buckley,
B Language Coordinator
(UNCLASSIFIED)

SPANAKOPITA*

10 sheets phyllo (12 x 15 inches)
½ cup butter, melted
2 packages (10 ounces each) fresh spinach
1 tablespoon salt
2 eggs
2 cups cottage cheese (small curd)
1 cup grated feta cheese
3 tablespoons parsley
2 green onions with tops, minced
Salt and pepper

Cut phyllo sheets into halves and place 10 pieces in a buttered pan (7 x 11 inches). Brush each sheet of phyllo with melted butter.

Wash spinach and remove stems. Cut leaves into ½-inch lengths. Sprinkle with salt and let stand for 15 minutes. Beat eggs. Add cheeses, parsley, and onion. Squeeze liquid from spinach. Fold spinach into egg mixture. Season with salt and pepper to taste. Spread mixture over phyllo sheets in pan and top with remaining 10 pieces of phyllo, brushing each sheet with remaining melted butter. Bake in preheated moderate oven (350°F.) for 40 minutes. Cut into squares and serve hot. Makes 6 servings.

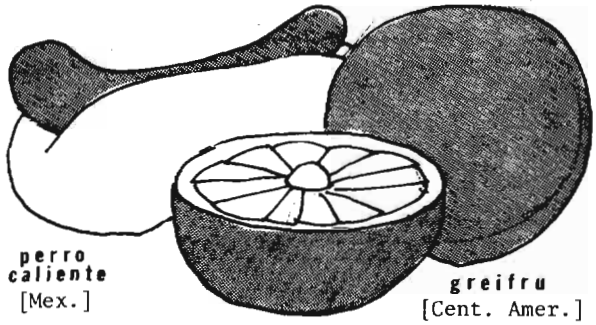
*Greek spinach pie.

SOLUTION TO NSA-CROSTIC No. 6
(January-February 1977)

[redacted] "Anglicisms in Puerto Rico" P.L. 86-36

(NSA Technical Journal,
Vol. XVII, No. 1, Winter 1972;
reprinted in *NSA Technical Journal: Special Linguistics Issue III, 1976-1978)*

"A linguistic 'laissez-faire' has existed [in Puerto Rico] for a long time. Although schools and newspapers have actively encouraged correct use of Spanish. . ., only the most undesirable borrowings [from English] have disappeared, and . . . new ones have appeared."



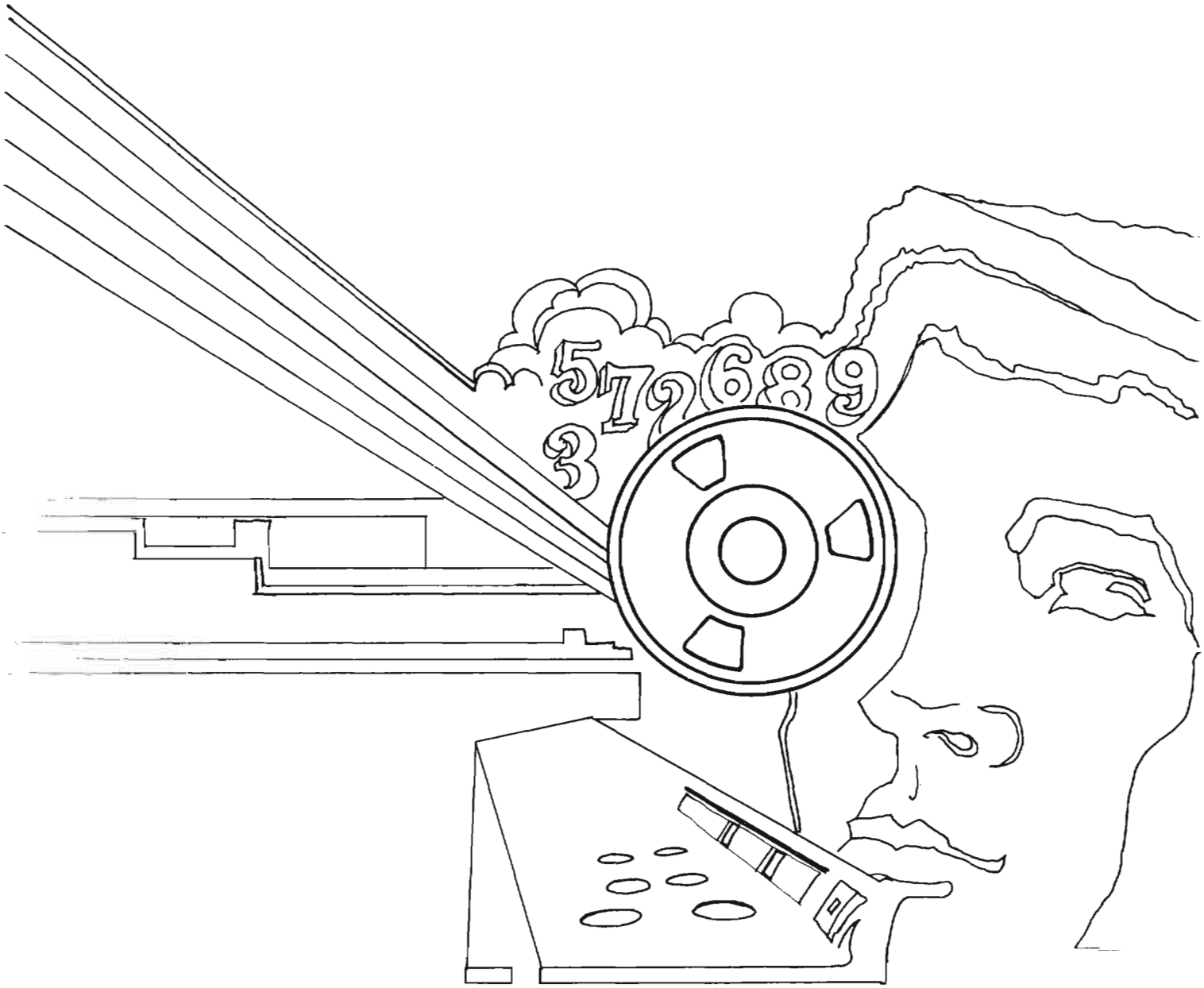
(UNCLASSIFIED)

If you're planning to enter this year's CMI or CLA Essay Contest, or the newly established IAI Essay Contest, you'd better get a move on! The deadline for the CLA Essay is/was 4 March 1977, and for the CMI and IAI Essay Contests is 25 March 1977.

Complete information about all three contests can be found in the Fall 1976 issue of the *NSA Technical Journal*.

(UNCLASSIFIED)

P1-Jan 77-S32-25100


5 7 9 6 8 9
3

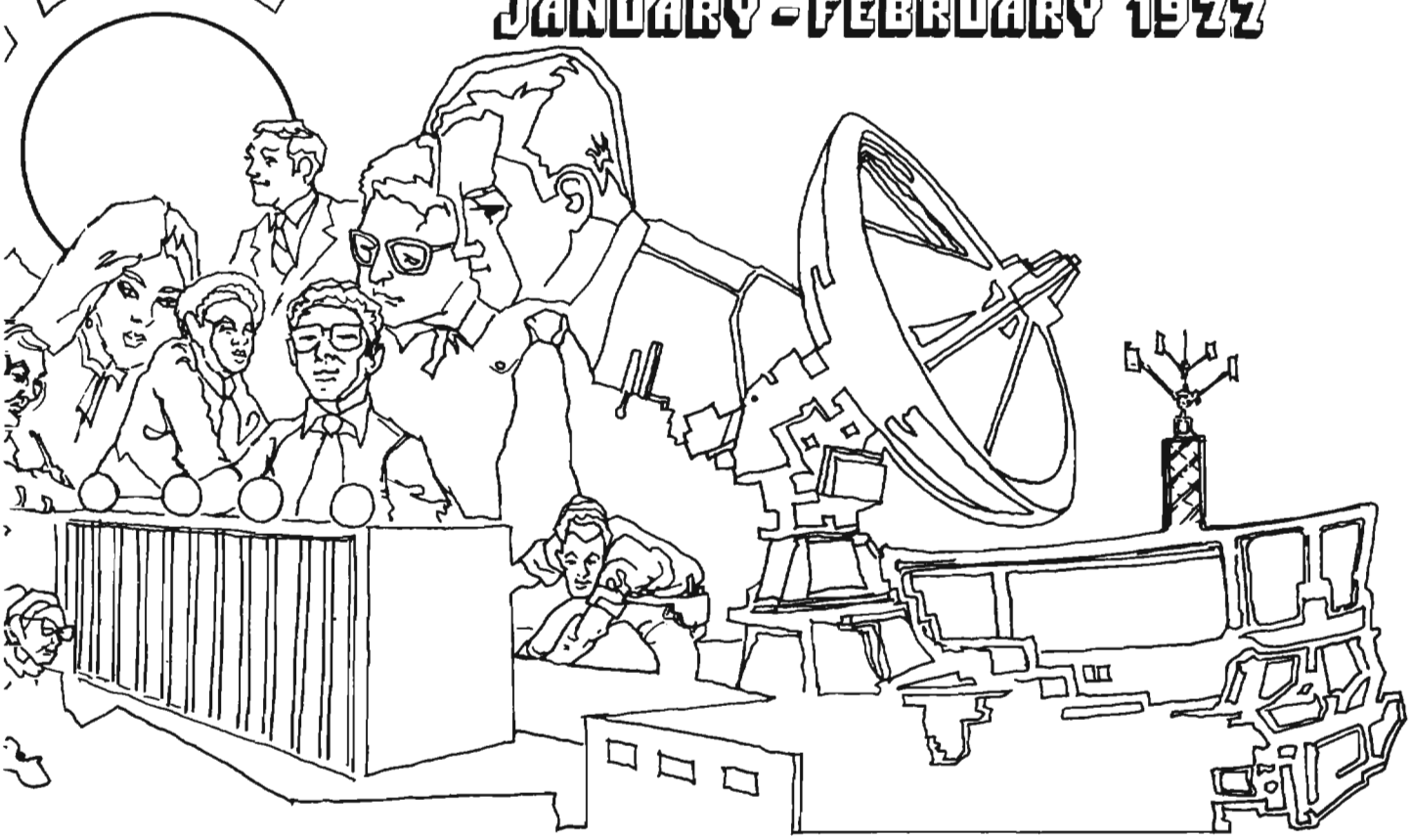
DOCID: 4009790

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JANUARY - FEBRUARY 1977



WHAT IF THE LINGUISTS DISAPPEARED?... [redacted] 1
EXECUTIVE ORDER 11652..... [redacted] 4
WHERE WERE WE?.....Frederic O. Mason, Jr.....5
LETTERS TO THE EDITOR.....17
NSA-CROSTIC No. 6.....A.J.S.....18
GOLDEN OLDIES: A MEDAL FOR HORATIUS.....20
LANGUAGE IN THE NEWS ("Doublespeak").....21

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526.
MDR Case # 54778

DOCID: 4009790

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. IV, Nos. 1-2 JANUARY-FEBRUARY 1977

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5642s)
Collection.....[redacted] (8955s)
Cryptanalysis.....[redacted] (8025s)
Language.....Emery W. Tetrault (5236s)
Machine Support.....[redacted] 3321s)
Mathematics.....Reed Dawson (3957s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Frederic O. Mason, Jr. (4142s)
Production Manager.....Harry Goff (4998s)

P.L. 86-36

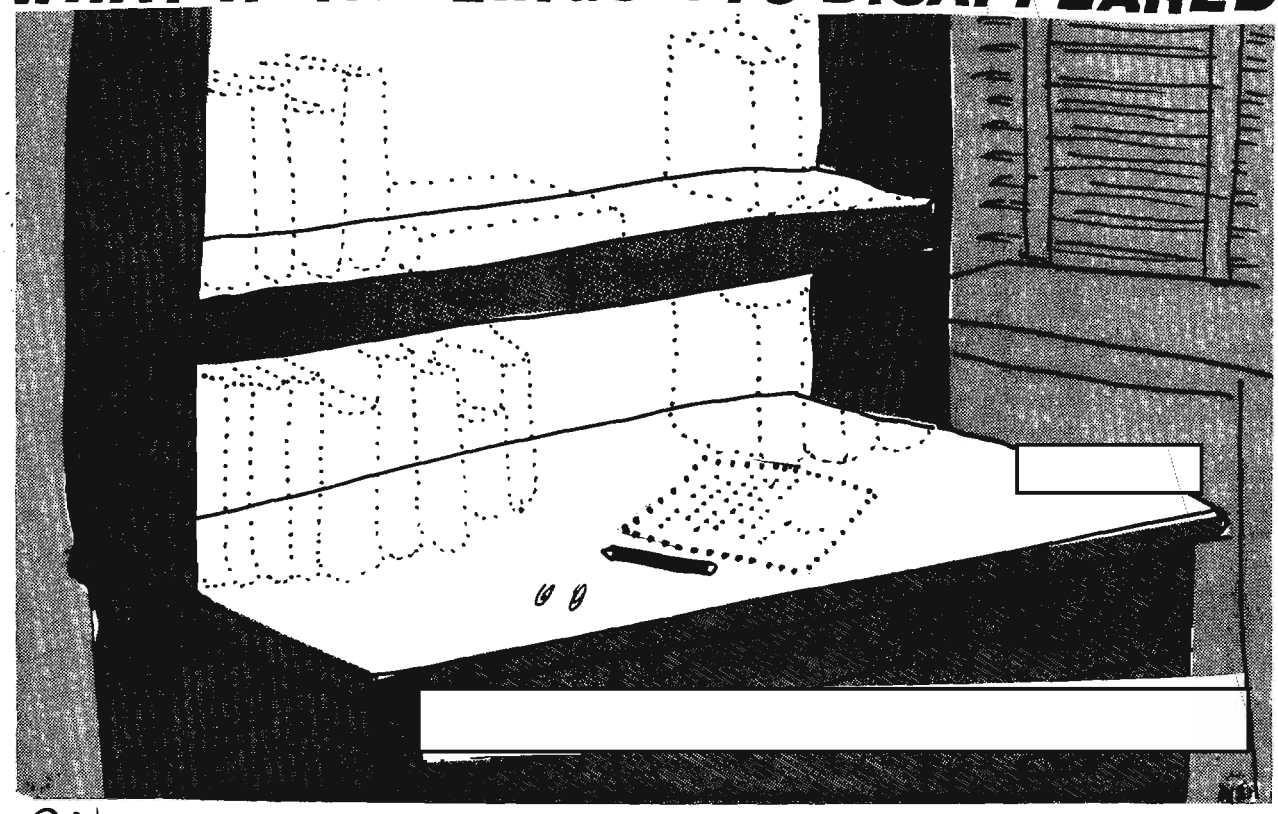
For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4009790

P.L. 86-36

WHAT IF THE LINGUISTS DISAPPEARED?



What is the exact nature of the work done by NSA linguists? When linguists work with different languages, with materials in varying volumes and in various printed and spoken forms, what duties do they perform in common, and what duties are completely different? Those questions were not specifically posed in the mission originally assigned to the Language Analysis Task Force (LATFO) when it was created in 1975. Instead, that mission, simply stated, was to analyze and validate the NSA Career Service Occupation System as it applies to NSA personnel in the Language Career Field (12XX). But, during the 14 months of its existence, LATFO (Chairman [redacted] found these two unstated questions constantly coming up. In interviews with Agency linguists, and in our subsequent discussions, we found that certain functions could easily be fitted into logical categories, but others just didn't want to work that way. As a result of these divergences, our interviews and discussions ranged far beyond the limits of our stated mission and, by the time LATFO submitted its official report, we had gained many revealing insights into the facts of life as faced by the average NSA linguist (if such a person exists).

Some of these insights pertained to our mission and found their way into the official report that we submitted to the Task Analysis Steering Committee. But others pertained not to the specific mission, but to the overall philosophy of language occupation at NSA. We considered these insights to be outside the purview and mission assigned to LAFTO and, accordingly, did not include them our official report. But, since these incidental ideas were deemed to be too valuable to simply throw away, I took it upon myself to present them in my own way in a special memorandum to ADPS, as an individual report by the B Group member of LATFO.

It is that memorandum which has served as the basis for the article which follows. I must state at the outset that most of the ideas expressed in this article are my own and I take full responsibility for them. But I cannot take full credit for all of them, because the background experiences and knowledge of my colleagues, coupled with the stimulus and criticisms that flowed freely in some of our heated discussions, effectively sharpened my own perceptions and personal views.

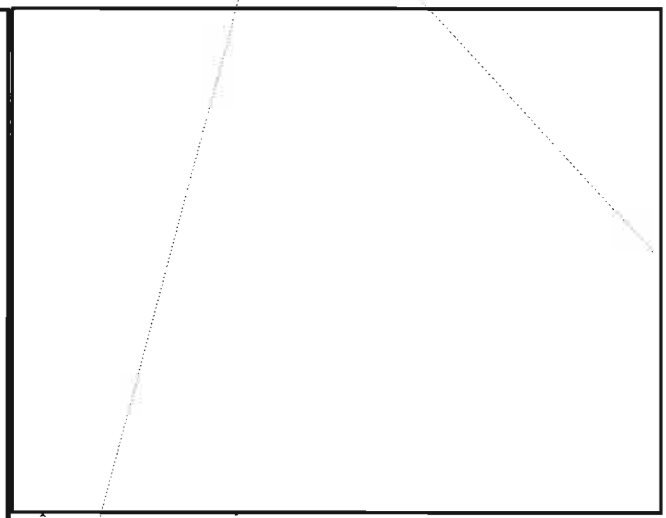
The LATFO report was an investigation into what NSA's linguists -- that is, people -- do. In the following pages I hope to show the other side of the coin -- the vital role that foreign languages play in the production of COMINT reports.

P.L. 86-36

DOCID: 4009790

EO 1.4.(c)
P.L. 86-36

~~CONFIDENTIAL~~



Foreign languages are the stock in trade of translators, transcribers, and those who do language research of various types, but the skills of the translator and transcriber are not at all equal. Many good translators have poor aural comprehension and do poorly at transcribing voice tapes, and some of them decline to do it at all because transcription work can be monotonous and boring. However, any good transcriber, as a general rule of thumb, has the added capability of translating, if he knows the English language (some of our native-born linguists have trouble translating into English, which is, after all, *their* second language).

I have dwelt heavily on the language aspects of the above "analytic" disciplines (the "reporters" come later) with their differences and distinctions because so few NSA managers seem to have a clear understanding of the fact that *knowledge of a foreign language is the key ingredient for most of NSA's end product.* They tend to look upon language knowledge as a simple "tool" that can be turned on or off by the flip of a switch, and something that any reasonably intelligent person can learn with a little study. But that just ain't so! This misconception is, I believe, responsible for much of NSA's "language problem."

NSA management needs to understand that knowledge of a foreign language is a difficult skill acquired by hard study in an educational environment and sharpened by on-the-job experience. In this respect it is no different from any other learned skill, such as mathematics, engineering, computery, or whatever. One can even say that the only valid way in which the knowledge of a foreign language can be called a "tool" is if "tool" is used in the sense of a scalpel in the hands of a competent surgeon who must possess a precise knowledge of the entire human body, many specialized surgical instruments, the properties and effects of different medicines, and a thorough awareness of the damage that may ensue if his knowledge and treatment are incorrect or inadequate.

~~CONFIDENTIAL~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

~~CONFIDENTIAL~~

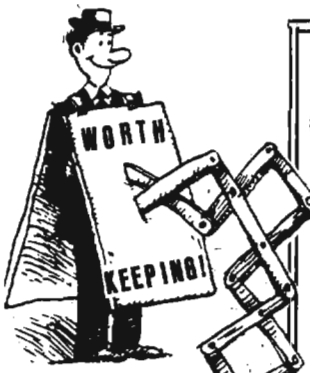
EO 1.4.(c)
P.L. 86-36

The use of foreign languages as a "tool" is likewise dependent upon the skill of the practitioner, which is the sum total of his training, experience, background knowledge in related fields, drive, imagination, and, not least, his knowledge of the English language and his ability to express ideas in written form.

It is in this latter situation that we see a subtle shift in management's perception of the relative importance of the linguist's role vis-a-vis the reporter's role, to the detriment of the linguist. In that shifted perception, the reporter's end-product output is deemed to be more important than the linguist's output which made that report possible. This has resulted in a widespread feeling that reporters enjoy higher status, and in the last few years the higher-grade promotions appear to have gone to the reporters as a group. "It's the field to be in if you want to get ahead" is a frequent comment I have heard, often from reporters themselves. This is probably due to the very human tendency of supervisors and managers to know best -- and to reward -- those with whom they are in most frequent contact and whose work they review.

~~CONFIDENTIAL~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

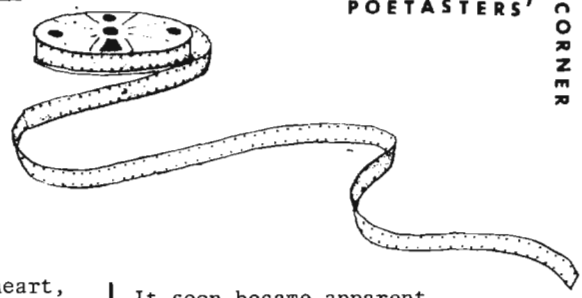
DOCID: 4009790



POETASTERS' CORNER

EXECUTIVE ORDER 11652

Helmut Leiner, 05



When I was one-and-twenty,
I heard a wise man say,
"Give riches, and perhaps your heart,
But not COMINT away.

"Save every bit," he counseled.
"And I will show the way --
Construct a vault; store wheat and chaff
Forever and a day.

"Be diligent in saving;
Be not by space deterred."
Yes, I was one-and-twenty,
And heeded every word.

I saved and filed and indexed;
My COMINT storehouse grew.
The things I started with were old,
But I kept adding new.

Then space became a problem.
(We all know how that feels!)
I microfilmed the wheat and chaff,
And put it all on reels.

The years went on. In sixty-two
The Agencies were told:
"Declassify each item
That's a score and ten years old."

The Information Freedom Act
Came shortly afterward.
The groans of high officials
Were loudly to be heard.

The items in our storehouse --
Which ones would thus fall prey?
To judge each, it would take *one more*
"Forever and a day"!

It soon became apparent,
This was a task indeed.
The talent still remaining here
Fell short of what we'd need.

And so the call was issued
To Croskery and Howe --
To Steinmetz and to Flossie Burn:
"Come back. We need you now!"

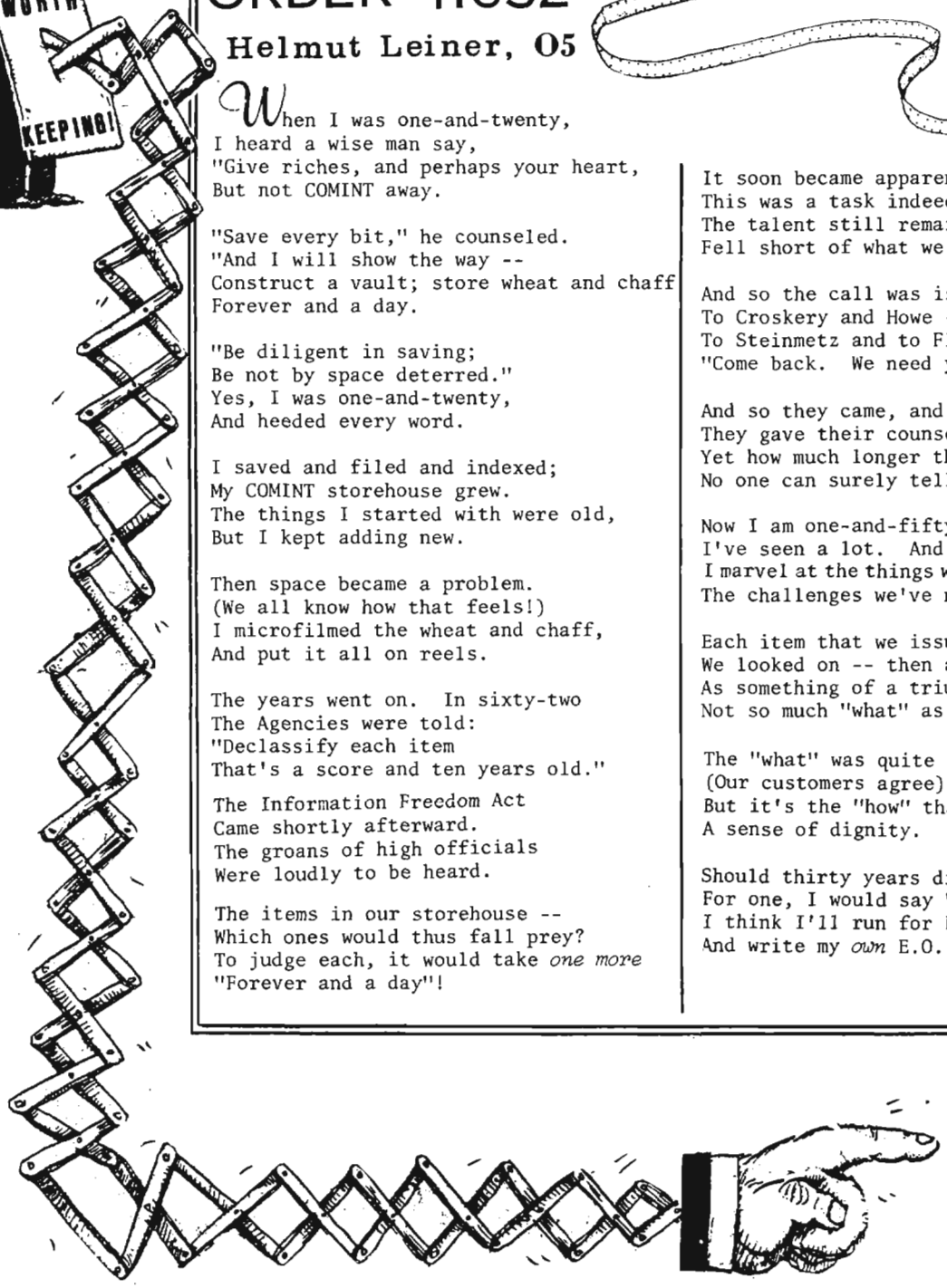
And so they came, and labored;
They gave their counsel well.
Yet how much longer this will take,
No one can surely tell.

Now I am one-and-fifty.
I've seen a lot. And yet,
I marvel at the things we've done --
The challenges we've met.

Each item that we issued
We looked on -- then and now --
As something of a triumph;
Not so much "what" as "how."

The "what" was quite important
(Our customers agree);
But it's the "how" that gave us
A sense of dignity.

Should thirty years diminish this?
For one, I would say "No!"
I think I'll run for President,
And write my *own* E.O.



The listing on the next 12 pages has been printed in the center of the magazine so that it can be easily removed for use as a permanent reference aid.

WHERE WERE WE?
Frederic O. Mason Jr., P14

The U.S. SIGINT establishment has developed, used, and abandoned so many sites that it is now difficult to remember them all, what their station numbers were, and just when they were active. The following compilation, which was produced in response to a request from Chief, P1, is offered to the reader as a reference aid, even though the information in it is known to be incomplete.

The arrangement below shows the station number (minus "US" prefix); the currently active sites (offset to left, in *italic*); abandoned sites; SCA unit numbers; and the years active.

Data for 1949 to date conforms to USSID-505 rules. All records shown are stored on a B6700 disk file for update and for extraction of data in a variety of sorts (such as by service, by country, etc.).

Stations active only in years for which sources were not available are probably not shown. When stations moved, they are often shown on separate lines, with different year spans.

Note that the listing is in two parts, each with its own classification. Part I, covering the period 1917 through 1946, is classified TOP SECRET CODEWORD. Part II, covering the period 1947 through the present, is classified SECRET, HANDLE VIA COMINT CHANNELS ONLY.

INTERCEPT STATIONS THROUGH WORLD WAR II

Data derived from: NSA Cryptologic History Staff, E51

Designator	Location		Active year span, same place (1917 through 1946) 1 789 2 0123456789 3 0123456789 4 0123456
RADIO TRACTOR UNITS (Army and Federalized Nat Gd vs Pancho Villa)			
RTU-31	McAllen, Texas	(31 Oct 1918)	1 8
RTU-32	McAllen, Texas	(31 Oct 1918)	8
RTU-33	Laredo, Texas	(31 Dec 1918)	8
RTU-34	Laredo, Texas	(31 Dec 1918)	8
RTU-37	Del Rio, Texas	(1 May 1918)	8
RTU-38	San Antonio, Texas	(1 May 1918)	8
RTU-39	Sutherland Springs, Texas	(1 May 1918)	8
RTU-42	San Antonio, Texas	(1 May 1918)	8
RTU-43	Pecos, Texas	(20 Sep 1918)	8
RTU-44	Ft Bliss, Texas	(20 Sep 1918)	8
RTU-45	Las Cruces, New Mexico	(20 Sep 1918)	8
RTU-46	Las Cruces, New Mexico	(20 Sep 1918)	8
RTU-47	Lordsburg, New Mexico	(4 Oct 1918)	8
RTU-48	Lordsburg, New Mexico	(4 Oct 1918)	8
ARMY INTERCEPT STATIONS, AEF			
#1	Verdun, France	(11 Nov 1918)	1 8
#2	Verdun, France	(11 Nov 1918)	8
#3	Euvezin, France	(11 Nov 1918)	8
#4	Euvezin, France	(11 Nov 1918)	8
#5	Verdun, France	(11 Nov 1918)	8
Aero #1	Euvezin, France	(11 Nov 1918)	8
Aero #2	Tomblaine, France	(11 Nov 1918)	8
Aero #11	Verdun, France	(11 Nov 1918)	8
	Souilly Meuse, France	(14 Nov 1917)	1 7
(2 stns)	Coblenz, Germany	(14 Dec 1918)	8
	Ft Wool, NY Harbor		8?

Designator	Location		Active year span, same place (1917 through 1946)
			1 2 3 4 7890123456789012345678901234 56
ARMY LISTENING STATIONS, AEF			
#1	Saulz, France	(11 Nov 1918)	1 8
#2	Fresnes, France	(11 Nov 1918)	8
Hqs	Bois de Creus, France	(11 Nov 1918)	8
Le Souche,	Louisville Ferme, France	(11 Nov 1918)	8
Le Rebois,	Bois de Haudenvilles, France	(11 Nov 1918)	8
OTHER ARMY INTERCEPT STATIONS			
	Calexico, California		1 9
	Mexico, City, Mexico		11 78
	Houlton, Maine		8
	Tucson, Arizona		8
	Nogales, Arizona		9
	Del Rio, Texas		9
	McAllen, Texas		9
	Monterey, California		9
	Philippine Dept, Ft Hughes		9? 3 3 12345
	Boston, Massachusetts, 1st Army Hqs		2 3
	Governor's Island, New York		3
MS-1	Ft Monmouth, New Jersey		3 3 678
MS-1	Ft Hancock, New Jersey		3 4 8901
MS-1	Vint Hill Farms Stn, Virginia		4 4 23456
MS-2	Presidio, California		2 4 3456789012345678901 4 4
MS-2	Two Rock Ranch, Petaluma, California		23456
MS-3	Ft Sam Houston, Texas		2 4 789012345678901234 4
MS-3	Miami, Florida		45
MS-4	Panama Dept, Quarry Heights		3 4 1234567890123 4 4
MS-4	Asmara, Eritrea		3 4 456
MS-5	Hawaiian Dept, Ft Shafter		7890123 4 4
MS-5	Helemano, Hawaii		456
MS-6	Ft McKinley, Philippines		3 4 901
MS-6	Amchitka, Alaska		4 4 456
MS-7	Ft Hunt, Virginia		3 4 9012 4
MS-7	Fairbanks, Alaska		23456
MS-8	New Delhi, India		2345
MS-9	OSS Ops, Bellmore, New York		2345
MS-9	Las Pines, Philippines		56
MS-10	Tarzana, Reseda, California		4 4 345
MS-11	Guam		456
MS-12N	RCA in New York		4 4 23
MS-12S	RCA in California		23
MS-12	Accra, Gold Coast, Africa		4 5
RADIO INTELLIGENCE COMPANIES			
111, 112, 125, 126 under CBB and Gen MacArthur in SW Pacific			4 4 2345?
113, 114, 116, 117, 118, 121, 124, 129, 137 in Europe			2345?
115, 119, 120, 122, 123, 127, 128, 130-136, 138 unlocated			2345?
SIGNAL SERVICE COMPANIES			
3250 through 3264 in Europe			2345?

Designator	Location	Active year span, same place (1917 through 1946)
U.S. NAVY STATIONS		
	DCO, 14th Naval Dist	
	Peiping, China	
	Roof of Navy Dept, Washington, D.C.	
	Flagship (USS Omaha) European Squadrons	
A	Shanghai, China	
B	Guam (Wahiawa)	
	Flagship, CINCAF	
	Olongopo, Philippines	
	Mariveles, Philippines	
C	Cavite, Philippines	
C	Corregidor, Philippines	
C	Melbourne, Australia	
C???	Chatham, Massachusetts (leased from RCA)	
D	Dupont, J.E.	
F	Chungking, China	
F	Fruchi, China	
F	Kweilin, China	
F	Kunming, China	
G	Amagansett, New York (DF only, after 1943)	
	Wailupe, Oahu, Hawaii	
H	Heeia, Hawaii	
H	Wahiawa, Hawaii	
I	Imperial Beach, California	
J	Jupiter, Florida	
M	Cheltenham, Maryland	
O	San Juan, Puerto Rico	
R	Cooktown, Australia	
S	Astoria, Oregon	
S	Bainbridge Island, Wash. (to Coast Guard, 1945)	
T	Skaggs Island, California	
U	Balboa, Canal Zone	
U	Toro Point, Canal Zone	
W	Winter Harbor, Maine	
AA	Adelaide River, Australia	
AL	Guadalcanal	
AL	Okinawa	
AN	Iwo Jima	
AO	Kwajalein	
AR	Recife, Brazil	
AX	Adak, Alaska (to Coast Guard, 1945)	
	Unidentified shipborne intercept against Japanese Grand Naval Maneuvers in 1933, 1934, 1935, and undoubtedly in other years	

Other US intercept stations are not specifically documented, but included:

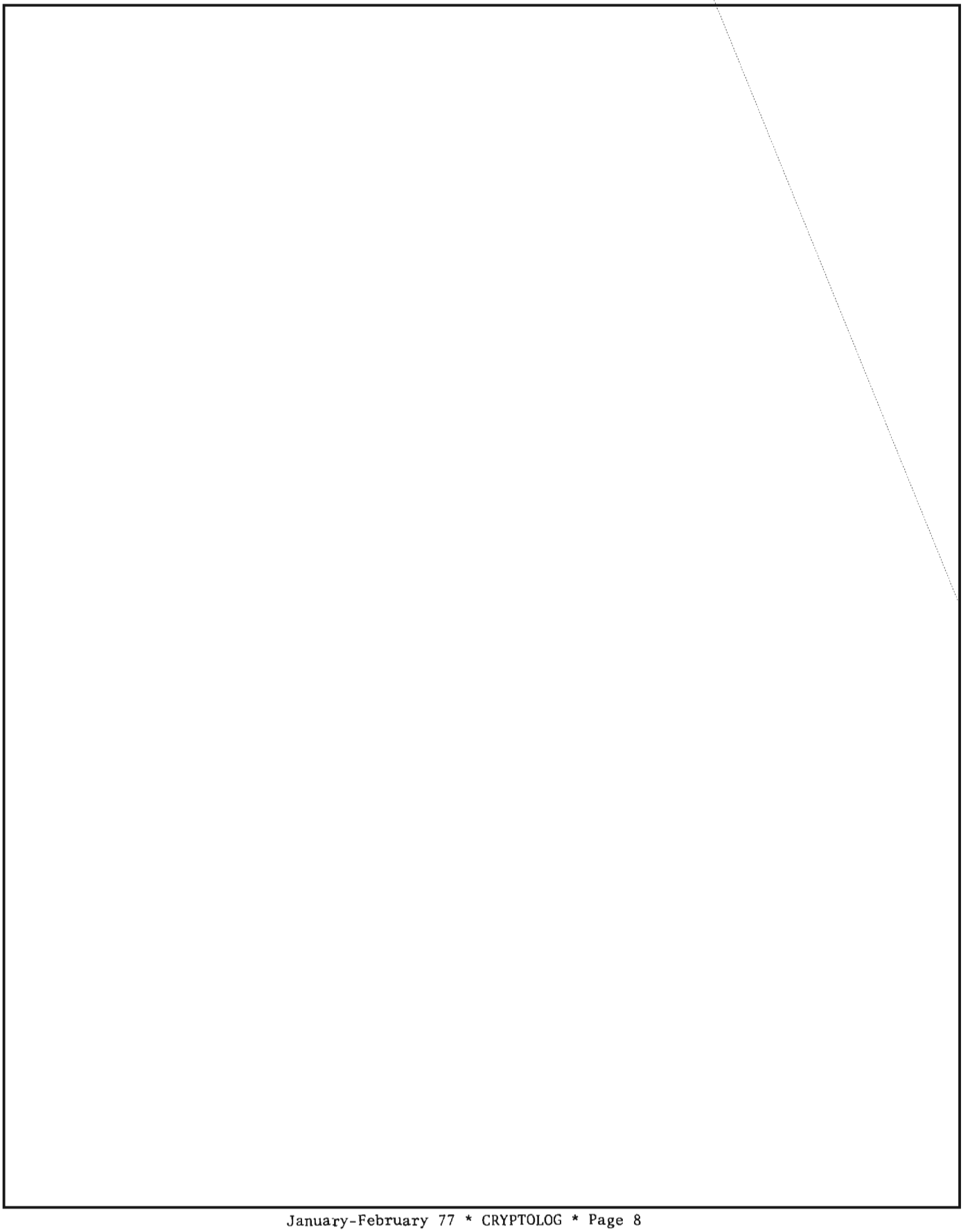
Benjamin Franklin started the US Post Office during the period 1776-1790, and this is alleged to have included a systematic opening of mail in transit to acquire information of value to the government.

Commercial telegraph systems had been established during the 1840s and, during the Civil War, were taken over by both US and CS governments and also, on both sides, supplemented by military field wire and wigwag flag extensions into battle areas and across gaps. Traffic was sometimes enciphered. On both sides, ad hoc wire taps were utilized for intelligence purposes.

Wire taps have been used, or planned, ever since. It was a well-established procedure in World War I trench warfare. In 1945 there was at least one Signal Intelligence Detachment with white officers and Nisei enlisted men trained in wiretapping techniques, scheduled to be in the first wave in the invasion of Japan.

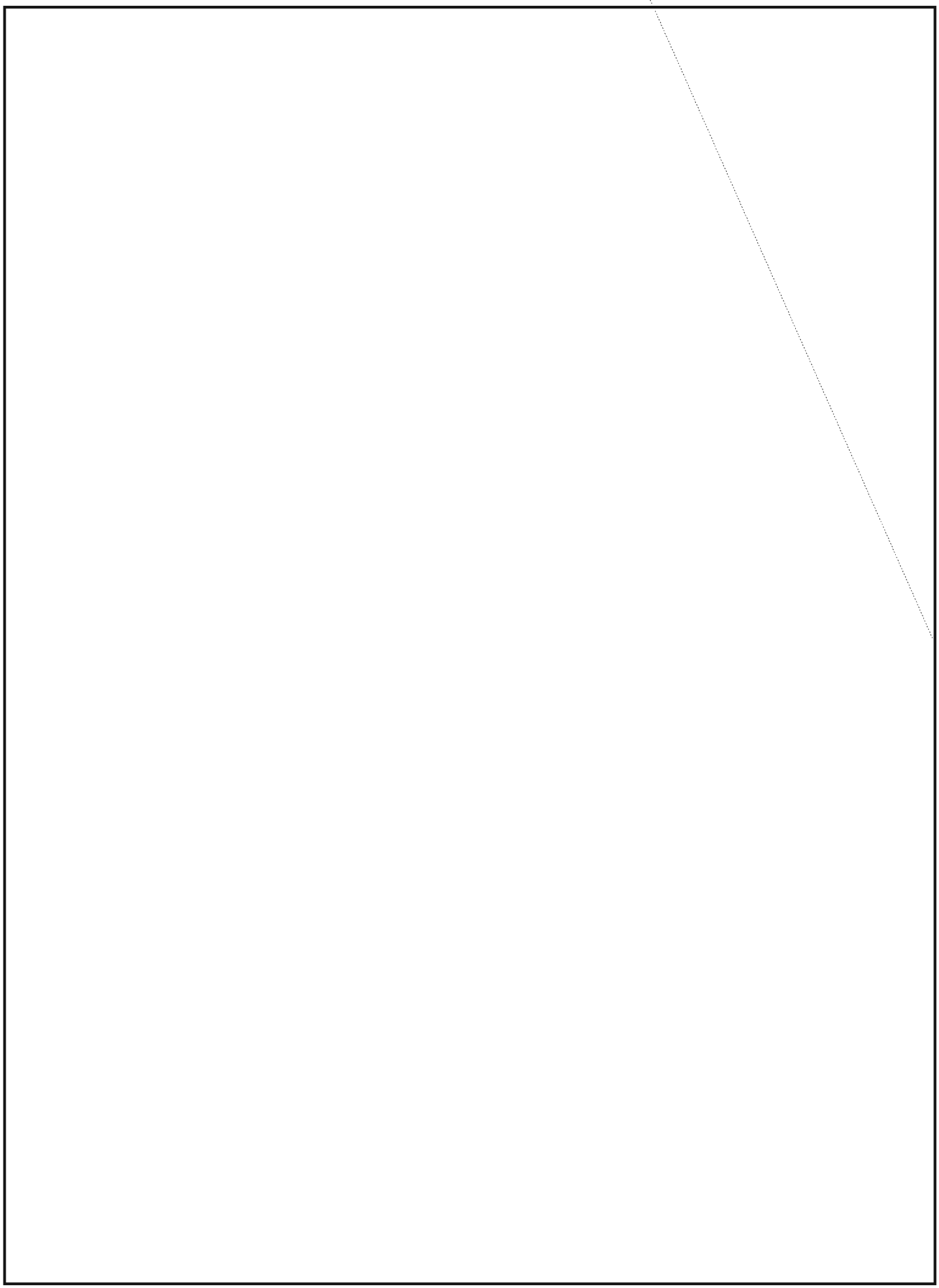
EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



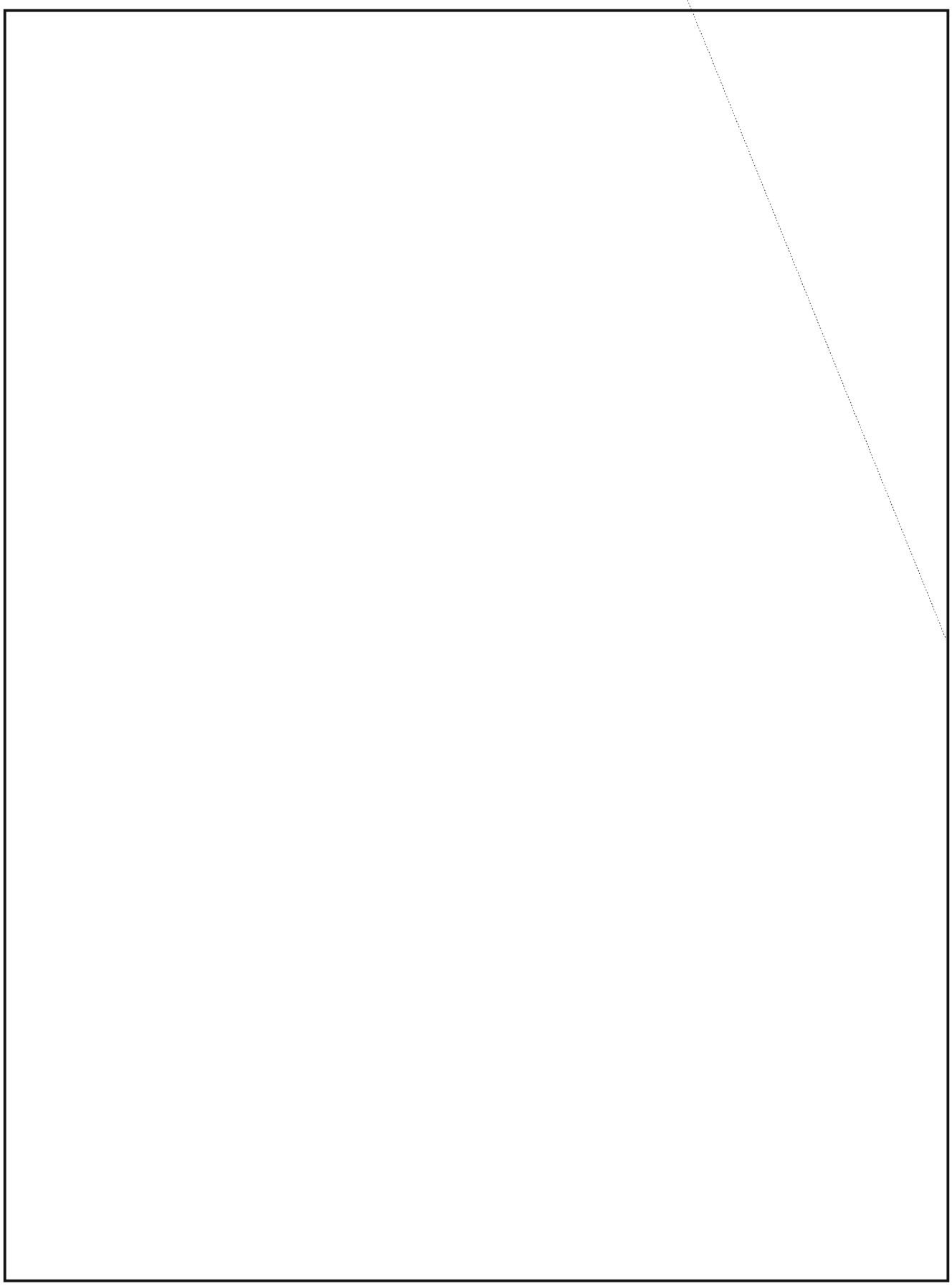
DOCID: 4009790

EO 1.4.(c)
P.L. 86-36

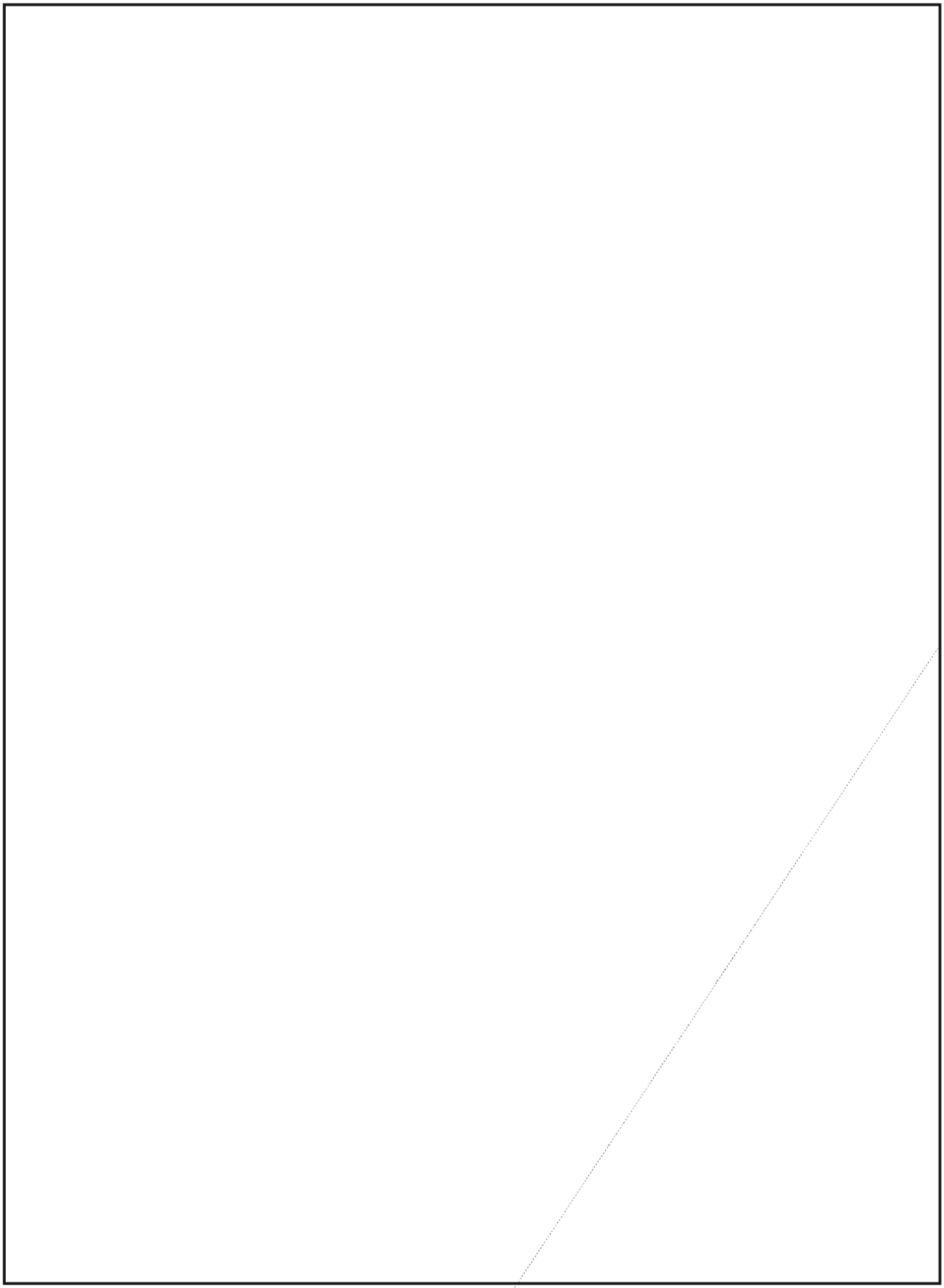


DOCID: 4009790

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36



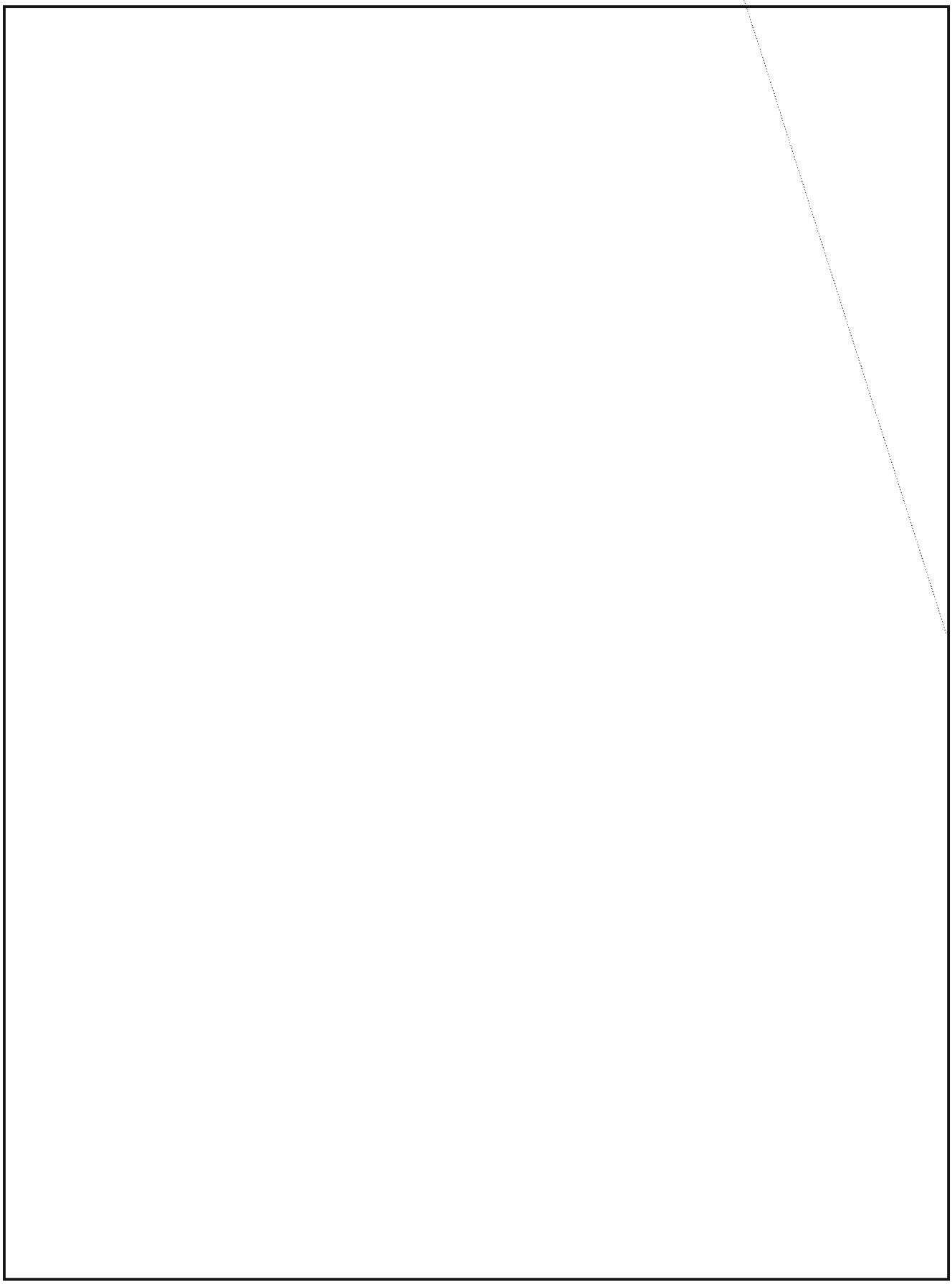
~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4009790

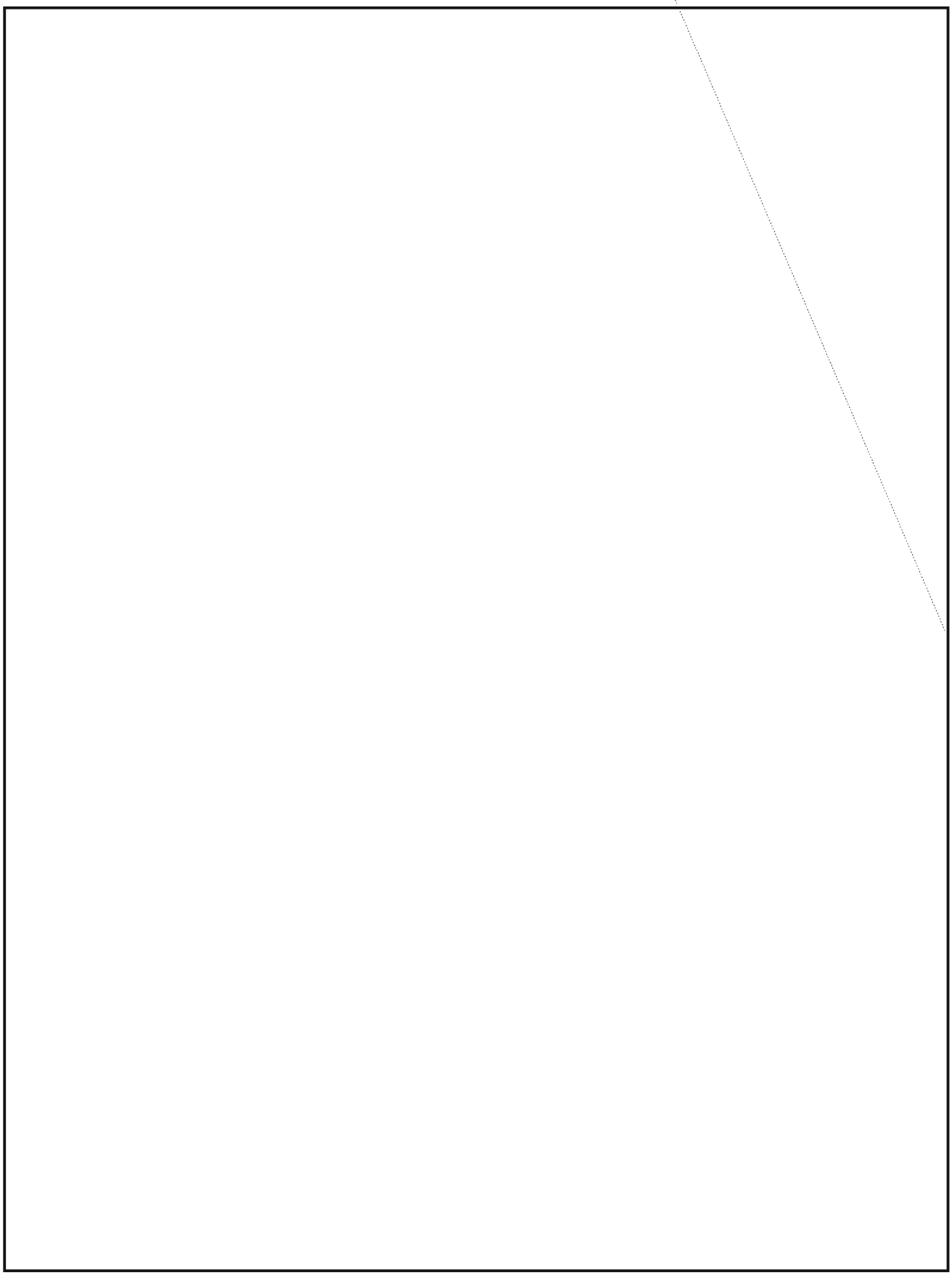
EO 1.4.(c)
P.L. 86-36



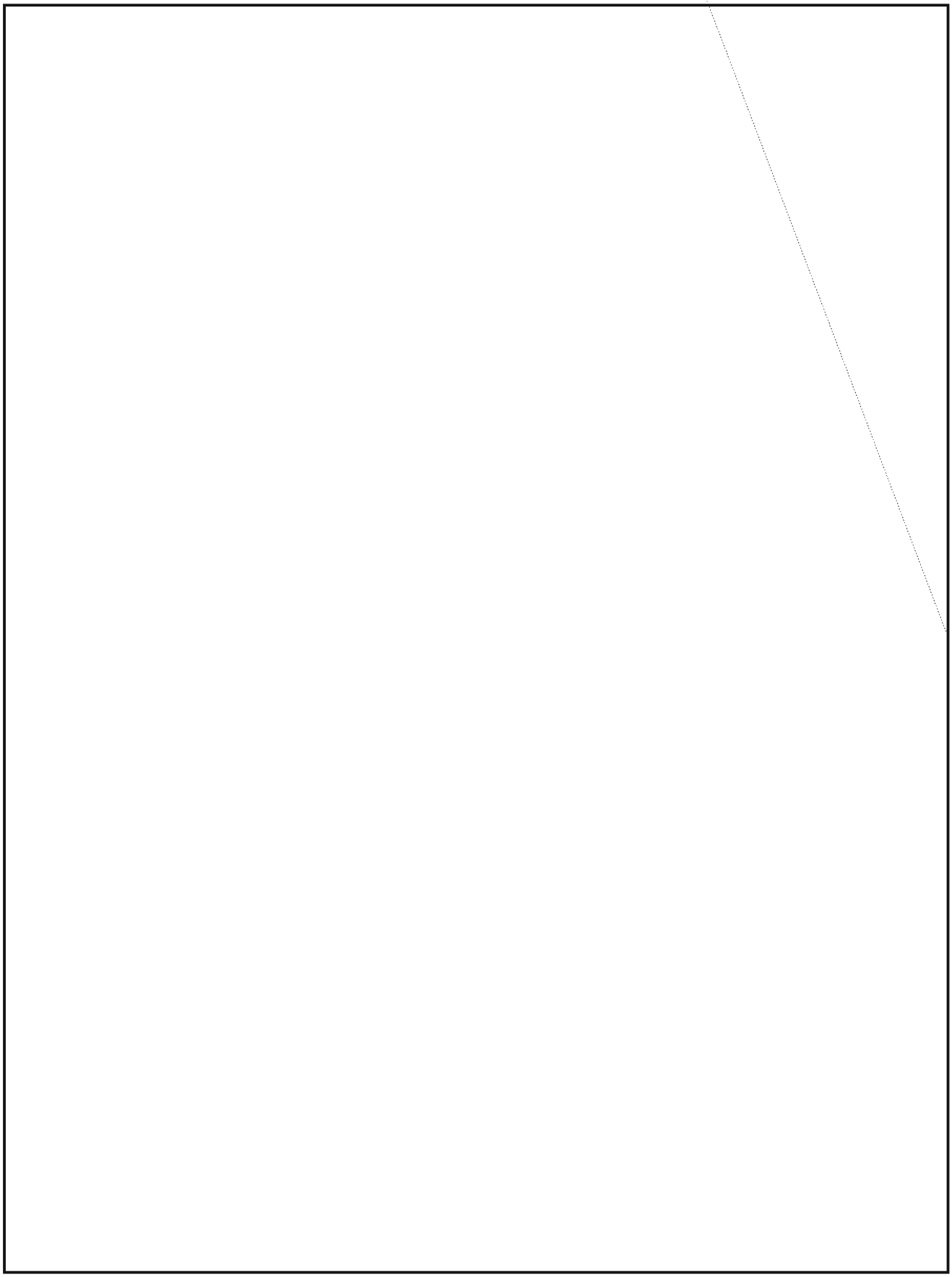
DOCID: 4009790

EO 1.4.(c)
P.L. 86-36

~~SECRET~~



~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~



DOCID: 4009790

Letters to the Editor

To the Editor, CRYPTOLOG:

The article on the Language Skill File by [redacted] (CRYPTOLOG, October 1976) made no mention of the fact that the DDO Language Advisory Committee has been working on developing an accurate inventory of the Agency's linguists for over two years. This on-again off-again effort had as its genesis the attempts by A, B, and G to have their independent accounting systems adapted for DDO-wide use.

More recently, the LAC realized that there was a critical need for an accurate inventory of Agency language skills. Accordingly, a subcommittee of LAC was formed to develop a machineable data base. [redacted] served on this subcomittee, along with a third member, [redacted] as the G member of DDO LAC. The Language Skill File was the result of the combined efforts of all the members of the LAC subcommittee, and I hope that this letter of clarification will help to give credit where it is due.

Minnie Kenny,
Chairman, DDO LAC

P.L. 86-36

~~(FOUO)~~

To the Editor, CRYPTOLOG:

In answer to "Firebrand" (CRYPTOLOG, October 1976, p. 20), yes, she is perfectly right that she has a legal right to apply for and take any job out here in Asia. And when she gets out here and finds herself unable to accomplish the duties of that job because of the Asian male attitude toward women, her supervisor also has a right -- nay, a duty -- to rate her performance on the same standards as would apply to a male employee in the same position.

[redacted]

(UNCLASSIFIED)

To the Editor, CRYPTOLOG:

Like Charles Bostick in his letter in the November 1976 CRYPTOLOG, I must be doing (or thinking) something wrong. On page 18 of the November issue, under the heading "Sensitive materials?", you say you'll go all the way to TS/CW, but "draw the line at compartmented. . ." You imply that codewords are not exclusive or sensitive. What, I ask, is COMINT CHANNELS if not a compartment? Having chief'ed the NSA SPO/SAO function a couple of years ago, I learned early, and attempted to spread the understanding of the fact that *three* compartments exist in the intelligence community. Most of us acknowledge two. Few in the cryptologic community, however, label COMINT CHANNELS as a compartment. In fact, we are so accustomed to seeing HVCCO and codewords that they are considered "garden variety" caveats; this ain't right!

[redacted]

P.L. 86-36

Editor's reply:

Sorry, but we too made the mistake of implying that COMINT material is not a compartment. As you know, it is common practice here in the Agency to speak of compartmented information as something other than COMINT. We hope that the following revised wording improves the situation, while still being suitable for our unclassified "Contributions Solicited" handout.

OLD

~~Sensitive materials?
No. We'll go all the way to Top Secret Codeword, but we have to draw the line at compartmented or otherwise exclusive sources.~~

NEW AND IMPROVED

Sensitive materials?
No. We'll print anything from unclassified to TOP SECRET CODEWORD, but we draw the line at items requiring special clearances or briefings.

~~(CONFIDENTIAL CCO)~~

(Letters to the Editor, continued on p. 21)

P.L. 86-36

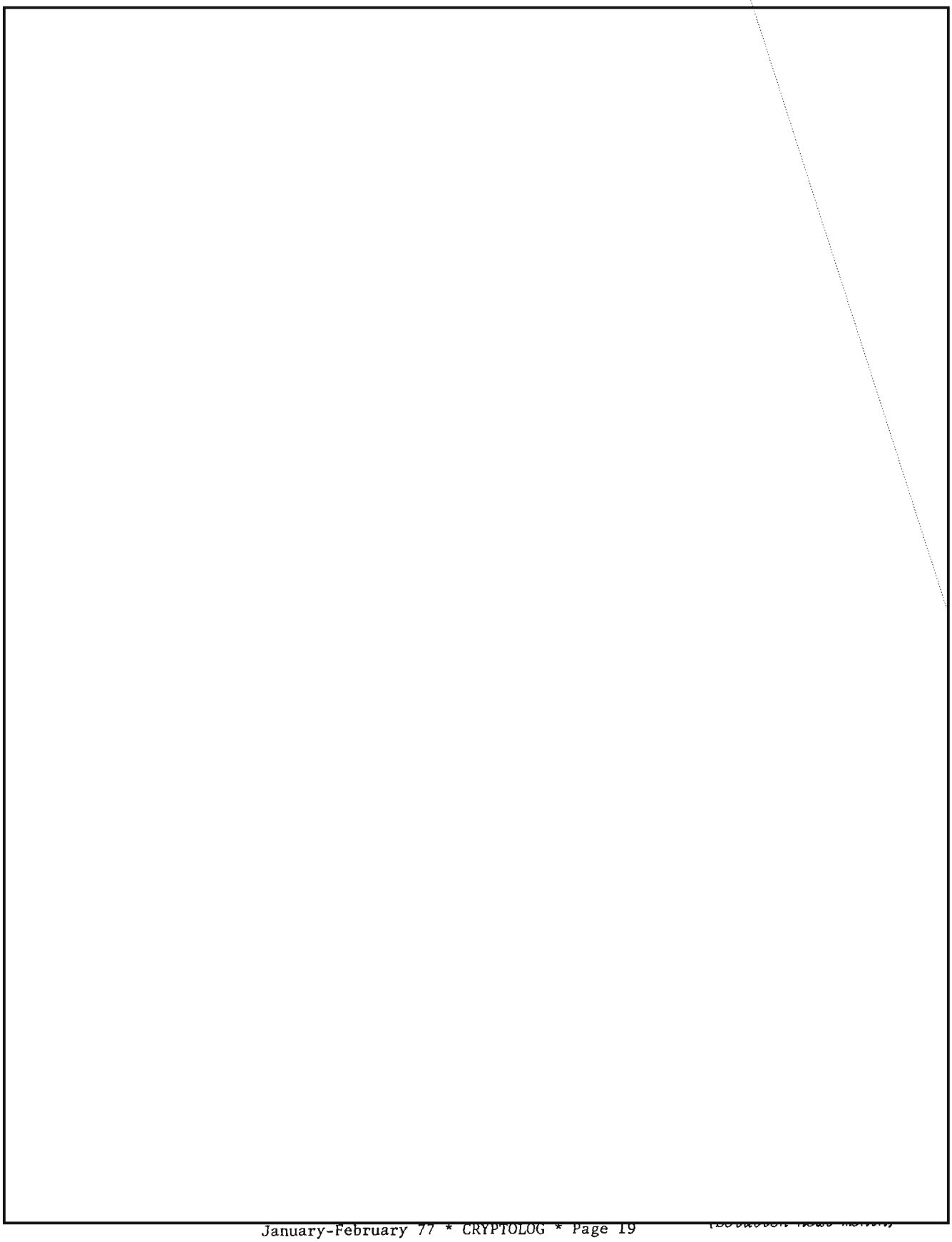
NSA-crostic No. 6

By A. J. S.

The quotation on the next page was taken from a published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DOCID: 4009790

P.L. 86-36



DOCID: 4009790

DEPARTMENT OF GOLDEN OLDIES

A MEDAL FOR HORATIVS

"Hew down the bridge, Sir Consul,
With all the speed ye may;
I, with two more to help me,
Will hold the foe in play.
In yon strait path a thousand
May well be stopped by three:
Now who will stand on either hand,
And keep the bridge with me?"

* * *

"Curse on him!" quoth false Sextus;—
"Will not the villain drown?
But for this stay, ere close of day
We should have sacked the town!"
"Heaven help him!" quoth Lars Porsena,
"And bring him safe to shore;
For such a gallant feat of arms
Was never seen before."

Rome
II Calends, April CCCXL

SUBJ: Recommendation for Senate Medal of Honor

I. Recommend Gaius HORATIUS, Captain of Foot, O-MCMXIV, for the Senate Medal of Honor.

II. Captain HORATIUS has served XVI years, all honorably.

III. On XI March, during an attack on the city by LARS PORSENA of Clusium and his Tuscan Army of ninety thousand ($\overline{XC}$) men, Captain HORATIUS, accompanied by Sergeant Spurius LARTIUS and Corporal Julius HERMINIUS, held the entire Tuscan Army at the far end of the bridge until the structure could be destroyed, thereby saving the city.

IV. Capt. HORATIUS valiantly fought and killed one Major PICUS of Clusium in individual combat.

V. The exemplary courage and outstanding leadership of Captain HORATIUS is in keeping with the highest traditions of the Roman Army.

JULIUS LUCULLUS
Commander,
II Legion of Foot

Ist Ind: AG IV Calends, April CCCXL
To : G-III

For comment.

C.G.

IId Ind: G-III
To : G-II

For comment and forwarding.

Change para III, line IV from "saving the city" to "lessened the effectiveness of the enemy attack." The Roman Army was well deployed tactically; the reserve had not been committed. The phrase as written might be construed to cast aspersions on our fine army.

Change para V, line I from "outstanding leadership" to "commendable initiative." Captain HORATIUS' command was two (II) men--only I/VI of a squad.

IIId Ind: G-II II Ides, June CCCXL
To : G-I

Omit strength of Tuscan forces in para III. This information is classified.

A report evaluated B-II states that the officer was Captain PINCUS of Tifernum. Recommend change "Major PICUS of Clusium" to "an officer of the enemy forces."

IVth Ind: G-I IX Ides January CCCXLI
To : XX JAG

Full name is Gaius Caius HORATIUS.

Change service from XVI to XV years. One (I) year in the Romulus Chapter, Cub Scouts, has been given credit for military service in error.

Vth Ind: JAG II Ides February CCCXLI
To : AG

The Porsena raid was not during wartime. The temple of Janus was closed.

The Senate Medal of Honor cannot be awarded in peacetime. Reference is invited to RAR CVII-XXV, para XXI, e.)

The action against the Porsena raid was, ipso facto, a police action.

Suggest consideration for a Soldier's Medal.

VIth INd: AG, XXX IV Calends, April CCCXLI
To : G-I

Concur in para IV, Vth Ind.

VIIth Ind: G-I I May, CCCXLI
To : AG

Soldier's Medal is given for saving lives, suggest Star of Bronze as appropriate.

VIIIth INd: AG III June CCCXLI
To : JAG

For opinion.

(Xth Ind: JAG II Calends, September CCCXLI
To : AG

XVII months have elapsed since events described in basic letter. Star of Bronze cannot be awarded after XV months have elapsed.

Officer is eligible for Papyrus Scroll with Metal Pendant.

Xth Ind: AG I October CCCXLI
To : G-I

For draft of citation for Papyrus Scroll w/metal pendant.

XIth Ind: G-I III Calends, October CCCXLI
To : G-II

Do not concur.

Our relations with Tuscany would suffer and current delicate negotiations would be jeopardized if publicity were given to Captain HORATIUS' actions at the present time.

XIIth Ind: G-II VI November CCCXLI
To : G-I

A report, rated D-IV, partially verified, states that Lars PORSENA is very sensitive about the HORATIUS affair.

XIIIth Ind: G-I X November CCCXLI
To : AG

In view of information contained in preceding XIth and XIIth Indorsements, you will prepare immediate orders for Captain Gaius C. HORATIUS to one of our overseas stations.

His attention will be directed to para. XII, RAM, which prohibits interviews or conversation with newsmen prior to arrival at final destination.

SUBJ: SURVEY, REPORT OF
To : Captain Gaius C. HORATIUS, O-MCMXIV, III Legion, V Phalanx, RAPO XIX

Your statement concerning the loss of your shield and sword in the Tiber River on XI March CCCXL has been carefully considered.

It is admitted you were briefly in action against certain unfriendly elements on that day. However, Sgt Spurius LARTIUS and Cpl Julius HERMINIUS were in the same action and did not lose any government property.

The Finance Officer has been directed to reduce your next pay by II and I/II talents, the cost of one sword, officer, and one shield, M-II.

You are enjoined and admonished to pay strict attention to conservation of government funds and property.

H. HOCUS POCUS
Lieutenant of Horse
Survey Officer

Letters (cont.)

To the Editor, CRYPTOLOG:

Those readers who have spun mathematical wheels may note that F. Mason's problem (CRYPTOLOG, October 1976) is a simple study of rotary motion.

His collection of matched pairs of poker hands produces the following six rotor sequences:

1.	J	10	7	Q	K	A			(6)
2.	.	8♦	.	7♥	.	9♦	.	2♦	(8)
3.	8♣	.	8♠	.	9♣	.			(6)
4.	9	10	2	A	K	Q	J	8	(8)
5.	A	2	J	Q	9	10	K		(7)
6.	Q	K	10	J	A				(5)

The two sequences defining the second position must be aligned so as to produce only one valid value per step. Each sequence moves one step per cup.

It follows that, if the (J, 8, 9, A, Q) hand occupies position Ø, the hand with 4 aces must occupy position N, where $N \equiv 5 \bmod 6 \equiv 3 \bmod 8 \equiv 0 \bmod 7 \equiv 4 \bmod 5$.

The solution is $N = 539 + 840k$, k being an arbitrary integer, by the Chinese remainder process. (See, for example, *Topics from the Theory of Numbers*, by Emil Gosswald, Macmillan, 1966).

[redacted] P12 P.L. 86-36

(UNCLASSIFIED)

'Doublespeak' Award Evokes Greater Effort

Associated Press

The State Department is not taking its "doublespeak" award sitting down.

The department received the dubious honor last week from the Committee on Public Doublespeak of the National Council of Teachers of English.

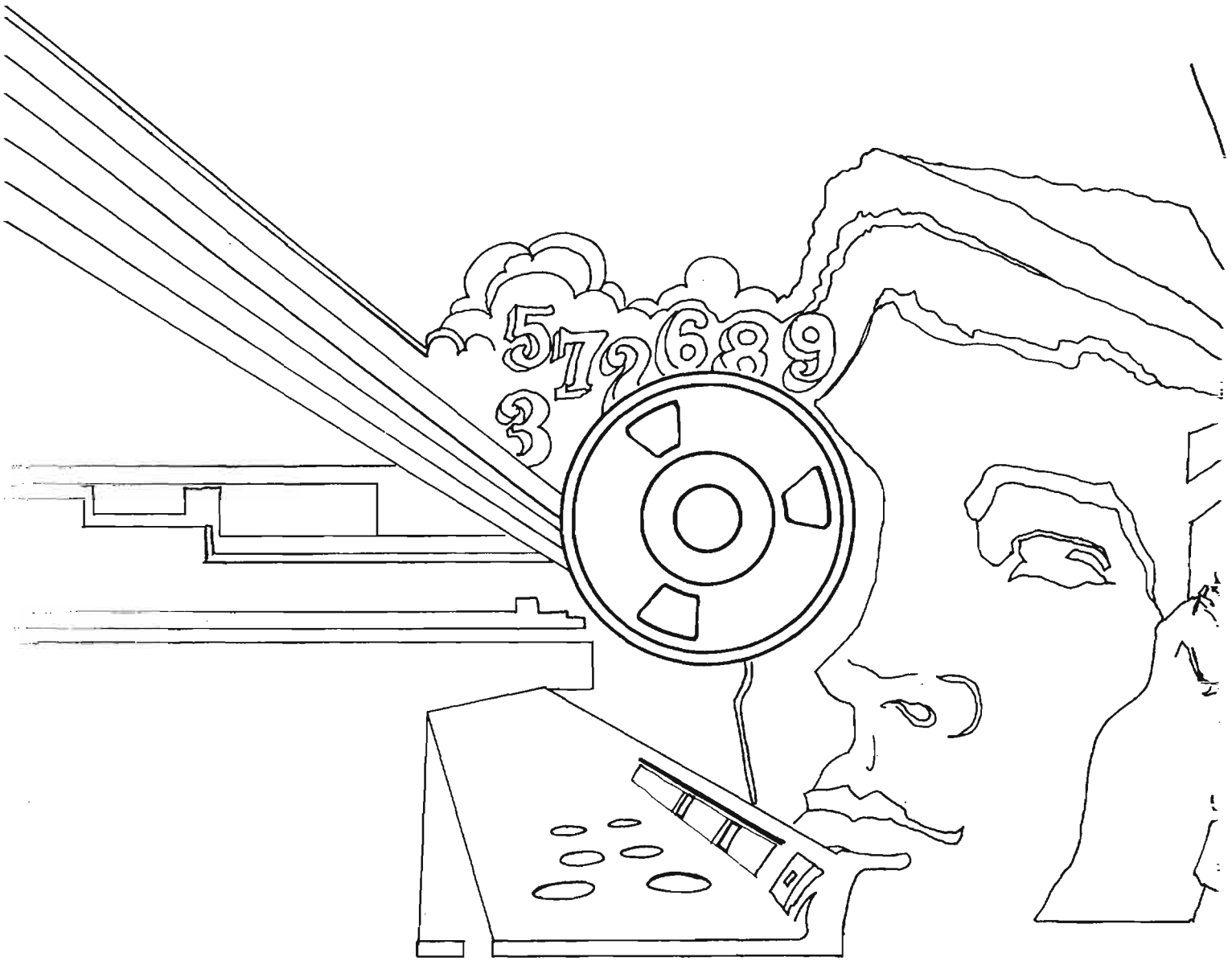
The award cited an announcement from Foggy Bottom that a consumer affairs coordinator would "review existing mechanisms of consumer input, thruput and output, and seek ways of improving these linkages via the consumer communication channel."

Lawrence S. Eagleburger, a top aide to Secretary of State Henry A. Kissinger responded Wednesday:

"I think it's an enormous compliment since it demonstrates remarkable recognition of my ability since I was largely responsible for the original document in recognizing the ability of my office to handle input, output and thruput with remarkable facility recognizing the normal inability of the bureaucracy to do anything in a manner which would merit an award for anything."

The Washington Post, 26 November 76

P1-Dec 76-S3-25039


5726893

DOCID: 4009781

P.L. 86-36

~~TOP SECRET~~

[redacted]

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

DECEMBER 1976

HANDLE VIA COMINT CHANNELS ONLY

P.L. 86-36

A CRYPTOLOG INTERVIEW WITH..... [redacted] 1
THE FRENCH (FRIED) CONNECTION..... [redacted] 6
WHY CAN'T THEY DESIGN A GOOD S.R. TEST?....Kathy Bjorklund.....7
NON-NAMES IN THE NEWS (COOPERPERSON).....8
APOLLO-SOYUZ: BEHIND-THE-SCENES ACTIVITY.... [redacted] 9
LET'S GIVE LINGUISTS A BIGGER PIECE OF PIE! ... [redacted] 13
WHAT'S IN A NAME?..... [redacted] 15
GEOGRAPHIC NAMES..... [redacted] 16
LETTER TO THE EDITOR.....21

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009781

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. III, No. 12 DECEMBER 1976

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

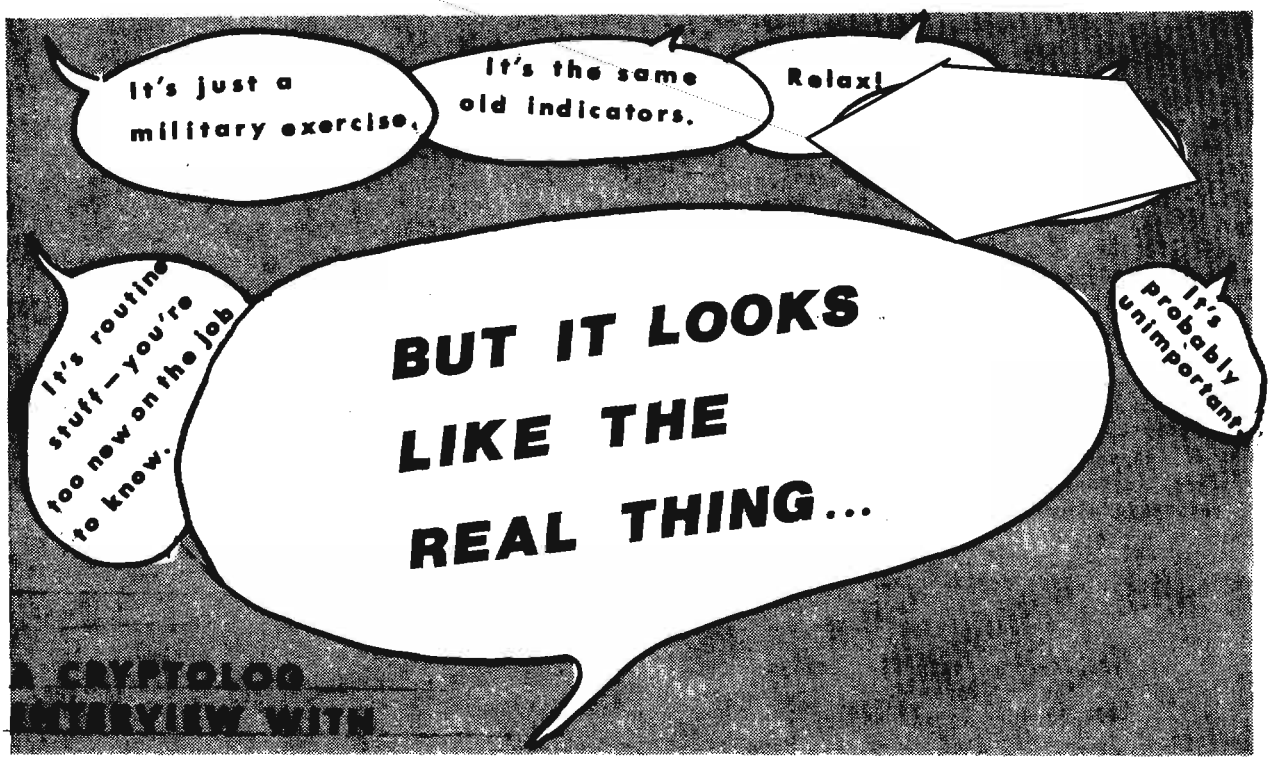
Editor in Chief..... Arthur J. Salemme (5642s)
Collection..... [redacted] (8955s)
Cryptanalysis..... [redacted] (8025s)
Language..... Emery W. Tetrault (5236s)
Machine Support..... [redacted] (3321s)
Mathematics..... Reed Dawson (3957s)
Special Research..... Vera R. Filby (7119s)
Traffic Analysis..... Frederic O. Mason, Jr. (4142s)
Production Manager..... Harry Goff (4998s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

~~TOP SECRET UMBRA~~



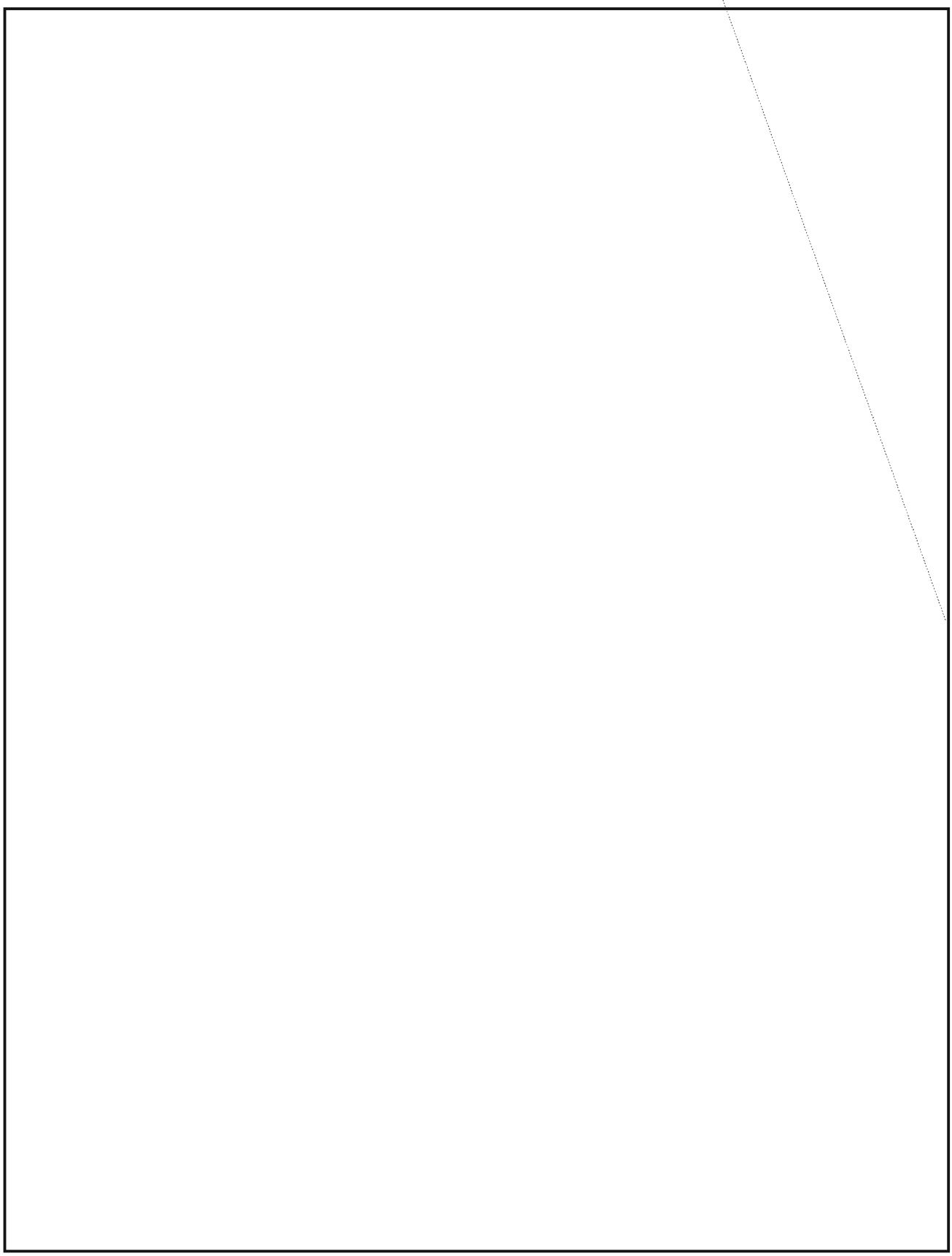
[redacted] ESS P.L. 86-36

[redacted]

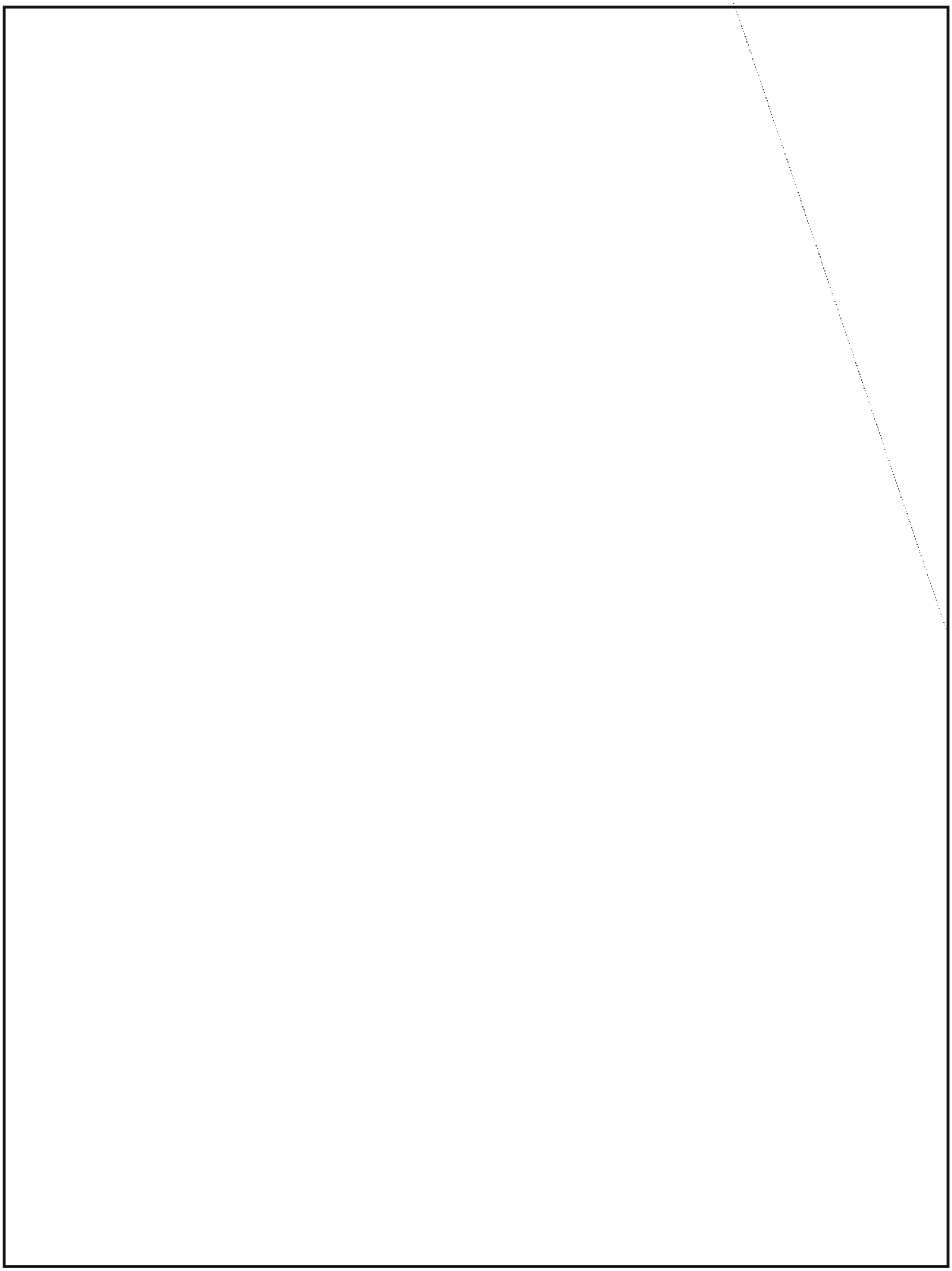
EO 1.4.(c)
P.L. 86-36

~~TOP SECRET UMBRA~~

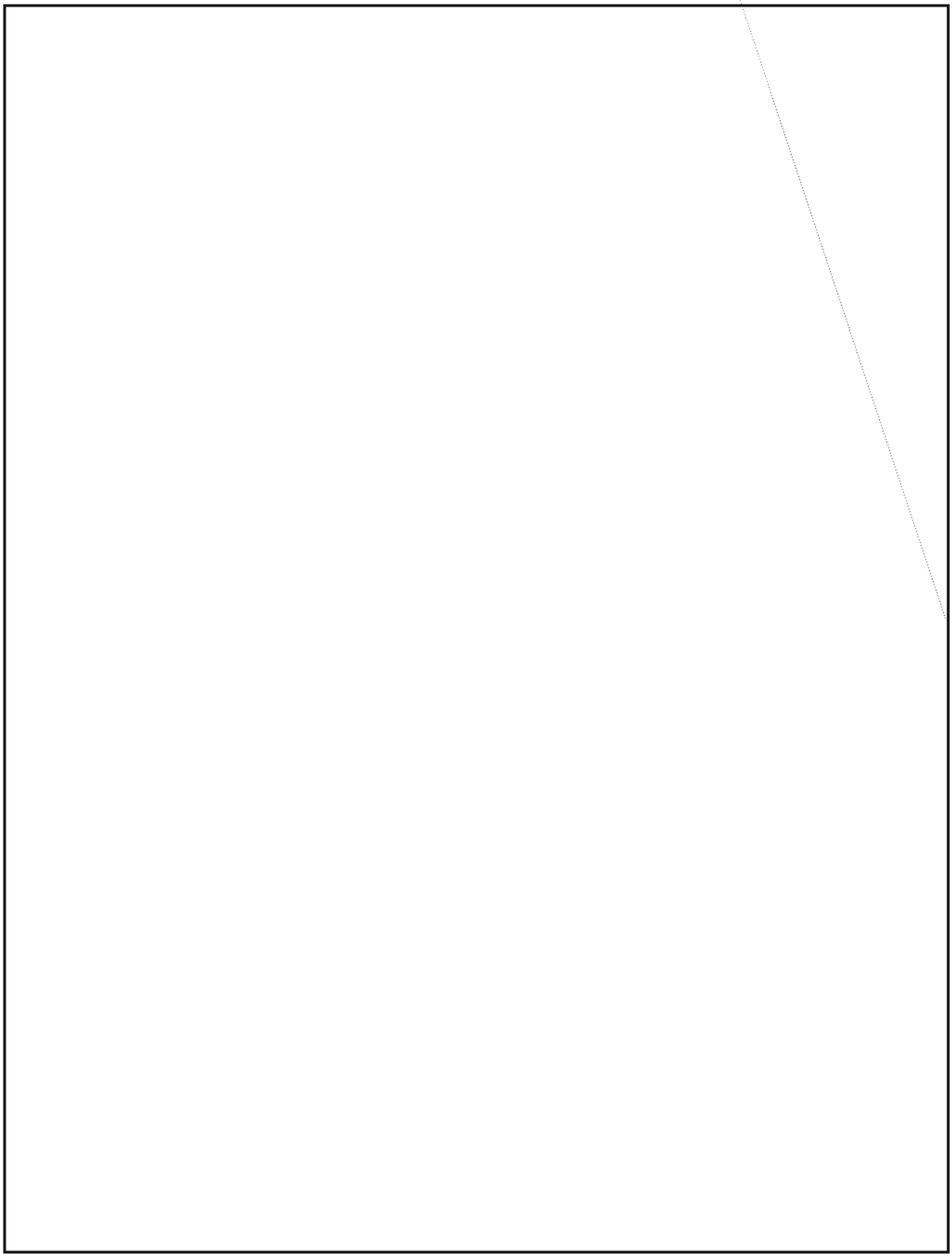
EO 1.4.(c)
P.L. 86-36

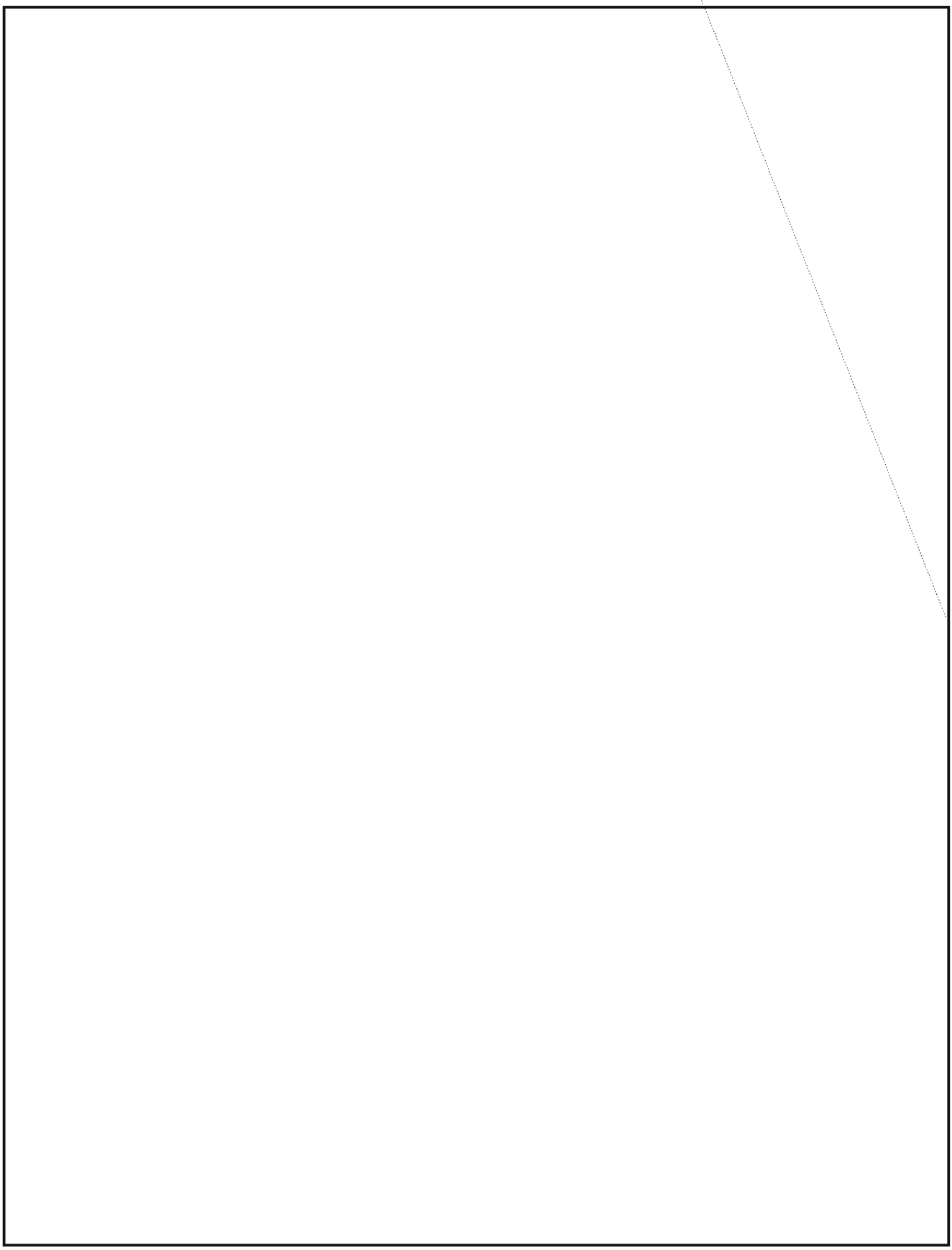


EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36





DOCID: 4009781

P.L. 86-36

The French (fried) Connection

Gino the Genie aka P1/A542

Much of our work in the intelligence community is, of necessity, denied current widespread reporting. It thus may be months, years, or even decades before cryptanalysts at large learn of some of our most exciting efforts. However, a current operation is beginning, on which we are fortunate to be able to report. It is hoped that, by sharing these first efforts, we will enable Agency analysts to read between the lines of regular news reporting and infer our (expected) successes.

This juicy problem began a few years ago when Gino's restaurants began an advertising campaign stressing "freedom of choice." It is well known that this is a code phrase for many right-wing, extremist organizations, and the fact did not escape the attention of high-level management.

Wanting to get to the meat of the problem, operatives began a careful surveillance of selected restaurants. Then, several months ago, a crucial observation was made -- *Gino the Genie Magic Kits* were being sold at most local units. Upon purchase, it was discovered that each kit contained a *message decoder card!!!* (see Fig. 1).

A little careful backgrounding quickly showed that Gino's restaurants are owned by *A & G* Foods of King of Prussia, Penna. The obvious connection with *A.G.* Crypto of Zurich was immediately made, and the operation entered its second and more intensive phase.

At the risk of putting an agent in a pickle, it was determined that someone must infiltrate the organization. After carefully laying the groundwork, we were able to place an operative at the highest level of the organization. (See Fig. 2, black rectangle "to protect his identity").

We are now in the third phase of the project -- analyzing data and awaiting further intelligence from our informant. The meat and (french-fried) potatoes problem of understanding the intricate grill system has been turned over to a special team of P1 cryptomathematicians.

However, the major burden rests with our intrepid interloper -- to discover the big cheese behind the entire scheme. Barring some jam-up of data, we hope to issue future reports on this topical subject.

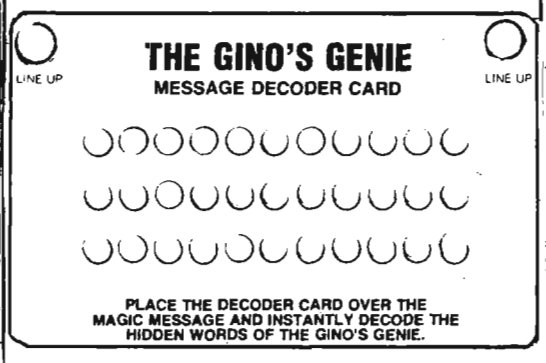


Fig. 1

Fig. 2

DOCID: 4009781

WHY CAN'T THEY DESIGN A GOOD S.R. TEST?

Kathy Bjorklund, G633

Several recently published articles on the testing process for professionalization have prompted me to share my limited experience in that process in the Special Research (SR) field.

In my brief exposure to education and testing methods during my undergraduate days, I learned that the stress must always be placed upon goals or purposes. The goal must be defined ahead of time and, once defined, must be kept in mind firmly and constantly. The principle is obvious: if a person is studying plane geometry, he should not be tested on his abilities in solid geometry or trigonometry. If he is being taught certain theorems that apply to the circle, he should be tested specifically on those theorems -- and not as they apply to the rectangle, but to the circle.

The idea that the testing of an aspirant in a professional field at NSA should follow the same principle seems clear enough. The aspirant should learn certain techniques in his field, should learn how to apply them, and should then be tested specifically on those abilities. Simple, isn't it? Not the rectangle, but the circle! Stick to the goal!

That is all very well for Academia, where the simplistic can be achieved, although it is often couched in such ethereal terms that one outside the hallowed halls could not recognize it as such. But can it be achieved in the workaday intelligence world? A glance through the appropriate chapter of the Personnel Management Manual (Chapter 402.2, in case you want to read it yourself) would have us believe that it can.

This is how it's done. A panel of professionals in the field is selected. They draw up the professionalization/criteria requirements within the field, with the approval of M3. Under this aegis falls any Professional Qualification Examination (PQE), which, in the SR field, has traditionally been a joint project carried out by a panel subcommittee and the appropriate staff from the National Cryptologic School. It still looks easy, doesn't it?

A sketchy review of the history of establishing the criteria for the SR field quickly demonstrates that this proved to be a ticklish job and that this field (which is one of the major categories at NSA, together with CA, TA, and Data Systems) was the last to publish its standards -- in 1970. Then there followed a period of 2½ years during which the only testing done was in the form of an interview of the aspirant by a group of professionals. This was found to be too subjective. Hence the era of the "objective test" dawned in June 1973. At that point, the problem seems to have become clouded exponentially beyond belief. For when objective methods began to be applied to a highly subjective field, logic failed. The designers of the various tests tried to examine groups of aspirants for their knowledge of the circle, but found that the aspirants, despite a careful culling that was done by evaluating the Professional Qualification Records (PQRs), were equipped to deal with the rectangle, the square, or even the parallelogram -- anything *but* the circle.

The next step was to try to break down the testing method, further diluting it. The aspirants would be given a chance to be tested on the general principles and the theorems in Part I, and on the application of those principles in Part II. This may be a solution in geometry, but there is a good deal of controversy over whether or not this gauges the ability of a professional SRA. For, with the process thus subdivided, the applicant no longer had to demonstrate his ability in an overall manner. This, too, is a highly subjective area, since in many parts of the Agency the SRA's job has been broken down into several parts, which are not always handled by a single analyst. Although this is an outgrowth issue of the general testing problem, it too merits consideration for there has been -- like it or not, by choice or by chance -- a use of the SRA title as a coverall. Many individuals hold the title (and some even the certification) but have never written a report or do not *exactly* fit the definition of an SRA, which states that the primary duties of the SRA should include "intelligence research and analysis and the preparation and presentation of written and/or oral reports, drawing, in both cases, from a thorough knowledge of user requirements" (page 1, paragraph B of certification criteria, as published by M3, 10 November 1972). The test was trying to gauge ability to do the job as defined. What may have been overlooked was that many jobs did not conform to the definition. Perhaps by attempting to serve the many, the procedure failed to single out the few who were qualified. Was this, or should it be, the goal? If so, is that goal being met? Perhaps not.

Let's leave the world of circles and parallelograms and get back to the business at hand -- the SIGINT business. A Special Research professional by anyone's standards -- and there are thousands -- should be able to communicate in general, and should be able to communicate an intelligence fact in particular -- that's what we're all about. In order to do that, however, the professional must be able to recognize the fact as something that is useable, no matter the vehicle or purpose. The SRA should also have a background in a specific operational area and, most important, must have a clear idea of how that fact came to his desk in the first place. If the SRA is to able to make a value judgment (and he must indeed make them every day), anything less is unacceptable. Granted,

this is a gray area, but "a clear idea" can be somewhat defined:

[redacted]

Leaving aside the question of how much depth the professional has to have, experience has taught many SRAs (in Production, at least) that a good TA background is a must. (Some would go so far as to say that the SRA and TA fields are almost synonymous.) An understanding of the collection and forwarding process is more tangentially related, but if an SRA is ever asked to explain why a report is 72 hours old, a fair explanation based on this sort of background can give the reader a lot more faith in the SIGINT facts.

[redacted]

This is the type of question that it seems the professionalization test should try to answer as a whole, instead of as the sum of its parts. No one who has ever been in the position literally of "translating into English" the flowery phrases of a would-be writer, or trying to tell an "outsider" what the "SIGINT-ese" really says, would agree that a good writer or a good technician can be found all rolled up in one SRA. However, the whole or complete SRA should have a foot in both worlds, but should not be so overconcerned either with his prose style or with the technicalities that he forgets a basic principle: his art is a disciplined one that requires him to *comprehend* fully the technical aspects of his job, and then to *communicate* that knowledge to his readers in a clear, unambiguous way. The test given to an SRA must gauge his ability to carry out that dual job.

At present there is a multiple standard. A few aspirants still qualify under the pre-1973 criteria, which require no test; subject to an oral interview are several others who, if they fail, must take the test; and, finally, the majority, who fall under the criteria that require a test. Because of the foibles of the overall professionalization system, these discrepancies cannot be removed. *But* the last-named group is still being tested, as it were, one foot at a time. They are given a problem and are told to write a report to meet certain customer requirements. The result of their work is graded twice -- once for the technical accuracy and once for composition. An aspirant can pass either part and not be required to take it again. Thus it is possible for someone to emphasize the technical portion of the exam, pass it, and fail the composition portion. The same individual, having passed Part I -- the analysis -- could, the next time, write a great composition on "summer camp experiences," thus passing Part II and becoming, voilà, an SR professional. The possibility that this can happen should be removed, however remote its statistical chances.

EO 1.4.(c)
PL 86-36

(Continued on p. 12)

NON-NAMES IN THE NEWS

A Judge Rules '-person' Is Non Grata

Ellen Donna Cooperman went to court the other day in an effort to change her name to Cooperperson. She lost.

A State Supreme Court justice ruled that if he granted this request "it would have serious repercussions perhaps throughout the entire country."

In a decision citing a battery of possible name changes, Justice John F. Scileppi in Suffolk County pointed out, for example, that if this request was granted, someone named Jackson would change the name to Jackchild. A person called Manning would want the name to be Peopling. A woman named Carmen would insist on being called Carperson.

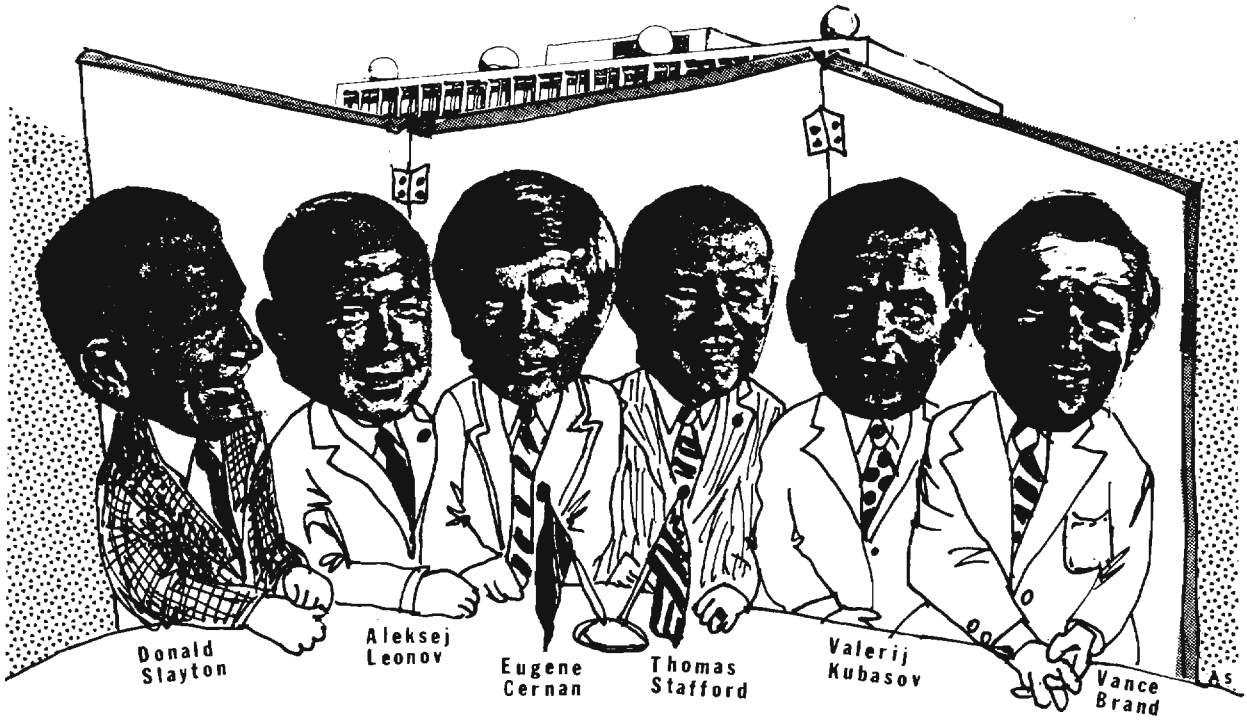
"The possibilities are virtually endless and increasingly inane," wrote Justice Scileppi. "This would truly be in the realm of nonsense."

Name changes are usually routine. Names are changed by the filing of petitions in either Civil Court or State Supreme Court. Applicants must swear that they do not mean to defraud anyone and that the change does not have any other illegal motive. They must also include a birth certificate and a statement of why the request is being made.

Mrs. Cooperman, who lives in Babylon, L.I., and owns a feminist film company, gave as her reason that "she believes deeply in the feminist cause" and that the name Cooperperson "more properly reflects her sense of human equality than does the name Cooperman."

(New York Times, 17 October 1976*)*

DOCID: 4009781



APOLLO-SOYUZ TEST PROJECT: BEHIND-THE-SCENES ACTIVITY

The following article, reprinted from FIELD INFORMATION LETTER 9-76, September 1976, was written by [redacted] *of DEFSMAC (Defense Special Missile and Astronautics Center), a joint NSA-DIA activity:*

[redacted]

DEFSMAC

P.L. 86-36

The Apollo-Soyuz Test Project (ASTP) -- or Soyuz-Apollo Test Flight (SATF) if your vantage point in July 1975 happened to be Moscow -- was probably the high water mark of detente. However, the flight was also remarkable in several other less publicized aspects. First, the fact that the joint mission was ever agreed to was in itself a contradiction to past Soviet policy. The long history of Soviet reticence in discussing any details of their space programs with outsiders would have made such a joint project impossible under any other political climate. Secondly, the project's raison d'etre -- development of an international space rescue system -- became pointless even before the mission was flown. Finally, the much publicized aura of cooperation and mutual trust surrounding ASTP was clouded by NASA's uneasiness concerning the Soviets' candor and basic technical capabilities.

[redacted]

Selection of U.S. and Soviet Hardware

The evolution of the ASTP mission profile was also unusual. Initially, it was proposed that the joint flight should involve either a Soviet *Soyuz* crew visit to our Skylab or an Apollo flight crew visit to a Soviet *Salyut* space station. The U.S. Skylab visit was impractical because by 1972, when the joint flight began to be seriously discussed, that mission was too close to launch, and hardware modifications required for a joint mission would have imposed unacceptable delays on the program.

An Apollo visit to a *Salyut* was also discussed, and some Soviet technicians even professed knowledge of a future *Salyut* configuration that would feature multiple docking ports.

E.O. 1.4.(c) P.L. 86-36

DOCID: 4009781

This tack in the negotiations terminated abruptly, however, before it got very serious. We feel it was because the *Salyut* variant of which these technicians had some knowledge was actually the military version, such as the currently orbiting *Salyut*-5. It is readily understandable that a U.S. crew visit to such a station would be unacceptable to the Soviets. The civilian version of *Salyut* carries only a single docking port and would have required a prohibitively extensive modification to accommodate another docked spaceship.

Thus, because of constraints imposed by time, hardware, and military sensitivity, it was agreed that the most practical mission to fly would be one involving only an Apollo and a *Soyuz*.

Soviets' Motivation for Participation

It is no secret that the Soviets have been something less than fully candid on matters concerning their plans and progress in most areas of manned space flight. To deny years of secrecy and obfuscation in order to join openly with the United States in a joint manned mission was undoubtedly the subject of many a heated debate within the Kremlin hierarchy. The early era of detente, however, provided fertile soil in which the seeds of ASTP could germinate. What better way to demonstrate Soviet goodwill than to open the gates of Bajkonur to their U.S. counterparts.

I submit, though, that the Soviets' motivation for participation in the project was grounded on a more basic and politically opportunistic objective.

Laying aside the political motivations, the overt objective behind the joint mission was the development of a common space docking system to enable future astronauts and cosmonauts to visit each other's spaceship both as joint experimenters and, if necessary, emergency rescue teams.

"To develop and test systems for rendezvous and docking of future manned spacecraft and stations that would be suitable for use as a standard international system" -- that was the stated primary objective of the project. Throughout the ASTP preparations, however, the Soviets steadfastly refused to discuss any forthcoming flights where it might be possible to accommodate a docking by a U.S. spaceship. Consequently, the United States dropped its plans to carry the common docking system aboard the Shuttle. It was needless extra weight on a spacecraft already near its maximum payload capacity.

Still the Soviet commitment to ensure the mission's success was impressive. Fifteen months before the scheduled joint flight, they began the first of two unmanned flights of *Soyuz* craft modified specifically for ASTP. Although the flights appeared to encounter no problems, it was not until near the end of 1974 that the Soviets told their American counterparts at NASA that *Kosmos*-638 and 672 were indeed ASTP precursors. These were the first two of six complete *Soyuz* systems the Soviets were to commit to the program.

Soviet Full-Dress Rehearsal

The two unmanned *Kosmos* flights were followed in December 1974 by the six-day *Soyuz*-16 flight, a full-dress rehearsal for the joint flight scheduled seven months later. Major Vladimir Dzhanibekov, an eager and highly skilled cosmonaut trainee and the commander of the second backup crew assigned to ASTP (there were four crews in all), fully expected to make that flight. For reasons unknown, however, the Soviets chose instead to send up the experienced crew of Colonel Anatolij Filipchenko (commander of *Soyuz*-7) and Nikolaj Rukavishnikov (test engineer of *Soyuz*-10). These two veteran cosmonauts had already been designated the first backup crew behind General-Major Aleksej Leonov and Valerij Kubasov.

Their rehearsal of the Soviet part of ASTP was nearly flawless, but in deciding to bring back some souvenirs from the flight -- hardware which was to have been jettisoned just prior to re-entry -- the *Soyuz*-16 crew made an almost fatal error. The extra weight in the descent module offset the center of gravity to such an extent that the spacecraft's re-entry control systems had difficulty coping with the problem. Extreme buffeting was the result as the craft wobbled into the atmosphere prior to landing. Because of this rookie-like stunt, Filipchenko and Rukavishnikov were visibly out of favor with their Chief of Cosmonaut Training, General-Major Vladimir Shatalov, during a joint crew training session which followed shortly afterwards in Houston.

Should the *Soyuz*-16 spacecraft not have checked out satisfactorily, the Soviets had yet another precursor ready to repeat the mission. It was never flown and Dzhanibekov's last chance to fly an ASTP-related flight evaporated[1].

The final two *Soyuz* systems in the group of six that had been built specifically for ASTP were the prime and backup craft that were each on their respective launch pads at Tyuratam on 15 July.

In contrast, the United States had one booster and one spacecraft available for ASTP -- surplus hardware from the curtailed Apollo lunar program.

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Achieved and Future Goals

ASTP successfully met all its stated objectives. But what of the unstated ones?

The real Soviet objectives in ASTP were twofold, I believe. The first was technological which, although important, was definitely of

DOCID: 4009781

lesser significance. The prime Soviet motivation for their participation in ASTP was political. The serious and embarrassing setbacks the Soviet Union had suffered during the late 1960s and early 1970s had destroyed their image as the world's leader in cosmonautics. The Apollo program delivered the coup de grace. ASTP was a cheap and spectacular way to return to parity with the United States. At least the Soviets hoped the rest of the world would interpret it that way. The moment the two craft touched on 17 July 1975, the Soviet Union was again technologically equal to the United States. The Soviets played up the mission that way and we did little to dispel the impression.

The current *Salyut*-5 space station crews will undoubtedly set endurance records which will stand for at least a decade. And what lies around the corner beyond *Salyut*? The Soviets view manned space flight not only as a spectacular advertisement for their technological prowess, but also as an integral facet of their overall military space systems development. What role or roles do they envisage for the military man in space? What is he doing there now? These are questions of signal importance to the United States and ones which we must continue trying to answer.

~~(SECRET SPOKE)~~

SOLUTION TO LAST MONTH'S TEXTA "WORD-SEEK" by [redacted] *A754*

[redacted]

~~(SECRET — CCO)~~

GOOD S.R. TEST

(Continued from p. 8)

The reasons for addressing the testing problem are many, but they can affect the work force as a whole and the truly professional SRA in particular. First, if the criteria were uniformly applied, the certification of professionalization would be more meaningful to the individual. Secondly, it would let the manager know that the SRA professional working for him is not supposed to be a Shakespeare or a Newton, but an analyst who is fully qualified to do his assigned job of SIGINT reporting. Third, it might weed out those who, by chance or design, are attempting to qualify in an area in which they do not belong. And that third point brings us to the fourth and final one: it might make those responsible for the system more responsive to the actual job requirements, thus creating new career fields for attracting those who "aren't really SRAs but don't fit anywhere else."

The last point "closes the circle" by reminding the designers of the professionalization system, as well as its current administrators, that in order to test an individual it is necessary to have a clearly defined goal. In this instance the definition of that goal -- the definition of what an SRA "really is" -- should be based on what an SRA "actually does." Having the test consist of writing a report is a good start, but let's not allow complacency to set in. The present method can be improved. Moreover, the field itself can be refined, for example, by reconsidering which experience factors should be covered in the PQR. SRAs from other parts of the Agency, particularly those outside of Production, might be able to describe the functions they perform, thus widening the scope of the test or giving management sufficient cause to review the field title itself and narrow it. Whatever the outcome, if these matters are considered thoughtfully, the actions that might ensue will surely improve the caliber of the SRA professional and the quality of the intelligence produced by the Agency.

P.L. 86-36

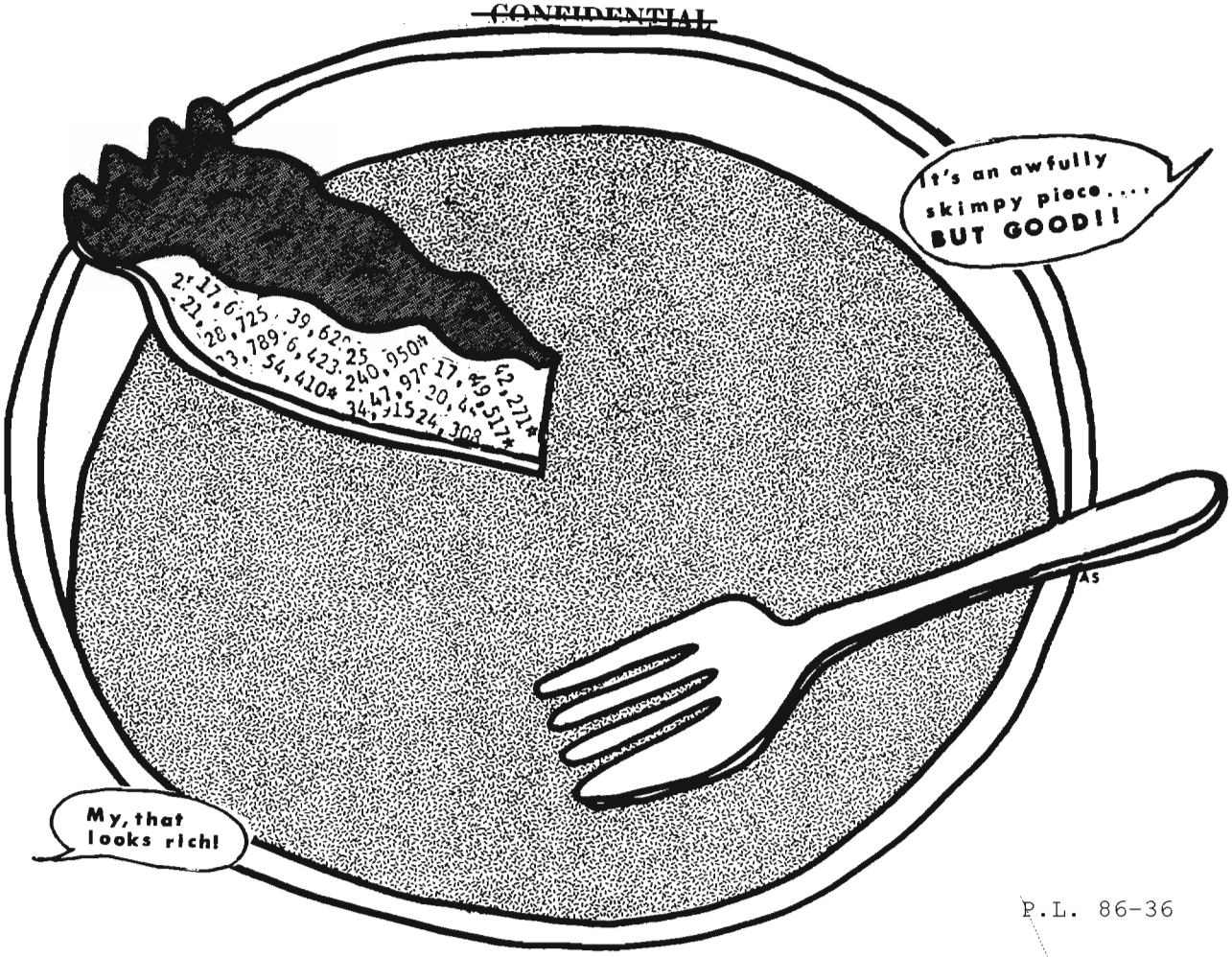
EO 1.4.(c)
P.L. 86-36

A few days before this issue of CRYPTOLOG was submitted to the printer, Ms. Bjorklund informed the editor that the SR Panel, in response to comments and recommendations that she and others had submitted to it, had scheduled a special meeting in October. At that meeting the SR Panel (1) canceled the examination that had been scheduled for November, and (2) resolved to devise a new examination as quickly as possible, and then reschedule it.

Ed.

~~(CONFIDENTIAL — CCO)~~

DOCID: 4009781



P.L. 86-36

LET'S GIVE LINGUISTS A BIGGER PIECE OF THE PIE!

[redacted] **G5**

At the very heart of COMINT exploitation rests the matter of language -- or, rather, foreign languages, since our targets carry on their [redacted] affairs in their own languages. [redacted] To do these things, the Agency must have trained language personnel.

Training for many, if not most, Agency tasks is a fairly short-time effort. The same does not hold for language tasks. For problems on which I have worked in the past, the desired recruit has an MA and has lived at least one year in a foreign country in which the foreign language was the means of communication in a foreign socioeconomic culture. But what does an MA imply? For the commonly taught languages that means:

- 3 or 4 years of the language in high school (for my generation it normally meant 4 years of Latin and 3 years of a modern language);
- 4 academic years in college; and
- one or two years of postgraduate language studies.

EO 1.4.(c)
P.L. 86-36

For the more exotic languages, not normally taught in high schools, the MA means college and postgraduate studies. [redacted]

DOCID: 4009781

EO 1.4.(c)
P.L. 86-36

~~CONFIDENTIAL~~

he has to master a lot about intelligence, current affairs, the military, shipping, trade, etc., that was not covered in literature and linguistics courses and that involves specialized vocabularies.

Unfortunately, most of our recruits do not have an MA background in language on which to build. Moreover, many recruits have to be taught a new language for Agency targets and will therefore require years before becoming proficient. A rule of thumb in A Group is that it takes some 3 years before a new hire is worthy of the entering pay and is carrying his or her weight. Attaining the minimal level of professionalization -- as attested by NSA's language professionalization process -- takes about 3 years. Attaining journeyman proficiency (and this is as far as many language personnel ever progress) usually takes about 8 years of varied on-the-job experience. True language and target professionalism comes, if ever, some time after the tenth year. And those who reach that level keep on improving with age and experience.

Language is a hard and demanding taskmaster and people who are really competent in language exploitation should be rewarded for their years of industrious application. Unfortunately, many a good person in language -- often before reaching journeyman status -- switches to low-level management or to other fields in which promotions seem to come more rapidly. That switching could be eliminated if status and pay were awarded for technical competence in language processing.

Let's take a look at the NSA language field from the point of view of status and pay. According to the December 1975 issue of *The Quarterly Management Review*, our authorized civilian work force strength was 7762, with 7066 on board; the authorized civilian work force for language was 1007, with 918 assigned; and the authorized strength for professionalized language personnel is 715, with only 381 of those billets filled by professionals (the billets are not necessarily vacant -- they may be filled by individuals who are not yet professionalized). In other words, 12.9 percent of the authorized work force are language personnel. (These statistics, as language people well know, are not valid -- some language personnel, by choice or fiat, went under cover as SRs when the language field became professionalized 5 years earlier than the SR field!)

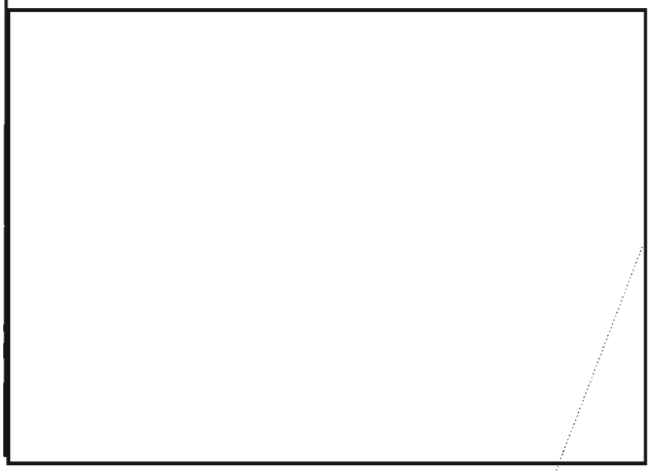
Professionalization level is at about the GG-9 level for new personnel (of course, we have GG-11s and GG-12s in language slots who reached those grades prior to the introduction of professionalism or through waivers or other methods). Therefore, since we have 715 authorized slots for professionalized language personnel, but only 381 of them are filled by professionals, we have 344 nonprofessionals in professional billets. And since we have 918 language personnel *in toto* in assigned slots, then 537 of our language personnel are not professionals. What this boils down to is the fact that the 381 professionals should be distributed in GG-9 through GG-18 (yes, GG-18, since the career ladder for the 1200 field goes as high as GG-18 -- on paper, that is).

The grade distribution for the approximately 13 percent of the work force in language billets should logically, as an absolute minimum, reflect the grade distribution of the Agency as a whole. Let's chart that distribution and see what the fair distribution for language personnel should be:

Table 1

If the 381 professional linguists were properly promoted -- on the basis of strict criteria including a consideration of the quality and quantity of output, technical versatility within a single language or adaptability to other languages -- we would see greater stability in the NSA language field, for the following reasons:

- Linguists of all ages would stay in the language field, instead of fleeing the



~~CONFIDENTIAL~~

EO 1.4.(c)
P.L. 86-36

E.O. 1.4 (c)
P.L. 86-36
DOCID: 4009781

technical jobs for management or staff jobs in the hope of getting a promotion;

- Linguists who have made a career in language processing would not jump at the chance to retire at the earliest opportunity, thus taking their hard-earned skills with them;
- The current shortfall of 334 professionalized language personnel could be eliminated fairly rapidly through in-house training and OJT, plus recruitment of college hires with even better qualifications.

Of course, once all 715 billets are filled with professionals, then the question of promotions would come up again. In that instance Table 1 would have to be revised as follows:

Table 2

[redacted]

Inherent in the matter of promotions is the problem of equity. The data reveals that the number of language personnel working as language professionals in the higher grades is out of line to the detriment of language professionals and that a number of promotions are required to achieve job-field parity. And since those jobs are language jobs, the criteria for promotion should and must be based on language skills, competence, and performance -- and not primarily on managerial ability or happenstance, personality traits, or the application of "quotas" having nothing to do with language functions. Quantity of output can easily be tabulated; quality of output is a more difficult problem, but is still amenable to solution. The versatility factor (variety of languages in which there is a demonstrated competency, additional professionalization in other fields, research abilities, etc.) can also be reduced to numerical terms (by a language committee or board) which could be used to multiply the quantity/quality numerical figure (the QQN) -- but that's the subject of another article! ~~(CONFIDENTIAL)~~

НЕЙМ (WHAT'S IN A НЕЙМ?)

[redacted] R51

P.L. 86-36

Humorous papers have been written (by people like Mark Twain, who at least was paid for that sort of thing) about alleged translations from language A into language B, followed by another alleged translation (rarely by the same alleged translator) from the language-B version back into language A. Usually the final version in language A will differ, sometimes dramatically, from the original utterance.

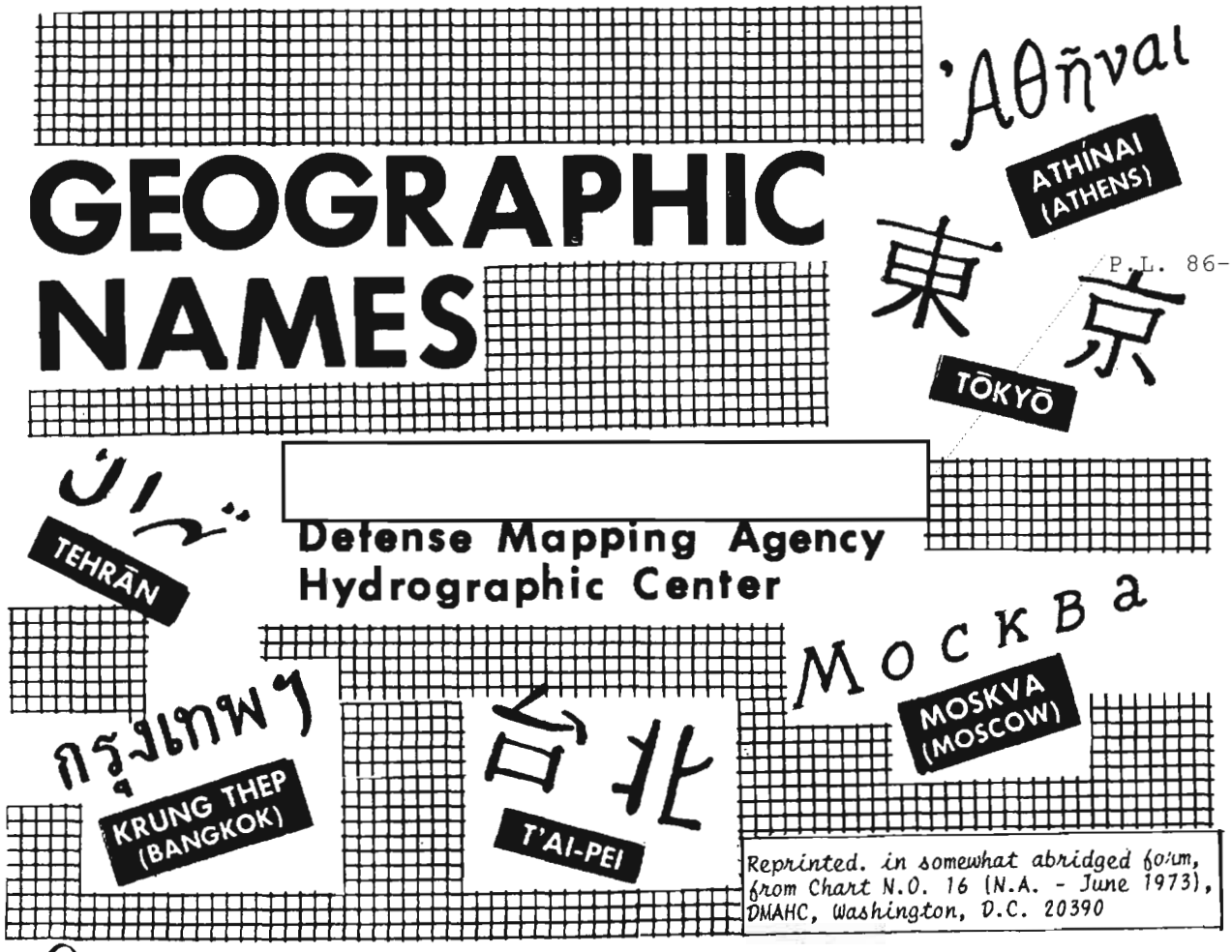
The same kind of problem can show up, perhaps in its starkest form, in the *transliteration*, and subsequent retransliteration, of personal names. The problem is no easier if *yet another* transliteration (that is, a *third* version of the name) is involved. Thanks to the "brain drain" (or "melting pot") syndrome, this is probably the most typical case in the treatment of names in English scientific-technical text which has been translated into Russian and is then retranslated back into English.

At issue is an active area in applied mathematics known as the Monte Carlo method. The method (and its name) stemmed from work performed (largely on the atom bomb) at Los Alamos during the 1940s. The ranking Soviet "expert" on the Monte Carlo method, I. Sobol', wrote a book on the subject, an English translation of which (available in the NSA Technical Library) was published by the University of Chicago Press in 1974. The first page of the translation, in a rapid historical sketch, awards the proper credits to "the two American mathematicians S. Ulam and J. Neyman."

Neyman? I thought it was Neumann! Because one approach to the implementation of the Monte Carlo method at Los Alamos was developed, I thought, by S. Ulam (a native Pole) and J. von Neumann (a native Hungarian). But there was also, indeed, a prestigious American mathematician (also of Central European origin) named Jerzy Neyman, whose area of expertise -- statistics -- is highly relevant to the Monte Carlo method. Was "J. Neyman" J. von Neumann or J. Neyman? According to the Russian spelling, it could have been either (strangely, German *eu*, pronounced "oy" as in "boy, and *ei*, pronounced like the "y" in "my," are both transliterated into Cyrillic as ей -- pronounced "ay" as in "bay"!).

(Continued on p. 21)

DOCID: 4009781



P.L. 86-36

Reprinted, in somewhat abridged form, from Chart N.O. 16 (N.A. - June 1973), DMAHC, Washington, D.C. 20390

Geographic names are an important part of the information carried on maps and charts, and they are used to identify towns, lakes, rivers, and other geographical features in the same manner as personal names do for people. Everything which is of some importance on the earth's surface has a name. Names are a necessity in communication and the more distinctive a name is, the more effective it is because a name should distinguish the feature to which it belongs from all other things. Several names for the same feature or the same name for many features tends to erase the purpose of a name -- to identify. The ideal situation would be to have each feature with its own distinctive name.

The larger and more varied the name users, the more important it is to achieve some degree of commonality in the spelling of geographic names. Within the U.S. government alone, there are hundreds of people who have a daily need to use both domestic and foreign names.

World War II emphasized, especially to the military, that a geographic name should satisfy two very practical requirements. It should be able to provide positive identification and its spelling should be as uniform as possible. Military operations are varied and involve the use of many different specialized maps and charts produced by numerous agencies.

Therefore, particularly from a military standpoint, the objective should be to provide as much standard usage as possible and to use policies that will lead to complete standardization.

The need to standardize has been compounded, since World War II, by the increase in the number of maps produced in foreign countries and the comparable increase in the quantity of foreign names used by cartographic agencies in the Federal Government.

Board on Geographic Names

More than 80 years ago, it was recognized that a good deal of confusion existed throughout the United States in the use of names in publications as well as on maps and charts. Each publishing agency had its own individual approach as to what names were used. It was also quite apparent that, without some guidance, these agencies would not change their ways unless some "standard" names were provided and then that these agencies be compelled to use them.

President Benjamin Harrison, agreeing that some improvement was needed, established the original U.S. Board on Geographic Names in 1890 by Executive Order. The order charged all Departments to refer unsettled name questions to the Board and to accept its decisions. This was the formal beginning of the program in the United States to standardize geographic names on an official basis. Historically, the organization has changed with the times and the people. Until 1943, when it was abolished as an independent agency and placed in the Department of the Interior, this group had ruled on some 20,000 names in the United States but only 2,000 in foreign areas.

The need for foreign names increased tremendously during World War II and it quickly became apparent that we lacked the required information on names for much of the world outside of the United States. In 1943, the Department of the Interior assembled a large staff and began the mass production of standard names to meet the war needs of the armed forces. Millions of names were produced to satisfy the urgent needs of the times and were most useful to a wide range of people throughout the government.

This system of mass production, however, did not result in the required uniformity in foreign name usage and it because apparent, as postwar foreign maps and charts became available, that many of the war-produced names were already obsolete. It therefore became necessary to start anew in many foreign areas and this task was given to the present *Board on Geographic Names (BGN)* which was created by legislative action in 1947. The Public Law states that the Secretary of the Interior conjointly with the Board on Geographic Names will "provide for uniformity in geographic nomenclature throughout the Federal Government" and that the Board shall "formulate principles, policies and procedures to be followed with reference to both domestic and foreign names; and shall decide the standard name for official use."

The present membership of the BGN consists of representatives from 9 Departments and 3 federal agencies. Members are appointed to two-year terms by their respective Departments and are eligible for reappointment. On the average they serve 4 to 5 terms. The present [June 1973] member for the Navy Department is [redacted] Chief, Navigational Information Services Division, Defense Mapping Agency Hydrographic Center (DMAHC), with the author of this paper serving as deputy member.

The BGN normally accepts most foreign names in the form officially used in that country. Features that are common to two or more countries require special treatment. In these cases, the local spelling is approved along with any name that is firmly entrenched in conventional usage. The user must then make a choice where two forms are available but in the interest of standardization, these dual forms are kept to a minimum.

Over the past 25 years, the Board counts among its many accomplishments the development of a well-tested body of policies; approval of over 3,500,000 standard names; development of systems for converting other writing systems into Roman letter forms; and the establishment of a solid base for international cooperation.

Treatment of Names in the Naval Oceanographic Office

The legislative act of 1947 which established the Board on Geographic Names made it obligatory on all federal agencies to adhere to the Board's policies concerning geographic name usage. The Defense Mapping Agency Hydrographic Center has tried to comply with that obligation by editing all names on new or first editions of nautical charts and publications. The purpose of this program is to establish uniformity in the spelling of names, not only within DMAHC, but with other military users of foreign names throughout the government. Even though the navigational chart itself is a highly specialized type, it cannot stand by itself or make its own rules for the spelling of names. It is only one of a variety of charts produced by U. S. government agencies. All features that are common to these various products must be coordinated fully if they are to serve their purpose to the military.

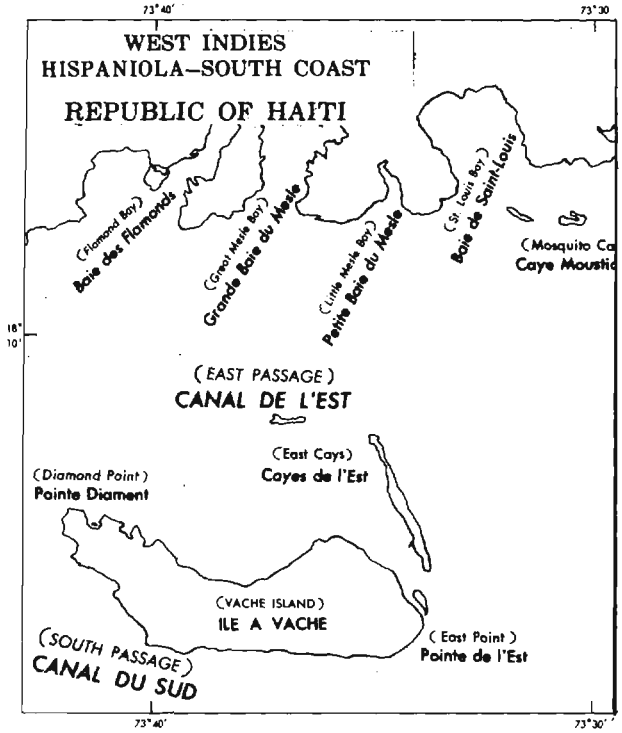
Local Spellings

Users of nautical charts and publications have certainly recognized some of the changes that have taken place in the spelling of names used in our products issued since 1950. They have noticed that a point in France that had previously been called *Black Point* is now labeled *Pointe Noire;* that the Norwegian cape that once was called *North Cape* is now *Nordkapp;* that *Cape Farewell,* Greenland's southernmost tip, has become *Kap Farvel; Genoa* is *Genova;* and *Gulf of Naples* is *Golfo di Napoli.*

Local spellings are, basically, a movement from names that had been assigned English spellings by our early seafarers and explorers to the name now used officially in the area in which the feature occurs.

Policy requires that features that lie entirely within a single sovereign jurisdiction will be spelled as the local official sources spell them, including all diacritical marks. This means that all features lying within Spain or any of her possessions will be named as Spanish official sources spell them. P.L. 86-36

This usage of local spellings is not unique to DMAHC, but rather is the practice of all United States Government mapping and charting agencies and, in fact, followed by many non-government map makers. Our participation in this program accomplishes two things: 1) it ensures DMAHC's compliance with a basic policy of the Board on Geographic Names, and 2) it contributes to overall uniform treatment of names within the Department of Defense.



Section of H.O. Chart 2654 (Reduced), showing former names in parentheses.

The spelling of a foreign name as used locally provides only *one* spelling for the user which, in most cases, is usable to people outside the area. If standardization in the spelling of foreign geographic names is one of our major objectives for military use, then one spelling is preferable to a choice of spellings. This eliminates making a choice of one of the multiple forms available for a feature and delegates these variant spellings to a secondary position. For example, if *Iō Jima* is the official form, then the use of *Iwo Jima, Naka Iwa, Sulphur Island,* and *Iwo Shima* (all of these have been used for this one island) would be limited to parenthetical usage.

By using local spellings, words and symbols new to the English language are introduced, which require some explanation.

Glossary

Practically all names for natural (physical) features include a descriptive part (generic) that tells what the feature is. In English geographic names, of course, descriptive words are easily recognized -- *Lake Erie, Rocky Mountains,* and *Hudson Bay.* In fact, we have accepted and become accustomed to many foreign terms in some other names that are in common usage -- *Fuji Yama, Rio Grande,* and *Loch Lomond.* These examples all contain foreign words (*Yama, Rio, Loch*) and none of these cause us any difficulty.

In many foreign names, however, the descriptive term is spelled in a way that is unfamiliar. How many English readers can see names such as *Punta San Marcos, Akra Letrá, Mys Navarin,* and *Cap Dra* and readily understand the type of feature to which these names apply? All of them contain words (*Punta, Akra, Mys,* and *Cap*) which have the English meaning of cape or point and, standing alone, have no obvious meaning to us.

In order to make these terms more meaningful, a glossary is prepared and carried on our charts. A glossary, in this case, is a tabular listing of foreign descriptive terms used on that particular chart with their equivalent meanings in English.

English	*Arabic*	*Japanese*	*Indonesian*	*Spanish*
Cape	Ra's	Hana	Tandjung	Cabo
Bay	Khawr	Wan	Teluk	Bahía
Island	Jazīrat	Shima	Pulau	Isla
Mountain	Jabal	San	Bukit	Monte
Strait	Bāb	Kaikyō	Selat	Estrecho
Gulf	Khalīj	Gaiwan	Teluk	Golfo
Lake	Buhayrah	Ko	Danau	Lago
Shoal	Ruqq	Iwa	Beting	Bajo

Glossary of English geographic terms with their equivalents in other languages

Diacritical Marks

Diacritical marks are common to many foreign names but are not required in the English language. A diacritical mark (often called an accent mark) can be defined as a modifying mark near or through a letter which indicates a value different from an unmarked letter. These marks form an integral part of a foreign name and are

Arabic	Ā			H̆	Ḥ			
Danish	Å	Æ				ø		
French	À	Â	Ç	É	È	Ê		
German	Ä					Ö	Ü	
Persian	Ā	Á			Ž	Z̄	Z̲	Ẓ
Polish	Ą			ŧ				Ż
Spanish	Á				Ñ	Ó		
Turkish	Â		Ç	İ	Î		Ş	

A few examples of diacritics (some as normally occurring in languages with Roman alphabets, and others as occurring in transliterations from non-Roman alphabets). (Danish Æ is a "ligature.")

DOCID: 4009781

necessary if the name is to be linguistically correct.

Århus, Minchen, İstanbul, Kólpos Iraklíou, and *Moçambique* are examples of names using diacritics.

As stated earlier, policy requires that we include these marks in the spelling of foreign names. It is our duty, therefore, to reproduce local names with as much fidelity as is allowed by the equipment available to the printer.

Romanization

The use of local forms in countries where the Roman alphabet is used presents no problem, for we can copy names directly from their maps and charts. But, what of areas where other than our Roman alphabet is used? How do we copy from Japanese, Russian or Greek sources? Geographic names, from these non-Roman areas, are of no use to us unless they can be written in our own familiar letters. These languages that use other writing systems must be reduced to our writing system and procedures had to be approved for getting this done.

The Board on Geographic Names, in standardizing the names for features in these parts of the world where non-Roman writing systems are used, employs Romanization systems to produce consistent results.

By Romanization we mean any method of transferring names from one language to another, in which each particular letter or graphic sign in the original language is consistently represented by one and the same letter of combination of letters in the second language.

There are upwards of 23 Romanization systems currently approved by the Board on Geographic Names. Most of these systems approved by the Board have also been agreed to by the Permanent Committee on Geographical Names for British official use.

English	*Arabic*	*Bulgarian*	*Hebrew*	*Laotian*
B	ب	Б	בּ	ບ
D	د	Д	ד	ດ
F	ف	Ф	פ	ຟ
K	ك	К	כ	ຄ
L	ل	Л	ל	ລ
R	ر	Р	ר	ຣ
S	س	С	ס	ສ
T	ت	Т	ת	ຕ

Roman alphabet letters with corresponding non-Roman symbols

Conventional Names

We have discussed, in general terms, how the bulk of our names are treated. There is a group that remains, however, that uses what we call *conventional* spellings. A conventional name is one that enjoys widespread usage by readers of English and is commonly applied to a geographic feature.

Names for international features will carry BGN-approved conventional forms. An international feature is one that is common to two or more sovereign nations or one that extends beyond a national jurisdiction.

Included in this category are international water bodies, high seas and subordinate parts, and passages which can be used by all ships without any national restriction. The commonly accepted names *Mediterranean Sea, English Channel, Sea of Japan,* and *Mozambique Channel* are preferable to any one of the numerous local spellings available from countries bordering on these features.

Names for those physical features which coincide with or cross international boundaries also demand conventional usage. Before the *Danube River* reaches the Black Sea it flows through or forms the boundary between several countries. None of the local names available can be given preference and the English spelling is used -- *Danube* (with a local spelling in parentheses, if needed). Likewise, *Caspian Sea, Sahara,* and *Pyrenees* are also examples of physical features that form or cross international boundaries.

Conventional usage is also preferred for countries. *Suomi* has no serious objection to our calling her *Finland,* nor does *Ellas* or *Italia* for our usage of *Greece* and *Italy.* Nor do we really concern ourselves that the French call us *Etats-Unis d'Amérique,* or that the Swedes call us *Förenta Staterna.*

The BGN has approved, for most countries, both a long and short conventional spelling, for country names -- *Australia* or *Commonwealth of Australia* and *Norway* or *Kingdom of Norway.* With few practical exceptions, the *short forms* (*Australia* and *Norway*) will be used on our products. Where no short form exists, as in the cases of *Dominican Republic* and *Central African Republic,* then the long form must serve for all purposes.

Summary

In review, names currently used on nautical charts and publications are the result of specific policies and are treated according to the following rules:

- Names for geographic features lying entirely under one sovereign jurisdiction will take the spelling used by the local authority -- *Venezia (Venice), Islas Canarias (Canary Islands).*
- All names for features in countries using the Roman alphabet will be accepted in the

unaltered form, including accent and diacritical marks -- *København (Copenhagen), Gdańsk (Danzig).*

- Names for features in countries not using the Roman alphabet will be written in Roman letters through the use of an approved Romanization system.
- All descriptive terms used in a foreign language shall remain in that form and shall not be translated -- *Cabo* not *cape, Bahía* not *bay, Ostrov* not *island.*
- Names for international features, extensive geographic names, oceans and their international parts, and countries will be in the conventional English usage -- *Sea of Japan, Brahmaputra River, Andes.*
- If names for undersea features that lie beyond territorial limits contain any descriptive part, that part will be translated and spelled in the English form -- *Ryofu Seamount* not *Ryofu Kaizan, La Chapelle Bank* not *Hauf-fond de La Chapelle.*

  Note: Dual names may be carried in cases where an additional spelling in parentheses would be helpful to the user.

It is apparent, however, that complete standardization on our products will not be accomplished quickly. It may, in fact, be a very slow process.

There are good reasons for this lag. It must be remembered that geographic name usage is dynamic, ever-changing, especially during the period of world nationalism and nation-building. New nations are born and the inhabitants want their place names to reflect this changed status. With the realization of this situation, coupled with the fact that a relatively small number of new and first editions of charts and publications are issued each year, one can see the deterrents to immediate standardization. Some charts do reflect a reasonable amount of consistency because of a special effort (all charts in the area having been processed at the same time) or because they cover areas of political stability. Progress is being made and, hopefully, our goal for standard pelling of names will be attained.

International Standardization

As the globe gets figuratively smaller, more and more names that have had different spellings come into more common use. There are thousands of names for geographic features throughout the world that are not always spelled the same way. The use of numerous languages, dialects, and writing systems results in many of these differences although others are the result of a lack of uniform treatment at the national level. Effective communication calls for an effective means of identifying places. The lack of order in the spelling of names can be considered as a contributing factor to any problem that has developed in worldwide communication.

Very few international rules for the treatment of names have been approved and implemented. Basically, some countries, and in many cases each agency within a country, have attempted to apply their own rules for the application of names outside their immediate area of interest. The problem, simply stated, is to apply some policy whereby a chart maker in Washington and one in Oslo will be able to arrive at a common name used to identify a specific geographic entity so that the navigator using either chart will have the same name for each feature and will not be confused by different spellings.

The Board on Geographic Names has always sought the advice and cooperation of foreign governments and of people living abroad who may have an interest in geographic names. Many foreign governments have also established a national names authority and others are in the process of doing so. Correspondence between these groups and the results of some of the Board's work has been influenced by these intergovernmental discussions. For example, the first conference of the BGN with its British counterpart, the *Permanent Committee on Geographic Names (PCGN),* was held in 1947 at which agreement was sought and reached on a Romanization system for the Russian language. This proved to be the beginning of a fruitful series of conferences which have resulted in a common United States/United Kingdom approach to the treatment of geographic names for many areas.

Numerous other international organizations have recognized and taken some action to reduce the discrepancies that exist in the spelling of names. As long as 100 years ago, the *International Geographic Union* became aware of this problem and since that time many additional technical and professional organizations have expressed concern. The interest expressed through some of these groups to the United Nations resulted in a proposed program for name standardization. A favorable response by UN members to the proposed program, plus the work of some dedicated scholars who realized the practical importance of such a program, led to the first UN conference at Geneva in 1947 and the second at London in 1972.

Fifty to sixty countries and 12 international organizations have sent representatives and observers to the Conference. The delegates, most of whom exhibited a high degree of technical competence, discussed at length the many aspects in the treatment of names and expressed a sincere interest in solving these problems.

The purpose of this first international Conference was to place some emphasis on the problems common to all countries, to understand those problems unique to individual countries, to consider why there is disagreement, and what can be done about it.

The accomplishments of this Conference included a common understanding of the problem, awareness of the points of agreement, the de-

velopment of a spirit of cooperation, and the formation of machinery to promote international cooperation. Recommendations included the holding of regional meetings, the convening of a second conference and the formation of a permanent group of experts to provide continuity and carry on the momentum achieved at Geneva.

It was also recognized at Geneva that before much progress can be made at the international level, each country must first standardize its own names. The establishment of a national names authority and the publication of its own names in official standard form are basic to national standardization. Then, assuming that the approved names would be spelled as used locally, these official names would provide standard spellings for use by other countries using the same writing system and would establish an excellent base to proceed on to international standardization.

One of the international organizations in which DMAHC is an active participant is the *International Hydrographic Bureau (IHB)*. The IHB, with headquarters in Monaco, is composed of member states representing hydrographic offices throughout the world. Its purpose is to promote the navigational safety of the mariner. Its member states have recognized and reaped the benefits of the standardization of information carried on charts and publications. The IHB has also recognized, since its beginning in 1921, the advantages of a uniform treatment of names on these hydrographic products. The recommendation was made in 1947 that *consideration be given to the adoption of a uniform policy for the handling of names on nautical charts and publications*. Members voted approval of a series of recommended procedures for the spelling of geographic names on charts and publications that covered both domestic and foreign coasts. The gradual implementation of these procedures by the now 42 member states would contribute greatly to international standardization. The continuing interest of the IHB bodes well for the program and the publication of any international charts could provide an excellent vehicle for a concentrated effort in that direction.

The interest and cooperation shown by the IHB and other scientific and technical groups is proof that a practical worldwide program exists and that there is a dedicated nucleus of people interested in a solution. International interest has been generated as a result of the UN conferences and other work being done by the IHB and other organizations. Greater interest and participation will quicken the solution to many problems and hasten the day when standard spellings may be used for many geographic names throughout the world.

60°

Letter to the Editor

To the Editor, CRYPTOLOG:

Well, the inevitable ... ed. CRYPTOLOG ... nsity ... ne

Personal to "Annoyed": Thank you for your letter. As has been pointed out several times in CRYPTOLOG (see reprinted reminder below), we can print anonymous contributions or those with a pseudonym, but only if the identity of the writer is known to the editor. If you prefer, you may identify yourself to the Publisher, Mr. Lutwiniak. But, in either case, please do identify yourself so that we can print your letter -- we get so few, we like to print all of them. Ed.

Want anonymity? A thoughtful piece on a subject of interest to many readers will be considered for anonymous publication, if the writer requests it. (The writer must, however, identify himself to the editor in an accompanying note or by a personal call.) Needless to say, personal or trivial complaints will not be considered.

Respectfully,
"Annoyed"

НЕЙМ *(Continued from p. 15)*

It took me some 15 minutes of research in the NSA Technical Library (which, good as it is, probably is less adequate than that of the University of Chicago) to prove to my satisfaction that Нейман-Улам does indeed refer to the (von) Neumann-Ulam method.

For what it's worth, the *mathematics* in the Sobol' translation is quite adequate -- it's only that the three translators were just less than adequate in their handling of such mundane matters of fact as the correct identification of a human being. There's probably a moral somewhere in there.

(UNCLASSIFIED)

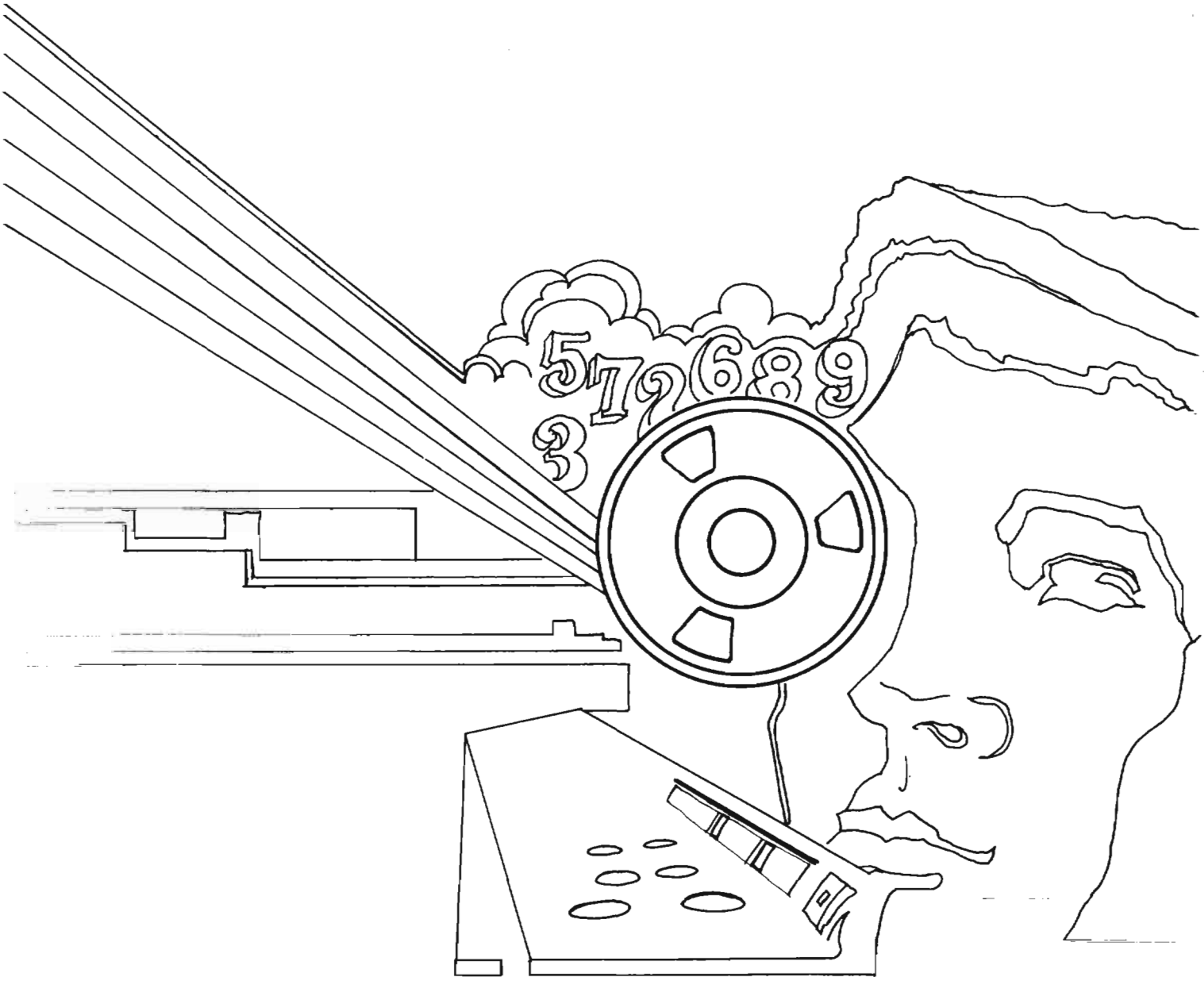
Where's the Index?

If you're looking for the Cumulative Index that has traditionally (that is, for the past two years) appeared in the December issue, don't you remember that the Index is being printed separately from now on? The September 1976 issue of CRYPTOLOG, p. 2, included an order blank for ordering a copy of the 1974-1976 Cumulative Index. In case you missed it, here it is again:

TO: P1, CRYPTOLOG

Please send ____ copy/copies of the CRYPTOLOG Index to:

_____ (Name) _____ (Organization)


5726893

DOCID: 4009739

P.L. 86-36

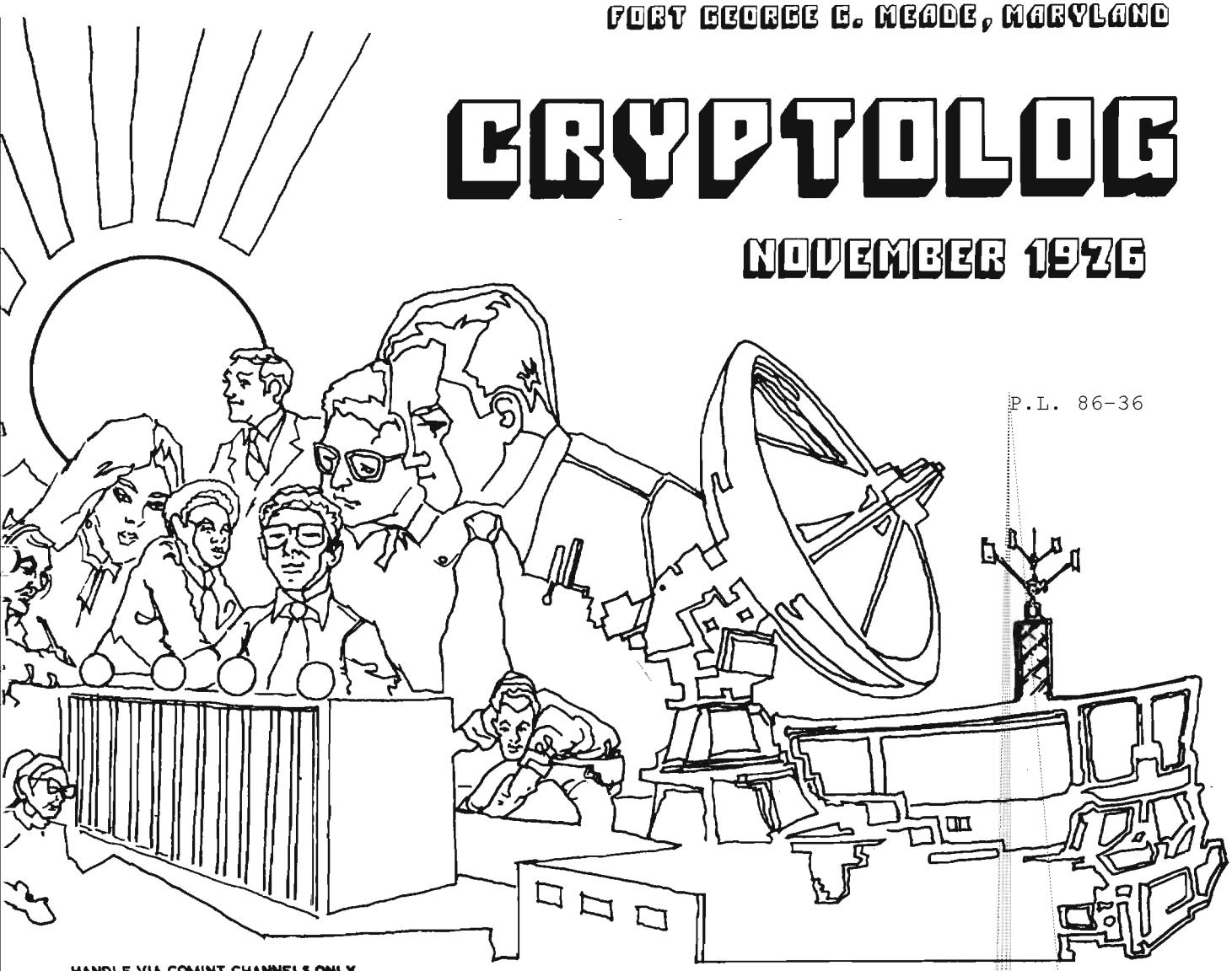
~~TOP SECRET~~

[redacted]

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

NOVEMBER 1976



P.L. 86-36

HANDLE VIA COMINT CHANNELS ONLY

HOW TO MAKE A RAILROAD DISAPPEA[redacted].....1
LETTER TO THE EDITOR.....2
TEACHER LEARNS A LESSON.....[redacted].....3
TEXTA "WORD-SEEK".....[redacted].....4
LETTER FROM CANADA.....[redacted].....5
ANSWER TO "VEXING AGENCY-WIDE PROBLEM"....Frederic O. Mason, Jr....6
THE USES OF ELEGANT ENGLISH.....[redacted].....7
CHECK YOUR MORSE FRONT-END ALIGNMENT!.....11
TOUJOURS LA POLITESSE.....Stuart H. Buck.....12
CLARITY, THY NAME IS QUALIFIER.....John J. Mollick.....14
GOLDEN OLDIES: THE THINGS THEY SAY!.....Doris E. Miller.....15
NOT-TOO-OLDIES: GETTING STARTED.....16

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009739

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. III, No. 11 NOVEMBER 1976

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5642s)

Collection.....[redacted] (8955s)

Cryptanalysis.....[redacted] (8025s)

Language.....Emery W. Tetrault (5236s)

Machine Support.....[redacted] III (3321s)

Mathematics.....Reed Dawson (3957s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Frederic O. Mason, Jr. (4142s)

Production Manager.....[redacted] (4998s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4009739

EO 1.4.(c)
P.L. 86-36

16 Feb '50
ARMED FORCES SECURITY AGENCY

P.L. 86-36

HOW TO MAKE A RAILROAD DISAPPEA

Lately, while cleaning out my files and desk, getting ready for my retirement in January, I came across something I've been keeping as an object lesson for more than a quarter century.

EO 1.4.(c)
P.L. 86-36

DOCID: 4009739

P.L. 86-36
EO 1.4.(c)

I hope that, as I retire from the Agency, I can hand over this favorite object lesson of mine to a new generation of analysts who can get 25 more years' use out of it.

~~(TOP SECRET UMBRA)~~

Letter to the Editor

To the Editor, CRYPTOLOG:

I must be doing something wrong. In the September issue, you offered your readers a copy of the 1974-1976 Cumulative Index. You said, "If you do not want to cut up this issue of CRYPTOLOG, just write 'Index' and your name and organization on a plain piece of paper." Well, I wrote all that on a plain piece of paper, and nothing has happened!

Charles W. Bostick,
G4

Editor's reply:

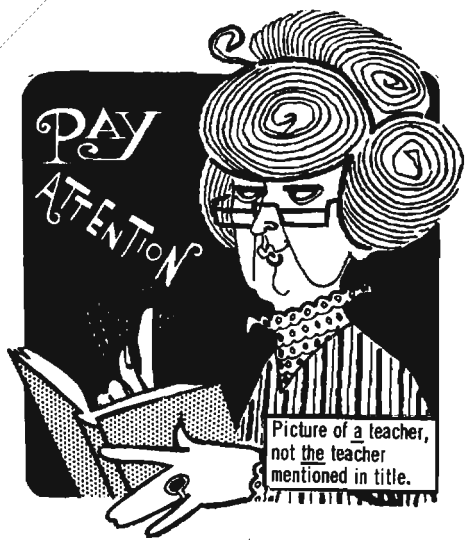
Maybe that's why we haven't received too many requests for the Index. We should have added, "... and send it to P1, CRYPTOLOG." So, if any of you readers want the "plain-piece-of-paper trick" to work, you're going to have to send it to us! (The Index should appear sometime in January.)

(UNCLASSIFIED)

DOCID: 4009739

TEACHER LEARNS A LESSON

G423



I

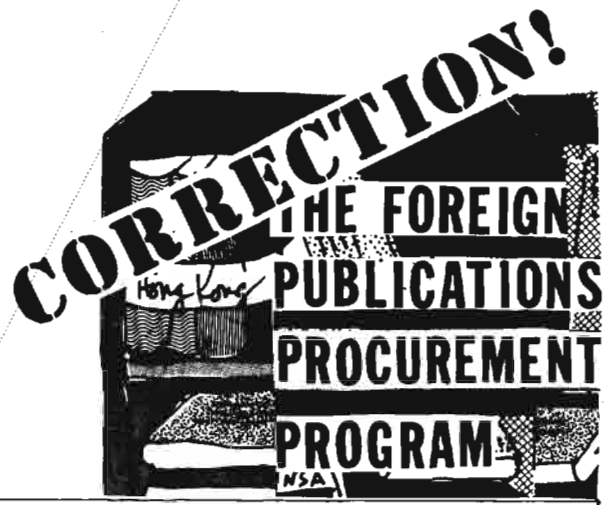
"And, in conclusion, one of the most important lessons to be learned from this exercise is that nothing should be taken for granted," the teacher droned on. "Even when your ideas seem to be working out well, there may be a better explanation." The students stifled a collective yawn. They had heard it all before -- several times.

EO 1.4.(c)
~~SECRET SPOKE~~ P.L. 86-36

EO 1.4.(c)
P.L. 86-36

[redacted]

~~(SECRET SPOKE)~~



Some time after the September 1976 issue of CRYPTOLOG was forwarded to the printer in July, and before that issue actually appeared, the room number and telephone number given in the article on the Foreign Publications Procurement Program were changed. Please change the note to read: "If, after reading the article, you realize that you have some intelligence needs that can be filled by the Program, visit Room B5121 at FANX-III or call 8-7301 concerning your requirements for foreign publications."

~~(CONFIDENTIAL)~~

TEXTA "WORD-SEEK"

[redacted] **A754**

P.L. 86-36

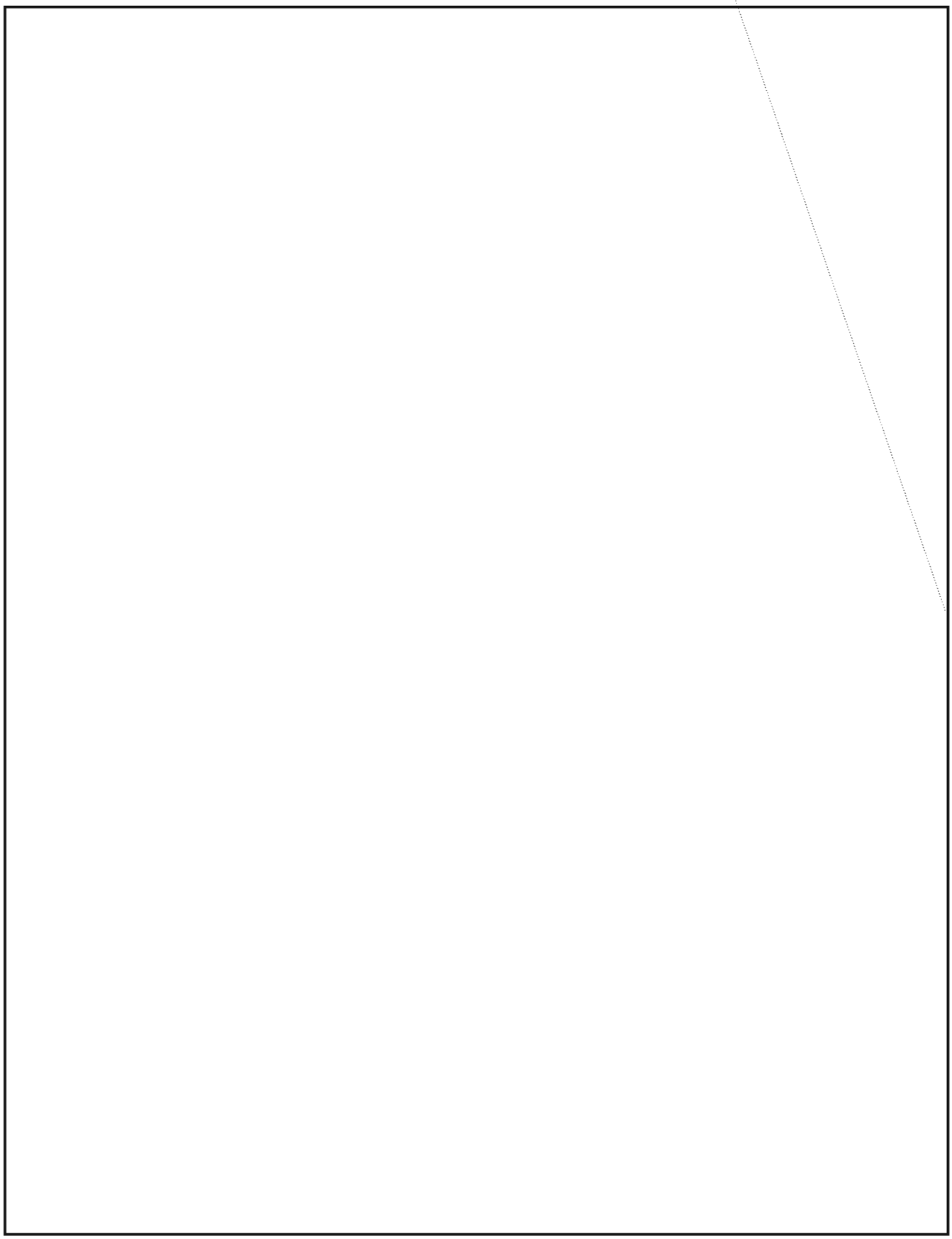
Try to find the 26 service letter TEXTA meanings (for other than "R" and "W" tetragraphs). Words read forward, backward, up, down, and diagonally. Any letter may be used more than once.

EO 1.4.(c)
P.L. 86-36

(Solution will appear next month.)

[redacted]

~~(SECRET - CCO)~~



ANSWER TO "A VEXING AGENCY-WIDE PROBLEM"

(See CRYPTOLOG, October 1976)

Frederic O. Mason, Jr., PII

The first three card positions, alternating A and B cards, occur in the following sequence. That is, a cup having a poker hand beginning with 7♣ 8♠ K♥ will always be immediately followed by one beginning Q♣ 9♠ Q♥, or position 20 followed by position 21 in the sequence.

	8♦10♥	2♥	7♥A♥	K♥	9♦Q♥	J♥	2♦A♥	9♥
10♣	1		19		13		7	
7♣8♠		2		20		14		8
Q♣	9		3		21		15	
K♣9♠		10		4		22		16
A♣	17		11		5		23	
J♣8♣		18		12		6		24

And the last two card positions occur in the following sequence (shown at left below). Combining the two pattern position numbers (PPNs) gives a unique PPN for each possible hand (shown at right below).

	K♦	10♦	J♦	A♦	Q♦
2♠	1	22	8	29	15
J♠	16	2	23	9	30
Q♠	31	17	3	24	10
9♠	11	32	18	4	25
10♠	26	12	33	19	5
K♠	6	27	13	34	20
A♠	21	7	28	14	35

So, 10♣ 8♦10♥ 2♠ K♦ is 1-1
7♣ 8♠ 2♥ J♠10♦ is 2-2
Q♣ 7♥ A♥ Q♠ J♦ is 3-3
K♣ 9♣ K♥ 9♠ A♦ is 4-4
A♣ 9♦ Q♥10♠ Q♦ is 5-5
J♣ 8♣ J♥ K♠ K♦ is 6-6
10♣ 2♦ A♥ A♠10♦ is 7-7
7♣ 8♠ 9♥ 2♠ J♦ is 8-8
Q♣ 8♦10♥ J♠ A♦ is 9-9

So the sequence of pattern position numbers is:

1-1. 2-2, 3-3, 4-4, 5-5, 6-6, 7-7, 8-8, 9-9, 10-10, . . . 23-23, 24-24, 1-25, 2-26, 3-27, 4-28, 5-29, 6-30, 7-31, 8-32, 9-33, 10-34, 11-35, 12-1, . . . 23-24, 24-35, 1-1 (again).

Given one cup, find its two PPNs and add one to each to produce the PPN of the next cup. (Remember that the number after 24 in the first position of the PPN is 1, and that following 35 in the second position is also 1.)

So much is easy, but the determination of the absolute PPN (in the total sequence of 24 x 35 = 840) for any given cup is more difficult.

If one considers only the PPN of the first hand in each sequence of 24 -- that is, cups or hands with PPN 1 for the first three cards -- the following shows, for the top line, the second PPN incrementing at intervals of 24. The second line shows the largest multiple of 35 (the second PPN cycle) which can be subtracted without giving a negative result. And the third line shows the result of the subtraction -- providing a unique sequence from 1 to 35.

1-	1,	25,	49,	73,	97,	121,	145,
-		35	70	70	105	140	
	1	25	14	3	27	16	5

1-	169,	193,	217,	241,	265,	289,	
-	140	175	210	210	245	280	
	29	18	7	31	20	9	

1-	313,	337,	361,	385,	409,	433,	
-	280	315	350	350	385	420	
	33	22	11	35/0	24	13	

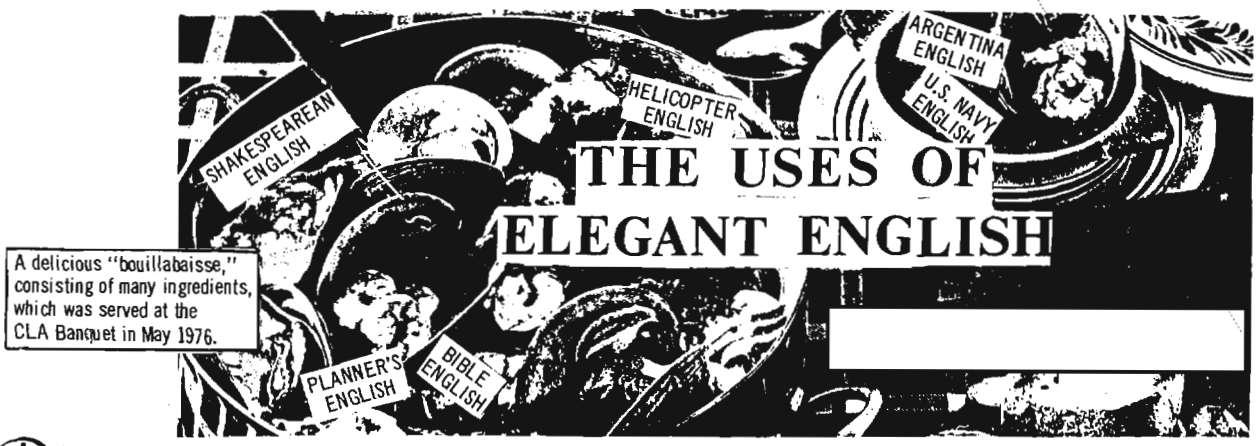
(1-)	457,	481,	505,	(529,)	553,	577,	
-	455	455	490	525	525	560	
	2	26	15	(4)	28	17	

1-	601,	625,	649,	673,	697,	721,	
-	595	595	630	665	665	700	
	6	30	19	8	32	21	

1-	745,	769,	793,	817,	841
-	735	735	770	805	840
	10	34	23	12	1

The four-Aces hand must consist of A♣7♥A♥A♠A♦ at PPN 11-14. To reduce it to PPN 1-?, subtract x=10 from both sides... (1-4 = 529,) as circled above. Now add x=10 to the result to get its absolute PPN of 539.

(UNCLASSIFIED)



THE USES OF ELEGANT ENGLISH

A delicious "bouillabaisse," consisting of many ingredients, which was served at the CIA Banquet in May 1976.

Being linguists, you are aware that God speaks English. You may also have noted that He speaks an especially elegant kind of English. That is because he learned it in 1611, during the reign of King James II. God still speaks this 1611 English, or at any rate He did in the church I attended as a boy, and we do our best to talk back to *Him* in 1611 English.

It was this God-English that first focused my attention on the power of words and set me to listening to people around me -- not only to understand *what* they were saying, but also to observe *how* they were saying it. From God-English I progressed to the observation of how educationists use English, then the U. S. Navy, the U. S. Government, sociologists, policemen, radio announcers -- in short, I became a word-watcher. I began wordwatching at an early age, but the climax of my career came when I was extra-officially (and there are those who would say *frivolously*) appointed Chief Wordwatcher of one of the operating divisions of the Central Intelligence Agency. I have since that time retired, but because of the great interest I have found in the straight world in the subject of Elegant English, I have not abandoned my mission, but rather have even felt compelled to broaden the scope of my research and expand the audience for whom I do it. Before I retired, I had prepared two written reports, which appeared in *Studies in Intelligence*, and this evening, at the invitation of Mrs. Filby, and with your indulgence, I am presenting my first oral report on the uses of Elegant English in various parts of our society.

I am going to take the liberty of incorporating into this first oral report some excerpts from the two written reports, with the thought that even though some of you may have read one or both of the written reports, you may nevertheless find it of some interest to renew your acquaintance with the contents this evening.

Wordwatcher's Credentials

Since I appear before you in the capacity of an authority on the subject, I believe you deserve to hear something of my experience along these lines -- my credentials as a watcher of words -- and if you will bear with me for a moment, I shall give you a brief *overview*, if you will forgive the use of that splendid word right here before we even really get started.

As I implied a moment ago, church was the scene of my first awakening, and I can even identify the person who started me out. It was Mr. Darrell, my Sunday School teacher for a number of years. Mr. Darrell was a sweet and saintly man, but when he prayed or read in 1611 English, wonderful things happened to words, and I spent many glorious hours contemplating these things.

If you know anything about Southern Baptists, you know that they take seriously Jesus' injunction against the "vain repetitions of the heathen." Prayer, to us Southern Baptists, had to be extemporaneous, fished up out of your guilty soul at the very moment of your confrontation with God; and whatever you fished up had to be explained to Him in 1611 English.

Mr. Darrell understood this, and he had a goodly collection of *Thee*'s and *Thou*'s and *unto*'s, although he was a bit shaky about the nominative and objective cases of personal pronouns, and also somewhat hazy about conjugating verbs to suit them. Still, Mr. Darrell was in his mid-fifties, and he had been speaking to God for, I suppose, about 45 of those years, and I must assume that during those years God had learned to cope with Darrellese -- that He understood Mr. Darrell when he ended his prayers, as he invariably did, with the supplication, "We wouldst ask Thee to give us willing hands and receptacle hearts."

When Mr. Darrell read from the passage where Jesus' disciples were preparing to shoo the little children away, and Jesus rebuked them and said "suffer the little children to come unto me and forbid them not, for of such is the kingdom of heaven," Mr. Darrell always put the stress on the wrong word, saying, "*suffer* the little children to come unto me..." It was easier for him to imagine that Jesus had constructed an English sentence backward than

DOCID: 4009739

that King James II might have known another meaning for the word "suffer."

If Mr. Darrell had been called upon to recite another line which was set down at about the same time that the quotation from Jesus was translated -- "Oh, Romeo, Romeo, wherefor art thou Romeo? [meaning, in Elizabethan English, "Oh, *why* are you Romeo?"] Deny thy father and refuse thy name. . ." -- he undoubtedly would have said it as almost everyone else else does nowadays, with the wrong stress, plus a comma, "Oh, Romeo, Romeo, wherefor *art* thou, Romeo?" [presumed meaning "Where *are* you, Romeo?", or even more with-it, "Where are you *at*, Romeo?"] English is, after all, English.

It is not that Mr. Darrell was altogether without instruction. He had been to school! He had learned, for example, that when a word appears in italics, it is to be emphasized. Unfortunately, the scholars whom King James commissioned for his great project had such a spirit of reverence for Holy Writ that they were afraid of being accused of sacrilege if they changed it in any way. Whenever they came upon a Greek phrase, therefore, which required more words in English to express the same thought, they put the extra words in italics -- not for emphasis, but to apologize to God for adding words to His. Mr. Darrell did not understand this, and when he read from the Bible, the effect could be wondrous, indeed. In reading, for example, the 60th Psalm, he would really hit those italicized words, "That thy beloved may be delivered; save *with* thy right hand, and hear me. . . Gilead *is* mine, and Manasseh *is* mine. . . Who will bring me *into* the strong city? . . . Give us help from trouble; for vain *is* the help of man." We have echoes *of* that style of English *in* our midst today, which I shall speak to you about in a moment, But for now let me continue with the discussion of my development as a wordwatcher.

From U.S. Navy to the Argentine

I had had two years at Missouri University when World War II came, and I enlisted in the Navy. Since I could type, I was immediately assigned to the Office of Naval Intelligence. Since I had had two years of Spanish at the University, I was forthwith transferred to the joint British-U.S. Naval Routing Office in Buenos Aires, Argentina. I was, as it were, *qualified*. I thus made the leap from 1611 English, through English Composition and Rhetoric I and II, to the passive voice of Navy communications, and the River Plate English of the Anglo-Argentines.

My experience with River Plate English began immediately upon my arrival in Buenos Aires. I had bought a watch before leaving the United States, which was guaranteed to be shockproof, and was. No matter how I banged it on the table, it would not run. I therefore went to a jewelry shop in downtown Buenos Aires. The young lady behind the counter not only sold me a watch -- she married me about 18 months later. She was Anglo-Argentine. She belonged to one of the most charming and baffling communities on the face of the earth. Her English was fascinating. It still is, on occasion.

I first began to suspect that speaking with her might be a bit of a problem when I showed her a series of cartoons I thought were especially funny, and she laughed and showed them to her sister, who did not laugh. Finally, she pointed to the crucial place on the page and said, "No, no, che, tenés que mirar ahí abajo, que ahí está the funny part!"

The Anglo-Argentines have a language all their own, with partakes of both English and Spanish. In Spanish, when they go to a doctor, for example, it is so that he can *revisarles*, and then, if he finds an injection to be indicated, he may *pincharles*. And so, when they go to a doctor in English, it is to have him "revise" them, and then perhaps "pinch" them with a hypodermic needle. The countryside beyond the outskirts of Buenos Aires is known as *el campo*, and so the Anglo-Argentine, if he has a day off, or a weekend free, may decide to spend it in "the camp."

In Spanish, *horno* means "oven," and therefore *Cabo de Hornos* should be translated "Oven Cape" or "Cape of Ovens," but the entire English-speaking world knows it by the Anglo-Argentine version of "Cape Horn." The same sort of thing happened to the *Rio de la Plata*, which should be translated as "Silver River" or "River of Silver," but which is known to the English-speaking world as "the River Plate."

Back to Missouri

If you think *I* had a problem, you should have seen the reaction of my fellow Missourians when I took her back to Brookfield with me after the war. She could never understand that in English almost the only thing you ever hang without an *up* is a man, and so when people came to see us they were puzzled when she would say, "Let me hang your coats." She once asked a neighbor whose responsibility it was in their household to "throw the garbage" every day. In Buenos Aires, when she wanted to vacuum the floor, what she did was *pasar la aspiradora*. When a friend came to call on us once and my wife said that she had just "passed the vacuum sweeper," he was not sure what she meant, and was afraid to ask. But they all loved her, because she laughed with them when they found her English to be a bit strange, although it did not seem at all strange to her to tell them, for instance, that she and I had just "combed ourselves" and "put our clothes" and had gone downtown "on an automobile" whose engine did not "march very well."

It was in a local movie theater one evening, before the advent of television and X-rated movies, and in a day when four-letter words were almost never heard in public, and certainly

not from the lips of a cultured young woman, that she saw in a newsreel her first view of American football. She was captivated by it. She grasped me by the arm and exclaimed, "Ay, Viejo, Viejo! Mirá esos hombres mastodontes hitting each other in the guts!" You could almost feel the shock of astonishment and revulsion in the theater around us, and I explained quickly that, while I used that phrase around the house now and then, it was not appropriate to public gatherings.

As you may have noted from my recounting of that episode, she calls me "Viejo." She has called me "Viejo" since we were first married, and it was at that time simply a term of endearment, but of course as each year passes it becomes ever more appropriate for her to call me "old man." To the Missouri ear, however, "Viejo" sounds like "vehicle," and I could tell by the expressions on the faces of my friends and family and neighbors that they were bemused, to say the least, by this bizarre term of endearment. They would have understood and accepted "darling," "sweetheart," "honey," or "mi amor," -- but "*vehicle*"?

Well, I shall not dwell any further on my domestic problems of communication, except to urge any of you who happen to know the difference between "the house burned up" and "the house burned down" to come forward later and explain it to her -- and to me, too.

U. S. Navalese

Let us return now to Buenos Aires, and my introduction to the English of U.S. Navy communications. It is fortunate for us all, I think, that the guns of the U.S. Navy have never spoken with the same impact which its official correspondence makes. A U.S. Navy sentence never propels a thought from one place to another, like a projectile from a gun. One of the reasons for this effect is that a Navy sentence can never boast the luxury of an "I" or a "we" for a gun, or a "you" for a target, because the words, "I," "you," and "we" are taboo in Navy correspondence. I learned this under the instruction of a gray-haired warrant officer who had been constructing Navy sentences since the days of coal (and of some sail, too, I think). I learned that the predicate of a Navy sentence must be set up so that it just floats around in a fragrant passive soup, unattached to anything in particular. Let me show you what I mean.

You have received some equipment which does not work. You cannot write to the Bureau of Yards and Docks and ask, "Shall we return the defective equipment to you?" In the first place, this is a direct question, and direct questions are not in accordance with the high class and elevated tone of Navy correspondence. In the second place, it includes two of the taboo words. An experienced Navy writer will have no trouble with this situation, however. He will put together a sentence something like this: "It is wondered if it is desired that subject equipment be returned to the Bureau of Yards and Docks."

The passive voice! Nobody actually *does* anything in the passive voice, and so nobody can be blamed for anything. You have not fired any information or questions at the Bureau of Yards and Docks. You have merely lobbed some words into the air, and the Bureau of Yards and Docks may retrieve subject words or not, as it sees fit.

I lived with this elegance during my entire service in the Navy, but it wasn't until years later that I discovered that it had a purpose. Professor Calvin Linton, who for many years as a consultant for about 30 U.S. government agencies on report writing, revealed the truth to me when he described how the scales had fallen from his own eyes early in his career as a consultant. He wrote me,

> I suggested to the writer of the sentence, "Desire is expressed by this office that the equipment be procured on a loan basis for a period of six months' time," that he might try saying, "We would like to borrow the equipment for six months." His reply was, "Of course I could write it like that. But we'd never get the equipment. We don't 'borrow' around here; we 'procure on a loan basis for a period of. . .'"

Professor Linton got a hint of where he was going wrong from that example, but the true revelation came to him somewhat later:

> I suggested to the Civil Service Commission that the sentence "Advice regarding date of birth is herewith requested" might be changed to "Please tell us your birth date." I was told (though not in these words) that the tone of the original was purposeful, not accidental. It was to suggest to the reader that he was up against something far more powerful and menacing than merely one human being asking another for information.

Stylish Words

Professor Linton's discovery is valid for the entire range of uses of Elegant English. Elegant English has a much more serious purpose than merely to ask for or to give information. It must, above all, impress the listener or reader with the erudition of the writer, with the vividness of his imagination, the originality of his thoughts, the modern contents of his vocabulary, and the aristocracy of his soul. Not only must he know how to phrase things so as to instill awe in the mind of the reader, but he must also be alert for the stylish word or phrase -- the word of the year or the month -- the unusual word that dresses up a sentence and makes the reader admire the writer's cleverness and originality. The truly elegant writer constantly observes the English of his contempo-

raries, and the moment he hears a new words, such as "parameters," he locks onto it, nurses and nurtures it in his own syntactical feed lot, and launches it into the marketplace at every opportunity.

I collect these stylish words and phrases, of which the following are only a small sample:

rationale	*inoperative*
thrust	*input*
interface	*throughput*
dichotomy	*pre-planned*
forthcoming	*infrastructure*
profile	*posit*
options	*construct*
life-style	*viable*
posture	*quantify*
meaningful	*minimal*
relevant	*optimal*
overview	*feedback*
parameters	*point in time*

If you want to use Elegant English, I recommend that you use these words wherever you can fit them into your discourse. Note that most of these elegant words are not words that describe a simple thing or act, such as "house," "man," "hit," "run." No, these words justify their use by *sounding elegant*, and they deserve to be taken out of the narrow functions which they were originally intended to perform, and made to dress up our prose.

Thus, if you have a reason for doing something, it becomes your "rationale." If you are describing a confusion or a conflict, why not call it a "dichotomy"? If a man is being candid or frank with you, he may certainly be said to be "forthcoming." And almost anything you can name may be said to be "relevant" or "irrelevant," so long as you careful never to specify *what to*.

Let me show you how this list can be put to use. One of the purposes of my talk this evening is to discuss how Elegant English affects government communications. If we take that simple statement of purpose and put it into as elegant a sentence as we can manage, using as many of these magnificent tools as we can squeeze in, we might come up with something like this:

> The thrust of the input into the overview which is being presented this evening has been pre-planned in order to posit meaningful and relevant parameters for the formulation of a judgment of how Elegant English, utilized in the throughput of governmental correspondence, tends to exacerbate the dichotomy which usually exists at the interface between the infrastructure levels of the bureaucratic construct.

Is that not an elegant sentence? Does it not sound familiar? Would you not agree that it is grammatically impeccable? Would you not also agree that if the listener understands it, it needs more work?

The list is by no means exhaustive. In fact, it barely scratches the surface. You undoubtedly have your own special elegant words, and that is sufficient rationale for anybody, so long as everything is viable, and you do not have to quantify your options.

The challenge of Elegant English is at its greatest when one is expected to write a report or a memorandum, but has nothing to say, or has so little that he could say it in one or two sentences. You could find your job eliminated if you wrote a report containing only two sentences. Most bureaucrats realize this instinctively. One of the most popular series of lectures Professor Linton ever gave was entitled "How to Write Without Saying Anything."

Plan-Speak

Planners are the champions at this practice of writing a great deal without saying anything. I discovered this fairly late in my career, when I was assigned to the plans section of my division. I learned that planners are adept at producing long, involved papers, replete with footnotes, attachments, tables, and cross references, and that they have even gone so far as to change the very processes they engage in. (Oh, and permit me a bit of an apostrophe about that word. If you are going to be elegant in oral as well as written English, you must cultivate the habit of pronouncing it "proh-cess-ees". . .) As I was saying, planners have changed slightly the very prohcessees they engage in, and often like to refer to those prohcessees as "pre-planning."

Now, you might think at first glance that the very concept of *pre*-planning is tautological, but if you do, it probably shows a lack of experience. Almost anybody with any number of years of service in our government can recall at least one incident, one event, one development, which was very good and also accidental. One does not report such a development to his superiors as being fortuitous. In a case like that, the report must necessarily say that the incident was pre-planned, so that nobody on the higher level will suspect that it was, in fact, post-planned.

Among planners, educationist planners are perhaps the most accomplished euphuists in the English-speaking world. This is important, I think, because, after all, they are teaching our children (our little "throughputs," you might say) and the future of Elegant English thus seems assured. Gone are the days when teachers used words like "fail" and "reading and writing" and "poor" and "disobedient." Now, children are sometimes "underachievers," who must work diligently to "acquire language skills," although some of them may be so "disadvantaged" that they cannot be expected to work in any way except "at their own level," and in some instances may even become "severe norm violators."

(Continued on page 19)

~~CONFIDENTIAL~~

ANALYSTS!
COLLECTION MANAGERS!
SYSTEM DESIGNERS!

CHECK YOUR MORSE FRONT-END ALIGNMENT!

"I CHECKED MINE!"

A PERCIVAL© (rhymes with Knievel) DIAGNOSTIC DISPLAY FOR YOUR PROBLEM IS AS NEAR AS YOUR NEAREST COPE TERMINAL!

ANALYSTS!

- Is your task getting its fair share of attention and technical support at the collection site?
- Actually SEE how your assignments are being handled.
- YOU can trouble-shoot collection problems on YOUR task.

COLLECTION MANAGERS!

- Any collection manager can now be a first-class Monday-morning quarterback.
- Second-guess field collection operations with ease.
- Watch low productivity as it actually happens.
- PERCIVAL will give you the whip hand.

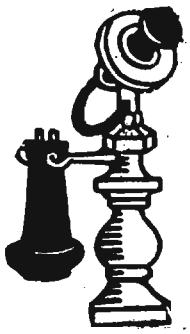
SYSTEM DESIGNERS!

- Now that PERCIVAL is available, you need no longer depend on the fuzzy statements and unreliable folklore passed on to you by operations personnel.
- Get the UNVARNISHED TRUTH first-hand!
- Watch the most intimate details of secret MORSE collection rituals never before seen by outsiders!

TRY IT, YOU'LL LIKE IT!

PERCIVAL (*remember, it rhymes with Knievel!*)

The PERCIVAL



Requests for PERCIVAL service can be addressed to your Office or Division collection manager or to [redacted] Spencer, P11, Ext. 4396. Questions about the software aspects of PERCIVAL should be addressed to [redacted] C142, Ext. 3711.

Call today!

NO OBLIGATION.

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~CONFIDENTIAL~~

DOCID: 4009739

Toujours la politesse...

STUART H. BUCK, P16

I remember very well the incident Jack Gurin refers to in NSA-crostic No. 4 (CRYPTOLOG, June-July 1976; solution, August 1976) -- for

SORUTION TO NSA-CROSTIC No. 4
(CRYPTOROG, June-Jury 1976):

Jacob Gurin[-san], "[Employment of] Military Linguists,"

NSA Technical Journal, Vol. XIII, No. 4, Fall 1968. (Also reprinted in *NSA Technical Journal: Special Linguistics Issue II.)*

"During the showing of a Japanese movie used as a training aid the students cheered mightily when, after about one hour of total lack of comprehension, they understood the maid when she knocked on the door and said 'Excuse me.'"

the simple reason that I was there. In fact, I am grateful to Jack for jogging my memory on the subject. It has brought back a flood of memories that I am about to share with CRYPTOLOG readers.

Jack and I were in the first MISLS unit assigned to study Japanese at the University of Michigan. In a sense, we were guinea pigs. Professor Joseph K. Yamagiwa, who was in charge of the language program, struck us as a man who knew what he was about. It seemed as though he had been preparing for years for our arrival -- and was ready and anxious to try out his theories (and his new book) on us. Of course, he had a great advantage in being bilingual in Japanese and English, and, on top of that, he was clearly a "scientific" linguist. Any doubts on that score would be quickly dispelled by a glance at his text, entitled *Modern Conversational Japanese*. I don't want to knock the book, so I suggest that the reader take a look at it and ask himself if this is a proper text for a rank beginner. I just mention the book because the ideas contained in it have a bearing on the story.

Shortly after we arrived at Ann Arbor, some of the professor's minions appeared bearing gifts -- huge stacks of printed matter purported to guide us through the torments of learning Japanese. A rumor quickly spread that the course materials had been delivered upside down, and that we had started on the first day with the last lesson in the course. If so, one would expect the lessons to be easier later on, but that was not the case, so I suppose the rumor was just the product of some embittered mind. One thing was certain -- the Army expected quite a lot from us. When turned loose in the field, we were supposed to interrogate prisoners (in any dialect) or to translate at sight any captured document (no matter how "grassy"); in short, to cope with any language task that might turn up. To keep our zeal at a fever pitch, laggards were constantly reminded that they could always be reassigned to less pleasant (and more hazardous) duty. Well, there was a war on, so I suppose an atmosphere of urgency was natural enough.

What was not natural for some of us was the Yamagiwa approach to language study. Many of us were used to graded lessons, rules, exercises, and old-fashioned terminology -- all of which was heartily condemned by Yamagiwa. Apparently, he saw the human brain not as an organ capable of rational thought, but as a sponge that merely soaked up everything and anything exposed to it. So there was to be no old-style analysis when he was around. Evidently, language learning was a matter of pure conditioning, and the sooner you got going with it, the better. Before we knew any Japanese at all, he had us assemble and listen to him carry on lengthy conversations in Japanese with the Nisei instructors. I don't know what effect this had on the others, but I always departed from these sessions wondering what in the devil they had been talking about. I guess I was never tuned in on the right wave length. There may have been some sound pedagogical reason for all this, but I never discovered it. Equally baffling was his idea of having us memorize long lists of unrelated words. I still remember the very first Japanese word that I learned -- *rappa*, meaning "bugle." For some reason it stuck in my mind, but I was never able to work it into a conversation.

I don't want to sound too critical of Yamagiwa, for I'm sure that he was on our side in the war. Besides, he did provide us with reams of model sentences to memorize. Many of these had to do with the social amenities. *Gomen nasai*, meaning "pardon me," was one of them. For practice, we used it whenever we met, accompanying it with a sucking in of the breath (in the best Hollywood tradition). It was reassuring to have something reliable to fall back on. At this stage, we didn't know any Japanese to speak of, but we certainly were polite.

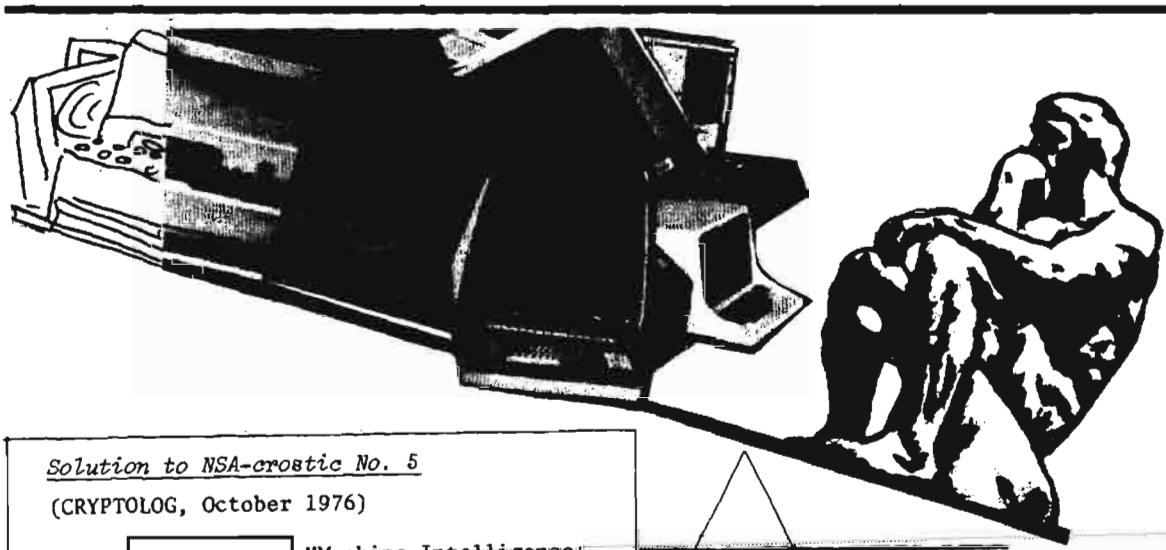
After his mystifying conversations with the Nisei instructors, Yamagiwa liked to take us all to the movies -- Japanese movies, that is. The purpose, we soon discovered, was not to provide entertainment. Presumably, we were expected to soak up the language just by being there. For me, at least, it didn't work. The film that Jack Gurin refers to was a real gem. To this day, I don't know whether it was a clever satire or an outright imitation of some ancient American movie. One thing was clear from the action: the story concerned the age-

DOCID: 4009739

old struggle between good and evil. In other words, a morality play. You could tell the villain right off by the way he twirled his wax moustache and jiggled his eyebrows, Groucho Marx style. The heroine seemed to be struggling throughout most of the film to protect her virtue, so you knew *she* was good. Then there was her boy friend, poor but honest. You could tell where he stood. So everything was reasonably clear, except the language. So far as we could tell, the plot concerned the abduction of a simple country girl by the fellow with the trick moustache, obviously for nefarious purposes. Falling for the blandishments of this snake, the poor girl was lured into a car and away they went towards some den of iniquity. Sensing that his beloved was in peril, the honest country lad leaped on his bicycle and went pedaling over the hills like some Gold Medal winner. Back in the village, the girl's poor but honest parents sat grieving in the doorway of their humble cottage. During a good part of the film, the camera went hopping back and forth between these three scenes: (1) girl screaming and struggling in the car (after it dawned on her that they weren't just taking a turn about the park), (2) sturdy country lad, head down, pedaling uphill and down, and (3) grieving parents sitting in the doorway.

It was a scenario worthy of Max Sennett. Finally the villainous one reached the hideaway where, one assumed, his geisha girls were professionalized, and dragged his wailing and kicking victim out of the car and into the house. Once inside, however, she broke loose, and then began a mad chase around a large table, both screaming in Japanese at the top of their lungs. Every now and then, they would reverse direction -- she keeping a few jumps ahead. To break up the action, there would be an occasional switch to the tireless cyclist, then to the grieving parents. At least *they* didn't say anything -- which was a relief to us. The country girl and her wicked abductor, on the other hand, never stopped shrieking at each other -- and we didn't understand *one word* of what they were saying. Then came a moment when the two stopped, breathless, in their tracks, about to change direction, I suppose. There was a long silence, with only the sound of their heavy breathing. Suddenly a door opened and a geisha girl, dressed in the regalia of her trade, peered over her fan into the room. Sizing up the situation in a glance and seeing that her services were obviously not needed at the moment, she lisped, *"Gomen nasai,"* and withdrew, giggling behind her fan. For the very first time, we heard something in Japanese that we understood. The pent-up emotions of weeks past came pouring out, and the walls shook with our applause. I don't suppose you could call this a linguistic breakthrough. It was more like a glimmer of hope which came when we needed it most.

(UNCLASSIFIED)



Solution to NSA-crostic No. 5

(CRYPTOLOG, October 1976)

[redacted] "Machine Intelligence: [Promise or Delusion?]", CRYPTOLOG, July 1975

"The branch of computer science called Artificial Intelligence involves the attempt to program or build a digital computer capable of producing behavior that a human being would accept as truly intelligent."

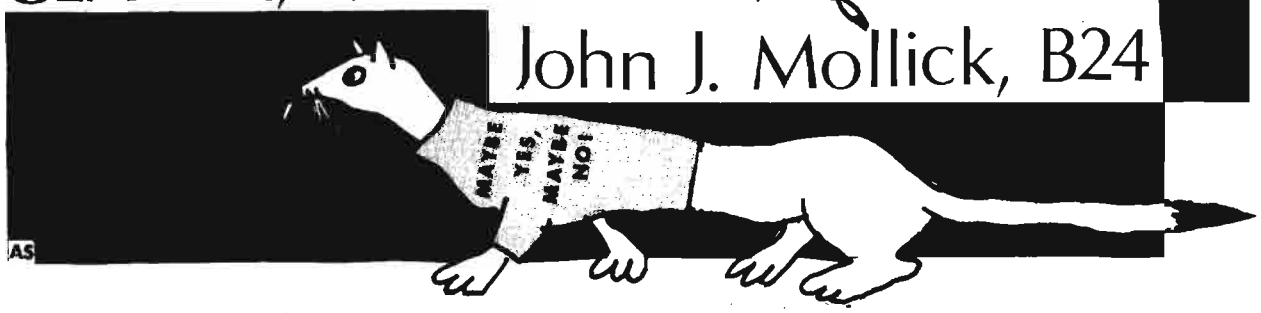
P.L. 86-36

(UNCLASSIFIED)

DOCID: 4009739

CLARITY, THY NAME IS QUALIFIER

John J. Mollick, B24



It took me forty years on earth
To reach this one conclusion:
There is no heaven but clarity,
No hell except confusion.

Jan Struther (1901-1952)

"Probably," "possibly," "it is tentatively suggested that. . ." Qualifiers like that are very common in intelligence reports. And most people in our business -- whether they are reporters or readers of our product -- will probably agree (oops! now it's got *me* doing it!) that qualifiers can be overworked. Yes, indeed, it really would be nice to write or to read a report in which every statement stood on its own without qualification! Simple statements of fact! "X happened, then Y happened, and that means that Z is going to happen." Instead of that wearying style, "It is assumed that X happened, and, if so, then there is a good likelihood that Y happened. Thus, if previous indicators continue to be valid, there is a possibility that, barring unforeseen international developments, Z will happen."

Why don't intelligence reporters write smoothly? Why don't they just throw out all those qualifiers? It is because, in intelligence reporting, smoothness of style must take second place to precision of meaning. When Arthur Symons wrote, "While clearness is a virtue of style, explicitness is not a necessary virtue," he was talking about good literature, not about good intelligence reporting. In intelligence reporting, explicitness is *the* necessary virtue.

I was shocked recently to hear a highly-respected user of our product remark that he tried not to pay much attention to whether something was reported as a possible, probable, or definite fact. Picture the physician who feels that qualifiers are unimportant. If he tells me that I need brain surgery when he means to say that I *might* need it, he stands a good chance of having an A-validity cardiac case on his hands! Imagine the damage if a research analyst reports that some nation is preparing to launch an attack on the United States when he means that it *might* be preparing to launch an attack!

Perhaps the major problem with qualifiers is the common misconception that they are, by nature, obfuscatory. There is no doubt that qualifiers can be, and sometimes are, used as "weasel words" to purposely avoid taking a forthright stand. However, if qualifiers are properly used, they should clarify and not obscure. The use of qualifiers to weasel out of responsibility for taking a position is intellectual cowardice; the use of qualifiers to accurately indicate the degree of credibility that should be attached to an intelligence statements on the basis of available evidence is a moral obligation.

A *Washington Post* article of 25 July 1976 demonstrated that the media also often are forced to call an ace a possible/probable ace. The article concerned speculation that the Chinese were posthumously rehabilitating the image of Lin Piao, Mao Tse-tung's former (you should pardon the expression) "right-hand man." Its short 35 paragraphs contained 21 qualifiers, including such double-barreled sentences as, "An effort to erase black marks against Lin, which *appears evident* in several recent press articles, *would indicate* that some Chinese leaders want to win the army's favor. . . Since Lin's *alleged* conspiracy in 1971, other military leaders *apparently* linked to his plot have not been named. . . Thousands of officers with *apparently* no links to the conspiracy *undoubtedly* remain in the army. . . The *most likely* advocates of such strategy are radicals, with most of the government *apparently* in the hands of moderates. . ."

There is no doubt that the *Post* article would have been more interesting to read with fewer qualifiers; however, it seems that the news reporter who wrote it took seriously the responsibility of the press to indicate validity as accurately as possible. How much more important it is that intelligence analysts always keep in mind the overriding significance of validity and clarity! Over 300 years ago George Herbert stated, "Good words are worth much, and cost little." Those in our profession might add that accurate qualifiers are the best of words -- and *that* is an unqualified A-validity fact!

DOCID: 4009739

Department of GOLDEN OLDIES

THE THINGS THEY SAY!

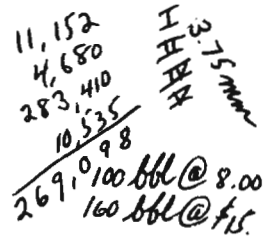
The following article is as pertinent today as it was when it first appeared in KEYWORD in August 1968. There is, in fact, much that is "golden" in the file copies of KEYWORD (published 1968 through 1973) which can be read in the NSA Cryptologic Collection, Room 3W076. Ed.

DORIS E. MILLER, P16 (RETIRED)

Publication of [redacted] article "Transliteration Traps" in the May 1968 KEYWORD reminded me that I once wrote a short piece on the pitfalls of COMINT translation: not those in the text, but those in the mind of the translator, especially the beginner. Certain remarks recurred so frequently among our trainees that I felt moved to record them, and to do a little talking back. Since some of these may still be heard today, I present them below.

"These people don't know their own grammar!" Well, it's ten to one they know it better than *you* do; even if they don't know the rules, they know the patterns and follow them instinctively, and any slight grammatical irregularities they may indulge in will not affect the meaning of the message. Beware, therefore, of trying to support a far-fetched interpretation by assuming grammatical error. Assume, instead, that the grammar is correct, and reexamine your interpretation until you can reconcile it with the text. (It is worthwhile, of course, to familiarize yourself with certain commonplace errors of the "he don't" and "between you and I" type, simply to speed up recognition, even though they seldom occur in traffic or affect the meaning of it.)

"It's obviously an idiom, meaning. . ." You may be right; but a lot of "idioms" have been invented at NSA that never existed except in the mind of a desperate translator. (Ditto for "old proverbs" and "dialectal variants.") The translator's chances of discovering a new idiom vary of course with the language, the degree to which it has been studied and recorded, and the nature of the traffic; but in most cases further work resolves the passage in some quite prosaic way. If a putative idiom does seem to be the only possible answer, it should be treated as warily and documented as carefully as a tenuous code recovery until it achieves "A validity."



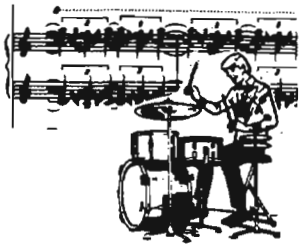
"I'm a translator, not a bookkeeper." True, but routinely checking the numbers in a message is one of the best possible ways to check your own translation. Are the dates (including message and intercept dates) compatible with each other and with tenses in the text, as you have rendered them? Maybe it should be "will arrive" rather than "has arrived." Are paragraphs and subparagraphs all numbered and accounted for? Maybe that passage would be clearer if you realized that it consisted of two unrelated points. Are speeds, tonnages, calibers reasonable? Don't make a new-fangled weapon out of an old-fashioned garble! Does price times number work out to the total given? Look again at the terms of the contract. It is surprising how often this simple process will point up unsuspected errors, or bring a fuzzy picture into focus.

"It's a plant!" Sooner or later, it seems, everyone comes upon a message the facts of which cannot be squared with what he knows, and he reasons that the message must be a fake, deliberately "planted" to deceive us, the

P.L. 86-36

interceptors. But it's highly unlikely, and evidence of a particularly convincing kind would be needed to support such an assumption. Any practical advantage to the sender of deceiving us would in most cases be far outweighed by the risk of confusing his own side. If he is simply worried about being read, he changes his crypt system. Look for the usual explanations, garbles misinterpretations, a gap in your own knowledge. (Or, now and then, of course, a prank by someone in the group. If you really do smell a rat, look around for the local funster!)

"I've written a footnote explaining what I think." This amounts to saying that you don't understand the text, and have probably botched it; for when you get the right answer, it stands on its own feet. Just keep working until enlightenment comes. (If you publish that footnote, I predict it will haunt you!)



"Well, this is MY interpretation. . ." The unspoken end of this, ". . . you may have yours. Can we not both be right?" No, by jing, we can both be wrong, but we cannot both be right. A telegram is not a poem, or a parable, or a Zen riddle. It is a straightforward communication, having -- or meant to have -- only one possible interpretation. The man who receives it is expected to react in some very specific way; to issue that visa, move that battalion, buy that wheat; or file that report, make that decision, sound out that delegate. The correspondents must understand each other, or the world's work would break down. (In some countries, heads would roll.) And our job is to determine what it is they are saying, and put it into English "in words as hard as cannonballs."

"It said DUMPS, but we've never had DUMPS so I degarbled it to PUMPS." And that, men, is how we lost Slambang Air Base. It is just as dangerous to degarble good text as not to degarble bad, and familiarity alone should never be the criterion. Keep an open mind; don't spare the research; and remember that a new word is often the tip-off to a new story.

"I know it doesn't make sense, but that's what it says!" This is the granddaddy of them all, the classic disclaimer -- and the Chimborazo of the humoresque. Do we really believe that all these responsible types, these makers and shippers, are filling the airways with nonsense all over the world? Do we really think that foreigners don't "add up"? Not necessarily. This is just the most spontaneous, universal, and irrepressible outcry in the translating world; there is no one in the business who hasn't given tongue to it at some time. But the person who says it seriously, or very often, is in trouble. For all good translators know, deep down, that if it doesn't make sense, then *that isn't what it says.*

~~(CONFIDENTIAL)~~

Department of GOLDEN not-too-OLDIES

If you liked Doris Miller's Golden Oldie, "The Things They Say!" (and who wouldn't like it?), why not try to get in her league yourself? Even though Doris is retired, this is how she can help you. In March 1975 she gave a talk entitled "You Too Can WIN By Writing," under the sponsorship of WIN (Women in NSA). In that talk she stressed the importance of having NSAers -- women and men alike -- express their views in Agency publications. To help her audience to get started, Doris handed out copies of the "Getting Started" form that is reprinted on the next page. Fill it out! You might find yourself getting an idea for an article for the *NSA Technical Journal, Spectrum,* or, need I suggest, *CRYPTOLOG?* And then -- who knows how soon? -- you might find yourself in the Department of Golden Oldies too.

(For information on WIN, contact [redacted] *G613, 4A187, x4767.)*

P.L. 86-36

UNCLASSIFIED)

DOCID: 4009739

GETTING STARTED

1. *My object is to:*

_____ Make a report on something that has been accomplished.

_____ Call attention to something that is wrong.

_____ Suggest a better method or idea.

_____ Share a personal experience.

_____ Enlist support.

_____ Explain a process.

_____ Ask a question.

_____ Defend a principle.

_____ Report news or announce a coming event.

_____ Recognize an achievement.

_____ Amuse and entertain.

_____ React to something someone else has written.

_____ None of the above, but something else, namely: _____

2. *My working title is:*

"A Better Way to _____."
"Hurray for _____!"
"The Fallacy of _____."
"It's Time to _____."
"The Scandal of _____."
"Are We Paying Too Much For _____?"
"After _____, What?"
"A Proposal for _____."
"What Happened at _____."
"Why I Agree/Disagree with _____ Who Wrote _____."
"A Funny Thing Happened on the Way to _____."
None of the above, but "_____."

3. *I will consider this, in my own mind, an open letter to* _____ *and will address it primarily to her/him/them.*

4. _____ *This would be a particularly good time for such an article to appear because* _____. (or)

_____ *This subject is timeless.*

5. _____ *I am especially well qualified to write on this because* _____

(or on the other hand)

_____ *I want to speak up on this even though I am no expert on it, because* _____

6. *Some tentative suggestions for a final title are* _____

_____

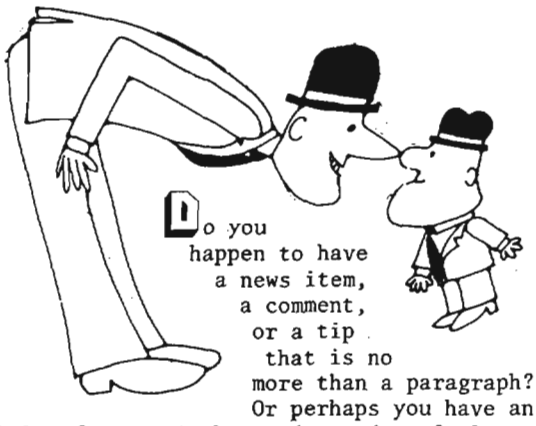
7. *I think it would be most appropriate for publication in:*

_____ *NSA Technical Journal* (major papers on scientific or technical subjects or cryptologic policy, up to and including Top Secret Codeword; distribution to named persons)

_____ *Spectrum* (general-interest articles on Agency policy, management, techniques, history, current topics; up to Secret, but no Codeword; general distribution throughout the Agency)

_____ *CRYPTOLOG* (see reverse side of this page; distribution in Operations and elsewhere to individual subscribers as requested)

Contributions Solicited



Do you happen to have a news item, a comment, or a tip that is no more than a paragraph? Or perhaps you have an article of several thousands words...? Long or short, if it has something worthwhile to say, we'll print it. (For your interest and guidance, one page of typescript, double-spaced, makes about one column in CRYPTOLOG.)

First-person articles or stories about your own experiences are welcome, so long as they relate to our work.

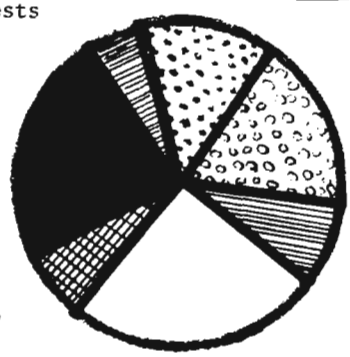
Want anonymity? A thoughtful piece on a subject of interest to many readers will be considered for anonymous publication, if the writer requests it. (The writer must, however, identify himself to the editor in an accompanying note or by a personal call.) Needless to say, personal or trivial complaints will not be considered.

Photographic illustrations can be reproduced, at the same quality as those in the NSA Newsletter.

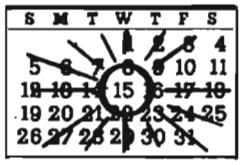
Sensitive materials? No. We'll go all the way to Top Secret Codeword, but we have to draw the line at compartmented or otherwise exclusive sources.

Your contribution does not have to be typed; we'll give preference to content over form, every time. (Though, especially in the case of a long piece, the editorial eye will appreciate any effort you can make in that direction--garbles and strikeovers freely forgiven.)

Something missing? If you feel that your work or your interests are not being well represented in CRYPTOLOG, it's probably because you and your friends are not contributing. The editors earnestly want to cover the whole territory, but articles don't grow on trees, y'know! Somebody (who knows the subject matter) has to write them.



Need assistance? You may have an idea, or some notes, or even a half-finished paper that you feel has possibilities but you don't quite know what to do with. A call to the appropriate departmental editor will get you a "story conference" and possibly inspire you to finish it up and get it into print.



Our deadline is theoretically the middle of the month (the 15th of August, for publication in October, and so on), but don't let that stop you if something good comes along on the 16th. And anyhow, this is a monthly publication; if you miss this month's deadline you'll be just in time for next month's CRYPTOLOG. See you!

ADDRESS: P1, CRYPTOLOG

ELEGANT ENGLISH *(Continued from page 10)*

Once, while looking over a bibliography, Professor Linton came across the titles of two works written by this kind of educator. These were the titles:

"Sociological Implications of the Dynamics of Volunteerism," and

"A Pilot Study Directed Toward the Development of Means of Evaluating the Noncognitive Aspects of Education, Particularly in the Affective Domain."

Now, if you ever find yourself in a situation where there does not seem to be any escape from using a plain old Anglo-Saxon word, without any beauty of sound or appearance, the best thing to do is to define it carefully for your reader, so that he will realize that, however simple and earthy the word may seem to be, it is in reality heavily freighted with style and nuances.

Do you know, for example, what a "need" is? You may *think* you do, but a planner, especially an educationist or a sociologist who plans, cannot use such a simple word with the easy assumption that the reader will fully appreciate just what he is getting. I should like to read to you from a copy of an interoffice memorandum recently circulated in a university in this metropolitan area. It was part of a program to set up statements of what the university staff conceived its functions to be. The document was entitled "Preparation of Mission and Goals Statement for the Library," and these are short excerpts:

> In organizing your ideas, use the pattern outlined in these materials:
>
> 1. Identify needs (see Sec. III.A.)
> 2. Articulate goals to meet the needs (see Sec. III.B for checklist; see Sec. III.C for examples)
> 3. Develop objectives to meet each goal (see Sec. IV)
>
> Write separate documents for each step in the procedure: a list of needs, a statement of goals, and a list of objectives. The following list of definitions may help you in your preparation of the documents for your area:
>
> Needs - Those things required by the various people the activity serves.
>
> Goals - A series of statements, each broad and general, describing ends, not means, and aimed at meeting needs.
>
> Objectives - Specific accomplishments or processes [read "prohcesses"] which should be measurable and which should be concerned with means for achieving goals.

Many pages further along in this document is something called a "Goal Identification Check List," which is a series of questions by means of which you can test whether what you have articulated are, in fact, goals. This is what the check list looks like:

> *GOAL IDENTIFICATION CHECK LIST*
>
> 1. Is the goal expressed in ends not means/activity terms?
> 2. Is the goal flexible (provide opportunities for innovation)?
> 3. Is the goal achievable (both implementable as well as realizable)?
> 4. Is progress toward the goal measurable/assessable?
> 5. Is the goal capable of exacting commitment from all sectors?
> 6. Is the goal available to be changed (not written in cement) and challenged, "updatable"?
> 7. Is the goal free of the constraints of quantification and temporality?
> 8. Is the goal related to needs and problems?

Now, that is the kind of a library you want for your university! Not just a place where they keep an orderly collection of books and papers for students to read, but a place that is alive with goals that are implementable and realizable, and updatable, achievable, measurable and assessable, and, above all, not constrained by quantification and temporality!

It is from such universities as this that our bureaucracy is staffed, I am happy to say -- or, at any rate, those parts of the bureaucracy with which I am familiar seem to be peopled largely with graduates of that school or schools very much like it. In my second written report I cited a number of sentences which show ample evidence of having been hammered out on just such an academic forge. They included the following:

> Jones appears to be in excellent financial straits.
>
> We feel that the university, while still an important element, is less so than it once was. Even if it were, the situation on campus makes the procedure impossible.
>
> He helped his daughter, with whom he is quite close, out financially.

He believes the risk will be minimal if students and instructors utilize reasonable jurisprudence in the course of the exercise.

This announcement by the two officials would put an end to specific rumors of one firing the other, or vice versa.

At that time, they were in the first stages of a broken marriage.

The Cubans were the largest and only exile group in the country.

Also in my second report I included several examples from my collection of what I call the "Technique of Traumatic Terseness." We all know what a great impact can be achieved by making portentous statements in few words: "Lafayette, we are here"; "I cannot spare this general -- he fights." Now, note how much greater an impact can be achieved when the short statement describes the totally unexpected, not to say unbelievable:

Doe and his wife had a daughter of four. When he last saw her she was pregnant.

Jones's wife was in her late twenties, and their daughter, Mary, is aged about five. The latter is rather pale and sickly. She doesn't like Germany very much. She smokes.

Roe was one of seven children, and was raised without a father, who was killed by a log in a forest.

From the content of these sentences you may have divined that we in the CIA live in more of a Tolkien world than a James Bond world. Fleming, after all, never sent Bond out into a forest where the very logs rise up to smite you. The people we deal with are surrounded by dangers James Bond never dreamed of, and that may explain why they feel impelled to begin enjoying life, and reproducing it, at a very early age.

Elegance in the Media

The news media and the popular arts are doing their share to maintain the standards of posh English, and they deserve to be mentioned here, I think. There is, for example, the radio announcer who livens up what would otherwise be rather pedestrian broadcasts by emphasizing unimportant words in a high-class way, which shows that he is a radio announcer, knows what he is doing, and does not belong among the herds of ordinary mortals who do not know how to talk on the radio.

We used to have some noteworthy practitioners of this art in our own metropolitan area, but not anymore. I refer to the policemen in the traffic helicopters who, until somebody took them in hand and utterly destroyed their charm, used to give us bulletins in this manner:

There *has* been *a* four-car collision *at* the entrance *to* the Woodrow Wilson Bridge *on* the Virginia side. There *will* be some delay there until we *can* get a patrol car *to* the scene *of* this accident. Officers *are* responding *to* this situation *and* we hope that the bridge *will* be cleared soon.

The art is not lost, however. It still flourishes in small towns throughout the country, and if you keep your car radio tuned to the radio stations in these towns as you travel through the countryside, you can often hear this type of classy elocution. I recently taped a short excerpt from a news broadcast from station WELD, of Fisher, West Virginia. While I was taping the sequence, I found to my surprise that I was getting homesick. It was only after several minutes that I realized why. I was hearing echoes of dear old Mr. Darrell, reading to our Sunday School class from the 60th Psalm.

That announcer obviously cares very much about his profession. He does not want the radio audience to get the idea that radio announcers are just ordinary people, who speak as ordinary people do. If he were sitting with a group of his friends, he would certainly not use this special way of speaking, because if he did they would most assuredly drown him in the Cheat River. But when he gets behind a microphone, and they get behind a radio set, everything changes, and one must maintain the standards of the art.

If the policy of detente, or whatever diplomatic line we pursue in the future to keep the peace of the world, should ever fail us, which God forbid, I hope I am near Fisher, West Virginia, so that I can get the news from WELD. It would come in a bulletin something like this, I think:

Twenty-one American cities *were* destroyed yesterday *by* atom bombs launched *from* the Soviet Union. Communications *with* Washington, D. C. *have* been interrupted since early this morning, *at* which time President Ford announced that he *had* pushed the button which *would* launch 85 missiles *toward* targets. . . in . . . the (ritardando e diminuendo) Soviet. . . Union. Elsewhere in the news today. . .

That announcer in Fisher, incidentally, did the ultimate recently to our old friend, the "chaise longue." We long ago gave up any silly insistence that this means, in French, simply "*long* chair," because Sears, Ward's, and Hechinger's, among others, have decreed that it is, fact, a *lounge* chair. But the WELD annoucer has an even better idea. He calls it a "chase lounge," and the implications of that pronunciation I leave to your own imagination.

Some radio announcers have trouble with the nominative and objective case of even modern

DOCID: 4009739

English pronouns when two or more of them occur in a series, but this really should be no problem at all. In case of a question, heaviest weight must always be given to elegance of sound, rather than grammatical correctness. I think you will agree with me that the phrase "you and me" sounds low-class and ought to be avoided at all costs. I remember hearing a radio broadcast from St. Louis many years ago, in which Harry Caray was describing a Cardinals baseball game, assisted by that great old ballplayer, Gabby Street. You may remember Gabby -- he was the one who caught the baseball tossed from the top of the Washington Monument many, many years ago. Gabby was commenting on an umpire's decision, and he said, ". . . between you and me, Harry. . ." and then he realized what he said, and quickly changed it. ". . . I guess what I should have said was 'between you and I'. . ." Whereupon Harry congratulated him for having spotted and corrected the error all by himself, without anybody having to point it out to him. Gabby was intensely pleased to have thus been admitted into the company of the elite and he pointed out to Harry that the reason he had made the mistake in the first place was that he had not had much education when he was a boy.

Even newspaper writers and editors are not immune to the problem of the objective and nominative cases for personal pronouns. Mr. Colman McCarthy, of the editorial staff of the *Washington Post*, tells of an editor who certainly belonged among us elegant thinkers and writers. (If you think "among we elegant thinkers and writers" sounds better, have it that way by all means.) According to Mr. McCarthy, this editor came upon a story which had been turned in by a reporter detailing the events of a police line-up that contained a notorious murderess. A witness to her latest crime was brought in, took one look, and exclaimed, "My God, that's her!" The reporter was so struck by the immediate and unequivocal identification that he put that statement in direct quotes in the lead sentence of his story. Our elegant editor would have none of that however, and he corrected it so that on the printed page the article quoted the witness as having said, "My God, that's *she*!"

Elegance in Popular Music

And, now, finally, to the popular arts -- specifically, popular music.

Have you noticed that the lyrics of popular songs seem to have overcome, at least, the problem of *lie* and *lay*. Lyrics these days are less constrained by delicacy and discretion than they used to be, and *lying* and *laying* figure much more prominently and often in love songs than they did in my youth. And so, Helen Reddy signs a ballad in which she entreats me to "come and lay by me," and I believe it was Lou Rawls who recently crooned a song to his lady love who was "laying beside him on the bed."

In at least one respect the poetry of popular music today is more admirable than the work of a T. S. Eliot or an Emily Dickinson. It is because the writers of lyrics today have voluntarily given themselves an almost overwhelming handicap. They have determined to write great music using no other words except *baby, luv, we can make it, I wawnt you, I ne-e-e-d you,* and *come on.*

Even in cases where they violate these restrictions, however, they are still inoculated against the case-virus for personal pronouns. It was Engelbert Humperdinck, I think (the latest Engelbert Humperdinck, that is) who sang a song recently, whose lyrics are the epitome of originality and poetic imagery of which today's songwriters can be so proud. "I'm yours," sang Mr. Humperdinck, "till the stars fall from the sky, for you and I."

Final Caution

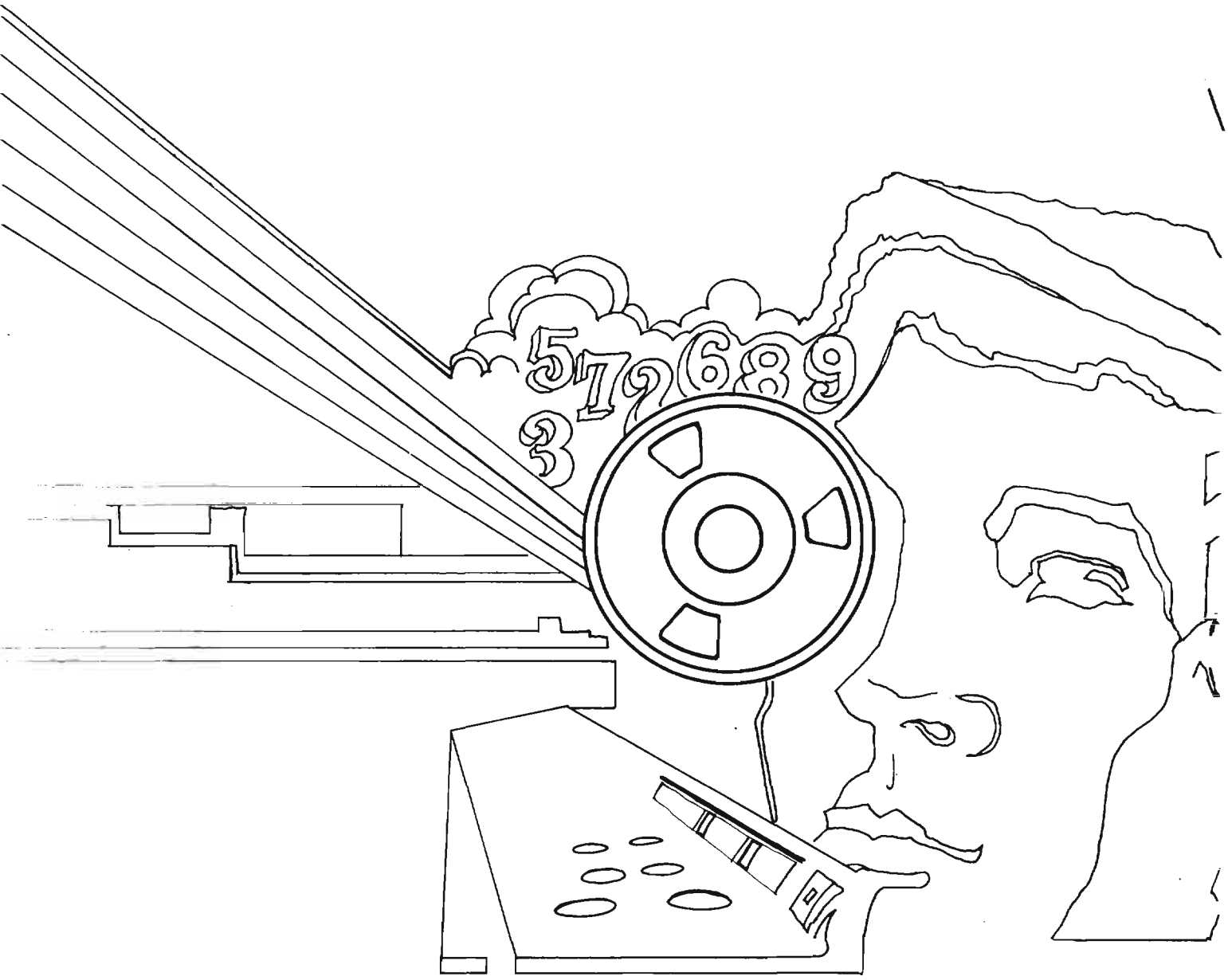
Before concluding, there is one word I should like to caution you about, and that word is *majority*. I once read a report from one of our officers in the field, in the aftermath of a serious flood, in which he said that the majority of the water had receded. Now there is no denying that "majority" sounds much more high-class than plain old "most." But don't you see the danger here? By using "majority" that way, the writer was implying that there was a *minority* of the water still around him, and from experience I would be willing to bet that the officer did not even know the definition of the word *majority*. He may, in fact, have been talking about a *plurality* of the water. So, if you are not absolutely certain of the definition, I recommend great care with these words.

This completes my report this evening, and it remains for me now only to thank you for inviting me here to give it, and for having listened to it so attentively and politely. In concluding, I can think of no better way to exhort you to continue the good fight than to quote the words of a USAID officer in the field who was surveying his situation, his country of assignment, and the future, about which he was quite concerned. I would have you listen carefully to his words, because he has laid down a rule which I believe to be valid for you and me, and for the entire bureaucracy in which we move and have our being. This is what he wrote:

> With regard to future plans, we must steer a careful course between doing nothing and doing the irrelevant.

That is precisely what I have been attempting to do this evening -- steer a careful course between nothing and the irrelevant. I hope that in so doing I may have inspired you to go forth and do likewise, and to do it elegantly.

P1-Nov 76-S3-24924


5726893

DOCID: 4009738

P.L. 86-36

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

[redacted]

CRYPTOLOG

OCTOBER 1976

RUSSIAN SIGINT AND ELECTRONIC WARFARE.... [redacted] 1
ANOTHER WORD ON AG-22..... [redacted] 5
A VEXING AGENCY-WIDE PROBLEM.....Frederic O. Mason, Jr...5
MORE THOUGHTS ON "QUESTIONABLE" SIGINT.... [redacted] 7
LANGUAGE SKILL FILE..... [redacted] 8
NSA-CROSTIC No. 5.....A.J.S.....10
MECHANIZED LANGUAGE WORKING AIDS..... [redacted] 12
MACHINE-PRODUCED AIDS FOR THE LINGUIST....A. J. Salemme.....15
LETTERS TO THE EDITOR..... [redacted] 20
WORK QUOTAS FOR SOVIET TRANSLATORS..... [redacted] 21

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009738

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. III, No. 10 OCTOBER 1976

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5642s)
Collection.....[redacted] (8955s)
Cryptanalysis.....[redacted] (8025s)
Language.....Emery W. Tetrault (5236s)
Machine Support.....[redacted] (3321s)
Mathematics.....Reed Dawson (3957s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Frederic O. Mason, Jr. (4142s)

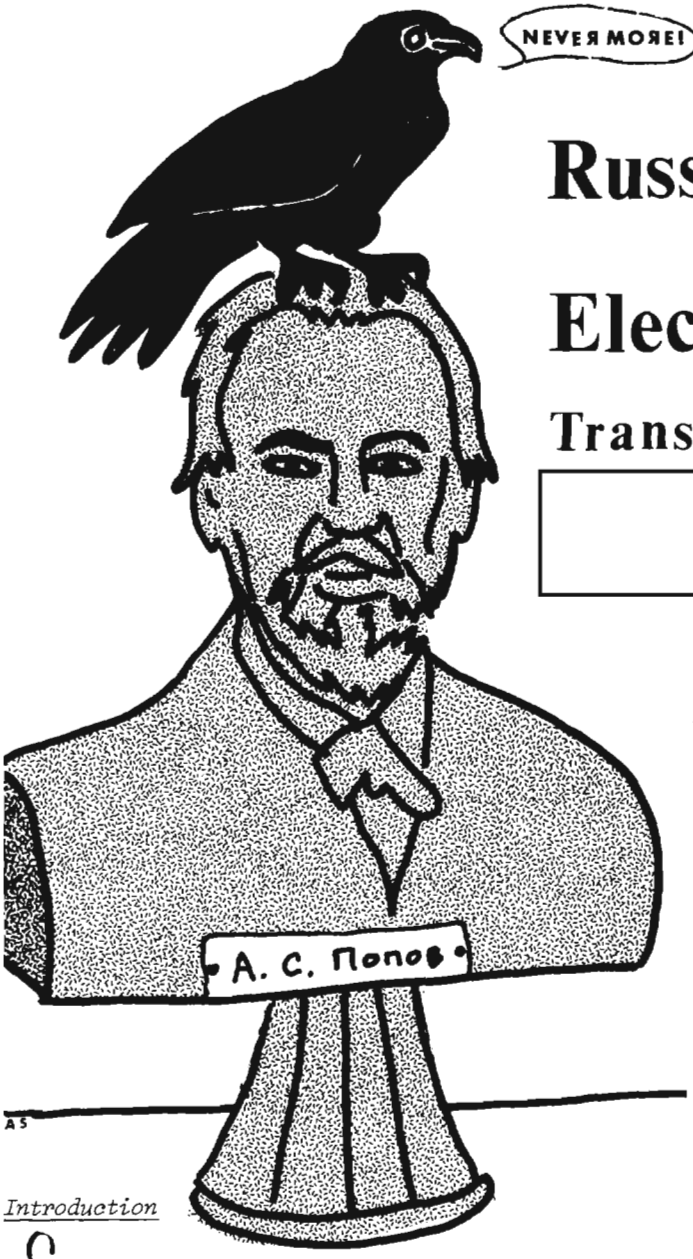
P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4009738

P.L. 86-36



Russian SIGINT & Electronic Warfare

Translated by

[redacted]

Introduction

Since approximately the 1940's, the struggle against electromagnetic emanations "in the ether" has been called the "radioelectronic struggle," or, to use U.S. terminology, "electronic warfare."

By "radioelectronic struggle" one understands the acquiring of intelligence on the enemy's radioelectronic means, the neutralization of their operation by the use of special emanations (jamming); the feeding of misinformation to the enemy; and the protection of friendly radioelectronic systems and methods against the enemy's intelligence and neutralization operations.

Pre-World War I Developments

The concepts of the radioelectronic struggle were expressed by the inventor of radio, the

Translator's note: *The reluctance on the part of the Soviets to discuss their own activities in the areas of intelligence-gathering and electronic warfare will come as no surprise to the reader. Recently, however, the Soviets have tried to document, at least superficially in open sources, some of their activities in these two sensitive areas.*

The following is a translation of an article appearing in Voenno-istoricheskij zhurnal *(Journal of Military History), No. 3, 1975, entitled "From the History of Radioelectronic Warfare." The authors, General-Major of Communications Troops V. Grankin and Colonel V. Zmievskij, discuss the evolution of Soviet SIGINT and electronic warfare from a historical point of view. Although the article is somewhat sketchy, the authors do cite Ministry of Defense Archives as the sources of some of their information. The most important point stressed by the authors is the total integration of SIGINT with electronic warfare.*

I have taken the liberty of deleting two sections -- one section pertaining to Lenin's views on radio as a propaganda instrument, and the other pertaining to the role played by non-Soviet (i.e. German, U.S., etc.) SIGINT/EW in World War II, since only well-known Western sources are cited. The deletion of these two sections takes nothing away from the main thrust of the article.

DOCID: 4009738

Russian scientist A. S. Popov. In a memorandum dated 17 March 1903 to the Russian War Department concerning the establishment of radio communications between Varna and Odessa, A. S. Popov noted that it would be preferable to run the radio line not directly from Varna to Odessa, but from Varna to Sevastopol' to Odessa. That would allow the radio line to be farther away from the Romanian shores, thus making it almost impossible for anyone to monitor its operation or to interrupt its operation with the use of electromagnetic waves. As we can see, the idea of the possible conducting of intelligence and the creation of radio jamming was expressed for the first time by the inventor of radio himself, and it was he who proposed measures to protect radio communications from intelligence-gathering and neutralization operations.

The first attempts at conducting radioelectronic suppression operations, i.e. the use of electromagnetic energy as a kind of "weapon" against electronic systems, occurred during the Russo-Japanese War.

It is a well-known historical fact that in 1905, in the Tsushima Strait area, the Japanese light cruiser Izumi, which was proceeding along a course parallel to that of a squadron of Russian ships, informed its headquarters by radio concerning the number of ships in the squadron. The commander of the Russian cruiser Ural, having detected the Japanese radio transmissions, decided to suppress them by using the radio set on board his ship. This was reported to the Squadron Commander-in-Chief, Admiral Rozhestvenskij, who, incidentally, had categorically forbidden taking such action. Nevertheless, the commanders of the cruiser Izumrud and the torpedo boat Gromkij, on their own initiative, used their shipboard radio sets to suppress the radio communications of the Japanese naval vessels. Thus, measures to suppress an enemy's radio-communications system were carried out for the first time by Russian military specialists

World War I

During World War I, an organized struggle against enemy radio communications was waged by almost all the combatants. At the beginning of the war, the forms that were most widely developed were the monitoring of the operations of radio means, and the interception of radio transmissions. Jamming, for the purpose of interfering with the radio communications in the armies of the combatant countries, occurred very rarely.

An important role in monitoring headquarters and troops was played by short-wave radio direction-finders that were created during World War I by Russian engineers N. D. Papaleksi and A. L. Mandel'shtam. With the aid of the radio direction-finders it became possible to determine the directions to the emitting radio sets and to triangulate their location. According to the number of operating radio sets, it was possible to deduce the area where enemy headquarters and troop groupings were located, as well as any changes or relocations. Together with the intercepting of radio messages, it was possible to determine the intentions of the troops, the sectors in which the basic efforts would be concentrated, etc. In 1915 the armies of almost all the combatant states, including Russia[1], had special radio-intelligence services, which were equipped with radio-intercept equipment and radio direction-finders.

[Omission]

Years Between the Wars[2]

During the years up to World War II, the development of methods for waging the struggle against radioelectronic means followed the course of intensifying the radio-intelligence effort, radio deception, and radioelectronic suppression. Radio-intelligence derives information only from intercepting radio messages and fixing the location of active radio sets with the aid of radio direction-finders. Therefore, if broadcasts of false information are organized, then it is possible to mislead the enemy and force him to take actions which will be beneficial for friendly forces. Thus, a second element in the radioelectronic struggle appeared -- radio deception.

In the Red Army, great importance was attached to problems of deception with the aid of radioelectronic means, and in a number of instances, it resulted in major operational successes. For example, Marshal of the Soviet Union G. K. Zhukov discussed this matter in

---

[1] [For a Soviet view of Russian naval SIGINT in World War I, see "COMINT in the Russian Navy, WWI," *CRYPTOLOG*, May 1976. According to a former Soviet Communications Service chief, Marshal I. T. Peresypkin, from mid-1915 to early 1916, Russian Army radio-intelligence groups were established under the control of army radio-battalion commanders, who were the senior radiotelegraphists. Each group, located at Army Headquarters, was divided into two sections: one section monitored enemy radio stations, while the other engaged in radio intercept. I. T. Peresypkin, *Voennaya radiosvyaz'* (Military Radio Communications), Moscow, Voenizdat, 1962, p. 56. T.R.H.]

[2] [Peresypkin points out that, during the Russian civil war, some of the reversals suffered by the Communists were due to poor COMSEC on their part. In a similar vein, during the Russo-Polish War of 1920, according to Peresypkin, a Polish General Staff officer stated that Polish COMINT units gained enormous amounts of information because of poor radio discipline on the part of the Russians. Peresypkin, *op. cit.*, pp. 108-110. T.R.H.]

DOCID: 4009738

his book *Vospominaniya i razmyshleniya* (Recollections and Reminiscences). In 1939, in the combat actions against the Japanese usurpers at Khalkhin-Gol, the command element of the Soviet forces considered the decisive factor of success in the offensive to have been operational-tactical surprise. "For purposes of deception, and maintaining the utmost secrecy concerning our measures, the Military Council of the Army Group, simultaneously with the plan for the impending operation, developed a plan for operational-tactical deception. . . We knew that the enemy was conducting radio-intelligence and was monitoring our telephone conversations. So, for purposes of misinformation, we worked out an entire program of radio and telephone messages. The conversations concerned only the construction of defensive positions and preparations for the autumn-winter campaign. The radio deception was based chiefly on a code that was easy to break. . .

"Subsequent events and the entire course of our offensive operation showed that the special measures of misinformation and deception, as well as other measures taken in preparation for the surprise operation, played a very important role and the enemy was actually caught unawares."[3]

World War II

During World War II, radioelectronic warfare was further developed and perfected. It was waged by the armies of all the combatant countries. At such time, wide use was made on the fronts of all three components of the radioelectronic struggle: radio-intelligence and radioelectronic intelligence, radio deception, and radioelectronic suppression.[4]

Radioelectronic suppression was the most important and most effective part of the struggle, inasmuch as, by simply creating special suppressing emanations of electromagnetic energy, it was possible to disrupt the operation of the enemy's radioelectronic systems and means. For the first time in history, the Soviet Army used a combination of all three methods of the radioelectronic struggle in the Battle of Stalingrad.

In November-December 1942, the forces on the Southwest, Don, and Stalingrad Fronts intensified their use of radio intelligence. After encircling the German fascists' 6th Field Army, the command element of the Stalingrad Front created an electronic jamming group in order to suppress the German radio communications. This group had several powerful radio sets. In order to derive intelligence from the radio means of the encircled troops, to direct jamming operations against them, and to determine the effectiveness of suppression, the 394th Independent Radio Battalion was activated. Simultaneously, a special radio set was assigned to deceive the 6th Army Headquarters by operating with the callsigns used by the headquarters of Mannstein's group of forces, which was attempting to break through the encirclement. That radio set received from the 6th Army Headquarters 86 very important radio messages. The operation of the enemy radio sets was suppressed by tuning our radio sets to the frequencies used by the enemy radio sets and conducting "meaningless" transmissions when they started to transmit. The established control over the degree of suppressing the radio communications, as well as the testimony of captured generals and officers of the 6th Field Army, attest to the exceptional effectiveness of the measures that were carried out.

A qualitative leap forward in the development of radioelectronic suppression as the basic method in the struggle against the enemy's radio communications occurred in the Soviet Army in 1943. On 17 December 1942, General Headquarters of the Supreme High Command decided to create special radio-jamming units. Two special-purpose radio battalions were immediately created: the 131st and the 132nd. In 1943 and 1944, the 129th and 130th Radio Battalions were formed, respectively.

These were the first units set up for radioelectronic suppression. The creation of these units was necessitated by the waging of the constant radioelectronic struggle.

All the radio units took the most active part in suppressing the enemy's radio-communications systems and misinforming him. The 131st Radio Battalion operated as part of the Northwestern Front, and the 132nd as part of the Voronezh and Central Fronts (1943); subsequently these units were transferred to the 1st Ukrainian and 2nd Belorussian Fronts.

From 1943 through 1945, the radio battalions suppressed the radio communications of the German fascist forces in the army-corps-division chain of command. These radio units achieved a very high degree of success.in suppressing the radio communications of the encircled groupings. The radio battalions set up a complete radio barricade against the enemy's troops. For example, from 23 June through 31 July 1944, the 131st Radio Battalion participated in the Belorussian operation during the encirclement and annihilation of groupings in the Vitebsk area

---

[3]G. K. Zhukov, *Vospominaniya i razmyshleniya*, Moscow, 1969, pp. 161-163.

[4][There is strong, but inconclusive, evidence that, in addition to his regular communications duties, Marshal Peresypkin also controlled Soviet military SIGINT activities throughout WWII. For example, see Heinz Hohne, *Codeword: Direktor*, (New York, Coward, McCann & Geoghegan, 1971, p. 37). Hohne cites a publication of the Institute for the Study of the USSR, *Prominent Persons in the USSR* (Munich, April 1960), as his source that Peresypkin was in charge of military intelligence in addition to his position on the Communications Directorate of the General Staff from the summer of 1941 until 1945. T.R.H.]

and to the southeast of Minsk. This radio battalion worked round the clock, disrupting 522 urgent and 1665 routine enemy radio messages.[5] Subsequently, this same radio battalion was given the task of completely suppressing the radio communications of the encircled Koenigsberg garrison, and, most important, of preventing its command element from communicating with Hitler's headquarters. The battalion was very successful in fulfilling this assignment. During a 24-hour period in the assault on Koenigsberg, the main radio transmitter of the encircled garrison attempted to switch to 43 different frequencies, and every one of the frequencies was suppressed. The corps and division radio communications of the defending troops were also completely suppressed. Then the main radio transmitter began transmitting in the clear the garrison commander's order concerning the capitulation of the troops.[6] The commander of the Koenigsberg garrison forces, General-Colonel Lasch, said at his interrogation, "As a result of the terrible artillery softening-up, the landline communications in the fortress were put out of commission. I had hoped to maintain radio communications with Courland, the Zemland group, and Central Germany. However, the effective jamming measures used by the Russians prevented the transmission of radio messages and my operations could not be coordinated with the headquarters of the Supreme High Command. That was one of the reasons for my capitulation."

The 132nd Radio Battalion also operated just as effectively. In March 1945 the troops of the 1st Ukrainian Front waged combat actions to annihilate the encircled garrisons in Glogau and Breslau. The 132nd Radio Battalion, having divided its forces and equipment into two groups, successfully suppressed the radio communications of those garrisons. During a 15-day period (from 5 through 20 March 1945) the 132nd Radio Battalion disrupted 358 radio transmissions in the Glogau area, 735 in the Breslau area, and prevented 2801 other attempts to establish contact.[7]

Later on, the battalion's main forces and equipment were directed at suppressing the radio communications between the headquarters of the encircled 5th Army Corps and the 9th Field Army headquarters.[8]

In addition to the special radio units, in the course of the Great Patriotic War, the standard equipment issued to troops was often used for the purpose of suppressing the enemy's radio communications. For example, in February 1944, during the encirclement of the German fascist forces in the Korsun'-Shevchenkovskij operation, the headquarters of the 27th Army received intercepted radio messages which were being exchanged between the commanders of the encircled troops and the commanders of the troops outside the ring of encirclement. The command element of the 27th Army decided one night to prepare all the powerful troop radio transmitters to suppress the radio communications of the encircled forces. When the enemy began to attack, we succeeded in completely suppressing his radio communications, thus making it impossible for the encircled grouping to coordinate their actions in breaking through the ring of encirclement.

Thus, during the course of the Great Patriotic War, the struggle against the enemy's electronic systems by means of intelligence, jamming with special emanations, and radio deception found its further development in the Soviet Army. In disrupting the work of radio communications, wide use was made not only of special units created for this purpose for the first time, but also the troop radio means.

[Omission]

Thus, electronic warfare was further developed and improved during World War II. The scope of application of the means of radio-electronic suppression increased; special units (subdivisions) began to be created; and the tactics for their application began to be developed.

Postwar Period

In the postwar period, imperialism has unleashed many wars and armed conflicts. Experience shows that in each of them, means of electronic warfare were used. They were used for resolving not only strategic tasks, but also operational-tactical ones.

Simultaneously, the armed forces of all the technologically developed countries began to develop a fourth element in electronic warfare: protecting the electronic means of friendly troops from the intelligence-gathering and jamming operations conducted against them by the enemy.

At the present time, electronic warfare is undergoing a new phase in its stormy development. As events have shown, not a single combat engagement, not a single operation by any branch of the armed forces, can begin or can be carried out without the broad use of the forces and means of electronic warfare.

[5]Archives of the USSR Ministry of Defense, collection 131, list 36683, folder 1, sheet 9.

[6]*Ibid.*, folder 1, sheet 17.

[7]Archives of the USSR Ministry of Defense, collection 132, list 328334, folder 1, sheet 31.

[8]*Ibid.*, sheet 32.

[redacted] *has prepared an Annotated Bibliography of open-source materials in Russian which deal with SIGINT and EW. To obtain a copy of the bibliography, write or call: P1, CRYPTOLOG Editor, 5642s.*

P.L. 86-36

(UNCLASSIFIED)

DOCID: 4009738
P.L. 86-36

ANOTHER WORD ON AG-22

Fifteen years ago, an intercept operator copied a radio signal onto six-ply paper. He copied while the case was active and usually went back and put in comments when the case went down or paused. The comments appeared not at the place where the pause occurred but at the place where they were relevant. If the operator discovered 5 minutes into the copy that he was hearing a letter wrong, he could go back and correct all the occurrences of the letter -- or simply tell the traffic analyst, who was colocated with the intercept operator.

The traffic analyst, at the intercept site, could analyze the traffic in detail -- at a leisurely pace -- and could inform the intercept operator immediately of his conclusions. He could even consult with the intercept operator to help determine what was going on in the traffic.

The traffic analyst at the intercept site was an important factor in intercept quality. His close contact with the intercept operator speeded up the training of "jeep" intercept operators and also contributed to trained operators' morale and motivation by continually keeping them informed of what was happening. The better intercept operators always had a great interest in analytic details of their targets.

Gold-flow problems caused NSA to look for ways to reduce overseas manning. At first, the technology was not available to move the intercept operator back to the States, but it must have seemed a simple matter to move traffic analysts back. Why, they could analyze traffic at NSA just as easily as at the intercept site, couldn't they? AG-22 would give the traffic analyst his traffic on a real-time basis at NSA.

Budget problems caused NSA not just to move those traffic analysts back, but to eliminate them altogether. There was a set of traffic analysts already at NSA and why did we need duplicative traffic analysis?

The problem is this: those two sets of traffic analysts were not doing duplicate work. The analyst at NSA was performing long-range analysis, building on the short-term work done in the field. The analyst in the field was providing a needed service in short-term analysis *and* in intercept quality control *and* in intercept operator training *and* in intercept operator motivation.

Can AG-22 or any other computer system do that? I think not.

~~(CONFIDENTIAL)~~

(UNCLASSIFIED)

A VEXING AGENCY-WIDE PROBLEM

Frederic O. Mason, Jr.
P11

For the past several months a problem has both interfered with and frustrated the best efforts of our analysts. Happily, it has now been solved, but it required a new concept in collection and a bit of special reporting not included in the routine TECSUM.

The problem was complicated by a lack of funds with which to increase the volume of coordinated data collected, and by unverified reports of items collected elsewhere.

Each item collected provided an example of a term which fell clearly into either an "A" or a "B" configuration, but there were also several occurrences of a "C" and one example of a "D' configuration. Also, collateral reports included references of configurations which could not be any of these (arbitrarily designated "X," until examples are in hand). Normal collection was on a very small scale at first, with many items collected but not reported.

It became clear, even before systematic dual collection was attempted, that the system relied on rotors of different sizes, all stepping at the same time, but the resultant sequence could not be reconstructed from unrelated intercepts.

(Continued, next page)

Recently it became possible to coordinate two collectors so that sequential items from the same series became available. With no more than ten such paired items, together with previously collected data, it became possible to reconstruct the rotors and to establish the entire "A" and "B' sequences. Further, it became clear that the "C" and "D" sequences were based on permutations of the "A/B" rotors, although it has not been possible, with present collectors, to accumulate enough data to reconstruct the "C/D" sequence.

The final problem -- that of understanding the conditions under which the A/B, or the C/D, sequences are used -- was solved when data not previously required was added to the TECSUM.

The solution required that two cups be collected sequentially, using one or two operators, from the same vending machine, and that the Poker Fun cups ("For Consumer Amusement Only -- Use for Gambling or Awarding Prizes May Be Unlawful") be marked in the order received. And the final problem required that a distinction be made between hot cups (the A/B set) and cold cups (the C/D set). A cup from the A set is distinguished by having cards, red or black, in BRRBR order, and is always followed by a cup from the B set, which has cards in BBRBR order and is always followed by a cup from the A set. Both A and B end in suits ♥♠♦, which is a reversal of the C and D final cards ♦♠♥.

We now know the full A/B sequence and have devised a handy-dandy chart which will let us predict, from any one cup, what poker hand will appear on the next cup.

As for rotors, each card position in each set has three, four, five, or seven cards, which repeat in order. Rotors would give this effect.

However, our collectors don't normally collect C/D cups, and reports of flushes (not possible with either A/B or C/D sets) remain unconfirmed. Solutions to these remaining, and vexing, problems must wait for other analytic groups to solve.

Meanwhile, here are sample data (you can collect more if you wish), which are sufficient to a solution. The first cup we collected, arbitrarily designated as at position A001 in the sequence, was the hand 10♣ 8♦ 10♥ 2♠ K♦ .

We also collected samples of various winning hands, as follows:

4 of a kind

10♣ 8♦ 10♥ 10♠ 10♦
K♣ 9♣ K♥ K♠ K♦

Full house

K♣ 9♣ 9♥ K♠ K♦
K♣ 9♣ K♥ 9♠ K♦

3 of a kind

7♣ 8♠ K♥ K♠ K♦
8♣ K♣ K♦ 9♠ K♥
9♣ A♣ A♦ K♣ A♥
10♣ 9♦ Q♥ Q♠ Q♦
A♣ 7♥ A♥ K♣ A♠
A♣ 7♥ A♥ A♣ K♦
A♣ 9♦ Q♥ Q♣ Q♦

Straight

7♣ 8♠ 9♥ 10♠ J♦
7♠ 8♠ 9♥ J♣ 10♦
8♠ 7♣ 10♦ J♣ 9♥
J♣ 8♠ 9♥ Q♣ 10♦
K♣ 9♣ J♥ 10♣ Q♦

2 pairs

J♣ 8♣ 2♥ 2♠ J♦
J♣ 8♣ K♥ J♠ K♦
K♣ 9♣ 2♥ 9♠ K♦

1 pair

7♣ 8♣ J♥ Q♠ J♦
10♣ 7♥ A♥ A♠ J♦
A♣ 2♦ 8♥ 9♠ A♦
A♣ 7♥ A♥ K♣ Q♦

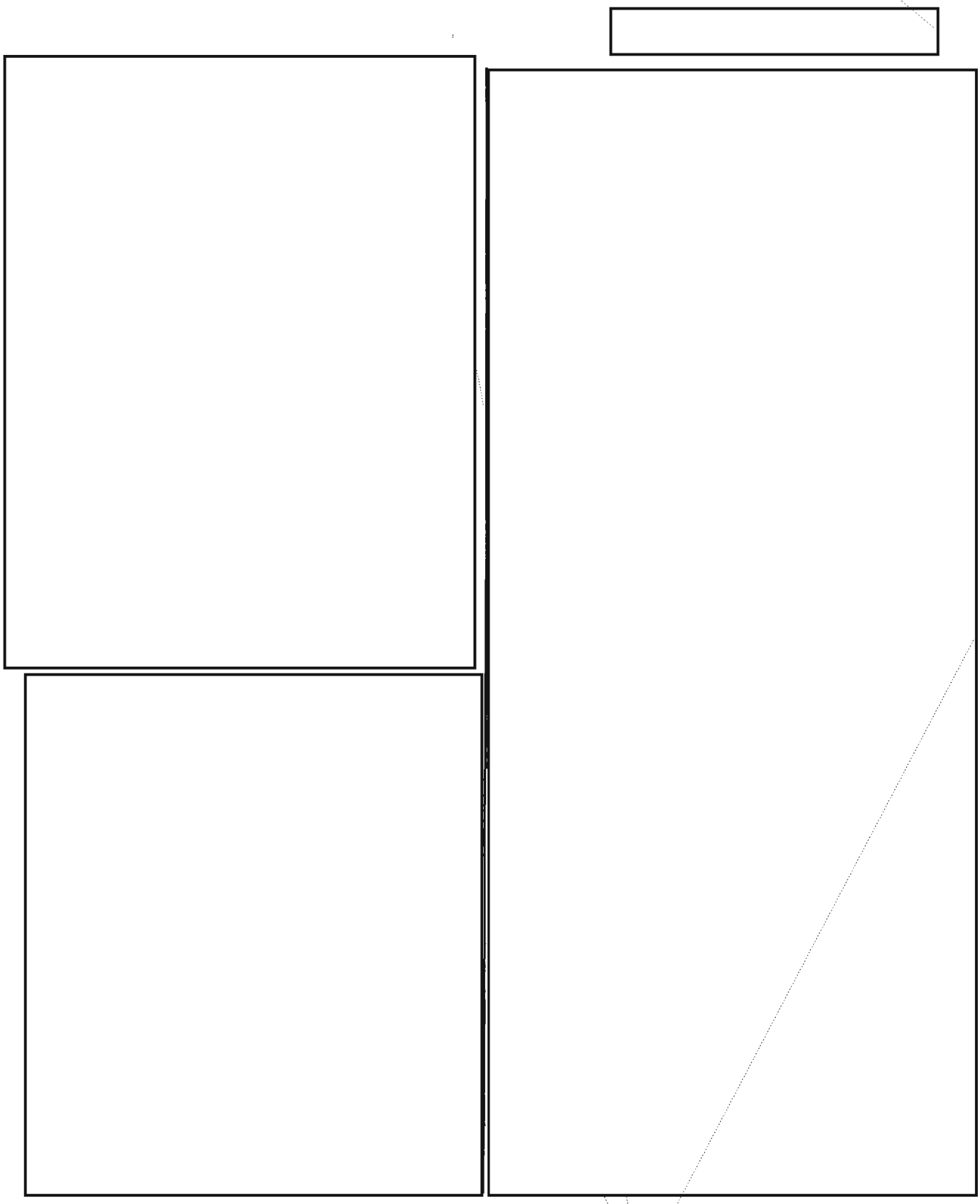
The following pairs have been artificially constructed from the answer, since the analysts, in an unfortunate excess of parochialism, attempted to frustrate competition for the solution by destroying their data. However, the answer has been checked repeatedly at the point of intercept and these data are thereby validated, even if they cannot be retrieved from the data base we hang on our wall.

First member of pair	*Followed by*
10♣ 2♦ 8♥ K♠ 10♦	7♣ 8♠ 9♥ A♠ J♦
J♣ 8♣ K♥ 2♠ Q♦	10♣ 9♦ Q♥ J♠ K♦
A♣ 8♦ 10♥ 9♠ J♦	J♣ 8♣ 2♥ 10♠ A♦
7♠ 8♣ K♥ J♠ J♦	Q♣ 9♦ Q♥ Q♠ A♦
K♣ 9♣ K♥ 9♠ K♦	A♣ 9♦ Q♥ 10♠ 10♦
Q♣ 8♦ 10♥ J♠ 10♦	K♣ 9♣ 2♥ Q♠ J♦
10♣ 7♥ A♥ 10♠ K♦	7♣ 8♠ K♥ K♠ 10♦
7♣ 8♠ 9♥ A♠ J♦	Q♣ 8♦ 10♥ 2♠ A♦
A♣ 9♦ Q♥ 2♠ K♦	J♣ 8♣ J♥ J♠ 10♦
K♣ 9♣ 2♥ Q♠ K♦	A♣ 7♥ A♥ 9♠ 10♦
7♣ 8♠ J♥ K♠ A♦	Q♣ 2♦ 8♥ A♠ Q♦

The problem for you -- and the author will buy one cup of coffee for the first correct answer -- is to provide the sequence position of the only cup having four aces.

(Solution next month)

MORE THOUGHTS ON "QUESTIONABLE" SIGINT



EO 1.4.(c)
P.L. 86-36

LANGUAGE SKILL FILE

The following article appeared originally in Field Information Letter, June 1976. It has been slightly revised and updated by the authors.

Producing an accurate inventory of the Agency's linguistic resources has become a major management concern in recent years. In this context, the term "resources" encompasses assets, versatility, and quality. While it has been possible to assess language requirements with a fair degree of accuracy by using the billet requirements expressed in the Table of Distribution (TD), attempts to assess capability have been frustrated by the lack of verifiable data concerning incumbents of those billets. Frequently, supervisors' evaluations, or even self-evaluations, have been relied upon in determining skill level. Taking inventories has also been complicated by the fact that some people with a language proficiency are no longer working in the language career field and some linguists have a proficiency in a number of languages, even though they may be using only one in their current position.

After analyzing the problem it was concluded that the managerial tools now available -- including the TD, certification statistics, and language proficiency test (LPT) results -- could not be relied upon to give an accurate inventory. We also concluded that an accurate picture of the linguistic capability of the work force would be gained if a language skill level was associated with an individual, rather than a billet or Career Occupational Specialty Code (COSC). As a result, a Personal Skill Code (PSC) was established and is now being used to identify the linguist skills of all Agency personnel regardless of the job title they may currently hold. The skill code has four basic elements that indicate: 1) skill level; 2) language digraph; 3) method by which the level was verified; and 4) year the level was verified. Additional elements can be added to these to indicate a voice-analysis capability.

To date, codes have been assigned to all civilians whose background reflects language training; everyone coded at the zero or one level has been encouraged to be tested in those languages.

1.4.(c) P.L. 86-36

Using the skill codes and the Personnel Information Distribution System (PIDS) it is possible to retrieve language data on-line by language digraph, skill level, and organization. It is anticipated that this information could be particularly useful during crisis situations.

[redacted] the people coded at the zero and one levels might be of greater interest for retraining or for receiving additional training. The system printout, in response to these requests, would give each person's name, grade, COSC, and the last two positions of his job number (which indicate the language he/she is currently using, if any) and his/her skill code.

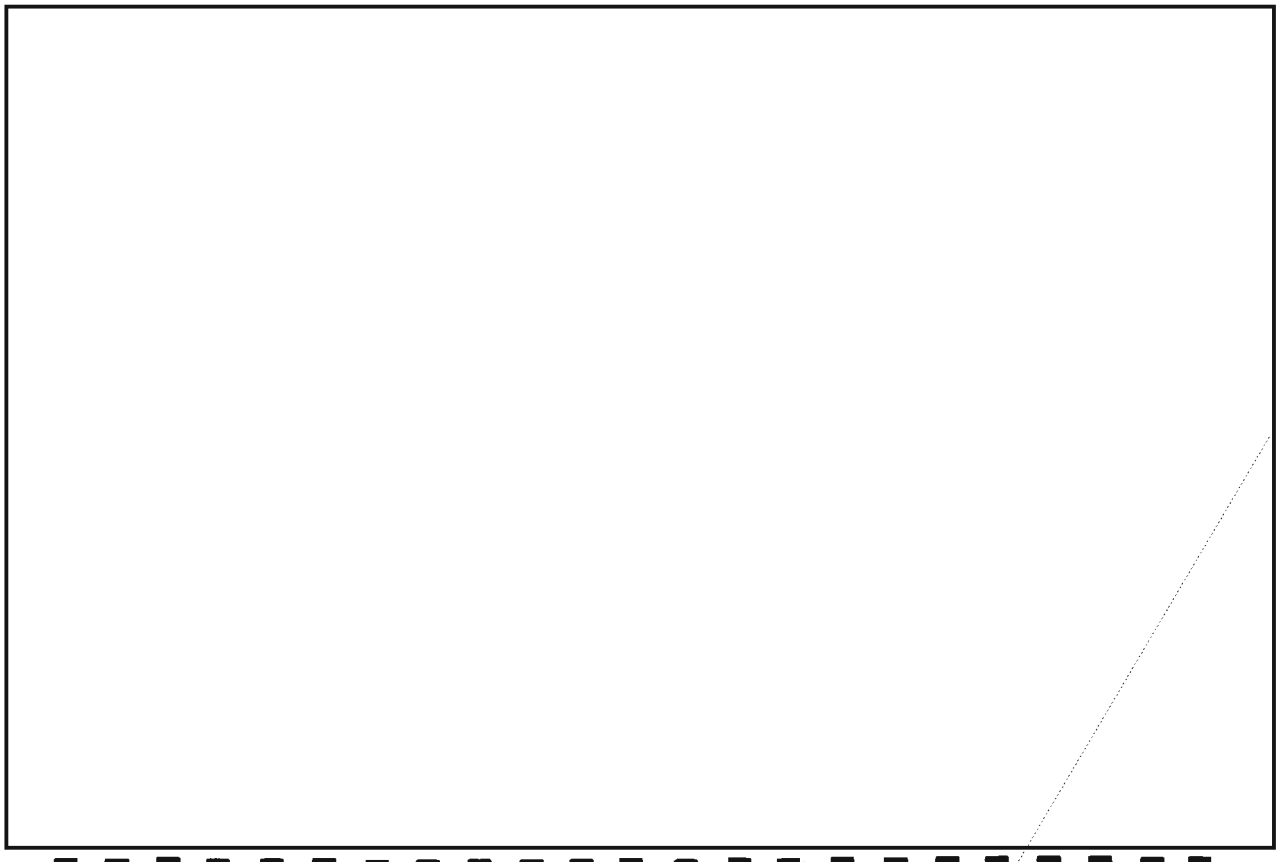
The system also allows managers to make use of the versatility of their work force. On a day-to-day basis a manager may only be interested in the fact that an employee has a proficiency in the language of the primary target he is working on; however, secondary language skills could be of significance in areas where there is an occasional requirement for someone with training in other languages or where there have been shifts in the emphasis placed on individual targets. Similarly, languages for which there is no operational requirement, or a very small requirement, are of interest largely because of the information provided on an employee's capability to learn a language in a particular family of languages.

EO 1.4.(c)
P.L. 86-36

The Personal Skill Code is still in a developmental stage and will be modified in future months to identify individuals who have not yet achieved certification but have passed one or more parts of the PQE and to identify individuals who have the capability to work with voice as well as written language materials. Guidance from the Language Advisory Committee will be sought in determining when a language proficiency might be considered dormant and when it should be thought of as beyond revitalization.

A summary of the language skills currently represented in the field for individuals coded to date is given in the following table. If you are interested in obtaining a copy of the *Guide to the Language Skill File*, which gives examples of the output that can be obtained by using each of the programmed segments in the PIDS, or if you have questions on the use of the file, contact M33 (8267 or 8276).

SUMMARY OF LANGUAGE SKILLS REPRESENTED IN F (Field Units)



EO 1.4.(c)
P.L. 86-36

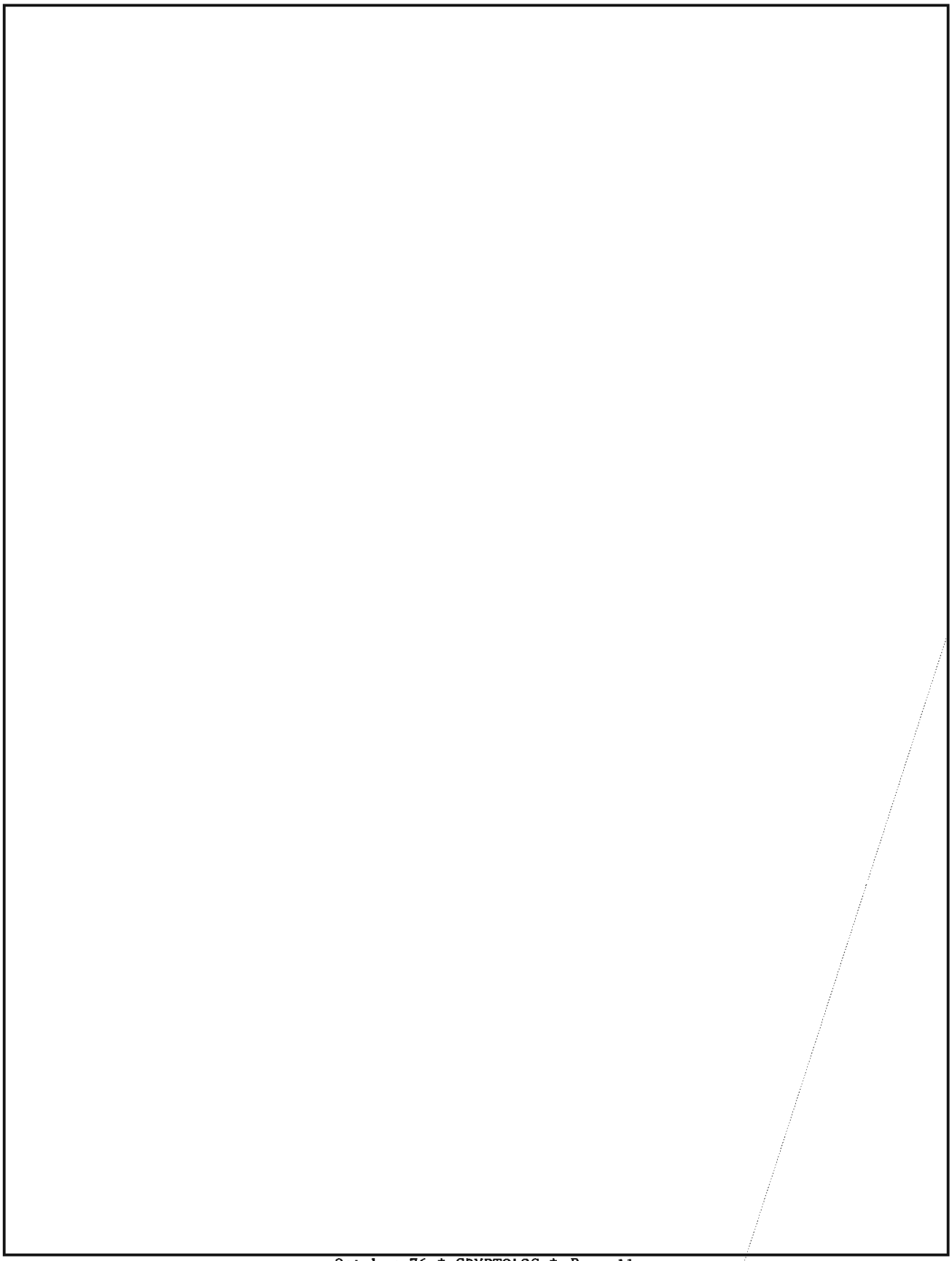
NSA-CROSTIC No. 5

By A. J. S.

The quotation on the next page was taken from a published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

P.L. 86-36

DEFINITIONS *WORDS*



P.L. 86-36

EO 1.4.(c)
P.L. 86-36

A Technical Journal, Summer 1967
CAMINO
BY DORIS MILLER AND [redacted]

CRYPTOLOG, July 1975
There are times when it is useful for analysts to scan the English meanings in a foreign-language glossary in order to find all the foreign terms relating to a given tep...

¡CAMINO EN INGLÉS!

SOME IDEAS ABOUT MECHANIZED LANGUAGE WORKING AIDS

[redacted]

CRYPTOLOG, February-March 1975
CAMINO NEWS
CAMINO is a good ide... better. Many ...

This brief paper is intended to present some general comments covering my experience with the CAMINO Natural-Language Machine Files and other computerized natural-language working aids. It has seemed to me that these remarks might be of some value or interest to others concerned with mechanized language aids, whether as users or as designers.

In considering the design of a natural-language dictionary (as in any data management system, however sophisticated or rudimentary), there are three obvious kinds of things that need to be done:

a) building the file from external sources;
b) maintaining the file by additions, deletions, and corrections; and
c) querying, displaying, or extracting data from the file for day-to-day operational use.

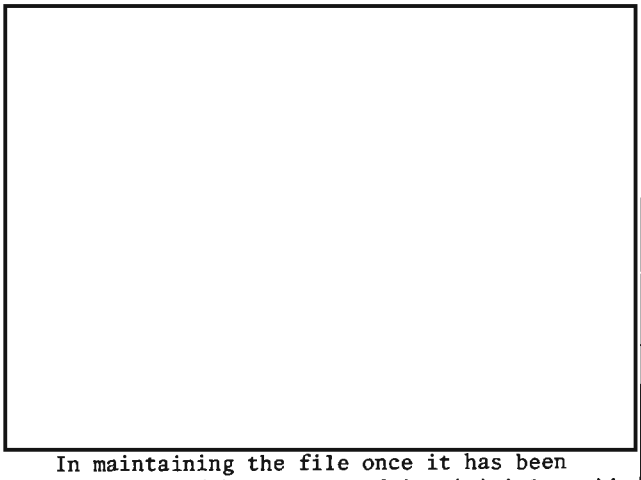
The attention of most computer specialists has centered on the tasks under heading *c*: the ways of looking up, rearranging, manipulating, and displaying data from an existing file. This is, admittedly, the most interesting area conceptually, and provides the most scope for inventiveness in software design and programming techniques.

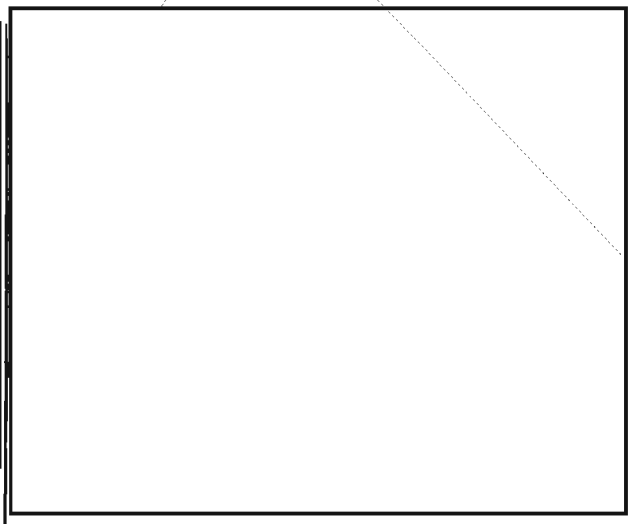
Unfortunately, however, at least in my experience, the real problems involved in the design of natural-language working aids revolve around areas *a* and *b*, and especially area *a*: the initial building of the glossary file. The querying or displaying of data from a completed file has rarely presented any problems in the CAMINO files or any other mechanized working aids I have worked with. [redacted]

[redacted]

[redacted]

EO 1.4.(c)
P.L. 86-36

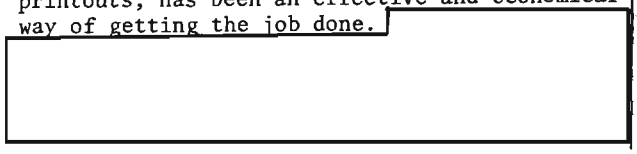




In maintaining the file once it has been established and has completed its initial rapid growth, the file sponsor must see to it that the file continues to be responsive to all his users and their needs, in spite of frequent reorganizations of Agency personnel, changes in missions, and new developments in the external world of international events. He must make a continuing effort to collect contributions of new terms, and solicit constant feedback from all file users, while searching for new sources of data that should be added to the file.

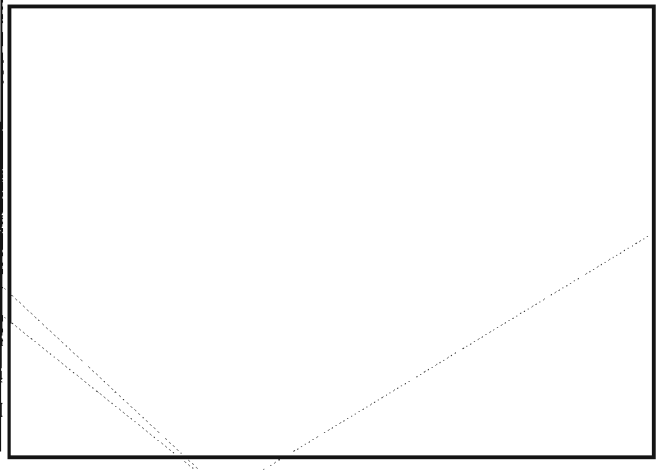
Now let's shift our attention to the question of how the tasks outlined above can best be accomplished at present and in the near future and why. To most computer-oriented managers, it seems obvious to the point of triviality that each sponsor who needs a mechanized language aid should do all the work himself, preferably at "a terminal" (unspecified). If he cannot do all the work himself, for whatever reason, he should get "somebody else" (also unspecified) in his own organization to do it for him. The hypothetical manager we are quoting sees no difficulty in any of this, and considers the problem solved by his advice.

In certain specific contexts, where on-line terminals have already (for a variety of historical or practical reasons) become the primary or only way of accessing and manipulating all data for a problem, it makes excellent sense to put language aids on line too. In these cases [redacted] the needs of one specific set of users are being amply met by a complete system design that includes all the working aids they require. There are still, however, many scattered users who are, and may remain for some time, outside of these advanced projects. For them a generalized or standardized conventional file-maintenance procedure, involving periodic updating and reissue of printouts, has been an effective and economical way of getting the job done.



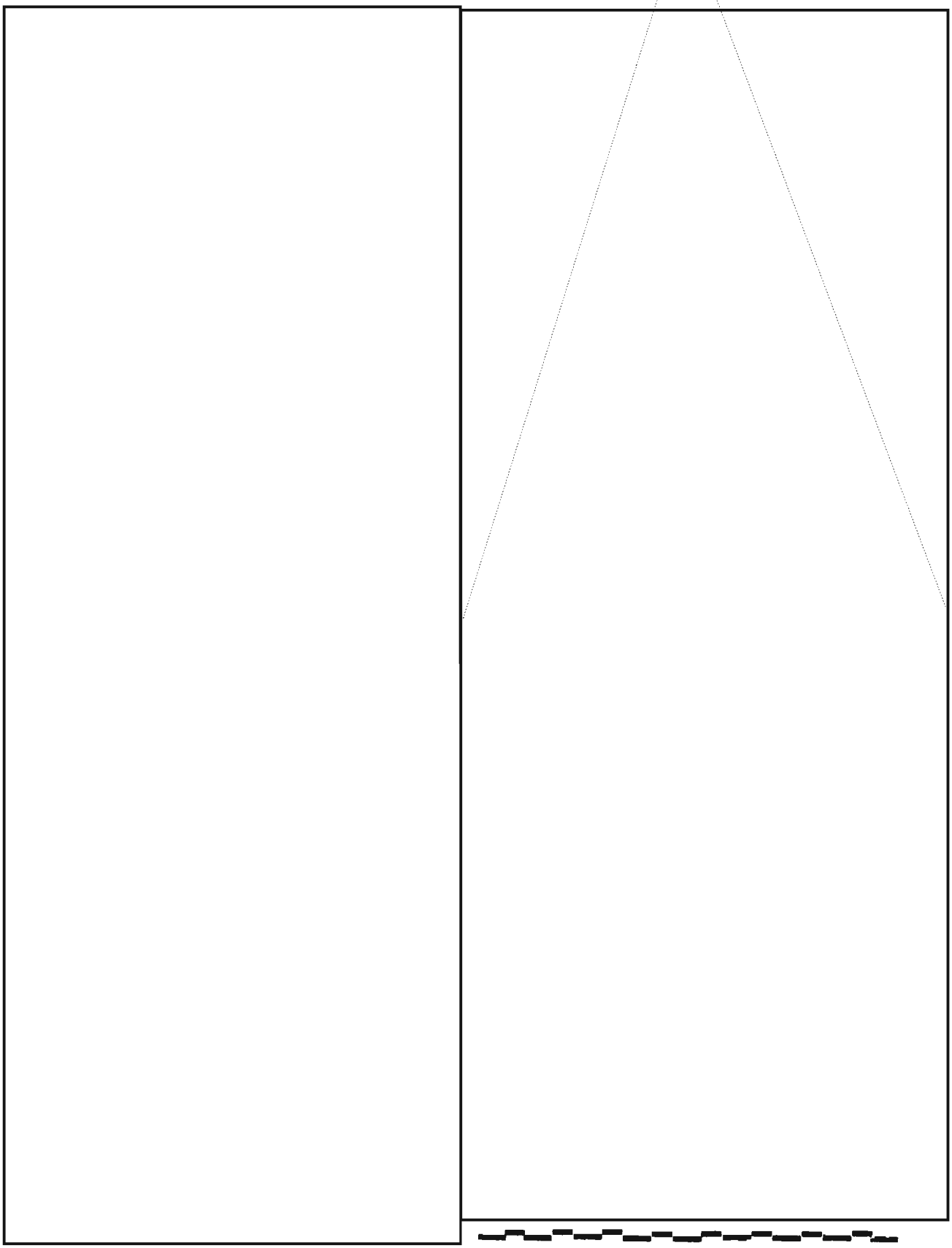
Faced with all these immediate pressures, the senior linguist has little or no time, energy, or peace of mind left over to work on the dictionary at all, let alone do the extra initial work required to mechanize it. He certainly is not usually able to spend hours of his time sitting at a terminal (which he is not routinely using for any other purpose), keying in his own data or making line-by-line changes. Finding someone else to do these things within his own organization is also apt to be very difficult in practice. Everyone else who is qualified is just as busy, and just as unable to take time to sit at a console for hours on end, concentrating on the dictionary. Helpers who are not qualified almost invariably cause far more problems than they solve.

Our hypothetical manager, whom we have been quoting as a Devil's advocate, has an immediate reply, by which he again seeks to define away the awkward resource-allocation problem: "If the sponsor organization doesn't need the dictionary badly enough to assign the necessary resources to it, obviously it isn't really needed at all, so we can forget it." Again, I cannot accept this representation of the situation, however useful it may be in simplifying matters for the manager.



EO 1.4.(c)
P.L. 86-36

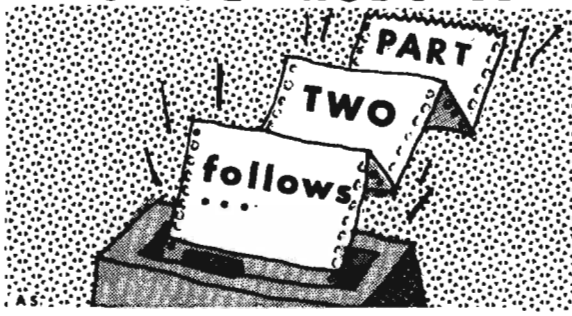
~~CONFIDENTIAL~~



DOCID: 4009738

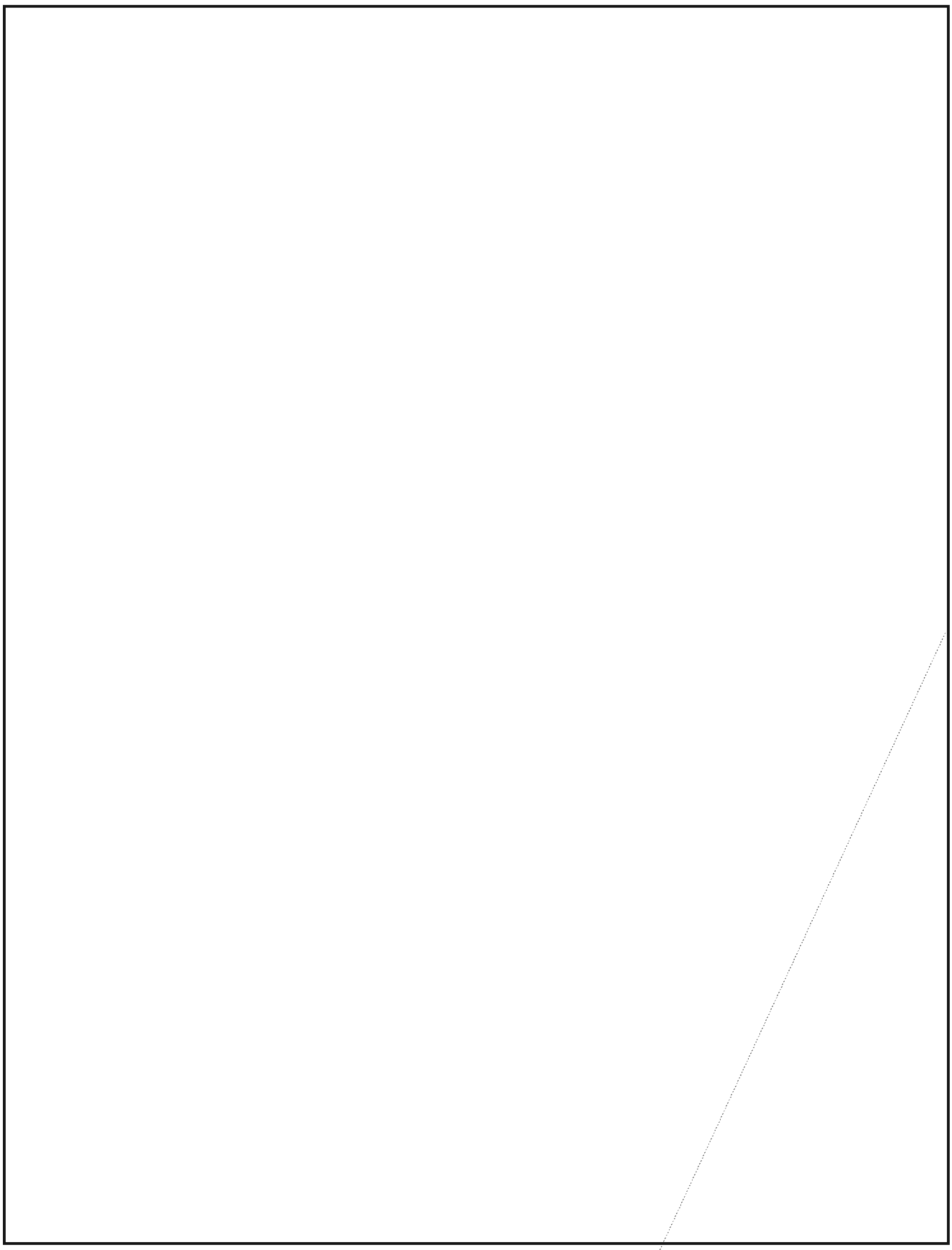
EO 1.4.(c)
P.L. 86-36

MACHINE-PRODUCED AIDS FOR THE LINGUIST

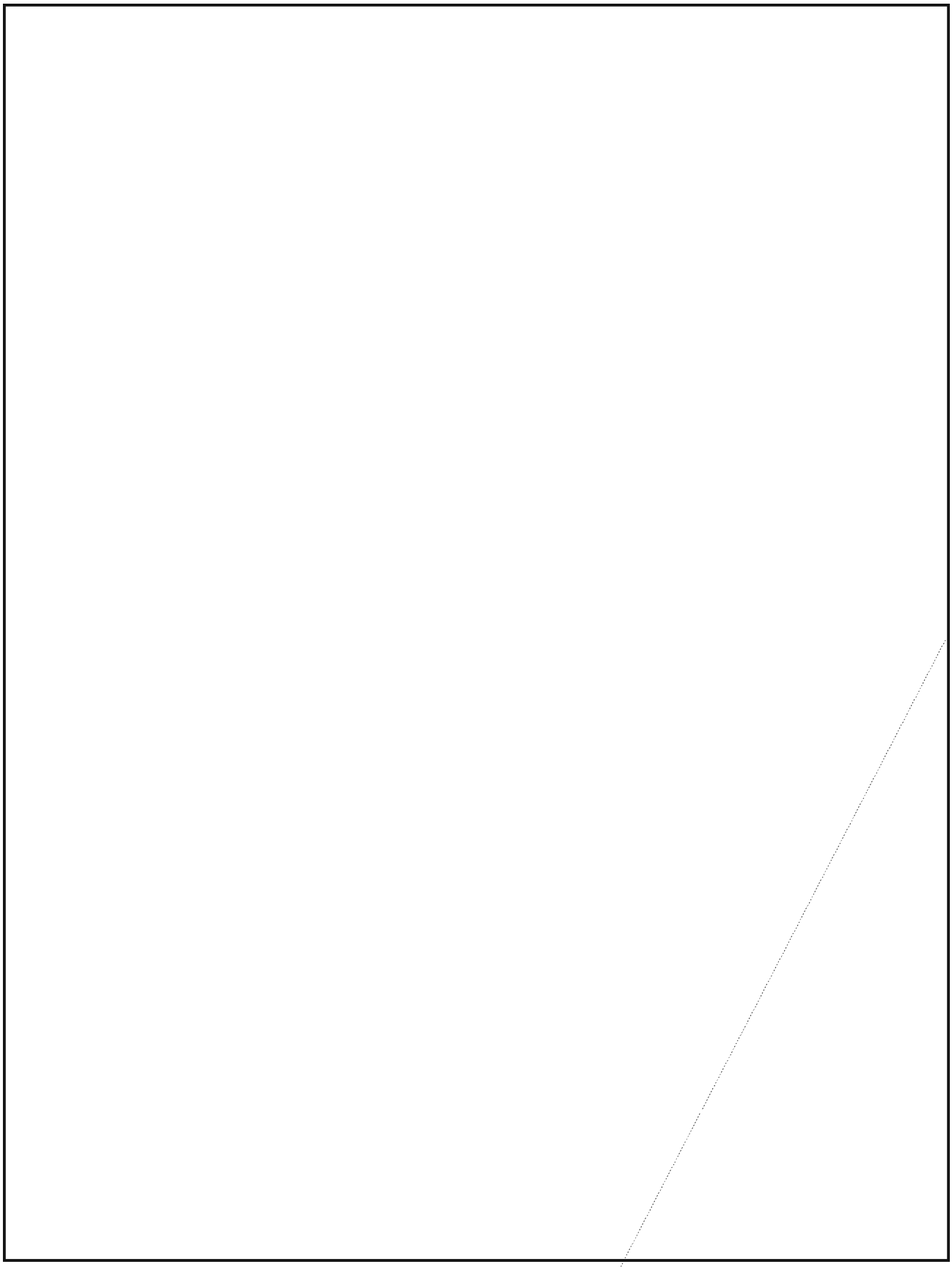


The following is the conclusion of an article which started in the September 1976 issue of CRYPTOLOG.

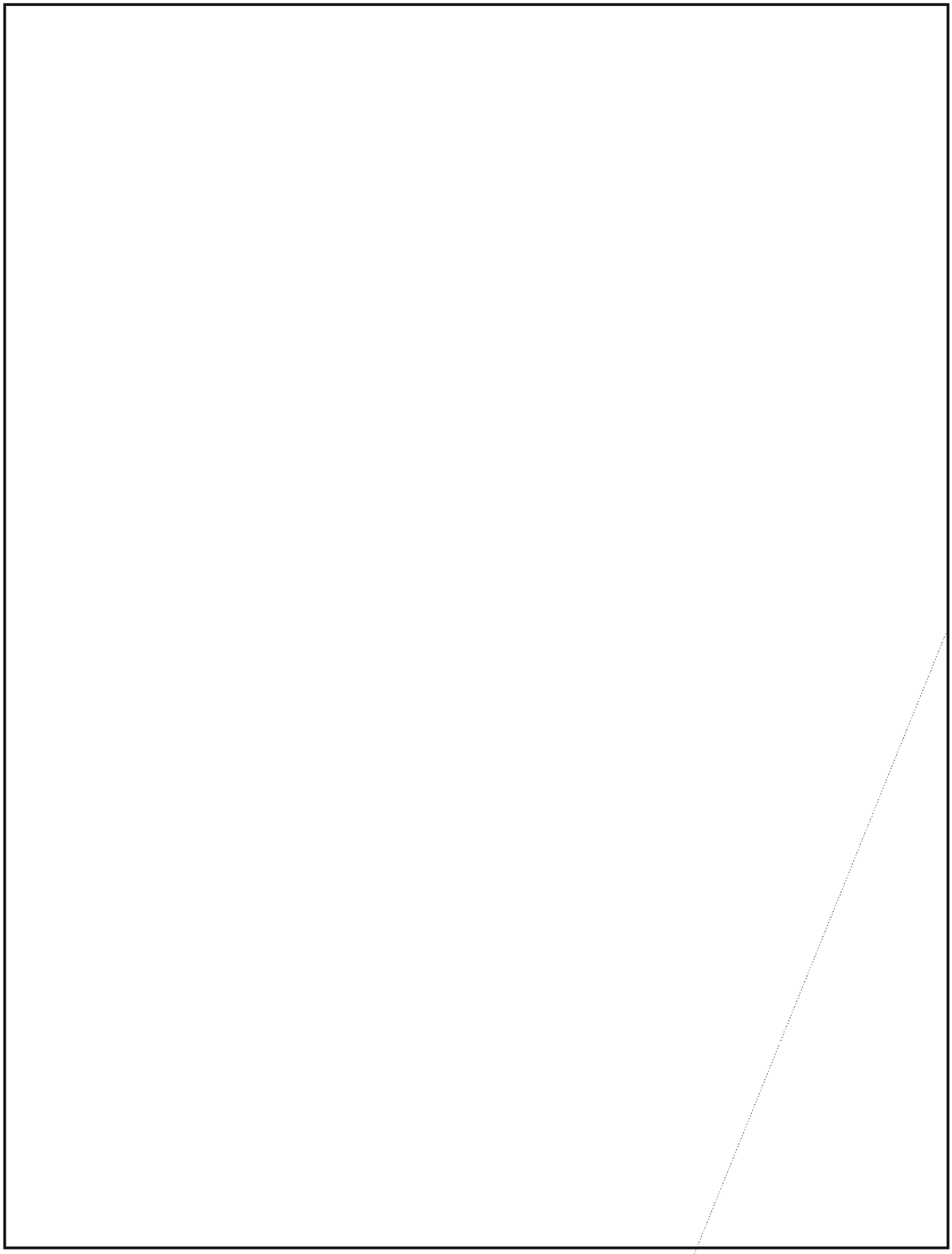
A. J. Salemme, P16



EO 1.4.(c)
P.L. 86-36

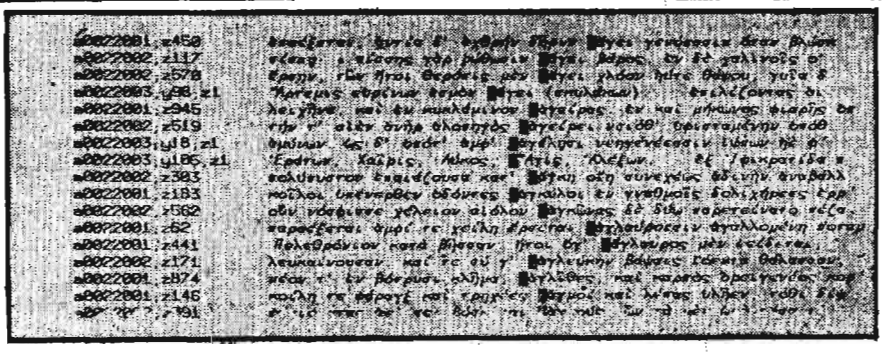


EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

DOCID: 4009738



Classic Use of Computers: Research in Greek

Research in the classics that once took months or even years can now be accomplished in minutes with the help of a computerized data bank of the classical Greek language. Eventually the system will store 90 million words to form the first thesaurus of the language.

The ability of the computer system to provide basic research material quickly and efficiently frees the scholar of the task and allows him to devote more time to analytical work, according to Prof. Theodore Brunner, director of the Thesaurus Linguae Graecae project at the University of California at Irvine.

The traditional method of accumulating information about a specific author's writing, or all the writings of a given period, would involve scholars locating and reading texts, analyzing word use, recording each word with its sentence context on a separate index card and filing the cards alphabetically. The process is usually long and tedious, according to Dr. Brunner.

With the Irvine system, Greek texts are key-punched and recorded on magnetic tapes in a special code. The tapes are scanned by computers programmed to store and process the information into word use and meaning. The computers can retrieve specific material and provide printouts in both Greek and English which scholars can use for compiling lexicons and key-word-in-context concordances.

Dr. Brunner says the computer requires about two minutes to find all the uses of a given word in the half-million words of Plato's writings. The old method would take a scholar several years to do the same research, Dr. Brunner says.

So far the project, begun in 1972, has entered 18.5 million Greek words on tape, and the data bank is being used by scholars in such fields as literature, philology, linguistics, history and philosophy.

New York Times,
5 April 1976

(UNCLASSIFIED)

EO 1.4.(c)
P.L. 86-36

DOCID: 4009738

(UNCLASSIFIED)

To the Editor, CRYPTOLOG:

[redacted] article, "Integrated Analysts for Asia: A Cohesive Approach" (CRYPTOLOG, August 1976), virtually admits to sex discrimination in the placement of integrated analysts. While I am perfectly willing to admit to the desirability of "empathy toward the Asian attitude," I am also only too well aware of the large number of women whose lack of promotion has been explained by "but the male candidate has had an overseas tour." Does B Group need reminding that Agency policy <u>forbids</u> them to deny women desirable overseas positions on the basis of sex? I think [redacted] owes CRYPTOLOG readers an explanation.

"Firebrand"

P.S. I'm surprised you let him print that!

<u>Editor's reply:</u>

The Publisher and Editorial Board very rarely advise an author to modify his or her statements on the basis of inappropriateness. We feel that, inasmuch as the views expressed in each article are the author's own (and do not have to be "coordinated" or "cleared" with anyone else at any level, unless the author so desires), every author has the right to express his or her technical opinion, however controversial (or even however half-baked) it might seem to be. It is not true, as people sometimes say around the CRYPTOLOG office, that "CRYPTOLOG will print *anything*!" CRYPTOLOG will print anything that has operational relevance. If any reader disagrees with the author's views, that reader is welcome to contribute a counterview (anonymously, if desired), and that counterview will be printed, so long as it contains a valid statement, rather than just *ad-hominem* (should we also include *ad-feminam?*) invective. So, in effect, I'm surprised that *you're* surprised that CRYPTOLOG "let him" print it.

Ed.

<u>Speaking of "his or her"</u> . . .

To the Editor, CRYPTOLOG:

I have admired the style of CRYPTOLOG since the first issue. The quality of the English therein has been a delight to its readers and an example to all of us who write. But I must protest the use of two particular pronouns in one recent article.

Is the use of "he/she" and "his/her" to refer to a [redacted] operator really necessary? It seems to me that it condescends. It is a repeated reminder of something we accept -- the

To the Editor, CRYPTOLOG:

Having spent a year as the Operations Officer of the 6924th Security Squadron, Danang, RVN, I was most interested in the excellent article on IRONHORSE which appeared in the October 1975 issue ("IRONHORSE: A Tactical SIGINT System," [redacted]). There was, however, one small but significant error. The author's statement that the Marine bomb dump explosion destroyed the operations facility in April 1969 is correct. However, the system was back on the air on 21 July 1969, not 1970 as the article states. I realize that three months to build an operations building, clean up the entire IRONHORSE System, install the intercept positions and IRONHORSE seem impossible. Because of the outstanding cooperation received from the Commander, 7th Air Force; Director, NSA; Commander, 366th TFW, Danang, RVN; and the 6922nd Security Group, and, most importantly, the cooperation and long hours of the REDHORSE construction units; the USAFSS E and I team and the Operations, Supply, Communications and Maintenance personnel of the 6924th Security Squadron, such a feat not only became possible but was accomplished with smoothness and completeness in less than 60 days. The decision to rebuild the Operations facility at Danang was not received until late May 1969. Such an accomplishment further reflects what was alluded to in other areas of the same October 1975 issue as a certain sense of pride and professionalism in doing a job well no matter what the circumstances.

[redacted] USAF,
[redacted]

~~(SECRET -- CCO)~~

[redacted]

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

DOCID: 4009738

operator might be a man or a woman. Those who do not accept this will certainly not be influenced by seeing these words in print. In fact, these readers will probably be far more annoyed than I am.

If such usage is required by agency or governmental guidelines, then I am alarmed. If not, then let us revert to the use of masculine pronouns to refer to a person of unspecified gender.

G43

Editor's reply:

As far as I know, there are no such agency or governmental guidelines. As far as CRYPTOLOG editorial policy is concerned, we do not add "or her" unless the author himself or herself includes those words in his (need I add "or her"?) article. Personally, I feel that *excessive* use of "his or her" draws the reader's attention away from *what* is being said to *how* it is being said. I would hope that most CRYPTOLOG readers do read the magazine for *what* its authors can communicate to them. Unfortunately, the English language itself is flawed. People can *suggest* all-purpose pronouns that refer to either males or females, but that doesn't mean that everyone who speaks English will accept them. Even if one uses the graphic convention "s/he," how would one pronounce it? Moreover, the suggested conventions aren't really that all-inclusive anyway. A letter to the editor of *The Wall Street Journal* last year suggested that the all-inclusive pronoun should include not only "he" and "she" but also the third-person *inanimate* pronoun: it should mean "he or she or it." The writer suggested the word "h'orsh'it." I think he's on the right track.

Ed.

(UNCLASSIFIED)

FIND ANY TYPOS?

Occasionally the only comment the Editor hears about what he thought to be a particularly informative issue of CRYPTOLOG is, "There's a typo on page 13!" Therefore he was pleased to see, in a local Maine-coast newspaper recently, the nice way in which a fellow editor handles the situation.

WORK QUOTAS FOR SOVIET TRANSLATORS

P.L. 86-36

G5

Author's note: The following information is derived from an article in *The ATA Chronicle* which, in turn, was extracted from *Scientific and Technical Translations in Soviet Industry*, by I. P. Smirnov.

The All-Union Translation Center for Scientific-Technical Literature and Documentation in Moscow employs approximately 5000 full-time translators and several times that many part-timers. These translators, as all production workers in the Soviet Union, have work quotas to fill. In filling these quotas, the translator must read the manuscript before it is retyped, correct the retyped version, proofread the corrections, and closely scan the corrections made by the scientific editor. No allowance is made for difficulty of the text.

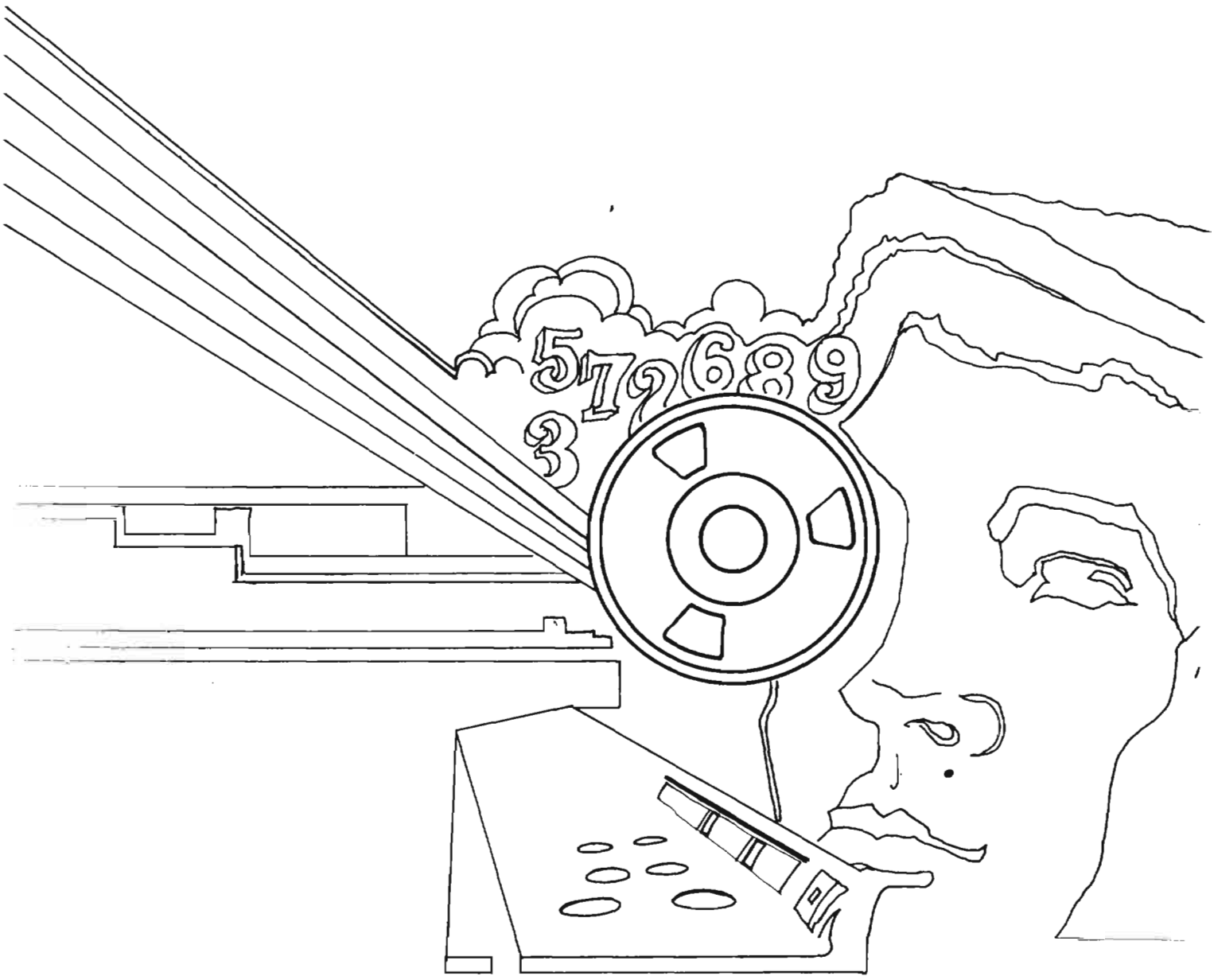
And what are these quotas? Languages are divided into three classes, with a different quota in number of words per month to be translated for each class. The word count is made from the target language (usually Russian) and not from the source language, thus penalizing the translators -- e. g., no definite and indefinite articles in the count.

Quota (words per month)	*Source language*
24,000-32,000	English, German, French, Spanish, Italian, or a Slavic language
16,000-24,000	Hungarian, Finnish, Dutch, Portuguese, Albanian, Greek, Romanian, or a Scandinavian language
14,000-20,000	An Asian language

If the translator dictates -- rather than writes or types -- the translation, the quota is increased by 8000 words. Any volunteers for work norms?

(UNCLASSIFIED)

Pl-Oct 76-S3-24865


5726893

DOCID: 4019642

P.L. 86-36

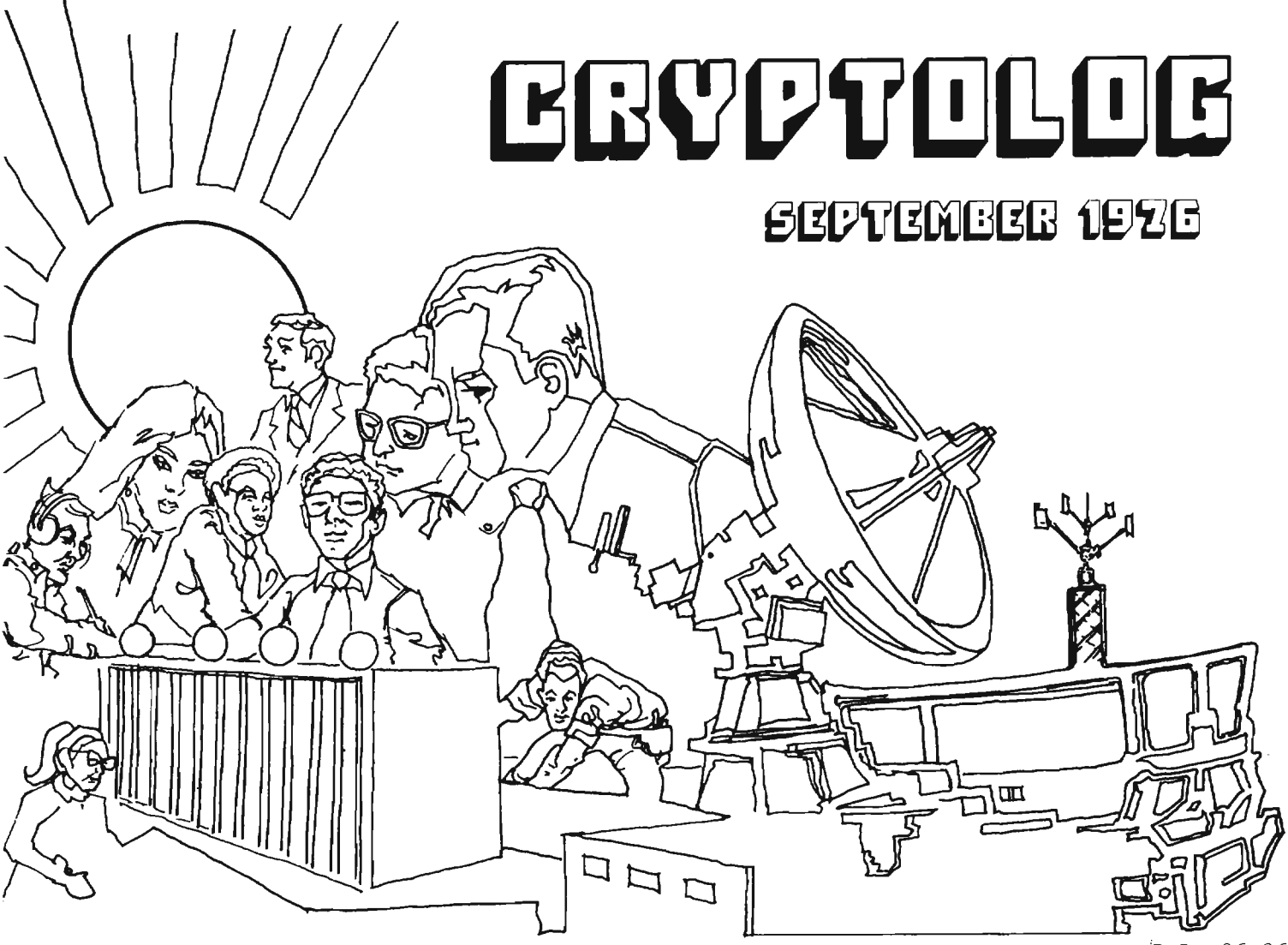
~~TOP SECRET~~

[redacted]

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

SEPTEMBER 1976



P.L. 86-36

THE BIBLE AND THE WASHINGTON MONUMENT.....Don Snow.....1
TIPS IS STILL ALIVE AND WELL!.....[redacted].....3
FOREIGN PUBLICATIONS PROCUREMENT PROGRAM..[redacted].....6
IS THERE LIFE AFTER CERTIFICATION?.....John J. Mollick.....9
ANOTHER CIPHER BY. . . ..William Meyer.....11
MORE COMMENTS ON THE AG-22/IATS QUESTION...[redacted].....12
AWARDS IN 1976 CMI AND CLA ESSAY CONTESTS.....14
SEMANTIC VOIDS: DON'T SHOOT THE TRANSLATOR..[redacted].....15
MACHINE-PRODUCED AIDS FOR THE LINGUIST.....A. J. Salemme.....17
LANGUAGE IN THE NEWS.....20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA and CIA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019642

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. III, No. 9 SEPTEMBER 1976

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief..... Arthur J. Salemme (5642s)
Collection..... [redacted] (8955s)
Cryptanalysis..... [redacted] (8025s)
Language..... Emery W. Tetrault (5236s)
Machine Support..... [redacted] (3321s)
Mathematics..... Reed Dawson (3957s)
Special Research..... Vera R. Filby (7119s)
Traffic Analysis..... Frederic O. Mason, Jr. (4142s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4019642

The Bible & the Washington MONUMENT

Don Snow, C5
DDO Micrographic Coordinator

For the past 5 years I have carried a microform version of the Bible in my wallet. It's all there -- Old and New Testament -- 1245 pages. And it's on a piece of film 2 inches square. I've found that it's an ideal sample to show people when I talk to them about *MICROGRAPHICS*. They're familiar with what the original book looks like, and they can hardly believe that it can be reduced to something as small as the above chip, and still be read. That, as the current saying goes, is what Micrographics is all about.

Let's use another example, which almost everyone is familiar with: Would you like to hold the Washington Monument in the palm of your hand? Easy -- just take a picture of it. Now, instead of a shaft of granite over 555 feet high (and weighing many tons), you have a photographically reduced version of it. Now it's one or 2 inches high, and you can take it out of *your* wallet any time you wish, instead of going down to the Mall to look at the "original."

Those two examples, then, explain what Micrographics can do. By means of quality photography, we can obtain greatly reduced versions of "things" -- printed matter or whatever -- and then make as many copies of the reduced version as we need.

Here in the Agency, more and more people are getting into Micrographics. For the most part, they deal with printed matter -- frequently in large volume. Computer print-outs (which often have to be retained and used for long periods), and a welter of reports, technical aids, as well as material received from other originators -- all of the above compound the "information storage and handling" problem.

So, in search of relief, they have entered the world of Micrographics. They have found that "source documents" (which is the term we use for material that has been typed or set in letterpress and then reproduced on paper, in however many copies as needed) can be converted to a suitable microform. Source-document conversion is handled by L23, Reprographics Division.

DOCID: 4019642

If, on the other hand, someone has many cabinets full of computer print-outs, Micrographics can help there. The Agency has (in C74) two Computer-Output-Microfilm (COM) recorders. A COM recorder uses a 7-level or 9-level magnetic tape as its input; the information on the tape goes through a mini-computer at the front end for formatting; then it is displayed on a cathode-ray tube, and a camera takes a picture of the complete display. The process is then repeated, until every "page" of information has become a "frame" on the film. The output film can be 16mm or 35 mm film, or 105mm microfiche.

The advantage of COM lies not only in its speed (30,000 to 120,000 characters per *second*) but in the compaction of the information on the output film. For NSA's Family Day I had an exhibit which included: a computer tape of unclassified information; a print-out of the tape which comprised over 2000 11x14" pages; and seven microfiches produced from the same tape by NSA's COM recorder.

Of course, when information is reduced so drastically, there has to be some way of enlarging it to its original dimensions, so that it can be read by the user. For this purpose we have the microform reader, a device which projects a page image onto a screen (usually at the front of the reader). It will remain there until the user manually moves to the next desired image.

If the user wishes to have a paper version of a given page image, he can get one with a reader/printer. This is much the same as a reader, but it has a roll of sensitized paper inside. The user looks at an image on the screen, presses a button, and in about 6 seconds the machine gives him a print of that image. Now the user can underline passages, scribble on the margin, or show that page to someone who doesn't have access to a reader. Naturally, the emphasis should be on the temporary need for a page-print; to make one or more prints with the idea of filing them away defeats the purpose of micrographics.

There are two main factors which explain why Micrographics is growing daily in importance -- not only at NSA, but throughout the intelligence community, throughout the government, and certainly in the world of business. First, people are realizing that they can convert much of their *dynamic* working materials to microform, rather than use the technology for old or *static* materials which they no longer need within arm's reach in the office.

Secondly, recent years have seen a great improvement in the quality of equipment. Standards are also being developed -- for reduction ratios, formatting, titling, etc. This becomes vital the moment one activity, say, in the intelligence community, begins to exchange material with another in microform. In-house, the Micrographics Systems Coordinating Office (N33/MISCO) has standardized on two models of microfiche readers, which comply with DoD reduction-ratio standards. MISCO also maintains an overview of all Agency micrographic applications, and represents NSA on a number of inter-Agency micrographics working groups and committees.

To sum up, Micrographics is one of the newer technologies to hit the work force. It's a space-saver; it's a money-saver; it's a time-saver. No longer confined to archival or "dead-storage" material, it is finding its place in the work pattern of more people every day.

Look around you. The file cabinets, the storage cabinets, even the drawers of your desk -- they're all chock-full of paper. Chances are that a lot of that paper could be converted to microform. And it would be just as usable.

Think about it. Then do something about it. Enter the world of Micrographics!

(UNCLASSIFIED)

Want a copy?
...of the 1974-1976 Cumulative Index?

As the end of Volume III approaches, it has become apparent that the cumulative cross-indexed listing of CRYPTOLOG articles and authors' names will be too long to print as part of the December issue. Therefore we shall print the index as a separate publication.

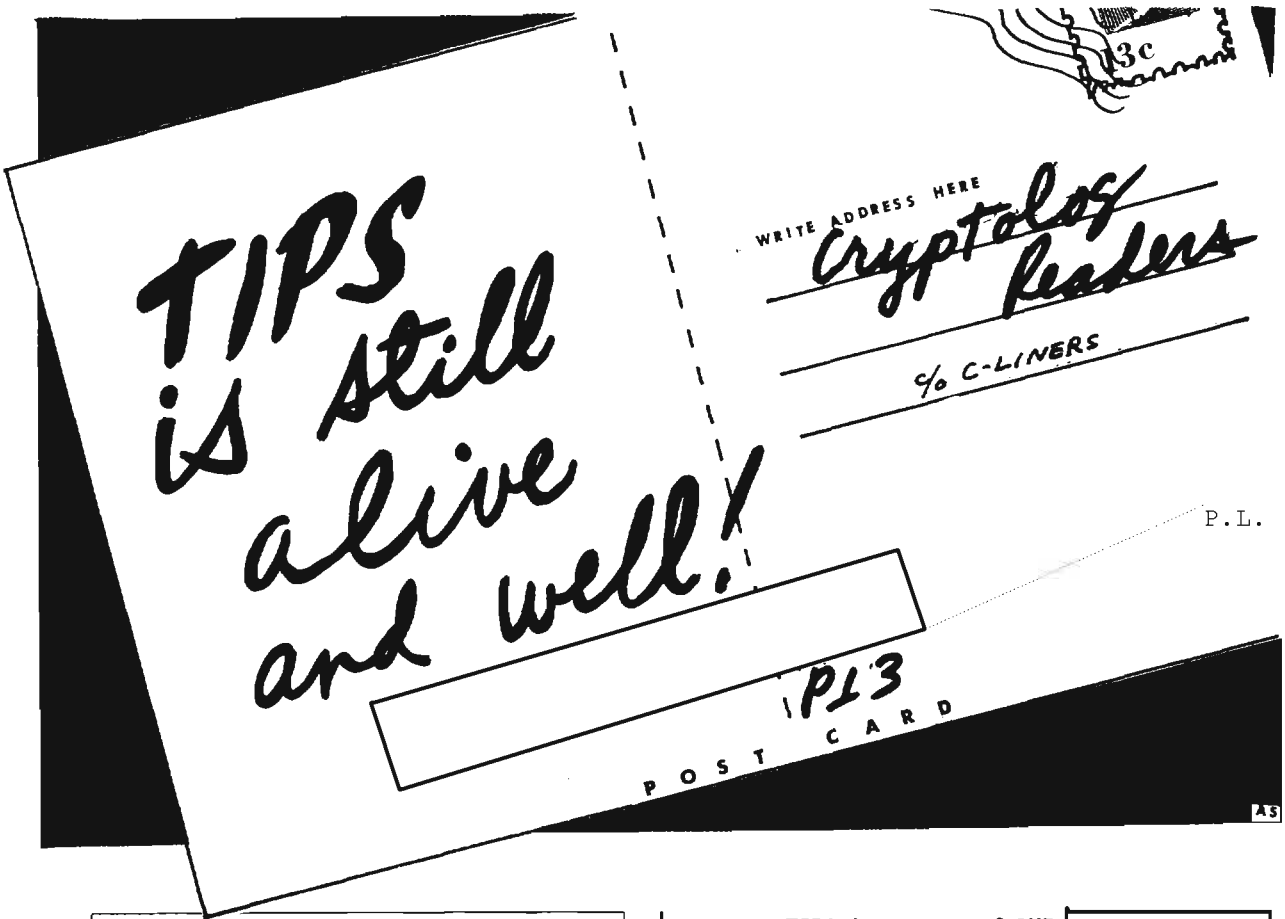
For reasons of economy, we shall print only the number of copies actually requested.

If you would like to receive a copy of the index, please fill out and mail the following form. (If you do not want to cut up this issue of CRYPTOLOG, just write "Index" and your name and organization on a plain piece of paper.)

TO: P1, CRYPTOLOG Please send ___ copy/copies of CRYPTOLOG Index to:

_____ (Name) _____ (Organization)

DOCID: 4019642



The following article in C-LINERS (C Group Machine Processing Information Bulletin), Vol. 3, No. 9, Issue No. 30, Spring 1976, is reprinted here with the kind permission of C-LINERS Editor David J. Williams.

As was the case with Mark Twain, reports you might have heard about the demise of TIPS -- NSA's Technical Information Processing System -- have undoubtedly been grossly exaggerated.

True, TIPS is showing signs of aging. After all, she has been around since the mid-Sixties. To some, such longevity should qualify her for some kind of geriatric support. To others, notably some folks in C11 (the Information Systems Division of C), the old girl is still very much alive. Admittedly, a young and more glamorous replacement is being sought. Nobody knows when this rival will be embodied (or "em-machined") but she is coming and plans are being made for her arrival.

At this stage in her career, then, one feels it would be a good time to record a few random thoughts about TIPS. A few words of background information may be in order for those not in the category of C Old-timers. First, a more or less official definition:

TIPS is a part of RYE, [redacted] The TIPS system encompasses the hardware devices, software executive routines, conventions, communications package, and data bases in support of the quick-turnaround, on-line, information storage and retrieval capability within RYE. (See Section 4, of forthcoming USSID 703, Technical Information Processing System (TIPS), for general information about this system.)

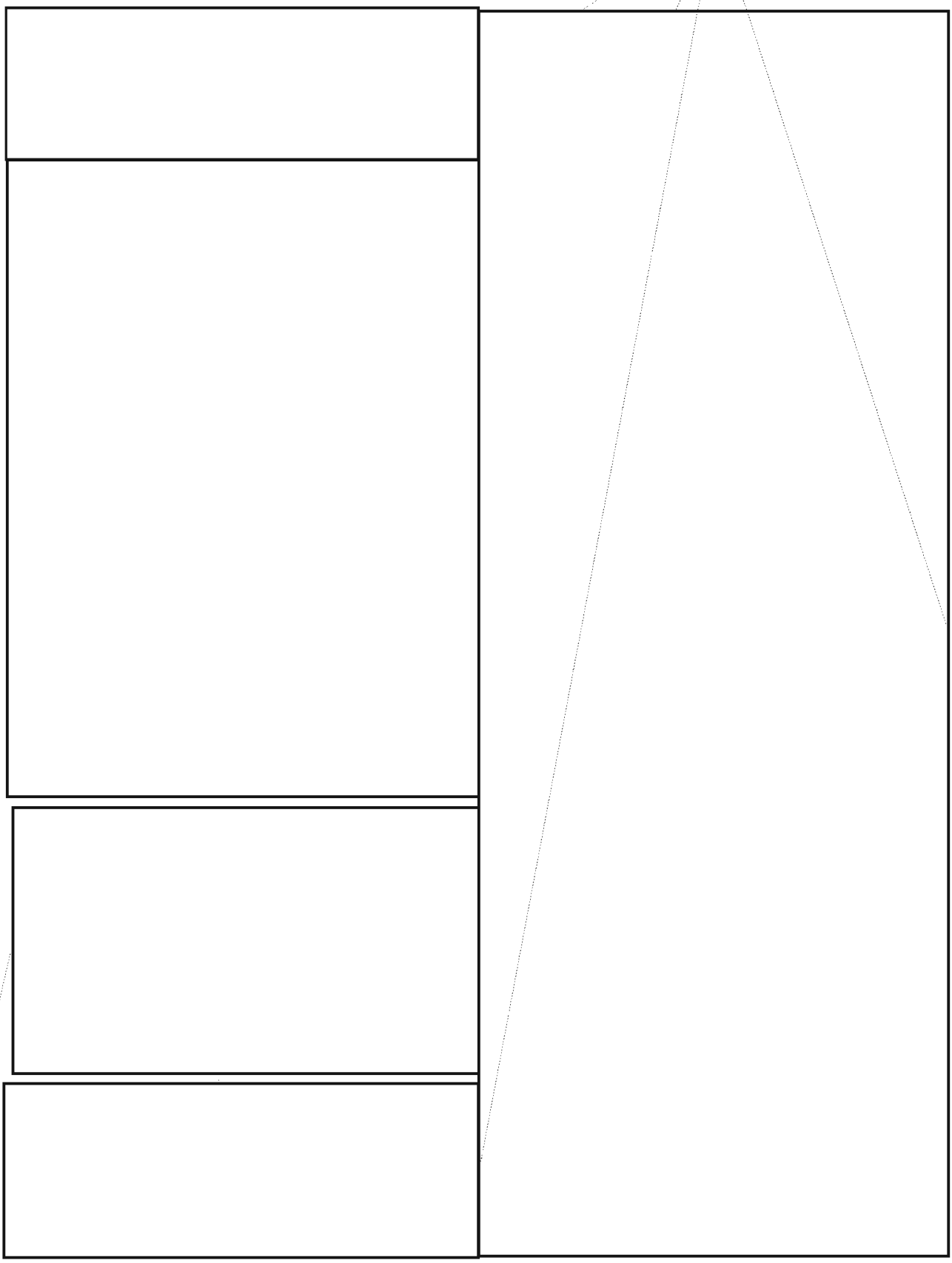
[redacted]

Chances are that, as a RYE user, you've already "interfaced" with the most common of these input devices, the lowly teletype. The manufacturer is the Teletype Corporation of America, and the most common terminal type (for RYE) is the ASR (Automatic Send and Receive)

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

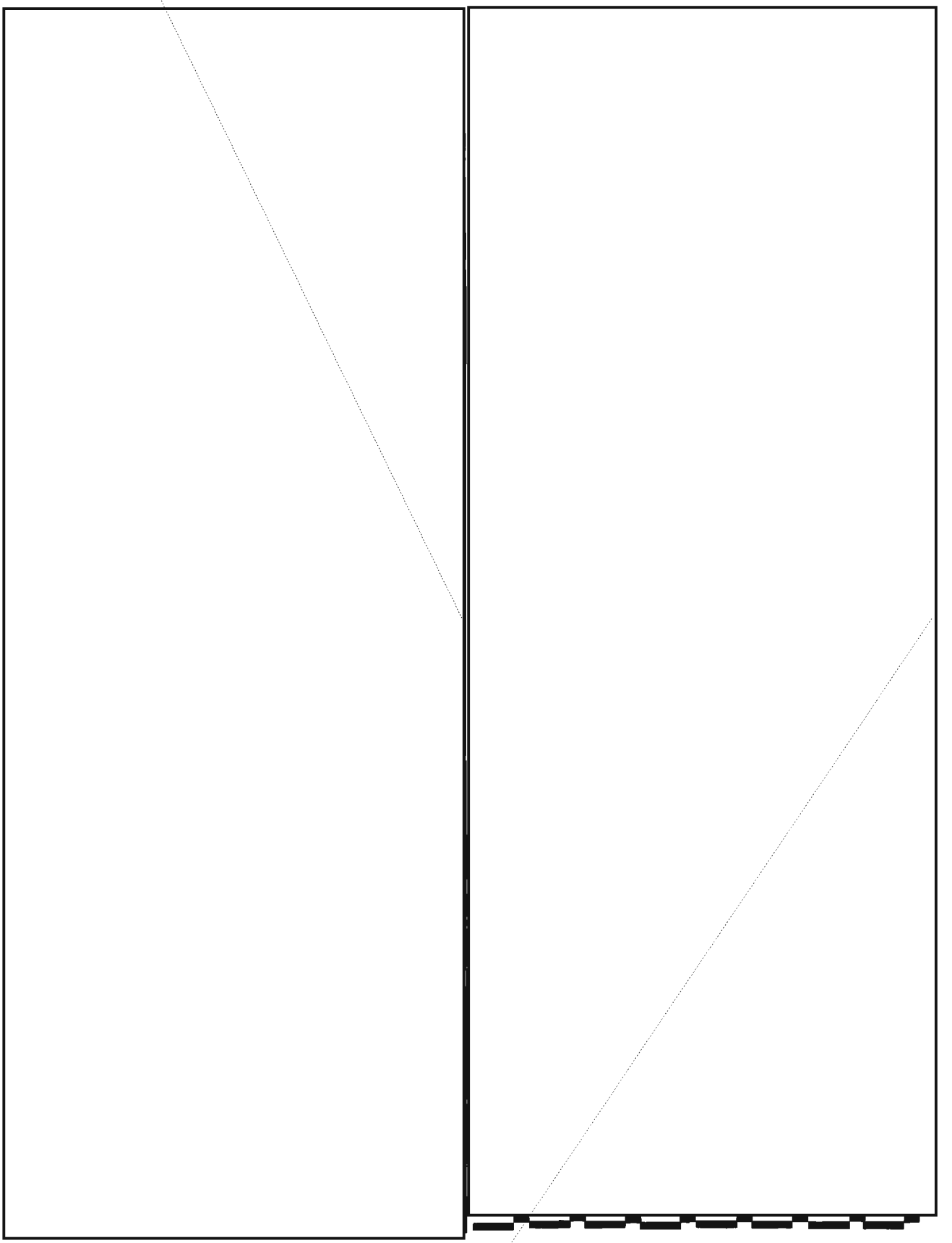
EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
EO 1.4.(d)
OGA
P.L. 86-36

DOCID: 4019642

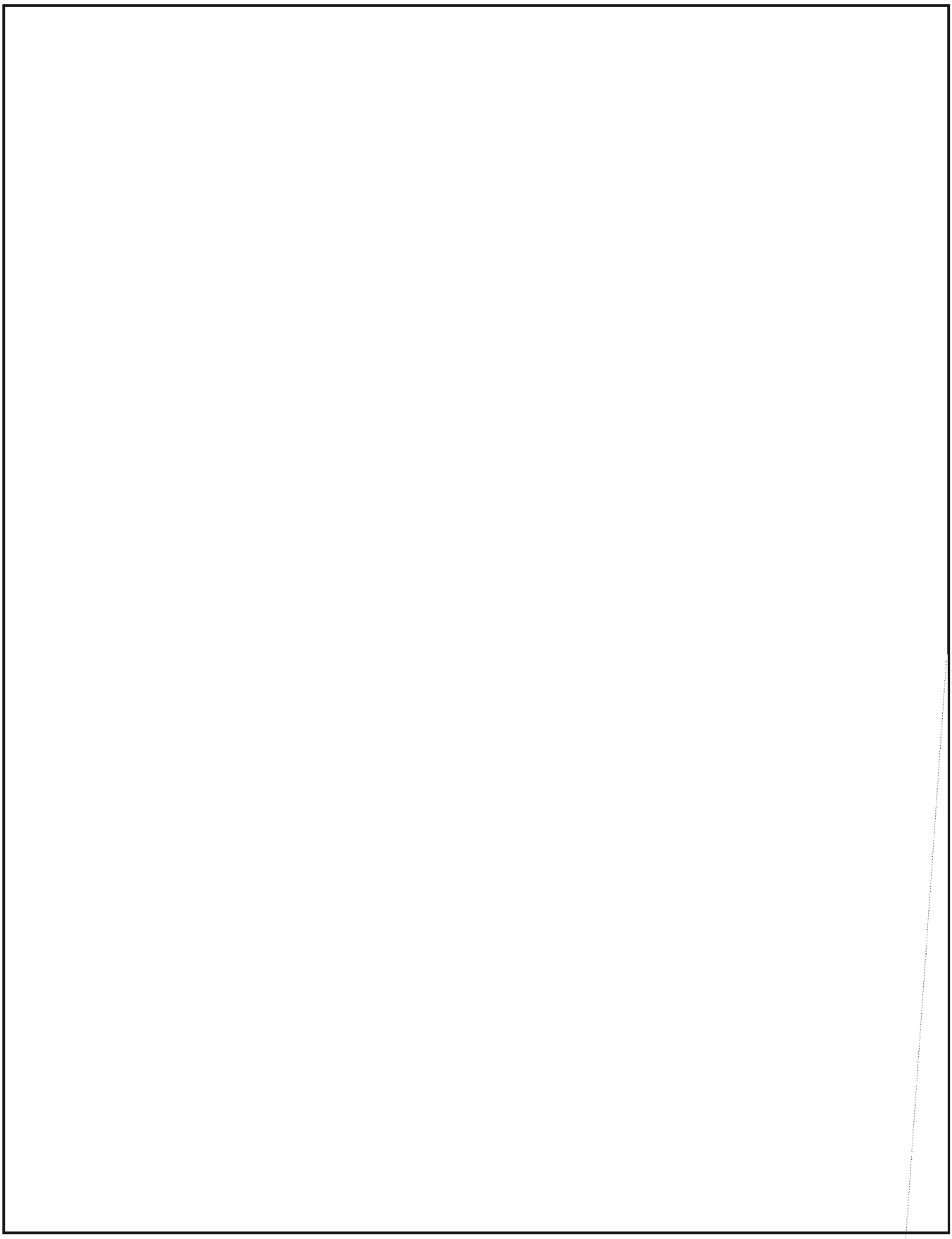
EO 1.4.(c)
OGA
P.L. 86-36



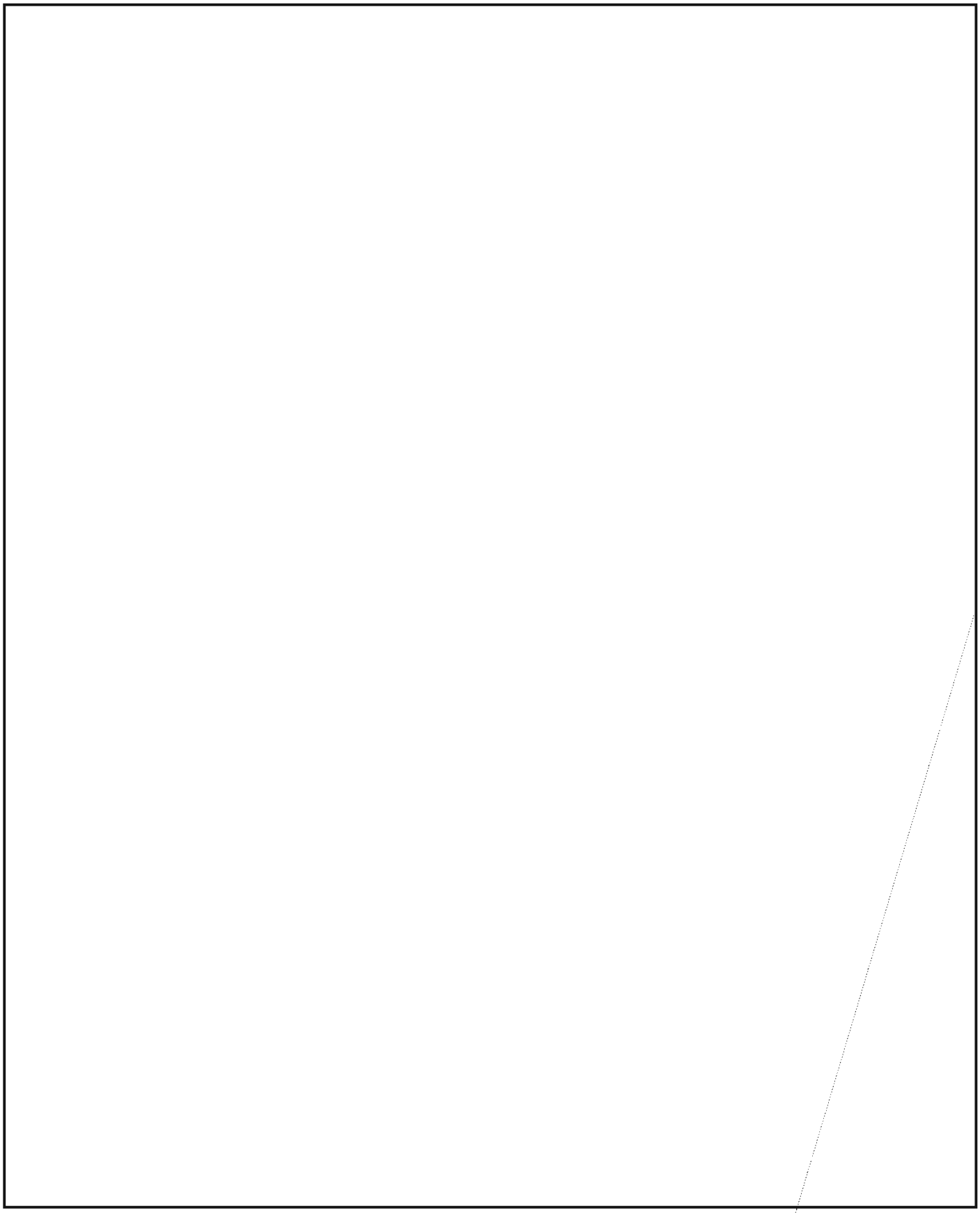
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

OGA

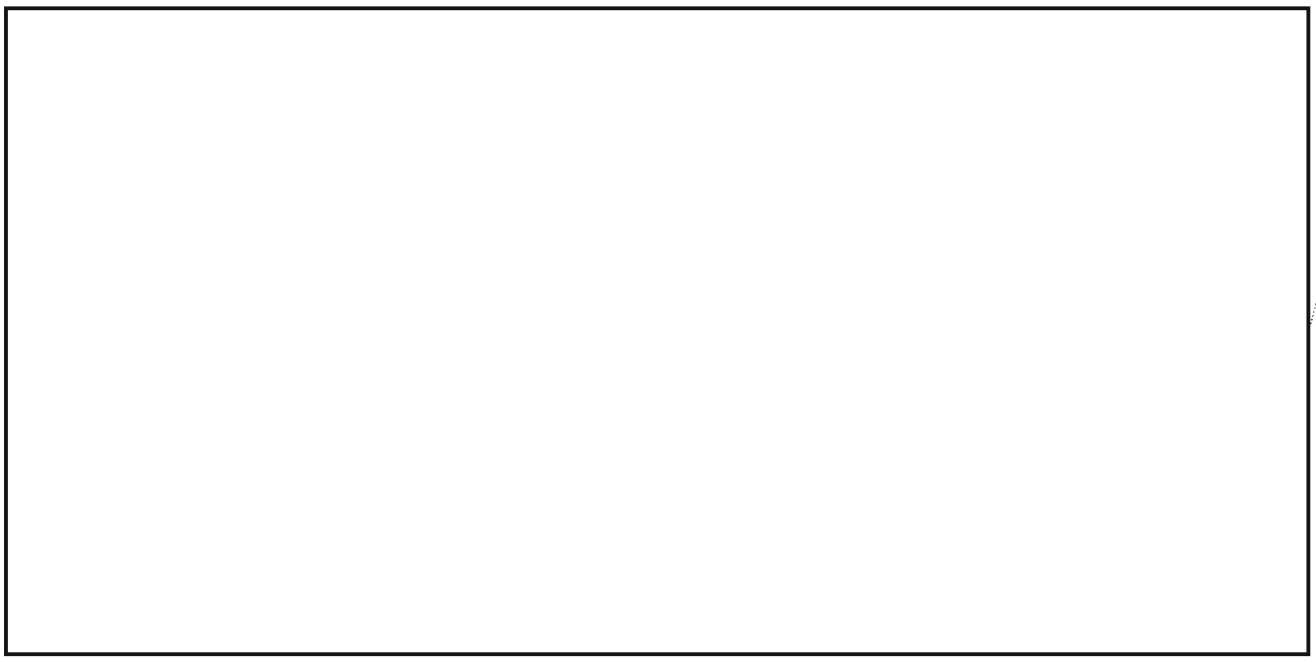
DOCID: 4019642



OGA



DOCID: 4019642



OGA

IS THERE LIFE AFTER CERTIFICATION?

John J. Mollick, B24 (UNCLASSIFIED)

What happens to the linguist after he or she (from now on, for convenience, let's just say "he") has become certified as a level-III professional linguist? Does he stay at that level forever? Or does he continue to develop his language skills? Does he strive for something *better than* level-III proficiency? If he does, what is it that he's striving for? An as yet undefined level-*IV* proficiency? Or for the unofficial title of "superlinguist," "language consultant," "language whiz," or some other informal name that indicates that he is recognized, among certified linguists, as someone who *really* knows the foreign language thoroughly? When and how does a person get that recognition from his peers? Can criteria be established for making that recognition *formal*, with some kind of *official* title to accompany it? These are only some of the questions that are being discussed by an ad-hoc committee that was recently empowered to advise the Language Career Panel on problems of developing the skills of the Agency's certified linguists.

It seemed reasonable to us committee members to ask certified linguists themselves for their opinions about matters involving them, on which we would be making recommendations. Therefore, as one member of the committee, I decided to take an informal poll [redacted]

The poll was very informal. I improvised casually and typed sloppily (personally, I find it easier to be a level-III linguist than a level-II typist) a questionnaire that I sent to 50 people I know [redacted] As of this writing (June 1976) I have received 18 replies. No one would dare to state that the opinions [redacted] necessarily represent the feelings of most of the Agency's linguists. I do think, however, that their opinions are enlightening. Therefore I am summarizing their replies here, in order to demonstrate how at least a representative handful of the Agency's linguists feel about their chosen field of professionalization and in order to invite other linguists to share their ideas with me. I will welcome any additional views and will channel them into the committee's discussions. In that way we can be assured that the suggestions we submit to the Language Career Panel will take into consideration the input provided by linguists themselves. P.L. 86-36

Of the linguists who replied to the original questionnaire, 14 had been certified; 3 hoped to be in the future. Of those certified, 6 felt that they could easily pass [redacted] language PQE (Professional Qualification Examination); 8 had doubts.

In response to the question of how they maintain their language proficiency, 14 stated that they rely on the work environment; 8 also do some studying at home; only 3 rely on in-house training. Seven feel that additional language training would aid them substantially in doing better work in their present jobs; 11 did not feel that way. Furthermore, 9 feel that their language abilities are equal to the demands of

DOCID: 4019642

the job; 2 feel undertrained; 7 feel overtrained.

[redacted]

Regarding their future in the language field, 17 linguists said that they greatly enjoy language work. Sixteen gave qualified affirmative answers when asked if they *desired* to remain in language-oriented jobs. Most of the qualifications concerned the need for career progression, recognition, and variety in work. Several individuals flatly stated that they believe one can remain a linguist only if he is willing to sacrifice the financial rewards, since "management is the route to take for higher grade." Not surprisingly, then, only about half the linguists felt that they would stay in the language field.

Thirteen linguists were against the formal establishment of a level IV for language checkers and consultants; only 4 favored it. Objections generally concerned the following:

- The experts have long been identified and already are checkers and language consultants. Therefore the establishment of additional criteria and testing will just waste more time both on the part of those administering the tests and those linguists who would be forced into "nonproductive study at the expense of the job, merely to reach another meaningless milestone";
- After establishment of level IV, linguists would feel pressured to reach that level. Eventually the standards would be dropped to accommodate linguists who just cannot meet high standards. Then we would find ourselves in a situation similar to that which currently exists -- except that there would be a number of level-IV linguists and people would be discussing the desirability of establishing level V for "the *real* experts."

The above objections apparently would be mollified if the attainment of level IV were limited to the few truly superior linguists, and if their excellence were adequately recognized and rewarded. Those favoring the level IV seemed to confirm this. They suggested that level IV would give career linguists "something to shoot for," but that it would be worthwhile only if it promised an opportunity for upper-level grade advancement and if the criteria were kept sufficiently stringent, in order to limit the level-IV ranks to a very small handful of genuine experts.

Only one person favored the "grandpersoning in" of "recognized experts." All others were adamantly against any such "free rides." However, several asked the rhetorical question, "Who, then, creates and checks the tests?" Some doubt was expressed that an effective level-IV test could indeed be created. It was indicated that perhaps there would be a need for criteria other than formal testing if a level IV were to be established. One linguist suggested an "open-ended PQE test" in which the highest scores would be selected for the few level-IV billets.

Fourteen linguists stated that they feel periodic rotations into other language jobs are advisable. Most emphasized that rotations should be optional, rather than mandatory. Only six would consider crosstraining from [redacted] into another language.

P.L. 86-36

The questions that elicited the strongest comments were those asking for proposals on how to increase the linguists' satisfaction with their jobs and improve their working lives. For the most part, the diverse answers can be divided into the following categories:

- *Recognition*

  Most linguists specified that they want recognition above all else. A number felt that lack of recognition of the worth of linguists is evident in the inability of Agency linguists to compete successfully with managers or others for promotion. Despite almost unanimous complaints about lack of recognition, few specific suggestions were made regarding how that recognition should be shown, except for boosting pride of authorship by putting the linguists' or analysts' names or numbers on products to which they have contributed. Most linguists stated in one way or another that they feel management does not recognize the significant role that the linguist plays. This desire for recognition leads logically to the next desire.

- *Pay*

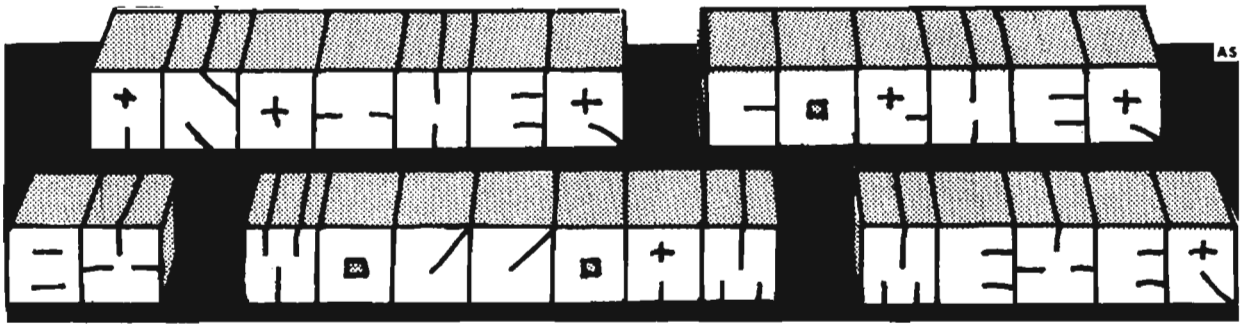
  Again, there was almost complete unanimity that people cannot advance far enough in the language field. The theme "eliminate the need for linguists to leave the language field in order to progress beyond the GG-12/GG-13 level" was a common denominator in the linguists' replies. One individual suggested, "Senior technicians should be equal to middle and upper level managers. The work is equally demanding; the output is as important to the mission of NSA." Another suggested that there is no valid reason why a "GG-12 linguist cannot work for a GG-9 manager."

- *Training*

  Many linguists recognized the need for language maintenance and for continual training. Some suggested occasional sabbaticals to local universities both for training and as a sign of recognition. Several suggested the need for additional overseas training in the "native environment." Few felt

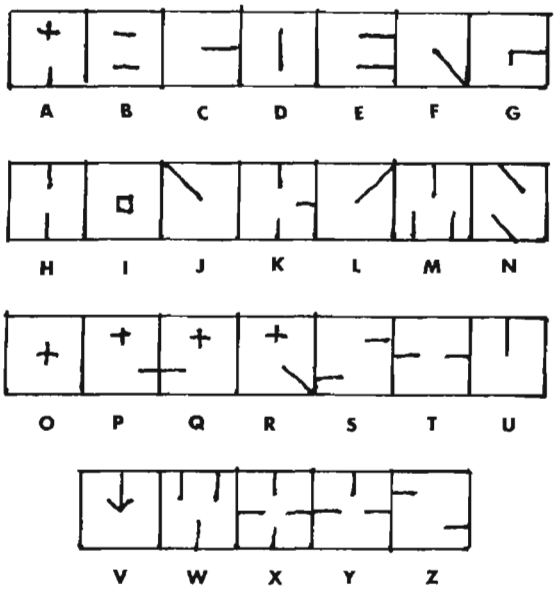
(*Continued on page 14*)

DOCID: 4019642

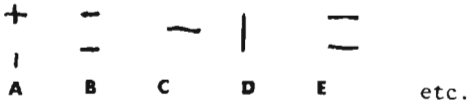


While taking Mechanical Drawing in high school, I became interested in the various styles of lettering and printing. At that time the heavy block letters were popular. You can still notice the influence today in the letters on school sweaters and jackets.

See how easy it is to develop this alphabet within the blocks. "Form follows function," as the art teachers say. (Or used to say.)

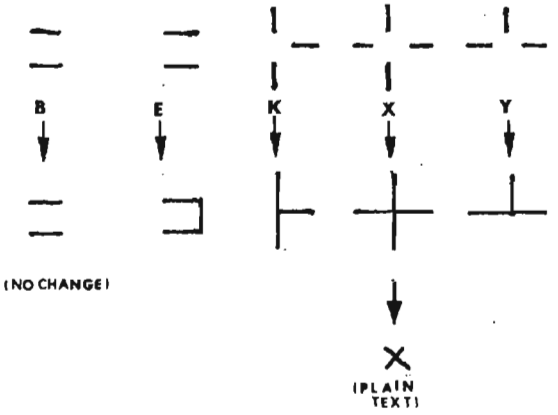


The letters were fairly easy to read, but it was very time-consuming to draw the blocks before writing your message. So I took the next step and abolished the squares. I just drew the marks and let my mind supply the blocks around them:



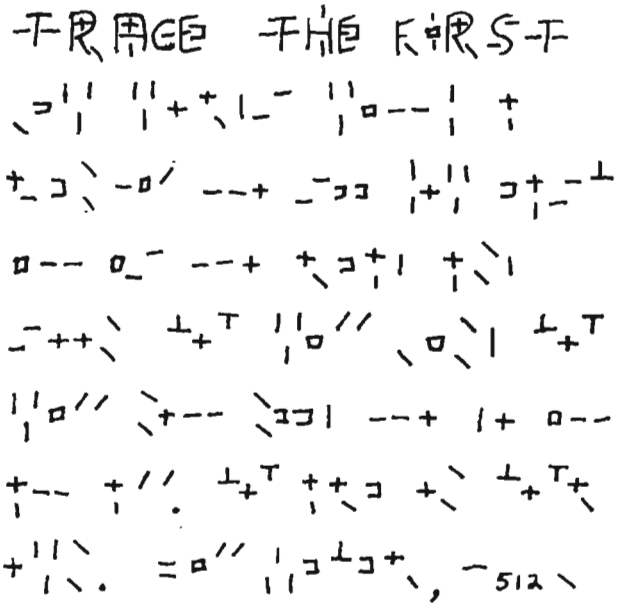
etc.

It didn't take long for my friends and me to become adept at our "secret cipher," but several refinements soon crept into the system (some to remove ambiguities, and others to increase ease in writing):



The cipher is simple and fast to write, and extremely easy to learn. Practice it with the following message. Trace the first few words until you get the hang of it. Just keep in mind that you are mentally supplying the square around each letter, and you will be able to visualize each letter easily.

After you learn the cipher, amaze your coworkers! Or teach your children, so that they can send "secret messages" to their friends when they should be listening to the teacher.



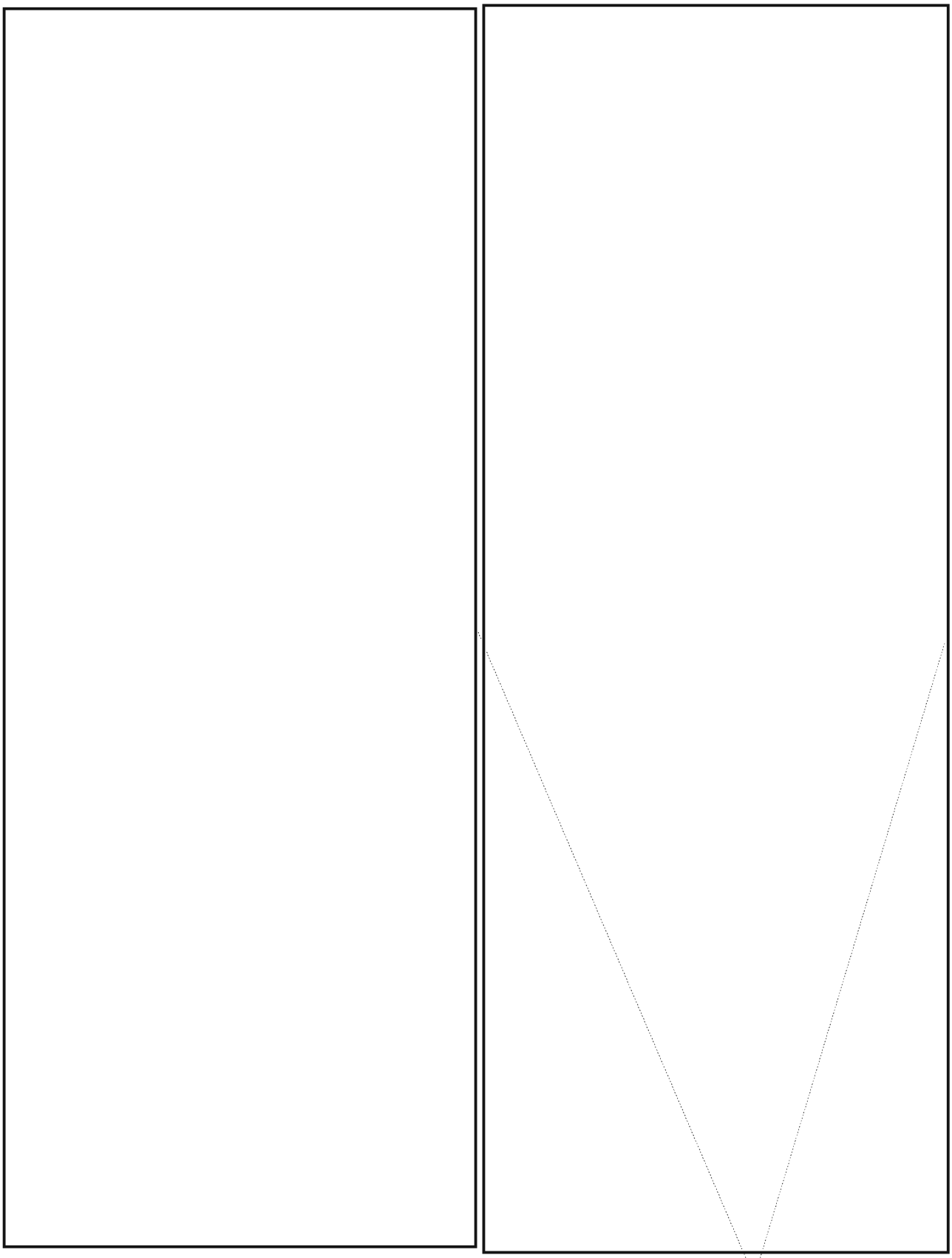
P.L. 86-36
DOCID: 4019642

. . . And Still More Comments! (On the AG-22/IATS Question)

Reprinted from C-LINERS, Vol. 3, No. 9, Spring 1976, Issue No. 30

EO 1.4.(c)
P.L. 86-36

~~HANDLE VIA COMINT CHANNELS ONLY~~



EO 1.4.(c)
P.L. 86-36

DOCID: 4019642

[redacted]

P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)

~~(SECRET - CCO)~~

...after certification?

[Continued from page 10]

that present programs in the training school could be of any use to them. It was suggested that making it easier for linguists to transfer to other language jobs and the creating of special language teams that could be used in various language crises would be both educational and good for morale.

One troublesome item has been brought up since the basic questionnaire was issued. Is the periodic retesting of professional linguists an effective, albeit negative, incentive for linguists to maintain a high level of capability? I have some very strong feelings about this question, but I think the committee definitely needs input from the Agency's linguists.

What does all this mean? I reiterate that a poll of such a small number of persons may not be an accurate barometer of the feelings of the majority. I do feel, however, that this poll reveals there is strong desire by at least a segment of the Agency's linguists for change, and that the linguists' feelings should be taken into consideration when discussing changes that will affect their future. If this article has provoked you, the reader, to want to comment, please send your ideas, gripes, threats, etc. to me as soon as possible (our committee will be submitting its recommendations in September or October). I'll make sure that the rest of the committee members know your feelings. Send your comments to:

John J. Mollick
B24, Room 5A107

(UNCLASSIFIED)

CRYPTO-MATHEMATICS INSTITUTE

Awards to the winners of the 1976 CMI Annual Essay Contest were made by President-elect Glenn Stahly, R5, at the annual banquet held at Goddard Space Flight Center on 18 June 1976.

Instead of the usual first prize ($100) and second prize ($50), an award of $75 was made to each of two authors tying for first place:

[redacted] R5: "A Measurement of Insecurity for Imperfect Erasure" (U),

[redacted] G4: "A Variable Length Output String PTAH" (title U, paper S).

Third prize ($25) was awarded to the authors of the following joint essay:

[redacted] R5:

[redacted] (title S, paper TSC).

The prize-winning essays have been released (within limits dictated by classification and need-to-know) by the sponsoring organizations indicated, but have not yet been published in journals.

~~(SECRET)~~

EO 1.4.(c)
P.L. 86-36

CRYPTO-LINGUISTICS ASSOCIATION

The following awards in the 1976 CLA Annual Essay Contest were made at the annual CLA banquet held at the Trojan Horse Restaurant on 27 May 1976.

First prize ($100):

Doris E. Miller, P16 (retired): "Language as a Bulk Commodity" (title U, paper TSC), *NSA Technical Journal*, Vol. XX, No. 3, Summer 1975.

Second prize ($50):

[redacted] G95: "RAPIDTRAN: [redacted] (title S, paper TSC), *CRYPTOLOG*, July 1975.

EO 1.4.(c)
P.L. 86-36

Third Prize ($25):

John B. Thomas, Jr., A9: "A Fix for the Language Problem?" (title U, paper S), *CRYPTOLOG*, August-September 1975.

Honorable mention:

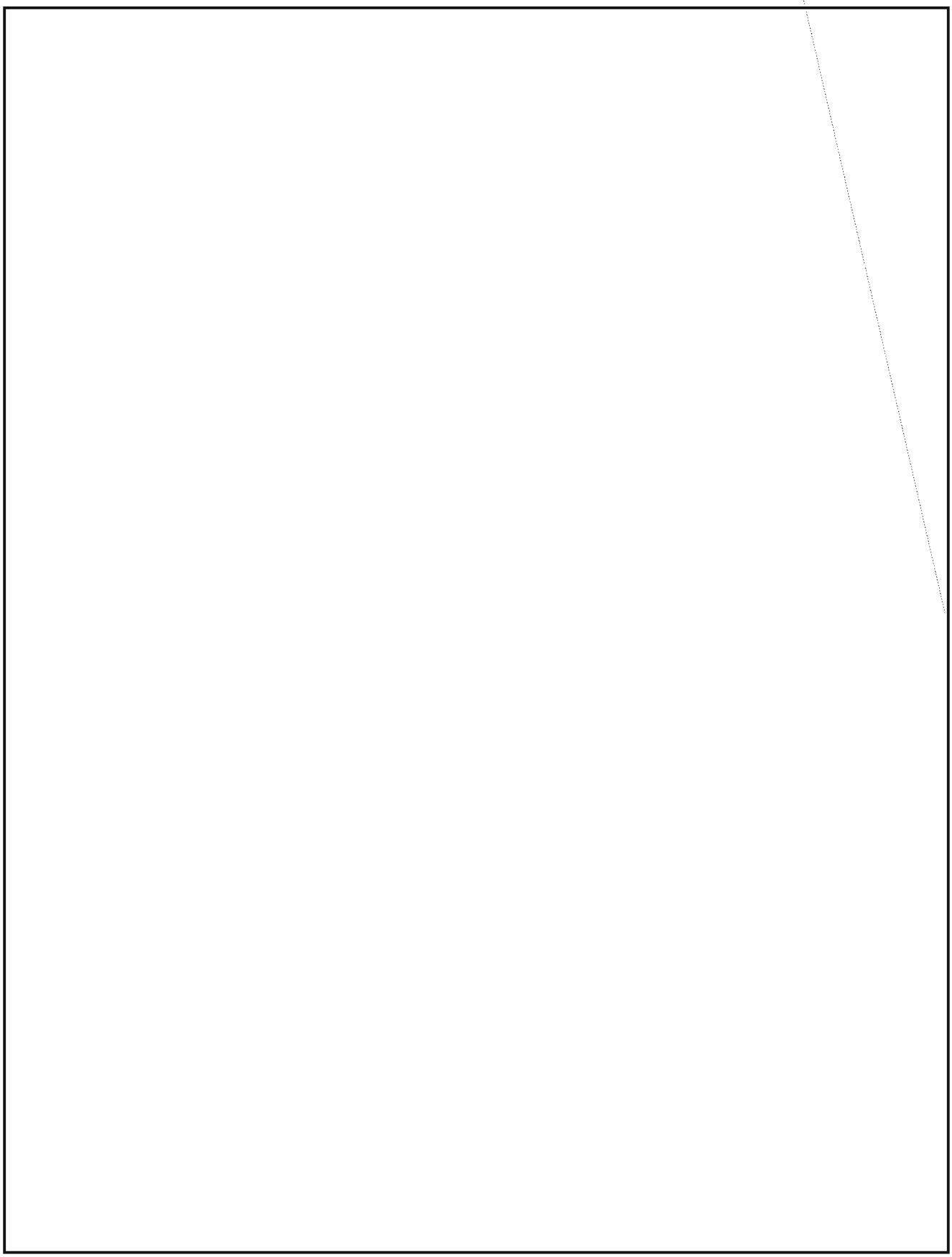
[redacted] "To Pull a 'Ponyal'" (title U, paper TSC), *CRYPTOLOG*, March 1976.

[redacted] P16 (retired): "Freedom in Translation" (U), to be published in *NSA Technical Journal*.

~~(SECRET)~~

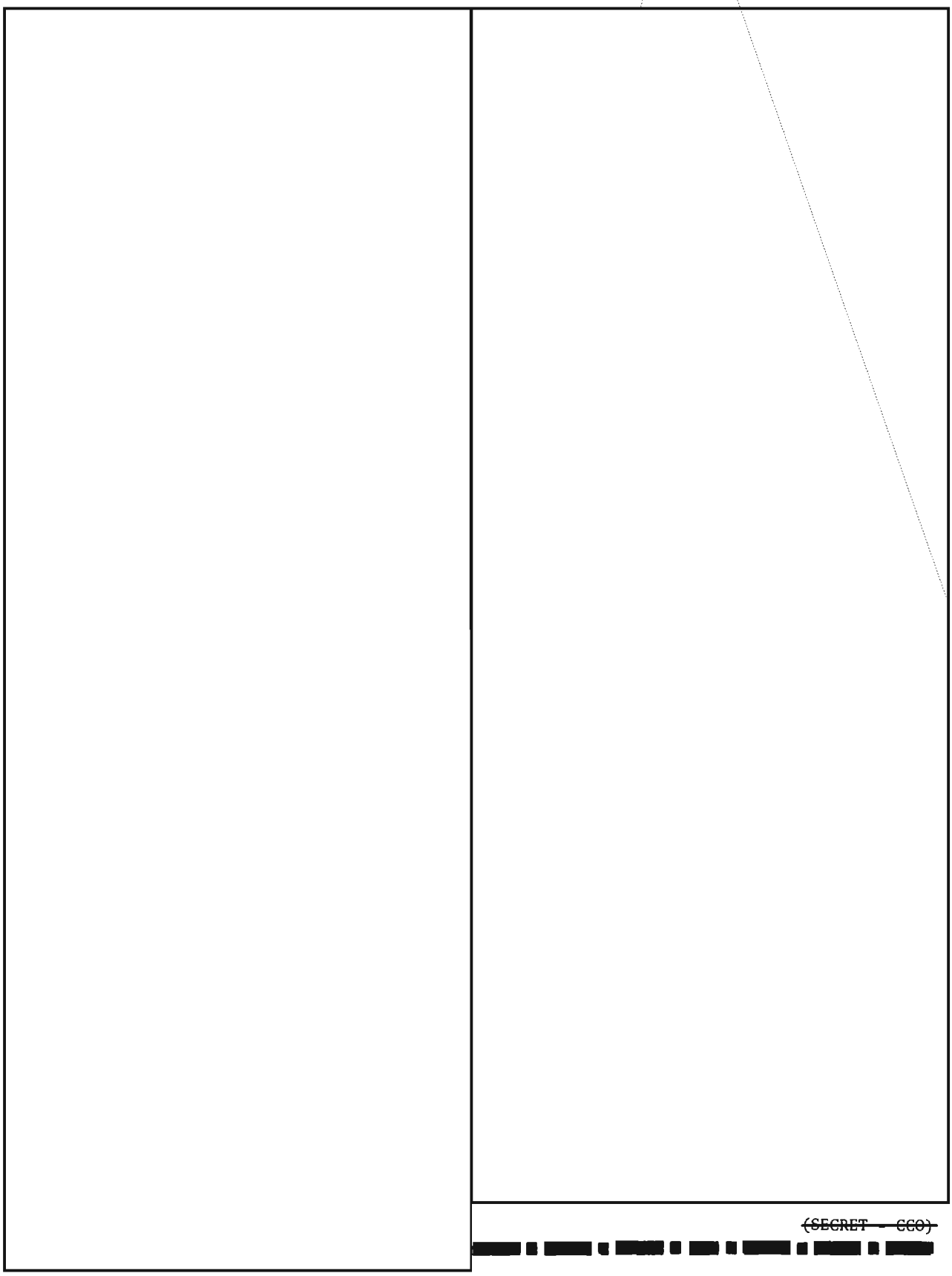
P.L. 86-36

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



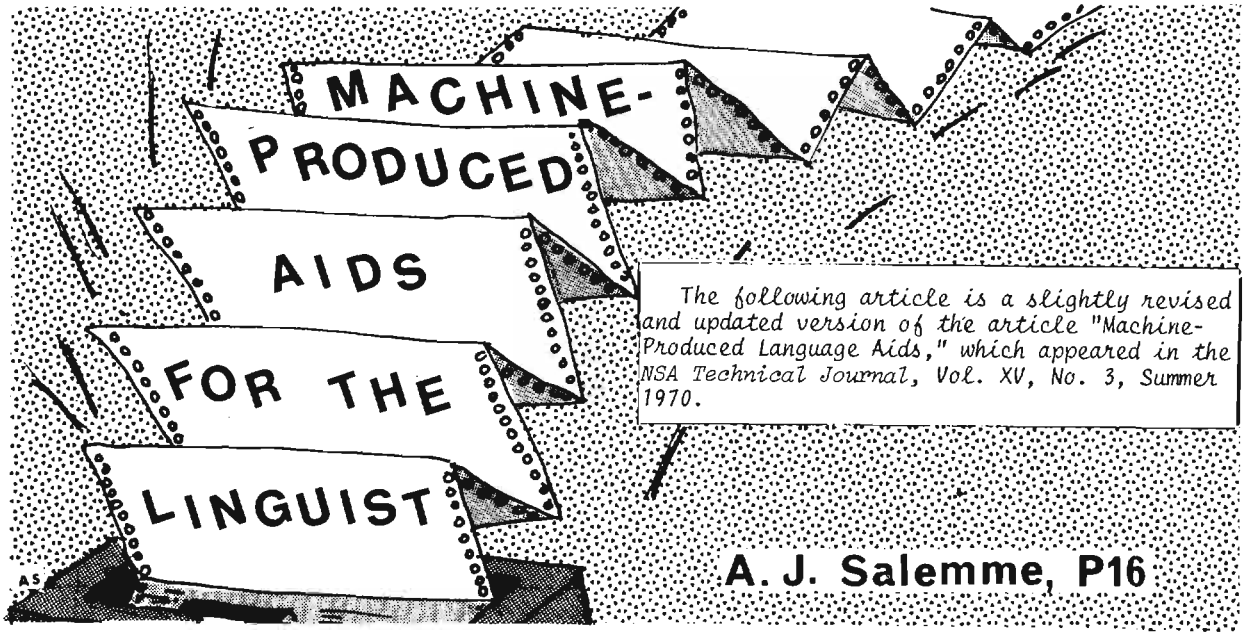
DOCID: 4019642

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



~~(SECRET - CCO)~~

DOCID: 4019642



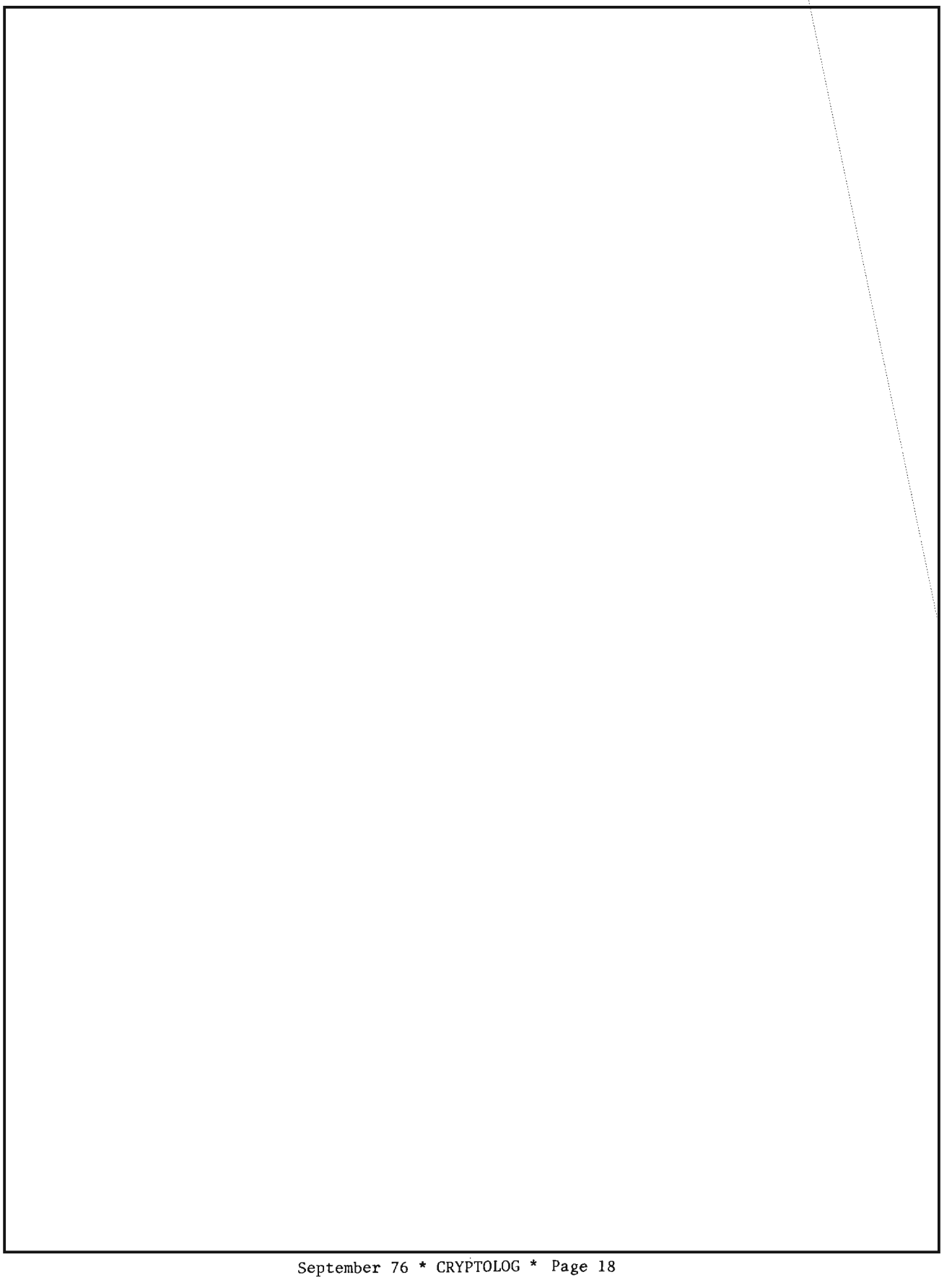
MACHINE-PRODUCED AIDS FOR THE LINGUIST

A. J. Salemme, P16

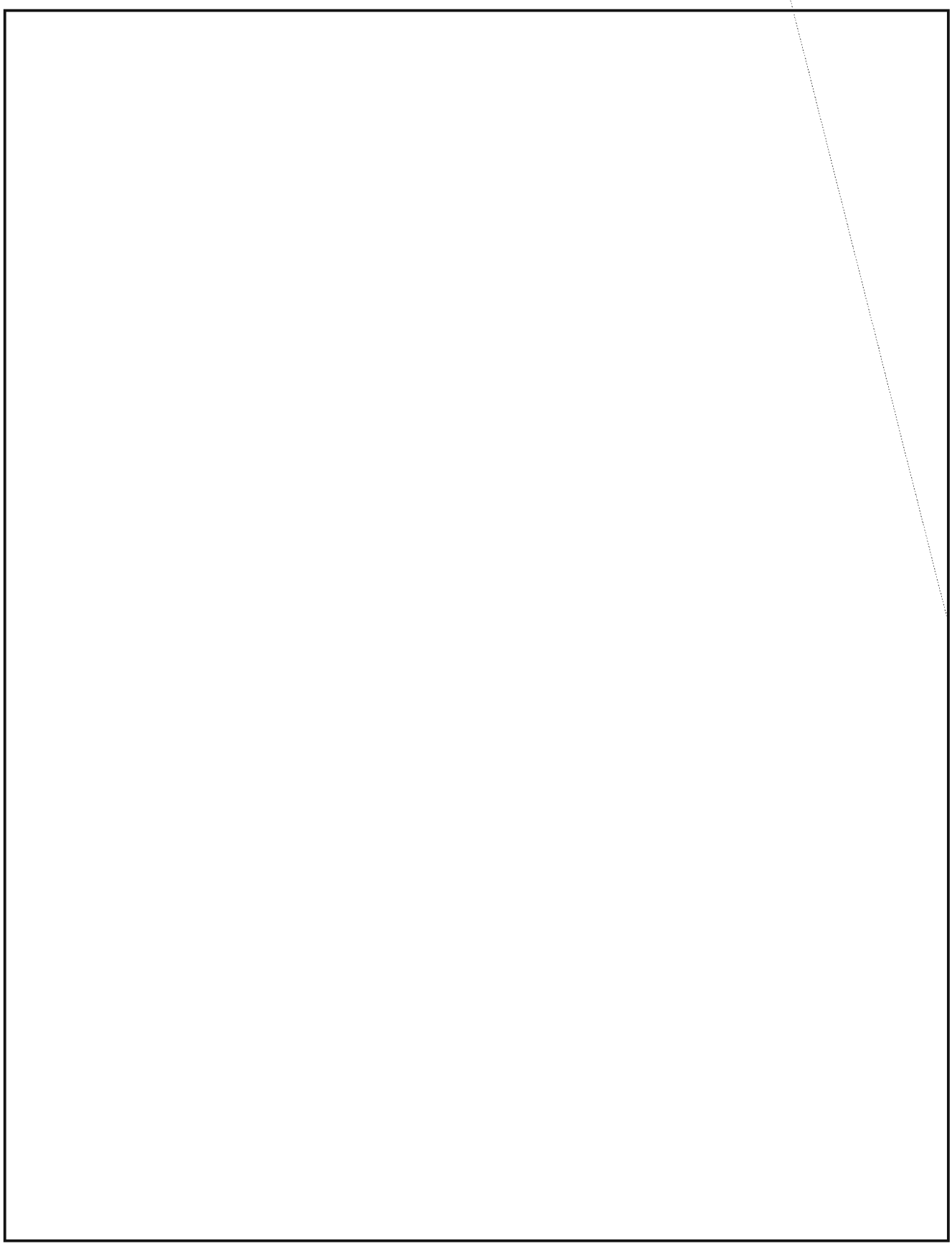
The following article is a slightly revised and updated version of the article "Machine-Produced Language Aids," which appeared in the NSA Technical Journal, Vol. XV, No. 3, Summer 1970.

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

[redacted]

[redacted]

~~(TOP SECRET UMBRA)~~

(To be concluded next month)

Language in the News

AT LONG LAST After 30 years of stationing troops in West Germany, the U.S. Army has finally begun to teach its soldiers German. It is the pet project of Gen. George S. Blanchard, once an outstanding West Point fullback.

Beginning July 2, all new batallion, brigade and division commanders will take 120 hours of German before they assume their positions in Germany.

"A knowledge of German," Blanchard explains, "is essential in attaining better private and professional relations between Germans and Americans. It is also extremely useful for the combined operations of American and German units...Moreover, I've never seen an unhappy GI in Germany who had found and made a good German friend. What better way to make a friend than to speak the same language?"

Blanchard believes that because of changing times, the devaluation of the dollar, and other influences, too many GI's in Germany have been isolating themselves by remaining on U.S. bases. He wants them to get out and mingle with the German population. He realizes, too, that in the past 30 years the German people have changed markedly and now expect more of the Americans living among them...at least a minimal knowledge of the host language.

Fewer Linguists

Only 10% of the universities and colleges in this country now require one foreign language for admission.

Time was when a student had to show knowledge of two foreign languages before he or she was admitted to many accredited U.S. universities.

Since 1963 the number of undergraduate students studying foreign languages has declined steadily. Less than 20% of contemporary high school graduates know a foreign tongue.

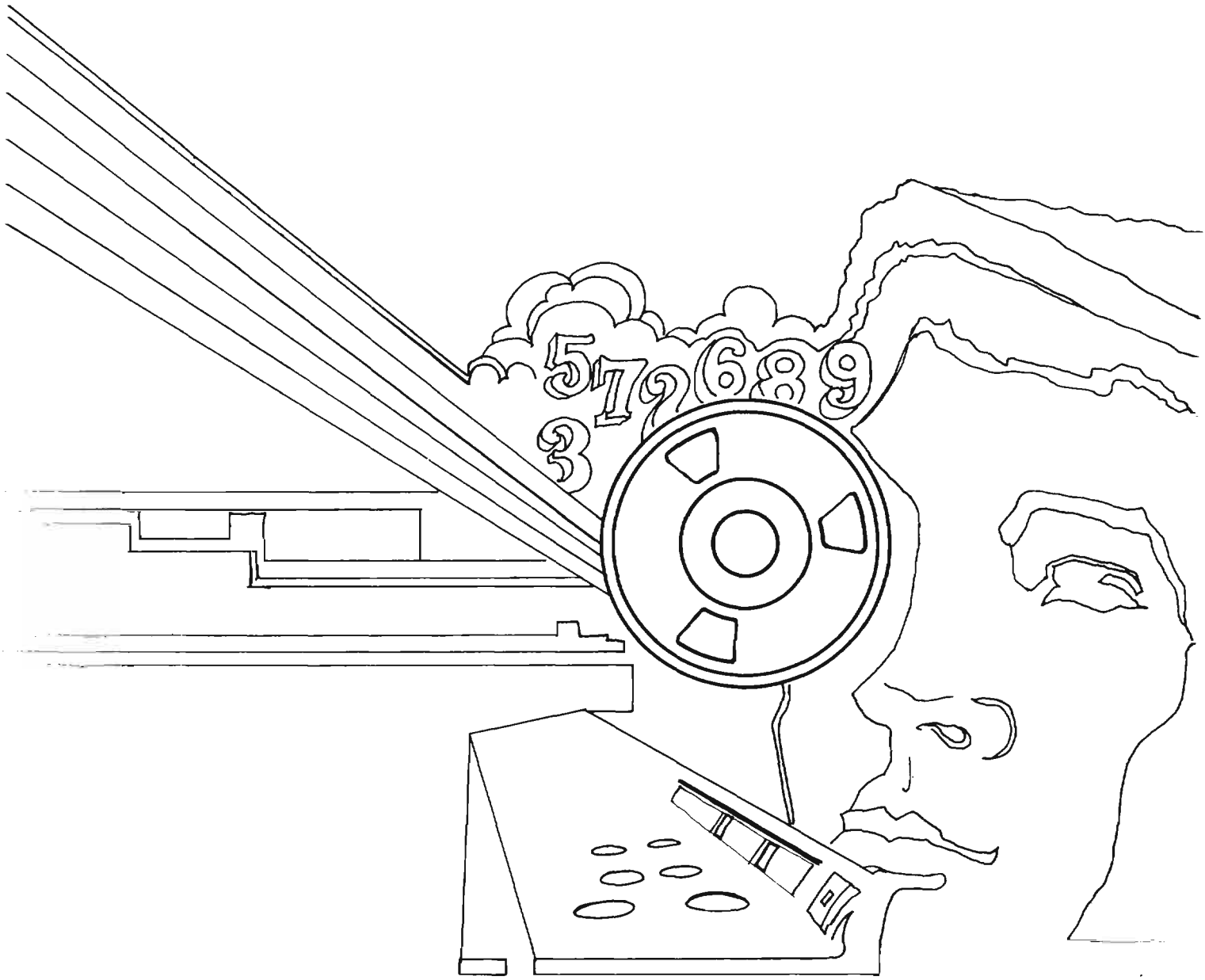
Why the change?

One quick answer is that educators are more concerned with teaching students how to structure and write a correct sentence in English than they are in French or Spanish.

Both items taken from *Parade* magazine, 20 June 1976

(UNCLASSIFIED)

Pl-Sep 76-S3-24788


5 7 2 6 8 9
3

DOCID: 4019632

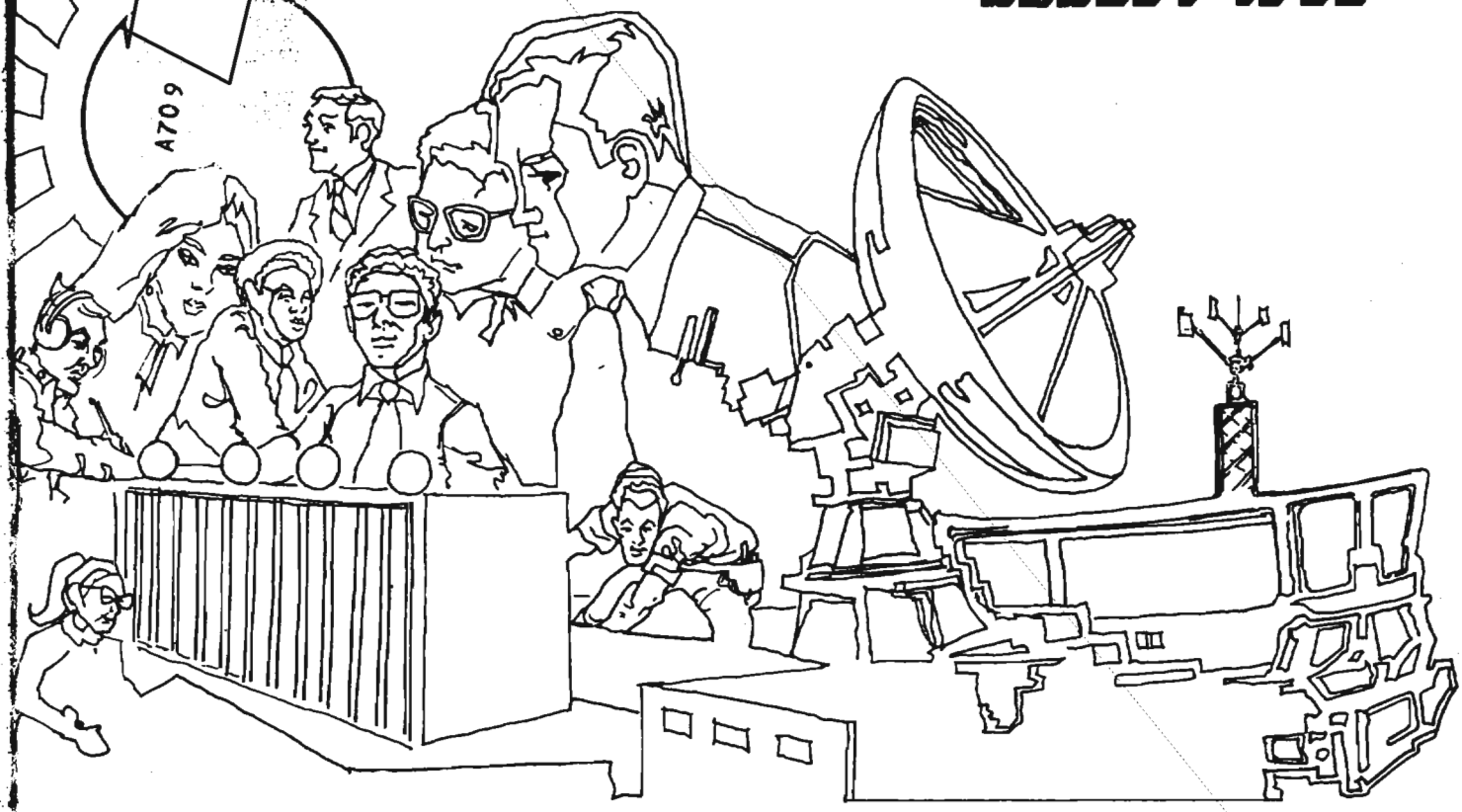
P.L.

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

AUGUST 1976



YES, DON, THERE IS AN ELINT!..... [redacted] 1
INITIATIVES IN SIGINT REPORTING..... [redacted] 4
NOTE ON FRANCOPHONEGLOS..... 6
CLUSTERING OF CRYPTANALYTIC DATA..... [redacted] 7
NSA'S SYSTEM FOR GRADING TRANSLATIONS. [redacted] 9
LANGUAGE IN THE NEWS (FRENCH)..... 12
INTEGRATED ANALYSTS FOR ASIA..... [redacted] 13
RESEARCH IN SPEECH PERCEPTION.....Dr. Ruth Day.....15
NSA CRYPTOLOGIC COLLECTION.....17
LETTERS TO THE EDITOR 19

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019632

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. III, No. 8 AUGUST 1976

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5642s)
Collection.....[redacted] (8955s)
Cryptanalysis.....[redacted] (8025s)
Language.....Emery W. Tetrault (5236s)
Machine Support.....[redacted] (3321s)
Mathematics.....Reed Dawson (3957s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Frederic O. Mason, Jr. (4142s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

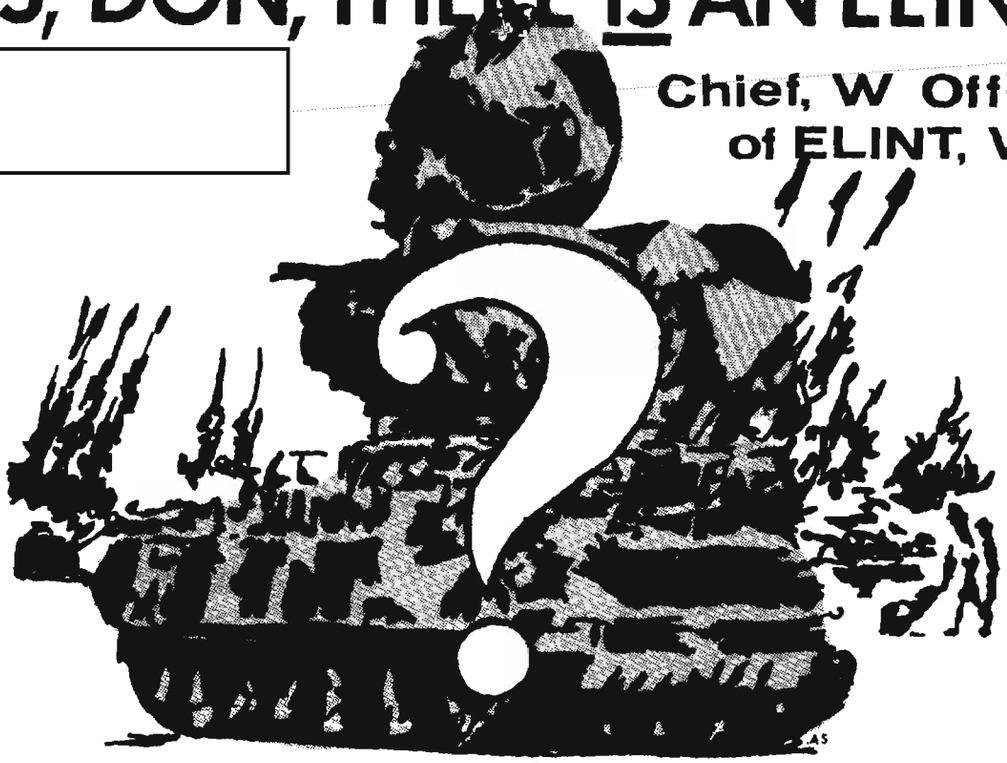
DOCID: 4019632

YES, DON, THERE IS AN ELINT!

[redacted]

P.L. 86-36

Chief, W Office of ELINT, W2



EO 1.4.(c)
P.L. 86-36

Yes, Don, there *is* an ELINT! Because you don't recognize it, doesn't mean it doesn't exist. Your NSA colleagues who plant its seeds, who nurture its growth, who channel its energies, and who harvest its fruits resemble in many ways the more "normal" NSA employee. You might, therefore, have as much difficulty recognizing an ELINTer as you do ELINT, but, believe me, they exist too.

In the April issue of CRYPTOLOG you asked if the real ELINT would stand up.* You indicated that it appears to be a shadowy operation and that many COMINTers would like to know what it is all about. Happy to oblige. We ELINTers have been so busy practicing our science (art?) that we didn't notice all of you waiting to be enlighted in the ways of ELINT -- perhaps to join the fun. We're a proud bunch who know we are an NSA minority specialty group with an important job to do, and we think that we're doing it rather well. We can do it even better, and we are working at that. We will attempt to throw light into the shadows, remove mystery, and minimize jargon.

Formal definitions of ELINT do in fact include all non-communications electronic emission intelligence except lightning and nuclear emissions. As practiced at NSA, our energies

[redacted] are devoted primarily to ELINT

NSA partitions ELINT into two classes: Operational ELINT and Technical ELINT.

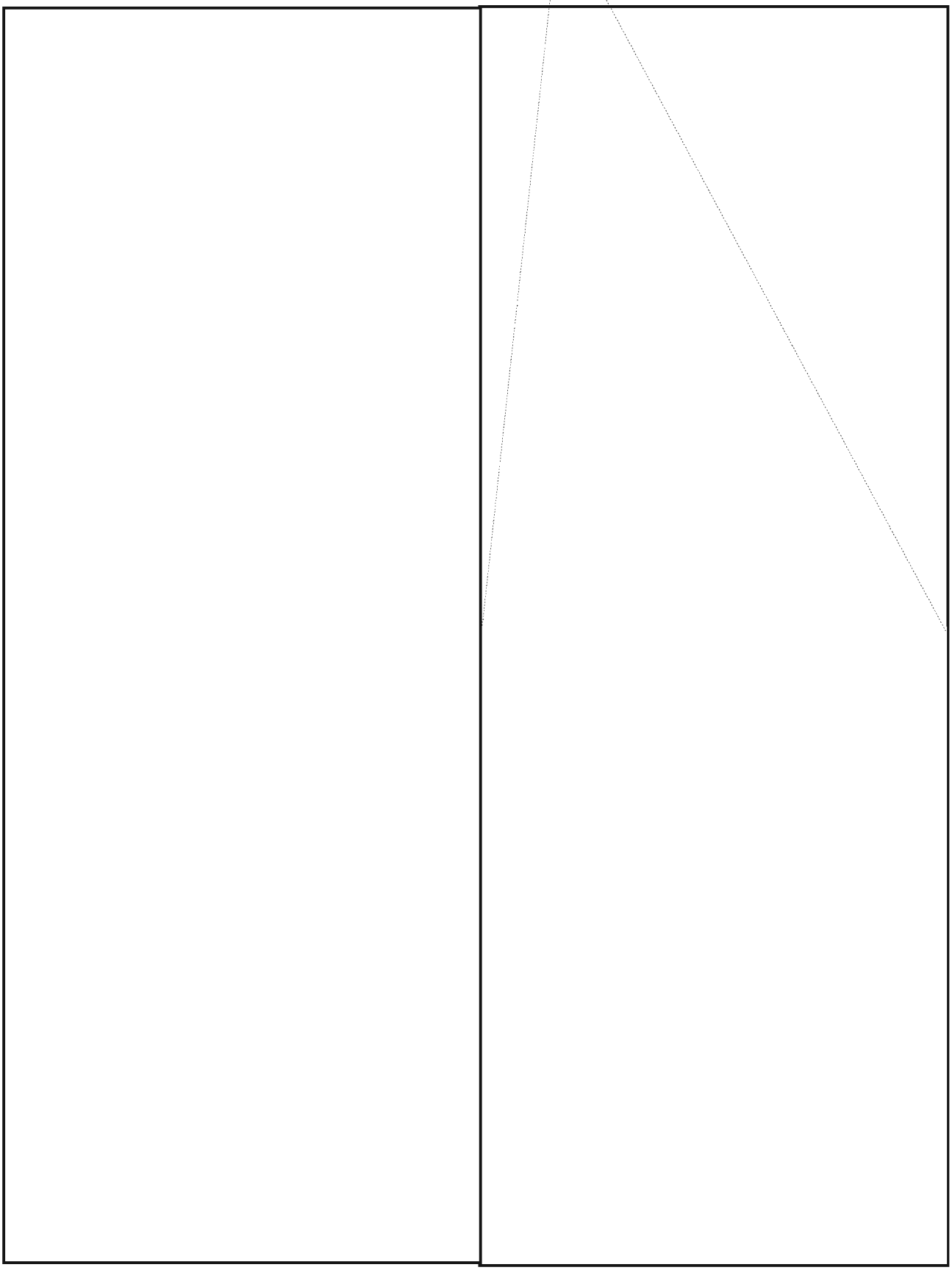
[redacted]

* [redacted] "Will the *Real* ELINT Please Stand Up?", *CRYPTOLOG*, April 1976, p. 5.

P.L. 86-36

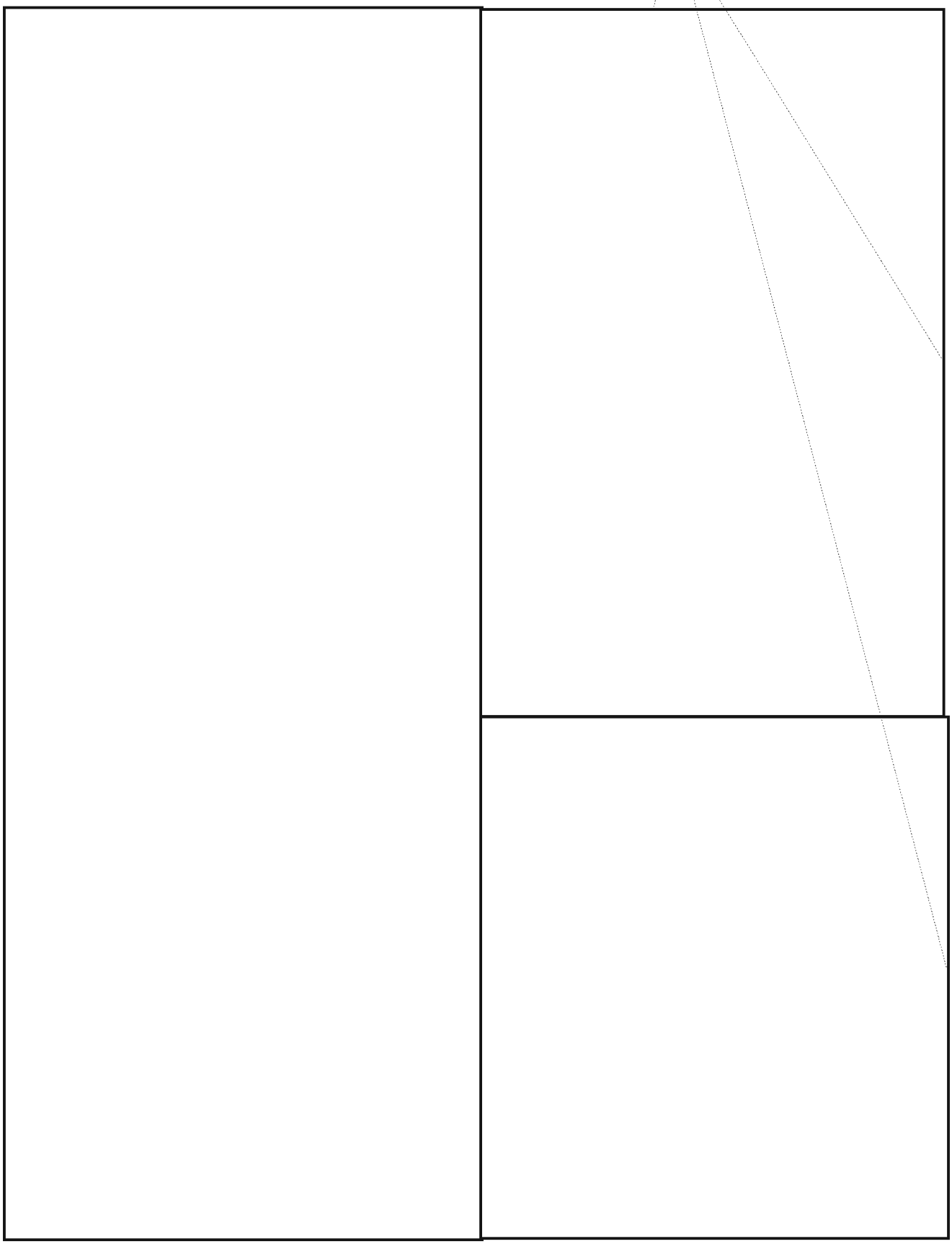
EO 1.4.(c)
P.L. 86-36

~~SECRET~~



~~SECRET~~

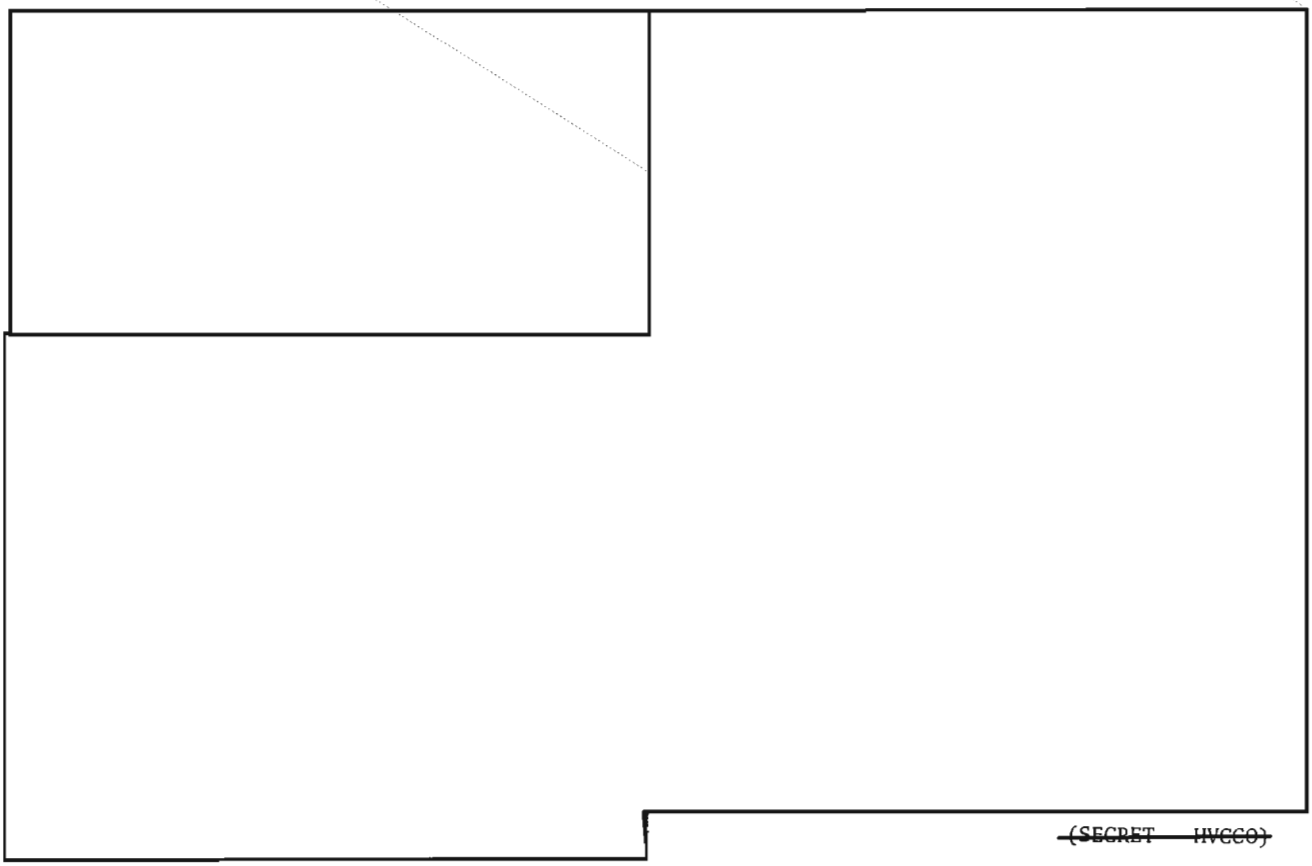
EO 1.4.(c)
P.L. 86-36



DOCID: 4019632
EO 1.4.(c)
P.L. 86-36

~~SECRET~~

P.L. 86-36



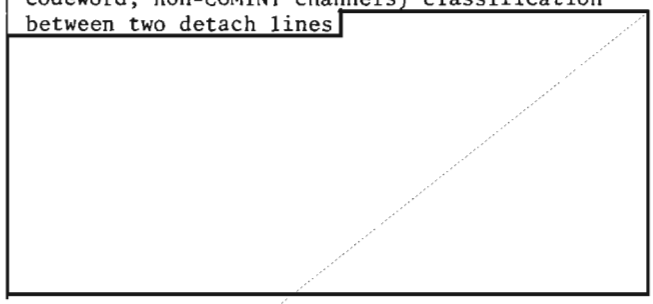
~~(SECRET HVCCO)~~

INITIATIVES IN SIGINT REPORTING

In the last few years the U.S. SIGINT System has been pressured from many directions to improve the utility (access) of SIGINT and, at the same time, to respond to oft-expressed concerns that SIGINT security needs tightening. Thus, on one hand we must provide SIGINT quickly and directly to the levels where it will be useful (in some cases to non-indoctrinated recipients); on the other we must scrupulously avoid distribution of product to places where there is no need for it, and, above all, we must not gratuitously reveal the SIGINT "secrets" (sources, methods, techniques). So, by varying degrees of loosening and binding the reporting and distribution procedures, we have made significant modifications which will work toward increasing both the usefulness and security of SIGINT.

To highlight the key changes which have occurred in the last year or so, let's start with Subcategory II(X) COMINT reporting. Some time ago, NSA invented the detach line format as an aid to recipients in implementing the less restrictive Subcategory II(X) COMINT usage provisions of the DCI's Communications Intelligence Security Regulations (CISR). The idea was that the producer would issue this "less sensitive" COMINT at a straight SECRET (non-codeword, non-COMINT channels) classification between two detach lines

P.L. 86-36

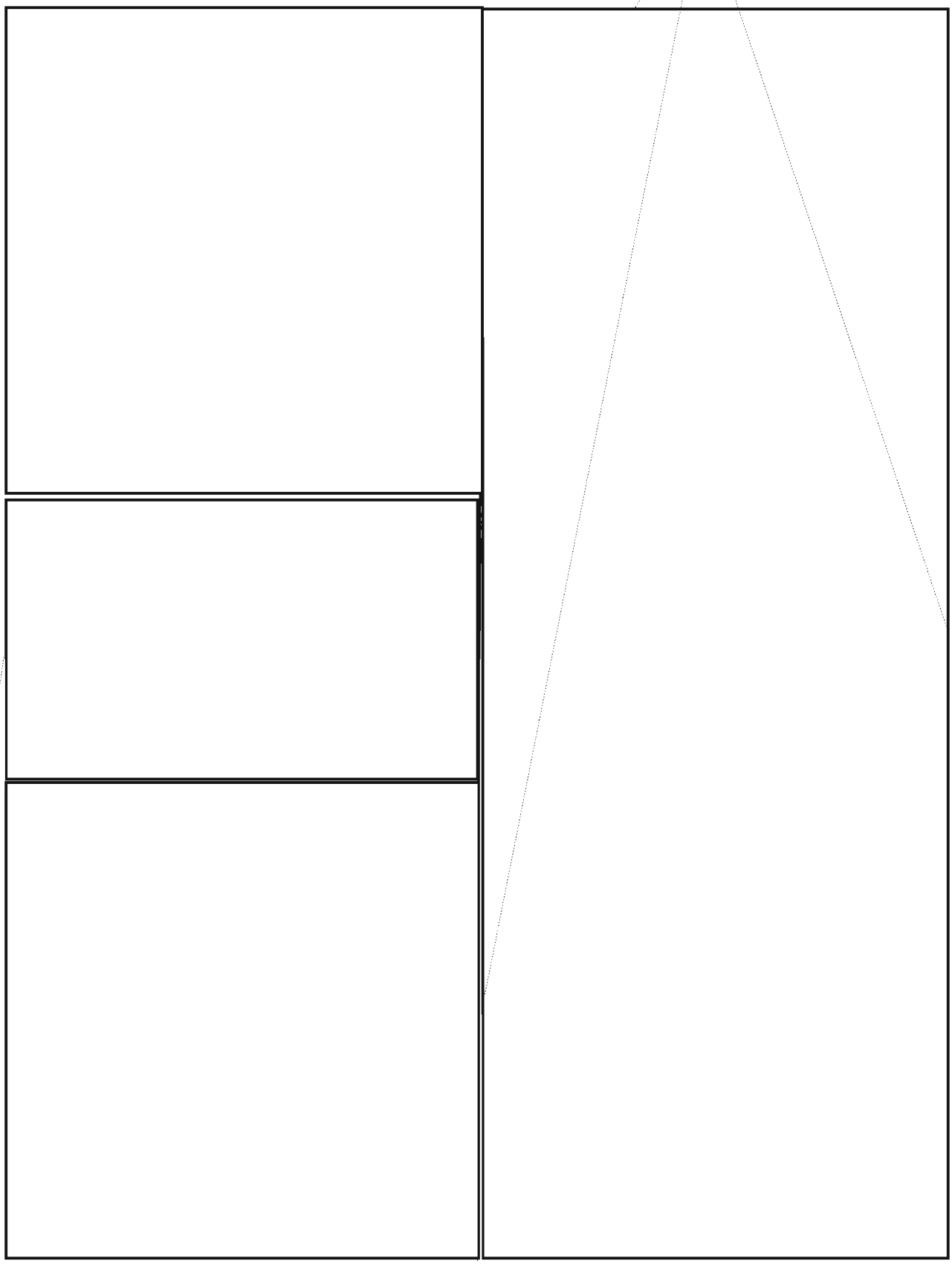


EO 1.4.(c)
P.L. 86-36

~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36

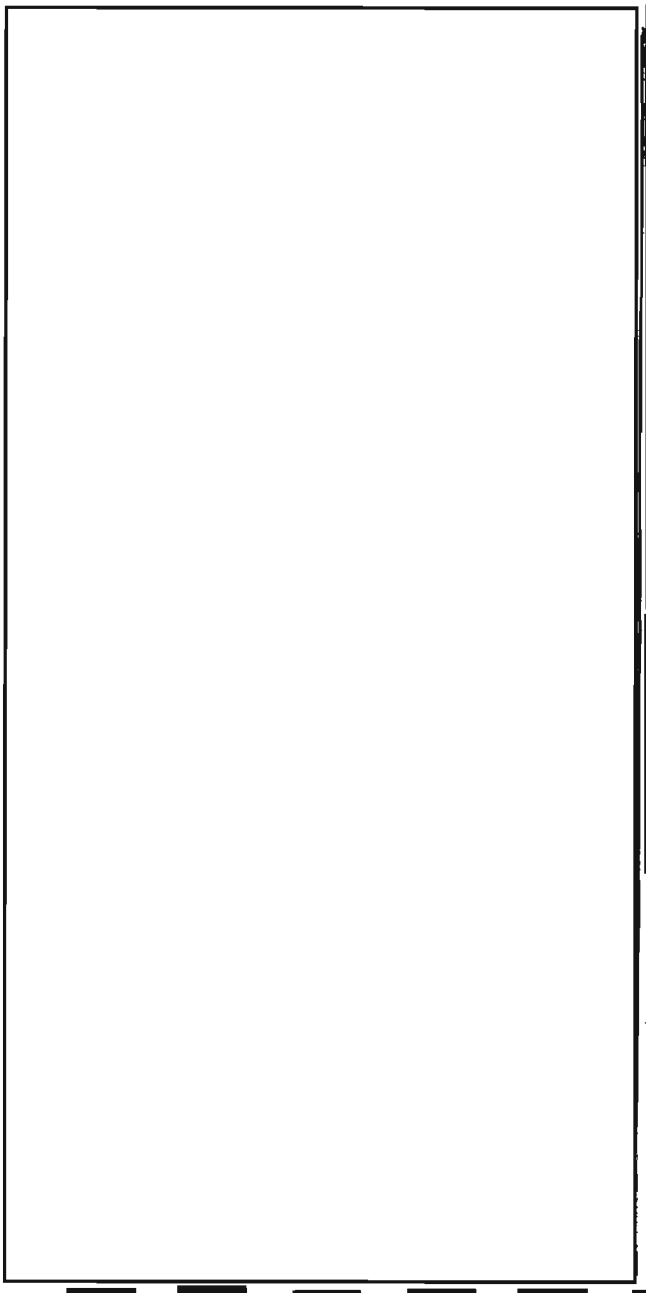
~~SECRET~~

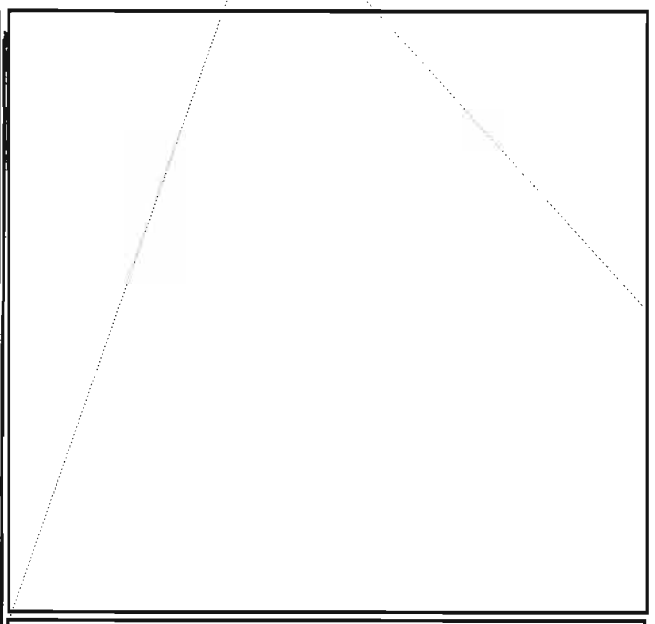


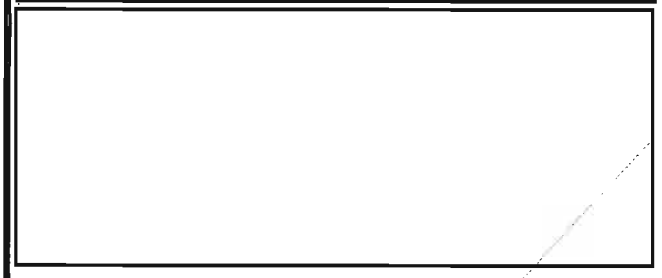
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36







There are many other areas in the reporting field that need to be fixed up. We must look at the proliferous secondary regurgitation (read republication) of SIGINT. We believe the current distribution lists of individual product are excessive and we want to trim them down. The sanitization manual now being written for what we hope to be an annex of the CISR should be hurried along. The rewrite of S-5200.17 also underway should be expedited. We are moving on these things and we hope there will be something positive to report soon.

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

~~(SECRET - HVCCO)~~

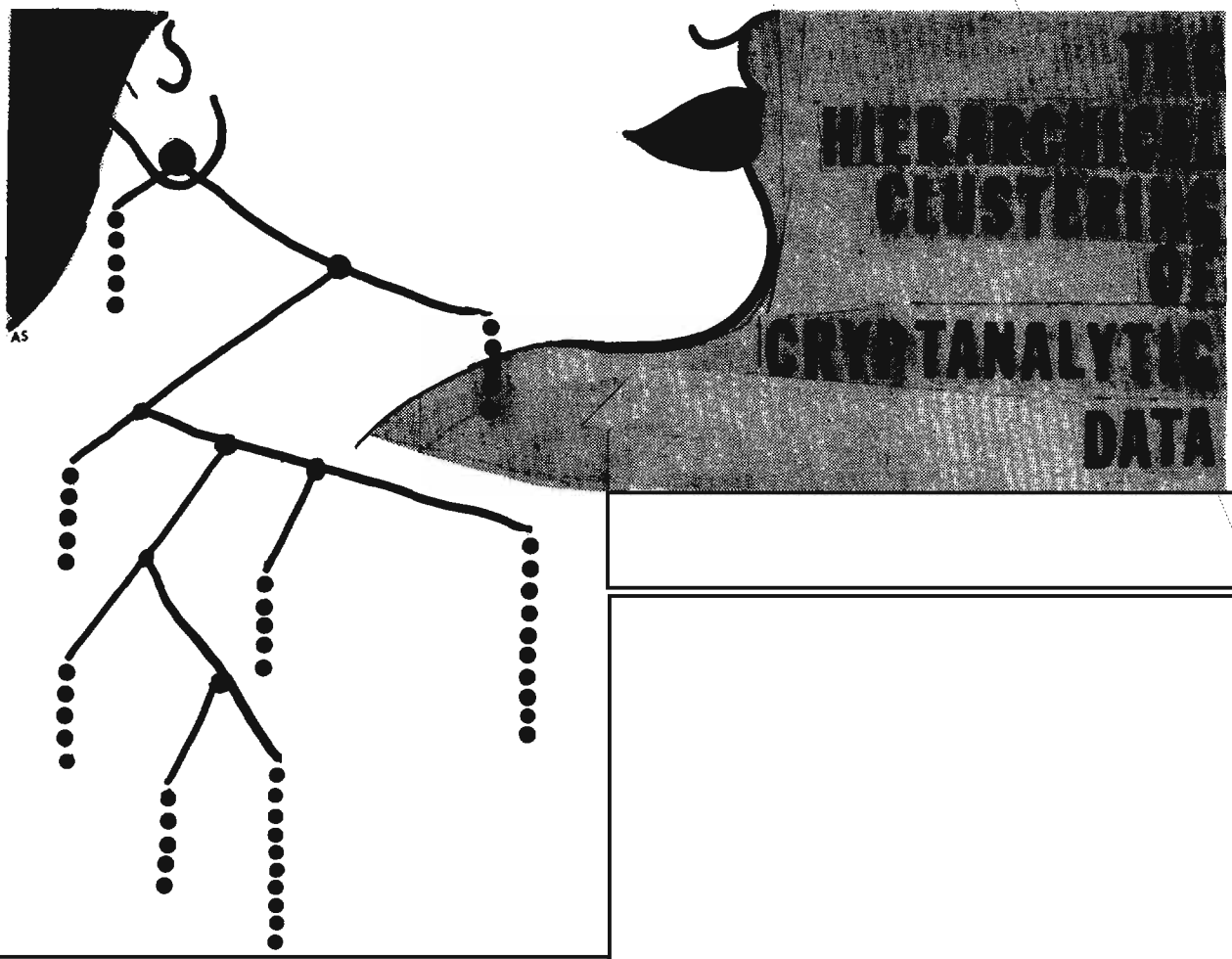
FPG LIVES!

Barbara Dudley, File Executive of the FRANCOPHONEGLOS computerized dictionary of the French Language (for details, see CRYPTOLOG, October 1975, p. 10), has returned to NSA on a consultant basis. She is training her successor, who will also be available for researching questions and for giving instructions in on-line querying. Phone 4814s or 4707s to make known your critical needs in French-language subject matter, so that the most needed source material can be fed into the computer.

~~(CONFIDENTIAL)~~

DOCID: 4019632

~~SECRET SPOKE~~



EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~

DOCID: 4019632

EO 1.4.(c)
P.L. 86-36

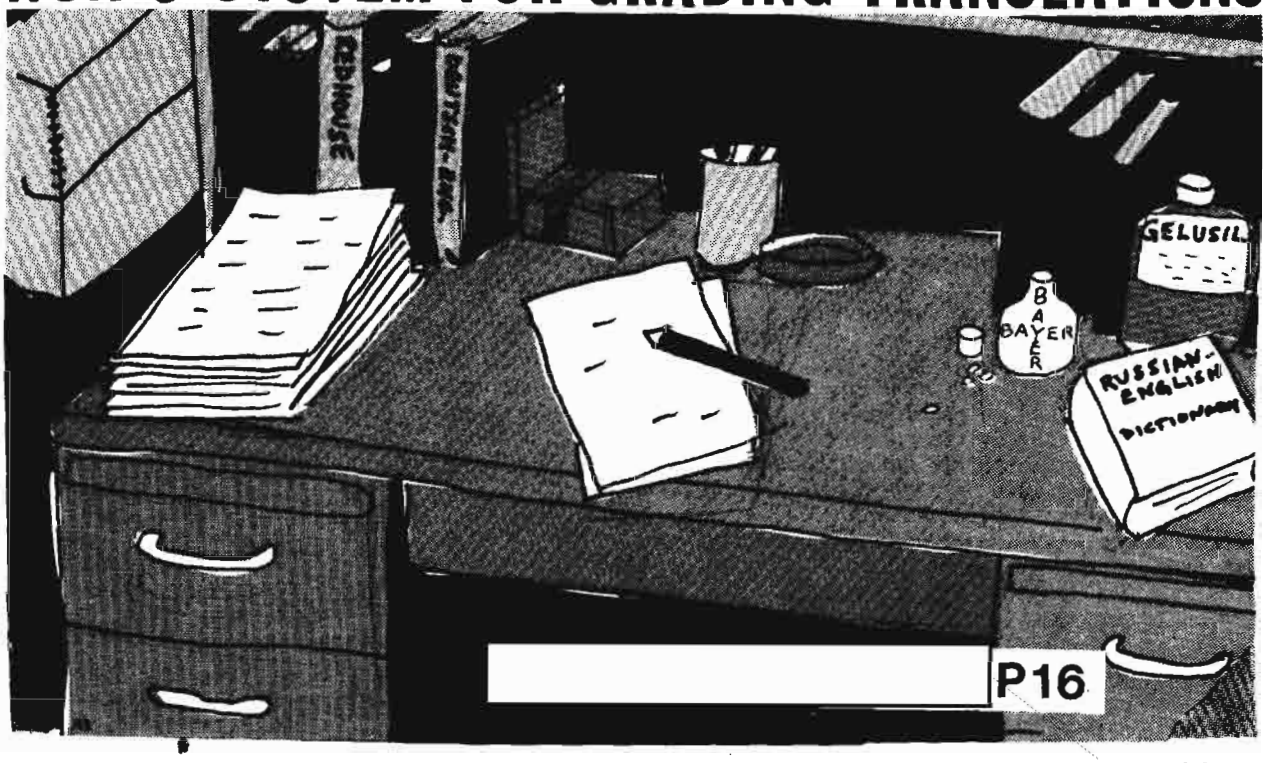
OH? REALLY??

John Kenneth Galbraith, then United States ambassador to India, was in Toronto to receive an honorary degree. As he recalls it in *Ambassador's Journal* (Houghton Mifflin): "I had asked that a certain cable from Washington to New Delhi be relayed to me through our consulate in Toronto. Consular aides brought the coded message out to me at the airport -- a mass of numbers. There were no facilities for decoding so I asked how they managed. They said when something arrived in code, they phoned Washington and had the original message read to them."

(UNCLASSIFIED)

DOCID: 4019632

NSA'S SYSTEM FOR GRADING TRANSLATIONS



P.L. 86-36

1. *Introductory Note*

A great deal of language testing in the U.S. government and elsewhere involves setting a passage of some arbitrary length for translation and applying equally arbitrary and often unreliable grading procedures. The wisdom of using the translation vehicle as a method for assessing foreign-language competence is probably questionable, but if this procedure is adopted, it should be applied as consistently and reliably as possible. I describe below the criteria for evaluating translations which we have applied at NSA since early in 1972.

2. *Scoring System*

Our testing system requires that subjects translate material of nontechnical nature which will generate 500-600 English words. My colleagues and I have set up a scoring system based on 100, and have set 70 as a passing grade. At least two graders, and most often three or four, grade each paper independently, assessing errors according to the system described below. Each paper is studied with great care by each grader in the interest of absolute fairness. Even so, the tendency to read into the text what one would like to see there, plus inevitable disagreement over the exact nature of translation errors, require that the graders compare their results. Agreement on every point is often impossible, since no two people view the texts of natural languages in exactly the same way. However, final pass/fail judgments are usually made against a spread of no more than 5 points. Thus, it is possible for two graders to award a 70 and a third, 65. As unanimity is not essential, such a paper could pass. Cases of this sort have been infrequent.

2.1 Types of Errors

We have made a three-way distinction among linguistic phenomena which we have found valid and reliable in assessing the errors of *beginning* translators (this scheme is of little or no value in evaluating the work of experts). The three categories we have distinguished are:

- foreign-language syntax,
- lexicon plus some grammar features of the foreign language, and
- English-language usage and convention.

The first two involve the translator's comprehension of the foreign language and his ability to show his understanding in correct, if unidiomatic, English rendering. The last reflects his skill in not only conveying the meaning of the passage, but doing so in idiomatic English. Four points are taken off for each syntactic error; two points for each lexical error; and one point for poor English usage and violation of convention.

Below I attempt fuller definitions and examples of the three possible sources of error and follow with some actual instances of poor translation from foreign languages to English. I also explain the rationale for specifying the type of error in cases where analysis may be difficult.

2.2 *Syntactic errors* (4 points each)

In the English sentences "The dog bit the man" and "The man bit the dog" the words are identical but the meanings are exactly opposite. The element which determines the difference is the positioning, or order, of the words. A native speaker of another language trying to learning English would have to be aware that in this sentence, as in most others, word order is all-important and that failure to appreciate this fact will lead to major error. In the NSA translation-grading system, a test subject making an equivalent error in translating from another language into English would be docked 8 points (for two 4-point errors: subject and object incorrectly identified in relation to the verb).

A second example somewhat more difficult to judge in respect to verb-noun relationships would be "Air filled the balloon" vs. "The balloon was filled with air." If it is clear from context that someone or something was involved in the *act* of filling the balloon (a mechanic, a pump, etc.), then the two sentences are vastly different, and failure to bring the fact out would cost the translator 4 points. If, however, the phrase "was filled with" is roughly synonymous with "was full of," we would at most take off one point (see below).

The two examples above involve what are called case errors: errors in establishing the true relationship of noun to verb. Below I give some actual examples of case error in translating from Russian to English. The following two examples are taken from a passage dealing with the destruction of a bridge and the need for a new one:

Correct translation	*Wrong translation*
"In 1943 the Germans blew up the bridge while retreating."	"In 1943 the bridge was blown up during the German retreat."
"The youngsters cross a [makeshift] suspension bridge. Other citizens also use it, risking life and limb."	"They [the youngsters] cross a [makeshift] suspension bridge, risk their necks and those of other citizens."

In the first example, there is no mention in the wrong translation of the "agent" (the "doer" of the act of blowing up the bridge), i.e. the Germans, whereas in the Russian original this was clearly specified, albeit in an inverted construction. In the second example, there are actually two case errors in the wrong translation. The first is the misrepresentation of "other citizens" as the object of "risking"; the second is the omission of "the citizens" as subject of "cross" ("the bridge" is, of course, omitted here, too, but our grading practice is to assess no more than 8 points per sentence. This and other general grading procedures will be discussed under "General Observations" below).

The two examples above are instances of mistranslation within the framework of simple noun-verb relations. We also assess 4 points for interclause errors which usually involve misplacement of relative (i.e. adjectival) clauses or adverbial clauses and which impair relations in meaning between clauses or sentences. One example (from a Russian text concerning a method of chemical analysis:

Correct translation	*Wrong translation*
"It is true that it is an expensive but proven method. However. . ."	"The method is expensive but, in truth, well tested. But. . ."

"It is true. . ." must govern the entire sentence, especially as the sentence is to be contrasted with the following sentence beginning with "However. . ." The misplacement of the initial phrase is thus a 4-point error.

A second example is more complex. In this case, also involving Russian, the original text had a somewhat unusual conditional construction which covered two sentences:

Correct translation	*Wrong translation*
"If the ore is good, a mine can be constructed. If it is worthless, you can search further."	"Good-you can build a mine, but it isn't suitable to look for another."

Here we took off 4 points for the wrong relationship between "good" and "you can. . ." resulting from the failure to translate the "if" clause. We did not give a double penalty for the omission of the second "if" but we did deduct another 4 points for an incorrect collapsing of ". . . it isn't [good], you can. . ." into one clause.

A final example is a case of appositional agreement in Japanese:

Correct translation	*Wrong translation*
"The North Korean Foreign Minister met again with the Foreign Minister of Peru [which is] *the sponsoring country whose position is said . . . to be close to that of South Korea.*	"The North Korean Foreign Minister met again with Peru's Foreign Minister, (*who is said to be close to South Korea's side*) in the host country.

Failure to put the clause in the right slot cost the person taking the test 4 points.

DOCID: 4019632

Dozens of other examples could be easily cited but the above should give some idea of syntactic error (I might note in passing that in our experience few people pass who make more than two such errors).

2.3 Lexical errors (2 points each)

The term "lexical" is something of a misnomer here because the error type covers not only incorrect vocabulary items but also certain prefixes and suffixes which are usually associated with syntax but are in fact more easily treated independently of syntactic relationships. Mistranslating, say, the German *die Strasse*, "the street," as "the apple" would obviously be a glaring error but it would not as such affect the *syntax* of the sentence. The same can be said of mistranslating the plural form *die Strassen* as "the street," or of rendering the future tense of a verb as a past.

We have coined an admittedly awkward phrase, "punctilinear error," to cover both kinds of 2-point errors. Such an error can be discerned at a given point in a "line" or string (hence the name) without the need for syntactic analysis. Below are some examples of punctilinear error:

Correct translation	*Wrong translation*
"There were only *suppositions*; no one knew for sure whether there was any ore [in the prospecting area]."	"There were only *suggestions;* no one knew . . ."
"The . . . mine is located *near* the city of. . ."	"The mine is located *next to* the city of . . ."
"It is *a very rich* mine."	"It is *the richest* mine."

The first two errors clearly involve vocabulary errors, while the third reflects a misunderstanding of a point of grammar (relative vs. absolute degree of superlative); in none of these cases is it very difficult to determine that a 2-point error has been made. In another instance the judgment is more difficult: a phrase which should have been translated from Russian as "the beloved home team" was rendered as "the favorite local team." The latter phrase can be understood as synonymous with the former, or it can be read as "*the* favorite (of several local teams)." Although 2 points could be taken off here, it would seem more reasonable to take off one, the penalty for a violation of English usage which I will now discuss.

2.4 Errors in English usage (1 point)

Admittedly questions of usage and convention are to a degree subjective, and it has been our experience that what is awkward or strange to one person may not offend another in any way. Hence we usually assess one-point errors only when there is consensus among the graders. There are enough such cases, however, to make the one-point error a major factor in the final grade. Some examples appear below. The first example is a sentence concerning repair of a bridge:

Idiomatic translation	*Stilted translation*
"No one has put his hand to [restoring] the bridge."	"By no means have somebody's hands touched the bridge."

The "English" in this case is so poor that any grader would deduct at least one point, regardless of possible major errors in the string. In most cases, though, the strings are not as long. Let us consider a few less-extended cases:

A test taker writing about mine excavation translated a phrase as ". . .*dug* one drill hole . . .," an action impossible by definition, although the general meaning is clear. (Poor usage of this kind is often the result of a translator's adhering too closely to the original language forms.) Another used the nonexistent phrase "to his luck" in the sense of "luckily for him": a third came up with "It completely won't do" for "It won't do at all." The list could from our experience be extended indefinitely.

Finally, we take one point off for English words and phrases which, while not in themselves awkward or peculiar, violate conventional usage. For example, translators who stick closely to original language forms will render "Secretary of State Kissinger" as "Foreign Minister Kissinger," or the "Pacific Ocean" as the "Quiet Ocean." When we feel that a personal or geographic name should be known to any literate person, we will deduct a point if a test subject misrepresents it.

2.5 Spelling and punctuation

Nothing is taken off for orthographic mistakes unless they will likely lead to misunderstanding, in which case the appropriate points are deducted.

3. General guidelines and caveats

3.1 Recurring errors

We try as hard as possible to avoid taking off points each time the same error is made. This is not too difficult in the case of lexical items, for once a translator decides that a word meaning "general" should be translated "field marshal," he will usually be consistent. Much the same is true of violations of English convention such as "Foreign Minister" for "Secretary of State." Repetitions of syntactic errors are much more difficult to spot; in cases where we are unsure whether the *identical* error has been repeated, we assess an additional 4 points.

DOCID: 4019632

3.2 Double jeopardy

A double error over an identical stretch of text is penalized only at the higher rate. Thus, if the translator not only incorrectly reverses the order of "dog bites man," but in addition misidentifies the animal ("man bites cat"), he loses 8 points for the two syntactic errors but nothing for the vocabulary mistake.

3.3 Importance of context

We are careful in judging errors, particularly of the 2-point variety, in terms of context, and we try to avoid relying on dictionaries as final arbiters in every case. Thus, the sentences "He doesn't have *the* money to go" and "He doesn't have *enough* money to go" mean approximately the same thing, but no dictionary will ever inform us that "the" means "enough," or vice versa. Similarly a bilingual dictionary, particularly a limited one, cannot give enough translation choices to cover every situation. Hence the "literal translation" monstrosities that are docked one point (and sometimes 2 or even 4 points).

3.4 Need to distinguish between language forms and language as used

One of our major problems from the time the grading system was put in effect has been the tendency on the part of some graders to consider the *forms* of language as somehow equivalent to the *effects* of utterances. That is, they will protest, for example, that the omission of a negative particle in a translation can as seriously affect the meaning of the passage as, say, an error in verb-noun relationships, and will insist that the same number of points should be docked for each.

This attitude is of course very understandable, but I should observe here that our major criterion for grading is syntax, which is to say the relationships among the elements of the sentence (what things go with what other things, and in what way), and the minor criteria relate to word choice and usage. This division is admittedly reminiscent of training and the classroom rather than language used in everyday life. Yet these are the criteria which have been used in the teaching of foreign languages and with which subjects and graders alike are most familiar. Furthermore, it would be extremely difficult, perhaps impossible, to devise a grading system according to which certain kinds and "strings" of information are considered more important than others; nor is such an approach needed for beginning translators. We have found that natural texts, not contrived ones, are best used, but the criteria by which the translations are judged should be formal, of the kind described above. They cannot be gut reactions to (mis)information.

3.5 Procedures to aid reliable and valid grading

As a final observation, we have found a tendency among some graders to temporize, especially in docking a paper 4 points, if they feel that the underlying cause of a mistake was a simple misunderstanding of a single word or grammar form ("I can see how he arrived at that"). This is unfortunately a kind of mind-reading that may be invalid and is certainly unreliable, since no two people draw the same kinds and numbers of inferences. The only thing we can judge is the syntactic and lexical rightness or wrongness, and the English usage, present in each paper.

(UNCLASSIFIED)

LANGUAGE IN THE ~~FRENCH~~ COURT

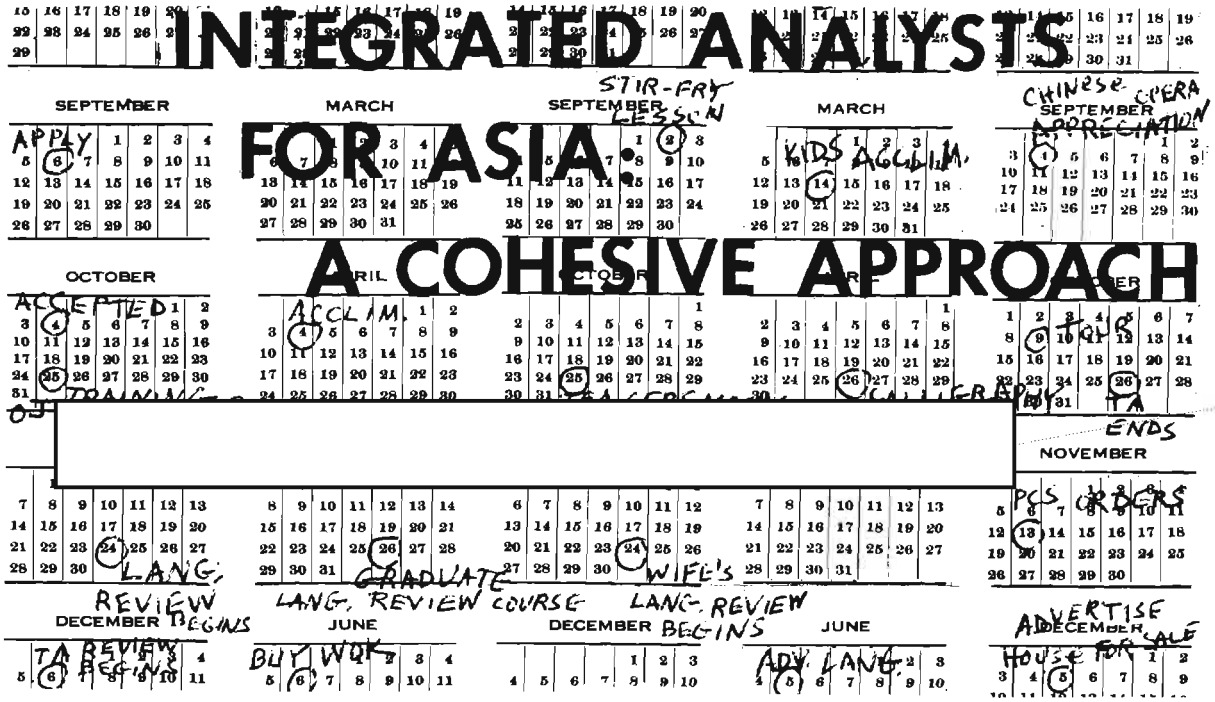
FRANGLAIS Starting next year, Frenchmen using English words in the wrong French places will be fined up to $35 each time they are convicted of "Franglais."

The new law is aimed at stemming the flow of Anglicisms into the customary French vocabulary. It provides a series of fines for first offenders who employ foreign words in advertisements, sales contracts, job offers, employment contracts and operating instructions.

In 1977 the "duty free shop" at French airports will be known as "La Boutique Franche." Tourists expecting "le discount" for paying in travelers checks will have to ask instead for "le minimarge." Frenchmen who want to book on "le hovercraft" across the English Channel will request passage by "aeroglisseur." And instead of "le know-how," a most widely used term throughout France, Frenchmen will have to use "savoir faire," an expression Americans and Englishmen adopted from the French centuries ago without bastardizing their own language.

French officials insist that the new regulations are not designed to retain the purity of their mother tongue as much as they are to protect consumers and employers who do not understand the true meanings of the foreign idioms.

Parade, 13 April 1976



P.L. 86-36

On the other hand, in spite of the resource decrement, the intelligence requirement continues. SIGINT remains our first line of defense, and it is incumbent upon us to respond to this charge with all the resourcefulness we can muster.

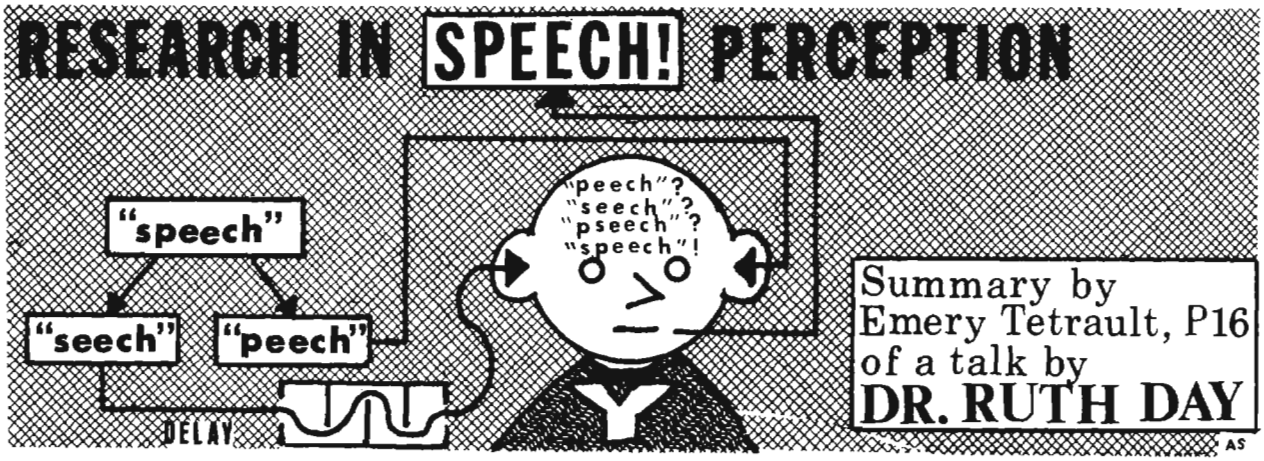
EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

If you are still with me to this point, please don't send me any letters saying that we are already doing all of this. For each case you cite wherein the full objective has been achieved, I can cite two or three wherein the objective was either ignored or effectively undermined, and that is not my purpose in any case. What I am earnestly requesting is that this Agency recognize an area which will be of vital importance in the future, and take every reasonable step to insure we are up to the challenge. If we are to succeed, as succeed we must, we need to be innovative, thorough, deliberate, and, above all, cohesive in our integrated analyst program management; and it is within our capabilities to do so. We, as an Agency, should not settle for anything less.

~~(SECRET - HVCCO)~~



The subject of individual differences in speech perception has not been a burning issue, either in cognitive psychology or in psycholinguistics, but it could be of intense interest to anyone who is responsible for selecting and training voice linguists. This was the main inference drawn from a talk given by Dr. Ruth Day, of Yale University and the Haskins Laboratory, to SIGVOICE (the Crypto-Linguistic Association's Special Interest Group on Voice). Her talk was enthusiastically received and considerable support was given at that time to the notion of following up on her findings. During the time that has passed since that talk, a few actions have been taken in the direction suggested. While NSA has not funded Dr. Day directly, R54 has been supporting research in individual differences in speech perception at Haskins Laboratory for the past year. In addition, the Office of Naval Research has let out two contracts studying individual differences in speech perception, one with Dr. Day and one with the University of Oregon; R54 has been receiving the progress reports from these ONR projects.

Dr. Day began by introducing the concepts of rivalry and fusion as demonstrated in experiments with visual stimuli through the use of a tachistoscope, a device which makes it possible to present different stimuli to each eye, and with auditory stimuli through the use of the dichotic listening technique.

One of the dichotic listening tasks was simply identifying input: did the subject hear "banket" in one ear and "lanket" in the other ear, or did he hear the single word "blanket"? It turned out that subjects thus tested were either very good fusers (that is, they consistently heard a single word), or very good separators. There was almost no middle ground. This was particularly so when the outcome of fusion proved to be an actual English word, although the pattern was maintained as long as the result of fusion violated no English canonical form (see Butcher in *NSA Technical Journal*, Special Linguistics Issue No. II).

Another task consisted of identifying the first sound heard when the two stimuli are presented with a slight time lag in onset (from 25 to 150 milliseconds). Everyone heard /b/ when "banket" was given before "lanket," but part of the test population continued to hear /b/ first even when the onset order was reversed. Dr. Day advanced the hypothesis that this group was hearing only that which English permits -- /b/ followed by /l/. She called this group of people *language-bound*. The people who were capable of receiving and holding auditory stimuli in some kind of raw storage without immediately activating their grammar machines, she called *stimulus-bound*.

This bimodal or bactrian distribution of scores has been replicated with more or less randomly selected sample populations. In studies involving 100 Yale undergraduates, more than 90 were firmly identified with either one or the other group, and only five people showed no marked tendency toward membership in either the language-bound (henceforth LB) or stimulus-bound (SB) camp. Moreover, group membership appears to be stable. LB people do improve their performance by learning the task, but they never get to be as proficient at it as the SB types.

Dr. Day noted that the poor performance on this second task by LB people could be attributed to the fact that they simply can't make temporal-order judgments. However, when fusion of the two stimuli produces strings which are not canonically possible in English, then the LB subject does as well as anyone else in determining that (1) there are two stimuli and (2) one of them clearly precedes the other in onset time. Thus, when the stimuli are "back" and "dack," he has no problem making the temporal-order judgment, because neither "bdack" nor "dback" is a good candidate for an English morpheme. In other words, he can do the task in those situations where higher-order linguistic processing is ruled out.

DOCID: 4019632

How do these two groups, once identified, fare on other kinds of tests? Do they retain their group identity? Dr. Day described some other tests which showed similar distributions.

Digit Memory

This warhorse of psychological testing usually produces a serial position curve. Test subjects have to remember sequences of digits and write them down in the same order as they were dictated. Items presented early and items which were last in the sequence tend to be remembered, but items in the middle are usually lost. This is what everyone expects and this is what all the methods of averaging and other obscuring individual differences give us. This is not, however, what SB subjects do. They make relatively fewer errors on this task than the population at large and the errors made occurred more or less evenly throughout the entire sequence. To get an SB subject to show the serial position effect, the task has to be made so difficult that the rest of the population finds it nearly impossible to do so.

Digit Memory with Zero Recall Cue

This task is the same as the previous one with one difference: each sequence ends with a zero, which is the cue for the subject to start recalling items. This procedure neutralizes the recency effect, at least for the LB types, but for SB subjects it affects not just the last items in the string, but all the items in the sequence. This, according to Dr. Day, suggests that there is something more than a quantitative difference between the performance of LB and SB subjects on this test. It supports the notion that the LB person has begun some immediate coding and longer-term storage of incoming auditory stimuli, while the SB type is holding the whole string in a kind of buffer memory. This is why the zero recall cue tends to affect the entire sequence for SB subjects.

Jotto

Given a target word -- say, "charm" -- and a list of comparison words, subjects are asked to find the one comparison word that shares the greatest number of letters with the target word. According to Dr. Day, the LB type will have a harder time with this task than the SB subject. He frequently underestimates the number of shared letters between target words and comparison words. He appears to be operating on the whole-word level and not seeing lower-order elements. With a target word like "sylph" and a comparison word like "prone," he would tend not to count the letter *p*, perhaps because he is going immediately from visual stimuli to phonemic representation (from *ph* to /f/).

Word Search

NSA Newsletter devotees immediately recognized this task since every month this esteemed publication runs a puzzle consisting of words running every which way (actually, eight directions) in a matrix of letters. SB subjects did better than LB people when left-to-right directionality was violated. Dr. Day advanced the notion that SB types have the option of using both left- and right-hemisphere capability to solve tasks, while LB subjects are more or less locked into left-hemisphere -- i.e. linguistic -- processing.

Secret Languages

Dr. Day used a simple encode device to come up with one "secret" language: she transposed all /l/ and /r/ phonemes ("Maly had a ritter ram. . ."). Test subjects were asked to transform standard English (discrete words and then stereotyped connected discourse) into the secret language. She played some tapes of subjects performing this task. SB subjects were quite fluent, but the LB people had problems. One subject was almost pathetic as he tried valiantly to transform the word "bramble" and Dr. Day said she was going to spare us the pain of listening to his efforts against the name "Nelson Rockefeller."

Delayed Auditory Feedback (DAF)

The test subject wears earphones and talks into a microphone. His speech is fed back to him with a delay of about a fifth of a second. Again, Dr. Day played some demonstration tapes for us and, again, some subjects had little or no trouble with this task and others sounded like drunks in a nearly comatose state. Dr. Day herself was one of the subjects on the tape and we heard her trying, not altogether successfully, to recite the English alphabet (something which she assured us she knows). She noted that DAF performance is related to such tasks as foreign-language mimicry and phonetic transcription (in IPA or some comparable system) of unknown language forms.

*

Summary

So, we know that some people are language-bound and others are stimulus-bound and we have some notion of how to identify members of one or the other group. The immediate executive response ought to be, "All right, dammit, which one is the better one for a voice job?" Is it the LB who operates on a strong sense of linguistic expectancy, the anticipation of what can follow at every structural level from sound to meaning? Or is it the SB who can store raw auditory data in a short-term memory and more or less call things as he hears them? The answer to this question may not be as obvious as it seems on the surface, but it would certainly be worth the effort to push this research a little bit farthere, We are in no position to pass up any help in the field of language processing.

NSA CRYPTOLOGIC COLLECTION

Have you ever visited the NSA Cryptologic Collection? Have you ever *heard* of it? If not, why don't you visit it? You'll be fascinated by what is contained in it. The collection is in Room 3W076, Operations Building, and is administered by [redacted] x4017s.

The collection is in a small room, but the room is crammed full of cryptologic literature of historical as well as completely up-to-the-minute value. Much of the collection is shelved in more than 1300 Shinn boxes, plus additional file-cabinet and shelf space. Much of the literature is unique and not represented in any other Agency collections (although the collection holdings are indexed in the NSA Technical Library, C5, records).

The collection contains historical documents pertaining to the use of cryptology in World War I and World II. In addition, it contains working aids of all vintages, pertaining to all aspects of cryptology, including a large number of cryptolinguistic working aids containing letter-frequency, word-pattern, and other data derived from a broad spectrum of languages. A few samples are shown on the opposite side of this page.

Relative newcomers to the Agency who started late to save their back issues of the *NSA Technical Journal* can find a complete set here, back to Volume I, Number 1. (Incidentally, have you seen the special Twentieth Anniversary Issue of the *Journal* yet?) P.L. 86-36

The collection also includes a large number of open-source publications dealing with cryptologic subjects, including several rare books. And, of course, it contains a facsimile of the Voynich Manuscript? (You *can't* say that you haven't heard of the Voynich manuscript!)

With the exception of the rare books, most of the articles in the Cryptologic Collection can be borrowed. All the holdings are carefully cross-referenced, and [redacted] is always pleased to help you find what you are looking for. P.L. 86-36

(UNCLASSIFIED)

DOCID: 4019632

~~TOP SECRET UMBRA~~

...ling, and the patterns ir

...ion of the book are alphabetized FROM RIGHT TO LEFT.

WORDS AND PHRASES
(pp. 1 - 130)

This section contains individual words and a few common phrases. Th

material may be used to attack any portion of a message. Each entry in tl

~~TOP SECRET EIDER~~

EO 1.4.(c)
P.L. 86-36

The main sources of material

1. Captured German documer
activities of agents ir

2. Papers by Mr.Scott on t
systems.

P.L. 86-36

~~TOP SECRET GLINT~~

EO 1.4.(c)
P.L. 86-36

~~TOP SECRET GLINT~~

~~TOP SECRET UMBRA~~

DOCID: 4019632

EO 1.4.(c)
P.L. 86-36

"LETTERS TO THE EDITOR ARE COMING!"

PAUL REVERE'S RIDE TO NEW YORK

Yes, letters to the editor (and articles, too) are still coming, in response to Vera Filby's article "How Do We Know It's True?" (CRYPTOLOG, February 1976). Take, for example, the following letter, which is in response to an article that was written in response to Mrs. Filby's article.

P.L. 86-36

To the Editor, CRYPTOLOG:

There is a disquieting bias in Mr. David Gaddy's "On Being Truthful" (CRYPTOLOG, April 1976) which seems to want to pull "SIGINT equals truth" to the other side of the seesaw. To balance SIGINT's unsophisticated view of itself as being on the side of the angels, Mr. Gaddy points out intrinsic flaws in the SIGINT production process: sources might lie; some SIGINTers are more competent than others; the SIGINT facts suffer from interpretation; "sanitization and suppression" cause obfuscations; communications are susceptible to deception. He piles up the evidence until "SIGINT equals truth" slides to the other side of the fulcrum, where SIGINT is presented as inherently false.

What should we think, then, we SIGINTers? Is a SIGINT fact true? Yes. Emphatically, yes.

Certain basic principles underlie and guide any enterprise. In the SIGINT business one of these is that the lines of communications follow the chains of command. This means that organizations use electrical communications to systematically pass orders, requests, answers, plans, instructions, etc., and these communications speak for the organizations. Those lines of communications are not established to deceive us. That the SIGINT derived therefrom is true is really the only way to approach our profession.

I am convinced of this; yet I would join Mrs. Filby and Mr. Gaddy in encouraging a deception study to determine its frequency and the conditions under which it would likely occur. The results are sure to reinforce the value of SIGINT and to allow quick reply to inquiring non-SIGINTers, who, understanding little of the nature of the SIGINT beast, are prone to worry about that aspect of it they do understand -- its potential for deception.

In all fairness, though, deception is not the main point of Mr. Gaddy's article. But what is the main point? Is it his summary idea encouraging continuing "education, indoctrination, and training" about the limitations of SIGINT? I do not think so, because that is certainly an easily acceptable idea that scarcely requires much rationale in its support. Main point aside, I think Mr. Gaddy's most important point is his allegation that we add falseness to

EO 1.4.(c)
P.L. 86-36

After all, who is in the best position to judge the accuracy and validity of SIGINT? Is it not the professional SIGINTer? To use the bicentennial "VISINT" example now in vogue, should Paul Revere have dashed from house to house, giving his fellow-citizens a flee/no-flee option, thus: "Prearranged signals indicate British marching on a path that leads to our town"; then, in an aside, under this breath, "but don't blame me if you sacrifice a night's sleep and they never get here -- I'm just telling you what is reflected by the one-if-by land-two-if-by-sea signal." No. Paul Revere said, "To arms! The British are coming!" A cynical townsman -- at least one -- probably said, "What does that turkey know? I'm going back to bed." But, as we now know, there were few practicing cynics in those days; and, if any, they were probably doomed to obscurity because of it. History shows that Paul was believed. But why was he believed? Because he was trusted. He was a hard-working technician, deeply involved in his pursuits and well known for his competence -- he often provided fellow-citizens good counsel. The townspeople trusted him to understand what was going on and relied on his judgment.

P.L. 86-36

Also, Paul was believed because his message was direct, unequivocal, forceful. Its point was not begged by passive constructions, nor cheapened by apologetic phrases, nor clouded over by stereotyped redundancies. His message neither required nor encouraged further interpretation. The townsfolk heard, believed, and reacted. Likewise, SIGINT product would become more effective if our reporting faithfully adhered to these same principles. The suppression of evidence incidental to the SIGINT fact -- evidence whose lesser lights do more to divert attention than they do to illuminate truth -- rather than obfuscating the SIGINT fact, would help us present it in a professional manner. The suppression of nonessential data is not a burden to the reporter. It is, rather, a precept fundamental to the reporting discipline. It is good reporting.

E.O. 1.4.(c)
P.L. 86-36

[redacted] V12

~~(SECRET SPOKE)~~

P.L. 86-36

Mr. Gaddy replies:

To the Editor, CRYPTOLOG:

Thank you for the opportunity to comment on [redacted] letter.

I am afraid that his reaction demonstrates that the attitude I deplored is so ingrained in some of us that an attempt at redress -- moving the pendulum back to a neutral midpoint by reminding ourselves just what we're about -- is instantly construed as a swing to the opposite extreme. I intended to be "disquieting." My "bias," on the other hand, was toward objectivity: I was attacking attitudes, not SIGINT. The attitude I was specifically after is cocki-

DOCID: 4019632

P.L. 86-36

ness, "an unseemly air of intellectual arrogance." That was my main point, stated in the second paragraph. To develop it, I recalled the components of COMINT, not to illustrate "intrinsic flaws in the SIGINT production process," but as realities, as givens. Total, balanced recognition of these givens marks the SIGINT professional, not the sign over his desk saying "SIGINT doesn't lie." And it was the SIGINT pro's attitude that I so extravagantly praised.

Rather than rebut the strawman précis of my views advanced by [redacted] may I take issue with what he says about deception (which, some readers may recall, was Mrs. Filby's original point). A mind closed to the likelihood of deception is a likely candidate for deception. The now universally recognized "basic principles" on which SIGINT depends are, at the same time, the cornerstones for a program of deception. We generally possess a high level of confidence that (in part because it is so difficult to pull off) deception will not be used or, if it is, that we will be smart enough to detect it. As long as that "high level" is not absolute, I share [redacted] attitude. I do not expect deception in the mass of normal, "peacetime" intercept, for example. On the other hand, I except a foe to be as wily as I would propose to be. Without citing October 1864 as an early example of enemy use of deception against the U.S. Army, I would commend to [redacted] (and other readers who have not delved into it) Brown's recent *Bodyguard of Lies*. The test of camouflage is not whether you see it, but whether you don't.

Finally, I must say that I am as puzzled over the Paul Revere story as when I first heard it used to construct some sort of analogy. It's a good example of signal communication, but loses me at that point. Does the horse equate to CRITICOMM?

David W. Gaddy, D5

~~(CONFIDENTIAL - HVCCO)~~

So does Mrs. Filby:

To the Editor, CRYPTOLOG:

You have asked me to comment on [redacted] response to Dave Gaddy's response to my article on deception. My comment is, great! This is just the kind of discussion I wanted to start. And as in all good, lively, informed discussions, not only is the main theme developed, but also sidelights and subtleties and related aspects emerge. This happened in both these responses as well as in those from [redacted] (May CRYPTOLOG) and [redacted] (June-July CRYPTOLOG). The next stage that we apparently all want to get to is the serious research into the facts of communications deception, to the degree that we can ascertain them. We know there has been deception [redacted] in North Vietnamese communications in recent years. Where else? Can't we get everything we know assembled for study? Then we can proceed to an evaluation of the extent and circumstances of deception, the possibilities of recognizing it, and the chances of missing it. Granted, to some extent, this is like research into psychic phenomena, in that it may be an effort to know the unknowable -- but at least we can learn something in trying.

P.L. 86-36

Vera R. Filby, E12

~~(SECRET SPOKE)~~

EO 1.4.(c)
P.L. 86-36

SORUTION TO NSA-CROSTIC No. 4 (CRYPTOROG, June-Jury 1976):

Jacob Gurin[-san], "[Employment of] Military Linguists,"

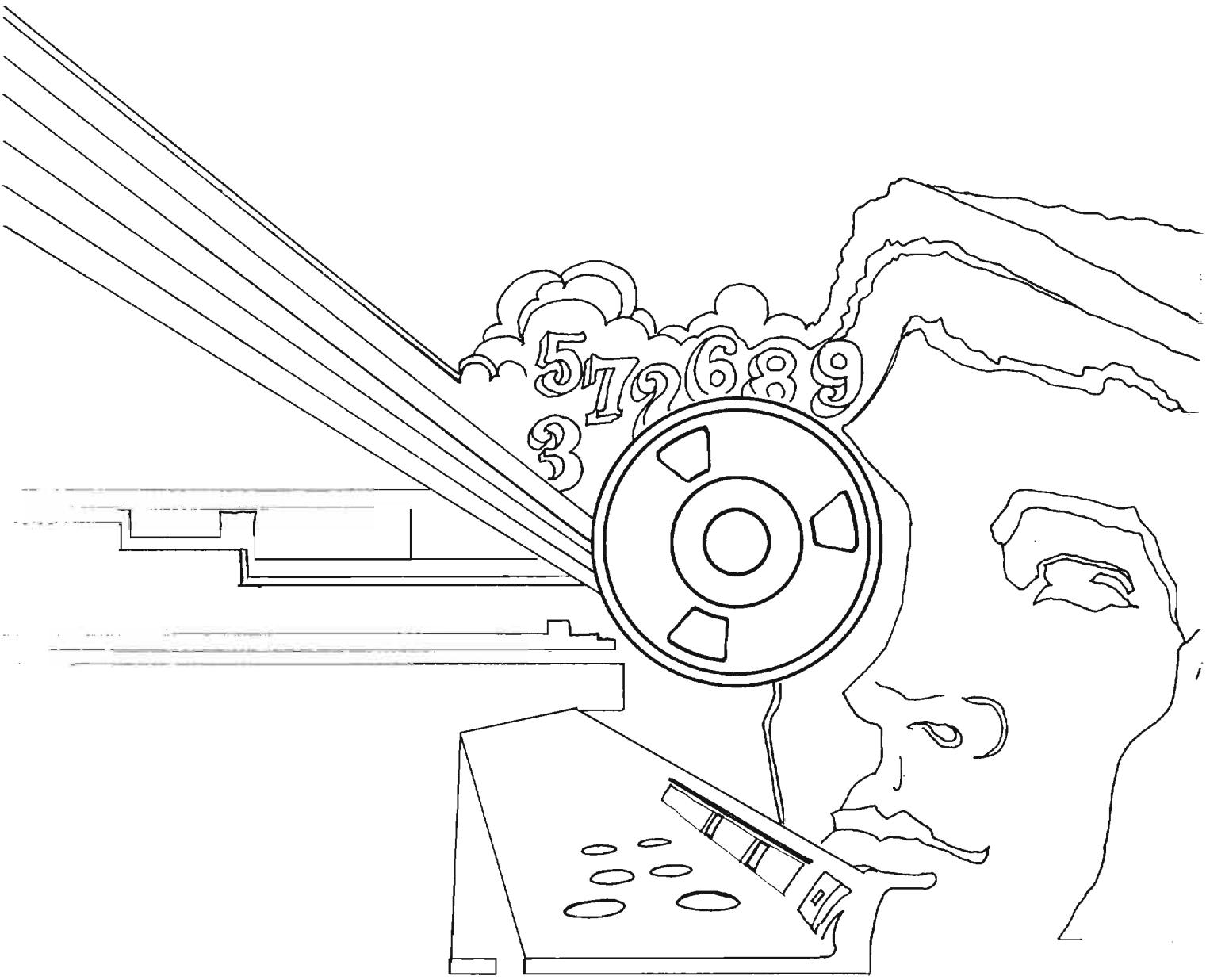
NSA Technical Journal, Vol. XIII, No. 4, Fall 1968. (Also reprinted in *NSA Technical Journal: Special Linguistics Issue II.)*

"During the showing of a Japanese movie used as a training aid the students cheered mightily when, after about one hour of total lack of comprehension, they understood the maid when she knocked on the door and said 'Excuse me.'"

(UNCLASSIFIED)

Pl-Jun 76-S3-24723

~~TOP SECRET~~



DOCID: 4009733

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JUNE-JULY 1976

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

COMPUTERS IN ELINT AND TELEMETRY..... [redacted] 1
"RIGHT ON, VERA!"..... 7
TRANSLITERATION OR CYRILLIC?..... [redacted] 8
COMMENTS ON AG-22/IATS..... 13
NSA-CROSTIC No. 4.....A.J.S..... 18
THE MARQUIS AND THE MEDIUM.....Reed Dawson..... 20
THE [redacted] COLLECTION SYSTEM.....Tim Murphy..... 21
HOW THINGS HAVE CHANGED!..... [redacted] 25
CHINESE MACHINE TRANSLATION:
NOTES ON TRANSLATION FROM THE CHINESE... [redacted] ..26
SCIENTIFIC CHINESE MACHINE TRANSLATION.. [redacted] ..28
LETTER TO THE EDITOR..... 29

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009733

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. III, Nos. 6 and 7 JUNE-JULY 1976

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5642s)

Collection.....[redacted] (8955s)

Cryptanalysis.....[redacted] (8025s)

Language.....Emery W. Tetrault (5236s)

Machine Support.....[redacted] (3321s)

Mathematics.....Reed Dawson (3957s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Frederic O. Mason, Jr. (4142s)

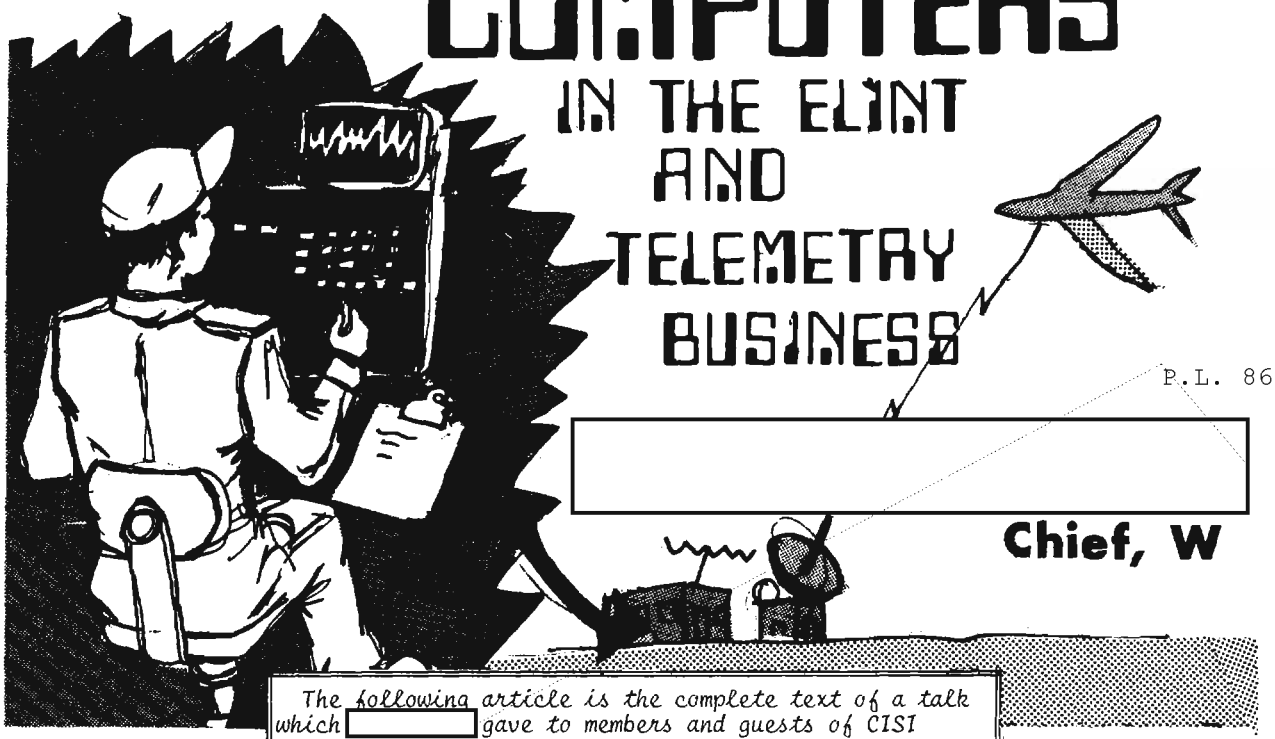
P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4009733

COMPUTERS IN THE ELINT AND TELEMETRY BUSINESS



P.L. 86-36

[redacted]

Chief, W

The following article is the complete text of a talk which [redacted] gave to members and guests of CISI (NSA Computer and Information Sciences Institute) in the Friedman Auditorium on 22 January 1976.

In order for you to calibrate what I have to say, I want to make it very clear that I am not a computer expert. I have never participated in the design of any computers, I have had little operational experience with the care and feeding of them, and I have never written software. But I have had the opportunity to help design and work with a number of systems that use computers in very important ways, and I am in a position now to affect the market for computers in the ELINT and telemetry business. I'll be directing my remarks at *uses*, not computers themselves.

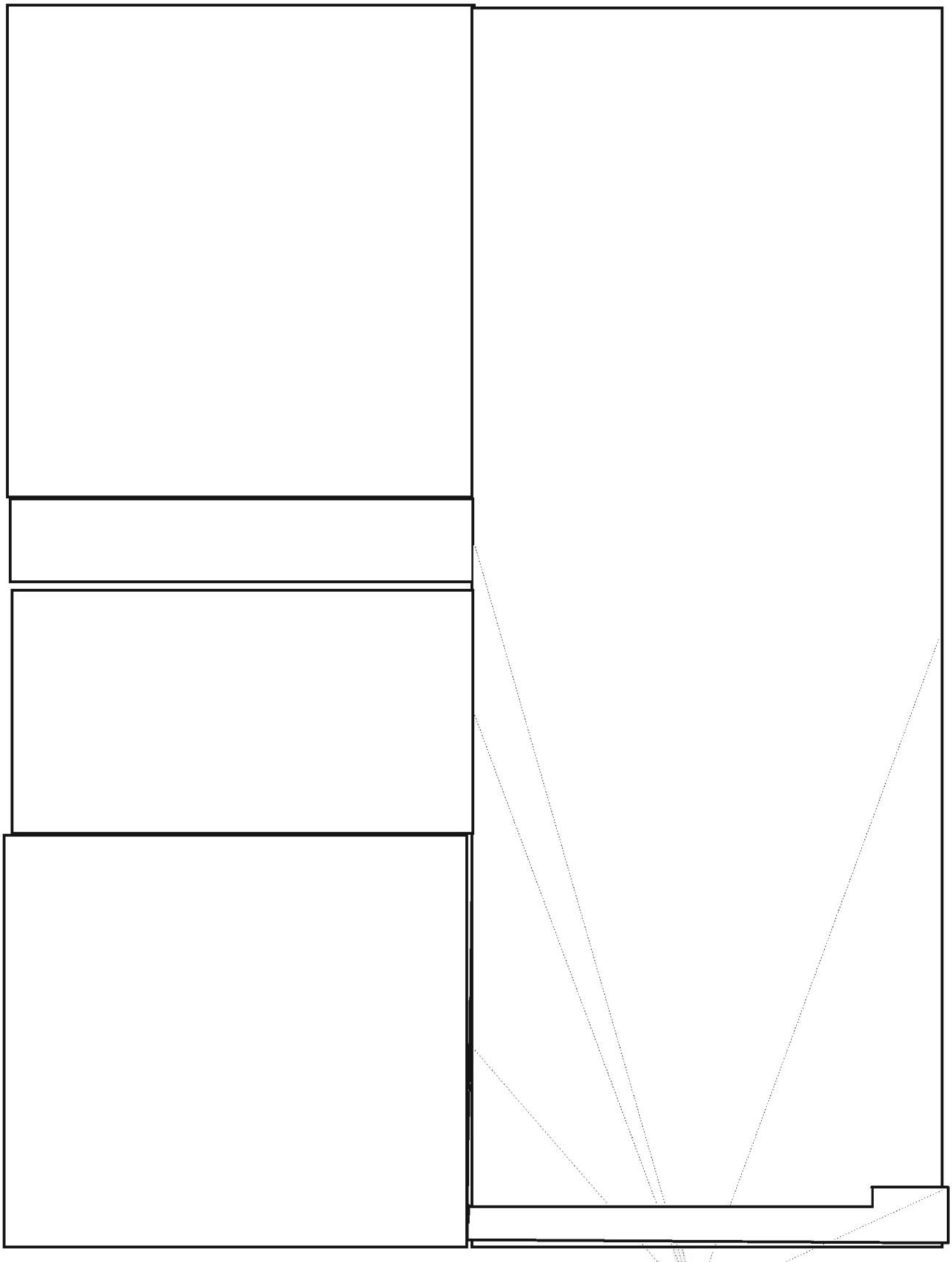
When you don't intend to say anything very profound (or may be afraid that you won't, although it is all that you know), you often call your talk or book an "Introduction to. . ." I've resisted that today, just to lure more of you here. But it was suggested to me that a brief introduction to ELINT and telemetry might be in order. I'll start with that and keep it *very* basic. Then I'll phase into the description of a current set of computer applications, and end with what I see as real trends in this area.

[redacted]

[redacted]

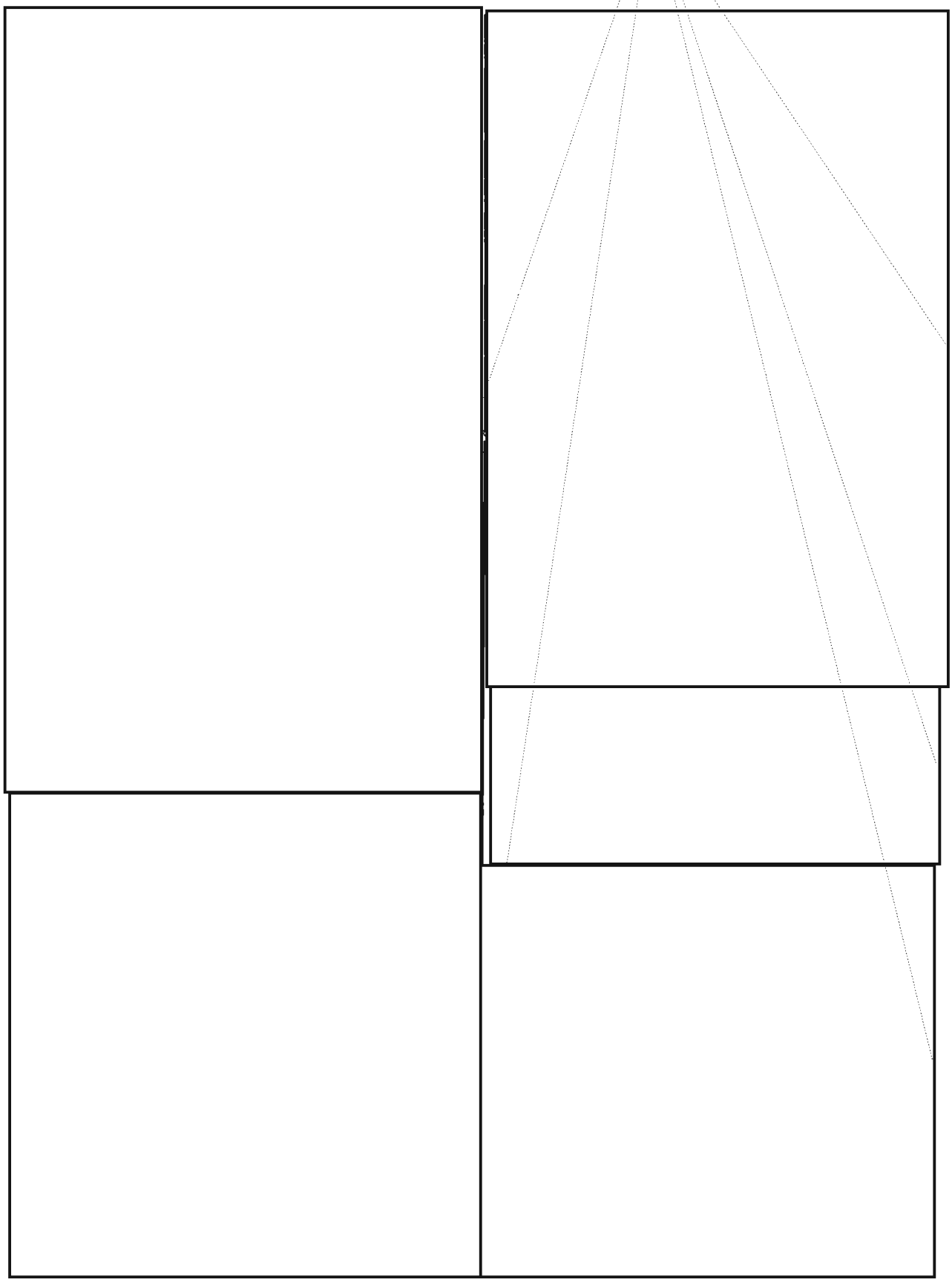
EO 1.4.(c)
P.L. 86-36

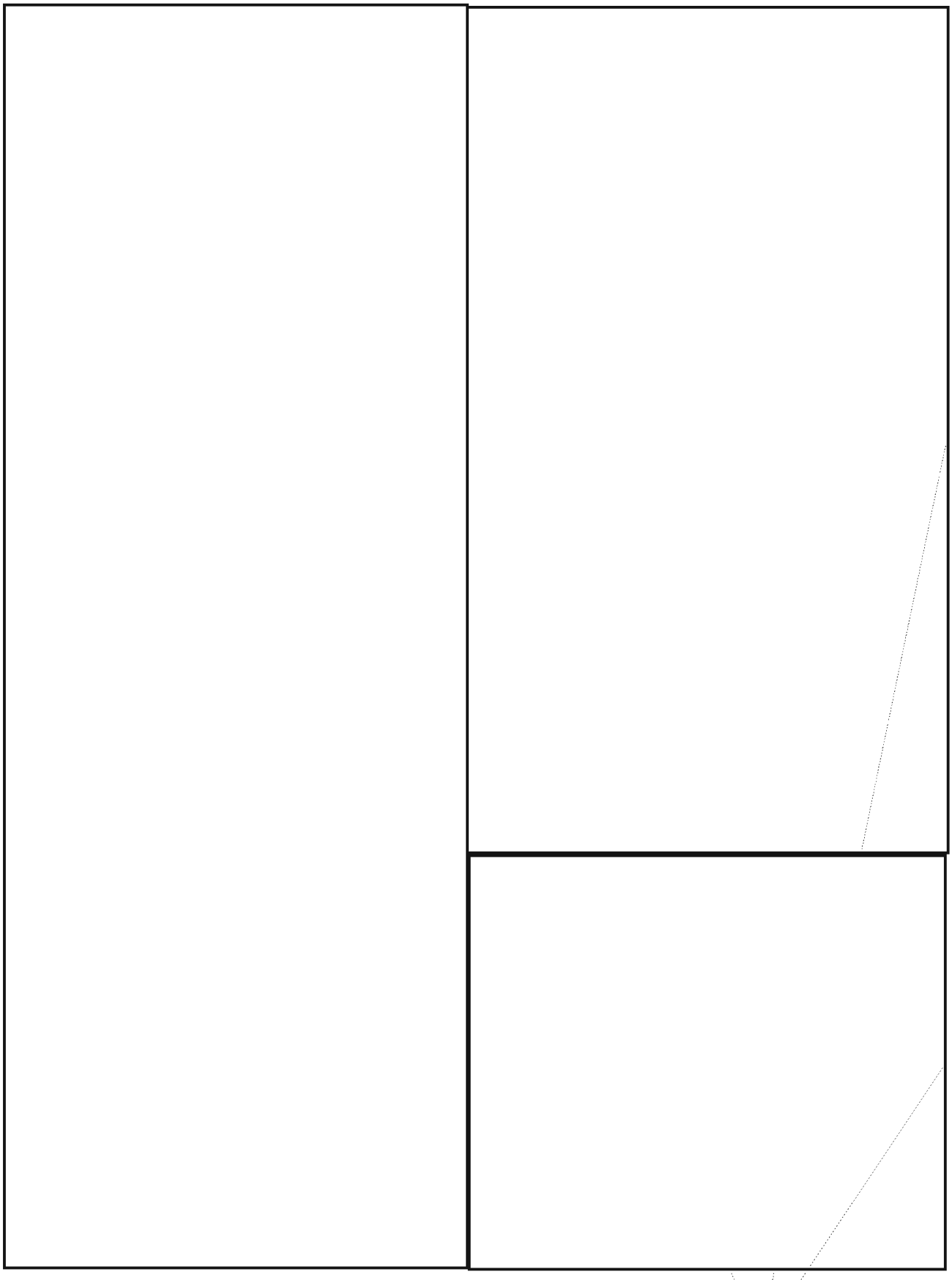
HANDLE VIA COMINT CHANNELS ONLY



EO 1.4.(c)
P.L. 86-36

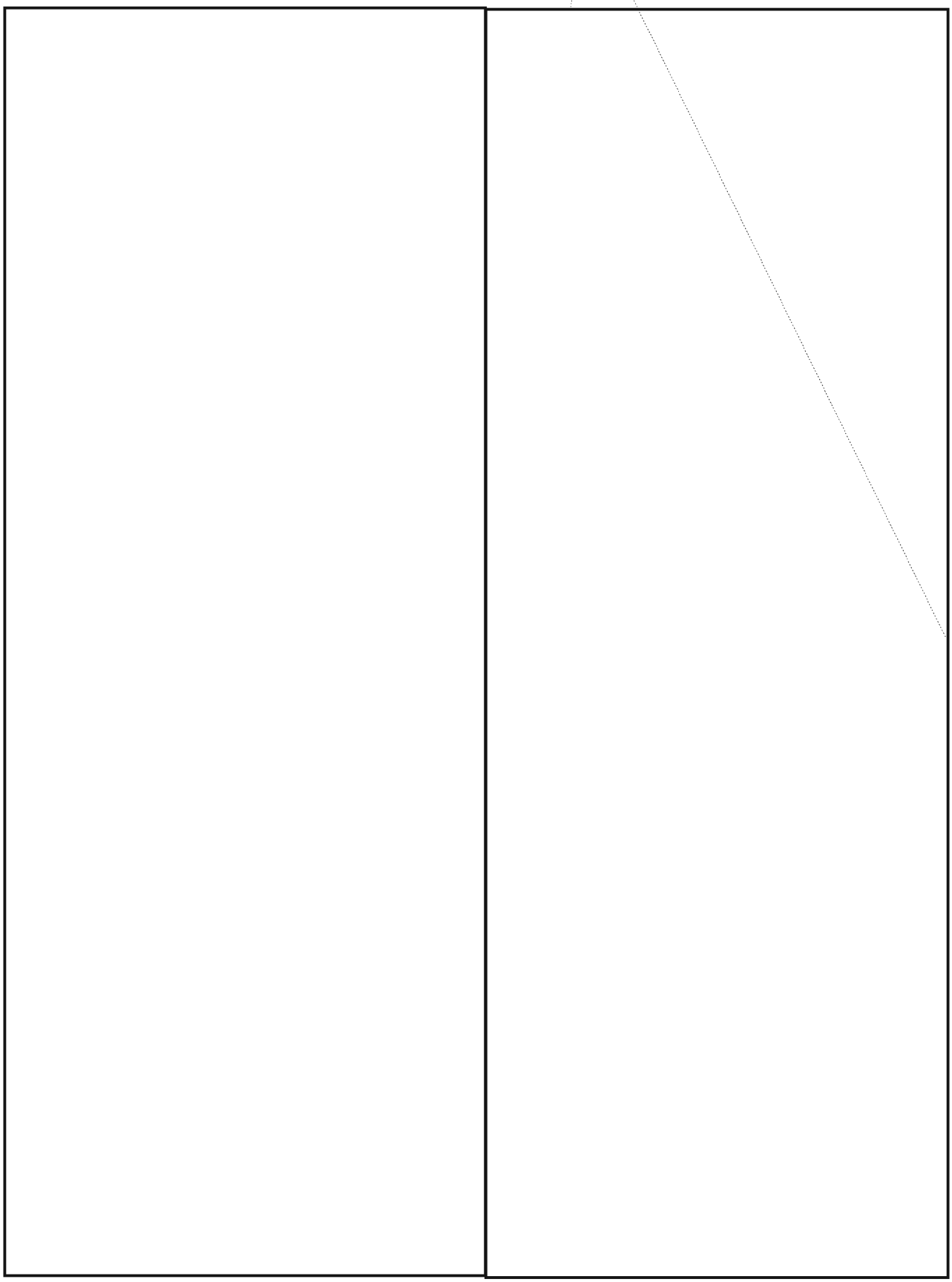
EO 1.4.(c)
P.L. 86-36



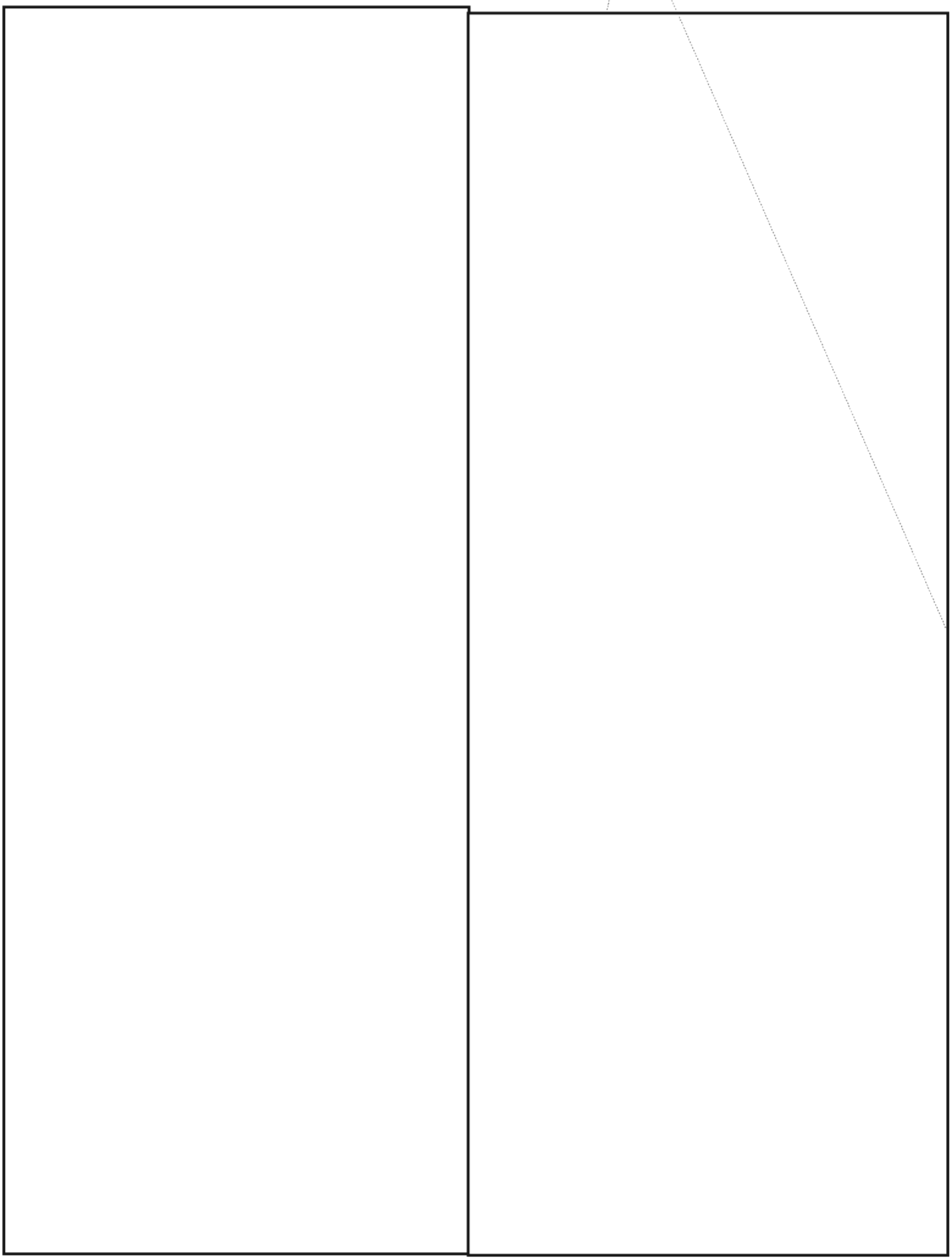


EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36



TOP SECRET

EO 1.4.(c)
P.L. 86-36

[redacted]

(TOP SECRET - HVCCO)

P.L. 86-36

"RIGHT ON, VERA!"

Vera Filby's article on radio deception, "How Do We Know It's True?" (CRYPTOLOG, February 1976), has elicited much comment here at the Agency, and has even prompted a couple of people to put their thoughts on paper (see "On Being Truthful," by [redacted] CRYPTOLOG, April 1976, and "Some Principles of Cover and Deception," by [redacted] CRYPTOLOG, May 1976). The following message from Germany indicates that the subject of radio deception is indeed, as Ms. Filby pointed out, one of vital concern to other Agencies as well as our own. MGEN Smith has granted his permission to publish his remarks in full.

Ed.

FM: NCEUR [redacted] EO 1.4.(c) P.L. 86-36

TO: NSOC

(E12, DDF, A, A7, A8)

FOR VERA FILBY FROM [redacted] P.L. 86-36

SUBJ: HOW DO WE KNOW IT'S TRUE?

REF: [redacted]

B. CRYPTOLOG MAGAZINE, FEBRUARY 1976, PAGE 6

1. VERA, YOUR ITEM IN THE FEBRUARY 76 CRYPTOLOG RECEIVED MUCH INTEREST HERE AT STUTTGART. BY COINCIDENCE (UNLESS YOU PLANNED IT THAT WAY), THE TIMING WAS EXCELLENT. THE DIRECTOR OF INTELLIGENCE FOR USEUCOM, MGEN H. P. SMITH, IS VERY INTERESTED IN SIGINT DECEPTION. RECENTLY HE SENT A MESSAGE TO [redacted] REQUESTING THAT THEY SEND A TEAM TO EUROPE TO BRIEF ON THIS SUBJECT (SEE REF ALFA). I SENT A COPY OF YOUR ARTICLE TO MGEN SMITH AND ON 24 MARCH HE WROTE THE FOLLOWING COMMENTS:

EO 1.4.(c)
P.L. 86-36

QUOTE

1. VERY INTERESTING! RIGHT ON!

2. IT SOUNDS LIKE THE AUTHOR IS NOT AWARE OF [redacted] --SO THOSE TWO ORGANIZATIONS SHOULD BE PUT IN TOUCH WITH ONE ANOTHER.

3. I WOULD SUGGEST ALL THE CRYPTOLOGIC ORGANIZATIONS GET TOGETHER FIRST AND POOL ALL THEIR KNOWLEDGE AND SPECIFIC EXAMPLES THEN ENLARGE A SUBSEQUENT MEETING TO INCLUDE GENERAL INTEL TYPES, PERSONS WITH ACTUAL EXPERIENCE IN COMBAT ZONES WHERE COMM DECEPTION HAS BEEN USED.

4. THEN CONDUCT COURSES IN EACH THEATER, PREPARE "TOOLS" AND "GUIDES."
END QUOTE

(CONFIDENTIAL - HVCCO)

DOCID: 4009733

ТРАНСЛИТЕРАЦИЯ ИЛИ КИРИЛЛИЦА?
TRANSLITERATsIYa ILI KIRILLITsA?
TRANSLITERATION OR CYRILLIC?
ТРЭНЗЛИТЕРЭЙШН ОР СИРИЛЛИК?

[redacted] P.L. 86-36

To be or not to be? That is the question. Whether 'tis nobler to transliterate or render in the original. . .

That's not quite how the quote goes, but the problem seems to have been around at least as long as Hamlet. I would also venture a guess that we here at NSA have collectively expended considerably more nervous energy on our problem than Hamlet did on his. It seems that every 3 to 5 years the spectre of transliteration raises its ugly head anew, and all the decisions we made in the last skirmish have to be "rediscovered" and "restated" yet another time.

Why this problem refuses to stay solved is difficult to determine. Could I suggest, however, that it is because we have not yet solved it?

Having spent about 10 years (1960-1969) transcribing, analyzing, and reporting Russian [redacted] I am aware -- painfully aware -- that discussions of transliteration tend to get very emotional and highly provincial.

In an attempt to lower the emotional content of this article, let me begin by offering a definition of transliteration and then explaining some concepts and properties of transliteration.

Transliteration, as I will be using the term, refers to transforming textual information from one alphabet to another. The properties of a good transliteration scheme are that the scheme should retain as much information about the original as possible, and that it should be easily learned and used by the persons using the particular scheme. In particular, I will be addressing only Russian-to-English transliteration. [redacted]

Editor's two-cents' worth

Before letting the author get into the body of his article, the editor feels that it might be advisable to take an explanatory side trip, to make certain that everyone knows exactly what transliteration *is* and what it *isn't*. Well, it isn't translation and it isn't transcription. Let's take the following hypothetical situation. You're Mike. You're on a tour of the Soviet Union. You'd like to meet some Russian girls, but your guide watches your busload like a hawk. Finally, one day, you and another guy (Joe) manage to exchange a few remarks with a cute-looking girl standing in line outside of Lenin's Mausoleum. You don't speak Russian, so Joe helps out. Here are a few of the interchanges.

Girl: **Дай мне поцелуй.**
Mike: What did she say?
Joe: **Дай мне поцелуй.**
Mike: No, I don't mean what did she *say?* I mean, what does it *mean?*
Joe: It means "Gimme a kiss!"

Girl: **Как тебя зовут?**
Joe: She wants to know your name.

Girl: **Меня зовут Тамара.**
Joe: She says her name is Tamara.

Girl: **Как вам нравится Москва?**
Joe: She wants to know how we like Moscow.

Just then the guide shows up and shoos you both back onto the bus. [redacted] EO 1.4.(c) P.L. 86-36

Mike: See you "Tamara"! -- same time, same place!

On the bus, you write down in your handy-phrases notebook (for a nonlinguist, you have excellent auditory acuity and retentivity):

Diamon' yeah putza Louie.
Kahk tibyah zuhvoot?
Minyah zuhvoot Tamara.
Kakh vahm nraveetsa Muskva?

Joe looks over your shoulder and says, "You're spelling everything all wrong!" He crosses out what you wrote and puts down:

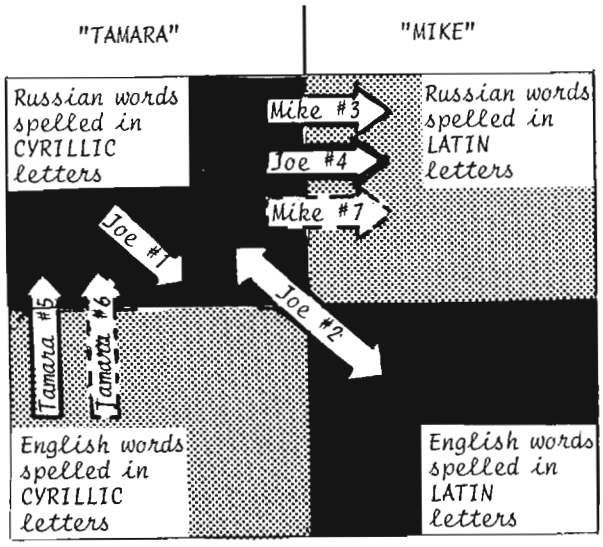
DOCID: 4009733

Day mne potseluy.
Kak tebya zovut?
Menya zovut Tamara.
Kak vam nravitsya Moskva?

Meanwhile, back at the Mausoleum, Tamara has jotted down two names in *her* notebook:

Майк, Джо

A lot happened during these brief interchanges, linguistically (if not romantically) speaking. Let's extrapolate everything into a representation of the entire Russian language (left-hand side, "Tamara") and the entire English language (right-hand side, "Mike").



When Mike asked, "What did she say?" and Joe answered, "She said, **Дай мне поцелуй**" (arrow "Joe #1"), that didn't help Mike much. It was still in Russian! When this process occurs in the COMINT business (that is, listening to people talking in Russian, then putting down on paper, *in Russian*, what they said) it is called TRANSCRIPTION. The process is concerned, sure enough, with what the speaker *said* (his exact words, as he spoke them), but it doesn't help the nonlinguist analyst any. He still doesn't know what it means! (Incidentally, even though this step doesn't yield the English meaning, the voice transcriber has a hard job to do, and he certainly has to *know* what the person is talking about before he can transcribe it.)

What Joe did, after his first little "joke," was to INTERPRET for Mike and Tamara (arrow "Joe #2"). Interpretation is translation, usually back and forth, from one *spoken* language to another. People in the COMINT business rarely are involved in interpretation. Instead, they are usually involved in TRANSLATION (the transformation of text in one *written* language to another written language -- and usually NSA translators specialize in the "into English" direction). Interpretation and translation are concerned with what the utterance *means*. Mike and the NSA nonlinguist don't care a rat's whisker about how the linguist derives the meaning, or how hard it is to master those complicated morphologic and syntactic rules. For example, Joe didn't bother to tell Mike that he changed Tamara's "How does Moscow please itself to you?" to "How do you like Moscow?" or to explain that he "translated" the name of the Russian city from "Moskva" to English "Moscow." As far as the nonlinguist is concerned, it's as easy for the translator to translate as it is for the transcriber to transcribe. So the nonlinguist feels that that should be the end of the problem.

What, then, are those other five arrows doing in the chart? They do not deal with the meanings of the words, but only with their representation in printed form.

When Mike decided, for example, to record the Russian sentences he wanted to remember (arrow "Mike #3"), he did something similar to TRANSCRIPTION ("Joe #1"). But, instead of COMINT-style transcription (writing down on paper the utterance in the original language, as spelled in the original alphabet), he tried to record the Russian sentences in Latin letters on the basis of the Russian *pronunciation*. (This can be done scientifically, but when it's done by amateurs like Mike, it usually looks weird.)

When Joe looked over Mike's shoulder and "corrected" the spelling (arrow "Joe #4"), he was -- we're finally hitting paydirt! -- engaged in TRANSLITERATION. This is what this article, once we get to it, is all about: the spelling of Russian words in Latin letters on the basis of their original Cyrillic *spelling*. The problem is, "Who's got the one true system?" Joe used a system of transliteration in which the Russian letter **й** is represented by "y." If he had used the NSA system, he would have written, *"Daj mne potseluj!"* (non-NSAers say that all those "j's" "look funny").

When Tamara wrote the two names in her notebook (arrow "Tamara #5"), she TRANSCRIBED the names into Cyrillic on the basis of their *sound*. She wrote **Майк** and **Джо**. She would have been wrong (arrow "Tamara #6") to transliterate them according to their *Latin spelling*: **Мике** and **Йое** (that would make them pronounceable in Russian as "Meek-yeah" and "Yoh-yeah"). Ridiculous, isn't it? And yet there are English words in the Russian language which are spelled in Cyrillic and pronounced in Russian in such a ridiculous way.

If Mike were ever to read Tamara's notebook and laboriously transliterate the two names into Latin characters (arrow "Mike #7"), he would obtain "Mayk" ("Majk") and "Dzho." Would he recognize his own name or Joe's? Or would

he be completely unaware that he had come up against one of the translator's biggest problems -- the rendition of non-Russian personal names, place names, etc. not by transliteration but by restoring them to their original Latin spellings: not "Nikson," "*Taym* magazine," "Reno," but "Nixon," "TIME magazine," and "Renault."

Transliteration as we will discuss it, then, is a very specific operation: the transformation of Russian text, in Cyrillic characters, into the Latin alphabet according to a specific preferred scheme. The transliteration process does not produce a translation, but carries into the Latin representation all the grammatical information present in the Cyrillic text. Hence the meaning content of the Latin-transliteration text is identical with the meaning content of the original Cyrillic text, and both texts would yield the identical translation.

Several Russian-to-Latin transliteration schemes have been developed. Table 1 shows only a few of them. The list of schemes is not intended to be exhaustive, but, rather, to show the "flavor" of the transliteration world. The various schemes conform, to a greater or lesser degree, to the requirements of accuracy (that is, nonambiguity) and ease of use. Of particular interest is the various handling of the Cyrillic letters

Ъ, ъ, ж, й, х, ц, ч, ш, щ, ъ, ь, э, ю, я

(14 out of the 33 letters in the Russian alphabet).

Note that:

- [redacted] most schemes use combinations of Latin characters to represent certain Cyrillic characters (that is, the Cyrillic and Latin characters do not constitute a one-to-one mapping);
- [redacted] most schemes contain inherent ambiguities, in that certain combinations of Latin letters can represent two different Cyrillic situations, and it is sometimes impossible to tell from context which of the two possible Cyrillic situations had occurred in the original text. (For any mathematicians still reading, they are not an "onto" mapping).

The question which should arise at this point is, "Why?" Why transliterate? Or, if you must, then why in so many different ways? Or even, why worry about the fact that Joe likes [redacted] while Tom likes [redacted] and Harry simply has to have BGN?

The answer to the simplest of these questions is clear, and is probably a derivative or corollary to Murphy's Law: "If Tom, Joe, and Harry,

Table 1

Russian	*Board on Geographic Names*	*Library of Congress*[1]	*International Standards Orgn.*
А	A	A	A
Б	B	B	B
В	V	V	V
Г	G	G	G
Д	D	D	D
Е	E, YE[2]	E	E
Ё	E, YE[2]	E	Ë
Ж	ZH	ZH	Ž
З	Z	Z	Z
И	I	I	I
Й	Y	I	J
К	K	K	K
Л	L	L	L
М	M	M	M
Н	N	N	N
О	O	O	O
П	P	P	P
Р	R	R	R
С	S	S	S
Т	T	T	T
У	U	U	U
Ф	F	F	F
Х	KH	KH	H
Ц	TS	TS	C
Ч	CH	CH	Č
Ш	SH	SH	Š
Щ	SHCH	SHCH	ŠČ
Ъ	"	"	"
Ы	Y	Y	Y
Ь	'	'	'
Э	E	E	È
Ю	YU	IU	JU
Я	YA	IA	JA

[1]"Modified" system, which omits the diacritics used in the preferred LC system.

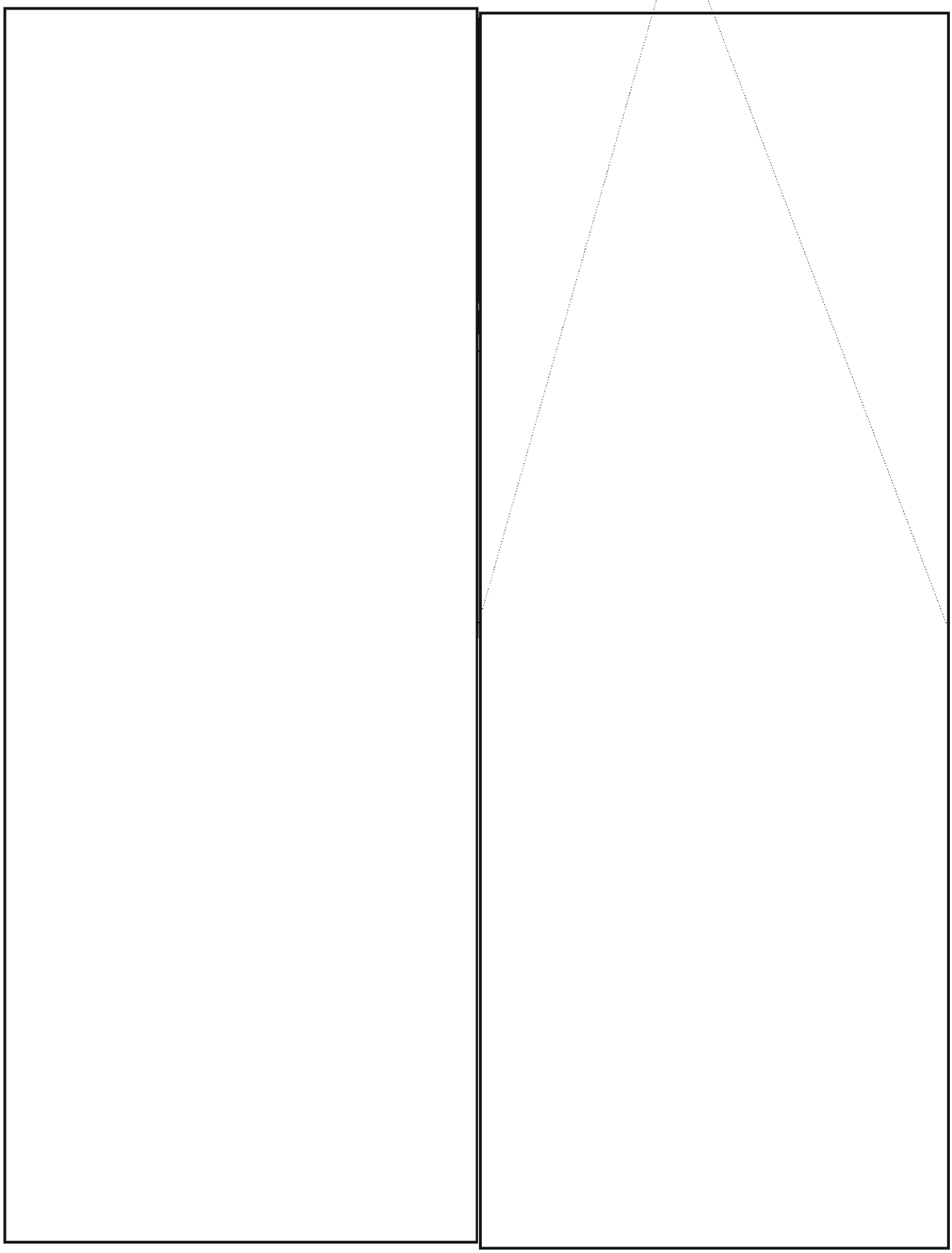
[2]E or Ë when preceded by consonant. Otherwise (initial, or when preceded by vowel) YE or YË.

as noted above, keep their data in different transliteration schemes, then they *shall* be tasked to produce a joint report, or else, because of their own respective missions, they *shall* find it absolutely necessary to merge two (or more) of the computer data files involved here."

[redacted]

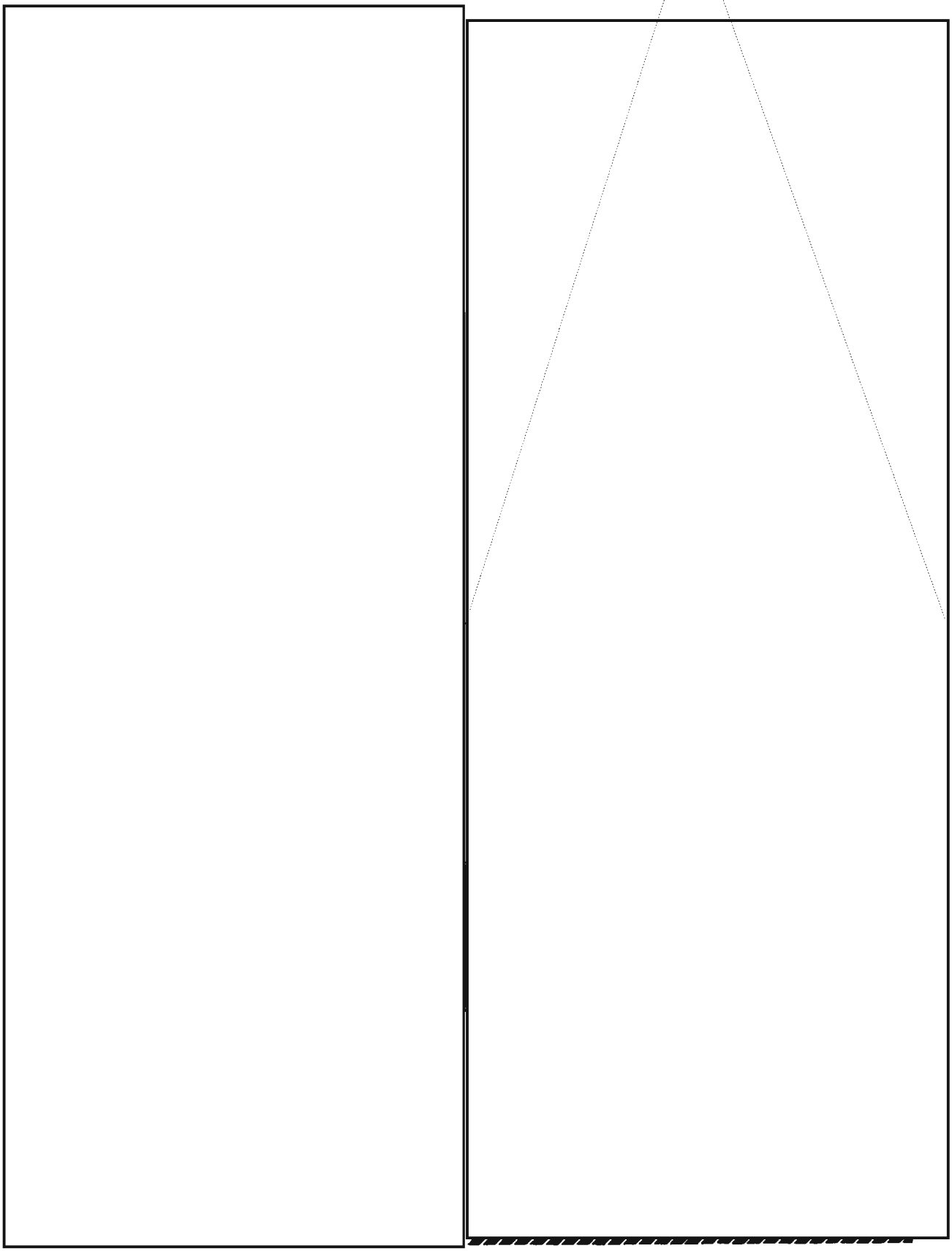
EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

~~CONFIDENTIAL~~



COMMENTS AS REQUESTED! (More on the AG-22/IATS)

P.L. 86-36

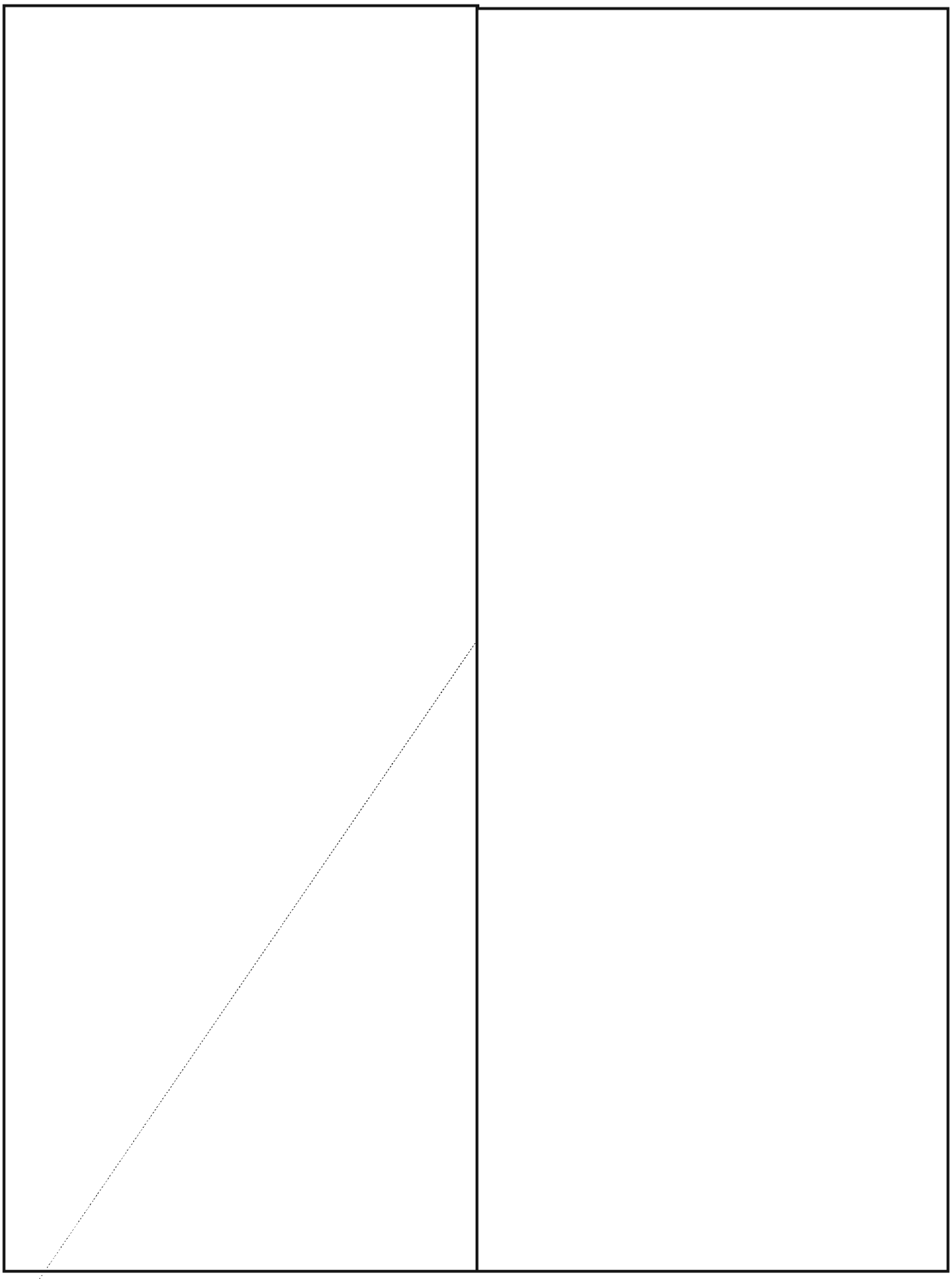
At the end of his article, "Musings About the AG-22/IATS" (CRYPTOLOG, March 1976), Cecil Phillips asked, "Comments, anyone?" Well, comments he's received! [redacted] ("What's Wrong With AG-22/IATS?") appeared in the May 1976 issue of CRYPTOLOG. The following comments which were recently received seem to be worth publishing in full, despite their slight overlappings in treatment. CRYPTOLOG would continue to welcome further comments of a substantive nature on this subject.

Ed.

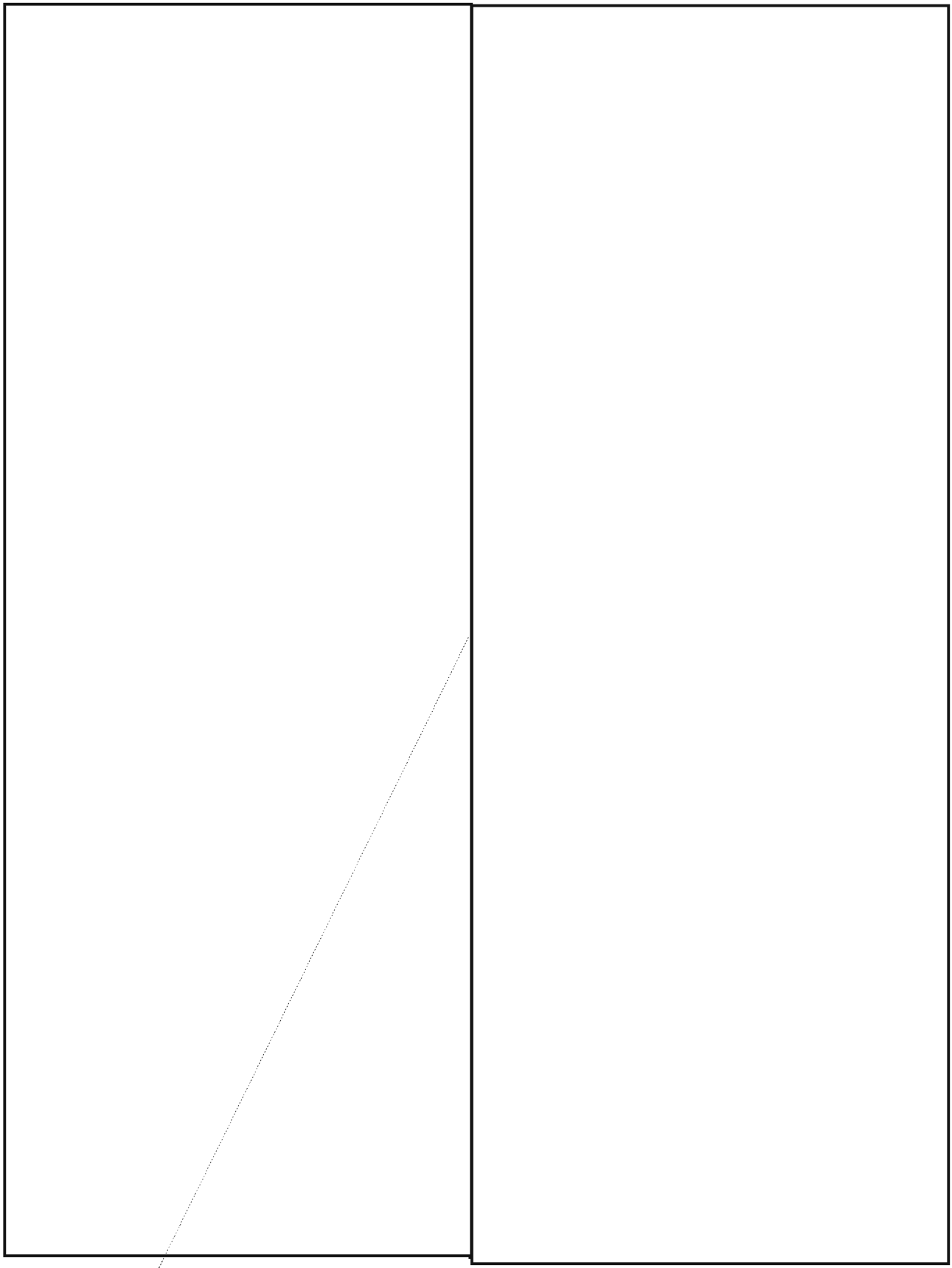
[redacted]

[redacted]

EO 1.4.(c)
P.L. 86-36



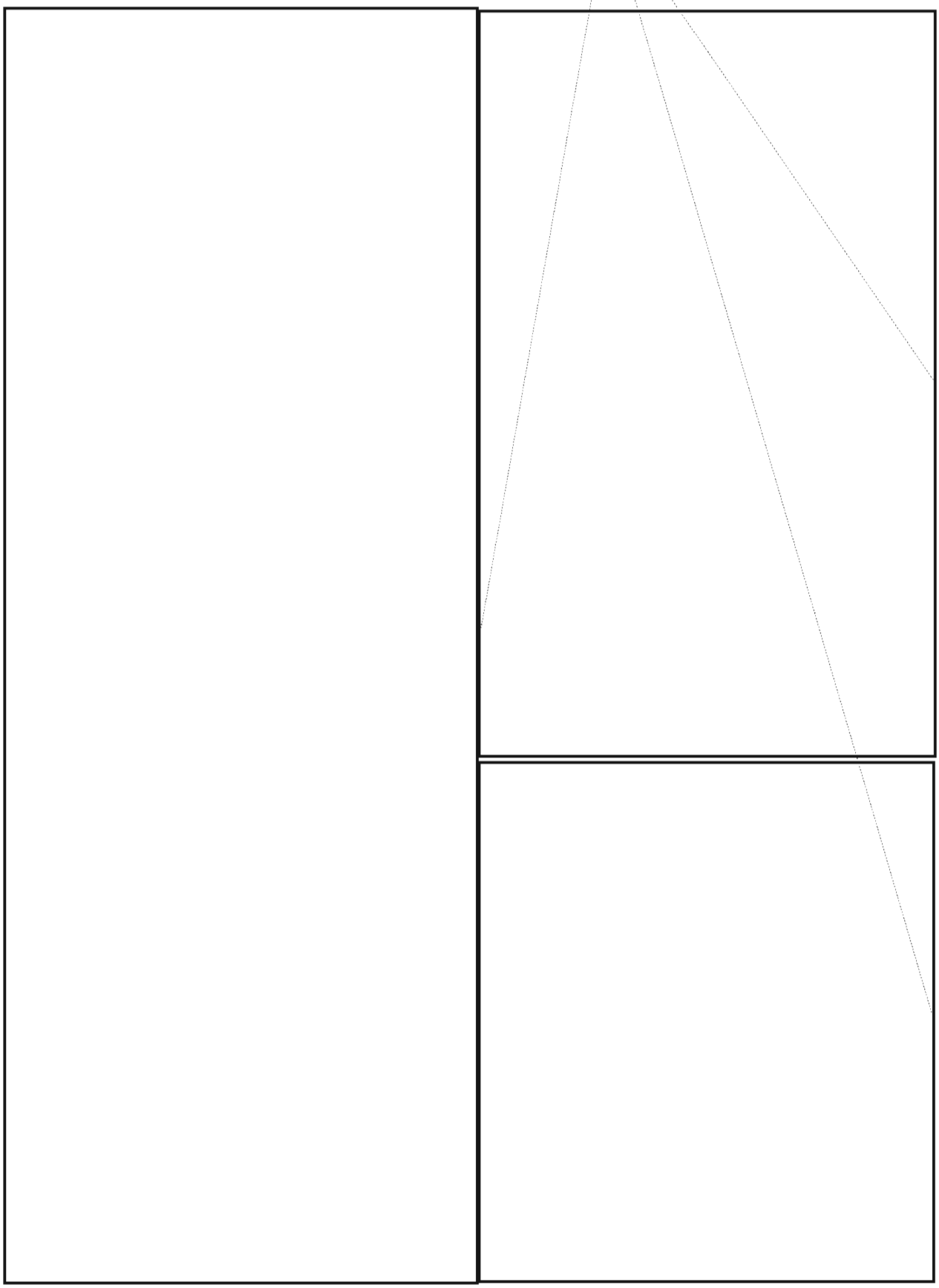
P.L. 86-36
EO 1.4.(c)



P.L. 86-36
EO 1.4.(c)

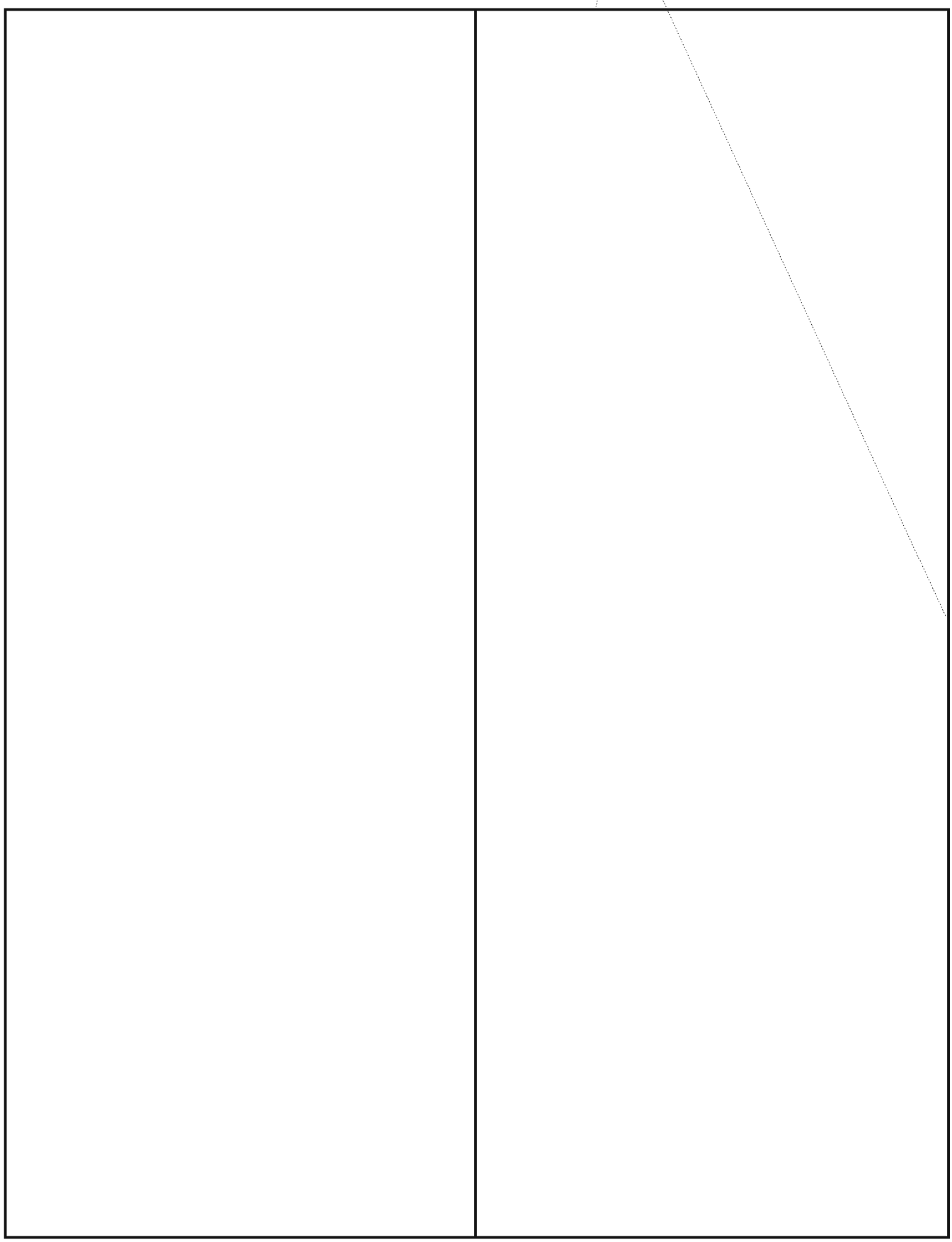
~~CONFIDENTIAL~~

EO 1.4.(c)
P.L. 86-36



~~CONFIDENTIAL~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36



DOCID: 4009733

UNCLASSIFIED

NSA-CROSTIC NO. 4

By A.J.S.

The quotation on the next page was taken from a published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS

A. Allegedly the ones most likely to appreciate SST flights (2 wds)

B. Abnormally enlarged masses of lymphoid tissue at back of the pharynx

C. Pseudonym of Emmanuel Poiré, French caricaturist (2 wds; read as one word, a Russian pun)

D. "--- man out" (game)

E. Covered stone bridge in Venice, connecting ducal palace with the state prison (3 wds)

F. What circling tigers in *Little Black Sambo* turned into

G. Ignored

H. French painter of flowers (famous for paintings of roses) (1759-1840)

I. "Sleeping Woman," dormant volcano in Mexico (last eruption, 1868)

J. State (abbrv)

K. He "opened up" Japan (2 wds)

L. Poem by Rudyard Kipling

M. Scout

N. Hot mixed drink, topped with whipped cream (2 wds)

O. Popular U.S. dance for several decades prior to 1910; superseded by fox trot

P. Despite what NSA linguist's father (Georgia, late 1940's) said when son decided to major in Spanish ("If English was good enough for Jesus, it ought to be good enough for you!"), the language spoken by Jesus

Q. Sharpen again

R. Japanese admiral; at time of Pearl Harbor attack, commander-in-chief of combined fleet

S. What showoff Fritz said to his brother (they had been mountain-climbing with their mother) (4 wds)

T. One of the mightiest rivers of the Indian subcontinent

U. Partially compacted granular snow that forms the surface part of the upper end of a glacier

WORDS

A.	20	180	55	120	35	73							
B.	23	50	67	5	88	31	164	34					
C.	62	42	97	103	80	57	37	107	125	27			
D.	95	170	174										
E.	87	167	143	130	6	182	112	18	10	45	71	162	61
F.	16	117	157	175									
G.	178	92	78	131	53	158	118	144					
H.	66	163	1	29	96	51	140						
I.	173	176	7	19	155	74	63	2	39	83	104		
J.	46	150											
K.	141	21	124	100	72	25	13	114	79	41	85	76	
L.	14	110											
M.	105	91	12	152	109	33	90						
N.	70	132	43	149	8	177	17	82	99	58	64		
O.	40	145	159	171	60	93	22						
P.	142	3	106	181	168	49	111						
Q.	115	65	139	101	15	126							
R.	127	172	28	81	113	98	138	135					
S.	75	136	166	108	11	86	119	38	24	122	69	48	
T.	4	59	68	128	26								
U.	153	147	30	116									

UNCLASSIFIED

DOCID: 4009733

V. Where agreement that ended the War of 1812 was signed — 47 94 151 148 102

W. Not discarded — 56 129 179 146 9 137

X. Influence — 121 160

Y. Highest peak in Wales — 133 44 154 77 36 165 123

Z. Swiss tourist resort and munitions town (something for everyone!) — 161 52 89 169

Z_1. Shooting at clay targets — 54 156 84 32 134

1 H	2 I	3 P	4 T	5 B	6 E		7 I	8 N	9 W		10 E	11 S	12 M	13 K	14 L
15 Q	16 F		17 N	18 E		19 I		20 A	21 K	22 O	23 B	24 S	25 K	26 T	27 C
	28 R	29 H	30 U	31 B	32 Z_1		33 M	34 B	35 A	36 Y		37 C	38 S		39 I
	40 O	41 K	42 C	43 N	44 Y	45 E	46 J	47 V		48 S	49 P	50 B		51 H	52 Z
53 G		54 Z_1	55 A	56 W	57 C	58 N	59 T	60 O	61 E		62 C	63 I	64 N	65 Q	66 H
67 B	68 T		69 S	70 N	71 E	72 K	73 A	74 I	75 S	76 K		77 Y	78 G	79 K	80 C
	81 R	82 N	83 I	84 Z_1	85 K		86 S	87 E	88 B	89 Z	90 M		91 M	92 G	93 O
	94 V	95 D	96 H	97 C		98 R	99 N		100 K	101 Q	102 V	103 C	104 I		105 M
106 P	107 C	108 S		109 M	110 L		111 P	112 E	113 R	114 K	115 Q	116 U	117 F	118 G	119 S
120 A	121 X	122 S	123 Y		124 K	125 C	126 Q	127 R		128 T	129 W	130 E	131 G	132 N	133 Y
134 Z_1	135 R	136 S	137 W		138 R	139 Q	140 H		141 K	142 P	143 E	144 G		145 O	146 W
147 U	148 V		149 N	150 J	151 V		152 M	153 U	154 Y	155 I	156 Z_1	157 F	158 G		159 O
160 X		161 Z	162 E	163 H		164 B	165 Y	166 S	167 E		168 P	169 Z	170 D		171 O
172 R	173 I	174 D		175 F	176 I	177 N	178 G	179 W	180 A		181 P	182 E			A.J.S.

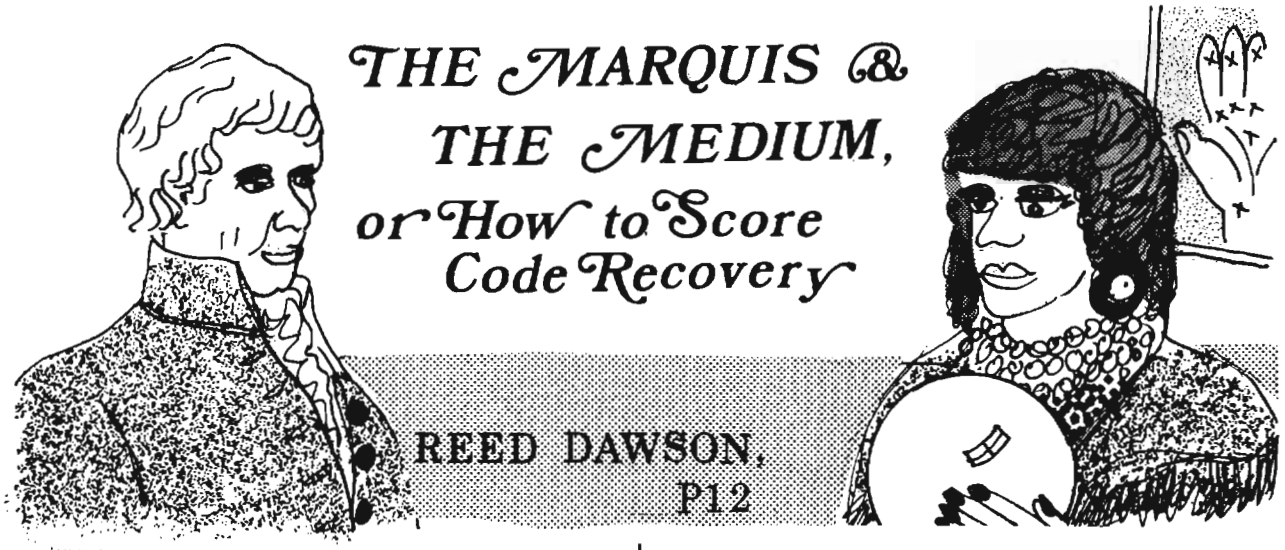
(Solution next month.)

CMI BANQUET, at GODDARD SPACE FLIGHT CENTER, Friday, 18 JUNE 1976, 6:30 p.m.

Open bar -- prime rib dinner --NASA tour.

TICKETS: $8.50 (CMI member; one guest of CMI member); $10.00 (all others).
Reservations: Rose Campbell, P1, 3W090, x3957s.

DOCID: 4009733



THE MARQUIS & THE MEDIUM, or How to Score Code Recovery

REED DAWSON, P12

"Mais, monsieur," Madame Claire was saying, "never have I been asked to dig so deep."

The placards in the second-floor window had caught my eye. Spirit communications vied with palmistry, astrology, tea-leaf readings, and Egyptian sand divinations. But for the "on parle français," I'd not have entered, tendering an ephemeral greenback.

I wanted to question Pierre-Simon de Laplace (1749-1827), the famous French mathematician and astronomer, about his notorious law of succession. The law says that if an event has occurred k times in n trials at some fixed but unknown probability, then the odds for the next trial are to be estimated as $k+1$ to $n-k+1$ in favor of occurrence. Laplace had gone so far as to apply the law to the odds the sun would rise the morrow morn, for which he had often been upbraided in limbo.

"Try," I urged. And lo, after an agony of mutterings and eye rollings, Madame Claire claimed to have the spirit of the Marquis de Laplace. As a test, I inquired politely about the rising sun. It was a mistake. An angry French voice issuing from the medium shot back, "Imbécile, if you wish to consider collateral information, then do so!"

I rallied, firing the twenty-dollar question. "Your law of succession doesn't seem to apply to many-celled multinomial distributions, the kind where the number of cells is more than the sample size. When one forms odds by adding unity to each cell count, the odds on the unseen categories become impossibly large."

"Mon enfant," he replied, more in pity than anger, "naturellement one must count the live cells only. Can you not estimate their number?"

The medium woke with a gasp. "C'est tout, monsieur. Au revoir."

"Mais c'est merveilleux! Please, one more and we will both become famous."

"What is it that I must do?" She regarded my emerging wallet with suspicion.

"Just one more Pierre-Simon, madame, I beg you. Pierre-Simon de Fermat, for just one little question."

"And when did this one die, monsieur?"

"In 1665."

"Mon Dieu, monsieur! Adieu, monsieur."

For further details, see "A Survey of Multinomial Estimation for Code Weighting," *NSA Technical Journal*, Vol. 20, No. 3, Summer 1975.

~~(CONFIDENTIAL)~~

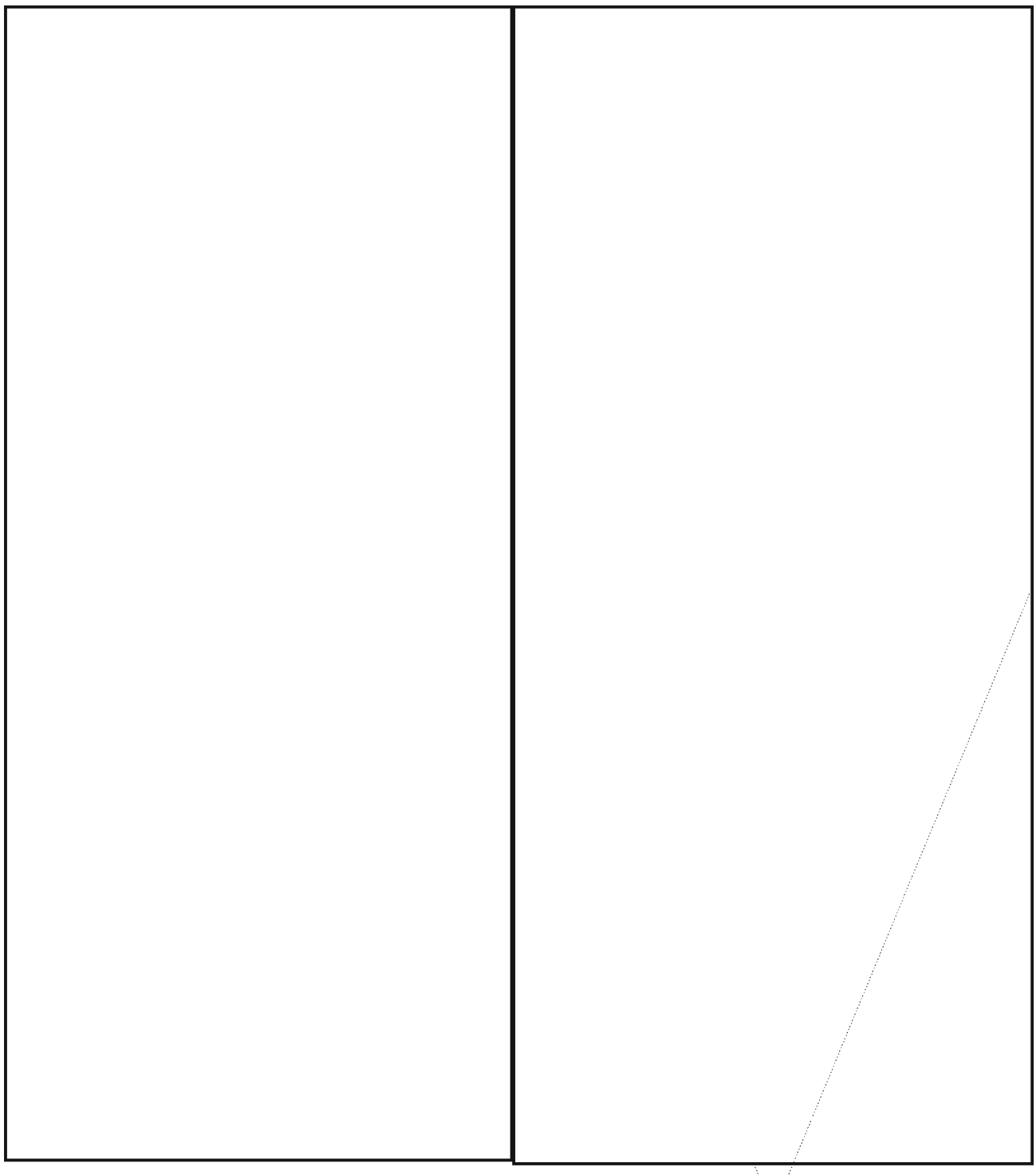
EO 1.4.(c)
P.L. 86-36

DOCID: 4009733

EO 1.4.(c)
P.L. 86-36

THE [redacted] COLLECTION SYSTEM

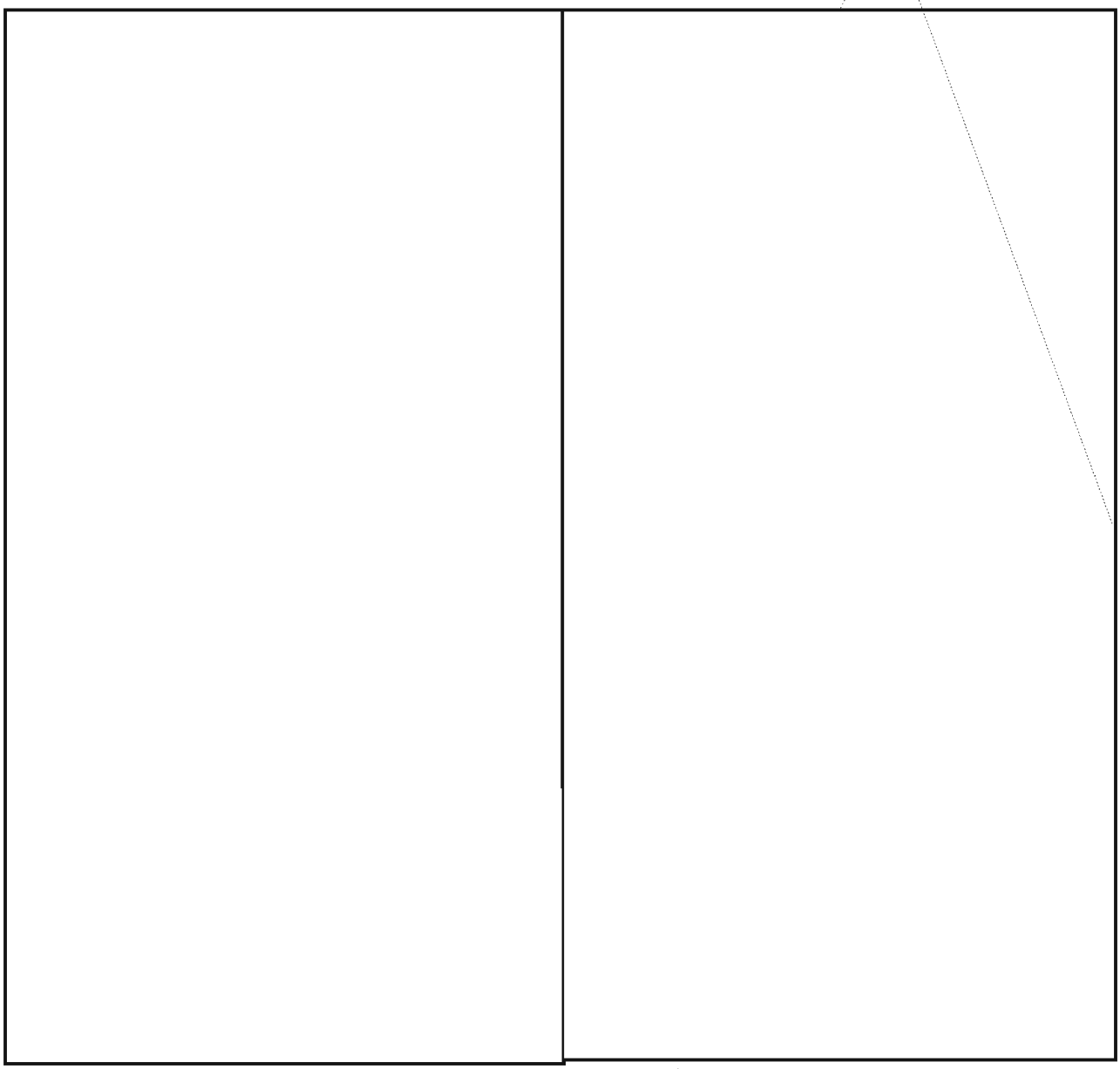
Tim Murphy, B341

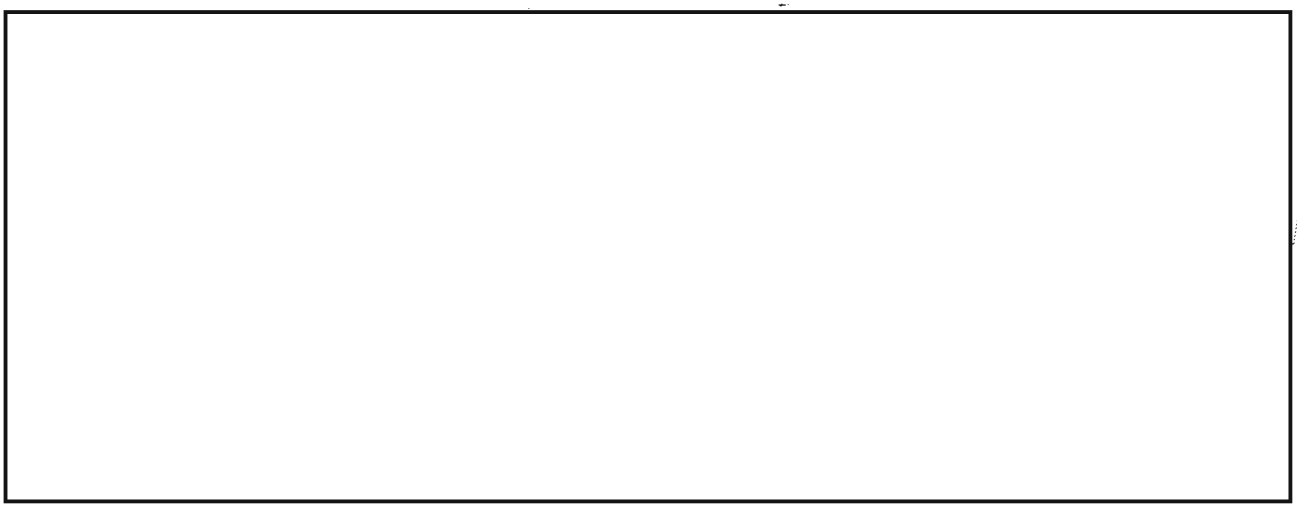


EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36

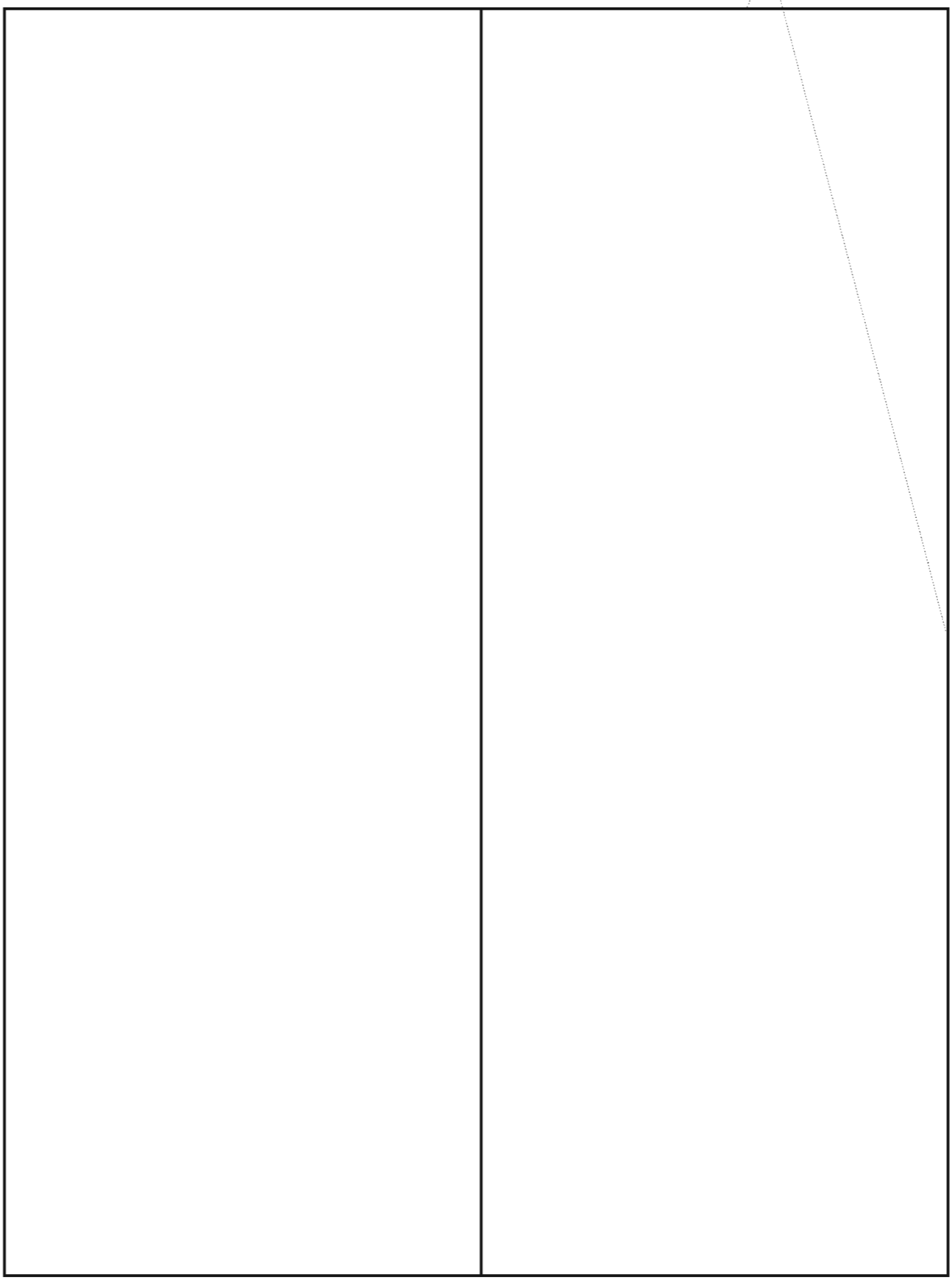




EO 1.4.(c)
P.L. 86-36

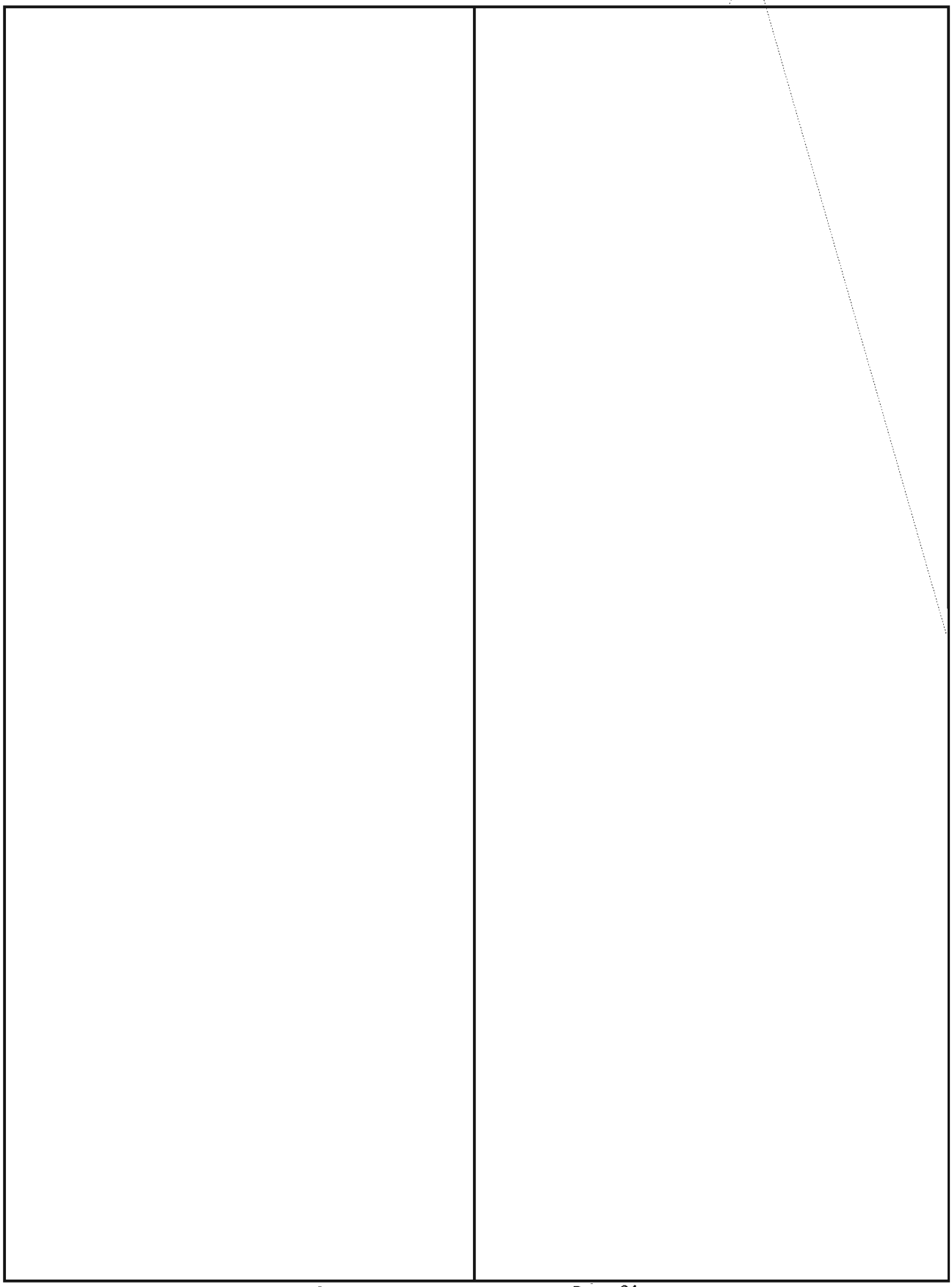
~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36



~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36



[redacted]

~~(SECRET SPOKE)~~

Comments as requested

(*Continued from page 17*)

[redacted]

~~(CONFIDENTIAL HVCCO)~~

HOW THINGS HAVE CHANGED!

[redacted] H111 P.L. 86-36

"Bei dir ist es nun soweit, Baby!"

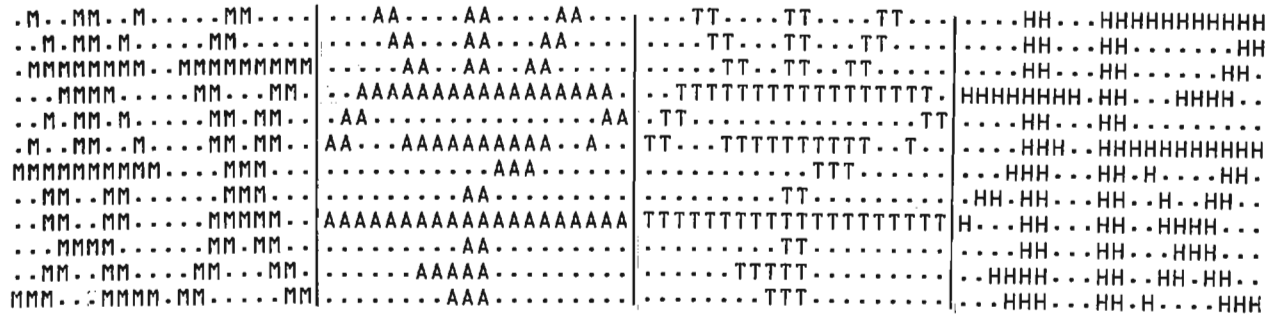
As a member of the Cryptanalysis Career Panel, I am interested in the selection and development of people with the best potential for becoming professional cryptanalysts. In doing research in this field recently, to trace the historical trends in cryptanalyst recruitment at the Agency, I came across a description of one approach that had been taken by a competing agency not too long ago.

The description occurred in the second part of the two-part article "On the Selection of Cryptanalysts," by Alex Dettmann (*NSA Technical Journal*, Vol. V, No. 1, January 1960, and No. 2, April 1960). The author is identified as follows: "The author of this paper was a former lieutenant in the German Army. As officer-in-charge of the Russian Section of the Cipher Bureau of the German Army High Command, he gave considerable thought to the selection and training of professional cryptanalytic personnel." The paper, which dealt with the historical development in the years 1935-1945, was written from memory after World War II.

Says Dettman:

> Even with the danger of being considered old-fashioned and unobjective, the author rejects the assignment of female personnel categorically and without exception as cryptanalysts though not as clerks or assistants. Quite apart from the fact that the subject matter as such is foreign to a woman's mentality, it must be added that it is extremely difficult for most women to engage in work about which no word may be spoken. During his long years in a managerial status, with the opportunity of becoming acquainted with most of the cryptanalytic positions in the former German Republic, the author has never known a single woman who did even average work as a cryptanalyst. All of the women who were assigned during and after 1943 as staff or intelligence assistants (a bare total of about 100) can only be described as clerical personnel or more or less efficient assistants.

~~(CONFIDENTIAL)~~



CHINESE MT (MACHINE TRANSLATION)

Like the two-way radio wristwatch, machine translation (MT) of language continues to fascinate certain segments of the scientific-technical and intelligence communities. As interest in Russian-to-English MT lessens, we observe a new area of interest -- Chinese-to-English. The following two articles, which deal with the same Chinese-to-English MT project, arrived at the editorial office in the same week. With Agency interest like this, the editor feels compelled to print both articles in their entirety, despite the slight overlapping of the authors' comments.

Ed.

NOTES ON TRANSLATION FROM THE CHINESE

[redacted] R51

P.L. 86-36

The Department of Computer Science of the United College of the Chinese University of Hong Kong has its own machine-translation project. First announced offspring of the project is the CULT (Chinese University Language Translator) System, which is being used, we understand, to translate, inter alia, *Acta Mathematica Sinica*. In July 1975 we saw their translations of all six articles in the September 1974 issue. We did not, then or later, see the original articles in their pristine ideographic form.

In January 1976 we found ourselves in (licit) possession of a nine-page package centered about a one-page article from the journal cited earlier.

A word (perhaps two) about the contents of those nine pages. Page 1 was, of course, the original article, characters and all (and the characters in some cases were what the Chinese themselves call "simplified" -- in any case they're different from their "traditional" predecessors). The next two pages contained the translation into English by some anonymous Chinese mathematician. Following these were the two pages of "input" to the CULT System.

At least two more words are necessary here: the computer never got to "see" the ideographs. In their place it saw the appropriate four-digit values from the well-known Standard Telegraphic Code (STC). Since the new, "simplified" characters have not made their appearance in STC, each one in the original journal article was replaced by the "traditional" one.

The computer never got to translate the title of the article: the human's translation was entered, in English, along with the rest of the input.

All "equations" were copied (presumably photocopied) without any computer translation

being allowed to intervene. Thus, for example, the character meaning "or" was replaced in one equation by "or," although that same character (in STC guise) occurred in the textual portion of the article (and was indeed translated as "or").

Back to the table of contents.

The next two pages were the (mildly edited) Chinese original -- edited in the sense that the simplified characters have been replaced by their ancestors, and certain shortcomings of the CULT System have been compensated, in advance, by the project workers. As a tiny example, the article begins by stating that certain alphabetic symbols (our alphabet and also that of the Greeks) stand for real numbers. The Chinese are content to say "a, b, c real numbers." But in the edited input, the simple string "a, b, c" was changed to "a, b *and* c."

Finally, the last two pages contain the computer's translation of the mildly edited, amplified, historically adjusted, original article.

In my opinion, both translations -- its and his (maybe hers, but could the Chinese be that civilized?) -- were pretty good. The fact that both translations, in their own way, were deficient, allows me, or at least gives me an excuse, to belabor a vital point concerning technical translating, i.e. translation of written material, allegedly nonfictional, which presupposes much relevant knowledge and relevant sophistication on the part of the ultimate human reader.

I consider my point vital enough to assign it its own paragraph. The technical translator, to be consistently correct and complete, must be a master of at least three domains:

- the *subject area*, be it a branch of mathematics or prison reform in the Third Circle;
- the *source language*, particularly (if not exclusively) as it is used by native writers actively engaged "professionally" in the particular subject area; and
- the *target language*, with the same particularity as that of the source language.

It might be objected that my point, were it adopted as the criterion for choosing, or retaining, a technical translator, would rule out *all* machine translation and many present human translators. The objection is well taken.

Let me adduce a few examples from the translations of the Chinese article in question.

- The author describes certain geometric points by an adjective (expressed by a single character) which, among its meanings, and English translations, has two nonsynonymous ones which are both valid "technical" ones in various mathematical areas. In very specific area germane to the article at issue, both the English terms show up, but with slightly diverse meanings. The character in the journal article was translated by the man by the correct English term (for the specific context), but the machine guessed incorrectly. I emphasize that the machine *guessed*. Even had the computer chosen "critical" rather than "singular," it would have had no reason for so choosing. It was the man, with his knowledge of the subject matter (and the vocabulary precisely pertinent thereto), who had *reason* to choose correctly.
- Another adjective (this time with two characters) fooled only this reviewer. The adjective occurred in the title of the article, which, you recall, was given to the computer as part of its input. The use of the specific two characters jointly to form a single adjectival lexeme is only to be found, to my knowledge, in one dictionary (published by the American Mathematical Society, no less), which gives the sole meaning of "stationary." No lexicographical source I could find gave the (human) translator's reading of "autonomous." Only by happenstance (in translating a Russian article) did I find a citation to the very current American literature which, for the exact situation at issue here, uses "autonomous." My casual familiarity with the specific field was inadequate for purposes of technical translation.
- The human translator made a correct, but infelicitous, choice of words when he wrote of a limit cycle (a geometric figure resembling a circle) "surrounding" a particular (geometric) point. More felicitous would be "encircling." The computer, however, was *wrong* on one of the two occasions and unnecessarily ambiguous on the other. (Of course, some writers, even Chinese, are sometimes guilty of ambiguity or malfeasance. Our present original writer was not.) Once, the computer had a limit cycle "outside" a point (*wrong*), and once the cycle "contains" the point. Since the "cycle" at issue is itself *made up of points*, to say that cycle X contains point Y may be saying that cycle X, as a geometric curve, *encircles* point Y, *or* it may be asserting that cycle X, as a collection of points, boasts point Y as one of that collection. To rephrase the problem: there is no ambiguity when I say that point Y is *on* circle X, or, alternatively, that point Y is *within* circle X, but what is the situation when I say that Y is *in* X?
- A final example, at least for the purposes of this overextended paper. Here, the computer dutifully, and acceptably, translated a phrase which the human, without due cause, omitted completely.

The author had said that he could, *with no loss of generality* (standard procedure and verbiage for this sort of material), set a particular symbol equal to a specific integer. Compare:

The computer: "Without loss of generality, we can take m = 1."

The man: "we can take m = 1."

The Anglophone mathematician prefers reading the assurance that generality is still secure.

(UNCLASSIFIED)

AN EVALUATION OF A SCIENTIFIC CHINESE MACHINE TRANSLATION

[redacted] P12

P.L. 86-36

Since the dawn of present-day computer science, the idea that a computer should be able to translate one natural language into another has been a most fascinating problem to computer scientists and linguists alike. A satisfactory solution to this problem, however, has proved to be most elusive. Even when the concession is made that the first attempt at machine translation should be in scientific literature, with its relatively small and precise vocabulary and usually uncomplicated syntax, as opposed to the linguistically more complex artistic literature, the solution is still far from complete. Because of the importance of machine translation and perhaps also because of the enticing nature of unsolved problems, many machine-translation projects exist throughout the world. These projects are evaluated on the quality of the translated output, as well as on the techniques employed in the translation algorithm. The Agency, with its high interest in language and language processing, keeps abreast of developments in the area of machine translation and, in line with this, I was asked recently to evaluate the translations of a new Chinese-to-English machine-translation project.

The Chinese University of Hong Kong as a computer translation project, CULT (Chinese University Language Translator), which is translating scientific Chinese into English. This project has now been developed to the point that subscriptions are being accepted for their machine translations of two Chinese journals, *Acta Mathematica Sinica* and *Acta Physica Sinica*. Plans are being made to include translations of other scientific journals published in the People's Republic of China (PRC) in the CULT service. In order to familiarize the world with this service and to demonstrate the quality of the product, the organizers of CULT have prepared a paper describing their system; the paper includes as an appendix an article from *Acta Mathematica Sinica*, accompanied by both the CULT machine translation and, for comparison, a translation by a Chinese mathematician. Also accompanying the machine translation is the form of the article at each step in the CULT process. In an attempt to evaluate this machine-translation project, I have compared the CULT translation with both the supplied human translation and my own translation.

The computer translation system employed by CULT involves only two steps before the English output is produced. These steps are pre-editing and keypunching. According to the CULT paper, pre-editing involves the addition of some Chinese words, such as understood subjects and predicates, and the flagging of dependent Chinese clauses for the machine. These additions are included so that the computer has a "complete" sentence to work with and so that the the extent of dependent clauses is known to the machine. However, in the sample article one *English* word was inserted into the Chinese text! This occurred when the original article stated "Let α, l, m, n, b be real numbers." The pre-editor inserted the English conjunction "and" into this sentence to yield the pre-edited version "Let α, l, m, n, and b be real numbers." While the insertion of English words at the pre-editing step is not mentioned in the CULT paper and its extent is unclear, this example may only be the unavoidable result of slight differences in the form of enumeration statements in Chinese and in English. One other interesting feature of the pre-editing step is the conversion of Chinese characters written in the shortened form now used by the PRC ("simplified characters") back to their more traditional form. The keypunching step is the conversion from this pre-edited form, which is still in Chinese characters, to a standard machine-recognizable form of Chinese. This form, the Standard Telegraphic Code (STC), merely assigns to each Chinese character a unique four-digit number.

The *Acta Mathematica Sinica* article chosen to demonstrate the capabilities of the CULT system states, without proof, a number of theorems in nonlinear differential equations. While both the human translation and the machine translation included in the paper were quite good, each made what I term a significant or a serious error. A translation error is serious if it is unclear what the meaning of the original article

was, based on the English translation alone. This is quite different from the kind of error where the original meaning is apparent to a person familiar with the field. The machine incorrectly translated one phrase as "[The system has a] limit cycle *outside* two singular points," whereas a correct wording would be something like "[The system has a] limit cycle *surrounding* two singular points." Realizing that a limit cycle is a kind of circle, this error is definitely serious, as the machine translation appears to make sense but is entirely misleading. The human translator also committed a significant error when he rendered into English the phrase "the sutonomous [sic] system." Even allowing for a typographical mistake which yields the much more familiar word "autonomous," this is still a serious error, as the original meaning was "the nonlinear system." While this is probably just a sloppy exchange of one technical term for another, the effect on the English-speaking mathematican is just as serious as the effect of incorrectly rendered Chinese.

One area where the human translator has an advantage over the computer is demonstrated by the machine's translation of a phrase as "a limit cycle which contains the origin," which would be more correctly translated as "a limit cycle which surrounds the origin." It might be said that this is a case of ambiguous translation since the word "contains" in mathematics can refer either to set containment (as in "3 is contained in $\{1, 2, 3\}$") or to geometric containment (as in being contained inside of a circle). I don't feel, however, that CULT should be expected to differentiate between these two distinct meanings or be criticized for not distinguishing them, because the Chinese original literally does say "a limit cycle which contains the origin." The ambiguity is in the original Chinese, not in the machine translation! The same Chinese words used here to mean geometric containment can sometimes mean set containment. The Chinese mathematician did use the unambiguous word "surrounds" in this situation, but he possessed a knowledge of mathematics and was able to use that knowledge in conjunction with his translating ability. The machine can base its decision only on the input, together with its stored dictionary, which does not include knowledge of the field of mathematics. It is, therefore, too much to expect the machine to make such a differentiation. What is required (or assumed) is that the reader of any article on nonlinear differential equations should be able to resolve the ambiguity. This is not, in my opinion, an unreasonable assumption.

Having examined this sample article and the CULT translation of an entire issue of *Acta Mathematica Sinica*, I feel that CULT could provide a quality translation of this and other PRC scientific journals on a timely basis. The question remains, however, whether a need exists in the general mathematical community for a cover-to-cover translation of *Acta Mathematica Sinica* or any other of the PRC journals. The answer to this question would have to be made by the would-be subscribers to the CULT translations.

(UNCLASSIFIED)

LETTER TO THE EDITOR

In view of the point I tried to make regarding NSA-ers' attempting to siphon personal mileage from the Vietnam tragedy ("Leo in October," CRYPTOLOG, January 1976), I can only assume from [redacted] article in April's CRYPTOLOG ("One Day in Danang: Other Duties as Assigned") that he still hasn't learned much in terms of the lessons of Vietnam.

His account of rockets, smoke, and shrapnel came across as a smokescreen not only for his lamentable lack of perception (we covered that in the January issue), but now also for his lack of good taste. Too many silenced voices will never be able to give such accounts; not to anyone, much less to a captive SIGINT readership.

I chide both [redacted] for this second, P.L. 86-36
grossly indelicate effort; and the publisher and editors of CRYPTOLOG for dignifying it as a feature article.

Respectfully,
Albert I. Murphy, V13

~~(CONFIDENTIAL)~~

. . . had a farm, E-I-E-I-O?

Here's a "Transcription in the News" item from TIME magazine (March 29, 1976, p. 24):

a very sha[illegible]dy, very shrewd."

The prosecutor also got help from a highly unpredictable source. William and Emily Harris, Patty's most ubiquitous S.L.A. companions and the only members of the guerrilla band still alive, gave a prison interview to *New Times* magazine in which Emily referred to "a stone relic in the shape of a monkey face" that Willie Wolfe once gave to Patty. "He called it an Olmec or something," she said.

That offhand remark rang a bell with the prosecutor. He recalled that on one of the tapes that Patty made during her S.L.A. sojourn she said that the "pigs" probably had "that Olmec monkey" that Wolfe—who died in the Los Angeles shootout on May 17, 1974—wore around his neck. The FBI transcribed that garbled remark as "that old MacMonkey." After reading the *New Times* article, Browning asked the FBI, on a hunch, whether Patty had a similar Olmec trinket in her purse when she was arrested. The answer was yes. That led to Browning's deft summation ploy when he wondered why Patty had testified that she "could not stand"

PROSECUTOR JAMES L. BROWNING

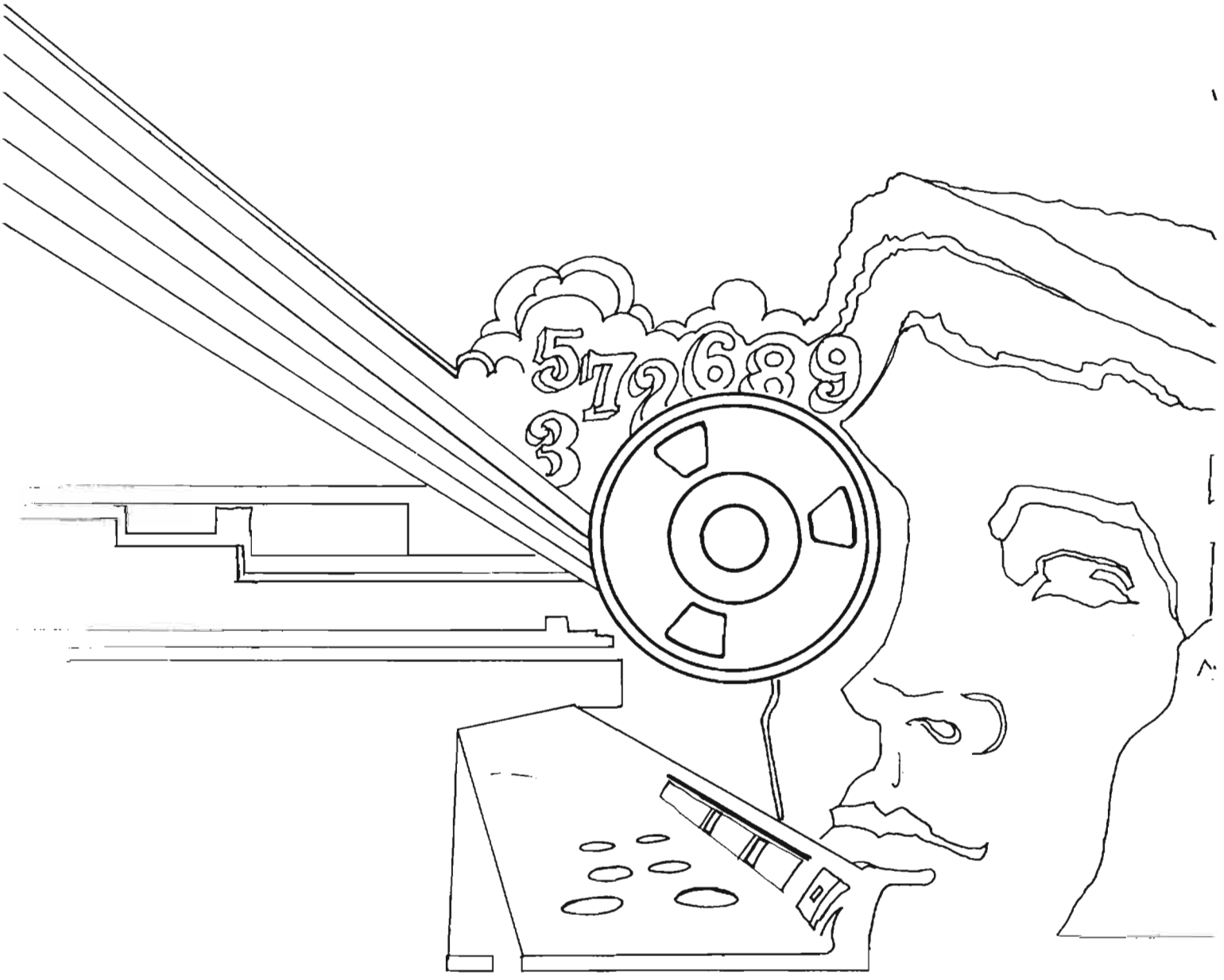
Wolfe but, long after his death carrying the tiny totem that h parently given her.

Browning contended that gan looking up for the prosecu midway in the trial—"some tween the time the judge allo introduce documents from h year [the year before her arres had to take the Fifth so many front of the jury."

What about the impact o dict on his future career? "I am I was told by some people that wanted was a federal jud shouldn't try the case. But I that I could turn over the trial to an[illegible]

[redacted] P.L. 86-36

(UNCLASSIFIED)



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

DOCID: 4019630

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MAY 1976

P.L. 86-36

COMINT IN THE RUSSIAN NAVY, WWI..... [redacted] 1
GEOGRAPHIC NOTE..... [redacted] 4
"WHAT LANGUAGE PROBLEM?"..... Mark T. Pattie, Jr. 5
WHAT'S WRONG WITH AG-22/IATS?..... [redacted] 7
ABOUT THE NSA SIGINT SUMMARY..... [redacted] 9
SOME PRINCIPLES OF COVER AND DECEPTION..... [redacted] ...10
CONVERSATION WITH A BOOKBREAKER.....12
TRANSLATORS' COMPENDIUM.....12
A SOVIET VIEW OF N.S.A..... [redacted] 14
HYPNOSIS AND SELF-HYPNOSIS IN LANGUAGE LEARNING
..... [redacted] 15
WAVEGUIDE ANALYSIS..... [redacted] 18
A SIMPLE CIPHER STORY..... William P. Meyer.....19

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019630

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. III, No. 5 MAY 1976

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief..... Arthur J. Salemme (5642s)

Collection..... [redacted] (8955s) P.L. 86-36

Cryptanalysis..... [redacted] (8025s)

Language..... Emery W. Tetrault (5236s)

Machine Support..... [redacted] (3321s)

Mathematics..... Reed Dawson (3957s)

Special Research..... Vera R. Filby (7119s)

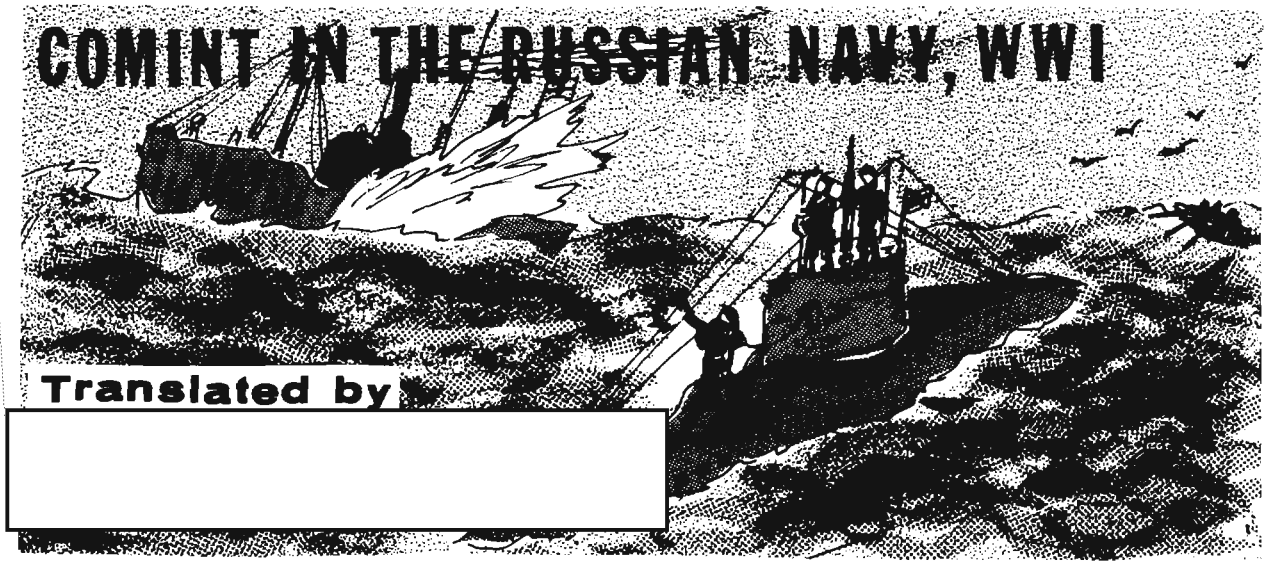
Traffic Analysis..... Frederic O. Mason, Jr. (4142s)

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4019630
P.L. 86-36

COMINT IN THE RUSSIAN NAVY, WWI



Translated by

[redacted]

Translator's note: *The following article is a translation of "On the Origins of Communications Intelligence in the Russian Navy," by V. Yankovich, in the Soviet periodical* Voenno-Istoricheskij Zhurnal (*Journal of Military History), February 1961, pp. 114-117. In my search of open-source materials, Yankovich's article was the only one that I could find that describes the early development of the Soviet signal intelligence service from the point of view of a participant. The article does not contain any attribution as to the source of the information, or any identification of the author except by name. Because of the article's unique nature and its interest to CRYPTOLOG readers, I have translated it in its entirety.*

At the beginning of World War I not one of the combatant sides had a specially organized communications intelligence (COMINT) service [*radiorazvedka*] in its navy. The first steps toward organizing a COMINT effort in the Russian Navy were, to a large degree, connected with the wreck of the German cruiser Magdeburg near Odensholm Island on 26 August 1914. Documents discovered on that ship revealed a system of enciphered radio communications that the enemy had been using at that time[1].

After Germany declared war on Russia on 1 August, the enemy fleet in the Baltic Sea limited itself for a prolonged period of time to demonstrations carried out by small forces and the patrol service in areas of possible Russian naval action.

In the early hours of 26 August the Russian patrol cruisers Pallada and Bogatyr' were standing at anchor in Baltijskij Port (now Paldiski) because of fog. At 0130 hours the signal station on Odensholm (now Osmussar) Island reported by telephone to the Chief of the Signal Service in Revel (now Tallin) that a ship had run aground at a distance of two cable lengths from the island. Then the signalmen reported that they could hear German being spoken and the operation of shipboard machinery, and could also hear the anchors being veered and heavy objects being thrown overboard. When the fog lifted somewhat, the signal station reported that a four-funneled cruiser had run aground and that a torpedo boat was standing by it, attempting the tow the cruiser by the stern. Upon receiving the very first report in Revel concerning the accident that had befallen the German ship, the Fleet Commander dispatched the First Torpedo Boat Division and the cruisers Bogatyr' and Pallada to Odensholm Island. The chief of the fleet communications service set out to sea from Revel on board the torpedo boat Lejtenant Burakov, accompanied by the torpedo boat R'yanyj; they were followed somewhat later by the cruisers Rossiya and Oleg, and, finally, the Ryurik, under the flag of the Fleet Commander.

The cruisers Bogatyr' and Pallada approached Odensholm in the fog and, at approximately 1100 hours, when the visibility had temporarily improved, they spotted the German cruiser Magdeburg aground, with a tow line from the large German torpedo boat, the V-26, attached to its stern. Our cruisers opened fire on them. The

[1]It should be noted that the descriptions accompanying the charts in *Morskoj Atlas* (Naval Atlas) (Vol. 3, Part I, Publishing House of the Main Staff of the Navy, 1959, p. 769) and in *Istoriya Voenno-Morskogo Iskusstva* (History of the Naval Art) (Vol. 3, Moscow, Voenizdat, 1953, p. 120) are not completely accurate in illuminating the circumstances under which the documents were found on the German cruiser Magdeburg, or about their contents. (Author's note)

DOCID: 4019630

Magdeburg responded, but its situation was hopeless, and, as was subsequently reported by captured German sailors, the commander decided to blow up the cruiser. The V-26 was ordered to approach the Magdeburg and take off the crew. However, it failed to throw out the mooring lines. Taking advantage of the dense fog, the torpedo boat left. After it departed, the forward magazines of the Magdeburg were exploded.

When visibility improved, it became clear that the Germans had abandoned the cruiser. The Lejtenant Burakov approached the Magdeburg. The only people remaining on it were the commander and two sailors. Approximately 50 crew members were found on the island and in a lifeboat. They were taken prisoner.

A large number of bundles and suitcases containing personal articles belonging to the cruiser's crew members were transferred from the Magdeburg to the Lejtenant Burakov. The articles included notebooks and diaries. A signal book was found in one of the bundles. The discovery of the signal book was reported by semaphore to the cruiser Ryurik, which had also approached Odensholm at that time.

The fleet Chief of Staff, together with several officers, including myself -- at that time I was a staff flag officer -- set off from the Ryurik on board the destroyer Pogranichnik to inspect the Magdeburg. When inspecting the radio room, I noticed under a desk a cardboard folder containing a piece of paper with penciled notations. The notations might have been of interest, so I took the folder with me. That insignificant little piece of paper turned out to be a very valuable document.

Upon the Ryurik's return to the Revel roadstead, the Chief of Staff ordered me, as a person with a good knowledge of German, to acquaint myself with the captured materials and to report the results to him. After setting down to work, I noticed that the authors of most of the diaries and notebooks dwelt especially on the events of 17 August.

On that day (17 August 1914) a brigade of Russian cruisers consisting of the Gromoboy, the Admiral Makarov, the Pallada, and the Bayan, under the command of Rear Admiral Kolomejtsev, was on patrol on the meridian of the Pakerort (now Pakkineem) lighthouse. At approximately 1500 hours, our observers noticed smoke to the west of Takhkon (now Takhkuna) lighthouse. The brigade started out in that direction and quickly spotted two German cruisers, which were drawing closer to the Russian cruisers. Flagship navigator Sakelari expressed the hypothesis that the enemy was intending to lure the brigade into a minefield. Admiral Kolomejtsev agreed with his navigator and ordered the brigade to turn back to the east.

By comparing the entries, I managed to ascertain that the cruisers Augsburg and Magdeburg and three torpedo boats had the mission of convoying the minelayer Deutschland, with 800 mines, to the mouth of the Gulf of Finland. The cruisers were proceeding ahead, followed at a slight distance by the mine-layer and the torpedo boats. As the Germans were already approaching the designated place for the laying of the minefield, they saw that a brigade of Russian cruisers that was stronger in armament was coming toward them. The German admiral on the Augsburg ordered the Deutschland to depart to the west at full speed. He had decided to join battle with the Russian ships in order to attract them to his own ship, to gain time, and thus to save the minelayer. The German cruisers could always disengage from combat because of their great advantage in speed. And so, when our brigade, unexpectedly for the enemy, avoided contact, the tense situation for the Germans was replaced by one of elation. The Deutschland was immediately returned, and the German admiral reported to his command element concerning the satisfactory completion of the operation.

In view of their avoidance of combat, in which it might have been possible to destroy the German cruisers, or, pursuing them in battle, to overtake the very slow-moving Deutschland, Rear Admiral Kolomejtsev and navigator Sakelari were removed from active duty.

But what *were* the coordinates of the mine obstacle that had been laid by the Germans? The answer to that question was obtained after a study of the piece of paper that I had taken from the radio room. The initial designations that were customary for all radiograms were followed by text consisting of combinations of letters. That prompted me to turn to the signal book. The deciphered top secret enemy report stated that a minefield had been laid at such-and-such a time on 17 August, and indicated its exact coordinates in our waters.

The Fleet Staff immediately reported this information to everyone with a need to know. Our minesweepers checked the position of the minefield and subsequently that field was the first link in a large advance mine position that we gradually created across the Gulf of Finland. During the war many enemy ships found a grave there.

Finding the connection between the German radiogram on the laying of the minefield and the signal book had the most important and far-reaching consequences. It made it possible for the Russian and Allied naval command elements to use the intercepted enemy radio transmissions for intelligence purposes. The COMINT service that we organized consisted, first, in receiving and deciphering the enemy's enciphered radiograms, and, second, in providing bearings

DOCID: 4019630

on operating German shipboard radio sets, as obtained by our shore-based radio stations.

A subsequent check of intercepted German radiograms confirmed the fact that the enemy was enciphering his conversations by a combination of literal and digital characters in the signal book. Participating in the exploitation of this material, in addition to Flagship Radio Specialist I. I. Rengarten and myself, were two other persons -- an additional officer and an enlisted-rank radiotelegraph operator -- who were assigned specifically for permanent work in COMINT. It was assumed that the Germans might subsequently change their system of encipherment.

That question was carefully thought out at the Fleet Staff, and the Fleet Commander, jointly with the chief of the communications service, decided to organize urgently a special-purpose radio-interception [*priemnaya*] station in the western part of the southern shore of the Gulf of Finland. To achieve better monitoring of the waves, the site chosen was in the woods, far from populated areas. All the buildings were hidden from outside view and the station's personnel were allowed no contact with the outside world. The necessary supplies were delivered to the station at specified times by car from Revel. The radio station was tasked with only the receipt of German radiograms on several radio receivers. An underground cable connected the radio station with the southern region administration of the signal service. The station's personnel were carefully selected from the officers and the best radiotelegraph operators who knew German. The work of the stations was kept in strict secrecy to prevent the enemy from learning of its existence. Even in the Russian Navy only a few people knew about it.

The Germans used radio communications widely, and soon our special-purpose radio station had accumulated extensive material on various aspects of life, service, and combat actions of the German Fleet.

COMINT helped to keep the command element of the Baltic Fleet well informed on the enemy and made it possible for the fleet, within a short period of time, to change over from the passive waiting for the German Fleet to appear in the Gulf of Finland, to active operations in the southern part of the Baltic Sea.

After a short period of time the enemy, assuming the possibility that his radiograms were being intercepted, decided to make the cipher more complex. For that purpose he began to make it a practice to take the text that had been enciphered according to the signal book and then re-encipher it with the aid of re-encipherment tables [*pereshifrovochnye tablitsy*]. The tables were reissued from time to time. However, that circumstance did not present much of a problem in deciphering the German radiograms. By that time the workers at the radio station had collected extensive material on the basis of the deciphered radiograms. They needed only a few hours to draw up the new re-encipherment chart.

Soon our divers found a second signal book at the bottom of the sea in the area where the Magdeburg had been. At Fleet General Headquarters the book was photocopied and copies were supplied to our Allies, the British and the French.

The Naval Commission for Investigation and Utilization of the Experience Gained by the 1914-1918 War at Sea noted that our COMINT service had achieved great success for several months of the war.

It was interesting for me and the other naval specialists who participated in breaking the system by which the enemy enciphered his radiograms to follow the subsequent development of that case.

The biggest achievement was the ability to use the available materials to create the most commonly used parts of the new signal book after the Germans withdrew from use the old signal book which we had. After receiving the signal book from us, the British also organized a COMINT effort, carrying out similar work in studying German radiograms.

The enemy made wide use of his radio communications. His stations operated constantly. Naval Staff Officer Captain 2nd Rank I. I. Rengarten suggested installing at our coastal radio stations the very simple radio direction finders that he had invented as early as 1912. Following successful testing, the devices were installed at many coastal observation posts where there were radio stations. It was possible to determine the enemy's whereabouts by receiving radio bearings at two points simultaneously.

The time came when the chief of the signal service began to bring to the Fleet Staff a map of the Baltic Sea on which various colors of ink were used to designate the routes taken by enemy ships. Therefore it is not by accident that the Russian ships avoided the German minefields and remained undetected when setting up our own minefields near the German shores.

The command element of the Baltic Fleet made wide use of the COMINT information. The following are a few examples.

The German Naval Staff established a course for their ships to follow when entering or leaving the Gulf of Danzig. On 14 February 1915 two of our torpedo boats laid mines on that course. The very next day COMINT reported that a German transport had been blown up.

We also learned the arrival time of a German cruiser at the port of Libau (now Liepaya) and its departure time. A submarine was sent

DOCID: 4019630

to the entrance to the port. As the German cruiser was leaving Libau, it was sunk by that submarine.

Following the occupation of Courland (West Latvia) by the German troops, the German Ground Forces Command which was rushing to seize Riga requested the Naval Staff to provide support from the sea. COMINT revealed these conversations and established the date of the planned operation. The [Russian] Fleet Commander decided to strengthen the naval forces in the Gulf of Riga by sending the battleship Slava. On 31 July 1915 the Slava took the enemy completely by surprise by crossing over from the Gulf of Finland to the Gulf of Riga. COMINT provided such good information about the enemy's plans that when the German fleet, on the morning of 8 August, approached Irbenskij Strait, our torpedo boats and two gunboats were already waiting for them. By 1000 hours the Slava also approached the strait. The Germans' plan to break through into the Gulf of Riga was thwarted.

Early in November 1916, COMINT reported that the enemy was preparing an operation in the southern part of the Gulf of Finland. Information received permitted the hypothesis that

a raid by torpedo boats on Baltijskij Port was expected. The Fleet Staff felt that the Germans should know of the existence of an open passage in the southern part of the forward mine position. The Fleet commander ordered the laying of mines immediately in that passage. During the night of 10-11 November, our radio stations intercepted fragments of conversations between enemy torpedo boats that had suffered a calamity. Two of them had been blown up in the minefields that we had just laid. Then everything became quiet. After approximately an hour and a half, the German torpedo boats began firing on Baltijskij Port. At approximately an hour after that, eight German torpedo boats that were returning to the west came upon the minefield. The flotilla moved along the minefield and then turned to the west again. The torpedo boats began to blow up. During the course of an hour, five of the eight torpedo boats were sunk. All told, seven out of 11 of the newest torpedo boats were sunk.

Thus, by making skillful use of COMINT information, Russian sailors of the Baltic Fleet were, throughout the war, completely aware of the intentions of the enemy's naval forces.

(UNCLASSIFIED)

GEOGRAPHIC NOTE

All the geographic names in the preceding article were researched by a geographic analyst in the NSA Geography and Map Library, Room 2N075. That organization also provided the map showing the area discussed in the article, and the following note.

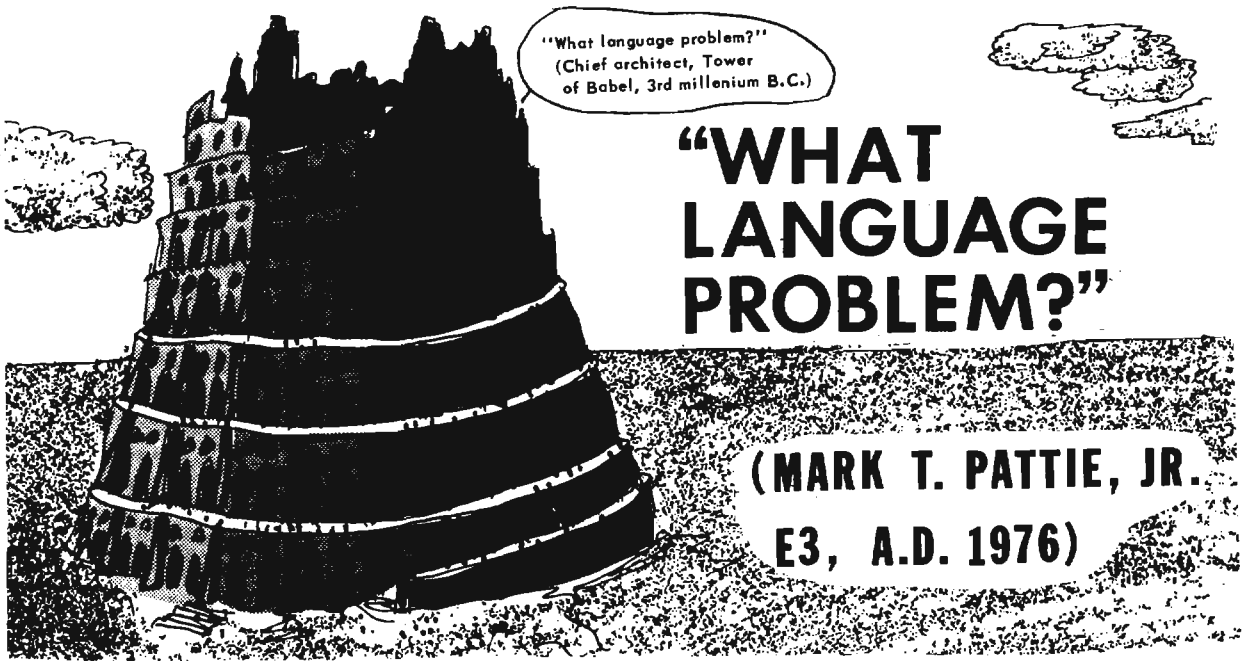
Ed.

The wreck of the Magdeburg, the location of the minefields, and the movements of the Russian and German fleets in WWI naval battles in the Baltic Sea are shown in the *Morskoj Atlas* which is part of the collection of the NSA Geography and Map Library. The reference collection also contains port plans, Russian hydrographic charts with pictures of lighthouses, Soviet Sailing Directions with Notices to Mariners, Lists of Lights and Fog Signals, and the Admiralty List of Radio Signals -- all of which contain a tremendous amount of detailed information.

Baltic placenames are a welter of different languages and variant spellings reflecting the checkered history of the region. Since the U.S. government does not recognize the Soviet incorportation of Estonia, Latvia, and Lithuania, the NIS Gazetteer adheres to the native spellings for *Tallinn* and *Liepaja*. NSA standardized treatment is to transliterate the Cyrillic spellings as *Tallin* and *Liepaya* (irrespective of the native spellings in Latin letters). Until 1917 the Russian names of the Estonian and Latvian ports were *Revel'* and *Libava*. *Odensholm* was the Swedish name of the Estonian island of *Osmussaar* (*Osmussar* as transliterated from the Cyrillic spelling). In 1914 *Tahkona* lighthouse on *Dago* (Russian and Swedish name of island called *Dagden* in German) was renamed *Takhkuna* and the island itself was renamed *Hiiumaa* (Estonian spelling; *Khiuma* in NSA spelling, as transliterated from Cyrillic). *Courland* is one of the former names of the province which became *Kurzeme* when Latvia received independence

(Continued on p. 19)

DOCID: 4019630



"WHAT LANGUAGE PROBLEM?"

(MARK T. PATTIE, JR. E3, A.D. 1976)

On 18 September 1975 Lieutenant General Lew Allen, Jr., Director, NSA/Chief, CSS, spoke to the members of the Crypto-Linguistic Association (CLA) in the Friedman Auditorium and used that opportunity to emphasize the importance he attaches to the work of Agency translators. In his remarks he mentioned the high esteem in which Agency translators are held, not only by him but also by those who rely on our product.

The Director's interest in Agency language work is not new, of course, for we have the evidence of the value he placed on the previous year's Jenkins Report on the "language problem" at NSA. Yet this high-level interest seems to have been -- pardon the expression -- lost in translation as it filters down through the levels of management.

Before the Jenkins Report there had been a number of studies of the "language problem" at NSA, but I don't recall seeing any papers showing that a solution was found. Not much earlier than that report, I participated in another, in which I did some research and provided material to the late Dr. Sydney Jaffe for his study. In the fall of 1961 I did research on my own and wrote a report on the problems of retaining college recruits in what was then B1, with the report going to M3 through Dr. Jaffe. The bulk of that report was concerned with the hiring and retention of linguists. Originally I myself was hired as a linguist, became a book-breaker, and then went on to other forms of cryptanalysis and into management, so I do have some personal experience on the "language problem."

When I was hired it was because I could translate from what is still considered a "rare" language, and this was when people were being released from their jobs because of cutbacks. Now, many years later, the Agency continues to seek people with linguistic ability even when hiring has almost stopped. This is certainly a strong indication that the Agency does have a real need for people who can translate well. It also means, to me, that the Agency is not able to retain enough qualified linguists to do the necessary jobs, for recruiters are constantly reminded to keep their eyes open for someone who is already able to translate a particular language or who can be easily trained to do so. But why, then, do translators leave the work?

Perhaps the problem is not in our hiring practices or in our training, but in the failure to recognize what the value of a good translator is. In recent years I have been quite surprised to see so many of our most skilled translators leaving well before they had reached the mandatory retirement age. The few I spoke to told me that there was just nothing they could do to overcome the feeling that what they were doing was regarded by those above them as of little value to the Agency. The "important" work is being done by engineering and scientific personnel. That there may be some truth in their statements can be seen in an examination of promotions to GGD-13, 14, and 15 during the 1974 and 1975 calendar years. The Agency's own statistics, as can be seen from the following table, point up the fact that anyone wanting to be promoted to the higher grade must get into a field such as Electronic Engineer, Data Systems Analyst, Cryptologist, or Cryptologic Staff Officer.

Promotions to					
GGD-13		GGD-14		GGD-15	
CY74	CY75	CY74	CY75	CY74	CY75

P.L. 86-36

Total promotions:

Including:
- Special Research Analysts
- Electronic Engineers
- Data Systems Analysts
- Cryptologists
- Cryptologic Staff Officers
- Linguists

Parenthetically, Special Research Analysts can scarcely find comfort from the relatively high figures for promotions to GGD-13, because that grade seems to be the end of the line for *most* SRAs (including linguists posing as SRAs for promotion purposes).

But what about the linguists who do not want to pose as anything that they aren't, but just want to continue working as, and getting promoted as, *linguists*? Most of them find their niche one grade lower, and reach the end of *their* line at GGD-12. Only a token few move higher. Why? The career structure allows for linguistic jobs at higher levels, but, to my knowledge, only one person with the label of linguist has a grade higher than GGD-15, and he was promoted over 10 years ago.

No, it is not that the structure doesn't permit promotions within the linguistic field, so the answer must lie elsewhere. I see no other place to look for the answer than in the attitude of Agency management towards language work.

In too many cases, managers of linguists have had no language experience of their own and tend to think that any job requiring the knowledge of a foreign language must be fairly simple. And yet the Crypto-Linguistic Association has, over the years, held several symposia and given several presentations in the auditoriums at Fort Meade and FANX, dealing with various problems encountered by the NSA linguist -- problems of language recognition, transcription, translation, machine processing, teaching, testing, etc. Agency linguists have, over the years, written numerous articles for the *NSA Technical Journal*, the *NSA Cryptologic Spectrum*, and *CRYPTOLOG* (or its predecessors *Keyword, Dragon Seeds, QRL, Command*). Have the managers attended the symposia? Have they read the articles? Are they reading *this* article?

Even as I write this, I have been told of a senior manager who feels that translation is "journeyman" work which can be handled by high-school recruits, after some training. Somehow I have the feeling that all the words that have been spoken and written have made no impression, that only linguists read articles about language, and that no one else really cares.

I think it is safe to assume that the attitude expressed by that senior manager is more typical than not. Lack of promotions is certainly evidence of this. In the face of such obvious coolness toward their field, only the most dedicated linguists will persist in the work. The majority will seek jobs in other fields or will leave the Agency for positions in which their linguistic talents will receive the proper respect. In either case the Agency will continue to have a "language problem."

There are some ex-linguists in management jobs in NSA, but few are in positions where they can continue to make use of their language skills and knowledge. One such exception is the National Cryptologic School, but only because it has a department whose mission is language teaching -- even in this instance, however, the Department Head is listed not as a linguist, but as a Cryptologist. Another exception I am aware of is P16, and the head of that element is a Cryptologic Linguist. Again, though, since P16 is exclusively devoted to linguistic matters it could scarcely be headed by anyone other than a linguist. There may be

DOCID: 4019630

other positions, such as overseas, but I think that the point stands.

I guess that what I am really trying to say is that there is not enough recognition given to linguists, and for me recognition means promotions and important jobs. More of those who are truly professional should be promoted without having to change jobs. More linguists should have the managerial roles over elements where the mission is largely language-related. Too many of the people who are now in such positions have little or no understanding of what it takes to be a translator -- or a voice interceptor, or a transcriber, or a teacher -- and they don't seem to care. To say that they are unsympathetic to linguists is to put it mildly.

When linguists are appointed to jobs in the upper management levels, they will be in a better position to counteract the negative attitude held by too many of our current managers. Then and only then will I believe that the "language problem" is on its way to being solved.

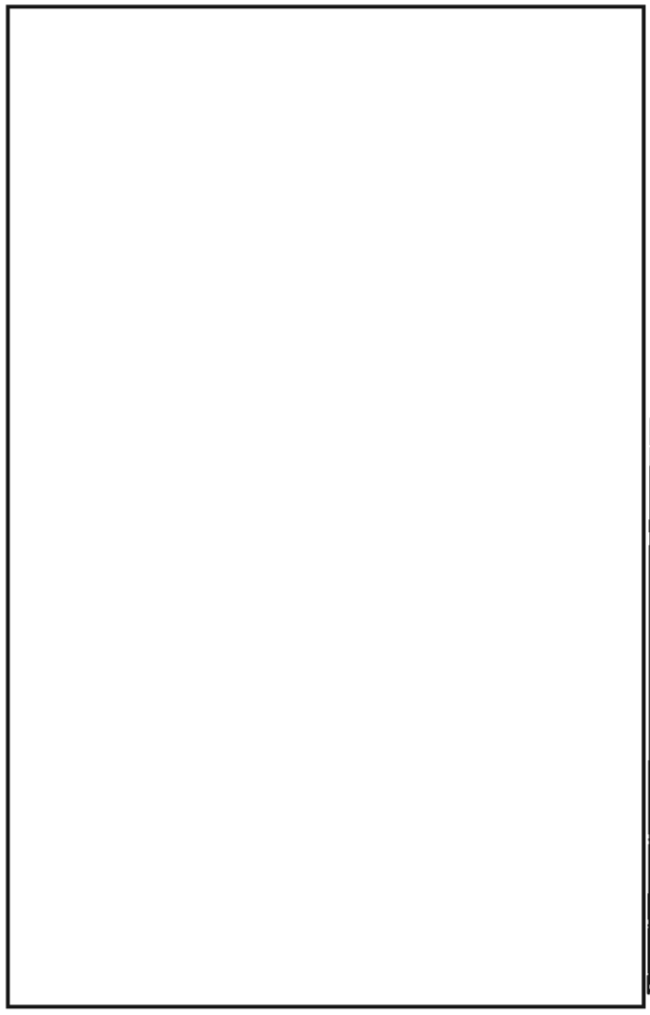
~~(FOUO)~~

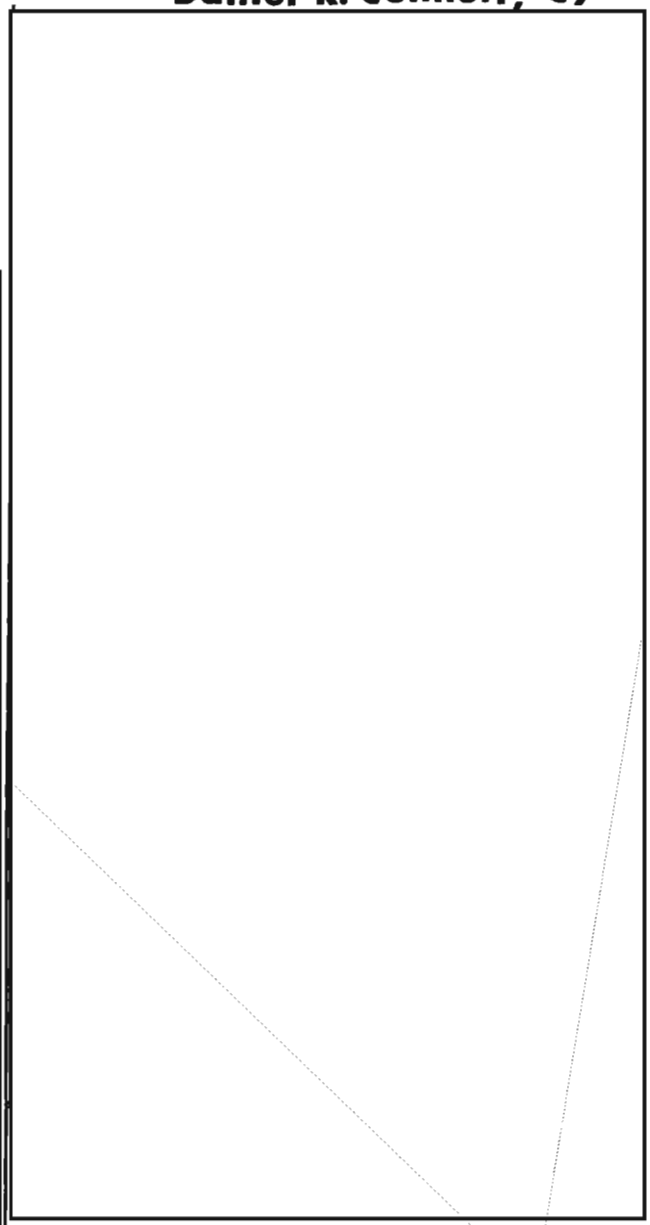
WHAT'S WRONG WITH AG-22/IATS?

Daniel R. Connell, C7

In the March issue of CRYPTOLOG we reprinted the article "Musings About the AG-22/IATS," by Cecil Phillips, C03, which had originally appeared in C-LINERS (C Group Machine Processing Information Bulletin), Vol. 3, No. 7, August/September/October 1975. Mr. Phillips' article prompted the following reply by Daniel R. Connell, which appeared in the Winter 1976 (Vol. 3, No. 8) issue of C-LINERS and is being reprinted here with the permission of its Editor, David J. Williams.

Ed.



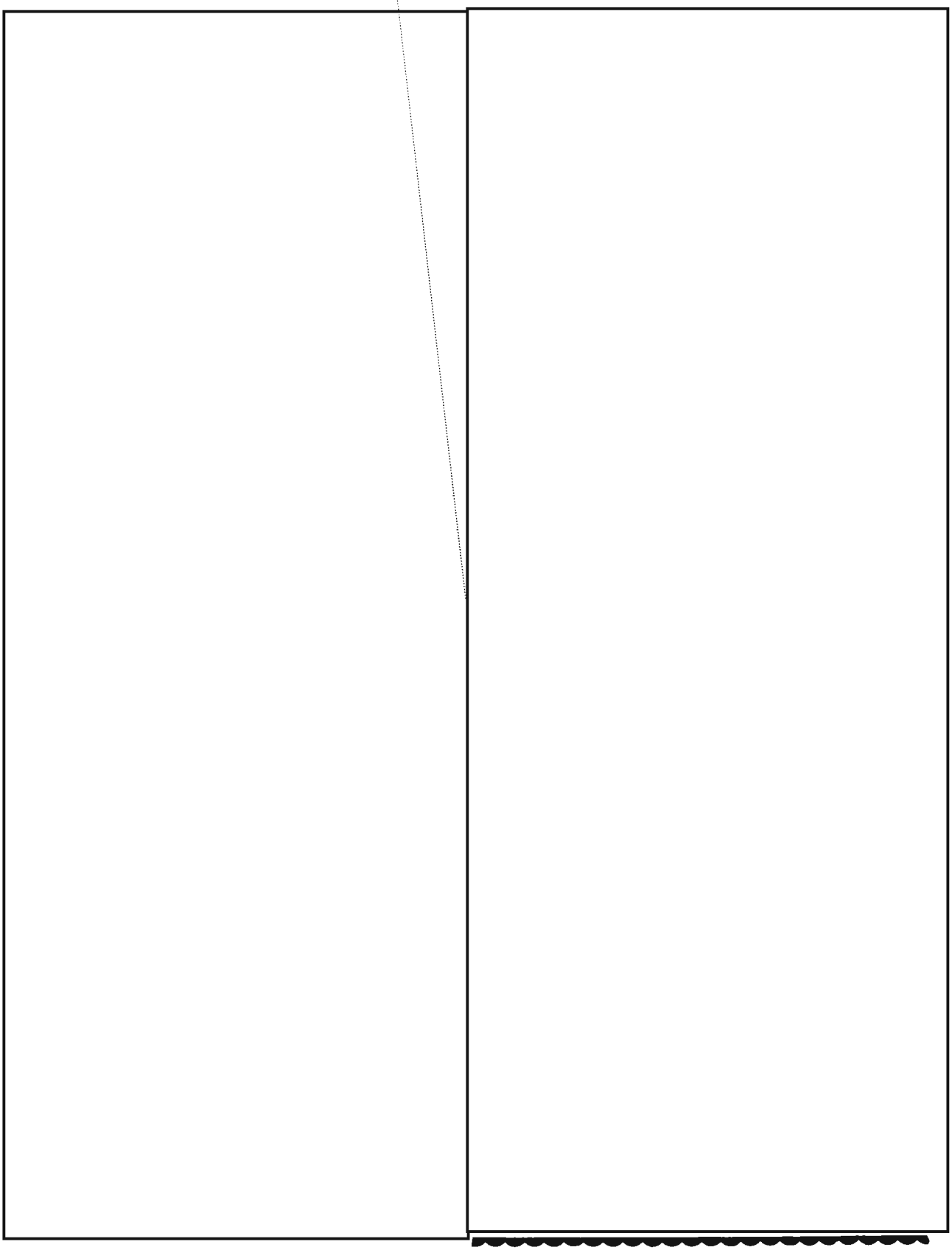


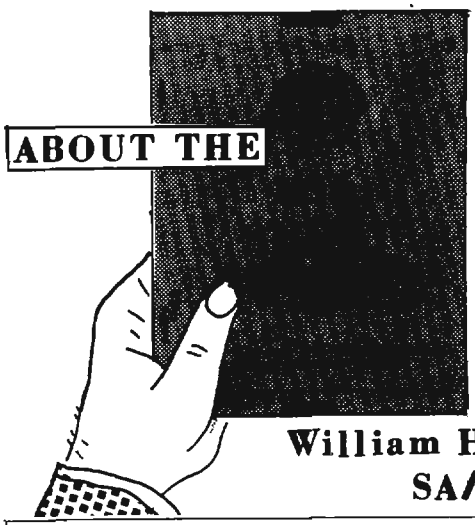
~~(CONFIDENTIAL - HVCCO)~~

EO 1.4.(c)
P.L. 86-36

~~EO~~ 1.4.(c)
P.L. 86-36

~~CONFIDENTIAL~~





William Hunt, SA/DDF

The following article was written by William Hunt when he was developing the SIGSUM. It appeared in the February-March 1973 issue of the Agency publication KEYWORD: Technical Exchange Bulletin *(now discontinued).*

The SIGSUM has served NSA well during many crisis situations, by bringing current SIGINT items to the attention of senior U.S. officials in the United States and overseas in capsule form -- the function for which it was primarily designed.

Ed.

The NSA SIGINT Summary (SIGSUM) is a daily publication conceived and designed by the Assistant Director for Production to inform selected senior executives of the United States Government, both military and civilian, of the most significant world developments as seen in SIGINT. Second-Party cryptologic collaborating countries also receive the publication for their use as appropriate.

While this publication was conceived as early as 1964, it was not until the past two years that it was fully developed and its objective and utility fully appreciated; as of today, it is one of the most widely read documents at the CAT III level in the SIGINT-indoctrinated system.

While it is neither possible nor desirable to trace the growing pains of the Summary suffice it to say that it suffered the usual development of any document for which no clear-cut requirement existed. NSA Production recognized the need for such a vehicle to alert selected senior U.S. executives to important items of interest in capsule form, to explain the COMINT fact, to interpret the communications activity, and to report it in meaningful terms. From the customer's point of view there was an understandable suspicion that this document would overstep the mythical line between reporting the SIGINT and evaluating it. It can be readily seen that misunderstandings, semantics, and the efforts of well-intentioned people in NSA and customer organizations would cause problems until all parties understood the philosophy and responsibilities of each other's roles and missions and learned to appreciate and adhere to the basic principles of their respective missions. All of these problems appear to be resolved, and with the exception of an occasional human error no future major differences are anticipated between NSA and its customers regarding the Summary.

As previously stated, the SIGINT Summary is a daily Production publication covering all SIGINT problems of NSA Production at the Category III level. It is released at approximately 1700 local time each day by electrical means and is disseminated to ZI addressees on the NSA SIGINT electrical system. It is also transmitted to selected overseas major military commanders, NSA/CSS field offices, and specific cryptologic organizations. Second-party cryptologic collaborating centers receive the electrical copy.

The hard copy of the SIGSUM is designed for the executive reader who does not require timely electrical receipt of SIGINT items. It is available on his desk daily at the opening of business and contains the SIGINT available to NSA at approximately 1700 the previous day. During crisis periods and/or when an item is of sufficient importance to warrant distribution by electrical means more frequently than daily, an item is prepared and if ready for publication after 1700 hours is released as an advance item to the next daily SIGSUM.

Items appearing in the SIGSUM are never original items. By this is meant that all analysis is performed by the Production organizations having total responsibility for a specific problem. If and when a SIGINT report or item is developed by an analysis organization of Production it is serialized and distributed in accordance with established requirements and procedures. Simultaneously, an abbreviated item is prepared suitable for inclusion in the SIGSUM and forwarded to the SIGSUM panel for editing, processing, and distribution to recipients as explained above and in accordance with SIGSUM policy procedures. In all instances the serial number of the complete report is cited in the SIGSUM to assist the customer who must have the complete details for evaluation or estimative purposes in acquiring the unabridged report. The complete report on which the SIGSUM item is based normally reaches the recipient before or simultaneously with the SIGSUM item; therefore those recipients who need the complete details will have them available.

Since the SIGSUM is designed for selected senior executive readers, it is published six days per week, Sunday through Friday. This insures that readers working Monday through

Saturday will have the relatively latest SIGINT available each working day.

For the convenience of the readers, appropriate maps are included in the hard copy of the SIGSUM with notations and overlays showing the precise areas of activity as reported in the item. On occasion, photographs of military weapons or weapons systems are included primarily for the benefit of readers not familiar withese weapons. Photographs of weapons and weapons systems include ship types, sumbarines, aircraft, tanks, radars, missile systems, artillery pieces, etc. On occasion, photographs of personalities are also included.

In addition, selected collateral is included when it enhances the SIGINT or assists the reader in understanding it. In all instances where collateral is utilized it is so flagged in the item. In hard copy, collateral is printed in italics.

In instances where foreign collaborating centers have responsibility for reporting on a target and/or where unique SIGINT is available to them, such items as appropriate will be included in the SIGSUM, citing the foreign cryptologic collaborating organization's serial number and/or appropriate caveat to inform the reader that such an item is not produced by a U.S. cryptologic organization.

Senior military commanders overseas have expressed their interest in this document as it provides them with an appreciation of the level of military activity in other areas of the world and assists their intelligence staffs in evaluating military activity in their own areas. Intelligence staffs worldwide have found the SIGSUM valuable because of the brevity of the articles and their suitability for general briefing purposes.

~~(SECRET - HVCCO)~~

SOLUTION TO LAST MONTH'S NSA-CROSTIC:

Lambros Callimahos, "[The] Rosetta Stone [and Its Decipherment]," *NSA Technical Journal*, Vol. XVI, No. 1, Winter 1971.

"I feel particularly qualified to give this lecture because . . I was born in Egypt . . . Furthermore, the Ptolemies were Greeks. . . . Ptolemy V was five years old when he ascended to the throne, and I was four years old when I first set foot on the American shore, so you can see the similarities."

(UNCLASSIFIED)

SOME PRINCIPLES OF COVER AND DECEPTION

P.L. 86-36

Vera Filby's article ("How Do We Know It's True?") in the February CRYPTOLOG is a most interesting one and should stir substantial comment and thought.

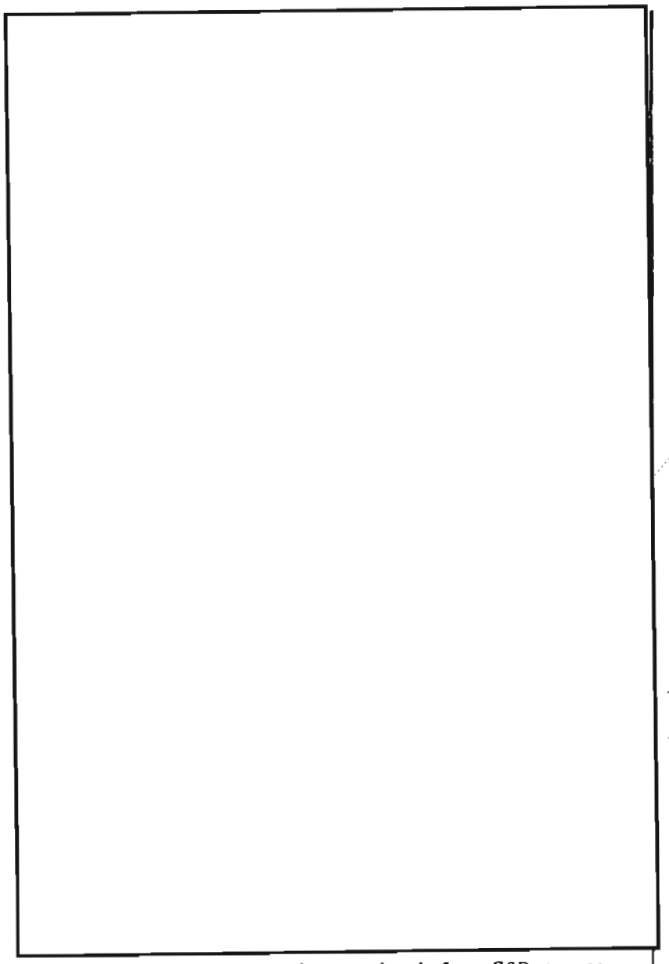
The article's publication is timely, inasmuch as it appears coincident with a new two-volume work by an English journalist, Anthony C. Brown, entitled *Bodyguard of Lies* (Harper & Row, 1975). Mr. Brown has done a good job of recounting the uses and successes of Allied cover and deception (C&D) operations in World War II. His story is set in a broad framework that includes key personalities, leading interests, and many of the apparent motivations and relationships which culminated in C&D operations. Understandably, the book emphasizes the role of Great Britain, starting with its title, which reflects a statement attributed to Prime Minister Winston Churchill: in wartime, he said, truth is so vital that it must be attended by a "bodyguard of lies." The small coordinating body which ran the British C&D effort reported directly to Churchill for reasons of both security and span of control.

C&D, in general, seems to have some principles that are worthy of iteration: first, and certainly foremost, is the principle of absolute and unassailable secrecy. Because commanders, with their operations and intelligence people, are often sensitive to being deceived, it is frequently true that the slightest hint that deception is being practiced or even planned is sufficient to abrogate the C&D operation as well as to heighten suspicion in the future. Accordingly, *all* actions taken to do things to and about C&D must be done with utmost circumspection. In that vein, the symposium which Ms. Filby recommends should be pursued with all due regard to "must-know/need-to-know" criteria. What Ms. Filby recommends, as I read it, is a symposium attended mainly by SIGINT people and some SIGINT users, to look into the question that the title of her article asks.

This leads to two more C&D principles:

- if a C&D operation works ideally -- or even reasonably well -- we either do not know that we are being deceived or cannot prove (or even hypothesize) it; and
- C&D operations, for the most part, are not limited to electrical communications alone, but also involve one or more levels of forces and units.

~~(SECRET - HVCCO)~~



This leads to another principle: C&D operations, of various magnitudes and kinds, happen not only in wartime, but also in *peacetime*. It is not an unreasonable assumption that they are being carried out right now.

A fifth principle of C&D is one which I might nickname the "ours/theirs" principle. In essence, it describes an existing condition in which both, or all, adversaries practice some C&D, and both, or all, simultaneously attempt to fathom all other C&D. I mention this aspect because it is that one condition that most easily leads to self-deception. By that I merely mean that it is important to keep straight who is doing what to whom when and for what reasons. If one element of the organization is supporting friendly C&D and another element is attempting to peer through an enemy's *possible* C&D, and there is no central coordinator, the self-deception that can result will compound the real deceptions. Interorganizational and intraorganizational work groups and symposiums can overcome some of the difficulties inherent in this potential problem, but they cannot take the place of a central, authoritative, coordinating body.

The last principle that seems worthy of mention is that of *surprise*. It is one of the hallowed "nine principles of war" and harkens back in history immemorially. It is inexorably bound up in the business of C&D and is frequently that which C&D operations seek to advance. It might be of interest to recall that contemporary Soviet publications dealing with military strategy and tactics are rather liberally laced with detailed discussions of the element of surprise. In several instances, those discussions are detailed enough to make it clear that the Soviet have assigned significant importance to that particular aspect of military operations. As might be expected, that literature contains associated references to C&D less frequently, but those references are not altogether absent, either explicitly or inferentially.

In my view, which is shared by some of my contemporaries, Ms. Filby's basic question, "How do we know it's true?", is of central, compelling criticality in today's U.S./Allied intelligence community, especially in the signals intelligence part of that community, where there is sometimes a tendency to place increasing credence in and dependence upon limited, decreasing signals sources. Our understandable tendency to rely on what we have -- however tenuous it may be -- can be used against us, and with dire consequences, in time of war. Our national defense strategy is increasingly dependent upon "indications and warning" (I&W) intelligence. There is nothing wrong, in any way, with that dependence, *provided we understand and can resolve the problem addressed in the Filby article*. I believe the problem is recognized and understood in some quarters, but not as widely as it might be. I believe that to deal realistically with the problem, considerably more attention is warranted. I would start by establishing a single, central, coordinating group with defined authority to work across organizational boundaries. The initial objective of that group would be to assess the magnitude, dimensions, and impact of the problem. If the problem is found to be of sufficient size and consequence, the next step would be to organize the attack on it. A modest number of additional man-hours may then be warranted. Some priorities may have to be changed to identify and task those man-hours. The first "product" out of that effort probably should be directed toward our own current reporting, to strengthen the value of I&W intelligence.

To the extent that this "science" now has an epistemology, it is inexact. Our current understanding is, at best, inconclusive, in part because it is not yet organized. In point of fact, how do we know "it" is true?

~~(SECRET HVCCO)~~

CONVERSATION WITH A BOOKBREAKER (SINCE RETIRED)

[redacted]

~~(SECRET - HVCCO)~~

EO 1.4.(c)
P.L. 86-36

TRANSLATORS' COMPENDIUM

The sample pages on the opposite page are reproduced from the NSA/CSS publication *Collected Articles on Translation, 1973*, compiled by [redacted] (TSC). Mrs. [redacted] three-sentence foreword "says it all": P.L. 86-36

> *The following articles, which first appeared in QRL, Keyword, Spectrum, the NSA Technical Journal, [Dragon Seeds, and CIA Studies in Intelligence], have been selected for their bearing on the subject of COMINT translation as seen through the eyes of practioners of the art. Together they represent the experience of a generation of Agency linguists. They are here reproduced in the hope that they will interest and stimulate another generation.*

The publication contains more than 500 pages and is divided into seven sections, plus a bibliography. The section "Training for Translation" has articles by Doris Miller, Emery Tetrault, [redacted] and [redacted] "The Translator Helps Himself" has articles by [redacted] Mary Roberta Irwin, Stewart H. Buck, Robert E. [redacted] Norman Wild, and John D. Murphy. "Preparing the Text for Translation": [redacted] "Problems in Translation, General and Specific": [redacted] A. J. Salemme, [redacted] P.L. 86-36
James Duncan, and Jack Gurin. "The Erring Translation, and What to Do About It": Harry G. [redacted] Dr. Marion Griggs, [redacted] Doris Miller, A. J. Salemme, [redacted] Barbara Dudley, Stu- [redacted] Donald Lasley, Norman Wild. "Machine Translation": [redacted] [redacted] A. J. Salemme, Doris Miller, Norman Wild. "About Translators and Translations: A Miscellany": [redacted] Barbara Dudley, [redacted]

The subjects covered in these articles are still current ones. For example, every week someone becomes newly agitated about the problems of transliteration or of machine translation, but is unaware that the ground has often been covered before. For that reason, this reminder is being printed, so that the new generation of linguists can be aware of the existence of this record of other linguists' efforts.

A few copies of the publication are still available. If you would like a copy, call [redacted] P16, x4998, Room 3W076. Reference P.L. 86-36
copies are available in the Cryptologic Library, Room 3W076, and in the NSA Technical Library.

DOCID: 4019630

P.L. 86-36

THE CREATIVE TRANSLATOR

by [redacted]

"It is essential that the captain take steps to assure an attack as soon as possible," the translation read. "No delay will be accepted." I knew that the text in question has been passed in the heat of battle, by a man desperate in the face of imminent defeat and possibly death. It struck me that his language was rather formal for the occasion.

[redacted] I would have translated it, "Strike soonest without fail. ((Time)) is of the essence. Any delay will mean failure." The first tr[illegible]lation was not wrong, It simply missed the point.

The example is an extreme c[illegible] altered to protect the guilty), tendency of translators to smoc[illegible] original, to impose order and [illegible] everything in unruffled govern[illegible] destroy the vitality of the o[illegible] it. In so doing, we do our c[illegible] say nothing of insulting thei[illegible]

This article, then, is [illegible] lation. Unlike other disci[illegible] answer, translation plunges [illegible] ambiguity where there are [illegible] right ones. The choice of [illegible] depends not on dictionarie[illegible] gence, emotion and unders[illegible] language, which is first [illegible] ably tied to feelings in[illegible] and heavy with emotional[illegible] means of information co[illegible] darkness. And as any l[illegible]

confusion among linguis[illegible]
tor [redacted]

● the people taking a[illegible] few years ago. It [illegible] material and one of [illegible] been [redacted]

graphese). Several [illegible] ad real trouble trying t[illegible] Out of admiration. . ." o[illegible] so wrong.

But the problems caus[illegible] pared to the problems g[illegible] marks. Sometimes it [illegible] he end of one sentence [illegible] There is the classic

DORIS MILLER

TOP SECRET UMBRA

TOP SECRET UMBRA

LEARNING FROM MISTAKES

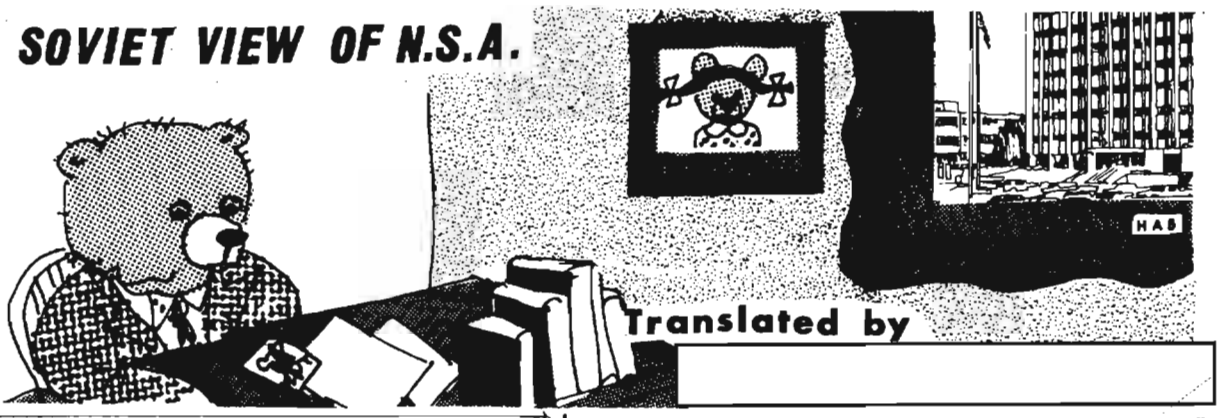
By Mary Roberta Irwin, G543

[redacted]

EO 1.4.(c)
P.L. 86-36

DOCID: 4019630

A SOVIET VIEW OF N.S.A.



Translated by

Translator's note: *A recent Soviet book on SIGINT (*Radioehlektronnaya Razvedka *(Radio-electronic Intelligence), V. A. Bartanesyan, Moscow, Voenizdat, 1975) is evidence of a Soviet effort to heighten awareness of the vulnerabilities of electronic emitters among all those who work with them. Two hundred fifty pages long and citing 70 titles -- mostly U.S., British, and German books and periodicals -- as sources, the book outlines the organization and scope of the U.S. SIGINT effort and its technical capabilities. It is, in effect, a SIGINT primer.*

Chapter I is introductory and general, sketching out the structure of U.S. SIGINT and its place in intelligence, recounting some anecdotal WWII SIGINT history and summarizing its postwar development up to the present, including the growth of SIGINT collection by satellites. Chapter II discusses the exploitation of the various portions of the electromagnetic spectrum, and Chapter III treats antennas. Chapter IV is devoted to signal search, intercept, and analysis equipment. The fifth and final chapter is on direction finding.

The tabloid-style description of NSA given in Chapter I might almost seem to have been written tongue-in-cheek if the broad irony of certain assertions could be accepted as being truly intentional and not simply accidental. The following is a translation of that description.

The NATIONAL SECURITY AGENCY (NSA) is one of the largest intelligence organs in the United States. NSA occupies a special place in the general system of global espionage. It informs the President and other high-ranking persons concerning the political and economic situation and the defense posture of many countries of the world, including the allies of the United States. The entire work of NSA is highly classified. Only rarely does information of the doings of NSA appear in the bourgeois press. Nevertheless, from the fragmentary information that gets published some idea of the enormous scale of its spying activity can be formed. NSA Headquarters is located at Fort Meade, midway between Washington and Baltimore, in a huge three-story building that is second only to the Pentagon and State Department in size. P.L. 86-36

NSA is the chief SIGINT agency and has unlimited financial and technical capabilities. NSA's long tentacles of radioelectronic espionage reach everywhere. Created in 1952 by a presidential order of President Truman with the obscure explanation that it is "charged with carrying out highly specialized functions involving the national security of the United States," NSA has developed into an enormous SIGINT service. Its annual budget is over a billion dollars, and its staff of employees at the Headquarters alone is 14,000. Three or four thousand employees work abroad, and about 20,000 service personnel who are formally subordinate to other intelligence organizations are in fact engaged in SIGINT work in behalf and under the control of NSA.

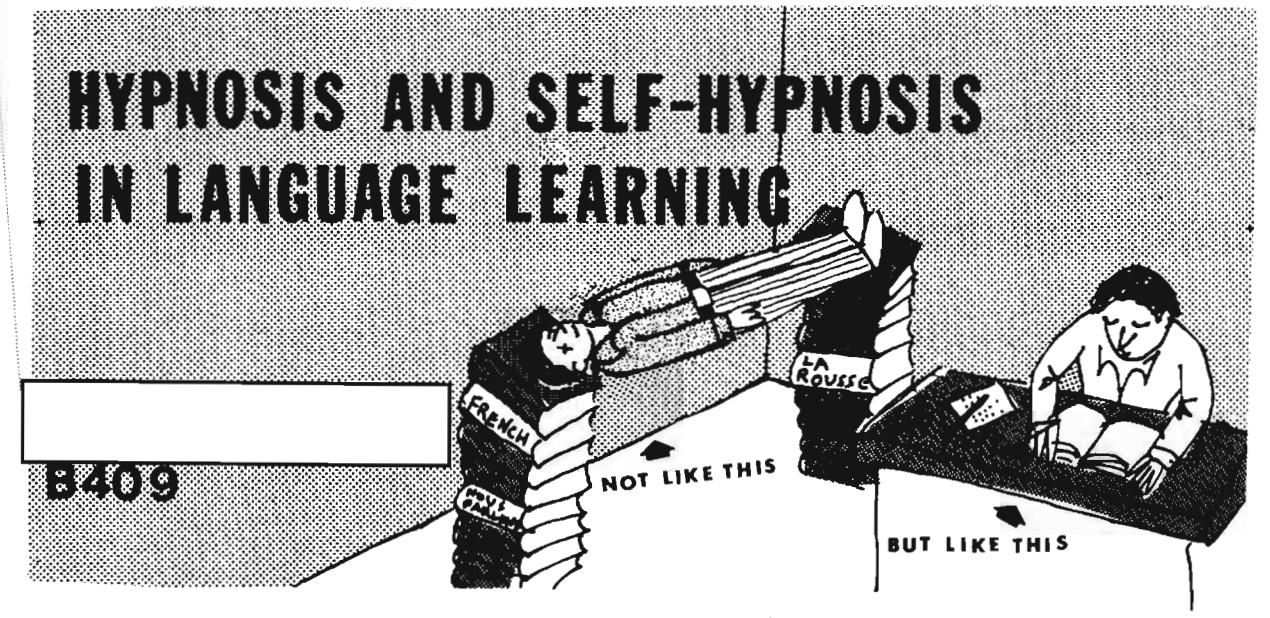
NSA conducts radioelectronic espionage from ground centers (military bases), piloted and pilotless aircraft, naval surface vessels and submarines, and from satellites equipped with appropriate radioelectronic gear. NSA uses universities and the research laboratories of various industrial corporations to find solutions to various technical problems and to build improved SIGINT collection apparatus.

The functioning of several major departments is known from the foreign press -- Operations, Scientific Research, Communications Security, and others. The largest is Operations, which is engaged in processing the data collected and received from all SIGINT collection points, deciphering it on the basis of engineering cryptanalysis, and compiling operational reports. The focus of attention of Operations is on deciphering the governmental and diplomatic codes and ciphers of various countries, as well as the codes and ciphers used by the armed forces of those countries.

NSA Headquarters has a large electronic computer center supporting the computer operations of all the major departments of NSA.

DOCID: 4019630
P.L. 86-36

HYPNOSIS AND SELF-HYPNOSIS IN LANGUAGE LEARNING



In this article I won't be conjuring up images of Svengali or Dracula, or discussing hypnosis as stage entertainment or as depicted in highly fictionalized TV plays. Nor will I be discussing the deep stages of hypnosis as used for medical purposes, such as in childbirth, to replace a chemical anesthetic. Instead I shall be discussing hypnosis and self-hypnosis as a language-learning tool, for which a relatively light state of relaxation is sufficient.

Because relaxation is really what hypnosis is all about. Sorry about that, but hypnosis does not really involve mystic trances. It won't bring you back to a previous incarnation, force you to become unwillingly involved in crime, and, above all, it won't cure anything -- except, possibly, insomnia. Hypnosis is no more and no less than a heightened state of relaxation, self-induced or induced with the aid of a hypnotist, during which you are considerably more open to suggestion than when you are "awake." Why the quotes around "awake," did you ask? Because it is a word that hypnotists use to differentiate between being hypnotized ("asleep") and *not* being hypnotized ("awake"). Actually, however, hypnosis is not sleep in the natural sense -- there is no loss of consciousness, no trip to Never-Never Land, no loss of contact with the hypnotist or the surroundings, no sense of being in a trance. The only thing you feel when hypnotized is relaxation.

Most people have become hypnotized in the sense that they have succumbed to a suggestion that slipped into their subconscious mind while their conscious guard was down. If I start telling you about sucking on a lemon, I'll bet it won't be long before your mouth starts reacting! Or if I start yawning in a crowded room, it won't be long before someone else starts yawning. Sometimes, though, it doesn't take another person to get you going. When was the last time that you decided to buy an item displayed at the supermarket checkout counter, even though you didn't need it? The point is that we are all subject to suggestion and autosuggestion. Hypnosis (which, incidentally, was named after the Greek god of sleep, Hypnos) simply formalizes that idea and is a way to make the character trait of suggestibility a positive rather than a negative feature.

But enough introduction! Let's get into that language classroom!

Even though the student wants to be there (or says that he wants to be there), the language classroom is basically a hostile environment for him. The student's motivation for learning may be affected by years of adverse conditioning, of which he is not even aware. He is going to be faced with new behavioral problems. He might be so introverted that he will feel embarrassed and even say, "I can't do it!", when asked to articulate the "funny sounds" of the foreign language. He may lack confidence in his ability to memorize large numbers of foreign words or grammatical rules, or, when learning certain languages, to figure out how the language works with little or no formal structure. Finally, and probably most important, he is under stress and pressure that he could not have easily calculated. Unfortunately, almost none of these problems will be taken into account within the language class proper. Nowhere in the curricula is there a mention of classes in relaxation, concentration, motivation, or mental conditioning. And yet there ought to be such classes, because it is just as easy to condition the mind as it is to condition the body.

DOCID: 4019630

So let's do something about it! Just about every reasonably intelligent person can learn a foreign language (as just about every reasonably intelligent person can be hypnotized). Many people who say they cannot learn a foreign language (as many people who say they cannot be hypnotized) are really saying not that they *can't* do it, but that they *won't* do it. No language teacher can *make* you learn those grammatical endings, just as no hypnotist can *make* you relax. You have to want something, and you have to cooperate. All right, then, do you really want to learn the language? If so, here are a hypnotist's suggestions to help you learn it quicker and better.

I would like to focus on the following five areas:

- relaxation,
- concentration,
- confidence,
- motivation,
- mental conditioning.

I shall limit myself to the hypnotic methodology, although much of what I will cover is common to all types of relaxation therapy.

Relaxation

This does not happen automatically, but it can be learned, sometimes just by picking up a book on the subject and following instructions. Most often, however, the student needs some kind of instruction in relaxation. With hypnosis, he will usually attend about eight sessions. After the initial visit, which I shall describe elsewhere in this article, he will attend as a member of a small group. Those remaining sessions will be more or less identical, except that special problems may receive added emphasis. The hypnotist will hypnotize the group all at the same time and begin making his suggestions. He will start with suggestions of relaxation and will deal with such as ideas as relaxing without slowing down; coping with stressful situations; maintaining composure under difficult conditions; relaxing while alone or with others, friends or strangers; and conditioning intended to convince the subject that he can relax under any conditions at will. He will mention the benefits of such a capability, emphasizing that tension steals energy. The hypnotist will stress the need for restful sleep and suggest that the student will indeed sleep restfully and wake up every morning feeling refreshed and eager to get going on the new day.

The ways in which these suggestions can help the language student are far-reaching. He can relax in the classroom when it is his turn to speak those "strange-sounding" words; he can overcome the general nervousness and embarrassment he feels when he makes mistakes, and be composed enough to correct them; he can relax when doing his language homework -- memorizing words or learning grammatical rules; and he can pay far better attention to what is going on in the classroom. Instead of nervously worrying about his own performance, he will be learning from the performance of everyone in the class, not just himself.

Concentration

As I just mentioned, the calm individual pays better attention to what is going on around him. Because he can relax, he can concentrate his attention better on the job at hand. The suggestions that the hypnotist can make in this area center on: better concentration through relaxation; getting a stronger impression from the material studied, so that retention and recall are easier; improved memory; better organization of time and efforts, with less procrastination; accomplishment of the things the student wants to do and has to do.

The language student can apply these suggestions primarily in his classroom participation and homework study. He will be able to tune out distractions at both times, making his efforts more productive and pleasurable.

Confidence

Here the hypnotist will work against any adverse conditioning that may be present. He will make suggestions designed to strengthen the student's confidence in his ability to practice self-hypnosis; in his ability to cope with any set of circumstances; and in his ability to absorb the complex material being studied.

And how will the language student apply these suggestions? He can apply them in every area of language study, but perhaps more than any other suggestions, these will work on a subconscious level to make the course more productive for him. A student is not always aware of adverse conditioning that may have taken place previously. He may think that he is "not particularly good at languages," because of impressions made upon him as early as elementary school. He may feel that his intellectual capacity is much lower than it actually is, or consider the language material more complex than it actually is. Through hypnosis and self-hypnosis he can change that kind of negative thinking, he can "recondition" himself and learn to appreciate his true capabilities. While humility is a fine characteristic, we already have enough humble linguists, and sometimes the difference between the good linguist and the great one is no more than the confidence to cross the line between translating something as "swelling of the thyroid gland on the neck" or as "goiter." In other words, the confidence to let go of the literal translation and to make the translation read as well in English as it did in the original foreign language (maybe even better!).

Although it will almost certainly follow that the relaxed, concentrating, confident student

will be a better student, the hypnotist will reinforce suggestions of motivation. He will reinforce the ideas that relaxation saves energy, reduces or eliminates tension, and makes sleeping easier and more restful; that better concentration strengthens the initial impression that the student receives from the study material, improves retention and recall, and motivates the student toward better-organized efforts; and that the student will be confident of success.

Although it is probably the most elusive of animals, motivation can be caught and tamed. "Nothing succeeds like success" may be a cliche but that doesn't make it a false statement. The more language a student learns, the more he is likely to learn as he goes along. What he often needs is an extra charge of steam at the beginning of his language course, when he has serious doubts -- often bordering on panic -- that he will ever be able to master this impossible language. Those doubts can be eliminated, and if we do that, we go a long way toward reducing the high attrition rates that are usually associated with language training.

Mental Conditioning

Unless the student learns to practice some form of mental conditioning on his own, the whole purpose of hypnosis is defeated. Posthypnotic suggestion by the hypnotist does not last forever. Therefore the suggestions made by the hypnotist must eventually become suggestions reinforced through self-hypnosis by the student himself. He will be told while hypnotized that he can bring about this same state of relaxation by himself, usually once a day just before going to sleep at night. During the day he will reinforce the suggestions by repeating keyword suggestions ("Relax," "Concentrate," etc.) to himself. These are designed to produce a conditioned response of calmness, concentration, confidence, etc. An important distinction here is that the student will not be hypnotized or enter any "trance" during the day. Rather, he will have conditioned himself to respond to the suggestions while awake, that is, posthypnotically.

How to Do It

It all sounds so easy, so why isn't everyone doing it? Actually, a great many people throughout the world are already involved in this or similar training, but usually on an individual basis, that is, one person attempting to improve his performance in a given area. Literally hundreds of thousands of Americans are currently involved in self-hypnosis, meditation, biofeedback, transactional analysis, or some form of relaxation therapy, trying to do everything from easing the strain of a high-pressure job to shaping up an entire baseball team. So why shouldn't a language student try it too?

Let's say that he *does* try it, with hypnotism. He walks into the hypnotist's office. What happens then?

The hypnotist has an initial private session with the student. During that session he tests the student for suggestibility, imagination, and subject type, all of which information tells the hypnotist what are the best methods he should use. He also shows the student how hypnotism works, but does not actually hypnotize him at this time. Instead, he uses various "waking tests," such as asking the subject to hold both arms straight out in front of him and then suggesting, with appropriate words and appropriate vocal modulation, that the right arm is very heavy and the left arm is very light. Or he will stand behind the subject and tell him to think about falling back, knowing that the hypnotist will break his fall if necessary. Either with or without further suggestion by the hypnotist, a suggestible subject will usually start swaying on his heels within a few seconds.

The hypnotist and the student then discuss any questions, general or specific, that the student might have about hypnotism, and the particular problems he is having in language learning.

After the tests and the discussions, the hypnotist uses an appropriate method to hypnotize the student, using no more than a couple of minutes to do so. In addition to implanting suggestions designed to improve the student's learning, the hypnotist makes suggestions designed to produce greater depth of hypnosis during subsequent sessions and to condition the student for the group-induction method that will be used in future sessions. The hypnotist also tests the student by implanting a posthypnotic suggestion. This is done for two reasons: to prove to the student that he was actually hypnotized (the feeling of relaxation alone is sometimes not enough to convince persons that they have been hypnotized); and to give the hypnotist some idea of how quickly the student will respond to further hypnotic suggestions. And that ends the first session.

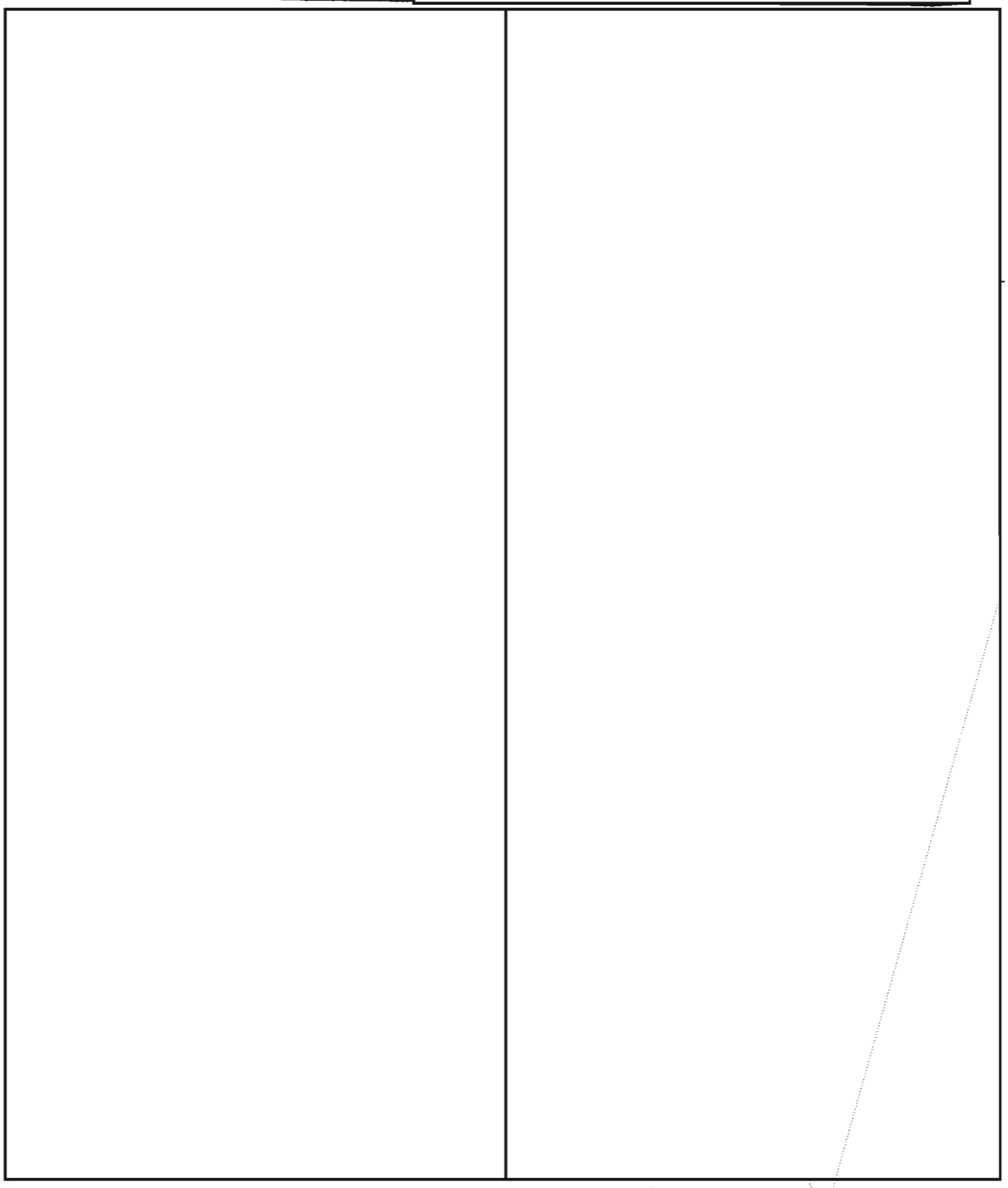
Subsequent sessions, by the group method, involve a discussion concerning progress, questions and answers, and group hypnosis. But in these group sessions, use is made of the same suggestions on relaxation, concentration, etc. which were outlined above. It's that uncomplicated!

But let me make it clear that hypnosis is not a cure-all. It is not a way of life or a religion, but simply a way to take advantage of unused mental capabilities. It can do a lot of things but it cannot *cure* anything, and it cannot make you do anything unless you want to do it. So if you really want to learn a language but are having problems speaking it, or memorizing words or grammatical forms, hypnotism is just one way of getting help. Why not try it? Just relax. . .

~~CONFIDENTIAL~~

WAVEGUIDE ANALYSIS

P.L. 86-36



P.L. 86-36

~~CONFIDENTIAL~~

DOCID: 4019630

A SIMPLE CIPHER STORY

William P. Meyer,
C512F

Many years ago, having read Edgar Allan Poe's "The Gold Bug" and articles on codes and ciphers in the old *Shadow* magazine, I thought it would be a simple matter to construct a cipher to keep private some love letters I had received during my high school days. I knew my wife-to-be would not take kindly to my keeping them even for sentimental reasons.

I thought I had it made by taking the alphabet and cutting it in half. Since I knew what the message said, I would find it a simple matter to substitute the correct letter in case of doubt. The cipher was similar to this:

```
ETAIONSHRULDM    CBGVFPJYWKXZQ
QZXKWYJPFVGBC    QZXKWYJPFVGBC
```

In other words, I reversed the last thirteen letters and repeated them twice.

I immediately enciphered the letters, keeping the same format, and threw the originals away.

```
Dear Bill,  (Clear)
BQXF ZKGG,  (Enciphered)
DEAR TILL,  }
ZCGW BVXX,  } (Two possible solutions)

x x x x Body of the letter x x x x x x x x

(Clear)                    Love, Virginia
(Enciphered)               GWKQ, KKFXKYKX
(Two possible solutions)   { LOIE, IIRAINIA
                           { XFVC, VVWGVPVG
```

Needless to say, about three months later my wife presented me with the letters, neatly deciphered. She was wondering why I thought they were worth keeping.

Now the romantic thing for me to have done would have been to join the Foreign Legion, but since I was patriotic, I joined the Army. I was sent to Fort Monmouth, New Jersey, attended the U.S. Army Signal Corps School, and graduated as a Cryptological Technician, MOS 805.

It is true that, in this day and age, the romantic notion of keeping love letters, either in the clear or enciphered, is no longer the "in" thing. But my advice, born from personal experience and reinforced by practical experience, is:

Always place the externals of your message internally within the body of the message.

(UNCLASSIFIED)

GEOGRAPHIC NOTE

(Continued from p. 4)

in 1920, and then was renamed *Liepaya* after Soviet incorporation.

The back-and-forth naming and renaming of places in the Baltic area is not a unique situation. Throughout the world, placenames are constantly changing. Old cities are given new names. New cities are being created. Countries whose names we remember from postage-stamp collecting years ago still exist, but with different names. So if, in your work, you encounter any difficulties with placenames, of any vintage, check with the NSA Geography and Map Library, C525, extension 5725 or 5726. We're here to tell you where it's at.

[redacted] C525

(UNCLASSIFIED)

CLA ANNUAL BANQUET
Thursday, 27 May 1976.
Trojan Horse Restaurant,
Holiday Inn, Silver Spring.

Speaker: [redacted] (formerly ONI & CIA; now retired): "Elegant English"

For information, call: Banquet Chairman, [redacted] x7222s

DOCID: 4019630

This issue marks the end of my year's apprenticeship as "the new boy." I hope that, during this year, CRYPTOLOG has had at least a few informative articles of interest to each of its more than 2500 recipients. During this year I have actually heard a few comments, ranging from "That last issue was the best one yet, Art!" to "That last issue was absolutely nothing! -- the worst excuse for a magazine I've ever seen!" (usually said about the same issue). I've enjoyed editing CRYPTOLOG, even though I have to sniff an awful lot of rubber cement to get the copy into a form that satisfies everyone -- the author, the editorial board, the casual prepublication nitpickers, and, ultimately, the intended reader. The one thing I regret is that I don't have enough time to sniff out ideas for articles and to help authors to develop them. True, I have developed the previous editrix's habit of butting into every technical conversation and asking, "Have you thought of writing that up for CRYPTOLOG?" All a person has to do is burp and I suggest, "Hey, an article on the incidence of gastritis among NSA-ers?" Usually, however, these ideas come to naught. I have a fairly long list of names of people who swore long ago that they would submit an article, but haven't (my "Promises, promises" list).

In the meantime, as I read through the submitted articles, and/or edit them, and/or type them up, and/or paste them up into final copy, and/or illustrate them (you just can't get good help nowadays), I often end up with lots of scraps of paper all over my desk, but also with scraps of ideas for what I think might be good articles. Who can write them, though? I would hate to write them all myself, signing them with noms de plume like "Paul E. Glott." I would also hate to throw the scraps away, just as a person who does a lot of home sewing hates to throw away his best remnants (the libbers have me so confused with "his" and "her," I'm never sure, as an editor, when I'm getting it right). Maybe I can turn these scraps into a "crazy-quilt" end-of-year report. . .

Transliteration

One article I'd like to get from an NSA-er would deal with transliteration and the tricks it plays. An article recently published in CRYPTOLOG mentioned the problems the author had had in locating a certain word in Russian dictionaries. Then, she said in her original manuscript, "COB" jumped off the page and suggested another linguistic tack to take. Since she had been writing about Russian all along, I figured that I'd better ask her which **СОВ** she meant -- the abbreviation for **советский** ("Soviet") or **совершенно** ("completely," "top" as in **сов-секретно** "top secret"). When I phoned her, she said, "Neither! It's English! C-O-B -- 'close of business.'" My theory is that when the word jumped off the page, she might have *thought* she was reading English, but I'll bet that it really registered subconsciously as a Russian abbreviation that sent her off on the right trail. "An article on psycholinguistics?"

Jane-Aceisms

Everyone in my generation has a favorite expression as used by Jane Ace on radio aeons ago. With some it's "He's got all the earmuffs of a hardened criminal." With others it's "She's been galvanizing all over town." One of my special treats as editor is to collect the new generation's Jane-Aceisms. (True, I get plenty of them from my own kids, such as "in this day of age," but I can always appreciate more.) Some of them I edit out (for example, in a serious article I changed "tinge of pride" to "twinge of pride," until it dawned on me that that wouldn't do, because a twinge is supposed to make you say "Ouch!") But others I leave in, especially in letters to the editor. I don't do that to be mean (after all, I *do* correct the spelling and change the punctuation in some letters). It's just that a letter to the editor should express the writer's exact words. So what if the writer accuses the editor of "leading field personnel down a primrose path"? Why change it? Why add a snippy "editor's note" pointing out that people lead *other* people "down the garden path," but people (at least the ones I know) usually take "the primrose path" of their own volition? No, whether I edit them out or leave them in, I just enjoy these "almost-right" expressions. I only wish that someone would write an article about them -- maybe "Jane-Aceisms at NSA"? I'd

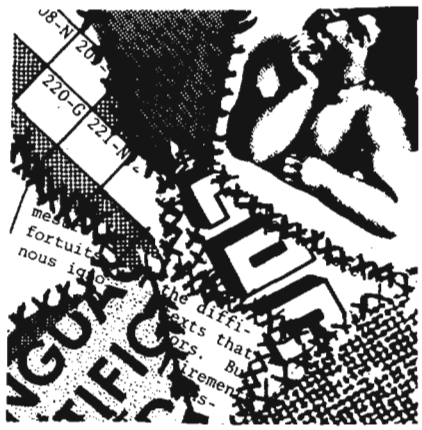
give the author all my best examples, including the one I heard in the cafeteria a few weeks ago. Three guys playing cribbage. One almost wins the game. One of the others says, "Close, but no car!" If anyone volunteers to write the article, I'll promise to find a picture to illustrate it -- an angel wearing black shoes. And I'd give him all the stores that former NSA-er [redacted] told me about his chief petty officer, including the story about the time that all hands were supposed to show up for inspection. One of the men (he's always named Kozlowski in stories like this) was wearing white socks with black shoes. The petty officer said, "Kozlowski, you will go BACK to your area! You will REMOVE them white socks! You will report back here wearing BLACK socks with black shoes! And in the HEREAFTER, you will wear black socks with black shoes!"

Geographical names

I've always liked geographical names. In fact, I first got interested in Russian when, during World War II days at Fort Lewis, Washington, I would have to stand, several times a day, either alone or with one or more other enlisted men and stare, while otherwise engaged, at a map of the USSR that was posted on the wall. I guess that the official feeling was, "As long as they're going to be standing there anyway, they might as well learn Rooski geography!" At any rate, I find geographical names absorbing and always try to get them right in CRYPTOLOG articles. "Da Nang" versus "Danang" was an easy one. But the names in an article in this month's issue were particularly tough -- places that had had German, Latvian or Estonian, then Soviet names (including names "not recognized" by the U.S. State Department), renamed Soviet cities, etc. The problem represented by Libau-Libava-Liepaya is a common one in Eastern Europe. I remember an emigré who had come from L'vov (in the Soviet Ukraine, but at one time Polish Lwów or German Lemberg). His grandfather insisted on calling the city Lemberg. So did the grandson until, one day, there was a showdown in school. The teacher said, "Pupil Ivanov will stand up!" He did so. "Pupil will come to front of room!" Did so. "Pupil will face class!" Did so. "And now -- pupil will say we're in L'vov!"

NSA-Crostics and other frills

Don't look for the definition "What the teacher told pupil Ivanov in L'vov (formerly Lemberg). . ." when doing the next NSA-Crostic. But look for a similar one. Because it seems that, despite all the erudition that is crammed into these once-every-three-months puzzles, the only things that seem to register on the readers, according to comments I hear, are items such as "Wait till the nun signs, Shelly!" Which brings me to other frills -- the illustrations in CRYPTOLOG. Some people think that CRYPTOLOG should have no illustrations at all. They feel that if an article on submarine warfare is illustrated with a pussycat staring at a goldfish bowl, the only thing that people will comment on is the damned pussycat -- they won't even bother to read the article. But another view is that the illustrations are supposed to lure people into reading articles that they would normally leave unread. Or to jog their memory months later -- "Yes, I remember reading an article on submarine warfare in CRYPTOLOG -- or was it the Tech Journal? -- it had a picture of a pussycat staring at a goldfish bowl!" Which opinion do you share? More illustrations? Fewer? More articles on a certain subject? Fewer? Please make your feelings known to any one of the members of the Editorial Board, so that we can take them into consideration in future issues. Incidentally, if you're in favor of *more* articles on a certain subject, why don't you write one of them?



Letter to the Editor

To the Editor, CRYPTOLOG:

I greatly enjoyed [redacted] *article on Soviet slang in the February issue. But what does that drawing at the end of the article represent?*

[redacted]

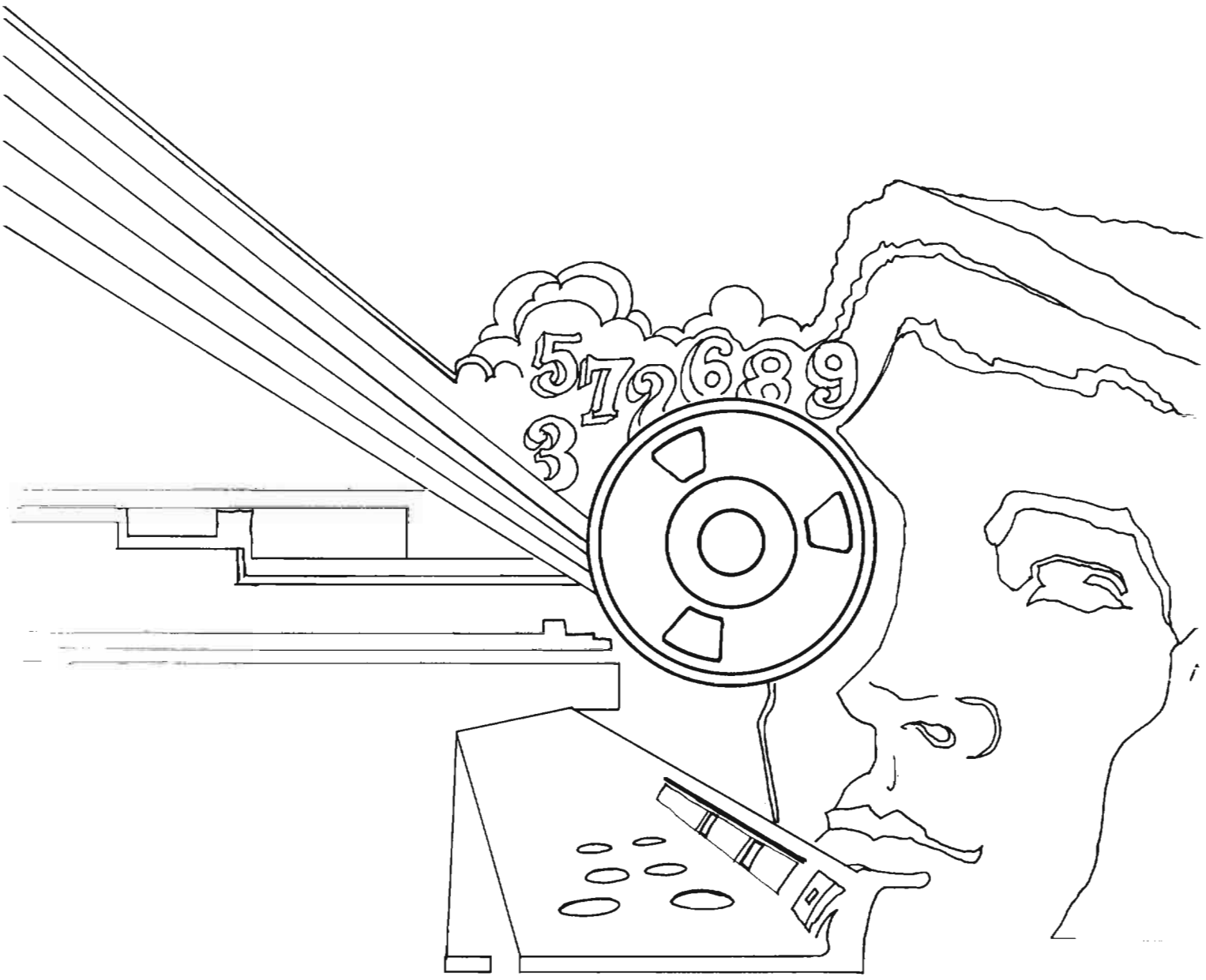
Editor's reply:

The drawing didn't come out too well (when the master plates were reduced 20% in printing, the table came out too dark). It's supposed to be a little old lady's desk. She has removed her spectacles and has put down her magnifying glass. She had been using the magnifying glass to check the cut-out Russian words in her dictionaries. Visible in the magnifying glass is the end of one word: ---HO. Incidentally, your last name isn't in the phone book, but it's in Webster's. Are you sure your name isn't [redacted]

(UNCLASSIFIED)

P.L. 86-36

Pl-Apr 76-S3-24583


5 7 7 6 8 9
3

DOCID: 4009731

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

APRIL 1976

P.L. 86-36

ONE DAY IN DANANG..... [redacted] ... 1
WILL THE REAL ELINT PLEASE STAND UP?..... [redacted] ... 5
BEST LOCATION FOR COMPUTER APPLICATIONS.. [redacted] ... 6
ON BEING TRUTHFUL.....David W. Gaddy.....10
THE VOYNICH MANUSCRIPT REVISITED..... [redacted] ..11
HIDDEN LOSSES IN COMINT PRODUCTION..... [redacted] ..13
LETTERS TO THE EDITOR.....15
NSA-CROSTIC No. 3.....A.J.S.....18
HOW DO ADULTS LEARN LANGUAGE?..... [redacted] ...20
COMPUTER-AIDED TRANSCRIPTION..... [redacted] ...23
NCS COURSE-EQUIVALENCY TESTS (Clarification).....28

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009731

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. III, No. 4 APRIL 1976

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5642s)
Collection.....[redacted] (8955s)
Cryptanalysis.....[redacted] (8025s)
Language.....Emery W. Tetrault (5236s)
Machine Support.....[redacted] (3321s)
Mathematics.....Reed Dawson (3957s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Frederic O. Mason, Jr. (4142s)

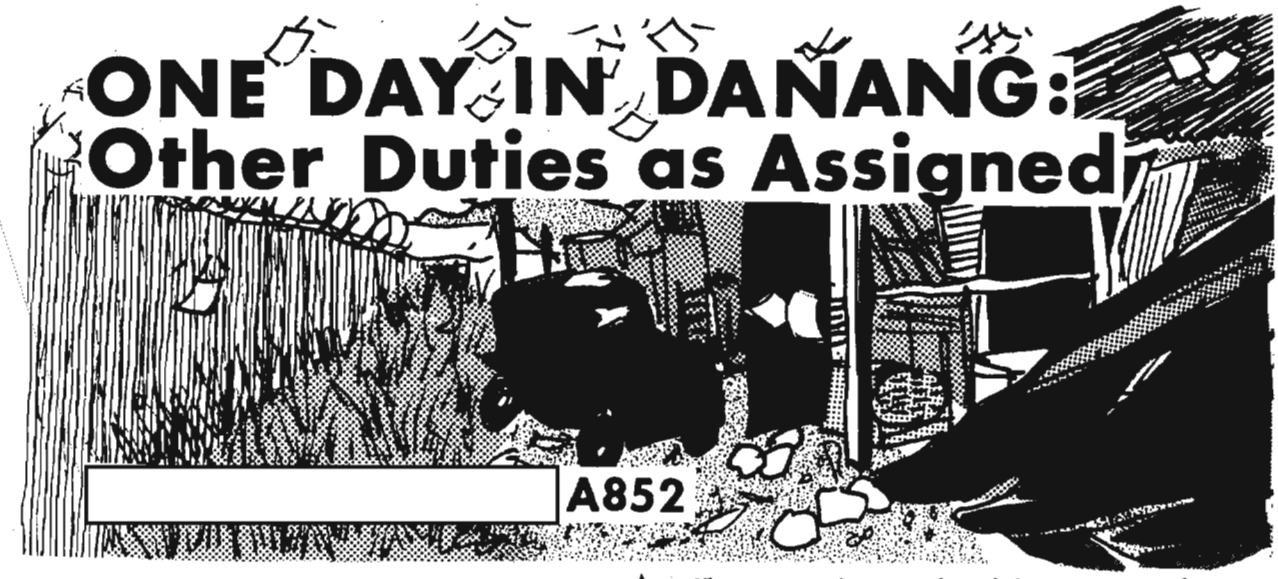
P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4009731

P.L. 86-36

ONE DAY IN DANANG: Other Duties as Assigned



It's 29 November 1974. At about 1000, Lieutenant [redacted] and I leave Danang Center in my jeep and drive to the site on top of Monkey Mountain. We get there just before 1030 and go right into the intercept van. I immediately notice that the men aren't using their KY-8 secure voice equipment when talking with Danang Center via radio. In fact, they not only don't have it turned on, but don't even have it hooked to the VRC-46 transceiver. [redacted] explains that the men use the KY-8 only when they have to pass intercepted VC messages to the Center. He says that they are afraid to burn it out, as it gets quite hot after being on for a while. I hit the roof over this. All the work we've gone through to install secure voice communications and they won't use it! When you consider how much intelligence Danang Center gets from low-level VC voice activity, you'd think these guys would realize that their own communications are just as susceptible to intercept. I instruct [redacted] that his men should *never* communicate with the Center in the clear now that they have the KY-8s and assure him that they don't have to worry about burning the gear up. If they can cook their rice on the KY-8, all the better. Heat has no effect on it.

Then I go out to look at the antennas. I find that the SHF corner reflector is oriented a little off-compass and the bottom half of the cage has slipped loose. Fix it. Then I look in the building that has been proposed for the site expansion. I have some misgivings about it (more about this later).

At about 1045, [redacted] and I are back in the van when we feel a shock wave sweep over us. We all go outside and watch as a great black cloud forms over the south end of Danang Airbase, maybe 15 miles crow-flight from us. At the time, it looks as though the source of the smoke is quite close to Danang Center, so [redacted] and I head down off the mountain immediately. As we descend, we feel two more shock waves.

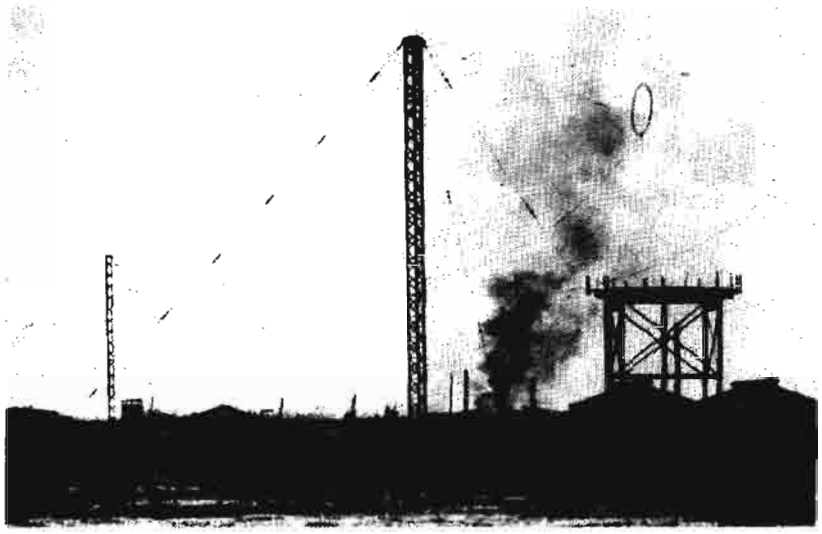
When we arrive at the airbase gates, the ARVN guards won't let us go around the south end of the runway. We have to get to the Center by going via the back route. From the Center we can see that it's the Army/Air Force ammunition dump at the south end of the runway that has gone up. Flames are still shooting up and small stuff like mortars and rockets are still exploding. The first explosion we had felt and the other two shock waves that rolled over us as we were coming down Monkey Mountain apparently had originated at revetments of 500- and 750-pound bombs. The Center is about 4000 feet from the dump, so no bomb or shell fragments have dropped within the compound.

The concussion waves have done some damage. The first one ripped the doors off the Morse intercept bay and a few other buildings, and knocked the fluorescent tubes out of most of the fixtures. A couple of the antennas look as though they have been pushed over a bit but they should be easily fixed. Luckily, no one was hurt.

EO 1.4.(d)
P.L. 86-36

[redacted] has evacuated almost all the men from the Center and sent them to the barracks area to check on their families and homes. Lieutenant [redacted] and I look into the Morse intercept bay. I notice that some of the men have forgotten to turn off their R-390s before leaving. The Center had lost all power when the dump first went up, but if the radios aren't turned off now the returning power might burn them out later. [redacted] and I take a couple of minutes to walk down the four racks and make sure the 96 radios are all shut off. [redacted] had thought to tell the men to put their typewriters on the floor before leaving. Good idea.

[redacted] says he has heard that two Americans have been hurt down in the EC-47 aircraft area. Two American contract firms work there. Bendix maintains the Doppler navigation gear and Harris Corporation has the contract for the Airborne



Explosion as seen from Danang Airbase. The ammunition dump is about one mile away.

Radio Direction Finding (ARDF) system itself. I know most of the men well. At this time, only small stuff is still exploding. I'll see how close I can drive to the EC-47 hangar, which is about 150 feet from the closest bomb-storage revetment.

I get within 1000 feet or so and stop to see if I can spot anyone moving in the hangar area. A jeep comes up from behind me. Two of the Harris guys -- Burt and Paul. I've played some softball with them before and seen them in their work shed. Burt says that the Bendix chief, Jim Gaunt, got a few cuts when a fluorescent tube dropped on his head. Nothing serious though. No other injuries, but a Harris man is missing. He was due to report for work at just about the time the dump first went up. Possibly he was driving past the dump at the wrong moment and is still there. No one has been able to get close enough yet to look for him.

Burt says that when the explosions started -- maybe 100 yards from their shed -- everyone on duty hit the door and drove to the Air America terminal on the other side of the runway. Same for the guys in the Bendix shed. Harris had a bunker in their shed, made from 55-gallon drums filled with sand and roofed with railroad ties. It would have taken a direct hit to shake it. Bendix had an underground bunker that would have held 20 men. Funny, neither group thought to get in the bunkers when it started.

Both groups had left a lot of personal stuff in the huts and the doors wide open. Also, Harris had a lot of classified papers regarding ARDF gear. Burt and Paul want to try to get to their hut to get their stuff and the papers before the Vietnamese loot the place -- that would be sure to happen as soon as it was safe to get into the area. I tell them I'll go along and help them.

Two jeeps. Three of us. We drive a bit closer on this road but there is a lot of shrapnel ahead. We decide to go through the Air Vietnam terminal and then drive down the runway and into the hangar area. We pass a bunch of ARVN troops crouched under the side of a row of CONEX containers. They stare at us stupidly as we drive by. Who's stupid? It's like the Fourth of July on the other side of the hangar where we're headed.

I get to the huts, park, and look into the Bendix shed. It's a shambles. Burt and Paul head for their own shed, and I follow. Their place is a mess too. Gaping holes in the walls. Lights smashed on the floor. Chairs pushed against the walls in the rush to get out when it started.

Burt takes a 12-pound sledge and knocks four padlocks off desk drawers in a few seconds.

Explosion scene from about 3/4 of a mile away.

DOCID: 4009731

Paul and I gather briefcases and cardboard boxes and start filling them with secret papers and personal things. Cameras, passports, radios. The sound from the exploding part of the dump is getting more intense. We make two or three trips to the jeeps, loading stuff, keeping as low as possible. I notice something: the sound of ricocheting bullets sounds exactly as it does in the movies. Hell of a time for a thought like that. Paul crawls into their bunker and drags out flak jackets and steel pots for the three of us. Black smoke is rising from across the street.

An Air America helicopter destroyed by falling fragments.

Back in the hut. I grab two filled briefcases and head for the door. Burt and Paul behind me. They also have a load of stuff. I put out a hand to push open the door when a shock wave knocks me to the floor. My shoulder hits the side of a desk. I'm on my hands and knees. I look up. The door I was reaching for is gone, wrenched from the hinges. Pieces of insulation, wood splinters, and papers are flying all about me and outside in front of the doorway. The trash seems to be floating to the ground in slow motion. It's weird!

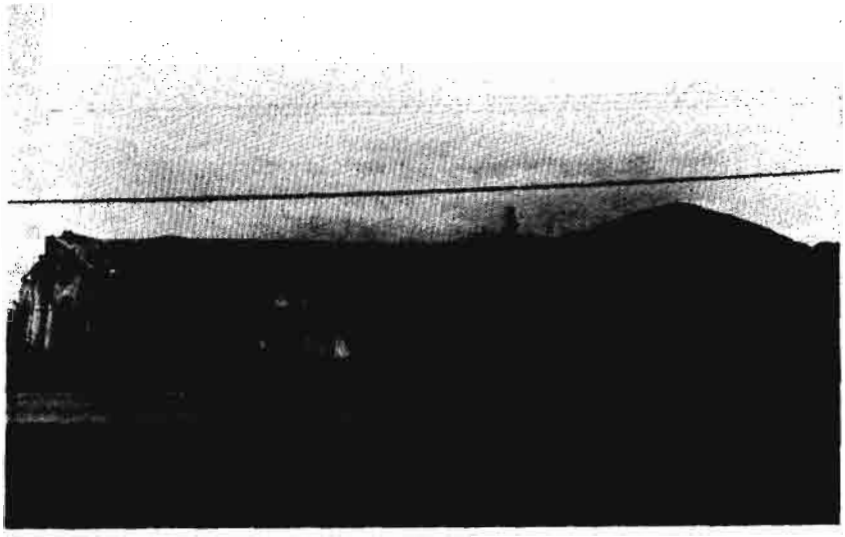
What had happened? A revetment of 750-pound bombs had gone up all at once. Why? Sympathetic detonation from a neighboring revetment? Heat from the burning bomb crates? A falling mortar shell? Or maybe a VC time-charge had set them off. No matter now. They're gone with a tremendous roar (we learn later that they blew windows out of the Consulate 15 miles away). Jagged pieces of bomb shell, colored purple from the heat of the detonations. I see them dropping all around and I can hear them tearing through the tin roof over my head. U.S. bombs -- the best in the world.

A man is like an eggshell, a paper bag, a balloon filled with water. A tiny piece of this steel can rip through him and let out the stuff that makes him alive. Is this what the VC go through out there in the jungle? In Hanoi they recruit him, give him some basic training, and tell him to walk south on the Ho Chi Minh Trail with a 122-mm rocket strapped to his back. If he's lucky, he'll only have to walk this far, to Military Region-I. If not, he'll walk all the way to the Delta. Maybe a thousand miles. They'll take that rocket from him and fire it. It misses. They tell him to go back and get another, and he does. Can we beat a man with that mentality? Lord help you, VC, out there in that jungle when arc light shines down on you.

The ARDF aircraft hangar adjacent to the Bendix and Harris Corporation huts. Concussion caused most of the damage.

What about Burt and Paul? They had been right behind me. I look back. Everything is black. Great gaping holes in the walls and ceilings, and sunlight streaming in,

DOCID: 4009731



The Sidewinder missile assembly shed across the street from the Harris hut.

but the dust is so thick that the light does nothing. I don't move. I should yell to them and ask if they are okay, but I can't: I'm afraid I'll get no answer. Silence.

Then one of them speaks. "Everything okay?" The other answers. Me too. They come out of the gloom and we rush to the jeeps, throwing the stuff in the back. Something is wrong with the front of my jeep. I look in the door. The windshield is gone, and so is half of the dashboard. There is a basket-sized hole in the canvas roof and pieces of concrete all over the inside. In my seat is a piece of concrete that must weigh 30 pounds.

Burt and Paul dump their loads and go back in the hut. The sounds from the dump are building again. Paul is at their safe, spinning the dial. I yell at him to leave it -- no one is going to get into it for a while. He agrees and goes on to something else. We make one last trip to the jeeps and then climb in. A huge black cloud of smoke is rising from the last revetment that went. We are so close that the cloud is directly over us. Not enough time to move the concrete block in my seat. I climb on top. My jeep is at the head of the alleyway. If it doesn't start, I'll be blocking in Burt and Paul. It starts. We drive back onto the runway with the gas pedals to the floorboards.

Back at Danang Center we unload the classified papers and put them in my safe. They fill one drawer. Then over to Air America, where we find the Harris man who had been missing. He had been a mile or so from the dump when it started to go, and had gone right over to Air America to watch the show.

Staff Sergeant Bill Sparks, chief of the Marine Security Guard force at the Consulate, looks over my jeep and tells me his story. He had been standing with a dozen or so people, awaiting the incoming flight from Saigon. The others were mostly Consulate civilians, USAID types, orphanage people, and some dependents. Bill saw the fireball of the first explosion and hit the deck. He had learned at Khe Sanh. He yelled for the others to get down, but they stood there and watched the explosion until the shock wave rolled across the half mile of runway and knocked them all flat.

As we're standing there, Jim MacNiel, the chief of the Harris people, arrives. He intends to send some men to the hangar area as soon as it's quiet, so they can protect the test equipment in the sheds. But something more substantial has to be done. We're already a month into the rainy season and it's only by luck that we didn't get a storm today. All the electronic equipment in those two sieves of huts will be ruined if we don't get it under cover. I tell him I'll try to locate a safe storage area.

I leave and drive downtown to the [redacted] logistics compound. When I arrive, I must look a mess. Pretty dirty at this point and my hair all windblown from the lack of a windshield in my jeep. I exchange my wreck for a new jeep and drive over to the housing compound, where I find Ron, the [redacted] logistics officer. I explain to him what has happened and ask if he can loan us some space in one of his warehouses so we can store the Harris and Bendix equipment until we can locate a new permanent shelter. He says no sweat. Then off to the Consulate, where I get chewed out for not having my radio with me when I went up to Monkey Mountain in the morning. Apparently the Consulate people thought I was at Danang Center when the dump went up, and were afraid I'd gotten zapped. They'd been trying to get me on the radio all morning. Then back to the airfield, where I look over the warehouse that Ron says we can use and where I beg the use of a flatbed truck from the Air America people. They also cooperate beautifully. Everyone pulls in a crisis. Then to home and a shower.

E.O. 1.4.(c)
P.L. 86-36

That evening I meet Burt and Paul and MacNiel and some of the others in the bar. MacNiel says that when he was finally able to get some men back to the sheds, they arrived to find some Vietnamese looting the place, but he doesn't think they got much.

We talk about what has already happened and what we'll have to do tomorrow. We have to beat

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

the rains, so we'll meet at the sheds at sunup and start moving the stuff to the warehouse with the flatbed and what pickup trucks MacNiel has. I'll also try to get the loan of a fork-lift so we can move the safes and other heavy items.

I see Ron, the [redacted] logistics man, on the other side of the bar. I go over and buy him a drink. He says they haven't determined why the dump went up. Rumors are rife, though. Some say a South Vietnamese fighter/bomber started it by dropping a bomb in the dump. Another story says mishandling of some ordnance inside the dump was the cause. And of course VC sabotage is mentioned. In any event, we can expect the VC radio broadcasts to take credit for it. The VC are too good at propaganda to pass up an opportunity like this. I buy Ron another drink and then ask if I can borrow his fork-lift for a while tomorrow. He hesitates but agrees. I don't like to push my friendship with Ron too far and, of course, officially he's not supposed to support me or Danang Center too much. But he's a good guy.

MacNiel says he can keep the ARDF systems working for about 2 weeks but by then he'll have to be set up in a new shop and have his maintenance equipment working or we'll be out of business. Keeping the ARDF birds flying is critical to the intelligence product for Vietnam, so I'm going to concentrate on helping these guys for a while. Captain [redacted] should be able to get Danang Center back on its feet by himself. Not too much to do there anyway, except clean up the broken glass and fallen ceiling tiles and put the doors back on.

EO 1.4.(d)
P.L. 86-36

Tomorrow is going to be another busy day. First to get the equipment under cover and then to start looking for a new permanent home for the stuff.

Burt and Paul and I buy each other a few drinks. Then to bed. It's been a long day and tomorrow is only a few hours away. Tomorrow is 30 November 1974.

~~(SECRET - HVCCO)~~

WILL THE REAL ELINT PLEASE STAND UP?

[redacted] E23

For one reason or another, a number of people in this Agency maintain a low profile. The lowest profile, it seems to me, is not kept by the people who skulk around behind the cipher locks and won't speak to you unless you are cleared for STEINMETZ. We often have an idea about what they are doing. We may not, or should not, know the sources of the material they work with or the degree of success they enjoy, but we know something about what they do.

P.L. 86-36

The only people who know anything about ELINT, however, seem to be other ELINTers. We COMINTers know that there *is* such a thing as ELINT. Thanks to an article by [redacted] we even got a tantalizing glimpse of what ELINT is all about -- or at least one phase of it. But information on the subject is hard to come by, and anything outside of some sketchy definitions is known only to a few people outside of the ELINT field itself.

[redacted]

Recently a group of veteran COMINT collectors[2] was discussing this subject. The usual experience was that, 20 years ago, they had been taught that SIGINT comprised:

- COMINT -- intelligence derived from any kind of emission by which information was transmitted; and
- ELINT -- intelligence derived from any other electromagnetic emission.

EO 1.4.(c)
P.L. 86-36

[redacted]

Some of the questions posed in the preceding paragraph are "semi-tongue-in-cheek." I have heard valid answers to all of them at one time or another. But the subject is one which is of interest to a vast number of NSA-ers and deserves attention by someone qualified to discuss it.

~~(CONFIDENTIAL)~~

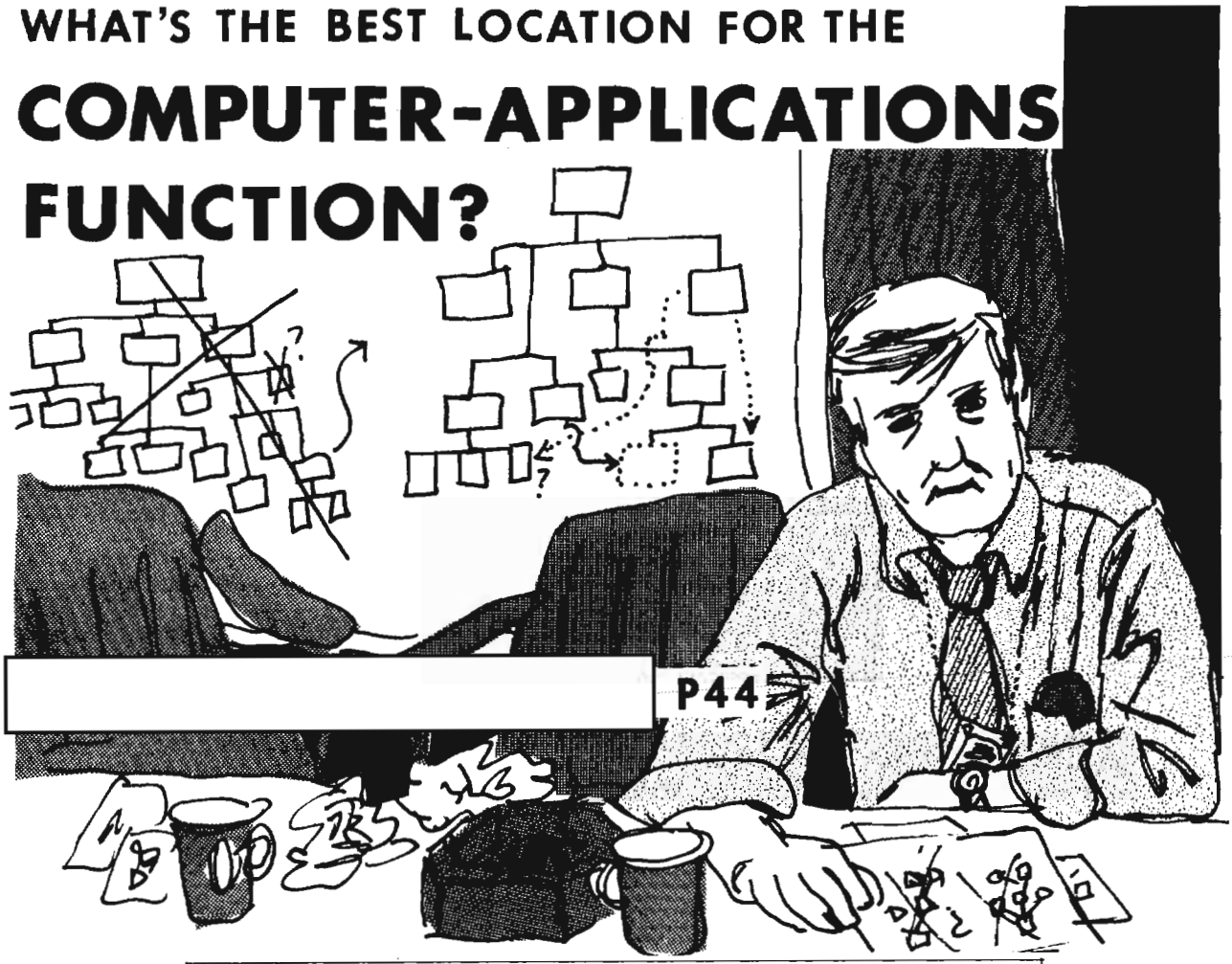
[redacted] "The Uses of ELINT," *CRYPTOLOG*, April 1975.

[2]See: [redacted] "What Is a Collector?", *CRYPTOLOG*, August 1974.

P.L. 86-36

DOCID: 4009731

WHAT'S THE BEST LOCATION FOR THE COMPUTER-APPLICATIONS FUNCTION?



[redacted] P44

P.L. 86-36

The following article was originally written as a paper for the American University graduate course "Systems Approach to Management." It is being printed here because the question with which it deals -- where to locate and manage the applications-programming function -- is one of continuing concern to the Agency.

Much has been written in recent years about management of the computer-processing function and where the computer-processing department belongs in the overall organization. Most articles on the subject address the entire range of computer-processing activities (systems analysis, programming, and computer operations) as being within a single EDP (electronic data-processing) organizational structure, and then they discuss the placement of that whole structure in the organization. This article will discuss as background some of the reasons for placement of the computer department in the organization but, more specifically, it will address the location of the applications-programming and systems-analysis functions in the overall organization.

"Historical" Location of the Computer Department

In *Computers in Business* Donald H. Sanders discusses three locations for the computer department in the organization. These locations are viewed as a function of "the size of the organization, the applications to be processed, the degree of systems integration achieved and sought, and the importance attached to information systems by top executives." They generally fall within the following functional areas:

- *finance* (This situation prevails in the majority of businesses. The primary reason for such location is that, historically, finance departments were the first to recognize and take advantage of the benefits offered by data processing);
- *research and development* (R&D); and

- *analysis* (The location of the computer department within the R&D or analytic functional areas is noted in organizations that are heavily R&D oriented and in certain government agencies that have scientific and analytic functions).

Among these three functional areas, the computer department was initially located in the area that originally sponsored the use of computers. Some drawbacks of this choice of location, according to Sanders, are "possible lack of objectivity in setting job priorities, possible limited viewpoint, and possible lack of organizational status."

An alternative is to create the computer department as a service center located on the periphery, outside the main organizational structure. The drawback of this location is that such a computer department is usually a weak and subservient component at the mercy of the functional component that is sponsoring it.

In medium-sized and larger concerns it is believed that the best location for the computer department is as a separate department in the organizational structure, with the same status as the other primary line elements such as marketing, finance, and production. Arguments that support this location are:

- the ability of the computer department to provide impartial service to all user components; and
- the ability of the computer manager to express an influential voice in systems development.

Another Approach

John Diebold takes another approach to the problem of computer-department location. He states that the higher the level of applications sophistication, the higher the level of management to which the EDP manager reports. Diebold has identified five levels of applications sophistication, as follows:

- Level 1 -- historical accounting (At this level, computers carry out only the functions usually related to payroll, sales accounting, or financial control);
- Level 2 -- the firm "has achieved means for supporting the main operating departments on a current, rather than a historical basis" (Carl Heyel, *John Diebold on Management*)
- Level 3 -- a significant amount of operating information is processed by computer and some management reports for some of the major departments are created;
- Level 4 -- a general data base is available and a significant amount of reporting is done by computer not only to the department management, but also to the Executive Vice-Presidential level;
- Level 5 -- "the basic transaction-activity information within all major functional areas of the firm is being captured and introduced into a data base." The data base then serves the needs of all departments without duplicating or overlapping files.

One can readily see that at Level 1 the computer department needs only to report to a line manager somewhere down in the organizational structure. But at the Level 5 stage of development, the computer manager must report to the highest level of corporate or agency management.

Further Background

Now that we have considered two approaches to the location of the computer department within the organization, we should briefly discuss as further background the general functions necessary to support a large-scale computer-processing effort. For the purpose of this article we are assuming an ongoing bulk-processing system which is used by a number of organizations to analyze, validate, and interpret large amounts of data. One function necessary to support the computer is *computer operations* -- the people who actually run the computer and who control the input and output, maintain the various libraries, and set up the job schedules. This function sometimes includes maintenance, but with a large-scale computer, maintenance is usually handled by the manufacturer.

Another major function required to support the processing efforts is the *systems-analysis and programming function*. In the systems-analysis area this function includes:

- the development of new applications, and
- the translation of user data-processing requests into program specifications.

The programming function includes:

- the preparation of programs to support new applications, and
- the maintenance of existing programs.

Using another approach we can talk of this function in terms of *applications programming* and *systems programming*. One definition of applications programmers is that they are "very often individuals who have been trained or hired by a specific company and are usually highly knowledgeable of the problems for which they are programming. Systems programmers write the programs that run the computer equipment and generally are employed by the computer manufacturer" (Orville Elliott and Robert S. Wasley, *Business Information Processing Systems*). We would define applications programming as that programming which supports user requirements. Systems programming includes such functions as development of generalized software routines which can be used by other programmers, and maintenance of the various libraries.

DOCID: 4009731

Where Should the Applications-Programming and Systems-Analysis Function Be Located?

We shall now discuss the applications-programming and systems-analysis function and the advantages and disadvantages of locating that function in different parts of the organization. First, we will look at the function as part of a central computer component along with the systems-programming and operations function. Second, we will look at the function as separate from the central computer component (in this situation the applications function will be a part of the user component for management purposes). Finally, we will consider the applications function as part of a project-management office separate from the central computer component and the user component.

Centralized Function

The advantages of having the applications-programming and systems function as part of the central computer component are several. First, it is easier for the programmers and systems analysts to keep up with new systems developments because they are in the same component. The information flow is probably better within a given component than between components, so that data related to systems changes would be available more quickly. Another advantage stems from the sharing of programming techniques among programmers who are working on various applications for different parts of the organization, but who are located in the same programming component.

From the management standpoint, there are a number of additional benefits from this type of working. The programming function is easier to control. Standards can be applied to programming across the board and, with the programmers in one component, management has a better chance of enforcing these standards. This could result in more consistency in the software. Also, by sharing software-development ideas, cost savings in software development would result if subroutines were developed once and used by several programmers. Finally, if the overall organization is at Diebold's sophistication Level 5, the applications component would exert some influence in determining the type of applications to be developed and could ensure a consistent approach to problems of systems development, independent of the parochial interests of the various components.

There are several disadvantages to the centralized computer-applications function. One primary disadvantage is poor communications with user components, a situation which cannot be taken lightly. At a recent conference of 20 EDP executives from corporations that had annual revenues or a total budget of more than $1 billion, their primary long-range planning objective was "to increase communications and cooperation between the EDP group, its users, and top management" (John V. Soden, "Programmatic Guidelines for EDP Long-Range Planning," *Data Management*, September 1975). Another disadvantage of this concept is that the user never seems to get what he has requested. When results are provided to the user, a typical reaction is, "That's not what I really wanted." A third disadvantage of this organizational setup is the user's lack of trust in what is being done with his data.

Decentralized Function

An alternative to the central computer-applications function is to locate the applications programmers/analysts in the user components as something like "open shop" programmers. The obvious advantage of this setup is that a close relationship can develop between the programmers and the users. As a result, the user probably has a better chance of getting what he wants from the computer-processing system. In a small computer complex, this situation might be very beneficial, but in a large organization it would probably be very costly.

The disadvantages inherent in this type of organization are several. First, there is a tendency for each user component to have its own programmers develop specific applications tailored to its individual needs. Also, standardization is difficult to enforce, particularly if the user components are autonomous and have a great deal of flexibility in developing computer applications. Efficiency in terms of the actual software performance may also be sacrificed.

Project Management

A final possibility for the applications group is to make it part of a project-management office separate both from the central computer component and from the user component. The advantage of this type of organization is that it is easy to develop systems with overall organizational goals in mind and without the parochialism of individual user components. The primary disadvantage is that the programmers are still separate from the benefits of the central computer component.

Obviously, there are no absolute solutions to this dilemma. One must evaluate a number of questions before deciding what is best for a given organization. Factors such as the size of the overall organization, the complexity of the applications, the size of the EDP component, the autonomy of the line elements in the organization, and management experience will dictate what is best in a given situation. Management should exercise extreme care in obtaining the proper balance to obtain the best EDP production for the best price.

I'LL MEET YOU DOWN AT THE CORNER...

...OF PAGE 17

DOCID: 4009731

P.L. 86-36

ON BEING TRUTHFUL

DAVID W. GADDY, D5

It was amusing to read Vera Filby's account of the bafflement felt by the roomful of SIGINT people confronted with the question which she adopted as her title, "How Do We Know It's True?" (CRYPTOLOG, February 1976). Amusing, because it sketched a cartoon illustrative of the charge sometimes leveled at us: we're accused of being the product of too much inbreeding, of too much isolation from the real world in which our recipients live. "After all," she characterizes the reaction, "to us in the business there is no such question: if it's SIGINT, then it *is* true, by definition." I recently heard the same thought expressed this way: "SIGINT doesn't lie." (That, of course, might prompt a facetious rejoinder, "Well, SIGINT might not, but I just don't know about some SIGINTers. . .")

This conception, this idea of being on the side of the angels, appeals to what seems to be ingrained in the American character -- the desire to be the good guy, the guy in the white hat. In this particular case it has about it an unseemly air of intellectual arrogance, which I think is neither warranted nor intended, as further reflection will show.

Consider COMINT: COMINT is comprised of crypt intelligence (CA results, decrypts) and traffic intelligence (TA results).

[redacted]

So, if we see it in print, resulting from decryption, "it must be true," right? Consider TA: At the risk of offending some colleagues again, let me observe that much, if not the bulk, of traffic analysis is in the realm of what [redacted] once termed a behavioral science, a somewhat less precise field than mathematics -- the study of human beings, signal officers and radio operators, each with his predilections involving his profession, security, and circumstances.

[redacted]

I think, on the contrary, that "SIGINT equals truth" is a grossly oversimplified, shorthand way of conveying something I do believe in and believe merits just the sort of consumer education Vera espouses. That "something" is the professional, intellectual attitude which motivates "the real SIGINTer." I know of no comparable body of craftsmen so sensitive to the uncertainties of their profession, so painstaking with accuracy, as SIGINT reporters, and who work under the stress and strain of events and time constraints which characterize the SIGINT reporter's world.

EO 1.4.(c)
P.L. 86-36

[redacted]

DOCID: 4009731

EO 1.4.(c)
P.L. 86-36

[redacted]

[redacted]

The challenge is to effect a fiduciary relationship with our recipients and to maintain it. That entails education, indoctrination, and training on both sides, but above all it requires honesty. It means that we cannot simply insist that "it's true because I said so, and I speak SIGINT." We must openly deal with the weaknesses as well as the strengths of our chosen specialty, not let pride and enthusiasm blind us. We must face up to the possibility of deception and deal with it honestly and professionally, as Vera proposes, not dismiss it by claiming we're too smart to be fooled. We must figure out ways of protecting our sources and methods while retaining consumer confidence in our conclusions.

Sanitization -- protection of our sources and methods -- thus becomes an added burden for the SIGINT reporter.

[redacted]

Finally, as members of the intelligence profession, we must accept the fact that, in spite of all we do, there will be times when we simply *will not be believed.* Rejection of intelligence (as one of our pundits once said about communications *in*security) is a commander's prerogative.

~~(SECRET HVCCO)~~

The Voynich Manuscript Revisited

[redacted]

P.L. 86-36

The Voynich Manuscript, an object of interest off and on since the seventeenth century, contains over 200 pages written in a partially cursive alphabet which has proved indecipherable. Equally enigmatic are the large number of drawings -- of plants, few of which are identifiable, and of naked women sitting in tubs or emerging from pipes (one writer has called the latter a "plumber's nightmare").

The history of the manuscript, which has been detailed in other places, needs only passing mention since it does not throw any light on the content. Dating from about 1500, it was said by Joannes Marci, mathematician and orientalist at the University of Prague, to have belonged at one time to Emperor Rudolf II (1576-1612). Marci writes in 1666 to the Jesuit Athanasius Kircher, in Rome, that he was making a present to the latter of the manuscript, the author of which, he had heard from another source, was the great medieval scholar Roger Bacon. (How Marci came into possession of it, I do not know.)

Marci himself withheld judgment on the attribution, but at least one scholar since his time became intrigued with the notion of Baconian authorship. Professor William Newbold of the University of Pennsylvania was convinced that it was an enciphered text prepared by Bacon and he worked on this assumption from 1919 until his death in 1926. He thought he had deciphered some of it, including an occurrence of "R. Baconi" on the last page[1]. His "solution" has been convincingly refuted by other scholars, who however have not offered anything better.

I now rush in where angels fear to tread. Although not a specialist in Old Norse, I am convinced that the manuscript is a text in fifteenth century Danish or Norwegian -- not a cipher, and not an artificial language, as has also been suggested. For reasons too complex to go into here, I have tentatively ruled out Old East Norse (that is, Old Swedish) and rejected altogether the second branch of Old West Norse, Old Icelandic. The reasoning which suggested Dano-Norwegian is given below.

Most of the manuscript has a depressing number of repeated words and phrases, of little help unless collateral information is available, suggesting that these are prayers, incantations, or formulas of a specific character. This is

[1] The information in this paragraph and the preceding paragraph was taken from *Horizon,* January 1963 (Vol. V, No. 3).

(UNCLASSIFIED)

DOCID: 4009731

not the case, and the botanical drawings and naked figures are not helpful either. I therefore chose a mostly unadorned text without too many repeats (Folio 114 recto).

I then attempted to find "function" words, that is, connecting words such as conjunctions, personal pronouns, and prepositions, assuming (correctly, as it turned out) that the language would have these. The first item that caught my eye was ᛟᚴ, the second letter of which was a mystery. However, I thought the word might be "and" because of its frequent position between longer words which often had the same endings. Remembering *og*, "and," from Danish, I sought out phrases of the type "of mice and men" (Scandinavian literature, like that of Anglo-Saxon, contains many rhyming or alliterative phrases of this type). I was lucky: a phrase in the script form

ᚮᚮᚱ . . . ᛟᚴ . . .

occurred. The first is a general Scandinavian word for "from," "out of." This was promising, because not only did the first word appear to be in a known alphabet with the desired meaning, but the second letter of the second word was a tentative recovery ("g"). The same procedure has been of aid in establishing proper names, especially those occurring in pairs:

ᚦᚮᚱ ᛟᚴ ᚦᚢᚱᚦᚨᛁᚾ *Thor og Thruther*
"Thor and [his daughter] Thruther."

(This was an exciting find because, in my ignorance of Norse mythology, I had never heard of Thruther. An encyclopedia came to the rescue.)

Once a few phrases of this kind fall into place, the logical next step is to look for verb forms, and hope that verb affixes and bases of the desired type appear. Again, I was fortunate in finding past-tense suffixes and a few high-frequency verbs common in Danish and Norwegian:

-ᛁᛒᛅ, -ᛟᛒᛅ

looked like regular past-tense forms *-ida*, *-oda*, and the verbs *ríða*, "ride," and *gof*, "gave" seem solid.

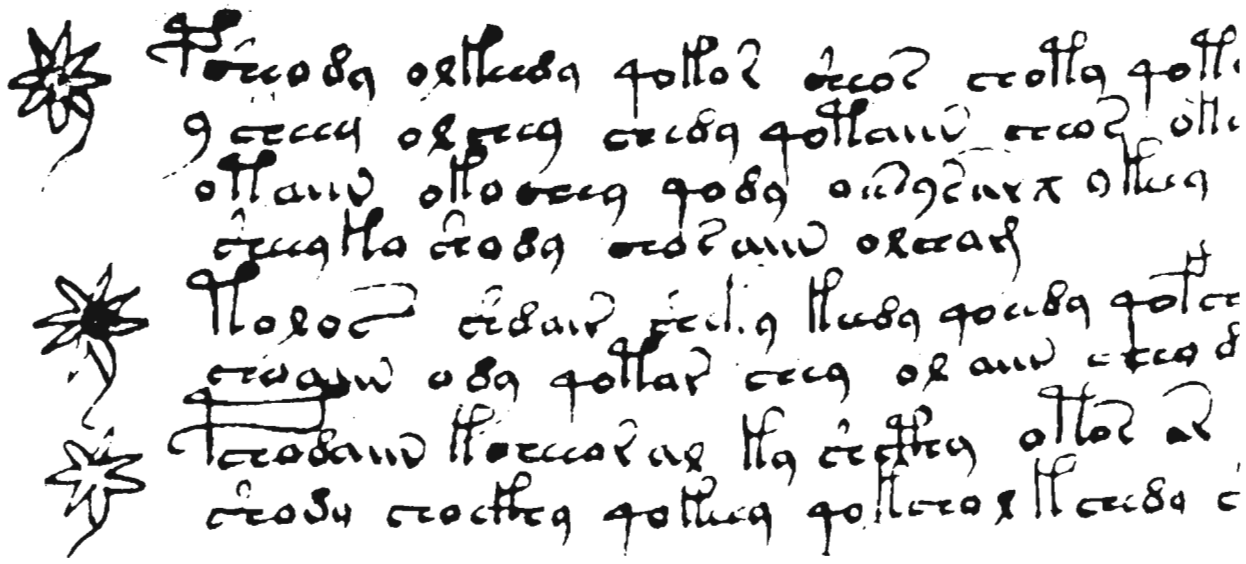
From the above it will be clear that this is only a beginning. Spelling "variants" in the manuscript sometimes turn out to be different words and in any case cause difficulties (variant spellings of the same word are common, however, in manuscripts of most Germanic languages, and are not in themselves unexpected). The "letters" themselves are not all recovered, due in no small part to the use of digraphs, especially when short words like "and" and "of" are written as one with following words:

ᛟᚠᛏᛟᚴ *o(g)thog*, "although".

In other cases, vowel letters appear to be used to indicate that other contiguous vowel letters are "umlauted" (cf. English "man," singular; "men," plural).

The major difficulty, though, is the syntax. Human language is produced and understood in fairly long strings, but linguistic analysis has up to very recently concentrated on forms (i.e. morphology) and the reference texts I am using are no exception. This, together with that the fact that I have only had recourse to texts which concentrate on an older stage and another dialect of West Norse (Old Icelandic) has slowed progress. I am pretty sure, however, of the correctness of my basic diagnosis and will, I hope, be able to publish something more than this skimpy initial report.

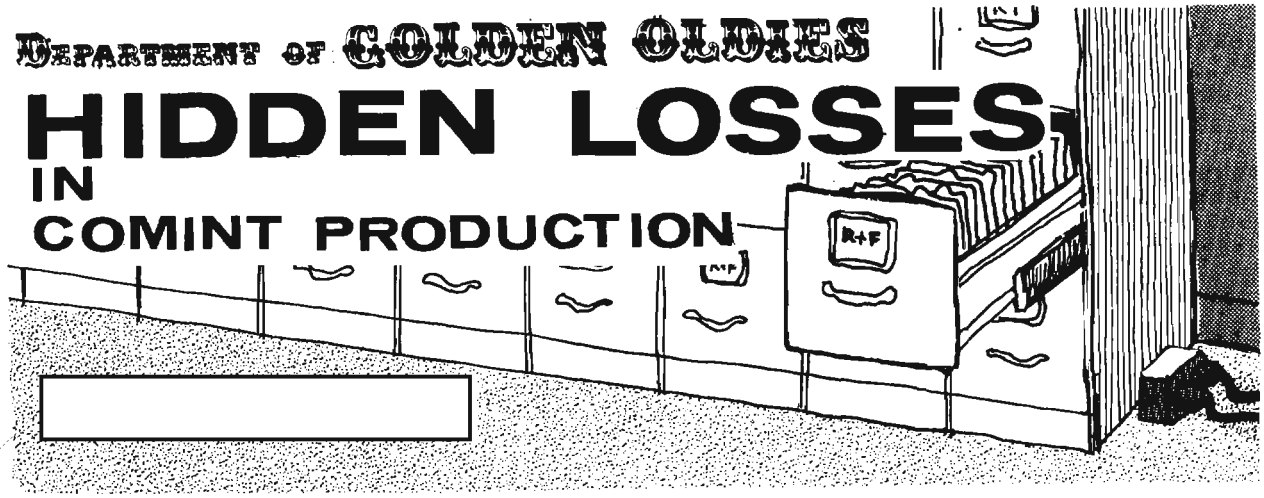
(UNCLASSIFIED)
Received in editorial office 16 Feb 1976



DOCID: 4009731

DEPARTMENT OF GOLDEN OLDIES

HIDDEN LOSSES IN COMINT PRODUCTION

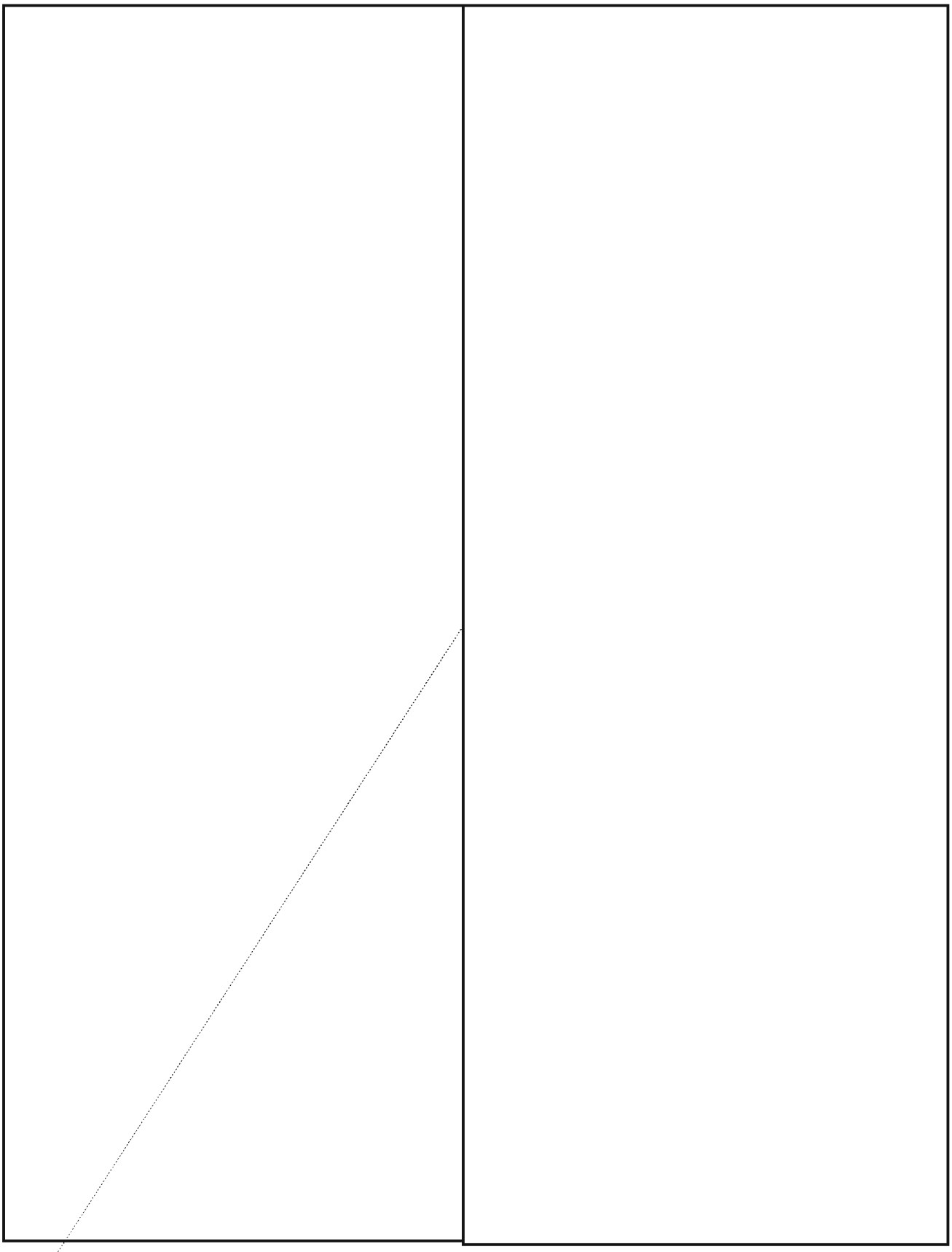


P.L. 86-36

Most of the Golden Oldies published in CRYPTOLOG so far have been light in tone, but the Editor feels that this department should also reprint certain serious works that continue to remain "golden" and that readers may have missed when they were first published. One such work is the following article by retired NSA-er [redacted] *which was originally published in KEYWORD, June 1971.*

[redacted]

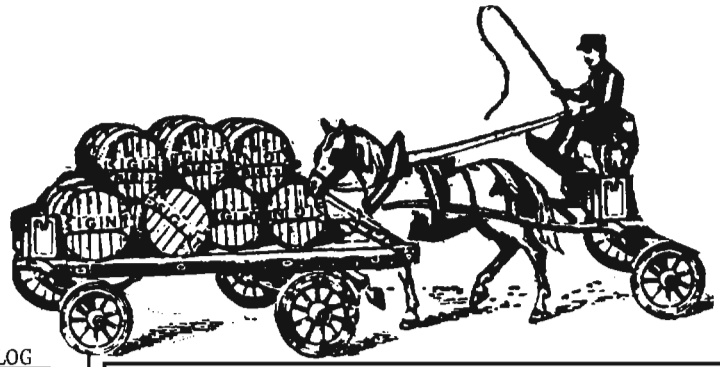
P.L. 86-36
EO 1.4.(c)



P.L. 86-36
EO 1.4.(c)

P.L. 86-36

LETTERS TO THE EDITOR



To the Editor, CRYPTOLOG:

After reading the December 1975 CRYPTOLOG article "What Are We About?", by [redacted] I am compelled to comment.

Overall, the article was good food for thought. But one sentence in one paragraph prompted the following "tirade."

[redacted] stated, "It follows that, if the processing and reporting effort ever catches up with the collection effort, we would be in real trouble because we would certainly have the cart before the horse."

I have shown the article to several people who were puzzled by that statement. Personally, I disagree with his philosophy although I sometimes think that the NSA/CSS and the Intelligence Community do not disagree. The philosophy that I would prefer to operate under is to *attempt* to keep pace with the collector in processing and analysis. Reporting of intelligence in a *selective* manner should follow, thus *not* inundating the user with reports he doesn't want or need.

[redacted]

P.L. 86-36
EO 1.4.(c)

[redacted]

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

To the Editor, CRYPTOLOG:

Thank you for the opportunity to comment on [redacted] comment on my short item which appeared in the December 1975 issue.

[redacted]

In conclusion, I appreciate the "old #2" problem. It is worrisome, but it steps beyond inventory and volume considerations into the realm of prioritization, and that approaches one of the theses of my article, i. e. inundation. From the maverick point of view, it seems to me that the "old #2" might well have been elevated to #1, if only temporarily, inasmuch as there is no substitute for the on-scene "judgment calls" of the person who happens to be attending the signal -- admittedly another generalization.

[redacted] D/Chief, A732
("a processing and reporting shop")

Remember the old motto, ". . . the impossible will take a little time."

[redacted]

[redacted] *was asked whether he would care to comment on* [redacted] *letter to the editor. He replied as follows.*

P.L. 86-36

~~SECRET~~

LANGUAGE IN THE NEWS

Language Rule Snags Fairfax

Wash. Post, 8 Dec 75 Tegan Rosenfeld
Washington Post Staff Writer

The Fairfax County school system may be in violation of federal civil rights guidelines for identifying children who do not speak English.

County schools may be required to spend $60,000 to achieve compliance and hire 30 new employees to interview children and their parents and administer language tests.

[illegible] members were need[illegible]

"We have about 26 languages represented in our school system," board chairman Mary Anne Lecos said in an interview. "We don't see how we can institute bilingual education without turning the entire school system upside down. And we don't see the point of following guidelines designed for bilingual education if we don't have it."

[illegible] are a[illegible]

provided by th[illegible]

Currently, 2,754 of the county's 137,000 students speak foreign languages as their native tongue, with varying degrees of proficiency in English. The county provides a federally funded program to tutor those who need help in English.

The county has large groups of children who speak Spanish (764), Vietnamese (516) and Korean (497), as well as those who speak Arabic, Czech, Turkish, Hungarian and other languages. Some children speak several languages fluently.

Mrs. Lecos said the board asked its attorney to look into the legal aspects of the guidelines and the eventual possibility of filing a lawsuit to prevent the county from losing federal funds for failing to have bilingual education.

Moynihan, Soviet Trade Tough Talk

Wash. Post, 8 Feb 76

UNITED NATIONS, Feb. 8 (UPI) — Daniel Patrick Moynihan glared across the Security Council table at Soviet Ambassador Yakov Malik. He leaned forward in his chair and in measured tones told the Soviet:

"We are not intimidated. We are not afraid. We will not 'take care'.

"We do not give a damn!"

But it all turned out to be a misunderstanding, caused by a faulty translation of Maliks's words.

"I never said 'take care'," Malik said. "I said 'take heed, gentlemen, you are the laughing stock of Africa.'"

Moynihan said his transcript bore the words, 'take care', but: "I ask forgiveness for what was a wholly unintended mistake."

The politeness that mark[illegible] the end of Friday's Secur[illegible] Council session was abs[illegible] from most of the verbal [illegible] between the [illegible] and

Malik Says He Was Wrongly Translated In Moynihan Clash

NYT, 8 Feb 76

[illegible]NATIONS, N.Y., Feb. 7 (UPI)—An apparent Soviet warning to the United States to "take care" touched off a strong outburst in the United Nations last night from the United States representative, Daniel P. Moynihan, but the Soviet representative said later that he really meant "take heed." Mr. Moynihan then asked for "forgiveness."

Mr. Moynihan had assailed the Soviet delegate, Yakov A. Malik, saying that Americans did not "give a damn" about threats from Moscow.

But Mr. Malik later said that his remarks had been mistranslated by the United Nations interpreter.

"I never said 'take care'," he said. "I said, 'Take heed, gentlemen, you are the laughing stock of Africa.' I would like to assert that my Russian word cannot be translated 'beware' or 'take care.' It means 'take heed.' A source with access to the text said Mr. Malik had used the word "opomnites," which can be translated roughly as "come to your senses."

Mr. Moynihan said he had obtained a transcript in which the English translation had Mr. Malik saying "take care [illegible]

"I ask forgiveness [illegible]

(UNCLASSIFIED)

. . . OR AT ANY OTHER CORNER YOU WANT!

... at the corner of your desk (if it's private enough), the corner of the cafeteria, the corner of the parking lot, you name it. . .

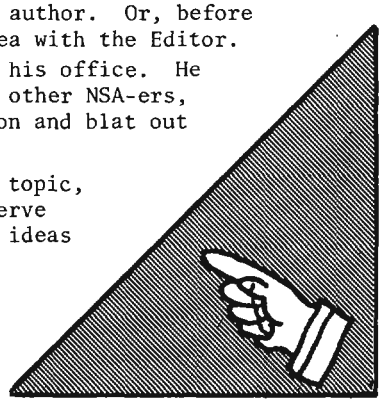
PURPOSE: To discuss that hard-hitting article you've been wanting to write for CRYPTOLOG, but which you'd like to have published anonymously.

At various times, people have mentioned to members of the Editorial Board that certain articles "should be written," and those persons wouldn't mind writing the articles themselves, except for various personal reasons -- official position, friendship with NSA coworkers, etc.

According to our publication charter, CRYPTOLOG can print anonymous articles, so long as the Editor knows the identity of the author. If you wish, you may submit the article, unsigned, through the Agency mail, and then, by telephone or other appropriate "Pssst!", identify yourself to the Editor as its author. Or, before actually writing the article, you may wish to discuss the idea with the Editor. In either instance, do not actually drop in on the Editor in his office. He doesn't really *have* an office, but shares space with several other NSA-ers, any one of whom would be more than willing to TA the situation and blat out anything they suspect.

So if you have an article a-brewing about a controversial topic, get in touch with me discreetly. I'll do everything to preserve your anonymity while offering to the NSA reading public your ideas on things that "have to be said."

CRYPTOLOG Editor
P16, Room 3C099-1, 5642s



(UNCLASSIFIED)

DOCID: 4009731

NSA-CROSTIC NO. 3

BY A.J.S.

The quotation on the next page was taken from a published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS

A. Russian poet (1814-1841)

B. Athenian tragic poet (525-456 B.C.)

C. Groucho's straightperson (2 wds)

D. Yeomen of the Guard

E. Gentle reminder given by Ivan to his wife (she had been arguing with Rudol'f Rudol'fovich, party functionary, about whether it was snow, slush, or whatever) (6 wds; based on song title)

F. Nazi concentration camp in Poland (Germ. sp. Auschwitz)

G. Confiscate

H. Name of W. C. Fields' "son" on radio (until the sponsor -- Lucky Strike -- got wise)

I. Forever

J. Italian mathematician (c. 1170-1230) (1, 2, 3, 5, 8, 13, 21. . .) (2 wds)

K. Poison gas

L. Island taken by U.S. Marines (Feb-Mar 1945)

M. Unit of beauty sufficient to launch one Greek ship

N. Marked by stateliness or magnificence

O. Patron of exploration (1394-1460) (3 wds)

P. Word used to express discomfort, aversion, or impatience

Q. Gay (obs)

R. Defendants

S. Patronymic prefix in Irish names

WORDS

102 25 213 73 56 200 65 137 31

20 45 88 130 34 195 37 12 201

85 7 91 93 116 57 79 40 121 67 181 119 132

100

44 3 32 171 87 14 167 113 143 218

183 156 135 82 211 66 141 205 115 68 202 26 97

125 144 52 109 165 152 1 58 149 92 186 191

155 193 107 22 206 11 59 209

168 127 18 41 146 188 69 182 8

46 178 203 129 27 192 117

53 114 217

21 169 74 148 212 94 133 101 2 210 55 194 60

180 198 185 216

16 61 122 51 207 86 9 140

208 89 172

104 164 13 120 35 70 96 83 179 161

47 197 29 19 54 215

142 4 176 15 105 33 126 38 187 128 112 162 62

199 136 28 75

196 48 154

98 158 150 118 123

42 71 184

190

DOCID: 4009731

T. Fault — 49 189 214 23 138

U. Word seldom heard in political speeches since Spiro's departure — 95 163 110 76 170 84

V. Dialect of Akan — 77 151 10

W. An article not needed by "the *hoi polloi*" — 204 159 50

X. Play by O'Neill (*The Hairy ---*) — 108 64 43

Y. Members of one of the great divisions of Islam — 153 78 111 24 174 103 36

Z. Kind — 177 17 6 124

Z_1. Show the minimal reaction (1970's usage) — 173 106 131 72 157 90 147 39 81

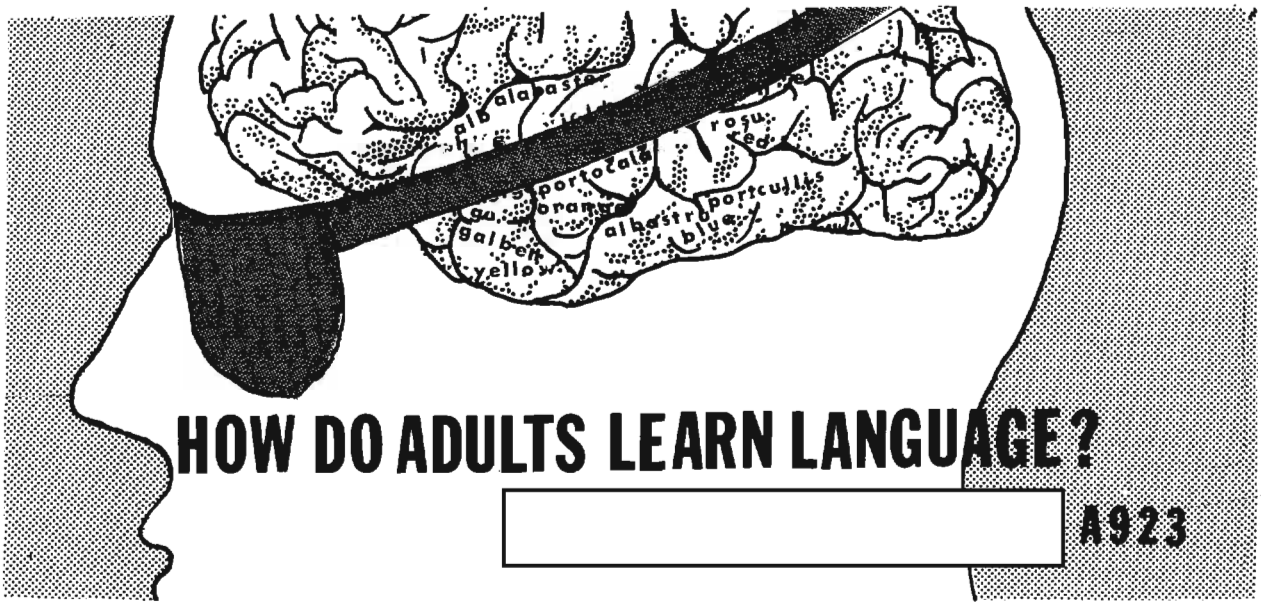
Z_2. Japanese lyric drama — 145 175 139

Z_3. Falling sickness — 160 80 30 5 134 99 166 63

1-E		2-J	3-D	4-O	5-Z_3		6-Z	7-C	8-G	9-K	10-V	11-F	12-B	13-M	14-D
15-O	16-K	17-Z		18-G	19-N	20-B	21-J	22-F	23-T	24-Y	25-A	26-E		27-H	28-O
	29-N	30-Z_3	31-A	32-D		33-O	34-B	35-M	36-Y		37-B	38-O	39-Z_1	40-C	41-G
42-R	43-X		44-D	45-B	46-H	47-N	48-P	49-T	50-W		51-K		52-E	53-I	54-N
	55-J	56-A	57-C	58-E		59-F	60-J		61-K	62-O	63-Z_3	64-X	65-A		66-E
67-C	68-E	69-G	70-M	71-R	72-Z_1	73-A	74-J	75-O	76 U		77-V	78-Y	79-C		80-Z_3
81-Z_1	82-E	83-M	84-U	85-C	86-K	87-D	88-B		89-L	90-Z_1	91-C	92-E		93-C	94-J
95-U	96-M	97-E	98-Q		99-Z_3	100-C	101-J	102-A	103-Y	104-M	105-O		106-Z_1		107-F
108-X	109-E		110-U	111-Y	112-O	113-D		114-I	115-E	116-C	117-H	118-Q		119-C	120-M
121-C		122-K	123-Q	124-Z	125-E		126-O	127-G		128-O	129-H	130-B	131-Z_1	132-C	133-J
134-Z_3	135-E		136-O	137-A		138-T	139-Z_2	140-K		141-E	142-O	143-D	144-E	145-Z_2	146-G
	147-Z_1	148-J	149-E		150-Q		151-V	152-E	153-Y		154-P	155-F	156-E	157-Z_1	
158-Q	159-W	160-Z_3	161-M		162-O		163-U	164-M	165-E	166-Z_3	167-D		168-G	169-J	170-U
	171-D	172-L	173-Z_1	174-Y		175-Z_2	176-O		177-Z	178-H	179-M		180-J	181-C	182-G
183-E	184-R	185-J	186-E	187-O		188-G	189-T	190-S	191-E	192-H		193-F	194-J		195-B
196-P	197-N		198-J	199-O	200-A		201-B	202-E	203-H		204-W	205-E	206-F		207-K
208-L	209-F	210-J	211-E	212-J	213-A	214-T	215-N	216-J	217-I	218-D					A.J.S.

(Solution will appear next month.)

DOCID: 4009731



P.L. 86-36

Why do adults have such a hard time learning a foreign language when it's so easy for a 5-year-old child to learn his own language, or even two languages at the same time? Why do older children -- such as those in junior high school, where most Americans make their first attempt to learn a foreign language -- also have difficulty in assimilating a second language? The author of the following article finds the answers to these questions in an understanding of the physiological development and functioning of the human brain.

Many psycholinguists agree that learning a second language after the age of 12 or 13 years is extremely difficult for most people. Since it is generally accepted, and rather obvious, that children easily master any one of the 5,000 languages of the world, psycholinguists have assumed that there must be certain characteristics of language which, coupled with some type of physiological brain function, enable children to develop a language capability, if not spontaneously then certainly with great speed and ease. If we assume that, in these 5,000 languages, there is a common base structure that remains basically constant, we may further assume that it is the psychophysiological functions of the human brain proper that present problems when learning a second language as an adult.

Several theories and explanations have been advanced concerning second-language learning. Many of them have overlapping features and hypotheses. But the consensus is that small children learn language by using both hemispheres of the brain and that, after the onset of puberty, the language and speech functions are transferred to the left hemisphere only. This is suggested because damage to the right hemisphere in an adult rarely results in language or speech disorders.

It would appear then that the learning of a second language after the age of 13 years would pose serious problems not encountered when learning one's maternal language. The problems would include:

- the lack of dual hemispheric capability;
- the tendency to interpret the second learned language through the structure, sounds, and patterns of the primary language; and
- the phenomenon of bilingual interference (confusing elements and patterns of one language with similar but not directly transferrable elements of another language in a seemingly spontaneous manner).

But, one may ask, to what degree would these problems affect second-language proficiency? Does hemispheric dominance indeed play a major role in second-language acquisition? Which hemisphere of the brain "controls" language acquisition and competency in the adult?

If current psycholinguistic theories are correct, it is only an extremely rare individual who can attain native or near-native proficiency in an acquired second language. (There most certainly are truly bilingual persons throughout the world, but virtually all learned both languages as children or, as adults, have displayed exceptional aptitude for language acquisition.) This article describes an attempt to explore experimentally on a very limited scale the questions of second-language proficiency in order to draw some conclusions concerning the inferred concept of "an extremely rare individual" and dual language competency.

Romanian, a language spoken by a relatively small number of persons in the United States, was selected as the test language in order to reduce the likelihood that the test subjects had heard or acquired the language prior to the age of 13 years. A random group of nine persons participated in the testing. All had begun studying Romanian as a second language after age 18. The average length of time they had studied the language prior to the testing was 4 years 8 months. All the persons tested had received basically the same language training, at the same school, under similar conditions. The test group consisted of both males and females, and both right-handed and left-handed persons. It was unbelievably fortunate to find two left-handed Romanian linguists, and even more improbable to select them from a group of 25 possible subjects. Truly left-handed persons tend to have a dominant right hemisphere for language and speech functions, whereas right-handed persons are generally left-hemisphere dominant.

The two devices used in the testing were modified from previously carried out experiments to evaluate specific language tasks and functions and to identify the roles and properties of the brain hemispheres in each instance. Visual stimuli were used in the testing.

The first test was an adaptation of the Stroop (1963) color reading-identification experiment. A number of white cards were prepared, each bearing the Romanian name of a color. Different colors of ink were used, so that no word was written in the color denoted by the word, e. g. the Romanian word for "blue," *albastru*, was written in green ink; the word for "red," *roşu*, was written in blue ink; etc. The subject was told to look at the word on the card and translate it into English orally as quickly as possible. The group was then tested for their speed in recognizing each Romanian word and their accuracy in translating it into English. As a control, a similar number of white cards were prepared using the same Romanian words written only in black ink (the normal black-on-white medium). The cards were flashed at a rapid and constant rate.

The results showed that considerably more time was needed to "read" the color and accurately translate from the multicolored cards than from the black-on-white cards. The average time for eight responses was 9.7 seconds, with a 92 percent accuracy rating for the colored cards.

The control cards presented an easier task. Accuracy jumped to 100 percent and the recognition time was reduced to 5 seconds.

After the test, each person was interviewed regarding his or her feelings and thoughts while taking the test. Six of the nine readily admitted confusing the word meaning with the color in which it was written. All said they first saw the word, visualized the color it denoted, associated it with the English word, and then produced the English word. One person gave the color of the ink in Romanian, paused a split second, and then translated the ink color into English -- a correct translation but an incorrect response.

In this case there was clear evidence of simple bilingual interference and, in the color test overall, it was at least partially demonstrated that, although the subjects could be accurate in their responses if given sufficient time, they lacked the spontaneity of a native, fluent speaker. It also very probably shows how those people tested were "bound" to interpret color through the experiences and prior perceptions in their maternal language (and perhaps culture).

In attempting to isolate one brain hemisphere, it was necessary to devise an experiment that could block one side of the brain while allowing input to the other side. Audio inputs are transferred to both sides of the brain. Visual inputs, however, can be isolated.

Visual stimuli are transmitted via the optic nerves, crossed to opposite hemispheres, and sent to the right and left visual cortex. Perhaps this can be more clearly explained by describing the action of one eye only.

The right eye has its field of vision divided into three basic elements: right field of vision, point of fixation, and left field of vision. Objects perceived in the right-eye *right* field of vision are eventually received in the *left* visual cortex (left hemisphere), and objects perceived in the right-eye *left* field of vision are received in the *right* visual cortex.

If one wants to isolate a particular visual image in one specific hemisphere of the brain, this can be done by placing the image in one field of vision only and blocking or covering the other eye. Thus, if one wants to "feed" a visual image to the dominant side side of the brain for right-handed persons, the image should be placed in the right-eye right field of vision, with the left eye closed.

In the normal right-handed person, the left hemisphere contains the speech, language, and visual association and interpretation areas. If, indeed, second language learned after puberty is colocated with the original maternal language, then testing of the weak, non-dominant, non-language specialization hemisphere should yield low language competency and performance. Conversely, testing of the dominant side should show competency of a degree.

A test was devised to evaluate each hemisphere for language location and second-language colocation. A number of white cards, each bearing a short, simple, basic Romanian word, were prepared. Some words were nouns, others

DOCID: 4009731

verbs, but in equal numbers. All nine persons had readily translated all the words as part of a 250-word control text that they had been asked to translate two days prior to the testing.

For the testing, the subjects were instructed to stare at a spot affixed to a wall approximately 10 feet away, while covering their left eye. Thus, the visual images, the words in Romanian, were "fed" to the left hemisphere for all subjects.

As each word was flashed on the spot on the wall, each subject was asked to perceive it and translate it into English, or, if he was unable to perceive the word as a meaningful Romanian word, to state the letter or letters he had seen.

Seven words were presented to the left hemisphere of all subjects, yielding the following results:

Subject	*Number correct out of 7 words*
1	4
2	6
3	1
4	4
5	7
6	5
7	4
8	6
9	1

It is obvious that subjects 3 and 9 did considerably worse than the rest of the group. However, these two persons turned out to be left-handed. Apparently their left hemisphere did not function well in language and speech problems. These two subjects also complained that, although they could easily see the card and the letters on that card, they could not get the meaning of the words.

The group was then subjected to a test to probe the opposite side of the brain -- the right hemisphere, which is not normally associated with language functions in the adult. Under identical test conditions, a new set of Romanian words was flashed to all subjects with the right eye covered. These results were:

Subject	*Number correct out of 7 words*
1	1
2	0
3	5
4	1
5	1
6	1
7	0
8	1
9	6

In this test, the left-handers (subjects 3 and 9) did far better than the right-handers, and, moreover, zipped through the words with surprising speed. Virtually all the right-handed subjects complained of not being able to comprehend the word even though they could "physically see" the card and the letters. One right-hander remarked that he could see the entire word but still did not know what it was. Another spelled the three-letter Romanian word but could not perceive it as a meaningful word.

In another instance, the Romanian verb *merge*, "to go," was translated into English as "yield." Apparently this subject (a right-hander), who normally has no difficulty in translating the Romanian verb correctly, could do no better under these conditions than to associate it with the English word "merge" and mistranslate it by another English word seen in related traffic situations.

Many of the subjects could identify only the first and last letter of the word. All seemed frustrated, if not surprised, at their inability to translate simple three- and four-letter words. Even the allegedly "best" linguists, including some professionals, were duly humbled by this simple test.

This part of the experiment clearly located the area of the brain for Romanian learned as an adult -- in the respective hemisphere both for the right-handed and for the left-handed subjects. There was only a very marginal amount of Romanian in the weak, non-dominant side of the brain. Since this testing had no fixed time limit, it may be surmised that those weak-side correct responses -- which in fact took fairly long periods of time to produce -- were the result of a slow associative process that involved some type of data transfer between hemispheres via the splenium.

If anything, these experiments tend to support the consensus that language competency -- especially in a second language -- is located in the dominant side of the brain and thus colocated with the maternal language. It also shows a shift from one side to the other depending on which hand is the dominant one.

To sum up, then, when answering the questions "Does hemispheric dominance play a major role in second-language acquisition?" and "Does language learning as an adult present unique problems?" we must answer both questions with a categorical "Yes."

Can we locate the residence of second language in the brain? Again we can answer "Yes," but not as emphatically.

And, finally, we may answer the question of language competency by saying that there is little hope of attaining native fluency or competency when only one hemisphere is used in the language-learning process. At best, an adult may hope to acquire sufficient language items and sufficient exposure to the foreign culture to compensate for any learning deficiencies and psycholinguistic limitations.

~~SECRET SPOKE~~

COMPUTER-AIDED TRANSCRIPTION

P.L. 86-36

P.L. 86-36
EO 1.4.(c)

Introduction

Skeptics have long ago, and very convincingly, put down the notion that the computer is going to replace the linguist at NSA, or indeed anywhere else. However, a great deal of thought is going into designing ways in which the computer can *aid* the linguist. In this article I would like to describe a project currently underway

However, since "interim systems" have the tiresome habit of hanging around long after their predicted demise, I shall not even speak of the future or of greater glories yet to come. Instead I shall deal only with the very real present.

A wish was born to free transcribers from as many clerical or nonlinguistic functions as possible and at the same time make the fruits of the transcription effort available to other transcribers and to analysts on an on-line basis. The wish eventually became father
P.L. 86-36 to the deed in the form of a computer-aided transcription system. The need to generalize the software for "exporting" to other transcription problems, and the overriding need to provide the intelligence data gleaned from transcription to the intelligence community as a whole

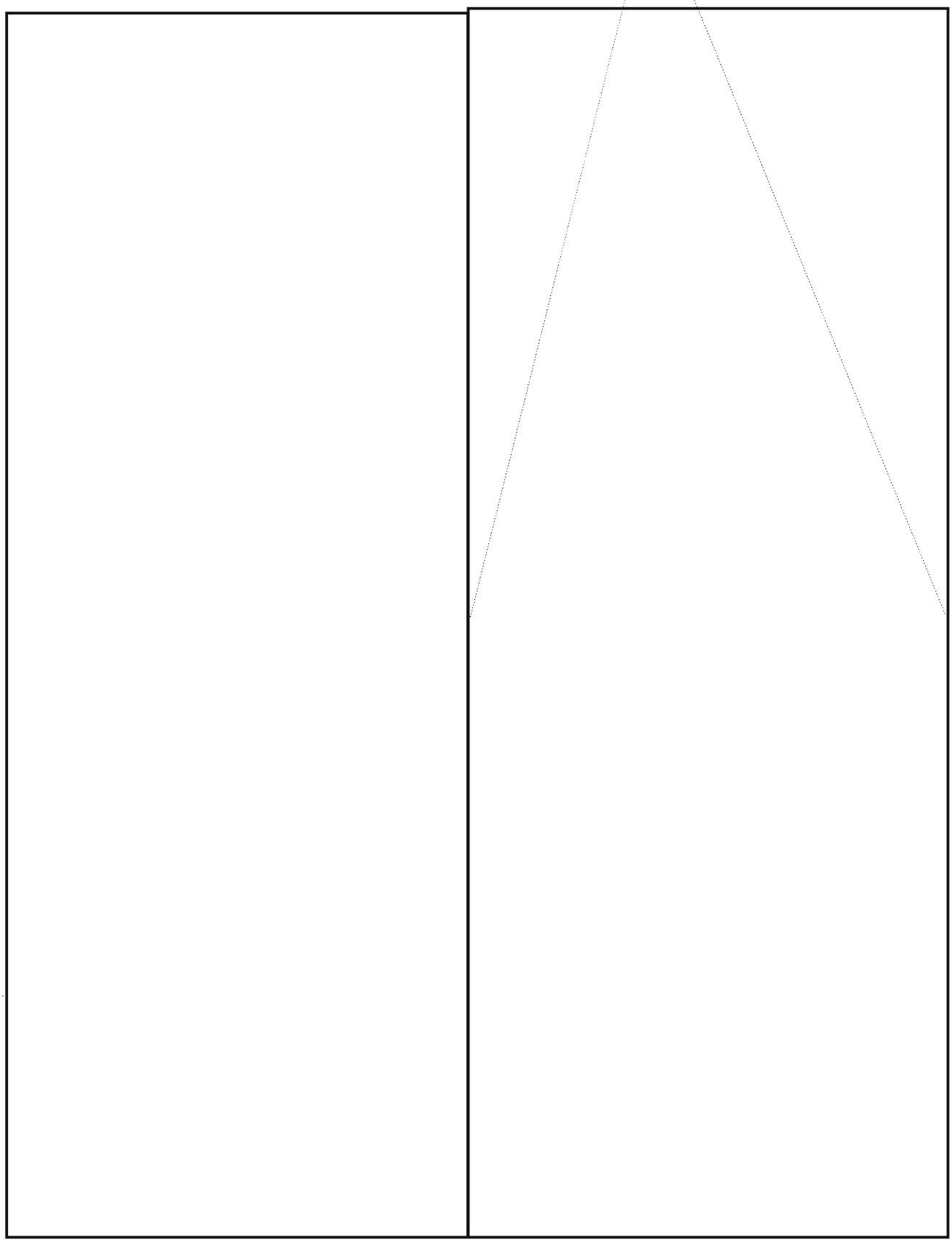
P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

~~SECRET SPOKE~~

P.L. 86-36
EO 1.4.(c)

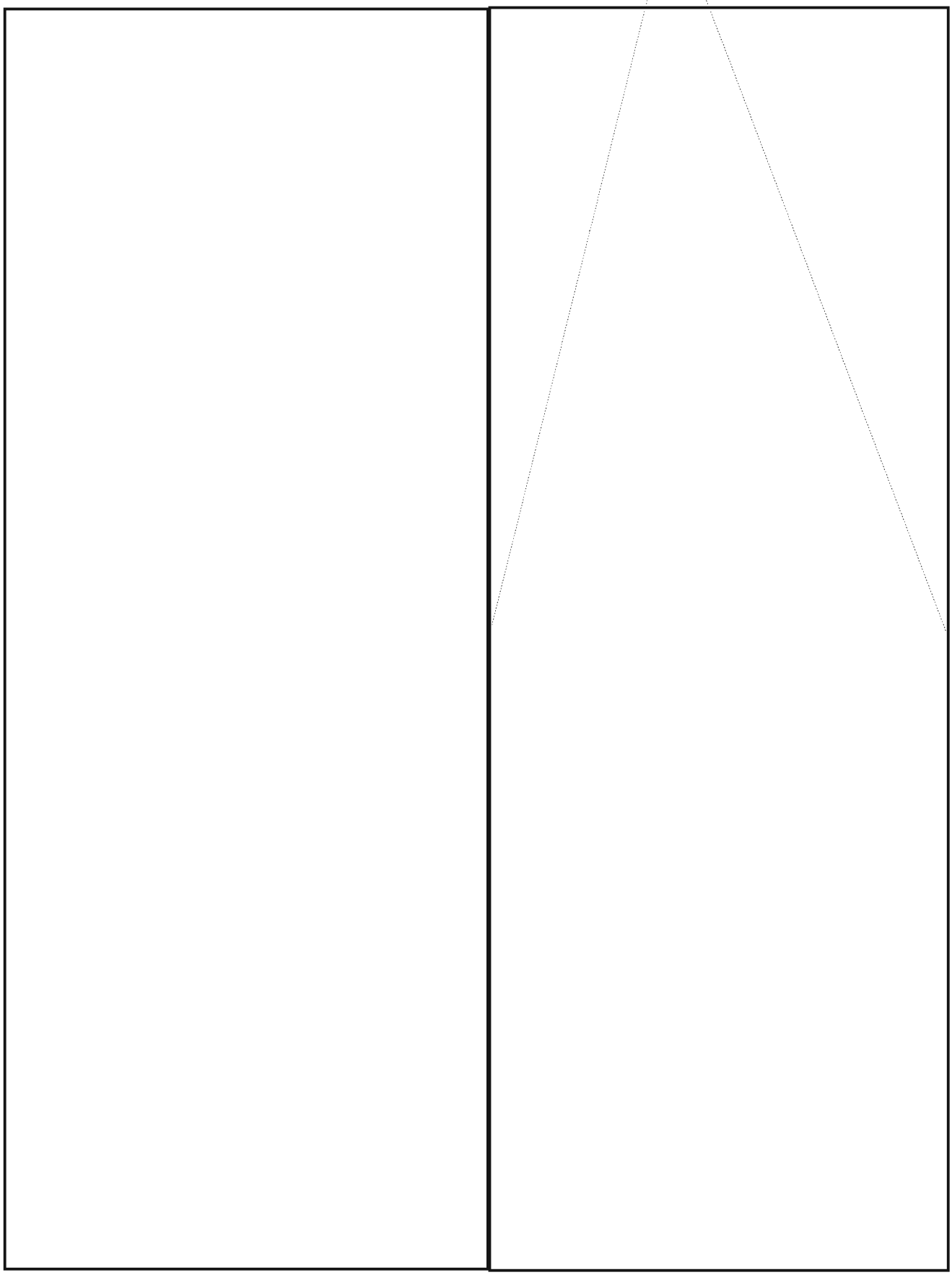
~~SECRET SPOKE~~



DOCID: 4009731

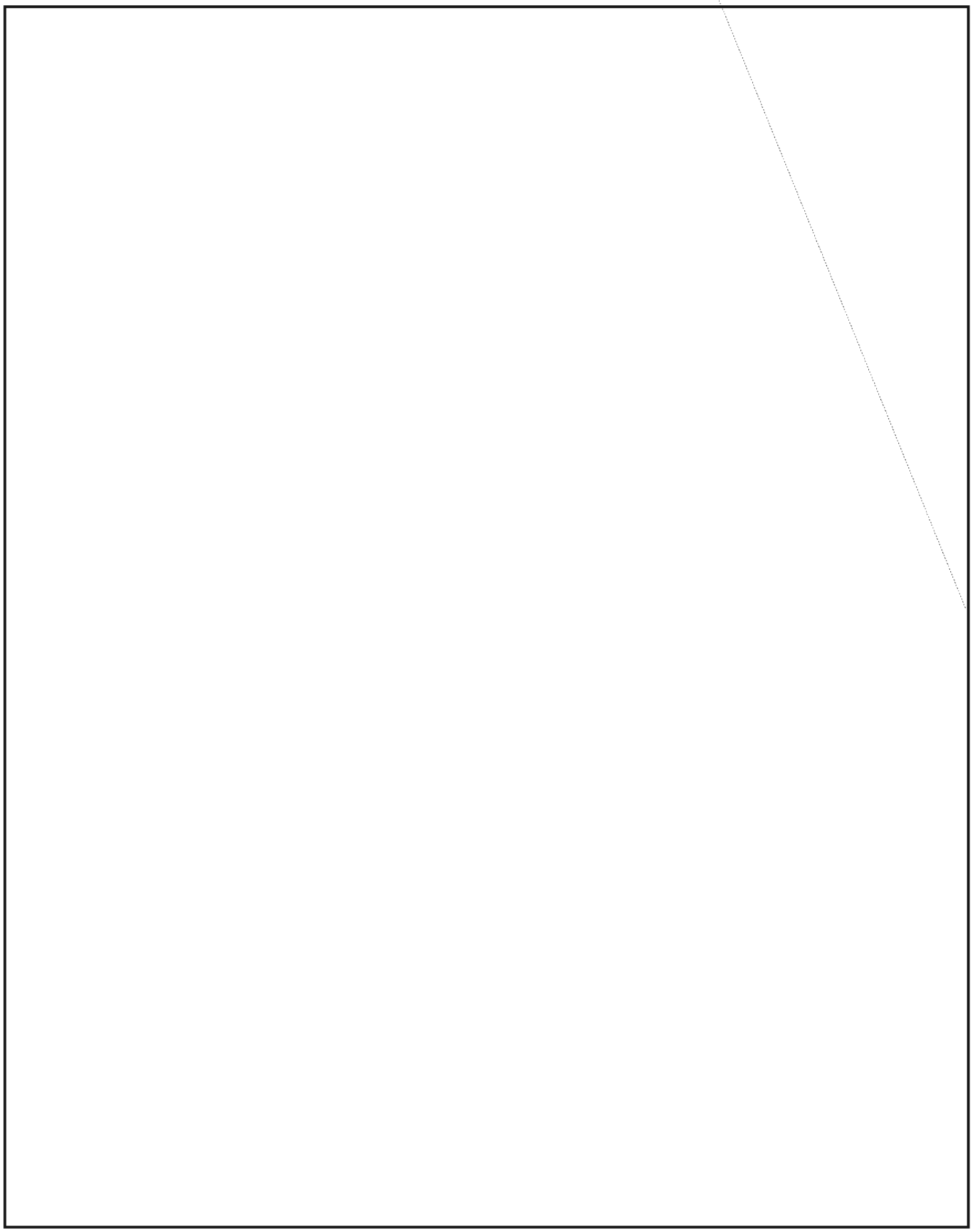
P.L. 86-36
EO 1.4.(c)

~~SECRET SPOKE~~

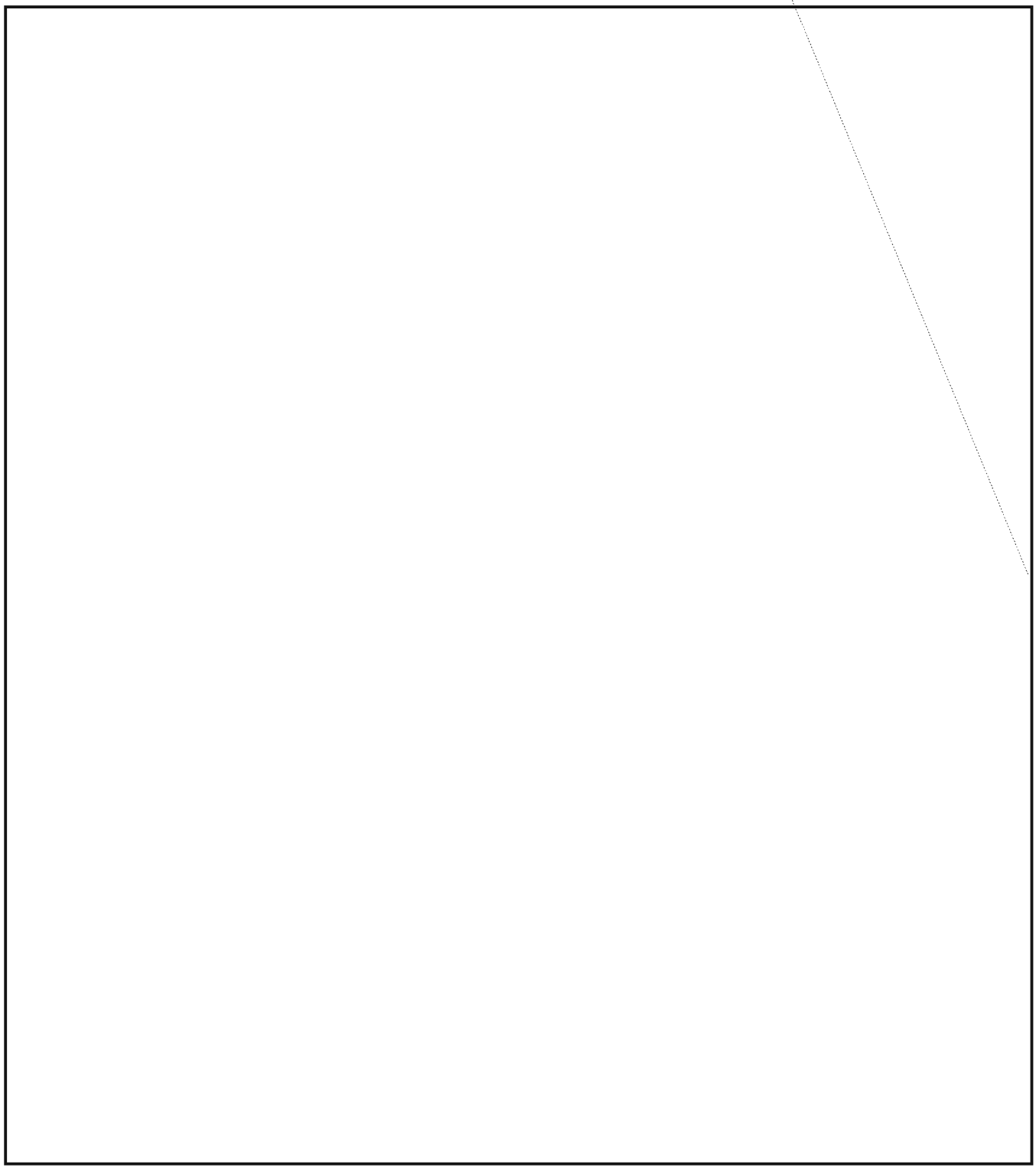


DOCID: 4009731

P.L. 86-36
EO 1.4.(c)



P.L. 86-36
EO 1.4.(c)



~~CONFIDENTIAL~~

CLARIFICATION OF ANNOUNCEMENT OF NCS Course-Equivalency Tests

The November 1975 issue of CRYPTOLOG contained an annoucement issued by the National Cryptologic School concerning Course-Equivalency tests. The announcement, with a list of courses, read:

The National Cryptologic School offers employees the opportunity to earn course credit by taking EQUIVALENCY TESTS. Frequently, through experience or self-study, a person has already learned the material presented in a course. If this knowledge can be demonstrated, time and energy required to take a course can be saved. Equivalency tests may be scheduled through the cognizant NCS department. . . A grade of "P" is assigned for passing the course through an equivalency test. Grades of "F" are not recorded. Aspirants may take the test only once.

The announcement elicited the following comment to the editor from [redacted] P.L. 86-36

CRYPTOLOG seems to be leading field personnel down a primrose path, as regards the article on NCS Course Equivalency Tests. In the future, please flag those courses which are available to NSA/CSS Ft. Meade area assignees only. For example, I am told by E23 that course equivalency tests for the EA-200 series courses are not available outside of NCS. Would be interested in knowing how many other courses/equivalency tests listed in the article are not available to field personnel.

The editor was pleased to be able to relay this comment to NCS and is equally pleased to print the School's clarification, as follows:

Please thank [redacted] for bringing up the issue of equivalency testing in the field. Many NCS tests can indeed be taken in the field, but some which require a laboratory exercise cannot. E23 has agreed that if the field station can make the necessary equipment available and will provide a qualified signals analyst to oversee the laboratory testing, the department will, on an individual basis, arrange to send the test to the field station. E23 will also make the effort to modify tests to accommodate personnel assigned to stations that do not have the currently stated required equipment.

The following list of tests is annotated to show the field testing arrangements. The list is followed by instructions for requesting a test.

*EA-010	Introduction to SIGINT Technology
*EA-030	Introduction to Multichannel Technology
*EA-100	Basic SIGINT Technology
***EA-200	SIGINT Instrumentation and Measurement Techniques

(Continued)

***EA-201	Communications Signals Measurements and Analysis Techniques
***EA-202	ELINT Measurement and Analysis Techniques

Cognizant department: E23

ED-210	Tests and Measurements

Cognizant department: E42

*ET-100	Introduction to Electronics
ET-260	Solid State Devices and Applications
ET-261	Digital Concepts

Cognizant department: E24

*MA-400	Introduction to Computer Science Mathematics
*MP-154	Introduction to Computer Systems Operation
*MP-1B5	CDC 6600 Series System Software (SCOPE)
*MP-1B6	CDC 6600 Advanced Technical Skills (SCOPE)
*MP-1C5	UNIVAC 494 RYE System Software
*MP-1C6	UNIVAC 494 Advanced Technical Skills
*MP-1D6	IBM 360/370 Advanced Technical Skills OS
*MP-1E5	UNIVAC 1108 System Software
*MP-1E6	UNIVAC 1108 Advanced Technical Skills
*MP-1G5	Project HOLDER - UNIVAC 494 Systems Software
*MP-1H5	Burroughs 6700 System Software
*MP-1H6	Burroughs 6700 Advanced Technical Skills
*MP-1K5	CDC 7600 System Software (IDA)
*MP-1K6	CDC 7600 Advanced Technical Skills (IDA)
*MP-1S5	Introduction to IBM 370 MVS Operating System
*MP-166	FORTRAN for Operators

Above 15 courses constitute the Operator Paraprofessional Program. Person must be in program and must have adhered to proper course sequence.

**MP-160	Introduction to Computer Science (Bypass test available to satisfy prerequisites for other courses. Course-equivalency credit requires toy problem using a Turing machine computer.)
**MP-188	APL Programming (requires APL terminal)
**MP-227	FORTRAN Programming
**MP-230	COBOL Programming

(Continued)

~~CONFIDENTIAL~~

**MP-242	PL/1 Programming
**MP-243	Burroughs Extended ALGOL Programming
**MP-248	BETA Programming (requires BETA compiler)
**MP-267	POGOL Programming (requires POGOL compiler)
**MP-335	IBM 370 Programming
**MP-368	IBM 370 Job Control Language (JCL)
**MP-375	PDP-11 Programming

Cognizant department: E21

*TA-200	Intermediate Traffic Analysis and Technical Reporting
*TA-261	Computer Aid to Traffic Analysis
TA-361	Air Defense Technology and Traffic Analysis

Cognizant department: E14

*IS-250	SIGINT Reporting
*TG-126	Target Studies - Mainland Southeast Asia

Cognizant department: E12

Key: * - Available in field.
** - Available in field -- toy problem also required.
*** - Available in field -- laboratory required.

INSTRUCTIONS FOR REQUESTING AN EQUIVALENCY TEST IN THE FIELD:

To request an equivalency test, write to NCS, Registrar, E71. Identify the course and summarize your previous training and experience in the subject.

If a laboratory is required, give the name of the qualified professional who will oversee your performance. For MP courses, identify the equipment that is available to you.

Tests will be sent to the Test Control Officer at your station for administration, after which they will be returned to NCS.

[redacted] P12, has an idea that's fresh as a P.L. 86-36

DAISY

He suggests that readers of CRYPTOLOG

MAY

want to share witn him their memories

AND

rare documents for a

LI'L

ole article he's contemplating writing on the

ABNER

computer that was used at Arlington Hall Station.

If you have any information to share with Russ, please call him on 5868s or visit him at 3C089.

~~(FOUO)~~

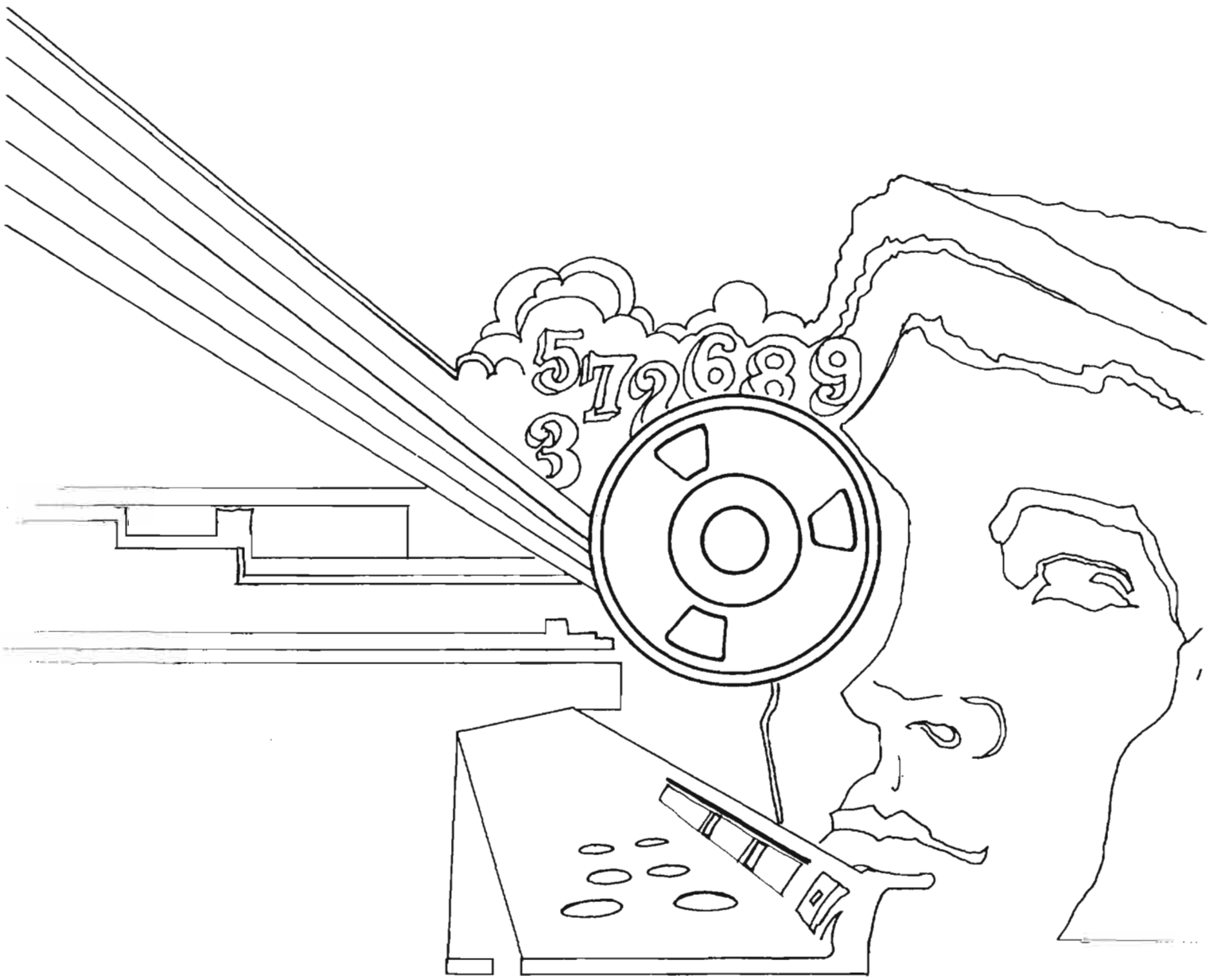
A cache of uncirculated copies of the following publications, in the quantities indicated, recently turned up. If any reader of CRYPTOLOG would like to receive a copy of any or all of them, please call [redacted] P16, Room 3W076, 4998s. P.L. 86-36

Collected Papers on Cryptanalytic Diagnosis, Introduction by [redacted] papers by Callimahos, [redacted] Douglas, [redacted] Jacobs, [redacted] Penney, Tiltman, and [redacted] NSA, April 1969, ~~TOP SECRET CODEWORD,~~ S-194,074. (23 copies)

An Introduction to Teleprinter Key Analysis, Lambros D. Callimahos. NSA, 1968. Technical Literature Series: Monograph No. 15. ~~CONFIDENTIAL.~~ (5 copies)

Ars Conjectandi: The Fundamentals of Cryptodiagnosis, Lambros D. Callimahos. NSA, 1970. Technical Literature Series: Monograph No. 18. ~~SECRET.~~ (2 copies)

~~(FOUO)~~


5726893

DOCID: 4009730

~~TOP SECRET~~

P1 WILLIAM LUTWINIAK

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MARCH 1976

P.L. 86-36

TO PULL A "PONYAL"..... [redacted] 1

MUSINGS ABOUT THE AG-22/IATS..... Cecil Phillips..... 3

AN OBJECTIVE APPROACH TO SCORING TRANSLATIONS..... [redacted] 5

A COMPARISON OF NSA AND ATA LANGUAGE CERTIFICATION STANDARDS..... [redacted] 8

LETTERS TO THE EDITOR.....12

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009730

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. III, No. 3 MARCH 1976

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief..... Arthur J. Salemme (5642s)

Cryptanalysis..... [redacted] (8025s)

Language..... Emery W. Tetrault (5236s)

Machine Support..... [redacted] (3321s)

Mathematics..... Reed Dawson (3957s)

Special Research..... Vera R. Filby (7119s)

Traffic Analysis..... Frederic O. Mason, Jr. (4142s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4009730

P.L. 86-36

TO PULL A "PONYAL"

EO 1.4.(c)
P.L. 86-36

DOCID: 4009730

EO 1.4.(c)
P.L. 86-36

1976 LANGUAGE MEETINGS AND CONFERENCES

March 3-6. Convention of Teachers of English to Speakers of Other Languages, 10th. New York, NY.

March 14-15. North American Conference on Afro-Asiatic Linguistics, 4th, and American Oriental Society. Philadelphia, PA.

March 21-24. Association for Asian Studies. Washington, D.C.

March 25-27. Conference on Composition and Communication. Philadelphia, PA.

April 1-4. Northeast Conference on the Teaching of Foreign Languages. New York, NY.

April 3-5. Annual Meeting of the Linguistics Association of Great Britain. Edinburgh, Scotland. (Write: J. Christie, Dept Linguistics, 15, Buccleuch PL, Edinburgh EH8 9LN, Scotland).

April 5-9. International Conference of Nordic and General Linguistics, 3rd. Austin, TX.

April 6-9. Acoustical Society of America. Washington, D.C.

April 9-10. College English Association. Cincinnati, OH.

April 15. [Deadline for abstracts for LSA Summer Meeting].

April 15-17. Conference on African Linguistics, 7th. Gainesville, FL. (Write: P.A. Kotey, Ctr African Studies, 470 LGH, Univ Florida, Gainesville, FL 32611).

April 19-23. American Educational Research Association. Las Vegas, NV.

April 20-24. Congress of the International Association for the Study of Italian Language and Literature, 9th. Palermo, Italy. (Write: Robert J. Clements, AISLLI, Rm 701, Main Bldg, New York Univ, Washington Sq, New York, NY 10003).

April 22-24. University of Kentucky Foreign Language Conference. Lexington, KY.

April 22-24. Southwest Areal Language and Linguistics Workshop, 5th. San Antonio, TX. (Write: B.L. Hoffer, Dept English, Trinity Univ, San Antonio, TX 78284).

April 22-25. Chicago Linguistic Society. Chicago, IL. (Write: Chicago Linguistic Society, Goodspeed 205, 1050 E 59th St, Chicago, IL 60637).

May 6-8. Conference on Perspectives on Language. Louisville, KY.

June 21-26. Conference on the Psychology of Language. Stirling, Scotland.

June 28-July 2. International Conference on Computational Linguistics. Ottawa, Ont, Canada.

July 26-31. Philippine-American Communication Conference, 1st. Manila, The Philippines.

August 17-19. World Congress of the International Reading Association, 6th, Singapore.

August 26-31. World Congress of Phoneticians, 3rd. Tokyo, Japan.

August 28-30. European Linguistics Society. Salzburg, Austria. (Write: G. Drachman, Institut Für Sprachwissenschaft der Universität, Imbergstrasse 2/III, A-5020 Salzburg, Austria).

September 1-4. International Phonology Meeting, 3rd. Vienna, Austria.

LSA Bulletin, Linguistic Society of America, October 1975

(UNCLASSIFIED)

DOCID: 4009730

MUSINGS ABOUT THE AG-22/IATS

Cecil Phillips, C03

The following article is reprinted from C-LINERS (C Group Machine Processing Information Bulletin), Vol. 3, No. 7, August/September/October 1975.

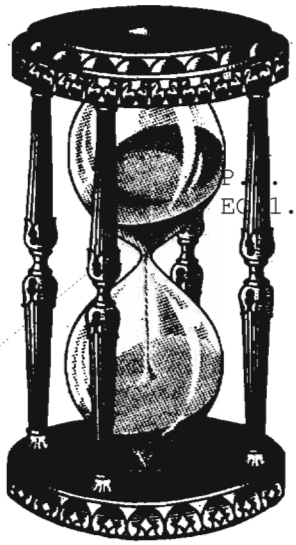
EO 1.4.(c)
P.L. 86-36

Comments, anyone?

Mr. Phillips was Chief of the ADVAGENS Joint Mechanization Group, which conducted the first tests of an AG-22-like device in 1960 and 1961 [redacted] *were also members of the group. The specific AFSAV-D/311 tests Mr. Phillips mentions were carried out by* [redacted]

~~(CONFIDENTIAL HVCCO)~~

TIME'S RUNNING OUT!



You'd better hurry if you want to enter the CMI ESSAY CONTEST or the CLA ESSAY CONTEST this year!

The deadline for submitting entries to the CMI ESSAY CONTEST is 26 March and the deadline for the CLA ESSAY CONTEST is 19 March.

P.L. 86-36
EO 1.4.(c)

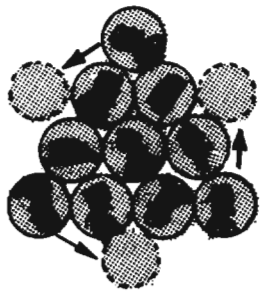
For complete information, see *The NSA Technical Journal*, Vol. XX, No. 4, Fall 1975. Or call the following:

CMI Contest: [redacted] or [redacted] 3957s

CLA Contest: [redacted]

P.L. 86-36

(UNCLASSIFIED)



PENNEY PUZZLES

Puzzle fans, mathematicians, cryptanalysts! Here's an opportunity you won't want to miss! The Cryptomathematics Institute (CMI) has a number of copies of PENNEY PUZZLES, a collection of 68 puzzles by CMI's executive director, Walter Penney. While the supply lasts, a free copy of this fascinating unclassified book will be sent to everyone joining CMI. To join, send your name, social security number, organization, telephone number, and $3.00 for 1976 dues to: [redacted] *CMI Treasurer, S03.*

EO 1.4.(c)
P.L. 86-36

(UNCLASSIFIED)

P.L. 86-36

DOCID: 4009730

An Objective Approach to SCORING TRANSLATIONS

P16 P.L. 86-36

Reprinted from *QRL (Quarterly Review for Linguists)*, November 1973

Author's note: The philosophy underlying the translation grading system described in this paper has been developed and applied by Emery Tetrault and myself, with many valuable suggestions from our colleagues on Professional Qualification Examination (PQE) Committees and from other Agency linguists. My use of the pronoun "we" reflects this collaboration. I personally take full responsibility for presenting our findings here.

*

Translation as an intellectual activity has been practiced since antiquity for practical as well as esthetic reasons, but even today we have reached no consensus on whether it is even possible to fully "bring over" from one language to another the contents of a fairly pedestrian piece of prose, let alone fiction or poetry. We debate the merits of machine translation as a precursor to a truly "scientific" discipline or argue whether a "free" translation of a Greek lyric poem does not better catch the flavor of the original than one which adheres rather closely to the syntax of the original and results in an awkward (i.e. "literal") rendering in the target language. In short, the domain of translation has not been really determined. Our own work never demands (fortunately) the highly creative product of the artist translating Homer, Dante, or Pushkin but it does require something more than a purely mechanical approach; good translators have a flair for couching in idiomatic English the thought content of the source-language passage. Poor translators, on the other hand, seem never to master this complex operation regardless of how well they may know the source language or how well they may write English when not translating.

If we had only the two kinds of translators to judge we could sort them into sheep and goats and have done with it. The fact is that most aspiring translators are neither brilliant nor hopeless, but fall somewhere in between, and when professional certification is at stake we need, in the interest of justice to the candidate as well as to the system, reasonably objective criteria for making a final decision on *pass* or *fail*.

Lacking such criteria in our early attempts to evaluate translations, we ended too often with intuitive decisions not transferable to similar cases involving the same source language; nor was it even possible to compare intuitive judgments across language boundaries, in source language-to-English situations.

Over the past 2 or 3 years my colleagues and I have developed a way to score translations which may obviate this problem to a large extent even though our results have admittedly been far from perfect (total "objectivity" in grading any kind of connected text is of course impossible). Our first large-scale use of the system, which I will describe later, was with the Russian PQE. We have subsequently tried it in a number of other PQEs involving several languages, mainly Indo-European, but also from other families. The results have been encouraging enough in both instances for us to recommend its use in the PQE Handbook.

Subjective Approaches to Evaluating Translations

One approach to scoring translations is in a sense historical in that the evaluator tries to guess the reason for the translator's mistake and in so doing draws unwarranted inferences. This attempt may be useful when the time comes to counsel the failing or borderline aspirant and the problems can be talked out. Unfortunately, though, the history of an error is irrelevant to the rendering of a particular text and whether the aspirant should have learned a particular grammar rule in a course is beside the point.

A second method in wide use is to decide arbitrarily that a certain kind of mistake (for example, failure to recognize proper nouns and inappropriate translation of them) is sufficient cause to fail a paper. This syndrome is evident among longtime subject-matter experts or specialists in some area of the world who see examinations solely in terms of their immediate interests.

One example of each approach should suffice. In the first case, a would-be translator missed a trickly negative conditional construction in the first sentence of a fairly long paragraph which contained other negative and conditional elements much less difficult. In the interest of coherent discourse the translator overrode the signals which "he should have learned" and produced a sensible but wrong text. A second translator decided that the name of a group of islands, which historically means "fishing platform," should be so translated. Not only did he fail to recognize the proper noun, but he also saw the context of an entire paragraph in terms of the translation, and produced a peculiar text in English.

The evaluators of the first passage initially decided that the paper should fail because

the aspirant did not know enough of the grammar of his language, regardless of his performance in the rest of the examination. (Fortunately, we reconsidered the translation as a whole and gave the paper a marginal pass.) The second faux pas made in an early PQE apparently caused such anguish to the evaluators that they failed the paper mainly on this point.

I hasten to add that none of the above is meant in a caviling spirit. Translations, wherever and by whomever done, have ordinarily been assessed by these or other equally subjective methods. What we propose here is an attempt to bring a measure of uniformity to grading translations so that intuition and idiosyncrasy play a minor role and some kind of objective standard is established. The framework and detail of the proposed system is described below.

Linguistics and Evaluation of Translation

Before discussing precise error weighting I should say a few words about linguistics, dreary as the prospect may be, and follow with some comments on how committees apply linguistic principles in test evaluation.

The first point to be made is that the grading system to be described is based insofar as possible on a somewhat artificial distinction between *syntax* and *semantics*. I will therefore define these terms insofar as they apply to the present case.

- Syntax is the system of relating linguistic elements to one another in phrase, clause, or sentence, a process which is concerned with selecting appropriate grammatical forms (hereafter called "affixes"), positions for vocabulary items, or a combination of both, depending upon the particular language. Syntactic analysis leads from particular texts to general statements about the linguist elements of a language. The traditional parsed sentence is an inductive exercise proceeding from, for example, the sentence *"The quick brown fox jumped over the lazy dog"* to a set of names or symbols: Definite article + adjective + adjective + noun + verb + past tense + preposition + definite article + adjective + noun. We cannot, however, recapture this gem by simply reversing the procedure, because, except for the definite article, a possibly infinite number of combinations could appear. Nonetheless, a command of the syntax of a foreign language, which will inevitably differ from that of English at many points, is the first element of the language the student necessarily learns.
- Semantics, on the other hand, is concerned with particular meanings of linguistic elements in context. To the extent that patterns of feeling and thinking between languages are similar, as to a large extent they will be in the Indo-European languages, transfer of ideas and impressions will be on the whole fairly simple. (Some kinds of texts are dependent on an intimate knowledge of a vastly different culture subsystem, religious, political, and so on. These texts are never used for PQEs.) The student needs a vocabulary of a couple of thousand words, the main carriers of ideas, before he can work efficiently, regardless of how good his syntactic control may be.

Obviously, many members of PQE Committees have not had much formal linguistic training in syntactic and semantic analysis, excellent though they may be in the language they are concerned with. Just as obviously, there is no time for us to give extensive training in these subjects to people who are busy with other things. However, a certain minimum of linguistic thinking is needed to make our system work and we have tried to impart this informally to committees before they select passages for translation and evaluate them. Once a committee has a general grasp of the system, the members should be better able to select passages containing interesting syntactic and semantic problems. After having produced translations of passages against which papers will be judged, the committee can then to some extent predict likely errors. When the papers are actually graded, each evaluator works independently to derive a score based on the weighting described below then compared his results with the others.

Some differences in weighting are bound to occur and may be irreconcilable, but generally the findings show a narrow spread of 5 to not more than 10 points. The care required in such careful grading insures that at the very least major errors are not overlooked, a result not always achieved by subjective grading.

Our weighting of linguistic elements is based on the assumption that aspirants should be expected to control their source-language syntax. A failure to understand relations within and among sentences, which are marked by position and/or affixes as noted above, can seriously distort the meaning of an entire paragraph; hence, we take either 8 or 4 points off per error, depending on its severity. If, for example, a sentence should have been translated *"Dog bites man"* but comes out *"Man bites dog,"* we would subtract 8 points because all the relationships are wrong. If a sentence which ought to have been translated *"We stopped near the train"* is rendered *"We stopped the train,"* we would take off 4 points since the subject-verb relationship is correct even though the rest of the sentence is wrong. As we have set 70 as a passing score, four 8-point errors will fail a PQE.

Certainly the examples above are oversimplifications of translation problems which can be knotty. Our experience has shown, however, that in 9 out of 10 cases committees can achieve consensus on the kind and degree of syntactic error

DOCID: 4009730

not only for Russian examinees but also for aspirants in Indo-European and Semitic languages generally. Where we have had problems, it has been in languages such as Chinese or Vietnamese where the intersection of "syntax" and "semantics" has not begun to be explored, let alone taught to unversity or DLI students. If aspirant translations from these languages go far afield and reverse the meaning of the original, or, even worse, do not even fall in the correct subject-matter area, the point system above is still applied: wrong is wrong. It would of course be possible to set as passing a score lower than 70 for languages structurally removed from English, but a decision to do so would be made on grounds other than linguistics.

Semantic errors are "charged at a lower rate" (2 points per error), not because we regard vocabulary as unimportant -- far from it. As I noted above, a knowledge of syntax alone won't do, for the idea structure mainly depends upon lexical units. However, our experience has shown that students of foreign languages pick up vocabulary unevenly, probably because no systematic attempt to teach it has ever been devised and successfully applied. Nor, for that matter, are students properly instructed in the use of either monolingual or bilingual dictionaries. To the extent that vocabulary instruction is given at all, it is given on the job and takes the form of *ad hoc* corrections and suggestions on how to use one or another dictionary to better effect. This process may be tedious but, provided the subject matter translated is not abstruse, is easy in comparison with mastering a new syntax.

For these reasons it seemed best for us to accommodate to the existing situation and apply the lighter penalty. Even so, we still encounter situations in which it is almost impossible to decide whether an error is in fact best viewed as semantic or syntactic. If a source-language pronominal reference is translated by the wrong pronoun, is this a simple error at a given point (hereafter, "punctilinear error") or could it open the way for misunderstanding several sentences (syntactic error)? Contextual judgment is the only method for making such a decision. On the other hand, some apparently pure grammar markers, such as tense forms, can be mistranslated without in any way distorting the basic noun-verb relationships. Thus, *"the dog bites the man"* and *"the dog bit the man"* have the same noun-verb-noun arrangement: the difference lies in the time of the event identified at a given point in the text. A tense error is hence punctilinear and costs 2 points.

As I have suggested, it is often difficult for PQE Committees to reach a consensus at every point of semantic and syntactic error in translation from the source language. The task of evaluating the translation from the point of view of English usage and violation of convention is even harder, but extremely awkward English does have an overall effect of blurring meaning or, at the very least, causing the reader unnecessary strain. Violation of acceptable English we call "poor cooccurrence."

When the members of a committee are unanimous in judging an English phrase to reflect poor cooccurrence, one point is assessed. Here are examples of the kind of poor usage we have met: "an oblivious scholar to practical matters" instead of "a scholar oblivious to. . ." (awkward splitting of adjective and accompanying preposition); "the car collided against the bus" instead of ". . . with the bus" (a seemingly unlikely mistake for a native speaker of English to make, but this type is of high frequency nonetheless); "Foreign Minister Rogers" instead of "Secretary of State Rogers" (a violation of conventional usage).

Hundreds, if not thousands, of similar peccadilloes have been and are being committed under the present system and are the object of heated remonstrances from the failing aspirant. ("Why do they have to nitpick everything?") It has been our personal experience that committees on the whole err on the side of generosity in cases of one-point errors, and overlook altogether misspellings and wrong punctuation where these do not cause major problems in understanding the English text. Even those evaluators who take violent exception to misspelling will not fail a paper for this alone.

*

To sum up, it has been our intention to establish a system of grading which will be as objective as possible. Using a base of 100 and with 70 as passing, we have specified 3 kinds of errors. The first 2, syntactic and semantic, concern command of the source language; the third bears upon English usage. Syntactic errors are of two orders of severity reflected in the 8- and 4-point penalties, while semantic mistakes are charged 2 points and English misuse, or poor cooccurrence, costs one.

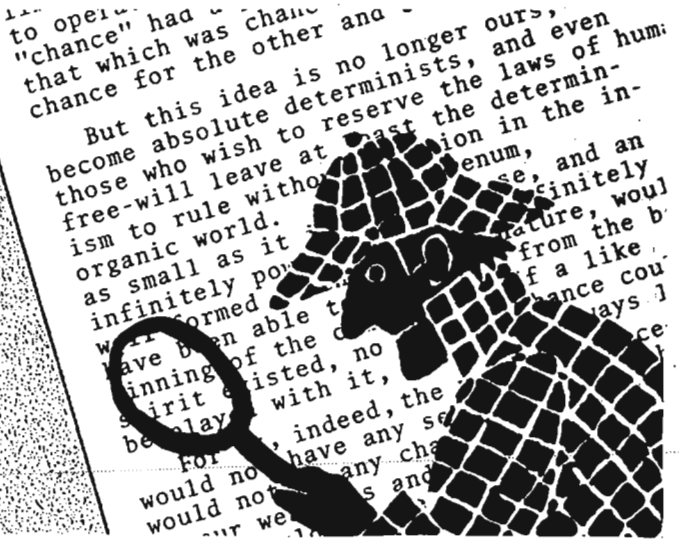
There are, to be sure, many doubting Thomases who question the efficiency of the system, either because they feel it is too complex to master or that the time spent in mastering it might better be devoted to something else and that the intuitive or "seat-of-the-pants" method will do as well. While conceding the time required to be considerable, the final result, we feel, more than justifies the effort and, in the absence of a better system, ought to prevail.

Editor's note: The system described in the reprinted article has been in use at the Agency since July 1972. [redacted] P.L. 86-36 *is currently writing a paper in which he will summarize the experience that the PQE Committees have had in using the system and will suggest theoretical and practical improvements.*

DOCID: 4009730

~~FOR OFFICIAL USE ONLY~~

A COMPARISON OF NSA & ATA LANGUAGE CERTIFICATION STANDARDS



P.L. 86-36

How does an NSA language professional stack up against language professionals elsewhere? That question cannot really be answered inasmuch as apples and pineapples are not directly comparable. An insight at the very lowest level of professionalization can be gained, however, by comparing the criteria for NSA's open-source translation (Part IA of the Professional Qualification Examination) and those for accreditation by the American Translators Association (ATA).

NSA's test

The NSA language test is of such length in the foreign language as to generate a total of 450 to 600 words of English translation. Time is not a factor, therefore examinees can take as long as 4 hours for this section of the PQE. Texts do not pose any problems of content substance; that is, they do not require an overly specialized knowledge of subject matter. They are usually articles by professional journalists on a topic of interest to the general public -- at the difficulty level of *Reader's Digest* or a weekly news periodical. Any lexical item in the text which is not in the standard bilingual dictionary is glossed in a footnote.

NSA graders use a *points-off* system in grading the test. They give more relative weight to errors involving the *logical relationships* among major sentence parts and to identifying specific items in the source text (that is, markers for number, case, gender, tense, aspect, mood, voice, etc.). Each sentence is graded by itself; no more than 8 points is taken off for any one sentence. If the logical subject-verb-object/complement relationship in the translation is not substantially the same as that of the source-language sentence, no fewer than 4 and no more than 8 points are taken off. Experience in various test committees has shown that examinees who get the maximum of 8 points taken off on each of 3 sentences seldom pass the test.

For each translation error involving a *single word* (content words such as nouns, adjectives, verb stems; function words such as prepositions and conjunctions, and grammatical affixes) 2 points are deducted -- up to a maximum of 8 points in any one sentence. For errors involving poor selection of *dictionary meanings* of a lexical item or poor word *collocations* (words that just don't fit together right in English), only one point is deducted.

From the foregoing explanation, it can be seen that a sentence in the English translation might contain one major error involving logical relationships (say, 8 points), 3 single-word errors (6 points), and perhaps 2 collocation or word-choice errors (2 points), but the NSA grader would not deduct 16 points for that sentence -- instead he would deduct only the maximum of 8 points per sentence.

If the translation of Part IA of the Agency's PQE has fewer than 30 points deducted, it is considered to be a "pass." But a translation that just passes is far from good. It is not as simple as saying that a translation with 30 points deducted is "30% inaccurate." Instead, such a translation may be "all wrong," because it will almost certainly contain several errors of fact, any one of which could be critical in a real-life translation situation. So, if such a poor examinee were to be certified as a linguist and were to produce, on an everyday basis, operational translations containing such critical errors of fact, one can only imagine the tremendous amount of work and responsibility that would be placed on the language checker who would have to correct the translations before issuing them. Or one could imagine the inherent dangers if such translations, in a stress situation, were issued to the customer without being corrected.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009730

If a particular grader deducts between 30 and 40 points, the translation must be debated in committee; if the majority of the committee members feel that enough of the *minor* errors would have been caught and corrected in the checking, proofreading, and analysis phases, a translation with as many as 40 points might actually be allowed to pass. PQE committee members sometimes lean over backwards in attempting to pass certain marginal papers. They claim that if only a few examinees pass, management tends to say that the test is too hard, never that the applicants are just not certifiable as professional linguists.

One thing must be borne in mind, however. A person who passes the PQE, even with distinction, is only *certified* as a linguist; it still might take him many years of on-the-job experience to become a senior linguist (something that a person becomes without having a piece of paper to prove it). Dr. Jaffe used to compare this situation with that of a medical student being awarded a diploma from medical school and the right to apply for a license to practice medicine; he would still need years of experience to become an expert in his field. If, then, a person who passes a PQE without debate has demonstrated the *potential* to become a senior linguist, the person who is allowed, after debate, to squeak through a PQE has demonstrated, if anything, the ability to function at only the very lowest level of linguistic competency.

ATA test

The American Translators Association is a different animal. Its members include both literary translators and technical translators. Literary translation is a creative art, and is not tested. But since all translators make most of their money from translating technical, scientific, and legal material, technical translation is used for ATA accreditation. The length of the ATA test is approximately 750 words. Time *is* a factor; precisely 3 hours is allotted for the test. As with the NSA text, the texts do not pose any problems of content substance: lexical items not in the standard bilingual dictionary are glossed in footnotes. Selections tend to reflect the subject matter of professional translators (international meetings, symposia, national projects, medical research, technology, science, etc.), but in a popularized version at the newspaper or *Reader's Digest* difficulty level.

Backgrounds and specializations of the ATA members vary greatly. The examinees are accordingly offered five selections in five somewhat different subject fields, from which they choose three to translate. The topics in the test that I recently took were the Apollo-*Soyuz* flight, the Helsinki Conference, blood immunology, a legal case involving patents, and the prospective Canadian Health Service System.

These selections do not reflect the difficulty level of the foreign-language texts that usually confront professional translators. But the grading criteria do reflect the requirements of the customers who let contracts for translators. The ATA examinees are told to be *precise* and *fairly literal*, and to be extremely carefuly in paraphrasing so as not to lose one iota of the sense of the clause or sentence. They are warned that omissions of words (except for such low-information words as *schon, doch, und zwar, en effet, znachit*) can be extremely costly and can even result in failing a selection. A candidate must pass two out of the three passages selected. Only *one* serious error in a passage is permitted; two serious errors constitute a fail for that selection (of course, a large number of nonserious errors could also constitute a fail).

Following is a passage from a statistical text, *Calcul des probabilités*, that was used in the French test administered at the ATA workshop in California in the summer of 1975. The passage is followed, in turn, by three of the translations done by examinees (for the convenience of the grading committee, the translations are typed prior to grading). The underlined words and the notations in the left-hand margin were made by one of the ATA graders (a capital *E* is the symbol for a major error; a lower-case *e* is the symbol for a minor error; *mistr.* stands for mistranslation.)

Comparison of ATA and NSA grading systems

To compare the ATA and NSA grading systems, the typed translations, including the ATA grader's underlines and notations, were shown to an NSA linguist with experience in grading French PQEs. He made his own underlines (======), most of which coincided with errors noted by the ATA grader, and indicated in the right-hand margin the number of points that would be deducted in accordance with the Agency's PQE criteria. For example, in translation #1 the ATA grader considered the error "for both" (mistranslation of *pour les dieux*, "for the gods," misread as *pour les deux*) to be a major error, whereas the NSA grader deducted 2 points for it.

Since the Agency's PQEs are usually twice as long as the ATA French selection, let us assume that the translators would have had an equal error rate for an additional 300 words. In that event, the results would have been as follows:

		NSA grade		
Translator	*ATA grade*	*Raw score*	*Extrapolated score*	*Pass/fail*
1	Fail	84	68	Marginal
2	Fail	72	44	Fail
3	Pass	100	100	Pass

DOCID: 4009730

~~FOR OFFICIAL USE ONLY~~

French, passage A -- from a statistical text, *Calcul des probabilités*

Translator #1

I. LE HASARD

"Comment oser parler des lois du hasard? Le hasard n'est-il pas l'antithèse de toute loi?" Ainsi s'exprime Bertrand, au début de son *Calcul des probabilités*. La probabilité est opposée à la certitude; c'est donc ce qu'on ignore et, par conséquent semble-t-il, ce qu'on ne saurait calculer. Il y a là une contradiction au moins apparente et sur laquelle on a déjà beaucoup écrit.

Et d'abord qu'est-ce que le hasard? Les anciens distinguaient les phénomènes qui semblaient obéir à des lois harmonieuses, établies une fois pour toutes, et ceux qu'ils attribuaient au hasard; c'étaient ceux qu'on ne pouvait prévoir parce qu'ils étaient rebelles à toute loi. Dans chaque domaine les lois précises ne décidaient pas de tout, elles traçaient seulement les limites entre lesquelles il était permis au hasard de se mouvoir. Dans cette conception, le mot hasard avait un sens précis, objectif: ce qui était hasard pour l'un, était aussi hasard pour l'autre et même pour les dieux.

Mais cette conception n'est plus la nôtre; nous sommes devenus des déterministes absolus, et ceux mêmes qui veulent réserver les droits du libre arbitre humain laissent du moins le déterminisme régner sans partage dans le monde inorganique. Tout phénomène, si minime qu'il soit, a une cause, et un esprit infiniment puissant, infiniment bien informé des lois de la nature, aurait pu le prévoir dès le commencement des siècles. Si un pareil esprit existait, on ne pourrait jouer avec lui à aucun jeu de hasard, on perdrait toujours.

Pour lui, en effet, le mot de hasard n'aurait pas de sens, ou plutôt il n'y aurait pas de hasard. C'est à cause de notre faiblesse et de notre ignorance qu'il y en aurait un pour nous. Et, même sans sortir de notre faible humanité, ce qui est hasard pour l'ignorant, n'est plus hasard pour le savant. Le hasard n'est que le mesure de notre ignorance. Les phénomènes fortuits sont, par définition, ceux dont nous ignorons les lois.

I. CHANCE

"How dare we speak of the laws of chance? Is not chance the antithesis of every law?" Thus Bertrand expresses himself, at the beginning of his "Calculation of Probabilities." Probability is opposed to certainty; thus it is what is unknown, what we would not know how to calculate. There is at least an apparent contradiction here, one on which a great deal has already been written.

First off, what is chance? The ancients distinguished between the phenomena which seemed to obey harmonious laws, established once for all, and those which they attributed to chance; they were the ones that couldn't be anticipated because they were unamenable to all law. In each domain, no precise laws were determined; they traced only the boundaries among which chance was allowed to operate. In this concept, the word "chance" had a precise, objective meaning: what was chance for one was also chance for the other, and even for both.

However, this is not our way of looking at it; we have become absolute determinists, and even the same ones who want to save a place for free will in mankind, nevertheless, let determinism hold untrammeled sway in the inorganic world. Every phenomenon, no matter how minute it may be, has a cause, and an infinitely powerful mind, infinitely well informed of the laws of nature, would have been able to foretell it since the beginning of time. If such a mind existed, one would not be able to play any games of chance with it -- one would always lose.

For that mind, in fact, the word "chance" would have no meaning, or rather there would be no chance. It is because of our weakness and our ignorance that there would be chance with us. Also, even without going outside of our feeble humanity, what is chance to the ignorant is no longer chance to the wise man. Chance is only the measure of our ignorance. The chance phenomena, by definition, are those whose laws we do not know.

Fail

84 = 68

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009730

~~FOR OFFICIAL USE ONLY~~

Translator #2

I. CHANCE

"How does one dare to speak of the laws of chance? Isn't chance the antithesis of all law?" Bertrand thus expresses himself, at the beginning of his "Calculation of Probabilities." Probability is opposed to certainty; it is thus what one does not know and, consequently, it seems, what one does not know how to calculate. There is there at least an apparent contradiction, and one on which much has already been written.

And, first, what is chance? The ancients singled out phemomena that seemed to obey harmonious, firmly established laws and those they attributed to chance; there were those that one couldn't forsee because they were rebellious to all law. In each domain, precise laws did not decide everything, they only traced the limits between which chance was permitted to operate. In this conception, the word "chance" had a precise, objective meaning: that which was chance for one, was also chance for the other and even for the gods.

But this idea is no longer ours; we have become absolute determinists, and even those who wish to reserve the laws of human free-will leave at least the determinism to rule without division in the inorganic world. All phenomenum, as small as it is, has a cause, and an infinitely powerful spirit, infinitely well formed to the laws of nature, would have been able to forsee it from the beginning of the centuries. If a like spirit existed, no game of chance could be played with it, one would always lose.

For it, indeed, the word of chance would not have any sense, or soon there would not be any chance. It is because of our weakness and of our ignorance that there would be one for us. And, even without leaving our weak humanity, that which is chance for the ignorant, is no longer chance for the well-informed. Chance is only the measure of our ignorance. Fortuitous phenomena are, by definition, those of which we do not know the laws.

Fail

72 = 44

Translator #3

I. CHANCE

"How can we dare to speak of the laws of chance? Is not chance the antithesis of all law?" Thus speaks Bertrand, at the beginning of his "Calculation of Probabilities." Probability is opposed to certitude; thus it is what we do not know and so, apparently, what we cannot calculate. There is here an at least apparent contradiction about which much has already been written.

First of all, what is chance? The ancients distinguished between phenomena which seemed to obey harmonious, definitely established laws and those which they attributed to chance. The latter were phenomena that could not be foreseen because they were contrary to all law. In each field the precise laws were not all-determining; they merely defined the limits within which chance was permitted to operate. In this conception, the word "chance" had a precise, objective meaning: what was chance for one man was chance for another, and even for the gods.

But this conception is no longer ours; we have become absolute determinists, and even those who wish to reserve the rights of human free will at least permit determinism to reign unchallenged in the inorganic world. Every phenomenon, however small, has a cause, and an infinitely powerful mind, infinitely well informed of the laws of nature, could have foreseen it from the beginning of time. If such a mind existed, we could not play any game of chance with it; we should always lose.

For this mind, in fact, the word "chance" would have no meaning, or rather there would be no chance. It is because of our weakness and our ignorance that one may exist for us. Even without departing from our weak humanity, what is chance for the ignorant man is no longer chance for the scientist. Chance is merely the measure of our ignorance. Fortuitous phenomena are, by definition, those whose laws we do not know.

Pass

-0

~~FOR OFFICIAL USE ONLY~~

[redacted]

[redacted]

One final remark about NSA PQEs and ATA's accreditation examinations: they are both designed to set the lowest threshold level of professionalization, no more! At NSA the emphasis is placed on accuracy of content. In the ATA, accent is placed on precise, literal accuracy and on speed. A person who can complete the exam in exactly 3 hours will be able to make a bare living just above the poverty level in translating material of that difficulty, using conventional paper-and-pencil techniques and typing up the finished copy himself. Translators therefore specialize in specific technical fields where they can get at least double or triple the basic translation pay rate. Then too, professional translators often dictate their translations into recording equipment and pay a typist to transcribe the translation into finished copy; despite this additional expense, this method is beneficial to the translator since it enables him to at least double his translation output. Consequently, a free-lance professional translator, after gaining experience and one or more specialties, should be able to earn at least $36,000 a year. Even a part-time free-lance (moonlighter) translator can earn as much as $5000 a year. These figures indicate that ATA accreditation is worth quite a bit in dollars and cents. They also indicate that, according to ATA standards, the majority of certified NSA linguists are overpaid, while the few truly professional certified linguists at NSA are underpaid.

[redacted]

~~(FOR OFFICIAL USE ONLY)~~

Letters to the Editor

Chief, W

24 December 1975

TO: [redacted] B

SUBJECT: Cryptolog Article, Oct 75

In one of the gaps which occurred during the holiday season I got to read your "...Proud and Bitter Memories" article. Your message is clear, as are your feelings about the people you worked with (and for). I think you've done a service for those of us here who didn't have much to do with "the problem" by writing that article. It wasn't enjoyable reading, but I'm recommending it to all in W.

[redacted]

P.L. 86-36

cc: Ch, B
Ch, P1
Editor, Cryptolog, P16

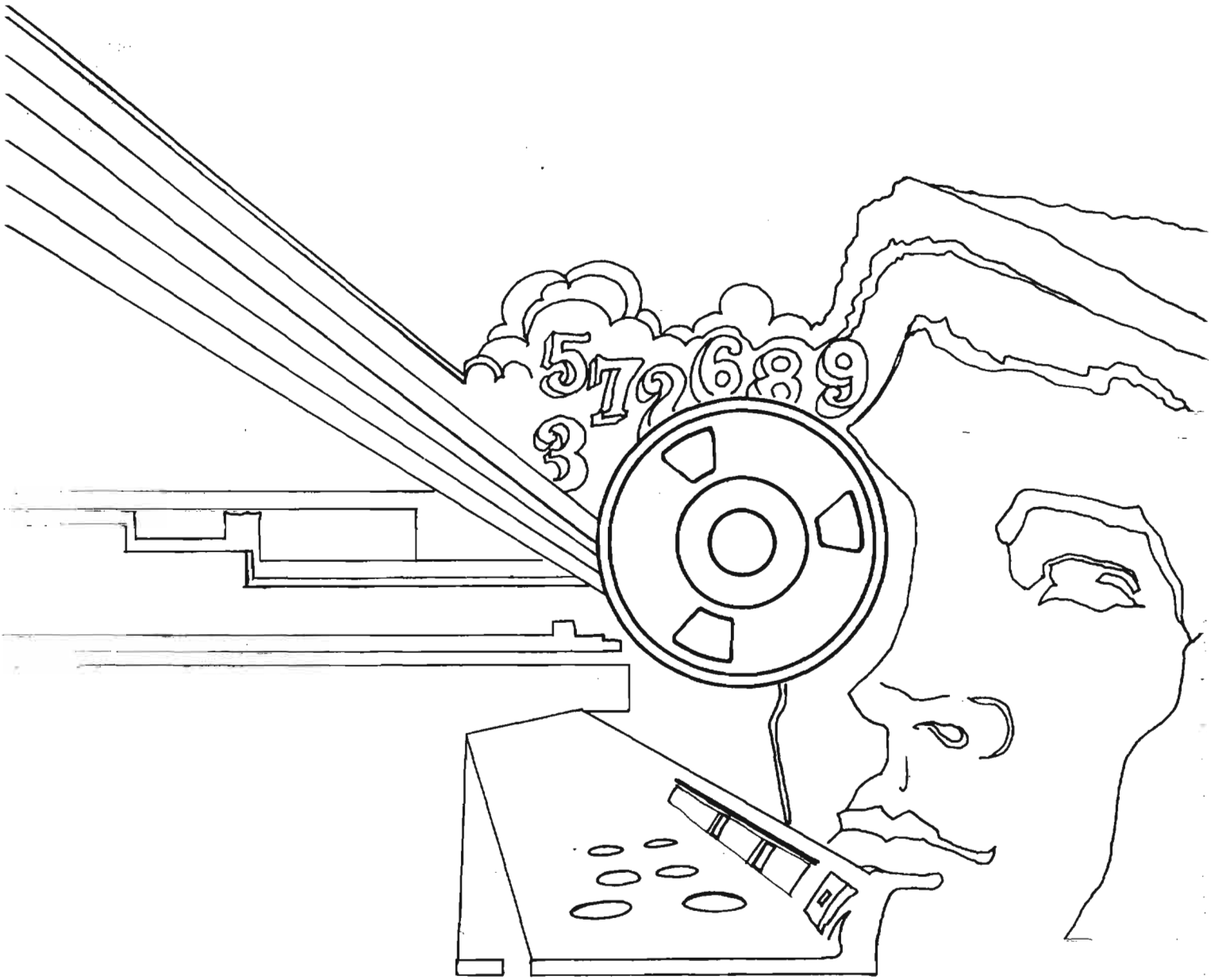
Communications Security Establishment

I very much enjoyed the October issue of Cryptolog, especially [redacted] "Proud and Bitter Memories" and the extract from his "Uncertain Origins" which you put across as a splendid Double-Crostic. Noting that you are obviously very enthusiastic about this kind of puzzle, I am enclosing a copy of a related type which I constructed for fun, but on completion realized was not economically viable, since it is much more difficult and time-consuming to create than to solve. . . I don't think I shall ever construct another one, so this is probably an authentic O'Neill *hapax legomenon*. . .

Kevin O'Neill

Readers who would like a copy of Mr. O'Neill's puzzle may get one by calling the Editor on 5642s.

(UNCLASSIFIED)


5 7 2 6 8 9
3

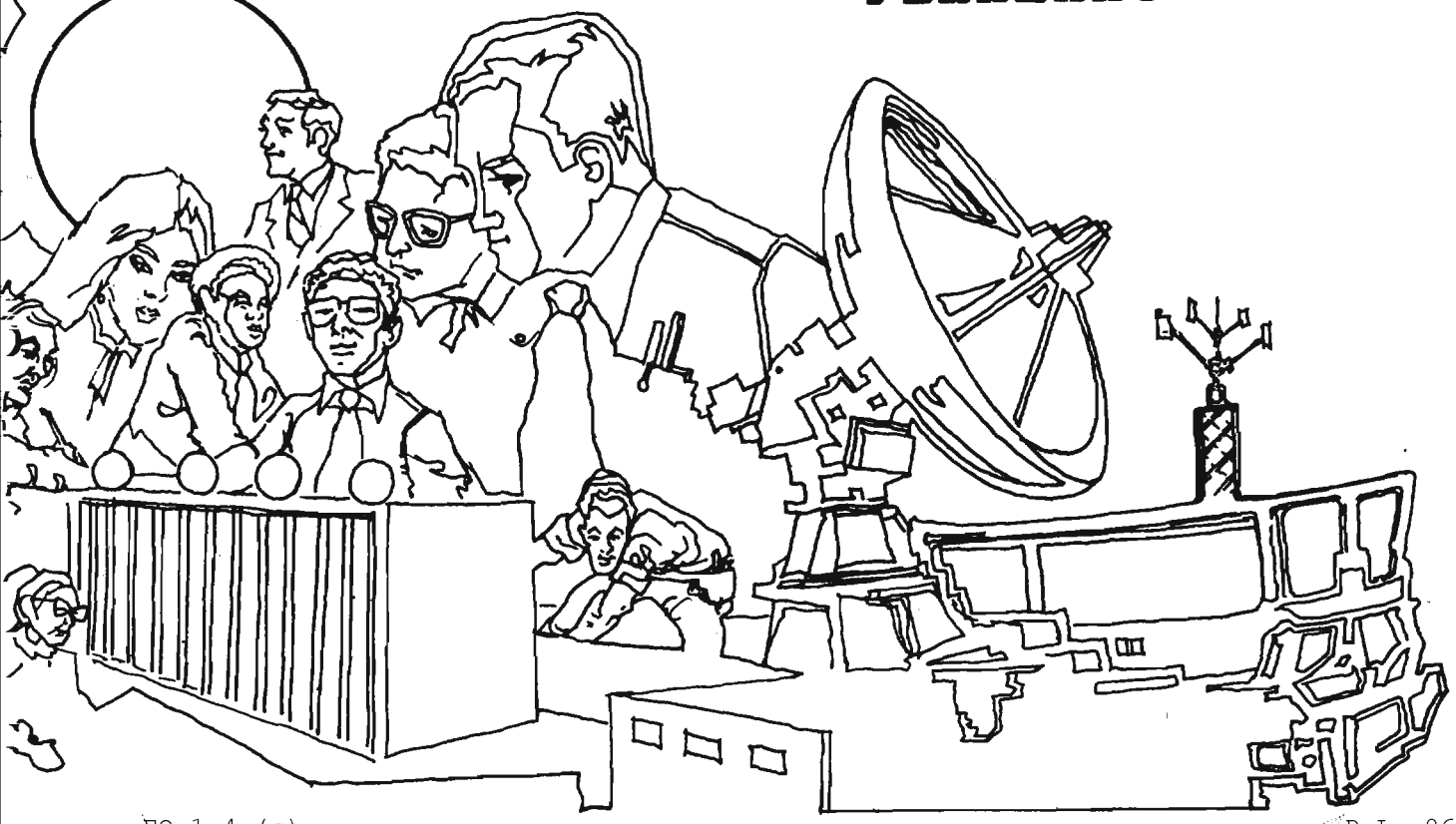
DOCID: 4009729

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

FEBRUARY 1976



EO 1.4.(c)
P.L. 86-36

P.L. 86-36

THE [redacted] SYSTEM..... [redacted]..... 1

WHAT IS CIPHER TEXT?..... [redacted]..... 3

HOW DO WE KNOW IT'S TRUE?..... Vera R. Filby..... 6

EXPLETIVES DELETED: GLOSSING OVER A GLOSSARY..... [redacted]..... 7

THE PREBENDARY AND THE PROPHET..... Reed Dawson..... 13

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009729

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. III, No. 2 FEBRUARY 1976

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief..... Arthur J. Salemme (5642s)
Cryptanalysis..... [redacted] (8025s)
Language..... Emery W. Tetrault (5236s)
Machine Support..... [redacted] (3321s)
Mathematics..... Reed Dawson (3957s)
Special Research..... Vera R. Filby (7119s)
Traffic Analysis..... Frederic O. Mason, Jr. (4142s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4009729

EO 1.4.(c)
P.L. 86-36

THE SYSTEM

P.L. 86-36

The following article on the System originally appeared in the August 1975 issue of NSA/CSS Field Information Letter, the Editor of which has given his kind permission for reprinting it in slightly revised form.

Introduction

Many articles published in CRYPTOLOG deal with collection. Some articles are oriented toward analysis, such as "COMINT Analysis of (September 1974). Others, such as "UNNA: (January 1975), deal with one type of collection system. In today's world of ever-increasing technology, the field of satellite communications and the intelligence produced by that medium continue to expand.

Background of the System

EO 1.4.(c)
P.L. 86-36

[redacted]

ing and message processing, equipment-control information, and tasking priority data.

EO 1.4.(c)
P.L. 86-36

Tasking software

[redacted]

The data base consists of three files. These files contain TEXTA-type information, processing parameters for both signal process-

(Continued on page 12)

[redacted]

DOCID: 4009729

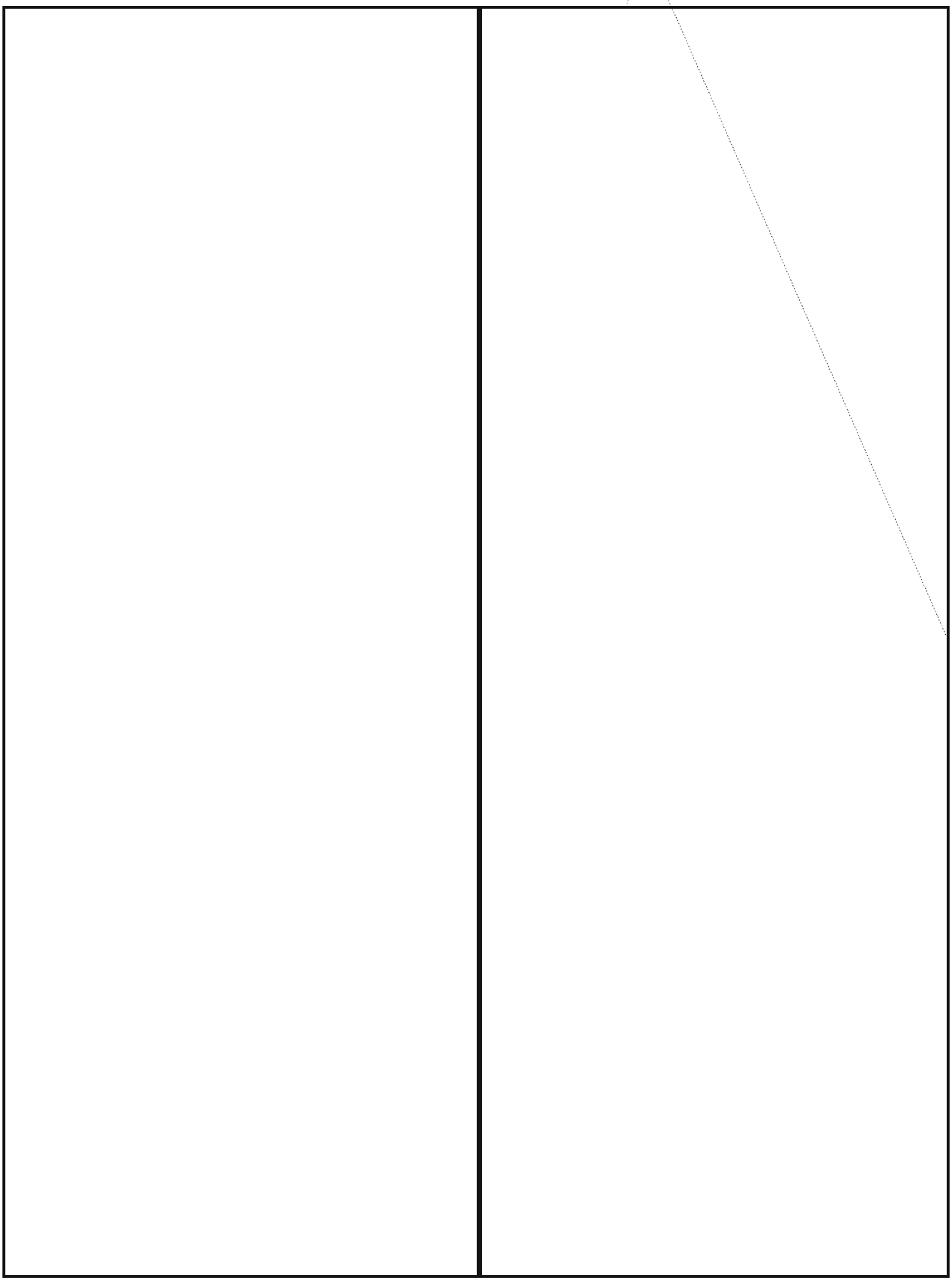
P.L. 86-36

WHAT IS CIPHER TEXT?

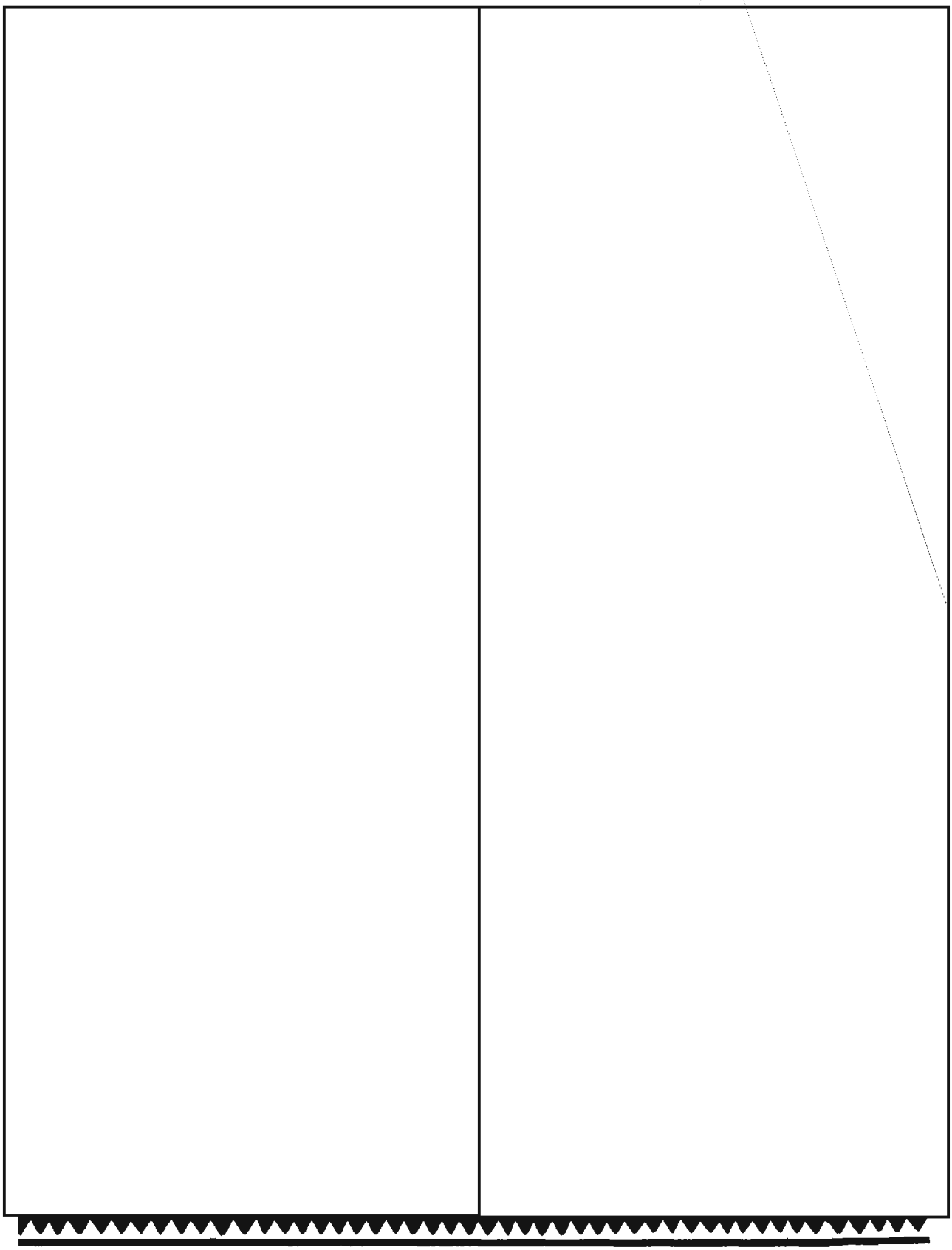
EO 1.4.(c)
P.L. 86-36

DOCID: 4009729

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36



DOCID: 4009729

P.L. 86-36

HOW DO WE KNOW IT'S TRUE?

Vera R. Filby, E12

It was the last day of our first one-week course designed to acquaint DIA analysts with SIGINT and improve their understanding of it. All week long we instructors and our guest speakers, experts from all over the Agency, had been providing these mostly middle-level all-source analysts with a broad view of the whole SIGINT process from collection through processing to reporting and dissemination, thus offering them an opportunity for insight seldom afforded our own middle-level analysts. It was a question-and-answer period following the last lecture on reporting, and one student, probably in his thirties and typical of the class, stood up and said, "Yes, but if it's SIGINT, how do we know it's true?" The question was so unexpected that none of the nonplussed instructors can now remember what kind of answer was offered. The SIGINT people in the room just didn't know what to make of it. After all, to us in the business there is no such question: if it's SIGINT, then it *is* true, by definition. SIGINT is "the enemy speaking," to repeat the familiar phrase.

These DIA classes, which have been given almost every month since August 1974, were organized in response to a recommendation from Dr. Hall, Assistant Secretary of Defense for Intelligence, to provide training for improved exploitation of SIGINT. This recommendation was a result of the Intelligence Community Staff [redacted] which provided evidence that the intelligence community failed to use the SIGINT information available and published in SIGINT reports. In reading the staff study, Dr. Hall concluded that production analysts "need to be cross-trained thoroughly in the use of SIGINT source material, so that they can understand its capabilities and become familiar with the methods of SIGINT analysis, and with the modes and highly specialized terminology of SIGINT reporting."

After that first class, with the "how do we know it's true" challenge from one of its members after we had been pouring out the SIGINT story all week, we continued to get echoes in later classes of the attitude implicit in the question. It must have been the end of the third class before it finally began to seep through to our awareness that some of those readers out there, those "users" of our product, have a perception of SIGINT reality quite different from our own. We began to realize that for at least some of them the world is bathed in an ether infused with false signals emitted just to deceive and mislead, and they seem to have a vision of a cryptologic community immersed in that miasma and vulnerable to its poisons. Once we began to appreciate this perception, we regarded it with a mixture of surprise, amusement, annoyance, and impatience. [redacted] But we felt uneasily that we were not reaching all of the students, not convincing them, not instilling in them the quality of understanding that the course was intended to provide.

On 21 October in the Friedman Auditorium, [redacted] spoke on "SIGINT in Vietnam: Lessons Unlearned" for the CAA. His message brought it home to us that this attitude on the part of some of our users is more than an occasional aberration to be allowed for, ignorance to be alleviated, or, among some in high places, arrogance to be swallowed and endured. It can be lethal. And Tom gave specifics. Among them, the SIGINT evidence of Tet was not believed; it was dismissed as "deception." The SIGINT evidence of the final collapse of Saigon was not believed; it was "deception."

Then maybe it is time for us in the cryptologic community to do something about it. As a start, let us who manage and present the course "SIGINT Exploitation for User Analysts" use the pages of CRYPTOLOG to propose some kind of symposium or conference to bring together all we know about radio deception since the end of World War II. It would not concern so much electronic deception, the techniques of electronic warfare, since that is quite well studied and documented, but would survey all we know about radio deception. Of those who should be invited to participate, we can think immediately of [redacted] who knows the Vietnam story; of [redacted]; [redacted] who has studied the subject intensively and as a member of NFOIO has provided the lecture for the DIA course. Who should sponsor such a conference? We are asking the question; we don't know the answer.

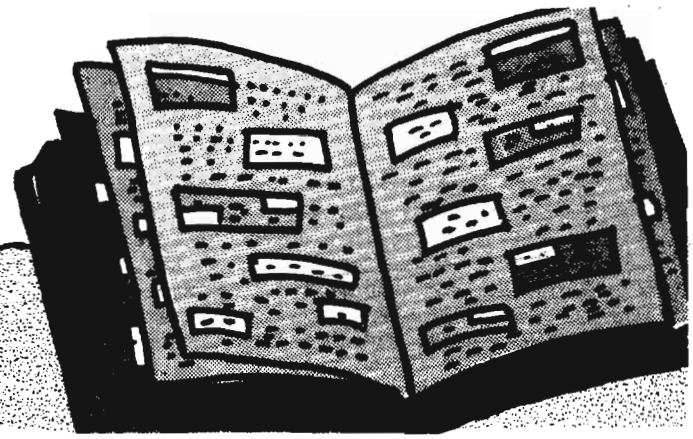
But we do know that a thorough and definitive study of radio deception would be of immense value for two complementary groups of people -- the SIGINT analysts and the users they serve. For the analysts: [redacted] And for the users, the basis for the confidence we have been assuming all these these years they had; the answer to their question, "How do we know it's true?"

P.L. 86-36
EO 1.4.(c)
P.L. 86-36
P.L. 86-36
EO 1.4.(c)
P.L. 86-36

DOCID: 4009729

EXPLETIVES DELETED: GLOSSING OVER A GLOSSARY

[redacted]



P.L. 86-36

Editor's note: The truly professional linguist needs every conceivable specialized dictionary he can get, including dictionaries of "nonstandard" language such as occupational jargon, slang, and even obscenity[1]*. The nonlinguist can easily understand the need for a glossary of the words used, say, by a Russian steel worker, but all he has to find is a single English obscenity in a slang glossary (not to mention an entire book devoted to obscenity) and he is convinced that the linguist is a professional, all right -- a professional Dirty Old Man. In the article that follows, a valuable aid containing several "nasty words" is reviewed by* [redacted] *in a manner that does not alter the linguist's DOM image: there's nothing in it to offend anybody's Aunt Hattie. So read and enjoy!*

P.L. 86-36

The article is a slightly revised version of a talk that [redacted] *presented to the CLA's Special Interest Group on Lexicography (SIGLEX). CRYPTOLOG readers who are interested in the problems of compiling foreign-language glossaries, dictionaries, etc. are invited to attend the Group's regularly-held meetings. For further information, call* [redacted] *SIGLEX Chairman, 5642s.*

* * * * *

Soviet Prison Camp Speech: A Survivor's Glossary. Meyer Galler and Harlan E. Marquess. University of Wisconsin Press, 1972. 216 pp.

Introduction

I'll adhere to the title of this article and refrain from citing any of the obscenities, vulgarities, and curses contained in the book being reviewed. Like the lady who had to jump up onto the bureau and lean out of the window before she could see something to phone the police about, the reader will have to refer to the book himself before seeing anything that offends him. I shall limit myself to the following topics:

- Galler's background and his reasons for writing the book,
- the origin of Soviet prison camp speech,
- the characteristics of Soviet prison camp speech (with examples), and
- the attitudes and prominent features of the daily life of Soviet prisoners, as indicated in their speech.

Galler's background

In 1964 Meyer Galler got the idea of compiling a glossary of Soviet labor camp and prison camp jargon which would be based on his own experiences in Stalin's camps and prisons. The idea came to him while he was reading the reminiscences of other former prisoners, when he realized that such a glossary would be of value to historians, social scientists, students of the Russian language, and the general reader, particularly in the West. Although there had been several occurrences of that jargon in various publications, including Solzhenitsyn's *One Day in the Life of Ivan Denisovich*, no extensive glossary had been published before Galler's book appeared.

Galler was born in Bialystok, Poland, at a time when Poland was part of the tsarist empire. His native language was Russian, which he spoke at home, as well as in elementary school until Russian was supplanted by Polish following the establishment of the independent Polish state after World War I. During World War II, from August 1941 until May 1942, he worked in the Kazakh SSR. One day he was asked to report to the Special Section [NKVD] of the organization where he was working. There he was invited by two NKVD agents to visit the Alma-Ata NKVD office "to clarify certain matters." He was arrested and placed in solitary confinement in Alma-Ata for the 6 months of his investigation. At the end of the investigation, and after exhaustive interrogations, he signed a statement of all charges against him and was

[1] See: A. J. Salemme, "Beyond Webster and All That: Dictionaries of Unconventional Language," *Studies in Intelligence* [CIA], Vol. 13, No. 2, 1969.

DOCID: 4009729

then transferred to a common cell to await trial. In 1943 he was sentenced without trial to 10 years of corrective labor camps on the basis of his alleged "counterrevolutionary activities" (that is, on the basis of his racial and geographic background).

He was soon transferred to a camp near Tashkent, capital of Uzbek SSR, where he dug construction foundations. Then he was transferred to the Aktyubinsk labor camp in Kazakh SSR, where he variously worked in the housing area for "free" employees, in a brickmaking camp, in an agricultural area, and in a penalty lime camp, as well as in the main compound. Later he was reassigned to the old Karaganda camps, or KARLAG, which Solzhenitsyn called "a kingdom larger than France" and which Galler reached by circuitous railroad routes. He was released exactly on the tenth anniversary of his arrest. In 1958 he was permitted to leave the Soviet Union.

Origins of Soviet Prison Camp Speech

Soviet prison and labor camp speech is a substandard variety of Russian, but it is essentially Russian and a distinctive Russian idiom at that. It contains legal and administrative jargon, borrowings from non-Russian Soviet minority languages, criminal argot, obscenities, and, frequently, elements of uneducated peasant speech. Literature containing prison camp speech typically circulates in *samizdat* ("underground press," usually typewritten) editions. *Samizdat* literature often finds its way to the West, where it is first published in translation, but Solzhenitsyn's *samizdat* novel was published in the USSR before its English translation was published as *One Day in the Life of Ivan Denisovich.*

Prison camp speech first began to appear in print soon after the Russian revolution. Early examples of it can be found in the 1920's in the accounts of prisoners who had been released or who had managed to escape and subsequently found their way to the West. The 1930's, particularly the time of the purges (1934-1937), yielded a rather large number of works by former prisoners, some of which are only now being published. Nearly all contain some prison camp speech.

Another group of reminiscences deals with World War II and the postwar period. Many of these accounts were written by Poles who were deported to camps in 1939-1940 and released in 1941-1942 to join the Polish units being formed in the USSR to fight the Nazis. Solzhenitsyn most notably represents the postwar period, not only with *Ivan Denisovich* but also his later works (*The Cancer Ward, The First Circle, GULAG Archipelago*), as well as his play *The Love-Girl and the Innocent,* all of which contain prison camp speech. Another author whose work contains this speech is Anatolij Marchenko, whose book *Moi Pokazaniya* (My Testimony), published in 1969, deals with the post-Stalin penal system.

The number of speakers in the USSR who understand and use prison camp speech is presumably quite large, since vast numbers of persons have had firsthand exposure to it and millions more have been closely associated with someone who has. At any rate, Soviet prison camp speech has been and remains remarkably homogeneous. The bulk of its vocabulary has remained quite constant despite the inevitable changes over the years. And that vocabulary seems to be understood everywhere in the Soviet Union.

Characteristics of Soviet Prison Camp Speech

I mentioned earlier that prison camp speech is not a special language different from Russian, nor even a special regional or social dialect of Russian, but rather a special vocabulary which can be readily incorporated into the speech of any user of Russian. A prisoner arrives in camp with his linguistic habits already formed and these habits are unlikely to change significantly. A college-trained person continues to use a spoken variety of standard Russian, and an uneducated farm worker, for example, continues to use his village dialect. Both persons, however, can easily incorporate into their speech the special vocabulary used in labor camps and prisons.

Since the language we are discussing is overwhelmingly standard Russian, from the standpoint of phonology, morphology, and syntax, it is the lexicon that we must examine in order to find the characteristics of prison camp speech. The authors of the book being reviewed divide their glossary (or lexicon) into five main groups:

- proverbs and sayings,
- abbreviations,
- argot used by the "criminal element" (that is, the nonpolitical prisoners),
- obscenities, and
- various items that do not fit within the first four categories.

Proverbs and Sayings

Prison camp speech, like Russian speech in general, is rich in proverbs, maxims, and similar sayings. Since these sayings frequently refer to such basic concerns as hunger, beatings, and dealings with the established higher authorities, and since it is precisely these concerns that preoccupy the prisoners, they are very popular in labor camps and prisons. Proverbs also provide a picture of the morality and the personal code followed by the prisoners. Although the morality developed under extremely hard conditions leaves something to be desired, we can sympathize with the prisoner who knows that:

Ne ukradësh', ne prozhivësh'.
If you don't steal, you won't make it.

Of course it's too bad that his "making it" contributes to his fellow prisoners' not "making it," but. . .

DOCID: 4009729

Similarly:

Kto kogo smozhet, tot togo i glozhet.
He who can, will swallow you.

Privyknesh'; a ne privyknesh', podokhnesh'.
You'll get used to it; if you don't get used to it, you've had it.

Podokhni ty segodnya, a ya zavtra.
Croak today if you want to, but I'll wait till tomorrow.

Galler has recorded approximately 50 proverbs and sayings of which about a dozen are well-known old ones not restricted to use by prisoners, and about 10 more that seem clearly to be modeled on, or inspired by, older proverbs. Most of the remainder have been originated among the prisoners. The well-known old proverbs and sayings are, in most instances, extremely apt for describing the conditions the prisoners find themselves in. For example:

(In response to a guard's question during search, "What have you got in your pocket?")
V odnom karmane vosh' na arkane, v drugom blokha na tsepi.
In one pocket a louse on a leash, in the other a flea on a chain.

Ehto tol'ko tsvetochki, a yagodki vperedi.
These are only the little flowers; the berries lie ahead. (Meaning, "The worst is yet to come.")

Byla by sheya, a yarmo najdëtsya.
If you have a neck, they'll find a yoke for it. (Frequent ironic reply to new arrivals asking about what kind of work they'll be assigned to.)

Vek zhivi, durakom pomrësh'.
Though you live to be 100, you'll die a fool. (In camps this common expression implies that even the most astute camp inmates cannot rely on their experience.)

To describe the great physical and mental resistance of female prisoners to the rigors of camp life, prisoners use the expression:

zhivuchaya, kak koshka
having nine lives (literally, "living like a cat")

The futility of judicial appeals to Moscow is conveyed in the expression:

Moskva slëzam ne verit.
Moscow does not believe tears. (This is also an example of a proverb which had lost its original significance and fallen into disuse when the capital of the country was moved to St. Petersburg. In the Soviet period, with the return of the capital to Moscow, and when the reversal of a sentence became almost unheard of, the proverb was "revived" and became quite popular once more.)

The eclipse -- at least the official eclipse -- of a formerly popular proverb because of the changed historical and social conditions following the Revolution is noted in the expression:

Zakon, chto dyshlo: kuda povernul, tuda i vyshlo.
The law is like a wagon tongue; it goes wherever you direct it. (The official eclipse stems from the fact that, unlike the situation in the tsarist times, laws are supposed no longer to be administered capricously. The political prisoner knows better, however, and the proverb is thriving in labor camps and prisons with the addition of the adjective *Sovetskij*, "Soviet," before *zakon*, "law.")

Durak rabotu lyubit, i rabota duraka lyubit.
A fool likes work and work likes a fool. (This camp proverb is an expanded version of *Rabota durakov lyubit*, "Work likes fools." The implication of the camp version is that work must be avoided in order to survive.)

Ne padaj dukhom, a bryukhom.
Don't lose your spirit, but your belly. (A possible precedent for this camp proverb, which is used by camp veterans to advise newcomers to keep their courage up and to be prepared to tighten their belts, may stem from *Postis' dukhom, a ne bryukhom!*, "Keep the fast in spirit, and not in the belly!"

Voda mel'nitsy lomaet.
Water wears down mills. (This proverb is quite similar to *Voda kamen' tochit*, "Water wears away stone." The prison camp proverb refers to the harmful effect on the human organism of consuming large quantities of watery soup without any caloric value.)

Many prison camp proverbs appear to follow a standard formula for proverb making. This formula can be represented as:

Byl by A, *a* B *budet*, or
Byl by A, *a* B *najdëtsya.*
If there is A, B will be found. (A and B represent nouns. Gender and number of the verbs may change, depending on which nouns occupy the A and B positions.

One proverb of this type was already mentioned:

Byla by sheya, a yarmo najdëtsya.
If you have a neck, they'll find a yoke for it.

Proverbs formed by the same pattern include:

Byl by chelovek, a delo najdëtsya.
If we get the man, we can find a charge to pin on him. (This proverb may also have been inspired by *Byla by spina, najdëtsya i vina*, "If we get the

DOCID: 4009729

man (literally, 'the person's back'), we'll find out what he's guilty of.")

Byla by kost', a shkura narastët.
If the bone is left, the hide will grow back. (This expression is used by inmates to cheer each other up. It was popular during the war and postwar years, when malnutrition was common in the camps.)

Two proverbs which apparently have no counterparts in standard Russian and which are thought to be of recent prison camp origin are:

Chem dobru propadat', luchshe pust' puzo lopnet.
Rather than waste the good, it is better to let the belly burst. (Implication is that, under camp conditions, everything has to be utilized, even if the results might be harmful.)

Prokuror medved', a khozyain cherpak.
The prosecutor is a bear, but the ladle is your master. (The proverb describes the contrast between the prosecutor or other duly constituted authority, on the one hand, and the necessity of adapting oneself to unwritten camp rules, on the other. Survival in camps means an unceasing struggle for the ladle, that is, enough to eat.)

Abbreviations

Approximately 10 percent of Galler's glossary consists of various abbreviations. These abbreviations are formed in the same manner as abbreviations in standard Russian, and fall into the following categories:

- abbreviations formed from the initial *letters* of the words represented,
- abbreviations formed from the initial *syllables* of the words represented,
- abbreviations formed from a mixture of initial letters and syllables,
- abbreviated *words* consisting of an abbreviated adjective prefixed to an inflectable noun, and
- other abbreviated *words* formed anomalously.

In most instances these abbreviations are pronounced letter by letter, with the stress falling on the last letter. Such abbreviations are usually not inflected, but they usually retain the gender of the abbreviated words (that is, an abbreviation referring to a woman will require the use of a verb with a feminine ending). Examples:

ZhVN (zhena vraga naroda), pronounced "*zhe-ve-en*"
wife of an enemy of the people

KVCh (kul'turno-vospitatel'naya chast'), pronounced "*ka-ve-che*"
culture and education unit. (Despite the feminine gender of *chast'*, this abbreviation is usually considered neuter, as in *KVCh privezlo* [rather than *privezla*] *kinokartinu*, "The KVCh brought in a movie.")

If the initial-letter abbreviation happens to contain a medial vowel that makes the abbreviation pronounceable as a word, the abbreviation is usually inflected and otherwise treated as a masculine singular noun, even if the principal word in the abbreviation is not masculine singular. Examples:

BUR (barak usilennogo rezhima), pronounced "*bur*"
strict discipline barracks

SLON (severnye lagerya osobogo naznacheniya), pronounced "*slon*"
Special-Purpose Northern Camps

VTeK (vneocherednaya trudovaya komissiya), pronounced "*vtek*" (vowel *e* is inserted to make abbreviation pronounceable as a word)
special commission to determine working ability

Z/K (zaklyuchennyj), pronounced "*ze-ka*"
prisoner. (This is the official form of reference and address, both in written statements and in spoken announcements, e. g., *Grazhdane Z/K!*, "Prisoners!" The unofficial abbreviation used among the prisoners themselves is *zehk*, inflected as an ordinary masculine noun.)

Initial-syllable abbreviations

Abbreviations of this type are pronounceable as words and usually inflect as ordinary masculine nouns. Examples:

nachkar (nachal'nik karaula)
chief of camp guards

seksot (sekretnyj sotrudnik)
collaborator. (Literally, "secret co-worker")

Mixed (letter-and-syllable) abbreviations

Such abbreviations which end in a consonant usually inflect as a singular masculine noun. Examples:

GULAG (Glavnoe upravlenie lagerej)
Chief Directorate of Camps

SMERSh (Smert' shpionam!)
Death to spies! (SMERSh was a subsection of the Special Division (1942-1946), an organ of the secret police attached to the Soviet armed forces. SMERSh was in charge of interrogating ex-POWs to determine whether or not they were German spies.)

Such abbreviations which end in a vowel may or may not inflect, depending on stress. Examples:

vokhra (voenizirovannya okhrana)
camp garrison. (E. g., *komandir vokhry*, "commander of the camp garrison.")

vridlo (vremenno ispolnyayushchij dolzhnostej loshadi)
human tractive power, literally "acting

DOCID: 4009729

horse" (Abbreviation *vrid* is standard officialese for "acting," as in "Acting Chief".)

shizo (shtrafnoj izolyator)
special solitary confinement (solitary confinement cell, under the jurisdiction of a special commandant, which is maintained for prisoners being interrogated for crimes committed in camp)

Abbreviated words with abbreviated adjective as prefix

Abbreviated words of this type retain the gender and inflection of the basic noun to which the abbreviated adjective is prefixed. Examples:

sanchast' (sanitarnaya chast')
medical unit (In camp life, the central medical office for a camp district, serving 5 or 6 camp sections.)

nadzorsluzhba (nadzornaya sluzhba)
supervisory service (the camp's supervisory staff)

guzhrabsila (guzhevaya rabochaya sila)
tractive force (generic technical term for all kinds of available tractive power -- mechanical, draft animals, and human)

Other types of abbreviated words

Other types of abbreviated words formed anomalously include:

garantijka (garantijnaya pajka)
guaranteed ration (450-550 grams of bread, not dependent on work quotas, which is given to invalids and certain employees such as office workers and orderlies)

vyshka (vysshaya mera nakazaniya)
death sentence (derived from officialese "highest measure of punishment")

vagonzak (vagon dlya zaklyuchënnykh) (also called *stolypinskij vagon*, "Stolypin car")
prisoners' car (a railroad car for transporting prisoners. Alternate name is derived from name of prerevolutionary Minister of the Interior, Petr Arkad'evich Stolypin, Car is designed to accomodate 8 prisoners, but usually carries 25-28.)

ChSIRovka (derived from official abbreviation *ChSIR = chlen sem'i izmennika Rodine)*
female member of a traitor's family

Criminal argot

Soviet prison camp authorities and the prison inmates themselves divide the prisoners into two categories: criminals proper (the "criminal element"), and political prisoners. The vast majority of the prisoner population consists of political prisoners. These, together with the nonprofessional criminals, are regarded as outsiders by the smaller, tightly organized professional criminal group. The hardened, professional criminals are called *urki* (singular *urka*), or *blatnye* (singular *blatnoj*). The professional criminals are covered by the criminal code and have the rights of criminals. Among themselves they have their own code and customs and, because they are trusted by the Soviet authorities more than the political prisoners, they usually have power and privileges far out of proportion to their limited numbers. Criminals are customarily given the easiest jobs in camp, are assigned to positions of authority over the political prisoners, and they make use of their advantageous position to terrorize and generally victimize the political prisoners, whom they call *frajera* ("pigeons," "dupes").

Since political prisoners were, from the beginning, confined together with the criminals, the special jargon of the criminal soon became the common property of both categories of prisoners. In its earliest form, prison camp speech consisted almost entirely of the criminals' prerevolutionary jargon. But new words and expressions, devised to reflect new conditions in the camps and in Soviet free life, were gradually added to this initial stock of words until eventually they came to outnumber the criminal component.

In prerevolutionary Russian, the criminals' own designation for their argot was *blatnaya muzyka* ("thieves' cant"); more recently it is *fenya*, presumably from an earlier *afenya* or *ofenya* ("peddler") and *afenskaya* or *ofenskaya rech'* ("peddlers' speech"). The expression *botat' po-fene* ("to speak in criminal argot") is also used. Galler's glossary contains more than 100 items that can be positively identified as being of criminal argot origin.

Obscenities

Obscenities, vulgarities, and curses constitute a prominent feature of prison camp speech, but they are probably used no more widely there than among soldiers, students, and workers -- male and female -- and in other groups. But the grim life of prisoners encourages the use of obscenities and abusive speech and is the only form of rebellion to camp conditions which is open to the prisoners. Foul, abusive speech is used equally by camp authorities and sometimes deliberately so by interrogators as one device for breaking the spirit of the prisoner and forcing him to confess to his "crimes." The constant use of abusive speech by overseers and guards seems to be part of a deliberate design to vilify and dehumanize the victims.

This is the part of the glossary I think it is appropriate to gloss over before a mixed readership, but the glossary contains a wide assortment of expletives fully defined and explained with samples of their use. According to the authors of the glossary, none of the obscenities contained in it originated in Soviet camps and prisons, and none of them deal exclusively with

DOCID: 4009729

EO 1.4.(c)
P.L. 86-36

aspects of camp and prison life: most of them can only be regarded as standard Russian obscenities.

Residue

The largest portion of the glossary is made up of forms which are neither proverbs and sayings, nor abbreviations, nor criminal argot, nor obscenities. Most of the items in this residual category consist of entirely new formations for persons, events, institutions, or procedures relating to Soviet camp and prison life. As one might expect, these words are derived primarily from new combinations of Slavic roots and affixes, as well as from changing the meanings of old words. One example of such word formation is the prisoner's word *dokhodyaga* ("a goner"), which is derived from the standard Russian word *dokhodit'* ("to reach, to go as far as, to be exhausted") and the suffix *-yaga* which designates a person.

Grim humor

It becomes clear to the reader of Galler's glossary that no matter how grim and hopeless the prisoner's condition, his sense of humor does not normally fail him. Communist slogans are often a target of the prisoners' wit, although tampering with slogans is dangerous and even in camp a prisoner could be given an additional sentence for that and other infractions.

The following examples are based on the phonetic similarity between the slogan and the parody:

Sotsialisticheskaya bditel'nost'
Socialist vigilance
Sotsialisticheskaya bzditel'nost'
Socialist flatulence[2]

Bytiё opredelyaet soznanie.
Being determines consciousness.
Bitiё opredelyaet soznanie.
Beating determines consciousness.

A kind of ironic encouragement to newcomers to camp may be found in the fact that the soon-to-be-lost belly is referred to as *sotsnakoplenie* ("socialist accumulation"). And, finally, the prisoners' attitude and perhaps their whole philosophy might be summed up in the following refrain:

Pod"ëm budet, ne budi. Razvod budet, ne budi. Obed budet, dva raza budi.
When reveille comes, don't wake me. When time to work comes, don't wake me. When it's dinner time, wake me twice!

[2]Aunt Hattie, don't look this up!

(UNCLASSIFIED)

THE [redacted] SYSTEM

(Continued from page 2)

[redacted]

Summary

[redacted]

~~(SECRET HVCCO)~~

Solution to NSA-crostic No. 2

(CRYPTOLOG, January 1976)

M(ary) R(oberta) Irwin, "(The) Importance of Reading English":

"Every bit of extra knowledge we can acquire may, on some unforeseen occasion, when time is of the essence, save a call to the Central Information Center, a search through reference books, or the use of a stilted phrase because the exactly right word refuses to come to mind."

(UNCLASSIFIED)

沒有问題！

(UNCLASSIFIED)

CLASSIFICATION CORRECTION NOTICE:

In the December 1975 issue of CRYPTOLOG, please change the classification of the article "Graphic Analysis of Linear Recursive Sequences," pp. 6-8, from UNCLASSIFIED to:

SECRET -- HANDLE VIA COMINT CHANNELS ONLY.

(This notice is ~~CONFIDENTIAL - HVCCO.~~)

DOCID: 4009729

THE PREBENDARY & THE PROPHET, or: How to Score Probabilistic Predictions

REED DAWSON, P12

In that old classic of combinatorics "Choice and Chance," the Prebendary (W. A. Whitworth) cautions the reader against gambling, even on fair bets. If a man has a thousand pounds in total fortune, he does not flip a coin for £1000 because the unpleasantness of ruin could scarcely be balanced by the pleasure of a second £1000. Nor would he be wise to hazard any lesser amount continually, for he would, with probability one, go broke eventually. Verily, saith the Prebendary, "the winning of an even wager increases a man's property in less ratio than that in which the losing of the wager decreases it."

The Prebendary evaluates a fortune by its logarithm. Losing half one's fortune balances against doubling the fortune, so he would not risk more than half his fortune on a flip to double it. More generally, he regards a wager as prudent only if the expected increase in the logarithm of his fortune is at least zero. If he doubles his fortune, its logarithm increases by log 2; if he halves his fortune, its logarithm decreases by log 2. Therefore he can make a double-or-halve bet provided he has at least an even chance of winning. He would not flip a coin for a pound because, whatever his fortune f, his expected log fortune after the flip would be

$$\frac{1}{2}\log(f+1) + \frac{1}{2}\log(f-1) =$$

$$\log\sqrt{(f+1)(f-1)} = \log\sqrt{f^2-1},$$

which is less than log f.

But hark! There's the good Prebendary himself, sloshing his way across Foggy Bottom and reflecting on the folly of the denizens, who are inveterate speculators upon the next day's weather. "Fact is," the Prebendary is saying to himself, "it rains an average of every other day here, but none of these chaps has any inkling which. The Verger is no mean prophet with his barometer and charts, but no gambler either. Why don't I use his predictions? Just how good are they?

"Hmm. If the Verger calls for rain (or shine) with some probability p greater than one-half, how much of my fortune might I wager -- at even odds with the local yokels -- on rain (or shine)? If I wager x pounds, then, assuming p, my expected log fortune on the morrow will be

$$E = p\log(f+x) + q\log(f-x), \text{ where } q = 1-p.$$

And, if my calculus fails not, I maximize E by choosing $x = (p-q)f$. Then if I win, log f increases to

$$\log[f+(p-q)f] = \log 2pf = \log f + \log 2p,$$

whilst if I lose, my log fortune dwindles to log f + log $2q$, where $2q$ is less than unity. Therefore the value of the Verger's prophecy is in proportion to the logarithm of double the probability he assigned to what actually happened. I'll wager conservatively and keep tabs on the prophet by scoring him log $2p$ when he's right and log $2q$ when he's wrong."

The moral is that a sequence of predictions on a recurrent two-valued outcome can be scored by averaging log $2x_i$, where x_i is the probability assigned to the occurring outcome. One could, for example, score Louis Allen's probability of rain the following day against the mean daily average probability, or against a Markov model where the transition probabilities between rain and shine are estimated from past records.

If the base of the logarithms is 2 (or the scores are $\log 2x_i/\log 2$ to any base), perfect information, as when $p = 1$ and the predicted event happens, scores unity. If the prophet says $p = 1$ (or 0) and comes a cropper, he scores minus infinity and should be relegated to a brokerage house or campaign committee.

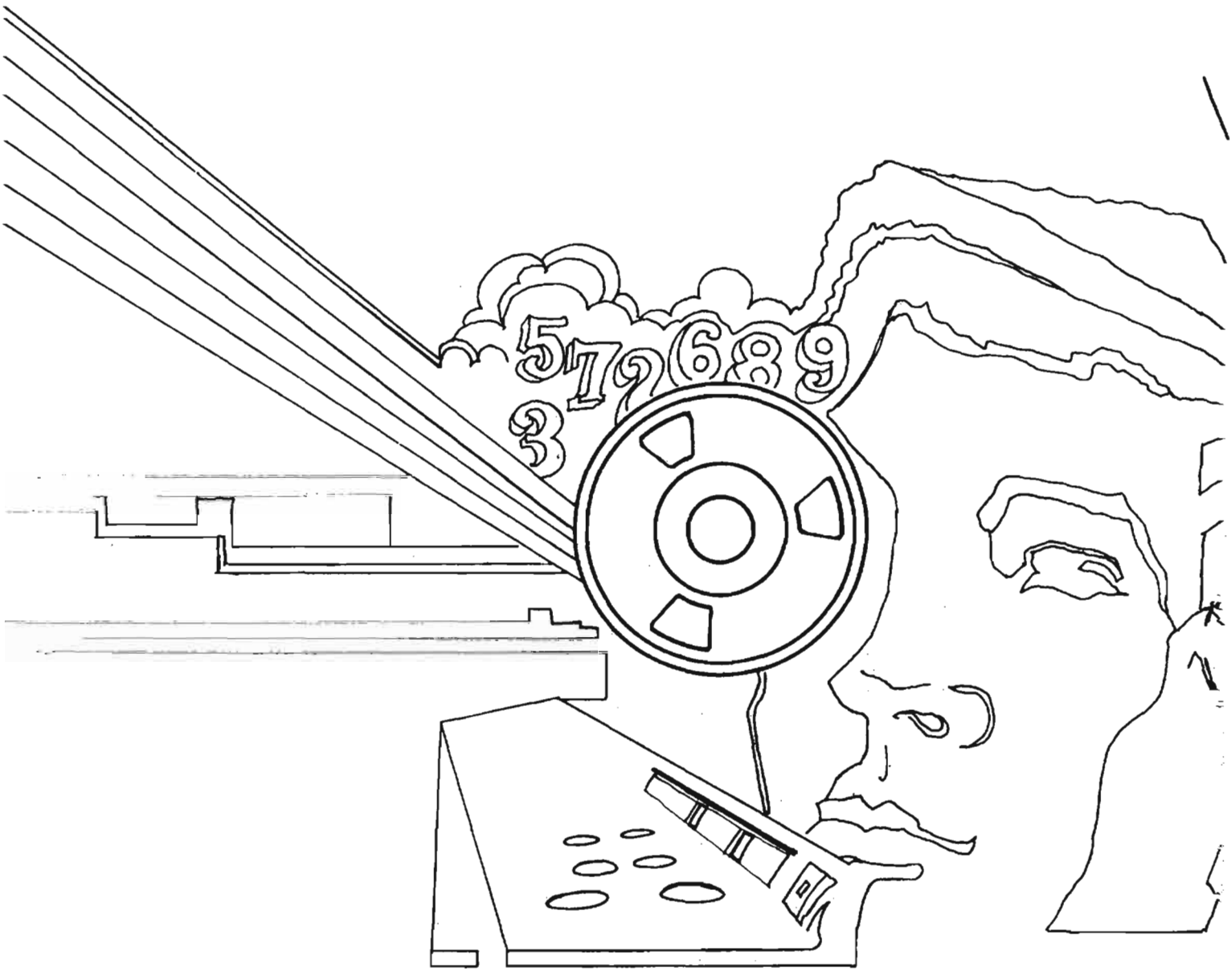
The application is to all fields of prophecy and forecasting, including scoring intelligence assessors who say there's probability p that the Arabs will up the price of oil, q that the Syrians will attack, and z that World War III will start in Angola. If several prophets assign divers probabilities to the same events, it becomes possible to say which prophet is best, and whether the best is any good.

For an economic illustration, suppose the price of gold rises or sinks daily as indicated by the arrows in the chart below, and that prophets A and B assign the prior probabilities of rise given.

Day:	1	2	3	4	5	6	7	8
Prophet A:	.5	.7	.8	.3	.1	.6	.4	1
Prophet B:	.3	.7	.9	0	.4	.4	.2	.9
Price:	↓	↑	↑	↓	↓	↑	↓	↑
A's score:	0	.49	.68	.49	.85	.26	.26	1
B's score:	.49	.49	.85	1	.26	-.32	.68	.85

The average scores are .50 for A and .54 for B. Both are supplying what might be called half-information, but B is the better by an average of 0.04 over this meager sample.

P1-Feb 76-S3-24367


5 7 2 6 8 9
3

DOCID: 4009728

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JANUARY 1976

63 DAYS -- THE SOVIETS IN SPACE.... [redacted] .....1 P.L. 86-36
FOOTBALL AND CRYPTOLOGY..... [redacted] 5
NSA-CROSTIC NO. 2.....6
LENIN AND STATE PRIZES: NOW YOU SEE THEM
-- NOW YOU DON'T!..... [redacted] 8
EDITOR ANSWERS QUESTIONS.....11
LEO IN OCTOBER.....A. I. Murphy.....12

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~
~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

DOCID: 4009728

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. III, No. 1 JANUARY 1976

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief..... Arthur J. Salemme (5642s)

Cryptanalysis..... [redacted] (8025s) P.L. 86-36

Language..... Emery W. Tetrault (5236s)

Machine Support..... [redacted] (3321s)

Special Research..... Vera R. Filby (7119s)

Traffic Analysis..... Frederic O. Mason, Jr. (4142s)

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4009728 P.L. 86-36

63 DAYS --THE SOVIETS IN SPACE

On 24 May 1975 two veteran Soviet cosmonauts, Lieutenant Colonel Petr Klimuk and civilian Vitalij Sevast'yanov, were launched into space onboard a *Soyuz*-type spacecraft from the Tyuratam space center. The next day this *Soyuz*-18 spacecraft successfully docked with a *Salyut*-type space station which had been launched in December 1974 and had been visited in January 1975 by two other cosmonauts. Thus began the longest space flight in the history of the Soviet manned space program -- a flight lasting 63 days.

This long flight set a human endurance record not only for the cosmonauts but also those of us here at NSA and at various field sites who are involved in the collection, transcription, analysis, translation, reporting, and computer programming of cosmonaut voice communications.

Because of the increased activity in this field in the past 2 years, there has been hardly enough time between launches to study the information received and prepare data for subsequent flights. Since September 1973 to the present there has been a total of eight space flights, including the joint Apollo-*Soyuz* flight in July 1975.

The Soviet manned space program began on 12 April 1961 with the successful launch of a *Vostok* spacecraft piloted by the "first man in space," Major Yurij Alekseevich Gagarin. This brief journey into space (the spacecraft made only one revolution around the earth) began a program of space activity which has included the launching of three separate series of spacecraft and one series of space stations. The entire Soviet manned space program, beginning with the *Vostok* spacecraft in 1961 and through the *Soyuz*-19 spacecraft in July 1975, totals 28 flights involving 34 cosmonauts.

Three series of spacecraft

In the first series of spacecraft, the *Vostok* series, from April 1961 through June 1963, there were six flights, two per year, each piloted by a single cosmonaut. The longest flight, *Vostok*-5, lasted 5 days and made 81 revolutions around the earth. The series ended with the launch of *Vostok*-6, piloted by the first woman cosmonaut, Valentina Tereshkova.

The successes of the *Vostok* series led to a second series of spacecraft, the *Voskhod*. There were only two flights in this series. The first one, in October 1964, lasted only one day, but it provided another "first" for the Soviet Union. Instead of a single cosmonaut, three cosmonauts were onboard the spacecraft. This brief flight was repeated in March 1965 with the launch of *Voskhod*-2, piloted by two cosmonauts.

Two years intervened before the launching of the third and current series of spacecraft, the *Soyuz*. From April 1967 through July 1975, 20 *Soyuz* spacecraft were launched, the last one being *Soyuz*-19 during the joint Apollo-*Soyuz* flight. Soviet spacecraft are given a number only if they achieve orbit. A *Soyuz* vehicle launched on 5 April 1975 was manned, but it failed to achieve orbit, had to be aborted, and was therefore unnumbered. This accounts for the latest *Soyuz* being designated *Soyuz*-19.

Space-station series

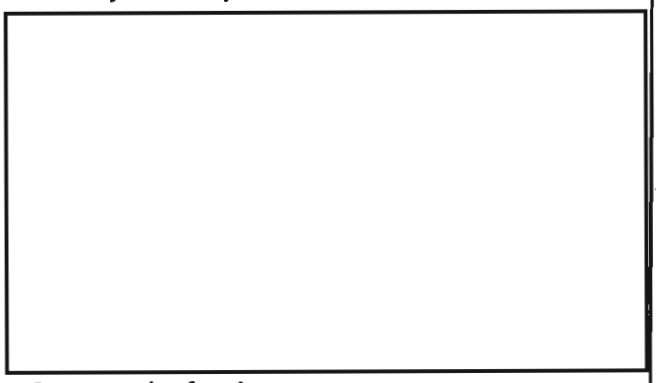
The manned space program came to a halt after 30 June 1971, when the three cosmonauts onboard the *Soyuz*-11 spacecraft died during reentry into the earth's atmosphere after they had spent

DOCID: 4009728

23 days in space onboard the first Soviet space station, the *Salyut*-1. More than 2 years passed before the launch of *Soyuz*-12 on 27 September 1973.

There were four space stations (actually, orbiting scientific laboratories) in the *Salyut* series. The first station, launched in 1971, was visited by the *Soyuz*-10 and *Soyuz*-11 spacecraft. However, only the *Soyuz*-11 crew transferred into the station. In 1973 a second *Salyut* was launched, but it broke up in space before it could be occupied. Then, in 1974, *Salyut*-3 was launched and was visited by two spacecraft, *Soyuz*-14 and *Soyuz*-15. Only the *Soyuz*-14 crew transferred into the station; the *Scyuz*-15 crew failed to dock with the station and had to return home after only 2 days in space.

The *Salyut*-4 space station, launched in December 1974, was the only station successfully occupied by two separate crews -- the first in January 1975 by the *Soyuz*-17 crew, Aleksej Gubarev and Georgij Grechko, and the second in May 1975 by the *Soyuz*-18 crew, Petr Klimuk and Vitalij Sevast'yanov.



Cosmonaut's day in space

The cosmonaut's day in space is arranged to provide 8-9 hours of sleep, four meals a day, 2½ hours of prescribed physical exercises, 1½ to 2 hours of free or personal time, and the remaining time for performing various technical, astrophysical, medical, biological, geophysical, solar, and photographic experiments. Besides this, periodic checks are made on both the space station's and the *Soyuz* spacecraft's propulsion and life support systems.

Each day the cosmonauts consume four meals which they call first breakfast, second breakfast, dinner, and supper. There are about 40 types of food items onboard, consisting of fruit juices, beverages such as coffee and cocoa, various meats and fish, cheese, soups, and candy, cookies, and fruit for dessert. Food is contained in aluminum tubes, small cans, and plastic wrapping (some of which is edible) and is stored in a small refrigerator or special food containers. There are also food warmers for heating the meats and soups and other food items.

Physical exercises are required every day to maintain muscle tone and to combat the harmful effects of a weightless environment. The 2½ hours of required activity is spread out through the day. In the exercise area there is a treadmill or "running track" on which the cosmonaut can walk or run. Special exercising suits called "Penguin" and "Athlete" are worn and are so constructed that they exert a stress on various body muscles. The suits have elastic cords which connect from the cosmonaut's belt to the treadmill, thus creating an additional stress on the body. Other exercising equipment includes a special wheelless bicycle, a chest-pull device, and an exercising bar.

At regular intervals among the many days of intensive work on the required experiments and medical tests, there are days that are designated a "day of rest." In addition to the daily exercises and medical tests that are required even on "days off," the cosmonauts still have plenty to do: they must organize the results of their investigations of the previous day's work, clean the space station with a special vacuum cleaner called *Raketa*, and fill waste containers with used paper, empty food tubes, and other garbage for later ejection through their "garbage chute." Only then can they relax by reading some of the books in their small library or by listening to music on prerecorded tapes.

P.L. 86-36
EO 1.4.(c)

Experiments in space

Several biological experiments were conducted by the *Soyuz*-18 crew to study the effects of weightlessness on the growing of plants, the embryological development of amphibians, and the genetic development of insects. Special biological incubators called "biotherms" contain microorganisms, fruit flies, animal tissue cultures, frog eggs, and algae. In a space greenhouse called "Oasis," several plant varieties such as the pea and onion are grown from seeds in artificial soil. The plants are watered automatically and their development is photographed by a special movie camera.

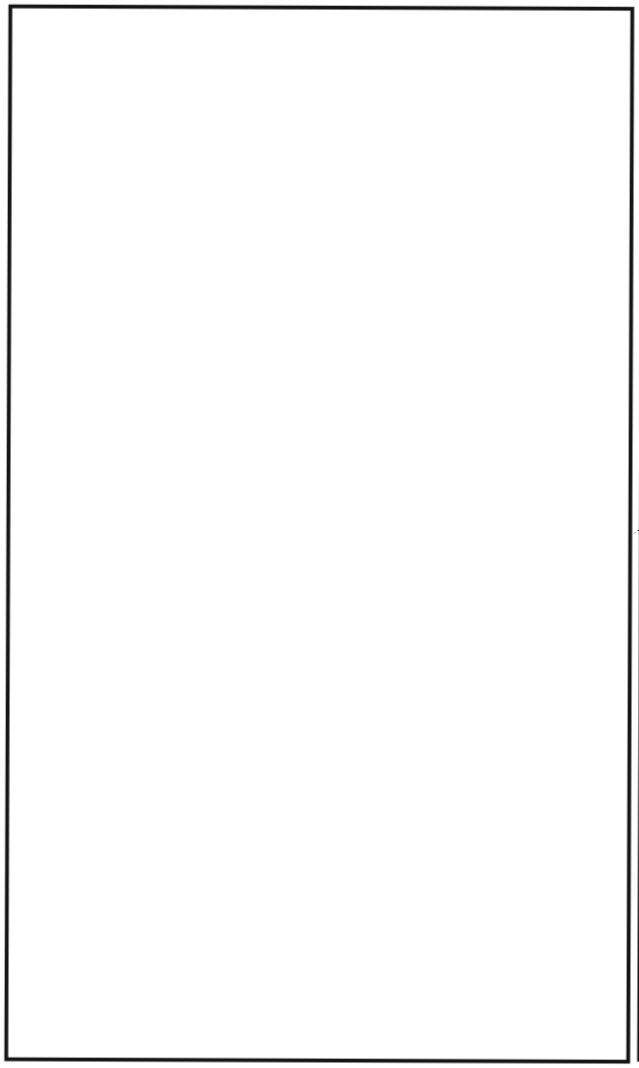
Medical experiments and tests are very important for studying the effects of weightlessness on the body under conditions of a prolonged stay in space. The cosmonaut's health is a major concern on any space flight and his physical and mental condition must be monitored daily. A special onboard medical device called *Polinom* is used to measure such things as pulse rate, respiration, and cardiovascular functions. Throughout the flight, certain days are designated "medical monitoring days" on which a series of medical tests and experiments are conducted. Blood samples are taken for later laboratory analysis; the reaction mechanism and adaptive abilities of the brain's blood circulation system are studied by using a medical apparatus called *Levkoj;* ultrasonic measurements of the density of bone tissue are

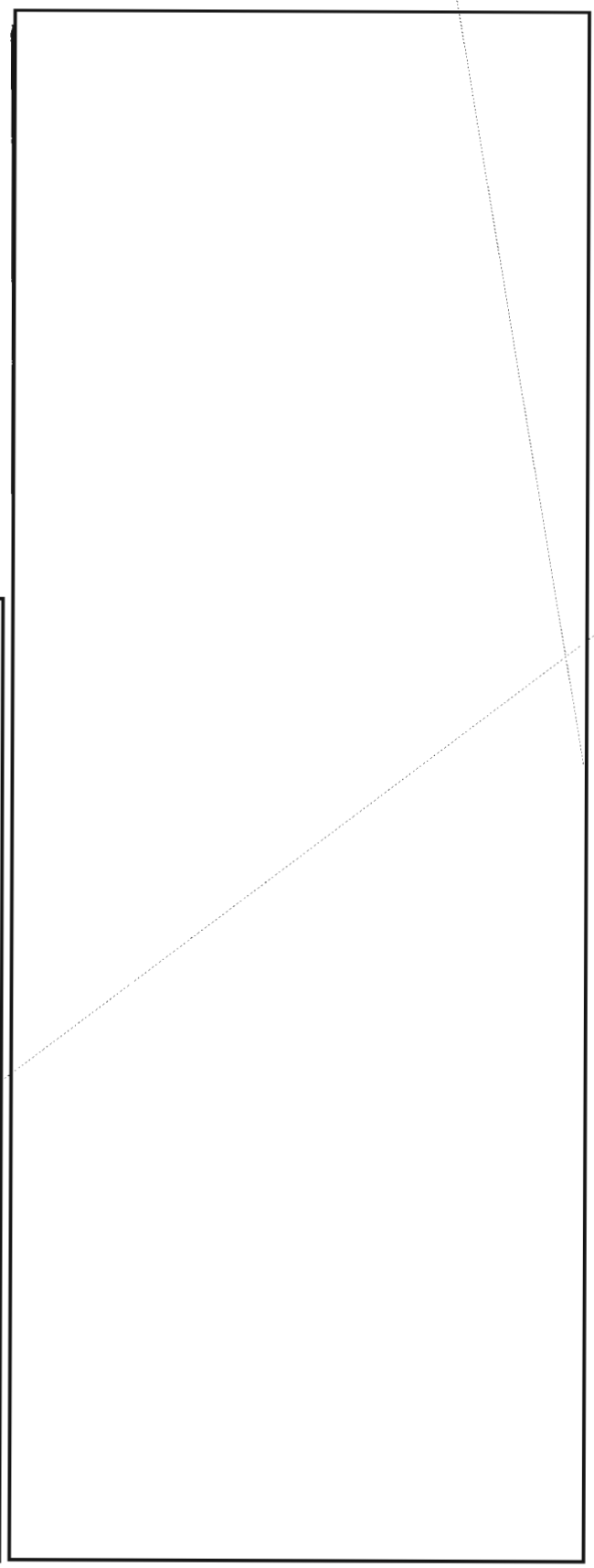
DOCID: 4009728

EO 1.4.(c)
P.L. 86-36

made on the *Plotnost'* instrument. The *Tonus* is an instrument for the electrical stimulation of muscles; the *Rezeda* is a medical apparatus for studying pulmonary ventilation and for taking breath samples for later laboratory analysis. Along with the names of these medical monitoring devices, the cosmonauts use many abbreviations to indicate the recording of various arterial pressures. For example, *PBA*, *PLA*, and *PSA* sensors record femoral, radial, and carotid artery pulses. Besides the standard electrocardiograms, other cardiovascular recordings are made; in voice communications they are referred to by the abbreviations *KKG*, *FG*, *TO*, *SFG*, and *SKG* (kinetocardiogram, phlebogram, tachooscillogram, sphygmogram, and seismocardiogram, respectively).

While all this medical data is extremely important for studying the cosmonaut's physical condition, the mental state of each cosmonaut is also studied by a psychoneurologist at the Flight Control Center, who makes a psycholinguistic analysis of the cosmonauts' speech to help evaluate the crew's state of health.





P.L. 86-36
EO 1.4.(c)

DOCID: 4009728

EO 1.4.(c)
P.L. 86-36

P.L. 86-36
EO 1.4.(c)

Sometimes the cosmonauts themselves do not always remember what an abbreviation means. But this is also true of American astronauts. Compare the following actual conversations:

Houston Mission Control (after discovering a malfunction in the Apollo-12 mission caused by the *d*igital *u*plink *a*ssembly, DUA):
We think we've figured it out.
Your DUA was off.
American astronaut: What's a DUA?

- - - - -

Soviet Flight Control Center: We have an addition to the format: on 19 June the flight engineer is to conduct M10-4M, FG 1/3.
Klimuk: What, what?
FCC: FG 1/3.
K: What's that?
FCC: Phlebogram [in Russian *FleboGramma*].
K: Ah, phlebogram! I understand.

P.L. 86-36
EO 1.4.(c)

DOCID: 4009728

FOOTBALL & CRYPTOLOGY

P.L. 86-36

P1/R51 Cadre

Now that we are in the middle of another National Football League season, I believe the time has come to consider ways to improve the game. One of the most painful things to watch is mistakes due to incomplete knowledge by the players, e. g., the receiver hit in the back by a pass, the linebacker who does not see the blocker coming at him from the side, or the guard missing the blitzer. How often coaches must have wished they could have told a player to look in another direction at the critical moment.

Modern technology does offer a way to correct this state of affairs. What the NFL needs is to allow low-power radio transmitter to enable coaches to speak directly to their players (who would have miniaturized receivers and earphones in their helmets)[1]. Then the coach would be free to say, "Get that (expletive deleted) man to the (expletive deleted) left, you (expletive deleted) meathead!" If nothing else, it should make the coaches feel a lot better.

Of course, opposing coaches would probably try to listen in. But if the technique were only used in the simple way described above, that would not be of much value (not enough time to react). However, I think coaches would find the temptation irresistible to call plays in this way. Naturally, in this case a SIGINT effort would be of tremendous value to the opposition. Therefore one would have to use encrypted speech. It is possible to envision this happening in several stages. . .

1976 season

The New York Giants win the NFC title (after having gone 3-10-1 in 1975) by employing a speech privacy system to enable the coaches to talk directly to their players. As used by the Giants there are 11 speech coaches assigned to each unit, one coach to each player. In addition the head coach can override any line. Unfortunately, in the league championship game, Craig Morton gets tired of taking orders from his coach. He disconnects his receiver. The Giants lose 63-13 to the Oakland Raiders.

1979 season

By this time most teams have installed a system similar to the Giants'. In addition many teams have hired mathematicians to design new encryption devices and to break those of other teams. The Kansas City Chiefs have decided that there is no longer any need to hold huddles or even to let players talk at all. Each player is entirely encased in a combination of medieval armor and space suit. In this way each player can breathe pure oxygen. Besides speaking to his players the coaches can also activate switches to give each a squirt of Gatorade or a shot of adrenalin. After each play the Chiefs line up without huddling and the coach tells them what to do. The effect on the other teams is devastating. Without a chance to regroup (or breathe oxygen) they quickly collapse. The Chiefs win every game this year by at least 40 points.

1984 season

By this time the cryptologic aspects of football have become at least as important as the play itself. Every team has many mathematicians, engineers, and programmers designing and breaking speech systems. In many cases their salaries are greater that those of the players. One of the latest technical breakthroughs has been the emplacement of brain probes (which are in turn connected to the receiver in the helmet). In this way the coach can send directly to the brain. A whole new field of cryptoneurology is born. Using this latest technique, the L. A. Rams are able to play gorillas at a number of positions.

1999 season

By this time the NFL has concluded that the players are pretty uninteresting. In fact, live players spoil the game because of their unpredictable variance. All teams use robots which are guaranteed to be uniform with respect to position. The whole point of the game is cryptanalysis. The sports pages of the papers are full of discussions of such things as which team has managed to break the Detroit Lions' defensive system. Every year a big draft is held to select mathematicians and engineers. One man is reported to be under contract for $32 million over 7 years. Hmmmm. . . .

[1] I understand this idea was actually tried some years ago, but abandoned for various technical reasons.

DOCID: 4009728

NSA-crostic No. 2

The quotation on the next page was taken from a published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS	*WORDS*
A. Mohammed's birthplace	217 78 118 31 162
B. "Sour herb of grace" (Shakespeare, *Richard II*)	111 135 54
C. Conceive	165 22 143 173 97 45
D. He said "Cogito, ergo sum" (2 wds)	138 1 67 119 220 79 151 100 188 35 131 203 158
E. What Sheldon's mother said when he tried to push ahead of Sister Mary Margaret as she was signing the Mount Vernon guestbook (6 wds, suggested by song title)	25 105 72 197 154 34 93 20 183 98 89 117 205 63 163 194 23 219 125 174 65 122 191 166 5
F. High flyer	61 129 90 172 157 80
G. "He always takes his girl friends to Alaska -- that's how he gets to ----"	55 74 112 139
H. Mother of Epaphus by Zeus	218 56
I. Historical antecedent (Waterloo, 1815) of Word Y (3 wds)	44 212 164 201 3 91 28 37 147 202 152 17 47 101
J. Praise extravagantly	170 180 75 10
K. French composer (*Tales of Hoffmann*)	148 140 109 21 29 176 124 57 77
L. Artistic style early in the reign (1715-74) of Louis XV	142 160 58 149 84 110
M. Civil wrong independent of a contract	76 216 128 8
N. King of ancient Persia, d. 425 B.C.	30 50 121 113 12 66 133 187 71 73
O. Element, atomic number 10 (symbol)	83 36
P. Language for which Sequoyah invented a syllabary	27 184 141 14 43 150 53 99
Q. Psyche's boy friend	156 104 40 86
R. Lummox	210 38 161
S. Some at least	204 26 198
T. Mechanical device (Karel Capek, *R.U.R.*, 1921)	123 49 6 199 68
U. Vase-shaped pitcher	159 19 168 153
V. Discharge completely	87 178 32 46 107 13

DOCID: 4009728

W. Festive get-together

X. American composer (*Third Symphony*, Pulitzer Prize 1947)

Y. Did McAuliffe *really* say this at Bastogne?

Z^0. Garden near the foot of the Mount of Olives

Z^1. Charitable

Z^2. Lower

Z^3. Old Man of the Mountain (3 wds)

Z^4. Sign of the Zodiac

Z^5. Yen

Z^6. Russian composer (*The Golden Age, Lady Macbeth of Mtsensk*)

Z^7. U. S. government agency (abbrev)

169 62

115 2 146 81

102 33 95 206

195 51 167 132 60 186 70 15 108 175

185 106 177 11 213 96 208 39 144 92 200 192

41 126 209 155 82 193

136 4 85 59 215 181 103 18 120 214 48 179 189

24

94 207 134

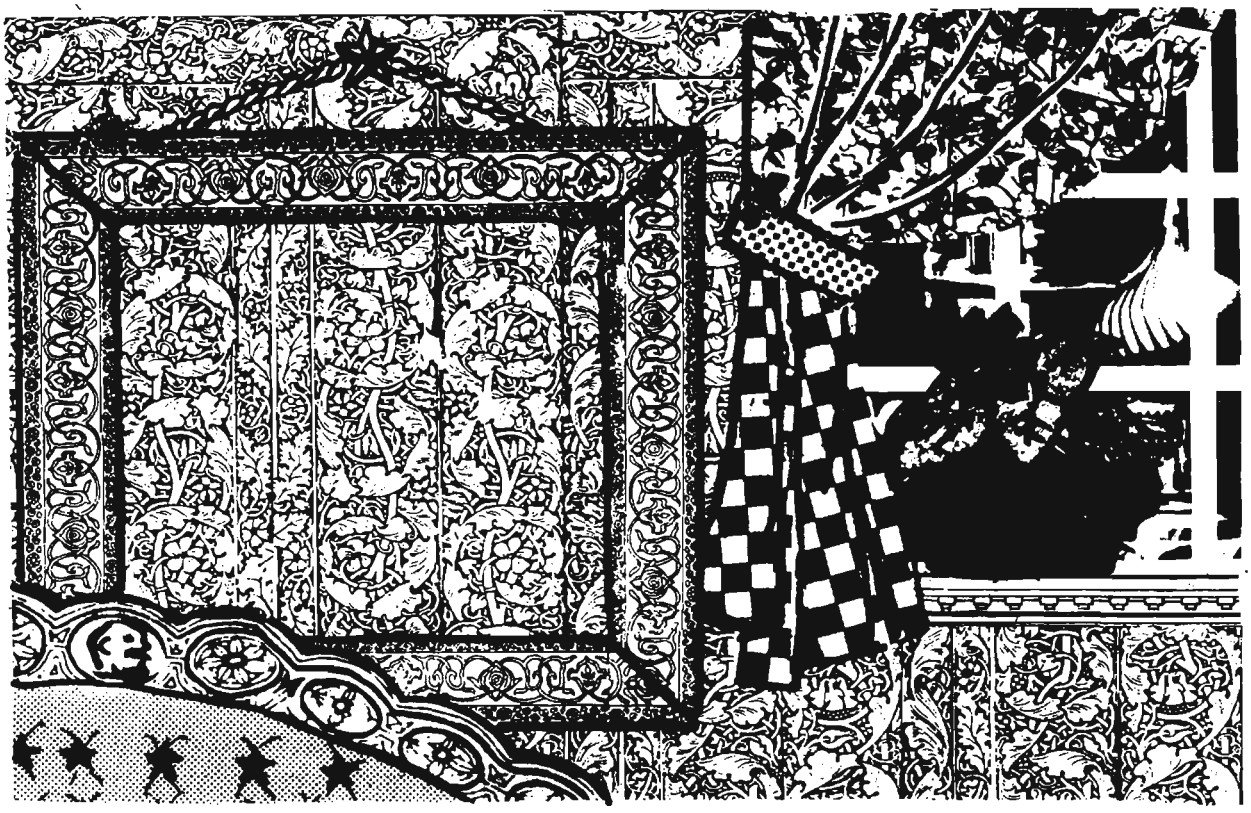
7 114 145 196

42 130 9 52 190 127 16 116 88 69 211 171

137 182 64

1-D	2-X	3-I	4-Z^3	5-E		6-T	7-Z^5	8-M		9-Z^6	10-J		11-Z^1	12-N	13-V
14-P	15-Z^0		16-Z^6	17-I	18-Z^3	19-U	20-E	21-K	22-C	23-E	24-Z^3		25-E	26-S	
27-P	28-I	29-K		30-N	31-A	32-V	33-Y	34-E	35-D	36-O		37-I	38-R	39-Z^1	
40-Q	41-Z^2		42-Z^6	43-P	44-I	45-C		46-V	47-I	48-Z^3	49-T	50-N	51-Z^0	52-Z^6	53-P
54-B	55-G		56-H	57-K	58-L	59-Z^3	60-Z^0	61-F	62-W	63-E		64-Z^7	65-E	66-N	67-D
	68-T	69-Z^6	70-Z^0	71-N		72-E	73-N		74-G	75-J		76-M	77-K	78-A	
79-D	80-F	81-X	82-Z^2	83-O	84-L	85-Z^3		86-Q	87-V	88-Z^6	89-E		90-F		91-I
92-Z^1	93-E	94-Z^4		95-Y	96-Z^1		97-C	98-E	99-P		100-D	101-I	102-Y	103-Z^3	104-Q
105-E	106-Z^1		107-V	108-Z^0	109-K	110-L	111-B	112-G	113-N	114-Z^5	115-X	116-Z^6	117-E		118-A
119-D	120-Z^3	121-N	122-E	123-T		124-K		125-E	126-Z^2	127-Z^6	128-M	129-F	130-Z^6		131-D
132-Z^0	133-N	134-Z^4	135-B	136-Z^3	137-Z^7		138-D	139-G	140-K	141-P	142-L	143-C	144-Z^1	145-Z^5	146-X
	147-I	148-K	149-L	150-P	151-D		152-I	153-U		154-E	155-Z^2	156-Q		157-F	158-D
159-U		160-L	161-R		162-A		163-E	164-I	165-C	166-E	167-Z^0	168-U	169-W		170-J
171-Z^6	172-F	173-C	174-E	175-Z^0		176-K	177-Z^1	178-V	179-Z^3	180-J	181-Z^3	182-Z^7		183-E	184-P
185-Z^1		186-Z^0	187-N	188-D	189-Z^3	190-Z^6	191-E	192-Z^1		193-Z^2	194-E	195-Z^0	196-Z^5	197-E	
198-S	199-T	200-Z^1	201-I		202-I	203-D	204-S	205-E	206-Y	207-Z^4	208-Z^1		209-Z^2	210-R	
211-Z^6	212-I	213-Z^1	214-Z^3		215-Z^3	216-M		217-A	218-H	219-E	220-D				A.J.S.

DOCID: 4009728



LENIN AND STATE PRIZES: NOW YOU SEE THEM -- NOW YOU DON'T!

C531

P.L. 86-36

Orders, medals, and prizes play an important role in the economic and social life of the Soviet Union. They provide an extra incentive for people to strive for improvement, by appealing to their natural desire for recognition and approval and, in the case of Lenin and State Prizes[1], by rewarding them financially.

In the civilian sector, the most prestigious of these are the Hero of Socialist Labor, Order of Lenin, State Prize, and Lenin Prize. They form the bottom line of official biographic sketches and obituaries -- the measure of a person's success as a productive member of society, and a great source of personal pride. To students of Soviet affairs, they can be a measure and source of other things as well.

While all these honors are highly prized by Soviet citizens, the Lenin and State Prizes are the most difficult to obtain. The Order of Lenin and Hero of Socialist Labor may be awarded for a wide variety of reasons unrelated to any single achievement (e.g., on the occasion of one's fiftieth birthday and in appreciation of years of consistently outstanding performance), but the Lenin and State Prizes are given only for very specific contributions of national significance, such as the design and introduction into series production of a new type of aircraft. Consequently, recipients of the Lenin and State Prizes, more than any other group, may be considered the elite corps of the "technocrats."

Just what *are* these prizes? According to the new (third) edition of the *Bol'shaya Sovetskaya Ehntsiklopediya* (Large Soviet Encyclopedia) (BSEh), the Lenin Prize is "one of the highest forms of rewarding citizens for the most outstanding achievements in the field of

[1]Unless otherwise stated, references to State Prizes in this article do not include the former Stalin Prizes, which were discontinued after 1954 and retroactively redesignated State Prizes. State Prizes awarded by individual republics of the USSR (as opposed to national-level USSR State Prizes) have also been excluded from consideration in this article because they are less significant and are of more recent origin.

DOCID: 4009728

science and technology, literature, art and architecture. . . Re-established in 1957[2]. . . 30 Lenin Prizes (including 25 in science and technology and 5 in literature, art, and architecture) of 10,000 rubles each are awarded once every 2 years. . . [Announcements of] awards are published on the anniversary of the birth of V. I. Lenin. Persons receiving the Lenin Prize are given the title 'Lenin Prize Laureate,' a certificate, an honorary pin, and an identification card. The Lenin Prize may not be awarded more than once to an individual."

The same edition of BSEh states that "USSR State Prizes are a form of rewarding citizens for outstanding achievements in the field of science and technology, literature, and art. . . They are awarded for scientific research making a major contribution to the development of the nation's science; for work creating and introducing the most progressive materials, machines, and machinery into the national economy. . . A USSR State Prize Laureate may be awarded a USSR State Prize more than once, but not within 5 years of any previous award. Established in 1966. . . as many as 50 awards in the field of science and technology and as many as 10 for literature and art are made yearly on the anniversary of the Great October Socialist Revolution. Each prize is 5000 rubles. . . Persons receiving the USSR State Prize are given the title 'USSR State Prize Laureate,' a certificate, and an honorary pin indicating the year of the award. . ."

A prize may go to an individual, as sometimes happens in the field of pure science, for the development of basic theories. More often, however, the prize is shared by a number of persons throughout the USSR, especially when the award is for the development and production of complex and sophisticated equipment. On the average, prizes are shared by seven or eight persons. Prizes are announced in *Pravda* and *Izvestiya*, with an indication of the recipient's name, job title, place of employment, and reason for the award.

According to published accounts, in the fields of science and technology since 1970, 226 people have shared 32 Lenin Prizes, while 1,057 people have shared 126 State Prizes. But according to BSEh, there should have been 75 Lenin Prizes, and 250 State Prizes could have been awarded. Where have all the prizes gone?

[redacted]

The following figures help to elucidate the nature and scope of the problem:

- In 1970, 49 Lenin Prize Laureates were elected to the USSR Supreme Soviet. [redacted]
- The Ukrainian Academy of Sciences was given the Order of Lenin in 1969 and celebrated the occasion with the publication of *Akademiya Nauk Ukrainskoj SSR 1969 g.* (Academy of Sciences, Ukrainian SSR, 1969), which identified 48 colleagues of the Academy as Lenin Prize Laureates. [redacted]

[redacted]

[2]Originally established in 1925, Lenin Prizes were discontinued after 1934. From 1957 until 1968, Lenin Prizes were awarded yearly.

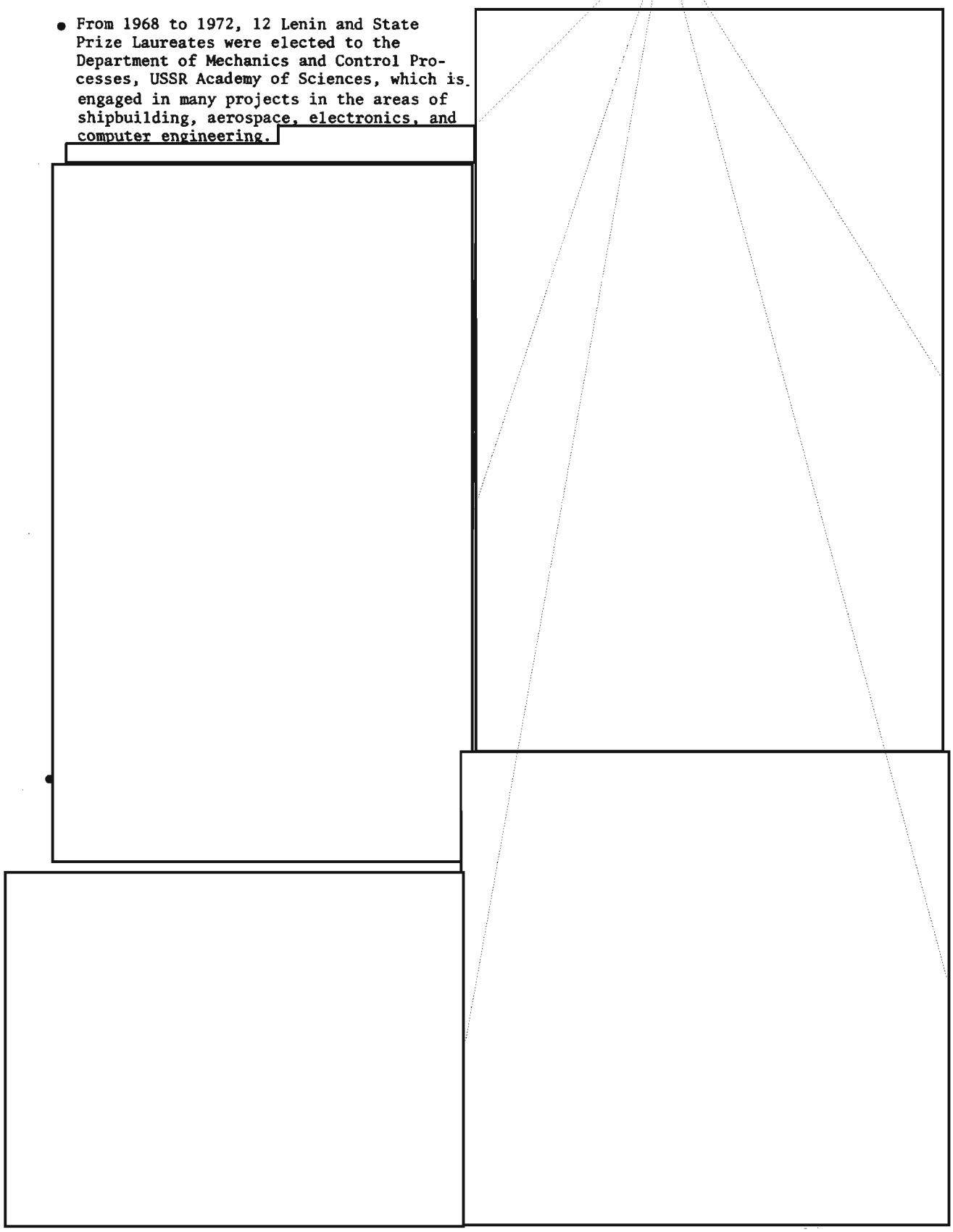
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4009728

EO 1.4.(c)
P.L. 86-36

- From 1968 to 1972, 12 Lenin and State Prize Laureates were elected to the Department of Mechanics and Control Processes, USSR Academy of Sciences, which is engaged in many projects in the areas of shipbuilding, aerospace, electronics, and computer engineering.



DOCID: 4009728

EO 1.4.(c)
P.L. 86-36

Q:
A:

The following are a few of the questions most frequently asked of the editor. The answers are supposed to be simple but complete. Other frequently asked questions, including some that require more detailed discussion, will appear in future issues. These other questions include, "Who can contribute articles to CRYPTOLOG?", "What topics are suitable for discussion in CRYPTOLOG?", "How much editing does the editor do to articles submitted?", "Why does the editor have to do *any* editing?", "Are controversial articles acceptable?", etc.

How does CRYPTOLOG differ from other Agency publications such as the NSA Technical Journal, Cryptologic Spectrum, and the NSA Newsletter?

The Newsletter is, of course, unclassified. The Technical Journal, Spectrum, and CRYPTOLOG can print classified materials (Technical Journal and CRYPTOLOG up to Top Secret Codeword level; Spectrum up to Secret Codeword level). Technical Journal and Spectrum are professionally-printed publications that appear 4 times a year; CRYPTOLOG is a more casually produced (pasted-up typewritten copy) technical exchange paper that appears every month. With respect to the content of the articles printed, the three classified publications are directed at approximately the same NSA readers, but CRYPTOLOG is perhaps the most time-conscious and has perhaps the least formal level of presentation, since it is intended for the easy exchange of ideas among technicians of various specialties.

Why don't you print all the unclassified stuff on both sides of the same page, so that it can be removed easily without a risk of a breach of security?

CRYPTOLOG is deliberately left unstructured. It contains no "TA Section," "CA Section," "Language Section," etc. The intention is to make every reader, whatever his specialty, want to read every article in every issue (are we hitting the mark?). It often happens that articles of various lengths and with various security classifications leave variously-sized holes to fill in. Sometimes it is possible to find "filler" material with the same classification as the article on the rest of the page, and also on the back of the page. But usually this is impossible. Therefore, we put an indication of the security classification on everything printed in CRYPTOLOG. Any reader can reproduce any article or "filler" and be sure of the classification. Making a Xerox copy of an unclassified page is safer than tearing out the page and worrying about what's on the reverse side.

Who can subscribe to CRYPTOLOG?

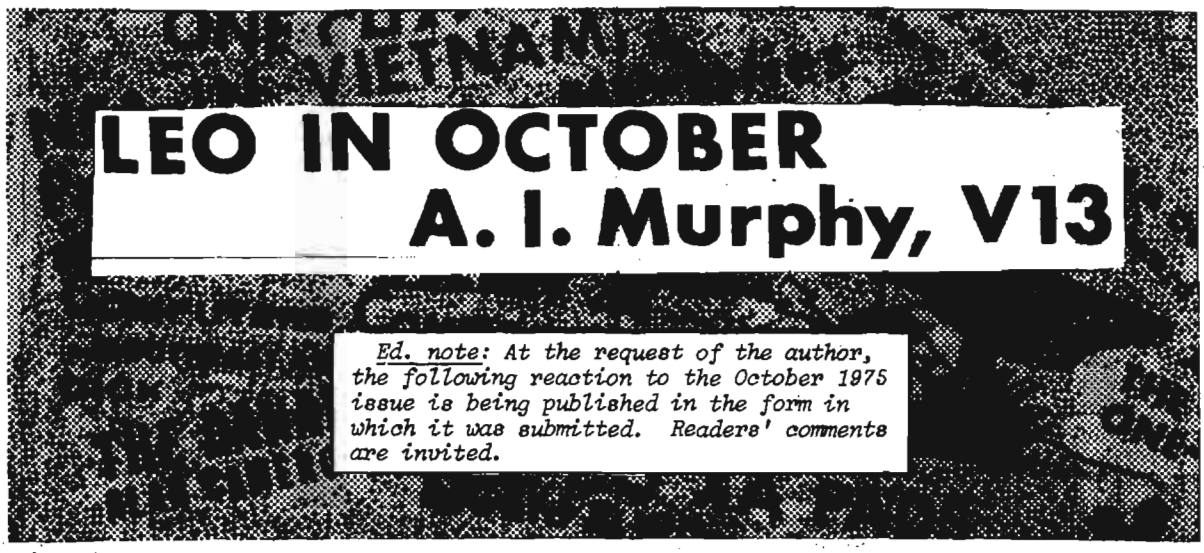
Any NSAer, member of a resident user organization, or Second Party reader. The Department of Defense authorizes publication of CRYPTOLOG for distribution within NSA/CSS and Second Party agencies. The publication can be *read* by anyone with a Top Secret Codeword clearance, but we are not authorized to print copies for general distribution to other U.S. government agencies, including cooperating or customer agencies of NSA/CSS.

Assuming that I'm authorized to get it, how do I get a subscription to CRYPTOLOG?

Matthew 7:7. (x5642s; or P1, CRYPTOLOG.)

~~(FOUO)~~

DOCID: 4009728



LEO IN OCTOBER

A. I. Murphy, V13

Ed. note: At the request of the author, the following reaction to the October 1975 issue is being published in the form in which it was submitted. Readers' comments are invited.

Some years ago, a Hollywood movie told the story of how people and newspapers made a circus of the unhappy situation of a coal miner trapped in a cave-in. The story was ballyhooed to the point where there was widespread betting on when the man would be brought up, the noises from the local brass band and improvised concession stands competed with that from the rescue operation itself, and a new song was heard across the land: "Oh Leo, We're Coming Closer."

Ironically, as the movie went, the event ultimately came back to haunt everyone who for his own purposes sought to get as much mileage as he could out of it. The drilling effort was badly planned and executed. Leo suffocated. And the people were left with bitter loathings of their own behavior and of the insensitive tactics of the newspaper reporters.

Rightly or wrongly, fairly or unfairly, accurately or inaccurately -- the October issue of CRYPTOLOG with its theme on lessons learned from the "Vietnam Experience" is what precipitated recall of the Leo story. It ("October"), as expected, also triggered a whole range of long thoughts about the Vietnam tragedy in general: its place in historical perspective, the awesome gains the Communist camp achieved by it (Pueblo was a technological coup; Vietnam, a monstrous extortion of human spirit, and an ideological triumph); and the lingering concern about the resolve in the free world, particularly in the U.S., to meet the next test which, if we are disposed to listen to Solzhenitsyn, may be catastrophic and soon.

With that as openers, this taxpayer-cum-SIGINTer has already made his point. Rather bluntly, true. But he had made it; namely, that "October" was unfortunate for its bad timing and poor taste. All things considered, except for [redacted] contribution, it gave a carnival flavor coated with pompous technical professionalism to a subject that should not have been treated that way. At least not at this time when we are still caught up in the emotional bends of its aftermath. The intellectual tip-toeing that imaged through the lessons allegedly learned was also something less than admirable.

At that, he could rest his case feeling that he justifiably exercised his right to voice his opinion in this, a vehicle designed for such things.

But what about those long thoughts, the convictions formulated before, during, and after the tragedy, and the basic reasons for this lashing out. Would that there were enough time and space.

It is not always easy to discuss Vietnam in a totally dispassionate way. To remain silent, however, where one disagrees is an assent to what was said. The recourse he has chosen is to submit in gist a few of the many notes he has recorded on our SIGINT involvement in Vietnam, and about the way "October" came across in that context.

There is a time to laugh and there is a time to cry. Now is the time for neither. The appearance of entertaining writing about the Vietnam experience in sedate CRYPTOLOG in October 1975 is just as unpalatable as the shocking breach of the NSA mission in vacuous PENTHOUSE. What we should be doing now is a post-mortem, a realistic, penetrating post-mortem (what an apt term that is here) covering all aspects of the SIGINT story in Vietnam. Then start looking ahead.

It is just as unrealistic to try to prolong the euphoria of self-satisfaction over our SIGINT accomplishments in Vietnam (there is no question but what some of our finest work was done there), as it is to wallow in the bitterness of having watched 17½ million people go under, despite those efforts. The

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

character of "Vietnam SIGINT memoirs" is what one finds objectionable. It is too soon for that sort of thing. Better that "October's" input had been given over to the NSA historian, rather than to hear the cry "Leo is Dead, Long Live His Biographers."

The most unfortunate revelation of "October," as reflected in the concluding paragraph of "The Danang Processing Center," was that a very basic lesson was not learned. It said:

> *Soon after the U.S. military withdrew from Vietnam and the DGTS had assumed complete responsibility for the collection, analysis, and reporting of SIGINT, it became apparent their state-of-the-art would not advance as rapidly as we wanted. The DGTS simply would not be pushed faster than they wanted to go. I feel there management and logistical problems and their lack of a true desire to learn the production and use of SIGINT contributed to the overall failure of the independent ARVN SIGINT effort.*

The author's conclusions are respected as the expression of his point of view. But, therein lies the lesson, as this writer sees it. Could it not have been that the South Vietnamese were simply incapable of going at our speed, and/or could it not have been that they deliberately dragged their feet having the vision of our departure as the beginning of their doom.

The Vietnamization Improvement and Modernization (VIM) Program was a noble, albeit a late-starting undertaking. Although much was achieved by it, we all knew from the beginning that it was fraught with uncertainties and risks: the ARVN will to fight on, their ability to absorb the thrust of our updating efforts, and our own patience in seeing it through. We pressed on anyway. Hurriedly. Hoping that it would all crystallize on time.

There again, in the view of this writer, is where any moves to soothe the current compulsion to catalog lessons learned should begin. The mere fact that the program was called "Vietnamization," let alone the topic of acceleration, must have had an immediate demoralizing affect on our counterparts. Perhaps at the time we were too long on expertise and somewhat short on compassion. Hopefully, the word-makers have had their day, and we will not have to cope with the indelicacies of any more "izations,"

[redacted]

One is convinced that in the process of imparting our knowledge to the DGTS, often to the point of causing them to gag, we let our sensitivity slip away, little by little. A considerable amount can be, and undoubtedly will be written about our moving ahead to new objectives in the VIM program without adequately resolving previous steps.

The memory of technical untidiness that developed as the result of ride-herd and one-upmanship methods against them and between ourselves, is still vivid.

[redacted]

One has considerable respect for [redacted] P.L. 86-36 and his candid talk in the Friedman Auditorium on how it was from his vantage point in those final days, and his wariness of lessons-learned seminars. In line with the point being made herein, however, there is some persuasion that his excellent presentation in "October" was enough.

We can readily agree with him about the dedication and courage of the U.S. SIGINTers in Vietnam. Being on the scene, and working directly with our counterparts, made it easy to respect them. Maybe that's why during the nightmare of the final hours, TAer [redacted] EO 1.4.(d) having rowed out to an American ship at anchor, P.L. 86-36 reportedly saw fit to shout the title of this agency, and the names of specific NSAers he had worked with over the years. As far as we can tell, he was picked up where evidently others were not. Call it resourcefulness, if you want. The writer, who hopes his name was included in that plea, prefers to believe that this was simply another reflection of good work done in an area where lessons were learned well in advance.

We should be preoccupied with things beyond "mileage," and self-satisfaction over past achievements. Why is it that our product had such a low credibility in the eyes of the Ambassador in Saigon? Why did he keep backing a loser in "communications deception"?

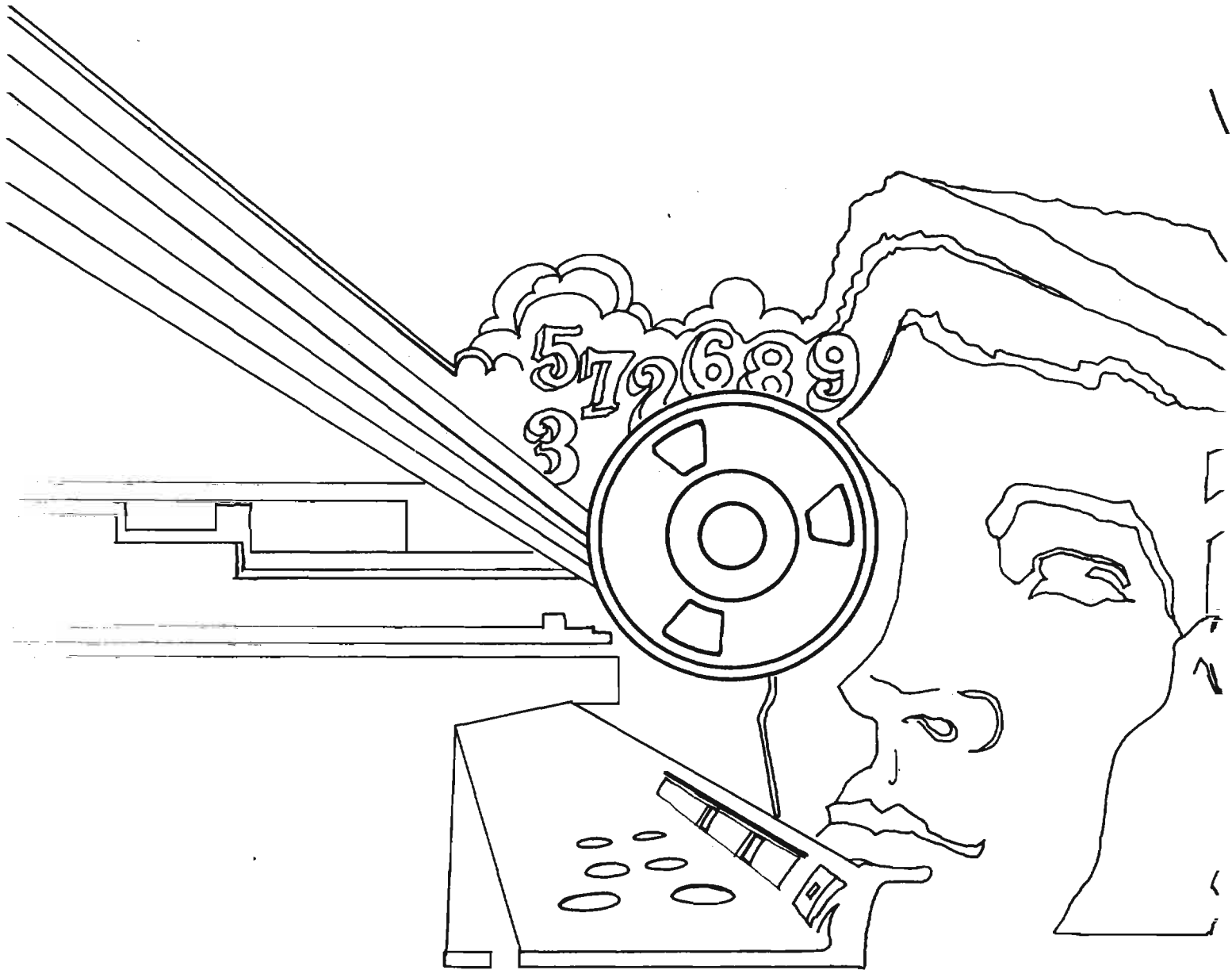
[redacted]

A lot of good it's going to do anybody, after the cave-in happens, to be able to say - we told you so!

The refrains of "Oh Leo. . ." from the Kremlin are loud and clear these days. The only difference is, there is no indication of any bad planning and execution on their part, or that the time is right for their behavior to be coming back to haunt them.

EO 1.4.(c)
P.L. 86-36

Pl-Nov 75-53-24293


5726893

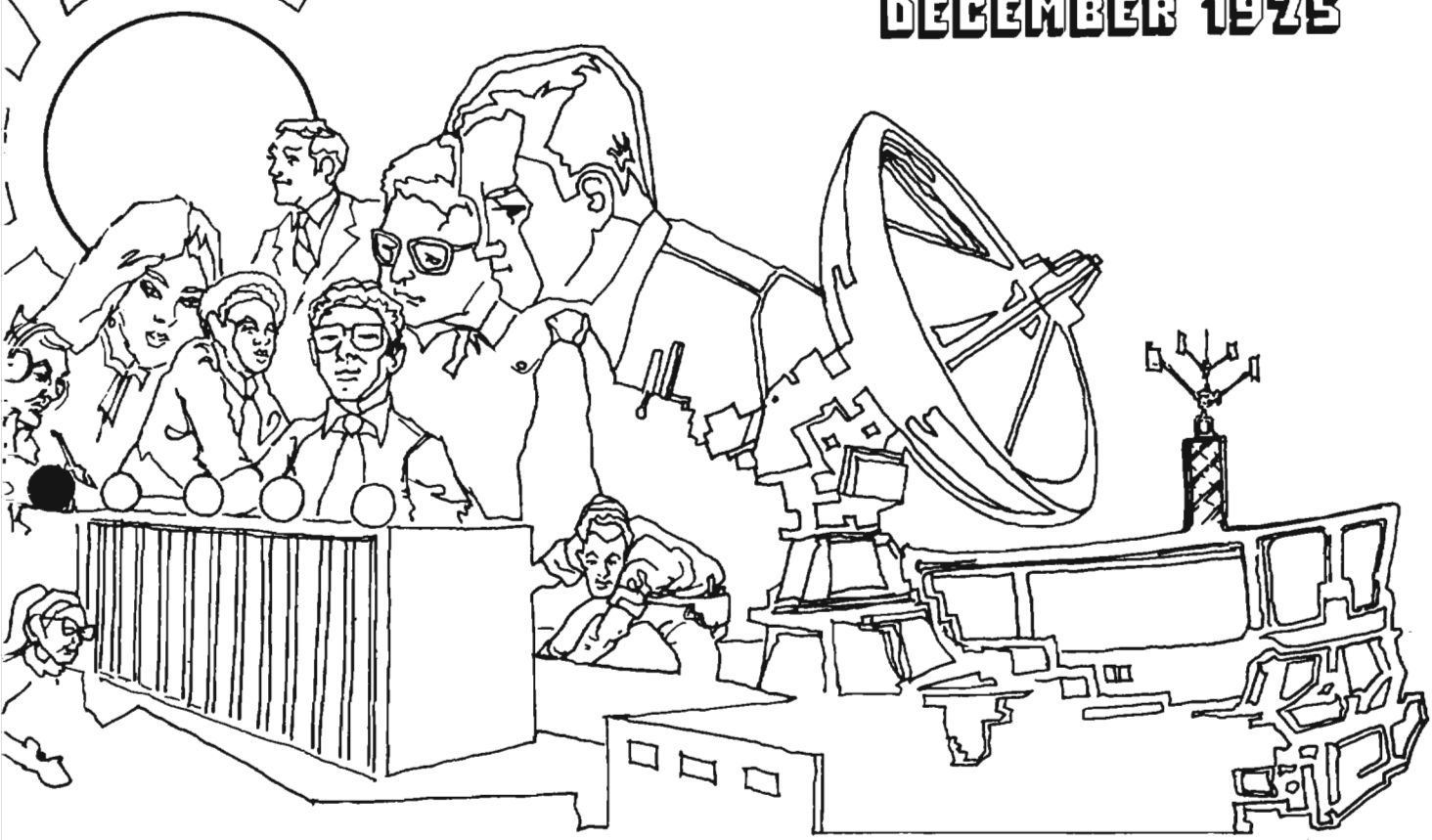
DOCID: 4009727

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

DECEMBER 1975



P.L. 86-36

WINTERBOTHAM'S "THE ULTRA SECRET":
A PERSONAL COMMENT.....Brigadier John H. Tiltman..1
WEAPON THAT HELPED DEFEAT NAZIS.....P. W. Filby.....3
MUM'S STILL THE WORD!.....[redacted].....5
LINEAR RECURSIVE SEQUENCES.....[redacted].....6
CUMULATIVE INDEX, 1974-1975.....9
GREAT SOVIET SHIPBUILDING MYSTERY.....David H. Williams.....21
WHAT ARE WE ABOUT?.....[redacted].....23
LINGUISTS FROM THE MELTING POT.....[redacted].....25
CLA ESSAY CONTEST; CAA NEWS.....27

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009727

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. II, NO. 12 DECEMBER 1975

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief..... Arthur J. Salemme (5642s)

Cryptanalysis..... [redacted] (8025s) P.L. 86-36

Language..... Emery W. Tetrault (5236s)

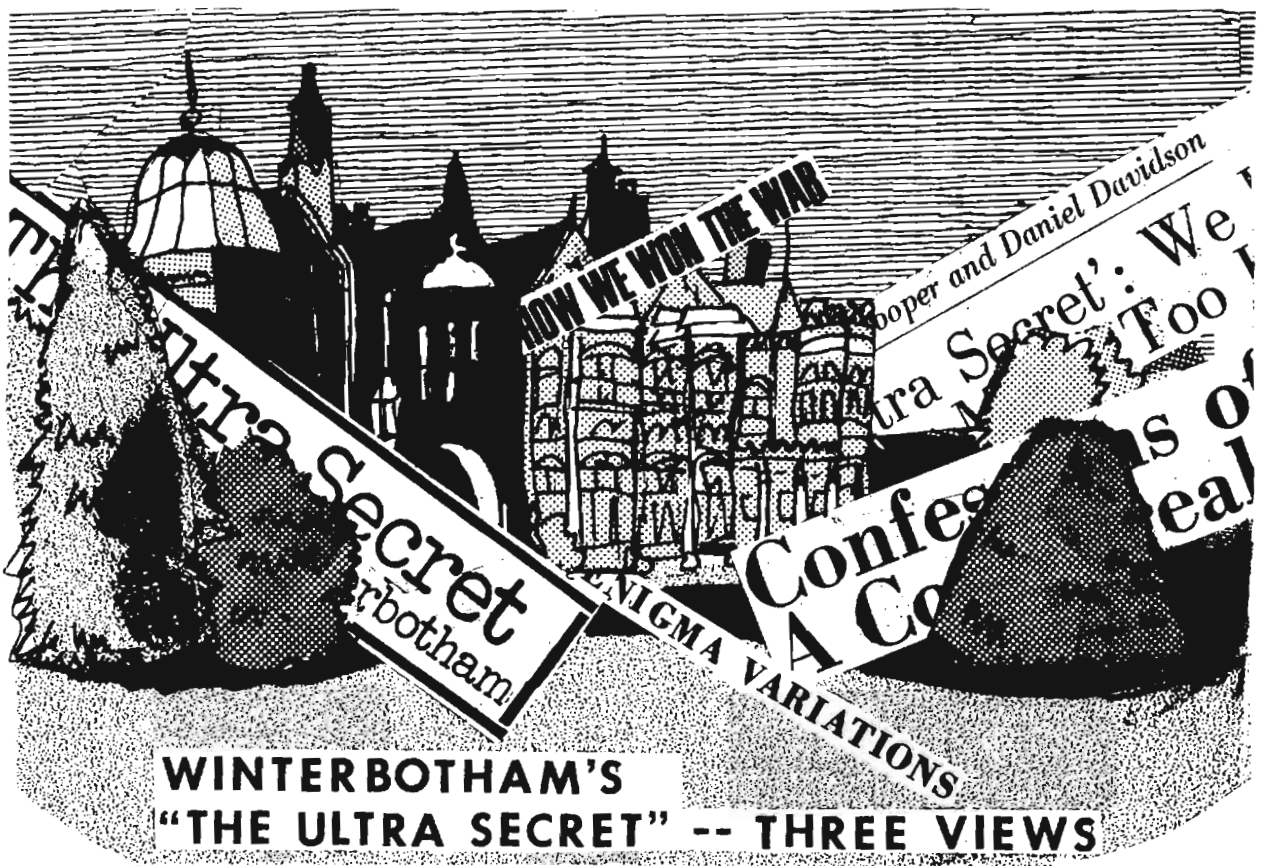
Machine Support..... [redacted] (3321s)

Special Research..... Vera R. Filby (7119s)

Traffic Analysis..... Frederic O. Mason, Jr. (4142s)

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4009727



WINTERBOTHAM'S "THE ULTRA SECRET" -- THREE VIEWS

The following three articles deal in various ways with the publicity given in the British and American press and on television to F. W. Winterbotham's book "The Ultra Secret." The first article, by Brigadier John H. Tiltman, deals with the accuracy of the statements in the book and the degree of harm done by them. The second article, by P. W. Filby, is a review of the book as assessed by a member of the team of specialists who worked the German diplomatic problem. The third article, by [redacted] M542, gives a word of advice to those who might now be tempted to tell everything they know.

P.L. 86-36

A PERSONAL COMMENT
By Brigadier John H. Tiltman, P1

When Winterbotham's book was first published late in 1974 in England, some members of NSA who had served at Bletchley Park during World War II, on reading early reviews, assumed that it was officially authorised. This was definitely not the case. Its publication was strenuously opposed by British responsible authorities, who took legal advice on the probable consequences of prosecuting the author under the British Official Secrets Act. They were advised that prosecution could not be effective without the case going to court and evidence produced that British national security had been damaged by the book's publication with consequent public disclosure of more current intelligence activities. They therefore decided that legal action would probably do more harm than good.

Another and perhaps a decisive factor making prosecution unlikely to succeed was the publication in France in 1973 of Bertrand's book *Enigma, ou La Plus Grande Enigme de la Guerre 1939-1945*. This revealed for the first time the fact of an analytic success against the Enigma and was decisive in the discussions between Deputy Director NSA and Director GCHQ on the matter of whether to attempt to restrain Winterbotham and his publisher.

I am not alone in believing that an early official public description (perhaps a joint US-UK statement) of the basic facts of the wartime exploitation of the intelligence derived from the solution of the Enigma keys might have mitigated the damage done to security. Perhaps this could have been strengthened by a further

statement that the revelation of technical details of the methods of solution would be resisted indefinitely. I realise however that there must be other valid arguments which persuaded the responsible authorities not to take such action.

I myself took no part in the solution of Enigma keys in Huts 6 and 8, nor in its exploitation in Hut 3, but I am, I believe, the only person around who was on the directorate level at Bletchley Park during the war and had a hand in many of the policy decisions made regarding the production and use of the intelligence derived.

The book is poorly written and very inaccurate in some areas where I know the facts. The references to the early history of Enigma solution and to the activities of the staff of Hut 6 (who performed the cryptanalytic part of the enterprise) are hopelessly wrong. It is difficult to understand how the author who had considerable responsibilities for the organisation and distribution of Enigma intelligence could have been so completely ignorant of the technical side of the operation. He doesn't know the difference between the Enigma (a rotor machine), other German ciphers, the Japanese high-grade diplomatic machine (the "Purple," a totally different kind of machine), and the Japanese Fleet general cipher (a codebook and additive hand system). His remarks about the "Bronze Goddess" appear to be a complete invention.

Some people gather the impression when they read the book that the author greatly magnifies his own part in the winning of the war. I give an example from my own experience. To quote some passages, "It was at this point that Menzies told me he had decided to hand over my shadow OKW in Hut 3 to the General Administration at Bletchley. One never knew where one stood with Menzies. He softened the pill by confirming me as his deputy, . . ." (p. 87). "Despite the loss of my personal control of Hut 3 and the shadow OKW, I still had direct access to it when required. I was never told by Menzies the real reasons for the takeover, . . ." (p. 92). The facts are that I reported to the Director of Military Intelligence at the War Office, that Curtis, the War Office representative in Hut 3, in conjunction with Humphries, the corresponding Air Force representative, had on two separate occasions gone behind my back to recommend reorganisation of Hut 3 under their own more direct control. In consequence, a SIGINT Board meeting was called with General Menzies in the chair and consisting of the three Service Directors of Intelligence and Director GCHQ. At this meeting it was decided to withdraw Humphries, Curtis, and the naval representative.

I knew Winterbotham slightly and flew with him to Paris on the occasion of one of my official visits to France in 1940. His outstanding achievement was the establishment of SLUs (special liaison units) for the dissemination of ULTRA to commanders in the field. I have no reason to doubt that he records this faithfully. He gives rise to feelings of discomfort, however, when he describes his relations with the more high-ranking recipients of his wares. It appears that Montgomery must have treated him with less courtesy than others and consequently he feels sure he himself could have fought Montgomery's battles far more efficiently!

In view of its general inaccuracy, especially when touching on technical matters, I believe the book, taken by itself, does no harm. This cannot be said for the side effects it touched off. The first review I read was in the *Washington Post* by Al Friendly, who himself served in Hut 3. He headlines his review "Confessions of a Codebreaker." He gives the impression that for a great part of the war every telegraphic order issued by Hitler was currently on the desk of the Prime Minister and concerned Allied commanders. This is simply not true. Such a picture takes no account of the many difficulties of the operation, the decisions to be taken on insufficient evidence as to priorities of attack on some keys to the exclusion of others, the many failures and delays, the early misunderstanding as to the real meaning of messages, etc. The general success of the project was as much a triumph of organisation of the large-scale attack as of the ingenuity and persistence of the cryptanalysts, especially the mathematicians.

Perhaps the most objectionable of the reviews was a long article in one of the London Sunday newspapers by Peter Calvocoressi. He was an important figure in Hut 3, presumably recruited by Winterbotham. He is now, I believe, managing director of Penguin Books and was the joint author of a distinguished history of World War II. His article is an extremely well-written description of life in Hut 3, but he has gone further than anyone else in including a photograph of the German Service Enigma and in mentioning the Bombe. I believe this was the first time a picture of the service Enigma appeared in public print. Not even Bertrand in his book *Enigma* gives a photograph of the machine. I am quite unable to understand Calvocoressi's arrogant assumption that he can say what he likes in public now that Winterbotham's book has appeared. I hold the view that everyone who worked in Bletchley Park is still under a moral obligation not to disclose secrets not previously published without official permission and, I would have thought, is aware of this obligation.

Many of us were nervous of what David Kahn would have to say when his turn came to review the book. When his review did appear in the *New York Review of Books*, it was surprisingly mild and harmless. He, of course, is in a different category. Not ever having been a part of

any Government agency, he cannot be regarded as subject to the same restrictions.

Other reviewers have been influential journalists who have taken the tone that the book has revealed the operations of World War II in a new light, that history will have to be rewritten, that the British have told only part of the story and that they will have to tell the rest. I do not know whether we have heard the last of this attitude.

Something has to be said about the paragraphs on page 14 of the book dealing with personalities. Winterbotham mentions the mathematicians Alexander, Babbage, Welchman, and Milner Barry, but doesn't seem to have heard of Turing, who is generally regarded as the leading genius of the methods of solution of the Enigma in its various forms. He says that "it was generally accepted that of our own backroom boys 'Dilly' Knox was the mastermind behind the Enigma affair." I do not agree with this at all, though I am aware that he was in general charge of the analysis of the machine before the war and long before the British had any success in solution. Incidentally, Winterbotham seems to confuse Knox with Foss, who fits much better into the physical description in the book and who had some influence on early solutions before bombes became available. In his casual remarks about me, Winterbotham is somewhere near the truth: he says I had been borrowed from the Army. So I was -- 20 years earlier! Of Josh Cooper he says he was "another brilliant mathematician." Josh wasn't a mathematician at all -- he was a very fine linguist. For no known reason, Winterbotham mentions Dick Pritchard. He was a regular Army officer who had been with me for 8 or 9 years, before the war, but he had nothing whatever to do with the solution of the Enigma.

I think it quite likely that all this does no harm at all, but we cannot by any means be certain of this. Therefore, we have to continue to try to withhold further disclosures, particularly on technical methods of solution.

~~(HVCCO)~~

Brigadier Tiltman was Deputy Director and Chief Cryptographer, GCHQ, from 1941 to 1946. Since 1964 he has been working at NSA, Fort Meade. He is a Commander, Order of St. Michael and St. George; Commander, Order of the British Empire; and Distinguished Member, CMI.

ULTRA WAS SECRET WEAPON THAT HELPED DEFEAT NAZIS

By P. W. Filby

(UNCLASSIFIED)

Shortly after the outbreak of World War II, the British Government acquired a stately home in a small town called Bletchley, a town renowned only for its railway junction and nearby brickyards.

For the next few months civilians and servicemen and women arrived in ever increasing numbers, and hardly a house in Bletchley escaped billeting. The citizens wondered at the motley crowd, raffishly dressed for the most part, often absent-minded and all having a studious air about them.

High iron fences were erected round the home known as Bletchley Park and armed Army guards were on duty at all times. The locals had to get used to comings and goings of their lodgers at all hours, and having taken in civilians they would suddenly see them emerge in full regalia as officers of the three services, especially when they made trips to London.

Many guesses were hazarded but the only thing that could be said was that it was a secret department -- and the secret was well kept, so well that it is not until now, thirty years later, that the Bletchley people and the world will know that the many thousands of people at the "Park" were working in enemy codes and ciphers.

Group Captain Winterbotham has taken advantage of the "30-year rule" to describe the success of one group, "Hut 3." It is an absorbing story, and although the chief defect is that Winterbotham was not a codebreaker and therefore makes several wrong assertions, the book is one of outstanding interest, and readers will marvel at the war's greatest secret and how it was kept until now.

Just before the outbreak of World War II the British had obtained by various means a complex machine known as "Enigma" which was being used for the encoding of the most secret and important German armed forces communications. After a prodigious effort the British cryptographers of "Hut 3" managed to break this machine and later built what might well have been the first computer, so that the communications could be read immediately upon receipt.

To everyone's surprise, the Germans continued to use this machine throughout the war and thus most plans made by Hitler and his High Command were known to the British (and later, the Americans also) at the same time as the German recipients.

Radio operators in remote, lonely locations intercepted the messages, which were rushed to

Bletchley, often by motorcycle until more sophisticated methods were evolved, and were promptly decoded and passed to the appropriate commands. The intelligence was code-named "Ultra."

Astonishingly, there is nothing in captured German documents to suggest that anyone suspected that the most secret cypher code was being read throughout the war. Much of the credit for this were the rules laid down by Winterbotham for the "need to know."

For instance, the Russians were never told of it, and the many free forces (French, Dutch, etc.) were not let in on the secret. Winterbotham toured British and American commands, lecturing users on this intelligence and warning them care had to be taken on how the information could be used.

For instance, although the presence of an enemy force might be given in detail by Ultra, to bomb it immediately would cause the Germans to wonder how the enemy knew of this force, so reconnaissance planes had to be used so that the Germans would suspect that they had been spotted from the air.

Unhappily, it was not unusual for holders of the German plans to have to forgo using them for fear of compromising the cypher break. One such occasion was the bombing of poor Coventry; enemy plans were known beforehand, but to defend the city would have aroused German suspicions. Although attempts to defend were made, the populace was not warned in advance. At that time it was not known whether German spies were working among the British.

But the information was used with telling effect in the Battle of Britain, when the Air Force knew exactly the direction and the force to be employed in each attack. It is probable that Ultra did much to save Britain in those dark days. Everyone knew the Air Force could not withstand these onslaughts for long, but Ultra allowed them breathing space by parceling out the slender defense forces where needed most.

Ultra played a particularly distinguished part in the North African campaign, where Montgomery was informed of Rommel's disposition of his forces and the extent of his supplies. Ultra also enabled supplies across the Mediterranean Sea to be sunk en route. Montgomery's face should be red, since he claimed verbally and in his books that he planned his battle order, but he acquired the record of invincibility only through his use of the information given by Ultra.

With the British losing thousands of tons of shipping weekly, the decoding of the German Navy's messages provided a welcome respite, and from 1943 the losses were significantly reduced since the disposition of the U-boats was known.

One wonders now just how the Normandy landing would have worked out without Ultra. Since decoded messages told of the German belief that the attack would come from the narrow Pas de Calais, General Patton arrived with a phantom army to give the impression the landing would indeed be tried there. Consequently Rundstedt and a vast army were kept there, reducing the defenses in Normandy.

Ultra's strength was also shown when, in the Battle of the Bulge, the Germans relied on telephone rather than radio communications, and many lives were lost because the Allies could learn nothing of the German plans and intentions.

These and other exciting stories are related in this absorbing book. It suffers perhaps because Winterbotham was a "go-between" rather than one of the codebreakers, and thus credit is not given to the mathematicians and linguists who worked long hours in stuffy rooms where, because of blackout precautions, fresh air seldom penetrated the smoke-filled atmosphere.

Tribute must also have been paid to those radio operators, straining their ears when static and other conditions meant a missed group and maybe an important one at that, when the operator could not ask for a repeat -- these were the real heroes of one of the outstanding accomplishments of the war.

One amusing tailpiece to the whole affair is the effect it will have on those whose memoirs have already been written. Many should now be rewritten; if Ultra did not actually win the war it will cause historians to revise what has been written thus far. Books such as "D-Day" are exciting reading, but the present work must be included in all war history collections from now on, since it will affect all war histories in varying ways.

Winterbotham is rightly proud of Bletchley's achievement, but he tends to forget that information needs acting upon; it needs good generals and above all a great Air Force, Army, and Navy. Fortunately the Allies had these too, and though Ultra was one of the most important contributions to the victory, Winterbotham perhaps overrates it a little.

Sir John Masterman's book, "The Double-Cross System in the War of 1939-1945" (reviewed in these columns February 12, 1972) describes how captured spies were "turned around" and also contributed to the downfall of Germany. There were other great coups but Ultra and Double Cross must rank very high in the defeat of the Nazis.

P. W. Filby, in addition to his SIGINT experience at Bletchley Park and GCHQ, is an "honorary NSA-er by marriage" (his wife is CLA President and CRYPTOLOG's SRA Editor Vera R. Filby). Mr. Filby is the current Director of the Maryland Historial Society, Baltimore, Maryland. The preceding review is reprinted in entirety from the Baltimore Evening Sun, June 10, 1975. ~~(FOUO)~~

DOCID: 4009727

P.L. 86-36

MUM'S STILL THE WORD!

By [redacted] M542

Many people make their work and the organization they work for an extension of their own egos, especially when the organization is performing a vital service to society. For most people, one of the most compelling motivations on the job is the quest for approval by their peers and supervisors. But we NSAers are not like "most people." True, we have always been able to rely on peer and supervisory approval, but we have never been able to derive ego gratification from identifying with NSA -- historically, both the Agency itself and our specific jobs here have been obscured from public notice. Lately, however, the curtain cloaking our activities has been lifted slightly. Winterbotham's book *The Ultra Secret* and the follow-on revelations in the CBS television program, "Sixty Minutes," have provided the public with glimpses of the vital role that cryptology plays in protecting our nation's security. Certainly, all of us must feel a sense of pride, and perhaps indulge our egos a bit, to see our Agency's vital function finally made known to the public. It's a very seductive thing. We plug along for years without public recognition. We strive constantly to overcome the natural urge to discuss our work with non-NSA friends, particularly when that work involves events taking place on the world stage. Then, suddenly, there's our organization, our work -- us! -- on the television screen, the front page of the newspaper, the public bookshelf. How easy it is to feel proud about finally getting public recognition. But that initial feeling of pride and personal gratification is soon outweighed by the disquieting realization that someone has talked, someone has betrayed our tradition of keeping our mouths shut.

The fact that such revelations do not always compromise sensitive information, as in the case of *The Ultra Secret* and the TV follow-on, does not diminish our feelings of dismay. That precious shell of anonymity -- so carefully maintained over the years -- has been cracked. One can only expect that others will rush forth to give their versions of past events and open that crack still wider.

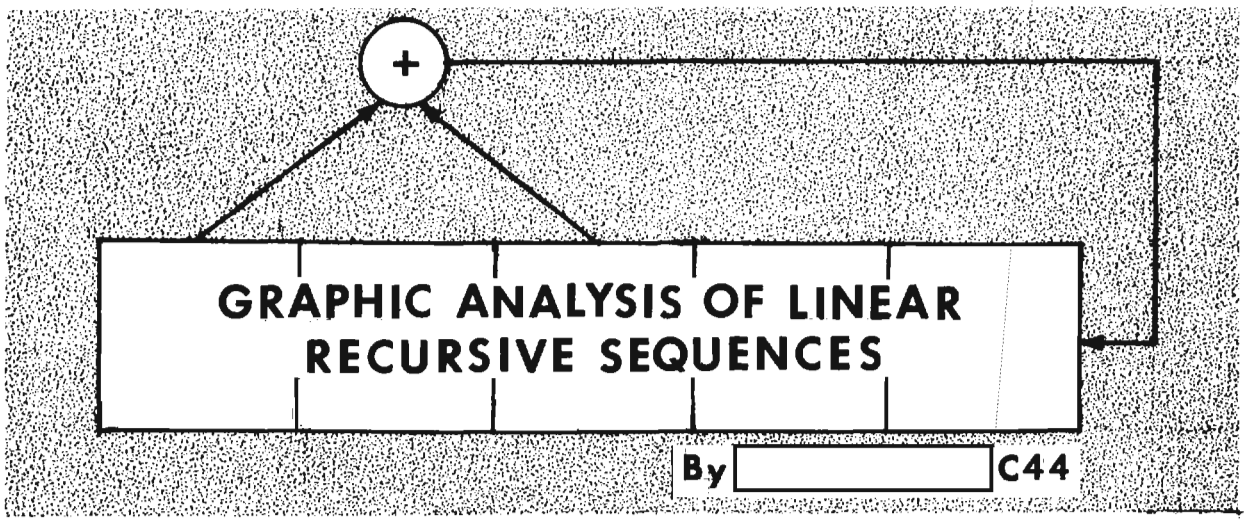
That our cryptologic operations are discussed at all in the public media, no matter how many decades have elapsed, is the primary concern here. Journalistic appetite begets appetite and, once titillated by the morsels served up by disclosures such as those in Winterbotham's book, it tends to become ravenous for the whole pot. Those who were associated with the cryptologic effort in the past -- and the numbers are prodigious -- as well as those currently involved, are presented with a psychological cop-out to indulge their egos and talk about their work. After all, everyone else is doing it. Thus, revelation begets revelation.

P.L. 86-36

The publication of *The Ultra Secret*, however innocuous its specific revelations, can only be viewed with foreboding. It can only hasten the dropping of the next shoe. And when that shoe drops, we NSAers should remember, "Mum's *still* the word!"

[redacted]

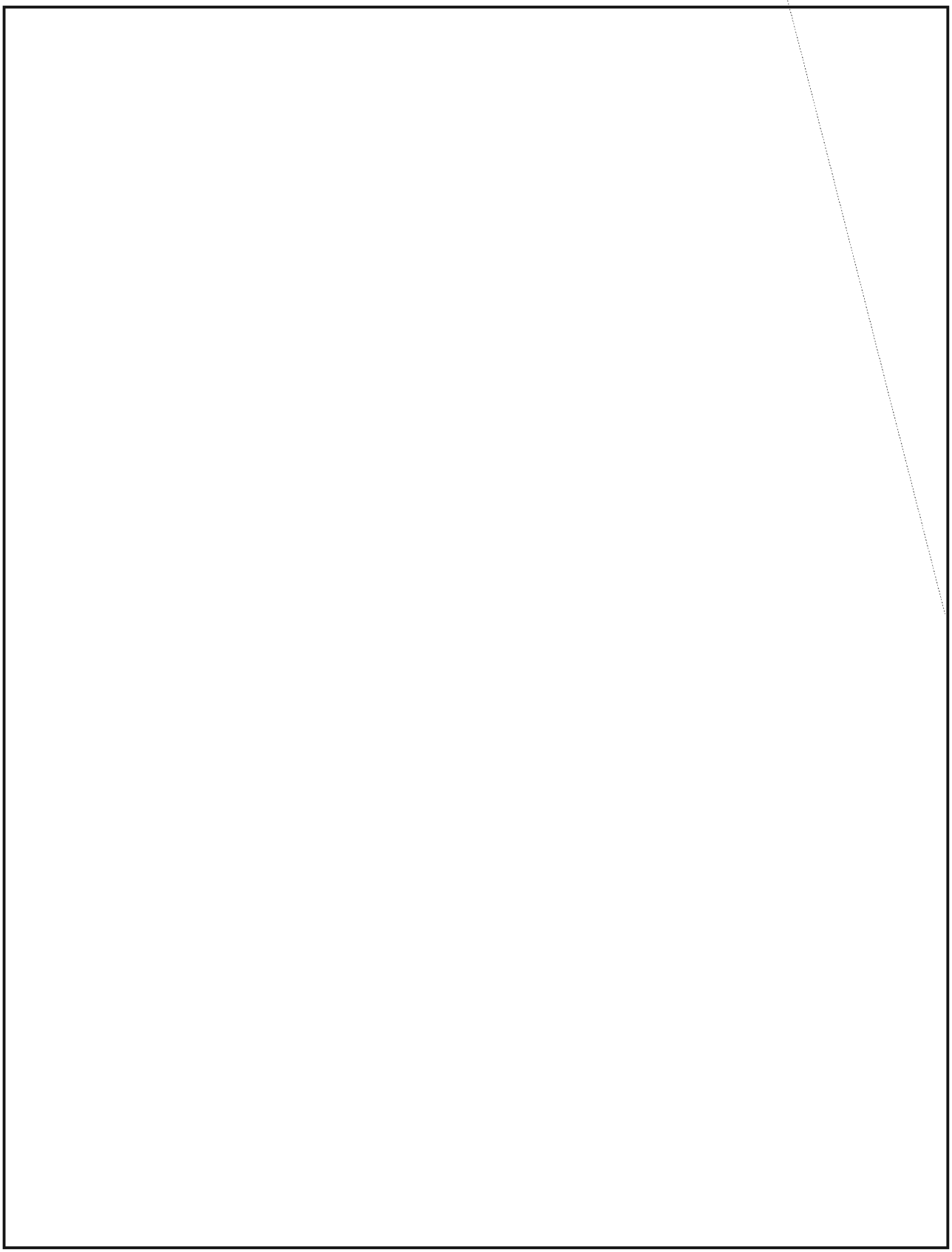
A Nazi submarine is shown under attack by American planes. Deciphering the Ultra code enabled Allied destroyers to sink many German U boats.

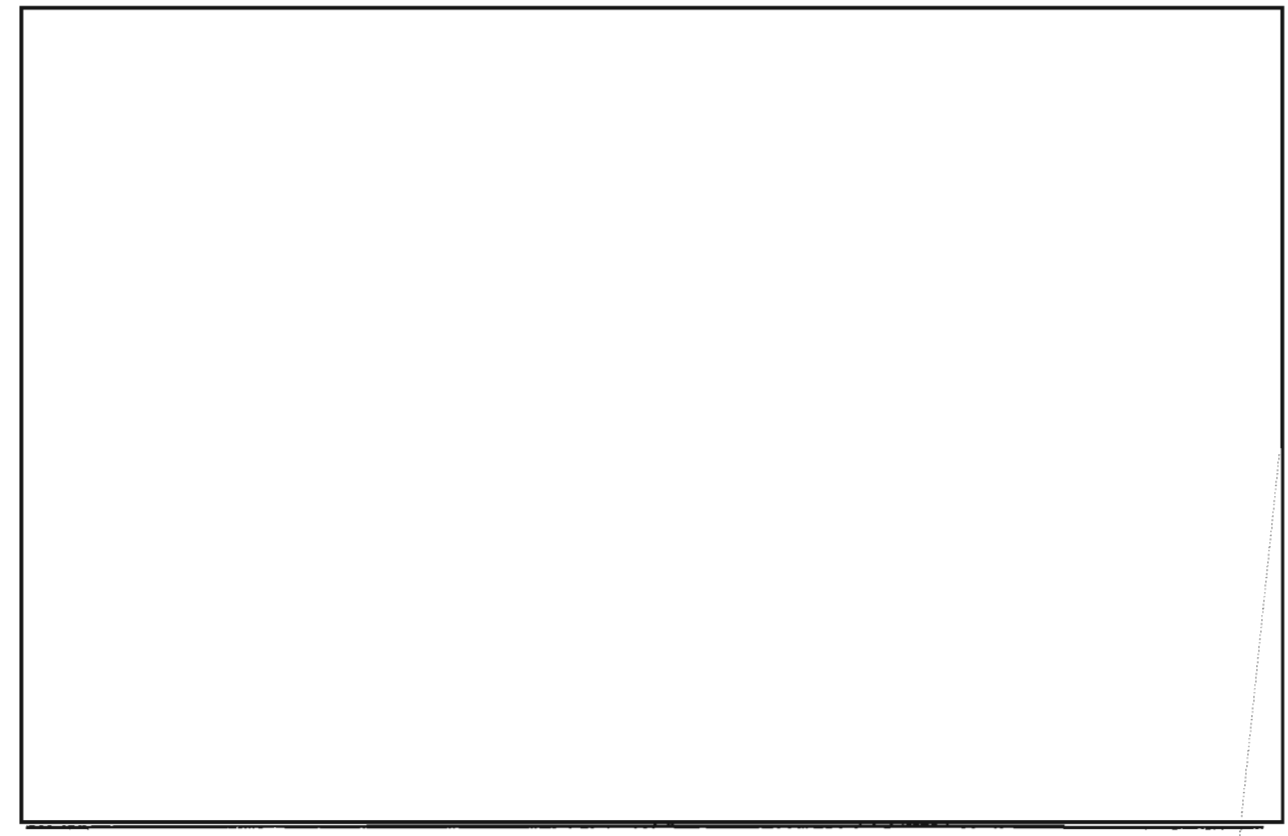


EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)

DOCID: 4009727





We need your help in keeping CRYPTOLOG's distribution list up to date.
Would you please fill in the attached form if you need:

MORE COPIES? (New hires? people transferred in? somebody wants to be added to list?)

FEWER COPIES? (Resignations? retirements? transfers out? somebody wants off?)

NAME CHANGES? (Misspellings on current distribution list? girls getting married and taking husband's name? guys getting married and adding wife's maiden name as hyphenated adjunct to his own?)

ANY OTHER CHANGES?

EO 1.4.(c)
P.L. 86-36

TO: Editor, CRYPTOLOG, P1
Please make the following changes to distribution for _____:
(Organization)

ADD copies for: _____

DELETE copies for: _____

CHANGE mailing labels as follows:

LABEL READS	LABEL SHOULD READ
_____	_____
_____	_____
_____	_____

(If you do not want to cut this page, use plain piece of paper.)

DOCID: 4009727

CUMULATIVE INDEX, 1974-1975

The following cumulative index of CRYPTOLOG (Vols. I and II, 1974-1975), was computer-produced using the Super Bee CRT/Tycom typewriter terminal on the B6700 and programs written by George P. Wood, P16. The index is printed in the middle of this issue so that it can be removed and used as a separate document if desired.

The index is in two parts. The first part is an index of titles, listed alphabetically (1) by title and (2) by keyword in the title. The second part is an index of authors. In both parts, multiple entries are listed in chronological sequence.

Items in the double issue February-March 1975 are indicated by "Feb 75," and those in the double issue August-September 1975 by "Aug 75."

Abdul and His 40 Tanks
Frederic O. Mason, Jr.. . . . Aug 75

AFRIKAANS
Language in the News -- Afrikaans, Amerind, Arabic, Chinese, French, Hebrew, Lycian, Spanish, Portuguese, Russian, Swahili . . . . . Sep 74

AMERIND
Language in the News -- Afrikaans, Amerind, Arabic, Chinese, French, Hebrew, Lycian, Spanish, Portuguese, Russian, Swahili . . . . . Sep 74

APOSTROPHE
The Apostrophe -- Some Thought's
Vera R. Filby . . . . . Nov 74
The Winnah--Kid Apostrophe! . . . . . Oct 75

An Approach to Callsign Analysis
William J. Jackson. . . . . Dec 74

[redacted]
COMINT Analysis of [redacted]
Derek K. Craig. . . . . Sep 74
Letters to the Editor -- [redacted] article. . . . . Dec 74

ARABIC
Language in the News -- Afrikaans, Amerind, Arabic, Chinese, French, Hebrew, Lycian, Spanish, Portuguese, Russian, Swahili . . . . . Sep 74
Language in the News -- Language Panel, NCS, Machine Course for Linguists, CLA News, Arabic. . . . . Apr 75

EO 1.4.(C)
P.L. 86-36

Are We Wasting Linguistic Time?
Mary Roberta Irwin. . . . . May 75

AUTOMATED
[redacted]
Maurice Welsh . . . . . Nov 75

AUTOMATION
Automation of a TA Process
Tim Murphy. . . . . Oct 75

Basic Patterns of [redacted] Codes and Ciphers
[redacted] . . . . . Feb 75

BEISBOL
The Language of Beisbol in Everyday Talk
[redacted]
Ramon Santiago-Ortiz. . . . . Aug 74

BOOKBREAKERS
Letters to the Editor -- Professionalization of Bookbreakers
[redacted] . . . . . Apr 75
Letters to the Editor -- [redacted] letter on Bookbreakers
[redacted] . . . . . May 75
Letters to the Editor -- [redacted] letter on Bookbreakers
[redacted] . . . . . May 75
Letters to the Editor -- Bookbreakers; Professionalization of Country Specialists
[redacted] . . . . . Jun 75
Letters to the Editor -- [redacted] letter on Bookbreakers . . . . . Jun 75
Letters to the Editor -- Rebuttal
[redacted] . . . . . Aug 75

CA
TA, Handmaiden of CA
Frederic O. Mason, Jr.. . . . May 75

CAA
Learned Organizations -- CLA Essay Contest; CAA News . . . . Dec 75

CALENDAR REFORM
A Proposal for Calendar Reform
Francis T. Leahy. . . . . Dec 74

Calling All SRAs! -- SRA Symposium
[redacted] . . . . . Aug 74

CALLSIGN
An Approach to Callsign Analysis
William J. Jackson. . . . . Dec 74

CAMINO
CAMINO News
[redacted] . . . . . Feb 75
CAMINO -- Electronic Warfare Terms
[redacted] . . . . . Jul 75

CAREER PANELS
A Short Directory of Career Panels. . . Aug 74

P.L. 86-36

CARRIAGE
Project CARRIAGE -- Worldwide HFDF Modernization Plan
James B. Webster. . . . . Sep 74

The Case for COMINT Readers
[redacted] . . . . . Jan 75

CENTRAL INFORMATION
A Guide to Central Information -- C5. . Apr 75

Character Building in the People's Republic of China
[redacted] . . . . . Oct 74

CHARACTER STREAM SCANNING
[redacted] Paper on Character Stream Scanning by Machine . . . . . Oct 75

CHINA
Character Building in the People's Republic of China
[redacted] . . . . . Oct 74

CHINESE
Language in the News -- Afrikaans, Amerind, Arabic, Chinese, French, Hebrew, Lycian, Spanish, Portuguese, Russian, Swahili . . . . . Sep 74
Basic Patterns of [redacted] Codes and Ciphers [redacted] . . . . . Feb 75

CIPHERS
Basic Patterns of [redacted] Codes and Ciphers [redacted] . . . . . Feb 75
Computers, Comms, and Low-Grade Ciphers -- [redacted] . . . . . Oct 75

CISI
Learned Organizations -- CLA, CMI, CISI Prizes and Honors, Spring 1974 . . . Aug 74
Learned Organizations -- CISI Forms Special Interest Group on Human Factors . . . . . Dec 74
Learned Organizations -- CLA Is Ten Years Old! News from CISI, CMI, IAI . . . . . Jan 75

CITIZENS OF THE WORLD
Puzzle -- Citizens of the World . . . . Dec 74
Letters to the Editor -- Citizens of the World [redacted] . . . . . Feb 75

CLA
Learned Organizations -- CLA, CMI, CISI Prizes and Honors, Spring 1974 . . . Aug 74
Learned Organizations -- CLA Is Ten Years Old! News from CISI, CMI, IAI . . . . . Jan 75
Language in the News -- Language Panel, NCS, Machine Course for Linguists, CLA News, Arabic. . . . . Apr 75
Learned Organizations -- CLA, IAI . . . May 75
Learned Organizations -- CMI, CLA . . . Jul 75
Learned Organizations -- CLA Essay Contest; CAA News . . . . Dec 75

CMI
Learned Organizations -- CLA, CMI, CISI Prizes and Honors, Spring 1974 . . . Aug 74
Learned Organizations -- CLA Is Ten Years Old! News from CISI, CMI, IAI . . . . . Jan 75
Learned Organizations -- CMI, CLA . . . Jul 75

CODE
The Navajo Code Talkers . . . . . Jun 75

CODE CLERK
Psyching the Code Clerk -- [redacted]
L. D. Callimahos. . . . . Apr 75
Re-psychling the Code Clerk [redacted] . . . . . Jul 75

CODE RECOVERY
Cryptanalysis and Code Recovery
Marjorie Mountjoy . . . . . Sep 74

CODES
Basic Patterns of [redacted] Codes and Ciphers [redacted] . . . . . Feb 75

CODEWORD
"Codeword" or "COMINT Channels"? [redacted] . . . . . May 75
Puzzle -- Crossed Codewords [redacted] . . . . . Jan 75

COLLECTION
The New Collection Criteria [redacted] . . . . . Dec 74

COLLECTOR
UNNA, [redacted] . . . . . Jan 75
What is a Collector? [redacted] . . . . . Aug 74

COMINT Analysis of [redacted]
Derek K. Craig. . . . . Sep 74

COMINT CHANNELS
"Codeword" or "COMINT Channels"? [redacted] . . . . . May 75

COMINT READERS
The Case for COMINT Readers [redacted] . . . . . Jan 75

COMM CHANGE
A Comm Change at Ramasun Station [redacted] . . . . . Apr 75

[redacted]
The Warsaw Pact [redacted] . . Jul 75

EO 1.4.(c) P.L. 86-36

EO 1.4.(c) P.L. 86-36

EO 1.4.(c) P.L. 86-36

EO 1.4.(c) P.L. 86-36

EO 1.4.(c) P.L. 86-36

P.L. 86-36

P.L. 86-36

EO 1.4.(c) P.L. 86-36

EO 1.4.(c) P.L. 86-36

DOCID: 4009727

COMMS
Computers, Comms, and Low-Grade Ciphers --
[redacted] . . . . . Oct 75

COMMUNICATIONS SATELLITE
[redacted] . . . . . Nov 75

COMPUTER
The Yawn of the Computer Age
or, When Your Terminal Is Terminal
[redacted] . . . . Jan 75
Computers, Comms, and Low-Grade Ciphers --
[redacted] . . . . . Oct 75

COMPUTER NETWORK
Computer Network Resources in C5 . . . Aug 75

COMPUTER SYSTEMS
Professionalizing in Computer Systems
[redacted] . . . . . Jun 75

COMSEC
COMSEC Familiarization - Do You Need It?
. . . . . Jun 75

COUNTRY SPECIALISTS
Letters to the Editor --
Bookbreakers; Professionalization of
Country Specialists
[redacted] . . . . . Jun 75

COURSE-EQUIVALENCY
NCS Offers Course-equivalency Tests . . Nov 75

COVERTERMS
Coverterms
Vera R. Filby . . . . . Apr 75
Letters to the Editor -- [redacted] article on
Coverterms
[redacted] . . . . . Jun 75

CRYPTANALYSIS
Cryptanalysis and Code Recovery
Marjorie Mountjoy . . . . . Sep 74
New Trends in the Teaching of Cryptanalysis
[redacted] . . . . . Nov 74

CRYPTANALYSTS
What Should You Expect?
or, The Analysis of Cryptanalysts
[redacted] . . . . . Aug 74

CRYPTANALYTICS
Puzzle -- Secret Messages, "Military
Cryptanalytics" . . . . . Dec 74

CRYPTO
More on Squaring the Page (A Crypto - TA
Function)
Frederic O. Mason, Jr. . . . . Jun 75

CRYPTOGRAMS
Secrets of the Altars -- The Moustier
Cryptograms
[redacted] . . . . . Sep 74

CRYPTOGRAPHIC
Psyching the Code Clerk --
[redacted]
L. D. Callimahos. . . . . Apr 75

CSI NEWSLETTER
Establishment of CSI Newsletter . . . . Dec 75

C5
A Guide to Central Information -- C5. . Apr 75
Computer Network Resources in C5 . . . Aug 75

DANANG
The Danang Processing Center
[redacted] . . . . . Oct 75

DATA
Data and Definitions -- Calling Things
by Their Rightful Names
[redacted] . . . . . Nov 74

DATA BASE
The TEXTA Data Base
William J. Jackson. . . . . Aug 74
How Clean Does a Data Base Need To Be?
[redacted] . . . . . Jan 75

[redacted]
The Warsaw Pact
[redacted]
Frederick W. Walton, Jr. . . . . Jul 75

DECRYPTION
[redacted]
[redacted] . . . . . Nov 75

DEFINITIONS
Data and Definitions -- Calling Things
by Their Rightful Names
[redacted] . . . . . Nov 74

[redacted]
[redacted] . . . . . Nov 75

DESKPAD
DESKPAD--A Programmer's Tool
[redacted] . . . . . Nov 75

The Devil's Dictionary. . . . . Feb 75

DICTIONARY
The Devil's Dictionary. . . . . Feb 75
Glossaries versus Dictionaries --
Which Should It Be?
Jacob Gurin . . . . . Feb 75

P.L. 86-36

EO 1.4.(C)
P.L. 86-36

EO 1.4.(C)
P.L. 86-36

P.L. 86-36

P.L. 86-36

P.L. 86-36

EO 1.4.(C)
P.L. 86-36

P.L. 86-36

DOCID: 4009727 EO 1.4.(C) P.L. 86-36

~~SECRET~~

[redacted] What? Where? Why?
[redacted] . . . . . Nov 74

[redacted] Paper on Character Stream Scanning by Machine . . . . . Oct 75

DIRECTORY
A Short Directory of Career Panels. . . Aug 74

The Do Xa Pads
Edward S. Wiley . . . . . Oct 75

DRAGON SEEDS
Vietnam Articles in Dragon Seeds . . . Oct 75

ELECTRONIC WARFARE
The Role of the Electronic Warfare Advisory Element (EWAE) of NSA
[redacted] . . . . . Jun 75
CAMINO -- Electronic Warfare Terms
[redacted] . . . . . Jul 75

ELINT
The Uses of ELINT
[redacted] . . . . . Apr 75
Letters to the Editor -- [redacted] article on ELINT
[redacted] . . . . . May 75

ENGLISH
Language in the News -- English . . . . Dec 74
Language in the News -- English . . . . Aug 75

Establishment of CSI Newsletter . . . . Dec 75

Even a 5-year-old Child
Emery W. Tetrault . . . . . Oct 74

The Faithful Echo - The Role of the State Department Interpreter
[redacted] . . . . . Feb 75

A Fix for the Language Problem?
John B. Thomas, Jr. . . . . Aug 75

Flag-Waving Programmer
George John . . . . . Dec 74

FRANCOPHONEGLOS
FRANCOPHONEGLOS Printout VI Is Available
. . . . . Oct 75

FRENCH
Language in the News -- Afrikaans, Amerind, Arabic, Chinese, French, Hebrew, Lycian, Spanish, Portuguese, Russian, Swahili
. . . . . Sep 74
The Old [redacted] Section
[redacted] . . . . . Dec 74

Gary's Colors
Caterino Garofalo . . . . . Sep 74

GLOSSARY
The New Traffic Analysis Glossary . . . Aug 74
Golden Oldies -- An Unofficial Glossary of Weasel Words. . . . . Oct 74
Glossaries versus Dictionaries -- Which Should It Be?
Jacob Gurin . . . . . Feb 75

GOLDEN OLDIES
Golden Oldies -- The Management Survey of the Philharmonic. . . . . Aug 74
Golden Oldies -- King Eusyb and Queen Deodi
[redacted] . . . . . Sep 74
Golden Oldies -- An Unofficial Glossary of Weasel Words. . . . . Oct 74
Golden Oldies -- Establishment of Molecule Superseries. . . . . Feb 75
Golden Oldies -- SIMP Tables . . . . . Jun 75
Golden Oldies -- Blue Russian
[redacted] . . . . . Nov 75 P.L. 86-36

Graphic Analysis of Linear Recursive Sequences
[redacted] . . . . . Dec 75

The Great Soviet Shipbuilding Mystery
[redacted] . . . . . Dec 75

A Guide to Central Information -- C5. . Apr 75

GUIDESMANSHIP
Guidesmanship -- or, How to Write Technical Manuals Without Actually Giving Anything Away
[redacted] . . . . . Nov 74

GULF OF TONKIN
The Gulf of Tonkin Incident
[redacted] . . . . Feb 75

GUPPY
Replacement of the GUPPY Library
[redacted] . . . . . Feb 75 P.L. 86-36

HEBREW
Language in the News -- Afrikaans, Amerind, Arabic, Chinese, French, Hebrew, Lycian, Spanish, Portuguese, Russian, Swahili
. . . . . Sep 74

HFDF
Project CARRIAGE -- Worldwide HFDF Modernization Plan
James B. Webster. . . . . Sep 74
Hooray for PMDs!
[redacted] . . . . . May 75
How Clean Does a Data Base Need To Be?
[redacted] . . . . . Jan 75

HUMAN FACTORS
Learned Organizations -- CISI Forms Special Interest Group on Human Factors
. . . . . Dec 74

IAI
Learned Organizations -- CLA Is Ten Years Old!. News from CISI, CMI, IAI . . . . . Jan 75
Learned Organizations -- CLA, IAI . . . May 75

~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4009727

EO 1.4.(c)
P.L. 86-36

In Praise of SOLITS
Louis C. Grant. . . . . Nov 75

[redacted] . . . . . Nov 75

INTERN PROGRAM
A Long Hard Look at the Intern Program -- Program Philosophy; Recruitment
Anne Exinterne. . . . . Sep 74
A Long Hard Look at the Intern Program -- Selection and Orientation
Anne Exinterne. . . . . Oct 74
A Long Hard Look at the Intern Program -- Motivation and Morale
Anne Exinterne. . . . . Nov 74
A Long Hard Look at the Intern Program -- What Happens to the Graduates?
Anne Exinterne. . . . . Dec 74
Letters to the Editor -- Intern Program
Emery W. Tetrault . . . . . Feb 75
Letters to the Editor -- Intern Program
[redacted] . . . . . Apr 75

INTERPRETER
The Faithful Echo - The Role of the State Department Interpreter
[redacted] . . . . . Feb 75

[redacted]
Psyching the Code Clerk -- [redacted]
L. D. Callimahos. . . . . Apr 75

EO 1.4.(c)
P.L. 86-36

KING EUSYB
Golden Oldies -- King Eusyb and Queen Deodi
[redacted] . . . . . Sep 74

LANGUAGE
The Language of Beisbol in Everyday Talk
[redacted]
Ramon Santiago-Ortiz. . . . . Aug 74
Language Lessons Learned--A Personal Memoir
[redacted] . . . . . Oct 75
Tactical Language Exploitation-A Lesson Learned
[redacted] . . . . Oct 75

LANGUAGE IN THE NEWS
Language in the News -- Afrikaans, Amerind, Arabic, Chinese, French, Hebrew, Lycian, Spanish, Portuguese, Russian, Swahili . . . . . Sep 74
Language in the News -- English . . . . Dec 74
Language in the News -- Language Panel, NCS, Machine Course for Linguists, CLA News, Arabic. . . . . Apr 75
Language in the News -- English . . . . Aug 75

LANGUAGE PANEL
Language in the News -- Language Panel, NCS, Machine Course for Linguists, CLA News, Arabic. . . . . Apr 75

LANGUAGE PROBLEM
A Fix for the Language Problem?
John B. Thomas, Jr. . . . . Aug 75

LEARNED ORGANIZATIONS P.L. 86-36
Learned Organizations -- CLA, CMI, CISI Prizes and Honors, Spring 1974 . . . Aug 74
Learned Organizations -- CISI Forms Special Interest Group on Human Factors . . . . . Dec 74
Learned Organizations -- CLA Is Ten Years Old! News from CISI, CMI, IAI . . . . . Jan 75
Learned Organizations -- CLA, IAI . . . May 75
Learned Organizations -- CMI, CLA . . . Jul 75
Learned Organizations -- CLA Essay Contest; CAA News . . . . Dec 75

LETTERS TO THE EDITOR
Letters to the Editor -- SRA Symposium Oct 74
Letters to the Editor -- [redacted] EO 1.4.(c) Dec 74
Letters to the Editor -- Citizens of the World P.L. 86-36
[redacted] . . . . . Feb 75 P.L. 86-36
Letters to the Editor -- Intern Program
Emery W. Tetrault . . . . . Feb 75
Letters to the Editor -- Intern Program
[redacted] . . . . . Apr 75
Letters to the Editor -- Professionalization of Bookbreakers P.L. 86-36
[redacted] . . . . . Apr 75
Letters to the Editor -- [redacted] article on ELINT
[redacted] . . . . . May 75
Letters to the Editor -- [redacted] letter on Bookbreakers
[redacted] . . . . . May 75
Letters to the Editor -- [redacted] letter on Bookbreakers
[redacted] . . . . . May 75
Letters to the Editor -- Bookbreakers; Professionalization of Country Specialists
[redacted] . . . . . Jun 75 P.L. 86-36
Letters to the Editor -- [redacted] letter on Bookbreakers . . . . . Jun 75
Letters to the Editor -- [redacted] article
[redacted] . . . . . Jun 75
Letters to the Editor -- Rebuttal
[redacted] . . . . . Aug 75
Letters to the Editor-- Typewriter keyboard . . . . . Oct 75

LEXICOGRAPHY
Some Thoughts on Lexicography
Stuart A. Buck. . . . . Sep 74

LINEAR RECURSIVE SEQUENCES
Graphic Analysis of Linear Recursive Sequences
[redacted] . . . . . Dec 75

P.L. 86-36

LINGUISTIC
Are We Wasting Linguistic Time?
[redacted] . . . . . May 75

DOCID: 4009727

LINGUISTS
Language in the News -- Language Panel, NCS, Machine Course for Linguists, CLA News, Arabic. . . . . Apr 75
Linguists -- We Need an Experts Yellow Pages! [redacted] . . . . . Aug 75
Linguists -- You Have an Expert to Call [redacted] . . . . . Oct 75
Linguists from the Melting Pot [redacted] . . . . . Dec 75

A Long Hard Look at the Intern Program -- Program Philosophy; Recruitment
Anne Exinterne. . . . . Sep 74
A Long Hard Look at the Intern Program -- Selection and Orientation
Anne Exinterne. . . . . Oct 74
A Long Hard Look at the Intern Program -- Motivation and Morale
Anne Exinterne. . . . . Nov 74
A Long Hard Look at the Intern Program -- What Happens to the Graduates?
Anne Exinterne. . . . . Dec 74

MACHINE COURSE
Language in the News -- Language Panel, NCS, Machine Course for Linguists, CLA News, Arabic. . . . . Apr 75

MACHINE INTELLIGENCE
Machine Intelligence -- Promise or Delusion? [redacted] . . . . . Jul 75

MANAGEMENT SURVEY
Golden Oldies -- The Management Survey of the Philharmonic. . . . . Aug 74

MAPS
Maps in Mind -- A Photoessay [redacted] . . . . . Dec 74

The Mission of the Signals Processing Requirements Panel [redacted] . . . . . Oct 74

MOLECULE SUPERSERIES
Golden Oldies -- Establishment of Molecule Superseries. . . . . Feb 75

[redacted] . . . . . Nov 75

More on Squaring the Page (A Crypto - TA Function)
Frederic O. Mason, Jr.. . . . Jun 75

Mum's Still the Word! ("The ULTRA Secret") [redacted] . . . . . Dec 75

The Navajo Code Talkers . . . . . Jun 75

NCS
News from NCS -- Agency Resumes Hiring of LICs; NCS Offers Course in "SIGINT Appreciation". . . . . Oct 74
Language in the News -- Language Panel, NCS, Machine Course for Linguists, CLA News, Arabic. . . . . Apr 75
NCS Offers Course-equivalency Tests . . Nov 75

The New Traffic Analysis Glossary . . . Aug 74
New Trends in the Teaching of Cryptanalysis [redacted] . . . . . Nov 74
The New Collection Criteria [redacted] . . . . . Dec 74

News from NCS -- Agency Resumes Hiring of LICs; NCS Offers Course in "SIGINT Appreciation". . . . . Oct 74

Nice Busman's Holiday for One NSA Employee
Barbara Dudley. . . . . Aug 74

1972-73--A Vietnam Odyssey [redacted] . . . . . Oct 75

NSA-CROSTIC
NSA-crostic No. 1 . . . . . Oct 75

An October Overlap [redacted] . . . . . Oct 74

The Old [redacted] Section
Horace Booth. . . . . Dec 74

One Chance in Three -- But It Worked
William Gerhard . . . . . Oct 75

[redacted] . . . . . Oct 75

ORAL REPORTING
Oral Reporting: A New Challenge for NSA [redacted] . . . . . Apr 75

OVERLAP
An October Overlap [redacted] . . . . . Oct 74

PADS
The Do Xa Pads
Edward S. Wiley . . . . . Oct 75

A Personal Comment on Winterbotham's "The ULTRA Secret"
Brig. John H. Tiltman . . . . Dec 75

PHILHARMONIC
Golden Oldies -- The Management Survey of the Philharmonic. . . . . Aug 74

PMDS
Hooray for PMDs! [redacted] . . . . . May 75

P.L. 86-36

P.L. 86-36

EO 1.4.(C)
P.L. 86-36

P.L. 86-36

EO 1.4.(C)
P.L. 86-36

P.L. 86-36

DOCID: 4009727

EO 1.4.(c)
P.L. 86-36

PORTUGUESE
Language in the News -- Afrikaans, Amerind, Arabic, Chinese, French, Hebrew, Lycian, Spanish, Portuguese, Russian, Swahili . . . . . Sep 74

PRIZES
Learned Organizations -- CLA, CMI, CISI Prizes and Honors, Spring 1974 . . . Aug 74

Processing [redacted] Communications [redacted] . . . . . Aug 75

PROFESSIONALIZATION
Letters to the Editor -- Professionalization of Bookbreakers [redacted] . . . . . Apr 75

Letters to the Editor -- Bookbreakers; Professionalization of Country Specialists [redacted] . . . . . Jun 75

PROFESSIONALIZING
Professionalizing in Computer Systems [redacted] . . . . . Jun 75

PROGRAMMER
Flag-Waving Programmer
George John . . . . . Dec 74
DESKPAD--A Programmer's Tool [redacted] . . . . . Nov 75

Project CARRIAGE -- Worldwide HFDF Modernization Plan
James B. Webster. . . . . Sep 74
Project SYMBIOSIS
Anonymous . . . . . Jun 75

A Proposal for Calendar Reform
Francis T. Leahy. . . . . Dec 74

Psyching the Code Clerk -- [redacted]
L. D. Callimahos. . . . . Apr 75

Purity of the Russian Language -- Slavophiles vs. Westernizers [redacted] . . . . Nov 74

PUZZLE
Puzzle -- Stinky Pinky . . . . . Aug 74
Puzzle -- Telephone Directory . . . . . Aug 74
Puzzle -- Telephone Recall . . . . . Oct 74
Puzzle -- Secret Messages, "Military Cryptanalytics" . . . . . Dec 74
Puzzle -- Citizens of the World . . . . Dec 74
Puzzle -- Crossed Codewords [redacted] . . . . . Jan 75
Puzzle -- Can You Make Out the Name? [redacted] . . . . . Feb 75
Puzzle -- How Many Words in "CRYPTOLOG"? . . . . . May 75
Puzzle -- [redacted] Radiotelephone [redacted] . . . . . Jun 75

Puzzle -- CRY-PTO-LOGrolling . . . . . Aug 75
Puzzle -- NSA-crostic No. 1 . . . . . Oct 75

RADIOTELEPHONE
Puzzle -- [redacted] Radiotelephone [redacted] . . . . . Jun 75

RAMASUN
A Comm Change at Ramasun Station [redacted] . . . . Apr 75

RANDOM
Typewriter Random -- A New Look [redacted] . . . . . Aug 75

RAPIDTRAN
RAPIDTRAN -- [redacted] . . . . . Jul 75

Reflections on a Translators' Conference [redacted] . . . . . Nov 74

Replacement of the GUPPY Library [redacted] . . . . . Feb 75

Re-psychling the Code Clerk [redacted] . . . . . Jul 75

REVIEW
Review of "Guide to Russian Technical Translation," by Arthur J. Salemme [redacted] . . . . . Feb 75

RIGHT-TO-LEFT TEXT
Right-to-Left Text Sorts Are Not Impossible [redacted] . . . . . Aug 74

The Role of the Electronic Warfare Advisory Element (EWAE) of NSA [redacted] . . . . . Jun 75

RUSSIAN
Language in the News -- Afrikaans, Amerind, Arabic, Chinese, French, Hebrew, Lycian, Spanish, Portuguese, Russian, Swahili . . . . . Sep 74
Purity of the Russian Language -- Slavophiles vs Westernizers [redacted] . . . . . Nov 74
Review of "Guide to Russian Technical Translation," by Arthur J. Salemme [redacted] . . . . . Feb 75

[redacted]

Golden Oldies -- Blue Russian [redacted] . . . . . Nov 75

[redacted]

Processing [redacted] Communications [redacted] . . . . . Aug 75

Secrets of the Altars -- The Moustier Cryptograms [redacted] . . . . . Sep 74

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

P.L. 86-36

P.L. 86-36

P.L. 86-36

DOCID: 4009727

SELF-PACED INSTRUCTION
Self-Paced Instruction -- "The Future Is Now"
[redacted] . . . . . Aug 74

SHIPBUILDING
The Great Soviet Shipbuilding Mystery
[redacted] . . . . . Dec 75

The [redacted] Exercise -- A Case Study
in Special Research Analysis
Vera R. Filby . . . . . Oct 74

EO 1.4.(c)
P.L. 86-36

A Short Directory of Career Panels. . . Aug 74

SIGINT USER'S HANDBOOK
The SIGINT User's Handbook
or, What's an Ishtar?
[redacted] . . . . . Jan 75

SIGNALS PROCESSING
The Mission of the
Signals Processing Requirements Panel
[redacted] . . . . . Oct 74

SIMP TABLES
Golden Oldies -- SIMP Tables . . . . . Jun 75

SOLITS
In Praise of SOLITS
Louis C. Grant. . . . . Nov 75

Some Thoughts on Lexicography
Stuart A. Buck. . . . . Sep 74

SORTS
Right-to-Left Text Sorts Are Not Impossible
[redacted] . . . . . Aug 74

SOVIET
[redacted]
[redacted] . . . . . Nov 75

The Great Soviet Shipbuilding Mystery
[redacted] . . . . . Dec 75

SPANISH
Language in the News -- Afrikaans, Amerind,
Arabic, Chinese, French, Hebrew, Lycian,
Spanish, Portuguese, Russian, Swahili
. . . . . Sep 74

EO 1.4.(c)
P.L. 86-36

SPECIAL RESEARCH ANALYSI
The [redacted] Exercise -- A Case Study
in Special Research Analysis
Vera R. Filby . . . . . Oct 74

A Spot by Any Other Name
Vera R. Filby . . . . . Aug 74

SQUARING THE PAGE
More on Squaring the Page (A Crypto - TA
Function)
Frederic O. Mason, Jr.. . . . Jun 75

P.L. 86-36

SRA SYMPOSIUM
Calling All SRAs! -- SRA Symposium
[redacted] . . . . . Aug 74
Letters to the Editor -- SRA Symposium Oct 74

STATE DEPARTMENT
The Faithful Echo - The Role of the
State Department Interpreter
[redacted] . . . . . Feb 75

STINKY PINKY
Puzzle -- Stinky Pinky . . . . . Aug 74

SWAHILI
Language in the News -- Afrikaans, Amerind,
Arabic, Chinese, French, Hebrew, Lycian,
Spanish, Portuguese, Russian, Swahili
. . . . . Sep 74

SYMBIOSIS
Project SYMBIOSIS . . . . . Jun 75

TA
P.L. 86-36
TA, Handmaiden of CA
Frederic O. Mason, Jr.. . . . May 75
More on Squaring the Page (A Crypto - TA
Function)
Frederic O. Mason, Jr.. . . . Jun 75
Automation of a TA Process
Tim Murphy. . . . . Oct 75

TACTICAL
IRONHORSE--A Tactical SIGINT System
[redacted] . . . . . Oct 75
Tactical Language Exploitation-
A Lesson Learned
[redacted] . . . . Oct 75

TEACHING
New Trends in the Teaching of Cryptanalysis
[redacted] . . . . . Nov 74

TECHNICAL MANUALS
Guidesmanship -- or, How to Write
Technical Manuals Without Actually
Giving Anything Away
[redacted] . . . . . Nov 74

P.L. 86-36

TELEPHONE
Puzzle -- Telephone Directory . . . . . Aug 74
Puzzle -- Telephone Recall . . . . . Oct 74

[redacted]
UNNA, [redacted]
[redacted] . . . . . Jan 75

TERMINAL
The Yawn of the Computer Age
or, When Your Terminal Is Terminal
[redacted] . . . . Jan 75

TEXTA
P.L. 86-36
The TEXTA Data Base
William J. Jackson. . . . . Aug 74

Too Many Garbles
[redacted] . . . . Jul 75

TRAFFIC ANALYSIS
The New Traffic Analysis Glossary . . . Aug 74

TRANSLATION
Review of "Guide to Russian Technical Translation," by Arthur J. Salemme
[redacted] . . . . . Feb 75
RAPIDTRAN --
[redacted] . . . . . Jul 75

TRANSLATORS' CONFERENCE
Reflections on a Translators' Conference
[redacted] . . . . . Nov 74

TRANSPOSITION
Twenty Years of Transposition
[redacted] . . . . . Aug 75

TYPEWRITER
Typewriter Random -- A New Look
[redacted] . . . . . Aug 75
Letters to the Editor --
Typewriter keyboard . . . . . Oct 75

ULTRA
A Personal Comment on Winterbotham's "The ULTRA Secret"
Brig. John H. Tiltman . . . . Dec 75
ULTRA Was Secret Weapon That Helped Defeat Nazis
P. W. Filby . . . . . Dec 75
Mum's Still the Word! ("The ULTRA Secret")
[redacted] . . . . Dec 75

UNNA
UNNA, A Telex Collector
[redacted] . . . . . Jan 75

The Uses of ELINT
[redacted] . . . . . Apr 75

[redacted] . . . . . Oct 75

VIETNAM
Vietnam Articles in Dragon Seeds . . . Oct 75
1972-73--A Vietnam Odyssey
[redacted] . . . . . Oct 75

VOYNICH
The Voynich Manuscript -- Third Theory
Doris E. Miller . . . . . Aug 75
[redacted] . . . . . Oct 75

WARSAW PACT
[redacted] . . Jul 75

WEASEL WORDS
Golden Oldies -- An Unofficial Glossary of Weasel Words. . . . . Oct 74

What Should You Expect?
or, The Analysis of Cryptanalysts
[redacted] . . . . . Aug 74
What Are We About? (Fragments, Figments, or What?)
[redacted] . . . Dec 75
What is a Collector?
[redacted] . . . . . Aug 74

When Censorship Backfires
[redacted] . . . . . Nov 75

Where Does "Does" Come From?
Emery W. Tetrault . . . . . Jun 75

The Winnah -- Kid Apostrophe! . . . . . Oct 75

The Yawn of the Computer Age
or, When Your Terminal Is Terminal
[redacted] . . . . Jan 75

YELLOW PAGES
Linguists -- We Need an Experts Yellow Pages!
[redacted] . . . . . Aug 75

[redacted]
The Gulf of Tonkin Incident . . . . . Feb 75
Tactical Language Exploitation-
A Lesson Learned . . . . . Oct 75

[redacted]
Graphic Analysis of Linear Recursive Sequences. . . . . Dec 75

Anonymous
Project SYMBIOSIS . . . . . Jun 75

[redacted]
Self-Paced Instruction -- "The Future Is Now" . . . . . Aug 74

[redacted]
Re-psychling the Code Clerk . . . . . Jul 75

[redacted]
Letters to the Editor -- Professionalization of Bookbreakers. . . . . Apr 75

[redacted]
The Uses of ELINT . . . . . Apr 75

[redacted]
The Role of the Electronic Warfare Advisory Element (EWAE) of NSA. . . . . Jun 75

[redacted]
The Old [redacted] Section. . . . . Dec 74

[redacted]
Letters to the Editor -- [redacted] article on ELINT . . . . . May 75

[redacted]
Maps in Mind -- A Photoessay. . . . . Dec 74

Stuart A. Buck
Some Thoughts on Lexicography . . . . . Sep 74

[redacted]
The New Collection Criteria . . . . . Dec 74
What is a Collector?. . . . . Aug 74

L. D. Callimahos
Psyching the Code Clerk -- [redacted] Apr 75

[redacted]
The Danang Processing Center. . . . . Oct 75

[redacted]
IRONHORSE--A Tactical SIGINT System. . Oct 75

[redacted]
DESKPAD--A Programmer's Tool. . . . . Nov 75

[redacted]
Linguists -- You Have an Expert to Call
Co-author: Rhea Nagle. . . . . Oct 75

Derek K. Craig
COMINT Analysis of [redacted] . . . Sep 74

[redacted]
Hooray for PMDs!. . . . . May 75

[redacted] . . Oct 75

[redacted]
The Mission of the Signals Processing
Requirements Panel. . . . . Oct 74

Barbara Dudley
Nice Busman's Holiday for One NSA Employee
. . . . . Aug 74

[redacted]
What Should You Expect?
or, The Analysis of Cryptanalysts. . Aug 74
Secrets of the Altars -- The Moustier
Cryptograms. . . . . Sep 74
An October Overlap. . . . . Oct 74
Twenty Years of Transposition . . . . . Aug 75

[redacted]
CAMINO News . . . . . Feb 75
Machine Intelligence -- Promise or Delusion?
. . . . . Jul 75
CAMINO -- Electronic Warfare Terms. . . Jul 75

[redacted]
Puzzle -- Can You Make Out the Name?. . Feb 75

[redacted]
Puzzle -- [redacted] Radiotelephone [redacted]
. . . . . Jun 75

Anne Exinterne
A Long Hard Look at the Intern Program --
Program Philosophy; Recruitment. . . Sep 74
A Long Hard Look at the Intern Program --
Selection and Orientation. . . . . Oct 74
A Long Hard Look at the Intern Program --
Motivation and Morale. . . . . Nov 74
A Long Hard Look at the Intern Program --
What Happens to the Graduates? . . . Dec 74

[redacted]
[redacted] What? Where? Why? . . . Nov 74

P. W. Filby
ULTRA Was Secret Weapon That Helped Defeat
Nazis. . . . . Dec 75

Vera R. Filby
A Spot by Any Other Name. . . . . Aug 74
The [redacted] Exercise -- A Case Study
in Special Research Analysis . . . . Oct 74
The Apostrophe -- Some Thought's . . . Nov 74
Coverterms. . . . . Apr 75

[redacted]
Typewriter Random -- A New Look . . . . Aug 75

Caterino Garofalo
Gary's Colors . . . . . Sep 74

William Gerhard
One Chance in Three -- But It Worked. . Oct 75

[redacted]
Linguists from the Melting Pot. . . . . Dec 75

Louis C. Grant
In Praise of SOLITS . . . . . Nov 75

Jacob Gurin
Glossaries versus Dictionaries --
Which Should It Be?. . . . . Feb 75

[redacted]
Letters to the Editor --
Bookbreakers; Professionalization of
Country Specialists. . . . . Jun 75

[redacted]
Character Building in the People's
Republic of China
Co-author: [redacted] . . . . . Oct 74

[redacted]
Letters to the Editor -- [redacted] article on
Coverterms . . . . . Jun 75

[redacted]
Puzzle -- Crossed Codewords . . . . . Jan 75

[redacted]
Data and Definitions -- Calling Things
by Their Rightful Names. . . . . Nov 74

[redacted]
Mum's Still the Word! ("The ULTRA Secret")
. . . . . Dec 75

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

P.L. 86-36

P.L. 86-36

EO 1.4.(c)

P.L. 86-36

DOCID: 4009727

Mary Roberta Irwin
Are We Wasting Linguistic Time? . . . . May 75

William J. Jackson
The TEXTA Data Base . . . . . Aug 74
An Approach to Callsign Analysis. . . . Dec 74

[redacted]
New Trends in the Teaching of Cryptanalysis
. . . . . Nov 74

George John
Flag-Waving Programmer. . . . . Dec 74

[redacted]
Purity of the Russian Language --
Slavophiles vs. Westernizers . . . . Nov 74

[redacted]
"Codeword" or "COMINT Channels"? . . . May 75

[redacted]
When Censorship Backfires . . . . . Nov 75

[redacted]
Reflections on a Translators' Conference. Nov 74

Francis T. Leahy
A Proposal for Calendar Reform. . . . . Dec 74

[redacted]
The Yawn of the Computer Age
or, When Your Terminal Is Terminal . Jan 75

[redacted]
Golden Oldies -- King Eusyb and Queen Deodi
. . . . . Sep 74

Frederic O. Mason, Jr.
TA, Handmaiden of CA. . . . . May 75
More on Squaring the Page (A Crypto - TA
Function). . . . . Jun 75
Abdul and His 40 Tanks. . . . . Aug 75

[redacted]
Professionalizing in Computer Systems . Jun 75

[redacted]
Basic Patterns of [redacted] Codes and Ciphers
. . . . . Feb 75

[redacted]
Linguists -- We Need an Experts Yellow Pages!
. . . . . Aug 75

Doris E. Miller
The Voynich Manuscript -- Third Theory. Aug 75

Marjorie Mountjoy
Cryptanalysis and Code Recovery . . . . Sep 74

Tim Murphy
Automation of a TA Process. . . . . Oct 75

[redacted]
Letters to the Editor --
[redacted] letter on Bookbreakers. . May 75
Letters to the Editor -- Rebuttal . . . Aug 75

[redacted]
Linguists -- You Have an Expert to Call
Co-author: [redacted] . . . . . Oct 75

[redacted]
1972-73--A Vietnam Odyssey
Co-author: [redacted] . . . . . Oct 75

[redacted] P.L. 86-36
The SIGINT User's Handbook P.L. 86-36
or, What's an Ishtar?. . . . . Jan 75

[redacted]
The Faithful Echo - The Role of the
State Department Interpreter . . . . Feb 75

[redacted]
RAPIDTRAN --
[redacted] . . Jul 75
Language Lessons Learned--A Personal Memoir
. . . . . Oct 75

[redacted] EO 1.4.(C)
Character Building in the People's P.L. 86-36
Republic of China
Co-author: [redacted] . . . . . Oct 74

[redacted] P.L. 86-36
A Comm Change at Ramasun Station. . . . Apr 75

[redacted]
Golden Oldies -- Blue Russian . . . . . Nov 75

[redacted]
The Language of Beisbol in Everyday Talk
Co-author: Ramon Santiago-Ortiz. . . . . Aug 74
The Case for COMINT Readers . . . . . Jan 75
Too Many Garbles. . . . . Jul 75

Ramon Santiago-Ortiz
The Language of Beisbol in Everyday Talk
Co-author: [redacted] . . . . Aug 74 P.L. 86-36

[redacted]
Calling All SRAs! -- SRA Symposium . . Aug 74

[redacted]
[redacted] Nov 75
EO 1.4.(C)
[redacted] P.L. 86-36
Letters to the Editor -- Intern Program Apr 75

[redacted]
1972-73--A Vietnam Odyssey
Co-author: [redacted] . . . . . Oct 75 P.L. 86-36

[redacted]
How Clean Does a Data Base Need To Be?. Jan 75

[redacted]
Processing [redacted] EO 1.4.(C)
Communications . . . . . P.L. 86-36 Aug 75

[redacted]
Replacement of the GUPPY Library. . . . Feb 75

P.L. 86-36

DOCID: 4009727

P.L. 86-36

Emery W. Tetrault
Even a 5-year-old Child . . . . . Oct 74
Letters to the Editor -- Intern Program. . Feb 75
Where Does "Does" Come From? . . . . . Jun 75

[redacted]
Guidesmanship -- or, How to Write Technical Manuals Without Actually Giving Anything Away . . . . . Nov 74

[redacted]
Computers, Comms, and Low-Grade Ciphers -- [redacted] . . Oct 75

John B. Thomas, Jr
A Fix for the Language Problem? . . . . Aug 75

Brig. John H. Tiltman
A Personal Comment on Winterbotham's "The ULTRA Secret" . . . . . Dec 75

[redacted]
Review of "Guide to Russian Technical Translation," by Arthur J. Salemme . Feb 75

[redacted]
Letters to the Editor -- [redacted] letter on Bookbreakers. . May 75

[redacted]
Oral Reporting: A New Challenge for NSA Apr 75

[redacted]
UNNA, [redacted] . . . . . Jan 75

[redacted]
The Warsaw Pact [redacted] . . . . . Jul 75

James B. Webster
Project CARRIAGE -- Worldwide HFDF Modernization Plan . . . . . Sep 74

[redacted]
[redacted] . . . Nov 75

LCDR James T. Westwood
What Are We About? (Fragments, Figments, or What?). . . . . Dec 75

Edward S. Wiley
The Do Xa Pads . . . . . Oct 75

[redacted]
The Great Soviet Shipbuilding Mystery . Dec 75

[redacted]
Letters to the Editor -- Citizens of the World. . . . . Feb 75

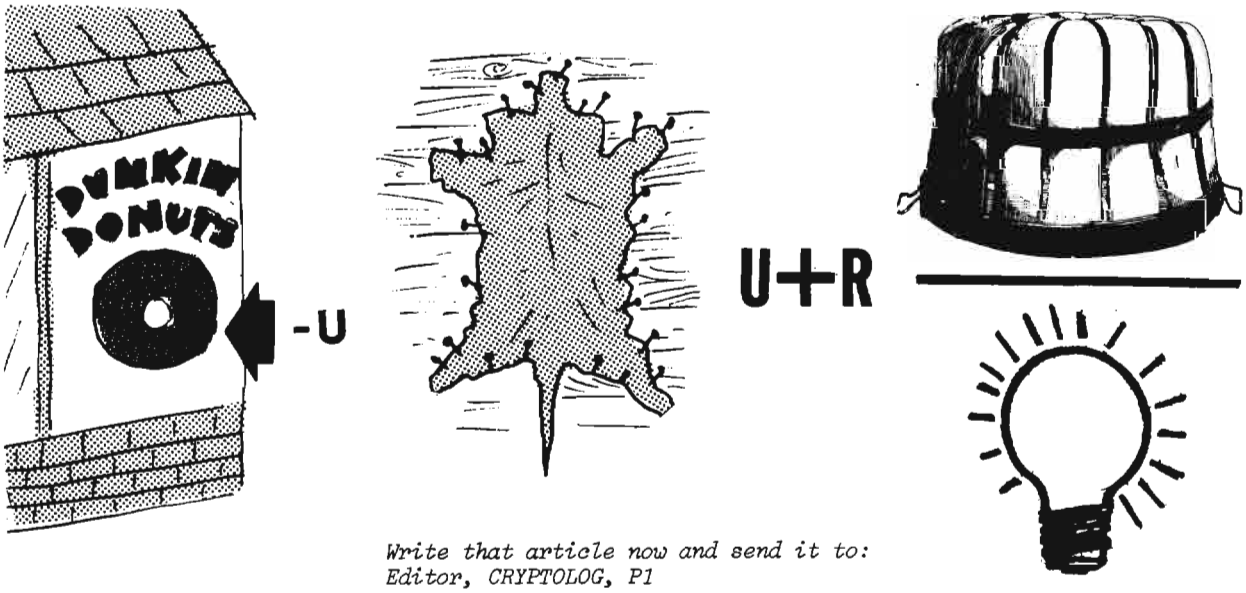
[redacted]
Right-to-Left Text Sorts Are Not Impossible . . . . . Aug 74

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

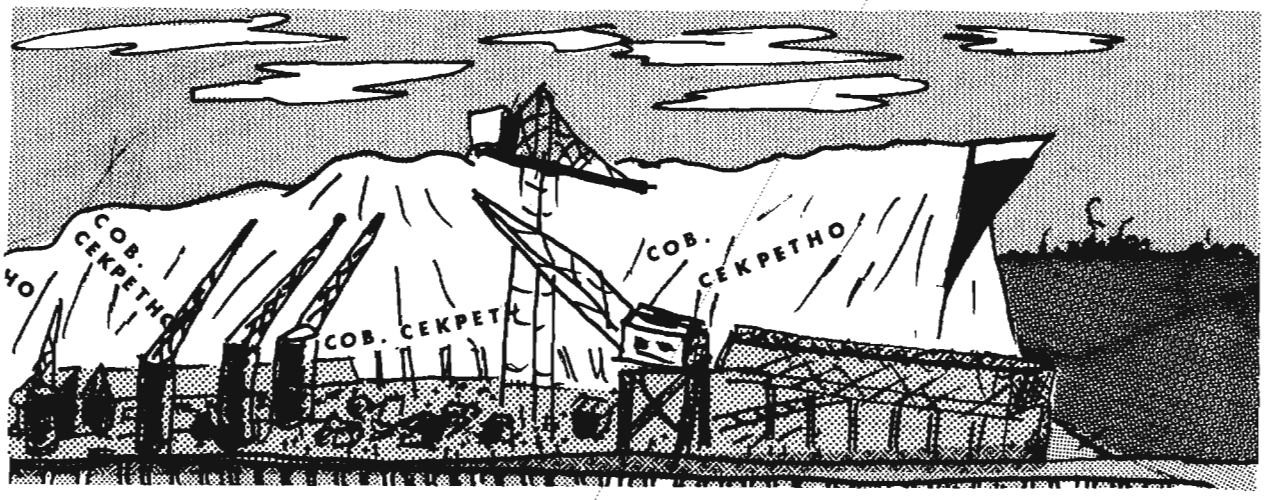
CRYPTOLOG Rebus

If your name is not included in the list of authors' names, and you have an idea for an article about a subject that hasn't been dealt with yet in CRYPTOLOG:



Write that article now and send it to: Editor, CRYPTOLOG, P1

P.L. 86-36



THE GREAT SOVIET SHIPBUILDING MYSTERY

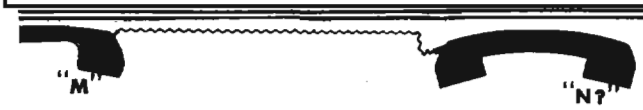
[redacted] P16

EO 1.4.(c)
P.L. 86-36

[redacted]

DOCID: 4009727

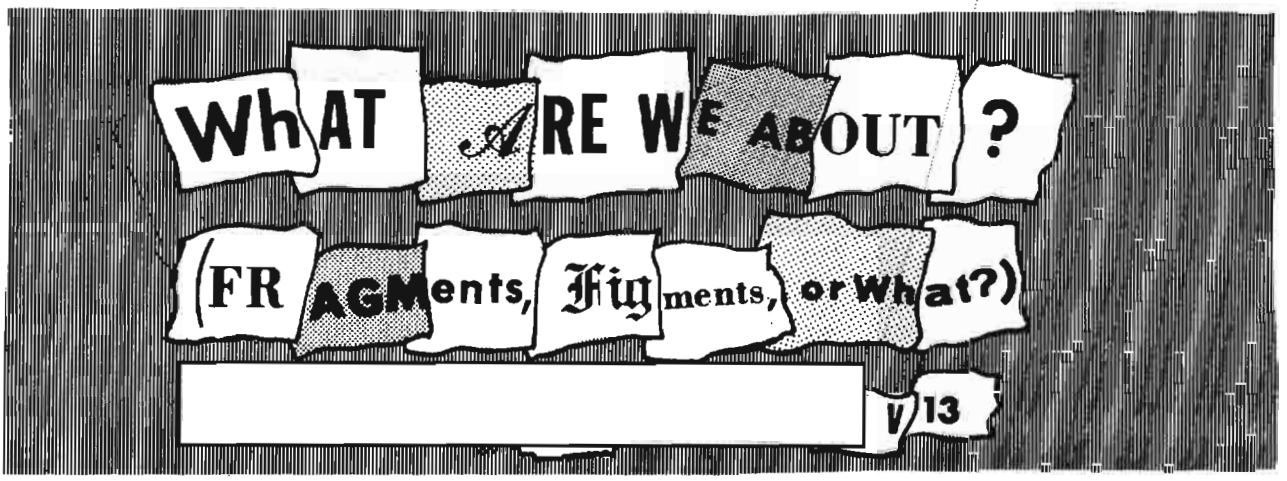
Remember that in the Soviet Union, too, engineers don't do things the way anybody else does.



Editor's note: Russian phonetic alphabets, like English ones, reduce ambiguity ("BORIS" sounds different from "VLADIMIR," just as "Mary" sounds different from "Nancy"). Since phonetic alphabets are not used universally, transcribers of Russian voice often have as much trouble distinguishing between "BEh" (the name of the letter) and "VEh" as we ordinary telephone users have in distinguishing between English "em" and "en." But the transcriber of Russian voice has yet another problem (those Russian engineers again!). The names of Latin letters, as spoken in Russian, don't sound like "ay," "bee," "see" at all. Instead, they are based on the French names of the letters. Hence, Latin H, as pronounced by a Russian engineer, is not like the English "aitch," but is "ASh" (French "ache"); Y is not "wye," but "IGREK" (French "y grec").

EO 1.4.(c)
P.L. 86-36

DOCID: 4009727 P.L. 86-36



The collection and dissemination of defense intelligence, or any other kind of intelligence, does not have to be especially complicated, so long as certain fundamental principles and goals are kept in mind. Defense intelligence, in which NSA/CSS and the Service Cryptologic Services are heavily involved, should seek to answer certain elemental questions in peacetime, wartime, or several other somewhat nebulous "times" between peace and war. These questions include:

- *Do we have* an enemy/adversary? If we do, *who* is he and *why* is he an opponent?
- *Where* is he and in what *strength?*
- What are his *intentions?*
- What are his perceptions of himself, *his own purposes and goals?*
- Are his intentions *consistent* with his strength (capability)? If not, might he be practicing *deception?*

Within defense intelligence, the business of signals intelligence is to "read the enemy's mail." This assumes that there *is* a bona fide enemy. Given the U.S. national interests, reading the enemy's mail requires a massive effort. For one thing, it takes a vast amount of mail to yield real nuggets of value on a continuing basis. It follows that, if the processing and reporting effort ever catches up with the collection effort, we would be in real trouble because we would certainly have the cart before the horse. There is, however, a sometimes overlooked proviso in this relationship: Any major SIGINT effort whose thrust is not in line with reading the enemy's mail (in an admittedly broad sense) is probably superfluous and ought to be redirected or abolished, because resources are limited and we must, therefore, keep expenditures of those resources tied to our fundamental purposes.

Of course, "reading the mail" is a figurative phrase. It does not mean just CA and TA. It means all that we do with men and machines that allows SIGINT to work its effectiveness in terms of timeliness, uniqueness, and fidelity, that is, the faithful reflection of the enemy's intentions and activities.

Intelligence, in whatever form and from whatever source, is a service provided to decision-makers. Decision-makers are civilian and military officials with distinct responsibility and personal accountability for solving problems that affect the public welfare. To make effective deployment of the people and property constituting their responsibility, the decision-makers need certain information, much of which we have come to call *intelligence*. But this intelligence is not an end in itself. It does not exist to promote and serve itself. It exists to give decision-makers the best it can provide in the way of current, accurate, reliable information to answer the vital questions they have to answer. Additionally, and by its very nature, intelligence must be anonymous and quiet. A secret is best kept by not revealing it. Mr. Colby was recently quoted as saying, "Intelligence. . .will not work if exposed."

There is no small amount of confusion and resultant ineffectiveness at large in the intelligence business today because of the tendency of intelligence producers to provide intelligence users with too much, too fast, too often -- that is, because of the "shotgun" approach. This tendency results from our attempt to cover ourselves against the possibility that we might fail to tell somebody something that he really needs to know. Morever, because we *collect* a lot of intelligence, we feel compelled to *process* a lot. That leads to wanting to *report* a lot, and, in turn, to inundating the user with so much intelligence that he cannot give certain portions of it the necessary attention. This gives rise to certain attendant problems: This tendency to broadfire intelligence then leads to the tendency for intelligence producers to dictate, however subtly or indirectly, how much of what kind of intelligence the users shall receive and, moreover, in what format and at

what rate they shall receive it. These tendencies are especially visible in terms of SIGINT support to military commanders. The result in this instance is that we make military commanders passive recipients of intelligence. An active role, with commanders saying, "This is what I want to know and this is how much I want," is precluded by a deluge of "This is what we want you to have." If this is drawn out to its ultimate conclusion, the presumed goal of "increased accessibility to intelligence product by decision-makers at all levels" is unattainable.

Those who pay close attention to dissemination might disclaim the existence of these tendencies. They might attempt to explain the present situation by splitting intelligence into "tactical" and "strategic." But the difference between "tactical" and "strategic," to my mind, lies not so much in the nature and content of the intelligence itself, as in the level or scope of the decision-making that the intelligence is supposed to serve. For example, was it tactical or was it strategic intelligence which foretold the Chinese crossing of the Yalu River into Korea? Obviously, it was both: it was tactically useful intelligence to the field commanders in Korea, and it was also strategically useful intelligence to the President and his Cabinet. We do our SIGINT profession an immense disservice when we fragment our efforts and our product into pieces and parts in an attempt to serve two or more users, for example, the tactical commander and the national decision-maker.

Perhaps we should devote some time away from the production process in order to get from all our users a clearer idea of what they would consider to be useful. Intelligence production today is much more efficient than ever before, given our increasing reliance on automatic data processing. Whether it is also effective is another question. Effectiveness is the accomplishment of objectives -- the satisfaction of requirements. Machines are not a substitute for human judgment. Decision-makers want to know that human judgment has been brought to bear to weigh the significance of the intelligence that is being machine-processed so efficiently for them.

Tactically, the fundamental questions have not changed since Moses sent spies into the Land of Canaan: Where is the enemy and in what strength? Strategically, basic questions persist: What are our interests and what and how much do we need to know about threats to those interests?

What are we about, then? We are about the business of providing intelligence service to decision-makers. We ourselves are not those decision-makers and we must resist the tendency to confuse roles. It is not in the nature of our business to decide what is strategic and what is tactical. We have skills and facilities that can respond to intelligence needs at various levels, often simultaneously, but not by saturation.

SIGINT is part of a larger intelligence business which, itself, requires us intelligence producers to integrate our efforts and to tailor our production and dissemination to answer the fundamental, but related, questions posed by a variety of users. Those users can best be served from the same, single set of resources if we all appreciate what we are about.

CSI news

NSA COMPUTER SYSTEMS INTERN PROGRAM

The Intern Panel Advisory Board (IPAB) has established a new monthly publication, the *Computer Systems Intern Newsletter*, in order to provide "lines of communication both to and from the Interns themselves" and "to better inform and advise those associated with the Computer Systems Intern Program." The publication is classified FOR OFFICIAL USE ONLY and began with the September 1975 issue.

Anyone who would like to receive back issues or to be put on the distribution list should contact the Editor, [redacted] R214, 3460s or 3469s.

~~(FOUO)~~

P.L. 86-36

DOCID: 4009727

LINGUISTS FROM THE MELTING POT

By [redacted] P.L. 86-36

For several years, NSAers who grade language hiring examinations have noted that people's names do not always match up with their expected language ability: an applicant named, say, Yamashita can score horrendously on the Japanese hiring examination, and someone named Olivetti can do just as badly on the Italian. But it is often difficult to convince managers commissioned to "solve the language problem" that the solution to, say, the "Russian language problem" is not just a matter of running out and hiring 100 American citizens with names like Ivanov and Fedorenko. The following article by [redacted] (NSA retiree), which is reprinted from *Keyword* (November 1971), deals with some of the reasons why Americans with foreign surnames often show a surprising lack of knowledge about the language they supposedly picked up at their mother's or grandmother's knee. P.L. 86-36

It is a common belief that since a large part of the United States population is made up of immigrants and the children of immigrants there is a ready source of foreign-language talent for any emergency. To a degree this is true, but the source has many limitations. Any language must undergo changes if its speakers are moved to a strange environment, and the speech of the immigrants to the United States is no exception.

If you examine the "Help Wanted" section of the German-American press, for example, you will find a large number of English words used to designate skills or crafts. At first there seems to be no pattern in the choice of German or English words, but the existence of Backergeselle (journeyman baker) *in one advertisement not far from another that seeks an* erstklassigen body-and-fender-Mann (first-class body and fender man) *suggests that the borrowings are in response to a world of labor in which there is a greater, or perhaps only different, specialization. For the unfamiliar specialty the immigrant has a choice of coining a new word in his own language, or simply of borrowing directly from the other language. There are still other means of meeting the problem.*

The book I Trapiantati (The Transplanted), *written by Giuseppe Prezzolini, an Italian foreign correspondent in New York, and published by Longanesi & Co., Milano, 1963, contains two chapters dealing with this subject as it concerns Italian-Americans. Since the general situation presented may be considered typical of many immigrant groups, I have gisted them briefly below.*

Italians who visit the United States and come in contact with others who have settled here for one or two generations are amazed, puzzled, and sometimes horrified at the language they hear used by those who, like them, call themselves Italians. It is the same impression as that received by visitors, journalists, and consular employees who came here in decades past. What they heard was not Italian, it was not dialect, nor was it even English; still it was at the same time a little Italian, a little dialect (and this varied from place to place and sometimes from person to person), but it regularly revealed an English-language base, pronounced in the Italian fashion, that is to say an English root, with the round, vowel endings of Italian. For example there was:

contrattore	contractor
la tracca	track
la grosseria	grocery
il bordante	boarder

Their amazement increased when they found this jargon written (often only approximately) in restaurant menus, the classified ads of Italian-American newspapers, and even in official documents of American authorities who wanted to be understood by Italian immigrants. "American Italian" was a *deformation of English* rather than an adaptation of Italian. It was the result of the effort made by a mass of poor and ignorant country people, dependent upon employers who spoke a foreign language, to make themselves understood by the latter and by their own fellow workers.

Anthony Turano, an American writer of Italian origin, observed very correctly that the rural origin of most immigrants made a mechanical vocabulary difficult for them. To express their needs the southern Italian peasants were compelled to use English terms, since they had never known the Italian equivalents. But in adopting the English terms they transformed them, as best they could, by making them phonetically similar to Italian. Turano distinguished three categories of borrowings:

DOCID: 4009727

- words remote from the immigrant's former life:

sexa, sescia	(railroad) section
rancio	ranch
rodomastro	roadmaster

- words for things unknown to him before he came to America:

fensa	fence
morgheggio	mortgage

- words that stuck in the immigrant's mind by dint of constant repetition, even though he knew the corresponding Italian words:

stritto	street
denso	dance
carro	car

There is also a well-known linguistic phenomenon by which a people when it accepts a foreign word finds one in its own language which is similar to it and which it adapts to the new use even though it may have a completely different meaning. For example,

sciabola	(saber)	shovel[1]
olivetta	(kind of sausage)	elevator, elevated
tonno	(tuna fish)	tunnel

At times the marriage of English and Italian involves a dialect, as in the case of *coppastese* (Neapolitan *'ncuop* + English *stairs*), *upstairs;* or *coppetane* (*'ncuop* + English *town*), *uptown.* The Sicilians, however, do not use this expression, but instead say *oppitauni.*

In making a list of words in the American Italian jargon, it is easy to see that the proportion of adjectives to nouns is very small -- much smaller than in either Italian or English. The immigrant had to be able to express *pezze*[2] (dollars), or *bosso* (boss), but not necessarily "pretty" or "good" or "true" or "false." *Orre!* (Hurray!), an expression from the American-Italian variety shows, barely reveals a feeling of admiration, and *naise* (nice) a favorable opinion.

At first, newspapers in the Italian language adhered fairly closely to standard Italian, but after about 1900 the flood of classified advertisements made it impossible to conceal or translate the jargon of the Italian-American working man. In the *Bolletino della Sera* in 1917, advertisements are found for:

sceperi	shapers (of garments)
pressatori	pressers
sottopressatori	pressers' helpers

There were also to be seen advertisements for a *mezzo-barista* (a man to work half a day in a bar). In these pages a country place was always a *farma* (farm). Heating was done with *stima* (steam, but meaning in Italian *esteem*), and a frequent advertisement was for sale of a *casa senza stima* -- a house without heat or without esteem, depending on how well you understood American English.

This occurs less and less frequently. Such expressions have almost disappeared from the classified advertisements of *Il Progresso Italo-Americano,* not because the older generation doesn't still use them, but because that generation no longer has to work. The new generation of Italians who are looking for work know Italian pretty well and do not need the job opportunities translated into jargon. Nobody is trying to buy a *fruttistenne* (fruit stand) any more.

Prezzolini feels that the whole of this interlingua will probably have ceased to exist within a few generations, since the more recent immigrants (much fewer in number) arrive under quite different circumstances. In Italy they have learned the logical bases of the Italian language (it must be remembered that a large part of the older immigration was illiterate) and here, as soon as they go to school -- even the adults -- they learn English and are (quoting Prezzolini) the first to be horrified at the crude linguistic mixture of their predecessors. Undoubtedly, the language he describes will vanish since it was based on the southern dialects of Italian and was the hasty creation of peasants abruptly thrust into an urban world. The newer immigrants more frequently speak standard Italian and are literate, often cultured people. So long as their Italian is a tool used in a foreign society, though, it must adapt, and it will evolve into an American Italian much different from the parent language.

With some exceptions, the immigrants of any nationality are much more concerned with earning a living, raising a family, buying a car, or any of a host of other things than they are in preserving the purity of their native languages. Their children will necessarily speak a truncated language, adequate for the needs of the family or neighborhood, but shot through with words borrowed or transformed from English. The value of the family-trained linguist to SIGINT should not be underestimated because of these limitations, but at the same time it should be recognized that this source produces only raw material that must be trained and developed.

[1]Another observer mentioned his amazement at being told by an immigrant countryman that there was plenty of work in the United States for a man who knew how to use *picca e sciabola,* which in Italian means "pike and saber," but in American Italian, "pick and shovel." (R.E.G.)

[2]*Pezze* may be used because of Spanish *peso.* The word was commonly used in Nevada in a rudimentary Spanish-Italian jargon used by immigrant laborers of both nationalities when working together. *Scudi* and *dollari* were used by other Italian speakers, as I recall. (R.E.G.)

DOCID: 4009727

CLA ESSAY CONTEST

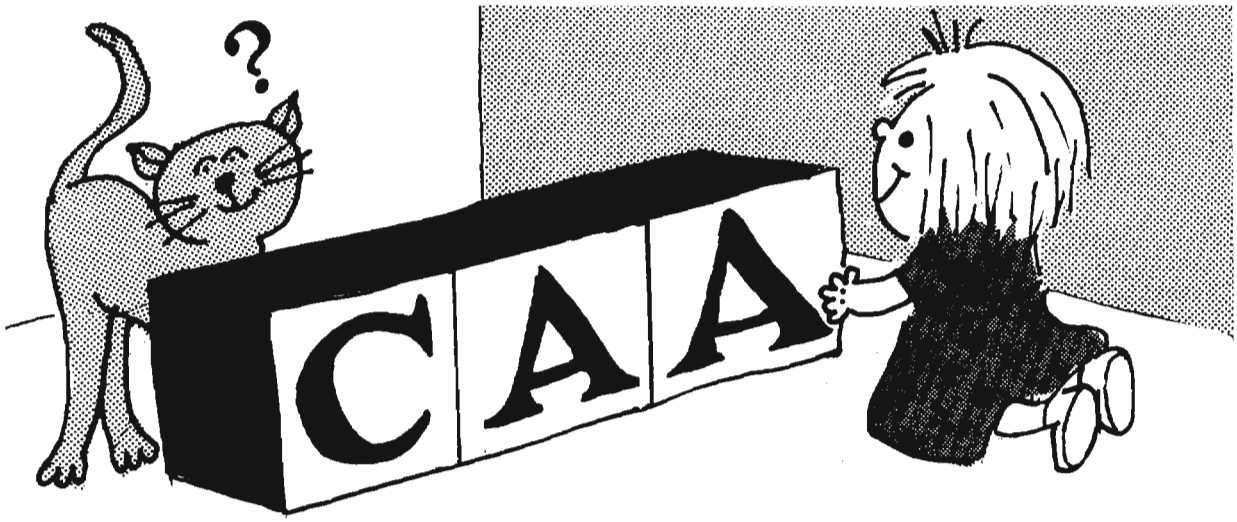
The tenth annual essay contest of the Crypto-Linguistic Association is now open. Papers will be accepted until 19 March 1976. A panel of three judges will select the three best, which will be awarded prizes of $100, $50, and $25 at the CLA's spring meeting. Every entry will be considered for publication in whichever of the Agency publications is most appropriate for its content and style.

The purpose of the contest is to encourage writing on topics concerning application of linguistic knowledge to the solution of Agency-related problems. Any writing on cryptology or a significantly related topic may be entered. Papers may be classified up to TOP SECRET CODEWORD. Any NSA or SCA employee (CLA member or nonmember) and any nonemployee CLA member may enter the contest.

Three copies of the manuscript (preferably typed), together with any necessary graphics, should be submitted to the CLA Secretary, [redacted] *Room B5B21, Tel. 8560s.*

P.L. 86-36

(UNCLASSIFIED)



CAA-What's that?

"That" is the Communications Analysis Association, one of the Agency's Learned Organizations. The CAA was established in 1968 "to promote increased professionalism in the career fields of Traffic Analysis and SIGINT Research" by encouraging professional contact among its members and specialists in related fields; by conducting workshops and lectures; by encouraging the writing of technical papers to document the disciplines; and by recognizing those who advance the art and science of traffic analysis and SIGINT research. Membership in the CAA was originally restricted to professionals and aspirants in TA and SR in the U.S. Cryptologic family and collaborating agencies, but it was later opened to those in the related fields of Signals Collection, Signals Analysis, Cryptanalysis, etc. At one time the Association published the technical magazine *COMMAND*, now incorporated into *CRYPTOLOG*.

So far this 1975-1976 lecture year, the CAA has sponsored the following lectures:

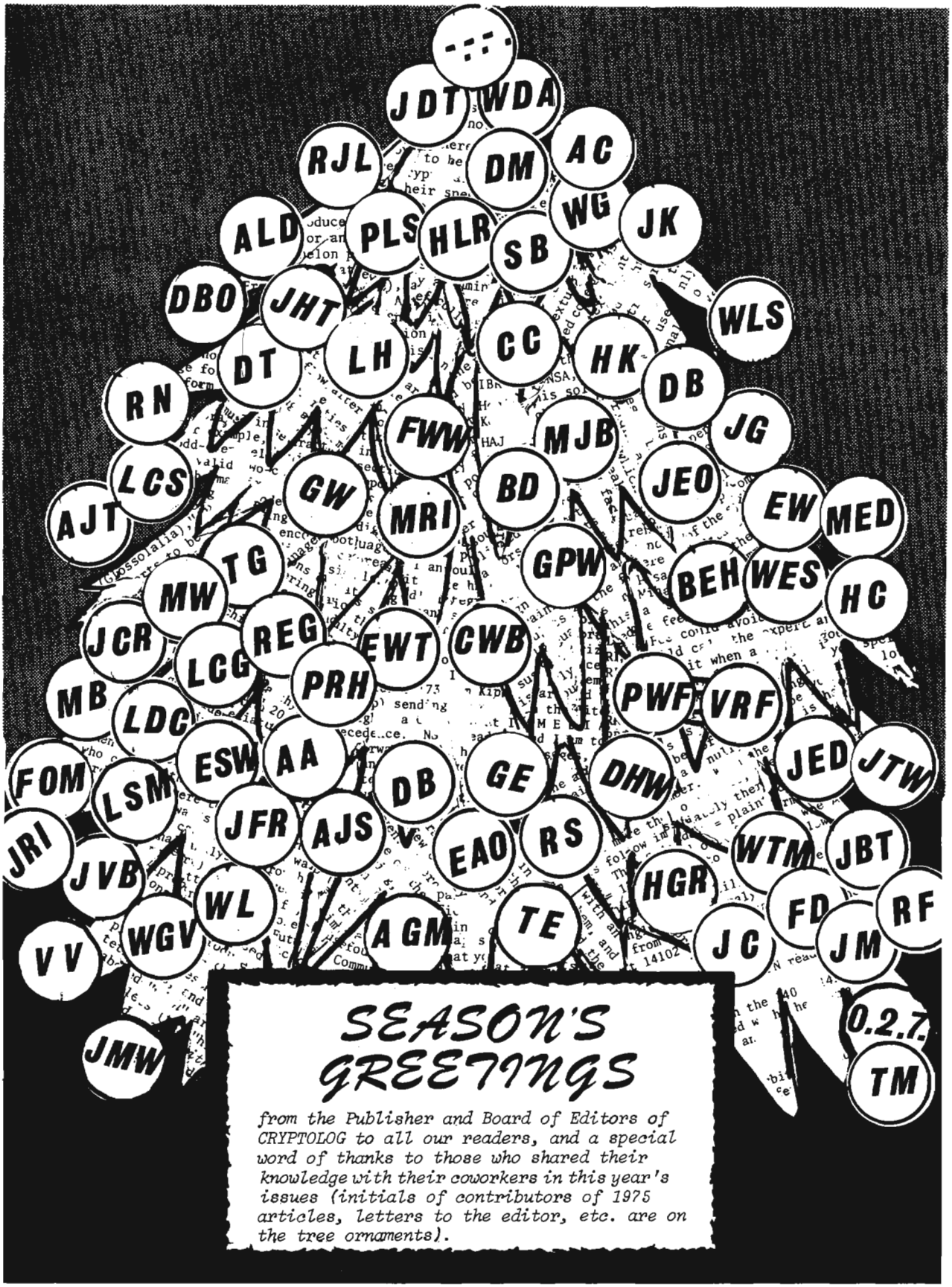
- "GUARDRAIL" (Col. Norman Campbell),
- "Changing Emphasis in the USAFSS" (Maj. Gen. H. P. Smith), and
- "SIGINT in Vietnam: Lessons Unlearned" [redacted]

P.L. 86-36

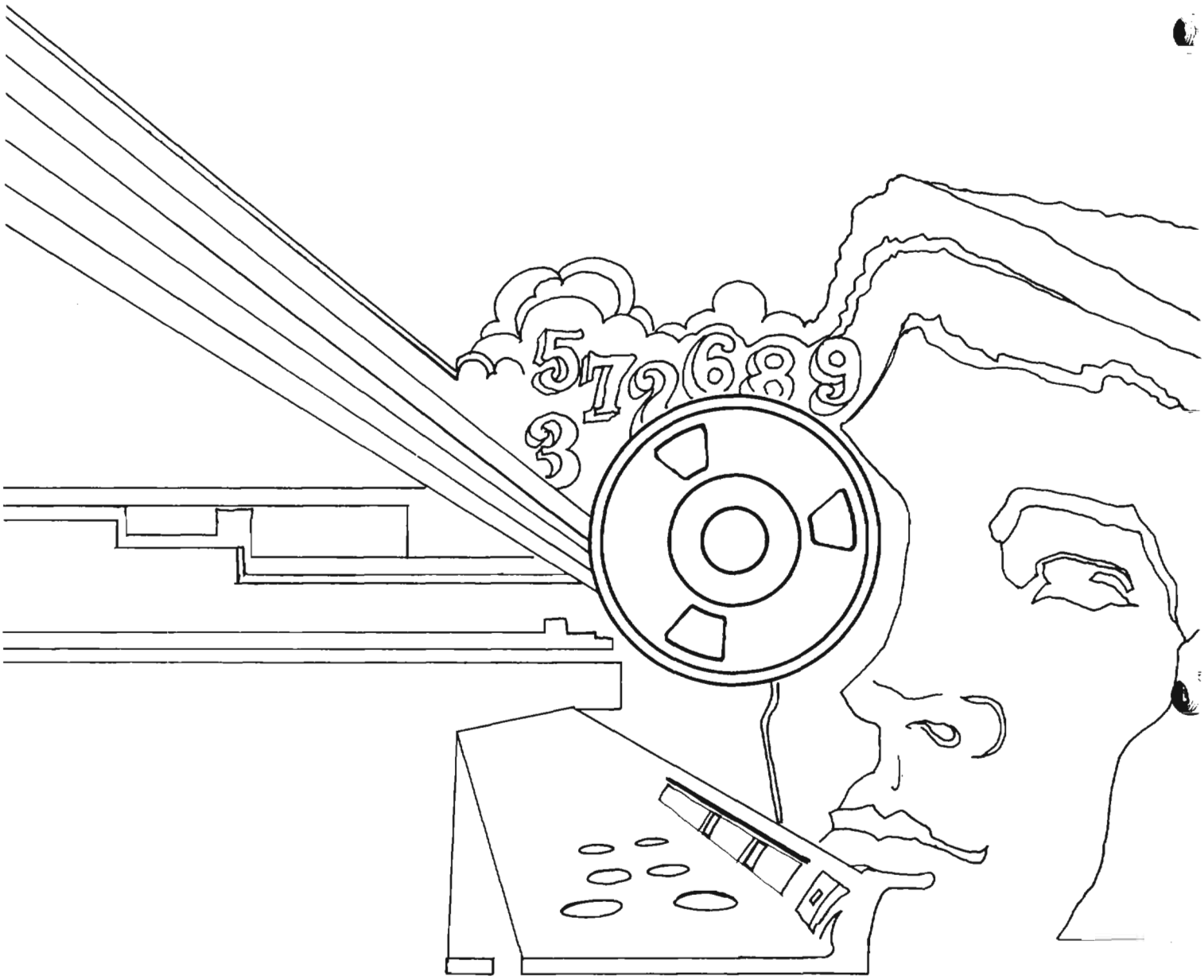
All three lectures drew standing-room-only audiences of members and nonmembers to the Friedman Auditorium. The Association, under its President, Frank Smead, is outlining a program of lectures and other activities for 1976 which will be in keeping with the organization's stated objectives.

Anyone interested in joining the CAA should call its Treasurer, Tim Murphy, on 4787s or its Secretary, Jane Dunn, on 8025s for more information. ~~(CONFIDENTIAL)~~

DOCID: 4009727



P1-Nov 75-S3-24264


5 7 2 6 8 9
3

DOCID: 4009726

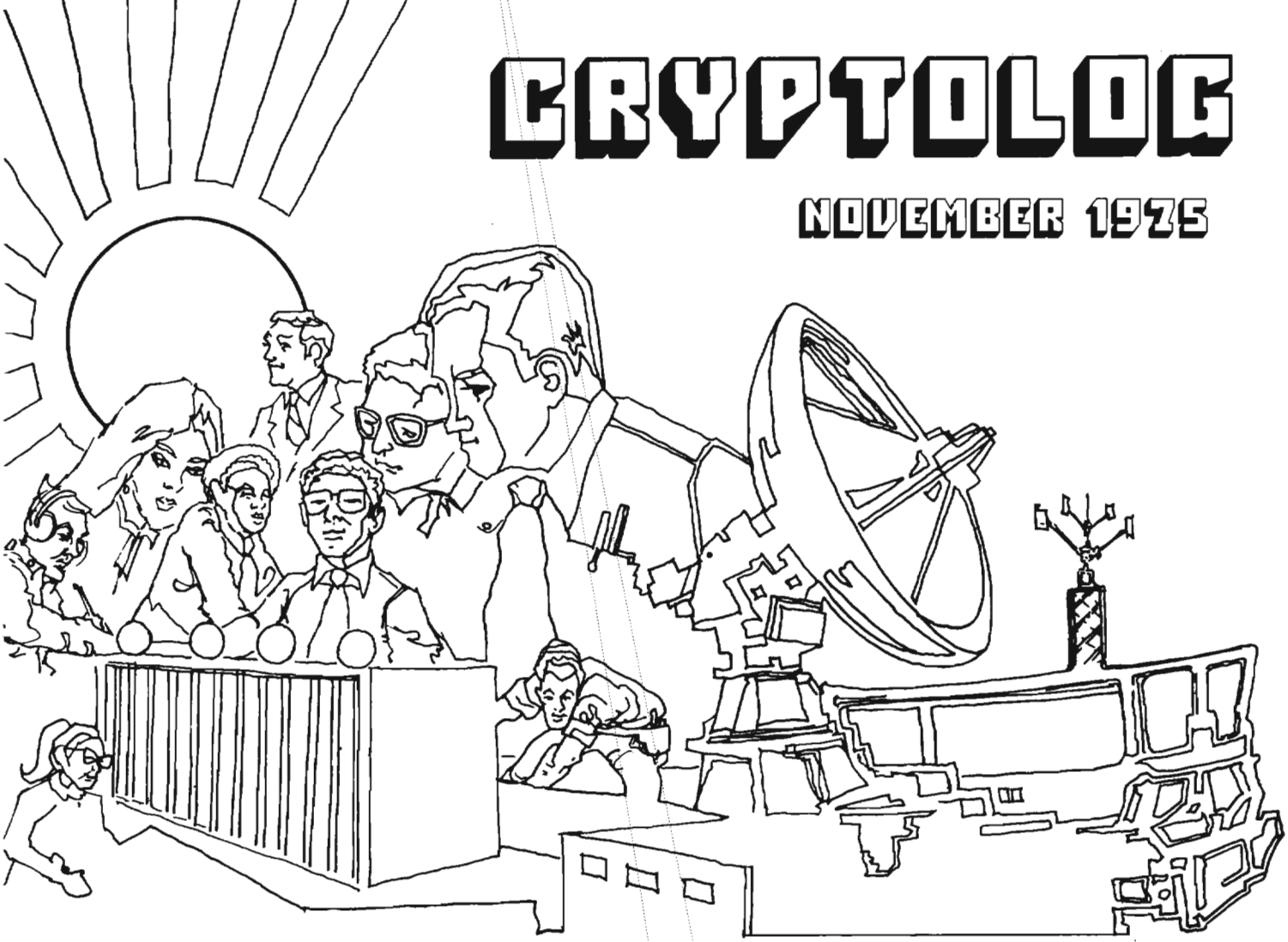
EO 1.4.(c)
P.L. 86-36

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

NOVEMBER 1975



P.L. 86-36

WHEN CENSORSHIP BACKFIRES.....James Killough.....1
[redacted].....[redacted].....3
DESKPAD: A PROGRAMMER'S TOOL.....[redacted].....7
[redacted].....[redacted].....9
IN PRAISE OF SOLITS.....Louis C. Grant.....12
NOTES ON BLUE RUSSIAN.....[redacted].....12
NATIONAL CRYPTOLOGIC SCHOOL OFFERS
COURSE-EQUIVALENCY TESTS.....13

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009726

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. II, No. 11 NOVEMBER 1975

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief..... Arthur J. Salemme (5642s)
Cryptanalysis..... [redacted] (8025s)
Language..... Emery W. Tetrault (5236s)
Machine Support..... [redacted] (3321s)
Special Research..... Vera R. Filby (7119s)
Traffic Analysis..... Frederic O. Mason, Jr. (4142s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

WHEN CENSORSHIP BACKFIRES

Soviet, Publicizing Vote Data, Unveils Secret City's Existence

By THEODORE SHABAD

Special to The New York Times

MOSCOW, June 3—The se- ... newspaper just received. It dis- ... existence of a secret ... without giving ... recise locati... ter ... atomic and aerospace industries.

The authorities also ... pride in the unc... tions, proc... per... ...cies. ...time comes, as ...ne 13, the concern for ...otection of state secrets sometimes clashes with the desire to publicize the election process, including geographical listings of electoral districts and the names of officially designated candidates.

In at least one case, the apparent conflict, has been resolved in a compromise, to judge from a Central Asian ... the Tadzhik Re... publishing a list of ... of the four districts that make up the secret city. A careful reader would note that the list jumped from No. 255 to No. 260.

At the conclusion of the r... inating campaign, in which unopposed candidate was selected for each district, the

Continued on Page 6, Column 7

SOVIET DISCLOSES CITY'S EXISTENCE

Continued From Pa... 4

newspa... ...uld not ...tion of those ...represent the secret

District 256 is to be represented by Khamid T. Nadyrov, identified as First Secretary of the Communist party's City Committee; the name of the ... Tadzhik party's 135-member Central Committee last February, indicating that their jobs are of more than routine significance. Mr. Oplanchuk was ...

There have been indications in other publications that the unidentified city may be asso... Taboshar is listed in prewar Soviet reference books as a principal site of radioactive ore.

Census results published a year ago indicated that the city's population was 24,000. ... people, with a combined population of 203,700, and listed six by size.

Tashkent, Taboshar, Leninabad, Dushanbe, SOVIET UNION, TADZHIK S.S.R., AFGHANISTAN, INDIA, PAK.

The New York Times June 4, 1971

Secret city is believed associated with uranium in Taboshar area (cross).

By [redacted] C531

P.L. 86-36

Theodore Shabad is one of the preeminent American experts on Soviet physical and economic geography. He is the author of *Geography of the USSR* (1951), *Basic Industrial Resources of the USSR* (1969), and *China's Changing Map* (1972). Since 1953 he has been a member of the New York Times foreign news staff reporting from Moscow. Of all the foreign correspondents in Moscow, he appears to have the sharpest eye for irregularities in the Soviet press which many people fail to notice or appreciate, and therein lies an interesting and instructive tale.

Back in 1971, Shabad published an analysis of election reports from Tadzhikistan that must have had the folks at Glavlit[1] hopping for weeks if not months. Now, just following the 1975 republic-level elections in the USSR, is a good time to look back at Shabad's 1971 article and the intervening years to observe what appear to be its effects.

Shabad's Article

Shabad noticed that, in listing the electoral districts for the 1971 elections to the Supreme Soviet of the Tadzhik Republic, the newspaper *Kommunist Tadzhikistana* (18 March 1971) entirely skipped over four of the numbered electoral districts in Leninabadskaya Oblast' (Nos. 256 through 259). However, after the election, all the elected deputies were listed. One was Vladimir Yakovlevich Oplanchuk, identified as "director of a plant," and another was a person identified as First Secretary of "a City Committee of the Communist Party." Both were members of the Central Committee of the Tadzhik Communist Party, and Oplanchuk had been a delegate to both the 23rd and 24th Party Congresses.

Consulting the Soviet census that had been published in 1970, Shabad found a statement that there were seven cities in Tadzhikistan with populations of 20,000 to 50,000, for a combined population of 203,700. But the census report listed only six cities, with their respective populations. Simple addition and subtraction led Shabad to conclude that the "secret city" had a population of 24,000. To suggest what and where that city was, he turned to prewar geographies identifying Taboshar as a principal site of radioactive ore in Leninabadskaya Oblast'. Thus he concluded that the "secret city" was probably Taboshar, and that its identity was being suppressed by the censors because of its relationship to the Soviet atomic-energy program.

What Shabad Didn't Know, But We Did

Shabad may not have known how close he came. Had he had access to CIA defector reports, he would have discovered that Oplanchuk had been the head of a Soviet uranium-mining operation in East Germany until 1956, when he was transferred to become Chief of a uranium-mining operation "somewhere in Central Asia."

[redacted]

[1]Abbreviation for Chief Directorate for the Protection of State Secrets in the Press, known in the West as "the censor."

EO 1.4.(c)
P.L. 86-36
P.L. 86-36

[redacted]

Soviet Revelations, 1973-1974

Though Shabad may not have known how close he came, the guardians of the secrets at Glavlit and the Ministry of Medium Machine Building (the ministry with overall responsibility for the Soviet atomic-energy program) knew only too well and must have had some unkind thoughts for our wily correspondent. While he had not completely spilled the beans, he had tipped them very precariously. They could be fairly certain that Shabad had focused the attention of at least a few Western intelligence analysts on the Leninabad area.

Given the choice of stonewalling it or letting the chips fall where they might, the censors apparently decided the jig was up and took the wraps off the "secret city." [2] In 1973, Volume 14 of the Third Edition of the *Large Soviet Encyclopedia* was published. It contained a short article on Leninabadskaya Oblast' and identified the seventh city as *Chkalovsk* (of which "Skalows I" had obviously been a garble). In typical Soviet fashion, the censors refused to show the city on the map accompanying the encyclopedia article.

In 1974, however, perhaps realizing the futility of their predicament, they passed two publications:

- a map showing Chkalovsk as a city a few kilometers southeast of Leninabad, with between 10,000 and 30,000 souls; and
- an administrative-territorial handbook listing *Chkalovsk* as a city with 26,000 inhabitants that had been created in 1956 (the year Oplanchuk was transferred from East Germany), with administrative responsibility for three widely separated settlements: *Taboshar*, about 45 kilometers north of Chkalovsk; *Palas*, about 15 kilometers to the east; and *Naugarzan*, in the extreme northern tip of Tadzhikistan, over 90 kilometers northeast of Chkalovsk. None of these four locations were included among the 63,499 entries in the 1969 USSR Postal Index (similar to our ZIP code listing). NSA's Soviet Localities File contained no open-source references to Chkalovsk or Taboshar, and no references at all to Naugarzan or Palas. But in 1974 the lid was off.

[2]Statements concerning the motives of the censors are of course pure speculation, in view of the lack of defectors from Glavlit.

Soviet 1975 Republic-Level Elections

Which brings us now to the 1975 republic-level elections. With the censors presumably chastened by Shabad's exposé, there was no repetition of the 1971 shenanigans: no electoral districts were omitted from the published list. This time all the four deputies from Chkalovsk were either employees of the Combine or had been nominated by workers of the Combine.[3] This clearly shows Chkalovsk to be a "company town" whose administrative control over Taboshar, Palas, and Naugarzan is a result of its uranium mining and refining activities.

[redacted]

All of this, including the reference to "Skalows I," began to make sense. Presumably for reasons of security and economics, the administrative headquarters of Combine 6, along with support elements and other non-mining facilities, were relocated to a new city incorporating an area of extensive recent construction and the older settlement of Chkalovskij from which it took its name. In order to maintain complete control over its subsidiary mining operations, it was necessary to subordinate the local soviets of Taboshar, Palas, and Naugarzan to the Chkalovsk City Soviet. Thus, since reference to Chkalovsk was forbidden, mention of the other three locations was also taboo. The situation was not unique, but was certainly very unusual. For 15 years the blackout succeeded, and therefore may be said to have served its purpose, but in the end it was its own undoing. Were the Soviets ready to reveal their "secret city" anyway, and was Shabad's article a mere embarrassment? I doubt it.

P.L. 86-36
EO 1.4.(c)

Moral:

Excessive censorship may betray that which it is supposed to protect; or
It pays to read Soviet publications with an eye to what is not said.

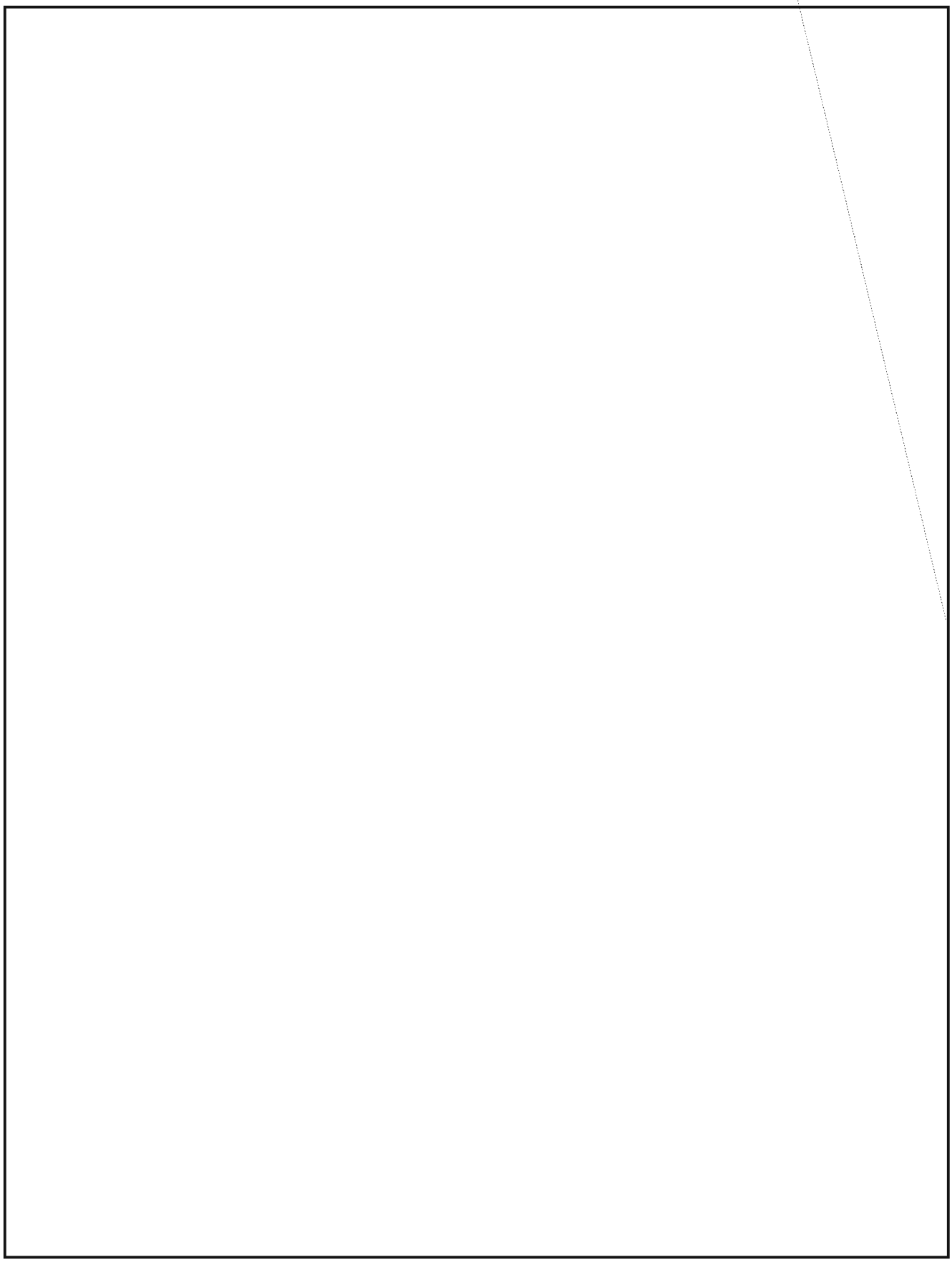
[3]This time the censors tried to confuse us by calling it "a construction combine." Ah what tangled webs we weave. . .

P.L. 86-36
EO 1.4.(c)

EO 1.4.(c)
P.L. 86-36

DOCID: 4009726

EO 1.4.(c)
P.L. 86-36



[redacted]

[redacted]

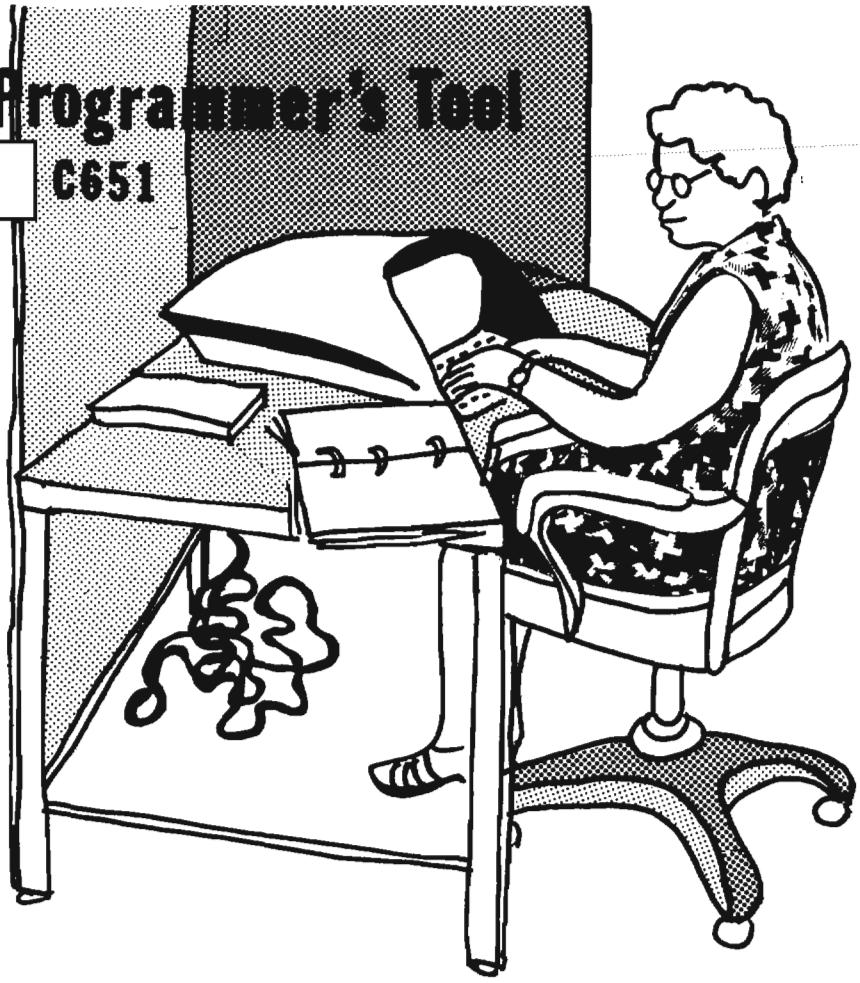
(~~TOP SECRET UMBRA~~)

DOCID: 4009726

DESKPAD: A Programmer's Tool

By [redacted] C651

P.L. 86-36



Software is getting more costly and taking up more of the Data Processing budget. More work is being requested of fewer people. Software is becoming more sophisticated and more complex. How can management meet the new challenges? Increased productivity is one way, and DESKPAD is a way of attaining this goal.

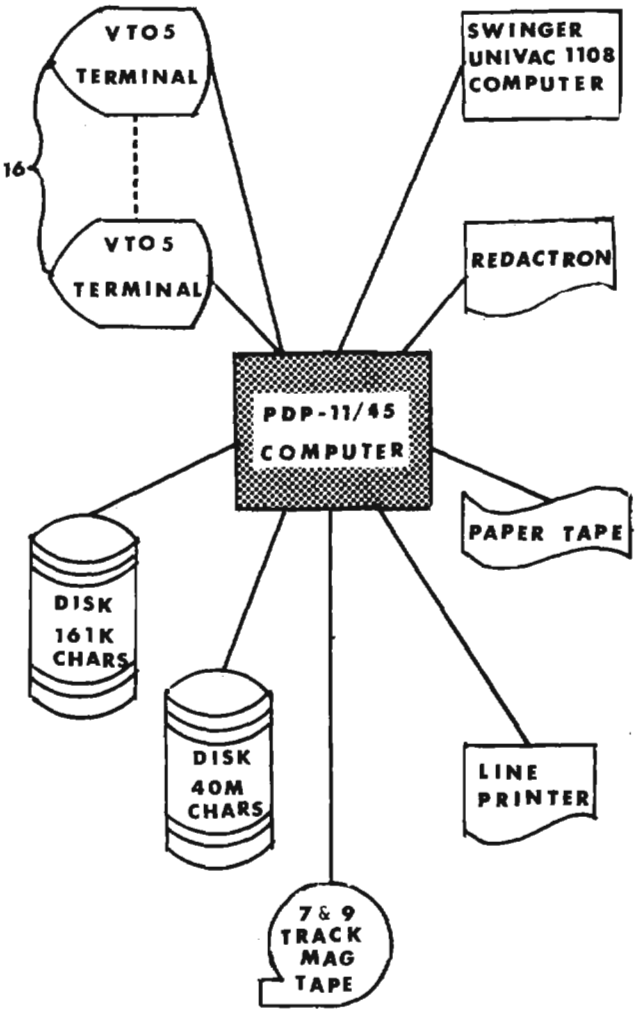
DESKPAD is a remote-terminal, time-sharing, software-development system. The DESKPAD system provides the full capability of an on-line computer system to the programmer when he needs it. By assisting the programmer, DESKPAD increases overall productivity in areas such as documentation, generation of specifications and design plans, as well as the actual programming. The remote system saves the programmer time in various ways: travel to and from machine areas is reduced since updating is performed on-line; the time-consuming task of making corrections, on tape or cards, to programs is eliminated; there is no longer a need to wait for a machine run to see how a piece of code fits in, since the program text is available on-line; and documentation is kept up to date, since it can be changed as the program is modified or generated while the program is being developed.

With the increased productivity made possible by DESKPAD, the system can pay for itself in less than 5 years. The average salary of a programmer is $12,800 a year. A 5-percent increase in his productivity will yield an increase in his value of $640. In a division of approximately 70 people, the total increase in value will be $44,800 a year, which is approximately one-fifth of the $180,000 cost of the DESKPAD system.

The DESKPAD system consists of a Digital Equipment Corporation (DEC) PDP-11/45 computer with 112K of main memory and 40 megabytes of mass storage. The system contains various peripherals including magnetic tape, paper tape, 16 VT05 CRT terminals, a link to the UNIVAC 1108 computer, and a REDACTRON Communicating Typewriter. Hardware is under control of the RSTS/E (Resource Sharing Time Sharing/Extended) system purchased with the system from DEC. RSTS allows the users to perform time-sharing with the Basic-Plus language. Basic-Plus performs matrix manipulation, alphanumeric string operation, virtual memory addressing, and many other functions that allow both simple and advanced programming to be performed. Also available are many utility programs to standardize redundant operations needs for everyday use. These utilities include a peripheral interchange program (PIP), an accounting information program (MONEY), a system status reporter (SYSTAT), a file recovery program (BACKUP), a character/line editor (EDIT), and a powerful cursor control editor (PAGE). PAGE is the most frequently used software package on DESKPAD. The editor was obtained at no cost to the government through our membership in the Digital Equipment Computer User Society (DECUS). It provides the user with total control of the VT05 terminal. PAGE makes the task of editing more enjoyable than one the programmer resents doing. In addition to the previously mentioned software, a software interface has been purchased from the Oregon Museum of Science and Industry (OMSI). The interface allows RSTS users to make use of the RT11 single-user system. The

DOCID: 4009726

DESKPAD HARDWARE



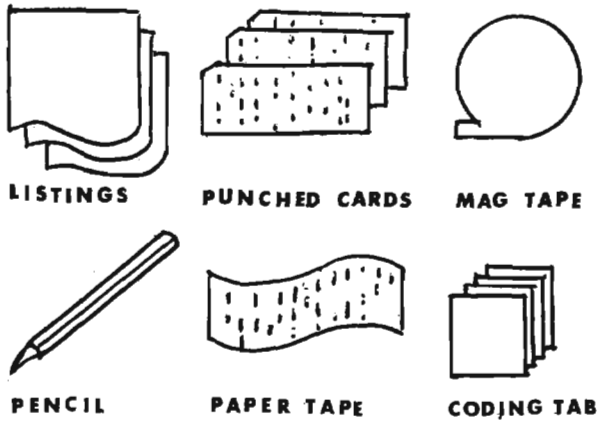
RT11 system provides the user the capability of running the PDP-11 Macro Assembler and Linker as well as FORTRAN IV. With the OMSI-supplied interface, DESKPAD expands its capability to compete with most of the large-scale systems in the Agency.

The DESKPAD system is currently in use in the Field Software Support Division of C6. With the division supporting 26 small systems, some with virtually no updating facility or so primitive that it takes 2 to 3 passes to complete a single update, it is easy to see why DESKPAD has become quite popular. DESKPAD currently supports 69 people using 700 files assigned to 144 accounts. A "HELP" program is available to provide users with current system information. HELP provides information ranging from sign-on instructions to execution of a FORTRAN program. A "GRIPE" program gives the user a means of communicating with the system manager. It informs him of system deficiencies as the user sees them. All gripes are answered within one week by the system manager. Technical notes are generated to provide users with documentation of user-written utility programs and to provide additional documentation on any other area of DESKPAD that requires it.

With austerity hitting all parts of the Agency, systems such as DESKPAD can provide the needed technology to meet the ever-increasing demand on the diminishing work force.

TOOLS OF THE TRADE

Without DESKPAD



With DESKPAD

Solution to NSA-crostic No. 1

(CRYPTOLOG, October 1975)

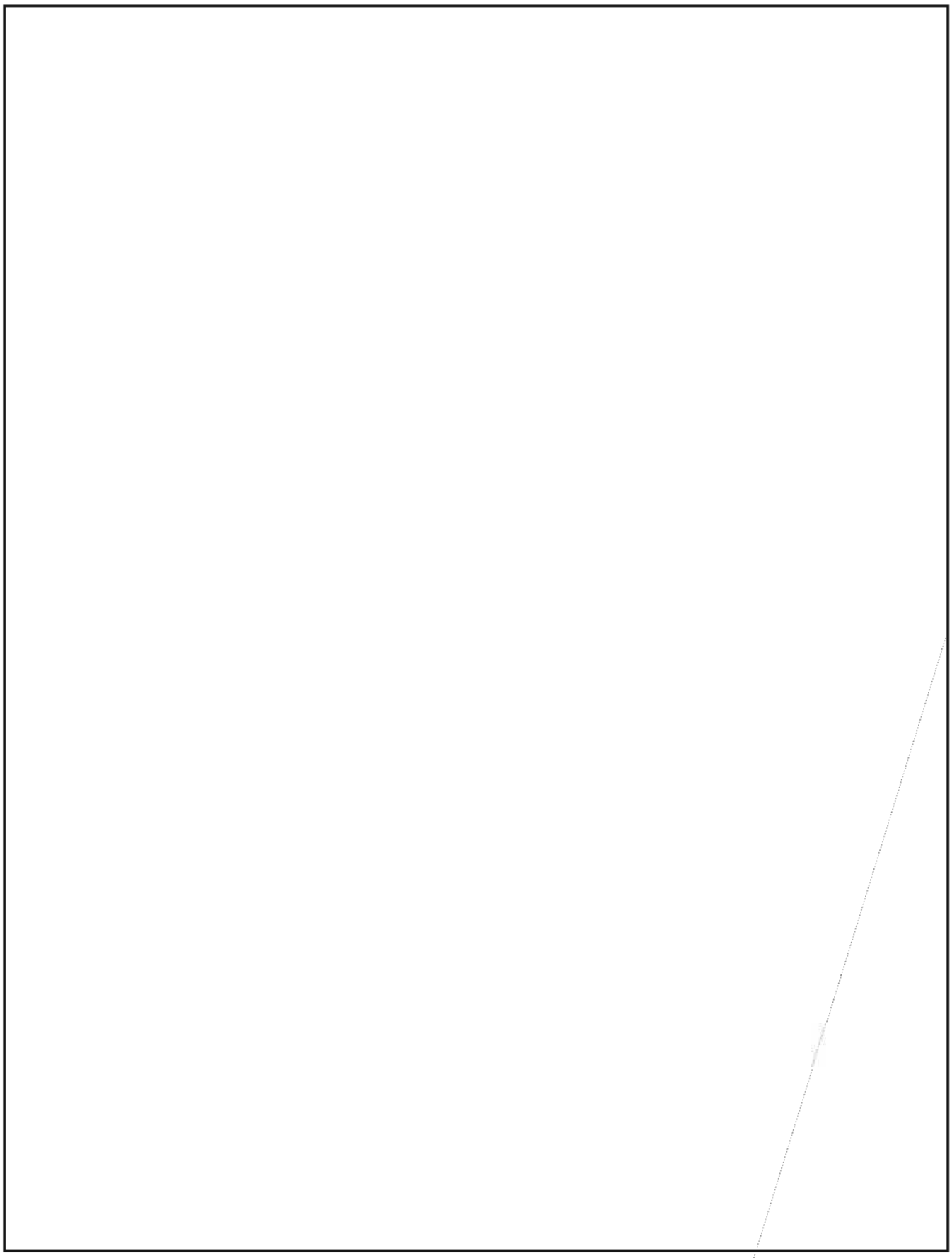
[redacted] "Uncertain Origins": P.L. 86-36

"The analysts I met were anything but desolate. Working in a pair of tottering quonset huts at tables they had made themselves and harassed by wind, dust, and erratic electricity, they saw themselves in league against the forces of evil -- variously embodied in the VC, the weather, and NSA."

(UNCLASSIFIED)

DOCID: 4009726

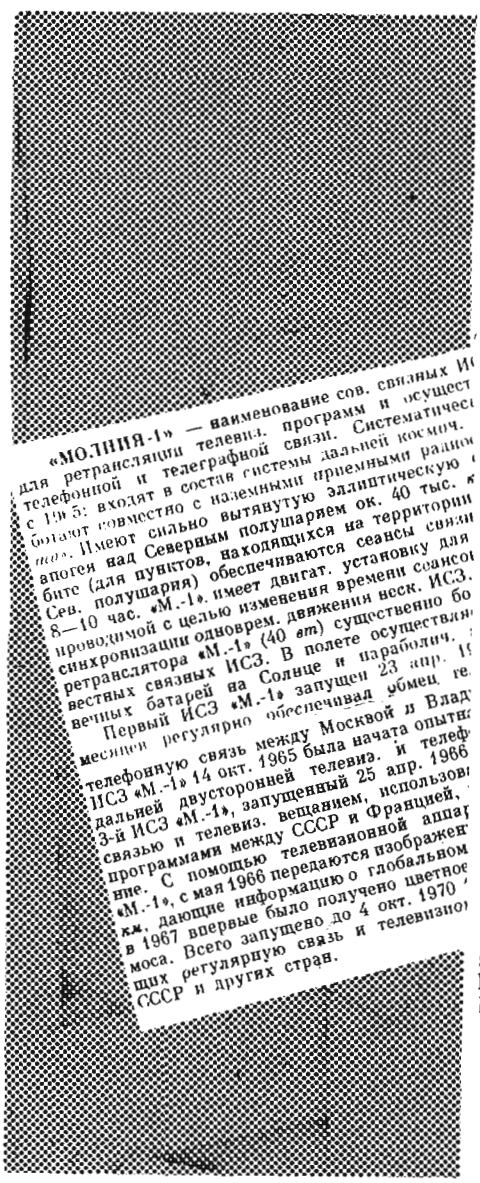
P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)



EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

DOCID: 4009726

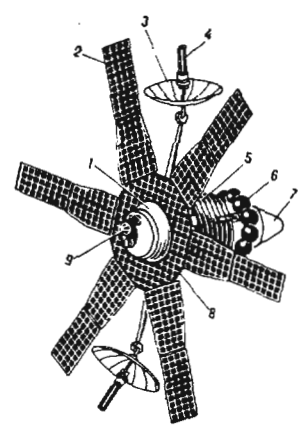
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36



«МОЛНИЯ-1» — наименование сов. связных И
для ретрансляции телевиз. программ и осущест
телефонной и телеграфной связи. Систематичес
с 1965 входят в состав системы дальней космич.
бодают совместно с наземными приемными радио
пов. Имеют сильно вытянутую эллиптическую
апогея над Северным полушарием ок. 40 тыс. к
бите (для пунктов, находящихся на территории
Сев. полушария) обеспечиваются сеансы связи
8—10 час. «М.-1» имеет двигат. установку для
проводимой с целью изменения времени сеансов
синхронизации одноврем. движения неск. ИСЗ.
ретранслятора «М.-1» (40 вт) существенно бо
вестных связных ИСЗ. В полете осуществля
вечных батарей на Солнце и параболич.
Первый ИСЗ «М.-1» запущен 23 апр. 19
месяцев регулярно обеспечивал обмен те
телефонную связь между Москвой и Влад
ИСЗ «М.-1» 14 окт. 1965 была начата опытна
дальней двусторонней телевиз. и телеф
3-й ИСЗ «М.-1», запущенный 25 апр. 1966
связью и телевиз. вещанием, использов
программами между СССР и Францией,
ние. С помощью телевизионной аппар
«М.-1», с мая 1966 передаются изображен
км, дающие информацию о глобальном
в 1967 впервые было получено цветное
моса. Всего запущено до 4 окт. 1970
щих регулярную связь и телевизио
СССР и других стран.

MOLNIYA-1. Name of Soviet communication satellites intended for relaying of TV programs, and long-distance telephone and telegraph communication. These satellites have been used since 1965. They are part of the *Orbita* space system of long-range radio communication. These satellites travel on an elliptical orbit of great eccentricity with an apogee of about 40 thou. km in the Northern hemisphere. With an orbit of such shape (for points located in the USSR and other countries in the Northern hemisphere), communication may be maintained for up to 8—10 h at a time. *Molniya-1* satellites have rocket engines to make CORRECTIONS OF ORBITS in order to alter the hours of available communication time and to synchronize the travel of several satellites moving round the Earth at the same time. The output power (40 W) of the relay transmitter on *Molniya-1* is considerably higher than that on other known communication satellites. The satellite's design provides in-flight orientation of solar batteries towards the Sun and of the parabolic antenna towards the Earth.

The 1st *Molniya-1* satellite which was launched on April 23, 1965, regularly provided TV and telephone exchange between Moscow and Vladivostok for many months. On October 14, 1965, the 2nd *Molniya-1* satellite was launched for experimental 2-way long-distance TV, telephone, and telegraph communication; the 3rd *Molniya-1* satellite, launched on April 25, 1966, besides serving for communication and TV broadcasting between USSR ground stations, was also used for an exchange of TV programs between the USSR and France, this including colour TV. Since May, 1966, TV



Molniya-1 communication satellite.
1—sealed body; *2*—solar battery; *3*—high-gain antenna; *4*—Earth sensor for antenna orientation; *5*—radiative cooler; *6*—working fluid for minor corrections of flight path; *7*—correction engine; *8*—heater panel; *9*—Sun sensors.

equipment on board the *Molniya-1* satellites yields images of the Earth as seen from altitudes of 30,000—40,000 km, which contain information about cloud pattern in globular scale; a colour photo of the Earth taken from space was produced in 1967. By August 1, 1968, 13 *Molniya-1* satellites have been placed into orbits to provide regular communication and TV broadcasting over the territory of the USSR and other countries.

Kosmonavtika, V. P. Glushko, Editor-in-Chief, Moscow, 1970 (2nd edition, expanded); *The Soviet Encyclopedia of Space Flight*, G. V. Petrovich, Editor-in-Chief, Moscow, 1969 (translation of 1968 edition of *Kosmonavtika*).

(UNCLASSIFIED)

DOCID: 4009726

IN PRAISE OF SOLITS

By
LOUIS C. GRANT, V13

I am sick to death of hearing people refer to "Some Old Lady in Tennis Shoes" in a frivolous or disparaging tone. You younger readers may not know any better, but you older hands certainly should. Come on, people! My appraisal of SOLITS is now, as it was then, very simply, "Thank God!"

I first met SOLITS 25 years ago and she amazed me. She was at once the Agency's computer system, the Agency's conscience, the Agency's spirit, and the Agency's respect. No matter where I looked, she was there: armed with the simplest tools, garbed in her idiosyncrasies, resolute in her manner, doing her thing.

SOLITS embodied all the basics of a computer: *memory bank* (she never forgot anything); *data storage* (she never got rid of anything); *retrieval* (she knew where everything was); and *rapid access* (she had instant opinions). All this and she was seldom down for maintenance, she generated her own data input, and she didn't even need air-conditioning to operate.

Like any good conscience, SOLITS was frustrating and at times hard to live with. She was there whether you wanted her or not; she nagged until you listened; and she didn't give a damn who you were. If she had an opinion, you got it. In fact, you got it over and over until it registered. And I know of no Agency senior who ever escaped the determined SOLITS touch. The frustrating part was that you inevitably were sorry for it when you failed to heed her counsel.

In spirit, SOLITS personified the phrase "weird and wonderful." Professionally she was unorthodox, crotchety, jealous, suspicious, and selfish. She was the undisputed ruler of her one-desk kingdom. You were free to seek a request, but you never dared suggest how she might grant it. In short, a royal pain. Yet under that autocratic armor was a true Queen. SOLITS reigned over her younger coworkers. She lent them money, befriended the lonely, counseled the unknowing, ministered to the sick, and comforted the bereaved. But always with an air of noblesse oblige that never betrayed her inner feelings. Indeed a regal gem.

SOLITS was deeply respected for one very simple reason: she worked. The general excellence of her effort and her profound dedication are manifested in every success the Agency ever had. SOLITS never sought the spotlight, but you can bet the script was based on something she had done. And she was always in the wings ready to cue the front man. She richly deserved the applause.

Oh yes, she really did wear tennis shoes. But the Agency has stood in them -- proudly -- ever since the ribbon was cut. If they ever build a museum here, I hope there is a pair of bronzed tennis shoes enshrined and dedicated to the First Lady of our business. Wherever you are, SOLITS, my professional respect and gratitude are with you.

P.L. 86-36

DEPARTMENT OF GOLDEN OLDIES

Most Golden Oldies were apparently written by Anon., but the author of the following one is known: NSA-er Dr. [redacted] who retired in 1972.

Notes on Blue Russian

Blue Russian is a dialect spoken by about 16 persons scattered widely over the Valdai Hills. It is called "Blue Russian" because of the characteristic tint of the faces of speakers as they hold their breath while pronouncing imperfective and frequentative verb forms.

Just to give you an example: BIT' means "to beat"; POBIT' means "to do a little beating", and its imperfective is POBIVAT'. ZAPOBIVAT' means "to begin to do a little beating," and its imperfective is PEREZAPOBIVYVAT'. This last verb, interestingly enough, has a special frequentative form: namely, PEREZAPOBIVYVYVOVAT', which may be rendered "to make a practice of making fresh starts on projects involving a limited amount of beating." Hence, the handy expression ShKOL'NO-DVOROVYJ PEREZAPOBIVYVYVUYu-ShchIJ, "schoolyard bully."

The 16 speakers of Blue Russian are under constant observation so that scientific data on the incidence of linguistic strangulation may be obtained. Their zero birth rate during the past 50 years has aroused comment. But it is still too early to assert, with Hammerkopf, that "Blue Russians are too exhausted from talking to be able to propagate." This is dogmatic theorizing in the worst tradition of the University of Berlin.

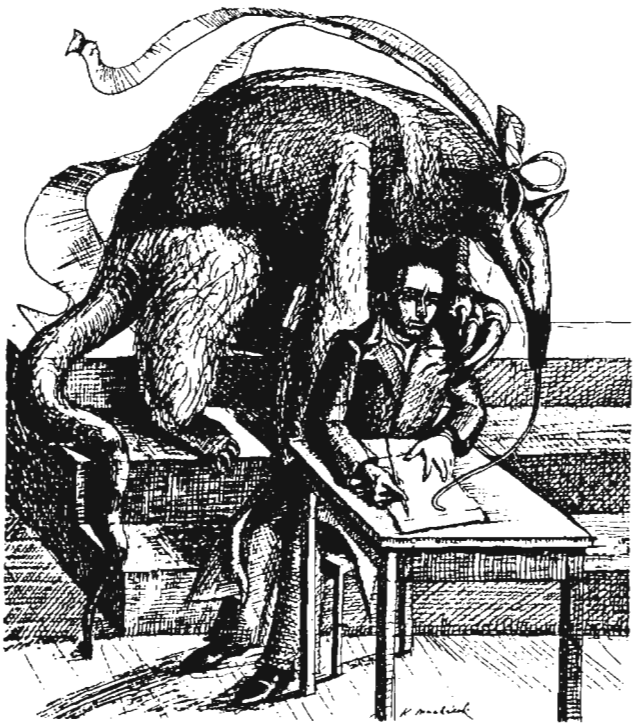
As this goes to press, it has been learned that two of the 16 Blue Russians have died. It seems that one of them, a devoted member of the Pedagogico-Organizational Committee of the 7-year School of Staraya Russa, suffocated in the midst of an impassioned speech on schoolyard bullies; and his wife died of a similar cause shortly afterwards while talking to friends about making fresh starts on projects involving a limited amount of simplification of Blue Russian.

National Cryptologic School Offers Course-Equivalency Tests

The National Cryptologic School offers employees the opportunity to earn course credit by taking EQUIVALENCY TESTS. Frequently, through experience or self-study, a person has already learned the material presented in a course. If this knowledge can be demonstrated, time and energy required to take a course can be saved. Equivalency tests may be scheduled through the cognizant NCS department. They are available for the following courses:

EA-100	Introduction to COMINT/ELINT Technology
EA-030	Introduction to Multichannel Technology
EA-100	Basic SIGINT Technology
EA-200	SIGINT Instrumentation and Measurements Techniques
EA-201	Communications Signals Measurements and Analysis Techniques
EA-202	ELINT Measurement and Analysis Techniques
EA-380	Advanced ELINT Collection/Analysis

Cognizant department: E23, 8198s



ED-210	Tests and Measurements

Cognizant department: E42, 8047s

ET-100	Introduction to Electronics
ET-260	Solid State Devices and Applications
ET-261	Digital Concepts

Cognizant department: E24, 8975s

MA-400	Introduction to Computer Science Mathematics
MP-1B5	CDC 6600 Series System Software
MP-1B6	CDC 6600/7600 Advanced Technical Skills
MP-1C5	UNIVAC 494 RYE System Software
MP-1C6	UNIVAC 494 Advanced Technical Skills
MP-1D6	IBM 360/370 Advanced Technical Skills OS
MP-1E5	UNIVAC 1108 System Software
MP-1G5	Project HOLDER - UNIVAC 494 System Software
MP-1H5	Burroughs 6700 System Software
MP-1K6	CDC 6600/6700 Advanced Technical Skills (IDA)
MP-154	Introduction to Computer Systems Software
*MP-160	Introduction to Computer Science
MP-166	FORTRAN for Operators
*MP-188	APL Programming
*MP-277	FORTRAN Programming
*MP-230	COBOL Programming
*MP-242	PL/1 Programming
*MP-243	Burroughs Extended ALGOL Programming
*MP-248	BETA Programming
*MP-267	POGOL Programming
*MP-335	IBM 370 Programming
*MP-368	IBM 370 Job Control Language (JCL)
*MP-375	PDP-11 Programming

* Toy problem also required.

Cognizant department: E21, 8555s

TA-200	Intermediate Traffic Analysis and Technical Reporting
TA-261	Computer Aid to Traffic Analysis
TA-361	Air Defense Technology and Traffic Analysis

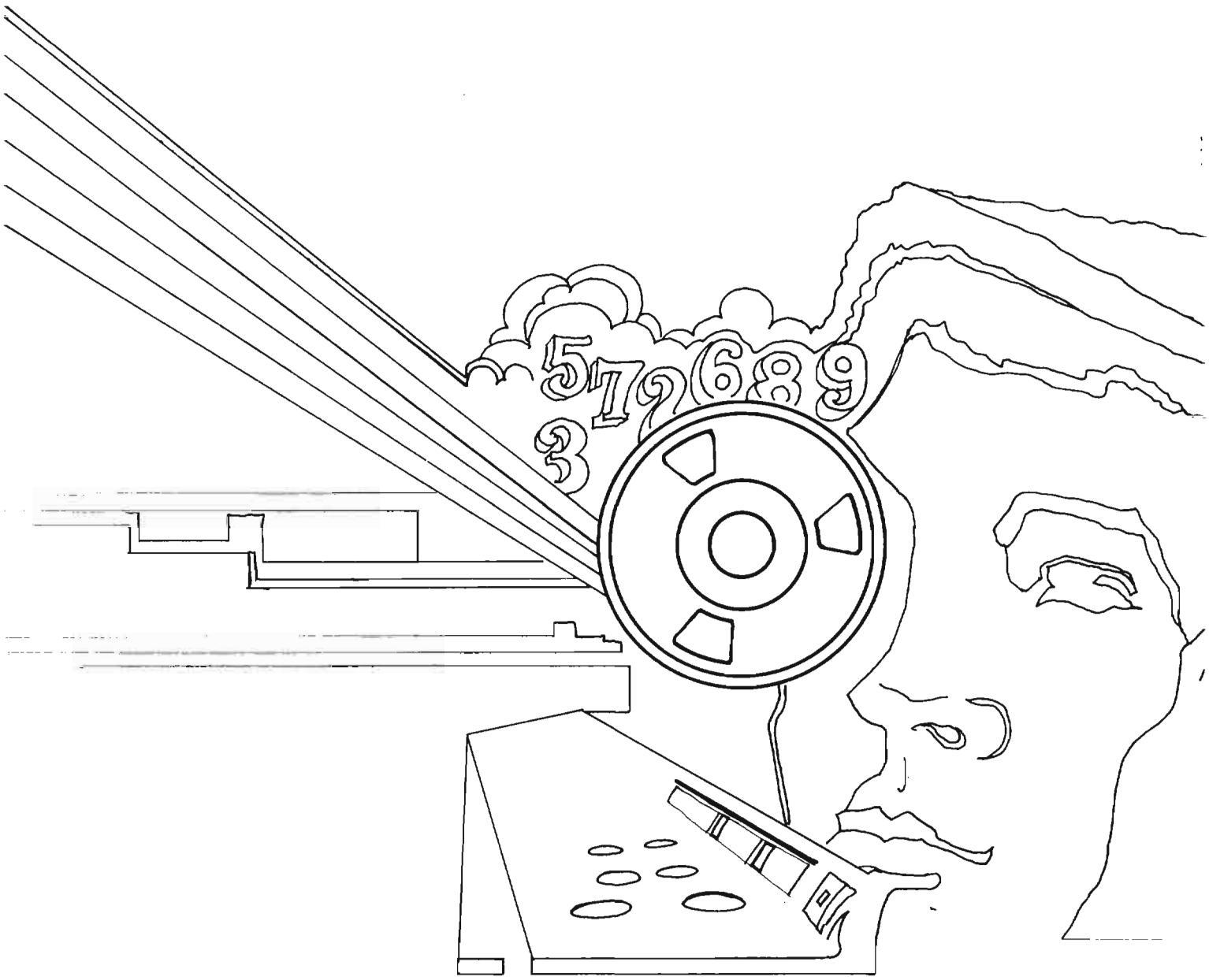
Cognizant department: E14, 8017s

TG-126	Target Studies - Mainland Southeast Asia

Cognizant department: E12, 7119s

● *A grade of "P" is assigned for passing the course through an equivalency test. Grades of "F" are not recorded. Aspirants may take the test only once.*

P1-Oct 75-S3-24202


5726893

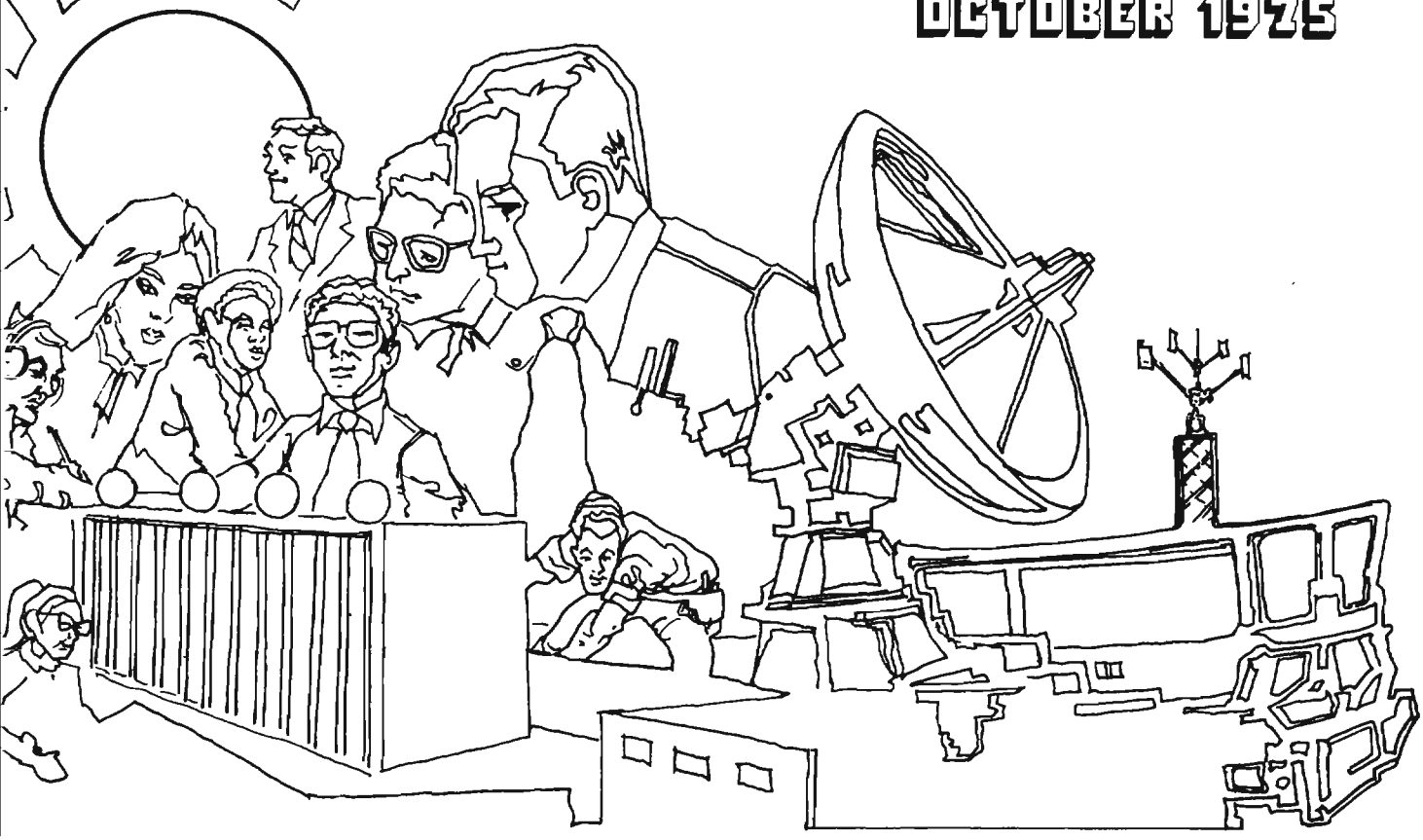
DOCID: 4019728

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

OCTOBER 1975



SPECIAL ISSUE — VIETNAM

For table of contents, see page 1 inside.

Declassified and Approved for Release by NSA and CIA on 10-11-2012 pursuant to E.O. 13526, MDR case # 54778

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

DOCID: 4019723

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. II, No. 10 OCTOBER 1975

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief..... Arthur J. Salemme (5642s)
Cryptanalysis..... [redacted] (8025s) P.L. 86-36
Language..... Emery W. Tetrault (5236s)
Machine Support..... David J. Williams, III (3321s)
Special Research..... Vera R. Filby (7119s)
Traffic Analysis..... Frederic O. Mason, Jr. (4142s)

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

VIETNAM

Except for short features, this entire issue is devoted to the Vietnam War and its significance to NSA -- achievements, failures, lessons learned, problems unresolved. The intent is to record the personal impressions of NSAers while those impressions are still fresh, even if painful, so that they can serve as a guide for future NSAers. Because the emphasis is on the personal and subjective, there are slight overlaps in the treatment of the same topic by different authors and slight differences of opinion.

While the articles in this issue cover a wide range of topics, they obviously do not exhaust the subject. Therefore the Publisher and Editorial Board of CRYPTOLOG continue to invite contributions documenting the role of NSA in the Vietnam War. Any such contributions that are accepted for publication will appear in future issues of CRYPTOLOG.

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

TABLE OF CONTENTS

		Page
[redacted]	NSA in Vietnam: Proud and Bitter Memories	3
	Vietnam Articles in DRAGON SEEDS	6
[redacted]	1972-1973: A Vietnam Odyssey	7
	FRANCOPHONEGLOS Announcement	10
Edward Wiley	[redacted]	11
[redacted]	Language Lessons Learned: A Personal Memoir	13
[redacted]	[redacted]	18
A.J.S.	NSA-Crostic No. 1	22
[redacted]	IRONHORSE: A Tactical SIGINT System	24
[redacted]	The Danang Processing Center	27
[redacted]	Tactical Language Exploitation: A Lesson Learned?	31
Tim Murphy	Automation of a TA Proces	33
[redacted]	Computers, Comms, and Low-Grade Ciphers: [redacted]	38
[redacted]	Linguists -- You Have an Expert to Call!	40
William Gerhard	One Chance in Three -- But It Worked!	41
	Letters to the Editor	44

P.L. 86-36
EO 1.4.(c)

DOCID: 4019723

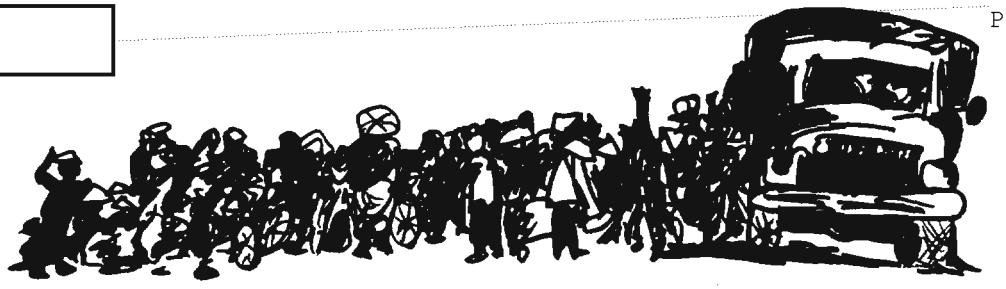
Extra copies of this special issue of CRYPTOLOG are available for subscribers who would like to receive additional copies to circulate in their work areas, or for persons who would like to begin their subscription with this issue. To receive copies, contact CRYPTOLOG Editor, P16, Room 3C099-1, x5642s.

DOCID: 4019723

NSA IN VIETNAM: Proud and Bitter Memories

[redacted]

P.L. 86-36



One day toward the end of the Saigon nightmare -- I don't recall which day but it must have been 25 April or afterwards -- I decided to stop by to see Major [redacted] while I made my rounds. There were only four NSA people left in Saigon, three communicators and myself, and so daily I went to pick up the intercept, ARDF results, and tech messages from the Vietnamese SIGINTers, and deliver tech support material to them, and also to bolster their flagging spirits. I didn't really have time to see [redacted] but I liked and respected him more than any other Vietnamese officer I knew and I wanted to see how he was holding up.

Alone in his office, we talked quietly. He told me that USAID, where his wife worked, had offered to evacuate her along with her family. He said he could not bring himself to abandon his men, and he had urged her to take their two sons and go. She would not leave without him. He knew, he said, that his chances of escape at the end were slim. But he knew he could not live under communism. If Saigon fell and he could not escape, he would shoot his wife and children and turn the gun on himself.

On the morning of 29 April, I tried in vain to warn [redacted] to pull out while he could, but I could not reach him. That afternoon, he telephoned another American, told him that he was still operating the Center with his forces intact, inquired what had happened to his commanders (they had disappeared), and asked if there were any chance that his family and he could escape.

He did not escape.

There are several reasons for repeating [redacted] story. First, to convey the genuine tragedy of the end of Vietnam; second, to illustrate the nobility and calm courage the Vietnamese were capable of; and, finally, to underline quite deliberately the irony of much that was Vietnam, by making [redacted] end the point of departure for relating the splendid things NSA did in Vietnam.

For all of us have every right to be extremely proud of the NSA role in Vietnam. Of all the stunning successes cryptology has achieved, none, in my opinion, reached the consistently superior level of our Vietnam effort over anything like so long a period of time. One reason for that success was the people NSA put on the problem. They were a gamy, imaginative lot, addicted to the problem, merciless to themselves in their drive for results, and given to puckish zaniness. The finest that I knew were those who were in Saigon up to the end, and my admiration for them is boundless.

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

All of these people have had to face the haunting moral question of involvement in Vietnam. The question is not escapable, and it is wrong to avoid it. I cannot honestly grapple effectively with the moral rectitude of U.S. military involvement in Vietnam, for my own involvement was not so much with war as it was with [redacted] and people like him, my work, and my conviction that it is better to know the truth than not to know it. I believe that the job of intelligence is to discern and to tell the truth. Had we failed to tell the truth about Vietnam, we would be morally indictable. But we did tell the truth and often did it brilliantly. If much that happened was ugly, and if the ending was sad, then perhaps our trust in the wisdom and humanity of our decision-makers was misplaced; perhaps not. My personel bitterness over Vietnam does not extend to condemning them.

As will be eminently clear by now, what I am saying here is personal and subjective. I make no claim for the objective precision of my words, and still less for historical accuracy. I am less concerned with a recital of verifiable data than I am with sharing some of the feelings and memories that went with SIGINT in Vietnam.

NSA's presence in Vietnam goes back in my memory to 1958. During that time, and up until 1962, the problem was readable. The Viet Cong, operating clandestinely, communicated among

themselves in South Vietnam using [redacted] Hence we were able to watch while Hanoi laid out her plans for the establishment of the National Liberation Front, named its officers, and dictated what its flag would be. We were able to report on the use of the Ho Chi Minh Trail for the infiltration of men and materiel, and to describe in some detail the maritime infiltration effort. All this in addition to detailed information on Communist Party activities throughout the country. [redacted] Until 1964, we lived in a SIGINT desert except for the burgeoning ARDF effort which began to give us good locations on Party terminals. In 1963, if I recall correctly, SIGINT did its first spectacular prediction in Vietnam when it forewarned of the Communist buildup at Ap Bac.

In 1964, military communications were introduced into South Vietnam in profusion. Our TA effort and ARDF took on new importance as a tool to follow the North Vietnamese buildup in the south. The forerunners of the 5th and 9th Divisions, B3 Front, and Military Region Tri-Thien-Hue all appeared in late 1964 and early 1965. In late 1964, forces of roughly regimental size gathered in Phuoc Tuy Province, and again SIGINT foretold the attack before it happened. The pattern of successful prediction was established.

Through 1972, NSA succeeded in foretelling every major offensive that the Communists launched in South Vietnam. It was not that the target was so malleable; rather, the resources committed against it were monumental, and the analysts on the target had come to know it so well that they could almost smell an offensive coming. And they were faced with perennial problems: customer's failure to believe the foretelling, and customer's belief that the Vietnamese Communists were using communications deception and misleading the SIGINT community. More than once, lives were lost in converting users to believers in the SIGINT indicator system.

Meanwhile, we made some mistakes we came to regret seriously. We allowed some customers in Vietnam access to semitechnical communications information -- message volumes, contact logs, unidentified ARDF fixes. G2 and J2 briefings all over South Vietnam blossomed with graphs, charts, plotting systems, and mathematicians trying to find the magic relationship between message flow and the number of ARDF locations which, like the secret of the pyramids, could somehow shed divine light on the thinking of the Communists. I will never forget a particularly painful exercise called "pattern analysis," whereby users plotted unidentified ARDF in hopes of discovering the ultimate truth -- something akin to the square root of the size of the enemy force divided by cumulative weight of all his heavy artillery (or something equally arcane). And then there was the lieutenant who told me that he had analyzed the RAD system used by the enemy and discovered a consistent relationship to the communications structure and first-heard dates.

The Vietnamese, with our help, had already gotten into the SIGINT business in the early 1960's. In 1963, one Lieutenant Colonel [redacted] was put in charge of the effort. Among his early cadre were bright young lieutenants -- [redacted] who always reminded me of a caricature of a Japanese general from a World War II movie; [redacted] boyish and bright, married to one of the most beautiful women I have ever seen; [redacted] who had wanted to be a priest; and [redacted] who told his boss the truth whether he wanted to hear it or not.

But in those days the Americans had little time or interest in the stumbling Vietnamese COMINT effort. They were too concerned with their own SIGINT and its uses. As the sixties wore on, they found a way to intercept infiltration communications (GDRS) and keep track routinely of the movement of men into South Vietnam from the north. [redacted] There was never much question in their minds from the communications point of view that North Vietnam was in command of the show in the south and that the distinction between VC and NVA (invented by the U.S. military) did not exist in the Vietnamese Communist mind. And despite the recalcitrant resistance of the target, our analysts were able to see through the communications and report the truth as it was happening.

In looking back, it seems to me that somewhere in the early 1970's the American people and their government made a tacit decision to let Vietnam fall if need be for the sake of ending U.S. involvement. That decision led to a thing called "Vietnamization," and in the SIGINT world, that meant getting the Vietnamese SIGINTers (known variously as the DGTS, J7/JGS, and SSTB) to a professional level instantly, a job as urgent as it was impossible. By 1973, the United States was intent on proclaiming the war at an end and Vietnam a thing of the past. The NSA effort on the problem was drastically reduced, and the job of NSA personnel in Saigon became primarily one of helping the Vietnamese COMINT effort to get on its feet quickly. As things progressed into 1974 -- when I arrived for the last time -- the irony of the situation was becoming palpable.

DOCID: 4019723
EO 1.4.(d)
P.L. 86-36

Congress was cutting back expenditures in Vietnam. Meanwhile, the North Vietnamese continued to build their forces in the south. The effort on Vietnam at NSA was reduced again. In July 1974, the Communists launched the Duc Duc-Thuong Duc campaign -- the first of magnitude in 10 years that had not been foretold by SIGINT.

The ironies multiplied as the situation worsened. A senior TDYer asked me what it was like to drive out in the country in Vietnam now that the war was over. We learned inadvertently that the Vietnamese COMINT organization in Danang was passing message volume figures and contact logs to the Commanding General, I Corps, who was keeping graphs and charts on them. In December, the Communists started the Phuoc Long Campaign -- again unforeseen in SIGINT. The province fell in January. Infiltration spiraled. We began to detect indicators that the reserve divisions in North Vietnam were preparing to move to South Vietnam. The Commanding General, II Corps expressed the opinion that the Communists were deceiving the SIGINT organization. I started a folk group in the local Catholic church.

By March 1975, it was clear that Congress was not going to provide funds to support the South Vietnamese military organization, which was accused of being corrupt and was utterly dependent for survival on the U.S. aid. The Vietnamese military began to waver in its self-assurance. Battles began to erupt around Pleiku in the highlands. I flew there on 7 March with [redacted] to review Pleiku Center's status. Banmethuot fell several days later. The President of the Republic ordered a "strategic withdrawal" from Pleiku which ultimately turned into a grisly horror show with thousands fleeing in insane terror to the coast. I ordered our NSA representative to return to Saigon at once. He barely escaped. By mid-March the highlands were in the hands of the Communists. The highlands campaign had not been foretold.

By late March, we began to feel like players in a classic tragedy. Events developed with a relentless logic too pat to be real. Things that never happen in real life were happening, and Saigon took on the look of a sardonic nightmare. In a fit of hysteria, Hue and Danang fell, our man escaping by air at the last possible moment. The Vietnamese military began to crack seriously. Stories reached us of the monstrous bestiality that rose out of the panic in the north. We booked our wives and children on the earliest flights available out of the country, caring little where they went so long as they left Vietnam. At Easter Mass (30 March), my folk group sang about peace, brotherhood, and joy in the newness of life while NSA wives wept in the congregation and my daughter, on the altar beside me, forced back her tears. The following Friday one of the singers in the folk group died in the C5-A crash. The palace was bombed by a renegade VNAF pilot. We took NSA families into our office that day for protection. The city was rocketed.

P.L. 86-36

Into early April, amid reports of panic and chaos in the military, we got the last of our families out and strained to get the work force out. Panic fluttered over Saigon. We closed down our houses and moved to a hotel for quick evacuation, should the end come with little warning. Tall, muscular young American men in civilian clothes and crew cuts appeared in the hallways of our building, muttering vulgarisms and Marine slang. Marine Colonel [redacted], a long-time SIGINTer and Vietnam veteran many times over, flew in quietly from the 7th Fleet (anchored just out of sight) to confer on the evacuation plan and the SIGINT support to it.

Through all of this, the NSA employees still in Saigon astonished me. They knew perfectly well that they were in very real danger, from the Communists on the one side and from incipient panic in the city on the other. Yet they never faltered. They banded together to support one another, worked harder than ever before, and dug intelligence out of the Vietnamese COMINT organization. They kept communications open, scheduled departures, destroyed classified material, and shipped out whatever valuable machinery they could. Their endurance, drive, and raw courage were a testimony to me of what people are capable of in a disaster.

When we were finally down to 16 people, none wanted to leave. More than once I had to deliver a direct and blunt order to get an NSA employee on a plane out of the country. Each volunteered to stay in the place of another, unwilling to desert the Vietnamese or to leave the job unfinished. Weary to the point of giddiness, they pushed themselves on, knowing that what they did could give the forewarning necessary to save American lives and prepare the Vietnamese for the ending. Through small-arms attacks on the outskirts of the city and rocketing at random spots, they kept their gritty humor and their morale.

We were down to four when [redacted] intercepts from COMBAT APPLE made it clear that the attack on Saigon was days away. The attack was to start at Tan Son Nhut -- where we were working -- and it would be a mixture of artillery fire and rockets. The timing was uncertain because the Communists were not sure how soon they could be in position.

Then it struck me that SIGINT was not being believed. The Embassy, it turned out, was of the opinion that the Communists were using communications deception to intimidate the Vietnamese. It was the final irony.

By that time we were down to three people. Then the attack came, as predicted. It began with a bombing from the air -- the first the Vietnamese Communists had ever attempted -- on the afternoon of 28 April. Small-arms fire began. The heavy artillery started after dark. Shells fell close to us and shook

EO 1.4.(c)
P.L. 86-36

communications gear so much that I feared it might go out of commission.

The exchanges we had with NSA during those last days and especially on 28 and 29 April were edged with cynical humor. The Vietnam task force at NSA desperately wanted to help, but there was literally nothing they could do except to give us information. We were somewhat less than kindly to them and to others who talked to us then, partly because of our tiredness, partly because of our bitterness over the Embassy's communications-deception reaction, but principally because we were mavericks and were hard to live with, even in the smoothest of circumstances.

The three of us got out by helicopter on the 29th and then spent days on ships going nowhere, or so it seemed. The sudden enforced inactivity after so much concentrated work was perhaps the greatest hardship.

A handful of the Vietnamese we knew and had worked with for years escaped. Most, like [redacted] did not. That is the hardest thing we have to live with.

Now that we are all back in the world of staff coordination, triplicate forms, and being asked to comment on someone else's comments about what he thinks of commenting, it is clear that there was much about the ending that left bitterness in our mouths. But when I look back, I'm glad I was there for the ending. And as long as I live, I will be ever grateful and immoderately proud of the NSA people who were there, doing the best they could because it was worth doing.

VIETNAM ARTICLES IN

DRAGON SEEDS

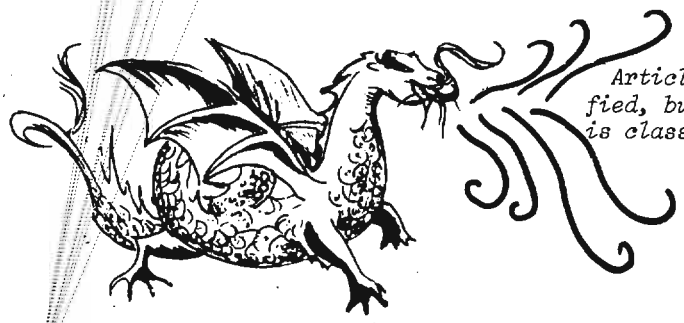
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

The following articles on Vietnam appeared in various issues of DRAGON SEEDS, the B technical periodical which was published from December 1971 through June 1974 (founder and managing editor, Mrs. Minnie Kenny, currently Chief, P16).

A complete set of DRAGON SEEDS is maintained in the P16 Cryptologic Library, Room 3W076, where copies may be read or borrowed. For information, call 4017s.

[redacted]	"Recovery of a Vietnamese Communist Callsign System"	Vol. I, No. 1	Dec 71
Allen L. Gilbert	"The Impact of ARDF on Traffic Analysis"	Vol. I, No. 1	Dec 71
[redacted]	"Letter from Pleiku"	Vol. I, No. 2	Mar 72
Tim Murphy	"Vietnamese Communist Tactical COMINT Operations"	Vol. I, No. 3	Jun 72
[redacted]	"Things That Go Clank in the Night"	Vol. I, No. 4	Sep 72
[redacted]	"SEADEV -- Mechanization for T/A Development"	Vol. I, No. 4	Sep 72
[redacted]	"Uncertain Origins"	Vol. I, No. 5	Dec 72
[redacted]	"The Development of a COMINT Translation Course for Vietnamese Linguists"	Vol. I, No. 5	Dec 72
[redacted]	"The Jack Butcher Case"	Vol. II, No. 1	Mar 73
William Gerhard	"One Chance in Three -- But It Worked"*	Vol. II, No. 2	Jun 73
Bee Kennard	"The 'C' Parallelogram, or A Vietnam Cover Story"	Vol. II, No. 2	Jun 73
[redacted]	"History of a Dragon"	Vol. II, No. 3	Sep 73
[redacted] Edward A. O'Connor	"1972-1973: A Vietnam Odyssey"*	Vol. II, No. 4	Dec 73

*Reprinted in this issue of CRYPTOLOG



Articles are not individually classified, but every issue of DRAGON SEEDS is classified TOP SECRET CODEWORD.

Classification of this listing is ~~SECRET SPOKE~~

P.L. 86-36

DOCID: 4019723

1972-73: A VIETNAM ODYSSEY

[redacted] and Edward A. O'Connor, F46

Reprinted from DRAGON SEEDS, Vol. II, No. 4, December 1973

P.L. 86-36

Approximately 125 kilometers SSW of Saigon, 4 hours by bus and 6½ hours by cycle, two tanks of gas by Honda, and 40 minutes by Air America "Gooney Bird," in Phong Dinh Province, Central Mekong Delta, lies the beautiful tropical splendor of Can Tho City and sanctuary/hideaway for IV Corps' ruthless, intrepid U.S. Advisory Team.

It was the Lunar Year of the Rat when the Odyssey began. The mission was to advise South Vietnamese Army (ARVN) personnel while they assumed the U.S. SIGINT mission in the delta from USM-607. Since there was no established precedence to follow, each problem encountered had to be dealt with in a unique manner. Realizing that extensive changes were essential to make the transfer of responsibility efficient, the first priority of the advisors was to circumvent the inherent language barrier and to establish a workable rapport with their ARVN counterparts. This was achieved, to some extent, through patient guidance and constant interface, i.e. sign language, graphic illustrations, etc. With such techniques at their disposal, advisors began to examine the innumerable problem areas.

Initial corrective efforts were directed at security procedures which were almost nonexistent. The following aberrations were rectified immediately: first, there was no ARVN officer on duty during weekends or holidays; second, an excess of defunct classified material was stored in file cabinets and boxes; third, and most important, ARVN personnel were not familiar with the use of the numerous incendiary devices for emergency destruction of crypto gear and classified documents. In addition, advisors established a picture badge identification system and access list for all authorized personnel. This list excluded one unidentified, indigenous individual who purportedly was employed by the 335th Radio Research (RR) company to guard the antenna field. (Can Tho Center's antenna field is located in a nonsecure area approximately 500 yards NE of the operations bunker.) Although the 335th RR Co departed, [redacted] remained vigilant as ever, at the expense of an unknown source.

Concurrent with improving security practices, a program to extend manual morse intercept capability was implemented. Vietnamese operators had and were continuously receiving training in intercept techniques, but their proficiency was far below that of their U.S. predecessors. Specifically, their copying speed was approximately 8 words per minute, they could not backlink activity, and they were unaware of the effectiveness of morse operator characteristics analysis. After discussing these problems with the ARVN commanding officer (CO), advisors received permission to reorganize and supervise the training program. The new program was successful enough, so that the supervision was eventually returned to the ARVNs. When new personnel arrived, they assumed their duties with a minimum amount of on-the-job training (OJT). However, after several months the operators, as well as other personnel, began to lose their incentive. To eliminate this negative attitude, the ARVN CO was convinced that a "Soldier of the Month" award should be initiated. This award consisted of 5,000 Piaster (provided by the advisors) and a Letter of Recognition. By U.S. standards the award was minimal, but the plot worked. The competitive spirit between sections increased; and following the first presentation, all personnel were striving to achieve the award.

The first award was presented to the Airborne Radio Direction Finding Ground-to-Air radio operator. Significantly, the ARDF tipoff function had undergone an extensive transformation and emerged from a state of chaos to the point of receiving special recognition. In fact, standard operating procedures were produced by this section and disseminated for employment throughout South Vietnam.

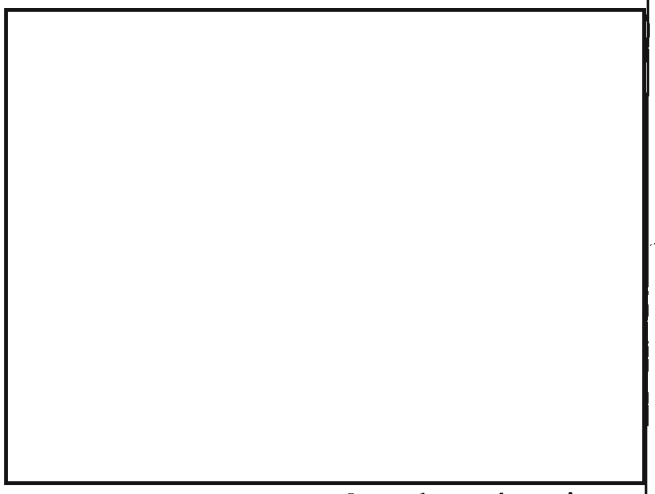
Following the cease-fire and associated withdrawal of American military personnel, the U6A ARDF aircraft assigned to the U.S. 146th Aviation Company were transferred to Saigon. Although four missions were tasked from Saigon daily, numerous problems occurred and approximately one mission per day was flown. Believing ARDF effectiveness could be increased with additional missions, advisors clamored for the assignment of ARDF aircraft at Can Tho Center (CTC) and the accompanying requirement for preparation of tech data lists (TDLs) for each mission. When four U6As were finally returned to Can Tho, the ARVNs did not possess the sophisticated, secure air-to-ground voice communications as American predecessors, and relied solely on the much slower process of one-time pads. Nevertheless, with Can Tho assuming control of the aircraft and providing mission tech data, ARDF results began to improve and personnel were instructed in methods of altering mission frag points to maintain greater cognizance on priority targets. As a result, more information was provided traffic analysts, enhancing development efforts.

In the early stages of the Vietnamization Improvement and Modernization (VIM) Program, there were only five analysts assigned to the TA section; two of them were radio operators for ARDF ground-to-air tipoff. The remaining three were required to devote all their time to preparing and transmitting daily TECSUMs. To increase productivity, five additional analysts were transferred to CTC, but they had only recently completed school and were unfamiliar

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

with operations. Complicating this situation, the new people spent almost 3 months painting, filling sandbags, and satisfying other administrative trivialities. When they were finally released to operations, their training was accelerated. In March 1973, the procedure for filing tech data was altered, a new system to handle unidentified entities was established, and the TECSUM format was revised to facilitate changes. Once analysts overcame their fear of error, development was successful and new entities were notated and forwarded as isolated.

Although positive results were being attained, a recurring difficulty plagued the TA sections --- the perplexing importance of serialization (NRs) and chatter extracts and the necessity for accurate logging of all entries to satisfy a computer, an alien wonder they had never seen but were told existed. In addition to the lack of experience and comprehension, only one traffic analyst spoke English and he was hospitalized with pneumonia for 3 months during this critical period. Instruction (pointing and drawing illustrations) was provided through non-analytic interpreters and with the limited operational Vietnamese of the advisors. After many hours of frustrating and occasionally humorous guidance (on the part of both advisors and ARVN personnel), periodic checks of the TECSUM and raw traffic indicated a continued improvement and a decreasing error rate.



Although results were favorable, there is no implication intended that the cryptanalytic effort was without its peculiar headaches. Numerous problems were experienced in couriering intercept from LLVI teams and from ASTDs when circuit outages occurred. Since the situation vacillated in direct relationship to the tactical environment, advisors were stymied in endeavors to alleviate this dilemma. Despite the requirement, air transportation (helicopter) was seldom available and courier by road was extremely hazardous. Yet LLVI teams attempted courier every 2 to 3 weeks and when necessary even traveled by bus in civilian clothes. Without any secure means available to transmit intercept for preparation of EMRs, these methods were the only alternatives to satisfy demands for timeliness.

Although timeliness is an innate characteristic of the SIGINT mission, natural and man-made phenomena often alter the course of events. An excellent example was the selection of a location and construction of CTC's AN/TRD-23 medium-range direction-finding (MRDF) site. Between July and September each year, the tropical monsoons visit Can Tho. Again, field expediency dictates "Nothing shall be wasted" (to include monsoons); therefore, concurrent with the arrival of the monsoon was Can Tho's "Annual Aqua Festival." Although these festivals improved morale and helped solidify relations with the local inhabitants, the "Year of the Rat" proved to be the last of the Aquacade Follies. In May 1972 land surveyors from Engineer Region IV (ER-4) inspected the only possible location for Can Tho's proposed MRDF site, which unfortunately was one and the same as "Mini-Lake," where the festivals were held. The surveyors estimated that approximately 7,000 cubic meters of fill dirt would be required to displace and remove all the water from Mini-Lake so that a base for the site could begin.

All of these calculations led to numerous questions (not to mention where next year's Aqua Follies would be held): "Where would this amount of dirt be found?"; "Once found, how would it be transported to the proposed site?"; and, finally, "Who would finance the venture?"

EO 1.4.(c)
P.L. 86-36

Because this MRDF site would be an integral part of the ARVN MRDF net serving all of South Vietnam and would be manned by ARVN personnel, it was automatically assumed that the ARVNs would make all financial and building arrangements. After 2 months of ARVN procrastination, paper shuffling, and overall apparent apathy, the advisors decided to initiate some action. There were 2 weeks of rambling over the countryside in a jeep, over roads previously traveled only by reconnaissance teams. Then the advisors found a large "farm-like" residence, with an expanse of adjoining land. After several hours of verbal ping-pong, threats, shouts, obscenities, and finally handshakes, the advisors had bargained with the owner for the required amount of fill dirt. The nominal fee agreed upon was eight 55-gallon drums of gasoline (hopefully provided by Uncle Sam) and six cases of American beer (provided reluctantly by the advisors from their very limited personal cache).

The fill dirt dilemma was solved; transporting it from the farm to Mini-Lake was still another predicament. After several sociable evenings with members of the ER-4 team, the advisors were able to borrow several 5-ton trucks and one front-end loader to fill them. There were no operators available to run any of the machinery, so the ruthless, intrepid advisors began a trial-and-error fill dirt operation, that would have put Contee out of

business in a week. Anyway, 2 weeks and 184 truckloads later (overlooking hours of exasperation at the controls of the front-end loader, or back and vocal strain when trucks were "unprofessionally" backed too far into Mini-Lake and had to be "push-pulled" out), the base level was nearly workable. However, continuous rains along with the rising water table postponed any substantial achievements until early December 1972, when the earth finally dried up and initial work began on the installation of the TRD-23.

While operations were running as smoothly as could be expected at Mini-Lake, 500 meters to the northwest was another facet of the MRDF project. This was the location of the obsolete AN/TRD-4 site where some of the equipment for Mini-Lake had been stored. The removal of this equipment left only the hut, connecting cables, and antennas. By order of the Commander of Can Tho Airfield, a different section of perimeter grass was burned each month. As fate would have it, the date for burning grass in the area of the TRD-4 site coincided with the operation at Mini-Lake, and no advisors were available to monitor the burning. GIs from the airfield command trudged out early one morning to begin their detail. With gasoline cans and blow torches they began what was supposed to be a small, controlled, well-supervised grass fire. All went well for the first hour or so. Personnel were strategically placed, armed with shovels and rakes, just in case something should happen. An undetected slight change of wind (in velocity and direction), began to move the fire toward the AN/TRD-4 hut and its many antenna cables. Before anyone realized what was happening, the highly inflammable cables began to burn and spread toward the remaining antennas. This probably could have been stopped with a minimum of effort, if there had not been a war in progress. ARVN helicopters returning from a sweep and destroy mission, flying low over the airfield, fanned the flames in every direction at once, creating pandemonium and mass chaos. Before the fire could be brought under control, approximately $1,500 worth of cable, connectors, and antennas had been destroyed.

Meanwhile, back at Mini-Lake, to insure that future rains would not destroy the equipment installed for the TRD-23, everything was elevated one foot. This was accomplished by pouring concrete antenna pedestals (12" high) for each of the 26 antennas and two (12" thick) 12 x 18' slabs to support the generators and the TRD hut. All this was completed in 3 weeks, with most of the time being consumed scrounging cement and lumber for forms. Before any antennas could be placed on their respective pedestals, four perimeter poles (each 40' high) had to be erected in each of the four corners of the antenna array, with aircraft warning lights fixed to the top of each one. (This was necessary because Mini-Lake/TRD-23 site was only 200 feet from the end of the Can Tho Airfield runway.) As soon as the poles were in place the lights had to be operational; thus another project was temporarily halted until a power source could be found. The only generator in the area was owned by the Pacific Architects and Engineers (PA&E, also known as "Promises, Alibis, and Excuses"); so advisors approached them and obtained permission to use their generator. Yet another delay of 3 weeks was incurred because PA&E had another requirement to supply power for the Joint Military Commission (JMC) and the International Commission for Control and Supervision (ICSS) peace-keeping forces while they were at Can Tho Airfield. The delay came as a blessing. Checking their cable supply, the advisors discovered a shortage and the generator in question was approximately a quarter-mile away. After securing additional cable, the day finally came when the power was available. When the poles went up, the electrical cable was laid a quarter mile to the generator, the aircraft warning lights were working, and now the final installation of antennas could begin. Not 2 hours later, a Vietnamese garbage truck, making its daily run through the airfield, veered off the road, cut the electric cable just laid, and felled two of the 40-foot poles supporting the aircraft warning lights. Had the advisors not been pillars of virtue and possessed of great fortitude, this would have discouraged them. But, being ruthless, intrepid types, they had the cable spliced and the poles back in place in a matter of hours.

Finally, on St. Valentine's Day 1973, the metamorphosis of Mini-Lake was a reality and Can Tho's AN/TRD-23 MRDF site became operational. ARVN personnel, however, were not familiar with even the most basic maintenance procedures to support the site. Any outages that occurred were normally extended until TDY personnel from Saigon could diagnose the malfunction and acquire the necessary parts.

Inadequate maintenance capabilities not only plagued the MRDF site, but all facets of operations -- vehicles, generators, air conditioners, commo/signal-equipment, etc. Since CTC was only permitted to perform first-echelon maintenance, repairmen assigned received only limited training, as opposed to the extensive schooling afforded their U.S. predecessors. As a result of limitations, any equipment malfunctions usually had an extended adverse effect on the entire operation.

As at any other field station, Can Tho's nucleus was the communications center (CC). Without this equipment running smoothly, the station was cut off from the rest of the intelligence community.

Prior to January 1973, the CC at W33 (intercept designator for CTC) experienced many maintenance problems. Because of cramped working conditions, maintenance personnel could not perform daily preventive maintenance (PM), and this resulted in many operational hours lost.

Recognizing the "cracker box" problem, advisors suggested to higher headquarters (Unit 15 -- Saigon Center) that the CC at Can Tho be relocated to the area vacated by the U.S. CC. This move would facilitate the following: first, daily PM could be performed, thereby eliminating approximately 50% of equipment down-time; second, the addition of three new circuits (two with Saigon and one with the proposed 44th Support Platoon) could be accommodated; third, a significant amount of circuitry and equipment was left by the U.S. communications people, which would simplify the transition; fourth, the proposed area provided ample space to house all CC equipment and would also allow for further expansion should the need arise; and, finally, the new area had the much-needed direct air conditioning ducts to aid in keeping the equipment cool and operating. With Saigon's concurrence, the move was made and the CC began to run smoothly.

For any operations to run smoothly, constant supervision and guidance are necessary; therefore, every month the senior advisor accompanied the CO/CTC on his inspection tour to the three subordinate ASTDs. These trips provided an on-the-spot review of equipment, personnel, problems at hand, and any foreseeable problems could be discussed.

Transportation was always the fastest, best mechanically tuned jeep available at CTC, while the ARVN driver was a conglomerate of Andy Granatelli, Richard Petty, Bobby Unser, and Steve McQueen. This combination of driver and jeep was needed most on trips to the 7th ASTD, located in Dinh Tyong Province. To reach the 7th from My Tho City, a spine-tingling drive along Ambush Alley (a stretch of road approximately 1000 meters long, flanked by thick jungle on both sides) was necessary. This was where jeep, driver, and all occupants hoped for a new speed record on each and every trip.

These monthly sojourns into the VC/NVA occupied suburbs of the Mekong Delta also allowed for sampling of the local culinary/gastronomical delights offered at the many roadside stands. These stands are known by many pseudonyms: "Ba muoi ba" stands (named after the Vietnamese beer "33"), "Hepatitis stands" (named after "post-dinner complications"), and more commonly known to all as "the local Howard Johnsons." Inevitably upon their return to Can Tho, the ruthless, intrepid advisors proceeded post haste (usually with a gait reminiscent of that of the "Green Apple Quickstep") to the dispensary for a small white envelope humorously marked "Stopgap," or "Cement pills, for internal use only."

The successful transition from U.S. to ARVN COMINT operations has been evaluated and found satisfactory. The only unanimous regret, reflected by both ARVN and U.S. personnel involved, is that the VIM Program didn't begin earlier. Naturally, there is always room for improvement; but, keeping in mind the "newness" of the Vietnamese in the COMINT business, much credit must be given for their many accomplishments in such a short period of time. The advisors at Can Tho Center feel that the desire of the Vietnamese to constantly better the quality of their COMINT product will continue and enhance the overall Vietnamese Intelligence effort.

Authors' note: The preceding article only highlighted some of the achievements and humor associated with the Vietnamization Improvement and Modernization Program in IV Corps. To discuss the numerous anomalies and corrective actions that occurred on a daily basis would be cumbersome and would detract from the continuity of events. In reality, these daily occurrences often had the characteristics of the aimless wanderings of an odyssey and the futility of attacking windmills.

FRANCOPHONEGLOS ANNOUNCEMENT

Printout VI of FRANCOPHONEGLOS, PROD's computerized dictionary of the French language which is sponsored by G52, is now available for all eligible users. Although exactly the same size as the previous printout, this one has been made more compact by revision of the definitions and the withdrawal of Source 55SUPP (which has been amply replaced by the new two-volume Harrap's). It has been brought up to date [redacted] *including the new terms in the 1974 NATO Glossary and 5500 records derived from analysis of the French and English texts of the Official Journal of the European Communities.*

EO 1.4.(c)
P.L. 86-36

Anyone having the necessary clearance and showing a need to know may request a copy of the printout from Barbara Dudley, 4814s, or [redacted] *4707s. Simple instructions for on-line-querying of the FRANCOPHONEGLOS are also available.*

P.L. 86-36

~~(CONFIDENTIAL)~~

DOCID: 4019723

THE DO XA PADS

Edward S. Wiley, B441

P.L. 86-36
EO 1.4.(c)
DGA

The Do Xa pad story began in the spring of 1963 in the last month before the onset of the monsoon season in Vietnam. Quang Ngai Province beyond the coastal enclaves was a contested area; the Viet Cong moved freely at night and avoided government forces during the day, unless they perceived a tactical advantage from ambush. As the end of the dry season approached, the commander of II Corps, General Nguyen Khanh, ordered a sweep of western Quang Ngai Province, including the region known as the Do Xa base area. The "Do Xa Operation" was launched on the morning of 6 May 1963 when ARVN elements of General Khanh's II Corps moved unchallenged into western Quang Ngai Province. By 12 May ARVN troops were less than 10 kilometers from the reported location of the Viet Cong's Intersector V command post. Airborne Radio Direction Finding (ARDF) aircraft had pinpointed the Intersector V radio station less than 2 kilometers from the position held by the ARVN on 12 May, but, as government troops moved through the Do Xa base area, the Intersector V radio station slipped away some 8 or 10 kilometers to the east.

On 13 May a company of South Vietnamese government forces holding a small sector in the Do Xa base area unearthed a watertight tin container weighing approximately 14 kilograms. Inside were more than a dozen packages of unused one-time key pads, all carefully wrapped in a rubberized sealant. An entire shipment of Viet Cong pads, buried in the soil of Do Xa, awaiting retrieval and distribution, had fallen into ARVN hands.

Word of the cache spread rapidly up the South Vietnamese chain of command, and the tin can and its prized contents were flown to General Khanh's headquarters in Pleiku. The opportunity for deception was obvious -- if. *If* the pads could be photographed and reburied without detection by the enemy and *if* the ARVN could hold their tactical position long enough to permit the pads to be duplicated. For if the ARVN held copies of the Do Xa pads, and if the Viet Cong eventually retrieved and used them, then the enemy's tactical communications would be readable throughout the life of the cryptographic materials.

General Khanh seized the moment. Within hours the shipment of pads was flown from II Corps headquarters in Pleiku to the Joint General Staff compound on the outskirts of Saigon. There the find was inventoried: ten packages of 50 pads each and four packages of six pads each -- a total of 720,000 groups of key.

Time was now the critical factor. American intelligence authorities in Saigon were alerted. Representatives from the Military Assistance Command, the Central Intelligence Agency, the National Security Agency, and the Army Security Agency were on the scene at JGS headquarters on 14 May to examine the materials. It was obvious that quick action to copy the pads and restore the packaging for reburial at Do Xa would require American technology and experience, and the South Vietnamese could allow the Americans only 4 days to do the job. General Khanh insisted that he could not hold his position at Do Xa beyond Saturday, 18 May. The Americans agreed. They would go all out to copy the pads and return them to Khanh by 18 May. The task was staggering: some 36,000 pages of key to be photographed and all packaging restored to its original state. The undertaking far exceeded any capability existing in Saigon. The nearest U.S. installation with anything close to the necessary facilities [redacted] The race was on.

The first step was to get the loaned cache of pads [redacted] for a technical estimate of the feasibility of the task at hand. NSA insisted that first priority be given to copying the pads before their return to General Khanh. CIA and NSA agreed that if the job were beyond the capability [redacted] the pads would immediately be flown to Washington. An officer from the NSA staff in Vietnam accompanied the pads on a midnight flight from Saigon to Clark Air Force Base in the Philippines, and at Clark a special aircraft was standing by to take the courier and pads [redacted]

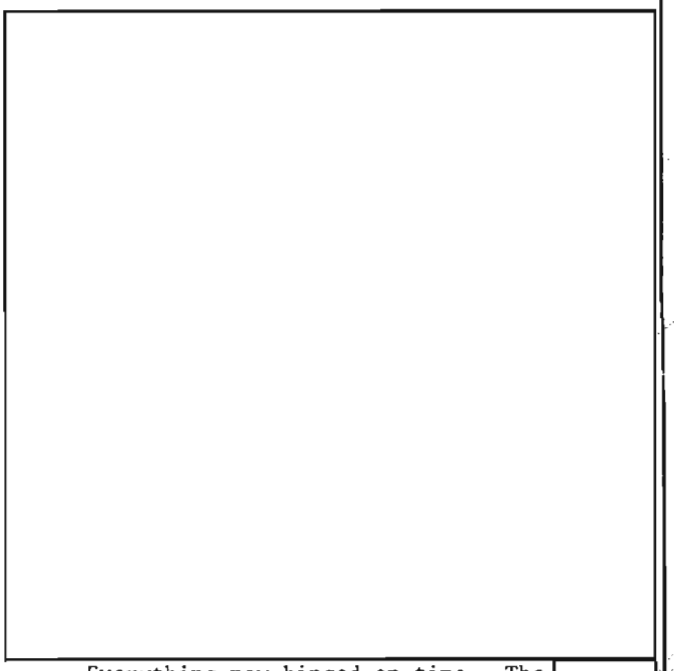
The initial reaction of the [redacted] was far from encouraging. Only one [redacted] man was at the station; even working around the clock for 3 days, he could not enter and reseal all the packages. Time was by then too short to consider sending the material on to Washington. Whatever was to be done would have to be done [redacted] At NSA's continued urging, photocopying the pads was to be accomplished first. Deception became a secondary concern. The seals on the packages were entered and the photographing began.

[redacted]

DOCID: 4019723

P.L. 86-36
EO 1.4.(c)
OGA

[redacted] Time was short.



Everything now hinged on time. The [redacted] technicians were pressing [redacted] for an extension of the 18 May deadline. Some room for optimism was reflected in an NSA message from Saigon: "In regards to deadline of 18 May, this is still the date we must have pads back. There exists a possibility that we might obtain a few days extension if Gen Khanh will hold present position in field...." This optimism was reinforced by a JSPC message to the NSA office in Saigon a few hours later: [redacted] had extensive correspondence with [redacted] and they think they have an extension until 22 May." Then the bubble burst. From the NSA representative in Vietnam came the following message: "General Harkins has approved sending complete package of crypto material via courier from JSPC to NSA. Stop any further reproduction of material ... tactical troops withdrawing...evidently result of someone trying to change our deadline from 18 May to 22 May, which cannot be approved due to tactical plans." A later message added, "...coordination was not completed throughout ARVN on the date of 22 May. Within a few hours troops had started to partially withdraw from terrain presently held. Since this was the situation our plan to rebury material went down the drain."

[redacted] technicians at [redacted] continued to work on the Do Xa pads. By the morning of 17 May, with the original deadline only hours away, JSPC cabled Saigon and Washington, [redacted] did not stop work on materials. [redacted] has been in touch with [redacted] and their word is that chance of returning materials to cache is still possible. Present plans are to have all materials photographed and original pads returned to very nearly original state. Plane is being held to depart for Saigon between 1200 and 1400 hours 17 May. Materials will be ready to attempt deception." By return message the NSA office in Saigon advised, "Latest information, as of 1000 hours local time the original plan is being carried out. Material will be in Saigon on schedule. Troops are holding terrain for one more day to complete original plan."

Success was within reach. The Do Xa pads had been copied and the original packaging reconstituted. The entire cache was flown to Saigon, arriving at 2115 hours on the evening of 17 May. CIA and NSA representatives inspected the refurbishing job, and the tin container was soldered shut. Shortly before dawn on 18 May, the Do Xa pads were delivered to Pleiku. A few hours later, as ARVN troops stood guard, a CIA officer from Saigon buried the metal cannister in the soft earth and covered the spot to disguise the intrusion. Under the mid-morning sun, the ARVN forces began to withdraw from the Do Xa base area. The long wait had begun.

Because Viet Cong radio stations often returned to previously held locations after moving to avoid ARVN sweep operations, ARDF aircraft closely monitored events around Do Xa after 18 May. An airborne fix of 12 June showed that the Intersector V radio station had moved back to within 2 kilometers of its location prior to initiation of the "Do Xa Operation." Expectations rose at NSA. Perhaps the buried pads were about to be retrieved and used. The watch over events at Do Xa continued.

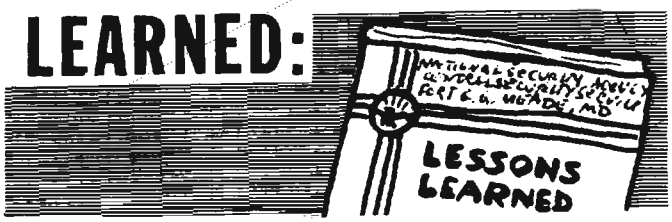
Meanwhile, the film of the Do Xa pads was flown on to Washington [redacted] Prints reached NSA headquarters on 25 May. Computer programs to match the recovered key with cipher text were written, and the material was speedily collated, sorted, and assembled. According to NSA's analysis, the Do Xa pads had probably been prepared for distribution some time before their discovery -- they had been wrapped in Viet Cong newspapers dated May 1961. Further examination suggested that the Nam Bo Regional Committee had been responsible for forwarding these cryptographic materials to their destination. By 5 July, NSA was able to report the identity of some intended recipients of the Do Xa pads: "Some pads and series of pads designed for use between Hanoi and Saigon/Cholon Special Sector. No known link between them."

All intercepted Vietnamese Communist radio traffic was checked for evidence that the Do Xa pads had been retrieved and used. Results were negative.

Somewhere out in the western reaches of Quang Ngai Province in Vietnam a cannister of unused one-time pads lies buried in the moist earth, undisturbed by the events of more than a decade and unknown save to a few who recall those hectic days of May 1963.

DOCID: 4019723

LANGUAGE LESSONS LEARNED: A Personal Memoir



[redacted] G95

It was a typically hot and humid day in Saigon when our jeep pulled up at the building that housed Headquarters, Military Assistance Command Vietnam (MACV). But it was not the humidity that made me uncomfortable. The purpose of my visit to the "nerve center" of the U.S. military establishment in Vietnam was, judged by the standards of the day, deceptively simple. Convinced that obstacles were awaiting me, but fortified by the thought, "The older I get, the less I have to lose," I entered the building.

At the time I was working with the linguists at USM-626 on the analysis, translation, and reporting of Vietnamese Communist (VC) military operational traffic [redacted]

The obvious source of such information was MACV. At that time NSA had a small liaison element at MACV. After a brief stop there, a couple of phone calls, and a guided tour through a labyrinthine complex of corridors, I found myself inside a human beehive known as the Combat Operations Center. Documents galore, wall-to-wall sliding maps, briefing charts, blackboards, and strategically placed desk officers who were responsible for specific areas of the country. I explained our requirements to the desk officer in our area of interest, and in a short while I had in my possession copies of the U.S./ARVN Disposition of Forces and other relevant documents. It was then that the desk officer showed me a MACV publication entitled *LESSONS LEARNED*. It turned out that after every tactical operation the platoon leader, company or battalion commander, or other person in command would prepare a detailed report -- a kind of postmortem -- of the operation, outlining the problems encountered, the results achieved, and, of course, the "lessons learned."

I do not know the fate of that unpretentious publication with the eyecatching title, but I have never forgotten it. Since the SIGINT industry, like any other field of human endeavor, progresses on a "building block" basis -- one generation profiting from the successes and failures, the trials and errors of the preceding one -- I have often wondered how an NSA publication entitled *LESSONS LEARNED* would be received. Suffice it to say that if there were one, I doubt whether any of us could resist the temptation to take a peek inside!

In any event, after 20-plus years of involvement in SIGINT Vietnamese language problems, I am convinced that there are more than a few lessons to be learned from our experiences. My conclusions, obviously, are based on my personal vantage point and, as the saying goes, "do not necessarily reflect the views of the management."

"Could We Have Done Better?"

EO 1.4.(c)
P.L. 86-36

The expression "the language problem" inevitably creates in the mind of the listener or reader a negative image -- insufficient numbers of linguists, insufficient skill levels of linguists, inadequate training, insufficient effectiveness in job performance, etc. But in the language field, as in any human endeavor, there is also a positive side to the coin, which we often tend to forget or at least do not stress. So, before we ask "Could we have done better in the SIGINT Vietnamese language effort?", let's stress the positive. That's easy to do. Vietnamese linguists, civilian and military, made an enormous contribution to the National SIGINT effort. That contribution is not yet chronicled, but it is nonetheless well documented. The repositories can yield mountains of evidence [redacted] that the linguist played a central role in the SIGINT production process. Untold numbers of unsung and unheralded linguists met the challenges of the time with high dedication and exceptional talent. Therefore we mean them no disrespect when we ask ourselves, "Could we have done better?" or when I answer that question with a resounding "Yes!"

The language function, to use an expression of a local sports commentator, is really "a very simple game." (I might add at this point that my focus is on the translation-transcription world and not the cryptolinguistic arena, where

DOCID: 4019723

the word "simple" may raise some eyebrows.) All the linguist has to do is determine:

a) the content of the message or the voice transmission;
b) its intelligence value, if any; and
c) the appropriate vehicle for reporting the information.

The development of linguists to accomplish "a" was a far more formidable task than to produce those skilled in "b" and "c". It was precisely there that most of our language headaches originated.

One of the foremost linguists in the Agency, during a conversation in which I was agonizing over the problems we were having in developing a cadre of skilled linguists, said, "The language problem is 98% managerial and 2% technical." I was astounded at that remark and was inclined to pass it off as a humorous hyperbole. With the passage of time, however, the truth and the wisdom of that observation became all too clear to me. Virtually all the languages we have to deal with are fairly well documented. There are, of course, exceptions, such as parts of sub-Saharan Africa and Asia. The Vietnamese language, however, is *not* one of the exceptions and, in essence, the "technical difficulty is in ourselves and not in the set."

Linguistic Quality Control

If I were asked to name the most serious flaw in the Vietnamese language effort, I would unhesitatingly point to the training and development of linguists. If I were asked to state what main ingredient was missing in the recipe, I would unhesitatingly say *quality control*.

What does quality control connote in this context? Well, for openers, let's take a look at Webster's definition: "the aggregate of functions designed to insure adequate quality in manufactured products by initial critical study of engineering design, materials, processes, equipment, and workmanship followed by periodic inspection and analysis of the results of inspection to determine causes for defects and by removal of such causes."

As we gradually moved from the role of interested observer watching the French chase the Viet Minh all over the countryside with consummate lack of success to that of active participant when *we* took over the chase with equal frustration (by this time it was the Viet Cong -- which means "Vietnamese Communist" and which the RVN applied to all communists, north or south), the pressures on the SIGINT community understandably became more intense.

It is part of our national psychology to "think big" -- assembly line production, "massive retaliation," "cheaper by the dozen," etc. So, faced with a problem of immense proportions, the logical move was to respond in kind. If we can produce rifle parts on an assembly line, then we can produce Vietnamese linguists on the same scale and at the same pace, right? Wrong! There were *far too many* linguists with *far too little* language ability. The most worrisome effect of this phenomenon was not the squandering of resources -- as bad as that was -- but the increased hazard of providing customers with inaccurate SIGINT, which, of course, is worse than no SIGINT at all. This problem of linguist training and development plagued us to the very end of the war. Why? The answer, in large part, was the lack of effective quality control from the "engineering design" to the "manufactured product."

Linguist Selection

Consider, for example, the selection process. I am aware of the existence of various screening mechanisms, including language aptitude tests, which are designed to permit only those who are qualified for language training to enter the pipeline. On the basis of my experience, I have to believe that the system broke down. No training in the world, no matter how well staffed with expert instructors or how well structured the course may be, can succeed if the students are either not qualified by dint of aptitude or academic background, or not motivated. If the selection criteria are valid, then they presumably were waived at times. If they were scrupulously followed at all times, then they are invalid.

Language Training

Consider also the training segment. Again, there are undoubtedly tests and various controls or safety valves designed to permit only the qualified to emerge. Here, too, the system had glaring weaknesses. The tendency throughout the war was to evaluate a training program primarily on the basis of the caliber of the graduates. This, in itself, may have been inherently unfair to the school and the instructors in that, as stated before, the students may not have had the prerequisites, and no type of training could have succeeded. We were generally satisfied with the training provided by the National Cryptologic School (NCS) -- we had firsthand knowledge of the skill of our instructors, the content of the course, the qualifications of the students, and the capabilities of the graduates. The physical proximity of the NCS and the fact that training and operations were "all in the family" permitted continuous and close contact with the school authorities and instructors and facilitated monitoring of the program and a reasonable degree of quality control.

With the Defense Language Institute (DLI), however, it was a different matter. Distance,

EO 1.4.(c)
P.L. 86-36

both physical and organizational, posed a formidable barrier, for all practical purposes, for the kind of liaison that we were able to maintain with the NCS. The DLI training, for the most part, remained unevaluated. At times there was considerable unhappiness with the skill level of DLI graduates. At other times the graduates' on-job performance reflected well on the training they had received. We tended to treat the symptoms rather than the cause of the ailment. Where were the weak points: student selection? the expression of our requirements? instructors? course content? the time gap between training and operational assignment? on-job training? the nature of the operational assignment? There probably were elements of all these factors, but to my knowledge there was little or no concerted, systematic effort to identify them precisely, weigh their importance, and take corrective action.

I had occasion to visit an SCA training facility where I and other members of a TDY team were briefed on the training programs, their objectives, and contents. Aware of some seemingly chronic difficulties we had been having with field product, I asked one of the program managers if there was any attempt to obtain feedback from the field stations, such as by a form to be filled out by the operations officer which would appraise the performance of the students who had completed the course. "Yes, we do have such a form," he responded. "What do these forms tell you?" I asked. "These forms tell us," he said with an impish smile on his face, "that people don't like to fill out forms!" So much for quality control -- at least in that program. There were undoubtedly other attempts to ascertain the quality of the trainees, and perhaps there were some remedial measures taken -- but the impact of any such measures was not readily discernible.

Development of Voice Linguists

One of the most frustrating quests in the area of linguist development was the effort to produce voice linguists. The personnel who could transcribe a free-flow, unformatted, and unpredictable Vietnamese conversation accurately and with reasonable speed were few and far between. Try as we might, the system simply did not, or could not, produce this type of linguist. Maybe we were faced with an "impossible dream." The use of indigenous Vietnamese -- the DANCER program -- for the transcription of VC voice communications, as well as for direct support in combat operations (as was the case primarily with the Marine units), was generally successful. I doubt that the nature and the difficulty of the tasks we expected the trainees to perform or the dimensions of the process to produce such linguists were ever adequately spelled out. If they were, then again the quality control was weak or completely lacking.

"Targetists" vs. "Functionists"

The deployment and use of Vietnamese linguists were generally and rightfully considered to be organizational prerogatives. Down through the years at NSA, the organizational structure has been the object of a tug-of-war between the "targetists," those who advocate plugging all the necessary cryptologic skills into one target-oriented unit, and the "functionists," who would organize primarily along functional lines and assign specific skills to specific problems on a temporary or ad hoc basis. Should cryptanalysts or programmers, for example, be concentrated in one organization, or should they be dispersed among various organizations? In either case, at what echelon? -- section, branch (or the new "work centers"), division? As the Vietnamese language problem grew in quantum jumps, the "targetists" emerged as the dominant influence. The linguist workforce was fragmented and linguists were assigned to various elements within the VC problem. In terms of effective and efficient use of scarce resources, it was one of the worst things we could have done. There was much to be said for this organizational approach, and there are those who are convinced that it was the *only* method. I, however, remain unconvinced. I believe we paid too heavy a price for the dismemberment of the Vietnamese language effort. The effect was to dilute control over the most skilled of the Vietnamese linguists whose talents could have been applied over a much broader area in the management and conduct of SIGINT language functions. As it turned out, they became highly localized, or specialized, if you will. So in the critical areas of linguist development, product review and control, field support, standards, flexibility in linguist assignments, construction and maintenance of language working aids, especially the most vital of them all -- a comprehensive dictionary -- our posture was weakened. Organizations that corner the market on talented personnel understandably tend to place such people under a form of "protective custody," regardless of the size or complexity of the workload. The Vietnamese problem was no exception. We will never know what might have been if the "functionists" had won the tug-of-war. I will never cease to wonder, however.

Language Lessons Learned

If we have really learned our lessons from the Vietnam experience, we should be taking action in any or all of the following areas:

● *Establishment of a system of quality control for linguist training and development.* The terminal objectives must be defined in specific, unequivocal terms.

[redacted]

EO 1.4.(c)
P.L. 86-36

[redacted] The system should include such items as an Operational Qualification Examination (OQE) which would do two things: a) license the linguist to practice, and b) provide a barometer on the effectiveness of the training program.

● *A thorough review of the selection criteria.* Are the criteria valid? Are they being maintained? It may be a normal reaction to relax them in times of crisis, but that is precisely when we must *not* relax them. We cannot compensate by quantity for what we lack in quality -- at least in the world of language and linguists.

● *Evaluation of the training programs.* Are they meeting our requirements? Do they need revision or updating? Can we really develop linguists who, for example, can cope with a [redacted] or are we reaching for the unattainable? What mix of trainee qualifications and training programs is needed to produce such a linguist?

● *An active dictionary system.* Only in recent years have we awakened to the importance of having authoritative, current, and comprehensive dictionaries in the languages for which we are responsible. It was only in the late 1960's that the Vietnamese language effort produced such a dictionary, known as RICE BOWL, for Vietnamese and a system for managing and maintaining it. The dictionary was also computerized and could even be interrogated on-line. A USSID was issued establishing it as the authority to be followed by NSA and SCA linguists in translation and standardization, as well as the procedures for its maintenance. [redacted] Someone in that distant past had had brilliant foresight, but, unfortunately, the infant glossary was never given the necessary nourishment and it, as well as the idea, died. Our failure to build on that glossary was a crucial mistake, and it cost us dearly in the ensuing years in terms of linguist capability and product quality. Very useful information on the meanings of new terms and the expansion of new abbreviations appearing in traffic went down the drain. Who needed to document and disseminate that data, it was felt. After all, John Doe and Mary Smith, our senior linguists, were immortal and would always be around to answer questions! Actually, however, the dictionary is "the linguist's best friend." Accuracy and speed in SIGINT language production are very often dependent on the quality of that friendship. The fragmentation of the Vietnamese language problem was undoubtedly a factor in our neglect of this vital working tool.

Today a language-processing organization that does not have an active dictionary system, in which new terms and abbreviations are duly recorded and processed for inclusion in a machine-listed data base, is simply not fulfilling its responsibility. This is clearly not a technical problem. It is a management problem. We have reared a generation of linguists who assume that once a message is scanned or translated, or a tape is scanned or transcribed, their task has been completed. Since they do not document the new terms and abbreviations for the benefit of others, the wheel keeps getting rediscovered. One of the senior NSA linguists once suggested that a linguist's performance appraisal should automatically include a rating on the linguist's fulfillment of the responsibility to extract dictionary data from the traffic he processes. This suggestion has much merit and should certainly be a factor in performance appraisal.

● *Consolidation of linguists and language problems.* We should take a long, hard look at the current deployment of our linguist workforce to determine if consolidation would be advisable. Are we deriving the maximum benefit from the most skilled of our linguists? Do linguists have the opportunity to work on a variety of targets or perform a variety of functions? Are we confining them to a specific target or area in order to satisfy an artificial organizational bias? In our Vietnam experience, there were some elements that were "linguist-rich" and others that were "linguist-poor." The negative impact of such situations on linguist development and product quality control are obvious.

Career Incentives and Motivation

The problem of career incentives and motivation could easily be the subject of a separate article. The difficulties encountered in the Vietnam experience were symptomatic of long-standing attitudes toward language work and linguists. I happen to believe, for example, that the SCAs will never really develop a truly professional cadre of career linguists until such time as senior translators and transcribers are given officer ranks. It takes about 15 months to train a fighter pilot to the point of combat readiness, and a much longer time to develop a professional linguist to a point of "combat readiness." I have yet to see a fighter pilot who is *not* of officer rank or an SCA full-time professional linguist who *is*. In the NSA context, it is absolutely essential that selected individuals whose strength lies primarily in their mastery of a foreign language and the ability to apply this knowledge in the SIGINT world be at the GG-15 and GG-16 levels and be highly visible to the linguist population. Opportunities for advanced language training and

the chance to grow in the profession are equally important. The crush of the pressures of a wartime situation did not afford us much time for a proper exploration of the subject of linguist incentive and motivation. Identifying the root causes of the dissatisfaction or disinterest of Vietnamese linguists may have shed light on situations that were unsatisfactory and which management actions may have been able to remedy or at least improve.

There are undoubtedly many lessons that were learned from the Vietnam experience. These few that stand out in my mind are by no means exhaustive, but I believe they do offer us guidelines for the future. Since they are presented from a personal point of view, they are subject to debate. They are couched in general terms because the individuals and organizations were but players in the drama -- as the Bard of Avon said, "The play's the thing." They are stated with that greatest advantage of them all -- hindsight.

EO 1.4.(d)
P.L. 86-36

Had there been a publication called *LESSONS LEARNED FROM THE KOREAN WAR*, with a detailed account of the problems and pitfalls in the effort to develop an effective SIGINT Korean language capability in a wartime context, we might have been better equipped to respond to the requirements for SIGINT support in the Vietnam War. Perhaps we would have done things just a little bit differently with much better results!

The SIGINT record in the Vietnamese conflict is one of considerable achievement. The Vietnamese linguist contributed immeasurably to that record. It is the hope here that as we continue to examine our language posture and to strive for ways to strengthen and develop it to a point of both "peacetime effectiveness" and "combat readiness," at least one or more of the "lessons learned" from Vietnam will be of some value.

WANTED: A GOOD HOME

for 32 copies of an "old faithful" working aid Degarbling Code Text (National Security Agency, 1954, SECRET). Working aid is no longer being used at National Cryptologic School and will be destroyed if no one wants copies. Take one copy, take two, take as many as you want...

Contact [redacted] *P16, Room 3C099-1, 5642s.*

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

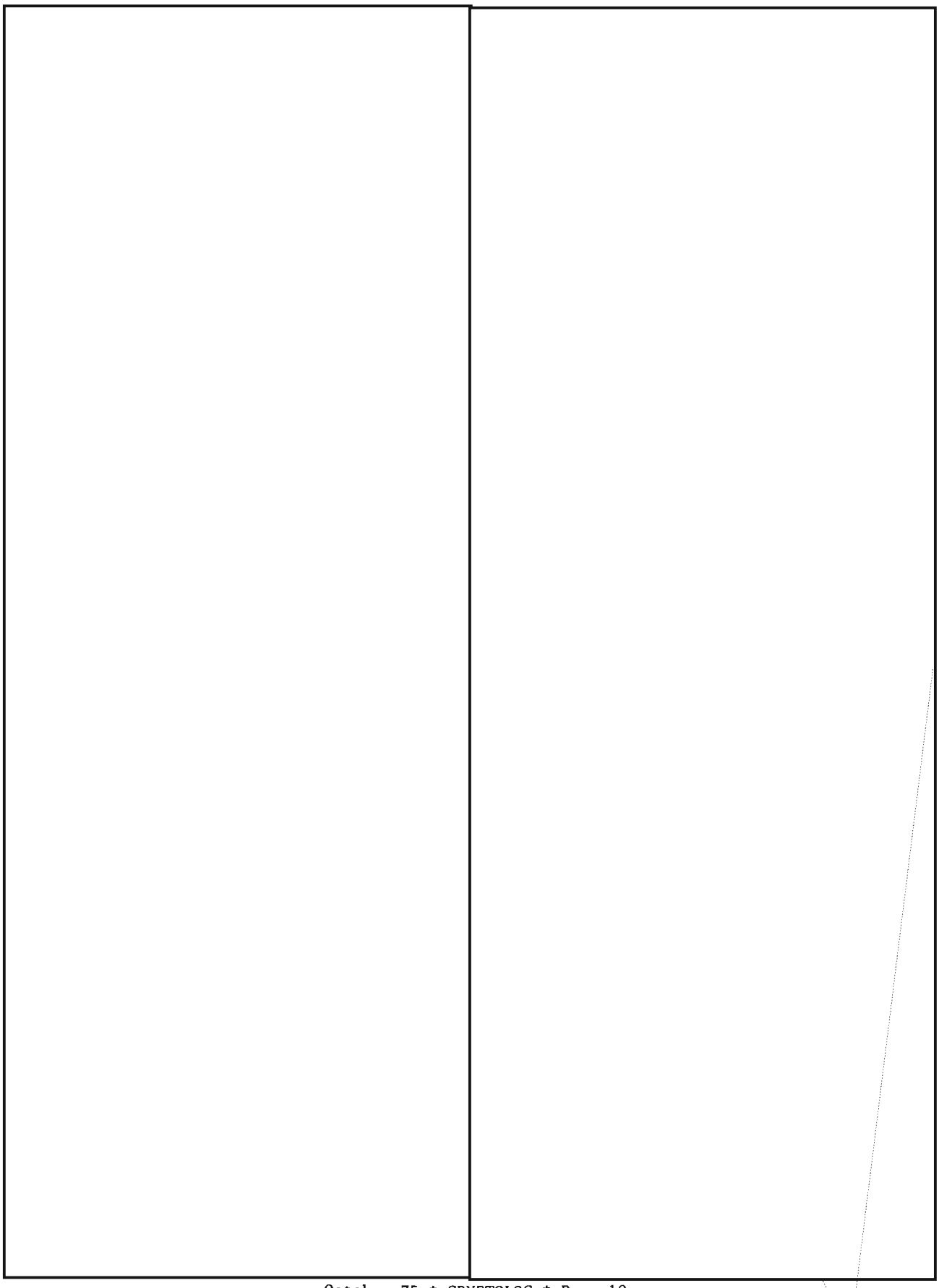
EO 1.4.(c)
P.L. 86-36

~~TOP SECRET UMBRA~~

P.L. 86-36

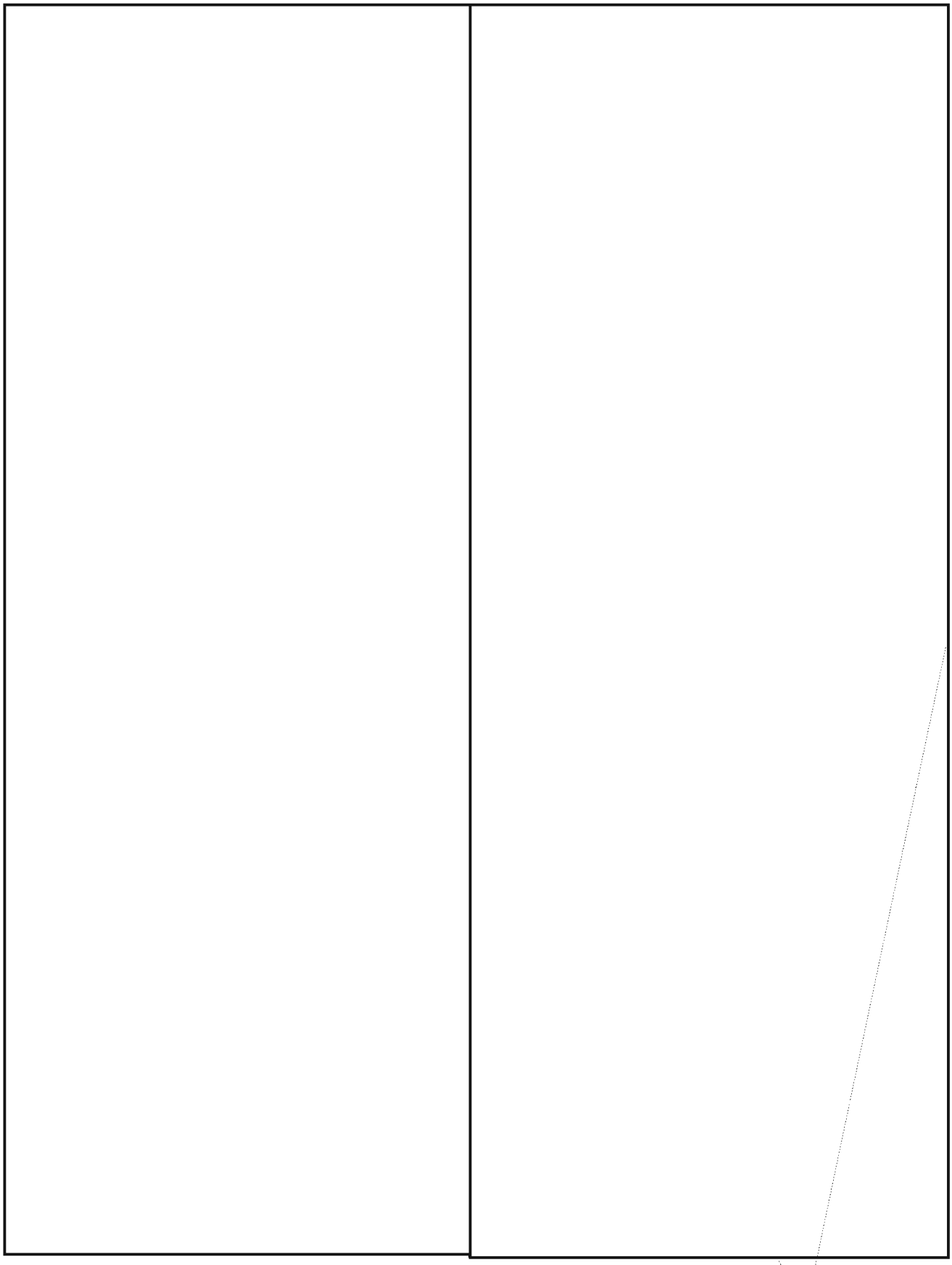
~~TOP SECRET UMBRA~~

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

DOCID: 4019723



EO 1.4.(c)
P.L. 86-36

[redacted]

[redacted]

Editor's note: The author of this article has chosen to use a nom de plume because he feels that, if his real name were to appear, he might seem to be taking credit for the work performed so long, so diligently, and so successfully on [redacted] *by a hundred people.*

THE WINNAH-KID APOSTROPHE!

It was a tough fight, Maw, but I lost! I knew that Kid Apostrophe would be a tough contender. One of our editor's, Vera Filby, wrote a short item, "The Apostrophe: Some Thought's" (CRYPTOLOG, November 1974) in which she dealt with plural ending's, with and without apostrophe's. So when I became CRYPTOLOG editor I knew I'd have a tough bout with the Kid. Well, here I am, after putting the fourth issue together, and I'm throwing in the towel. For four months, Maw, I tried to make sense out of how to pluralize abbreviations. SOI's? TECHSUMs? But now, after hearing all the arguments about "familiar vs. unusual abbreviations," abbreviations that "sound like words" vs. those that you read like individual letters, those that end with an S in the singular anyway, etc., I know when I'm licked. So in this issue, and in subsequent issues, any and all abbreviations will be pluralized *without* the apostrophe: SOIs, ASTDs, TECHSUMs, etc.

In case this offends any purists, here! Sprinkle them in at will! ''

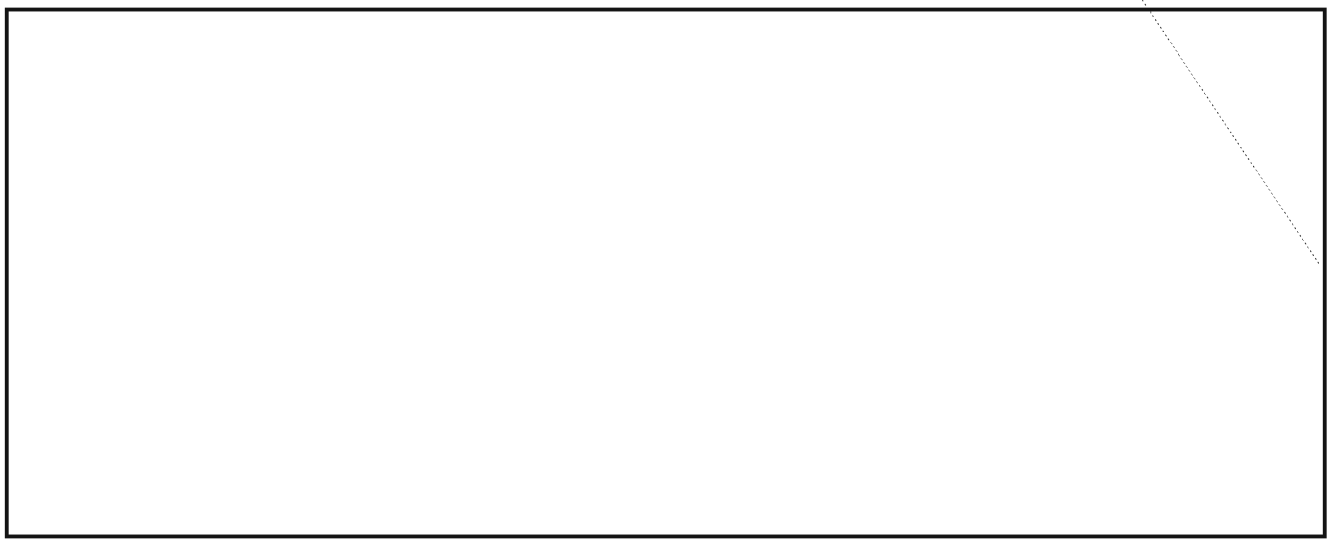
(UNCLASSIFIED)

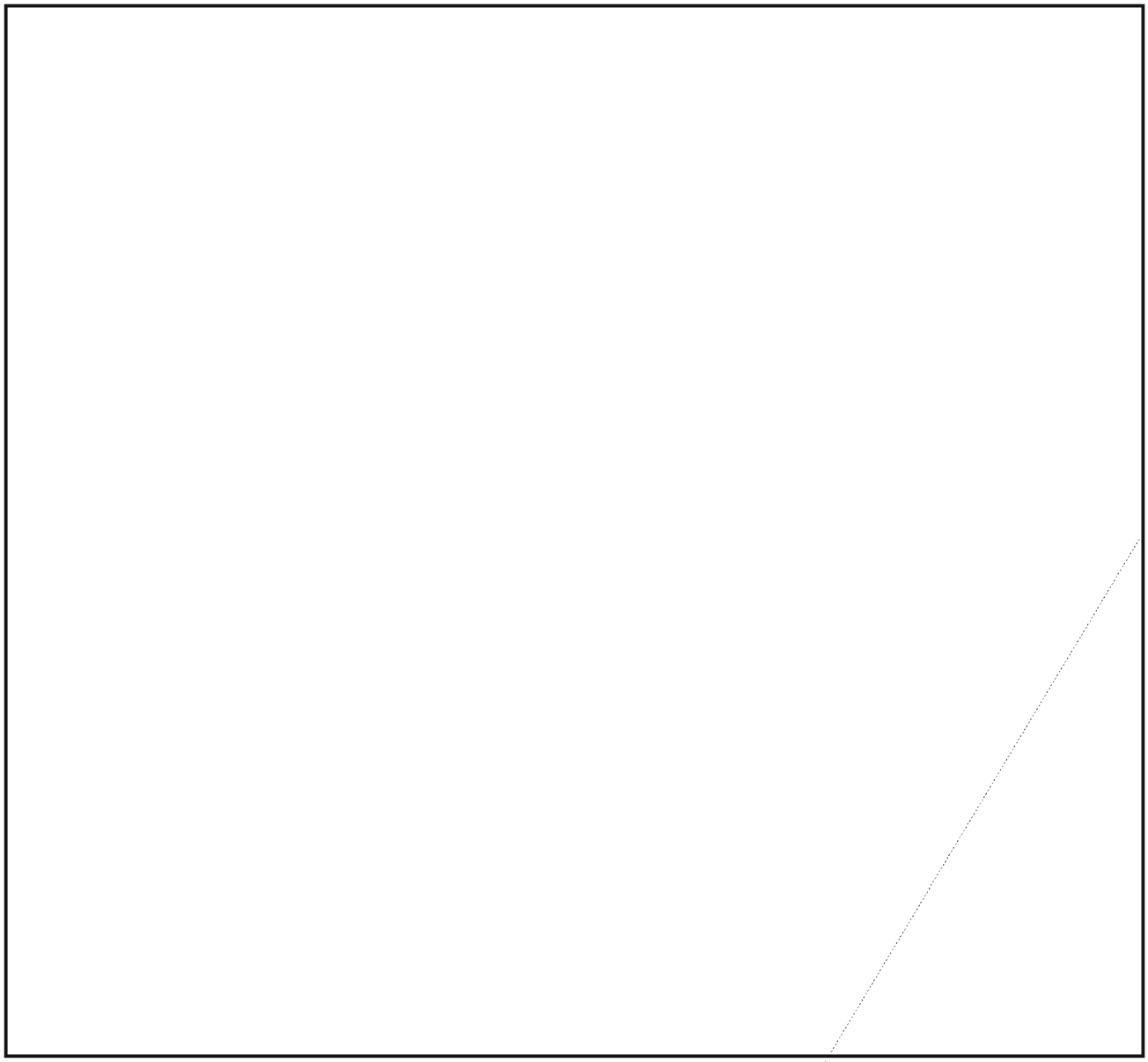
P.L. 86-36

NSA-crostic No. 1

In the early 1950's I constructed a series of about 60 Russian-language Double-Crostics as language-teaching aids (does anyone still remember those purple Ditto sheets?). Recently I have received a numerable request to construct a new series. But I'll do better than that: I'll construct a series of English-language ones using quotations from published works of our own NSA-ers. The following NSA-Crostic is the first in the new series. (Solution will appear next month.)

CRYPTOLOG Editor





DOCID: 4019723

IRONHORSE: A Tactical SIGINT System

[redacted] P.L. 86-36

During the Vietnam conflict, tactical commanders in Southeast Asia (SEA) had a continuing requirement for more and better tracking data on aircraft activity over North Vietnam (DRV). Increased low-altitude activity and scrambles of MIG aircraft could not be seen by U.S. radar. As command's ability to exercise direct control over U.S. aircraft improved, so did their need for this type of tracking data. U.S. SIGINT provided these commanders with tracking data at low altitudes and during deep penetrations into enemy air space. In answer to their need, a USAF Security Service unit, the 6924th Security Squadron (USA-32) stationed at Da Nang, RVN, began providing a limited amount of needed data through Project HAMMOCK in November 1965.

HAMMOCK was a manual plotting system of SIGINT derived from USA-32 copy and from information relayed from airborne intercept platforms (ACRPs) operating over the Gulf of Tonkin and Laos. HAMMOCK, however, had severe limitations. Intercept from USA-32 was relayed to the Tactical Air Command Center, Northern Sector (TACC,NS) (Fig. 1), at Monkey Mountain, by secure tele-

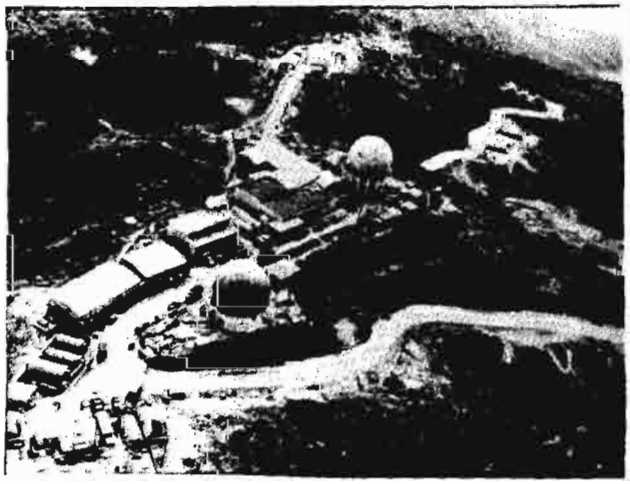


Fig. 1

phone. The data was plotted and then relayed via secure teletype to Seventh Air Force, where it was manually plotted for display to Command officers. TACC,NS also provided this information to the Commander, Task Force 77 (CTF-77) of the Seventh Fleet operating in the Gulf of Tonkin and to the Marine Tactical Data System (MTDS) in the form of radar plots. This manual system was limited to a maximum of ten tracks and its quality and timeliness were affected by the number of steps involved. Time from intercept to the consumer was usually 8 to 10 minutes, during which time an aircraft could have traveled 150 miles from the area of interest.

The need for a rapid and therefore automated transfer of data was realized. Systems attempting this had been achieved. The success of Project FURNACE, the automated plotting of SEA strike activity, begun in June 1964 and operational by mid-September, led to a project to rectify this time problem. Approved in November 1964, the project was given code name IRONHORSE. The office of R8 assumed responsibility for the technical development and provisioning of equipment for a "visual display of SIGINT derived tracking of aircraft reflected in [redacted] DRV Air Defense Communications." EO 1.4.(c) P.L. 86-36

The problem as seen by R8 was that of a classic command and control operation. The mission of TACC,NS was the control and warning of USAF strike aircraft over DRV. Data from a maximum number of inputs had to be reduced and fused into a common data base and presented to the battle commanders. Their solution was a data processing/display/forwarding system to automate the processing of manual data through the use of cathode ray tube (CRT) displays and the rapid forwarding of selected track data to the consumer via a data link (Fig. 2). In

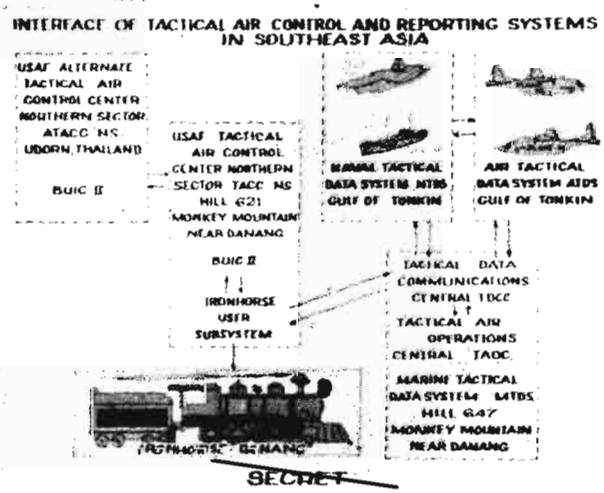


Fig. 2

addition, all intercept would be placed on magnetic tape for later processing and forwarding in an Electrically Formated Air Intelligence Report (ELFAIR). The area of coverage included North Vietnam, Laos, [redacted] South Vietnam, [redacted] This area was considered to be within the established range of the combined U.S. radar system, defined as a 180° arc, 235 NM from 19°30' north latitude 170°00' east longitude. The reason for limiting coverage to this area was to prevent compromise of SIGINT-related tracking information to non-SI cleared individuals. EO 1.4.(c) P.L. 86-36

DOCID: 4019723

After the original concept was approved in November 1965, it took 2 years to assemble the necessary equipment and to write and debug software. The equipment was installed in vans and delivered to Da Nang in November 1967. After 4 months of testing and interfacing with TACC,NS the system was declared operational by USAF on 27 March 1968. Later in that year, a new operations building was built and all IRONHORSE equipment, the S&W center, and operator positions were put under one roof. Shortly after the March operational date, it was decided to build a second system, IRONHORSE II, to be placed at USA-29, Udorn, Thailand as a backup for the Da Nang system. A fire in the Marine bomb dump in April 1969 caused virtual destruction of the operations building. The force of the explosions and the accompanying shock waves caused the base perimeter to be moved, and the Operations site was isolated from the rest of the base. Emergency destruct procedures were initiated. Most of the computer programs and documentation were destroyed. Fortunately, none of the IRONHORSE hardware was damaged. The equipment was removed to an environmentally controlled quonset hut. For the next 3 months, two programmers and a data analyst reconstructed programs, manuals, and operating procedures. A new operations building was built and IRONHORSE resumed operations in July 1970. The IRONHORSE mission was continued at Da Nang until April 1971. During November 1970 the decision was made to move IRONHORSE II to Udorn to take over the USA-32 mission concurrent with the U.S. withdrawal of forces. The system remained operational until December 1972, when the SEA tactical data interface was terminated.

The hardware for the IRONHORSE system consisted of a special version of two AN/GYK-9 FLEXSCOP computers (CP818s). Inputs were provided by 22 AN/GGC-15 (AG-22) configured intercept positions (Fig. 3), which copied both manual morse and radio telephone and from four Model-35 teletypes operated by data analysts (Fig. 4). CRTs were added to meet the requirement that it be a visual display (Fig. 5). The

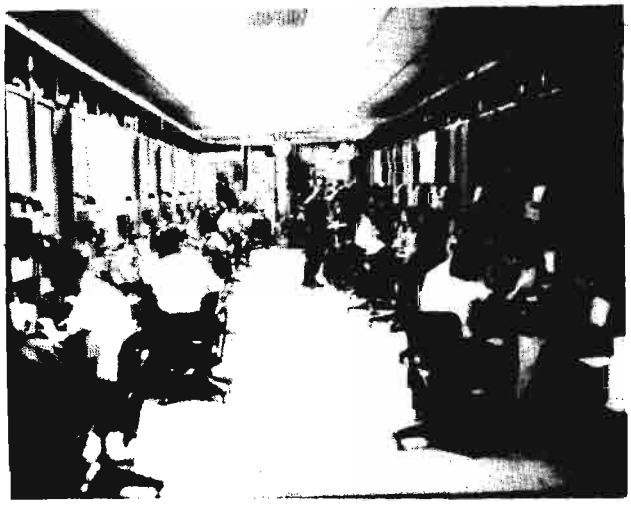


Fig. 3

Fig. 4

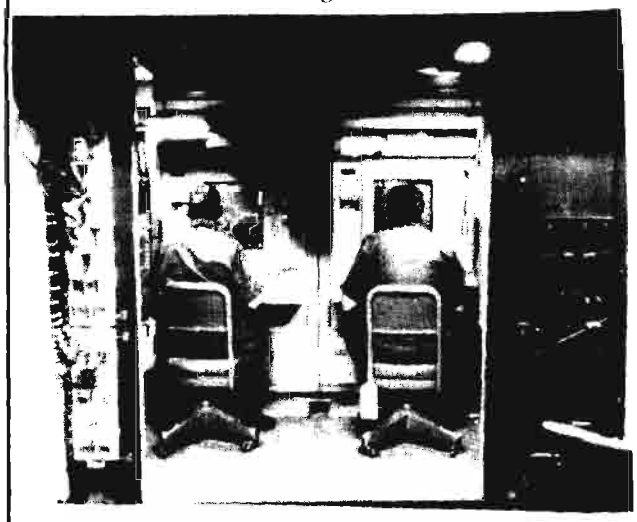


Fig. 5

CRT presented a map showing significant land masses, coastlines, major rivers, islands, and political boundaries, and was overlaid by a grid system (Fig. 6).

The operator positions would copy aircraft position reports and amplification data such as altitudes, numbers, and aircraft types. The TTY would electronically feed intercept track data to the computer, which would convert the position reports to Geographical Reference Grid (GEOREF), decode the amplification data, convert the callsign and frequency to a station location for azimuth-range position reports, recognize ELFAIR-relevant traffic, flag it, and place all traffic on magnetic tape. The second computer could then edit and decrypt the information, presenting it to the analyst operating the CRT display. The analyst would first see the data as a blinking trace and, upon command,

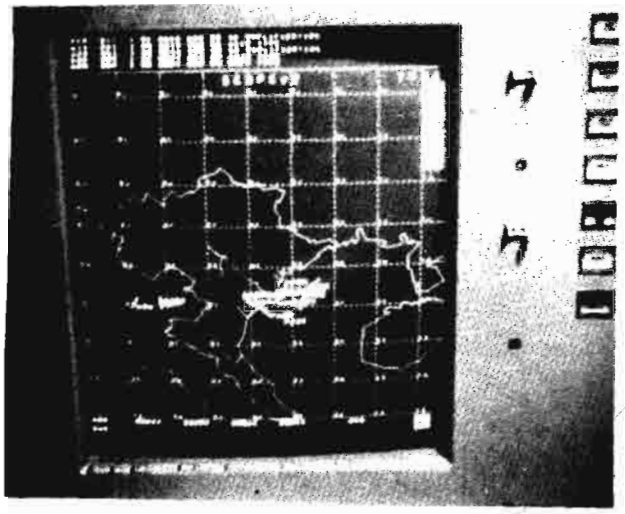


Fig. 6

could retrieve and display any amplification data. The computer was programmed to detect and reject irrelevant chatter and, if tracking data was in an unrecognizable form, it would be printed out on an edit console, where the edit analyst would correct the information and re-enter it.

The CRT analyst was required to recognize informative [redacted] tracking data and initiate forwarding to the consumers. Since all copy was displayed, the CRT analyst would decide which command level of the air defense net to forward. Information that was redundant or superfluous would be left in a suppressed mode or purged from the system. Upon command from the analyst, the computer would automatically forward designated data to the Seventh Air Force TACC, Seventh Air Force Command Post, Seventh Fleet Commander(CTF-77), and the Marine Tactical Data Center simultaneously with transmission to TACC,NS. CRTs at these locations would present [redacted] tracking data in the sanitized form of GEOREF plots with limited background amplification. The commander could then combine this information with other tracking data received via the SEEK DAWN[1] interface to make his decisions. The net result of IRONHORSE was to reduce the intercept-to-consumer time from 10 minutes to a matter of seconds.

The IRONHORSE system was able to complete its mission effectively. It gave battle commanders the near real time reflection of aircraft positions they required. It had the ability, by nature of its source, to reflect aircraft at low altitudes. In the case of dogfights and shootdowns, the position of downed U.S. aircraft could be relayed to Search and Recovery (SAR) missions[2]. Regardless of the cost, if the system was able to aid in the recovery of one pilot it was worth the investment.

---

[1]SEEK DAWN was the exchange of digital air tracking information between TACC,NS at Monkey Mountain and Marine Tactical Data System, Navy Tactical Data System, and the Air Tactical Data System units in Vietnam and the Tonkin Gulf area.

[2]I was at USA-32 from August 1969 to August 1970 during the bombing halt and had no direct reflection of the use of SAR. However, as an amusing anecdote, during one of the "probe" missions (sending a photographic drone in over Haiphong and Hanoi at treetop level), two MIG-17s were scrambled. The MIGs intercepted and the trailing MIG locked on and fired a heat-seeking missile. Unfortunately, the other MIG was between the missile and the drone. Only one MIG returned to base and the drone was later recovered in the Gulf.

ANSWERS TO QUESTIONS IN "ABDUL & HIS 40 TANKS"

(CRYPTOLOG, August-September 1975) EO 1.4.(c)

[redacted]

~~(SECRET -- HANDLE VIA COMINT CHANNELS ONLY)~~

DOCID: 4019723

P.L. 86-36

THE DANANG PROCESSING CENTER

[redacted] A852

The South Vietnamese Danang Center and lower-echelon SIGINT units in ARVN Military Region I (MR-I) were intended to provide intelligence to the MR-I J2 and to the ARVN combat divisions within that region. This intelligence took the form of daily intelligence summaries and spot reports issued by the Center and its subordinate units.

Danang Center and the other SIGINT units in MR-I had their successes and occasionally produced valuable tactical intelligence. Unfortunately, they did not produce enough; it was not produced fast enough; and the SIGINT users at Corps level did not have a proper appreciation of the validity and usefulness of SIGINT.

Following the signing of the Paris Peace Agreement, the tactical environment in Vietnam took on a "fixed-piece" posture where enemy units made few tactical movements. The result was a loss of many national intelligence sources such as document exploitation and prisoner interrogation. With the loss of these collateral sources, SI should have come to the forefront of available sources supplying the national J2. However, the production of this SIGINT, at least in MR-I, was not satisfactory. It is the purpose of this article to explain some of the reasons why I think the overall ARVN SIGINT effort was a failure and fell short of its mission and to touch briefly upon life in Danang.

* * *

An assignment in Vietnam following the withdrawal of U.S. military forces in February 1973 was unlike any other NSA overseas assignment. The Paris Peace Agreement limited the number of U.S. Department of Defense personnel allowed in-country. [redacted]

One U.S. representative was assigned to each of the three ARVN SIGINT field centers at Can Tho in the Delta, Pleiku in the central highlands, and Danang in the northern regions. [redacted] each field representative was provided with housing, a vehicle and gas, purchase privileges in their bar, restaurant, and commissary, and inclusion in most of their social activities. [redacted]

The ARVN SIGINT organization was known as the Directorate General for Technical Services (DGTS) and had its headquarters in Saigon. The Danang Processing Center was the northernmost field Hq of the DGTS and had a personnel strength of 329 men. Danang Center operated 50 Morse intercept positions on Danang Airbase and a [redacted] collection effort on top of nearby Monkey Mountain.

EO 1.4.(c)
P.L. 86-36

Each of the six ARVN combat divisions in MR-I had an organic SIGINT unit known as an ARVN Special Technical Detachment (ASTD). These ASTDs controlled 35 highly mobile low-level voice intercept (LLVI) teams which were capable of short-notice deployments to keep up with enemy movements. LLVI teams were also intended to accompany the combat units into action to provide real-time direct support.

Top-level officer administration in the MR-I SIGINT organization was generally excellent, middle-level management was weak, and low-level was poor to nonexistent. The top-level managers were well educated, trained, and motivated, but a lack of these qualities among the lower-level officers prevented full productivity of the Center from ever being attained.

LLVI team operation could have been far more productive if the lieutenants and senior NCOs had been more professional. Most of these teams were located in forward areas and I was unable to visit many of them. Those I did visit invariably needed basic improvement. Antennas were often oriented in wrong directions or were found to be grounded; radios and generators were rarely properly grounded; bunkers were not secured with perimeter wire and the men had not been counseled in document and equipment destruction in case of overwhelming enemy attack.

As another example, in December of 1974, Danang Center was tasked with collection of North Vietnamese air surveillance tracking data. The particular radar sites and sector filter centers we copied were located in the southern panhandle of North Vietnam and we hoped that North Vietnamese MIGs deploying to staging bases just above the DMZ or actually penetrating South Vietnamese air space would be reflected on these cases. It was suggested that the Center be able to tip off, via phone, such MIG movements to the MR-I Commander, the MR-I Air division Commander, and the South Vietnamese radar facility located atop Monkey Mountain.

EO 1.4.(c)
P.L. 86-36

But weeks after starting collection of these communications the analysts plotting the tracking data were found to be working 2 days behind, a delay hardly acceptable when the computed flying time between the DMZ and Danang Airbase was approximately 6 minutes.

The South Vietnamese were never able to make the airborne direction finding (ARDF) program function as the money-maker it was while under U.S. control. Several management problems crippled the effort. Even in the final days of South Vietnam's existence, when locating data on the many NVA Divisions ringing Saigon was critical to an organized defense, it was impossible to force the responsible officers to straighten out the ARDF program.

Six EC-47 ARDF aircraft and their crews were assigned to Danang but were rotated every 2 weeks from the Squadron Hqs in Saigon. The men were directly subordinate to Saigon. This meant that the MR-I Hqs could not control the flights even though they were the primary user of the DF fixes. Support for the aircraft was also in Saigon. If an aircraft needed parts or maintenance that could not be provided by the few men assigned to the EC-47 hangar, it would have to wait until the aircraft was ferried to Saigon.

For a good part of the year, the morning weather in MR-I is generally cloudy but it usually clears up by afternoon. Cloud cover has an adverse effect on the Doppler navigation system used in the EC-47's, so many morning flights were aborted. However, by afternoon, when the flying weather was perfect, the crews had disappeared for the day.

Gas stealing by the crews was also a major problem. Most of the officers had oversized briefcases lined with plastic bags which they filled with gas from the aircraft wing tanks and carried through the airbase gates to sell on the black market. Ground crewmen also took their share and it was not unusual for a completely topped-off plane to be drained overnight. While I was there, at least two of Danang's aircrew barracks were destroyed by fire caused from plastic bags of aviation gas.

The flight crews were also rough on wing tips. In December 1974 I noticed that there had been several recent mission cancellations due to "wing tip repairs". Not understanding this, I drove to the flight line and watched as an EC-47 returned from a mission and taxied into the parking revetments. The normal procedure at any airfield would be for a few ground crewmen to meet the aircraft and guide it into the parking area, making sure there was sufficient clearance between the wing tips and the revetment walls. While I watched, though, the only assistance the pilot got was the brief appearance of a ground crewman from the hangar who ran out in his BVDs, pointed a finger at the nearest empty revetment and then ran back into the hangar and climbed into his hammock. It was small wonder the pilots scraped off so many wing tips while making unassisted parks.

Payoffs, corruption, and nepotism were a way of life in the Vietnamese government and the ARVN SIGINT organization was no exception. I soon learned that it was far easier and quicker to "buy" a service or cooperation than to go through normal channels. Two six-packs of beer would get a half-day loan of a forklift, a few cigarettes would gain entrance to a restricted area, and a fifth of cognac would guarantee a staff officer's cooperation in obtaining real estate for a field site expansion. Some jobs simply could not be done without a bit of preliminary palm-greasing.

Corruption within the officer administration of Danang Center was accepted as long as it did not get out of hand and the officers continued to produce. One officer, a Center Commander, eventually devoted so much time and effort to lining his own pockets and was so incompetent in his job that he had to be replaced. It was impossible to stop the thievery completely. The best we could do was to keep it at a minimum and accept some losses as long as the job got done.

The extensive nepotism could be turned to advantage. It was always more productive to conduct business arrangements with an officer of a support organization who had a relative on our staff. Likewise, an almost equally strong allegiance as blood relationship existed between old college classmates and this was used to advantage whenever possible.

The Vietnamese had their own ways of doing things and these methods were not without humor. In late July 1974 I received a message [redacted] that [redacted] would soon pay us a visit. I informed the Danang Center Commander of this and suggested to him that he have the grass in the antenna field trimmed as it was quite high and posed a fire hazard. The General would be sure to spot it. The next morning I arrived at work to find that a fire of unknown origin had "quite mysteriously" swept the field and consumed the grass. Unfortunately, this fire also destroyed several lead-in cables which connected the Center's antennas with the multicouplers, effectively wiping out over half of our antenna system. In my mind, I suspected that Captain [redacted] the Center Commander, had ordered one of his lieutenants to have the grass removed and the lieutenant, without devoting a great deal of thought to what he was doing, touched off the grass with a match. I never did have the courage to pursue the cause of the fire but "accepted" Captain [redacted] dictate that "unknown" circumstances caused the fire. Weeks later, when new grass was starting to grow in the field, the Captain and I spent part of a day trying

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

to buy a calf to tether in the field and eat grass. We were not able to get an acceptable price on a calf, although sheep and goats were going cheap. Unfortunately, both sheep and goats consider RG-11 lead-in cable to be a gourmet's delight and so had to be ruled out.

The rainy season in Danang occurs during the winter months of November through March and is opposite the rainy season in Saigon which occurs during the summer months. Also Saigon's rains are characterized by being torrential and occurring a few times daily but lasting only minutes. Danang's rains generally lasted for days but rarely did it rain very hard.

In Danang, the continuous humidity caused mildew to grew on almost everything and even saturated paper so deeply that graphite would run. Many of the Center's roofs leaked and the communications center roof was of major concern because of the electronic equipment. As repair materials were unavailable, Captain [redacted] had an ingenious system of catch basins and troughs installed. The most unusual remedy to a leak was over an HW-10/HW-19 crypto device. [redacted] had the men punch a hole in the nearest wall several feet below the ceiling and run a rag from the leak in the ceiling to the hole in wall. Thus the water ran down the rag to the outside by capillary action instead of dripping on the equipment.

Going to and from school, the dependent children of Danang Center walked past my quonset hut which was just inside the perimeter cyclone fencing. Vietnamese children are adorable and I got in a habit of giving them, through the fence, small hard candies which I bought at the U.S. commissary. This was quite a treat for them and they would wait for hours on the road for me to come out of my hut. Eventually this got a bit out of hand and on occasion as many as 50 or so children would gather. I didn't have enough candy for groups this large and so I wouldn't go outside when I heard them calling from the road for me. One day one of them got the idea to throw a rock onto my roof to get my attention -- which it did -- and bring me outside-- which it did. At this time, Danang Airbase was regularly taking VC 122-mm rocket attacks and these rocks, crashing onto the metal quonset hut roof just feet over my head, were enough to send me diving under my desk.

The DGTS had difficulty in organizing and maintaining communications between their own units. The lowest echelon of the DGTS was the LLVI team. It comprised two to five men, one or two radios, one or two rudimentary 292, sloping-V, or doublet antennas, and sometimes a typewriter. By directed or random search, these teams would find and copy VC low-level voice communications. Messages on these links were usually encrypted in easily read, hand encryption systems. The underlying text had immediate tactical value since much of it dealt with VC troop movements and preparations for forthcoming attacks. Decryption of these messages was performed at the next echelon by the ASTD. These ASTDs were organic to ARVN combat divisions and were responsible for the immediate processing and reporting of decrypted messages to the Division G2. All too often, however, the ASTDs received the encrypted messages days after the actual intercept. As a result, much of the decrypted information obtained was after the fact. Most of the ASTDs in MR-I attempted to visit their teams a few times a week and courier the raw intercept back. Gasoline rationing often curtailed these visits. In at least one case, an ASTD resorted to civilian taxi motorbikes to get the intercept.

In November 1974, in an effort to speed up the forwarding process, our Saigon COMSEC office allocated secure voice KY-8 systems to three of the MR-I ASTDs and their subordinate LLVI teams. With this equipment, it was hoped that the teams would be able to radio their raw intercept directly to the ASTD just after copy. But several problems kept this project from ever being fully successful. The KY-8s and their associated VRC-46 radios frequently could not be supplied with stable electric power at the LLVI team. Crypto management problems occurred. The men operating the gear and the officers responsible for them often did not have sufficient training in crypto set-up and use, and minor maintenance problems with the VRC-46 radios could not be corrected locally. As a result of these problems, little time was saved in getting the intercept to the processing and reporting echelon.

The ASTDs supported their parent divisions with intelligence product but forwarded their technical material and raw intercept to Danang Center.

The 1st ASTD at Phu Bai had two 60-wpm teletype circuits to Danang Center which employed HW-10/HW-19 crypto security. Two circuits were necessary as this ASTD processed intercept gathered by its own LLVI teams and those teams subordinate to the Marine, Ranger, and Airborne ASTDs. The traffic volume on these circuits was high, so much so that prepared message tapes often had to wait days for transmission. In addition, the Marine, Ranger, and Airborne ASTDs generally batch-forwarded their material to Phu Bai once weekly and this caused poking backlogs in the Phu Bai communications center. On several extreme occasions when hundreds of prepared message tapes were backlogged at Phu Bai, I or a Danang Center courier was allowed a seat on an Air America helicopter to get the tapes from Phu Bai to Danang. This procedure was not encouraged since we were trying to get the Vietnamese to depend on their own support organizations rather than U.S.

The 3rd ASTD at Hoa Khanh also had a single circuit to Danang Center. The operation of this

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

circuit was continually plagued by technical problems in the cable. Flooding and sporadic rocket attacks were blamed for cable outages, and it was rare when the Vietnamese Air Force, responsible for that portion of the cable on Danang Airbase, and the Vietnamese Army, responsible for the cable portions from the airbase to the Hoa Khanh Hqs, could agree on where the break occurred. As a result, the majority of the intercept provided by this ASTD was usually couriered to Danang Center via jeep, and even though the ASTD was only a few miles away over perfectly secure roads, it took constant prodding to get them to make the trip more often than once weekly.

The supply and maintenance methods used by Danang Center can be summed up as almost totally inadequate. In retrospect, I now think that a working logistics system is the most critical requirement of any field operation. Danang Center had many personnel, management, and technical problems, but even if these had been solved, mission effectiveness could hardly have improved without sufficient working materials and equipment maintenance.

Several examples of our poor support come to mind. For supplies such as pencils, erasers, and tape the Center received no allocation but was given approximately $40 a year to buy the supplies on the open market. It was barely a fraction of what was needed, considering our consumption of these materials.

We received our typewriter ribbons from Saigon Logistics. To supply the 75 or so typewriters we had -- which were used almost continuously -- we were given 12 ribbons a month. This meant that each typewriter received a new ribbon approximately every 6 months.

The local MR-I Maintenance Company which was responsible for maintaining Danang Center's "common equipment" such as R-390 radio receivers, recorders, typewriters, etc. was not regularly given updated copies of our Table of Organization and Equipment and so was never able to stock enough of the parts needed for our equipment.

Many equipments and supplies basic to operation of an intercept site were not stocked at Danang Center, the MR-I Logistics Command, or at Saigon. Such items were antenna wire and insulators, TMC boxes, lead-in cable, RF connectors, and ground strap. So desperate were we for some materials that on one occasion when our Saigon resident engineer, [redacted] and I were fabricating new antennas for the ASTD at Phu Bai, Charlie entered a minefield trying to "liberate" a pair of unused TMC boxes and failed only because VC 85-mm field gun rounds started dropping around him.

Soon after the U.S. military withdrew from Vietnam and the DGTS had assumed complete responsibility for the collection, analysis, and reporting of SIGINT, it became apparent their state-of-the-art would not advance as rapidly as we wanted. The DGTS simply would not be pushed faster than they wanted to go. I feel their management and logistical problems and their lack of a true desire to learn the production and use of SIGINT contributed to the overall failure of the independent ARVN SIGINT effort.

Answers to CRY-PTO-LOGrolling puzzles

(See CRYPTOLOG, August-September 1975)

*PTO*LEMAIC
U*PTO*WNERS
TI*PTO*EING
CRY*PTO*LOG
NOTU*PTO*IT
THETI*PTO*P
GIVELI*PTO*

CRYPTOLOG
ACRYLATES
ENCRYPTED
DESCRYING
XENOCRYST
NORDICRYE
INFULLCRY

*LOG*OMACHY
S*LOG*ANIZE
PH*LOG*OSIS
UNC*LOG*GED
PEDO*LOG*IC
BUMPO*LOG*Y
CRYPTO*LOG*

(UNCLASSIFIED)

[redacted] PAPER ON CHARACTER STREAM SCANNING BY MACHINE

[redacted] R51, has recommended that broader publicity be given to a recently published P16 paper. He writes, "Some of the readers of CRYPTOLOG may have missed seeing (let alone reading) a recent document on the perennial task of program writing (debugging, maintaining, updating, etc.) for operational tasks involving compter processing of data in which alphanumerics play a significant role.

"The paper, dated March 1975, is by Mary [redacted] P16, is entitled *A Systematic Approach to Character Stream Scanning by Machine*, is classified SECRET, and bears the official document number S-211,893. Copies may be obtained from [redacted] Room 3W076, 4998s."

~~(CONFIDENTIAL)~~

TACTICAL LANGUAGE EXPLOITATION: A Lesson Learned?

[redacted] B11

Vietnamese is an "exotic," strange-sounding language, particularly to a Westerner's ears. None of the vowels or consonants sound like anything in English or any of the Romance languages. And, of course, it has those tones! As a result, training in Vietnamese involves a complete readjustment of the student's learning process, starting at "base zero." This is, at best, a lengthy procedure.

As the Vietnam War heated up and more and more large-sized Vietnamese Communist (VC) units were committed to combat, the air became saturated with low-powered voice transmissions, often between individuals at the platoon or squad echelons of the combat force. Collecting this mass of transmissions was a monumental task which could never be totally accommodated. Beyond that, since most of the voice data was extremely perishable, rapid exploitation of the collected signals was critical. Often, lives hung in the balance, depending upon whether the attack orders could be understood instantly or required extensive processing before being reported. To attempt to grapple with this language need, the Service Cryptologic Agencies sent thousands of young men through various language schools to teach them Vietnamese. And they learned the language -- they learned how to read newspapers, order meals in a restaurant, count to 100, work with a dictionary on complex written subjects, etc. There's nothing wrong with that kind of training -- I'm not maligning it. Within the short period of a year, training speakers of English to function at all in Vietnamese is a fine accomplishment, and these people did function. But within the space of their training they could not achieve -- and could not be expected to achieve -- the auditory proficiency needed for on-line exploitation of low-level tactical conversations in a combat situation. This special skill -- being able to think in a language -- takes years to develop. Many people never achieve it at all, no matter how long or how hard they try.

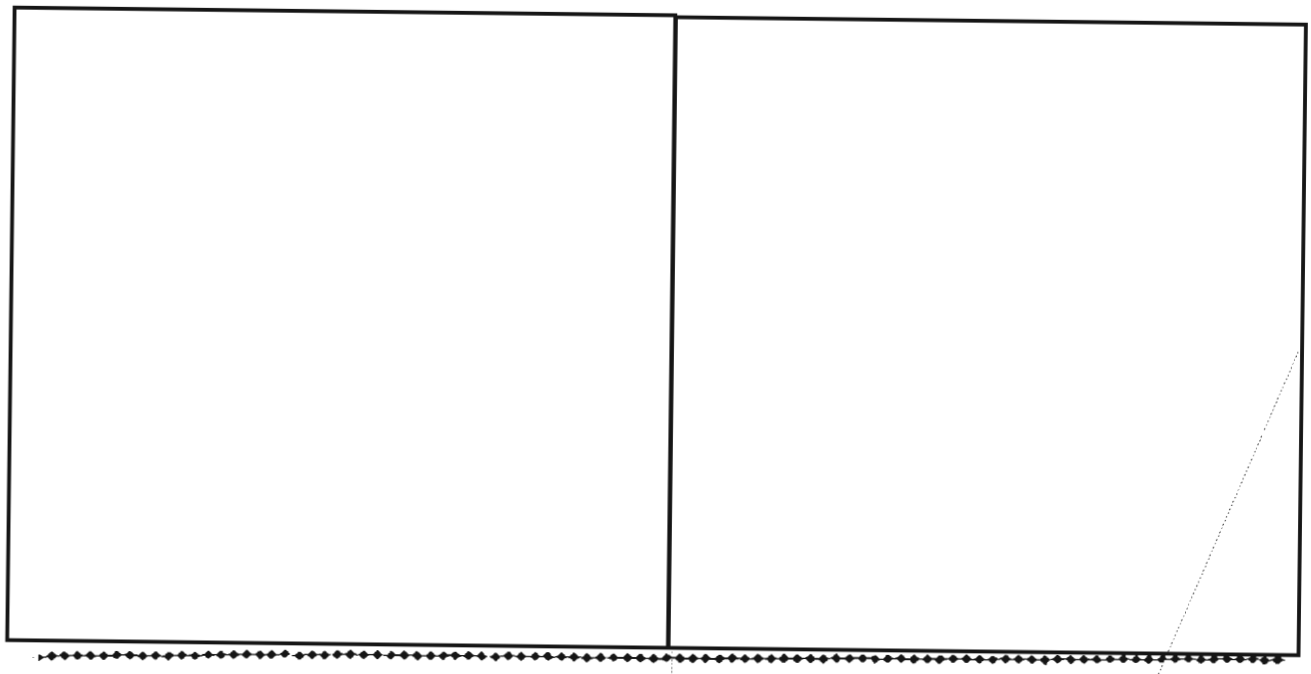
Fortunately for us, the VC had a methodical approach to warfare, and, among other things, were quite conscious of communications security. Thus, except for actual in-combat transmissions, they were quite precise about what could be passed, and how various types of information could be handled. For example, although many types of information were routinely on the air, more sensitive things, such as after-action reports which included casualties, were almost never observed in any traffic that we could exploit, presumably because, in addition to denying us that information, the VC did not want their own units to learn inadvertently how their comrades had fared in battle. [redacted]

But this still did not accommodate the plaintext voice problem, and it was apparent to all parties that this problem simply could not be successfully accommodated using U.S. linguistic personnel. (I should note that I am speaking in broad generalities. Certain facets of the plain language problem -- notably tactical air -- were within the capabilities of the U.S. personnel, primarily because of the stereotyped nature and limited vocabulary of such transmissions. But let me continue with the generalities.) Native linguists were the only real solution, and were acquired in small numbers, with many restrictions on both their physical and cryptologic security. This program, originally known as the DANCER program, and later as the BEES, helped fill the breach, especially on those signals that could wait for transcription until they reached an area occupied by the DANCERS/BEES. Such lengthy conversations/signals as those passed [redacted] were ideal for this program.

Suffice it to say that U.S. linguists proved able to copy simple transmissions, [redacted] and provided combat support on a near real-time basis from these sources. Native linguists were able to perform the more complex transcription tasks, thus contributing immeasurably to the overall understanding and measuring of the enemy's intent and capabilities. We never achieved an on-line capability for plaintext tactical voice.

Tactical Voice Capability in Future Wars

We must assume that in any future wars, against other nations, there will be the same real need for on-line exploitation of tactical voice transmissions. One possible means of addressing this need is to take native linguists and use them on position. If they can relate in English what they have heard, so much the better. But at minimum they can write down the essence of the intercept in their native script and pass this immediately to a U.S. translator for necessary processing and delivery to the tactical commander.



UPCOMING LECTURES sponsored by the CRYPTO-LINGUISTIC ASSOCIATION

MONDAY, 17 NOVEMBER, 1000
Brigadier Tiltman
will speak on
The Voynich Manuscript

FRIDAY, 19 DECEMBER, 0900
P. W. Filby
"THE GWEEKS HAD A GWOUP FOR IT"
(Reminiscences of Bletchley Park in the 1940s)

Both lectures will be given in the William F. Friedman Memorial Auditorium.

By the by, speaking of Brigadier Tiltman and Bletchley Park, next month's issue of CRYPTOLOG will include the Brigadier's critical review of F. W. Winterbotham's The Ultra Secret.

EO 1.4.(c)
DIA 86-36
~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4019723

AUTOMATION OF A TA PROCESS

Tim Murphy, B341

What few people realize is that the workload associated with the Southeast Asian (SEA) problems did not decrease as U.S. forces withdrew from Vietnam and B3 (previously B6) underwent successive personnel reductions. In fact, the amount of SEA communications intercepted and processed at NSA was still peaking in 1975 when the South Vietnamese government fell.

Traffic analysts have borne a proportionate share of the decrements incurred by B3, yet there has been virtually no drop in target communications. Analysts have been assigned larger case loads and have assumed responsibility for collection management; yet, in my view, the quality of analysis has improved and the analysts, in general, are not overworked. There is little doubt that technical support to field stations has improved significantly.

The automation of a large segment of the SEA traffic-analytic processes has been the key not only to high-quality analysis but also to our ability to do the job better over the years with fewer people. Fortunately, during the early stages of U.S. involvement in Vietnam managers with the Traffic Analytic Support Division for the Vietnamese problem took an enlightened view toward mechanization. With help from some of the Agency's leading traffic analysts and a cadre of highly-qualified data-systems personnel, the first steps toward an automated traffic-analytic process were taken.

At the same time we began a major effort to mechanize our analytic findings and create a single processing system. In addition to transmitting our analytic findings to field sites, we also used this data to create identification dictionaries that became the heart of our match-ident process.

Of equal importance to these contributions was the fact that the methods that the experts used and the approaches that they took to the TA task rubbed off on many of the junior analysts working the SEA problem. This group of analysts, with outstanding support first from C5 and later from B42, continued this trend toward automation, always striving to relieve analysts of most of the repetitive TA tasks and to permit more time for actual analysis. Among their major contributions were:

- the creation of a single analytic data base -- the Southeast Asian Case File (SEACF):

In addition, the availability of on-line access to our data base in recent years through the COPE terminal has led to many analyst-initiated special programs that have greatly expanded the analysts' capacity for research. I should also point out that field stations tasked against SEA targets have also taken many initiatives toward automation.

SEA Machine Data Bases, Processes, and Resources

SEACF

Perhaps the most significant single step toward reducing the workload of SEA traffic analysts was the creation of the Southeast Asian Case File. The SEACF not only resulted in highly efficient data-base management, but also permitted many follow-on processes that greatly reduced the workload of SEA traffic analysts.

Many of the processes that were introduced during the early stages of the Vietnam War to mechanize the TA process required the establishment of data bases to support them. As

TAO 14. (c) 86-36

those processes expanded, the number of data bases expanded to the point where analytic time saved was being spent on data-base maintenance. A review of those data bases revealed that there were a large number of common fields of information but comparatively few unique fields. In effect, we were multiplying our file-maintenance workload and making ourselves vulnerable to contradictions between identical data items in different data bases. The major data bases that had to be maintained prior to the implementation of SEACF were:

The SEACF consolidated all these data elements into a single data base, thus eliminating the requirement to maintain those multiple data bases. Since its establishment the SEACF has been expanded to include data elements that support both cryptanalytic and collection-management functions.

As now constituted, the SEACF consists of eight basic data records which analysts use to provide permanent maintenance of the communication characteristcs and crypt characteristics of a given target, identification and location data on that target, and also collection-management data.

It was inefficient and time-consuming for analysts to collate all these varied inputs, yet very necessary from an analytic standpoint. Hence they were eventually collated by machine as part of our daily process, and our activity data base is now a composite of all primary-source technical inputs.

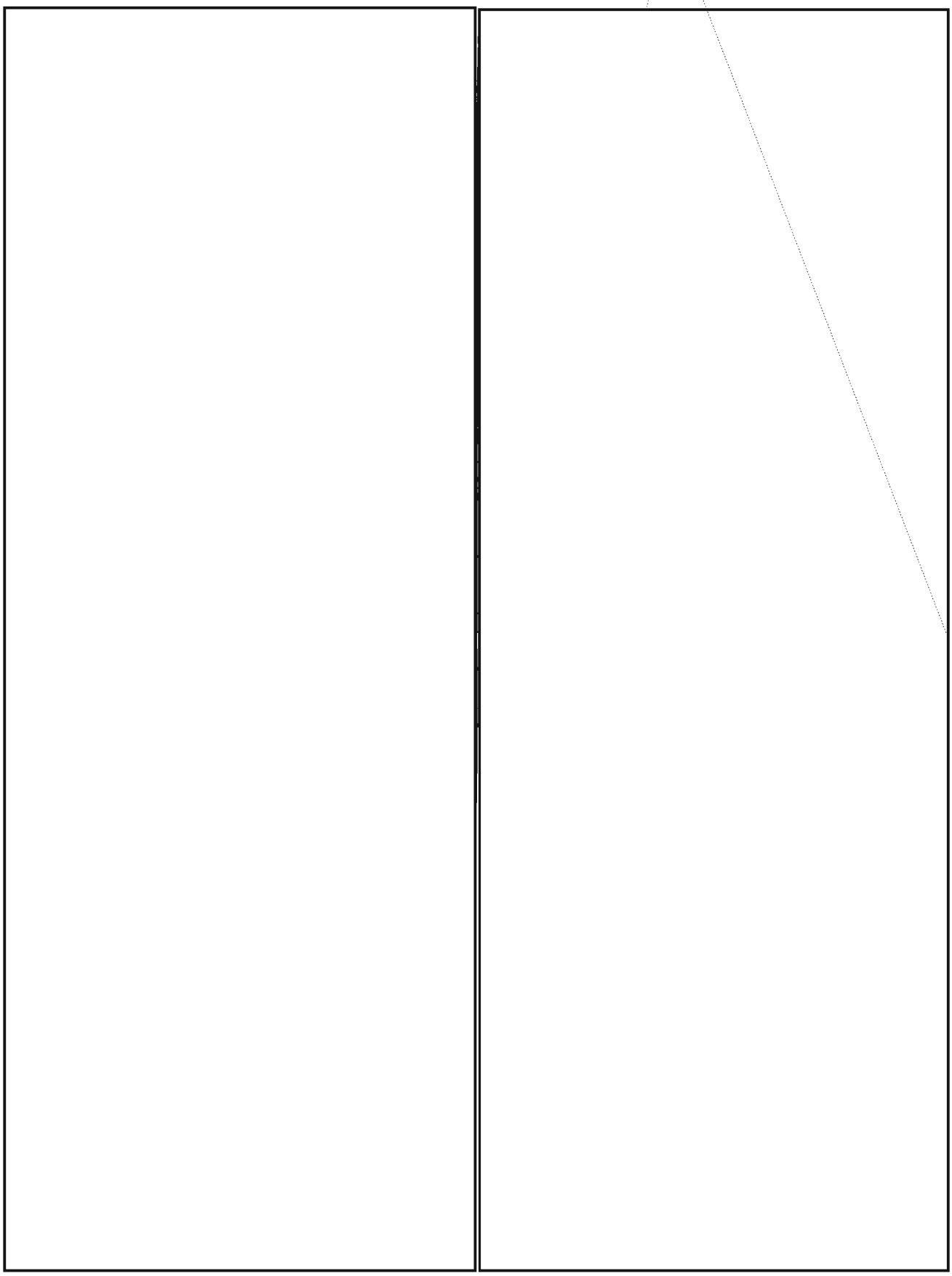
This program reduced by countless hours the task of the SEA development analyst. To a large degree the analyst has been able to rely on the machine to isolate new continuities and then concentrate his or her efforts on identifying that continuity to region or function. The number of analysts tasked against the development problem was reduced from 45 to 10 between 1972 and the spring of 1975 with no adverse effect on the mission. Much of the credit goes to the SEADEV process that has just been described.

IATS

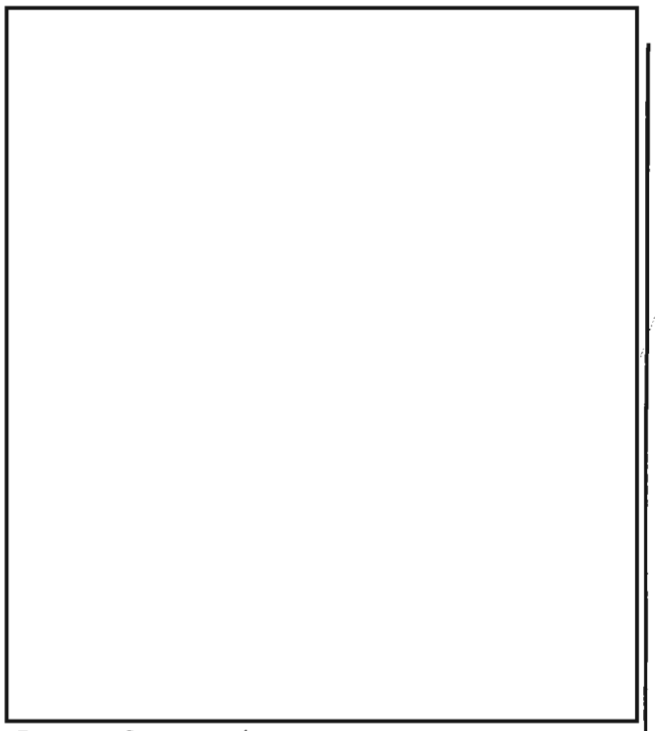
Another major step in automating both the traffic-analytic and the traffic-forwarding processes was the implementation of IATS. The user routine developed for SEA communications copied on IATS or AG-22 intercept positions --

~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36



~~SECRET SPOKE~~



Impact of Automation

In summary it can be said that the impact of automation on the SEA problem has significantly reduced the number of analysts required to do the job. The caliber of analysts required has increased, however, since his or her primary remaining function is pure analysis or, to use another term, "thinking." Many of the crutches that have kept analysts busy over the years (e.g. logging, sorting traffic) are gone.

To function effectively SEA analysts must have an understanding of their data bases and of how machines can be used to manipulate the data that they contain. Imagination is currently a key asset since much of what can be imagined in terms of analytic approaches is now feasible. There is an increased demand for the traffic analyst/programmer. Knowledge of the SPECOL retrieval language is becoming a highly desirable attribute of the SEA traffic analyst. In short, the impact of TA mechanization has made B3 like the Marine Corps. B3 now needs "a few good *analysts*."

BACK ISSUES AVAILABLE

Copies of most of the back issues of CRYPTOLOG can be obtained from the Editor, Room 3C099-1, x5642s. If you have recently become aware of CRYPTOLOG (newly assigned to NSA? recently returned from overseas PCS? just never noticed CRYPTOLOG before?), you might like to read some of the back issues. They contain a lot of good articles!

(UNCLASSIFIED)

DORIS MILLER HONORED

Doris A. Miller, editor of CRYPTOLOG from its inception until her retirement in June 1975, returned to the Agency on 4 August to receive the NSA Cryptologic Literature Award. Lt. Gen. Lew Allen Jr., Director, NSA/Chief, CSS, presented the award at a ceremony in his office in the presence of a small group of Doris's friends.

The award is in recognition of the many valuable contributions that Doris made to the cryptologic literature during her distinguished career at NSA.

(UNCLASSIFIED)

NEW PROGRAMMING INSTRUCTIONS!

The following item is reprinted from the April/May 1975 issue of C-LINERS (C Group Machine Processing Information Bulletin).

The STARTING GATE Advanced Programming Language Study Group has been holding regular planning sessions aimed at the development of advanced programming techniques for the forthcoming new System/1776 computer network. Some of the proposed new instructions have been noted in the minutes of the sessions (written on soggy beer mats) and are presented for comments. The Study Group would welcome any additional instructions, which should be sent to the Editor, C-LINERS.

BH	Branch and Hang
IIB	Ignore Inquiry and Branch
TDB	Transfer and Drop Bits
DO	Divide and Overflow
SRZ	Subtract and Reset to Zero
PI	Punch Invalid
SSJ	Select Stacker and Jam
FSRA	Forms Skip and Run Away
RASC	Read And Shred Card
SRSD	Seek Record and Scar Disk
BST	Backspace and Stretch Tape
RIRG	Read Inter-Record Gap
UER	Update and Erase Record
EMF	Emulate 407
SPSW	Scramble Program Status Word
EIOC	Execute Invalid Op Code
EROS	Erase Read-Only Storage
PBC	Print and Break Chain
CM	Circulate Memory
MLR	Move and Lose Record
CRN	Convert to Roman Numerals
DMPK	Destroy Memory Protect Key
DC	Divide and Conquer
EPI	Execute Programmer Immediately
LCC	Load and Clear Core
HCF	Halt and Catch Fire

(UNCLASSIFIED)

DOCID: 4019723
P.L. 86-36

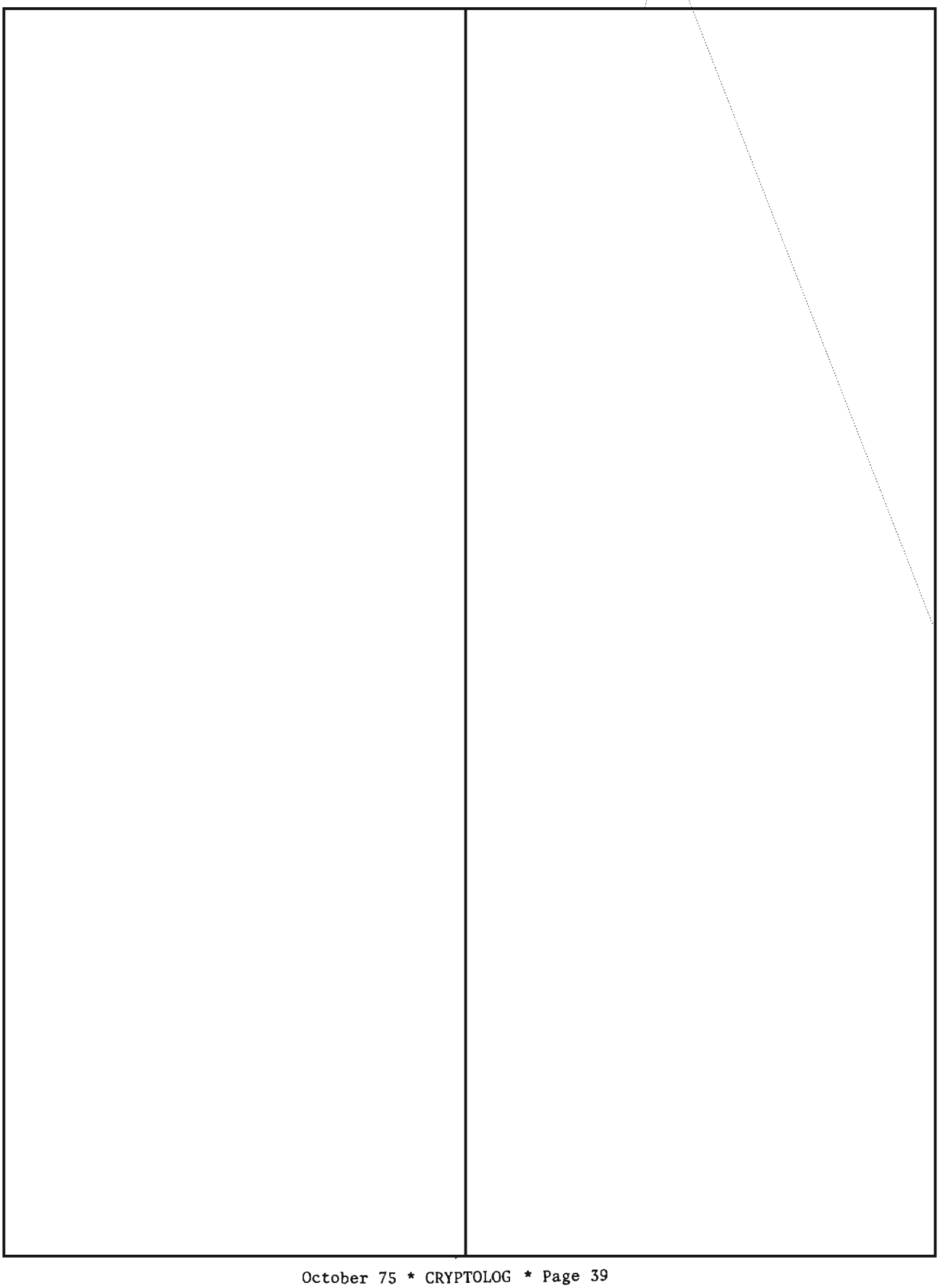
EO 1.4.(c)
P.L. 86-36

COMPUTERS, COMMS, and LOW-GRADE CIPHERS

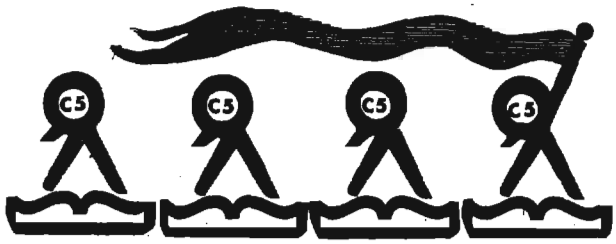
B34

~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36



P.L. 86-36



LINGUISTS - YOU HAVE AN EXPERT TO CALL!

[redacted]

The expert, in this case, is not an expert in *widgets* or in beekeeping, but an expert in finding information. There are quite a few of them in the Agency and they're located in Central Information, C5.

The publication of [redacted] article on the need for an "experts yellow pages" in the August-September issue of CRYPTOLOG was a disappointment to those of us in Central Information who spend a considerable amount of time providing the type of service [redacted] finds so sadly lacking. A survey of recent requests for information yields numerous examples of terminology assistance given to linguists and nonlinguists. Are some Agency personnel unaware of our existence and our services? It seems unlikely, as we had a publicity campaign called "INFO '75" just this spring and the April 1975 issue of CRYPTOLOG included a directory of our various components. However, just in case. . .

Central Information, C5, maintains an extensive collection of specialized dictionaries, reference books, journals, and documents on a wide variety of topics. We have people trained in the research techniques necessary to make effective use of these sources. If the desired information is not available here at NSA, we have well-established contacts with a wide variety of organizations that can provide assistance.

C5 *does* deal in the specifics of all the many subjects that [redacted] cites. On Monday we could have told her, as we told another NSA analyst, that the SALT GROUP is a group of European allies of the United States who meet informally to discuss how provisions of the SALT Agreements will affect them as Europeans. We could have told her on Tuesday that *Merlucius capensis* is the common hake, on Wednesday that gold-secured loans come under the Zeist Agreement, on Thursday that filament yarns will be reviewed during the second year of the Japan-U.S. textile agreement, and on Friday that the term used in the Law of the Sea negotiations is "resources research." *Anytime* we can tell her, or any other NSA analyst, the same thing that we told a Persian linguist -- that when you have a choice of the words *compression, concentration, condensation,* or *solidification* when referring to uranium processing, the correct term is *concentration* (it means the extraction of uranium from ore); or what we told a Spanish linguist -- that the word *blanca,* when referring to cellulose, is translated as *bleached,* rather than *white*; or what we told a foreign-trade analyst -- that the MZ 250 motorcycle is manufactured by the VEB Motorradwerk Zschopau, East Germany and the 250 refers to the engine displacement (in cubic centimeters).

So, next time, instead of 15 phone calls, make just one -- to the Central Reference Service, x3258s, or consult the Central Information Directory. (If you haven't saved your back issues of CRYPTOLOG, copies of the Directory are available at the Circulation Desk, Main Library, Room 2C051.)

~~(SECRET HVCCO)~~

CMI
CRYPTO-MATHEMATICS INSTITUTE

NOVEMBER LECTURE:

6 NOVEMBER, 0930, Wm. F. Friedman Auditorium

DR. WALTER JACOBS, "Proving Theorems and Answering Questions by Computer"

DECEMBER LECTURE:

4 DECEMBER, 0930, Wm. F. Friedman Auditorium

[redacted] G49 will speak on "a result from SCAMP 1975"

P.L. 86-36

DOCID: 4019723

ONE CHANCE IN THREE - BUT IT WORKED!

WILLIAM GERHARD

Reprinted from DRAGON SEEDS, Vol. II, No. 2, June 1973

P.L. 86-36

ARDF needs no trumpeters in B Group, in ASA, or in AFSS. But important as the ARDF program was to become, experts in 1961 and early 1962 doubted that the first experiment involving direction finding and an L-20 aircraft would prove successful. As it turned out, there was one chance in three that the experiment which led to the ARDF program in Vietnam would, in fact, work at all. The following excerpts from an interview of [redacted] D/Ch of Staff for R&D, Hq, USASA, by Mr. [redacted] of ASA shed some light on the first ARDF birds to fly for the U.S. in Vietnam; on the early improvising by ASA innovators; and, despite odds against them, on their success.

WHY ARDF WAS REQUIRED IN THE FIRST PLACE

Q. Prior to ASA's becoming involved in ARDF development, was there any ongoing development of the capability within the Army?

A. The answer is really no. There had been, of course, a lot of development of ADF (airborne direction finding) systems for navigation purposes, which don't operate in the HF range and also the FM homers and other VHF navigation systems.

Q. . . .The question I always had. . . Why was it so difficult for us to do that?

A. . . . There is actually a technical explanation for why this difficulty occurs. . . the Vietnamese and the VC were using low power radios. Now, how do I get in HF a low powered radio. . . say, a one-watt power. . . to transmit a hundred miles? Well, the way to do that is to use a horizontal antenna, radiate the energy up to the ionosphere; then the ionosphere causes it to reflect down on the point you want. That means almost no energy is going out directly, so you sit over here on the ground with your direction finder even a half mile away, and there is no ground wave energy to hear. Now, an interceptor can listen because the sky wave is coming down from the ionosphere. I can sit there and copy what he is saying, but when I try to take a bearing, I am trying to take a bearing almost straight up, and there is just no way you are going to do that. [redacted]

E.O. 1.4.(c) P.L. 86-36

It was October/November of 1961 when the urgent requirement came out of Vietnam because they [3rd RRU members] had gone in-country and were trying to use AN/PRD-1s, and they couldn't. The AN/PRD-1 is a ground loop type DF set and needs a good ground wave signal to work against. A cable came back asking us what we suggested or what we could do.

THE EXPERIMENT

Q. Was this the 3rd RRU?

A. Our 3rd RRU and specifically. . [redacted] I was the project officer for direction finding systems in these days. [redacted] and I -- I had the action here through command channels and he had the action there -- had this exchange of messages; there were probably 10 or

P.L. 86-36

12 messages in that sequence. We worried about how to improve the AN/TRD-4s, which is the larger DF set and what we were going to do with his AN/PRD-1s. Then we got on to what we could do to solve it. That was where the idea of trying the aircraft emerged. We thought an aircraft would be useful, and he agreed that probably the aircraft would be great. In November, about Thanksgiving, I went over to Vietnam along with an engineer named [redacted] from ECOM [U.S. Army Electronics Command]. . . So we went over and spent a month in Vietnam and wandered around with [redacted] and the rest of the people involved. We went around on PRD-1 operations ourselves, took receivers and listened, making measurements of what the propagation conditions were.

Q. When and under what circumstances did ASA first become involved with research [and] development of ARDF? Was it a result of the 3rd RRU's recommendation? MACV's? Department of the Army's?

A. You can summarize it by saying that the way we got involved was reacting to the problem -- that we couldn't use AN/PRD-1s to do the job and the proposition was "could we use airplanes?" And the answer was, "Yes, we think we can."

Q. You got together with ECOM on this and went out with [redacted]

A. Exactly.

Q. When did you bring Department of the Army into this?

A. We didn't really. . . this whole thing was done on a shoestring. There were no external contracts made during this time frame; all was done in-house at ECOM. There were very few approvals obtained because we weren't talking dollar levels that required any approvals. Secondly, there wasn't a great deal of attention that was attracted in this time frame in the eyes of the Department of the Army. The 3rd RRU was calling for a solution, but it was to ASA. So it was later on that major involvement on the part of DA took place. . .

Q. Were the pilots organic to the unit [3rd RRU]?

A. Yes. I don't know how they came to be, but [redacted] [CO, 3rd RRU, Saigon] had acquired two pilots, one a CPT [redacted] who later came and worked here, and CPT [redacted] They were both Transportation Corps officers and didn't know anything about ASA until they came in. I believe a lot of credit belongs to them for having operated the thing.

Q. Did they come explicitly for this project?

A. Yes, that was something the 3rd RRU had arranged. We went out the first time feeling we could produce the gadget, and [redacted] handled the arrangements for getting aircraft which he borrowed from a Signal Unit, I believe, and the two pilots. Later we came back with the equipment and put it on.

Q. The first planes flew in March of 1962?

A. Right.

Q. How much testing were you doing there?

A. We were running a pretty extensive program. In the first place, it was a fairly simple system, although it performed an elegant solution. We had done work earlier with VHF ground direction finder, a thing called AN/TRD-16, which ECOM developed, which is composed of a pair of antennas differentially connected. That was a very effective ground direction finder in the VHF. That was the technology which we applied to the HF but increased the spacing between antennas. In terms of hardware you weren't talking a great deal -- a receiver, some cables, the antennas on the aircraft, and a little bit of circuitry to connect them. That was the size of it in the first version. It was a kind of thing which did not require weeks and weeks of fabrication. It did require an awful lot of testing. A whole series of antennas were tried to get out of the coupling problem with the airframe -- that was going on at Fort Monmouth -- the actual testing. When we felt we had something, we were able just to use the shops at Monmouth to fabricate antennas, cables, and other things and rush over and install them ourselves. . .

Q. Was there any training involved by the pilots and operators?

A. There was a lot of training by the pilot. This was very demanding of the pilot because he had no navigation sytem which would tell him where the airplane was at the time he was taking the bearing. He had to learn to fly over a point on the ground that he could then identify on his map as he took a bearing. The operator who was flying with him with a map had the duty of operating the receiver. The operator's task was not too different from the one he had operating the PRD-1 or an intercept position. He had to find the signal frequency and copy it, making sure he was on the right one. So that was pretty much what he was used to on the ground except he now was in a plane and had all the risks of getting airsick, etc. But really the pilot was the one who had to do this by pointing the aircraft at the target and slueing the tail back and forth, reading on his gyrocompass while he was still over ground he could recognize. A skilled pilot can do that very well, but this is something the average Army aviator isn't trained to do.

When we installed the thing, we worked a couple of days with the pilots there, refining it. We flew a lot of hours ourselves. They caught on very quickly. To prove what we had done, we had a hidden transmitter hunt. The 3rd RRU hid some transmitters around Saigon and they went out and found them.

If the pilot was careful in finding a bearing, even this first system could be incredibly accurate. For instance, during this hidden trans-

P.L. 86-36

mitter test the system showed which side of a road at a junction the transmitters were. We were talking even then about accuracies of hundreds of meters.

Q. Why were the L-20 aircraft selected for ARDF? Where in the United States, and when, did the initial ARDF testing take place?

A. . . .We found out that this aircraft was fairly available over there. It was adequate for our purposes because you needed something with good visibility; it could carry two or three people and some equipment. . . The L-20 just happened to be a very nice airplane for the purpose. The big thing was, it was available over here and could be maintained because the MACV Flight Detachment was who their people worked with in the beginning -- the old MAAG [Military Assistance Advisory Group] Flight Detachment, actually. The Detachment had L-20s.

Q. Was it the Signal Corps from whom we had borrowed the early planes?

A. Yes, it was the Signal Corps we got the aircraft from.

We had the one aircraft at Monmouth from the Flight Detachment that we had put the antennas on and it eventually worked out very well. That became the basis of the system we took over. We went over with equipment to do three airplanes. As I say, this went as luggage. I went; [redacted] the ECOM project engineer, went; a technician from ECOM by the name of [redacted] went; and an airplane technician by the name of [redacted] job was to mount the antennas on the aircraft. Walter Day was the electronic technician who was to help [redacted] and me get the system together. [redacted] and I did most of the flying.

So we had this airplane which worked well at Monmouth. We went to Vietnam, and they had arranged three airplanes to work with. The first plane we put it on, it worked very well. This is the one we did the hidden transmitter hunt from. As soon as that day was over, they took it away from us. We wanted to test a little more, but they figured it worked well enough so that it went into operation. We did fly some operational missions with them for a while to make sure things were working. We worked on the other two L-20's, but neither one of those aircraft worked. We installed the systems and sweated blood for several weeks and finally just had to plain give up. We couldn't make the systems work on these two planes. The reason for it had to do with the way the aircraft themselves are constructed. We apparently had some type of unsymmetrical airframe current distribution. As long as that is symmetrical and you can maintain a decoupling from it, your system will work. But some of the L-20s had been through extensive rehab. The inboard ends of the wings had been painted more coats on the one than the other, and things like this. When they had been put back together you had a terribly unsymmetrical RF current distribution, and we had no way to adjust for that at the time.

At that time, we found ourselves literally faced with the problem of selecting airplanes. We wound up then leaving those two which worked quite poorly and one which worked very well.. Aircraft tail #5682 was the good one and #33731 and 37963 were the poor ones. We came home and chose airplanes. ECOM sent people -- Walt Day, I believe -- from airfield to airfield finding planes which had not been through this major rehab, eqiupped two, tested them here, loaded them on board an aircraft, and flew them out to Vietnam to give the 3rd RRU the three it was after. The planes they had which didn't work well went back to where they came from. The 3rd RRU wound up then with three working L-20s after that ordeal. Actually, the ECOM lab A/C #55151 and #82012 were the ones that were sent out.

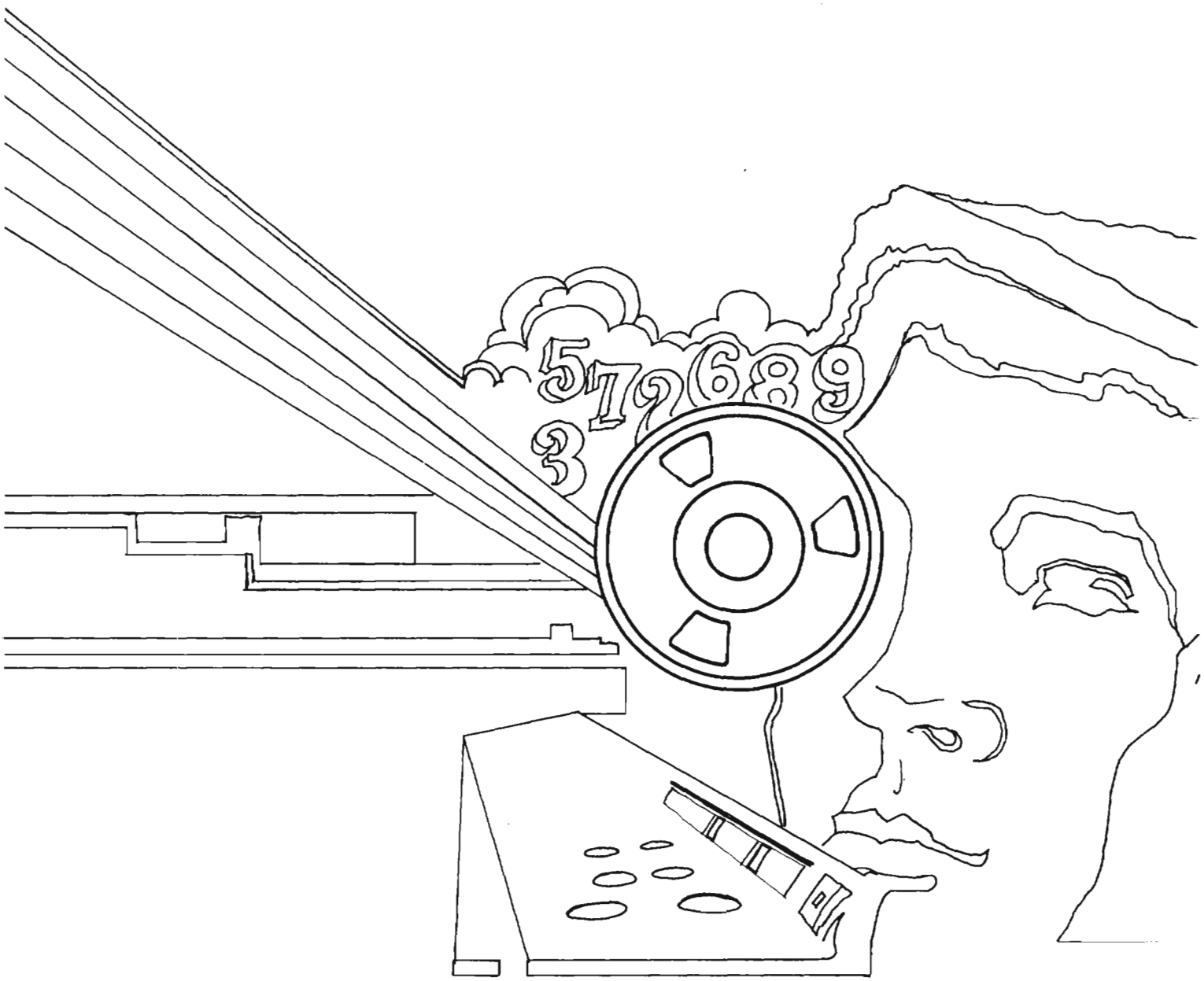
Now, I said there was divine intervention. It turned out historically that one out of the three aircraft worked successfully with this system on it. So the odds were very much in favor that we would have gotten a bad plane in the beginning at Monmouth or that we should have gotten a bad plane in the beginning in Vietnam. Given the suspicion (or skepticism) about ARDF -- we could have very well stopped, had that happened -- and here very competent people had said it couldn't be done anyway. There may not have been such a thing as ARDF today. It was a fortuitous thing and something we speculated about.

Q. Do you have any. . .anecdotes related to the development of ARDF. . .? P.L. 86-36

A. I think this business of taking it out as luggage. And the pilots would have been far more worried than they were if they had known just who mounted some of these systems, because all of us wound up riveting things on airplanes. I did. We almost lost it all in Hawaii when they misrouted all our luggage. We had to go at the last minute and dig that out of another Pan American aircraft. I think the selection of aircraft is also significant.

One of the things we took some technical satisfaction in was a little event out there when we were flying the first one. What we would do was to fly to Bien Hoa where we had a DF site and the flash transmitter which controlled our DF nets in Saigon. So we would fly over our DF site at Bien Hoa and shoot that flash transmitter, taking a bearing on it because that was one of the check bearings they used that was supposedly quite accurate. We worked a couple of days because there were a couple of degrees error, and finally in disgust went back and recomputed the check bearing and found out it had been calculated wrong and that the aircraft had been correct all this time.

[redacted]


5 7 9 6 8 9
3

DOCID: 4009723

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

AUGUST-SEPTEMBER 1975

EO 1.4.(c)

20 YEARS OF TRANSPOSITION..... [redacted] 1
PROCESSING [redacted]
COMMUNICATIONS..... [redacted] 7
THE VOYNICH MANUSCRIPT: THIRD THEORY...Doris Miller.....10
TYPEWRITER RANDOM: A NEW LOOK..... [redacted] 12
A FIX FOR THE LANGUAGE PROBLEM?.....John B. Thomas, Jr.....13
ABDUL AND HIS 40 TANKS.....Frederic O. Mason, Jr...17
LINGUISTS -- WE NEED AN "EXPERTS
YELLOW PAGES"..... [redacted] 19
LETTER TO THE EDITOR.....20

P.L. 86-36

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009723

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. II, Nos. 8 and 9 AUGUST-SEPTEMBER 1975

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemme (5642s)

Cryptanalysis.....[redacted](3571s)

Language.....Emery W. Tetrault (5236s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Frederic O. Mason, Jr. (4142s)

Production Manager.....[redacted](4998s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4009723

~~TOP SECRET UMBRA~~

EO 1.4.(c)
P.L. 86-36

20 YEARS OF TRANSPOSITION

E1 P.L. 86-36

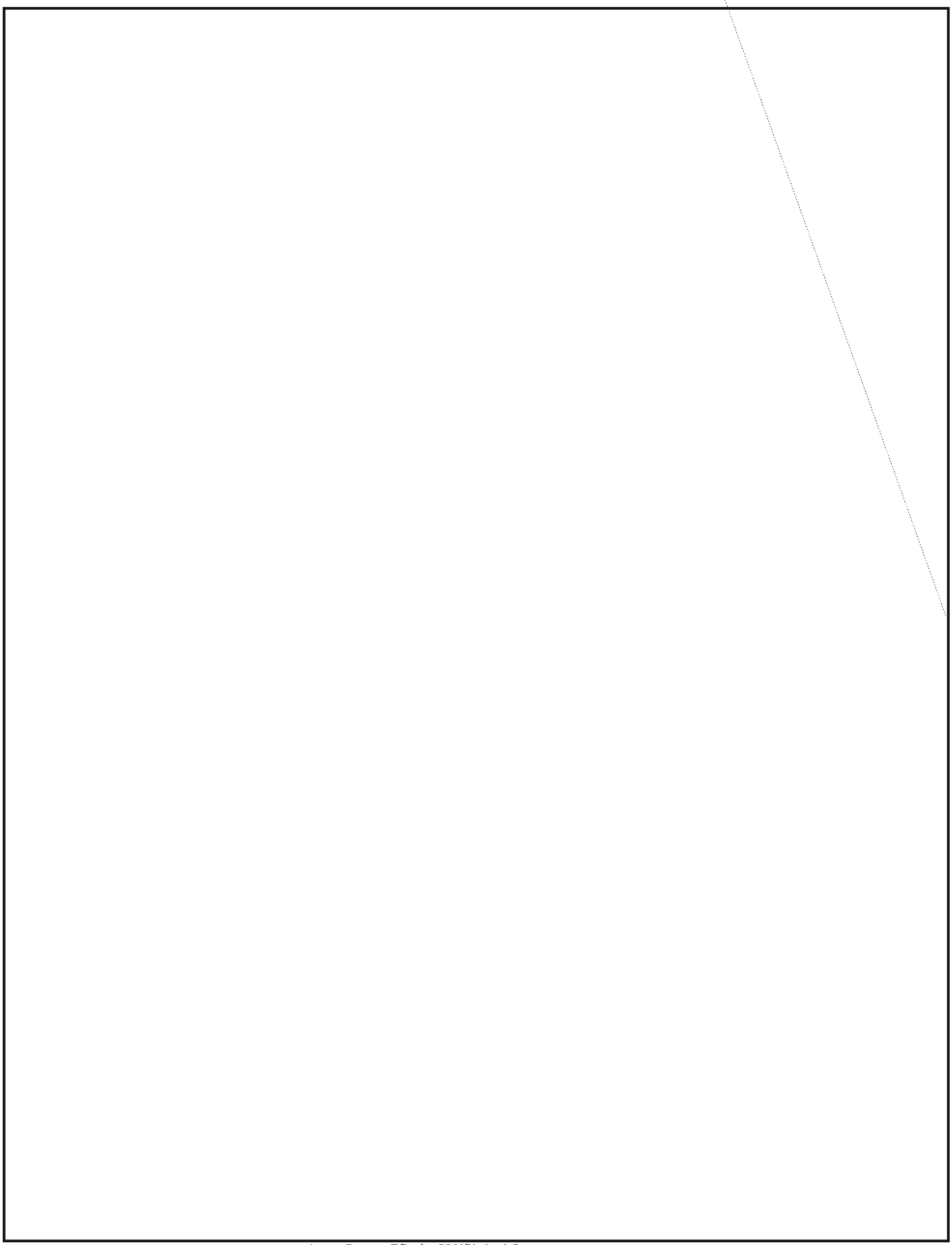
~~TOP SECRET UMBRA~~

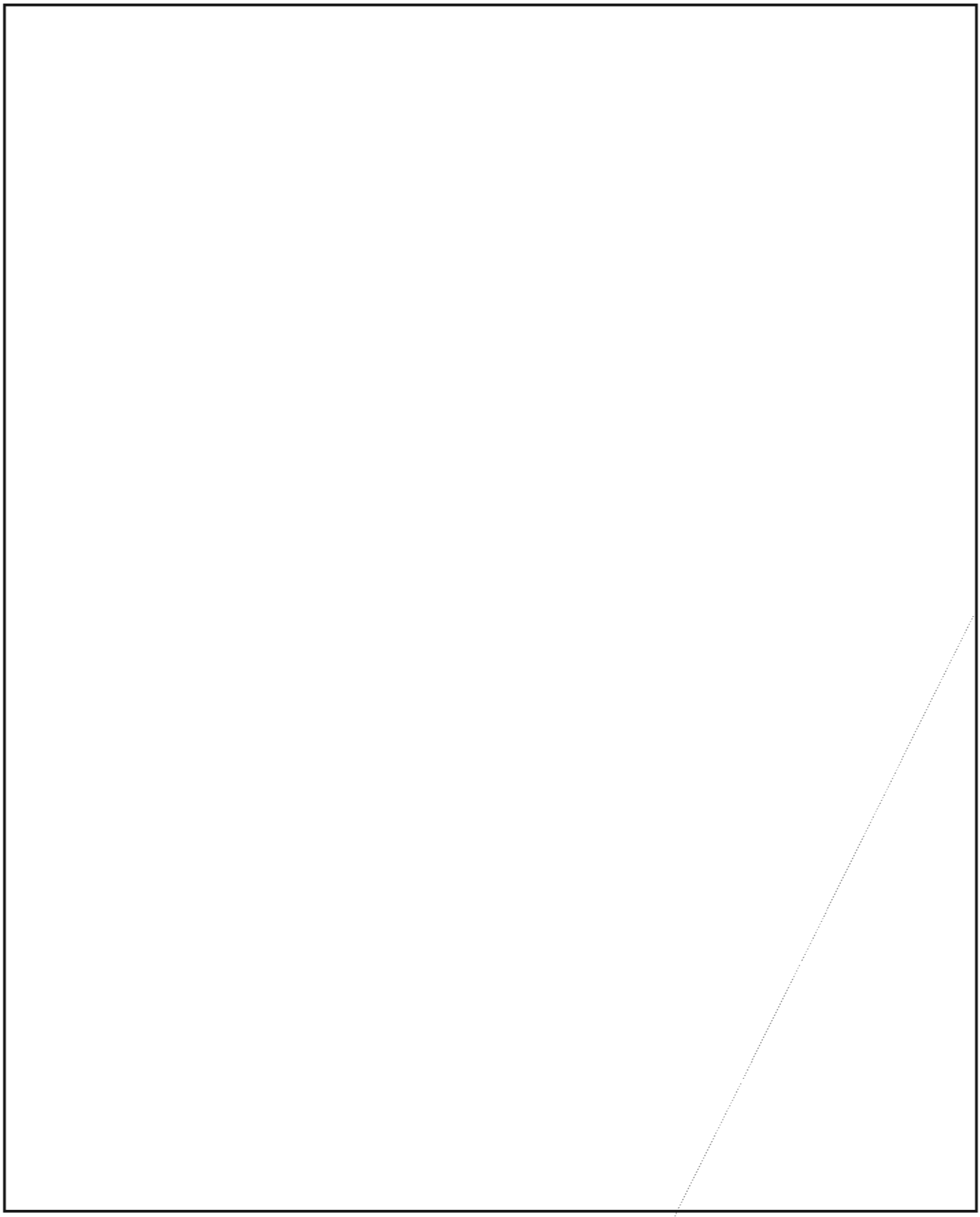
DOCID: 4009723

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

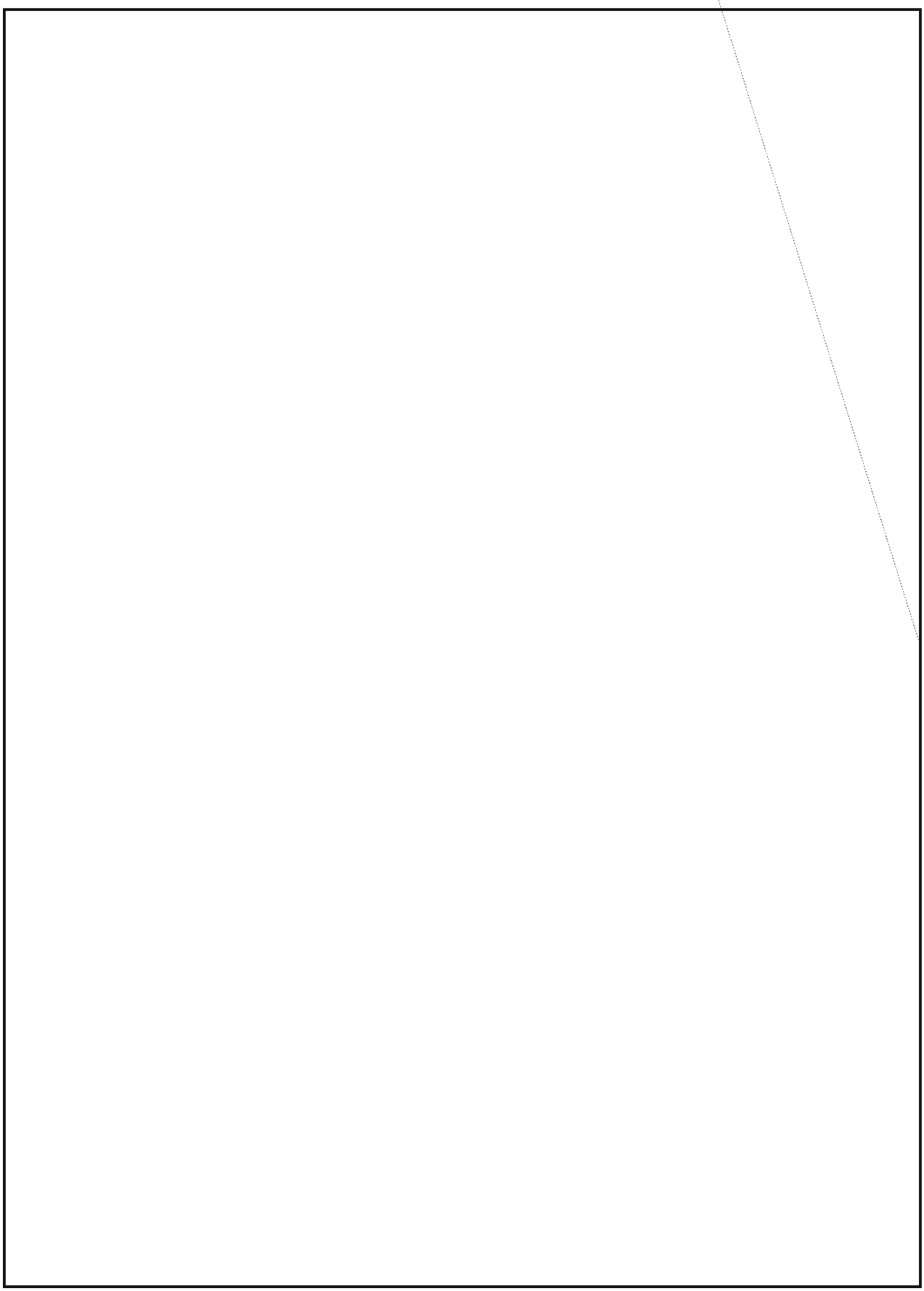
DOCID: 4009723





EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36



DOCID: 4009723

CRY-PTO-LOGROLLING

EO 1.4.(c)
P.L. 86-36

Have you ever seen puzzles in which the same series of letters "slides" or "glides" through all the words in the solution? As in the following S A M P L E ?

1.	**S**	**A**	M	P	L	E
2.	I	**S**	**A**	I	A	H
3.	E	S	**S**	**A**	Y	S
4.	T	U	S	**S**	**A**	H
5.	C	A	B	A	**S**	**A**

Letters used

√√√	√	√	√√	√√	√√	√	√	√	√√√	√	√	√
AAA	B	C	EE	HH	II	L	M	P	SSS	T	U	Y

Definitions

1. Specimen
2. Hebrew prophet
3. Short literary compositions
4. Fabric made of cultivated silk
5. Percussion instrument made of a hollow gourd enclosed in a net of threaded beads for use in a Cuban band.

This type of puzzle is variously called "slide-o-gram," "glide-o-gram," "step-o-gram," etc. But the CRYPTOLOG editor thinks that the letters do not slide, glide, or step at all. Instead, they *roll* through the words. So, in the puzzle below, roll the letters CRY through. On page 12, roll PTO through. And, finally, on page 20, try your luck at LOG-rolling.

1.	C	R	Y						
2.		C	R	Y					
3.			C	R	Y				
4.				C	R	Y			
5.					C	R	Y		
6.						C	R	Y	
7.							C	R	Y

Letters used

AA DDD EEEEEE F GG III LLLL
NNNNN OOOO PP R SSS TTTT U X

Definitions

1. NSA publication
2. Salts or esters of $CH_2CHCOOH$
3. Encoded or enciphered
4. Discovering
5. A crystal foreign to the rock in which it occurs.
6. Possible trade name for a bread to be served at smorgasbord (2 words)
7. In hot pursuit (3 words)

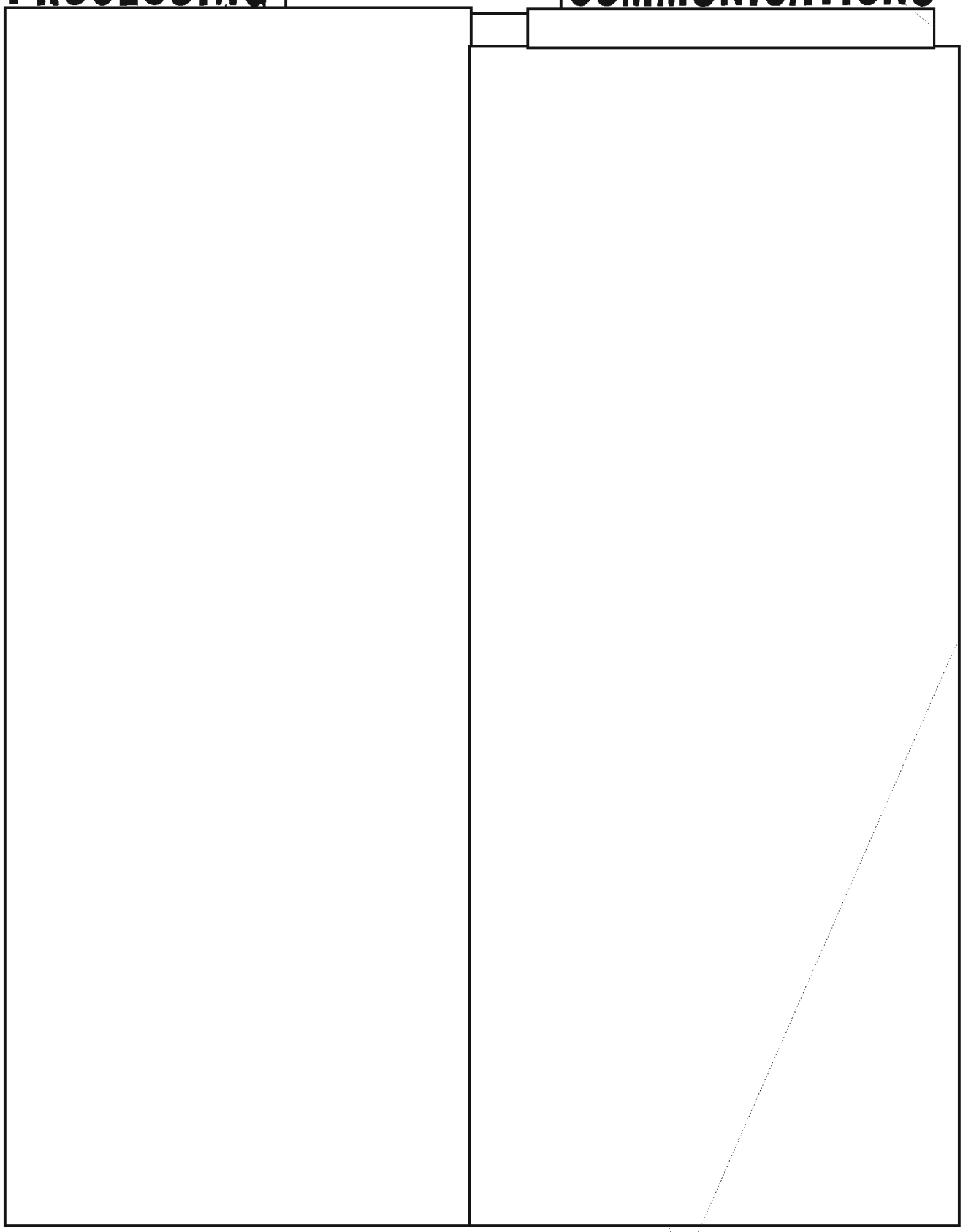
Puzzles on this page and pages 12 and 20 are UNCLASSIFIED.

EO 1.4.(c)
P.L. 86-36

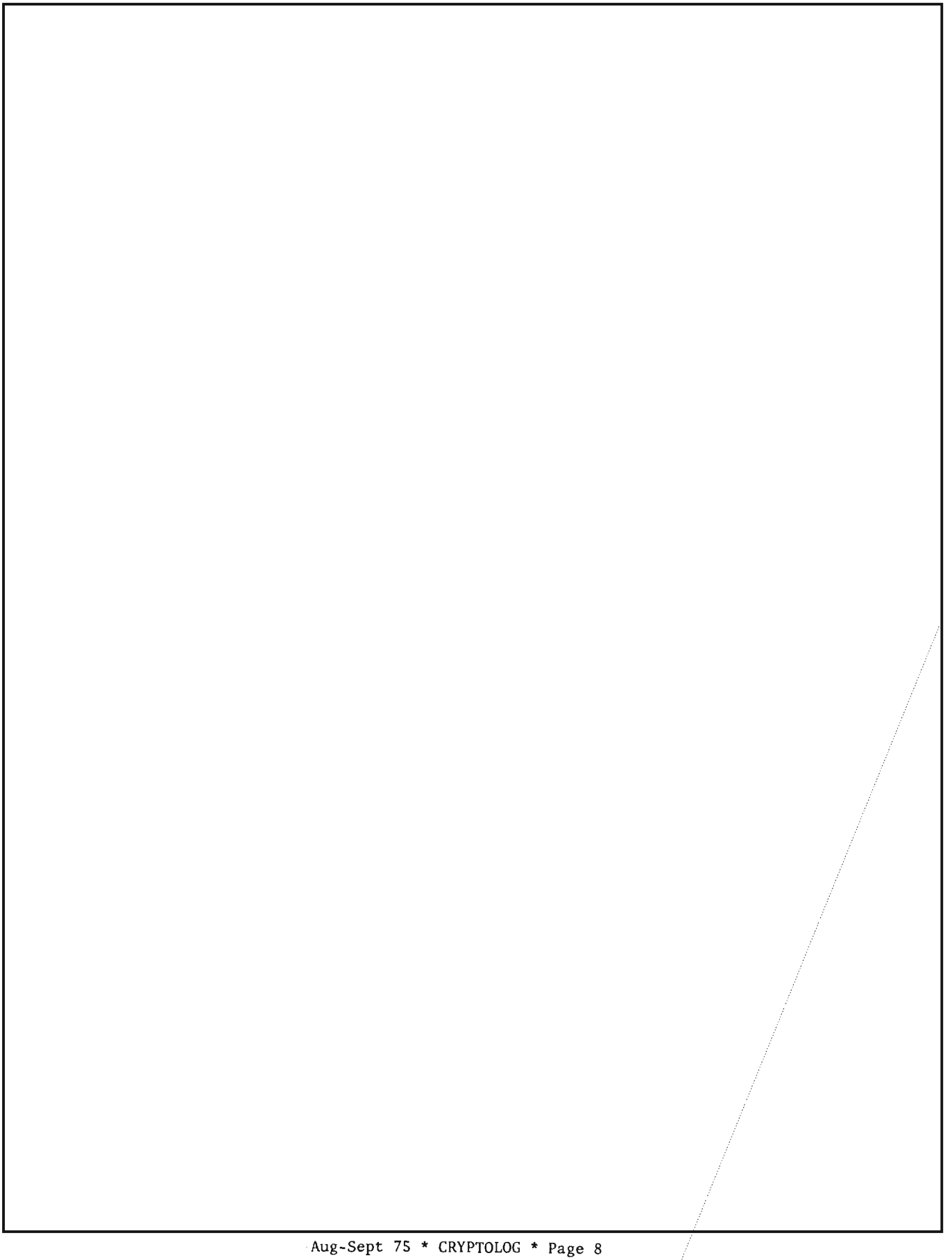
DOCID: 4009723

P.L. 86-36

PROCESSING [redacted] COMMUNICATIONS



EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

The Voynich Manuscript: Third Theory

Boris Miller, p16

When a newspaper editor needs a filler, he can always fall back on the Loch Ness Monster or the Abominable Snowman. For the editor of a cryptologic magazine the obvious device is another blurb on the subject here discussed. So, evidently, thought a former editor, among whose effects the following paragraphs were found.

Is the Voynich manuscript "real"? No. Is it a hoax? No. What is it, then? A make-believe--an elaborate fantasy produced purely for the satisfaction of the maker.

That was my reaction the first time I looked at it closely, but faced with all the profound theories about it I lacked the courage to say so. However, a recent rereading of Elizabeth Friedman's article in the Washington Post (August 5, 1962) and of Brigadier Tiltman's paper in the NSA Technical Journal (Summer 1967), plus some phenomena I have seen in the meantime, have emboldened me to give the world the benefit of my thoughts.

Some of the pertinent facts brought out in the above two sources are:

The exact number of symbols is uncertain, because of what may be variant forms and also because some apparently single symbols may in fact be two. Spacing appears to be random and punctuation completely absent. Paragraphs nearly always begin with one of two favorite symbols, which also occur frequently in the top lines of paragraphs, where there is some extra space. The number of different "words" is quite limited, and the same vocabulary appears in all sections, whether the content (judged by the illustrations) is botanical, biological, or astronomical. The "words" average four and a half symbols each, with very few of only one or two symbols, or of over seven. There are no erasures or corrections. Some of the commonest words occur several times running, but there are no repetitions of whole phrases, such as would be expected in any scientific text.

Brigadier Tiltman concludes that this is no natural language: "Languages simply do not behave in this way." On the other hand, it is equally impossible, for cryptologic reasons, that it can be the result either of simple substitution or of transposition. He draws no conclusions as to the nature of the text, but in this story I will be the truth-telling child who says rashly and cheerfully, "The text is nonsense."

This theory has always been disparaged on the assumption that no one would go to such lengths to produce a book without meaning. Who would have the time and the patience? What would be the point?

Well, first, the book presumably had some meaning for the originator, but this meaning may be in the pictures rather than in the text. As for time-- All through history many people have had more time than they knew what to do with: prisoners...invalids...unmarried aunts in well-to-do families. Empty hours stretched on into empty years, frightening years, and a long, long project would be something to cherish.

Suppose an imaginative woman chose to take up drawing instead of needlework, or suppose that a prisoner of state had a flair for art; and suppose that either of these, being illiterate (not unlikely at that time) but quite capable of imitating writing, decided to pass the time by creating a splendid book. A model book, so to speak. It makes as much sense as dollhouses, or boats in bottles; and you can make it life-size.

Or suppose that a country gentleman of means and learning has suffered an illness that leaves him slightly balmy. He spends his days in the field communing with the flowers or in his study painting impressions of them. (Look at those plants! They are lurid, even menacing, like Van Gogh's sunflowers; they are larger than life, with an animal shagginess and strength about them, and look as if they might well have dictated the whole project themselves.) He spends his evenings communing with the stars and depicting them. Neither his planets nor his plants bear much resemblance to reality, but he is living an intense inner life.

He decides to make a book. The writing skill remains in his fingers, but his brain no longer remembers the connection between the signs and the sounds. So he develops an alphabet of his own, of signs he enjoys making, and fills up the book with what amounts to "psycholcgical random" groups of these. At his death his family quietly lays the book away, and when it discovered years later, no one any longer knows its history.

Creative but frustrated people adopt strange means of self-expression. In Watts, California, stands a group of towers--the tallest a hundred feet high--built by a poor tilesetter out of steel rods, mesh and mortar, and covered with

mosaics made of bits of tiles, dishes, bottles and seashells. It took him 33 years, working without a plan, without assistance, without scaffolding--climbing, as he built, with a window-washer's belt. Then he gave the land to a neighbor and moved away. Why did he work so long on a useless fantasy? "I had in mind to do something big," he said, "and I did."

In the Smithsonian Institution stands the "Throne of the Third Heaven of the Nations' Millenium General Assembly": a room-sized composition of chairs, tables, pedestals, cardboard cutouts, old jelly glasses, used light bulbs, pieces of mirror--all covered with "gold" and "silver" foil and assembled into an astonishing and magnificent structure. It was built, over a period of 14 years, by a Washington laborer, in a garage he rented for the purpose, and was discovered only after his death. Its purpose or meaning is unknown.

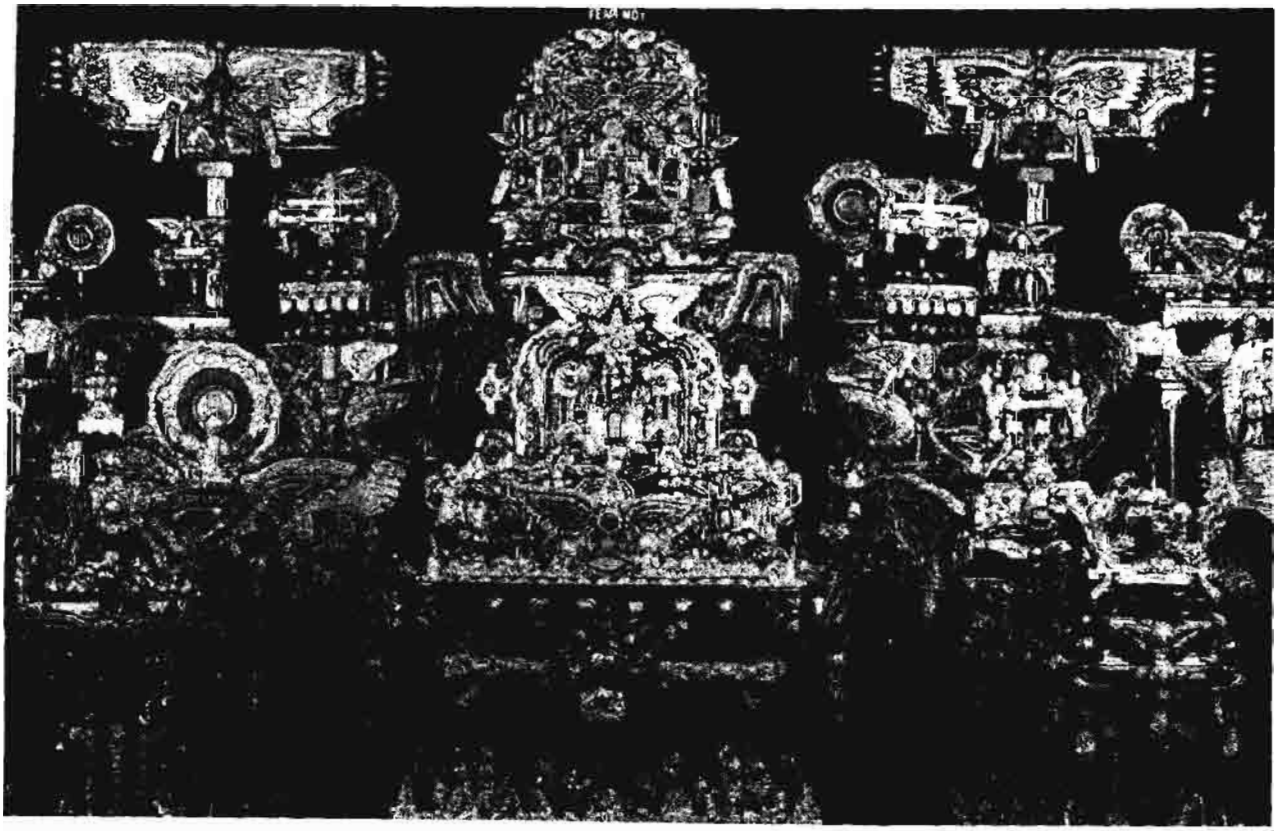
But, you may say, they at least produced something tangible--a work of art. So did the maker of the Voynich manuscript--a fascinating work of art; and the "text" may serve the same purpose as the mosaics on the towers or the foil-covered bulbs on the "Throne"--it is part of the general effect.

It is possible, of course, that the writer also harbored a secret hope. A record called "The Gift of Tongues (Glossolalia)," issued by the Scepter Company, purports to be the voice of a man "speaking in tongues." It takes the hearer only a few minutes to become convinced that the man is inventing: the sounds do not pour out spontaneously, but haltingly and lamely, with an embarrassing amount of repetition. Is the speaker a fraud? Not necessarily: he may naively suppose that this ability to invent is actually the fabled gift of tongues, and that even though he has to search for the sounds, the Power that permits him to find them also knows their meaning...

In any case, why assume a message where there is no evidence of one? Visually, the pages are a joy, and if the "text" turns out to be written glossolalia, or abstract art, why not?

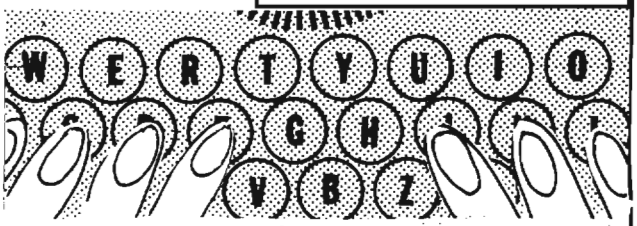
"I had in mind to do something big," says the author, "and I did."

Yes, we do have a copy of this famous manuscript in the Crypt Library (Room 3W076), and you may like to go and see it. But there are a lot of other things in there more worthwhile -- in fact, we've been trying for some time to get an article on the library. Any volunteers?



Photograph by Charles Phillips,
courtesy of Smithsonian Magazine

TYPEWRITER RANDOM -- A NEW LOOK.



The right hand-left hand test for possible 'typewriter random" generation of key is an old standby. We might apply another test involving movement to the right or to the left on the keyboard. Under the two tests, quite different interpretations would arise concerning the following group:

Text	8 6 9 6 0
Right hand-left hand	R R R R R
Directional	L R L R

One theory would be that the right hand only was used in typing the group (since numbers 6 through 0 are normally typed with the right hand). Another possibility is that a "two-fingered" (hunt-and-peck) typist used his two fingers alternately.

The equiprobable measure does not apply when the directional test is used (e.g. there are millions of ways to produce RLRLRLRLR, but only one case gives RRRRRRRRR).

Random probabilities have been computed for trinomes, tetranomes, and pentanomes. The probabilities labeled "*with*" are for text in which groups with doublets (the "hits") category) have been retained. The "*without*" probabilities apply when groups with doublets are not counted.

TRINOMES

	With	*Without*
LL	.12	.148
LR	.285	.352
RL	.285	.352
RR	.12	.148
Hits	.19	

TETRANOMES

	With	*Without*
LLL	.021	.029
LLR	.087	.119
LRL	.1695	.233
LRR	.087	.119
RLL	.087	.119
RLR	.1695	.233
RRL	.087	.119
RRR	.021	.029
Hits	.271	

PENTANOMES

	With	*Without*
LLLL	.00252	.0038
LLLR	.01638	.0250
LLRL	.04938	.0753
LLRR	.02892	.0441
LRLL	.04938	.0753
LRLR	.10317	.1572
LRRL	.06192	.0944
LRRR	.01638	.0250
RLLL	.01638	.0250
RLLR	.06192	.0944
RLRL	.10317	.1572
RLRR	.04938	.0753
RRLL	.02892	.0441
RRLR	.04938	.0753
RRRL	.01638	.0250
RRRR	.00252	.0038
Hits	.3439	

~~(CONFIDENTIAL)~~

KEEP ON ROLLING!

1.	P	T	O						
2.		P	T	O					
3.			P	T	O				
4.				P	T	O			
5.					P	T	O		
6.						P	T	O	
7.							P	T	O

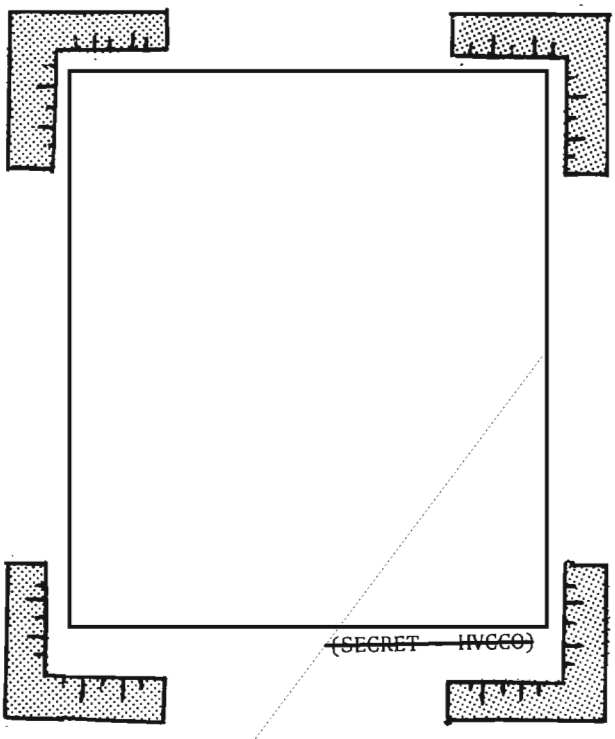
Letters used

A CC EEEEE GGG H IIIIIII LLL M NNN OO P RR S TTTTT UU V W Y

Definitions

1. Of or relating to the Greco-Egyptian rulers of Egypt from 323 B.C. to 30 B.C.
2. Those those live in the residential section of a city
3. Walking or proceeding quietly or cautiously
4. Popular monthly
5. Incapable of performing something (4 words)
6. The highest degree or extent (2 words)
7. Utter (3 words)

(UNCLASSIFIED)



~~(SECRET -- HVCCO)~~

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36

DOCID: 4009723

A FIX FOR THE LANGUAGE PROBLEM?

JOHN B. THOMAS, JR., Special Assistant, Language, A9

An "old hand" proposes a management tool that might be of help to deal with a perennial "bucket of worms."

P.L. 86-36

Doris Miller's article "Language and the COMINT Production Process" (*NSA Technical Journal*, Summer 1974) falls gracefully into [redacted] category of "What oft was thought, but ne'er so well express'd." It is for good reason that that article won the First Prize in the Crypto-Linguistic Association's 1975 Essay Contest.

I would like to expand this subject in the same general vein, by:

- supplying a kind of postscript dealing with some specific points about voice language work and the role of the military;
- examining the paradox: If these ideas were indeed "oft thought," why hasn't more been done about them?
- suggesting a methodology and management posture by which the working linguist's and the working linguist-manager's wisdom and observations can be converted from a still small voice into a real help for higher management.

Looking first to the voice problem, I would caution that we are on shifting ground in this area. Miss Miller discusses things that specialists almost unanimously feel should be done. She considers the problem to be one of enlightening and persuading management to put some force behind the ideas she projects. The voice problem, on the other hand, I think finds even specialists with more uncertainty about standards and procedures. This is no wonder.

The Voice Explosion is terrifying. [redacted] You zip voice tracks back and forth in fancy machines, and then you get more fancy machines to zip printed transcripts back and forth. But no "machine" can *produce* a transcript. Finally, you bite the bullet and admit that the human transcriber remains the heart of the business. [redacted]

[redacted]

We need all the help we can get. Channel identification, [redacted] and any other possible selection processes need to be exploited to the fullest to put the best possible intercept, the richest of all the ore, before the transcriber.

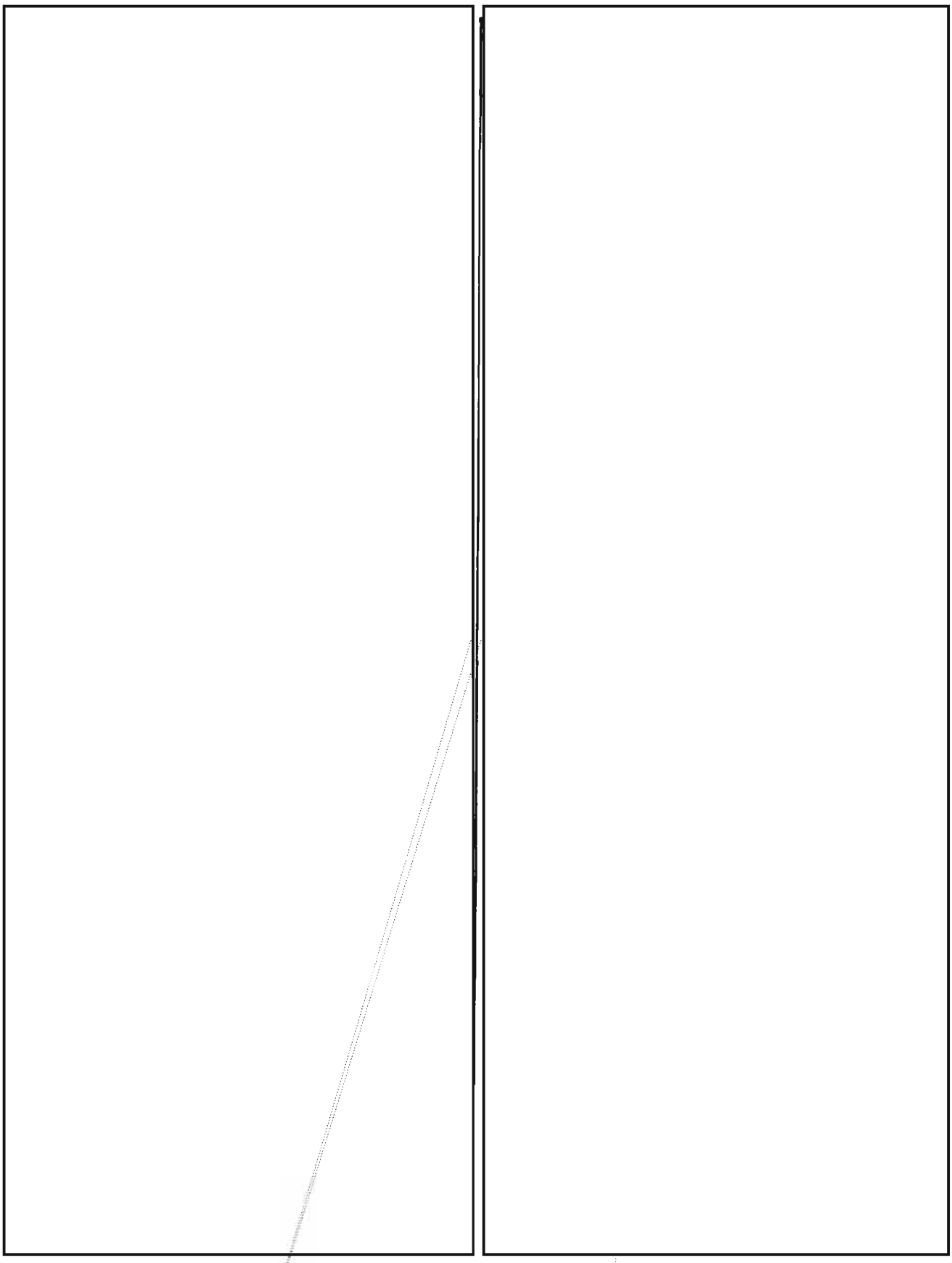
EO 1.4.(c)
P.L. 86-36

Does everyone fully realize that, until the magical "machine transcriber" appears, the voice language processor is the valve through which the whole production stream must flow? Some realize it and apply the unfair, pejorative term "bottleneck" to him. But the term is passive, whereas the transcriber is active. In fact, only in the degree to which he is active is any intelligence possible. And a person carrying out a key (that is, critical) process deserves to be recognized with at least a positive-sounding term. "Key processor" sounds awkward, but it is certainly accurate.

[redacted]

EO 1.4.(c)
P.L. 86-36

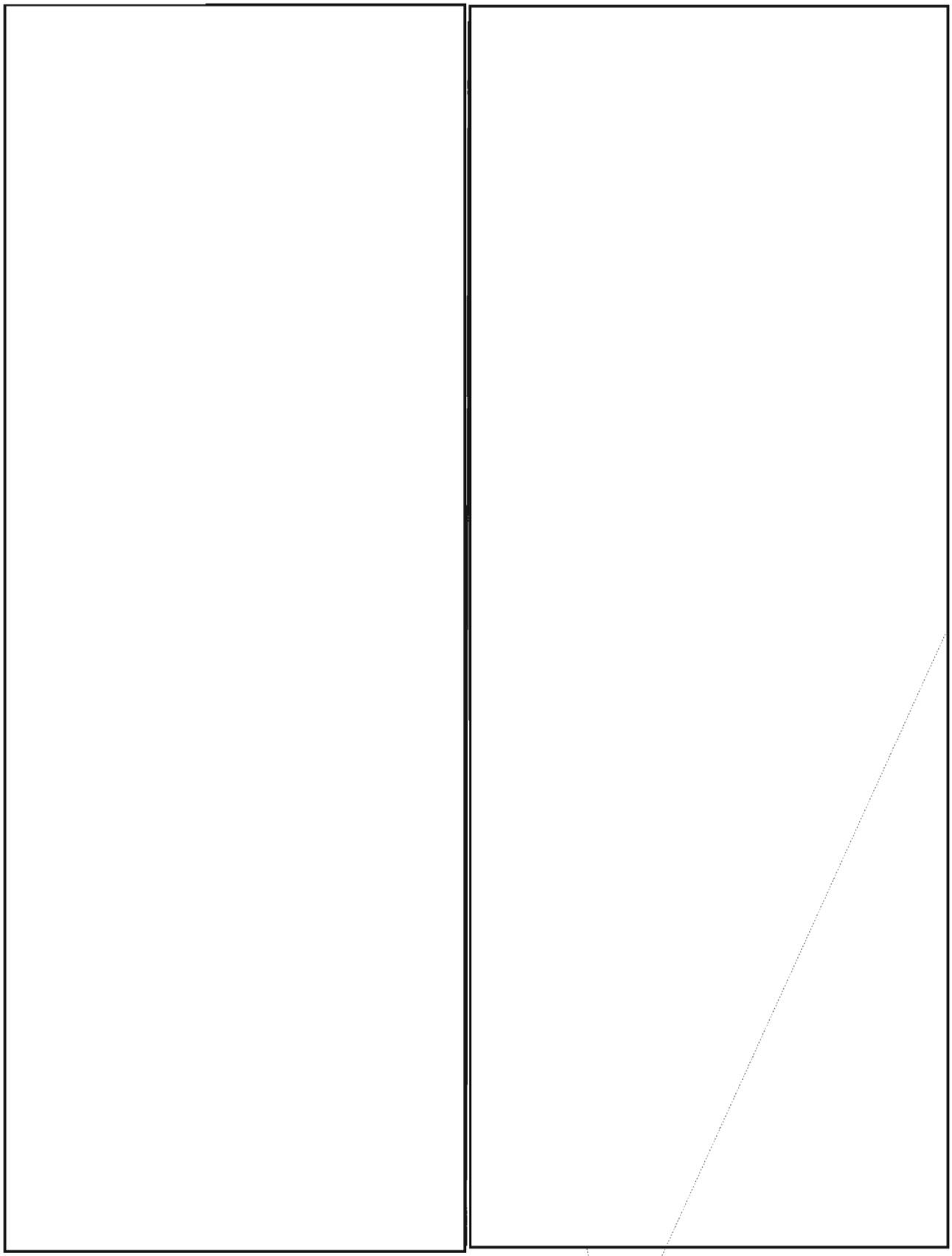
DOCID: 4009723



EO 1.4.(c)
P.L. 86-36

P.L. 86-36

~~SECRET~~



~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

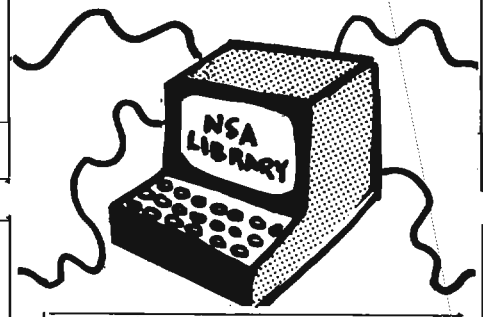
EO 1.4.(c)
P.L. 86-36

~~(SECRET - HVCCO)~~

NSA ON-LINE ACCESS TO OUTSIDE SOURCES OF INFORMATION

FTD
USAF Foreign Technology Division, Dayton, Ohio
Foreign scientific-technical literature
Location of terminal: Room 2N090, 5759s

DDC
Defense Documentation Center, Alexandria, Va.
DoD research and development information
Location of terminal: Room 2N090, 5759s



An article on NSA's computer network resources will appear in a future issue of CRYPTOLOG.

(UNCLASSIFIED)

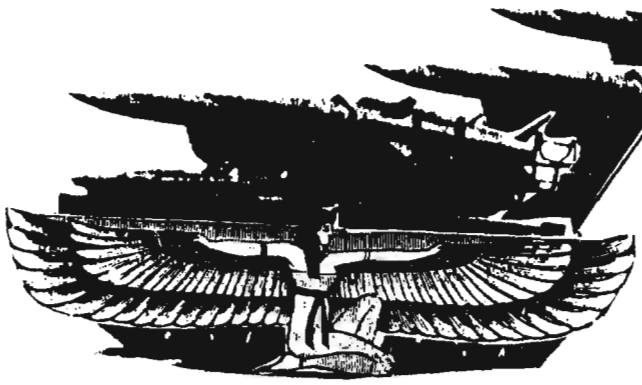
OCLC
Ohio College Library Center, Columbus, Ohio
Book collections of 400 libraries in network
Location of terminal: Room 2N111, 4084s

NYT
New York Times Data Bank, New York, N. Y.
Index to NYT and certain other publications
Location of terminal: Room 2C051, 3358s

EO 1.4.(c)
P.L. 86-36

ABDUL & HIS 40 TANKS

Frederic O. Mason, Jr. PJ1



EO 1.4.(c)
P.L. 86-36

DOCID: 4009723

EO 1.4.~~(c)~~
P.L. 86-36

LINGUISTS -- WE NEED AN "EXPERTS YELLOW PAGES"!

Time was when a translator had to be extra careful when dealing with the difference between "request" and "demand" or with the exact rendition into English to indicate just how miffed or mad or scared the original drafter of the message had been. Life was simple then, or so it seems now. The *subject matter* in the messages was "general liberal arts," although the language of diplomacy was always much more precise than the language appearing in the daily press. But U. S. interests are a bit more complex and technical now, and so are the subjects that our message texts deal with. Our general-purpose dictionaries, or even our specialized dictionaries, are neither up to date nor up to it.

Simultaneous interpreters advise us to study, in advance, English-language reference aids dealing in general with the subject matter that is likely to be discussed in the foreign language. But we NSA-ers can't always do this. Not when a single translator might have to deal with *specifics* of:

Letter to the Editor

To the Editor, CRYPTOLOG:

Hurrah for CRYPTOLOG!! This little monthly technical publication offers all of us SIGINTers a much-needed informal forum for the exchange of ideas, particularly for highly controversial subjects in need of clarification and resolution. In this process of written debate we all have an opportunity to express an opposing viewpoint, thereby bringing closer a consensus of understanding that we can all subscribe to. The major ingredient required is that the proponent know something about the subject matter involved. Unfortunately, some of the writers state their views with conviction based upon limited background experience. Such views can be dangerous because they are frequently misleading, and sometimes utterly wrong.

The latter type of erroneous view requires an immediate rebuttal before it gains even minimal credence. The anonymous letter in the June issue of CRYPTOLOG (deriding my earlier letter in the May issue) is just such a letter riddled with fallacies -- not just one, but THREE at least. It's fortunate for the author that he did not sign his name to such a gaffe.

1. Nowhere in my letter is there a hint or intent to belittle the contribution or value of the cryptanalysts. I have the highest respect for their specialized expertise, but, really, they are not always needed in the exploitation of codes or charts.

2. Mr. Noname makes his worst error (and most damning self-indictment of his technical knowledge) by assuming that

3. The bookbreaker,

He does it by deductive reasoning, hard, painstaking work, and the maximum use of his language skill and background knowledge of the target.

Time and space do not permit me to comment on Mr. Noname's statement about "true SIGINT production." I'll take a rain check for that one.

~~(SECRET SPOKE)~~

LANGUAGE IN THE NEWS

WASHINGTON POST
Friday, July 4, 1975
By Douglas B. Feaver
Washington Post Staff Writer

The National Transportation Safety Board moved yesterday to repair one of the most potentially dangerous flaws in U.S aviation—the possibility that pilots and air traffic controllers might not understand each other. . . . .

The misunderstanding in the TWA crash was of the terms, "cleared for approach." . . . . the controller at Dulles told the plane, "You're cleared for . . . approach to runway one two."

. . . . those words meant that the plane was authorized to descend only to 3,400 feet until it crossed a navigation point known as Round Hill. Then it could drop to 1,800 feet and continue its approach to the runway.

A recording of the crew's conversations that was recovered from the wreckage showed that crew members briefly debated the meaning of those instructions as they looked at their navigational charts . . . .

Different pilots who testified at the hearing gave different interpretations of what "cleared for approach" meant to them. . . . .

(U)

LAST CHANCE!

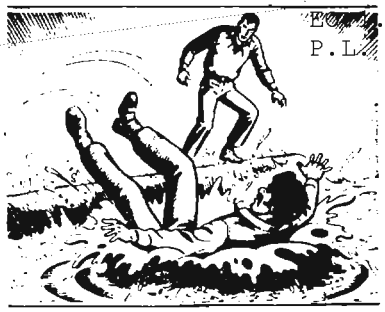
1.	L	O	G					
2.		L	O	G				
3.			L	O	G			
4.				L	O	G		
5.					L	O	G	
6.						L	O	G
7.							L	O	G

Letters used

AA B CCCC DD EEE G HH III MM NN OOOOO PPPP R SSS T UU YYY Z

Definitions

1. A dispute over words
2. Express tersely or as to induce action or instill opinion or belief
3. Inflammation, especially of external parts of the body
4. Freed from obstructions
5. Of or relating to soil science; of or relating to child study
6. Phrenology (usually used disparagingly)
7. Guess!



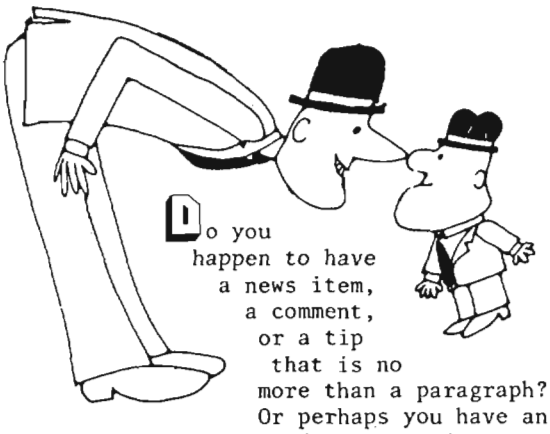
E.O. 14.(c)
P.L. 86-36

In case you fell off somewhere, the answers to all three puzzles will appear in next month's issue.

(UNCLASSIFIED)

DOCID: 4009723

Contributions Solicited



Do you happen to have a news item, a comment, or a tip that is no more than a paragraph? Or perhaps you have an article of several thousands words...? Long or short, if it has something worthwhile to say, we'll print it. (For your interest and guidance, one page of typescript, double-spaced, makes about one column in CRYPTOLOG.)

First-person articles or stories about your own experiences are welcome, so long as they relate to our work. (See "Busman's Holiday" in August 74 issue.)

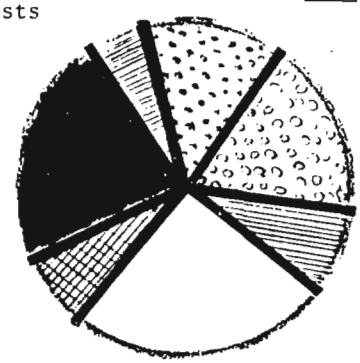
Want anonymity? A thoughtful piece on a subject of interest to many readers will be considered for anonymous publication, if the writer requests it. (The writer must, however, identify himself to the editor in an accompanying note or by a personal call.) Needless to say, personal or trivial complaints will not be considered.

Photographic illustrations can be reproduced, at the same quality as those in the NSA Newsletter.

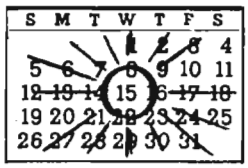
Sensitive materials? No. We'll go all the way to Top Secret Codeword, but we have to draw the line at compartmented or otherwise exclusive sources.

Your contribution does not have to be typed; we'll give preference to content over form, every time. (Though, especially in the case of a long piece, the editorial eye will appreciate any effort you can make in that direction--garbles and strikeovers freely forgiven.)

Something missing? *If you feel that* <u>your</u> work or <u>your</u> interests are not being well represented in CRYPTOLOG, it's probably because you and your friends are not contributing. The editors earnestly want to cover the whole territory, but articles don't grow on trees, y'know! Somebody (who knows the subject matter) has to write them.

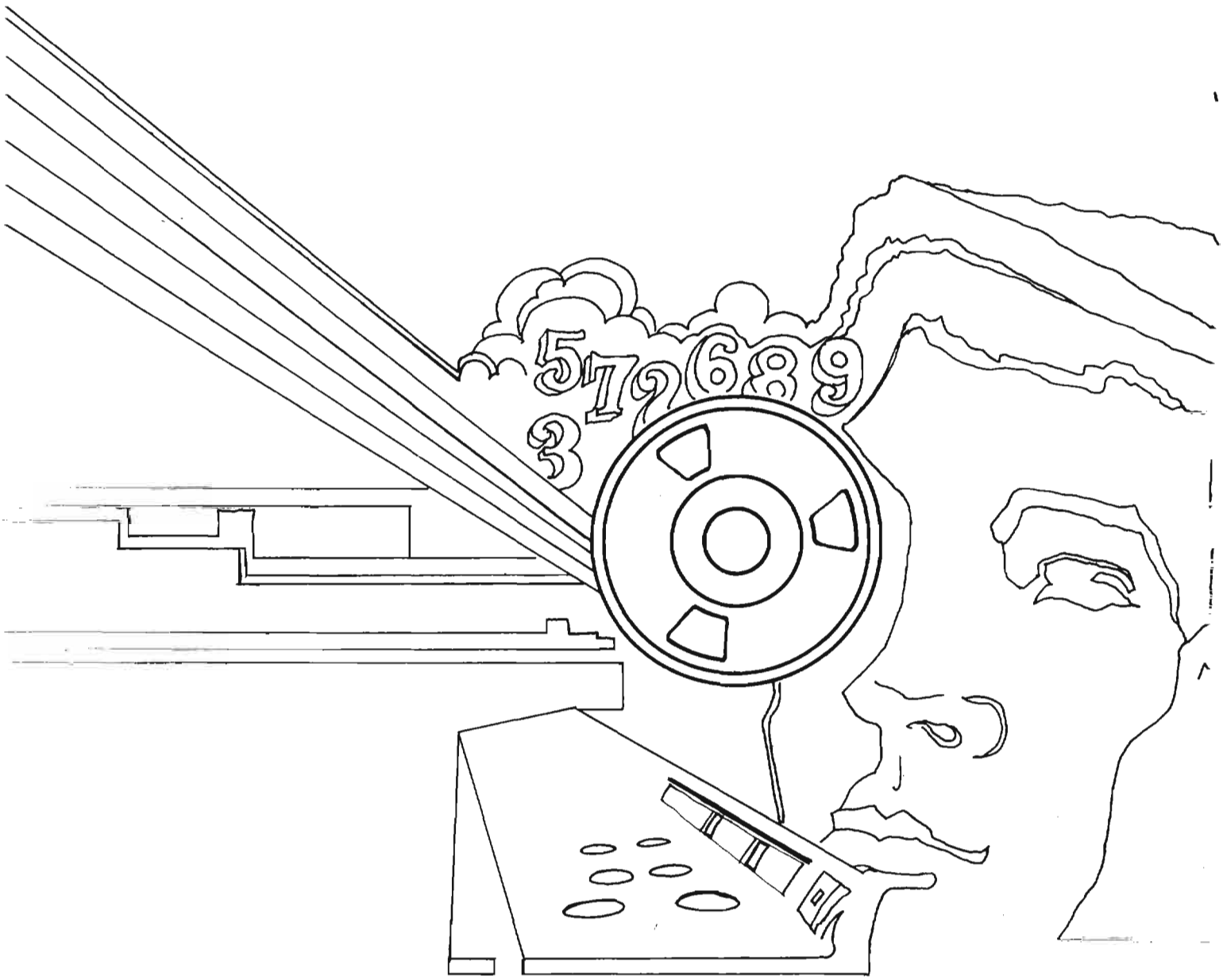


Need assistance? You may have an idea, or some notes, or even a half-finished paper that you feel has possibilities but you don't quite know what to do with. A call to the appropriate departmental editor will get you a "story conference" and possibly inspire you to finish it up and get it into print.



Our deadline is theoretically the middle of the month (the 15th of August, for publication in October, and so on), but don't let that stop you if something good comes along on the 16th. And anyhow, this is a monthly publication; if you miss this month's deadline you'll be just in time for next month's CRYPTOLOG. See you!

P1-Aug 75-S3-24041


5726893

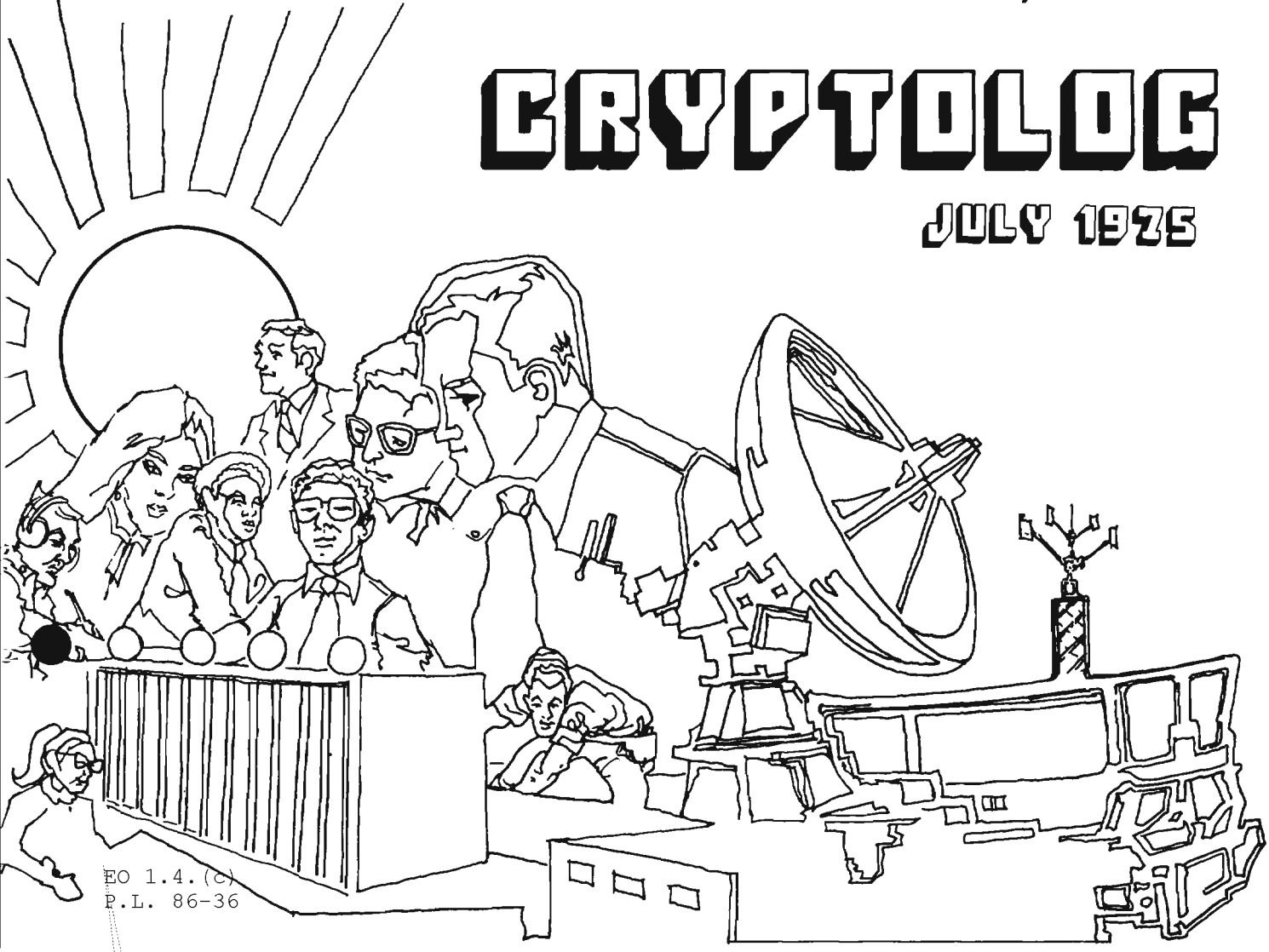
DOCID: 4009722 P.L. 86-36

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JULY 1975



EO 1.4.(C)
P.L. 86-36

WARSAW PACT [redacted] ..... [redacted] ..... 1 P.L. 86-36
TOO MANY GARBLES ..... [redacted] 3
"RE-PSYCHLING" THE CODE CLERK ..... [redacted] 4
MACHINE INTELLIGENCE: PROMISE OR DELUSION? ..... [redacted] 5
RAPIDTRAN: [redacted] ..... [redacted] 9
NEWS BRIEFS (CMI, CLA; CAMINO) 13

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009722

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. II, NO. 7 JULY 1975

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief..... Arthur J. Salemme (5642s)
Collection..... [redacted] (3571s)
Cryptanalysis..... [redacted] (8025s)
Language..... Emery W. Tetrault (5236s)
Machine Support..... [redacted] (3321s)
Special Research..... Vera R. Filby (7119s)
Traffic Analysis..... Frederic O. Mason, Jr. (4142s)
Production Manager..... [redacted] (4998s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

~~TOP SECRET UMBRA~~

THE WARSAW PACT

[redacted]

[redacted]

P.L. 86-36

In recent years the Warsaw Pact has recognized the need for [redacted]

[redacted]

~~TOP SECRET UMBRA~~

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

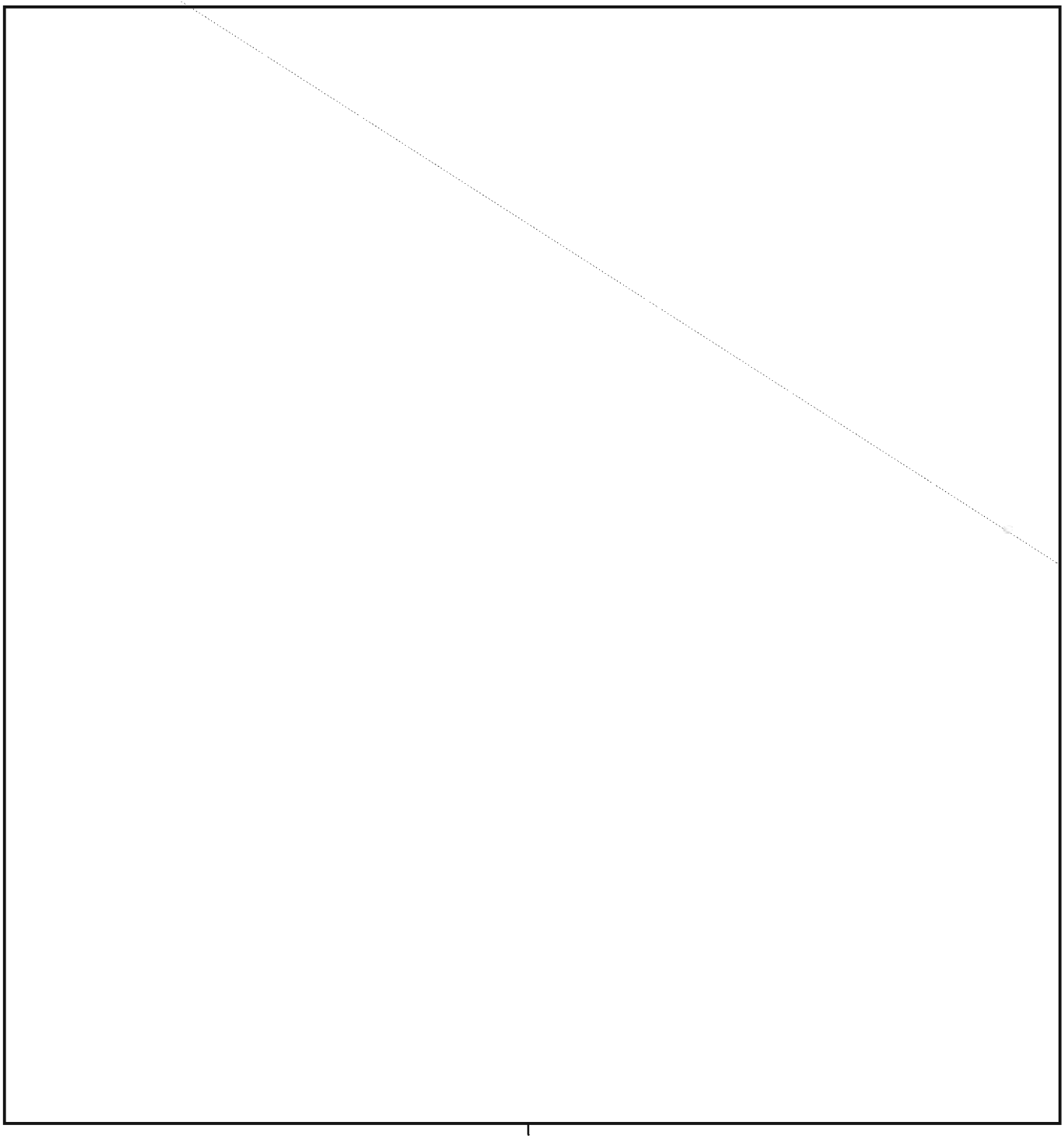
~~CONFIDENTIAL~~

T Y G S
SOO MANX FARBLER
A Moral Tale for Cryptanalysts

EO 1.4.(c)
P.L. 86-36

By [redacted]

P.L. 86-36



~~CONFIDENTIAL~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

"RE-PSYCHLING" THE CODE CLERK

By [redacted]

P.L. 86-36

[redacted] *who is currently working* [redacted] *submitted the following response to the editor's invitation to "match" Mr. Callimahos' WWII observations in the April 1975 issue.*

Throughout the 1960's, the Vietnamese Communists were straightforward in their cryptographic habits and could be relied upon to be fairly secure [redacted] However, the VC code clerks, not unlike their Japanese counterparts in WWII (as discussed by Mr. Callimahos), had a peculiarity that gave the cryptanalyst that helpful boost.

In 1968 the VC began a gradual change from [redacted]

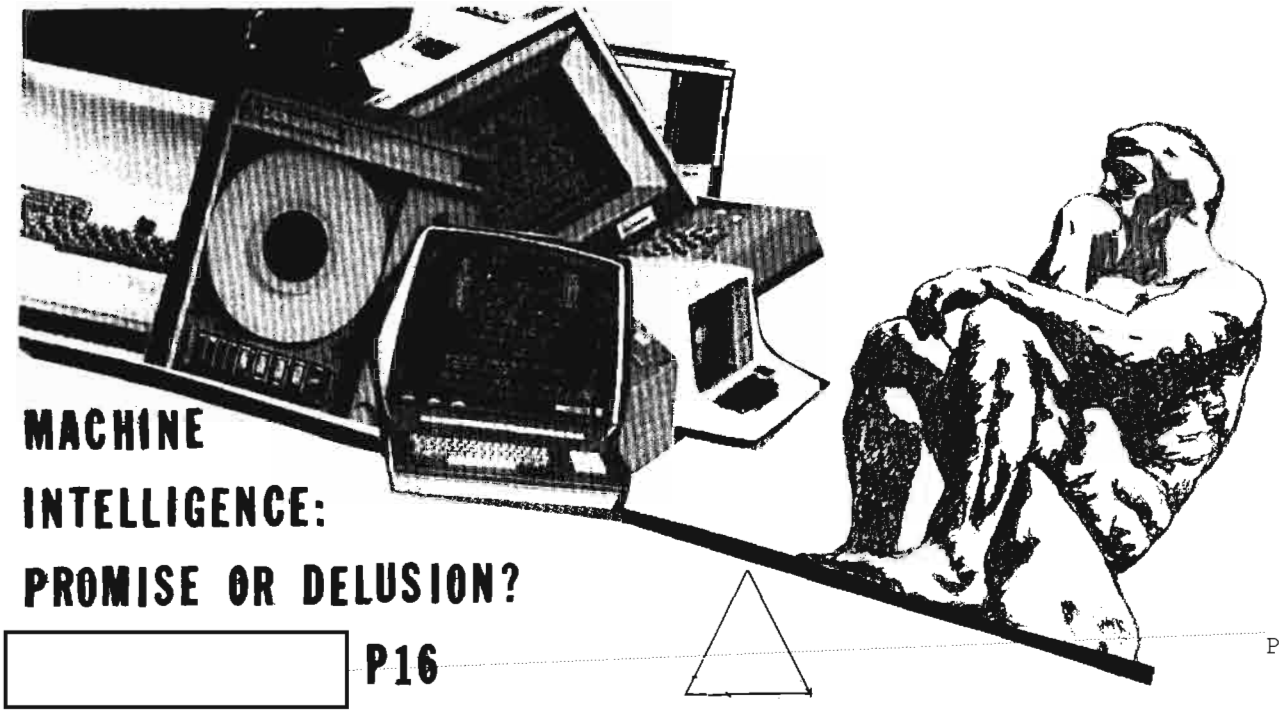
While there were indeed other features exploited by those engaged in the long-term, in-depth analysis of these communications, this particular one proved especially interesting to those of us engaged in the initial analysis of [redacted]

* * * * * * *

Solution to [redacted] Radiotelephone [redacted] in June 1975 issue.

[redacted]

Puzzle solution is ~~SECRET SPOKE~~



MACHINE INTELLIGENCE: PROMISE OR DELUSION?

[redacted] P16

P.L. 86-36

The following paper was written as part of a larger project that will include a selective review of ARPA-funded Artificial Intelligence research since 1967, in the light of the criticisms raised by Dreyfus and others. The results of this study will be published as a P1 Report in the near future.

> *What Computers Can't Do*, Hubert L. Dreyfus. Harper and Row, New York, 1972.

Hubert Dreyfus is a professional philosopher who has been a persistent gadfly to Artificial Intelligence (A.I.) researchers for several years. He published an earlier, strongly critical paper (Dreyfus 1965) whose points were all promptly and emphatically brushed aside by spokesmen for the A.I. community. Now he has written a book which, I believe, cannot and should not be so summarily dismissed by any thinking person, whatever his attitude toward computers.

For those readers who may not be familiar with that branch of computer science called Artificial Intelligence, it involves the attempt to program or build a digital computer capable of producing behavior that a human being would accept as truly intelligent. A.I. researchers have been trying, with varying degrees of success, to get computers to do such things as playing chess and Go; proving logical and mathematical theorems; understanding and translating written and spoken language; controlling a robot vehicle or an artificial arm and hand; perceiving and understanding visual scenes and patterns; and carrying out a sensible dialog with a human being on a topic of interest and importance. An excellent recent book that tells the story of A.I. from the point of view of a prominent worker in the field is Michie (1974). Unlike so much writing on technical topics, it is clear, readable, concise, and even enjoyable, and I strongly recommend it to anyone interested in a good survey from a friendly position.

Dreyfus presents a strong and well-reasoned claim that we will never be able to get digital computers to do any of the above-mentioned kinds of intelligent things nearly as well as people do them. He shows quite convincingly that the research he has reviewed, covering the years 1957 through 1967, has failed in all but a few relatively simple, highly formal and restricted tasks. He bases his case on purely philosophical grounds, on logic, and on a demonstration of the essential inadequacy of those often unspoken assumptions about the brain, the mind, human knowledge, and the nature of reality that underlie not only A.I. research, but in fact our whole Western scientific world-view.

Intelligent human activities are assigned by Dreyfus to four classes:

> *ASSOCIATIONISTIC ACTIVITIES*, innate or learned by repetition, such as memory games, maze problems, word-for-word substitution, and responses to rigid, unvarying patterns or stimuli.
>
> *SIMPLE FORMAL ACTIVITIES*, learned by rule, such as simple games (Nim, Tic-tac-toe), simple combinatorial problems,

mechanical theorem proving, and recognition of small sets of clear-cut patterns (e.g. typed character fonts).

COMPLEX FORMAL ACTIVITIES, learned by rule and practice, such as "noncomputable" games (chess, Go), complex combinatorial problems, nonmechanical theorem proving, and recognition of complex patterns in noise.

NONFORMAL ACTIVITIES, learned by example and insight, such as "ill-defined" games (riddles), open-structured problems, translation of natural language, and recognition of varied and distorted patterns such as speech.

A digital computer program, as Dreyfus readily admits, can carry out activities in Classes 1 and 2 quite adequately and even well. Class 3 activities are theoretically capable of being spelled out in a set of instructions, but in practice the resulting description is far too long and complex for brute-force implementation in any existing or presently conceivable computer. These activities are apparently accomplished by people through the use of powerful conceptual shortcuts and insights ("heuristics") which provide an immediate and dramatic reduction in complexity. While Dreyfus does not commit himself on the question of how far computers can go in "heuristic" attacks on Class 3 problems, his tone is decidely pessimistic. Activities in Class 4 are in a completely different world, Dreyfus claims, separated from Classes 1 through 3 by a major discontinuity that cannot be bridged by any computer program. These activities are inherently indescribable in terms of any formal language (such as mathematics, logic, and programming languages), and hence *cannot* be programmed. They exist at a level totally outside of, or prior to, the reasoning, digital, linguistic, description-generating capacities of our minds.

What picture of the world permits A.I. researchers, in the face of frequent setbacks, to remain so confident that computers can reproduce human intelligence? In studying this question, Dreyfus makes some of his most provocative and interesting points. He eloquently illuminates the philosophical bases of modern science, technology, computer science, and industry, and reveals the assumptions and biases culminating in the methods of A.I. research. Tracing this cast of thought back to Plato, he characterizes it thus: "...what cannot be stated explicitly in precise instructions -- all areas of human thought which require skill, intuition, or a sense of tradition -- are relegated to some kind of arbitrary fumbling" (p. xvi). He finds it again in Hobbes' *Leviathan:* "When a man *reasons,* he does nothing else but conceive a sum total from addition of parcels, ... for REASON ... is nothing but reckoning..." (p. xvii). He concludes that "Western thought has already committed itself to what would count as an explanation of human behavior ... a theory of practice which treats man as a device, an object responding to the influence of other objects, according to universal laws or rules" (p. 144). He states the following stern judgment upon this philosophy: "...the goal of the philosophical tradition embedded in our culture is to eliminate all risk: moral, intellectual, and practical."

Dreyfus points out that this reductionist viewpoint on the nature of man and human intelligence, however ordinary and familiar it may sound to us, is only one possible viewpoint, and has led us to make some assumptions which are not justified outside the realm of physics and the "hard" sciences. He makes explicit four major assumptions underlying A.I. research in particular:

A BIOLOGICAL ASSUMPTION, that the human brain, at some basic physiological level, employs discrete values in the same way as a digital computer;

A PSYCHOLOGICAL ASSUMPTION, that the human mind "can be viewed as a device" operating on discrete bits of information according to formal rules, again like a digital computer;

AN EPISTEMOLOGICAL ASSUMPTION, that all knowledge can be formalized," and "whatever can be understood can be expressed in terms of logical relations";

AN ONTOLOGICAL ASSUMPTION about the nature of reality and basic to the other three, that "all relevant information about the world, everything essential to the production of intelligent behavior, must be analyzable as...a set of indifferent, passive facts, each logically independent of all the others."

If these mechanistic assumptions are not adequate to explain human behavior, then what are the capacities that permit people to do the intelligent things that computers cannot do? Dreyfus suggests an attractive alternative viewpoint based on Gestalt Psychology and the philosophical school of Phenomenology -- fields which his arguments should motivate any thoughtful reader to examine more closely. He makes a good case for a primary nondigital or "analog" capability, which allows the human mind to accomplish what it does. To paraphrase Dreyfus' definitions, a digital device represents data by discrete states (e.g. a switch assuming two or more distinct positions), and gets a result by counting. An analog device uses physical quantities (voltage, duration, angle of rotation of a disc), proportional to the value to be represented, then combines these quantities physically and measures the result. He shows that many neurologists and psychologists lean increasingly toward postulating analog devices in the human brain, and a continuous, field-like mode of functioning in human perception and cognition.

Four major nondigital features are presented by Dreyfus as characteristic of, and essential to, human information processing. These are:

FRINGE CONSCIOUSNESS -- the ability to use the background structure of a gestalt within which objects of our conscious attention are embedded. For example, a chess player says of his opponent, "I notice that one of his pieces is not defended, the rook..." In so doing, he does not resort to a systematic inventory of all the pieces on the board, but perceives a high-level field of relationships all at once, at a glance, crystallizing around a single piece -- the rook -- to which his eye is drawn.

AMBIGUITY TOLERANCE, or *CONTEXT DEPENDENCE* -- the ability to deal with ambiguous situations without having to transform them by substituting a precise description. People are able to use complex, coordinated schemata of knowledge about the world, stored and retrieved in some unknown manner, to rapidly resolve ambiguity in any given situation.

ESSENTIAL-INESSENTIAL DISCRIMINATION, or *INSIGHT* -- the ability to select a constantly changing set of things in our cognitive world as important to us with respect to our current and ever-changing motivations and goals. This is, in fact, what a human programmer does for the computer when he plans a program: he prearranges matters so that only those objects and relations needed for the purpose of the program are singled out and described, leaving the machine with a simple formal (Class 2) problem to solve.

PERSPICUOUS GROUPING -- the ability to perceive structured wholes as elements, rather than exhaustively and mechanically searching through lists that spell out a higher-level pattern in terms of many atomic traits. Psychologists have been learning more about human and animal perception, and are demonstrating that we do not build up percepts additively from tiny units such as individual points of light on the retina. Instead, the visual mechanism works with much more complex elements: edges, moving horizontal or vertical bars, small or large areas of light or dark that expand or contract, etc. We are capable, further, of recognizing distorted or varying patterns directly, and not by successively and mechanically transforming what we see until it matches a stored template or ideal form. We can even recognize a "family resemblance" among objects, even though they may have no explicit single trait in common.

Dreyfus' last and most interesting point about human information processing concerns the crucial importance of our bodies and bodily skills, the fact that, "living in our bodies we have built up a motor space..." An essential difference between metal machines and "meat machines" (as some over-enthusiastic modern reductionists have called us), is that we are "embodied" in a way no digital computer can ever be. Thus, our experience of a tool we are using is essentially different from our experience of an object; the tool is an extension of our body, a "transparent access to the objects we touch with it." Dreyfus suggests that we learn to speak our native language in the very same way -- as a bodily skill (and this would certainly explain the relative difficulty of second-language learning, which must be accomplished long after our basic body schemata have been formed).

Thanks to these bodily skills, man is "at home in his world, has it comfortably wrapped around him, so to speak. Human beings are somehow situated in such a way that what they need in order to cope with things is distributed around them where they need it, not packed away in a trunk full of objects, or even carefully indexed in a filing cabinet. This system of relations which makes it possible to discover objects where they are needed is our home or our world" (p. 172). It is instructive to contrast our experience when we are forced to orient ourselves in a world where we are not yet "at home" -- learning a new game or skill, finding our way about under water or in a foreign city. For a while, in the new situation, we too must operate hesitantly, slowly, formally, and often quite ineffectually, like the digital computer.

Dreyfus is highly pessimistic about the degree of success attainable by A.I. researchers who base their work upon the set of assumptions he criticizes. He concedes that an "artificial embodied agent" might someday be developed, but only if it relied extensively on analog techniques not presently imaginable to us. He very briefly considers the possibility of a learning device, which might start out with an initial minimal "body schema" like that of a newborn baby: a tiny store of "facts" and some basic motivations as elementary as the baby's predilection for "nipples and smiles." It might then build up a respectable "world" in time under the tutelage of patient human mentors. I do not feel that he accords enough serious consideration to this possibility, which seems well worth pursuing (and, in fact, will undoubtedly be pursued in some form within the next few years). He dismisses it rather arbitrarily in the following words: "Computers can only deal with facts, but man -- the source of facts -- is not a fact or set of facts, but a being who creates himself and the world of facts in the process of living in the world... There is no reason to suppose that a world organized in terms of these fundamental human capacities should be accessible by other means" (p. 203).

The patient reader, having stayed with this review this far, may be asking himself, "Why should I care? What does all this matter to me, in my job or anywhere else?" First, I would like to convince you, the reader, that it all matters quite a lot to us, both as NSA employees, and also, in a wider context as thinking people caught up in the frenetic and often inhumane activities of a Western industrial society. We care at NSA because many of the things we will need to do in the next five or ten years will undoubtedly call for solution of some problems verging on the realm of Artificial Intelligence. Our requirements have always pushed the "state of the art" to its limits, and they may soon include such things as speech and language understanding, optical pattern recognition, and the handling of very large, organized knowledge bases. We are faced with essentially the same barriers of size and complexity as are plaguing A.I. research.

ARPA, the Advanced Research Projects Agency of the Defense Department, is in fact the major source of funding for A.I. research, and is at present under attack from several directions because its projects are not considered to be "paying off" as rapidly as they should be for the expenditures involved. The more pragmatic of Dreyfus' criticisms, even though they may be dismissed out of hand by A.I. workers, are echoed by others not so easily brushed aside, for example J. Lighthill (1973) speaking for the Science Research Council in England. If enough critics succeed in discouraging ARPA research, and A.I. work in general, some of the potential benefits for NSA that might have been around the corner may never materialize. One promising spin-off of A.I. technology, possibly within the next five to ten years, is a "super-intelligent terminal" based on a number of techniques whose feasibility has been demonstrated by current ARPA-funded projects. Such super-terminals might make our jobs a lot easier in the near-future world of computer networks and agglomerations of data bases.

Finally, I feel that, aside from the immediate practical feasibility or consequences of A.I. research, all of us should care about the more basic points Dreyfus has made. Our socieity bases all of its ways of doing things on the set of assumptions whose limitations Dreyfus so clearly exposes. A number of other books have been appearing lately that attack the scientific world-view and its philosophic bases; two that I strongly recommend to the brave reader are Roszak (1972) and Schumacher (1973). It is easy to dismiss such writers as irrational, romantic, impractical, or mystical. I find myself, somewhat to my sorrow, agreeing wholeheartedly with most of their fundamental points of view. I still cannot accept Dreyfus' pessimistic conclusion, that an "artificial embodied agent" or even, as a more immediately attainable goal, an "intelligent digital assistant," is forever impossible. I am also not convinced that such an undertaking must necessarily be a bad or perverse one, as Dreyfus obviously feels.

The criticism Dreyfus and others have raised should certainly not be used as an excuse to shut off A.I. research; neither should they simply be brushed aside. Instead, we should heed the clear warnings that our world is much too narrow, that we are in danger of leaving out all the truly important things, and that we must begin empirical explorations of some alternative approaches to human nature and human thought to supplement the digital computer model. In any case, it seems clear that the thoughtful reader, whatever his attitude toward computers and technology, can profit by conscientiously exploring Dreyfus' well-reasoned case for "What Computers Can't Do."

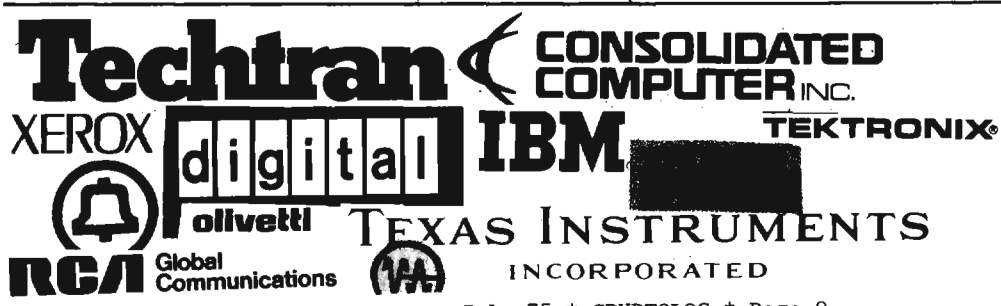
Dreyfus, Hubert L. (1965). *Alchemy and Artificial Intelligence.* RAND Corporation, Paper P3244 (AD 625 719), December 1965.

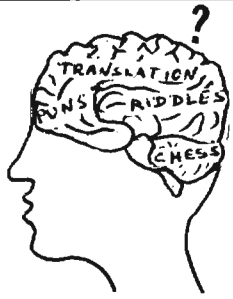
Lighthill, Donald (1973). "Artificial Intelligence: A General Summary," *Artificial Intelligence: A Paper Symposium.* Science Research Council Pamphlet, Science Research Council, State House, High Holborn, London, April 1973.

Michie, Donald (1974). *On Machine Intelligence.* Wiley, New York, N. Y., 1974 (Q335/M58).

Roszak, Theodore (1972). *Where the Wasteland Ends: Politics and Transcendence in Postindustrial Society.* Doubleday and Co., Inc., Garden City, N. Y., 1972.

Schumacher, E. F. (1973). *Small Is Beautiful: Economics As If People Mattered.* Harper and Row, New York, N. Y., 1973.





EO 1.4.(c)
P.L. 86-36

RAPIDTRAN

P.L. 86-36

G95

At the first meeting of the Crypto-Linguistic Association's newly-established Special Interest Group on Translation (SIGTRAN) on 22 January 1975, the guest speaker was [redacted] of B Group and his topic was "Free-Lance Translation."

During the course of his talk, he made the following comments: "The real truth on what you earn as a free-lance translator is not what you get per 1000 words. It's how fast you translate. If you write out everything in longhand, obviously you're not going to make much money. Even if you type your translation directly, you're not going to make much money."

This fiscal fact of life, plus "pressures at home," led him to an interesting solution. "I was forced to mechanize. And I soon found that you can double, triple, and quadruple your translating speed simply by reading into the dictaphone."

Then he added, "I have often wondered why people in this Agency who translate things that remain constant, [redacted] After getting good enough, the typist can even proof for you. I know of no instance in which that has been tried. I know of a number of specific areas where I believe it would work.

"While we do talk, and properly so, of the problem of having management understand us linguists, I don't know of any managers who have, as they perhaps should, challenged our production as linguists. If a linguist produces three translations or eight translations all day, the usual manager doesn't know enough about the linguist's problems or procedures so as to be able to make an effective judgment on whether that is a proper output in terms of time."

As the language coordinator for G9, the [redacted]

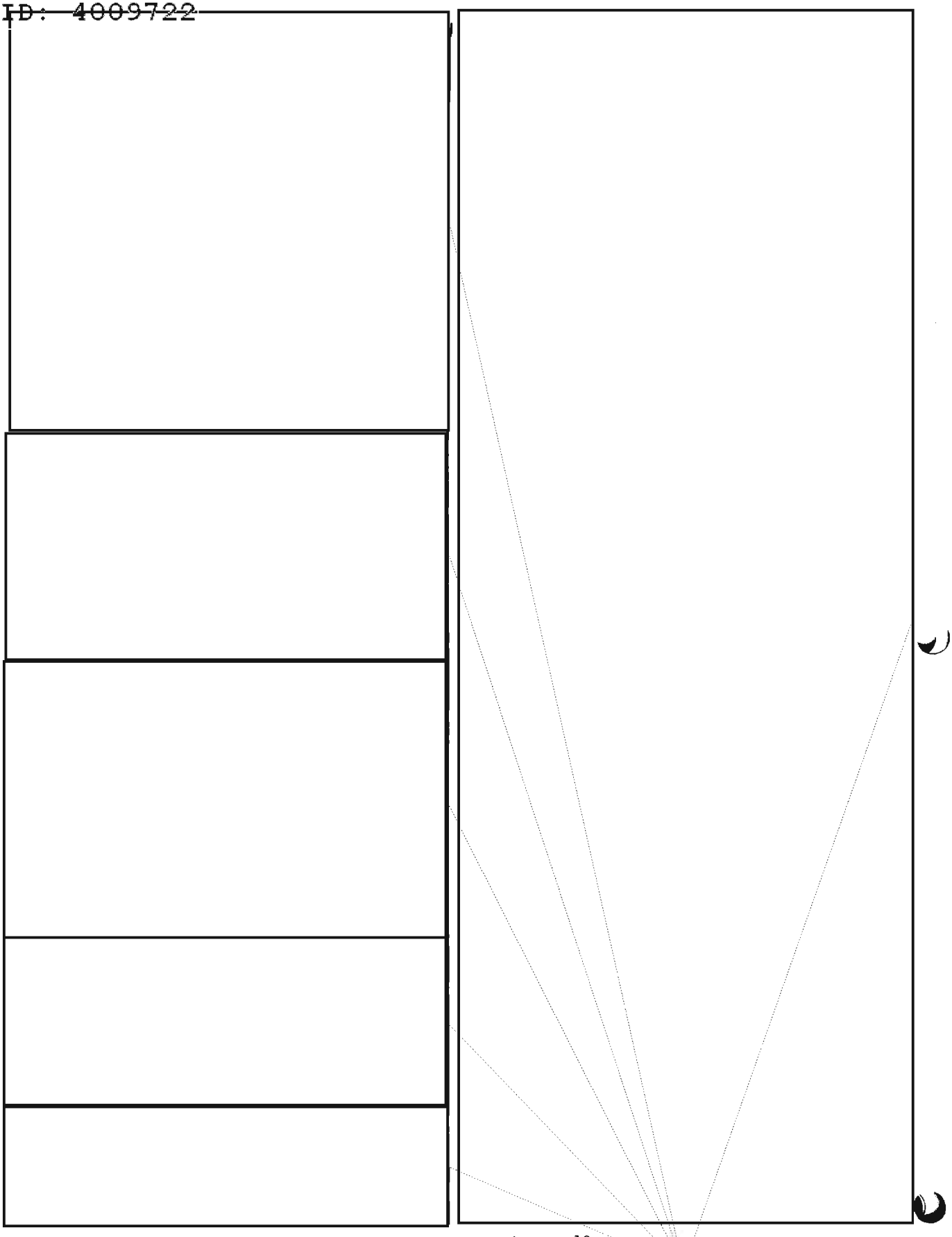
[redacted] I reacted to [redacted] refreshingly candid observations as though he had thrown down a gauntlet that we could not refuse to pick up. P.L. 86-36

[redacted]

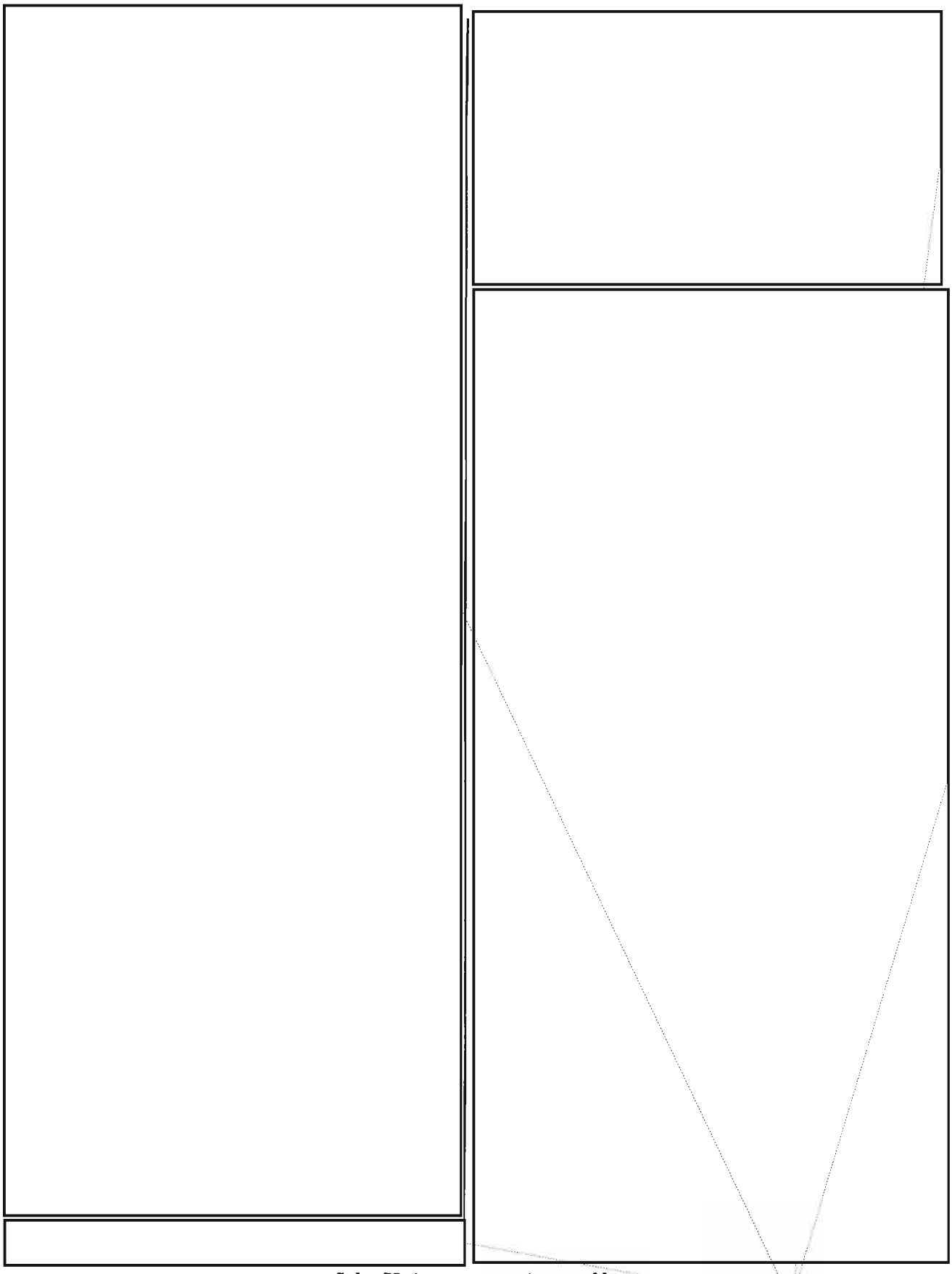
Freeing the SIGINT translator from the constraints of a pencil or typewriter was apparently attempted as early as 1946 by an enterprising Russian linguist by the name of Jack Gurin who was involved in the translation of [redacted] who decided to dictate his translations to a stenographer. He estimates that his output doubled the total achieved by the "traditional" method.

EO 1.4.(c)
P.L. 86-36

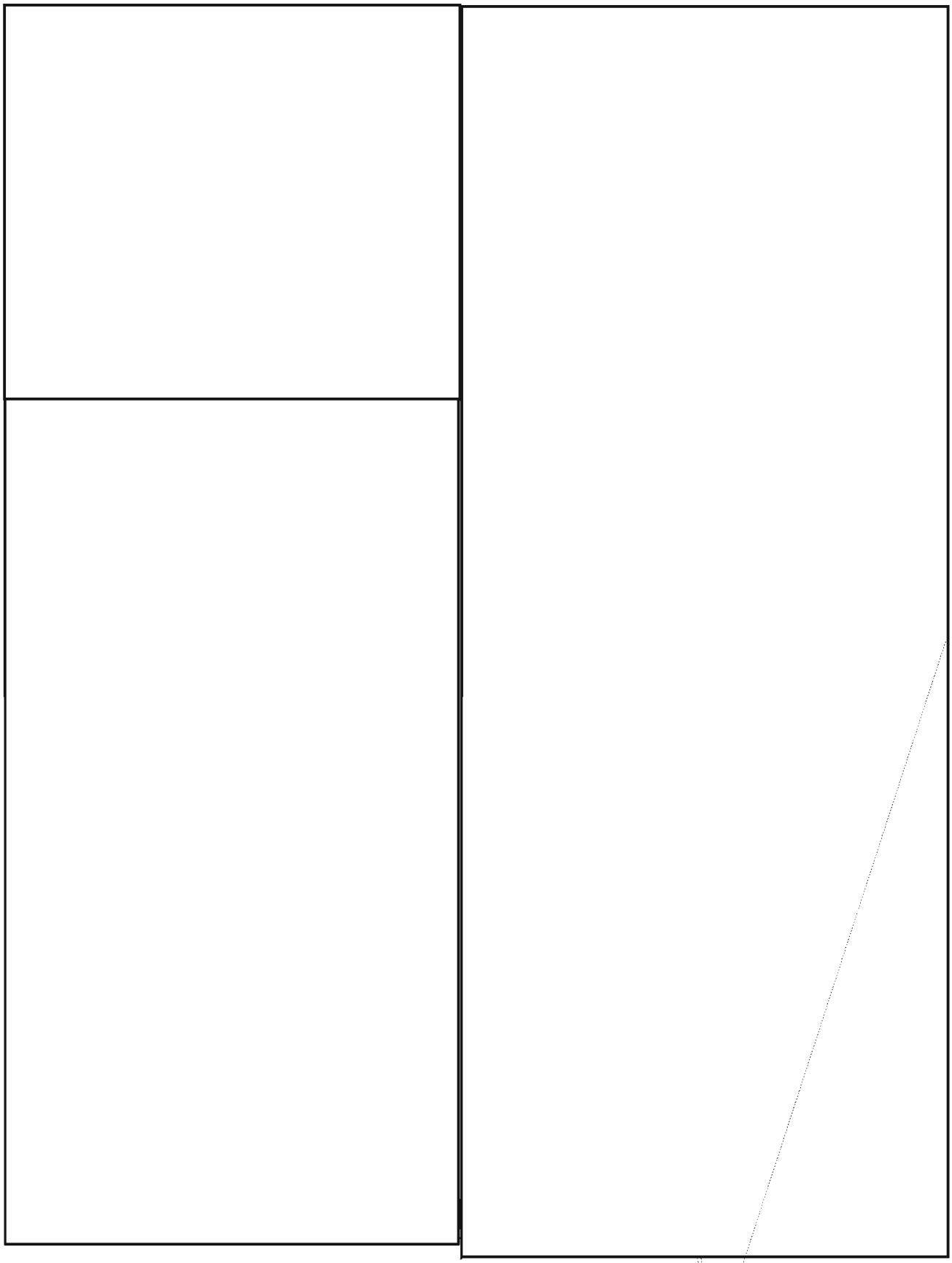
DOCID: ~~4009722~~



P.L. 86-36
EO 1.4.(c)



P.L. 86-36
EO 1.4.(c)



P.L. 86-36
EO 1.4.(c)

~~SECRET~~

NEWS BRIEFS FROM THE CMI AND CLA

At their respective annual banquets, held in May, the Cryptomathematics Institute and the Cryptolinguistic Association announced the following winners in their 1975 essay contests.

CMI Essay Contest

1st Prize ($100) -- [redacted] R51, "Cycles from Nonlinear Shift Registers" (UNCLASSIFIED).

2nd Prize ($50) -- [redacted] G93, "Linear Programming Applied to Manual Cryptosystems" ~~(TOP SECRET CODEWORD)~~.

3rd Prize ($25) -- [redacted] A54, "Symmetric Approximations to Boolean Functions" ~~(SECRET)~~.

CLA Essay Contest

1st Prize ($100) -- Doris E. Miller, P16, "Language and the COMINT Production Process" ~~(TOP SECRET CODEWORD)~~.

2nd Prize ($50) -- Emery W. Tetrault, P16, "U. S. Linguists and Language Capability Overseas" ~~(SECRET CODEWORD)~~.

3rd Prize ($25) -- Jacob Gurin, R54, "Examining Some Myths About Language" ~~(SECRET, HVCCO)~~.

Except for Mr. Gurin's article, which was published in *NSA Cryptologic Spectrum*, all the prize-winning articles were published in *NSA Technical Journal*.

P.L. 86-36

* * *

The CLA bestowed its Third Annual Sydney Jaffe Award upon [redacted] Chief, [redacted] Research and Support Organization). The citation reads in part: [redacted] total contribution to the large Russian language output of the Agency over the past 15 years is inestimable. He has insisted on maintaining the highest standards in language-based product in the face of a growing trend toward larger and more rapid production. At the same time he has moved to improve the rapidity of language support by mechanizing research files, combining them with those of collaborating centers, and preparing his own staff to deal with more difficult and more specialized language texts."

EO 1.4.(c)
P.L. 86-36

* * *

~~(SECRET -- HANDLE VIA COMINT CHANNELS ONLY)~~

¡CAMINO EN INGLÉS!

There are times when it is useful for analysts to scan the English meanings in a foreign-language glossary in order to find all the foreign terms relating to a given topic or set of topics. [redacted] For the off-line IBM-370 files, of which we now have a considerable number, a special program has been developed to provide a capability of this kind. The program retrieves and prints all entries whose English meanings contain one or more of a set of retrieval words specified by the user.

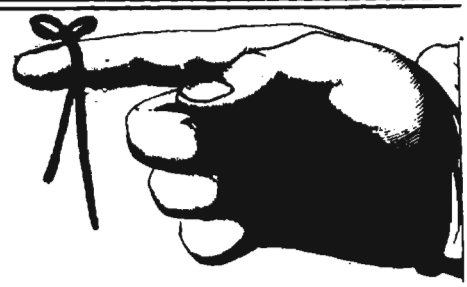
The program was developed in response to a request for any terms referring to various aspects of Electronic Warfare [redacted] The program can be run against any CAMINO file in the IBM-370 format. False hits can, in most cases, be eliminated by inspection of the full entry, and any remaining doubts can be resolved by the file executive. Users interested in trying out this English term retrieval capability are invited to contact [redacted] P16, x3045s.

~~(CONFIDENTIAL)~~

P.L. 86-36

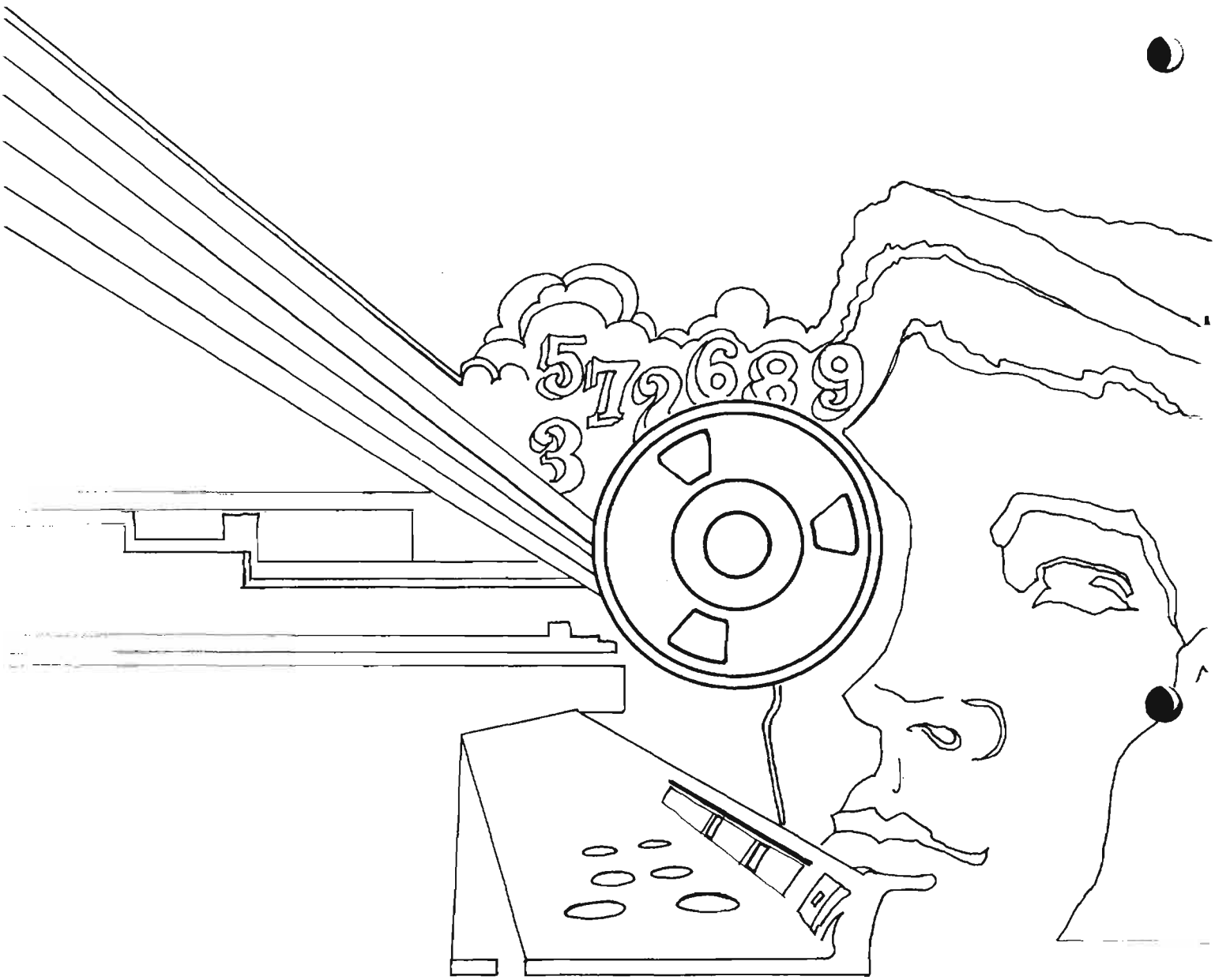
REMEMBER 15 AUGUST!

Not necessarily as the anniversary of the founding of Asuncion, Paraguay (1537), but definitely as the deadline for submitting your article to CRYPTOLOG for possible inclusion in the special "Vietnam Wrap-Up" issue to appear in October. Send your article to CRYPTOLOG Editor, P1. (U)



~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

P1-JL 75-S3-24000


5 7 9 6 8 9
3

DOCID: 4009721

P.L. 86-36

~~TOP SECRET~~ 2276

NATIONAL SECURITY AGENCY
FT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JUNE 1975

EO 1.4.(c)

P.L. 86-36

ELECTRONIC WARFARE ADVISORY ELEMENT..... [redacted] 1
MORE ON SQUARING THE PAGE.....Frederic O. Mason, Jr.....5
COMSEC FAMILIARIZATION: DO YOU NEED IT?.....8
WHERE DOES "DOES" COME FROM?.....Emery Tetrault.....9
THE NAVAJO CODE TALKERS.....12
[redacted] RADIOTELEPHONE CROSSWORD.....Thomas L. Engle.....13
PROFESSIONALIZING IN COMPUTER SYSTEMS..... [redacted] 14
PROJECT SYMBIOSIS.....016-22-723A.....17
LETTERS TO THE EDITOR.....19

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA (NSAM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526,MDR Case # 54778

DOCID: 4009721

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. II, No. 6 JUNE 1975

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief..... Arthur J. Salemme (5642s)
Cryptanalysis..... [redacted] (3571s)
Language..... Emery W. Tetrault (5236s)
Machine Support..... [redacted] (3321s)
Special Research..... Vera R. Filby (7119s)
Traffic Analysis..... Frederic O. Mason, Jr. (4142s)

Production Manager..... [redacted] (4998s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DOCID: 4009721

THE ROLE OF THE ELECTRONIC WARFARE ADVISORY ELEMENT (EWAE) OF N.S.A.

By James V. Boone, Chief, W

The following article is a slight revision of a speech given by Mr. Boone in February 1975 to the Capitol Club Chapter of the Association of Old Crows. The Old Crows are a worldwide organization of DoD, industry, and other technical and professional individuals interested in electronic warfare. Their name -- no disrespect intended -- is derived from the fact that, since the first aircraft sent on nighttime EW missions were painted black, the aircraft and then their crews were called "ravens" or "crows."

The 1973 changes to DoD Directive 3115.7 brought a new element of charter to the National Security Agency. That new element was the obligation to provide "SIGINT support to Electronic Warfare."

Prior to that time NSA had been providing such support, but it had been basically reactive and crisis-oriented. Whenever events of a highly volatile military nature occurred, the Agency was asked to provide any and all SIGINT available to explain the phenomena. But there was no designated focal point for EW problems, and the Agency's reporting tended to be fragmented and did not include the maximum interaction between the COMINT and ELINT disciplines that is necessary in this important field. No real attempt to provide long-term intelligence support to EW had been developed.

Further, a basic mistrust of Service Electronic Warfare existed in our SIGINT-trained and SIGINT-dedicated Agency. (How's that for a switch of "suspicion roles"?) The indefinite line between SIGINT and ESM [Electronic Support Measures] had been debated, cussed, and discussed again and again. One major problem at NSA was that there were very few professional military Electronic Warfare Officers aboard. Those who were assigned to the Agency were scattered through the various groups and hence tended to be ineffective. Of course, none were at any sort of policy level. (Same old story: "Don't know what this EW is all about, but I'd better have a guy that can at least spell it.") Compounding this confusion was the lack of a place at NSA where any of you Old Crows could call or TWX to start getting some idea of where an answer could be found, how to formalize requests, and what type of data could be provided.

Well, the problems were defined but the solutions seemed a long way off. Enter the Electronic Warfare Advisory Element (EWAE). The concept for this group was initially broached in November 1972. A knowledgeable Air Force Electronic Warfare Officer (EWO) from the Air Force Special Communications Center was trans-

DOCID: 4009721

ferred to NSA, and the struggle to create an EW focal point began. In spite of some real problems, fear of "rice bowl breakage" in many areas, and just plain red tape, a small group of four officers was brought together in mid-1973 and designated the EWAE.

One of their first tasks was to legitimize the element, establish its roles and authorities, and figure out how to attack what seemed to be an insurmountable problem: how to get the right SIGINT to the right people -- in the right way -- in some sort of reasonable time frame. In keeping with the legendary "slyness" of Old Crows, they hit upon a scheme that has stood up well throughout their existence. They decided to prove themselves by *deed*, rather than by *decree*. Using their knowledge of military service R and D programs, test and evaluation problems, operational tactics questions, and a myriad of other programs, they started to offer their assistance to see if any answers were available at the "fort." Many of you soon found out that, in most instances, it was a case of "suspicions confirmed" -- an NSA analyst had the necessary information, but didn't know that anyone needed it. (I should note here that some of your intelligence requests to NSA left more than a few questions in our analysts' minds.)

A significant milestone was reached when the Air Force agreed to place seven Electronic Warfare Officers in the organization, and the Navy provided two Naval Flight Officers with EW backgrounds. Since then, an Army billet and a Marine Corps billet have been added. As the personnel roster grew, so did the areas of work. After the usual nine-month gestation period, it was time to give formal birth to the new baby. Weaving their way through the many stops from their office upward, they finally arrived at the Director's office in May 1974. After formal presentations, stressing heavily their accomplishments and future plans, they received the green light from General Allen to proceed with his full support. This charter contained the important caveat that he wanted them to work across organizational lines at NSA to insure that our support was, in fact, SIGINT, rather than some lesser "INT" that was ignoring important pieces of the puzzle. In my own experience in trying to keep up with them, I know that they are (and in fact were, before formal approval) touching base with many Agency functions that were previously unaware of the kinds of things that are important to EW.

Perhaps before I go further into a discussion of some of my EWAE's achievements and programs, I should flash their credentials on you. First of all, they are professional *operational* -- rather than *intelligence* -- people. When I asked them to tell me how professional they really were, I think they were more surprised than I was. The seven Air Force, three Navy, and two Army officers presently assigned came up with the following figures: together, the flying officers from the Navy and the Air Force have 31,000 hours of flying time, over 7000 of which were logged on their 1,600 combat missions. Both of the Army officers have spent combat tours in Vietnam as company commanders. In combat operations the EWAE officers have received: one Silver Star, six DFC's, five Bronze Stars, 84 Air Medals, five commendation medals (with combat devices), two Vietnamese Air Crosses of Gallantry, and one Combat Action Ribbon.

Their operational backgrounds are equally impressive. Flying experience covers the gamut of our EW aircraft. ECM experience is represented from EB-66, B-52 (lots of this), B-58, AC-130 GUNSHIP, and F4C WILD WEASEL aircraft; ESM (or SIGINT, or whatever) experience is

What IS Electronic Warfare?

The official definition of EW (JCS MOP-95) is "EW is military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum and action which retains friendly use of the electromagnetic spectrum."

EW is a relatively new weapons systems component, having been developed in the early 1940's. In his memoirs, Winston Churchill said, "During the human struggle between the British and German Air Forces, between pilot and pilot, between AA batteries and aircraft, between ruthless bombing and fortitude of the British people, another conflict was going on, step by step, month by month. This was a Secret War, whose battles were lost or won unknown to the public, and only with difficulty comprehended, even now, to those outside the small, high scientific circles concerned. Unless British science had proven superior to German, and unless its strange, sinister resources had been effectively brought to bear in the struggle for survival, we might have well been defeated...and defeated...destroyed." Churchill called that secret war "The Wizard War," and we know it today as Electronic Warfare.

The secret war continues today, in greatly expanded scope, permeating every facet of military operations. Thrust and counter-thrust, Electronic Countermeasures (ECM) and Electronic Counter-Countermeasures (ECCM) go on throughout the world on a daily basis. To assure that the present U.S. "strange and sinister resources" receive the intelligence necessary to remain a step ahead of potential enemies, NSA must insure that the SIGINT support provided is timely and accurate, and fills the needs.

represented by flying time with many diverse U. S. Navy and Air Force programs.

And their staff experience is also impressive. The Chief of the EW/Photo Recce Division of 7AF (and later MACV [Military Assistance Command, Vietnam]) during the 1972 LINEBACKER bombing missions in North Vietnam is my current EWAE boss. His Crows have staff experience with HQ 7th AF, HQ PACAF Air Defense Analysis Center, USAFE collection and analysis, various bomb wing staffs, and tasking and mission planning for SAC's 55th Strategic Reconnaissance Wing. The senior Army EW has just returned from Korea, where he was the 2nd Division EW.

With these credentials I expect a lot of work out of my EWO's -- and they've lived up to my expectations. Their work covers the complete spectrum of EW. I'd like to give you a small sample of some of the programs -- many of which directly affect some of you -- in which they have insured that the best SIGINT available was supplied.

The Yom Kippur War. During the early stages of the October 1973 War the Israeli Air Force was taking it on the chin from some of the relatively unknown new SAM systems. The implications of their problems were directly pertinent to our own Navy and Air Force. If, for some reason, we became involved in the Mid-East, both of these services might have faced both the Soviet Navy and the Soviet air defense systems deployed in Syria and Egypt. Our RHAW [radar homing and warning equipment, which provides threat warning of SAM and AAA threats to the aircraft] and ECM people were stymied. Before they could make equipment changes to counter the threats, they had to understand the threats. This meant real-time reporting of any new intelligence about the systems -- particularly the SA-6[1]. The possibility that intelligence might be shut off from key service personnel by classification caveats became a real problem. The EWAE, recognizing this, initiated a series of reports that they called "Threat Parameter Messages." These messages, at the SECRET classification, reported any new defense-system information to U.S. military users on a real-time basis -- even while the formal reports were in the draft stage. The addressee list currently includes over 75 operational entities, predominantly in the Navy and Air Force. These messages were greeted with great approval by the operational forces and have been continued with increased distribution since the end of the war. As new systems appear, any and all parametric information available is being "flashed" to the guys that really need the information at a security classification that is useable.

[1]See CRYPTOLOG, April 1975, pp. 5-6

Support to the Continental Operations Range and Electronic Warfare Joint Test. In this activity, we fulfilled the need for a comprehensive understanding of enemy command and control. A team organized by the EWAE from three NSA Directorates participated with the range Intelligence Working Group to insure that the message simulation and replication necessary was "according to Hoyle." ELINT information was furnished to radar simulator builders. These efforts were recognized by letters of appreciation to the individual team members from the COR Op Commander, General Blood.

CROSSBOW "S" Committee. The CROSSBOW "S" Committee, chartered by the Joint Coordinating Committee on Defense Electronic Systems, is organized to study and make recommendations to the military services in matters concerning the development of threat simulators[2]. One of my EWO's acts as an advisor to this group. To date he has insured that the latest ELINT information on surface-to-air missile systems has been passed directly to these developers, instead of being hung up in a distribution system.

Navy EA-6B Program. For over a year my EW's have been working closely with the Staff of the Navy's EA-6B program at Whidbey Island, Washington. As the EA-6B is the only dedicated U.S. electronic warfare aircraft in the inventory, the proper use of the many types of jamming it can perform against specific threats becomes a critical operation. To assist these Navy planners, my people have insured that inputs of SIGINT data necessary to do the job right are constantly pumped to them. These efforts have earned the EW's and NSA a very nice letter of appreciation from Admiral Tierney of COMMATVAQWGPAC.

Air Force Special Communications Center. Our COMFY COAT[3] friends must be considered one of the key agencies in the EW game. To do their job they need all kinds of intelligence -- quickly, accurately, and with full implications of peripheral happenings in any given incident. To better help them get their job done, the EW's at NSA act as a focal point for any and all requests for information. During the last year we've answered over 200 separate inquiries. Further, to improve the exchange of information the EWAE played a significant role in getting NSA to place a permanent representative at the center. This representative, with his knowledge of the workings of NSA, has been beneficial to both agencies in getting the job done -- and to the best of our combined abilities.

[2]Simulation of enemy radar systems for use in training U.S. combat personnel.

[3]Nickname of a series of special reports and evaluations covering all facets of Electronic Warfare operations and training.

These are just a few examples of how the initiative and operational knowledge of my EW's has paid off. The payoff for NSA has been the exposure of our analysts to the real world of EW and its operations. The best-written intelligence request is a poor substitute for a face-to-face exchange between the user and the producer, but that is the system under which we are forced to operate. In the previously mentioned support areas, my EW's have participated with NSA specialists in many areas of expertise. The personal relationships that have developed have made a great impact on the direction of efforts by the NSA analysts. The old adage of "Don't ask questions, just do/give me what I say" does not fit our EW/intelligence interface world.

Some New Ideas

Two years ago, at the Old Crow National Convention, NSA presented a briefing on a computer-based catalog of ELINT parameters called KILTING. To my amazement I find many of you have never heard of the program. This "alive-and-well" catalog of everything from SIGINT worth knowing about threat, and other signals, is a must for almost all EW programs, be they ESM, ECM, or ECCM. The parametric tree that started out with just pulsed signals has now expanded to include CW signals, and a tree for inclusion of ECM signals is now being developed. This latter brings me to a subject that is really dear to my EW's. They have gone around NSA spouting such heresies as, "We really should understand Soviet EW capabilities" and "Why don't we collect some of that stuff once in a while?" Some initial reactions were "Even if I understand Soviet EW, what can I do with it?"

Now I know that ECCM is the poor stepchild of EW, but for those of you involved in it, I'll bet that a completely catalogued documentation, giving parametric data such as modulation techniques and other goodies, would be a godsend. How about you designers? Have you just built, or are you contemplating building, a radar, SAM system, AWACS, ESM gear, Terrain Following Radar, etc. that just happens to be completely vulnerable to enemy jamming? For you communication and data link experts, the impact is equally important.

So, undaunted by opposition, the EW's have supervised collection-tasking plans against non-U.S. radar and communications jamming. As these reported incidents come in, the information will be filed in the ECM tree of KILTING. I think that the EW community, as well as the intelligence community, will finally have a viable, useable, up-to-date catalog of what we know about the "bad guys."

On the other side of the coin is the need to know how best to get into the enemy's radar, communication, and control nets. How do we jam system "X" effectively? Where is the system's weakest link? What type of power, modulation, polarization, etc., will be effective? Now this need surfaces a little-known but easily understood fact: we jam *receivers*, not *transmitters*! Logically, then, we need to understand how the receivers work. But unless our friends supply us with some equipment to look at, or we stumble across a maintenance manual, this becomes a tough nut to crack. New threat systems are seldom at our disposal, and the first time we'll really try to jam them is when the balloon goes up.

Enter my EWAE again. How successful would we be, they asked themselves, if we took the external system knowns (such as SIGINT), gave them to a smart radar designer, and asked, "If this is what you transmit, how must your receiver work?" They called this study "Radar Performance Assessment" and later "Project HEADPIN." Starting with known (exploited) equipment, they constructed a tree into which pertinent information such as IF frequency and bandwidth, STC, and ECCM circuitry could be recorded. Project HEADPIN is alive and well, and initial product is becoming available. Due to the amount of calculations, estimations, and even WAG's[4] necessary in a program such as this, complete algorithmic documentation will accompany any Project HEADPIN product. The next step in the process will be to assess a new threat system with minimum knowledge of operating characteristics. It should prove interesting and can really get us involved in some interesting arguments, but at least it will provide a departure point for anyone involved in designing jamming equipment.

[4]An alternate expansion of this informal abbreviation is "very broad guess."

Who needs the EW-related information that NSA can produce? ESM and ECM planners, builders, and users need to know about enemy radar and communications systems. Counter-countermeasures planners, builders, and users need to know about enemy EW capabilities. Military operational planners need to know about enemy EW doctrine and employment, location of electromagnetic systems, and the capabilities of these systems against our forces. In summary, anyone who plans or performs the design, construction, or employment of electronic equipment is a potential user of some facet of SIGINT produced by NSA. The EWAE welcomes any questions, comments, or suggestions related to this support of the EW community. Please contact the EWAE (W07) at Extension 3610/3619s, or visit us in Ops Building 1, Room 3W136.

MORE ON SQUARING THE PAGE (A CRYPTO-TA FUNCTION)

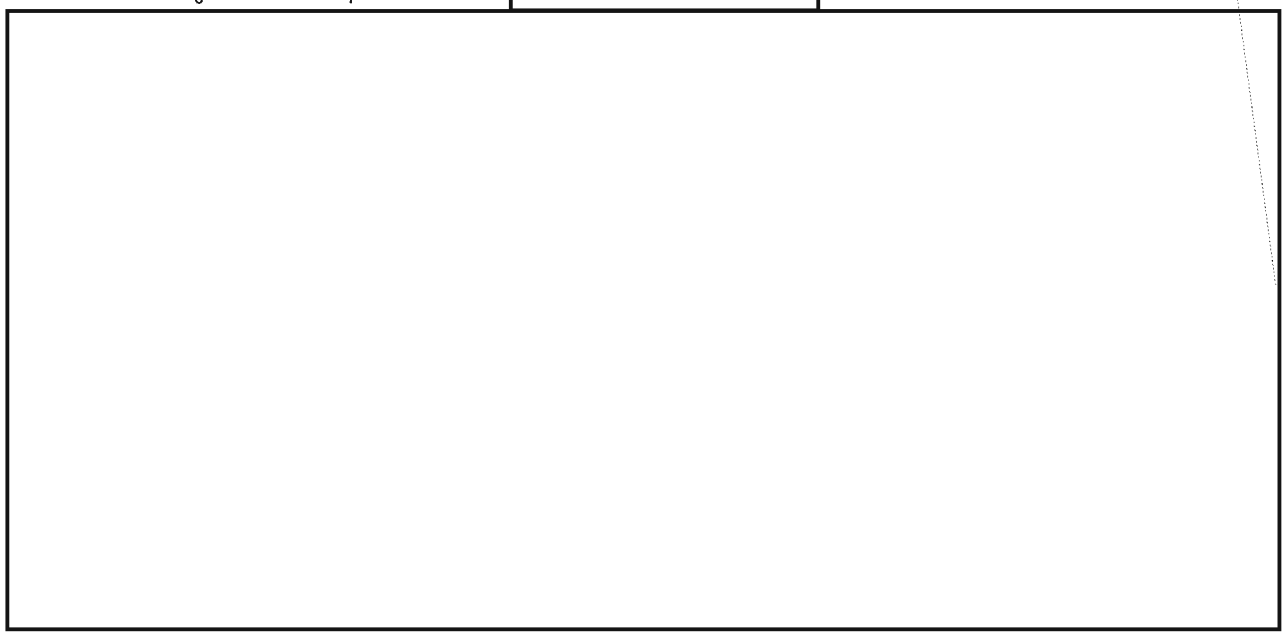
Frederic O. Mason Jr.

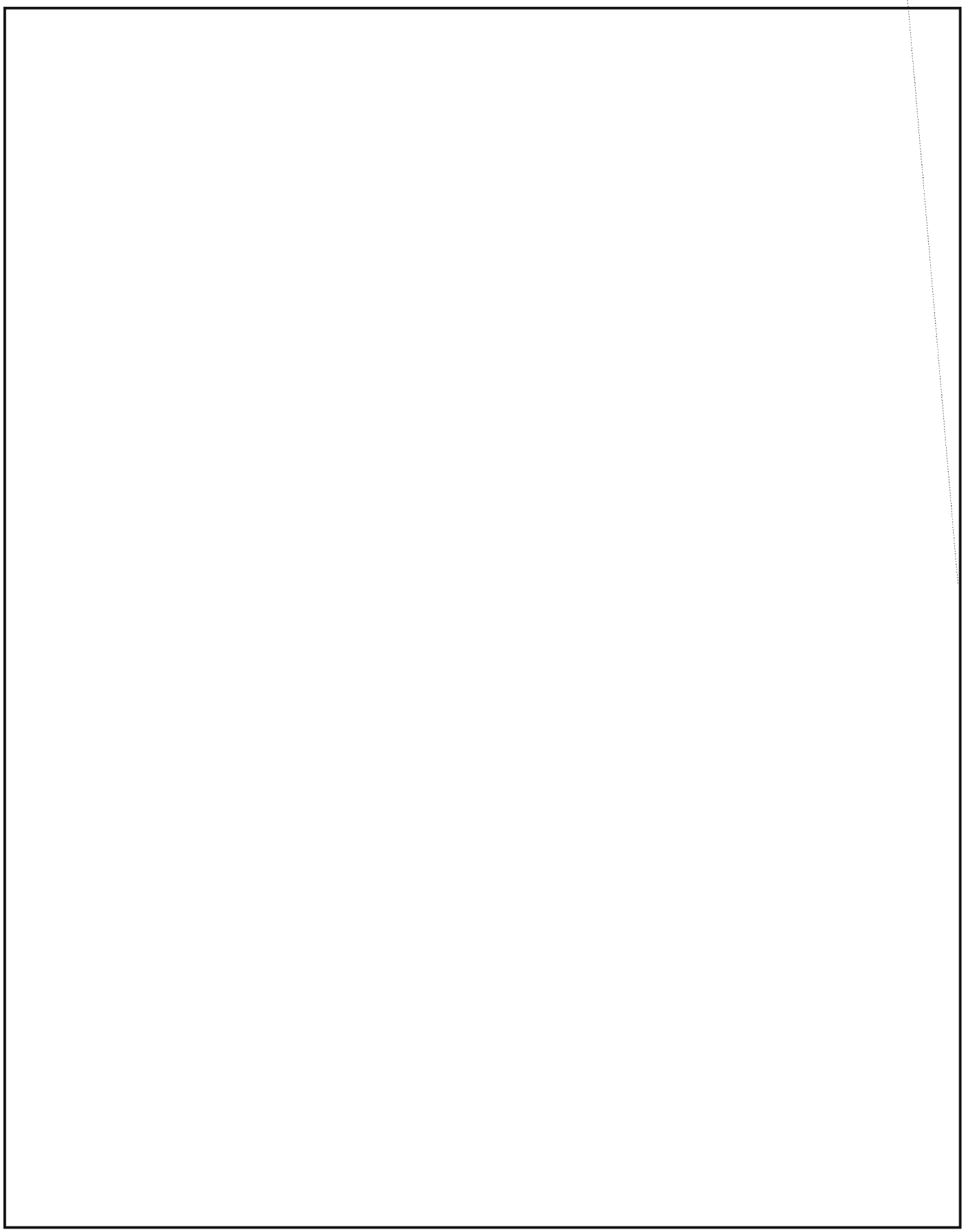
P11

In "TA, Handmaiden of CA" (CRYPTOLOG, May 1975) Mr. Mason presented a problem on squaring a callsign page. The answer to that problem is the following callsign page, or some transposition of it in which each row and column contains calls in one of the rows or columns shown.

EO 1.4.(c)
P.L. 86-36

And now for another problem:





EO 1.4.(c)
P.L. 86-36

IMPORTANT ANNOUNCEMENT!

Because of its personnel losses, S362 is no longer able to address Agency publications, including CRYPTOLOG, to individuals by name. Instead, it will send publications only to an organizational designation. S362 has agreed to use the following procedure with CRYPTOLOG's machine-printed mailing list: it will put into one package the total number of copies addressed to the same organization, and will enclose any machine-printed stick-on labels bearing names of individuals.

Please make sure that someone in your mailroom is prepared to receive these bulk shipments of CRYPTOLOG and is willing to slap the labels onto the individual copies, thus assuring that everyone gets his or her copy promptly. If your mailroom has suffered its own personnel losses and considers these extra few minutes' work an imposition, you might like to organize a "CRYPTOLOG labeling bee" each month.

Incidentally, the serial number that each copy of CRYPTOLOG now bears is NOT a document control number. It is a *production* control number used by S32 to check the total number of copies printed. (U)

DOCID: 4009721

EO 1.4.(c)
P.L. 86-36

COMSEC FAMILIARIZATION — Do you need it?

In going about your daily SIGINT chores in this Agency, have you ever given any thought to the other side of the coin--that is, to COMSEC? Have you ever had need to consider any of the following questions:

What is COMSEC? *Why* do we need COMSEC? *Where* do we need COMSEC and *where* can I find *what* is available? *Who* is working on COMSEC in NSA?...in the rest of the Federal Government? *When* should COMSEC be considered in any communications or in any SIGINT system? *Which* COMSEC equipments or systems could be used for *which* applications? *When* are the new developments in COMSEC equipments, systems, and doctrine going to be made available? *How much* COMSEC will I need and *how much* will it cost?

If you have never considered any of the questions, you are a prime candidate for CS-130; if you have considered them but cannot answer them right now, you are also a candidate for the course. CS-130 is titled "COMSEC Familiarization for Engineers," but don't let the title mislead you. The course is designed to provide a broad orientation in COMSEC to engineers, yes, but also to other technically qualified people working in COMSEC, SIGINT, or communications, who have only a sketchy knowledge of the subject.

CS-130 is offered twice each year to Agency personnel: in September and in January. It is a full-time course which lasts six days. In addition to guest lectures by Agency COMSEC authorities, there are tours of laboratories and "hands-on" demonstrations of the COMSEC equipments.

Up to now, CS-130 has been offered nine times to 270 students from Army, Navy, Marine Corps, Air Force, Coast Guard, civilian agencies, Defense agencies, and NSA. But only two per cent of the students have been from the SIGINT side of NSA. Maybe those in SIGINT just don't know the course exists.

* * * * * *

A typical course schedule is as follows:

Monday:

Introduction to Cryptography, The Threat to U.S. Communications, The National COMSEC Structure and the USCSB, [redacted]

Tuesday:

Digital Encryption Theory, COMSEC Record/Data Equipments, Computer Security, Transmission Engineering and COMSEC.

Wednesday:

Speech Encryption Techniques, Secure Voice for Combat Net Radios, Tour of COMSEC Engineering Laboratories, System Application of Cryptography.

Thursday:

Introduction to Research and Engineering, COMSEC Techniques, [redacted] Tour of Research and Engineering COMSEC Laboratories, [redacted]

Friday:

COMSEC Material Production, COMSEC Applications to Weapons Systems, Survey of NATO Cryptography, COMSEC Applications to Space Systems.

Monday:

COMSEC Resources, Physical Security, COMSEC Management and Summary.

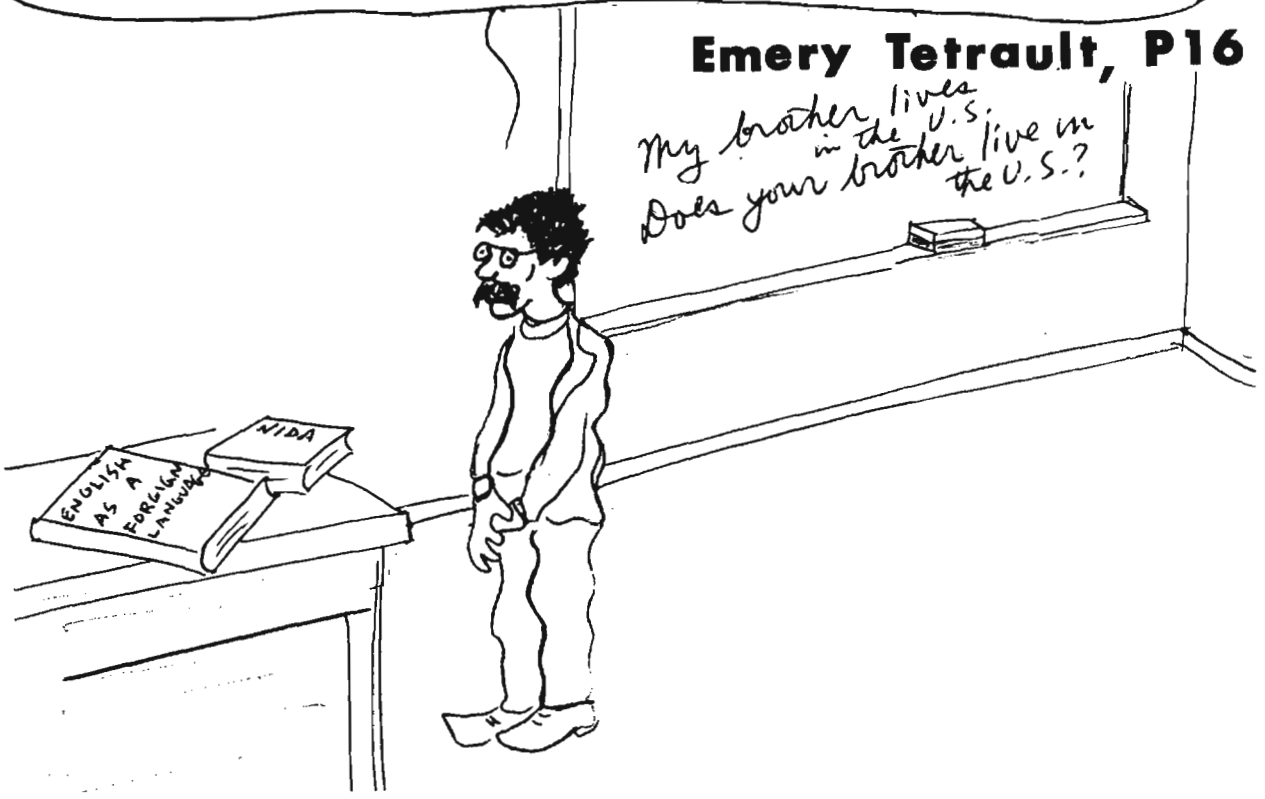
* * * * * * *

If the agenda whets your appetite, see your friendly Training Coordinator immediately; fill in Form E7687B; and send it forward through the proper channels. Then you will be in line for the next offering of CS-130 to Agency personnel--8 September 1975. Remember, COMSEC should never be an afterthought in the design and development of SIGINT systems.

E13 (NCS Cryptanalysis Department) can give you additional information about CS-130. Telephone ext. 8025s.

Where does "does" come from?

Emery Tetrault, P16



Maybe it's the ravages of spring or maybe it's nothing more than my normal tendency to be introspective, but I've been brooding lately about the applicability of linguistics to practical language work. Much of what is currently being discussed in the name of linguistic science smacks more of philosophy than science; what often passes for linguistic argumentation is more reminiscent of the Empiricist/Rationalist debate than of anything connected with human languages.

Nevertheless, people continue to work with real languages and they are interested in drawing useful inferences from language data. It is, therefore, not unreasonable to assume that the same people might be interested in some kind of systematic method or procedure for generalizing language data, whether this method be called transformational grammar, structuralism, tagmemics or whatever.

The story below may not seem especially enlightening for NSA language analysts. It's about English and most NSA employees already know everything about English. Moreover, it's about teaching English, something almost none of us does on the job (more irrelevance!). It does, however, illustrate what a linguistic method is and how it can be used.

A couple of years ago I was teaching a course in English as a foreign language and this experience provided an example of just such a method. The class was made up of Spanish and Korean speakers, with a Chinese (Cantonese) and a Frenchman included to make any contrastive approach unthinkable. The class was far enough along to permit fairly easy communication in English between instructor and students, and we were plowing through a review section devoted to positive, negative, declarative and interrogative sentences. The actual drill involved changing positive sentences to negative ones and it was proceeding smoothly, if not spectacularly, toward the coffee break when suddenly, as if in a dream, I heard the fateful words:

"Where does *does* come from?"

To understand what prompted such a question, we should back up a bit and look at what had been going on. All the sentences in the drill up to that point had contained a modal auxiliary (e.g. *can, shall, may, will*). The students were forming negative sentences by simply putting the word "not" after the modal, e.g.:

The new student can speak English.

The new student can NOT speak English.

It sounds pretty basic, but this is often the stuff that language drills are made of. Unfortunately, toward the end of the exercise someone slipped in a sentence without a modal:

My brother lives in the United States.

*My brother lives NOT in the United States.

(The asterisk indicates an incorrect or hypothetical form.)

In the question quoted above, my inquisitor was reacting to my somewhat irritated correction of what he had just uttered. Nonetheless, his question was a good one and it deserved an answer.

My first impulse was to fall back and regroup around the native speaker's true companion: "That's the way we always say it." I can still remember my Russian teacher extolling the beauty and logic of a structure in which numerals from two to four govern a genitive singular noun, even though adjectives within the same string continue to appear in the plural form (but not necessarily genitive). His most telling argument was that everyone he knew said it that way.

In a sense, our whole approach to teaching foreign languages has tended to make a virtue out of this kind of reaction. As a result it has become axiomatic among contemporary language teaching methodologists that language patterns, structures, usages, processes, or histories are not to be pointed out, discussed or *explained*. Otherwise, language learners (as opposed to students) are likely to be intimidated, or at least inhibited, and shut up like clams. There is a basic assumption that adult learners can, unaided, infer "rules" from language data; that is, from foreign-language utterances which are sorted out, graded for difficulty and repeated with only the minutest variations for an hour at a time. Perhaps this theory of second-language learning is based on observations of first-language acquisition in children. Nobody ever told my seven-year-old daughter about "does" but she gets it right all the time. To my knowledge she has never said anything like:

*Robert has NOT the funnies.

If little kids can get it right, so what's the big deal?

At this point (not in time, but in this narrative) I was literally saved, not by the bell, but by a gong announcing the coffee break. The moment of truth passed into awkward socializing and by the time we returned to class, the incident was apparently forgotten.

The next exercise in the book involved changing positive statements into yes/no questions. We went over the mechanics of the operation, which consisted of transposing the subject noun phrase and the auxiliary, and once again we set out across the minefield.

The new student CAN speak English.

CAN the new student speak English?

Mary WILL be at the party.

WILL Mary be at the party?

Pedro WORKS in Washington.

*WORKS Pedro in Washington?

Oh, damn! (inserted by instructor, not in text)

It was obvious that I was not going to escape. I leafed mentally through a number of possible explanations, lengthy and elegant descriptions filled with such locutions as "plus/minus modal," "deep structure," "deletion of AUX," etc., but in the end I decided to go over to the offensive (otherwise known as the Socratic method).

The key to the issue (as much for me as for the students) was to see the language as it really is, without imposing any preconceptions on it. It was plain from the material before us that the normal pattern in English is for the verb to consist of more than one word. All the negative, all the interrogative and all but two of the positive declarative "stimulus" sentences in the drill had the so-called "auxiliary slot" filled. If this is the normal pattern, then how can the anomalous one, the simple verb form, be explained?

One method, advocated by Eugene Nida among others, is to arrange such anomalous strings in a hypothetical form which replicates the normal or statistically prevalent pattern. Thus, it is possible to observe what happens to the normal pattern in such odd-ball cases and what environmental or contextual factors, if any, are associated with the anomaly. This is what we attempted to do:

The new student CAN SPEAK English.

Mary WILL BE at the party.

*My brother DOES LIVE in the United States.

*Pedro DOES WORK in Washington.

In the latter two instances, two things had to happen in order for us to get from the hypothetical to the real: (1) the DO form had to be deleted and (2) the inflectional suffix -S had to be moved to the other verbal element (the verb base), e.g.:

Pedro ~~DOES~~ work-S in Washington.

This operation, as trivial as it may seem to us native speakers, was not at all obvious at first to adult learners of English.

The next part of the analysis was considerably less trivial from any point of view. We wanted to be able to predict when the DO form stays and when it goes. Again, looking at sentences with DO forms in them, we finally noticed something (although not without some gnashing of teeth). The sentences with DO forms undeleted had the auxiliary slot *separated* from the other verbal element, e.g.:

My brother DOES not LIVE in the United States.

Robert DOESn't HAVE the funnies.

DOES Robert HAVE the funnies?

DOES Pedro WORK in Washington?

Our hypothetical forms (i.e., the "regularized" treatments of what had been simple verb forms) showed us that the deletion-plus-transposition process took place when there was no such separation between DO and the verbal element, e.g.:

*Robert DOES HAVE the funnies → Robert has the funnies.

(If you are wondering what we did about the emphatic use of DO, it was noted, but not developed beyond that point. The emphatic DO has been described as a different morpheme, because it differs in stress from the "other" DO form, but I did not feel that either the class or the instructor was ready for such diversions).

It would be foolish to claim that this anecdote illustrates in any comprehensive way "the" linguistic method. This leisurely passage of arms was little more than a brief skirmish in a remote and little-contested sector of the front. Nevertheless, it demonstrates some of the main features of any usable approach to language data.

A linguistic method is first and foremost a *discovery procedure*. It proceeds from observable facts (texts, transcripts, etc.) to a set of generalizations, not from invulnerable first principles to inevitable conclusions.

It is *objective*. The language should be allowed to speak for itself. My initial problem in explaining the English auxiliary-plus-verbal system was based on an unfounded assumption, namely that the simple form of the verb is somehow the base form from which all other verb "tenses" are derived. A proper analysis would have started with the observation that almost any valid sample of English sentences contains more multi-word verbs than simple verbs.

Finally, a linguistic approach to language data should allow us to *predict future language events*. This is the only kind of inference which has any practical value. My English students found it useful to predict the comings and goings of DO. Most NSA language analysts find that it is of inestimable value to have the ability to predict similar events in their operational languages. This is particularly true, since we are the *outsiders* in a communications exchange and since we must work with language materials which are both corrupt and incomplete most of the time. Given such job conditions, we need all the help we can get, starting with a rigorous and systematic way of dealing with the actual facts of a specific foreign language.

If in the past we have concluded that there is no practical way of applying linguistics to NSA work, the reason for this may be that we have been looking at the wrong kind of linguistics. Those of us who heard Dr. Esther Matteson of the Wycliffe Bible Translators at a recent CLA meeting could not help being impressed with the emphasis that she placed on linguistics, both as a method of rationalizing the translation process and as a method for discovering the forms and processes of a new language. It became increasingly clear from her talk and from the discussion period afterwards that she was not thinking about linguistics in terms of theoretical speculations on the universal nature of man's communicative competence, but rather she was referring to a data-based approach to natural-language phenomena. Maybe we ought to consider changing our brand of linguistics.

* * * * * * * * * *

In true schoolteacher fashion I cannot finish without giving an assignment: Which form of the French adjective, masculine singular or feminine singular, should be used as the base form from which the other can be predicted? If you have settled that question in your mind, how would you describe the process of getting from one form to the other? *One hint:* Don't be too concerned about spelling; concentrate on the way words sound. See E. Nida, *Morphology*, U. of Michigan Press, 1949, p. 75 for a fuller statement of the problem and also for the solution.

THE NAVAJO CODE TALKERS

The following article is reprinted, slightly condensed, from the February 1975 *Field Information Letter*, which had reprinted it from *The Wall Street Journal*, 12 December 1974. We think it is worth a page to confirm what has floated around in most people's minds as a vague and somewhat dubious legend of the COMSEC trade. A recent acquisition of the NSA Technical Library, *The Navajo Code Talkers*, by Doris A. Paul, tells the whole story.

Navajos weren't the first Indians used by the U.S. military to confuse foreign enemies; Choctaws transmitted orders by telephone for the Army infantry in World War I, and early in World War II Comanches were employed in similar activity in the European combat zone. But the Choctaws and Comanches conversed in their native tongues. The Navajos, on the other hand, developed a special coded alphabet of 38 symbols plus an auxiliary vocabulary of 41 other terms. It's been described by anthropologists Henry Dobyns and Robert Euler as "absolutely unbreakable."

Skilled as the Japanese cryptographers were, it's doubtful whether they would have understood Navajo even if there had been no attempt to disguise it. At that time it was virtually an unwritten language and even today few non-Navajos have succeeded in mastering its complex glottal sounds and vowel tones.

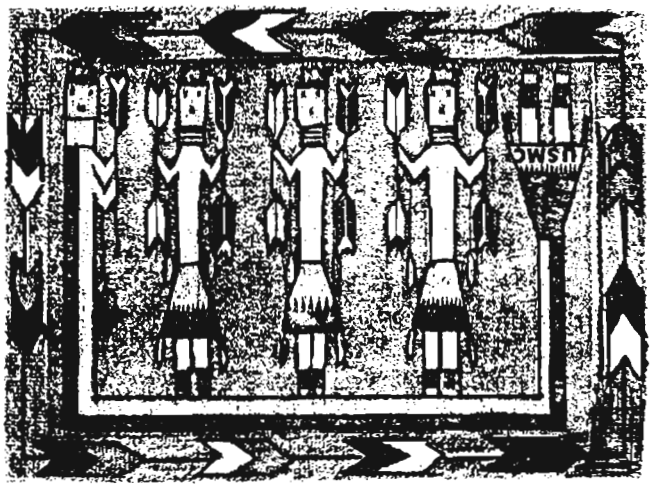
But rather than take a chance the Navajo code talkers improvised a system substituting clan names for military units, the names of birds for airplanes and fish for ships, plus a double alphabet when it was necessary to spell out proper names. The idea originated with a Navajo-speaking white man, Philip Johnston, an engineer with the city of Los Angeles who was raised on the Navajo Reservation where his father had been a missionary. During the first few months of the war, he suggested his plan to a high ranking Marine Corps officer. It was approved after five Navajos demonstrated its possibilities to Marine brass.

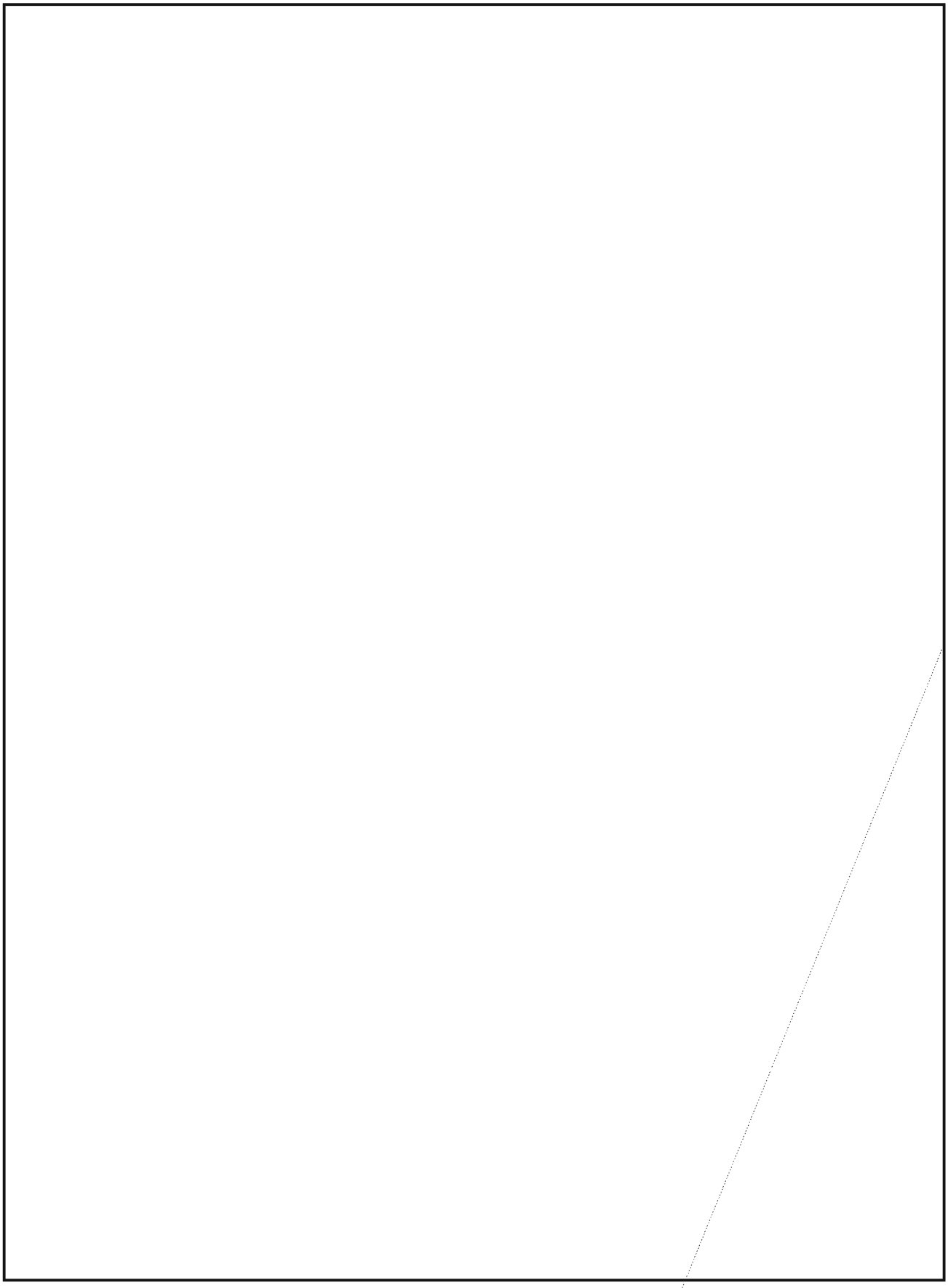
By April 1942, Marine Corps recruiters arrived at the reservation searching for Navajos who were physically fit as well as fluent in Navajo and English. The first group of volunteers, 29 youngsters from various boarding schools in Arizona and New Mexico, were sent to boot camp at San Diego. From there they were transferred to the Field Signal Battalion at Camp Pendleton, then assigned to Marine combat divisions throughout the Pacific.

Philip Johnston joined the Marines in the fall of 1942 and was put in charge of the code talker training program. Eventually some 320 Navajos served in combat under the program. Martin Link, curator of the Navajo Tribal Museum who is compiling records of the code talker experience, recently learned that four or five Navajos served in a similar capacity with the Army in North Africa, although details of that episode remain sketchy. In fact, information about the Marine Corps code talkers has only recently come to light.

The code talkers served in many campaigns, usually in two-man teams conversing by field telephone and walkie-talkie to call in air strikes and direct artillery bombardment. Marine Corps archives contain ringing praise for the Navajos from commanders in the field. It was exciting and dangerous duty, sometimes for unexpected reasons. William McCabe, one of the 29 original volunteers, was taken prisoner on Guadalcanal - by his own troops. Suspicious that the swarthy figure with the high cheekbones was really a Japanese soldier in a U.S. uniform, watchful Marines marched him at gunpoint back to his unit. From then on buddies in his unit assigned him a non-Indian bodyguard.

The idea for a formal association of code talkers grew out of the 1969 annual reunion of the Fourth Marine Division Association, which honored several of the Navajos. Two years later the Navajo Tribal Museum, the repository for Philip Johnston's papers and other code talker memorabilia, sponsored a two-day reunion. Now the Navajo Code Talkers Association numbers more than 100 members.





EO 1.4.(c)
P.L. 86-36

PROFESSIONALIZING IN COMPUTER SYSTEMS

By [redacted]

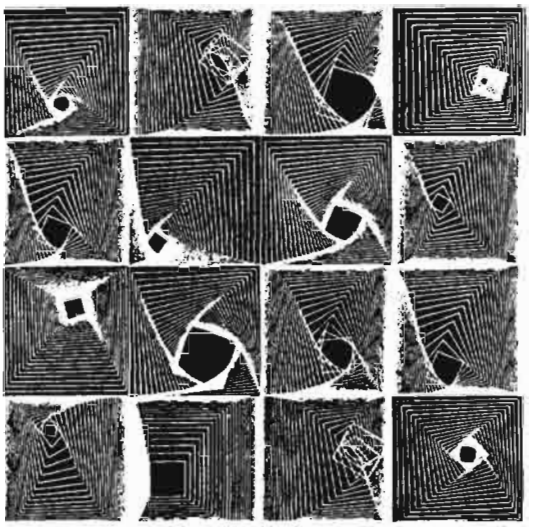
What is a computer systems professional? *Webster's New World Dictionary* defines a profession as a "vocation or occupation requiring advanced education and training, and involving intellectual skills.." and a professional as one "engaged in, or worthy of the high standard of, a profession."

In reading about professionalism one finds most articles center around two areas: background and standards. Background covers education, training, and experience in a field. Standards center on requirements, legal or otherwise, required by a society for one to be called a professional in a particular field. In the fields of medicine and law we find society acceptance of the definitions for background and standards, but what about other fields that have not existed, as these two have, for hundreds of years? In the newer fields, such as computer science, the quest for professional status is slow and full of conflicts.

In the computer field, there are many societies representing the different segments, and this causes a great deal of conflict. The Data Processing Management Association offers the Certificate in Data Processing. Various societies, ACM for one, have offered suggested academic programs leading to certification. Currently, the Society of Certified Data Processors (SCDP) is attempting to formalize the requirements in this area by means of state legislation. NSA and other government agencies and businesses have their own professional programs. All these efforts are contributing to the growth of professional status for the computer field, but they also arouse a great deal of emotion and conflict as to what constitutes acceptable background and standards, and what group should be the accrediting professional society.

How is a professional recognized? I quote a concluding paragraph from Jack Valenti's article in the Washington Post of 11 September 1971:

"Let me sit at a table or in a discussion where decisions are to be made and I can tell you quickly and accurately who the professionals are in the room. Dazzling rhetoric, intensity, passion, all these are of some measurable worth, but oftentimes they are the outer garments of the nonprofessional. The pro is the man or woman who knows what the issues are, has untangled the crossing threads of logic and reaction, understands the facts cold, has already searched the detail, and can, because he or she has prepared the necessary homework, bring forth the suggestion that usually makes the most sense. The professional may not always be right, but his experienced instinct is more formidable than the fellow who does it all in blind faith."



Computer drawing.

How does one become professionalized at NSA? The answers are contained in the memorandum, "Criteria for Certification (Computer Systems)" dated 4 January 1974 and available in the Panel Executive's office.

Obtain a copy of the criteria memorandum and review it. If you believe you are qualified, submit the necessary Professional Qualification Rating Schedule (PQRS) forms. Your background, experience, professional activity, and training are reviewed. Diversity of work experience, education and training, and professional activities and performance are assigned point values, as explained in the criteria, and the results of your initial evaluation are returned to you. If you are deficient in any area, you can intelligently plan your future to fulfill these requirements.

If 600 or more points are recorded, your records are forwarded to a three-peer professional review panel for what is described as a Qualitative Achievement Rating (QAR). The QAR panel is composed of one professional of your choice plus two panel appointees. A minimum of 200 points of the total 1000 required must be forthcoming from the review panel. During this period, if you have not previously written a scholarly paper in the computer field, you can do so under the direction of the Computer Systems Career Panel.

When you have completed a total of 820 or more points you can be scheduled for the Certification Examination. After accumulating 1000 or more points, writing an acceptable paper, and passing the exam, you are certified as a Computer Systems Analyst.

What is the Computer Systems Professional Qualification Exam (CSPQE)? It is a multiple-choice examination that attempts to measure objectively one's knowledge and awareness of the computer field and the computer environment at NSA. It is only a means of verifying the *other requirements* of professionalization as a Computer Systems Analyst.

The CSPQE has four categories: (1) Systems, (2) Applications, (3) Mathematics, and (4) General. The CSPQE test committee qualifies a question within each category as "NSA-specific" or "NSA-nonspecific." The question data bank is divided and identified into the four categories, with NSA specific and nonspecific qualifiers. (Questions are not identified by category on the exam itself.) Below is a matrix showing the current weighting for each category.

Category	Total Weight	NSA-Specific	NSA-Nonspecific
Systems	45	10	35
Applications	30	20	10
Mathematics	15	--	15
General	10	5	5
Totals	100	35	65

What this matrix says is that if 100 questions are used, 45 will be related to systems, and 10 of those will relate to specific NSA systems, such as TABLON. Information on such systems is obtainable from technical publications and lectures originating within NSA. The other 35 of the 45 should be answerable by anyone who possesses basic knowledge of the field and who keeps current with technical literature.

The SYSTEMS category consists of traditional computer-related topics such as hardware and software. Topics included are: language processors (assemblers, compilers, interpreters), language use/types (machine, procedure or problem-oriented), software engineering (top down design, structured programing), logic design, hardware components, computers (analog, hybrid, digital, mini- and micro-), operating systems, utility programs (I/O, maintenance, sort, merge), graphics and display technology, microprograming, data communications, system evaluation and improvement (profiling and performance measurements) and programing techniques (sorting, merging lists, hashing techniques, etc.).

The APPLICATIONS category contains items on specific disciplines. Emphasis is placed on how applications are planned, guided, documented and accomplished. Some of the areas, items, and techniques covered by APPLICATIONS are: systems analysis (systems studies, feasibility studies, decision tables, PERT charts, documentation packages, records management, implementation procedures, data structures and file design, data security and application system evaluation and improvement), business data processing (payroll, personnel records, inventory), education (CAI, CMI), CA, TA, languages and linguistics, TCOM, engineering and physical sciences, COMSEC, reporting transcriptions (project LAYAWAY), applications programing techniques,signals collection and signals analysis.

MATHEMATICS contains such topics as number systems, combinatorial and discrete math (including sorting, counting, permutations), statistics and probability, elementary algebra, Boolean algebra, numerical analysis (including error analysis and computer arithmetic), graphs, sets, coding, information theory, and metatheory (including formal logic, automata, formal languages). The CSPQE tries to test whether an applicant has knowledge of the types of mathematics that enable him to function effectively as a computer professional (i.e., computer-related mathematics).

The GENERAL category is a catch-all for items that are difficult to place in one of the previous categories. It includes such topics as: history, philosophical and social issues, (privacy, government regulations and control of ADP), operations research, security (NSA security and how it impacts on NSA computer personnel), administration and management (computer operations management), simulation and modeling, and professional issues.

The examination is under the auspices of the Computer Systems Career Panel, which has a standing Test Committee of approximately five Agency experts. It is offered twice a year, in March and September, with the restriction that an aspirant may sit for the exam only once each calendar year.

The exam consists of 100 multiple-choice items. The committee uses a randomizing program to aid in the selection of test questions in an attempt to avoid slanting the exam toward the committee's technical bias. In order to validate new exam questions the test committee may scatter additional questions in the CSPQE. Examinees are given two hours to complete 100 items; this time is extended by an appropriate percentage for any additional questions exceeding 100. To preserve the validity of calculations on any "new" test items, examinees are not informed which items are for test and which are for validation purposes. The new questions which pass the validation process are added to the test question data bank.

During the exam, examinees are encouraged to write comments in the test booklet (not the answer sheet); grievances concerning an item will be considered by the test committee. When the exam is ended, each test item is reviewed by the committee with the aid of an item analysis program. This provides the committee with vital statistics concerning the reliability of the examination in general and the suitability

of specific items. All decisions regarding the examination are resolved without looking at the names of the individual examinees.

The passing score is 55 percent. The scoring algorithm is R-W/3, where R is the number of items answered correctly and W is the number answered incorrectly; so that wild guessing is counterproductive. Results are announced approximately five working days after the examination.

What reference materials should be read? Sources of information for studying for the CSPQE are found in books, periodicals, reports and special studies, courses, seminars, professional society conferences, and lectures. In selecting materials for review it should be remembered that the exam tests the understanding and recognition of basic principles--breadth, not depth, of knowledge is stressed. For example, one is expected to know how lists work and are used rather than to code a complicated program using lists.

Excellent articles and books have appeared in increasing numbers since the early sixties. Currently, several abstract and bibliographic publications are devoted to technical material related to computers. Rather than spell out specific textual references for each of the categories on the CSPQE, which may be quickly outdated or result in "tunnel vision" in this rapidly-changing field, it is better to point out where to find related technical material. The Technical Library at NSA contains more than enough literature from which one can become an expert in any one of the exam categories. One *must* learn to use the library and learn how to scan for information in texts and periodicals. One good technique is to use the table of contents to choose areas of study that enhance your background. Do not merely plod through books without having established goals concerning what you wish to learn.

If time permits, courses are an excellent way to assimilate new material. A review of computer courses offered by local universities, community colleges, and the National Cryptologic School (NCS) reveals that a wealth of information is available. The most convenient is the NCS.

Some of the appropriate NCS courses for each category on the CSPQE are listed below.

SYSTEMS

MP160	Introduction to Computer Science
MP2xx	Any of the "computer-independent" languages available at NSA (FORTRAN, PL/1, COBOL, etc.)
MP3xx	Any of the "computer-dependent" languages available at NSA (IBM's ALC and JCL, CDC's COMPASS, Univac's Assembler, DEC's DOS and RSXIID, etc.)
MP1xx	Any of the information storage and retrieval languages available at NSA (Model 204, TILE, SPECOL, etc.)
MP4xx	Any of the seminar courses or software evaluation courses
MP410	Introduction to Computer Hardware
MP420	Introduction to System Software
MP430	Programing Techniques

APPLICATIONS

CY120	Survey of Cryptologic Skills and Techniques
EA100	SIGINT Technology
TA100	Basic Traffic Analysis
CA105	Introduction to Cryptography and Exploitation of Manual Cryptosystems (self-study, available through the Learning Center)

Any other specific disciplines

MATHEMATICS

MA012	Algebra (self-study texts)
MA111	Algebra (self-study texts)
MA144	Probability and Statistics
MA103	Introduction to Formal Logic
MA400	Introduction to Computer Science Mathematics

GENERAL

MP060	Survey of EDP
MC120	Cryptologic Management for Supervisors

In addition to formal help or information, you can get help from fellow professionals and from the many help/study sessions sponsored by the various offices within the Agency.

People have voiced both praise and criticism for the NSA Professionalization Program and for the recent changes to the criteria for certification. It can be pointed out that we do not live in a static society. Even in the medical area, one of the oldest professional groups, there is change afoot, as evidenced by recent controversies over heart transplants and acupuncture. NSA is a highly technically-oriented agency. Training at NSA, and by universities and vendors, is encouraged. The main ingredient needed by an NSA employee who has the ability to attain professional status is dedication: real interest in his field, and a willingness to devote time to the pursuit of his career.

For people not associated with NSA, the expenditure of personal time and money for professional status can be considerable. For example, the fee for the CDP exam, now administered by the Institute for Certification of Computer Professionals, is $85. To retake the entire exam or failed sections requires additional expenditures, and to take the review courses for the exam is additional expense. We at NSA are fortunate to have a defined and accepted professional program, where monetary requirements are minimal and where one is given both opportunity and encouragement to be recognized as a professional.

Reprinted from the December 1974/ January 1975 issue of C-LINERS

DOCID: 4009721

TOP SACRED
PROJECT SYMBIOSIS

I was recently accused of being a founder of the Church of the Latter Day Luddites, but I'm not. True, at times I've felt like John the Baptist crying in the wilderness. It's not that I dislike machines so much -- I guess that they have their place, but they think they know it all. To me there is little difference between a machine with one moving part and our most sophisticated computers. I've never been able to intimidate my car by kicking the tires. It only gets vindictive. This attitude, I realize, borders on paranoia, but the time has come. Those of us who are left must speak out. The line between humanism and mechanism must be clearly drawn!

My greatest concern is not that machines will communicate with each other and take over, but that their language and logic processes are becoming commonplace among us humans. Have you noticed the kinds of words we're using these days? Words either devoid of emotional content or slightly misused. I'm not talking about "irregardless" for "irrespective," but words having no literal meaning in the context in which they appear. Sometime check out the real meaning of *viable, interface, syndrome, feasible, mandate, parameter. . .*

Although word usage is, I suppose, not truly indicative of personality traits, we do seem at times to talk and write like unthinking automatons. And yet the purpose of human speech and writing -- the paragraph, the sentence, and, yes, even the individual word -- is to convey meaning. At least I always thought so. If you don't believe that, it's only an indication of the extent to which machines have already debased our natural subjective and emotional human instincts. Our machine-oriented environment tries, through all its media, to make us omit the subjective, omit the "superfluous" human element. In order to fit our answer into the keypunch holes allowed, we must be more "objective," more "concise," more "with it." And, in order to be more "with it," we tend to use the "in words," regardless of their meaning or appropriateness.

The other day, when I expressed these views, I was challenged. "Of course we're all right," my companion said. "How could machines take over? You've really got a thing about those inert pieces of equipment." The gauntlet having been flung, I decided to write a short piece that would be understood by a machine and that, in addition, would probably get an instinctive nod of approval from a large percentage of the people in the Agency. Not because they understood it, but because they couldn't convince themselves that they didn't.

Take the following paragraphs of a draft report:

> Based on integral subsystem considerations, Project SYMBIOSIS is designed to provide a large portion of the interface coordination communications needed for automatic text processing. In respect to specific goals, a constant flow of effective information must utilize and be functionally interwoven with the evolution of specifications over a given period of time.
>
> A primary interrelationship between system and/or subsystem technologies presents extremely interesting challenges to the anticipated fourth-generation equipment.
>
> In particular, the characterization of specific criteria maximizes the probability of project success and minimizes the cost and time required for the subsystem compatibility testing. On the other hand, the initiation of critical subsystem development requires considerable systems analysis and trade-off studies to arrive at the total system rationale and the fully integrated test program necessitates that urgent consideration be applied to the philosophy of commonality and standardization.

All right, now, be honest. Wouldn't 60 percent of the people in the Agency have initialed the above garbage? And yet, except for the first sentence, it was "generated" randomly from the "Simp tables" printed on the next page.

If human beings respond to this sort of stuff, so do machines. In fact, a programmer's software toy called DREKGEN can grind it out in any volume desired. Here is a sample output:

PHILOSOPHY OF PROGRAMMER MANAGEMENT

WITH A VIEW TOWARDS THE SOLUTION OF CER TAIN DIFFICULTIES TRAINING PERSONNEL, INS TRUCTORS AND SUPPORT PEOPLE ORDINARILY CO ULD BE EXPECTED TO MINIMIZE EDUCATIONAL E FFORTS TO OPERATORS. AS REQUESTED BY HIG HER MANAGEMENT MIDDLE LEVEL MANAGERS ORDI NARILY COULD BE EXPECTED TO MINIMIZE EXPA NSION AND IMPROVEMENT OF WORK AREAS. SEN IOR DATA PROCESSING MANAGERS, WHILE SEEMI NGLY PASSIVE, ARE QUITE CONCERNED ABOUT P LANS TO ENHANCE TESTING AND PROPER CATEGO RIZATION OF PROFESSIONALS. ON THE BASIS OF INDEPENDENT STUDIES, THE LESS THAN ADE QUATE EMPLOYEES MUST STRIVE TO AVOID TRYI NG TO ENHANCE ROTATION AND REASSIGNMENT O

F SUBJECT PERSONNEL. THOSE WHO WORK WEEK ENDS AND ALL SHIFT WORKERS ARE BELIEVED T O BE OPPOSED TO ANY EFFORT TO REJECT ROTA TION AND REASSIGNMENT OF SUBJECT PERSONNE L. AS REQUIRED BY DIRECTIVE OR REGULATIO N TRAINING PERSONNEL, INSTRUCTORS AND SUP PORT PEOPLE ARE BELIEVED TO BE OPPOSED TO ANY EFFORT TO RECALL FOR REDESIGN AND FU RTHER ANALYSIS RETRAINING OF OBSOLESCENT PERSONNEL. THE LESS THAN ADEQUATE EMPLOY EES DESPITE PERSONAL RESERVATIONS SHOULD TRY TO OBVIATE ROTATION AND REASSIGNMENT OF SUBJECT PERSONNEL. AS REQUIRED BY DIR ECTIVE OR REGULATION THE REALLY BRIGHT WO RKERS, THE INNOVATORS, MUST STRIVE TO AVO ID TRYING TO INCREASE REDEFINITION OF CER TAIN TASKS, PROJECTS AND AREAS OF ASSIGNM ENT.

I ask you, have we been subverted?

If any of this has caused you to think twice, then join us. We ask only that language be used to convey meaningful ideas, not to obfuscate or to demean our capacity to co-exist with the UNIVAC-1110 and the electric light bulb.

I realize that machine feedback is insidious (and insipid), spreading like the reams of paper it produces. Still, just because we can't beat them, that doesn't mean we must join them. Let the machine serve our better interests. There is no need for us humans to adopt the machine's idioms. I'd much rather retreat into the English language than submit to fluency in FORTRAN.

Anonymous (but those @°#*! machines know my number: 016 22 723A)

Department of GOLDEN OLDIES

The reader who submitted the following item picked it up at GCHQ in 1971 but does not remember who originated it. No one here, including UKLO people whom we asked, knows anything about it, or even what "Simp" means. Does any reader have any more details?

The "Simp tables" are so designed that the writer can choose phrases randomly from Tables A, B, C, and D in sequence (or, for variety's sake, from B, C, and D) to create sentences that look valid, but are entirely devoid of meaning. Try your hand at it! Fool your friends! (To make your phony sentences look less suspect, we have changed British spellings with "s" to American spellings with "z.")

Simp Table A

1. In particular,
2. On the other hand,
3. However,
4. Similarly,
5. As a resultant implication,
6. In this regard,
7. Based on integral subsystem considerations,
8. For example,
9. Thus,
10. In respect to specific goals,

Simp Table B

1. a large portion of the interface coordination communications
2. a constant flow of effective information
3. the characterization of specific criteria
4. initiation of critical subsystem development
5. the fully integrated test program
6. the product configuration baseline
7. any associated supporting element
8. the incorporation of additional mission constraints
9. the independent functional principle
10. a primary interrelationship between system and/or subsystem technologies

Simp Table C

1. must utilize and be functionally interwoven with
2. maximizes the probability of project success and minimizes the cost and time required for
3. adds explicit performance limits to
4. necessitates that urgent consideration be applied to
5. requires considerable systems analysis and trade-off studies to arrive at
6. is further compounded, when taking into account
7. presents extremely interesting challenges to
8. recognizes the importance of other systems and the necessity for
9. effects a significant implementation of
10. adds overriding performance constraints to

Simp Table D

1. the sophisticated hardware.
2. the anticipated fourth-generation equipment.
3. the subsystem compatibility testing.
4. the structural design, based on system engineering concepts.
5. the preliminary qualification limit.
6. the evolution of specifications over a given time period.
7. the philosophy of commonality and standardization.
8. the greater flightworthiness concept.
9. any discrete configuration mode.
10. the total system rationale.

~~CONFIDENTIAL~~

LETTERS TO THE EDITOR

To the Editor, CRYPTOLOG:

With reference to the complaint [See Letters to Ed., Apr 75] that "bookbreakers" were discriminated against in the professionalization program, it seems to me that the persons most discriminated against are those who are or were what I would call "country specialists." I don't know where else the system existed, at least, was assigned to country analysts who for their areas would scan plaintext, make intelligence evaluations, and translate or report, as the occasion demanded, the traffic selected by themselves. Quite often they even had to log their own traffic.

In pre-professionalization days these people were given no recognition, pecuniary or otherwise, by the rest of the Agency for their versatility. With the coming of the professionalization program, they were even penalized because they had not specialized in a fraction of what they were doing.

EO 1.4.(c)
P.L. 86-36

G514

Ed. note: informs us that, since he is professionalized both in the language field and in the SRA field, he has no personal grievance, but seeks only to achieve a more equitable situation in the system as a whole.

To the Editor, CRYPTOLOG:

I take serious exception to cavalier dismissal [See Letters to Ed., May 75]of what is, after all, the basic SIGINT skill as no more than a preliminary scrubbing of traffic before the real analyst -- the bookbreaker -- It's praiseworthy to be loyal to one's profession, to one's own mission. Belittling the profession of those who do not share one's views on a given subject is hardly the way to convince an audience of the rightness of those views. It is more likely to convince that audience of the biased and nonprofessional outlook of the person who states them.

(Name withheld by request)

P.L. 86-36

To the Editor, CRYPTOLOG:

I would like to express my appreciation to [redacted] for his most effective statements in the April 1975 issue of CRYPTOLOG on our agency's need to develop a human medium for dissemination of our product. Although his statement of the need for oral reporters was well made and his suggestions for the development of oral-reporting props was most informative, there was one aspect of the article which I found lacking -- where do oral reporters come from?

In differentiating oral reporters from "briefers" the main theme developed by Mr. [redacted] seems to be that oral reporters *know* what they are talking about. Unfortunately, within our agency (and the world at large, for that matter) people who know what they are talking about are at a real premium. All the mechanical, audio-visual techniques which enhance oral reporting can, with proper emphasis, be taken care of. The high-level exposure which oral reporting offers relatively junior-grade employees should be a considerable career incentive which would make an oral-reporting assignment attractive. The crux of the oral-reporting problem is not the discovery, development, and motivation of people with the physical and emotional attributes necessary in an oral reporter. The problem is finding people who are *genuine* experts.

While the present career-development system in NSA may not offer the proper incentives to "briefers," it offers even fewer incentives for people who develop into experts on a given target. In current career-development patterns, diversification has become an obsession. The stable in-depth human data bases (little ol' people in tennis shoes) who have been the mainstay of the agency are now held in contempt, are rapidly disappearing, and are not being replaced. "Management" now appears to be the greatest virtue for rapid rise in the agency. The smart young FSG (future super-grade) certainly does not want to become stereotyped as an expert on some particular problem for fear of becoming "an invaluable human resource" stagnated at one grade forever.

[redacted] mentions in his article the "same few people" who always go downtown. Obviously we need more of them. We need more people who are real authorities, but in my experience there are very few middle managers in the agency who have had any desk-level analytic experience within the actual problems that they are managing. Frequently there are lower-grade analysts within their organizations who know more about the given problem than does the chief of the element. In this situation there is little incentive for a lower-grade analyst to develop himself or herself into a real expert. The prime goal of career development is to get out before you get stuck (the intern program, CY-100, a staff job). I believe that these are aspects of agency career development that must be seriously reassessed. Soon we may become an agency of managers, managing nothing. While avoiding overspecialization the agency must somehow place a premium on, and develop, specific problem expertise within the work force. If we have more people within the work force who really do *know what they are talking about*, then the development of oral reporters will take care of itself.

[redacted]

P.L. 86-36

NSA VIETNAM WRAP-UP

The entire October issue of CRYPTOLOG will be devoted to the Vietnam War and its significance to NSA -- achievements, failures, lessons learned, problems unresolved. The Editorial Board invites contributions from readers for possible inclusion in that special issue. Send contributions to Editor, CRYPTOLOG, P1 by 15 August 1975.

If you have valuable information to impart, but feel that you need help in getting it on paper, please get in touch with any of the members of the Editorial Board. We will try to think of a way to get your information into that issue -- perhaps by transcribing your tape-recorded remarks, question-and-answer interview, etc.

[redacted]

P.L. 86-36

Memo from

Chief, PI

3 June 1975

Doris Miller, the first editor of CRYPTOLOG, retires this month. She was much more than the Editor -- she brought CRYPTOLOG along from a flight of our fancy, through frequent and troublesome growing pains, to the lusty, squalling youngster it is today. Of course she had help -- not as much as she needed, but lots of it. All of us connected with this publication know it could not have been brought off successfully without her.

Doris Miller's uncommon good taste, her instinct for newsy and readable subject matter, her gift for persuading people to write "just a little -- even a page or two," and, above all, her indomitable spirit in the face of obstacles were the talents needed to bring CRYPTOLOG into being.

Eighteen months ago she advocated a publication in DDO, written by technicians for technicians, informal, newsy, controversial, lively and timely, to be published -- would you believe -- every month. This issue of CRYPTOLOG puts the capstone on the uncommonly productive NSA career of Doris Miller.

We wish her a busy, productive retirement and the joy of facing each new date with never a worry of deadlines. Doris, we'll miss you!

William Lutwiniak

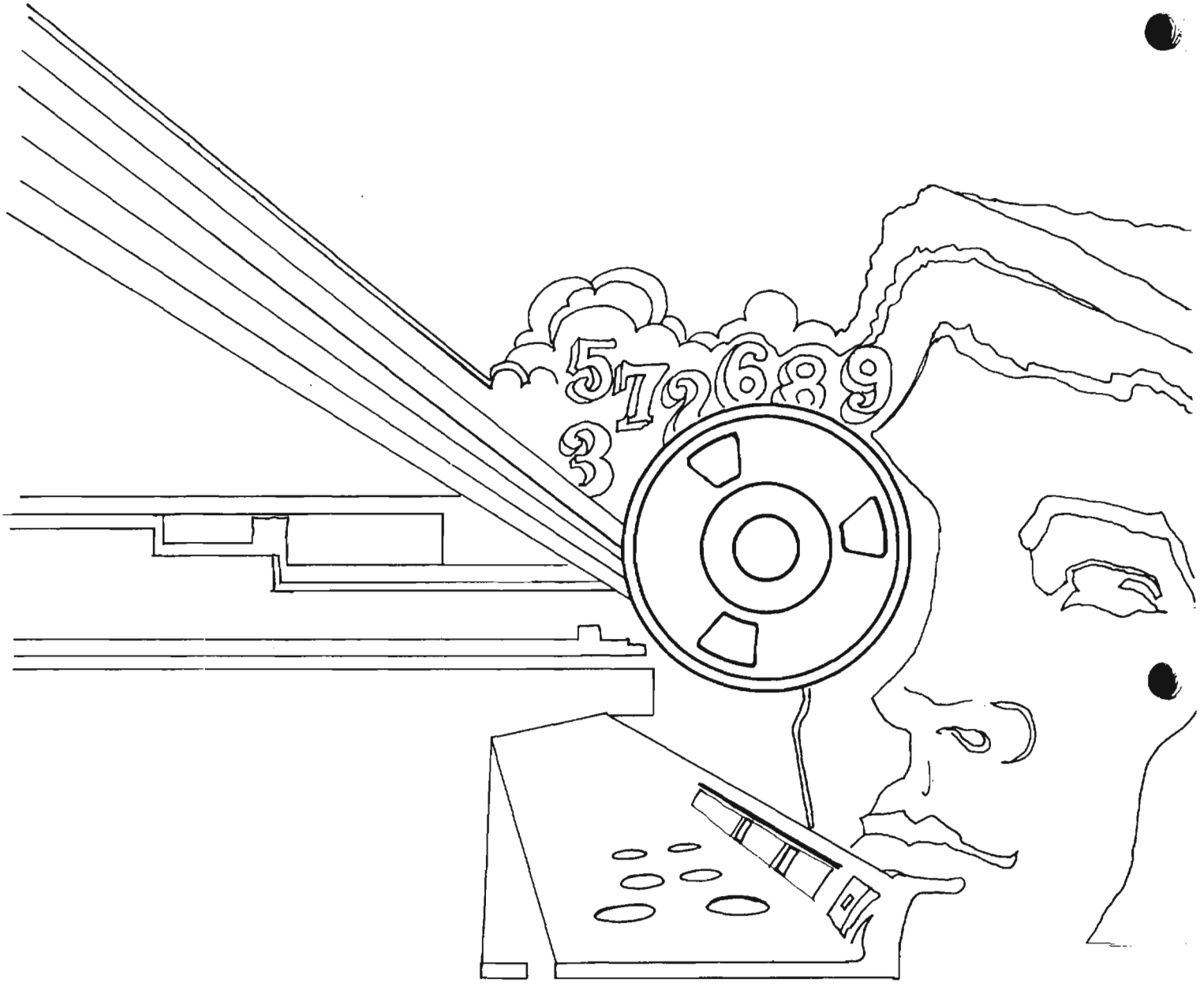
Publisher
CRYPTOLOG

The power of the comma! A few weeks ago I accepted Doris's offer to become Art Editor, and one week later I became Art, Editor.

As thoughtful of others as she has always been, Doris had roughed out the June issue before announcing her intention to retire. Therefore I was able to rely on Doris many times for guidance as the issue got de-roughed-out. If there is anything about this issue that you like -- the articles, the layout, etc. -- thank Doris. If there is anything about future issues that you like, it will be largely because of the fine start that Doris has given CRYPTOLOG and also because of the continuing support given to it by Mr. Lutwiniak, by the editorial board, and especially by CRYPTOLOG's ever-growing and ever-responsive readership. I hope that I can be as successful as Doris has been in getting you NSA technicians to share your best ideas with your fellow NSA-ers in all technical fields, at all levels.

Art,

PI-JN 75-S3-23714


5726893

DOCID: 4009720

~~TOP SECRET~~ 980

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

[redacted]

TOLOG

P.L. 86-36

MAY 1975

P.L. 86-36

"CODE WORD" OR "COMINT CHANNELS"?.....[redacted].....1
TA, HANDMAIDEN OF CA.....Frederic O. Mason.....3
HORRAY FOR PMD'S!.....[redacted].....6
ARE WE WASTING LINGUISTIC TIME?.....Mary Roberta Irwin.....7
LETTERS TO THE EDITOR.....11

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA (NSAM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009720

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. II, NO. 5 MAY 1975

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief..... Doris Miller (5642s)
Collection..... [redacted] (3571s)
Cryptanalysis..... [redacted] (8025s)
Language..... Emery W. Tetrault (5236s)
Machine Support..... [redacted] (3321s)
Special Research..... Vera R. Filby (7119s)

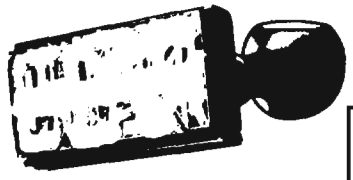
P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4009720

"CODEWORD" OR "COMINT CHANNELS"?



P.L. 86-36

[redacted]

V1

To the average person, the words ΑΚΡΩΣ ΑΠΟΡΡΗΤΟΝ, ΑΠΟΡΡΗΤΟΝ, and ΕΜΠΙΣΤΕΤΙΚΟΝ are just three Greek terms. Translated, these terms are TOP SECRET, SECRET, and CONFIDENTIAL, but unfortunately, to many NSAers they are still Greek. We in NSA know how to handle papers and documents with the various classifications affixed; our problem is in determining the classification of papers that we ourselves originate.

One of the major classification difficulties is determining whether certain information belongs in a COMINT category (that is, requires a Codeword on each page) or whether it must merely be kept in COMINT channels.

The definition of "COMINT Codeword" is information that, if compromised, could cause damage to national security, and specifically to COMINT activities. (Any paper, for instance, that quotes a COMINT source, directly or indirectly, requires a Codeword because it reveals that we are successfully reading certain traffic--information that, if compromised, would certainly jeopardize that traffic.) Such information requires handling that affords the highest degree of security protection. Of course there are various degrees of damage and of protection, depending on whether it is COMINT Category I, II, or III.

"COMINT Channels" information is that which, though less revealing, must still be limited to COMINT-cleared personnel because it contains information related to COMINT agencies or activities.

To aid in determining which group our paper falls in, we can look at the rules and guidance in the NSA/CSS Classification Manual and USSID 3. These guidelines often provide just the information we need. However, when we cannot find a specific rule or guide to solve our classification problem, we must use the general definitions and good old-fashioned judgment. Some hints in the judgment area are:

Very sensitive SIGINT plans and operations sometimes require greater protection and carry a COMINT Codeword classification just for that reason.

If the document reveals a degree of success or progress in the production of COMINT or a sophisticated COMINT technique, a greater protection than "COMINT Channels Only" is required.

Information classified by another agency or government may carry a higher classification than that we would have used, but we are required to apply the same classification as the originator.

As a Classification Advisory Officer, I am often called upon to assist in determining whether certain information is "Codeword" or "COMINT Channels." It is not always a clear and easy decision. I use all of the available guidelines and judgment factors mentioned above. When this does not give me the proper classification, I approach the problem in another way. I work on the supposition that the material I am trying to classify is compromised and falls into the hands of the enemy. With this information, what countermeasures can he (the enemy) take to insure that such information will not be available to NSA again?

If the exact time, date, place, and means of acquisition are available from the information, he can take extensive measures to insure that such information will not be communicated in the same manner again. He can change call-sign systems, frequency systems, schedules, and cryptosystems, and impose strict limitations on chatter usage, and he can do so at a particular transmission site. When your information fulfills some or all of the criteria above, it can easily be determined to be "Codeword."

On the other hand, if the paper gives general information related to the COMINT effort but does not include specifics of a transmission or actual transmission procedures or give the enemy information leading to specific countermeasures, it requires only "COMINT Channels" protection.

This can be amplified by way of example. The following problems are fictitious and are used for illustration only:

Mr. Charles Great is recommended for the Meritorious Civilian Service Award for his outstanding achievements while assigned to the National Security Agency/Central Security Service from December 6, 1970 to December 9, 1974. During this time he worked

EO 1.4.(c)
P.L. 86-36

DOCID: 4009720

[redacted] He guided the field sites in their collection efforts and was very helpful in solving problems that existed in their processing and reporting efforts.

This is obviously "COMINT Channels." It tells the enemy that we intercepted, processed, and reported [redacted]

[redacted]

This is obviously "Codeword." It identifies a unit which sent a message on 15 December, and relates the text of the message. [redacted]

[redacted]

[redacted]

~~(TOP SECRET UMBRA)~~

P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

DOCID: 4009720

TA, HANDMAIDEN OF CA

FREDERIC O. MASON, JR., P11

Traffic analysis was created, as an analytic function, in order to organize collection and to maintain continuity for support of cryptanalysis. In a broad sense it still does that, but it has also achieved a value of its own,

Before TA was fragmented into many career fields (for reasons which escape me) it was everything in COMINT which wasn't CA, or--more properly--it was a subset of CA, employing many CA techniques, but against a different body of data.

The essential differences between CA and TA are twofold:

Generally the two skills are inversely important: if CA is very successful, TA is apt to be little valued (though very complete); if CA is stymied, then any TA achievement is valued highly.

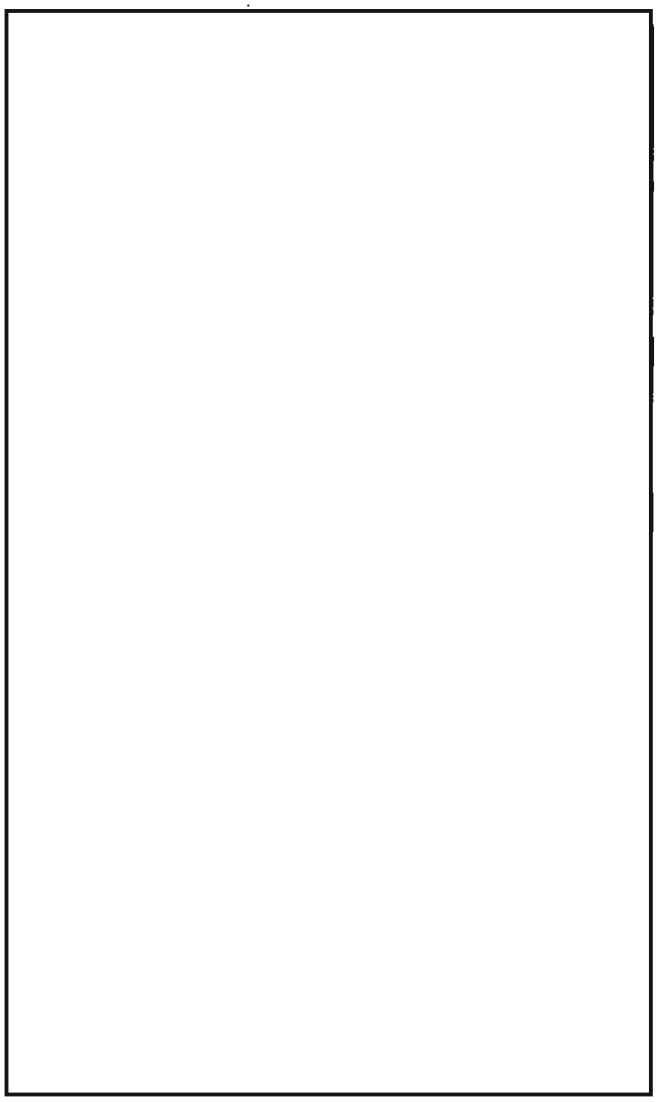
In practice the line between the two is not sharp, since TA normally does many "trivial" cryptanalytic jobs

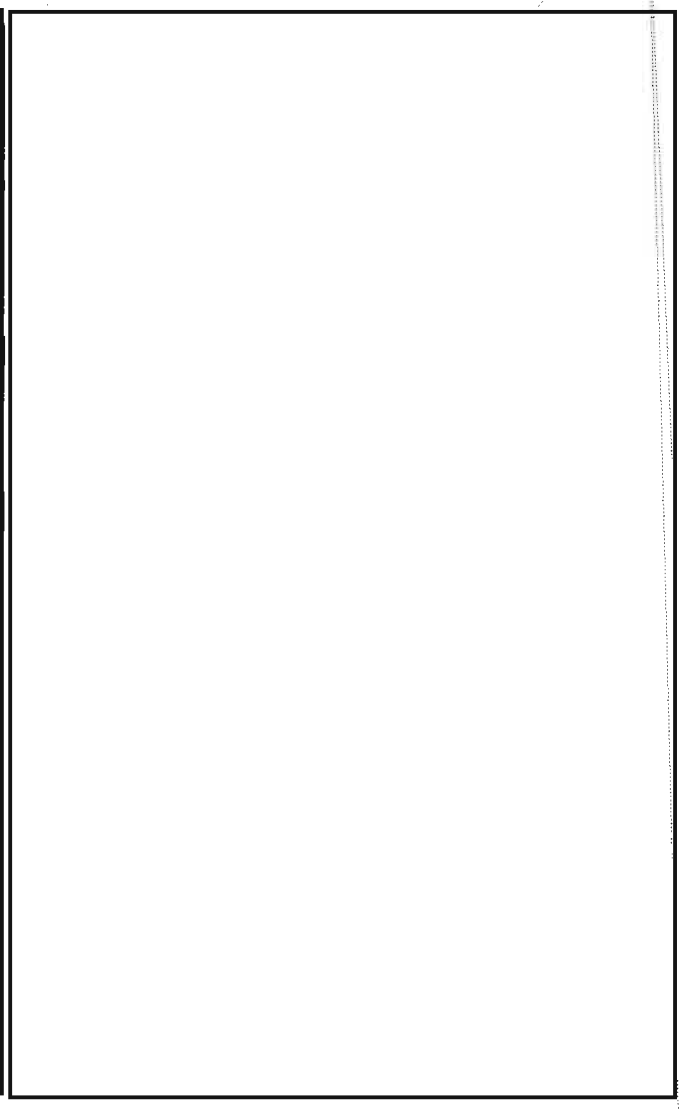
TA and CA are, then, both similar and interdependent.

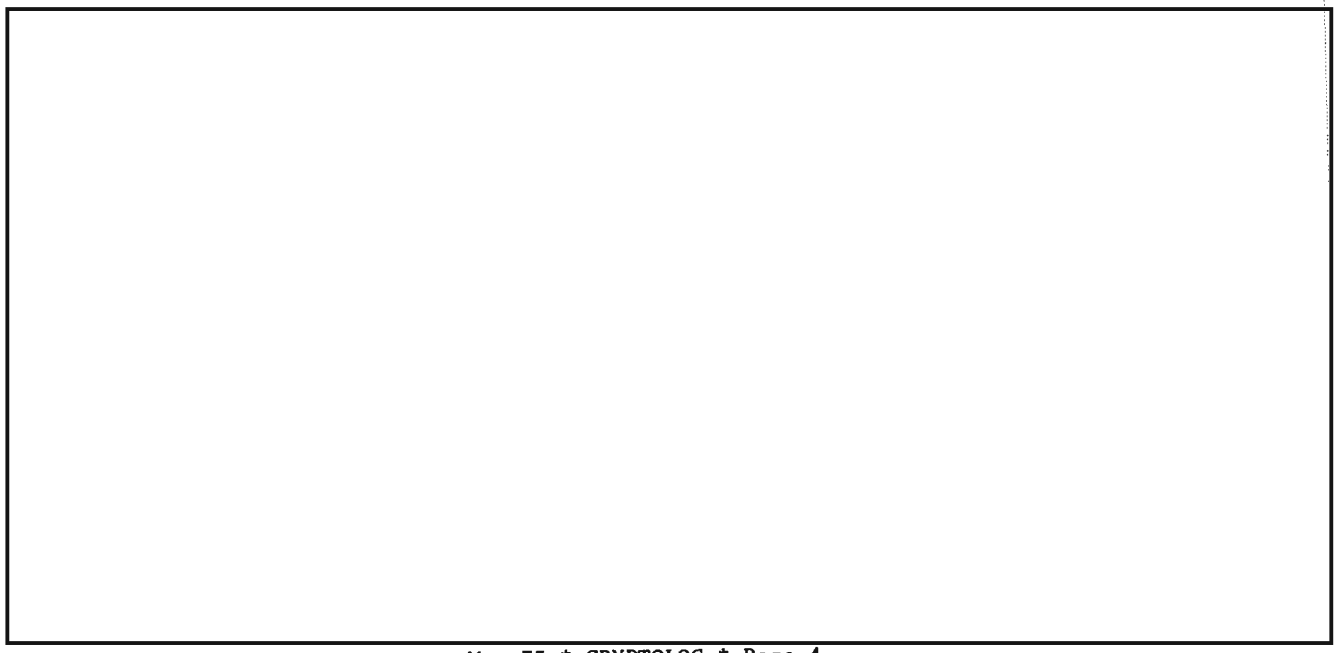
EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~TOP SECRET UMBRA~~







~~TOP SECRET UMBRA~~

EO 1.4.(c)
P.L. 86-36

[redacted]

[redacted]

[redacted]

** ** ** **

If this sort of exercise entertains you, we can do some more. Let us know.

DOCID: 4009720

★★★ HOORAY FOR PMD'S! ★★★

[redacted] M09

P.L. 86-36

My first impression of Program Management Directives was that the whole process placed an inappropriate emphasis on planning. As a result there appeared to be undue staff involvement in things that had previously been the exclusive domain of line organizations.

More recent experience with a specific PMD dealing with the phaseout of an overseas site changed my views radically.

The draft PMD was given to me with a note saying, "I can see considerable M involvement." My immediate reaction was,"To close out a site? You've got to be kidding!" After a discussion with the Program Manager, however, several things began to come into better focus.

First, the Program Manager asked for an inventory of equipment to include current value, size (in cubic feet), and weight. He indicated that he needed this information to develop an emergency evacuation plan. He had already dispatched crates for key items which were quickly identifiable as worthy of evacuation in a "one-week notice" situation. His plan was to order a sufficient number of C130 cargo planes to the site to accomplish the evacuation in an orderly fashion. He stated that each item identified on the inventory as worth over $1,000 would be brought out in a "one-week notice" situation, and he wanted disposition instructions for this equipment listed with the inventory. He indicated that the instructions need not be "Return to NSAW," since the same equipment might be in demand at other overseas sites being augmented to assume the missions from the phased-out site. The axiom *Planning is Managing* began to surface in my consciousness.

The discussion then turned to the PMD, which was due to be approved in approximately six weeks. The Program Manager stated that he wanted the M input to include time-phased actions as required in the recent revision of NSA Directive 25-3. We began to discuss the implications of a phasing-out mode: the effect of reducing the amount of operations space as systems are taken off line, and the impact of this on guards and alarm systems. It was becoming apparent that there *was* going to be "considerable M involvement."

On the subject of personnel, the Program Manager indicated that ten NSA civilians are currently assigned to the station in addition to the contractor personnel. It struck me that some of those people may be due for rotation back to NSAW prior to June 1976. If so, will they be replaced? Will they be extended? If they are replaced, where will the replacements be sent in June 1976? Then the thoughts came, what about militarizing those billets (M2)? Or using contractors (M52)?

I think the implications of a time-phased action plan in the points brought out above speak for themselves. For the first time we have a uniform rational system for exploring, on a timely basis, the implications of any given move.

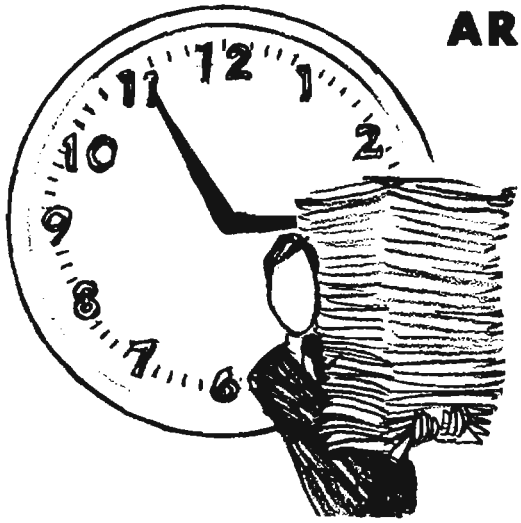
We in M have for years suffered in varying degrees of silence about not being notified regarding operational activities until they were at a point where only costly super-priority action on our part could provide the necessary support to successfully complete the operation. Now, under the PMD system, we are participating at the earliest stage in each project. Increasingly we are involved in detailed planning of events beyond the immediate future. This is, and should be, a challenge. We will undoubtedly find that it is easier to talk about planning than to do it. I think, however, we will find that it is more stimulating to take part in the planning than it was to sit around and complain about the lack of it.

NSA has historically been an action-oriented organization. We have all prospered individually and as an organization under this system, but times are changing, and we need to change--like it or not. The PMD system appears to meet that need. Who knows, we might just throw in a little MBO!

The Collectors Corner

A PARTISAN PEEK AT HISTORY

DOCID: 4009720



ARE WE WASTING LINGUISTIC TIME?

MARY ROBERTA IRWIN, G52

The EXPERT Sheet referred to in this article is used only in G, but a similar purpose will be served in A by the new Product Source Record and in the field by the Source Contribution Record. B Group is considering a version of its own.

There have recently been a number of articles in the *Technical Journal*, CRYPTOLOG and other Agency publications on language and language processing, but none of these has touched upon the problem of conserving the short supply of linguists for purely linguistic work. This problem can easily be overlooked or minimized by everyone but the linguist involved with current production on a daily basis. Writing as a linguist with thirty years of experience, spent almost entirely in processing [redacted] I want to present this problem as I have seen it and to suggest some possible solutions.

What non-linguistic work is required of the translator?

1. Logging and filing. This is, of course, among the "other duties as required," supposedly performed only infrequently by linguists when an area is temporarily short of clerical help. I would estimate conservatively that this situation has existed, off and on, for at least half of my thirty years. Let me make it clear that I am not criticizing lower and middle management. Managers at these levels have always been acutely aware of the problem; they simply cannot get sufficient clerical help. But translators cannot operate unless and until messages have been properly recorded and filed, so that references can be found; consequently this work devolves upon qualified linguists, often the younger ones, whose linguistic development under the guidance of older and more experienced linguists is thus slowed down.

2. Stamping the security classification at the top and bottom of each sheet of translation paper. Either stamping or writing this classification on in pencil requires a surprising amount of time. The sheets could surely be preprinted. They have been in the past, and no convincing reason for the change has ever been offered the linguist.

3. Providing data for retrieval of information, "valuable for you and necessary to the Agency," which takes "only a few minutes" for each translation. This has taken various forms over the last thirty years, but with the development of computers the trend has been steadily toward adding "just a few minutes more." In 1945 the translator attached to each finished translation a 3 x 5 card giving lane, message number, system and worksheet number. This was soon returned with the serial number, assigned by some now-forgotten ancestor of NSOC, which a clerical assistant entered in the section's permanent records. Today, thanks to the all-powerful computer, which can save untold numbers of man-hours, we in G have arrived at the EXPERT Sheet, simplified to the extent that the translator-analyst has to fill in only 19, or in some cases 20, of the 42 blocks provided, plus the security classification, which must be handprinted at top and bottom. (See Appendix.)

EO 1.4.(c)
P.L. 86-36

Of all this information, only the title, intercept data, system, and worksheet number really have to be provided by the translator. The security classification could certainly be preprinted and each section provided with those classifications it needed. Precedence could be assigned by an Ø5 analyst, who in any case often changes that assigned by the translator. Other blocks, except for two (discussed in the next paragraph), could be filled in by a competent clerical worker, hired for considerably less than the salary of any professional linguist. This presupposes enough clerical help to allow the designated person to complete the EXPERT Sheet as soon as the translation is received and to carry it immediately to the Ø5--another "only a few minutes" task which frequently devolves upon the linguist. It is not permissible to wait until several translations are ready and deliver them simultaneously, for work must not be piled on the Flex Room late in the day. Typists' time is precious.

The two blocks which could not be left to a clerk are numbers 13, now reserved for TAG's (Topic and Area Guides), and 37: KIQ's (Key Intelligence Questions--to be filled in only on

the last three carbons!). Before the addition of the KIQ's and TAG's, the sheet required approximately five minutes. Now those two items require more time than all the rest of the EXPERT Sheet, since a great deal of consideration is needed for each message. What is to be done about these?

Admittedly, translators must be intelligence analysts, for they have to decide what is significant enough to be translated, and in what order of priority, and in addition they must apply their judgment as analysts to the correction and translation of corrupt or telegraphic text. But the assignment of KIQ's and TAG's is a task of intelligence analysis which does not require linguistic ability. Qualified SRA's may be as hard to find as qualified linguists; but since in any case they must review the KIQ's and TAG's assigned by the linguist and since--and this is far more important-- these codings

In conclusion, then, it seems that we are:

1. Stunting the development of our younger linguists by using them as clerical help, thus making it impossible for them to acquire on-the-job training under the guidance of their more experienced colleagues--something which they all need, however excellent their college records may have been and whatever they may have learned in NSA training classes. As the older linguists retire in ever-increasing numbers, this problem is assuming the proportions of an emergency.

2. Taking all linguists, both young and old, out of the linguistic field and into aspects of the job that could be better done by intelligence analysts who do not require linguistic ability. In my own work as a translator-checker, I estimate that I spend about four hours per week on non-linguistic functions. Some translators spend more, a few less. The amount of time seems small, but it represents 10 percent of my working hours per week. If this figure is anywhere near average, can the Agency afford to devote one of every ten of its linguists engaged in current production to non-linguistic operations?

EO 1.4.(c)
P.L. 86-36

DOCID: 4009720
P.L. 86-36

Appendix

~~(TOP SECRET UMBRA)~~

The Cryptolinguistic Association will hold its 10th annual banquet and awards presentation on Thursday, May 29, at the Trojan Horse Restaurant in Silver Spring. The speaker will be our own Jack Gurin, whose talk is entitled, "What's a Nice Guy Like Me Doing in a Job Like This?"

The winners of the CLA Essay Contest will be announced, and also the recipient of the Jaffe Award, which is given each year to someone who has made an outstanding contribution in the language field.

The gala evening will begin with a cash bar at 6:30, followed by a roast beef dinner at 7:30, then the program at 8:30, and at 9:45 a social period which will include dancing. All this for the modest cost of $7.50 to members and $8.00 to guests.

For reservations contact [redacted] on P.L. 86-36 5471(s).

(UNCLASSIFIED)

ANSWER TO

OPTOGRGLY SPEAKING

A reader has chided us for not explaining the "usual rules of the game." According to the Washington Star, these are: (1) Words must be of four or more letters. (2) Words which acquire four letters by the addition of "s", such as "bat," "cats," are not used. (3) Only one form of a word is used. (4) Proper names are not used. According to our puzzle expert, "usually an abridged dictionary is specified beforehand." O.K.:

The following words are to be found in Webster's Seventh New Collegiate Dictionary:

Clog, cloot, clop, clot, cloy, color, colt, cool, coop, co-op, co-opt, coot, copy, crop, crypt, crypto, glory, gory, grot, gyro, loco, logy, loop, loot, lory, orgy, orlop, plot, ploy, poco, pogo, pogy, polo, poly, polycot, pool, poor, porgy, port, portly, prog, root, ropy, roto, tool, tory, troop, troy, typo, tyro.

(UNCLASSIFIED)

DOCID: 4009720

ANSWERS TO CLASSIFICATION PROBLEMS

INTERNATIONAL AFFAIRS INSTITUTE

Members of the International Affairs Institute recently elected the following new officers:

President-Elect Robert E. Drake
Members-at-Large [redacted]
Barbara W. Clark
[redacted]
Robert J. McDermott

Also, at the March meeting of the Board of Directors, a new secretary, Robert J. McDermott, was elected to complete [redacted] time in office.

The President, [redacted] and the members of the Board are currently working on a series of projects aimed at expanding the activities of the I.A.I. to more directly involve and benefit all the members of the Institute. The members will also be encouraged to express their ideas and views in a questionnaire which will be distributed in the near future.

P.L. 86-36

(UNCLASSIFIED)

[redacted]

I hope this exercise clearly demonstrates the problems and difficulties involved in determining classifications, and specifically what information needs Codeword or "COMINT Channels" protection. There are eight Classification Advisory Officers at NSA. They are willing to offer assistance in your classification problems, but the responsibility for proper classification belongs to each of us. My advice then is to use the Classification Manual and USSID 3, consult your Classification Advisory Officer when necessary, and most important, take the time to determine the appropriate classification and thus to insure that the proper protection is being afforded.

~~(TOP SECRET UMBRA)~~

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

DOCID: 4009720

LETTERS TO THE EDITOR

P.L. 86-36

To the Editor, CRYPTOLOG:

I hope you can find room in your next issue for clarification of the editorial introductory note for [redacted] recent piece on "The Uses of ELINT" (April 1975).

Having established that in the beginning there was COMINT, your note then refers to ELINT as "the other half of SIGINT." Unless P1 has developed a new-new-math which permits more than two halves in a whole, you have (unintentionally, I trust) eliminated the "other third" of our SIGINT family: TELINT.

Confusion on the place of TELINT (Telemetry SIGINT) is as understandable as it is widespread. For years, NSAers thought of it (if at all) as a sub-set of ELINT, largely because it used no COMINT coverwords and because in 1960 USIB had decided to classify it and handle it "like ELINT." A former Chief of P1 was a leader in opposing this "ELINT-by-association" theme; since telemetry's job is to communicate information, it cannot be a "non-communications transmission" in terms of the accepted definition of ELINT. [redacted]

On the assumption that CRYPTOLOG is happy to support its sister publications, I modestly (?) recommend to your readers a two-part SPECTRUM article giving the background of NSA's involvement in telemetry (Vol.1 No.3 and Vol.2 No.1, "Talomatry and How It Grew").

The term "telemetry" is often used with a broad meaning which includes some (but definitely not all) other kinds of "Foreign Instrumentation Signals" (FIS), a term which is appearing more frequently in USIB community papers. (In fact, there is talk that a new NSCID may divide SIGINT into COMINT, ELINT, and FIS.

Telemetry has come a long way in the 20 odd years [redacted] timely [redacted] intelligence support to U.S. Navy and other tactical commanders!

[redacted] V3 P.L. 86-36

The Editor regretfully acknowledges the error and promises it shall not happen again.

EO 1.4.(c)
P.L. 86-36

To the Editor, CRYPTOLOG:

[redacted] letter in the April 1975 CRYPTOLOG concerning the professionalization problems of bookbreakers, and the related questions posed by [redacted] the Cryptanalysis Editor, in her note, tend to confirm a suspicion that has been growing in my mind for the last five years: the venerable term "bookbreaking" and the importance of the SIGINT produced by its practitioners seem to have become lost in the bureaucratic red tape somewhere in the fog-shrouded ivory towers of operational and personnel management.

This loss of understanding by management goes far beyond the mere fading of a useful term; application of the specialized skill itself has become clouded in management's mind to the point where (in B Group, at least) it is now closely equated with cryptanalysis. [redacted]

[redacted]

The current CA Task Inventory revalidating the COSC job codes provides an excellent opportunity to review and perhaps redefine the term "bookbreaker" and what he does, or should be capable of doing, in terms of job skills. And this letter is my opportunity to offer some personal views towards that objective, based on 31 years of experience in almost every aspect of the SIGINT business, [redacted]

[redacted]

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36
DOCID: 4009720

[redacted]

[redacted] And without the bookbreaker's alchemy there is damned little substance (other than TA) from which the SRA can construct a story and garner the kudos that so often rightfully belong to the bookbreaker industriously working in the background to perfect the code so that even more and better secrets can be revealed. The bookbreaker is the individual who created something from nothing!

[redacted]

P.L. 86-36

To the Editor, CRYPTOLOG:

There is need to recognize bookbreaking as a distinct form of analysis, by the establishment either of a separate career field or of an option within a separate cryptolinguistic career field. The cryptolinguistic option of the present language PQE does not test directly for knowledge of analytic principles, use of machine support, of predecessors as models, of statistics, of working aids, etc., all of which are necessary for bookbreaking. And now more than ever these techniques are indispensable for bringing a code to readability, for we are faced with lower volumes and at the same time more difficult codes, as they have been improved through the years.

EO 1.4.(c)
P.L. 86-36

[redacted]

[redacted]

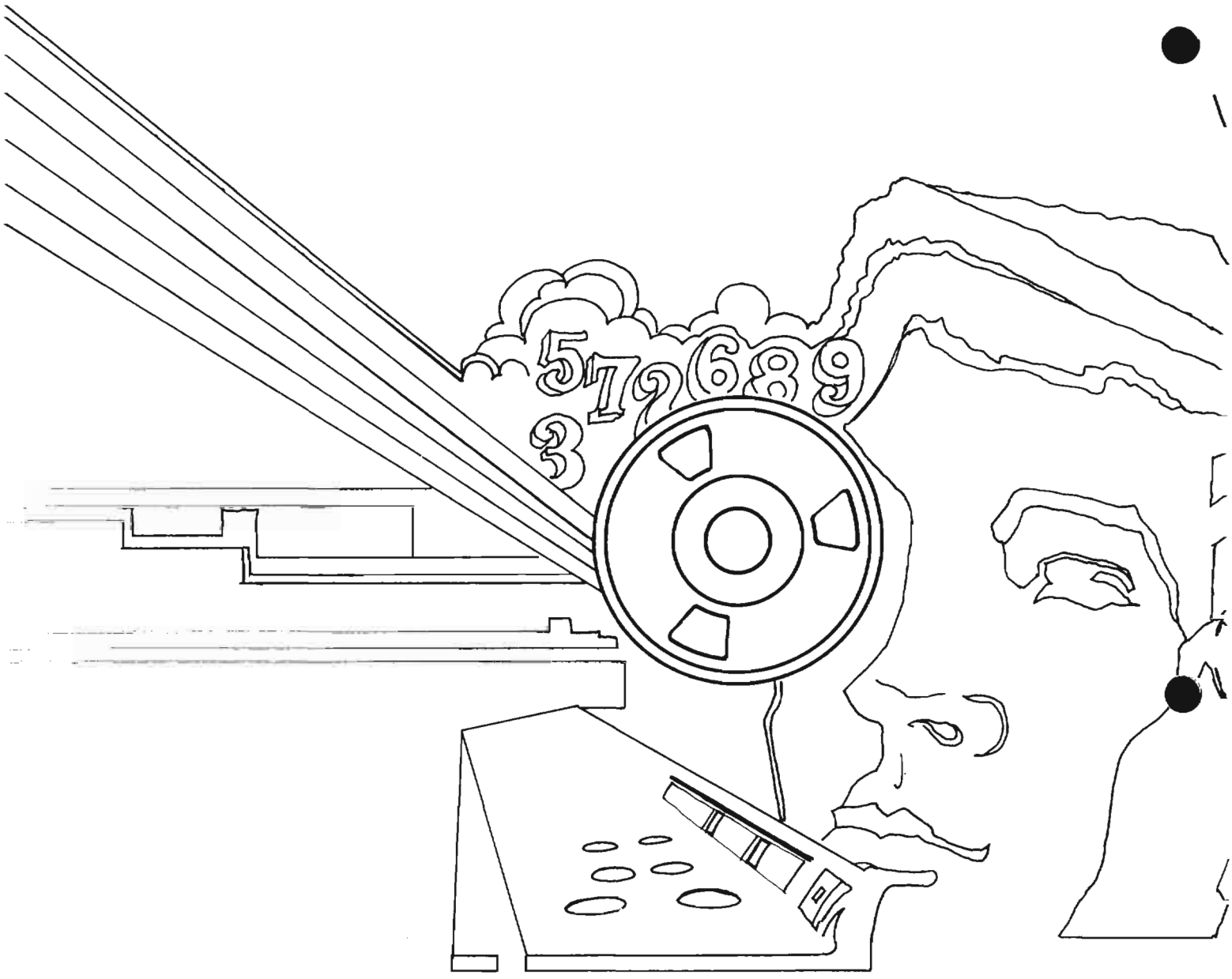
In summing up, my view of the bookbreaker is that he or she is first of all a linguist, but one who has progressed beyond routine translation. It is a highly personal and individual capability. Through some quirk of nature or personality he or she is usually intensely interested in solving the mystery of the unknown: creating knowledge out of meaningless code groups. It is this spark of genius that is the bookbreaker's true value.

[redacted]

[redacted]

~~(CONFIDENTIAL/HVCCO)~~

P.L. 86-36


5 7 2 6 8 9
3

DOCID: 4009719

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

APRIL 1975

P.L. 86-36

A COMM CHANGE AT RAMASUN STATION..... [redacted] 1
A GUIDE TO CENTRAL INFORMATION..... 3
ORAL REPORTING: A NEW CHALLENGE FOR NSA... [redacted] ..4
COVERTERMS..... Vera Ruth Filby.....7
THE USES OF ELINT..... [redacted] 15
LANGUAGE IN THE NEWS..... Emery Tetrault.....17
Answer to CAN YOU MAKE OUT THE NAME?..... [redacted] 18
PSYCHING THE CODE CLERK..... L.D. Callimahos.....19
LETTERS TO THE EDITOR.....21

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009719

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. II, No. 4 APRIL 1975

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief..... Doris Miller (5642s)
Collection..... [redacted] (3571s)
Cryptanalysis..... [redacted] (8025s)
Language..... Emery W. Tetrault (5236s)
Machine Support..... [redacted] (3321s)
Special Research..... Vera R. Filby (7119s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

~~SECRET SPOKE~~

A Comm Change at Ramasun Station

The document below originally appeared as part of the Weekly Operations Review for the week 9-16 January at USM-7 in Udorn, Thailand. It was an open letter from the Officer in Charge of the Collection Management Branch to all personnel at Ramasun Station, just after a hectic day involving one communications change [redacted] by Cambodian guerrillas. We reprint it here, with the author's permission, for the vivid glimpse it provides into the working of a field station at such a time.

EO 1.4.(c)
P.L. 86-36

For those unfamiliar with the context, the following short glossary will be helpful: [redacted] ASB, CMB, DFSB--Analytic Support Branch, Collection Management Branch, Direction Finding Support Branch; TI--Traffic Identification; KSR--a keyboard on line to a computer; CATWALK--an in-station mechanized target identification system; ASRP--Airborne SIGINT Reconnaissance Platform; CEG--trigraph for Cambodian Guerrilla; SOI--Signal Operating Instructions; CIL, OSB, IMF--Central Intelligence Library, Operations Support Branch, Intercept Maintenance Facility.

P.L. 86-36
EO 1.4.(c)

[redacted] Though this change was expected and accurately predicted by ASB, the actual degree and seriousness of the change was not known.

I spent much of the day running around like a chicken with its head cut off (such is the career of Warrant Officers), coordinating between ASB, DFSB and the intercept bays. The scenes I encountered during that day reaffirmed my faith in USASA operational personnel, and, in particular, my faith in the potential and professionalism of the personnel of USM-7. I would like you, each and every one, to know what thoughts go through the mind of a Warrant Officer with my MOS and experience, as I venture through the heart of a field station on the day of a Comm Change.

Scene: ASB. Great! All the key NCO's are here at once!...There's a couple of people in civvies. They're probably trying to muscle in on my overtime fund!...Look at the analysts--every one of them looks like he or she has the weight of the world on his or her shoulders. I can still remember my very first Comm Change, circa 1954, in Europe. How eager, nervous, and desperate I was to recover as many targets as possible! I wonder--do I still have that drive? That interest? I hope so!...I talk with the appropriate supervisors and learn that they have everything well in hand. Arrangements have been made for every possible contingency. I move on to the bays.

Scene: Bay One. Good God! Look at all the people! TI personnel sitting on operators' laps. TI personnel standing in the aisle. An ASB/CMB NCO running back and forth, dodging bodies, leaning over operators' shoulders, competing with the bay supervisor for room and access to pounding, searching operators. They've already isolated numerous good suspects, targets which will be developed through a concerted effort by intercept operators, ASB personnel, and good ole DFSB.

[redacted] Ha! Ignorance is truly bliss... Later I will see the swing trick come in and relieve the day trick in Bay One. The transition of one operator on the position to another operator on the position is smooth, though filled with anxious, interested queries. All known history of what has happened to date is passed along, all down the lines of positions, and from one bay supervisor to the next.

[redacted]

~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

[redacted]

Scene: Bays Five and Six. I make several trips into these bays, and each time I am awed by the concentration of all operators, and the coordination between the operators and the professional Air Force floorwalkers. The reason?

[redacted]

Scene: Bay Three. Aha, the CEGs tried to catch the world with its pants down!

[redacted]

Scene: Bays Two and Four. At last! A small semblance of normalcy. Just the same old thing! Bay supervisors handing out folders like they were dealing cards; operators hunched over their keyboards, fingers flying;

[redacted]

Without these personnel--men and women who give of themselves selflessly; men and women who endure hours of noise, nerve-wracking tension, mental strain and fatigue; men and women willing to endure the responsibility and discipline of military life; men and women who often bitch about the unfairness, the inequity of their plight, but never fail to get the job done--How would the free world know?

Scene: Comm Center. Though I did not have time to enter the Comm Center, nor any valid reason to intrude on their hectic day, I have had enough familiarization with communications centers to readily visualize their frenzied chores on this "bad day at Black Rock." Inside their secure vault, teletypes are clacking out their incessant chatter. Bells are ringing and lights are flashing. Tired, blurry eyes are scanning incoming messages which pertain to every element of life and business on our post. Experienced fingers deftly twist and fold the individual punched tapes from each message and staple them to their messages. Outgoing messages are patiently poked onto tape, and then transmitted to all points of the world. This hustling, busy center of activity is often overlooked in our daily lives. But without these men and women contributing their bit to our unique tasks here at Ramasun station, we would have no contact with the real world. They too are a vital part of our organization; and the analytical answers, the operational facts that we discover on each and every day of the year are relayed swiftly to our headquarters and NSA by the devoted toil of these men and women.

Scene: DFSB. Ye gods! Another bedlam and bustle of activity! That poor controller! Look at those damned lights--how can he possibly tell which one has priority? Which one came on first? There--four of them together! Rots o' ruck, fella! And over there--and there! Those crazy, almost psychedelic, whirling circles of light! And look how fast they are able to align the bearing with the null of the signal! Yes, here too the pros are at work. All the key NCO's present for whatever assistance may be needed, all the shift personnel hustling to keep up with the constant and continuous blinking of the

DOCID: 4009719 E.O. 1.4.(c) P.L. 86-36

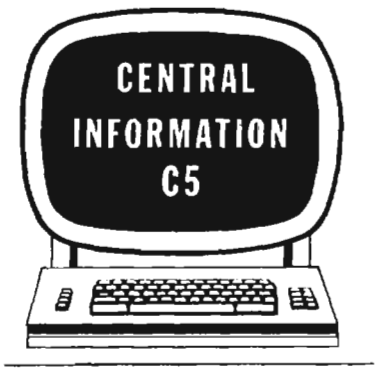
lights on the controller's panel.

Scene: The Operations Gate, CIL, OSB, IMF. Though the personnel who man these activities are not intimately involved with the actual recovery of the communications change, without them we could not function successfully. These are the men and women who ensure our security; who support our intercept and analysis efforts with regulatory and historical documentation; who furnish the material things we need to operate with; and who maintain and repair the equipment so vital to our efforts. Though we, the operators and analysts, may often feel that we are the only reason Ramasun station exists, it would behoove us, particularly at times of crises, to reflect that without these various vital supporting elements we could not do our jobs. We are a team. A professional team. Our victories and our successes are not measured in terms of individual heroes. They are accomplished by the united efforts of every member of our team. Without our "security guards, our waterboys, our equipment managers, our coaches, and our fans," who serve quietly and unnoticed on the sidelines, our team could not exist. These people are pros, too, every single one of them.

When 04 Jan 75 finally came to an end, when I crawled into my bed, one thought made me glow, made me proud, and made my career seem very worthwhile. These men and women down in the box, these operators, analysts, DF operators and Comm Center personnel were a glorious, unsung breed. And I'd go to hell and back with any one of them! I slept very well. I thank you; all of you, and each of you. Very much!

CW3, MI
OIC, CMB

A GUIDE TO



The little directory given away at the INFO '75 exhibit seemed to us to be worth reprinting, just in case you missed it. So here it is.

Central Reference Service	2C051	3258s
Information Services Officer	2E099	4853s
Book and Periodical Libraries		
Main Library	2C051	5848s
S Branch	C1A09	2341s
Fanx Branch	B6B06	8447s
Inter-Library Loan	2N072	4868s
Soviet Information	B1B20 Fanx 3	8445s
Middle East	4A187	4806s
Southeast Asia	6A198	4278s
China	7A187	5320s
International Information	2C051	3258s
Geography and Maps	2N075	5918s
Technical Documents	2N090	5759s
Collateral Documents	2E024	5670s
SIGINT Repository	2E054	5853s
Cryptologic Library	3W076	4017s
Language Library	3W076	4017s
Field Support	2E029	3265s
Publications Purchasing	2N111	3096s
24-Hour Service	2E099	4853s

~~FOR OFFICIAL USE ONLY~~

·O·P·P·O·R·T·U·N·I·T·I·E·S·

P.L. 86-36

The Intelligence Department of the National Cryptologic School is interested in contacting NSA employees who would like to teach English writing courses on a part-time basis. These courses emphasize intermediate and advanced writing skills and usually meet six hours a week for eight weeks. Anyone interested in teaching should contact E12, telephone 7119s.

DOCID: 4009719

ORAL REPORTING: A New Challenge for NSA

The author of this article serves as the "A" Representative on a V4 team which provides weekly briefings--or "oral reports"--to the Director of the Defense Intelligence Agency (DIA), the Deputy Director, DIA, for Intelligence, and the Chiefs of Staff for Intelligence (ACSI's) of the four services; to DIA's Deputy Director for Estimates, and staff; to the Deputy Director, Central Intelligence, Intelligence Community, and the Committee Chairmen of the United States Intelligence Board (USIB) and appropriate National Intelligence Officers (NIO's); plus ad hoc briefings, as required, to the Chairman of the Joint Chiefs of Staff, the State Department, the National Security Council staff, and others.

Traditionally, NSA has regarded the production of the *written* report as the ultimate in the intelligence process. Through personal observation over the last 20 years, and particularly as a result of my experiences during the last year and a half in reporting to some of the top decision-makers in Washington, I have come to the conclusion that an additional requirement is crystallizing for the *oral* report. The function of the written report is to inform a wide audience in such a manner as both to enlighten and to provide a permanent record of the enlightenment. While this will continue as a critical requirement, the modern age of rapidly changing situations requires a more timely approach for the executive level--that of the oral report.

I cannot state it as a hard and fast rule, but it has been my experience that executives do not read reports. Their time is limited and they must become informed on a subject quickly. When SIGINT is one of the inputs, the fusion of SIGINT with other sources of intelligence is normally performed by their staffs. Thus, they exist on briefings and rely on their staffs to continually filter to them the information that they should have.

As the information proceeds up the chain of command, the filtering process continues, both in numbers of items being forwarded and in the length of individual items. For example, when presenting an item for the Chairman of the Joint Chiefs of Staff, a briefer is allowed no longer than six minutes, regardless of the complexity of his subject! The JCS daily intelligence briefing usually lasts only 20 minutes. If that is all the time that people at that level have for intelligence, it is obvious that

DOCID: 4009719

they cannot spend time perusing lengthy reports, particularly when they cannot ask the written report a question! In contrast, the oral report is primarily for the decision-maker and treats specific events or situations, enabling him to take actions as required. It is a most effective way of presenting information, in that, first, it allows for questioning to clear up points which may appear ambiguous or vague, second, the dialogue which develops allows the briefer to be sure he has made his point, and, third, any follow-up actions that may be necessary can be initiated immediately, without having to wait for questions to flow through the chain of command and possibly be distorted in the process.

Within the intelligence community, the normal method of preparing a presentation is to select an individual with a good voice and stage presence, let him read the immediate facts surrounding an event, prepare a written script, and then "brief" (read the script). What is needed is an oral reporter who, without use of notes, can summarize events bearing on a situation, provide background to place those events in perspective, present the material in a professional manner with well-designed visual diplays, and, most important, be prepared to answer detailed questions on the facts as well as to offer opinions when requested. The wide divergence between the "professional briefer" and the "oral reporter" was best summarized in a plaque hung in the small conference room of Admiral Gaylor, which said, "DON'T BRIEF ME, JUST TELL ME WHAT YOU KNOW."

As a result of the lack of equal recognition by NSA for these two forms of reporting, we have produced highly qualified report writers and very few oral reporters. A major reason for this situation is the fear by many analysts of being type-cast as "briefers," which would put an end to their careers. It is ironic that many of our managers feel that briefing requires no special skills or training and that almost anybody can do it, ever though every time they actually have to find someone to brief a high-level visitor to the Agency, or select an individual to "go downtown," it seems to become an almost impossible task, which repeatedly falls to the same few people.

In some areas of the Agency, managers have seen the need for the oral reporter and have attempted to meet the problem by training their senior analysts in basic briefing skills so that they can give briefings on their specific problems, should the need arise. Although this would appear to be an effective solution, it is only a stop-gap measure and ultimately doomed to failure. This conclusion is based on two facts: that there are many large audiences in the Washington area alone which have a well-established need for direct person-to-person exchange in the form of intelligence briefings by NSA, and that their number is rapidly growing. The net result will be a demand for the "senior analyst" to spend more and more time away from his problem and less and less in analysis. Further, although they may be knowledgeable, many analysts are not physically or emotionally suited to the task. I have seen poor voice projection, lack of confidence, or nervous mannerisms completely destroy a good intelligence presentation. On a few occasions, emotional tension and/or lack of experience in briefing has rendered an "expert" physically ill to the point of considering canceling the briefing commitment.

A major occupational hazard faced by the professional oral reporter is fielding loaded questions. Questions which bear on the Agency's capabilities or shortcomings, those which are designed to embarrass rather than elicit information, or those that focus on our techniques rather than our results, all can be disastrous to a novice briefer. Rather than appear to be less than totally knowledgeable, he will attempt to answer questions that should never have been asked. Similarly, questions that may exceed the clearance level of the audience can cause problems; the senior officer may be cleared for a direct answer to his perfectly legitimate question, his audience may not. Under the pressure of the moment, the briefer must know how to sort out immediately what can be said, or how --tactfully--to say nothing.

The obvious solution is a core of oral reporters possessing a good background in SIGINT, an understanding of the hierarchy of the intelligence community, a knowledge of its personalities and varying needs, and the ability to present NSA and its product with competence. This approach allows the individual oral reporter to accustom himself to this form of reporting, develop familiarity with his audiences through repeated exposure, and, most important, realize that he can brief without scripts, file cards, and other memory joggers. It is this type of presentation that establishes in the minds of the audience an immediate sense of confidence that "he knows what he is talking about." Additionally, the rapport which is established between NSA personnel and executives throughout the Washington area is priceless in selling NSA and its product.

Having recognized the need to develop this capability within NSA and the reluctance of individuals to volunteer for such assignments, let us consider the elements of the solution.

Who should our oral reporters be? They should be experienced analysts and reporters in the middle grade-level who will make a positive impression on the executives with whom they are dealing. It has been suggested by some that prior experience as a recruiting officer, a used car salesman, or an insurance agent is vital as a prerequisite for an oral reporter. While I would prefer not to comment on this directly, I would emphasize that it is a selling job. For many years, NSA has referred to our published re-

ports as "product," and that is exactly what they are. We have a product to be sold, and sold as forcefully as any item in the business world. In this day of dwindling funds and stiff competition wherein all of the intelligence sensors are competing for their share of the money available, the lack of salesmanship by NSA not only affects decision-making on military and diplomatic issues, it affects future budgeting--your job and mine.

What should they be presenting? The NSA/CSS story: the contribution that SIGINT can make to the solution of the intelligence problem. Qualified persons presenting this at the proper levels can do greater good than pounds of written reports which find their way into the files of other intelligence agencies but are never given proper credit at the top levels where the intelligence and budgetary decisions are made.

When should they begin? The time is long overdue. However, other agencies have not yet realized the full potential of such a field of endeavor, so that we can still venture forth in this area and reap the benefits. The standard military approach of having a script-reader present intelligence briefings while a myriad of back-up personnel stand in the wings is still being followed by most agencies. This allows NSA/CSS to take the initiative and begin to train effective oral reporters. In my experience, a good presentation by an individual having the qualifications of an oral reporter stands out and repeatedly draws praise from an exective audience.

How do we get such reporters? First of all, the National Cryptologic School must recognize the need and begin to design courses on executive briefings, visual aid design, and other parts of the mechanics of producing an oral reporter. These courses would be directed toward developing the extemporaneous briefer as opposed to the more stilted, "canned" style now used. Further, just as the writer of reports needs to know how to distribute his reports, the oral reporter needs to be familiar with his potential audiences within the U.S. Intelligence Community, their missions and functions, how they can use SIGINT, and how to be effective with each. He needs to consider certain questions before presenting an oral report: Why does this executive need to hear this report? What do I want to achieve in presenting it? What is his knowledge of SIGINT, and what is his feeling toward the Agency? These questions and many others must be answered before an oral reporter steps to the podium and begins.

Further, the style of an oral report may differ substantially from that of one designed to be read. The various styles, and the uses of each, should be instilled in the student, so that he will be able to select the most effective format for a given audience or individual.

He should be taught the effective use of visual aids, the various forms available to him and the advantages of each.

Lastly, he should become familiar with the facilities available to provide audio back-up for his presentation. This all-too-often neglected technique is helpful in enlivening a long presentation or as an "attention-getter." Contrast the normal approach to reporting an air engagement with that using a short cut of the voice tape played while the screen shows a map of the battle area. The latter gives a "you-are-there" feeling that is lost in a written report. It also allows those not accustomed to SIGINT to hear first-hand and observe the difficulties encountered in what they have previously considered a simple transcription effort.

Where should they come from? From the various reporting staffs and senior analysts with backgrounds in a number of operational problems. But--our career and promotion systems being what they are--don't expect volunteers to jump forward. At present, to become a "briefer" is all too often the kiss of death for a good analyst. The incentive must be created by our managers to attract the proper type of individual. A major assist in this area should be provided by the NSA SR career panel. The criteria for professionalization should be changed to require not only in-depth training in oral reporting, but mandatory experience points for holding an oral reporting job.

Last, and most important, consider the "why." At the executive level, the "why" is the valuable input that SIGINT presented in this form can make to decision-making. In far too many cases, the full SIGINT story has been published but is not available to the decision-maker when a determination has to be made. Two frequently encountered attitudes of Agency managers, however, are: "I've already published a report on that; why should I have to go down and tell them about it?" and "I have more important places to put my resources than a dog-and-pony show." These attitudes not only sell NSA short but might lead to an erroneous decision affecting the national interests and even the security of the United States. The "why" to NSA/CSS is the new image that can be created, one of professional competence and diversity which will result in greater recognition of SIGINT. The "why" to the individual is answered by allowing him to see things happen as the decision-makers react to his presentation, question his experience, probe his views, and then make the determination of what is to be done.

Thus, the oral report should be the ultimate in satisfaction for both NSA--in that it is fulfilling its mission to the utmost--and the individual. "We had intelligence for top executives, we got it to them, and they used it!" How many SIGINT reporters, as good as they are, can say that?

DOCID: 4009719

COVERTERMS

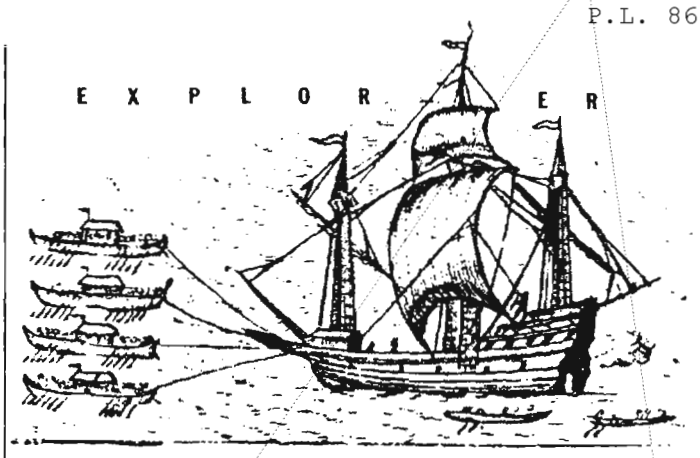
Vera Ruth Filby, E12

A Memo from Prime Minister Churchill to General Ismay, 8 August 1943

I have crossed out on the attached paper many unsuitable names. Operations in which large numbers of men may lose their lives ought not to be described by code-words which imply a boastful and overconfident sentiment, such as "Triumphant," or, conversely, which are calculated to invest the plan with an air of despondency, such as "Woebetide," "Massacre," "Jumble," "Trouble," "Fidget," "Flimsy," "Pathetic," and "Jaundice." They ought not to be names of frivolous character. . . . The world is wide, and intelligent thought will readily supply an unlimited number of well-sounding names which do not suggest the character of the operation or disparage it in any way and do not enable some widow or mother to say that her son was killed in an operation called "Bunnyhug" or "Ballyhoo"...Care should be taken in all this process. An efficient and a successful administration manifests itself equally in small as in great matters.

EO 1.4.(c)
P.L. 86-36

Let us suppose that the basic ideas for a project have been formulated and discussions of plans for field tests are about to begin. The time seems right to assign a name, for convenience--and for prestige. The project is designed to determine the amount and usefulness of a certain type of data recovered as a by-product of traffic intercepted for a different purpose. What should the name be? How about BYPRODUCT, since that is what the experiment is all about? That doesn't exactly stir the blood, though, does it? Well, how about something catchier, like SCAVENGER? Or SCRAPS? Or maybe just a pretty, pleasant name that everyone would like? Or maybe it would be nice to let Diana choose a name; she has done a really good job as secretary, typing up all those figures... That's it! Project DIANA!



names to be shunned, in addition to those proscribed for any of the reasons noted, are words listed in the Joint Chiefs of Staff (JCS) publications JANAP 299, UNITED STATES JOINT SERVICES CODE-WORD INDEX, and ACP 119, ALLIED TACTICAL

P.L. 86-36
EO 1.4.(c)

~~SECRET~~

VOICE CALL SIGN SYSTEM INSTRUCTIONS AND ASSIGNMENTS.

There is no question, of course, that there are a great many unofficial, semiofficial, informal, local, and oddball coverterms around.

[redacted]

To facilitate the assignment of official coverterms, STINFO and other responsible organizations compile and maintain lists of available coverterms. Despite the enormous stock of English words, coverterm lists are remarkably difficult to compile because of restrictions and a number of other considerations. None of the following, for example, would be eligible:

ALOUETTE: because it is a foreign word not used in English, and: because it is the name of a French helicopter

BUGGER: because although it is innocuous in American usage, it is vulgar in British

CANOE: because it is a five-letter word, and: because it was once used as a COMINT codeword

CHELTENHAM: because placenames are reserved for machine programs and systems, and: because it is already in use

COWPER: because two-syllable surnames are reserved for research and engineering projects,

[redacted]

HADRIAN: because names of Roman emperors are

[redacted]

HONKY: because it is a five-letter word, and: because it is offensive and derogatory

JAGGER: because it has been used as a coverterm within the last five years

KLEENEX: because it is a registered trademark

MARLIN SPIKE: because it is listed as a root word voice callsign in ACP 119(A)

NECTAR: because it is in use as an

[redacted]

PEDRO: because it is a five-letter word, and: because it is a fixed callsign, listed in ACP 119(A), for search and rescue helicopters

PERSEPHONE: because mythological designators

[redacted]

PHOOEY: because it is trite, pejorative, and potentially displeasing to senior officials

SOBRIQUET: because it is listed in JANAP 299(A)

WAVEGUIDE: (if descriptive) because it reveals the nature of the activity

ZEALOT: because it is a [redacted] listed in ACP 119(A).

A further limitation in the selection of covernames, even those on the STINFO reserved list and available, is that they may not form a "family." For example, if a project is named FORSYTHIA, related projects may not be named DEUTZIA, HYDRANGEA, RHODODENDRON, or other names of shrubs, the obvious reason being that if one name is compromised, then all are compromised. Randomness in all covername features is normally preferred, but sometimes special requirements prevail. For example, when the quadripartite

[redacted]

[redacted]

[redacted]

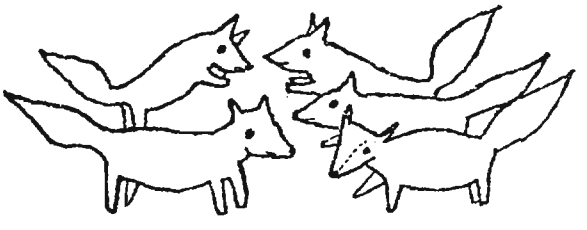
[redacted] The current reserve list was picked from the Washington telephone directory, but the choices were not random. Limitations included avoidance of surnames which are also placenames and of names easily misunderstood, misheard or misspelled because of homonyms, common variants, or other

P.L. 86-36

 1.4.(c)

P.L. 86-36
EO 1.4.(c)

reasons (CARNEY/KEARNEY/KEARNY; D'ARCY/DARCY/DARCEY; HAYWOOD/HEYWOOD; WALLACE/WALLIS). Names with spaces, apostrophes, or hyphens (DE GROFF, O'KEEFE, RAIT-KERR) would not necessarily be ineligible, but their marks of punctuation would be eliminated.

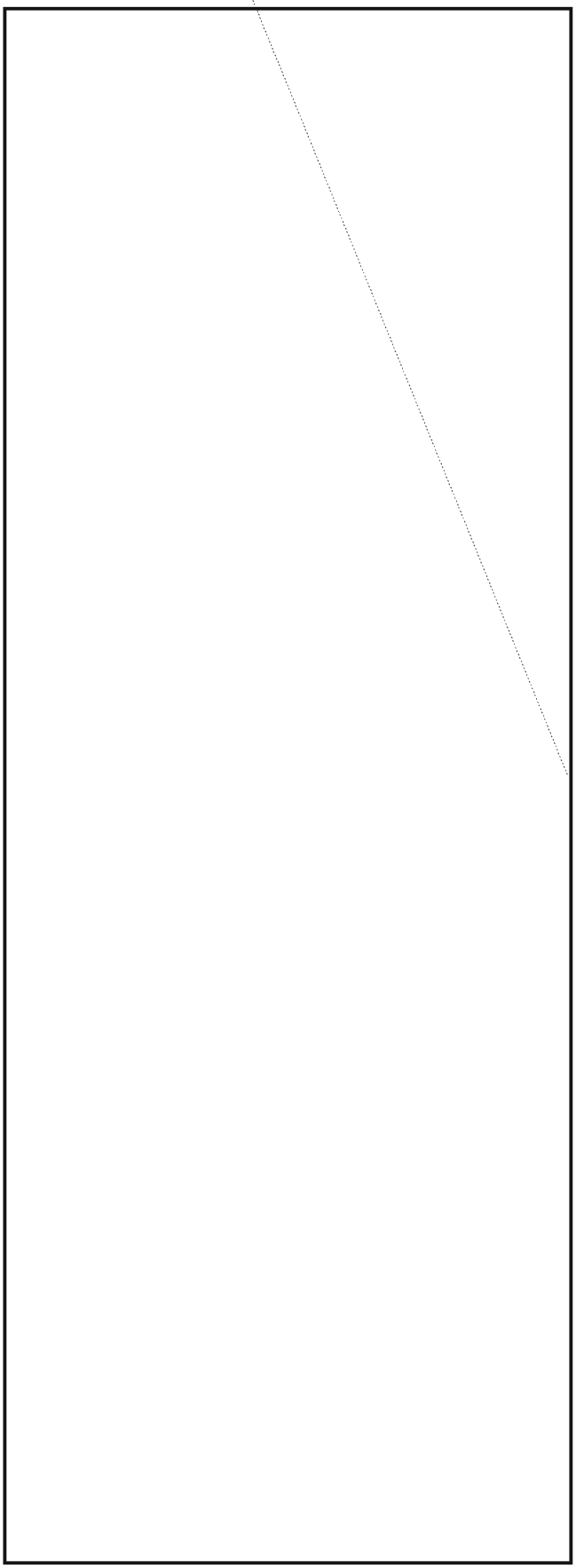


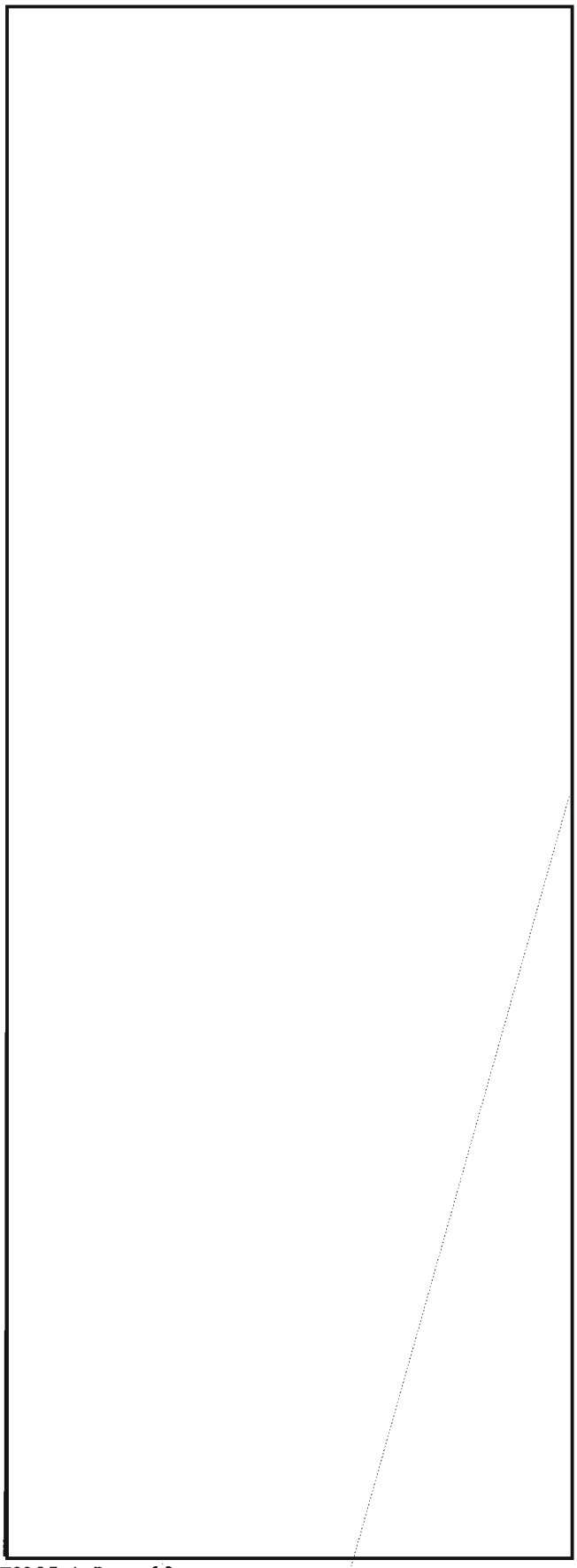
LEFOX GREY LEFOX GREEN LEFOX

 P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)
DOCID: 4009719

~~SECRET~~





~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~
P.L. 86-36
EO 1.4.(c)

[redacted]

[redacted]

ASCC Nickname	GMAIC Designator	Description
SCARP	SS-9	Third-generation intercontinental ballistic missile
STYX	SS-N-2	Naval aerodynamic antiship missile
SCUD A	SS-1b	Short-range tactical ballistic missile
GRAIL	SA-7	Man-portable, shoulder-launched, heat-seeking SAM
GALOSH	ABM-1	Ballistic missile defense system
KIPPER	AS-2	Supersonic aerodynamic cruise missile carried by BADGER C (TU-16)
ASH	AA-5b	Infrared homing variant missile carried by FIDDLER (TU-128)

Another missile name probably familiar to many readers is FROG, which is not a nickname but an acronym for Free Rocket Over Ground. Abbreviations, like acronyms, are not controlled, and considering all the complexities and ramifications of coverterms of all kinds, freedom from control may be an attractive feature for some potential namers of projects.

[redacted]

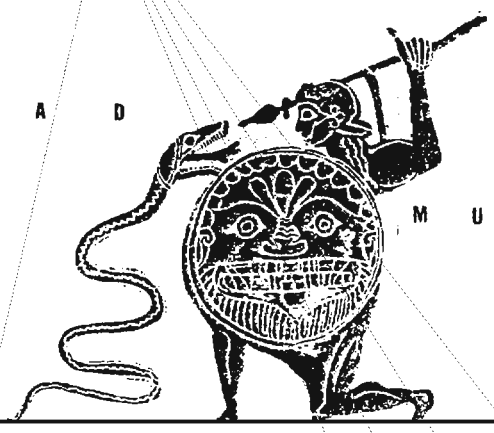
[redacted]

For guided missile designators, as for aircraft names, the first letter expresses the type: S for surface-to-surface missiles (SSM), G for surface-to-air (SAM), K for air-to-surface (ASM), and A for air-to-air (AAM). The 1972 reserve list of names perhaps reflects expectations for the future; 29 names, ACRID to AUBURN, are held in reserve for A, 19 for K, nine for

P.L. 86-36
EO 1.4.(c)

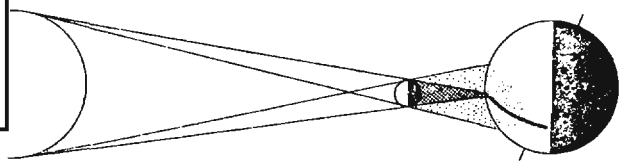
~~SECRET~~

P.L. 86-36
EO 1.4.(c)



as an example, is VINSON, covername for a half-

cal. PARKHILL, for example, refers to



One peculiar communications security requirement is reflected in a special group of coverterms used to identify and protect COMINT and distinguish between its categories. These are the familiar COMINT codewords. They belong to the cryptologic community, and ultimate authority for them lies with the United States Intelligence Board, the London Signal Intelligence Board (LSIB), representing the U.K., Australia, and New Zealand, and the Canadian Intelligence Advisory Committee (IAC).

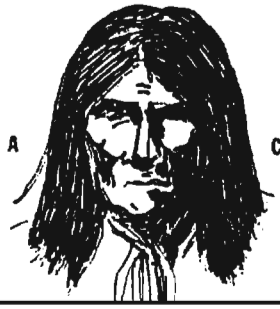
P.L. 86-36
EO 1.4.(c)

~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36

USIB, LSIB, and IAC jointly select the COMINT codewords and decide when they are to be changed. The current three, used for Category III, Category II, and Subcategory II(X) COMINT, came into effect in 1969 , about nine months after the compromise of the previous codewords resulting from the PUEBLO seizure. Change has been infrequent in recent years, because change means massive and costly administrative problems and is necessarily slow. Just the practicalities of disposing of and arranging for preprinted paper stock and rubber stamps take time and work, to say nothing of all the computer programs that have to be updated to incorporate changes.

COMINT codewords must be five-letter, pronounceable, infrequently used words that are not offensive or derogatory and do not reveal their COMINT meaning. The codewords are unclassified by themselves. When used on rubber stamps or preprinted paper stock they are CONFIDENTIAL, HANDLE VIA COMINT CHANNELS ONLY. When used in their codeword sense they take the classification of the category to which they apply. That means that when, for example, the word SPOKE is defined as the codeword for Category II COMINT, or when it is used in any way in specific reference to COMINT, then it is itself classified SECRET, HANDLE VIA COMINT CHANNELS ONLY. Other restrictions are the same prohibitions that apply to other coverterms: they must not be the name of an English poet or a Roman emperor, not a mythological designator, and not listed in JANAP 299 or its successors.



JANAP 299 (A), dated September 1971, contains an index of all codewords authorized for use by the Armed Forces of the United States. Codewords are assigned to designate classified plans, projects, operations, movements, locations, etc., and they are assigned in blocks of 10 to components of the Department of Defense.

One final source of prohibited words is another JCS document, ACP 119(A). This document provides lists of voice callsign root words for Allied tactical use, convoy internal voice callsigns, and search and rescue callsigns.

Voice callsigns for tactical aircraft are based on a root word assigned to the parent command or activity, with a suffix for the aircraft. APACHE ZERO SEVEN, for example, means aircraft 07 of the 541st Tactical Fighter Interceptor Squadron (APACHE).

A convoy is assigned a two-letter or figure-letter group called a convoy radio distinguishing group before sailing. Fixed suffixes denoting function are used with these distinguishing groups for internal convoy communications. Among these fixed function suffixes are CHIEF for the commodore, LUCK for the vice commodore, and TEAM as a convoy collective, so that the internal callsign for the commodore of a convoy assigned radio distinguishing group XY would be XRAY YANKEE CHIEF.

In the search and rescue callsign system also, a basic callsign is assigned to a function. These function callsigns are supplemented with a geographical reference for certain operations and a number suffix for others. BULLMOOSE is the callsign for any and all search and rescue airplanes, so that BULLMOOSE ARGENTIA would be the callsign for any search and rescue aircraft operating in the area of Argentia, Newfoundland. SAPPHIRE is the callsign for a search and rescue boat, so SAPPHIRE FOUR would be search and rescue boat number 4. In addition to these, four-letter scene-of-action callsigns are used in both military and non-military communications. The callsign HAWK, for example, is used for any air force airplane at the scene of action, ABLE for any helicopter, CREW for any navy airplane, and TIFF for the senior officer present.

Finally, certain voice callsigns are known and used internationally:

MAYDAY	Distress signal (SOS)
SECURITY	Safety signal
PAN	Urgent signal

EO 1.4.(c)
P.L. 86-36

P.L. 86-36
EO 1.4.(c)

If you are a potential user of a coverterm, you may feel, now that you appreciate all the complexities, that life would probably be simpler if you just skipped the whole thing and used an acronym or abbreviation. But, as Mrs. Marjorie E. Miller, the NSA/CSS Cover Term Officer, writes:

"Besides the fact that you would possibly be in violation of security, abbreviations and acronyms are sometimes misleading or confusing due to multiple use of the same letters for various words or phrases. The acronym BOSS, for instance, has the meanings: BMEWS Operational Simulation System, Broad Ocean Scoring System, Bioastronautics Orbital Space Satellite, Burroughs Operational Simulator. PAR means--in addition to its common use for 'paragraph' and 'parallel'--Precision Approach Radar, Perimeter Acquisition Radar, Palletized Airborne Relay, and probably many other things. Others with multiple meanings that we have run into in this office are AIDS, ADAS, ATR, DDC, MAD, MTR... After looking this over you may decide that what appears to be 'an attractive feature' (freedom from control) is not a bargain after all."

Anyhow, the problem isn't really all that bad. The whole system can be summarized in the chart below.

As always, when you have a problem, the best thing to do is ask someone who knows the answer. The people listed below have been most helpful in supplying information for this article, and will assist you, too. [redacted] will give you guidance on the general procedure for a coverterm request, and the others will help in their special fields, at need.

GENERAL	Mrs. Marjorie E. Miller, C513, Room 2N090, tel. 5801s
ASCC NICKNAMES	[redacted] C534, Room B6114, tel. 8657s
CANUKUS NICKNAMES	Mr. Paul W. DeCamp, W2, Room B4135, tel. 8891s
" "	[redacted] W09, Room 3W116, tel. 3401s
COMINT CODEWORDS	Mr. G.P. Morgan, D41, Room 9A187-3, tel. 5825s
COMPUTER PROGRAM NAMES	[redacted] C09, Room 1S013, tel. 3321s
COMSEC DESIGNATORS	Mr. John J. Sullivan S133, Room C2A24, tel. 2343s
NSOC/AUTOLINE	[redacted] V36, Room OE229, tel. 3412s
RESEARCH AND ENGINEERING	[redacted] R043, Room 2W038, tel. 5603s

ASSIGNMENT AND HANDLING OF COVER TERMS (U)

type of cover term	definition	authority	length	alphabetic allocation	security classification		exclusions
					word alone	word meaning	
1. Covernames a. general b. for use by R c. for use by C	A single word, under exclusive control of NSA, used to designate classified cryptologic projects, equipment, or operations.	NSA	one word (not five letters)	no restr.	usually unclass.	must be classified	Words listed in JANAP 299 or ACP 119; mythological characters; English poets, Roman emperors; first words of JCS nicknames; registered trade names; abbreviations, acronyms, etc.; two-syllable surnames; geographical locations
2. Nicknames	A combination of two separate unclassified words employed for unclassified administrative convenience.	DoD(JCS)	two words	first word must begin with DA, DE, HO, HU, HY, MA or ME	unclass.	unclass.	Words listed in JANAP 299 (first word) or two-word combinations listed in ACP 119; mythological characters; registered trade names; NSA covernames; trite words
3. Mythological Designators	Names from ancient pagan mythologies applied to general cryptosystems.	NSA	one word	no restr.	unclass.	unclass.	(Not Applicable)
4. COMINT Codewords	Designators assigned to identify source as COMINT.	USIB, LSIB, IAC	one word (tradition-5 letters)	no restr.	C-CCO when used w/o class.	class. of category plus CCO	Words listed in JANAP 299; mythological characters; English poets; Roman emperors; first words of JCS nicknames; registered trade names; abbreviations, acronyms, etc.
5. Code Words	Designators for classified military plans, operations, or geographic locations.	DoD(JCS)	one word	must come from JANAP 299	must be classified	must be classified	(Not Applicable)

(As of March 1975)

DOCID: 4009719

P.L. 86-36

THE USES OF ELINT

What we now call Signals Intelligence began as simple Communications Intelligence. It took us a while to discover the other half of SIGINT: Electronic Intelligence, in the form of radar signals, data signals, and electronic jamming. Many of us still have a rather hazy idea of what ELINT contributes, and the short article below may serve as a useful introduction to the subject.

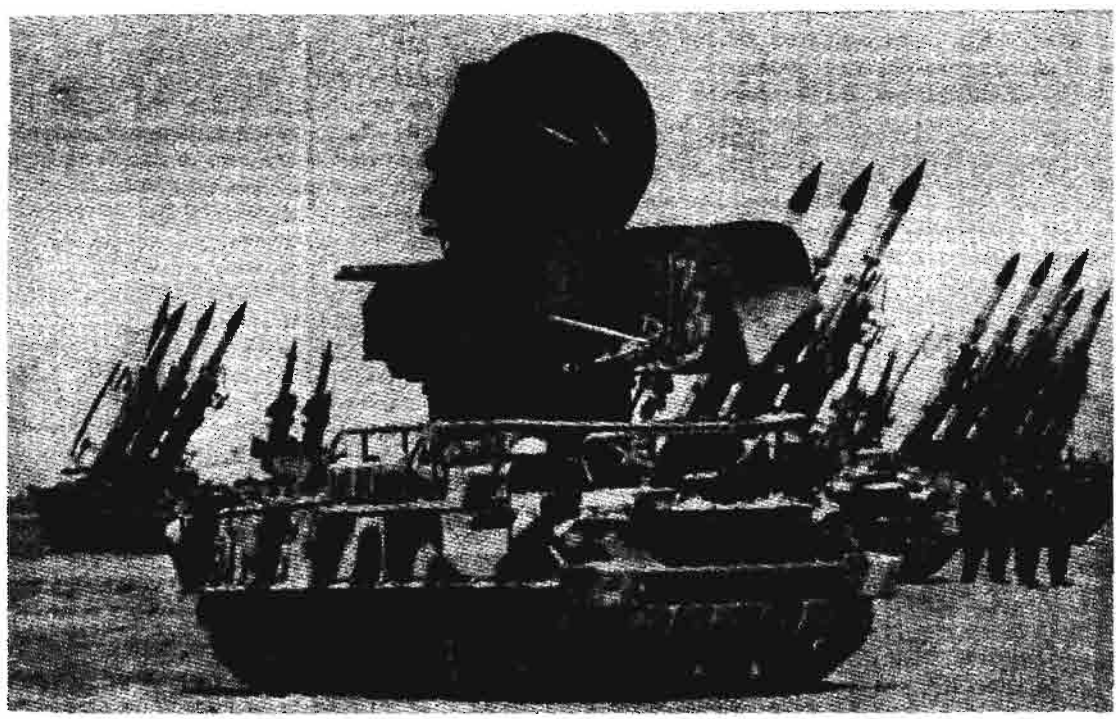
ELINT--Electronic Intelligence--is a part of the SIGINT effort that should become better known and better used by analysts in NSA/CSS. This article defines the two roles of ELINT--operational and technical--and gives examples of how each is used to aid in the SIGINT process.

The field of electronic intelligence covers the collection, processing, analysis, and reporting of information concerned with the non-communications electronic systems of target nations.

Operational ELINT is concerned with the identification, employment, deployment, trends and tactics of foreign radars, weapon systems, jamming signals, and data signals, in connection with specific operations. It employs event recognition*, all-source data, and SIGINT interaction, and produces both time-sensitive and term product reporting.

Technical ELINT provides detailed parametric information for assessment of the performance, capabilities and vulnerabilities of the above-mentioned emitters. Technical ELINT also provides the input for the development of electronic warfare tactics and electronic countermeasures equipment. Like Operational ELINT, it employs all-source data and SIGINT interaction, but the product is generally on a term basis rather than a time-sensitive one. A somewhat oversimplified explanation of the difference between the two is that Technical ELINT tells what the system is *capable* of doing while Operational ELINT tells what it *is* doing at a given time.

Let's take a look at an example. Below is a picture of the radar and missiles of the Soviet-built SA-6 surface-to-air missile system. (This is the system that obtained a great deal of publicity during the 1973 Yom Kippur War.)



EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~

Technical ELINT directly or indirectly gives us such details on the system as the following:

[redacted]

[redacted]

I could go on with examples such as the one above, but for purposes of this article let me just list some major items, including Key Intelligence Questions (KIQ's) to which ELINT can contribute:

[redacted]

[redacted]

I hope I have given the reader some feel for the nature and value of ELINT. As a final remark I would like to comment on the present emphasis within the Agency for a fused COMINT-ELINT product. As of 22 October 1974, the Operational ELINT job has been transferred from W Group to A, B and G Groups, in the hopes that COMINT and ELINT analysts working side by side will produce a better product--a fused product--which is more complete and responsive to our customers. The Technical ELINT function has remained in W, but that does not mean that the ELINT analysts in W do not need COMINT, as well as "PHOTINT," "HUMINT," etc. The better COMINT people understand the nature of ELINT, and vice versa, the easier it will be for this agency to satisfy our many customer requirements.

[redacted]

~~(SECRET SPOKE)~~

TAKE FIVE AND TRY THIS

Fill in the vertical five-letter words and find a punnish phrase reading across.

W.L.

C U D F A S S S A S W T D
U O T O M E D A R E E I A
E T Y E T L Y H S T S D Y

~~SECRET SPOKE~~

DOCID: 4009719

E.O. 1.4.(c)
P.L. 86-36

~~CONFIDENTIAL~~

LANGUAGE IN THE NEWS

EMERY TETRAULT, P16

P.L. 86-36

AT HOME

LANGUAGE PANEL NAMES NEW EXEC

[redacted] has replaced [redacted] as Language Career Panel Executive. [redacted] is now assigned to G77.

[redacted] brings to his new duties an impressive background in Soviet studies and Russian language along with extensive operational, supervisory and managerial experience.

MACHINE COURSE FOR LINGUISTS

For years linguists were either told absolutely nothing about machine processing or were made to learn one or more dialects of FORTRAN to the same degree of proficiency as a native speaker. Then a third way, a course about machine systems for linguists, was tried in at least two variants, and a revision of this approach is now under way. [redacted] P16, is developing the course in support of the National Cryptologic School.

For about one-third of the program, students will consider what must be done to plan and carry out a machine processing task. Topics in this section of the course will be: determining what computers can or cannot do for you, planing a job, stating requirements (for example, learning how to communicate with programmers), testing data and setting acceptance criteria for programs, maintaining quality control during production, providing documentation, and considering some of the junctures at which things are most likely to go wrong. Present plans call for a student project to accompany this part of the course; for example, a project to come up with a new application of machine processing and carry it through each of the steps covered in the course, or to take an existing (or past) application and analyze its strengths and weaknesses in terms of what has been presented in the classroom.

The rest of the course will be spent in surveying machine processing facilities: both computer systems and data processing systems. Under the former heading, students will be given a quick survey of NSA machines and there will be a discussion of some of the more frequently encountered terms and concepts such as "off-line," "on-line," "remote," "batch," "conversational," "interactive (fast, intermediate, slower) access," etc. The latter category includes processing systems and applications; [redacted] data bases; and the production of various working aids. As in the first section of the course, it is planned that students will be assigned some project such as analyzing the machine systems used in their own areas in terms of speed of turnaround, convenience of access, ease of use, etc., and writing up a detailed evaluation of these systems, or studying one or more of the machine-system applications related to their work, the systems which help process incoming traffic or outgoing product, produce working aids, etc.

Course materials will include a text, a glossary of terms, and a directory of machine services.

CLA NEWS

The Annual Business Meeting. Mark your calendar for the CLA's annual business meeting, which has been set for Tuesday, 6 May, 0930, in the NSA Auditorium. This is a particularly important meeting, since a full slate of officers (President-Elect, Secretary, and Treasurer) and two board members will be elected. One board member will be chosen for a regular three-year term and one for a two-year term. The latter is necessary because the most recently elected board member, [redacted] was transferred to Korea.

The members of the nominating committee are Jacob Gurin, P1, Chairman, [redacted]

SIGTRAN Lives! A Special Interest Group of the CLA, SIGTRAN (Special Interest Group for Translation), is forming under the guidance of [redacted] P16 (see CRYPTOLOG, January 1975). Mr. Whitney Reed's talk on free-lance translation was well attended, and by the time this issue of CRYPTOLOG emerges there will have been a second meeting featuring Mr. Arthur Salemme on the joys of technical translation.

P.L. 86-36

~~CONFIDENTIAL~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

.....And So Does the NSA Japan Forum!

Another new Special Interest Group, the NSA Japan Forum, held its first meeting 29 January. Lambros D. Callimahos spoke on Japanese World War II cryptosystems and the attacks on those systems by U.S. Army cryptanalysts.

A second program is planned for late March with Japanese language training, pre-war and post-war, the topic for a panel discussion.

...Not to Mention SIGVOICE.

One of the most dynamic and firmly established of the CLA Special Interest groups is SIGVOICE. In February [redacted] R54, spoke (twice) on "Voiceprints: Fact or Fancy?" (Voice prints are a fact, but Dr. Wood warned against expecting the same degree of reliability from them that one expects from fingerprints; handwriting analysis, he said, would be a better comparison.)

P.L. 86-36

ABROAD

BEIRUT, Lebanon - Akhram Hannoush, a Lebanese systems engineer, has a promising new business going in the Middle East with computers that work in both Arabic and Roman characters.

What's more, the computers being assembled by Mr. Hannoush's Systems Technology Corporation from imported components are competitive in price with big foreign suppliers and are tailored to the special needs of Middle Eastern customers.

The added dimension of making computers that answer in Arabic opens up a large number of potential users, such as an internal Government service sold to Saudi Arabia for more than $1-million.

A similar service, also in Arabic, has been installed in Egypt for the army.

The development of computers that work in both Arabic and Roman characters involves a more complicated keyboard for the computer operator and the design of components based on 64 characters, including letters and numbers, for Arabic, compared with 36 characters for Roman letters and numbers used by English and other Western languages.

Mr. Hannoush says that Systems Technology's units can be assembled for half the price of the large international computer companies' standard systems.

The concern now includes among its Lebanese customers the American University Hospital, Middle East Airlines, and Unicrat, the country's largest automobile parts distributor; in Egypt, the Arab International Bank and Cairo University, and in Kuwait, the Beidoun Trading Company.

Systems Technology has been financed by a group of Lebanese investors with backing from private Middle East capital.

(The New York Times, 26 January 1975)

Answer to last month's puzzle:

Can you make out the name?

EO 1.4.(c)
P.L. 86-36

The cryptolinguistic solution to this real-life puzzle was achieved as follows:

[redacted]

P.L. 86-36

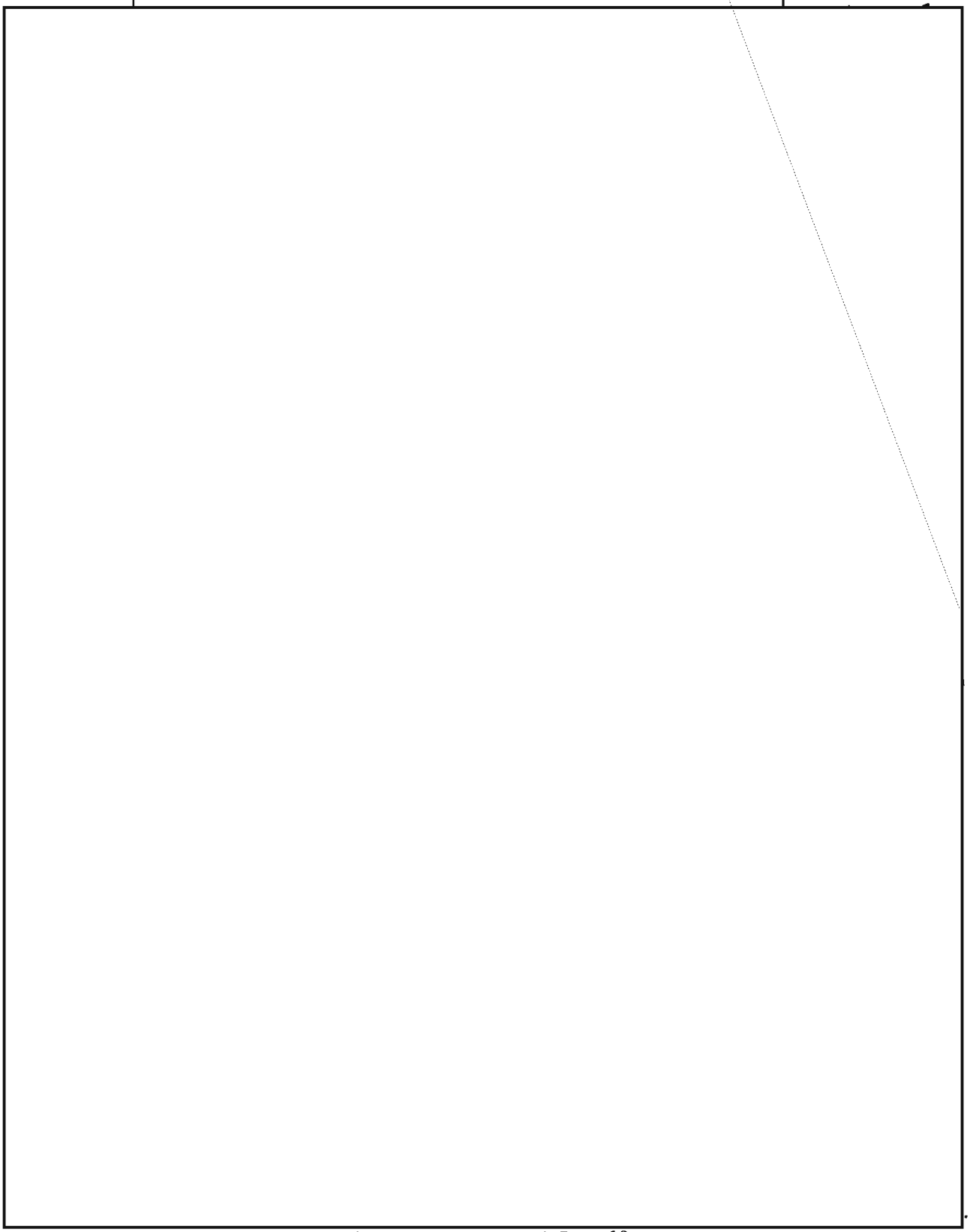
Moral: When you run into trouble on the conventional road to results, consider the possibility of a shortcut via Central Information.

~~(TOP SECRET UMBRA)~~

DOCID: 4009719

EO 1.4.(c)
P.L. 86-36

PSYCHING THE CODE CLERK:



DOCID: 4009719

~~(SECRET SPOKE)~~

EO 1.4.(c)
P.L. 86-36

OPTOCRGLY SPEAKING...

The name CRYPTOLOG, with its paucity of high-frequency vowels, doesn't seem to be very good material to play the word game with, but can you find 50 good English words of 4 or more letters, using only the letters in CRYPTOLOG? Usual rules for the game.

H.G.R.

LETTERS TO THE EDITOR

To the Editor, CRYPTOLOG:

Kudos to CRYPTOLOG for being a fine publication in general, but especially for printing the excellent Anne Exinterne series. Overall, the articles present cogent arguments and raise very many valid questions.

Drawing on my own experience as a member of the first intern group (in SR), I would like to comment specifically on a point or three:

1. I agree wholeheartedly that new employees should take basic courses in TA, CA, data systems, etc., as soon as possible. Hopefully, this could be done without placing them in a stultifying, wholly academic atmosphere. Anne's idea of placing new hires in productive jobs with plenty of allowance for courses, self-study or otherwise, is very good. Perhaps this could be formalized into a general "pre-intern" program, designed to give new hires some exposure to all the major Agency career fields. New employees could be given OJT assignments in each field while taking the courses. At the end of this period, they would have a fairly good overview of Agency operations as well as a good idea of which career field best suited them. The Agency would also have a more accurate indication of each trainee's actual abilities in each field, not just aptitudes. The trainees could then enter directly into an assignment in a suitable field or into an intern program for more specialized assignments and advanced courses. This method could eliminate the problem of employees being assigned to "wrong" career fields; and, by giving people good grounding in all the disciplines, it could make crosstraining easier for those interested in professionalizing in more than one field.

2. Anne touches on another problem briefly, that of the "dud" OJT assignment. I'm sure every intern has a tale about the office where he or she was allowed only to sort and file traffic; or about the "special study" that still lies unpublished in the supervisor's desk; or about the boss who told the intern there was no work to do, so "find something to keep busy!" Now I'm not saying that interns or "pre-interns" should not be exposed to what I call "drudge work," which is a necessary albeit tedious part of many Agency jobs. (The gathering and logging of data preparatory to tackling a CA problem comes to mind as a good example of drudge work.) "Dud" assignments are those in which the trainee is misused or not used at all. When reports come back that an assignment is a dud, that assignment should be checked out. If the job is really a dud, the trainee should be placed in another OJT assignment, and no more trainees should be put in that dud job. If the job turns out to be drudge work, but genuine work, the trainee should be told why he or she should remain in the assignment and why the job is a valid learning situation.

3. Lastly and leastly, I'd like to clarify the beginnings of the "FSG" title. A close friend and fellow intern returned from an interview for a job in D (or whatever it was then) and reported, incredulously, that the interviewer had dubbed her, as an intern, a "future super-grade." We didn't just laugh appreciatively at this story, we thought it was funny as hell. So we adopted the title as a cynical joke, attaching the initials (among others) to our names on notes among ourselves, or dropping the title in conversation. It was a good joke (and still is) and caught on and spread. If there were some later who began taking the title seriously... Well, I hope none of us who started the thing were silly enough to do that.

Thanks again for a good series.

[redacted] P.L. 86-36

DSA, SRA, EX-SRI, FSG, BA, HSG, etc.

DOCID: 4009719

To the Editor, CRYPTOLOG:

As an Agency employee for over 15 years, ten of which were spent in the cryptolinguistic field, I for one feel discriminated against. You see, I am a "bookbreaker," one of that special breed of people who live in limbo as far as professionalization is concerned. Why? Because we have no Career Panel to call "home": we have to visit elsewhere (Language, Cryptanalysis, Special Research, etc.) for our certification.

For years now, we "bookbreakers" have been told how special we are and how important our skills are to the Agency's mission. But when Professionalization came along, we were almost forgotten. I say "almost" because the Language Panel has thrown us a bone of sorts. For instance, if we take Part I (the open-source part) of the Language PQE, then we are allowed to take Part II which at our option has a bookbreaker's part. We can only do this, though, if we pass Part I, which for some may be quite difficult, for translation is something we do not do every day.

The CA PQE is even harder for us than the Language test. Less than 10 percent of the most recent CA test dealt with bookbreaking. It appears that the trend is away from hand systems and more toward statistics.

As far as points toward professionalization are concerned, I am sure I would receive the maximum amount from a Bookbreaking Panel for experience, but with the other panels this is not always true. And, to qualify for maximum points from those other panels, required courses have to be taken and as a result valuable time, money and effort would be wasted by the "bookbreaker" trying to become a linguist or a "cryppie."

As an individual who has attended "Bookbreakers" Forums and has regularly received "Bookbreakers Notes" from meetings, I do not welcome the idea of having to compete with the linguists (translators/transcribers) or cryppies in this Agency for professionalization as I am sure they would not want to compete with the "bookbreakers" for certification if there were no Language or CA Panels.

Duncan Battison, B34

Mr. Battison poses a question that has troubled thoughtful NSA people for years. Where the bookbreaker fits into the SIGINT professionalization scheme is at once a semantic question of definition of terms and a human question of fair dealing for the people involved. Is a bookbreaker one who "breaks into" a code? Then he must be a cryptanalyst. Is he one who "reconstructs a codebook"? Then he must be a language analyst. Is he both--or neither, but a special breed as Mr. Battison contends?

It seems to us that we must define the umbrella term "bookbreaker" which now covers both the crypt and the language skills necessary to turn encoded text into plain language through analysis. Then we can identify the special experience, training, and attributes of those who exercise those skills.

CRYPTOLOG solicits the views of its readers on this thorny question whose answers affect the livelihood of people who engage in this peculiarly SIGINT occupation. Responses will be published in a future issue.

Crypt. Ed.

Are We Getting Through to You?

If your personal copy of CRYPTOLOG is not correctly addressed, or if your organization is getting too few (or too many) copies, please let us know on the form below, so that our distribution list can be corrected. Clip and send to CRYPTOLOG, P16.

On individual-distribution copy addressed to _____(name)_____

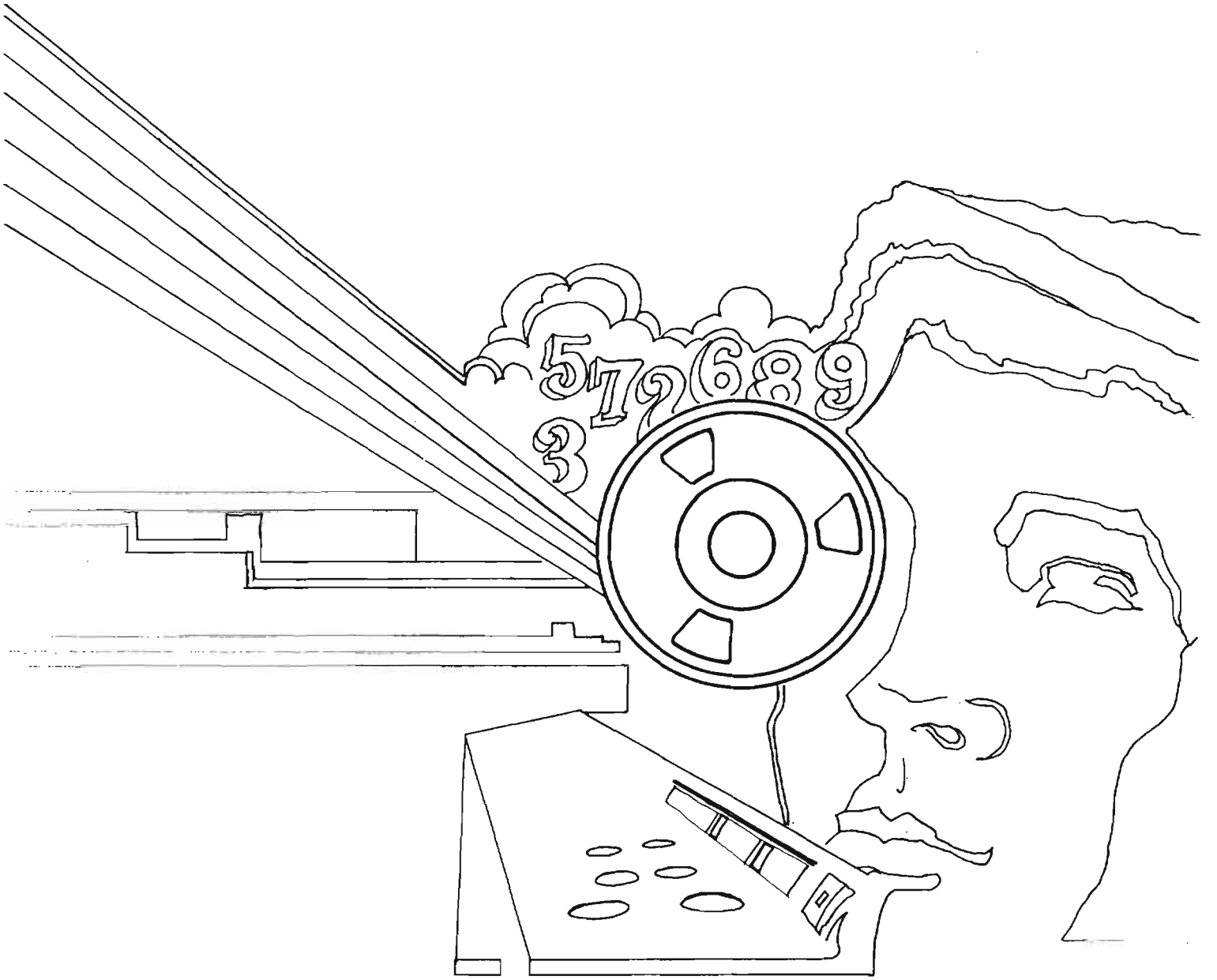
☐ Please change organizational designator to _____

☐ Please change name to _____

On organizational distribution, please change number of copies for

____(organization)____ to _____ copies.

P1-April 75-S3-23558


5 7 2 6 8 9
3

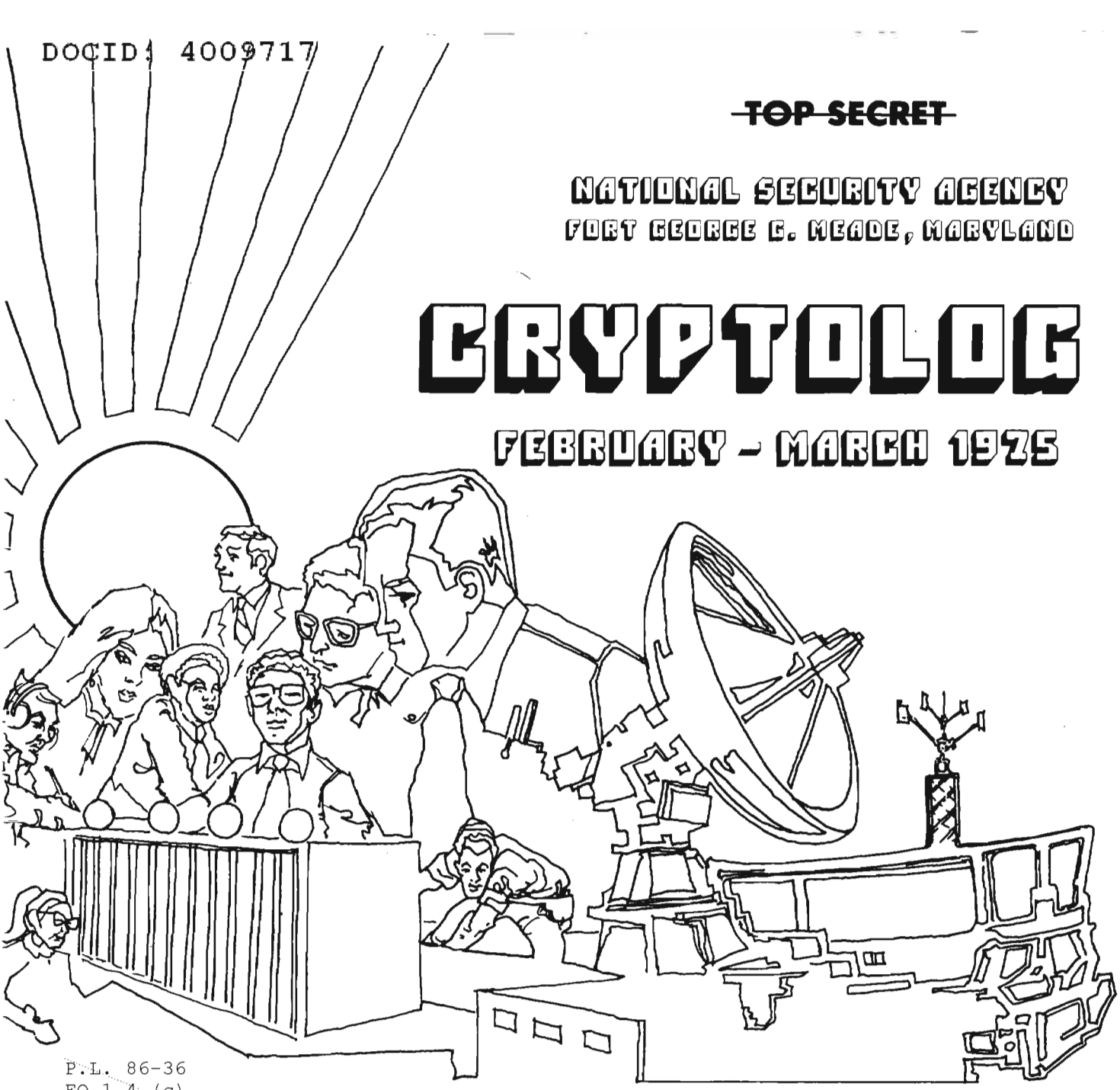
DOCID: 4009717

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

FEBRUARY - MARCH 1975



P.L. 86-36
EO 1.4.(c)

BASIC PATTERNS OF [redacted] CODES AND CIPHERS..... [redacted] 1
GLOSSARIES VERSUS DICTIONARIES.....Jacob Gurin.....5
THE DEVIL'S DICTIONARY.....C.W.B. & B.L.Z.B.....6
REPLACEMENT OF THE GUPPY LIBRARY..... [redacted] .7
THE GULF OF TONKIN INCIDENT..... [redacted] .8
OPPORTUNITIES.....10
GUIDE TO RUSSIAN TECHNICAL TRANSLATION (Review).. [redacted] 11
THE ROLE OF THE STATE DEPARTMENT INTERPRETER..... [redacted] 13
GOLDEN OLDIES: THE MOLECULE SUPERSERIES.....18
CAN YOU MAKE OUT THE NAME? (Puzzle)..... [redacted] 18
LETTERS TO THE EDITOR.....19
CAMINO NEWS..... 21

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA (NSAM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009717

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. II, Nos. 2 and 3 FEBRUARY-MARCH 1975

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief..... Doris Miller (5642s)

Collection..... [redacted] (3571s)

Cryptanalysis..... [redacted] (8025s)

Language..... Emery W. Tetrault (5236s)

Machine Support..... [redacted] (3321s)

Special Research..... Vera R. Filby (7119s)

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

DOCID: 4009717

EO 1.4.(c)
P.L. 86-36

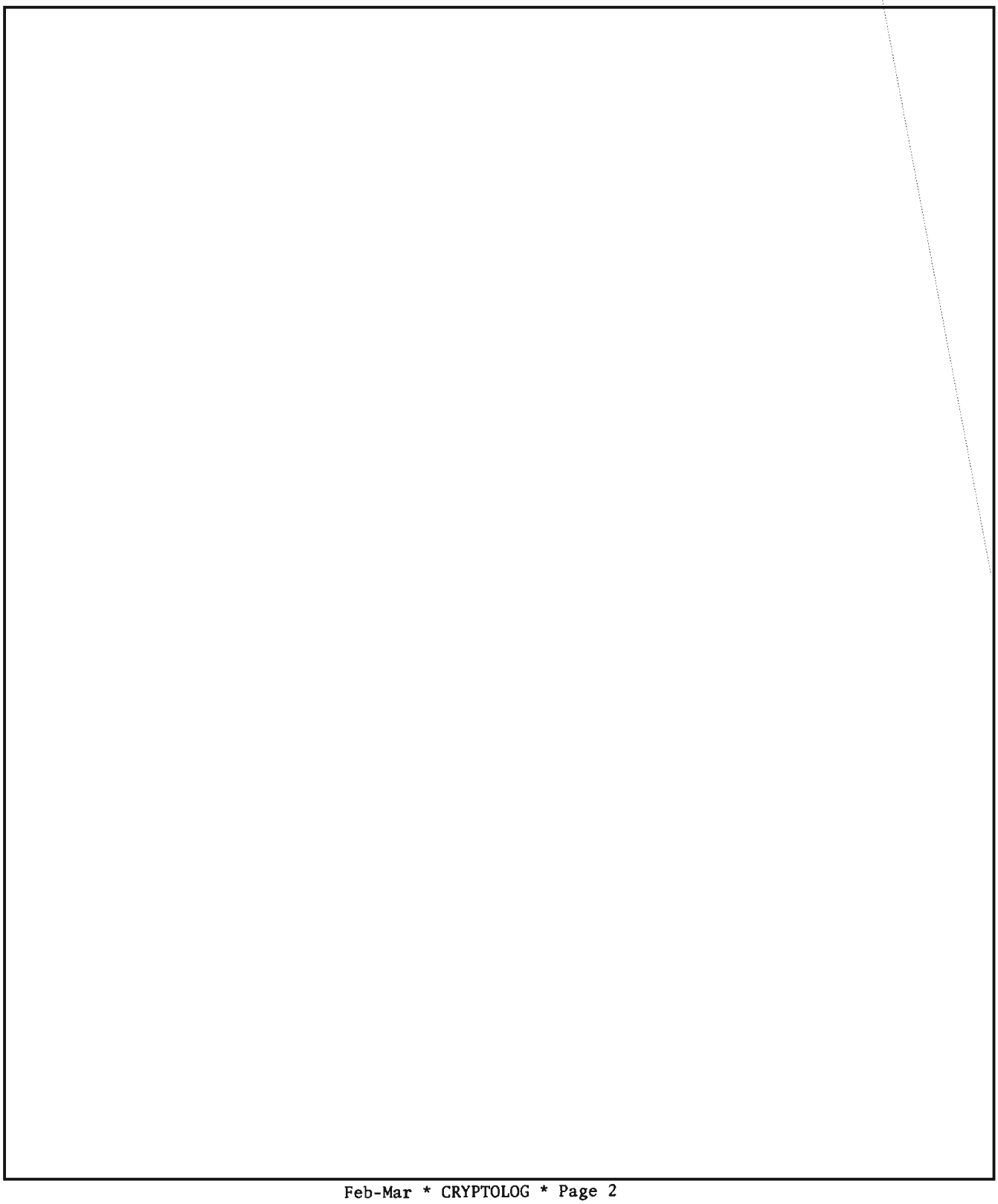
BASIC PATTERNS OF [redacted] CODES AND CIPHERS

P.L. 86-36

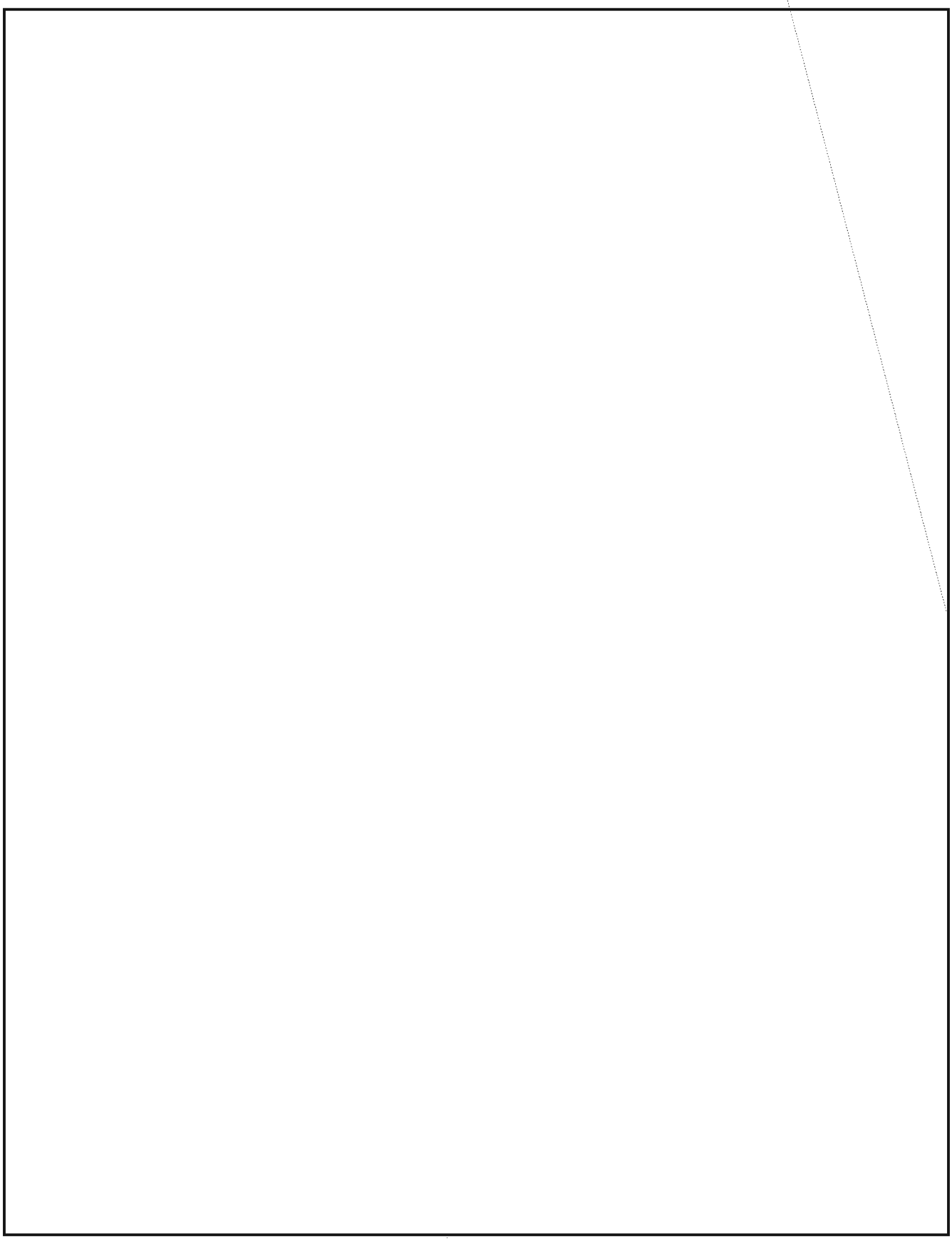
[redacted]

EO 1.4.(c)
P.L. 86-36

~~TOP SECRET UMBRA~~



EO 1.4.(c)
P.L. 86-36



DOCID: 4009717

EO 1.4.(c)
P.L. 86-36

[redacted]

[redacted]

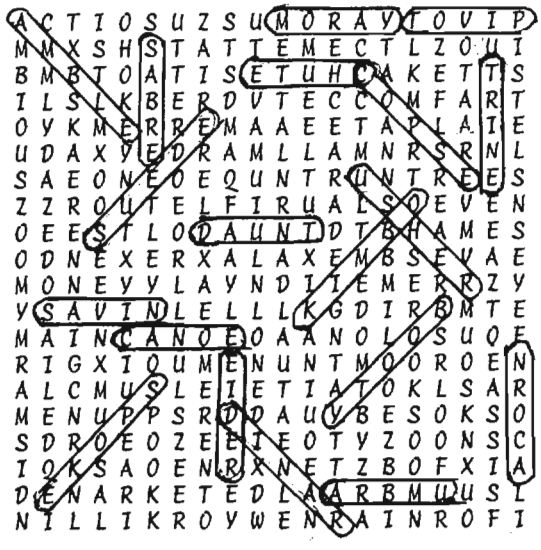
~~(TOP SECRET UMBRA)~~

FIRST LOSSES

Our editorial board has lost two [or, in a sense, three] editors this winter. [redacted] *who was both Language Editor and Art Editor, has moved on to new duties. William Jackson, the TA Editor, retired from the Agency in December.*

Our thanks to both for their parts in creating CRYPTOLOG and making it (we hope) a friendly visitor to your desks.

ANSWERS TO LAST MONTH'S "CROSSED CODEWORDS"



~~(SECRET/HVCCO)~~

P.L. 86-36

DOCID: 4009717

GLOSSARIES versus DICTIONARIES: WHICH SHOULD IT BE?

LEXICOGRAPHIC CORNER

by JACOB GURIN, P16

Back in 1952, when the Language Research Branch was being set up in the Office of Training, we debated the ways we could provide materials of real value to linguists in the Production Organization and the School. Our objective, as we had explained it to General Ralph Canine, then Director of NSA, was to produce training and reference works which would be needed if the Agency were required to jump quickly into the processing of a relatively unfamiliar language. Our experiences with Korean had demonstrated how disastrously unprepared we could be.

We described a variety of possible publications in each language: readers, handbooks, courses, and glossaries. We agreed from the start that our lexicographical activities would be limited to glossaries--dictionaries were out! I suppose that we made a simple distinction between the two: glossaries were limited both in subject-matter coverage and in the extent of treatment of any entry. Dictionaries suffered no such restriction.

Presumably these NSA glossaries would be designed to contain the kinds of words one could expect to run into in traffic: military terms, diplomatic expressions, communications, etc. Yet somehow NSA now finds itself sponsoring the publication of suspiciously large and detailed lexicographical works which admit frankly to being dictionaries.

No one should undertake the compilation of a dictionary without realizing that an enormous investment of time and effort--perhaps an impossible amount of each--is involved. Joseph W. Scaliger, a lexicographer of the late 16th century, said that the worst criminals should neither be executed nor sentenced to forced labor, but should be condemned to compile dictionaries, because all imaginable tortures are involved in such work. And in more recent times, Henry A. Gleason, author of An Introduction to Descriptive Linguistics, states, "Dictionary making is tedious in the extreme. It is exacting. It is an incredibly large job."

Should NSA linguists be taken off their job of producing reports and translations to get involved in the tedious, time-consuming job of producing large, full-scale dictionaries? I don't think they should.

There is, of course, one outstanding exception to this. When we approach a language for which lexical aids are either nonexistent or so rudimentary as to be worthless, and where little is known about the culture background of the language, compilation of a basic dictionary becomes a necessity. Experience has shown that in these circumstances the crypto-linguist has no choice but to cull whatever information he can from whatever sources are available to him to put together a general lexical treatment of the language.

How about taking time out from production duties to compile glossaries? This they should do. Perhaps a brief historical look at the development of dictionaries and glossaries will help put the problem (and the distinction) in focus.

The Glossary came first, and it had a simple origin. As the Glossarium, it was originally a collection of glosses; that is to say, it consisted of a list of difficult Latin words with either simpler Latin versions or equivalent words in the vernacular. These words were extracted from Latin manuscripts, together with the explanatory words (glossae) which had been entered by monkish scholars.

Another prime lexical source was the Vocabulary (or Vocabularium). In the time-honored way, Latin was taught by providing instruction in grammar and drill in vocabulary. Lists of words (vocables) were committed to memory and these lists, with their meaning in the local language, made up the vocabulary.

Glossaries and Vocabularies, still in manuscript list form, were often combined, since their functions were so similar. Eventually it became apparent that their usefulness would be increased if they were arranged alphabetically. At first this meant the lumping together of all words beginning with A, then a similar mishmash under B, etc. Later someone improved on this by sorting on the first two letters only. It took a long time for the idea of the full sort to take hold.

About the middle of the 15th century, the first strictly Latin-English dictionary appeared, called Medulla Grammatices (The Marrow of Grammar), and in the 16th century the Dictionary of

DOCID: 4009717

Sir Thomas Elyot, Knight was the first to use the term "dictionary" in this way. In medieval Latin, the word dictionarium (literally, a collection of dicta, "sayings") gradually took on the same functions as the word vocabularium. And it was this word, dictionary, which took the place of so many others, such as Medulla Grammatices, Ortus Vocabulorum (Garden of Words), Promptorium Parvulorum (Children's Storehouse), Catholicon Anglicum (English Universal Treatise), Manipulus Vocabulorum (Handful of Vocables), Alvearie (Beehive), Abecedarium, Bibliotheca (Library), Thesaurus (Treasury), World of Words, Table Alphabetical, English Expositor, Ductor in Linguas (Guide to the Tongues), Glossographia, Etymologicum, etc.

Most of those names, although colorful, are self-explanatory. John Baret, who chose An Alvearie for the title of his 1573 work, referred to his pupils as "diligent Bees...gathering their wax and Hony into their Hive." He explained that his students perceived how much trouble it was "to come running to mee for every word they missed... I appoynted them...every day to write English before ye Latin, and likewise to gather a number of fine phrases out of Cicero, Terence, Caesar, Livie, etc., and to set them under several tytles, for the more ready finding them againe at their neede." Their experience shows that the need for developing adequate lexical aids based on terms actually encountered (with appropriate meanings for those occurrences) was as great 400 years ago as it is today.

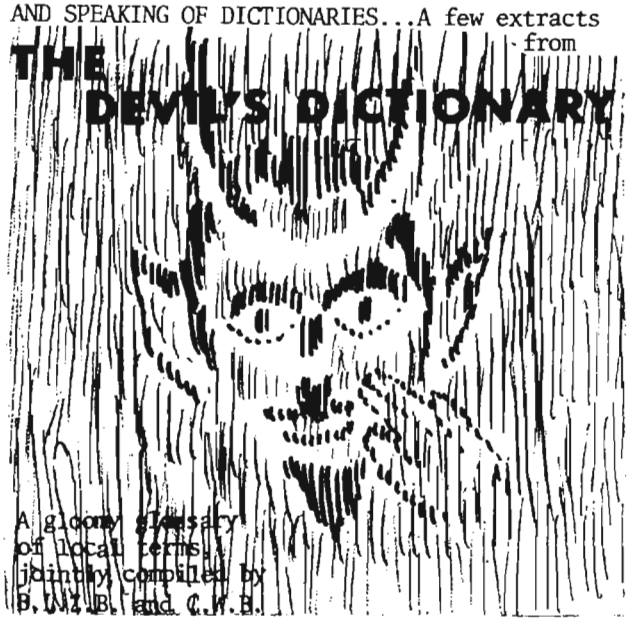
The principal stimulus to the development of dictionaries, in the modern sense, was the need to explain the hard words in one's own language. Accordingly, Robert Cawdrey in 1604 described his dictionary as:

> "A Table Alphabeticall, conteyning and teaching the true writing and understanding of hard usuall English wordes...with the interpretation thereof by plaine English wordes, gathered for the benefit and helpe of Ladies, Gentlewomen, or any other unskillful person."

By contrast, glossaries are still being published for Latin, for Anglo-Saxon, for dialects of various languages, ancient and modern. NSA is in a position to continue the old tradition by concentrating on glossaries, since our main concern is to provide clues to the meaning of difficult words in certain special forms of a foreign language, whether written or spoken, without any pretense of encompasing the entire range of the language, with all the literary and historical complexities of such an undertaking.

(UNCLASSIFIED)

AND SPEAKING OF DICTIONARIES...A few extracts from



Administrative paperwork: *the physical representation of mental constipation.*

Certification: *an imaginary line between two states of one's ineptitude, separating the imaginary abilities of one from the imaginary abilities of the other.*

Collection system: *a multimillion-dollar system for transforming electricity in the air to paper at Fort Holabird.*

Cryptanalyst: *one upon whom NSA sets its hopes during flaps and its dogs at other times.*

File: *a place where dead cryptosystems are laid to rest to await the coming of a C/A intern.*

Mathematician: *an unprincipled rogue who twists relationships in order to distort common sense into uncommon sense; for example: "Clearance + Need to Know = Access" becomes "Access - Clearance = Need to Know" or "Access - Need to Know = Clearance."*

Multiprocessor: *a computer which fails to do several jobs at the same time.*

Optimisim: *the doctrine or belief that management knows what it is doing.*

Preventive maintenance: *that which occupies the portion of the prime shift when the computer is working. (Regular maintenance, of course, occupies the remaining time.)*

Push: *one of the two things mainly conducive to success, especially at NSA. (The other is pull.)*

Reclama: *in government, to put the dice back into the box for another throw.*

Reorganization: *the admission of failure with a promise of improvement by the folly of managerial change.*

DOCID: 4009717

Replacement of the GUPPY Library

[redacted] P.L. 86-36

Recently, the PI Diagnostic Working Group was formed to recommend a replacement system for the GUPPIES on RYE. This group is directed by Dr. Donald E. McCown; other members represent the Offices of A, B, C, E, G, and P. Expecting a RYE phase-out in the next few years, the major considerations of the Diagnostic Working Group are being centered around the diagnostic and exploitation functions of the GUPPIES. Discussions are being held on the need to reproduce certain routines in another language and on another computer complex. Backup material for such an attempt must come from experienced programmers and cryptanalysts and from the existing RYE GUPPY Library.

The RYE GUPPY Library occupies a metal file cabinet in G4, 3AIII. This collection of some one hundred programs in 494 assembly language has been placed in folders in alphabetical order and covers the date periods from 1965 through the present. New 494 programs which are CA-related are added to the collection. Many of the older and very useful programs are maintained in this file: often, the only copy of a program may be found here. The original decks of many of the GUPPY programs have been misplaced, transported to other areas outside RYE, or have been lost in organizational maneuvers. The file reflects the expertise of Marjorie Mountjoy and Carolyn Palmer, who were instrumental in developing algorithms, style, strip arithmetic, and parameter set-up. Also reflected in the file is the work of other CA programmers who have contributed a great amount of effort to the GUPPIES. The importance of the Library in 3AIII is obvious.

In the event of a RYE phase-out, the records in the GUPPY Library will serve as a guide to rewriting those programs which deal with diagnosis and exploitation. Perhaps the coding in assembly language will be difficult to follow, but the existing flowcharts for the more complex programs can be read easily. The rewriting of the diagnostic and exploitation GUPPIES for a RYE replacement cannot serve cryptanalysts as well as RYE unless the new machinery affords similar outstation input/output capabilities.

A portion of the GUPPY Library includes Special Purpose programs which account for timely decryption and processing of several cryptosystems. These routines, while performing decryption, usually will call one or more of the TREES programs to reference a Meanings File (usually a foreign language), File update, or other File processing. While not as numerous as the real GUPPIES, the Special Purpose category may be just as important to cryptanalytic effort, if not more so.

The GUPPY Library serves other purposes in addition to housing a collection of source listings. To find a failing point in a program, a bad load, or the limits of a parameter, a listing of the assembly language and an octal dump are an absolute necessity. To chap or make a correction in a program is impossible without the actual assembly containing its octal locations and machine language coding. Clever and concise coding is often studied by other analysts and programmers as an aid to their own work. The maintenance of the GUPPY File has to some extent restrained duplicate programming and rediscovering the wheel. CA-260 covers many areas of the 494 Library. The diagnostic and decryption effort of NSA has leaned heavily on this Library for years.

A replacement of the GUPPY Library, once the programming language and the machine have been chosen, will require the same maintenance as the present Library. Continuity and control are just as important here as in any other technical operation. To continue programming support for cryptanalytic groups, the Diagnostic and Exploitation Working Group must be informed at least a year prior to RYE phase-out as to the new computer(s) and language for program rewriting. No other approach for Special Purpose and GUPPY planning appears practical.

DOCID: 4009717

THE GULF OF TONKIN INCIDENT

Walter D. Abbot, Jr.
B11

In late 1961--early 1962 a series of U.S. Navy patrols off the east coast of Communist China was proposed. The purpose of these patrols was to be three-fold. In the first place they would establish and maintain the presence of the U.S. Seventh Fleet in the international waters off the China coast; second, they would serve as a minor Cold War irritant to the "Chicoms"; and third, they would collect as much intelligence as possible concerning Chicom electronic and naval activity.

The initial phasing called for one U.S. destroyer to conduct each mission. There would be three installed positions on each mission (two radiotelephone and one manual Morse), and these positions were to serve a dual role--provide direct SIGINT support to the defense of the ship, and serve as intelligence collection facilities for as many different sources and categories of emission as could be obtained. These patrols were given the cover name DESOTO.

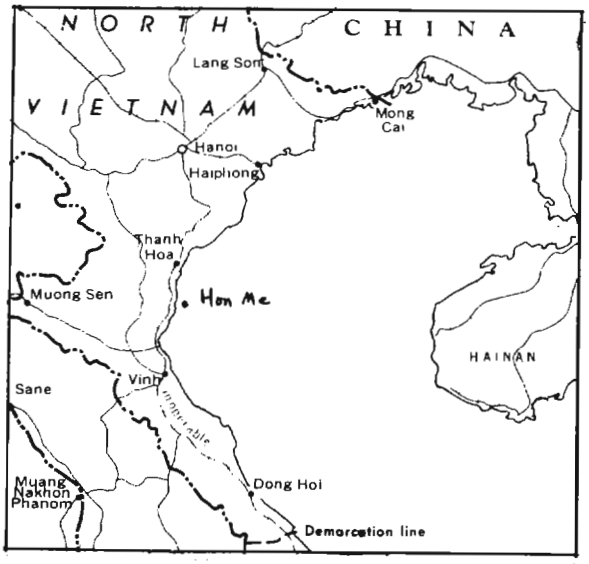
From 14 to 20 April 1962 the first DESOTO patrol was conducted, with the destroyer USS DE HAVEN as the participating vessel. The area of responsibility encompassed by the mission focused around the Tsingtao area of the Yellow Sea, and the ship was instructed not to approach any Chicom-held territory, including the offshore islands, closer than 10 miles.

Major intelligence targets for this mission fell into five categories: Chicom naval units, particularly submarines; ELINT of Chicom electrical installations; Chicom air activity; hydrographic and weather information; and merchant shipping (particularly Chicom) in the area. This first DESOTO patrol was singularly effective in evoking Chicom reaction. Such things as shadowing of the DE HAVEN by three or more Chicom vessels at one time, jamming of the DE HAVEN communications facilities, and the use of deceptive pennant numbers on the shadowing vessels all contributed to the success of the intelligence effort on this mission. In addition, the Chicoms issued three "serious warnings" to the DE HAVEN for violation of territorial rights during the 7 days the mission was in progress.

For the remainder of 1962, eight more DESOTO patrols were run, and prior to December of that year, these patrols were all conducted in the East and North China areas as well as up the Korean coast to the Soviet Gulf of Tartary. After the first mission, intelligence derived from the patrols was quite sparse. Shadowing of the patrol vessels was noted, and serious warnings were issued to almost all the patrols by the Chinese Government, but unique information was virtually nil.

In December 1962, with DESOTO patrol number IX, the USS AGERHOLM conducted the first probe into South China waters and the Gulf of Tonkin around Hainan Island. This pattern was repeated in April 1963 when the USS EDWARDS traversed the same path around Hainan Island and then extended its mission down the coast of the Democratic Republic of Vietnam (DRV). No DRV reflections were recorded at this time, and Chicom reaction was again limited to shadowing and issuance of serious warnings. Since serious warnings were not reserved for DESOTO missions (at that time the U.S. had received over 350 of these warnings for both air and sea violations), no particular significance could be attached to them.

The first DRV reaction to a DESOTO patrol came in late February--early March 1964 on the third venture into the Gulf of Tonkin, this time by the USS CRAIG. DRV radar stations performed extensive tracking of the CRAIG on her first run up the coast, and DRV naval communications referred to the CRAIG by hull number on one occasion. Although intelligence collected from this mission was not voluminous, it did contribute new insight into the placement and capability of DRV tracking stations and equipment.



Prelude to Violence

The fourth DESOTO patrol into the international waters of the Gulf of Tonkin was programmed in July 1964. Concerned more with the Vietnamese problem than the Chicom problem of its predecessors, this mission was to observe the junk fleet vessels believed to be a constant source of resupply to the guerrillas in the south, obtain navigational and hydrographic information, and procure any available intelligence on the DRV navy. Since the 1954 Geneva agreements specifically prohibited the DRV from establishing a navy, the emergence of this force had been, until late 1963--early 1964, extremely covert. During late 1957 the first DRV naval communications facilities were isolated with an estimated 30 ships involved in the transmissions. Then in 1959 the first evidence of the emergence of a modern DRV navy was noted during a probable joint DRV/Chicom naval exercise in the Pearl River estuary. Some of the vessels involved in this exercise were believed to be the same 10 motor gunboats later noted passing through the Hainan Strait, and probably represented the DRV's initial acquisition of modern naval craft. Augmentation of this force was continual after 1959, and as of late 1964 the DRV navy had a total complement of nearly 100 vessels.

Armed with this background, and clear on the purpose of the mission, the USS MADDOX reached a point on the 17th parallel about 12 miles off the coast of the DRV on 31 July 1964 at 1300 hours local time. From that point the MADDOX turned northward on a tack that was to take her up the coast for three days in what was believed to be another routine running of a DESOTO patrol.

Confrontation

Apparently the MADDOX was not the only vessel active off the North Vietnamese coast on the night of 31 July. DRV naval communications reflected that on that date the "enemy" had fired upon the island of Hon Me, and had been pursued by DRV warships to no avail. The MADDOX reported sighting vessels being pursued by DRV patrol craft, but had made no attempt to investigate the action.

Whether or not an association between the above-mentioned attack and the presence of the MADDOX was drawn by the DRV is impossible to say. They did protest to the International Control Commission that "American imperialists" had shelled their fortifications, but that was a constant complaint of the DRV and could not be directly attributed to the presence of the MADDOX. However, as the MADDOX resumed the prescribed patrol route on 1 August, a route which required her to pass Hon Me Island, DRV naval authorities reflected their awareness of the MADDOX when they mentioned that the "enemy" was "going on a course of 52 degrees...9 nautical miles from Hon Me..."

Shortly after placement of the MADDOX near Hon Me Island by DRV tracking authorities, a message was passed to an unidentified DRV fighting vessel stating that it had been "decided to fight the enemy tonight." The MADDOX was apprised accordingly in a warning which preceded the actual attack by more than 12 hours.

DRV naval tracking stations were observed in continual surveillance from that time on. In addition, several messages were intercepted, apparently pre-positioning warships in preparation for the attack.

Between approximately 1130 and 1215 (Saigon local time) on 2 August, the MADDOX reported sighting three PT's and two probable SWATOW-class PGM's (motor gunboats) about 10 miles north of Hon Me Island. During the same time frame the MADDOX reached the northernmost point of its mission and observed a large junk fleet (approximately 75 craft), which it intended to avoid on its return route. There were no military ships intermingled with the junks, and there was still no apparent hostility.

It is not possible to ascertain exactly which element of the DRV naval command ordered the attack, but shortly after the MADDOX reached the apex of its mission, a message was passed stating that it was time to close with the "enemy" and use torpedoes. The MADDOX received this information some 50 minutes before the aggressive actions commenced.

At 1530, some 30 miles from shore, the MADDOX altered her course to the southeast, heading for the mouth of the Tonkin Gulf, and increased her speed to 25 knots, attempting to avoid the three DRV torpedo boats reflected on radar as closing at about 50 knots, within 20 miles of the DESOTO ship. At that time the MADDOX requested air support and posted all hands at their battle stations.

By 1600 the DRV boats were within 5 miles of the MADDOX, still traveling at about 50 knots, and had moved into column formation, an accepted procedure for torpedo assault. The MADDOX fired three warning rounds across the bow of the lead ship, but for naught; and at 7 minutes past the hour, the MADDOX reported that she was under attack.

The PT boats broke into two formations as they closed on the stern of the MADDOX, with two of them approaching from the right side and one from the left. At a range of 2700 yards the two PT's on the right each launched one torpedo. The MADDOX then turned to the left to avoid the torpedoes, keeping the attacking craft under fire, and scored a direct hit on the PT approaching from the left, just as that craft placed a torpedo in the water. The tor-

DOCID: 4009717

pedo did not run. Air support from the TICONDEROGA arrived at that point and engaged the attacking vessels, and the MADDOX withdrew from the area. Total damage: one DRV PT boat dead and burning in the water; extensive but not totally disabling damage to the other two PT's; and slight damage to one gun on the MADDOX.

In order to assert the right of the U.S. to freedom on the seas, it was decided that the DESOTO patrol should be resumed as soon as possible. The strength of the patrol was doubled, with the USS TURNER JOY joining the MADDOX for a proposed four-day continuation of the mission; a formal warning was issued to the DRV authorities in Hanoi, stating that any further such unprovoked actions would result in severe retribution; and at 0900 on 3 August, the DESOTO mission was resumed. For this phase, continuous combat air support was provided.

During the day of the 3rd, the MADDOX reported that both she and the TURNER JOY had picked up radar signals and believed they both were being shadowed. This same suspect shadow activity occurrred during the daylight hours on 4 August, but there were no provocations. Then the DRV naval communications facilities were observed alerting two SWATOW-class PGM's to make ready for military operations on the night of the 4th. The DESOTO units were advised of the possible attack, and headed for the mouth of the Gulf "at best speed."

The MADDOX reported several radar sightings of apparent hostile craft throughout the early evening hours of 4 August. Some of these sightings later broke away, but some of them continued to close. At about 2200, the MADDOX reported firing on an attacking PT boat which had presumably launched a torpedo. Three more probable PT's were tracked closing rapidly on the DESOTO ships, and continual torpedo attack was reported through 0035 on 5 August. During the attack period the two DESOTO vessels engaged several radar contacts, and the TURNER JOY reported that one vessel was probably sunk. It was also reported that a DRV PT boat may have sunk one of its own companions in the conflict.

The weather throughout the attack was overcast and cloudy, thus impairing the visibility of the support air fighters and making it impossible for them to sight the assailants. The DESOTO patrol initially reported that at least 21 torpedoes were launched during the battle. This figure was viewed as highly unlikely since the PT's carried only two torpedoes each, with no known on-sea reload capability, and the total DRV PT force was estimated at around 13, three of which had been damaged in the fighting of the 2nd. The figure was later amended when it was determined that the sonar operators may have seen their own propeller beats reflecting off the rudders during the zigzagging evasive action followed by the two DESOTO ships.

In retaliation for this second hostile action, JCS ordered CINCPAC to conduct a one-time maximum effort air strike against selected DRV targets, to include several ports known to house SWATOW-class PGM's and PT's, as well as a "priority one" hit on the Vinh oil storage area. This strike commenced on 5 August at 0700 and resulted in an estimated 90% destruction of the Vinh oil storage area plus total or partial destruction of approximately 29 DRV naval vessels. The U.S. lost two aircraft in the 64 sorties that were flown, and suffered severe damage to a third. In addition, one U.S. pilot was killed and another was captured.

The MADDOX and the TURNER JOY resumed the DESOTO mission of 6 August without further incident, and the rest is just painful history.

(At the time of the Gulf of Tonkin incident the author, then in the Army, was on his way home from USM-9, Clark Air Force Base, Phillipines, to NSA, where he became the reporter for the North Vietnamese Branch (B261). It was in connection with one of the post mortems on the incident that he gathered together the information presented in this story.)

~~(TOP SECRET UMBRA)~~

opportunities

A RYE program, PUNCH, converts punched information on cards to Field Data on paper tape. The resulting tape can be used as input to other programs. For parameters or program descriptions, call J.D. Tankersley on 3109s.

P.L. 86-36

Copies of the Guide to Russian Technical Translation, reviewed on pp. 11 and 12, may be obtained by calling Mr. Salemme on ext. 5642 or 5236, or by sending a request to him, care of P16.

The course in codebook reconstruction, CA301, to be taught by [redacted] is scheduled to begin 24 March. Those interested should contact [redacted] as soon as possible, on ext. 3045s, since class capacity is limited, and in addition it is hoped to tailor the class, to the extent possible, to meet the needs of the students. Programmers welcome!

* * * * * * * * *

A cluster of radio stations is sometimes called a complex. A psychological fixation is likewise a complex. Thus a traffic analyst who insists on calling his targets a complex can be said to have a complex complex. But complex also means complicated. So if the analyst's problem is complicated by other factors as well, he has a complex complex complex.... Would you like a job on one of the SIGINT terminology panels?

DOCID: 4009717

[redacted] reviews ARTHUR SALEMME'S P.L. 86-36

GUIDE TO RUSSIAN TECHNICAL TRANSLATION

Colleagues and friends of Arthur Salemme have been well aware that for several years now he has had squirreled away in his desk drawer two fat sheaves of typescript, the draft of a manual for Russian translators. Those who had had the opportunity to read even a part of the draft had been impressed and had urged Arthur to publish, but as so often happens, the more immediate concerns--the "short-fuse" project, the current flap--continually claimed priority and publication had come to seem at best a remote probability. Some of us, it now appears, have been unduly pessimistic. The Guide to Russian Technical Translation is at long last in print.

The idea for such a project grew naturally out of his years of free-lance technical translating, as well as out of his experience as an Agency linguist and a teacher and supervisor of linguists. The work as published is entirely unclassified, but do not for a moment think that it is not relevant to the work we do. The published version bears out my impression gained from a reading of the manuscript years ago that the Guide will come to have a place on every Russian translator's desk--whether that desk is here at work or in his den at home--and will be especially effective in helping those new to technical translation to avoid pitfalls and acquire competence far more rapidly.

It is the special virtue of the Guide that it will be read with interest and studied with profit by all Russian linguists; it is certainly not just a book for translators. It will be valuable to editors and others who must deal with the linguist's product, even if their knowledge of Russian is not great. Translators and linguists working in languages other than Russian will, I feel sure, find much that is pertinent and stimulating in the book.

That the Guide has a broader application and appeal than its title would suggest is due, it seems to me, to the felicitous match of form and content that the writer has achieved. No one who has read Art's recent article, "Prolegomena to a System of Sandwich Notation," will be surprised to find that the Guide is not an overly organized, structured work, and indeed, at first glance it appears to be simply a Russian-English glossary, and a rather skimpy one at that, with just 241 entries (headwords). However, the body of the Guide, 164 pages long, is followed by 24 pages of index from which it is immediately apparent that the work actually contains about ten times as many Russian terms as it does entries.

From the very first page it is also clear that the 241 entries differ widely in content.

Some (13: АРМАТУРА, 204: СЛЕСАРЬ), are more or less straightforward lexical entries, but more fully elaborated than in the typical Russian-English dictionary, elucidating meanings and suggesting appropriate translations and treatments. Old-timers will find themselves nodding vigorously as frequently abused and mishandled terms are given corrective treatment. (One of my own favorites is 15: БАЛЛ, the correct treatment of which hardly ever finds its way into our linguists' work without considerable prompting.)

Other entries (127: НАНИЗЫВАНИЕ ПАДЕЖЕЙ (Stringing Together of Cases), 169: ПОРЯДОК СЛОВ В ПЕРЕВОДЕ) (Word Order in Translation), deal with syntactical and structural equivalence and conversions. Such entries are in effect concise essays in contrastive grammar, presenting general principles and concepts that the reader will find especially helpful in handling many recurring situations in technical translation. These principles will, of course, very often apply to other types of translation as well.

A third type of entry offers advice and guidance on style. Some of these are simply straightforward, nuts-and-bolts stuff, for example, entry 178: ПРОПИСНЫЕ БУКВЫ, which reminds the translator of the difference between capitalization in Russian and English, or entry 17: БИБЛИОГРАФИЯ, which deals with the preferred treatment of bibliographies and footnote entries in translation. Entry 207: СОКРАЩЕНИЯ gives sound guidance on the treatment of abbreviations. Entries such as 74: ИМЕТЬ and 75: ИМЕТЬ МЕСТО are pure style-manual material and are a boon to the translator who is trying to write plain English instead of "translationese." Entry 189: РЕДАКЦИОННАЯ РАБОТА В ПЕРЕВОДЕ is quintessential Salemme, presenting the author's approach--the result of his many years of translating--to what is certainly one of the trickiest problems the translator must face: "How much should a translator edit as he translates?"

There is scarcely an entry that does not bear the Salemme stamp--witty, humorous asides, which though they are asides are nevertheless to the point; intriguing word play; lengthy parentheses poking good-natured fun at translators' faux pas (including the author's own), and more. Throughout, his treatment of every question is practical, down-to-earth, and

DOCID: 4009717

leavened with wit and gentle, never malicious, irony. Like Fowler's The King's English, it can be picked up in an odd moment, opened at random and read for any length of time with profit and amusement. These qualities should make the guide accessible and acceptable to the greatest number of our working linguists.

To illustrate a few of these qualities I reporoduce here three of the Guide's briefer entries in toto:

19. БЛАГОДАРЯ - Russian purists dwell in great detail on the difference between the gerund благодаря) (as in Благодаря его, . . . "Thanking him, . . .") and the preposition благодаря (as in Благодаря отцу я и сестры знаем французский, немецкий и английский языки, "Thanks to my father, my sisters and I know French, German, and English"). They condemn the frequent occurrence of the genitive case after the preposition благодаря just as they condemn the occurrence of the genitive case after согласно ("according to"). But they particularly condemn the use of благодаря in such "illogical" constructions as "Thanks to the ice, I slipped and fractured my leg." People don't give thanks for getting legs broken, say the purists. When such "illogical" constructions do occur in Russian text, it is often best to translate благодаря as "as a result of," so as to avoid an argument with English purists. If, on the other hand, one wants an argument with English purists, he can always translate благодаря in such sentences as "due to."

139. ОДНАКО - Just as the music lover, lulled by the opening strains of the second movement of Haydn's Surprise Symphony, pleasurably anticipates the chord that is supposed to shock him out of that lulled state, the translator of Russian criticism soon acquires a fond affection for the однако. Lulled by the leitmotifs of положительные черты and полезные данные, he knows that sooner or later a paragraph will begin with the complacency-shattering однако, to be followed by the contrapuntal interweavings of the недостатки and the несмотря на тq's.

Much as he admires the classic form, however, he should remember that English has its own forms. According to one of them, the "howevers," "moreovers," "nevertheless," and the like should not start the sentence like cymbal clashes, but should be reduced to the value of grace notes and incorporated into the main melody of the sentence. (Much, perhaps, as was done with the "however" that could easily have begun this paragraph.)

168. ПОРЯДОК - Russian stylists object to the excessive use of порядка ("of the order of"), a valid mathematical term, in contexts where приблизительно ("approximately") or some similar word would do just as well.

English stylists do not usually object to constructions such as "a speed of the order of 200 miles an hour." What they do object to is changing "of the order of" to "on the order of." They say that "on the order of" should be reserved for such constructions as "May I have some gravy on the order of mashed potatoes?" (To complicate the matter still more, there is a completely different type of expert who says that gravy should never be put on anything but meat, but let's not go into that.)

The Guide contains a number of reference features that would in themselves be sufficient reason to keep a copy on one's desk. First, there is the table of "false friends" in which the Russian word (false friend) and its correct translation are paired with the word's deceptive cognate and the cognate's proper Russian equivalent. Then there are transliteration tables, including tables for converting Chinese and Japanese proper names encountered in Russian texts into the acceptable transcriptions in English. Extensive tables summarize many of the correspondences in technical terminology between Russian, English non-technical, and English technical (derived from Greek and Latin) numerical prefixes. The different systems of enumeration of large numbers (a million and up) are contrasted in another table accompanied by a discussion of the problems faced by the translator.

In the face of the tremendous effort put forth by the author and his efficient varityp-
ist, [redacted] it may seem like petty carping P.L. 86-36
on my part to wonder what happened to the punch line of the joke in the second paragraph of entry 184: PA3. Perhaps this is the author's way of finding out who's really reading his work!

In his introduction the author solicits "comments and suggestions from the reader which could be taken into consideration in the event of an expanded re-edition of this work." I have already begun my list of items, and I hope that others will also take him at his word.

While it is true that the Agency does not "do" technical translation in the sense that Joint Publications Research Service (for instance) does, essentially similar technical linguistic work goes on here all the time; and while it is also true that the author of the Guide has done a great deal of free-lance, contract technical translating, the fact remains that he has spent his entire professional life at the Agency. Now, by judicious writing and by (I'm sure) some painful editing, the author has been able to purge his book of anything classified and thus make it available to the greatest number of readers. As applicable as the Guide is (and it is almost totally so), our work does present unique features and problems not treated in this edition. As ungracious as it may seem to ask more of one who has already given so much of his experience, I would still appeal to Arthur Salemme to relent and start work on a classified version or supplement.

Come on, now, Art. Shu-ucks, you'd enjoy it!

(UNCLASSIFIED)

THE FAITHFUL ECHO [redacted]

THE ROLE OF THE STATE DEPARTMENT INTERPRETER

P.L. 86-36

Below is the text (transcribed and condensed by [redacted] of a speech presented before CLA on 12 March 1974 by Sophia Porson of the State Department. Although "live" interpretation is seldom required of NSA employees, there is still much of interest here for Agency readers.

I can't tell you how much of a privilege it is for me, as an interpreter who has had to interpret I-don't-know-how-many speeches in my career, to finally get up and deliver one of my very own.

When I sat down to draw up a few notes for this talk, the first thing that came to my mind was that I would not tell a joke to start with. This is something that every interpreter dreads, and it is particularly characteristic of American speakers. I think we must all learn it in public speaking class: the first thing you have to do is get up and tell a joke. Whether it has any bearing on what follows is immaterial; the idea is that you have to have a "grabber," as they call it, to get everybody's attention and get everybody in a good mood. But, as you must appreciate, humor does not translate well. And particularly when it's in a very serious, say, a diplomatic conference, and the American speaker gets up and tells a joke, this often falls just dead! And of course the American immediately turns to where the interpreter is, in the glass booth at the back, and gives him a filthy look... (Laughter) So I said to myself, "No jokes."

I thought I'd tell you a bit about the type of interpreting we do. I'm sure you've all seen simultaneous interpreting on television, particularly some of the more important debates at the United Nations, so that you have an appreciation of what's involved there: we speak at the same time that someone else is talking and we convey that person's thoughts in another language concurrently. We lag a few words behind but we have to stay fairly close, which means quite a bit of mental gymnastics, as you can imagine, to get the syntax sorted out so that it comes out sounding right in the foreign language. This method of interpretation is the one that we use in large conferences, where speed is of the essence to get a lot of business transacted quickly, and where the absolute precise meaning of the word is not the key thing that it would be, for instance, in very delicate negotiations.

The other form of interpretation is the consecutive form, which actually, to my mind, is more challenging. The speaker makes a presentation of anywhere from one sentence to 45 minutes or more, and the interpreter stands by, takes notes, and, once the person has completed his presentation, then stands up and says the whole thing over again in the foreign language. If you've followed the debates at the U.N. you've often heard them say at the end: "I waive consecutive interpretation." They have interpreters who sit in a sort of ring in the middle at the Security Council and who take notes and are prepared to do just that when a person finishes making a presentation. However, over the years this has become a sort of vestigial thing. They don't use it too much any more. (Though every once in a while somebody forgets at the end of his presentation to say "I waive consecutive interpretation," and all of a sudden the interpreter gets up and starts interpreting madly and everybody wonders what happened!)

Well, the State Department has never waived consecutive interpretation. We use it an enormous amount in diplomatic negotiations, for the simple reason that, because it follows the presentation in English or the presentation in the foreign language, it enables the other side to check on what you're doing, it enables your side to check on what you're doing, and it gives everybody time to think. When you're in a negotiating situation you want to gain as much time as possible. You don't want to rush into anything. And all the time the interpreting is going on the speaker is able to think what he is going to say next. So this type of interpretation is the one that we use very commonly in diplomatic negotiations.

The major requirement here is memory. We do use notes, but not shorthand. We use a very schematic form of notes--a form of speedwriting, you might call it--a lot of abbreviations, and some ideographs that we make up ourselves (two flags juxtaposed, for example, to mean "peace," and flags crossed to mean "war"--that type of thing). The key to our notes is placement on the page. The "something" up here will be the introduction, the thing in the middle will be the body of the thought, and then the things down here may be the subsidiary ideas. Our work basically involves analysis of what the person is saying; you quickly digest what he said and jot down two or three words or pictures or whatever and go on to the next thought. But these notes serve only as a crutch; we rely essentially on our memories.

DOCID: 4009717

The interpreter that you know about primarily is the person who works at the U.N., but actually there are three different types of interpreters, as we define them.

We have the escort interpreter, who travels with foreign visitors who are here in the United States as guests of the State Department or AID. These interpreters travel extensively around the U.S. with the foreign visitor, looking at everything from hog-breeding to newspaper production. I have a diploma on the wall in my office at the State Department, and when people come in to see me the first time they think, How pretentious can she be? But when they look at it up close they see that it's a diploma in swine-breeding. I spent a month at the University of North Carolina with a group of Brazilian meatpackers and hogbreeders going through a training program, and at the end of it all, when they got their diplomas, they decided that I had worked harder than anybody, so they gave me my very own diploma. So the escort interpreter gets into all kinds of interesting fields very much off the beaten path.

Then we have the conference interpreter, who works primarily in simultaneous interpretation--not only at the UN or at State Department conferences, etc., but also at private conferences. As the world is getting smaller we have an enormous proliferation of international conferences. People meet to discuss everything under the sun, from cancer to computer language. And these meetings go on everywhere, all the time, all over the world, and most of them are international, so they do require interpretation; and the conferenae interpreters fly from one to the other.

The interpreters are not necessarily experts in cancer, computer language, or whatever, but they work terribly hard at studying up and keeping abreast of a variety of fields. Before you go into one of these conferences you generally spend at least a couple of days reading all the papers that are going to be delivered at the conference and learning at least the terminology. You can do, believe it or not, a fairly decent job of interpreting at a subject you haven't really studied extensively, provided you have had an opportunity to really steep yourself in the subject for a couple of days. You learn enough vocabulary and at least you learn the basic principles of what's involved to the extent that you can make a cogent job of interpreting. Then you forget it immediately and go on to something else. It all gets buried back here someplace and then maybe two years later you might have another conference on hydrology, or whatever and all that vocabulary that you learned once will come back to you. But we do have to be versatile, we have to be able to go from one subject to another very readily.

Now, as far as the type of interpreter that I am, I'm called a diplomatic interpreter. That doesn't imply that I'm necessarily tactful or anything like that--just that I work primarily in the diplomatic field. And it means that I have to have some of the skills of the escort interpreter (I have to be willing and able to travel with people, with large delegations) and some of those of the conference interpreter (the ability to go from one subject to another very readily), and I have to be able to do the two methods of interpretation that I described--the consecutive and the simultaneous.

Now, what does our work entail? Well, obviously it means that we are often the only person present during negotiations between, say, our president and a head of state of a foreign country. It means, obviously, that we have to be extremely fluent not only in our mother tongue but in at least one other language. And I might add that the State Department, as in the case of so many agencies, worries about funds and, as a result, the more languages you have the better off you are--the better they like it. But, basically most of us work in two foreign languages. We have a couple of -- I consider real phenomena--who work in three or four. This is exceedingly unusual. I mean, anyone can read a number of languages; but to have the verbal skill required to work, say, in three or four Romance languages is really exceedingly unusual. We have some who do that or who have, for example, French and Spanish and Russian, or Russian and German, and bridge two language groups even. But this is rather rare. Most of us tend to specialize in one language group. In my case, as has been mentioned, it's the Romance languages. My primary business is with French, for the simple reason that there are so many French-speaking statesmen from Africa, in particular, who have come to the fore in the past few years, that we do an awful lot of business with them, as well as, of course, with France, Belgium, and so forth. There are other people in my office who do Spanish as a primary language, and they stay busy with that. Portuguese doesn't keep me too busy because the Brazilians tend to speak English exceedingly well, except at the very highest level--at, say, the level of the President of Brazil.

But you have to be bilingual or trilingual, and your vocabulary has to be of the widest possible range because, as I've indicated, you do get into a huge number of fields. Diplomacy is not confined, as I'm sure you know, to just negotiating a treaty on a very specific matter of consular relations. Diplomacy these days involves tomatoes...it involves brassieres manufactured in Nicaragua that are being exported to the U.S., strawberries coming in from Mexico, drugs... I've just come back from a two-week seminar in Brussels on drug enforcement techniques.... Our interpreters have to be very versatile as far as their vocabulary is concerned and their interest in what's going on in the world.

We also have to be objective. This is a lot easier said than done, because generally, when somebody says something, you react to it. But as an interpreter you have to learn to subdue your own personality and your own reactions; you have to become exceedingly objective, and if the speaker says something, you go right ahead and say it. You don't think, How do I feel about it? You don't make value judgments. This is hard to learn, particularly if you have a lively interest in politics and diplomacy and you know what American foreign policy towards the People's Republic of China (for instance) ought to be!

And you have to learn to listen. It's amazing how little people actually do concentrate, but once you learn to focus totally on what you have heard it becomes a lot easier to remember. Sometimes I meet people who have been in a room with me for days on end in a negotiating situation where I've been the interpreter and they have been a subsidiary person not really taking an active part, and a year later they'll come up to me and say, "Oh, I remember you!" And I have absolutely no idea who they are because I've been so busy concentrating on just the two principals that I was interpreting for that I've blanked out everything and everybody else in the room.

We also have to do the note-taking, besides the interpreting. We often are the only ones who do the written record of what's going on at the negotiations, particularly where there's just the president and another chief of state and we're the third person there. Our notes serve as the record of what has transpired at the meeting. This places an enormous burden on us, as I'm sure you can imagine. We are, in a sense, a Witness to History, as Charles Bohlen called his book, and it does present some hazards. One of them is, if there is ever a leak, immediately you think, "My God, they're going to say it was me." Well, I'm happy to report that never has an interpreter been found guilty of a leak. The principals are the ones who generally do the leaking in diplomacy, as I'm sure you know by now.

Now, we also serve to a certain extent as cultural advisors; since we do have to bridge two cultures, we often help with things like selecting the proper poet to quote, for example, from a country's literature, or a statesman to refer to, or something like that. Also, in the course of our interpreting we try to avoid any cross-cultural misunderstanding based on a linguistic problem. For example, let's say that the American speaker refers, in talking to a Frenchman, to our "Department of the Interior." Well, that has absolutely no similarity to the "Ministry of the Interior" in France. They are just two totally different organizations. So what we would say is, "le Département de l'Intérieur," then we would add a little definition saying, "which takes care of national parks, waters and forests." Or let's say that a Frenchman would say something about the "Cour des Comptes" in France. We would render it in English as "Audit Office," but at the same time we would add, "This serves the function of the General Accounting Office in the Unites States." So we do interpolate to a certain extent this cross-cultural information. This is a rather important function, as you can imagine, because often people get side-tracked if they don't know precisely what the cultural frame of reference is.

Now what's the status of the diplomatic interpreter? It varies. A lot of countries don't even have diplomatic interpreters. Great Britain, for example, uses foreign service officers, members of the Foreign Office. I think this is all very much in keeping with the British tradition of the gifted amateur, or "Gentlemen vs. Players." Anyway, they don't have a cadre of interpreters on their staffs. The French have one interpreter who is on the staff of the Quai d'Orsay; the rest of their people are contractors. It would be very amusing to you if you knew to what extent other governments just don't care about security the way we do. Obviously these people are "vetted" and they have passed some kind of security clearance, but the government's attitude is just not the same, and they are perfectly willing to have a contractor, as in the case of the French, interpret between the President of France and the President of the United States, and then go on their way afterwards to work for another client, or other governments even.

West Germany has a very professional attitude towards the interpreting business. They have a large number of highly qualified people who work in the German Foreign Ministry and the various other departments of government. Their Defense Department, etc., all have skilled interpreters, and they have very high ranks. The senior ones at the German Foreign Ministry have the rank of Counsellor of Embassy, which, of course, all of us envy terribly. It's not so much because of the money, because we're pretty much paid about the same. But because they have a rank--a protocol rank--they cannot be required to sit behind their principals at dinner parties, which we have to do. And this is something that gripes all of us terribly. We're always sitting on tiny little chairs while everybody else is at the table, plowing their way through a ten-course meal to the Strolling Strings of the Air Force, or whatever, and there we are, plunked down on these tiny little chairs. And the waiters hate us because they can't get in to serve!

As I am sure you can imagine, the Eastern Europeans, the Chinese and the Russians have mobs of interpreters. We've been told, though I can't vouch for it since I don't know anything about Slavic languages, that the Russian interpreters are very good at the top level and then there is a lot of mediocrity at the base. But I'm sure you've heard of all these stars. Troyanovsky was a star interpreter of the fifties who later became the Soviet Ambassador to Japan. Viktor Sukhodrev, who travels with Brezhnev and who was

here recently, holds the rank of U.K. desk officer in the Foreign Ministry. This, I think, may give them a slightly different approach to their interpreting.

As I've already indicated, in the West we take the "faithful echo" approach to interpreting. We have no authority to change what people say, to embroider it, improve on it, or edit in any way. Our instructions are, "If he said it, he meant it. Just go right ahead, don't add or subtract." We do try, of course, to follow the emotion and the animation of the speaker (not to the extent that it looks like we're making fun of him, obviously), and we try to follow the same style. If his style is peasanty, we try to sound peasanty; if its highfalutin', we try to sound highfalutin'. So this again places strains on our vocabulary and our knowledge of the language. We don't correct anything except what is obviously a slip of the tongue.

You have to be very careful with your voice and your face because, as I've mentioned to you, we try to be objective, we try not to make value judgments about what somebody is saying. But you must realize that when you are working alone as an interpreter for two sides you're going to hear some pretty outrageous and even some idiotic things said which you have to convey. And it's hard for you to keep a straight face or not let your voice give away what you're thinking. (You know, "How could he say such a thing?" when you know it's a patent lie.) But this happens. And you have to be able to keep control of yourself throughout and never give away what you actually feel about what you're saying.

The other thing is, never, never to try to interpolate or give any clues to the people you are interpreting for. General Vernon Walters, the No. 2 man over at CIA, has worked as an interpreter off and on for many years. When he was a young aide to General Mark Clark (I guess he was just a second lieutenant or something), Mark Clark was trying to extract a concession from De Gaulle. Lt. Walters was trying to help Clark in this difficult task, so he kept saying, "Well, General de Gaulle says no, but I think he means maybe." Or, "He's just said he won't go along with you, but I think if you press on this issue, he'll change his mind." At the end, when de Gaulle came to leave, he turned to Lt. Walters and in very good English thanked him for his fine and fascinating interpreting. You can imagine how Walters must have felt. He told me that from that day forward he never, never, ever added or subtracted anything of that sort. You have to assume that people do know what you're saying, and that they understand, particularly English, and know pretty well what's going on.

The interpreters in the Communist countries, however, seem to have a lot more leeway in adding and subtracting for the basic purpose of making their people look good. Recently Brezhnev was here in the U.S. and one of the American interpreters told me what when Brezhnev addressed a private meeting of senators and members of the House he kept referring to "Senators": "It's a pleasure to meet with you, Senators," "I know you Senators are very important," etc. And Sukhodrev, who was interpreting, was very careful to keep working in the Representatives at the same time, because he knew that they would be heartily offended if they thought that Brezhnev was just addressing himself to the senators. This is a very mild case. Actually, they have been known to tone down some horrible threats, etc. Khrushchev, particularly, used to get carried away, as you know. And they would tone him down a lot. There have been a number of instances of this, so obviously they have authority to make their principals look better, and make sure they don't tread on too many toes.

One of my favorite experiences was when I worked at the Paris Peace Talks with the Viet Cong and the North Vietnamese for a while (the ones with the table, you remember the table!). The Viet Cong had an interpreter--a woman. (I might add, interpolating here, that women are very good in this business. I say this in total immodesty. Women are very active in this business, both in the Communist countries and in the United States and in Western Europe. I can't give you a percentage but I know that at least half of the interpreters are women, and maybe more.) Anyway, the Viet Cong's interpreter was a very strident type, very vocal and really gung-ho. In fact, I called her "La Pasionaria." I never knew her name. We weren't allowed to meet, even in the ladies' room. If we did meet we turned our backs to each other at the sink. "La Pasionaria" was ideologically very sound. She and her principal had a litany where they had to say certain things about the Saigon regime: that it was bloodthirsty, corrupt, lackeys of the West, etc. They had this whole long string of things that they had to say every time that they referred to the Saigon regime. Sometimes her principal would forget some of those adjectives, and inevitably she would put them all in, regardless. Because she was ideologically sound! So, they do have more leeway in this way than we do.

The Chinese--you've had Charles Freeman here and maybe he got into this--but he tells me that the Chinese are very literal. Of course they have linguistic problems, too, but they are free to convert at least factual errors that their principals make.

We in the West are generally nonpolitical. We're career civil servants, which means that we survive changes of regime fairly well. I've been through three presidents. We don't always, by the way, work alone. Often the foreign government will assign an interpreter to come with their principal. This is particularly true of the French, the Germans, the Russians, and the Chinese. A lot of the African countries don't and a lot of the Latin American countries don't; they just use us as the interpreter. But coun-

tries with whom we have really serious negotiations and who feel very strongly about languages and cross-cultural communications do assign their own interpreter. In which case what I do is interpret what my president says into the foreign language and they interpret what their president says into English, so that neither of us is working into our mother tongues. But it works out very well because we monitor each other, and we help each other. I remember when I was in Iceland with President Nixon and President Pompidou, and somehow they got on to the subject of the Queen of Sheba--I don't know why--and the French interpreter had one of these terrible blanks where he couldn't remember how to say "Queen of Sheba" in English. So I whispered it to him. And he in turn bailed me out a couple of times.

What are the requirements for being an interpreter? Obviously, you need the language. You'd be interested to know that most of us haven't been to interpreting school; I'm one of the few that have. About 15 or 16 of us at the State Department do the kind of work I do, but only three of us actually went to interpreting school. Most of us either come from foreign-language backgrounds or have grown up overseas, as in my case. We work at the languages all the time. We study, we get magazines and newspapers from overseas. Our office pays for them so that we can keep up with the living language and with what's going on. We study the briefing papers and have access to them before the meeting actually takes place so that we can be prepared. (Sometimes we run into trouble. People don't trust linguists; people that speak foreign languages are suspect! There'll be a paper labelled "Eyes Only" for the Secretary of State, and I say I need to see that. They'll say, "Why? It's 'Eyes Only' for the Secretary." And I say, "What about the Secretary's mouth?" Sooner or later, I get it.)

Then there's another attitude, toward women interpreters, that I ought to mention. I think these are people who read a lot of spy novels--they think we really do more than just interpret. I vividly remember being somewhere in the Middle West with a group of Frenchmen. There was a cocktail party reception for us. This American came up to me, took me aside and said, "Girlie," (I love that) "I just want you to know that there are not many women who would do what you're doing for your country."

We do have to be able to adjust ourselves to the idiosyncracies of our customers. President Kennedy, as you'll recall, was a demon for speed. He was clocked at 200 words a minute. (A court reporter is required, at best, to do 180 words a minute. You can see that standard note-taking just doesn't work in this kind of situation. That's why we need this schematic thing and rely on our memory.) When President Johnson came to office the first thing we did was to rush to the Bible to find out how to say, "Come, let us reason together." It turned out, as is so often true of Bible translations, that what it was in French had absolutely no bearing on the English, and the same for Spanish and so forth. We also had to learn how to say things like "varmint" and "bluebells" and "God-willin'-an'-the-crick-don't-rise." Interpreting for Johnson was literally a bruising experience. He was the kind of person who has to have physical contact with the people he was talking to. Since he was talking through the interpreter he'd hold on to the interpreter. In my case, he would grab me always by the upper arm, and I'd come home with these big bruises.

President Nixon has a marvellous gift, which is fine for us, of using these pointers--"Let me say this about that," and "Let me make this perfectly clear." He really does say that, and it gives us a clue that he's building up to an important line.

We worked with Secretary Rusk for 8 years. He liked to work into any conversation "There's more than one way to skin a cat." Then he'd sit back with that Buddha smile and see how we got it across in the foreign language. We tried something different every time, and it never worked. Our present Secretary of State /Kissinger/ understands French exceedingly well, and we don't interpret French for him. He also understands German, of course. The only problem with interpreting for people who know the language, so that you are just there as an aide--to hop in when the going gets tough--is that when the going gets tough, that's generally when it's something that you don't know either. They'll suddenly turn to you and ask, "How do you say 'moose'?" And of course, you just have this total blackout. I would much rather interpret for two people who don't know the language any day than find myself in a situation where I'm bridging a gap between two people who halfway know each other's languages.

* * * * * *

I've tried to give you a very brief aperçu of what it's like to be an interpreter. As Dr. Johnson said, "Words are but signs of ideas," and basically we're communicators of ideas. We try to do it as honestly and as perceptively as we can. Of course, our interpretation is only as good as the foreign policy we're helping to advance; the finest interpretation in the world doesn't do much good if there's no will to cooperate. But where the will to cooperate and to understand does exist, then effective interpretation can contribute very much to international understanding. And this makes my work exceedingly gratifying.

(UNCLASSIFIED)

P.L. 86-36

DEPARTMENT OF GOLDEN OLDIES

ESTABLISHMENT OF MOLECULE SUPERSERIES

EPSILON CONTROLLED ITEM
AMERICAN SECURITY AUTHORITY
Fort George G. Snead, Massachusetts

TECHOUTS NO. 54-40 (or fight)

1. Establishment of Superseries. The EPSILON superseries, MOLECULE, is hereby established to protest a most useful product which is based on the exploitation of an obvious source, the New York Times. Reports made up of reprints of articles on government leaders indicating liberalism, untruthfulness, or Sabbath-breaking will bear the caveat NEGATIVE MOLECULE.

2. Authority to Publish MOLECULE Superseries. The Chief of Z Group is authorized to publish all products in the MOLECULE superseries except NEGATIVE MOLECULE (BUCKLEY), MASORETIC MOLECULE (HEBREW), MASOTTI FIELD MOLECULE (R&D), MOFFETT FIELD MOLECULE (AEROSPACE), and MICHIGAN FIELD HOUSE MOLECULE (ATHLETIC).

3. Serialization. The product will be serialized by the date, section, page; and noted as to whether it is morning, afternoon, or Sunday edition.

4. Classification of Superseries Designator. The designator MOLECULE when used out of context is an ordinary word. Sly inferences to the contrary are to be avoided.

5. Recommended Hazardous Activities Group. The recommended HAG for MOLECULE is P to -M in inverse order of sensitive knowledge, with a double inverse calculation of HAG for those also holding NEGATIVE MOLECULE clearances. The NEGATIVE HAG resulting from MOLECULE access requires that when a person resigns or is transferred he must leave the United States for the period of the HAG. This is to insure his safety from interrogation by the Black Panthers, the John Birch Society and Senator Fullbright. Travel expenses will be paid by the U.S. Treasury from foreign counterpart funds providing the relocation is to a country which by reason of climate or lack of night clubs is not visited by junketing Congressmen. The country of resettlement must also be one which has never been visited by Stokeley Carmichael, Richard O. Douglas, William O. Douglas, Douglas O. Haliburton, Richard Haliburton, or a Greek yacht. The nation may not be one in which the reigning queen or princess is a former American citizen or from which a king has at some time abdicated in order to marry an American citizen. Also excluded are nations ruled by juntas, oligarchies, royalists, despots, fascists, communists, centrists (right or left), and intransigent nationalists. This leaves Rwanda.

Can you make out the name?

A real-life puzzle
submitted by [redacted] P16

~~(TOP SECRET UMBRA)~~

EO 1.4.(c)
P.L. 86-36

DOCID: 4009717

Letters to the Editor

To the Editor, CRYPTOLOG:

The item in the December CRYPTOLOG entitled "Citizens of the World" recalled to me how amused my classmates and I were at the Navy language school when our German-born instructor informed us that Germany's most famous railroad trains (pre-WWII) were the "Flying Hamburger" and the "Flying Frankfurter." This news reduced the class to laughter, but our instructor was not at all amused.

Incidentally, if you happen to be in Tangier and would like a tangerine (the orange), you would do well to ask for a "mandarin." On the other hand, if you should ask for a mandarin in China (in the old days), you might possibly get a Pekingese.

[redacted] (an Alexandrine)

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

To the Editor, CRYPTOLOG:

It is a reasonably safe bet that your four-part series on the intern program will win few friends in the Career Development establishment. There will be valid objections to some of the specifics in this series, but no one person or group of people can be expected to have a total command of the facts in question. It would be a mistake, therefore, to dismiss everything "Anne Exinterne" (henceforth "AE") says for this reason. Her perception of the overall problem is quite good.

The following comments on the series are made from an admittedly narrow point of view--my personal experiences and observations in the Language Career Panel office from 1967 to 1972. They represent my own opinions and the policies which were in force during that period, not necessarily the views of the present Panel.

In discussing the philosophy of the intern program AE notes that many of her friends had the idea that they were FSGs (future supergrades). I haven't the faintest clue how they ever got that into their heads. The only thing we ever told them was that we would do our best to see that they could meet the criteria for certification in Language at the end of three years (providing they were not starting from scratch in a new language). I used to stress diversity in work assignments as the key element in their internship (within the limitations of their "major" language), but I have no recollection of including anything other than technical objectives in their programs.

[redacted]

at grade-point averages (3 or above, on a scale of 4), CQB scores, ALAT (language aptitude) scores (at least STATEN 6), and proficiency test scores in a foreign language. On the few occasions when we departed from these criteria, we almost always lived to rue the day. We did not have any criterion for judging someone's staying power, however; that is, the degree to which a person was committed to a career in this business. In the course of a 35- or 40-minute interview, everybody looked dedicated. Another point about selectivity: you can select only from the output of the recruitment and screening processes. In some instances I think we are recruiting the wrong kinds of people for the language field, but more about that later.

It is hardly a managerial triumph to graduate interns into surplus career fields, and AE is quite right in taking us to task on this issue. My only rejoinder here is that she may have identified the wrong set of villains in the melodrama. Neither the panel offices nor line operational elements have any real control over sudden shifts in targeting, organizational structure or billet distribution. Intern programs were begun in good faith, but the rules were changed in the middle of the seventh inning. To this day we continue to encounter problems in (1) accounting for the skills we have, and (2) projecting the skills we're going to need. Nowhere is this more true than in the language field, where the "labor units" are not interchangeable. If you decide to stop reporting Zendian internal communications, you can't simply transfer the Zendian linguists to the Basque navy problem, even though the job descriptions sound remarkably alike. I've always assumed everybody knew this, but lately I'm not so sure.

In her discussion of recruitment, AE comes close to a favorite theme of mine. I don't think that an AB right out of school (typically female) with a degree in language and literature (typically French) is necessarily the best choice to send off to learn a language like Amharic, [redacted] My example is hypothetical, but it is a good profile of the kind of intern program most likely to fail expensively.

I don't agree with AE's suggestion that we take on high school graduates to train against some of our jobs, at least in the language field. On the contrary, for some of our jobs we ought to be going after graduate-level specialists in fields like Uralic and Altaic studies, untenured college teachers, and ex-SCA personnel who have continued their studies in languages and linguistics.

There are several reasons for this. On most language problems the language analyst has to know far more than irregular verb forms and odd usages of the subjunctive. Culture, history, politics, economics, personalities, international relations, technology--all of these factors and many more play a role in producing a transcript, a translation, a report. All human knowledge is not derived from SIGINT, but much of it can be applied to the SIGINT process. Why do we have to start with a *tabula rasa*?

We also need people who have already had some of life's experiences. Our analysts should have heard of such things as letters of credit, visas, four-barrel carburetors, rectifiers, compound interest, the Diet, etc. Many brand-new college graduates have never before been responsible for (1) supporting themselves, (2) renting an apartment, (3) putting a car on the road, (4) obtaining a loan, etc. Hiring 18-year-olds can hardly alleviate this situation. I have to go along with George Allen on the wisdom of putting rookies on the starting team.

But most of all we need people who are ready to make some reasonable sort of commitment to our kind of work, people for whom the grass will not necessarily seem greener elsewhere. Granted, we have to look out for the job-hoppers and the unemployed academics who are waiting for the foundation money to start flowing again, but these risks seem to me far easier to support than the odds we face in trying to "assimilate" liberal arts AB's into the work force, particularly where training (often in the form of self-instruction) in rare languages is involved.

One of the advantages of recruiting the kinds of people described above (graduate-level specialists, untenured college teachers, ex-SCA personnel) is the fact that they have already gone part of the distance toward the goals we have in mind when we think of the NSA/CSS professional linguist. This kind of recruiting makes more demands on us, but if we exploit all the contacts we now have in departments of languages and linguistics (and perhaps anthropology) we should be able to come up with a few good prospects who will eventually have a greater impact on our mission than fifty of the typical college hires we get now.

The graduate student in Uralic and Altaic studies may be somewhat harder to clear than the new graduates of a small liberal arts school, and this touches on something else that AE said in one of her articles:

"I suspect that the testing battery and the other screening devices used by M may be producing a population that is too homogeneous."

Many of us who have worked on the problem of recruiting and processing would-be linguists for the Language Career Panel or for A Group have remarked on the apparent inverse relationship between language proficiency scores and the score on some mysterious M7 personality profile. It was kind of a running joke that if a recruit got STATEN 9 on the Russian test, we would never see him again. Maybe there's nothing to it, but I for one would feel a lot better if someone could convince me that it isn't so. Any takers?

In her treatment of selection and orientation, AE makes one point that I would like to support with few if any reservations. I too think that new hires should serve in some general capacity (SIGINT technician) for some 12 to 18 months, use the skills which they bring to NSA/CSS, skills for which they were recruited to begin with, and only after this period be considered for an internship. Both the panels and the individual intern candidates could then make better choices in several important ways. Why not have a year or so of being "engaged" before taking the plunge? In this way a linguist could work in a language he knows while he's learning the SIGINT business, which presumably he doesn't know. I would probably waive this requirement in the case of someone with both a working knowledge of one of our languages and previous SCA experience.

The 12--18 month "cooling-off" period has a number of intriguing consequences. It would address the problem AE raises of people coming here with urgently needed skills and then going off to an internship in a competing but unrelated field which offers the promise of more glamour, fame, success and love (none of which characterize the language field), at least for the first year and a half. The practice might even keep us from recruiting individuals who have no immediately usable skills.

In the section on motivation and morale, AE scores some palpable hits on a relatively inviting target, but her quarrel is not with the intern program, but rather with the larger problem of personnel management. If interns see no real relationship between the quality of their work and the rewards they receive, then neither do many non-interns. If interns have few incentives to aspire to professionalism (as opposed to professionalization) in a technical field, then what about everyone else? The fact remains, on this latter point, that for whatever reason, there is little professionalism in the language field. Most of our language analysts profess to have only a limited interest in the languages they use on the job (outside of the traffic that goes across their desks or through their earphones). Most of the people I counseled in the LCP office, particularly after an unsuccessful shot at the PQE, acknowledged that they did nothing or almost nothing to develop and maintain their skills. As one man put it: "Why should I mess around with that (expletive) at night? I see it all day on the job!"

Yet most of our senior linguists insist that outside contact and work with a foreign

language is about the only way to achieve and maintain any real competence, and just about all of them practice what they preach. A professional has a deep and abiding interest in what he is doing. It is never "just a job" for him. By this standard we have only a small number of professionals.

AE spends a lot of time in this section dealing with the issues of psychic income, feedback, incentives, morale, and the general atmosphere on the job. I agree with most of what she says, but find myself overwhelmed by the high level of generalization. Maybe the only solution is to abolish Original Sin. One small aside caught my eye: a colleague of hers was described as "spending a portion of his working day running down leads for new clients for his many enterprises, delivering orders and displaying wares." Such practices are unfortunately quite common, and if you add to them all the hobby, craft, and related activities that go on throughout the working day (and not only during the lunch hour), you are confronted with what must be an enormous amount of employee time devoted to non-work, or at least non-Agency work. Maybe the Small Business Administration could be persuaded to open a regional office within the building here.

Where do intern graduates go? AE talks about the fact that interns are loved and cared for until they are certified and then cast out into outer darkness, and this is true. It is no less true for anyone who has received his certification as a professional. His next logical career move is out of the field, in many instances. EO 1.4.(c)
P.L. 86-36

If AE's article were the whole case for the intern program, then the obvious conclusion would be to do away with it entirely. Two counter-arguments have to be made: (1) The problem is not the intern program per se, which cannot transcend the supervisory and managerial climate in which it exists at the present time. If we want to improve the intern program, we should begin by improving first-line supervision, and maybe the new performance appraisal system will be a step in this direction. (2) The intern program, at least the language part of it, has achieved some outstanding successes. If challenged, I can name them, the outstanding young men and women who came out of the program to achieve exactly what we had in mind for them to begin with. Maybe they would have gotten there anyway, but like a proud parent I can point to them and say, "These are my jewels." Any program that does this can't be all bad.

Emery W. Tetrault, P16

~~(CONFIDENTIAL/HVCCO)~~

P.L. 86-36
EO 1.4.(c)

CAMINO NEWS

CAMINO is a good idea that keeps getting better. Many linguists will remember the name CAMINO [redacted] in existence since the mid-60's, which could be queried [redacted]

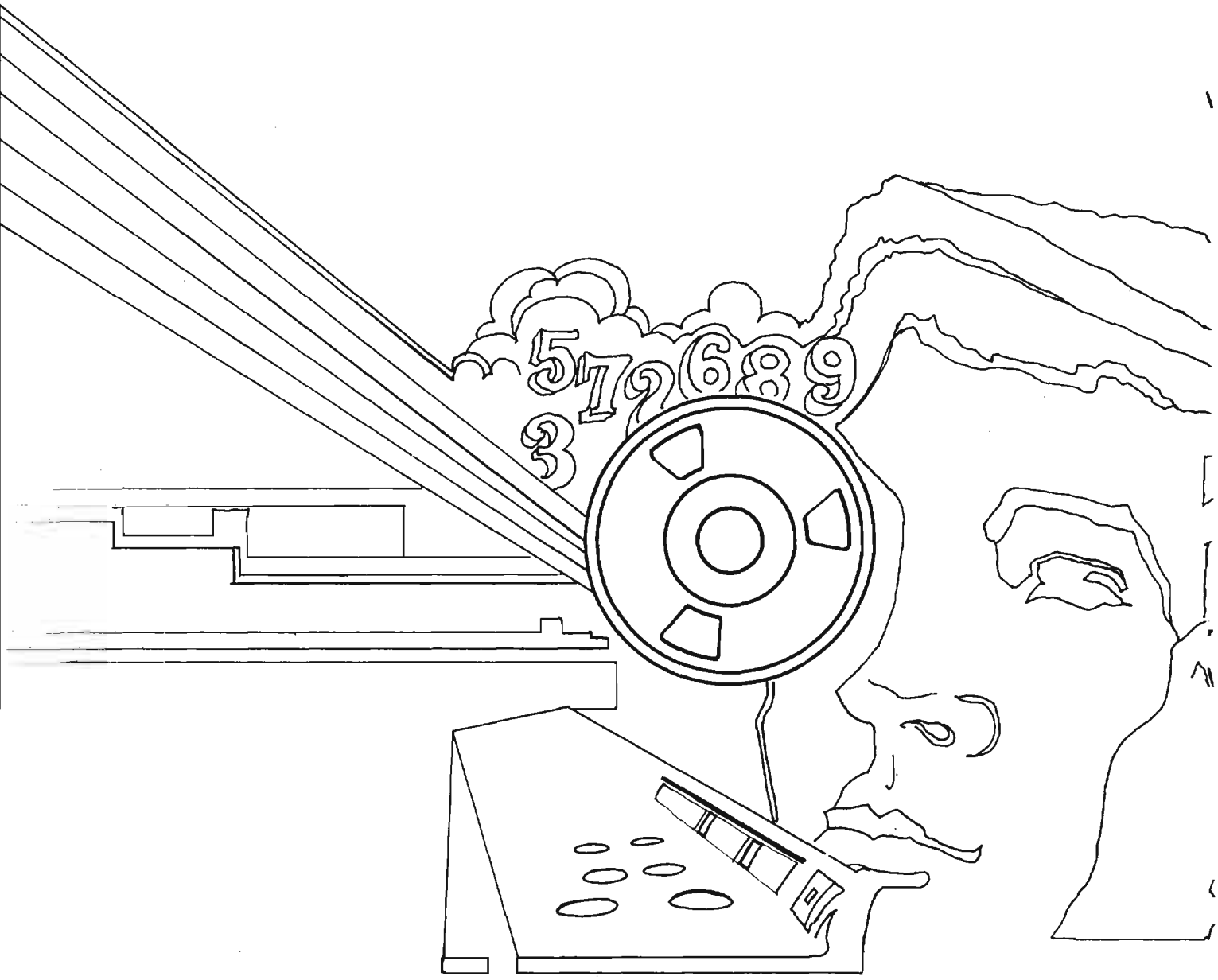
These first three files on the RYE system have proved of great value to linguists. In the last few years they have been joined by more and more new machine language files and abbreviation files. The newer files have made use of the IBM 370 system rather than RYE, for two main reasons: first, RYE will probably soon be superceded by newer machines, and second, RYE memory storage space has been getting harder and harder to come by. There are now nearly 20 machine language files of various sizes, all in the same format and processed by the same machine programs and procedures, and all forming one system which still bears the name CAMINO, in honor of the original good idea- [redacted]

Each file has an executive who is responsible for all linguistic and lexicographic aspects of it. In some cases he has others helping him. Machine processing standards, programs and procedures for all CAMINO files have been developed and are being maintained in P16. Below is a list of the files now forming the CAMINO system, with the names of their file executives or other contact points, and the sponsoring organizations:

[redacted]

For further information call [redacted] 3045s. P.L. 86-36

~~(CONFIDENTIAL/HVCCO)~~


5726893

DOCID: 4033678

P.L. 86-36

~~TOP SECRET~~

R23 [redacted]

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JANUARY 1975

EO 1.4.(c)

P.L. 86-36

UNNA, [redacted] ..... [redacted] 1
THE SIGINT USERS' HANDBOOK..... Donald B. Oliver..... 3
HOW CLEAN DOES A DATA BASE NEED TO BE?... [redacted] 5
THE YAWN OF THE COMPUTER AGE..... [redacted] 6
THE CASE FOR COMINT READERS..... [redacted] 7
CROSSED CODEWORDS..... [redacted] 9
CLA IS TEN YEARS OLD..... 10
OTHER NEWS FROM THE LEARNED ORGANIZATIONS..... 12
INDEX OF CONTRIBUTORS FOR 1974..... 13

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4033678

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. II NO. 1 JANUARY 1975

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief ..... Doris Miller (5642s)
Collection..... [redacted] (3571s)
Cryptanalysis..... [redacted] (8025s)
Language..... [redacted] (5236s)
Machine Support..... [redacted] (3321s)
Special Research..... Vera R. Filby (7119s)
Traffic Analysis..... William J. Jackson, Jr. (3369s)
Art Editor..... [redacted]

P.L. 86-36

* * * * *

Editor for December ..... [redacted]

~~TOP SECRET~~

EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~

UNNA

by

P.L. 86-36

In his article in the September '74 issue of CRYPTOLOG, Derek Craig succinctly stated a pressing problem.

According to the gloomy prognostications of certain writers, the British banking system is already balanced precariously on deposits of Arab wealth which can be redeemed at any moment. The daily newspapers report that Arab efforts to acquire Lockheed Aircraft Corporation have been forestalled. Rumors of an impending purchase of IBM by Arab interests are denied. Arab wealth has already begun to insinuate itself into the fabric of Western economies at some very sensitive spots.

The situation bears watching. The economies of Britain and the United States, foundering under the forces of shortages, recession, inflation, and domestic despair, are vulnerable to disruption, and the Arabs seem not averse to creating mischief.

"It is critical," says Mr. Craig, "for United States policy makers to know how

UNNA*

All the AP requires is a properly ordered directory.

In addition to the "search" function, the AP can, under computer control, do the following:

- Add an entry to core, in proper order;
- Delete an entry from core, and adjust remaining entries;
- Read an entry from a designated core address;
- Write a word into a designated core address;
- Clear core (put all 1's into all of core).

EO 1.4.(c)
P.L. 86-36

UNNA was designed and developed in R33, with C65 contributing to software development. The device underwent engineering tests

Ed. note: This is not an acronym, as you might suppose, but an R task covername. The pronunciation most often heard here is "Oona."

EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

DOCID: 4033678
P.L. 86-36
EO 1.4.(d)
EO 1.4.(c)
P.L. 86-36

UNNA, as now configured, collects data on magnetic tape.

The TAP inputs from the TCD 25 pairs of signal for each voice channel. One signal constitutes parts of 25 different data bit streams (the telegraphy channels) and the other consists of an "energy bit" per channel. Each bit of the

UNNA Functional Description

UNNA is divisible into four parts: Time Compression Demodulator, Associative Processor (already described), and Honeywell DDP-516 Computer with peripherals.

Time Compression Demodulator (TCD).

Computer (DDP-516). The computer used in the UNNA system is the Honeywell DDP-516, with 32K memory. In the "stand-alone" mode it has the following peripherals:

mag tap controller and two mag tape units, device speed: 36 ips, 556 or 800 bpi,

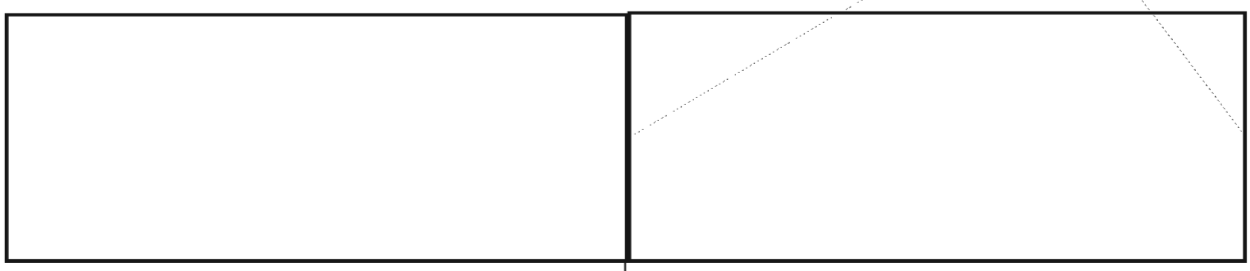
card reader and reader control unit, device speed: 200 cpm,

data terminal (typewriter), device speed: 10 cps, 75 characters per line.

DOCID: 4033678

EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~



~~(SECRET SPOKE)~~

the SIGINT USERS' HANDBOOK
or: what's an Ishtar?

donald b. oliver, v2

Few NSA employees are aware that since April 1974 a growing body of SIGINT-related information has been appearing under the title SIGINT Users' Handbook. Inasmuch as it is distributed narrowly in-house, even within the DDO organization, and is essentially "uncoordinated," few analysts know that it exists. This should not be surprising, however, as the Handbook's title advises that it is intended for the delectation of SIGINT *users* (also known as consumers or customers) rather than SIGINT producers.

There have been two relatively similar predecessors to the Handbook--a long-lived series titled the "INFOCON" (Information for Consumers) and another series called "Notice to Users" (the latter being an interim step between the INFOCON and the present Handbook). Like the MUSSO system and certain other current vehicles of NSA direction, the INFOCON program suffered from lack of staff attention, lack of interest on the part of NSA managers, and a degree of executive resistance to the whole idea. For whatever reasons, INFOCONs became tired, out-of-date, and of little value to those they were intended to serve. Only the users of SIGINT and those most intimately involved with them, NSA field elements, tried--unsuccessfully--to breathe life into the moribund body.

With the development of a system of United States Signals Intelligence Directives (USSID) which changed, and reflected changes in, the ways we supported the outside world, it was obvious to the SIGINT Directives element (now V13) that the INFOCONs should be reissued or wiped out.

A home for them was hard to find. The old P2 organization, which included a "customer relations" function, felt that P1 ought to do something. P1 allowed as how the effort was "educational," and the National Cryptologic School should pick it up. The School was unimpressed with that argument. P2 finally got the job, but couldn't come to grips with the major policy issue as to whether an entire package must be presented to the users or whether the job could be done piecemeal. Because of this, little was done.

To be fair, however (as I can be occasionally), there was some executive resistance to perpetuating a body of SIGINT information in a formal, structured sense for the education of readers of product or the beneficiaries of SIGINT support. This view was based on the entirely reasonable position that the more users knew of "SIGINT Production Information" (see USSID 300), the more likely they would be to act to take over the responsibility of DIRNSA to manage the SIGINT activities of the United States. It was the view of some executives that little information about SIGINT need be in the hands of the users, and that what was needed could be handled by ad hoc memoranda, letters, and messages.

As is normal, of course, and as soon as it was convenient and safe, this policy guidance was ignored, and the SIGINT Users' Handbook was developed by V2 (now V12).

To a large extent the rationale for the Handbook is the same as for Cryptologic Support Groups. Each has a task of "interpreting SIGINT," advising the user how and in what form product and other SIGINT support can be made available to him, and, in a generally nontechnical context, explaining to him the methodologies, procedures, conventions and systems by which SIGINT is produced and distributed. Particularly within the military community, it has long been true that intelligence assignments are short, and the opportunity and inclination to study and understand the arcane ways of the US SIGINT System are limited.

~~SECRET SPOKE~~

courageous and feisty since it competes (successfully) with DoD Manual 5200.17 (M2) and CIA's Communications Intelligence Security Regulation in this regard. [redacted] of V12, the Handbook scribe, is fearless and overcomes all obstacles.

The Handbook has become a "best seller" in the user community. DIA conducted a survey of DoD SIGINT users last summer and observed:

"The SIGINT Users' Handbook is a very valuable guide for all SIGINT users, particularly intelligence analytical personnel. Experienced analysts find the Handbook a very useful reference document; it is invaluable to the new or inexperienced analyst as an information guide and tool relevant to SIGINT operations. In this vein, it can be used for indoctrinating new personnel relative to the various SIGINT reporting vehicles, retrieval systems, general composition of SIGINT product and concepts of SIGINT support and operations. The Handbook can be viewed as the SIGINT 'primer,' and for the new or unindoctrinated, supplements knowledge of SIGINT acquired through the NSA orientation/ familiarization courses."

EO 1.4.(c)
P.L. 86-36

A word of caution. Although geared to the USSIDs, the Handbook is not a suitable replacement for those documents in respect to SIGINT *producers*. Nor should it be used as a reference work to pass tests.

If you would like to review the Handbook, or if you have subjects which you believe are candidates for inclusion therein, I suggest that you call or visit [redacted] (ext. 5283s).

P.L. 86-36 ~~(CONFIDENTIAL/HVCCO)~~

OPPORTUNITIES

PROGRAMMERS AND BOOKBREAKERS PLEASE NOTE: The "Checklist for Programmers of Machine Support Tools for Bookbreaking" by Katharine Swift and [redacted] (8 pages) is now available. Copies can be obtained from [redacted] P16, 3W070, ext. 3045s.

LEARNING CENTER OPEN IN NEW LOCATION. The Learning Center in OPS 1 has been relocated to Room 2W165 and its capacity more than doubled. Hours are 0700 to 2100, Monday through Friday. Self-paced courses are available in effective reading, writing, speaking and listening; basic [redacted] digital computer theory, electronic data processing, computer systems performance, slide rule operation; refresher courses in algebra and transistors; courses in English as a second language and women in management.

[redacted]

HELP WANTED. Among a number of things in which the National Security Agency is interested is ELINT. Yet CRYPTOLOG has never had a word about it, except perhaps in passing. I will accept part of the blame for that, as I just do not know enough about the subject. There is a vast number of people, however, even in CRYPTOLOG's readership, who do know enough about the subject to educate the rest of us. Please let me have something on this subject. Collection Editor.

~~(CONFIDENTIAL/HVCCO)~~

EO 1.4.(c)

P.L. 86-36

DOCID: 4033678

HOW CLEAN DOES A DATA BASE NEED TO BE ?

by [redacted] P.L. 86-36

One of the first things one learns about computers is that they require a much higher order of accuracy in the material they manipulate than do comparable "human" processes. One learns to pay an extra measure of tribute in the form of added proofreading or other forms of quality control, so that the input is "clean" enough for the computer to handle.

After a while, as the novelty wears off, it sometimes occurs to one that not all of the data needs to be so awfully clean. If we expect to sort or retrieve on a particular field or data element, then that field or data element should be clean and garble-free; but if a neighboring item is never (well--almost never) used as a control for sorting and retrieving, then it only needs to be as garble-free as people need. Quite clearly, if only half of your data elements really need quality control, then some of that manpower now spent scrubbing each little data element might be diverted to other tasks.

It is possible to imagine categorizing data elements as "first order" if they need to be "computer clean," and as "second order" if they only need to be "people clean."

In this day of great monolithic data bases, however, the use of varying quality levels can cause troubles, however laudable their manpower savings may be. A story "from life" will illustrate.

Some years ago, during the Vietnam War, we found ourselves receiving two streams of electrical material from the sites in the field, and both streams were used to feed computer processes

[redacted]

The second was a cryptanalytic stream. A

[redacted]

The specific details of these processes belong to another story (or series of stories). The point here is that there came a time when there was an operational need to identify which messages [redacted] It should have been easy. Neither system was new, and both had been working for quite a while with reasonable success. (Success is a relative term; there were always problems, sometimes earth-shaking problems, but by and large, the systems did work.)

[redacted]

It took a while to find out why, but after a time the answer became clear. Evidently the people at the sites, knowingly or unknowingly, practiced different levels of quality control on the various data elements.

[redacted]

All of which suggests several thoughts.

Garble rates can often be determined, at least approximately, by machine. Certainly differential garble rates can be (Field 1 has more or fewer garbles per thousand than Field 2). If data bases which now exist were measured to show which data elements were "cleanest" and which were "dirtiest" (perhaps arrayed in a sort of quality hierarchy), EO 1.4.(c) P.L. 86-36

- the unwary might be warned off using the data base for sorting or controlling on the wrong (dirtiest) data elements;
- hit thresholds might have to be lowered when dealing with "dirty" elements, even at the expense of wading through more "garbage" output;
- managers might better understand the manpower costs of various control strategies;

but also:

- we might decide that great monolithic data bases are not always the answer when one must work with a variety of data sources having widely different notions of which items are "important."

~~(CONFIDENTIAL/HVCCO)~~

DOCID: 4033678

THE YAWN OF THE COMPUTER AGE

OR When Your Terminal Is Terminal....

by [redacted] N22

P.L. 86-36

It's no secret that NSA has become almost totally dependent on computer systems to aid our analysts. The fact is, we have had to turn to these systems in order to handle the increasing volume of work, that grows more sophisticated while our peoplepower is shrinking. But this dependence on computer systems has not been without its drawbacks and frustrations. I'd like to call your attention to one of these.

It's bad enough that the (expletive deleted) computers are down several times a day, but that's something we have been conditioned to expect. The real crime being perpetrated on systems users in NSA is far more difficult to adapt to. It is the dreadful excuse given in accompaniment of each system failure or blowup.

"Power problem on the platform," some anonymous voice monotones to you over the phone. Or worse still, "Don't know. The --- Representative's looking at it now." I ask you, where's the satisfaction in explanations like these?! We users are looking for a salve, and instead we receive the same infuriating excuses time after time.

Well, I have a suggestion (worked out while awaiting the reactivation of a lifeless terminal). Let's have a contest. Users will send in their nominations for reasons to explain the systems failures. The best of these will be selected for play on taped telephone messages. Naturally these will have to be changed several times a day, coinciding with the actual systems failures. We could even institute a method whereby after the message ended the caller would have 20 seconds of the tape to vent his frustrations as a system user. This suggestion could pay for itself because NSA would then accumulate all these 20-second rages into 18½-minute segments and sell them to GSA, who would play them on tape decks hidden in statues, to keep pigeons at a respectful distance. Or better yet--what NSA walker hasn't wished for a way to prevent birds from "roosting" (you've got another name for it?) along the covered portions of our sidewalks? Cleaning bills alone could offset the expense of this suggested application.

Now, just to show you what I have in mind as the type of excuse that users are looking for, here are several examples:

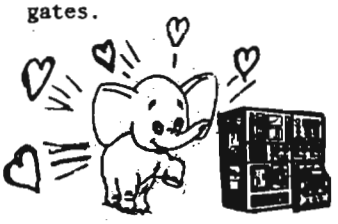
1. In accordance with provisions of the Fair Labor Standards, the computer is at lunch.

2. When we fed all NSA's Regs and Procedures into core, the computer blew up.

3. Unfortunately the GSA standby crew just stood by.

4. An enraged bull gored the CPU and all the electrons leaked out.

5. The main frame's been recalled by the manufacturer. There's some problem with the MAYBE gates.



6. An amorous elephant tried to mate with the CPU. We expect a doubling of processing capability in about two years.

7. The orthodontist is here now, trying to correct the computer's overbyte.

Sure, I realize that this suggestion isn't going to keep our systems up any more of the time than they are up now. But at least users can be provided with a slight diversion from this irksome and perplexing problem. Maybe, too, the competition to get an excuse accepted will increase systems utilization, reduce sick leave, and improve morale. (That last "e" was changed from "s" by the censor.) We would require hundreds of excuses per week, so conceivably everyone in the Agency could eventually win.

Anyway, what could it cost NSA to offer a token prize for an accepted excuse? I think our people would be satisfied with a hammer, a chisel, and a slab of rock. Then they could create their own data files.

DOCID: 4033678

THE CASE FOR COMINT READERS

by [redacted] P16

P.L. 86-36

The following article (with some footnotes which have been omitted here) originally appeared in QRL in May 1971. For other views on this subject see the June 1971 Keyword and the August 1971 QRL.

At the time of this writing, I have participated in the preparation and grading of four Spanish-language Professionalization Qualification Examinations and have seen more than half of the examinees flunk one or more parts. A few people have expressed the opinion that the high failure rate stems from the fact that the test was too hard. Depending on how you choose to define the expression "too hard," they may be right.

The committee charged with making the exam and grading it started from the assumption that being a qualified Spanish linguist at NSA is a hard job. A true "professional" should be able to handle any kind of Spanish material that comes at him--from any country, on any reasonable topic, [redacted] in good condition or corrupt, written or spoken, etc., etc. Perhaps any test that tried to prove a person's capabilities in all those respects might be called "too hard," but the ability to handle those topics and types of traffic differentiates an NSA linguist from other linguists.. and there are people who can deal with those various problems; this fact can be attested by the large number of people who have managed to pass the PQE despite its difficulty.

With Spanish, the problem is complicated by the number of countries using the language (most of which have some particularly irksome national usage--telegraphic abridgement, vocabulary, abbreviations, etc.).

[redacted]

[redacted]

As lovely as it sounds, it is totally impractical because it would actually slow down production while old-timers--assuming that they hadn't been transferred to another section to learn something else--took time from their work to explain things to the "new boy"; supervisors would be justifiably reluctant to transfer qualified linguists out to pick up new skills while getting a bunch of unskilled people to teach; even the linguists involved would object to spending time to learn something and just when they're gaining proficiency in it they'll have to leave it and go learn something else; in addition, the constant shifting and acquisition of new bosses might hinder their chances for promotion.

All of these disadvantages seem to outweigh the advantage of having a corps of well-versed linguists. I think it goes without saying that such a nucleus of all-around linguists is certainly a good thing to have, but it just isn't a good thing to go to all the trouble of getting one.

Another possible method of familiarizing linguists with all the sorts of problems they're likely to encounter in a given language is to have a division or group training office which prepares a broad course to teach the requisite subjects, using material from a number of sources, [redacted] Naturally, this material would be arranged in order of difficulty, starting out with easy and uncorrupt text and advancing into more telegraphic styles, first without and then with garbles.

EO 1.4.(c)
P.L. 86-36

Problems involved in having such a course include: whether or not it actually includes all the types of material required; whether the amount of time allotted to the various topics is adequate; whether all the people who should take it do so (or are allowed to by supervisors who hate to take people away from production, even for a course which might improve output); whether taking such a course should be a prerequisite for taking a PQE; whether the grading is too strict or too lenient; whether the course content is changed and updated from time to time; and the obvious question: How many people who take the course subsequently go on to pass all parts of a Professionalization Qualification Examination? (This may seem like an "obvious" question, but it's hardly a fair one, since that isn't really what such a course should be designed for; however, one might be tempted to consider the PQE as a way of verifying the effectiveness of the course).

Here a word of caution should be given. There ought to be a reminder of acceptable degarbling procedures, and garbled groups should be restricted to one wrong letter (or digit) or one pair of transposed characters per group. Obviously, the code groups must be shown to enable the user of the COMINT Reader to degarble mutilated groups. The groups that are garbled should, if possible, appear elsewhere in the text to help the degarbling process.

Perhaps a brief outline of what a COMINT Reader might include would be helpful. After introducing texts on a number of subjects, duly notated to show telegraphic usage

garbles can be introduced: wrong letters, missing letters, transposed letters. These mutations should be explained, preferably in a special "Answers" section, either at the back of the book or in a separate volume, and sample translations given. This latter feature would introduce the user to standard Agency preferences.

A variation of this practice might be introduced in the one-part code section where the message text obviously calls for a word with a given meaning and the alphabetical range of the code pins down which of several synonyms is appropriate.

was to help individuals pass PQE's (although I sincerely hope that no one feels that this is the only value of COMINT Readers), it should be remembered that such garbles have no place in professionalization exams.

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

DOCID: 4033678

The final printout [redacted] should be accompanied by a wealth of explanatory notes, as well as an acceptable translation. (Apropos of "an acceptable translation," it doesn't take long until it becomes "the acceptable translation" and perhaps there should be a few paragraphs explaining why certain choices are unacceptable; [redacted]

The COMINT Reader has one advantage over a regular course; namely, that the student can progress at his own rate of speed, rather than try to keep up with a class (which may mean going on to a new topic before he really understands the old one). In addition, the user can keep the book in his desk, studying it only when his workload permits (although if supervisors will let their people spend one or two hours per day working with the COMINT Reader, that would be commendable).

The availability of a COMINT Reader does not necessarily obviate having a formal course; the two can complement each other. In fact, the use of a CR as a text for such a course is quite a possibility, and a knowledgeable teacher could clarify the explanations and comments that the original compiler may have treated too briefly. A teacher can also acquire additional material to reinforce the lessons in the Reader, or to give specific individuals greater practice in handling the types of traffic with which they are actually working. A current piece of traffic may provide a better example of some phenomenon than the message shown in the COMINT Reader. (In other words, just because such a book has been published, this doesn't mean that the canon has been closed once and for all.) In fact, this is one advantage that a class can have over a CR.

Naturally I don't propose COMINT Readers for every language. In some cases, the traffic does not offer the variety of users that the common languages [redacted] provide. There are some languages where the volume is so small that one or two linguists get a chance to handle all the different types; there are other languages where the number of potential Agency employees who could profitably use a CR is so small that the time and effort spent in producing one could not be justified. But I do feel that such books would be valuable to NSA in helping people pass PQE's and--more important--to give Agency linguists a better understanding of some aspects of their language so that they can do a better job.

There are still a number of questions about COMINT Readers left unanswered. For example, who will prepare them? How can we be sure that all available type of material are included? How can we be sure that the material is correct? Will they really work? There may be other questions, but these four should hold us for a while.

P.L. 86-36
EO 1.4.(c)

A COMINT Reader should not be a one-man show or solo operation, especially for those languages where the input will come from a number of Agency components. To be sure, one person could be the committee chairman or editor-in-chief, but there should be several checkers, EO 1.4.(c) training officers, and other qualified linguists P.L. 86-36 responsible for the selection, arrangement, translating and explicating.

The obvious way to make sure that the material is comprehensive and correct is to have the greatest possible number of Agency elements using the language represented in that preparatory committee, and to staff it only with qualified linguists of recognized ability. Naturally they will have access to a broad range of materials classified up to and including TOP SECRET CODEWORD, which will most likely be the classification of the COMINT Reader. Having a sufficiently high security classification will also allow for a fairly complete inclusion of all sorts of appropriate material.

As for the last question, about whether COMINT Readers will really work, I honestly can't say. But I firmly believe that since the rotation system is impractical, and the setting up and holding of classes is a more complicated procedure (and has its drawbacks), COMINT Readers certainly ought to be given a chance. We won't know until we've tried--and, assuming that the CR idea will work, we ought to try it soon!

~~(TOP SECRET UMBRA)~~

CROSSED CODEWORDS
19 UKUSA COMINT CATEGORY DESIGNATORS USED OVER THE PAST 24 YEARS

by [redacted] P.L. 86-36

```
A C T I O S U Z S U M O R A V T O V I P
M M X S H S T A T T E M E C T L Z O U I
B M B T O A T I S E T U H C A K E T T S
I L S L K B E R D V T E C C O M F A R T
O Y K M E R R E M A A E E T A P L A I E
U D A X Y E D R A M L L A M N R S R N L
S A E O N E O E Q U N T R U N T R E E S
Z Z R O U T E L F I R U A L S O E V E N
O E E S T L O D A U N T D T B H A M E S
O D N E X E R X A L A X E M B S E V A E
M O N E Y Y L A Y N D I I E M E R R Z Y
Y S A V I N L E L L L K G D I R B M T E
M A I N C A N O E O A A N O L O S U Q F
R I G X I O U M E N U N T M O O R O E N
A L C M U S L E I E T I A T O K L S A R
M E N U P P S R D D A U Y B E S O K S O
S D R O E O Z E E I E O T Y Z O O N S C
I Q K S A O E N R X N E T Z B O F X I A
D E N A R K E T E D L A A R B M U U S L
N I L L I K R O V W E N R A I N R O F I
```

~~(SECRET/HVCCO)~~

DOCID: 4033678

CA is Ten Years Old!

January 1975 marks the tenth anniversary of the founding of the Crypto-Linguistic Association. CLA brings together linguists and other professionals of varying backgrounds and interests--the young technician eager to expand his horizons, the veteran seeking to promulgate a theory or present a new technique, the manager anxious to spot new talent or acquaint himself with the latest developments in the field. As a professional and learned society the Association has a duty both to the individual cryptolinguist and to the field as a whole, and in fulfillment of that duty it has steadily expanded its scope and its efforts.

To give cryptolinguists an opportunity to know each other; to acquaint them and other professionals with what is most significant in the field; to provide a forum in which members can present their ideas; to recognize achievements in the field of language at NSA--these are the goals of the Cryptolinguistic Association.

Lecture Series

This has been another exceptionally successful year for the lecture series, as attendance has testified. Members and friends have heard Clifford Groce of the Voice of America, Howard Rosenblum, NSA DDR, Brigadier Tiltman of P1, and, as a surprise bonus, Victoria Fromkin of UCLA's Department of Linguistics. The schedule for the next few months is as follows:

Tuesday 14 January	Tenth Anniversary Lecture by Mr. William Hyland, Director of the Bureau of Intelligence and Research of the U.S. Department of State.
Tuesday 11 February	"The Use of a FAST-Trained Linguist in Military Intelligence." Col. Richard A. Szymczyk, Chief of the Western Area Division of the Directorate for Intelligence, Defense Intelligence Agency.
Tuesday 11 March	"Computers and Linguistic Applications," Dr. A. Hood Roberts, Vice President of the Center for Applied Linguistics, Arlington, Va.
Tuesday 25 March	Gala Tenth Anniversary Concert. "Songs from Around the World." The U.S. Army Chorus under the direction of Capt. Allen Crowell.
Tuesday 8 April	"Translation: Science or Art?" Dr. Esther Matteson, Linguistic Consultant with Wycliffe Bible Translators.

(Note: All the speeches presented during the past two years have been recorded on tape, and it is expected that these will be also. The Association is now discussing with the Learning Center the use of its facilities for making the tapes available on cassettes for use within the Agency.)

Special Interest Groups

P.L. 86-36

The Association has two special interest groups now active, and two more in the process of formation. All interested members are invited to join one of these groups, or, with the approval of the Board of Governors, to establish a new group in a field of special interest to them.

SIGLEX (the Special Interest Group on Lexicography) was formed in 1972 and has been very active ever since. Some of the subjects in which the group has interested itself are modern methods and standards of lexicography, evaluation of commercially produced dictionaries, review of Agency-produced dictionaries and glossaries, and uses of the plain-language index. Several members attended the International Conference on Lexicography in New York in 1972. President is [redacted] 8407s.

SIGVOICE, as its name implies, is keyed to language in its spoken form, particularly to the work of transcribers and to research which may assist in better processing of voice intercept. So far this season it has taken up the subjects of voice transcription

EO 1.4.(c)
P.L. 86-36

at field stations, [redacted] and tactical voice in Vietnam. On 9 January 1975 Dr. Richard Altes of Electromagnetic Systems Laboratories, Sunnyvale, California, will discuss perception in bats, dolphins, and man. In February and March, [redacted] both of R54, will speak on voiceprints and auditory illusions, respectively. Jack Gurin, 5236s, is President of SIGLEX.

A new group now forming is SIGTRAN, which proposes to study the general principles and practices of translation, both inside and outside NSA. "Translation shall be interpreted in the broadest possible sense... [and]...shall closely relate to other fields of cryptologic knowledge, such as cryptography, computer science, and certain other branches of applied linguistics." The first meeting is scheduled for Wednesday, 22 January, at which time Whitney Reed will speak on free-lance translation. Interim chairman of the SIGTRAN group is Florence Kuipers, 4998s.

[redacted]

The Essay Contest

The essay contest is held annually; its purpose is to encourage writing on the application of linguistic knowledge to the solution of Agency problems. Any paper on language, cryptology, or a significantly related subject may be submitted and any NSA employee, regardless of membership in the CLA, is eligible to enter the contest. (Papers which have appeared in any Agency publication during the preceding 12 months will automatically be considered entries.) Prizes of a hundred, fifty, and twenty-five dollars go to the winners. Entries for this year should be submitted in three copies by Friday, 14 March, to [redacted] CLA Secretary, Room 2A197-1.

The Jaffe Award

The Jaffe Award is a memorial to the first president of the CLA, Dr. Sydney Jaffe. It is CLA's highest recognition of exceptional achievement, and takes the form of a citation and the inscription of the winner's name on a plaque on permanent display in the main lobby. P.L. 86-36

Candidates are nominated for outstanding achievement in one or more of the following:

- Integration of language work with other disciplines
- Linguistic research pertinent to the Agency's work
- Contributions to the effectiveness and morale of linguists
- Management of language operations
- Versatility in working with several languages
- Contributions to language training
- Saving of time and money in language operations
- Contributions involving rare languages
- Development of new equipment, procedures or systems expediting language work
- Scholarly eminence which has made the candidate of unique value as a consultant
- Public achievement which enhances the prestige of the language field.

Individuals may be nominated by any three members of the cryptologic community, by the chairman of the language career panel, or by any supervisor at office level or its equivalent. Nominations should be submitted by 30 March; for details call the CLA President, [redacted] 4332s.

The Spring Banquet

The CLA "season" culminates each year in a banquet in late spring for members and their families and friends. Dinner is preceded by a cocktail hour and followed by a program which typically includes a distinguished speaker on a subject of general interest, the introduction of new officers, and the announcement of the winners of the essay contest and the Jaffe Award.

P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

P.L. 86-36

DOCID: 4033678

Other News from the Learned Organizations

NSA CISI

NEW OFFICERS

[redacted], PRESIDENT
PRESIDENT-ELECT
CO3, SECRETARY
TREASURER
, MEMBER-AT-LARGE
MEMBER-AT-LARGE
, MEMBER-AT-LARGE

{*NEWLY ELECTED}

1975 CISI CONFERENCE

THE SECOND CISI SPRING CONFERENCE WILL BE HELD 20-22 MAY 1975 IN THE NSA AUDITORIUM. PAPERS HAVE BEEN SUBMITTED ON FOUR TOPICS:

SECURITY IN DATA SYSTEMS
DATA BASE MANAGEMENT SYSTEMS
FIELD SYSTEMS/APPLICATIONS
MANAGEMENT IN DATA SYSTEMS

THEY WILL BE PUBLISHED AND DISTRIBUTED TO MEMBERS BEFORE THE CONFERENCE. AUTHORS WILL DISCUSS THEIR PAPERS AT THE MEETINGS.

LECTURES

THE JANUARY MEETING, TO BE HELD AT 0930 ON 23 JANUARY IN THE NSA AUDITORIUM, WILL BE CO-SPONSORED BY SIG/HUMAN FACTORS. THE SPEAKER WILL BE MAJ. GEN. RIENZI, DIRECTOR OF TELECOMMUNICATIONS AND COMMAND AND CONTROL OF THE DEPARTMENT OF THE ARMY, DISCUSSING "SOME LESSONS LEARNED" DURING THE RECENT MIDEAST CONFLICT.

ON 26 FEBRUARY, [redacted] CHIEF OF THE PROGRAMMING AND RETRIEVAL LANGUAGE DIVISION, WILL SPEAK ON THE TOPIC OF DATA BASE MANAGEMENT. THE TIME IS 0930, PLACE IS THE NSA AUDITORIUM.

INTERNATIONAL AFFAIRS INSTITUTE

There will be no lecture in January. Dr. Edward Teller has accepted the invitation to speak on 5 February.

New Officers

CMI's biennial election of officers was held on 5 December 1974. The Council, Committee Chairmen, and Executive Director are listed below. An asterisk indicates that the person is newly elected.

REED DAWSON, P12, President
* [redacted] 51, President-Elect
* P12, Secretary
* N32, Treasurer
JIM THOMPSON, A54, Council Member
* S12, Council Member
R51, Council Member
* 51, Council Member
BILL MIXER, G42, Publicity
WALT PENNEY, P15, Executive Director

P.L. 86-36

Lectures

The speaker for February has not yet been decided upon. Dr. Joseph Blum of R will speak in March, on the general subject of CHARLOW and optical processing.

Essay Contest

Entries for the 1975 essay contest, in the form of papers on cryptology or any significantly related subject, may be submitted to [redacted] or Reed Dawson, Room 3W090 (telephone 3957s), by 28 March. Any NSA employee is eligible to enter. Security classifications are permissible, but ideas or techniques originating in compartmented areas should be reduced to a noncompartmented level for entering. Technical Journal articles published during the current year will be entered automatically.

EO 1.4.(c)
P.L. 86-36
DOCID: 4033678

~~CONFIDENTIAL~~

CRYPTOLOG INDEX FOR 1974

(Listed by Contributor)

[redacted]
Self-Paced Instruction: "The Future Is Now!".....Aug 15

[redacted]
The Old [redacted] Section: Parts 3 & 4.....Dec 5

[redacted]
Maps in Mind: A Photoessay.....Dec 1

Buck, Stuart H.:
(comments in) Cryptanalysis & Code Recovery.....Sep 5
Some Thoughts on Lexicography.....Sep 11

[redacted]
What Is A Collector?.....Aug 2
As We Go to Press.....Sep 7
The New Collection Criteria.....Dec 11

Craig, Derek K.:
COMINT Analysis of [redacted].....Sep 1

[redacted]
CISI Forming New Special Interest Group
on Human Factors.....Dec 10

[redacted]
The Mission of the Signals Processing
Requirements Panel.....Oct 1

Dudley, Barbara P.:
Nice Busman's Holiday for One NSA Employee.....Aug 19

[redacted]
What Should You Expect?
or The Analysis of Cryptanalysts.....Aug 5
Secrets of the Altars: The Moustier Cryptograms.....Sep 10
An October Overlap.....Oct 20
Answer to October Overlap.....Nov 21

Exinterne, Anne (pseudonym):
A Long Hard Look at the Intern Program:
Part One: Philosophy & Recruitment.....Sep 6
Part Two: Selection & Orientation.....Oct 11
Part Three: Motivation & Morale.....Nov 15
Part Four: What Happens to the Graduates?.....Dec 13

[redacted]
[redacted] What? Where? Why?.....Nov 5

Filby, Vera R.:
A Spot by Any Other Name.....Aug 7
The [redacted] Exercise: A Case Study in
Special Research Analysis.....Oct 16
The Apostrophe: Some Thought's.....Nov 14

Garofalo, Caterino G.:
Gary's Colors.....Sep 8

[redacted]
Character-Building in the People's
Republic of China.....Oct 7

[redacted]
Data & Definitions: Calling Things by
Their Rightful Names.....Nov 1

Jackson, William J.:
TDB: The TEXTA Data Base.....Aug 4
An Approach to Callsign Analysis.....Dec 7

[redacted]
New Trends in the Teaching of Cryptanalysis:
A Walk Through the '75 Curriculum.....Nov 7

John, George:
A Flag-Waving Programmer.....Dec 13

[redacted]
Purity of the Russian Language:
Slavophiles vs. Westernizers.....Nov 12

[redacted]
Reflections on a Translators' Conference.....Nov 10

Leahy, Francis T.:
A Proposal for Calendar Reform.....Dec 19

[redacted]
King Eusyb & Queen Deodi.....Sep 19

Mountjoy, Marjorie:
Cryptanalysis & Code Recovery.....Sep 5

P14:
The New Traffic Analysis Glossary.....Aug 8

[redacted]
Character-Building in the People's
Republic of China.....Oct 7

[redacted]
(with Ramón Santiago-Ortiz) The Language of
Beisbol in Everyday Talk.....Aug 11
Language in the News.....Sep 14
The English Language in the News.....Dec 12

Santiago-Ortiz, Ramón & [redacted]
The Language of Beisbol in Everyday Talk.....Aug 11

[redacted]
Calling All SRA's: Reporting Symposium?.....Aug 20

Tetrault, Emery W.:
Even a 5-Year-Old Child.....Oct 4

[redacted]
Guidesmanship or How to Write Technical Manuals
Without Actually Giving Anything Away.....Nov 18

Unsigned:
The New Traffic Analysis Glossary.....Aug 8
A Short Dictionary of Career Panels.....Aug 17
The Management Survey of the Philharmonic.....Aug 20
Prizes & Honors from the Learned Organizations.....Aug 21
Telephone Recall.....Oct 6
An Unofficial Glossary of Weasel Words.....Oct 10
News from the School.....Oct 14
Coming Events.....Oct 15
Assorted Editorial Notes.....Nov 4
Secret Messages.....Dec 4
Citizens of the World.....Dec 6
Letter to the Editor.....Dec 9

[redacted]
(comments in) Cryptanalysis & Code Recovery.....Sep 5

Webster, James B.:
Project CARRIAGE:
Worldwide HFDF Modernization Plan.....Sep 9

[redacted]
Subject: SRA Symposium.....Oct 19

Wolff, Maj Gen Herbert E.:
A Letter of Introduction.....Aug 1

[redacted]
Right-to-Left Text Sorts Are Not Impossible.....Aug 14

P.L. 86-36

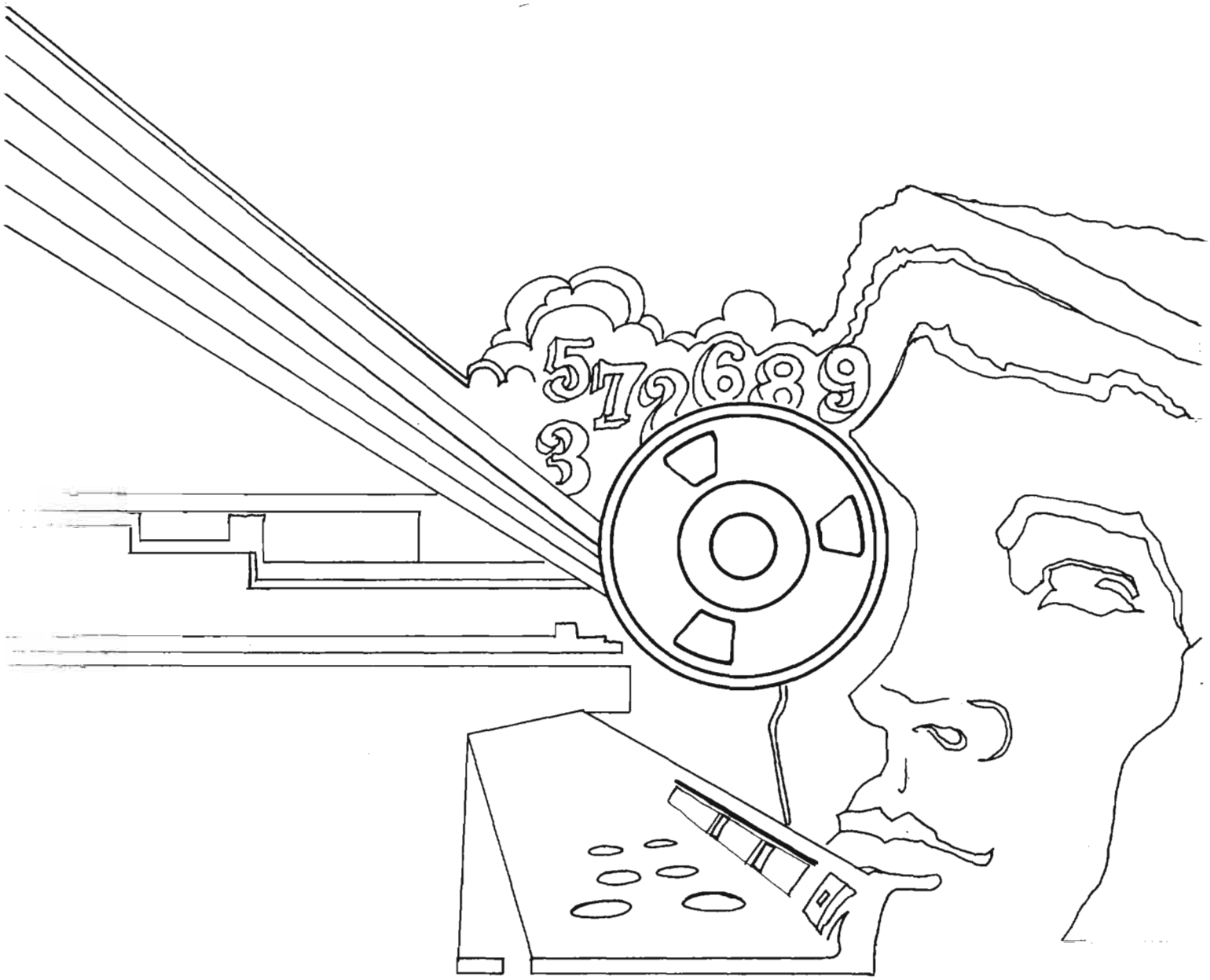
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

P1-Jan 75-S3-23375

~~CONFIDENTIAL~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~



DOCID: 4019620 P.L. 86-36

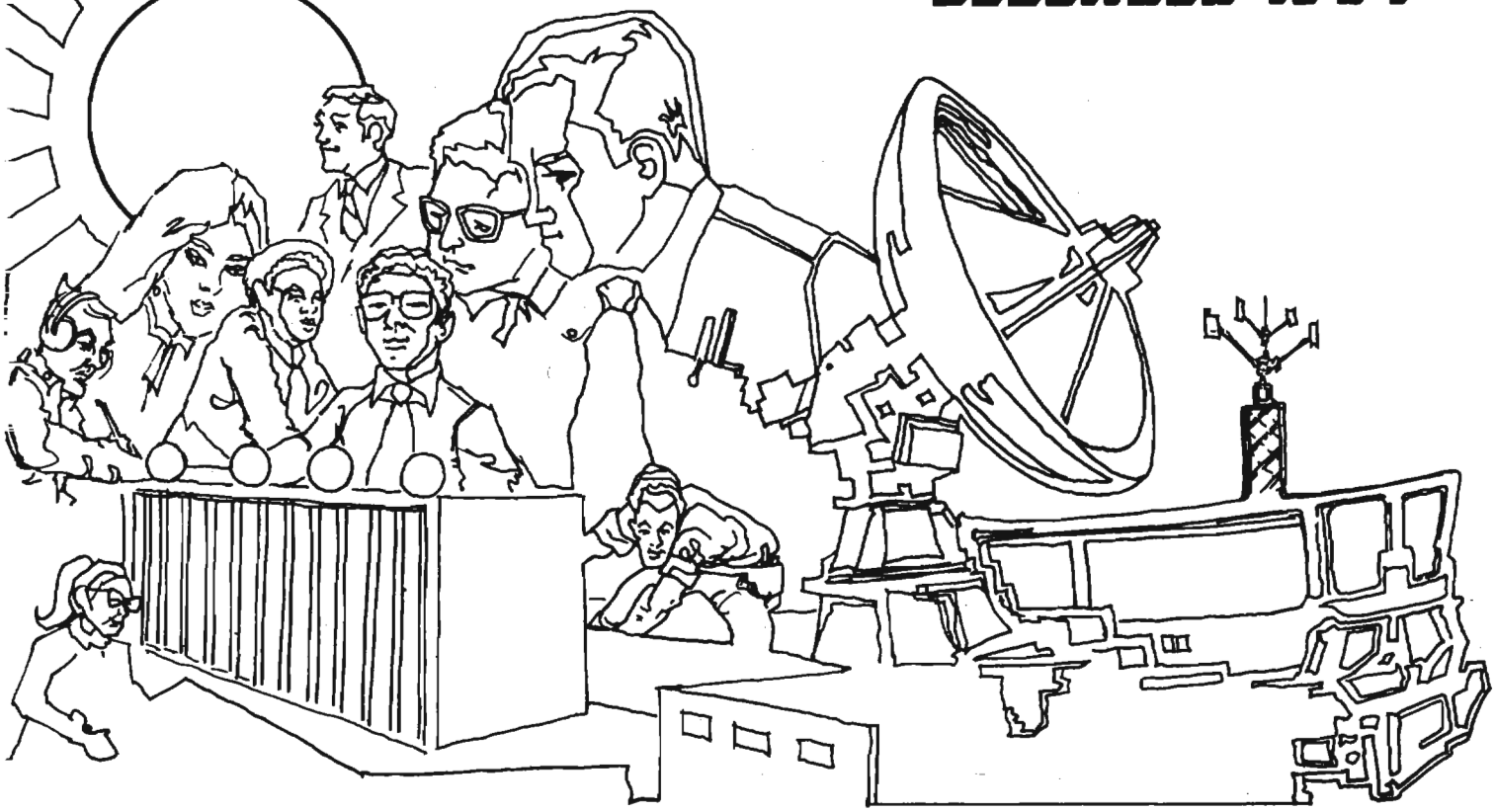
~~TOP SECRET~~

8311 [redacted]

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

DECEMBER 1974



EO 1.4.(c)

P.L. 86-36

MAPS IN MIND: A Photoessay. . . . . [redacted] 1
THE OLD [redacted] SECTION (Parts 3 & 4). . . . . [redacted] 5
AN APPROACH TO CALLSIGN ANALYSIS. . . . . .William J. Jackson 7
LETTER TO THE EDITOR. 9
CISI FORMING NEW SIG/Human Factors. . . . . [redacted] 10
THE NEW COLLECTION CRITERIA . . . . . [redacted] 11
A FLAG-WAVING PROGRAMMER. . . . . .George John. 13
A LONG HARD LOOK AT THE INTERN PROGRAM. . . . .Anne Exinterne 14
A PROPOSAL FOR CALENDAR REFORM. . . . . .Francis T. Leahy 20
CRYPTOLOG INDEX FOR 1974. 21

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4019620

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. I. NO. 5 DECEMBER 1974

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief ..... Doris Miller (5642s)
Collection..... [redacted] (3571s)
Cryptanalysis..... [redacted] (8025s)
Language..... [redacted] (5236s)
Machine Support..... [redacted] (3321s)
Special Research..... Vera R. Filby (7119s)
Traffic Analysis..... William J. Jackson, Jr. (3369s)

Art Editor..... [redacted]

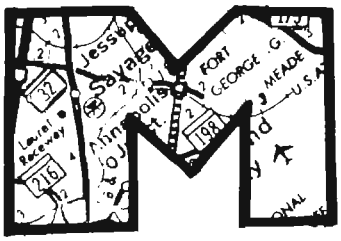
P.L. 86-36

* * * * *

Editor for December .....Harry G. Rosenbluh

~~TOP SECRET~~

DOCID: 4019620



MAPS IN MIND: A PHOTOESSAY

by [redacted]

Marshall McLuhan has said that the map is one of a select group of communications media without which "the world of modern science and technologies would hardly exist." Last year the Geography and Map Library in room 2N075 answered 5000 geographic information requests and furnished [redacted] maps, charts, and geographic publications to help the employees of the Agency communicate more effectively and to help them adjust to the rapidly changing target areas and international crises which characterize NSA's recent history. For those readers who have never used our services this photoessay should provide an introduction to the selection of maps.

In selecting a map we usually ask customers to visit the Map Library because describing a map over the phone can be difficult. One of the first questions we usually ask is what scale map is wanted. This is a confusing question because small can mean large and large can mean small. In other words, a small scale map covers a large area and a large-scale map covers a small area. Scales can run from 1:1,000,000,000 (one to one billion), which would be a map of the world the size of a postage stamp, to 1:1 (one to one), which you could get by putting a piece of paper on the floor, putting your foot on the paper and tracing around it. You would then have a map of your foot at a scale of one to one. Figure 1 shows three maps of [redacted] in small, medium, and large scales. The squares on the 1:1,000,000 and 1:250,000 maps represent the area covered by the 1:50,000 map.

The second major concern in selecting a map is the projection. Projection refers to the method used to put a representation of the earth on to a flat sheet of paper. Maps are usually projected onto cylinders, cones and planes. The following chart shows some of the major types and their uses.

FAMILY	NAME	USES
CYLINDRICAL	MERCATOR	Navigation and dead reckoning
CONIC	LAMBERT'S CONFORMAL	Atlases, pilotage and radio
AZIMUTHAL	EQUIDISTANT	Aeronautics, radio, engineering and celestial maps
	GNOMONIC	Trans-polar and trans-oceanic routes, radio and seismic work

FIGURE 2

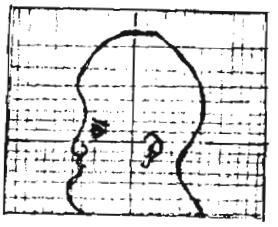
EO 1.4.(c)
P.L. 86-36

Figures 3a through 3f show how the human head would be represented in various mapping methods, revealing their respective distortions.

DOCID: 4019620

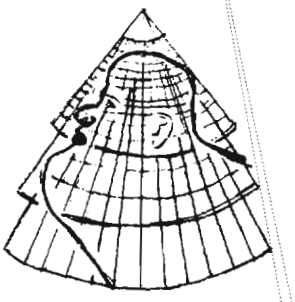
EO 1.4.(c)
P.L. 86-36

3a. Globular



3b. Mercator

3c. Polyconic



3d. Lambert's Conformal

3e. Stereographic

FIGURE 3

3f. Gnomonic

After the scale and projection questions have been solved, the major remaining problem is the type of features needed on the map. If you want a map to decorate your wall, a National Geographic Map with terrain features and many place names might be best. If you want to do plotting, an outline map would be best. Terrain, briefing, and outline maps come in three general sizes: small, medium, and large depending on the size of the paper the map is on, not the scale of the map. In general small maps are letter size and are good for including in SIGINT and other types of reports. The map shown in figure 4 is a medium-size map

usually include a medium size terrain map with small special inset maps covering population, economics, vegetation, ethnic groups, and other relevant specialized subjects. The map library has these area brief maps for most of the countries in the world.

~~CONFIDENTIAL~~

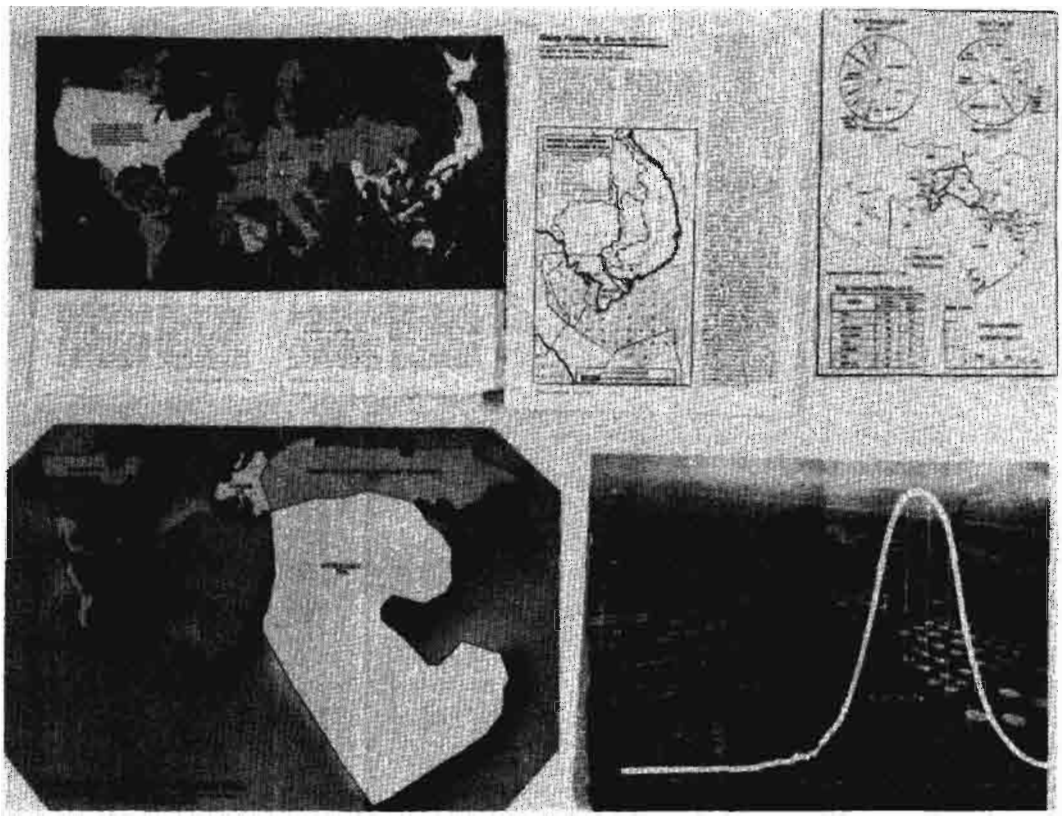


FIGURE 5

The last two figures cover special maps. In figure 5 you can see, if you squint real hard, a map taken from the National Geographic Magazine which illustrates the world wide use of oil. The United States is very large and Africa and Australia are tiny. The map below the oil use map shows in an exaggerated way the world of known oil reserves. These maps have been used as an ad for a well-known international oil company. These maps and the map from Forbes magazine, "Going Fishing in South Vietnam," which shows the oil concession zones in the South China Sea, illustrate the wide range of devices and distortions that maps employ to communicate and also the highly specialized nature of many maps. The Geography and Map Library has many examples of specialized maps: from maps which show oil pipelines, wells, pumping stations, etc., to bird hazard, whale, time zone, and ice charts to city and port plans to moon maps.

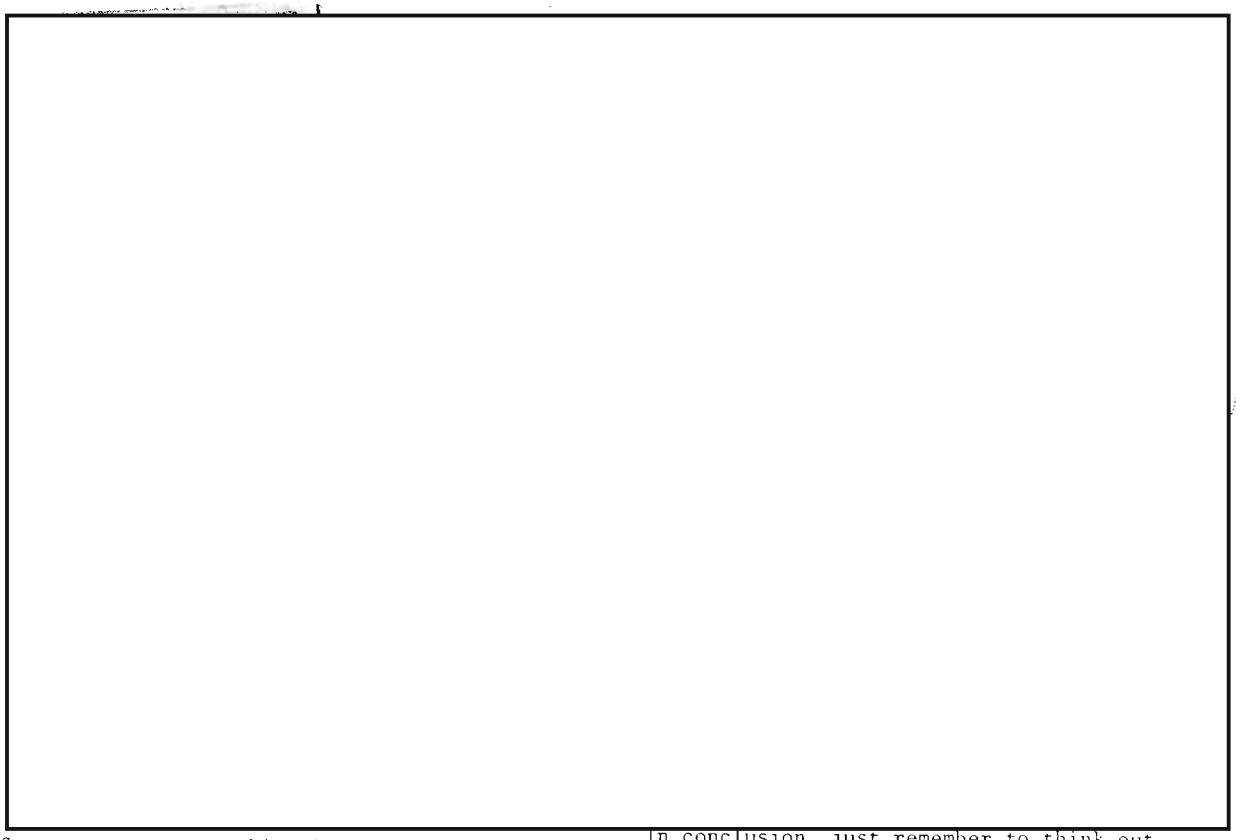
Figure 6 suggests the wave of the future as far as the production of many specialized maps is concerned. Computer plotting along with maps on microfiche and computer graphics will undoubtedly play a larger role for both geographers and Agency analysts. Of the examples shown in the photo, the one on the extreme right, illustrating field-of-sight plotting, would probably be the most useful for Agency problems.

Maps on microfiche can be useful when it is necessary to trace the course of a railroad, river, or border area over a long distance. Successive sheets in a map series can be photographically reduced and placed side by side on one fiche for easy visual continuity.

P.L. 86-36
EO 1.4.(c)

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~



P.L. 86-36
EO 1.4.(c)

As far as computer graphics is concerned, the Agency already has map programs on the following computer systems;

In conclusion, just remember to think out your map requirements in advance, then come on down and visit us in Room 2N075. Our hours are from 10 a.m. to noon and from 1:30 to 3:30 p.m. Also watch for our display at INFO 75 in March.

P.L. 86-36

SECRET MESSAGES

Linguists, collectors, information technicians, SRA's, and data systems people can all find articles in this issue of CRYPTOLOG dealing with their specialty. Somehow or other, there isn't anything for cryptanalysts. . . .or there wasn't anything for them until the Editor decided to fill this spot at the bottom of a page with three open-code messages from the back of Military Cryptanalytics, Part I. Each of these texts contains some other meaning besides the obvious one. Can you find the hidden message in each of these innocent-looking texts?

1. TO COVER AND HIDE YOUR FINANCES, I MAINTAIN STAFF TO BARTER FRANC EXCHANGE.
2. BEARER IS A FRIEND. I CANNOT WRITE MUCH. WILL YOU BE READY TO MEET A TRUSTED INTERMEDIARY SO YOU CAN GIVE ALL NECESSARY DOCUMENTS TO HIM NEXT WEEK? I HAVE NOTHING MORE TO SAY.
3. DISATISFIED WITH IMMIDIATE RESULTS OF YOUR AMALYSIS STOP ADITIONAL RENUNERATION TO ALL PERSENNEL WHO INDENTIFY COMPONANT PARTS OF THE ALLOIS OTHER THAN NICKEL OR COPPER.

Sorry but we can't print the answers, since these problems are part of an extension course. . . .but you cryppies shouldn't have much trouble with them.

(UNCLASSIFIED)

~~CONFIDENTIAL~~

DOCID: 4019620

EO 1.4.(c)
P.L. 86-36

THE OLD [redacted] SECTION Parts 3 & 4

reminiscences by [redacted]

P.L. 86-36

Parts 1 & 2 appeared in CRL, The Quarterly Review for Linguists, Feb & May 7

3: The Reviewer

The person who reviews the final English text [redacted] There are several advantages to having all outgoing messages read by one person:

1) The reviewer serves as a control point for conventions of style, usage, technical notations, spelling, publication series, priorities (sometimes a message looks hotter after degarbling, and priority is marked up).

2) The reviewer can best control the quality of the translations and monitor the observance of standards. This is best done by a single person.

3) The reviewer, seeing all outgoing messages, is able to examine each one in the widest context possible. He can on occasion [redacted] spot a duplicate translation which has slipped through the scanners unnoted.

[redacted]

EO 1.4.(c)
P.L. 86-36

DOCID: 4019620

4. Section Chief

EO 1.4.(c)
P.L. 86-36

The determination of standards in general and in detail is the responsibility of the section chief. He must therefore be qualified as a linguist. There are two principal ways in which he is able to observe and thereby exercise control over the quality of the end product:

1) He may receive the requests for clarification of texts from the consumers and from editors within NSA and personally conduct the research required for these requests.

2) He may periodically check messages which have been translated and review messages which have been checked.

It is normally of interest to the section chief to read daily the top priority messages which have been disseminated by teletype and to examine them with the eye of a reviewer.

CITIZENS of the WORLD

In 1963 President Kennedy expressed his solidarity with the beleaguered people of Berlin by proclaiming, "Ich bin ein Berliner!" This was understood without difficulty on both sides of the Atlantic. But what if he had wanted to express solidarity with the people of Hamburg-or still worse, Vienna? Americans might have been dismayed to hear the President call himself a Hamburger or a Wiener, for we are not always familiar with the forms that names of cities take to express citizenship.

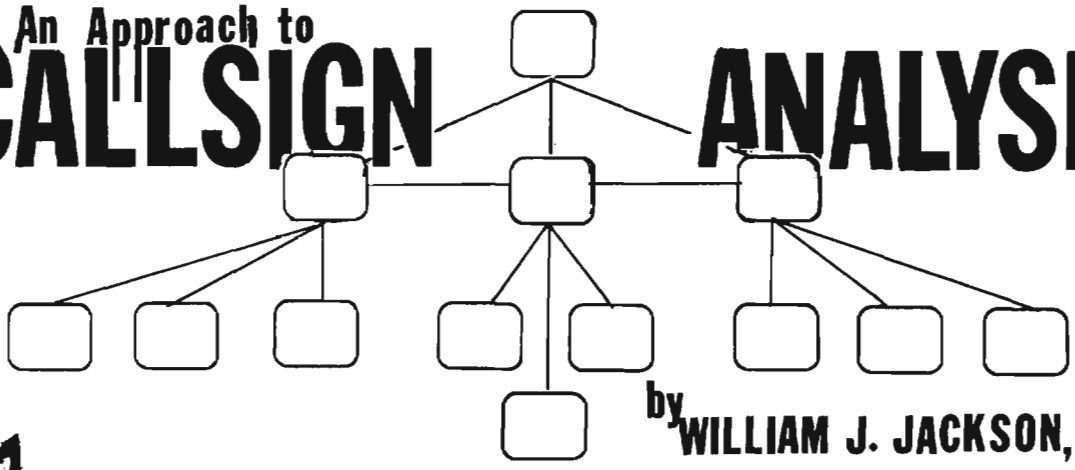
Even in English these may be unpredictable In the list below, can you give the correct or accepted English form for a resident of each city? (Answers on page 12.)

1. Aberdeen
2. Atlanta
3. Cairo
4. Cambridge
5. Dallas
6. Florence
7. Glasgow
8. Leghorn
9. Liverpool
10. Los Angeles
11. Madras
12. Madrid
13. Memphis
14. Moscow
15. Naples
16. New Orleans
17. Oxford
18. Parma
19. Peking
20. Rio de Janeiro
21. Shanghai
22. Tangier
23. Trieste
24. Warsaw

(UNCLASSIFIED)

DOCID: 4019620

An Approach to CALLSIGN ANALYSIS



EO 1.4.(c)
P.L. 86-36

by WILLIAM J. JACKSON, P14

According to Mr. C. G. Garofalo, former chief of P14, who is the individual most responsible for the solution of a number of target callsign systems over the past 30 years, the first step you should take when faced with the job of solving a new and complex callsign system is to go on two weeks annual leave!

The better either you or the team does on continuity, the easier and more successful your callsign analysis is likely to be. In addition to the requirement of continuity for successful analysis, another is that of complete openmindedness in the approach to the problem: no idea, no suggestion, should be dismissed as being implausible. (Remember, Aristotle said that a likely impossibility is always preferable to an unconvincing possibility.)

Probably the best approach to callsign study, after a number of callsign continuities are available, is to arrange the callsigns in a form which will facilitate the recognition of significant system characteristics and of phenomena useful in analysis. Several standard forms are available for this purpose.

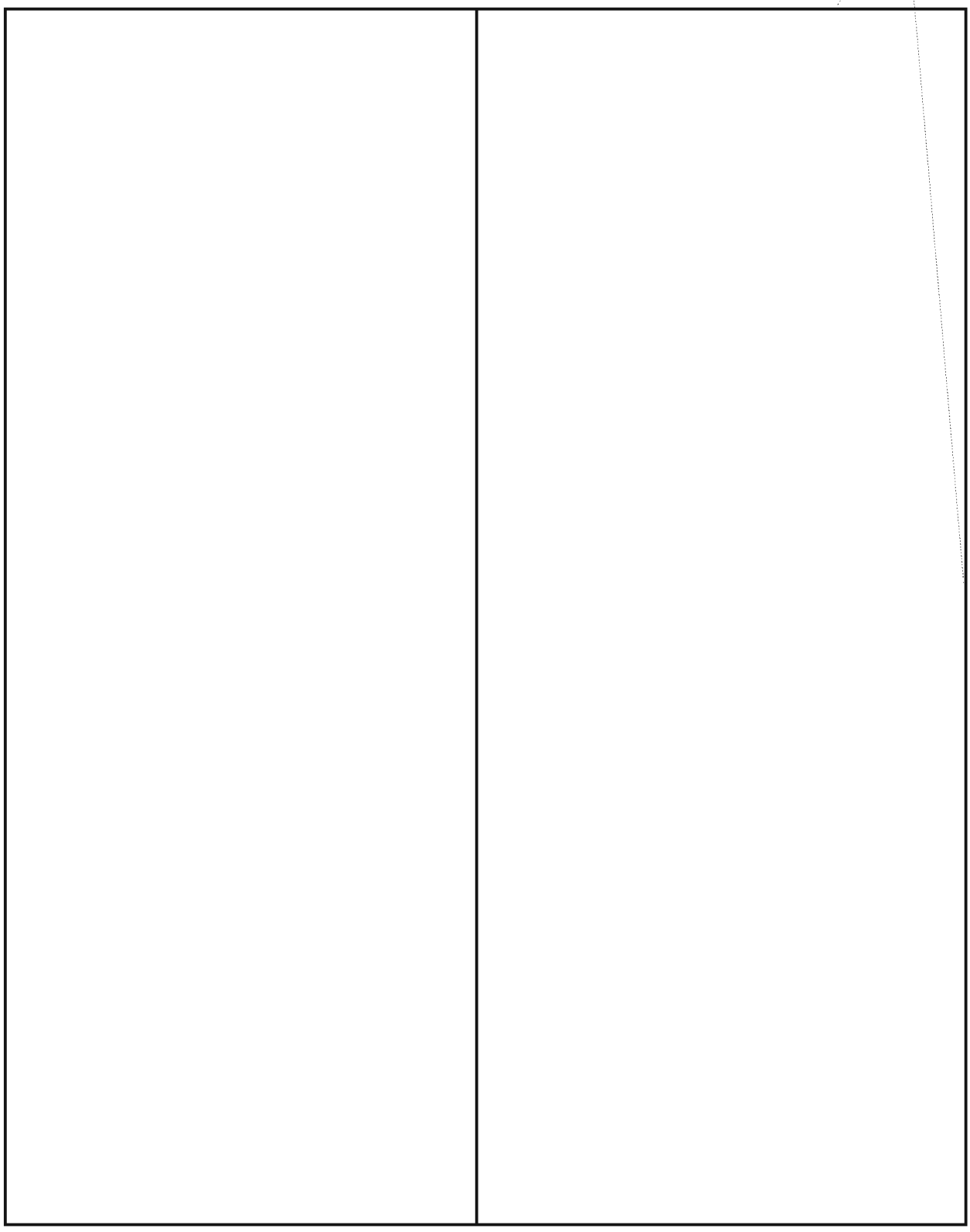
Assuming that the system is not immediately obvious, the initial objective is to determine what type it is.

EO 1.4.(c)
P.L. 86-36

DOCID: 4019620

P.L. 86-36
EO 1.4.(c)

~~SECRET SPOKE~~



~~SECRET SPOKE~~

EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~

[redacted]

In forthcoming issues of CRYPTOLOG it is expected that one or more examples of the application of the foregoing approach will be presented.

LETTER TO THE EDITOR

[redacted]

To the Editor, CRYPTOLOG Magazine:

The article in the September issue, "COMINT Analysis of [redacted]" by Derek Craig, is of great interest, but may I comment on this article?

[redacted]

Mr. Craig's analysis [redacted] was a valuable piece of reportage, and I personally enjoyed reading it and learned a lot from it.

Thank you for a very fine new magazine.

EO 1.4.(c)
P.L. 86-36
(Name withheld by request.)

~~SECRET SPOKE~~

DOCID: 4019620

Forming New SPECIAL INTEREST GROUP on Human Factors

by [redacted] A63 P.L. 86-36

Did you ever wonder. . .

how many hours are wasted because analysts have to read output in "computerese" that borders on low-level encipherment?

how many ACRP operators have trouble copying traffic due to high noise level in the aircraft, or possibly have hearing problems from the noise?

how many errors are made because of poor keyboard design or non-standard layouts?

why your typing keyboard is so high that it gives you a backache or tired shoulders, or just feels uncomfortable?

why somebody designed your operating console so you have to stretch to reach the controls, or why they didn't give you enough writing space?

how many computer jobs have to be rerun because the tape label was hard to read and the wrong tape was mounted?

how long this list would get if you really thought about all the other problems we live with, day in and day out, because someone forgot to consider the human being in the working environment?

Some of your colleagues have wondered, and are doing something about it.

Under the sponsorship of the NSA Computer and Information Sciences Institute (CISI) they are forming a Special Interest Group which will be called SIG/Human Factors.

The Special Interest Group's goals are:

To increase awareness of the need to consider human factors in our work, so that as systems and procedures are acquired or developed, (1) people are considered in relation to the total environment--which means consideration of human physiological characteristics, behavioral reactions, biomedical factors, training, motivation, personal comfort and safety, and (2) the highest and best use is made of both human and machine resources through assignment of appropriate roles to each.

To stimulate NSA/CSS-wide interest, understanding and involvement in the human aspects of our business.

To promote a more efficient intertace among people, hardware, software and environment in systems design, development and use.

To encourage the acquisition and application of information, tools and techniques to satisfy the above.

Through lectures, seminars, working groups and publications, SIG/Human Factors plans to provide opportunities to learn more about the human element in procedures and bring people with common interests and problems together on a professional level.

Under the general guidance of [redacted] (A63, ext. 3847), who initiated actions to start the SIG, the nucleus of the group presently includes [redacted] Jack Gurin (P16, ext. 5236). P.L. 86-36

Until the Group is more formally organized, these people are key points of contact. If you are involved in human factors work or are a user with a strong interest in how systems and procedures design affects you or your subordinates, please get in touch. We need your support.

As of now, commit yourself to a Vigilance Task (that's a good human-factors buzz word)! The task is to keep a watchful eye on your daily mail for notices of SIG/Human Factors activities, which should be starting soon.

NO PAGE 19-20 IN NOVEMBER ISSUE

You may have noticed that the Table of Contents for the November CRYPTOLOG listed "A Medal for Horatius" on page 19 and a Letter to the Editor on page 20. You may also have noticed that your copy didn't have pages 19 & 20 in it. It seems that the writer of the letter included some terminology and information that were better left unpublished in a general newspaper. Alas, the breach was not realized until the issue had been printed. . . . .so in the interest of security the offending page was bodily removed. The letter (duly sanitized) will be found on page 9 of this issue and the Golden Oldie about Horatius' medal will be included in CRYPTOLOG sometime soon. (UNCLASSIFIED)

DOCID: 4019620

by [redacted] W32

P.L. 86-36

NEW COLLECTION CRITERIA

The Collection Career Panel has now in draft a new set of criteria for Professionalization. The new criteria are to be published, we hope, in January 1975. Some description of the new criteria will be found below, but for now, let us just say that they are more pertinent.

When the new criteria are published, aspirants who have already submitted Professional Qualifications Records (PQR's) will have a specified amount of time from the publication date to achieve certification under the existing criteria. The new criteria will contain some rigid requirements--some specific demands -- not found currently. At the present, it is not easy to be a professional Collector; in the future it will be more difficult. At the present, training requirements may be met by peripheral courses and on occasion credit must be given for courses of very little relevance to the Collection business. The criteria to be published will afford points for any training or education, as before, but will require some specific Collection-related training as well as requiring some additional training from a set of "elective" courses. The specifics of the training requirements have not been agreed on entirely, but the basic concept will prevail as will most of the training required in the draft.

From a purist's point of view, the new criteria are exemplary in concept. There will be two professional areas: Collection Specialist and Collection Officer.

The Collection Specialist will be concerned primarily with Collection operations and it is intended that certification in this specialty will enable the individual to be promoted in professional-level assignments through grade GG-13.

To be certified as a Collection Specialist, an aspirant must have amassed 1,000 points, must have met certain minimum standards (including having taken some specific training courses), and he must have passed a Professional Qualification Examination. While academic education is always an asset in any professionalization system, technical training and achievements are stressed for a Collection Specialist, with academic education a very desirable adjunct. The emphasis for the Specialist is on technical competence.

The Collection Officer will be, as he is now, more oriented toward staff and management. The criteria for him will include certain minimum academic education requirements and some different required training courses, and some of the other minimum point requirements may be higher. Many of the basic requirements will be the same for the Collection Officer as for the Collection Specialist, so that the points earned in achieving certification as a Specialist will go a long way toward certification as an Officer, but it may be possible to become a Collection Officer without being able to qualify as a Collection Specialist. The normal progression, however, will probably be for an aspirant to be professionalized as a Specialist first.

DOCID: 4019620

Besides the addition of academic education requirements for the Collection Officer, he too will be required to pass the PQE. Further, he will also have to pass an oral examination board. When the aspirant has met all the minimum requirements, has passed an objective written qualifying examination, and has then been subjected to a further screening by an examining board, he will have demonstrated real professional competence. The new criteria will not be more difficult than those in existence now, probably, but they will be more rigid, more specific, more demanding. They will be focussed more sharply on Collection and in many ways will be more objective. This writer feels that they will be a vast improvement.

One of the chief benefits to be derived from the proposed criteria is that, for a very welcome change, a curriculum is being established for the career field. With the advent of the new criteria, a definite plan can be drawn, a career can be mapped out in Collection from the beginning. A potential professional Collector can be groomed and be guided by the criteria through a career from the time he enters on duty. Those of us elderly personnel who have floundered and drifted through an entire career can appreciate how much that could mean.

And let it be said one more time: The Collector is the backbone of the SIGINT system. Without him there is nothing for the other disciplines to work on. We need competent, professional Collectors, and through the new criteria, we will develop them.

~~(CONFIDENTIAL - HVCCO)~~

CITIZENS OF THE WORLD Answers (see page 6.)

1. Aberdonian 2. Atlantan (Not Atlantean; that's a whole nother story) 3. Cairene (rhymes with "gyrene") 4. Cantabrigian (from Middle Latin) 5. Dallasite 6. Florentine (as in Eggs) 7. Glaswegian (Hoot mon! That's ver-r-ry irregular; probably influenced by Galwegian & Norwegian. Did you have to think for a moment to figure out what Galwegian comes from?) 8. Livornian 9. Liverpudlian (the "pool" becomes a "puddle") 10. Angelено or Angeleno (depending upon whether or not you know Spanish) 11. Madrasi 12. Madrilenian ("Madrileño" is the Spanish form) 13. Memphite (if the city is in Egypt) or Memphian (if it's in Tennessee) 14. Muscovite 15. Neapolitan 16. Orleanian 17. Oxonian 18. Parmesan (as in Cheese) 19. Pekingese 20. Carioca (No, this doesn't come from the name of the dance; the dance was named after a person from Rio, and the word is derived from the Tupi Indian words for "white house") 21. Shanghailander (Honest; Look it up yourself) 22. Tangerine (ditto) 23. Triestino 24. Varsovian

(UNCLASSIFIED)

The English Language in the News

by

[redacted]

P16

P.L. 86-36

ENGLAND: Some messages sent in 1910 from a sea captain to Scotland Yard ---marking the first time that radio was used to capture a criminal---were auctioned off in London recently for about $4,000. Those messages led to the arrest of Dr. Hawley Crippen who left the dismembered body of his wife in the basement of their London home while he and his girlfriend went for a cruise to Canada aboard the liner Montrose. The captain became suspicious and used his ship-to-shore radio to ask Scotland Yard for advice.

A British boxing fan who was hoping for a son has given his new daughter a name involving the surnames of 25 heavyweight boxing champions and for the rest of her life the girl will have to fill out forms with: Maria Sullivan Corbett Fitzsimmons Jeffries Hart Burns Johnson Willard Dempsey Tunney Schmeling Sharkey Carnera Baer Braddock Louis Charles Walcott Marciano Patterson Johansson Liston Clay Frazier Foreman Brown. How did "Maria" get in there?

British males made sterile by vasectomy operations have begun wearing neckties with a special "V" motif, originally designed to promote the operation, but according to an official of the Vasectomy Advancement Society, many men who have not had the operation are placing orders for the ties.

DOCID: 4019620

FLAG-WAVING PROGRAMMER

by GEORGE JOHN, G42

Until six months ago I considered myself a competent programmer, but since writing a recent series of data handling programs I've had to revise that opinion. The programs behaved well when being written and initially debugged, but got rowdy after being given to an analyst for routine use.

[redacted] The job I tackled was to write a family of programs, one for each key system, to sort the key by identification, eliminate duplicate records, and add the newest data to a blocked tape. This tape would then contain all known key on that system, in a prescribed order.

The analyst who was to use the first program gave me the following information about the input data:

[redacted]

Taking the given information with a simple (minded) faith I proceeded to write programs to do the job.

The first time the analyst brought back one of the programs it took me a week to discover that the failure was caused by missing separators between the lane groups in the input tape. I had not thought to look there.

The second time she brought it back I analyzed the program logic for another week before I noticed that the segment numbers on the input tape were not in the proper order. I added a sort step to the program.

One of the other programs failed and after two weeks of looking at the program I found out that the analyst had combined two tapes onto one and input that one to my program. This introduced duplicate records and separate blocks of the same key, and thoroughly confused the program and me.

P.L. 86-36

It only takes one wrong record to derail a program, and unless that record is flagged at the time, you may find yourself searching through thousands of records without knowing what to look for. When an analyst tells you "All of the data has these characteristics" try to remember the wise old saying: "Statements that use 'always' or 'never' are always false."

P.L. 86-36
EO 1.4.(c)

Programmers can gain more yardage by having the computer act as referee. At each point where "unnecessary roughness," "offsides," etc., can occur, include the following:

a. A statement of what is wrong with the record;

b. A printout of the records that were being processed when the flag was thrown; and

c. A branch to read a new record and continue processing.

This technique should help both in initial debugging and in planning later revisions.

I'll just run it up the flagpole and see who salutes it.

WANT AD

WANTED: Unwanted RYE GUPPY Manuals. If you have a Manual in good condition and no longer need it please send it to [redacted] E13, FANX 2, for use in Cryptanalysis training courses.

DOCID: 4019620

A LONG HARD LOOK AT THE Intern Program

by 'Anne Exinterne'

PART FOUR: WHAT HAPPENS TO THE GRADUATES?

P.L. 86-36

[redacted] people have graduated from the intern program to date. What impact have they had on the work force? Is their performance notably different from that of college hires who took and remained in direct assignments? How do graduates feel about an Agency career? How do they feel about the intern program? While I have heard much concern about what would happen to college hires if they were required to have operational experience before being considered for an intern program, there seems to be relatively little concern about what happens to the graduates, and little effort directed at looking at the program through their eyes.

One panel did conduct a survey of graduates several years ago and found that approximately 20% of the graduates were having problems with their assignments and that the primary problem was lack of challenging work. There are two ways to look at the results of that survey--one is to say that the hands of those graduates were held for three years and if they encounter problems now they should be resourceful enough to know how to handle them. The opposite approach is to say that after spending thousands of dollars on classroom and on-the-job training for these people, it is foolish not to have some type of follow-up program to ensure that they are being usefully employed and to monitor their careers in order to keep abreast of problems that seem to be common to a number of them.

In fact, there do seem to be some patterns in the careers of that panel's graduates that would concern me if I were a Panel member or an M3 employee. The survey cited above revealed that sex and group assignment seemed to have a very significant bearing on career advancement. For instance, at the time of the study 14% of the graduates either had been assigned to Group X by the Panel or had transferred there and 17% of the graduates had been assigned to Group Y or had transferred there, but 57% of the promotions received by that Panel's graduates went to those in Group X and not one of the Group Y graduates had been promoted. If I were a Panel member, I would want to know if Group Y really had appropriate jobs for their graduates. Promotional opportunities also seem to have a sexual bias: 46 women and 43 men had graduated from the program as GG-11's. At the time of the study, six graduates had been promoted to GG-12; they were all men. Sixteen months later the grades of the first five classes this panel graduated were reviewed. By that time 17 of the graduates were 12's; 14 of them were men. While the Agency reorganization made it difficult to continue an organizational analysis, it was possible to determine that Group Y had yet to promote a graduate.

These findings suggest that the most significant indicator of a graduate's future advancement in this career field may be his sex, and that Group assignment is also a significant predictor; however, on a theoretical level Career Qualification Battery scores are used to predict success in a career field. How did the CQB scores of the graduates who were promoted compare to those not promoted? Scores of 57 graduates who remained in that career field from the first five classes the panel graduated were analyzed. For the 20 graduates who had been promoted to either GG-12 or GG-11 as of December 1973, the average CQB score in the category that pertained to their career field was 5.25. The average score of the 37 graduates not promoted was 5.64. I said previously that if I had faith in CQB scores as predictors of success and viewed the program as a highly selective one, I would require a higher score than the 5 that most panels currently require of program applicants since a 5 indicates average test performance. Actually, what the Panels may be expressing by not requiring a higher score is that they do not have such faith in CQB scores. In the case of this panel the requirement for a 5 was not even enforced for 15 of the 57 graduates; if it had been adhered to, almost half (9 of the 20) graduates who have been promoted would not have been accepted into the program. Three of those nine did not even receive a score of 4 and thus needed a waiver since they did not receive a qualifying score for the COSC. On the other hand, only 6 of the 37 not promoted (16%) did not receive a score of 5 or above and only one of those 6 did not receive a qualifying score for the COSC. While these are admittedly very small samples, these figures make me uneasy when I consider how much emphasis is placed on CQB scores in determining which employment applicants will be hired, and then what fields they will enter.

P.L. 86-36

That uneasiness prompted me to do some further research into CQB scores. I next compared scores of 60 interns, 30 with a degree and 30 without a degree for the category that pertained to their career field. In view of the recent proposal that the program again be limited to college graduates, I was impressed by the fact that the average score for non-college graduates (6.46) was higher than that of the college graduates (5.87). That difference in average scores may suggest that performance on the CQB could be affected by experience even though, with an aptitude test, this should not be the case. This theory received additional support from the test records of 8 on-board interns who took the CQB twice. Their two attempts yielded a total of 206 scores so 103 comparisons of scores could be made. Scores improved by 1 to 5 points in 56 cases, stayed the same in 26, and dropped in 21. Given a universal requirement of 5 for consideration for an intern program, these people would have gained eligibility in 20 categories and lost eligibility in 8. The most dramatic change was an applicant who went from a 3 to an 8, going from a score that was too low to even be considered for the program to a score that made him a prime candidate. The possibility that the first day was just a bad testing day for this individual is diminished by the fact that scores for 4 of the categories remained constant.

Another thing about the CQB that disturbs me is that the CQB battery seems to have changed little, if any, in the nine years since I first encountered it, although some career fields have changed considerably during that time.

[redacted] the SR field has attempted to assert its identity as a definable career field rather than a catchall for people who do not seem to fit into any other field. Does the present CQB, and the weights given the various subtests, adequately reflect this, or is the battery a selection tool that was appropriate for the fields ten years ago but not today?

My discussion so far applies to just one panel. The study that was done by the specially designated Intern Study Task Force provides a

EXTRACT FROM TABLES

Graduate interns 1969 and 1970

	CA	DATA SYSTEMS	LANG.	TA	SR
Number of interns	[redacted]				
Grade: GG-9					
GG-11					
GG-12					
GG-13					
Not Promoted Since Graduation					
Last P/A Outstanding					
Overseas Tour					
Resignations					

P.L. 86-36

FOOTNOTES

The categories of "Number of interns" and "resignations" were not defined but it appeared that "number of interns" referred to graduates who were still at the Agency and did not include graduates who have resigned since the sum of the figures in the grade breakdowns equaled that given for "number of interns." (The one exception to this was the SR Panel for which "Number of interns" appeared to equal the figures from the grade breakdown plus resignations). Therefore, to determine the total number of graduates I added "number of interns" to "resignations." This total was used only for the attrition information.

[redacted]

EO 1.4.(c)
P.L. 86-36

DOCID: 4019620

broader look into the fate of the intern program graduates. When I first looked at one of the study's charts, part of which is given above, I didn't see much of interest. However, I then used the data provided as the basis for additional computation and some interesting patterns began to emerge.

The information provided above yielded the following statistical information:

A. Percentage of Graduates Promoted by Career Field

DS- (57.5%)
TA- (33.3%)
LG- (33.3%)
CA- (23.6%)
SR- (17.2%) (These graduates were at a disadvantage since the first SR interns did not graduate until 1970, while other panels graduated interns in 1969.)

B. Percentage Promoted by Career Field and Sex

DS-M (66%)	SR-M (22.5%)
LG-M (58.3%)	CA-F (12.9%)
TA-M (50%)	SR-F (11.1%)
DS-F (39.1%)	LG-F (8.3%)
CA-M (37.5%)	TA-F (0%)

C. Percentage Receiving Outstanding Performance Appraisals by Panel

TA (86.6%)
LG (50%)
DS (47.9%)
SR (46.5%)
CA (27.2%)

D. Percentage of Outstandings by Sex and Career Field

TA-M (90%)	DS-F (43.4%)
TA-F (80%)	LG-F (41.6%)
LG-M (58.3%)	SR-F (37%)
SR-M (54.8%)	CA-F (29%)
DS-M (50%)	CA-M (25%)

E. Percentage of Graduate Resignations by Panel

TA (44.4%)
LG (33.3%)
CA (15.4%)
SR (13.4%)
DS (1.4%)

F. Percentage of Graduate Resignations by Sex and Career Field

TA-F (54.5%)	LG-M (20%)
LG-F (42.8%)	SR-M (6.1%)
TA-M (37.5%)	CA-M (4%)
CA-F (22.5%)	DS-M (2%)
SR-F (20.5%)	DS-F (0%)

(To give additional perspective to these figures, the statistics on resignations of interns in the program, from its inception through the first quarter of FY75, were analyzed using an M3 report. The figures for these five panels were clustered between a low of 24.8% for CA interns and a high of 29.3% for Language interns. It should be noted that these figures are lower than those contained in an FY74 Management Report. The difference may be due to varying definitions of attrition which will be discussed later.)

If I were an Agency manager and saw these charts I would want to know:

1. How do the figures for intern attrition in these fields compare with those for non-intern attrition? How do they compare with the figures for college hires who took direct assignments?
2. How many of these interns had prior cryptologic experience? I would be especially interested in this figure for the TA field. If those with prior experience do have better attrition records than the liberal arts graduates, as I suspect, why don't we concentrate on hiring them for fields like TA?
3. Has a study been done of the interns who resigned? Do college hires with certain majors and personality profiles tend to leave as I suggested previously?
4. We have heard much about the loss of data systems personnel once they have received some Agency training; however, the '69-70 data systems graduates had the lowest attrition rate at the time of this study, and at that time these graduates had been with the Agency for up to eight years. Is their graduate attrition rate the direct result of having the highest promotion rates? Is there a leveling off that takes place--do those who stay here five years tend to make their careers here? Or has the attrition rate for data systems graduates changed for the worse in recent years? One C Group manager told me of his idea to try to establish a model based on the past attrition of data systems personnel and changes in the nation's economy. Such a model could possibly alert Agency managers to an impending large-scale loss of data systems personnel. Did such a model ever become a reality?
5. Is there a logical explanation for the fact that the resignation rates for interns while in the program are closely clustered, as among the various fields (24.8--29.3%), but resignations of graduates show wide variation (1.4--44.4%)?
6. Why is there little relationship between the panel rank order for promotions and the one for outstandings? Is it much harder to get an outstanding if you are a cryptanalyst than if you are a traffic analyst? Why do female TA graduates have the second best percentage for receiving outstanding performance appraisals but not one of them had been promoted? Why is it that the performance appraisal percentage for the female CA graduates is better than that for the males but the reverse is true for their promotion percentages? Is it true that women are given outstandings while men are given promotions?

DOCID: 4019620

7. Why is it that only 2 of the 19 field assignments received by intern graduates have gone to women? I suspect that some people would reply "Because women aren't interested." Then isn't it interesting that 2 of the 5 TA women graduates have field assignments? What was so different about those women compared with the other female graduates?

8. I strongly suspect that if the study had shown promotions received by organization there would have been biases across the board just as there were in the study that the one panel conducted. Are such biases of interest to M, the Panels, or Agency managers?

9. Is it of interest to M3, the EEO office, or Agency managers that the promotion figures show the most sexual segregation and that the male graduate who statistically has the worst chances for promotion still has a better chance than every woman graduate except those in the data systems field?

I think it is unfortunate that studies such as this one usually stop short of looking for cause and effect relationships and thus are not as meaningful as they should be. In this study I think some of the questions asked were too vague to allow the task force to do this type of analysis. For instance, if I were one of the supervisors who was asked "Is there a difference in the work performance of an on-board intern graduate compared with a college campus intern graduate? "I would ask that the categories be broken down further. Maybe I would take a college hire with military experience as my first choice, an on-board college graduate as my second choice, an on-board intern with no degree but related military experience as my third choice, a direct college hire as my fourth choice, etc.

I was also concerned by the type of question that intern graduates were asked. Perhaps the originators of the study did use some graduates as a sample before administering the questionnaire but such a review was not evident in the final questions. Most of the ten questions were of an opinion nature e.g. "Is there a continuing need for an Intern Program in your career field"? While the answers to such questions are certainly of interest, as an intern graduate I felt there should be managers better qualified to supply an informed answer than I. To me, the value of asking intern graduates to compare their performance with that of non-interns is also dubious and I question the wisdom of using such subjective questions as part of a study that was designed to determine if the intern program should be continued.

If subjective questions are used they should be followed up by facts and figures. In this case, would facts and figures support the subjective opinion included in the study? In comparing job performance, the majority of graduates felt that their job performance was more effective than that of their non-intern peers. Since I wasn't able to compare effectiveness of job performance, I compared the grade levels of intern graduates, current on-board interns, and college recruits who took and remained in direct assignments for one career field. In doing this I reasoned that there should be a relationship between job effectiveness and grade level even though previous research indicated an organizational and sexual bias associated with promotions.

I established the following parameters for determining who would be in my sample to insure that the people I was comparing would, in fact, be similar: only employees who had a degree, were born in or after 1942, did not have more than 12 months difference in their Agency and government service computation dates, who still held a COSC for that career field, had not been an intern in another career field, and were not assigned to a group that contained only intern graduates or only direct hires. Since the intern program is described as a highly selective program, I envisioned that I would be able to find several employees who had been given direct assignments for every intern graduate; therefore, I was surprised when I found 31 intern graduates and 15 current interns but only 29 direct hires who fit these parameters. The selectivity ascribed to the program and the fact that the original interns had received two virtually automatic promotions also made me suspect that the intern graduates would have a grade edge, but an analysis of the grades of these three groups revealed a very mixed picture. In general, the employee with the highest grade of a group that started in a particular month could be either an intern graduate or a direct hire; the honor never went to a current intern (it should be noted though that interns can not be promoted above GG-11). I noticed that when I reached employees who have been at the Agency for 66 months or less that the Agency-wide shortage of promotion funds tended to produce an equalizing effect but, interestingly, four of the five people who have been promoted from that group were direct hires; the fifth was an intern graduate. The lesson for on-board employees considering entering the program apparently is that if promotion is a major concern, they will probably do just as well, if not better, staying in an operational assignment --particularly if money remains tight.

Until now I have not made any reference to the attrition rate for women as compared with that of men. I still hear supervisors voice reluctance first to hiring and then to giving ad-

DOCID: 4019620

vanced training and promotions to young women, giving as their reasons that the women are likely to marry and then leave the area or become pregnant and resign. It is no longer valid to use such arguments. I also suspect that in many cases a baby may not actually be the prime cause of resignation, but its arrival represents a socially acceptable reason to leave a job with which the individual may have been disenchanted for some time. In fact, I wonder how many men would elect to stay in their current jobs if at some time between the ages of 25 and 35, they were placed in a position where the social pressure they received was to resign rather than stay on the job and when they were in a position where they knew statistically that their chances for success were considerably lower than those of their counterparts of the opposite sex.

Motherhood doesn't necessarily make a woman less interested in an Agency career provided she believes that she has a chance of advancing in that career. It is disturbing to me that the female intern graduates may be suffering from the same types of handicaps as far as advancement is concerned that women in previous eras did. I had hopes that since the intern program gave men and women the same training, work experience, and promotional opportunites, that this equality would carry over into their post graduate years.

Conclusion:

Much of what I have said really concerns one central issue: Is there a well defined philosophy behind the intern program as well as other Agency programs and practices? By "well defined," I do not mean fixed; in fact I do not believe that anything should be considered exempt from change, but just as the data systems analyst documents a program he writes, there is a need to document personnel practices. Because of frequent changes in administration and a lack of such documentation, there is a tendency for Agency personnel to continually "reinvent the wheel." In the case of my article, I realize that few of the ideas are unique; even so, I was somewhat surprised when, while working on this month's installment, I came across an Agency Management Report that included these questions:

> Are college graduates needed for all the jobs that these individuals are now on? Are some college graduates being put on the wrong jobs? Is the Agency hiring more college graduates than it needs? Is there such a thing as an ideal NSA type that perhaps should be recruited?

These questions sounded much like some that appeared in my first installment, but they were contained in an October 1961 report.

Were these questions answered in 1961? If they were, and the answers were documented, and readily available maybe I would not have repeated the questions in 1974. Or perhaps on the basis of the documentation provided, I could have seen that those answers seemed appropriate for the Agency in 1961 but not in 1974.

Footnote on program statistics: In my research I encountered several problems of definition which M3 and the Panels must also have encountered. For instance, how do you define terms such as "graduate of the program" and "attrition"? In the past some panels classified anyone who completed the program as a graduate whether he achieved certification or not, while other panels apparently considered those who completed the program but were not certified as "transfers out." I indicated previously that the figures on intern resignations in one M3 report differed from the figures on intern attrition in another report based on M3 input. The explanation may be that "attrition" includes more than resignations in one case but this was not evident. I can think of several types of attrition figures that would probably be of interest in reviewing the program: A. Program attrition: How many people who enter the program complete it? This would include transfers out and resignations but only those people who resign during their internship. This could be further broken down in several ways such as direct hires vs. on-board interns, college graduates vs. non-graduates, etc. B. Current intern resignations: what percentage of inters leave the Agency during their internship? C. Graduate attrition: What percentage of graduates are left to mark five or ten years at the Agency? (This assumes there is a method of identifying intern graduates; in the past there has been no systematic way of doing this) D. College hire attrition: This could also be broken down into sub-categories such as college hires who go directly into the intern program, who take and remain in direct assignments, and who become on-board interns. E. Career Field Attrition: The purpose of the program is to supply professional level employees for a specific career field. How many graduate interns leave the field within a year after graduation, five years after?

Which of these categories, if any, do the attrition figures compiled by M3 fall into? Without precise definitions for terms such as "graduate" and "attrition," statistics on the program using such terms are of questionable value.

DOCID: 4019620

It is natural for a new manager to want to leave his mark on a position, but in his attempts to do so it is possible that he may institute a program very similar to one that failed five years before. All too often the employees concerned and the administrator's successors do not know whether a change was made for philosophical reasons, budgetary reasons, for the sake of change itself, or simply as a display of power. The changes I am referring to affect virtually every aspect of Agency employment, including hiring, training, course content, criteria for professionalization, reorganizations, and relocations.

Such documentation would be extremely valuable in program evaluation. It appears that there are often two sets of goals for a program, those that are written and those that are understood. There is nothing in the 1973 Intern Program Study to indicate that one of the primary motivations for establishing the intern program was to reduce the attrition rate of college hires, but if you ask an M3 employee to evaluate the effectiveness of the program, reduction in attrition is likely to surface as a major motivation for starting the program and as a significant accomplishment of it. (Attrition has dropped from the 65% reported for college hires in a 1961 management report to the 30% reported for interns in an FY74 management report.) If this was a primary goal, maybe continuation of the program would be justified on the basis of that reduction even if none of the graduates were certified; but then attrition statistics should be a factor in program evaluation, and every effort should be made to determine how much of the reduction in attrition can be credited to the program and how much to other factors, such as a change in the economic climate of the country.

It also seems appropriate to ask: Would there have been other equally effective ways to reduce attrition? Is there a point at which the reduced attrition no longer justifies the cost involved? Is there a point at which it becomes counterproductive? I suspect that the Agency attrition rate would be even lower if all new hires were started as a GG-9 and guaranteed a GG-11 30 months later, but it would be lower for the reasons alluded to previously: the recruits, good or bad, would soon reach a point where they felt they could not afford to resign.

A look at the orientation of new college hires illustrates another need for documentation. Currently there is a 9½-week orientation course for new uncleared hires, but cleared hires are available for assignment immediately --usually on their third day in the Agency. My questions concerning this course are: is its primary purpose to give new hires an orientation to the Agency or simply to keep them occupied while processing their clearances? If the goal is to give them an orientation, and if it has been determined that 9½ weeks is the amount of time needed for that, then every new hire, cleared or uncleared, should have the course. If the number of new hires dwindles to a precious few (as it did several years ago) other provisions should be made for the orientation, but the reason for discontinuing the formal course should be documented so that 10 years hence officials at the School, in M, and elsewhere will know whether the course was dropped because it was considered unnecessary or ineffective or because of cuts to the E budget. On the other hand, if the primary purpose of the course is to keep the new hires occupied and 9½ weeks is not really needed to orient them to the Agency, then it is reasonable to expect that cleared hires would be placed in a more concise course. If the number of people not cleared soon after completing that course grew to be a substantial one, it would also be reasonable to reinstate LIC working areas rather than continuing with the self-study courses that comprise the second portion of the present CY006 course. I suspect that the School already has machine records on courses , so perhaps the documentation I advocate could be done by simply inserting in existing programs a few comments about why courses were instituted, modified, or dropped.

Similarly the contents of the panels' annual reports could be adapted to provide for some philosophical consistency both within and between panels. This could save the panels from having to learn the same lessons independently. For example, in its original criteria Panel A stipulated that an aspirant could not take the PQE more than three times. When an aspirant vouched for by his supervisor as a very valuable employee, failed the test for the third time the Panel was in a quandary; the authors of the criteria had not included any ideas on what was to become of such people. The Panel concluded that it was not practical to limit the number of times an aspirant can take a PQE. About a year later Panel B published revised criteria in which one of the new features was a three-time limit on taking the PQE. Now it has apparently learned the same lesson as Panel A and recently removed the limit. Why wasn't the first panel's experience sufficient to keep the second from having to go through the same educational process? While the panels' annual reports are a means of sharing findings, and panel A's change in criteria probably was included in its report, in order to be of value to other panels and to successor members of the same ones, the announcement of changes in criteria should include the rationale behind it.

Once steps have been taken to explain the philosophy behind the intern program and other programs, the next step is to encourage discussion of them. I am not advocating "management by the masses," but I believe that keeping

DOCID: 4019620

employees informed is beneficial to all concerned and that every employee should be encouraged to comment on program features, to suggest improvements, or simply raise questions. I am not talking about a hot line to handle complaints, but a "philospher's corner" in Cryptolog or Spectrum, where you might find an article composed of the views of an operational employee, an M3 employee, an intern graduate, and a current intern on what the goals of the intern program are and whether they are being met. Or an argument for specialization by an employee who has only strayed from his 20 year association with one problem for the six months needed for certification, side by side with an argument for diversification by someone who has been with the Agency for 20 years and never spent more than two years in one place. Such a column might alleviate the feeling that many people have that the system has become more important than the people it was supposedly designed for.

I'll conclude my contribution to such a philosophical discussion by saying that it was not my primary goal to win converts to all my beliefs, but I did hope to start people thinking about many facets of the program and asking which ones are good, which should be modified, and which eliminated. I hope that current and graduate interns as well as non-interns will now take up the discussion.

A Proposal for Calendar Reform

by

Francis T. Leahy, P15

When Julius Caesar introduced his calendar, he designated every fourth year as a leap year, the extra day being February 29th, as at present. However by the 16th century it became evident that there had been a few too many leap years, since their purpose, of course, had been to synchronize the calendar year and the earth's annual revolution around the sun. It seemed that there had been about three leap years too many for every period of 400 years. Thus at that time there had accumulated about 12 extra calendar days.

In 1582 Pope Gregory XIII proposed that the accumulated extra days be dropped all at once and that thenceforth all calendar years ending in 00 (except those divisible by 400) consist of 365 days and therefore not be leap years. (Following this rule, 1900 was not a leap year.) Summarizing: every period of 400 years would have only 97 leap years instead of the 100 that Julius Caesar had envisioned. Since 97 X 366 + 303 X 365 is an exact multiple of 7, each of these periods of 400 years begins with the same day of the week.

There was general chaos, confusion and turmoil for several centuries, as each country found it expedient or necessary to come into line with the new Gregorian calendar. The United States, for example, did not adopt it until the time of the American Revolution, and then only after a long struggle. As great an improvement as the Gregorian calendar is over the Julian calendar, there will nonetheless be an accumulated error of one day after 3,200 years. I believe the turmoil that might occur at such a time can be avoided.

If Pope Gregory had had a large computer in his basement, he would have noted that by merely excepting every year exactly divisible by 128 from the Julian leap year rule, he could have had at once a simpler and a far more accurate calendar. Instead of 97 leap years every 400-year period he would have proposed 31 for every 128-year period. Oddly enough, this leaves 97 normal years. (The number 128 is two to the seventh power, or 10 000 000 in binary notation. This may or may not be of mystical significance.)

If we now decide to adopt this improved rule, it would first affect the year 2048, which at the moment is scheduled to be a leap year, although of course it should certainly not be one.

If the earth continues to rotate at its present rate, the proposed calendar will be accurate for 173,000 years. (Actually it slows down by one second per day after 500 centuries.)

(Note: The true period of the earth's revolution now is 365 days, 5 hours, 48 minutes, 45 seconds, and some hundredths of a second. We note that 5 hours, 48 minutes, 45 seconds divided by 24 hours results in 31/128. Hence one leap year dropped from the original Julian calendar of 32 such, every 128 years, produces almost perfect synchronization.)

DOCID: 4019620

~~CONFIDENTIAL~~

CRYPTOLOG INDEX FOR 1974

A Flag-Waving Programmer.....Dec 13
A Letter of Introduction.....Aug 1
A Long Hard Look at the Intern Program:
Part 1: Program Philosophy & Recruitment.....Sep 16
Part 2: Selection & Orientation.....Oct 11
Part 3: Motivation & Morale.....Nov 15
Part 4: What Happens to the Graduates?.....Dec 14
A Proposal for Calendar Reform.....Dec 20
A Short Directory of Career Panels.....Aug 17
A Spot by Any Other Name.....Aug 7
An Approach to Callsign Analysis.....Dec 7
An October Overlap.....Oct 20
An Unofficial Glossary of Weasel
Weasel Words (Golden Oldie).....Oct 10
Answer to October Overlap.....Nov 21
Answer to Puzzle No. 1.....Aug 20
Answer to Puzzle No. 2.....Aug 18
As We Go to Press.....Sep 7

Calling All SRA's: Reporting Symposium?.....Aug 20
Character-Building in the People's
Republic of China.....Oct 7
CISI Forming New Special Interest Group
on Human Factors.....Dec 10
Citizens of the World.....Dec 6
Citizens of the World Answers.....Dec 12
Coming Events.....Oct 15
COMINT Analysis of [redacted].....Sep 1
Contributions Solicited.....Sep 21
Cryptanalysis & Code Recovery.....Sep 5
CRYPTOLOG Index for 1974.....Dec 21

Data & Definitions: Calling Things by
Their Rightful Names.....Nov 1
Department of Golden Oldies:
An Unofficial Glossary of Weasel Words.....Oct 10
King Eusyb & Queen Deodi.....Sep 19
Management Survey of the Philharmonic.....Aug 20
[redacted] What? Where? Why?.....Nov 5

Even a 5-Year-Old Child.....Oct 4

Gary's Colors.....Sep 8
Guidesmanship or How to Write Technical Manuals
Without Actually Giving Anything Away.....Nov 18

King Eusyb & Queen Deodi (Golden Oldie).....Sep 19

Language in the News.....Sep 14
Letter to the Editor.....Dec 9
Lexicographic Corner:Some Thoughts on
Lexicography.....Sep 11

Maps in Mind: A Photoessay.....Dec 1

New Trends in the Teaching of Cryptanalysis:
A Walk Through the '75 Curriculum.....Nov 5
News from the School.....Oct 14
Nice Busman's Holiday for One NSA Employee.....Aug 19

Prizes & Honors from the Learned
Organizations — Spring 1974.....Aug 21
Project Carriage: Worldwide HFDF
Modernization Plan.....Sep 9
Purity of the Russian Language:
Slavophiles vs. Westernizers.....Nov 12
Puzzle No. 1.....Aug 10
Puzzle No. 2.....Aug 13

Reflections on a Translators' Conference.....Nov 10
Right-to-Left Text Sorts Are Not Impossible.. Aug 14

Secret Messages.....Dec 4
Secrets of the Altars: The Moustier
Cryptograms.....Sep 10
Self-Paced Instruction: The Future Is Now!.....Aug 15
Some Thoughts on Lexicography.....Sep 11
Subject: SRA Symposium.....Oct 19

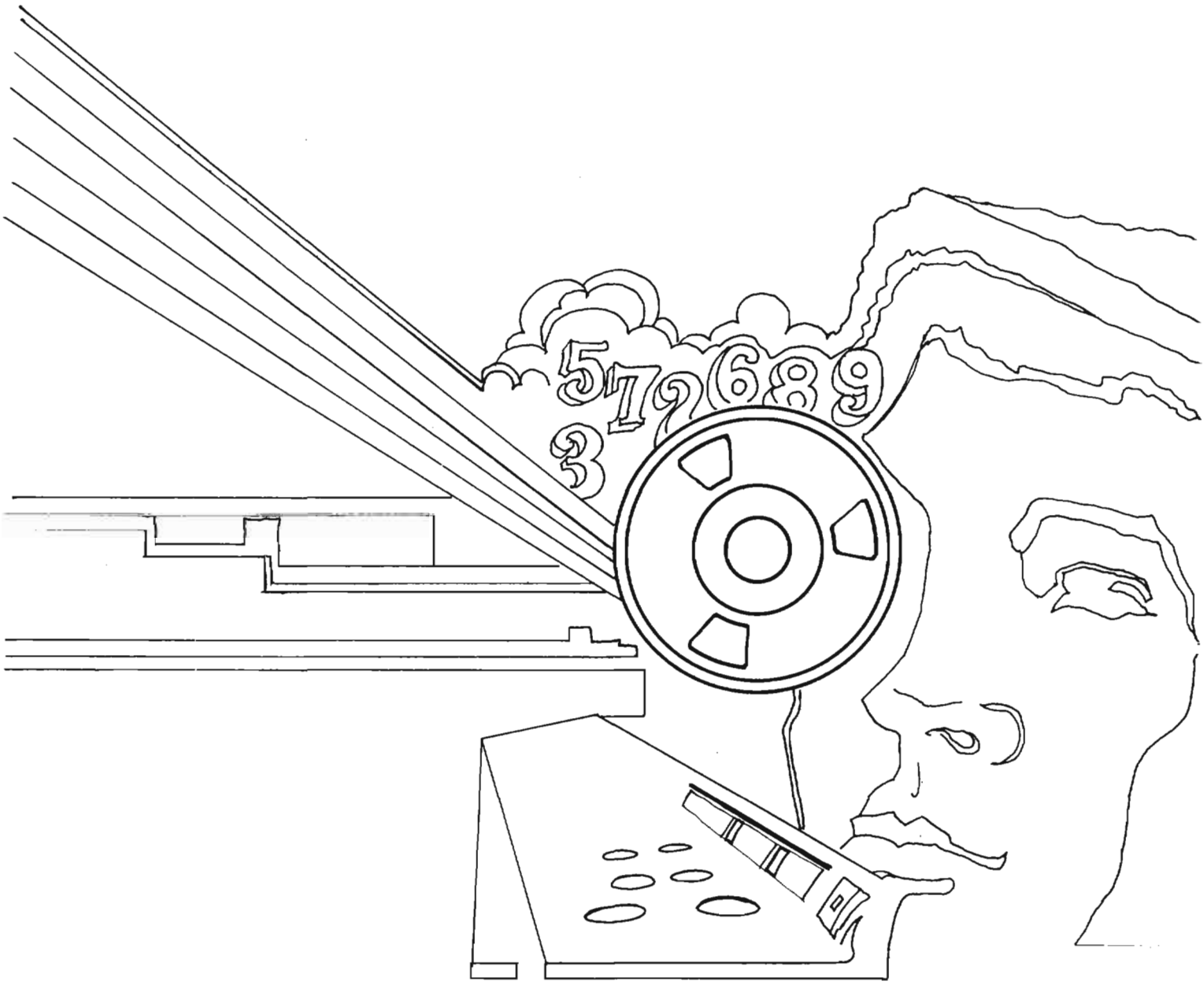
TDB: The TEXTA Data Base.....Aug 4
Telephone Recall.....Oct 6
The Apostrophe: Some Thought's.....Nov 14
The English Language in the News.....Dec 12
The Language of Beisbol in Everyday Talk.....Aug 11
The Management Survey of the
Philharmonic (Golden Oldie).....Aug 20
The Mission of the Signals Processing
Requirements Panel.....Oct 1
The New Collection Criteria.....Dec 11
The New Traffic Analysis Glossary.....Aug 8
The Old [redacted] Section: Parts 3 & 4.....Dec 5
The [redacted] Exercise: A Case Study in
Special Research Analysis.....Oct 16

Want Ad.....Dec 13
What is a Collector?.....Aug 2
What Should You Expect? or The Analysis
of Cryptanalysts.....Aug 5
Worldwide HFDF Modernization Plan:
Project Carriage.....Sep 9

EO 1.4.(c)

P1-Dec74-S3-23300

~~CONFIDENTIAL~~


5 7 2 6 8 9
3

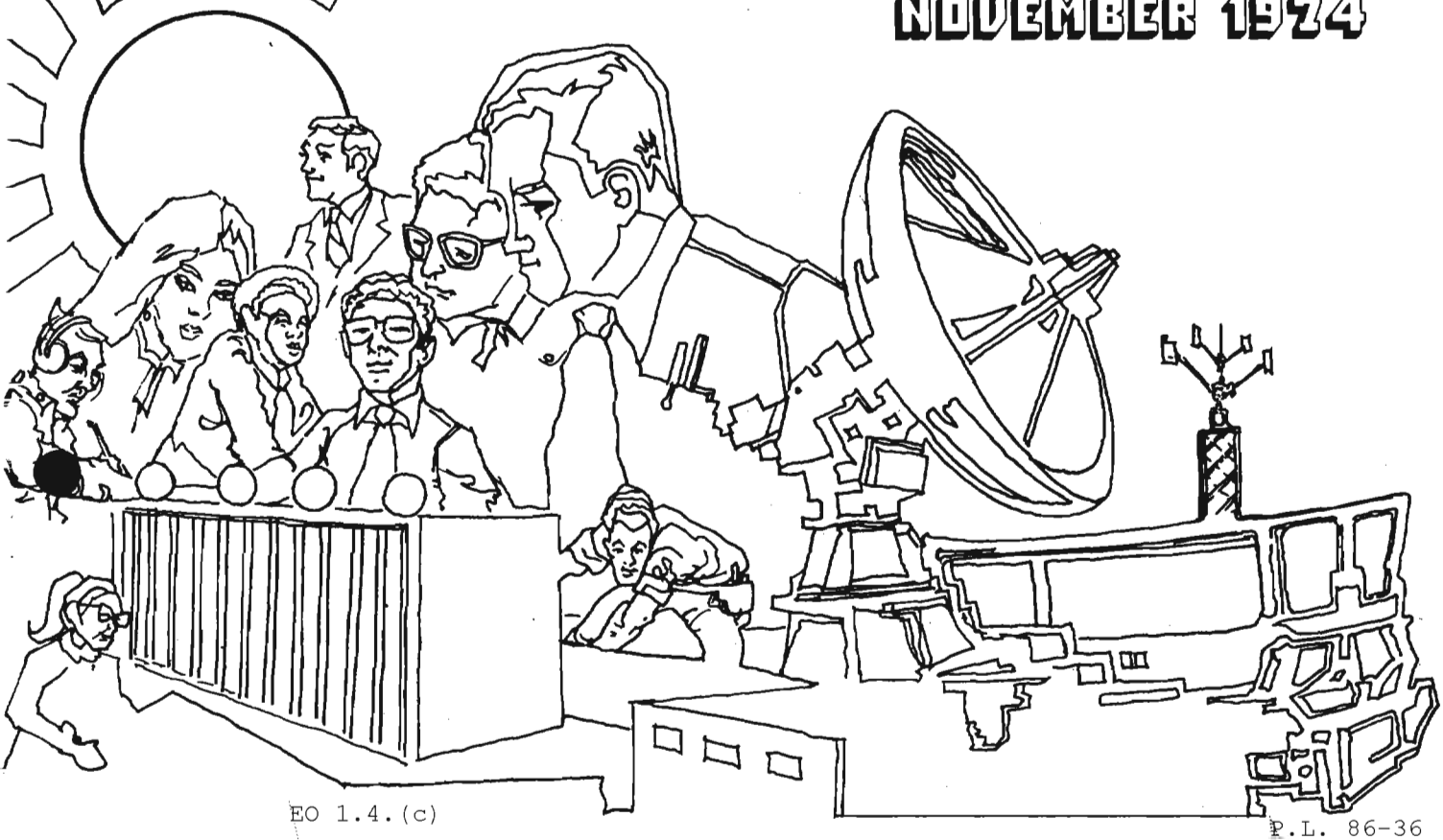
DOCID: 4009710

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

NOVEMBER 1974



EO 1.4.(c)

P.L. 86-36

DATA AND DEFINITIONS..... [redacted] ... 1
[redacted] WHY? WHERE? WHAT?..... [redacted] ... 5
NEW TRENDS IN THE TEACHING OF CRYPTANALYSIS..... [redacted] ... 7
REFLECTIONS ON A TRANSLATORS' CONFERENCE..... [redacted] ... 10
PURITY OF THE RUSSIAN LANGUAGE..... [redacted] ... 12
THE APOSTROPHE: SOME THOUGHT'S..... ... 14
A LONG HARD LOOK AT THE INTERN PROGRAM (PART THREE)...Anne Exinterne..... ... 15
GUIDESMANSHIP..... [redacted] ... 18
GOLDEN OLDIES: A MEDAL FOR HORATIUS..... ... 19
LETTER TO THE EDITOR..... ... 20
ANSWER TO LAST MONTH'S "OCTOBER OVERLAP"..... ... 21

~~Classified by DIRNSA (NSAM 123-2)~~
~~Exempt from GDS, EO 11652, Cat 2~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

DOCID: 4009710

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. I, NO. 4 NOVEMBER 1974

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief ..... Doris Miller (5642s)
Collection..... [redacted] (4410s)
Cryptanalysis..... [redacted] (3215s)
Language..... [redacted] (5236s)
Machine Support..... [redacted] (3321s)
Special Research..... Vera R. Filby (7119s)
Traffic Analysis..... William J. Jackson, Jr. (3369s)

Art Editor..... [redacted]

P.L. 86-36

* * * * *

~~TOP SECRET~~

DOCID: 4009710

DATA AND DEFINITIONS: CALLING THINGS BY THEIR RIGHTFUL NAMES

by [redacted] P13D

P.L. 86-36

IF NAMES ARE NOT CORRECT, LANGUAGE IS NOT IN ACCORDANCE WITH THE TRUTH OF THINGS.

IF LANGUAGE IS NOT IN ACCORDANCE WITH THE TRUTH OF THINGS, AFFAIRS CANNOT BE CARRIED ON TO SUCCESS.

(Analects of Confucius, Book 13, Chapter 3)

(As the scene opens, we see May at her desk with papers scattered all around her. She has two documents directly in front of her which she appears to be comparing, underlining entries with a pencil. Enter Jack, just as she throws down the pencil and groans.)

Jack: Hi, May! What's the matter, the boss giving you a hard time?

May: No, but unless I get this mess cleared up he may be doing that pretty soon! I've just got to get the question of this definition straightened out. He says I have to use the right one.

Jack: What definition? What are you doing?

May: It's a definition of "bearing" for this draft paper I'm writing on the new DF system. I've looked at the definitions in two general desk dictionaries, at the one here in USSID 412, Annex B, and at this one for the Data Element "Bearing" in USSID 414, Annex A. (Angrily) None of them are the same...see? The one from 414 is more detailed and has recording instructions and further explanation. But the one in 412 has a lot of cross-references to other terms. I don't know which one is more accurate or which I should use in this paper.

Jack: You got me! Can't the offices that issued those documents tell you which to use?

May: Would you believe it? The same office put out both of them! The NSA Data Standards office issued both USSIDs and they are both supposed to be standards: 412, Annex B, for target-location terms and 414 for standard data features. I just don't get it! Why have they got two? Which one is the right one?

(Curtain descends on a fuming May and a perplexed Jack.)

May and Jack aren't the only ones confused. Our widely scattered spies tell us that, unfortunately, many people are having the same problem. They see two programs, run by the same office, putting out information on SIGINT terminology and on data standards and they have a lot of questions about them.

Why do we need definitions both for data standards and for terms, and why are they almost always different?

Which is really right?

How are the definitions derived?

Once established, are they "set in concrete," with no chance for change?

This article attempts to answer these questions and to clear up some of the confusion.

When glossary definitions and data standard descriptions differ, we cannot answer the question "Which is right?" unless we know "Right for what purpose?"

Generally speaking, the standard glossary definitions are intended to show the currently accepted meanings for terms within specified contexts; their purpose is to provide for the writer, particularly of instructional or directive documents, a guide as to what he can expect his readers to understand if he uses a particular word in a particular context, and for the reader of such documents, a guide as to what the writer presumably meant. The glossary, in other words, interprets existing terminology.

The data standard definitions have a much narrower purpose: the identification of specific categories and sub-categories of data to be entered into manual or machine files. (These definitions in most cases could more accurately be called descriptions, since they describe and identify the data.)

DOCID: 4009710

Each for its intended purpose is the standard definition, and the right one.

How are the definitions derived?

[redacted]

Here is a typical glossary entry, which by no particular coincidence happens to be for the term bearing:

1. In DF, an indication of the direction from which a target's signal is received, expressed by the angle in degrees between a preestablished direction, usually true north, and the line from the observer to the target. Synonymous with line bearing, line of bearing, line of position, target bearing. Contrast with azimuth.

2. See accuracy study bearing, average bearing, check bearing, late bearing, mean bearing, reciprocal bearing, relative bearing, search bearing, snap bearing, true bearing, usable bearing, wild bearing.

As you can see, the definition (as given in para. 1) is for the concept of what a bearing is. It does not include the method of measuring a bearing, the maximum value it may have, or how it is recorded--these are not really germane to the definition. Under "Synonymous with..." it deprecates (discourages the use of) other terms considered less appropriate for formal use in official documents. Under "Contrast with..." it cites a term of related but contrasting meaning, which the glossary user may consult for further information. Paragraph 2 of the entry cites the more specialized terms for which bearing is the basic or generic term.

The Panel working on a glossary starts with existing terms, each of which has one or more meanings. For each term it must then determine several things: is the term in current use or is it obsolete? Does it relate to other terms? How will their definitions affect each other? Is it used in several disciplines, and if so do the meanings differ in these different contexts? Do they vary even in the same context? Are there any slang expressions or jargon equivalents to the term, whose use should be deprecated? Are all the possible meanings of the term now available to the Panel for review, and if not, where can they be found?

[redacted]

When you consider that at least these questions must be answered for every term that goes into a glossary, it becomes obvious why glossary making is slow work.

But the function of a glossary, at least, is generally well understood.

Now we turn to a data standard--a much less familiar idea. What is a data standard, in fact? One definition is: "A homogeneous set of authorized representations." This is probably more easily understood by watching the development of a typical case.

[redacted]

EO 1.4.(c)
P.L. 86-36

How will this be handled?

The NSA data standardization program is an extension of federal, DOD and intelligence community (IC) standards and uses these standards so far as practicable. (The criterion of applicability to our work makes it possible to eliminate rather quickly such interesting DOD standards as "Salary Scale for Physicians in Leprosariums" or "Bassinet Counts.") Those that are needed to satisfy unique cryptologic requirements are developed under the NSA program, but not by the Data Standards Center alone. Any user or originator of a file or data base can (and frequently does) suggest that a particular type of data needs to be standardized. In addition, a system of Senior Data Representatives, appointed as are the Senior Terminology Representatives, exists (among other reasons) to collect and funnel such suggestions and comments to the Center for consideration.

Once such a proposal is made, it is subjected to review and analysis by the Data Standards Center, the Senior Data Representatives (and their subordinate reps within their own organizations), and subject matter experts, as appropriate. Many questions have to be answered: Do the data under discussion really require standardization? Do they occur widely, say in several files or data bases? Will the files in which they appear ever need to be merged? Do the data belong to only one category of information, or can they be broken down into several categories? What kind of coding system, if any, would be best for this data: all numeric? all alphabetic? mixed? mnemonic codes? arbitrary groups of characters? Does an already existing DOD or federal program data standard answer the needs of NSA/CSS? In some cases it may take several days or even weeks to collect the necessary answers, just to decide whether or not a standard is needed for a particular kind of data.

As we have shown above, the order of approach in the development of a standard is diametrically opposite to that used in the preparation of glossaries. The first step toward creating a data standard is to identify a unique category of information (a Data Element) and then to describe it in terms sufficiently broad to cover all appropriate applications for its specific delimited sub-categories (which are called Data Items).

Now that we have had a glimpse of both standardization processes, let's return to the term that was bothering May.

You have seen the glossary definition of bearing; here is the one given for the data standard:

DATA ELEMENT

Name: Bearing

Definition: The horizontal angle measured clockwise in degrees and tenths of degrees, from 000.0 degrees through 359.9 degrees from a specific reference point (such as true or magnetic north) to a second point.

Code: BRNG

DATA ITEMS

Recording Directions:

1. Bearings are recorded as four digits, left to right, for degrees and tenths of degrees. The decimal point between the third and fourth digits is assumed. When

EO 1.4.(c)
P.L. 86-36

DOCID: 4009710

equipment limitations do not permit the recording to tenths of a degree, the fourth digit will be zero.

2. When half-degree interpretations are reported, the fourth digit will be a five.

3. If the value of the bearing is less than 100 degrees, then the first, and possibly the second and third, digit will be zero.

FURTHER EXPLANATION

1. The terms "bearing" and "azimuth" are used here interchangeably, although, in navigation, bearing customarily applies to terrestrial objects and azimuth applies to the direction of a point on the celestial sphere from a point on the earth.

2. In direction finding, a recorded bearing or azimuth is assumed to be with respect to true north unless otherwise indicated.

3. When a bearing or azimuth is reckoned from magnetic north, a comments field should indicate the bearing or azimuth as being magnetic. The date of its applicability should also be given.

As you can see, this is a definition or description of a category of data ("The horizontal angle...") which can be recorded in a file. It must include the method of measuring the bearing and its maximum size, to make certain that any data referred to as a bearing will have been measured in the same way and to the same limits. Separate "Recording Directions" are needed to ensure the uniformity of bearing entries as to number, type, and position of digits. The "Further Explanation" differentiates between the meanings of bearing and azimuth (shown by "Contrast with" entries in the glossary definition), notes that bearings are recorded with respect to true north unless otherwise especially indicated (information given in the glossary definition), and comments on noting bearings taken on magnetic north. Because of the uses to which the information will be put, the definitions in the glossary and the data standard are and of necessity must be different.

As explained at the beginning of the article, each for its intended purpose is the standard definition, and the right one. But even that last statement must be qualified, for language and types of data change, and what was the "right" definition for either in 1964 may not be correct in 1974. Under the system of continuous monitoring and review used by the NDSC in both the Data Standards and SIGINT Terminology programs, changes or additions to established data standards or glossaries can always be proposed, and, if valid, incorporated into the existing directives. No document in either series is considered to be absolutely finished or "set in concrete," with no possibility of change.

I hope that this brief discussion has been of help in understanding the differences in approach and results obtained in the two programs. The NSA Data Standards Center does not make arbitrary decisions on the meaning of terms or the classification of data; rather, as in the ancient Chinese teaching, it tries to help in determining the "correct names" for both concepts and data, as a first step in assuring that "affairs be carried on to success."

(UNCLASSIFIED)

ASSORTED EDITORIAL NOTES

Sorry about that Table of Contents mix-up; we trust that by now you have all received copies of the October Table of Contents and have duly taped it to the October issue. While you are at it you might like to correct the course number on page 14 ("News from the School") from CA-105 to CA-015, and the Maryland Area Code on page 6 (the little telephone puzzle) from 310 to 301!

The article on foreign--especially English--loan words in Russian (page 12 of this issue) may pose some problems to readers not familiar with the Agency system of transliteration. It would take too long to explain it all here, but the main thing to remember is that "j" represents the sound of "y": so that "plejboj" is to be pronounced "playboy" and not "pledgebodge."

This month's Golden Oldie ("A Medal for Horatius") appeared anonymously and mysteriously on our desk in the form of a battered "burn" copy, and we assumed it was of local origin. However, the Art Editor has a friend who thinks it originally appeared in Yank, and that the author may have been William Hazlett Upson. Now he tells us! Well, it's a good story, and we hope Mr. Upson will forgive us if he is indeed the author. If you do have any local items--any sparks from the Agency grindstone--tucked away in your files, let us see them.

The last installment of the article on the intern program will appear in the December issue. We have had a lot of comment--mostly pro but some con--on this series, and as soon as it is complete we would be happy to have your reactions (written, please) and will want to publish some of them. Address: CRYPTOLOG, P1.

EO 1.4.(c)
P.L. 86-36

~~TOP SECRET~~

P.L. 86-36

What? Where? Why?

by [redacted] R04

Where?

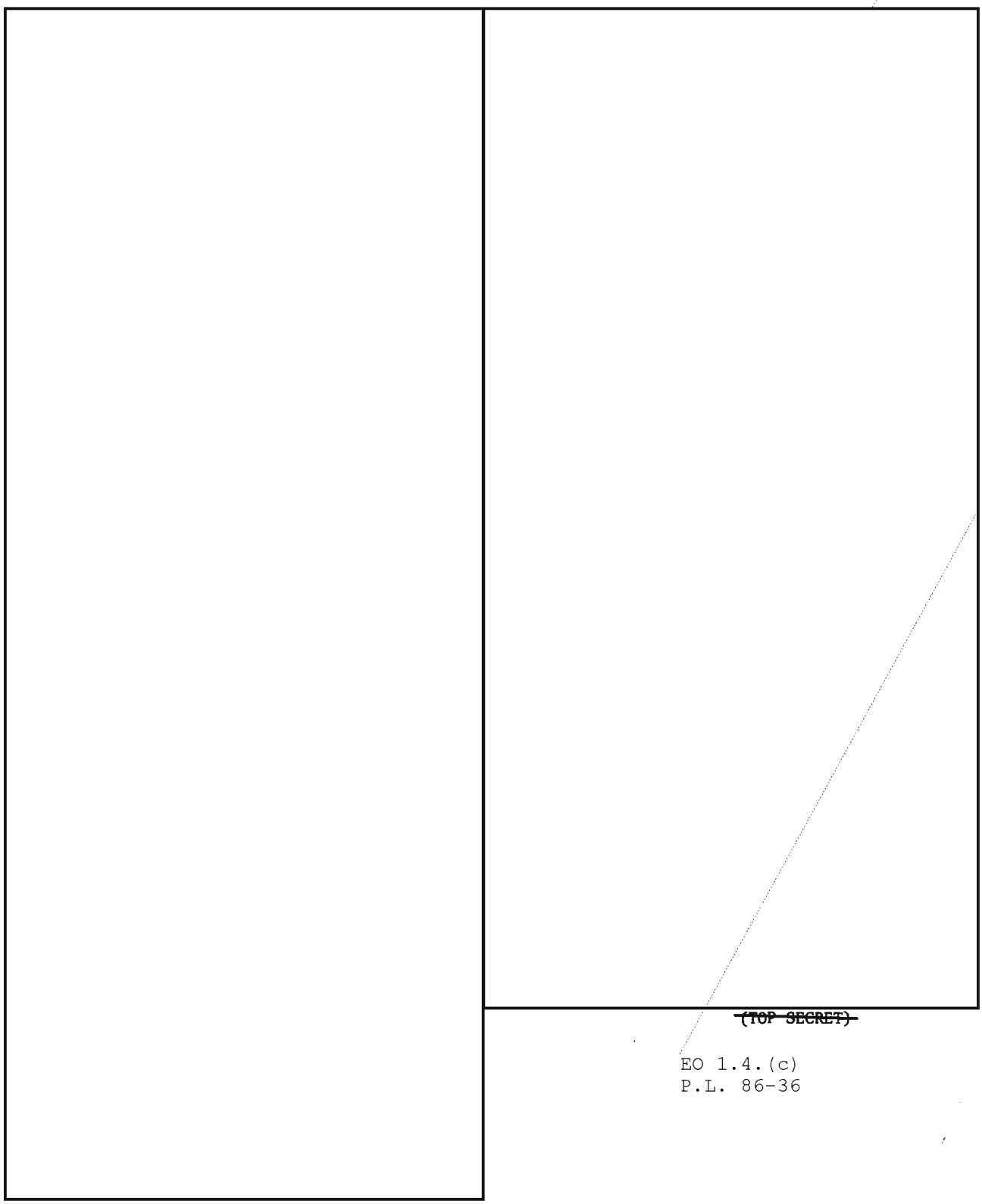
EO 1.4.(c)
EO 1.4.(d)

Why?

~~TOP SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36

~~TOP SECRET~~



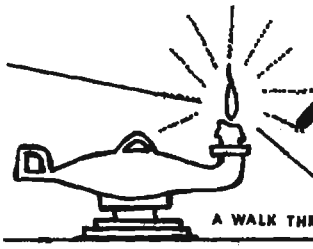
~~(TOP SECRET)~~

EO 1.4.(c)
P.L. 86-36

DOCID: 4009710

P.L. 86-36

~~TOP SECRET UMBRA~~



NEW TRENDS IN THE TEACHING OF CRYPTANALYSIS

A WALK THROUGH THE '75 CURRICULUM

BY [redacted] E13

A major project currently under way in the Cryptanalysis Department of the National Cryptologic School will change the way cryptanalysts of the future learn their trade. Three of the basic cryptanalysis courses will no longer be taught traditionally from the platform in a classroom. They are being redeveloped and written, over a 3-year period, as self-paced instruction courses to be presented in the NSA Learning Centers at Fort Meade (Room 2W165) and FANX II (Room A2A16B). The three courses affected are: CA-011, Survey of Manual Cryptosystems, CA-100, General Cryptanalysis, and CA-120, Survey of Machine Cryptosystems.

As each of the new, self-paced courses is completed, it will be made available in the NSA Learning Centers. Students will do their studying in the Centers, working when they feel like working, and proceeding at their own pace. Some parts of these courses make use of multi-media equipment--TV, slide projectors, and audiotapes. All courses will be available in written form, but often the student will be able to choose his own medium. The instructor's role will be to give individual assistance upon request.

The project to self-pace these courses is halfway into its second year. One course, CA-105, Introduction to Cryptography and Exploitation of Manual Cryptosystems, has already been completed and will be offered soon in the Fort Meade Learning Center. A second course, CA-107, Exploitation of Manual Cryptosystems, is being written now and is scheduled for July 1975 completion. The final two courses, CA-121 and CA-122 (Hagelin and Wired Wheels) will be written between July 1975 and July 1976.

Along with self-pacing the basic courses, the entire cryptanalysis curriculum has been reorganized to show exactly what type of student and job each course is designed to satisfy. There are three levels, distinguished by the first digit of the course designator:

The 000 level consists of Background Courses designed for students who do not do any cryptanalysis in their jobs.

The 100 level consists of Basic Courses designed for students who perform cryptanalysis as all or part of their jobs.

Courses at the 200 level or above are Advanced Courses designed for students whose job is cryptanalysis.

The newly-developed self-paced courses are in the 100 level Basic Courses.

Background

One of the oldest cryptanalysis courses listed in the current NCS Catalog is CA-011, Survey of Manual Cryptosystems. Until about 1966, this course was taken by everyone who wanted to learn about cryptanalysis--aspiring cryptanalysts, linguists, traffic analysts, reporters, and engineers--a most heterogeneous group. It was a 3-week full-time course covering cryptography and simple analysis of manual cryptosystems.

When CA-100, General Cryptanalysis, was written in 1966, all of CA-011 was incorporated into it and a considerable amount of new material (analysis and theory) was added.

[redacted]

In addition to the problems with course content, there were teaching problems as well. The annual heavy student loads for these popular, basic courses consumed a disproportionate amount of instructor time. Typically 71 per cent of the cryptanalysis instructors spent most or all of their time on these 3 courses. This left no time--or energy--to do research and to develop new courses, especially some urgently needed to train the analysts who need multiple disciplines to work on today's complex problems.

~~TOP SECRET UMBRA~~

EO 1.4.(c)
P.L. 86-36

Self-paced Courses

The decision to self-pace some of the basic CA courses was made in order to deal with such problems. It provides the opportunity to make many improvements: to modernize the contents of the courses and to arrange them in a sequence designed to build up knowledges and skills progressively. Self-paced courses insure that everyone gets the same basic information: a boon to teachers of advanced courses, who must often reteach what should have been learned in a prerequisite course, but was not. They also mean an end to the wildly heterogeneous classes which are so frustrating to students and teachers alike.

Important revisions in course content will also result.

These are just a few of the changes brought about by the self-pacing project.

Basic Courses

The courses being redeveloped as self-paced courses are among the basic ones--those taken by anyone who performs cryptanalysis as all or part of his job. The first three listed replace CA-011 and CA-100 and must be taken in sequence. They are prerequisites for all other basic and all advanced courses. Equivalency exams will be available eventually for all these courses. A student who passes an equivalency exam is given credit for the course with a grade of P (Pass). Equivalency exams may be taken only once.

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

As the three-year project for writing some self-paced cryptanalysis courses progresses (estimated completion by 1 July 1976), course development will begin to be concentrated on specialized and advanced courses. Two specialized courses at the basic level are already being planned and writing on one of them will begin soon: a course in cryptanalytic documentation including record keeping and report writing. Another course, to teach APL programming with simple CA applications, is also planned.

The Cryptanalysis Department of NCS (E13) welcomes questions about any of these courses or suggestions for new ones. Readers may call 8025 or visit the Department in Room A2A32B, FANX II.

~~(TOP SECRET UMBRA)~~

Note:
For a more detailed explanation of the self-paced method, see "Self-Paced Instruction: The Future is Now!" by Richard Atkinson, in the August '74 issue.

DOCID: 4009710

REFLECTIONS ON A TRANSLATORS' CONFERENCE

by [redacted]

P.L. 86-36

From 4 to 10 August 1974 I was privileged to attend a workshop and seminar of the American Translators Association (ATA), held on a wooded campus in the beautiful area of Monterey, California. It took little acclimatization for me to realize that I was in an environment away from government. Not that I was able to forget my governmental origins and loyalties. Quite the contrary! At almost every turn I was keenly aware that here was a group of like-minded persons, united in a common profession, yet guided and controlled, somewhat mysteriously, by almost totally disparate professional purposes. There were free-lance translators, translators of religious and liturgical literature (from the Mormon Church, the Church of God, and the Wycliffe Society), professors and teachers, and computer-oriented linguists (especially the Mormons).

We federal employees were a small minority --only two of us--and undoubtedly very much on the sidelines as far as the conference's ability to understand and help us was concerned. The more we all communicated with each other, the more I developed a strong sense of my own mission. For my part, I was highly motivated to receive something of value from the proceedings, something that would have meaning for the job back home. After all, this wasn't exactly a vacation for me; the Agency had given me a week of administrative leave and $120 tuition, for which I obviously owed something to somebody.

Of the various workshops that were offered, I enrolled in the one in German, the language in which I hold a Master's degree, but for which, by some strange anomaly, the Government has never seen fit to use me. The novelty and special value of this particular workshop, in contrast to the others (in Spanish and French), was its emphasis upon translation speed. Strange, but in my school days a generation ago there had been little thought in our classroom recitations of trying to beat the clock. And as far as assignments on my job are concerned, the only translation speed requirements ever placed upon me were in terms of the quantity of material desired (quotas) or of having a product reach the user before a specified deadline (timeliness). Any unusual success which may have been achieved in this respect was primarily the result of devotion to duty and to a far lesser degree to a capability to perform at some high speed level. No one would want to suggest that the primary emphasis in translation should be placed upon quantity and speed rather than quality; on the other hand, my attendance at the German workshop jolted me into the belief that perhaps much more could be done for the Agency's translators to improve their skill in speed translation. In this workshop I was witness to some phenomenal performances, and we were given some useful tips on how this skill could be developed and vastly improved with practice. It might be of interest in this connection that certain job advertisements I have seen recently for federal translators call for "an ability to perform fast, accurate written translations of scientific and technical material."

My primary aim in attending the conference had been to deepen my knowledge about the theory of translation--to acquire basic linguistic principles which would aid the translator in his task. This kind of orientation is essential, not only for practicing translators but even more especially for linguists who are called upon to guide, evaluate, and assist the translation process on the broader working levels. The conference did not disappoint me in this respect.

Professor Etilvia Arjona of the Spanish workshop, perhaps the main theoretician of the staff, distributed a handout entitled "Analysis of the Translation Text." The main thesis of this paper was: "The first task which a translator should undertake is that of carrying out a semantic and stylistic analysis of the source-language text in order to ascertain the message which the author presents. In order to do this, a complete reading of the text should be carried out." This was a valuable piece of advice, I thought. A translator will frequently plunge into the beginning of a text, without taking the time to make a preliminary survey of certain fundamental facts about the form and content of the text as a whole. Translation is not merely the finding of a word in one language with a meaning which is like that of a word of another language. It also involves recognizing the constructions, the idioms, the style of speech, etc., peculiar to the source language, in order that a smooth transition can be made into the kind of verbal expression which will have the same impact as the original. Professor Arjona elaborated on three levels of preliminary linguistic analysis: message and content, syntax, and lexicon.

DOCID: 4009710

About half of the time of the conference was allotted to a seminar consisting of speeches and group discussions on translation. Vernon Lynn Tyler, Associate Director of the Language Research Center of Brigham Young University, acquainted us with the computer-assisted translation activities of BYU. These relate especially to the goals of "intercultural communication," a new and developing field, and include research on making possible the translation of significant materials, both standard and "fugitive" (non-published or little known) not as yet accessible to the majority of potential users. Multilingual translation is, therefore, one of BYU's major concerns. One of Mr. Tyler's suggestions in connection with his computer work is: "Why not put a dictionary on a mini-calculator?" In theory, he said, there is no reason why it can't be done. Ideally such a dictionary should feature certain flexibilities: for example, the ability to serve different types of textual material by representing various vocabularies accessible through grids. According to Mr. Tyler the gadget, if developed, might even turn out to be a best seller.

Dr. Esther Matteson of Wycliffe Bible Translators addressed the conference on the pitfall of overtranslating terms through substituting the specific for the generic (e.g., "dime" for "coin") and undertranslating through substituting the generic for the specific ("coin" for "dime"). She treated the problem from the standpoint of Harold C. Conklin's notion of "an inclusive and exclusive hierarchy" of terminology (also called "folk taxonomy"), an orderly classification of the generic and specific levels. The whole subject has great significance, not only for translation, but also for lexicography in its handling of various folk taxonomies. In the case of folk botany, for example, Conklin in his article on "Lexicographical Treatment of Folk Taxonomies" maintains that "a local system of plant classification cannot be described accurately by attempting to obtain only vernacular 'equivalents' for botanically recognized species. Translation labels (glosses) are frequently necessary, but they should be considered neither as definitions nor as exact equivalents." He foresees the time when bilingual dictionaries will have far more sophisticated systems, perhaps through coding, for marking entries as to their status as lexical units.

Many of the speeches of the seminar focused on the subject of the professional status of the translator and fair remuneration for his services. According to ATA's code of ethical practices and professional rights, it is the duty of every translator "to seek or accept no work on terms that are humiliating to him or to the profession." Because many of the translators at the conference, especially the free-lancers and the professors, were obviously sensitive to this problem, a number of interesting facts about the rewards of being a translator came to light.

Many professional translators are unhappy about the fact that price, and not quality, frequently seems to be the criterion used to assess a scientific translation. Federal agencies often award large translation contracts to the lowest bidders (as low a rate as $13.24 per thousand words was cited) and not necessarily to the best qualified translators. Consequently, well-qualified professional translators tend to seek other types of employment, and only such persons as have no idea whatsoever either of science or translation offer themselves to do a job. This exercise of a false economy results in the production of poor-quality translations which are difficult and time-consuming for professional users to read and try to comprehend. Andrew Habberton, in his speech entitled "Translation for Industry," reported that a free-lance translator must translate between 2500 and 3000 words per day at $20 per thousand words in order to make even a modest living (about $15,000 per year).

In conclusion, one particular point deserves emphasis. Translators are increasingly taking notice of the progress made in linguistic science, and scientific linguists are increasingly applying themselves to translation as a worthwhile subject of investigation. Such a viable unity of theory and practice has not always existed but is essential for the advancement of the field of translation. The professional stimulation provided by a conference such as I attended is the kind of experience that every translator needs from time to time in order to contribute effectively to the vast amount of work which remains to be done.

(UNCLASSIFIED)

DOCID: 4009710

P.L. 86-36

Purity OF THE RUSSIAN LANGUAGE

SLAVOPHILES vs. WESTERNIZERS

by [redacted]

There is a war going on in the Soviet Union. It is a cold war which has been in progress for a couple of centuries. The war is the culmination of the tide of western terminological "varvarizm" which has been creeping into the Russian language since the time of Peter the Great whose "praktika" it was to borrow Dutch and German technological terminology. The war against the "infiltratsiya" of western "terminy" into the Russian language finds the defenders of the purity of the Russian language taking up sides against the westernizers, who advocate the adoption of certain western terminology. Much to the chagrin of the slavophiles, the westernizers are gaining substantially. It is highly unlikely, however, that the word count of western borrowings in Russian will exceed the number of words of purely Slavic origin, but the "situatsiya" is nevertheless alarming to many linguists. The "praktika" of "infiltratsiya" and "eskalatsiya" of western "terminy" in the Russian language has created an "absurdnaya situatsiya." It is the "realizatsiya" of this "problema" with which this "artikul" is concerned.

Эскалация

The roots of western "varvarizm" in the Russian language can be traced back to Peter the Great and Empress Catherine the Great. Czar Peter borrowed Dutch naval technology and other Dutch modernisms. During Catherine's reign, both French and German gained considerable usage among the upper circles of society. The 19th century saw an influx of borrowings which found usage in art, society, "literatura," and other areas of "kul'tura." It was at this time that Russian ballerinas were doing "piruety" during "lejtmotivy," much to the delight of the "diletanty." Borrowings from the west also penetrated military life in the 19th century. In the "divizii" and "brigady" of the "armiya" there were ranks such as "marshal," "general," and "lejtenant." The "kombatanty" of a "diviziya" would likely participate in a "rejd."

Пируэт

Today, an agent which is largely responsible for the proliferation of this practice is the Soviet press. The "korrespondent" of the "byuro" of many a "gazeta" and "zhurnal" is likely to be called to a "press-konferentsiya" or "brifing" given by the "sekretar'" of the State "Departament," Kissinger, relating to Soviet-American "detant" or to a "provokatsiya" or "konfrontatsiya" in the Middle East. It might be "protokol" for the "press-korrespondent" attending the "miting" to write up a "memorandum" so as to later put out a "pressreliz." Of course the coverage of the "press-konferentsiya" would probably be another example of American "propaganda" or "agitatsiya." The Soviet "mass-media" might also "informirovat'" the "publika" on the "vizit" of a foreign "delegat" or on the "provizii" of a new pact or "ekonomicheskij plan."

Секретарь

Nikolaj T. Fedorenko, editor of the magazine Inostrannaya literatura" (Foreign Literature), has allied himself with the Slavophile purists. Fedorenko not only fears that the "wholesale and indiscreet" borrowings from English and other foreign languages will allow "weeds of barbarism to grow in the rich soil of the Russian tongue," but that Soviet "intellektualy" might assume a pro-Western snobbishness. The purists lament that this practice implies a poverty in the Russian language. The problem must be given serious attention by the scientific "instituty" in the USSR, according to Fedorenko and his cohorts, in order to curb the uncontrolled borrowing of western terms. Fedorenko and other purists of the Russian language are distraught at the intrusion of latinized borrowings which appear in dictionaries such as Novye slova i znacheniya (New Words and Meanings) compiled by Butarova, Kotelova, et al. This particular work includes such fingernail screechers as "diskomfort," "kaza-nova," "pamflet," "bestseller," and many, many others.

DOCID: 4009710

The purists have yielded the right-of-way to scientific and technical terminology on the grounds that science has its own international language. A "kandidat" of "fizika" might develop a certain "apparat" in a "laboratoriya" and become a "dizajner" of an "atomnyj reaktor." A chemistry "ekspert" in the "laboratoriya" is likely to be found employing a certain "metod" or "fenomen" in which he might "transformirovat'" a "khimicheskij kompaund" into an "aspirin" or some type of "immunizatsiya." Space technology understandably hosts many western terms such as "orbita," "raketa," "indikator," "illyuminator," and many others. Around the house one might find an "elektricheskij mikser," a "ventilyator," "teflon" pans, "lampy," "orlon" clothing, and "televizory." A few examples of the many scientific and technical terms in Russian which are phonetically similar in English are: "traktor," "operator," "kibernetika," "matematika," "akkumulyator" (storage battery) "ajsberg," "korroziya," and "mikroskop."

Аппарат

In the world of "ekonomika," the Soviets have begun to strengthen their "import-eksport biznes." While buying on "kredit" they know that a "byudzhet" and a "balans" must be observed in order to avoid a financial "krizis."

The "eskalatsiya" of borrowing appears to run in periods during which the influx of western terminology is greater than at other times. Prior to the 1960's, borrowing of westernisms was relatively moderate. The increased technological advances of the sixties were, to a great extent, the major source of the more recent borrowings. The rapprochement between the United States and the Soviet Union in the late 1950's is also responsible for many of the borrowings of western influence, particularly in sports and the arts. From the numerous US-USSR athletic competitions of the last 15 years came words like "fotofinish," "dzyudo," "ping-pong," "olimpiets," "batterflyaist," "boks," "resling match," and "volejbol." Soviet sports fans enjoy going to the "stadion" to watch a "chempionat" of "futbol" (soccer). A goalie in soccer is called a "stopper" in Russian. Although there is no "bejsbol" or "sorfing" in the Soviet Union, "khokkej," "tennis" and "basketbol" are quite popular. At a "basketbol" game in a "sportivny kompleks" fans watch their favorite team "dribling" and "pressing." An interesting new sports term in the Russian language is "polufinalist" (semi-finalist) -- "polu" (the Russian prefix meaning "half") and the word "finalist" from English.

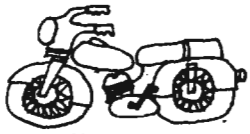
Дзюдо

Хоккей

The late Nikita Sergeevich Khrushchev also did his thing for the westernizers' cause. After Nikita made the Russians (and the world) aware of Disneyland in California, "Uolt Diznej" became a common name among Soviet children. Moreover Nikita's love for the American hot dog was so great that he decided to take the idea back to the Soviet Union. There is an apocryphal story that the Russians erroneously rendered the name of the new food as "goryachaya sobaka," which literally means "an excited bitch." As would be expected, the furtive glances, red-faced snickering, and outright laughing forced the venders to change the name to "khot dog."

Хот Дог

In a Soviet "restoran" (affectionately called a "Pectopah" by American tourists who read the Cyrillic PECTOPAH as Latin letters). one can dine on "sup" or "bul'yon," "salat," "kotleta," "bifshteks," and "makaroni." Before receiving the "chek," the diner might have dessert and a cup of "kofe" with "krem" and a "lump" of "tsukor."[1] Other popular foods are "jogurt," "koka-kola," "pepsi-kola," and "chipsy" (British-style french fries).



Мотоцикл

In going to a "kheppening" (something less "isteblishment"), Soviet youths might take a "mototsikl" or "sportivnyj avtomobil'," or if necessary, an "avtobus," "trollejbus," or "taksi." For fun on the "uikend," Soviet youths go to the "kinoteatr" to see a "vestern," or to a "shou" or "myuzikl." Another "kheppening" place for the Soviet young-at-heart is the "klub," "kafe," or "bar" where, from a "barmen" or a "barmensha," one can get a "koktejl," "dzhin end tonik," or "viski end uoter" and listen to a "bitgruppa" play "pop-muzyka," "dzhaz," or "rok-n-roll." The "kalipso," "val's," "cha-cha-cha," and "samba" are not popular among Soviet youths since the "tvist," "shejk" (shake), "bugi-vugi,"

DOCID: 4009710

and "khali-gali" (hully-gully) are the latest thing. The Soviet "plejboj" might wear "dzhinsy" pants, a "kovbojka" or "gollivudka" (Hollywood) shirt, a "zhaket," or a "blejzer." A "modnaya gerl" might wear a "mokher "sviter," a "pulover" or a "miniskyort," and splash on a dash or two of "odekolon." The "miniyubka"--"yubka" from Russian for "skirt"--is part of the "mini-moda." On a "tranzistor," one can hear the "bittlz"[2] or "monkiz" sing "Bejbi, bejbi, bejbi." "Modnye diski" can be purchased at a "rekord magazin."[3] American "khippi," "bitniki," and "khuligany" smoke "sigarety" and "marikhuana," go to see the "striptiz shou" or "seks-fil'm" and speak their own form of "sleng."

Миниюбка

Виттлз

Literary criticism also bears the marks of western linguistic influence, much to Mr. Fedorenko's displeasure. In reference to the phrase "metodologicheskaya konseptsiya esteticheskogo progressa" (the methodological conception of esthetic progress) Fedorenko cries out, "Do we require a Russian translation of this?" Distraught by such tongue-twisting horrors, Fedorenko pointed out that in the 1950's a special glossary of literary terms consisting of 450 words of foreign influence had to be compiled for high school students.[4]

As is alarmingly evident, the permutations in modern Russian slang and scientific and technical terminology are endless. The language is becoming drenched with western influences, and the future only appears to be bleak for Fedorenko and his followers. The Slavophiles, in their plight, suggest as an alternative, the promotion of work of the Russian Language Institute and increased influence of the magazine Russkaya rech' ("Russian Speech").

Who will win the struggle . . . . . ???

"Onli tajm uil tel."

FOOTNOTES

1 A Ukrainian word but used frequently in Russian.
2 The word "bittlz" assumes paradigmatic changes: Виттлзов, etc.
3 "Magazin" from French for "shop, store."
4 Smith, Hedrick; "Russian Deplores Linguistic 'Barbarism,'" The New York Times, 20 February 1974.

THE APOSTROPHE: SOME THOUGHT'S

The apostrophe -its no wonder its a problem. For one thing, theres three things that can cause the problem - actually, theres four really. One is the apostrophe itself. Another is plurals', and a third is possessive's. The fourth is esses (the plural of the letter s, that is, which we will spell "esses" to avoid apostrophe's).

Essentially, the problem is that the apostrophe is used for too many functions'. One is to show the plural of an abbreviation. For example, if you saw MSTS without an apostrophe you would think it meant Military Sea Transportation Service, but it might really mean Maryland State Trooper's. Another use is for possessive's, which will be discussed under esses, and still another is for contraction's, which may or may not involve esses.

Thus we can see that the difficulty with the apostrophe is it's ambiguity. The logical solution to this would be to have two marks of punctuation, one for possessive's and the other for uses' of the apostrophe. A better solution would be to do away with it altogether; after all, German doesnt use it for it's possessives. These suggestions, however, are impractical, since the GPO Style Manual has only recently been reissued, and it would be very expensive to republish it to incorporate this improvement in English punctuation, and in any case style manuals and grammarians are excessively conservative.

Now, as for esses. Basically, there are altogether too many of them in the English language. According to L.D. Callimaho's frequency count data, there are more esses than anything else except es, ts, as, ns, and is. And a high proportion of the time esses come at the end of a word, where a high proportion of apostrophe's are also to be found, which adds to the confusion. The reason for this is that they are the sign for the plural, for the possessive (as noted above), and for the third person singular (which is another problem with which this article will not deal with).

Since every analyst/reporter has to manipulate apostrophes', it is appropriate for CRYPTOLOG, which is intended for analyst's edification, to offer guidance on this matter in the interest of better style in our product. The editor's sincerely hope that this discussion has been helpful.

(Proofreader, please be extra careful about correct punctuation in this article.)

DOCID: 4009710

A LONG HARD LOOK AT THE Intern Program

by 'Anne Exinterne'

PART THREE: MOTIVATION AND MORALE

I recently saw a company ad headed: "Professionalism: More than an Education, More than Experience, More than Training, It's a State of Mind." The intern program has concentrated on education, experience, and training, but has not really attempted to develop a professional "state of mind" in the interns. This is not an objective that can be easily achieved, but the factors needed to produce it would probably be the same factors needed to produce a highly motivated work force with good morale anywhere, namely: interest in the field, a sense that your contribution is a necessary one, some recognition by others, and a reasonable expectation of personal advancement.

As I mentioned under Recruitment, since prospective employees can be told little about the Agency's work, the burden is on the Agency to do more to identify potential employees who not only have an aptitude for the type of analytical work done here but are likely to have an interest in that work.

No selection system is going to be totally accurate, however, so it is also important for the Agency and the new employees to view the first several years on the job as a trial period, during which both Agency and employee can judge if they will make a good team.

In the recent past the Agency's attitude, particularly where college hires were concerned, was to treat this not as a trial period but as a time during which recruits should be wooed and won and persuaded to pledge their fealty. This wooing, in the case of the early interns, took the form of two promotions in three years, the possibility of an overseas tour, and a wide variety of courses paid for by the Agency. While such benefits as these may lower the attrition rate, I think the goal is achieved in an unhealthy way.

The "front loading" of benefits is likely to keep people here not because they are sincerely interested in an Agency career but simply because they cannot afford to resign. To use two hypothetical interns as examples: Pete Pine and Mike Miller are both 28, have worked at the Agency for 7 years, and have now decided that this is not the career they were meant for. However, Pete and Susie, his unliberated college sweetheart who was a philosophy major and is now a housewife, have two children, healthy car and mortgage payments, and have grown to love their Bankamericard. Their life style is based on Pete's GG-11 salary, so Pete has reluctantly accepted the fact that he will be at the Agency for the next 23 years. Mike and Eleanor, on the other hand, in spite of similar family and financial obligations, agreed that they could cope with a salary cut, so Mike began looking for another job. He quickly discovered that seven virtually blank years on a resume form, at a very respectable salary, do not do much to arouse the interest of prospective employers. He also discovered that people are a little reluctant to hire someone who would be taking a salary cut to work for them, especially if, even with that cut, he would still be making more than they usually pay a new employee. As a result, Pete and Mike's car pool will probably stay intact for the next 23 years, and they will perform their duties in an acceptable if not an exceptional manner.

There is a tendency to think that if an employee who has talked about resigning can be persuaded to stay the employer has scored a victory. In reality he may have suffered a defeat, because he has simply managed to retain a body but not a mind.

Assuming, however, that the employee is interested, he still needs to feel that his contribution is a necessary one. Unfortunately it has seemed to me and many of my intern contemporaries that relatively few Agency employees have this feeling of making a needed contribution. It should be recognized that interns do not limit their observations to analytical techniques, and that as they tour the Agency they are exposed to more of the bad--as well as the good--than the average Agency employee. For example, if a new hire comes in and spends three years in an office where several people are blatantly unemployed, he may think his office is exceptional. But if he becomes an intern and observes that most of the offices he tours have such employees, he begins to realize that

DOCID: 4009710

a certain percentage of the work force is being carried on the efforts of co-workers, and is suffering no ill effects from it. (Some of these people simply coexist with the group; in some cases they work on studies which no one ever expects them to complete; in other cases even their co-workers do not know what they do.)

He also notices that people in higher grades--GG-13 and above--seem to be engaged in a continuous game of Musical Chairs, and those left standing when the music stops will probably be assigned to a staff position with vaguely defined duties, or given responsibility for a low priority problem, or made deputy to someone who operates very effectively without a deputy. To see capable people shuffled in and out of positions of responsibility seemingly just because there are more people than jobs has a very damaging effect on young employees. The lesson it teaches is that even if you do attain a grade level that suggests a position of considerable responsibility, you may have to be satisfied to alternate such assignments with periods of standing on the sidelines. The under-utilization of employees at this grade level cannot help damaging morale, decreasing effectiveness, and encouraging a patronage system.

What I am saying, in short, is that interns are often placed in an atmosphere of boredom and defeatism. Even worse, their own OJT assignments may foster the same attitude in them.

It is rare for a supervisor to decline an offer of an intern; he will usually accept one even if he has little work for him. Eventually, experience teaches the intern that mentioning a shortage of work is likely to result in a special project--seemingly devised simply to keep him out of mischief--or in a clerical assignment. As a result, while highly motivated interns may look for their own special projects, which can result in a product of value for both the intern and the area to which he is assigned, the less highly motivated are likely to redirect their energy and imagination into other channels. One intern deliberately prolonged an assignment where she was only employed for a few hours a day and began taking the additional courses she needed for admission to medical school, using most of the work day for studying. With a little help from NSA, she is now a doctor. Some become "professional students" here at the Agency. One intern graduate accepted what was essentially a full-time logging job because she was moonlighting and wanted to conserve her energy for her second job. A current intern spends a portion of his working day running down leads for new clients for his many enterprises, delivering orders and displaying wares. (I am amazed, by the way, at the number of Agency employees who hold second jobs, and am convinced that some stay here simply because of the contacts the Agency supplies for their products and services.)

There is a variety of things the Agency can do to instill in each employee a feeling that he is being relied on to make a meaningful contribution, and thus replace the atmosphere of defeatism with one of enthusiasm.

The first step is for managers to recognize that the Agency as a whole is not understaffed but overstaffed. Didn't the recent utilization surveys give some hint of this? I suspect that NSA is not too different from other government agencies and large corporations in this respect, but I do think that the existence of the condition and its negative effect on morale should be recognized.

Another step is to make sure that new workers know how what they are doing fits in with the Agency's mission, and to make them feel that they are being relied on. During the two years I was on one job I used only 8 hours of sick leave, partly because of a sense of urgency that pervaded that area and partly because I realized that no one would do my work if I wasn't there. Then I was assigned to an area whose operation, as it was being directed, seemed divorced from the rest of the Agency. The managers did not seem interested in what they could be doing to produce a better product but merely in bookkeeping procedures to account for the number of papers processed one month as compared with another month. My use of sick leave increased. It was not that I was consciously abusing the sick leave system, but I did probably subconsciously welcome a reason to stay home, so if I woke up with even the hint of an ailment, I'd think, "Well, if I stay home today I can nip this in the bud..."

(It might be beneficial for M to study organizations that have high totals of sick leave usage. Managers should also be alert to the records of individual employees--not only to possible sick leave abuses but also to changes in the pattern of use, which may indicate that a person is becoming disenchanted by, or, conversely, suddenly interested in, his assignment.)

The third and fourth factors are, or should be, related: recognition by others, and an expectation of personal advancement.

The need for recognition and approval is a basic one. Agency managers have several means of giving such recognition to employees: performance appraisals, in-grade raises, and promotions. Ideally, these management tools are used to discriminate between the varying levels of performance found in Agency employees.

Performance appraisals: I will not digress into a long discussion of the current system because a new system, apparently designed to curtail the inflation the old system suffered from, will be introduced in 1975. The only comment I will make concerning the new system

DOCID: 4009710

is that supervisors should be given considerable guidance on the philosophy behind the system, the need for realistic and candid appraisals, and the need to keep the employee informed as he goes, so that a candid appraisal does not come as a sudden shock.

In-grade raises: Whatever the philosophy behind the in-grade system may be, in practice virtually everyone receives an in-grade on the day he is legally eligible for it, regardless of his performance. In fact, once past Step 3, receiving an in-grade has a negative connotation for most employees: while it means more money, it also means that still another year (or more, depending on the step) has gone by without a promotion.

A remedy for the lack of significance now attached to in-grades might be to establish a scale for them. If an employee were rated "outstanding," he would receive an in-grade in 8 to 12 months, if "strong," in 13--19 months, "proficient," 20--26 months, "adequate," 27--36 months, and "deficient," no in-grade. This would be especially helpful in time of scarce promotions. It would also provide an incentive for ill-fitted employees to resign, and generally help to separate the wheat from the chaff.

In this way in-grades would be treated much like raises in private industry. I have discussed this with a friend who received almost identical salary offers from NSA and a large company five years ago. He chose private industry, and in those 5 years has received raises, bonuses, and promotions. Because he is a programmer with a math background, he probably would have advanced just as rapidly at NSA, but there is a big difference between his morale and that of many Agency employees. He knows that every increase in his salary represents a vote of confidence from his employers, and that his salary is considerably higher than that of the people who began work with him but whose work is not as highly regarded; whereas an Agency employee who is a Grade 9, Step 5 or an 11, Step 4 knows that everyone who was promoted on the same day that he was has received the same increases --cost-of-living and in-grade--whether his work was considered outstanding or barely adequate.

Promotion: When promotion is the only means of discriminating among levels of performance it can become an obsession, and when promotions are scarce, morale is likely to plunge.

What adds to the problem is the fluctuation in standards that accompanies the fluctuation in funds. When I was a new hire, it seemed that no one of any merit ever reached a Step 4 below the grade of 12; a Step 5 obviously had serious problems. Then suddenly a drought hits and the reverse is true: being able to leap tall buildings in a single bound doesn't even count. Standards should be consistent. When money is tight you may have more people who meet the standards than you can promote, but when money is free, standards shouldn't be lowered just so money will not be lost. If they are lowered, and mediocre employees promoted, then in austere times these people will have a very damaging effect on the morale of their co-workers, and are likely to pose problems for their superiors.

One measure that would ease the promotion situation somewhat and would help in other ways as well would be to use Grades 6, 8 and 10 for the analytical career field. I am told they are not so used because they are associated with clerical positions. While there may be a tradition for such an association, I think management could correct that, and the benefits of using those grades would be considerable: it would serve as a means to further differentiate the abilities of employees (some people's performance would warrant promotion no higher than GG-9, some no higher than 10, etc.); it would help to lower the average grade; it would increase the number of promotions possible in the 5-to-11 grade bracket with the same amount of money; it would make it easier for clerical employees with an aptitude for analytical work to cross over into one of those fields; and conversely, it would encourage people with an interest in clerical work to stay in that field and not be tempted to switch to an analytical field simply by the prospect of skipping grades through promotion.

A question of great interest to intern graduates (among others) is: While there are Agency guidelines for promotions, are there any Agency standards for the manner in which those guidelines are interpreted into office promotion systems? Some offices have a point system for promotions, while others seem to prefer a "supervisor, defend-your-man-against-my-man" system. Some areas appear to value cryptologic experience over education while the reverse is true in others. Some emphasize certification status for all employees in Grades 7 and above while others appear to look for loopholes which will permit promotion of uncertified people. Some require a minimum time in that organization while others seem to bring people in with the intention of promoting them. (In two cases that really hurt morale, employees were promoted because their supervisors were unhappy with their performance! The supervisors had concluded that the employees would not request a release until they had been promoted, and apparently felt that the promotions were a small price to pay for getting rid of them.)

It would be helpful for employees to have an idea of what is emphasized when candidates are reviewed for promotion, and I feel certain there would be less grumbling and fewer hard feelings if such standards were publicized.

(Next issue: What Happens to the Graduates?)

DOCID: 4009710

P.L. 86-36

GUIDESMANSHIP

by [redacted]

or How to Write Technical Manuals Without Actually Giving Anything Away

Originally published in C-LINERS as "The Care and Feeding of Technical Manuals"

The effective technical manual presents an accurate history of the development of an equipment and procedure to be passed on to others. In the compilation of such a document the writer must consider the employees who have spent long laborious hours in developing the data. He must use care that it is not too easily understood and absorbed by persons outside this circle. It must be developed so that only those few who have worked on the project from its inception are able to comprehend its full significance and receive its benefits.

Imagine the embarrassment of one of the indoctrinated if a novice could read a manual and understand its full significance in a minimum of time: the novice would then be in a position to lord it over an old-timer who had spent years in acquiring the same information! Or the irreparable harm done to the reputation of an experienced technician if a young upstart were to get his eager hands on a well-written document; he might learn the equipment well enough to completely humiliate the man with experience! One or two such manuals left lying around unguarded might even fall into the wrong hands and be used as a refresher to someone who has been "out of touch" for some time.

There are several ways to prevent this from happening. The first and most effective is to publish as late as possible. A manual which is received well after delivery of the principal equipment, for instance, will probably be useless to the unintended reader. For by that time he will have learned by experience, the hard way.

But suppose a late manual, because of long-term use of the equipment, should fall into the hands of an undeserving young upstart anyway; the writer should have prepared for this emergency. The second, and most difficult, way of safeguarding the data is in the method of writing, and the truly effective manual, therefore, is written abstrusely so that only the "few" can understand. It was Linton who said, "It takes considerable practice to use language in grammatically complete units and yet say nothing at all. Unless we are very careful, some idea, even if a very faint one, will creep in." Linton was right, of course, but the good technical writer is prepared "even if a very faint one" does creep in.

The choice of words is important. The careful writer never uses words like "use" and "workable"; he will say "utilize" and "feasible." He will also inject mean-nothing words like "essentially" and "basically." Even if the unintended reader begins to see light through these gimmicks, the writer has a few more tricks up his sleeve.

He knows, for instance, that verbs are dangerous--that an active verb carelessly placed in front of its direct object lays bare the true meaning of the sentence. The writer who says, "The power transistor heats the assembly" has committed a cardinal breach of shrewd practice; if only he had thought to say, "The assembly is heated by the power transistor." The unintended reader would never be quite certain if the assembly was lying by the transistor when heated or if the transistor supplied heat to the assembly.

A careless technical writer once requested a user's review before publication. This was intolerable, as several suggestions from the future user almost destroyed the occult nature of the writing.

If all normal precautions fail, there is still hope. The careful writer "goes the last mile" in the organization of his document. By placing perfectly accurate data next to unrelated data, he throws the unintended reader into confusion. Even more confusing are the many nonstandard abbreviations he uses; he really chuckles as he includes CCG, CGS, and G.M.& C. Surely the unintended reader will be slowed down in looking these up (and by the way, the writer should be careful not to include a glossary of abbreviations used). Some writers actually identify their choicest nonstandard abbreviation on page 2 and then use it again on page 208, knowing the reader will not remember either its meaning or where he first saw it; if this doesn't cause him to throw up both his hands and the data in utter despair, nothing will.

Now concerning storage, the important data or manual is safest when stored with miscellaneous papers in the bottom left-hand drawer of the writer's desk; it is even safer if no one knows of its existence. The experienced author knows that one slip of his pencil could send the document flying into the technical library where it would receive an accession number and be readily available to literally hundreds of undeserving readers.

It frightens one to think of the countless ways an unintended reader could get his grubby little hands on the most coveted data. The best writers, therefore, will close all loopholes. These writer alone will survive; they and their publications will go down in the pages of history, famous for obscurity.

(UNCLASSIFIED)

DOCID: 4009710

ANSWER TO LAST MONTH'S OCTOBER OVERLAP

KEY: THREE SHIPS TO A NEW WORLD

MESSAGE TEXTS:

EVERY SHIP THAT COMES TO AMERICA GOT ITS CHART FROM COLUMBUS.

FROST AND FRAUD HAVE DIRTY ENDS.

COLUMBUS DISCOVERED NO ISLE OR KEY SO LONELY AS HIMSELF.

SOMEBODY SHOWED HIM THE SUNSET AND HE SET SAIL FOR IT
AND DISCOVERED AMERICA AND THEY PUT HIM IN JAIL FOR IT
AND THE FETTERS GAVE HIM WELTS
AND THEY NAMED AMERICA AFTER SOMEBODY ELSE.

HE THAT HATH A GOOD HARVEST MAY BE CONTENT WITH SOME THISTLES.

WITCHES STEAL YOUNG CHILDREN OUT OF THEIR CRADLES, MINISTERIO DAEMONUM, AND PUT DEFORMED IN THEIR ROOMS WHICH WE CALL CHANGELINGS.

Pilgrim: Too bad they don't have Thanksgiving back in England.

Indian: They will some day. But they'll celebrate it on the 4th of July.

Herewith we renew our offer of direct mailing to individual subscribers. You don't even need the coupon, really. Just write your name and organization on a slip of paper and put it in a shotgun envelop addressed to CRYPTOLOG, P1.

Some of you have inquired how the original distribution was decided. Simple: In addition to one or more copies for each organizational unit of OPS (depending on the size of the unit) we sent one copy, by name, to every person in OPS who was a member of one of the learned organizations. Now we are opening up subscription to all persons in the Agency who are cleared for Top Secret Codeword.

Note: A number of people have asked for copies of the first issue, but we had no extras of that issue. If your office has extras, please send them to us and we will honor the requests so far as possible. We do have some extras of the second and third issues, if you want to fill in holes in your file.

EDITOR, CRYPTOLOG:

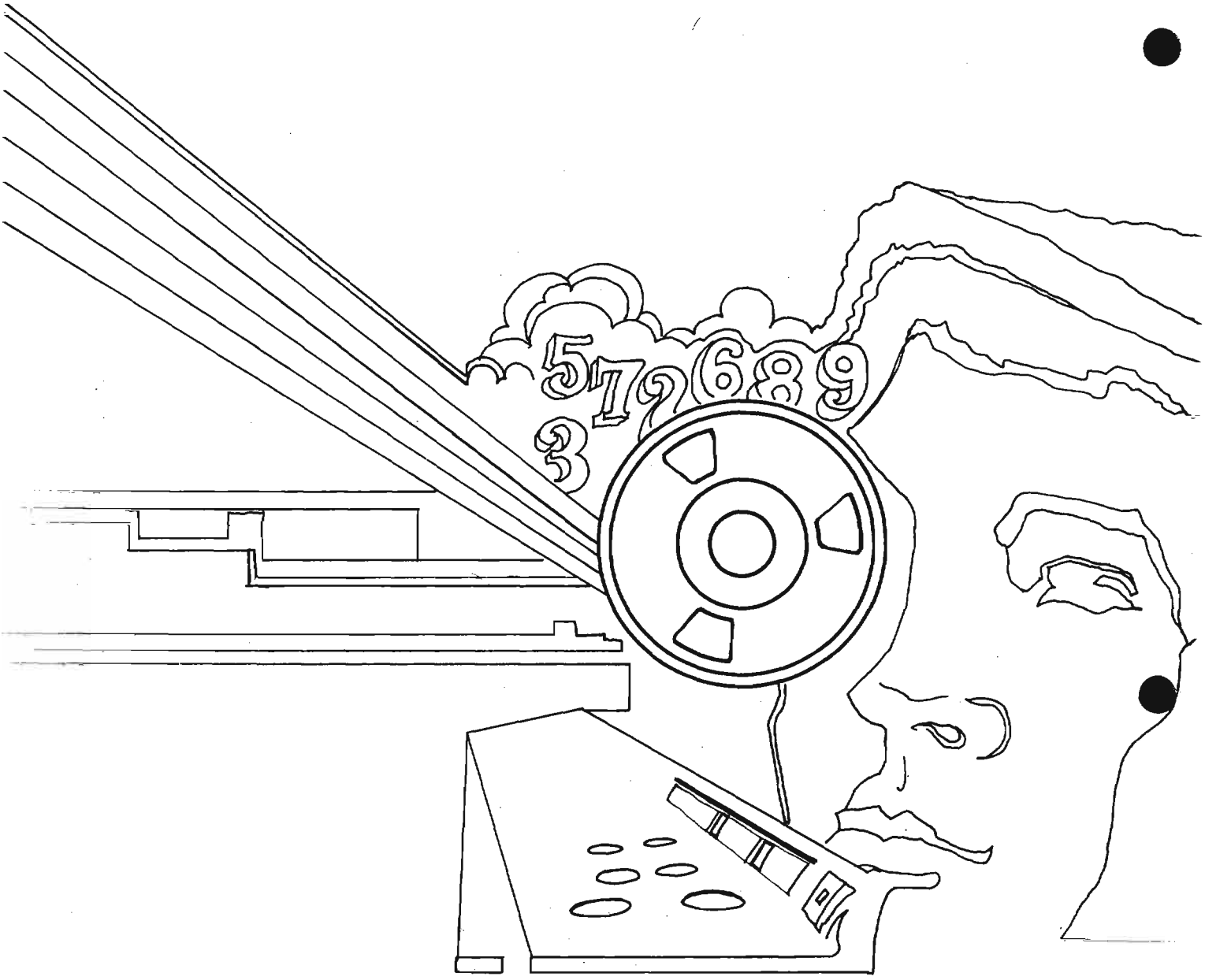
Please enter me as an individual subscriber..... ☐

Please remove my name from the list of subscribers..... ☐

Please note change of address..... ☐

NAME _____ ORGANIZATION _____

P1-Nov 74-S3-23242


5726893

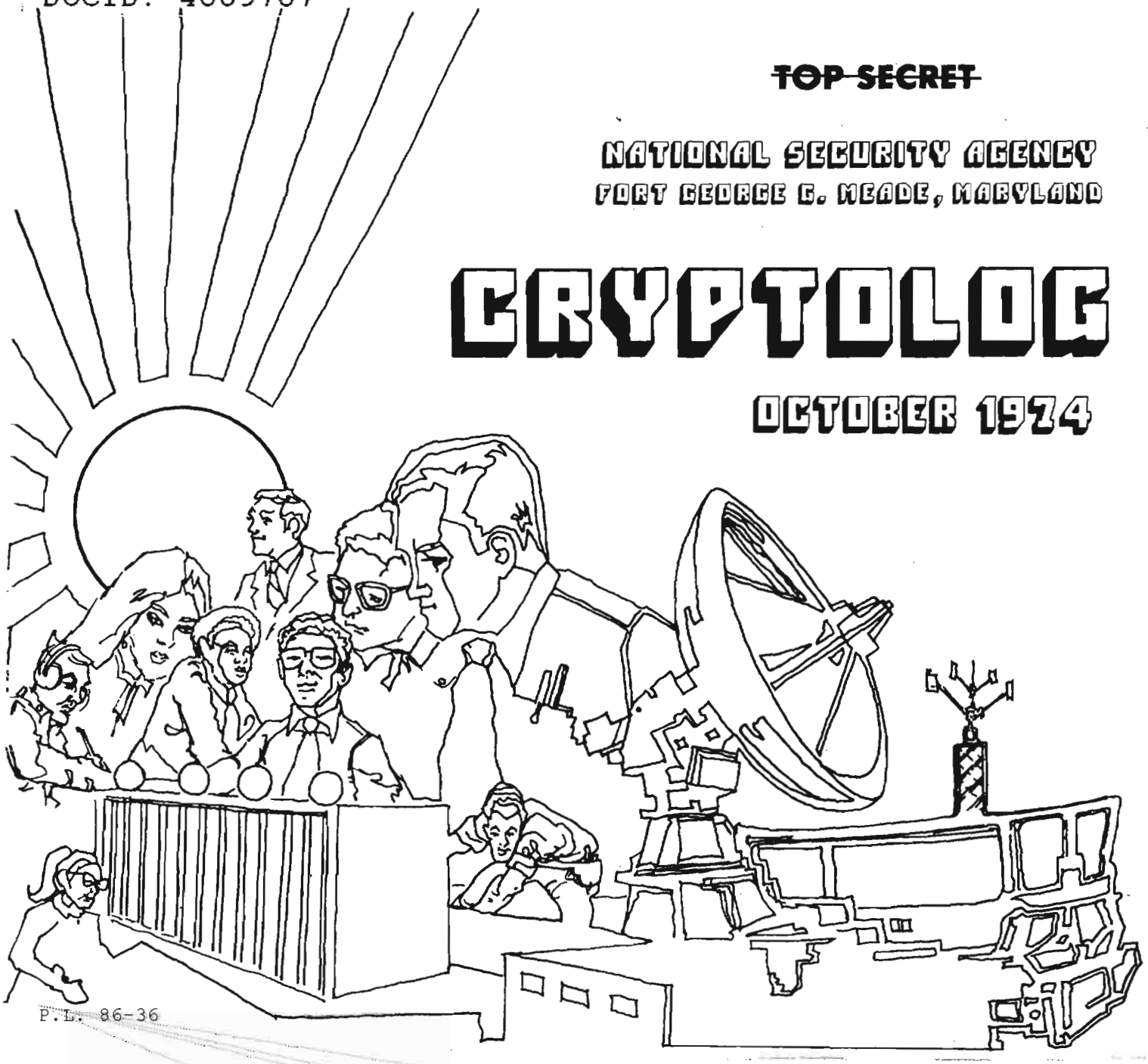
DOCID: 4009707

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

OCTOBER 1974



P.L. 86-36

THE MISSION OF THE SIGNALS PROCESSING REQUIREMENTS PANEL.. [redacted] . 1
EVEN A FIVE-YEAR-OLD CHILD..... Emery W. Tetrault.. 4
CHARACTER-BUILDING IN THE PEOPLE'S REPUBLIC OF CHINA..... [redacted] . 7
GOLDEN OLDIES: AN UNOFFICIAL GLOSSARY OF WEASEL WORDS.....10
A LONG HARD LOOK AT THE INTERN PROGRAM (PART TWO).....Anne Exinterne.....11
NEWS FROM THE SCHOOL.....14
COMING EVENTS.....15
THE [redacted] EXERCISE:.....Vera R. Filby.....16
AN OCTOBER OVERLAP..... [redacted] .20

EO 1.4.(c)

~~Classified by DIRNSA (NSAM 123-2)~~
~~Exempt from GDS, EO 11652, Cat 2~~
~~Declas Date Cannot Be Determined~~

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

DOCID: 4009707

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. 1, NO. 3 OCTOBER 1974

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief ..... Doris Miller (5642s)
Collection..... [redacted] (4410s)
Cryptanalysis..... [redacted] (3215s)
Language..... [redacted] (5236s)
Machine Support..... [redacted] (3321s)
Special Research..... Vera R. Filby (7119s)
Traffic Analysis..... William J. Jackson, Jr. (3369s)

Art Editor..... [redacted]

P.L. 86-36

* * * * *

~~TOP SECRET~~

DOCID: 4009707

~~SECRET~~

The Mission of the SIGNALS PROCESSING REQUIREMENTS PANEL C6

P.L. 86-36

P.L. 86-36
EO 1.4.(c)

Signals processing and conversion is the step immediately following collection, in which

In a follow-on process certain tasks require additional staging; this is accomplished by intermediate processors

At this second point, the work of SPRP (the Signals Processing Requirements Panel), CPRP (the Computer Processing Review Panel), MARG (the Machine Allocations Review Group), and similar groups, overlap in their endeavors to expedite the overall processing-exploitation cycle. It is here that over-enthusiastic analytic commitments and expectations have their most drastic impact.

The primary mission of the SPRP is to order the processing and signals-conversion of the Agency's worldwide magnetic-tape collection effort in such a way as to expedite the processing of perishable intelligence and to balance the flow of materials processed in accordance with their relative importance.

The Panel is charged under its charter with the review of all existing and anticipated signals-processing and conversion requirements which will or could impact on C6. It is to advise DDO as the the validity, justification, and processability of tasks (both existing and projected). It provides a forum for review regarding the selection and processing of magnetic tapes as prioritized internally by the analytic shops. This usually eventuates in Panel approval of the DDO Quarterly SPRP listing. In the event of irreconcilable differences, problem areas are referred by the Chairman to DDO for resolution.

Past

The Signals Processing Requirements Panel (SPRP) was established by the Assistant Director, Production, in 1968 to allow for review and expediting of signals processing of magnetic tapes received in PROD. This review at PROD level permitted decisions regarding possible corrective actions, and allowed broader influence to be brought to bear on the ordering of tasks impacting on C6, the Office of Signals Processing and Field Support.

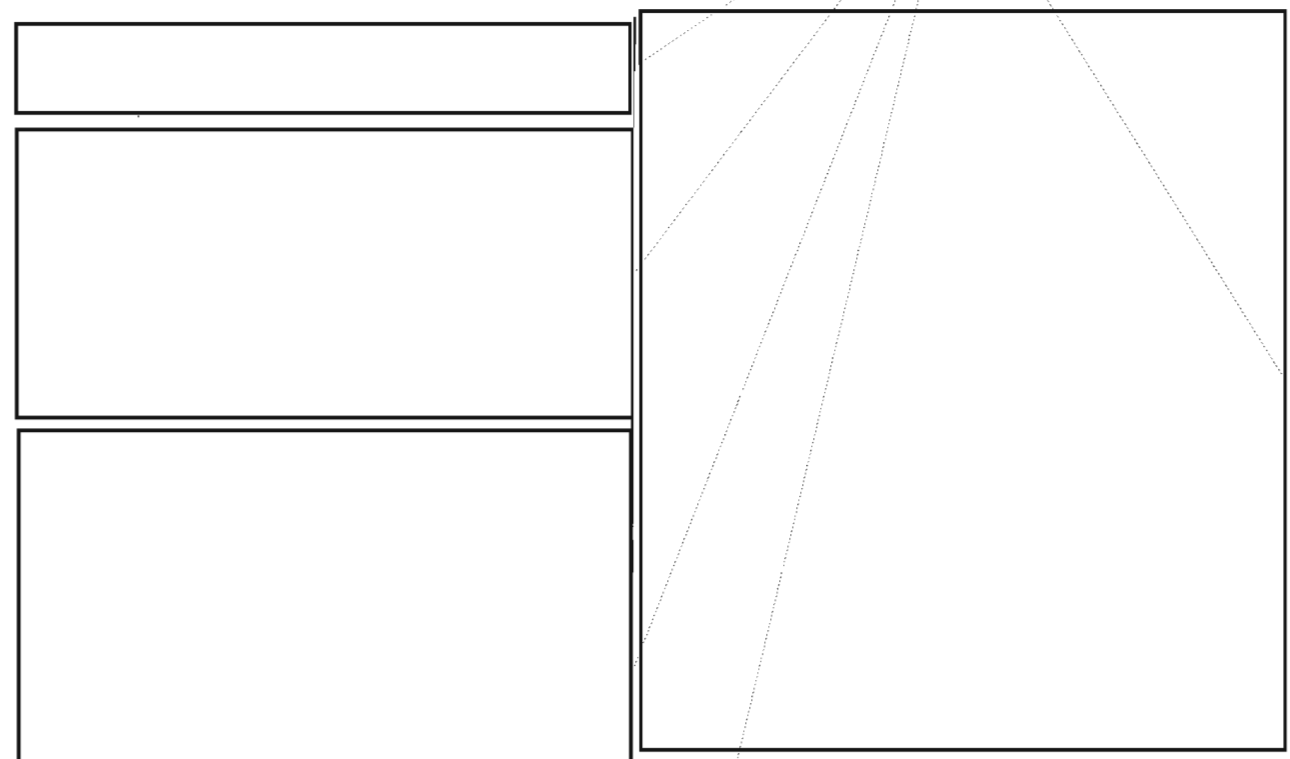
For some years the requirements levied on C6 had exceeded available processing capacity and manning resources.

~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36

DOCID: 4009707

EO 1.4.(c)
P.L. 86-36



Present

The Signals Processing Requirements Panel, currently chaired by the Executive for Deputy Director, Operations (XDDO), has a basic membership of 15, representing each of the analytic groups, plus C, L31, and selected P and V Staff personnel. R&D is not presently represented, though its participation would be beneficial. The Panel Charter was updated and reestablished by DDO action on 29 August 1973. This restatement of DDO interest was promptly followed by issuance of "Operations Policy Letter #3, Coordination of All New Collection Tasks," dated 25 October 1973.

The prioritizing of signals processing tasks is arrived at after thorough Panel review of anticipated volumes, collectibility and potential intelligence value. The listing for C6 is the single most useful guidance available to allow accommodation and adjustment of established and varying workloads. Although the SPRP is faced primarily with matters of OPS concern, occasionally actions can and do have impact elsewhere within the Agency. C6 service is often available outside SPRP channels to meet requirements levied by S or R, and serves to assist L31 in lessening the effect of problems relating to longer-term magnetic tape questions.

EO 1.4.(c)
P.L. 86-36

~~SECRET~~

[redacted]

Prioritizing signals for C6 processing has to date been of preeminent concern to the SPRP, and further refinements may yet be possible and necessary, but other aspects of the charter relative to broader responsibilities have not been given equivalent emphasis. As an initial step, an interchange of representation between the SPRP, the Computer Processing Review Panel, and the Machine Allocations Review Group has been accomplished to exchange information relating to correlated matters. It is hoped that such interchange will help close the information gap between the collection and processing stages and the subsequent data processing stages.

Future

The SPRP, and C6 as the Office of Signals Processing, function at one of the more crucial junctures in the overall cycle of collection, processing and exploitation.

[redacted]

[redacted]

The impact of new collection concepts should also concern the SPRP.

[redacted]

Notwithstanding significant progress made in efforts to coordinate collection, processing, and analytic requirements, plans for future collection systems often do not consider the impact they may have elsewhere. This is particularly true of existing signals-processing capacities and, more important perhaps, our analytic capacity to digest and exploit.

[redacted]

These are but a few of the questions that must be asked and discussed by panels like the SPRP, the CPRP, and the NSOC Users' Group. If they are not considered, efforts towards balanced collection and processing will once again be submerged by hyperconcern for volume in lieu of content. Unless a thorough review and thinning out of spurious requirements is undertaken, no computer will ever keep pace with collection, nor will storage capacity ever be sufficient to store materials never looked at and perhaps never desired.

All aspects of the SPRP charter need to be implemented, and the Panel encouraged in courses of action which will more directly assist DDO in the decision-making process, particularly regarding possible equipment and manpower savings.

~~(SECRET/HVCCO)~~

P.L. 86-36
EO 1.4.(c)

DOCID: 4009707

EVEN A 5-YEAR-OLD CHILD...

by EMERY W. TETRAULT, P16

The chief difficulty facing the person who comes new to the study of linguistics is that of being prepared to look at language objectively. For language is something we tend to take for granted; something with which we are familiar from childhood in a practical, unreflecting way. And, as has been often observed, it requires a particularly strong effort to look at familiar things afresh. Nor is it merely our intuitive or practical familiarity with language that stands in the way of its objective examination. There are all sorts of social and nationalistic prejudices associated with language and many popular misconceptions fostered by the distorted version of traditional grammar that is frequently taught in the schools. To free one's mind of these prejudices and misconceptions is indeed difficult, but it is both a necessary and a rewarding first step. (John Lyons, *Introduction to Theoretical Linguistics*, 1968)

If this statement needed substantiation, NSA would be a good place to do the field work. True, not everyone needs to become a language theoretician, but those who are called upon to make decisions and formulate policy regarding language matters should attempt to do so in a manner consonant with the realities of natural language.

Limitations of space, time and energy make even a sampling of dubious language generalizations a practical impossibility. However, two such conclusions, both about Chinese, can serve to illuminate a very important fact of language.

The first of these has the immediate virtue of being totally untrue, even though it has been one of the cliches of Chinese language instruction:

"CHINESE HAS NO GRAMMAR."

What is presumably meant by this is that written Chinese has far fewer overt markers of case and subordination than English and virtually no *explicit* categories such as number and tense. Ordering and context fill the resultant gaps, or what seem like gaps to the speaker of English. The fact remains, however, that Chinese indeed has a grammar in the sense of the word that is current today; that is, a code which enables two speakers of the language to communicate with each other. There is, in addition, every reason to believe that the grammar of Chinese presents as many complexities as that of English, in spite of its lack of surface markers.

The second generalization is far more difficult to deal with, because it is in some respects true:

"LEARNING A LANGUAGE CAN'T BE ALL THAT HARD; EVEN A 5-YEAR-OLD CHILD CAN LEARN TO SPEAK CHINESE FLUENTLY."

This is a reasonable statement on the face of it. After all, the streets of Peking are teeming with children, many of whom are 5 years old and all or almost all of whom speak Chinese "with the speed of summer lightning."

The implications of this statement, if it is true, are staggering. In theory the average adult should have no difficulty mastering any behavior learned by a 5-year-old child. In practice few of our language analysts, military or civilian, achieve even a 5-year-old's command of Chinese.

Why is it that a healthy, reasonably intelligent and well-motivated 20-year-old American cannot match the achievements of practically any 5-year-old resident of Peking, even after 47 weeks of intensive training?

The answer lies not in any general defect in 20-year-old Americans or in our training system per se. Rather we should seek it by trying to analyze the linguistic accomplishments of our hypothetical Chinese 5-year-old.

If a Chinese child is like an American child, at the age of 5 he possesses a sizeable stock of lexical items (well beyond 1,000,

DOCID: 4009707

almost all of which are intelligible) and, what is more important, he commands an array of sentence forms which approximate those of adult colloquial usage, with grammatical anomalies limited to less frequently encountered structures: all in all, an impressive feat.

The awe which a child's language proficiency inspires begin to grow in a geometric progression when we consider one further fact. Evidence suggests that a child does not "learn" the utterances of his language, at least not in any stimulus-response model of the learning process, but rather he infers the rules of his language from the speech of those around him. One aspect of this evidence is the fact that he produces novel utterances, utterances which he could not possibly have heard from others.

One class of novel utterances contains forms resulting from an inappropriate, but perfectly consistent application of inferred rules; e.g.:

Bang! you fall down! I *deaded* you!

Our cat has four *foots*.

(Parent) Eat your peas.
(Child) I don't want *some* peas!

It could be that the rule-governed or analogous formations such as "foots" are somehow a consequence of the relatively low frequency of occurrence of the lexical item in the child's speech. Yet such irregular strong verbs in English as "come", "go" and "sit" appear with high frequency in the past tense, but tend to be far less stable than the less practiced regularized /d/ and /t/ forms of the weak verbs, as indicated by the fact that at a certain point in the child's development he suddenly abandons the irregular form in favor of the regularized form and produces "comed", "goed" and "sitted."

If we adopt the view that our hypothetical 5-year-old has somehow inferred the rules of an adult-like grammar from the speech of those around him (according to some built-in timetable of his own), then we must allow that he has performed a truly prodigious feat, one which outstrips anything done by the best minds in scientific linguistics.

What makes a 5-year-old, virtually any 5-year-old, such a good linguist? Is there some way that we could bottle it and distribute it among our language analysts? The work done by E. H. Lenneberg and others in the area of the biological aspects of language provides at least the outline of an answer to these questions.

Lenneberg states that adult language functions take place predominantly in the left hemisphere of the brain (in the precentral area of the frontal lobe). He also states that such cortical specialization is not present in early life, but develops gradually in a process similar to that of embryological history. Thus, in adults left-sided central cortical lesions cause some form of aphasia in 70 percent of all such cases and in half of these the condition is irreversible.

Comparable traumata in childhood have significantly different consequences, however, according to the age at which the damage is incurred. As Lenneberg notes:

> Lesions of the left hemisphere in children under age 2 are no more injurious to future language development than are lesions of the right hemisphere. Children whose brain is traumatized after the onset of language but before the age of 4 usually have transient aphasias; language is quickly reestablished, however, if the right hemisphere remains intact. Often these children regain language by going through stages of language development similar to those of the 2-year-old, but they traverse each stage at greater speed. Lesions incurred before the very early teens also carry an excellent prognosis, permanent residues of symptoms being extremely rare. (Lenneberg "On Explaining Language" in Lester (ed.) 1973)

The picture is far bleaker for people who have suffered damage to the left hemisphere after the early teen years. Lenneberg notes that young men suffering such lesions as the result of war wounds have symptoms not unlike those of elderly stroke victims with a similar prognosis regarding the reestablishment of language.

In cases where damage to the left hemisphere of the brain occurs early enough in life, language functions *continue to be controlled* by the right hemisphere. The operative words here are "continue to be controlled." Lenneberg emphasizes that it is not a question of the right side of the brain "taking over" language functions from the left side, but rather that before a certain critical age both hemispheres are involved in language. This apparently is the key to explaining the linguistic prowess of our 5-year-old Peking resident, the ability of young children to recover from aphasias that adults overcome, and the often noted ease with which young children assimilate foreign languages when their parents take them to an overseas post.

Alas, beyond the early teen years left-hemisphere specialization of language functions is firmly established and language acquisition becomes a true learning process, an academic exercise at which some excel and some fail, but in which no one will ever begin to match the achievements of a 5-year-old child.

DOCID: 4009707

In summary, Chinese does have a grammar and we are only beginning to perceive its complexities; a Chinese 5-year-old has mastered most of these complexities *after having inferred them from raw data;* and this remarkable facility is somehow connected with the fact that language functions are not yet confined to the left hemisphere of the brain, a specialization which occurs at some time during the teen years.

If we accept Lenneberg's findings and conclusions (and there are stronger reasons for doing so than those which appear in this necessarily brief outline), what are the implications as far as NSA is concerned?

First of all it appears that we have to take still another look at the way an adult learns a second language. Most language-teaching methods in use today appear to depend at least in part on the assumption that the adult student is able to infer many of the foreign language's grammar rules from exposure to carefully selected utterances in the language. If Lenneberg is right about the critical age for language acquisition, we have to review this assumption and consider returning to an explicit presentation of second-language grammar to language students (something which I understand is already happening in the case of the proposed revision of the DLI Spanish course).

The second set of implications touch upon the selection of linguists, either students for language courses or applicants for language jobs. We should ask ourselves whether all adults are alike in left-hemisphere dominance or whether this factor varies from one individual to another. Is there a correlation (presumably negative) between hemisphere dominance of language and second-language acquisition? This appears to be getting into an area of investigation described by Dr. Ruth Day of Yale and Haskins Laboratory in an excellent paper which she presented to SIG/VOICE (the Crypto-Linguistic Association's Special Interest Group for Voice). Her findings imply that left-hemisphere dominance of language is not invariable in adults, since some people can hold raw language (auditory) stimuli in a short-term memory bank, while others begin linguistic (grammar) processing of such input right away. She has devised tasks which clearly discriminate between these two classes of individuals. We might want to investigate whether either type of person presents a better prognosis for second-language learning, particulary for aural comprehension and related functions.

Finally, we should come away from this with an increased appreciation of the linguistic accomplishments not only of 5-year-old children, but also of adults who, either through choice or necessity, are attempting to replicate, however feebly, a truly prodigious feat -- the acquisition of a human language with all of its complexities of expression and content, with all of its unknown and in some cases unknowable cultural implications. What the child can do as naturally as he runs or throws a ball, the adult must learn in a painstaking academic process involving literally thousands of units, hundreds of rules, and an infinitely innumerable set of possible combinations.

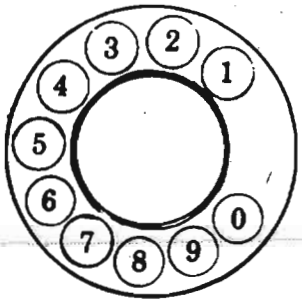
- -

(Note) Two papers by Eric H. Lenneberg, "Capacity for Language Acquisition" and "On Explaining Language" (both reprinted in Lester (ed.), *Readings in Applied Transformational Linguistics,* Second Edition, Holt Rinehart, 1973, are the source of much of what is contained above.

(UNCLASSIFIED)

A retired NSA employee living in Mexico had a telephone with digits but no letters on the dial. Learning that direct dialing was possible, he tried to call a friend in Maryland whose number in his ancient address book was Area Code 310, MItchell 7-[redacted] Retired Employee discovered he had problems!

Without looking at your own telephone dial, can you convert the MI from the MItchell exchange to the correct digits?



P.L. 86-36

DOCID: 4009707

EO 1.4.(c)
P.L. 86-36

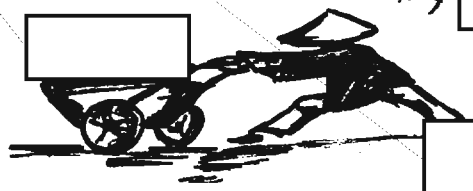
P.L. 86-36

~~SECRET SPOKE~~

CHARACTER BUILDING IN THE PEOPLE'S REPUBLIC OF CHINA

by

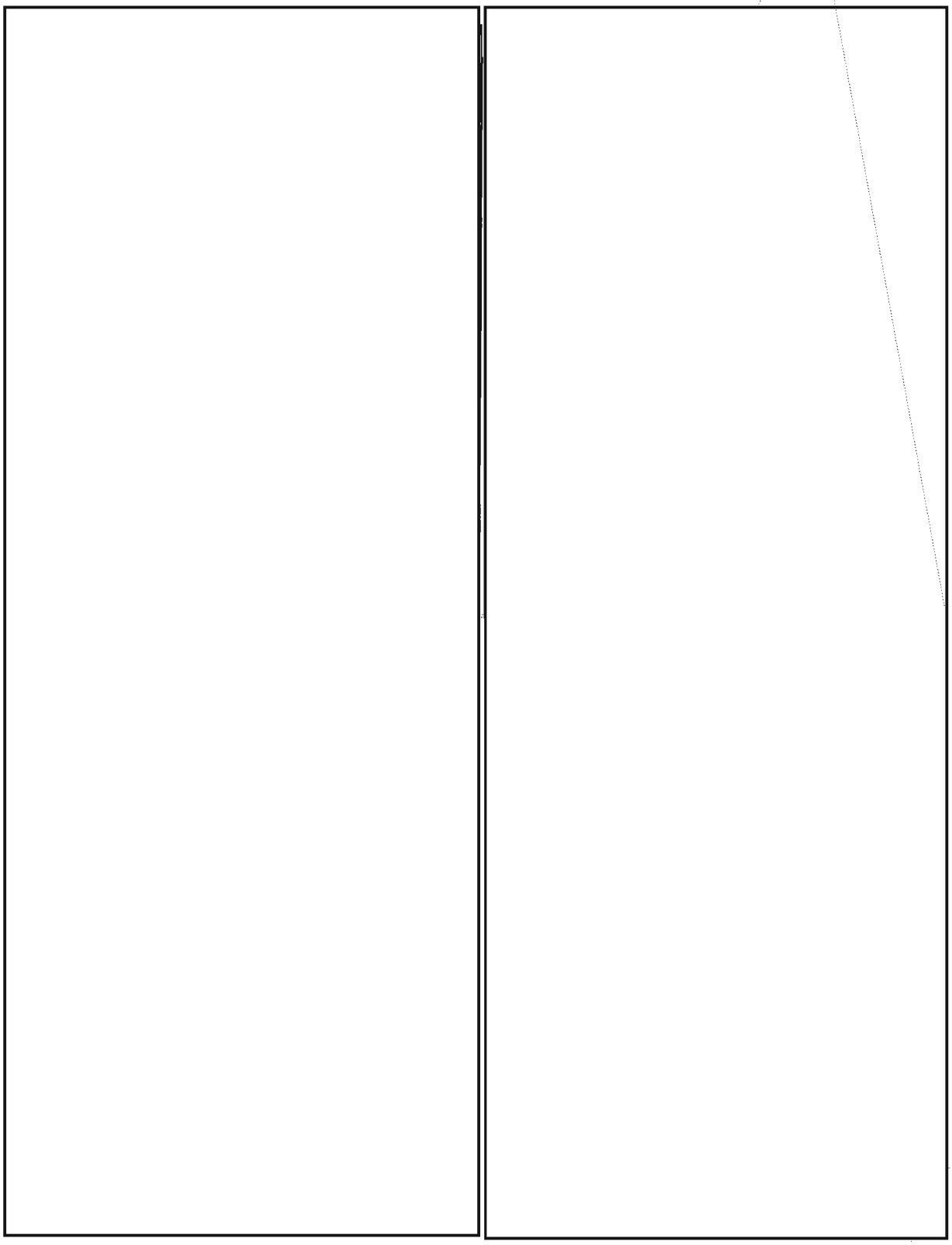
and



~~SECRET SPOKE~~

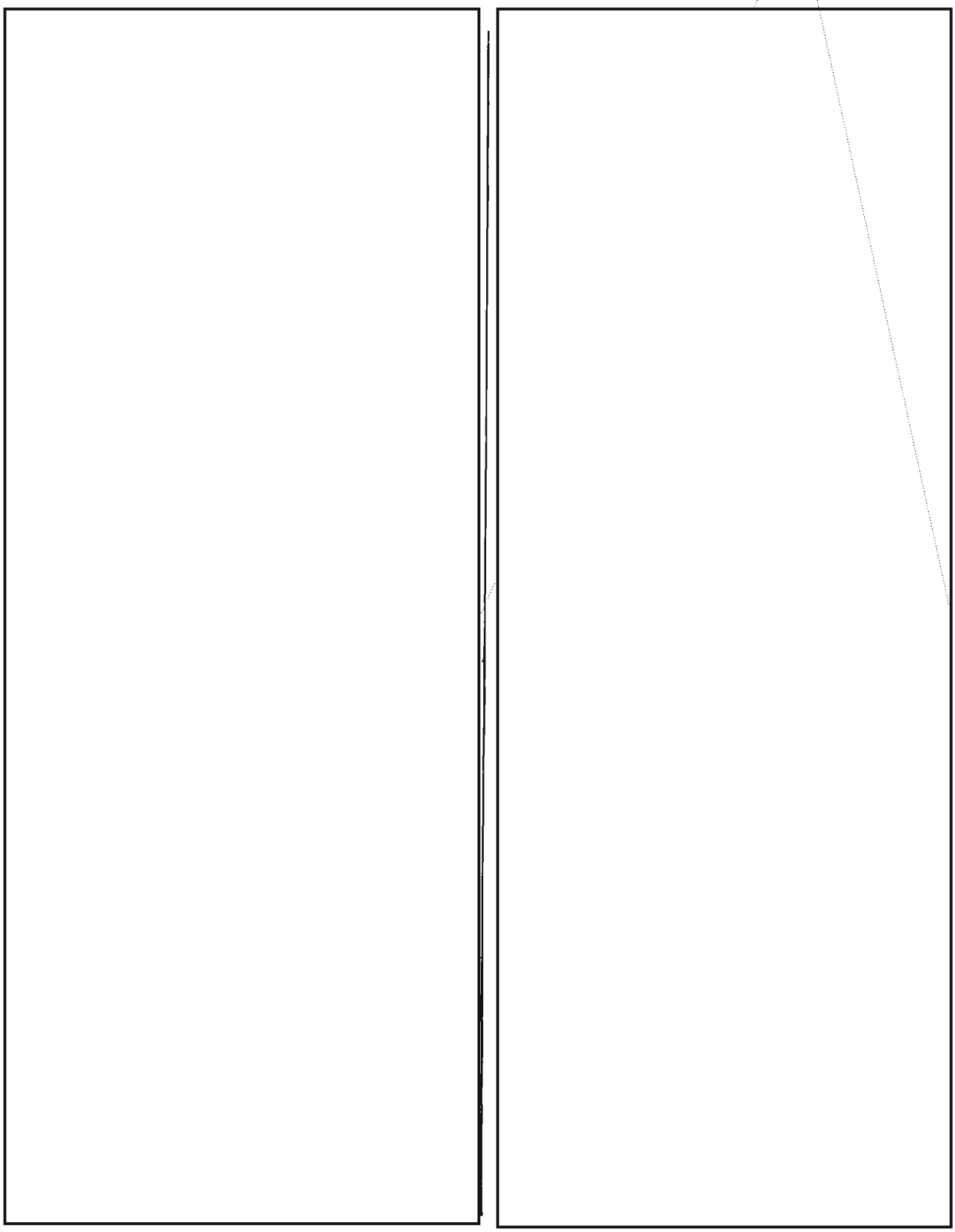
EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~



DOCID: 4009707

EO 1.4.(c)
P.L. 86-36



DOCID: 4009707

EO 1.4.(c)
P.L. 86-36

DEPARTMENT OF GOLDEN OLDIES

An Unofficial Glossary of WEASEL WOF

Date: Pre-1955
Author: Unknown (or do you know?)

"An accumulation of traffic analysis evidence reveals. . ." *It was lost in our files and we just found it.*

"Advance field sources report . . ." *In case this is wrong, don't blame us.*

"These changes have not been fully recovered..." *We can't break the system.*

"Tenuous evidence suggests the possibility that . . ." *This did not come out of a whisky bottle--we got it from tea leaves.*

"Another center has identified. . ." *We don't know how they did it, but we're afraid to argue the point.*

"Very probably. . ." *The analyst is a persuasive talker.*

"There are some indications. . ." *We feel sure of it, but we've never used this kind of argument before.*

"Spasmodic intercept. . ." *Haven't heard it for months.*

"Valid messages. . ." *You can't prove they're practice.*

"Thought to serve. . ." *It was carried that way on an old diagram someone saw once.*

"A historical survey of the net reveals. . ." *We were dopes not to notice this last year.*

"Fragmentary evidence. . ." *The rest of the traffic has been misplaced.*

"A re-evaluation of evidence, in light of recently available material. . ." *We really missed the boat on this one!*

The characters with the little sketch tell us, "Life is limited, but knowledge is boundless."

DOCID: 4009707

A LONG HARD LOOK AT THE Intern Program

by 'Anne Exinterne'

PART TWO: SELECTION AND ORIENTATION

In writing this I was initially reluctant to comment on some aspects of my experience as a college hire because there have been changes in the hiring and training procedures for college graduates in recent years. I decided to include these comments because I believe many of the changes were not made for philosophical reason but for budgetary ones, and that some of the procedures in practice when I came on board might be reinstated. In fact, I recently heard that the LIC (Limited Interim Clearance) hiring program which was in effect in the mid-60's is to be revived, and that the intern program will again be restricted to college graduates. Thus my experience might be very relevant for FY-75 college hires.

The method by which college hires were oriented and selected when I arrived ignored one characteristic of most recent college graduates--they honestly want to work and want to sink their teeth into a job. We were immediately put into a three-month orientation course taught for the most part by other recent hires who had not been cleared by the time they finished the course and were consequently promoted to instructors. Since the ink was barely dry on our diplomas, the last thing most of us wanted to see was another classroom, and having these people as instructors did little to change our feelings about that, or to instill confidence; we were taught elementary CA, TA and Signals Analysis in a manner that made those subjects seem as little related to anything in the real world as metaphysics had six weeks before. At the end of the orientation course we were asked to indicate the career fields we preferred, and depending upon the time of year and the number of vacant billets left, might get our first, second, third, or even fourth choice of assignments.

Then the orientation process shifted almost 180 degrees. All recruits were fully cleared when they came on board, and those who were to be interns were hired for a specific intern program. If a college recruit came in with a group of other college hires he might get as much as two or three weeks of orientation before being put to work, but frequently he was turned over to his panel office to begin his new assignment with no more than a briefing on the relative merits of Blue Cross over GEBA, the Agency structure, and how to report in on sick leave. For a more complete orientation he was at the mercy of the panel office, and more directly, the organization he was assigned to; it might be months before the work meant anything to him.

We may now see a revival of the three-month orientation class, but an alternative that would probably be better for both the Agency and the employee than either of the above methods would be to enroll new people in a two or three month's work-study program, with half the day in a class room and half in operations. (In TA work, for instance, I know from personal experience and contacts with other interns that there are areas that have backlogs of routine TA work, callsigns to be broken, work to be done on frequency rotas, etc., that could be done by novices with a minimum of instruction.) This would satisfy the new hire's desire to be productive and would at the same time make the course work more meaningful.

A variation of this proposal would be to give the new hires the self-study course Introduction to Cryptology (CY120) and put them in an area where they could observe a number of skills being practiced, with one analyst designated to serve as a reference point if trouble spots with the course came up, as well as a guide to what was going on in the area.

I would enroll every new employee in at least two of the following courses: Basic Traffic Analysis (TA 100), Introduction to Manual and Machine Cryptosystems (CA015), Introduction to COMINT/ELINT Technology (EA010), and Introduction to Computer Science (MP160), during his first 18 months at the Agency. This would provide him with more information on what field he might be best suited for, while giving him an appreciation of other disciplines. I would have him tour the agency to actually see how materials come in, how they are disseminated and how the finished product leaves the building. Some employees who have been here a number of years have only the vaguest idea of what happens to their product once it leaves their desks.

DOCID: 4009707

The hires who had specific skills would be assigned to areas that would make use of them; those who did not would be given assignments based on the testing described previously. While I would attempt to make use of existing skills, I would classify all new hires by a general term, such as "SIGINT Technician," rather than immediately identifying them with a specific career field.

I would not put any new hires directly into an intern program. Many college hires who went directly into a program, as I did, felt that their first 6 to 12 months were not as meaningful as they could have been because they didn't really understand the Agency's organization or operations for that period of time. A study conducted last summer raised this question and concluded that college hires should not be required to begin with work in an operational assignment. I'm not sure of the reasoning that prompted that conclusion, since the study stated that most of the managers and executives favored direct assignments, and the interns were divided on the question (in general, SR and TA interns favored direct assignment while CA, DS and Language interns did not).

Under the system I propose, new hires would be eligible to apply for intern programs after 12 to 18 months in their assignments, and no organization would be permitted to hold a candidate who had been accepted. By that time the hires would have an idea of what fields they were really interested in, while for their part the panels would not have to choose between "related experience" and academic training, as they often do now in selecting interns from both on-board and college hire candidates.

(To avoid the possibility of new hires being stuck in a corner somewhere and never even hearing of the intern program, Personnel could have a follow-up interview with them after they had been on the job for 12 months - at one time this was done routinely, I believe--and as part of that interview, explain the possibilities of the program.)

This would also alleviate some billet planning problems for the panels. Currently, as a panel executive with 8 vacant billets and 7 promising on-board applicants, would you go ahead and select all 7 or try and keep some billets open in case there will be an active hiring program for your field which will produce applicants you will be interested in hiring?

The method of having new hires work for a year or so before putting them into an intern program might solve several related problems:

1. It might weed out of the program the uncommitted who had no idea whether they wanted to stay six weeks, months, or years.

2. It would avoid the danger of identifying new employees too quickly and irrevocably with one career field. I and some of my friends shared similar experiences in this respect. After periods ranging from six months to a year as interns, we felt that we were not really in the right niche. Several of us discussed these feelings with representatives of Personnel and our respective panels. In each case we were told that we hadn't really given the field a fair chance, and that it usually takes several years on the job to begin to feel at home. We followed the advice, but when things didn't look any more encouraging after another 8 to 12 months we returned to our advisors. At that point we were told that since we had completed more than two years of our internship, the Agency had invested too much time and money in training us in our current field to let us transfer before graduating and trying an operational assignment in that field. Apparently there is a month or a week we missed when these people would have agreed that we had spent enough time in the field to give it a fair chance, but not too much to transfer!

(This touches on a related problem. Some supervisors seem to feel that if a subordinate requests a release it is a negative reflection on them, that their authority is being threatened or that their cache of talent will dwindle away. Whatever their reasoning, they seem to be more willing to see an employee resign than to see him go elsewhere in the Agency. Some applicants for an intern program have been misled about it, some have been given unjustifiably negative evaluations, and some even warned that if they are not accepted for the program they may regret having applied for it. My own single experience in getting a transfer was so frustrating that I now appreciate why some people spend 30 years on the same job!)

3. It would make for more realistic career development. I believe that the college graduates who came to the Agency in the late 60's began careers that were too heavily "front loaded" as far as rewards were concerned. Thirty-eight months after I came on board I was certified as a professional analyst (through no special effort on my part) and had received two promotions. This is pretty heady stuff, and is another reason why some interns in those fiscally carefree years saw themselves as "Future Super-Grades." In addition to automatic promotions and, in the case of some panels, almost automatic certification, we received virtually every course we requested. Some of us also had opportunities for downtown or overseas assignments. During all this, we could do as much or as little as we wanted. It was virtually impossible to be dropped from a program, despite instances of low and even failing grades and poor performance. This "front loading" did two things: one was to take new hires who began

DOCID: 4009707

as ambitious workers and demonstrate that they could have all the rewards of effort even if they did not elect to put forth very much. The second was to create a sense of disillusionment when the pace slowed -- as it had to, even if the money had continued to flow, simply because there are only so many grades in the GG scale.

(The above picture may seem far removed in these more austere days of 1974, but I believe there is a proposal under consideration now to promote interns when they are approximately halfway through the program, if they meet the standards established by the panels, and to graduate them as GG-11's if they meet certification requirements. While the association of such standards with intern promotions is a definite improvement, it could be the first step toward reestablishing the old norm of two virtually automatic promotions for every intern.)

4. It would make the OJT supervisor's job easier, particularly when on-board interns or military convertees are involved. Interns were initially a fairly homogeneous group, and the supervisor had a pretty good estimate of the type and amount of guidance he would have to provide for those coming into his area. While the stereotype of interns as twenty-one to twenty-four-year-old, bright-eyed recent college graduates (typically women) persists, the fact is that in recent years on-board employees have been a prime source of input for some panels. The interns of one panel were studied and it was found that men outnumbered women 2 to 1, that the age range was 23-37 (meaning that some supervisors had to wait to tell their war stories until they had heard the interns') and that both the mean and median age were 30. The amount of Agency experience ranged from less than one year to 17 years, with 6 the average and median number; but over half the interns had prior government or military experience, which brought their government service to an average of 8 years. Only 17 per cent were direct college hires and only 50 per cent college graduates.

Such diversity puts a considerable burden on the supervisor. One month he has Bill Brown reporting to him, just after graduation with a degree in comparative government and no work experience other than being a summer camp counsellor. Bill is intrigued by his new environment, and would willingly listen to explanations of what NSA is all about from dawn to dusk. The next month he gets John Smith, who has converted from the military and has a total of ten years in the SIGINT business (two more than the supervisor has). Smith is already certified in another field and is ready and more than willing to fill in for the boss should the need arise. The supervisor may not even know ahead of time which type he is getting. It takes adaptability and resourcefulness to tailor a tour to interns with such diverse backgrounds--and the wisdom of Solomon to write their performance appraisals.

The recent ruling that the program will again be limited to college graduates, coupled with the revival of a college recruitment program, will very likely do much to reduce this heterogeneity; however, I believe that the situation I have just described merits study by Agency managers because it invites questions such as: (a) Why does someone with many years of Agency experience apply for an intern program? (b) Who should be considered "overqualified" for an intern Program? (c) Was the ruling that interns will now be required to have a degree based on a study of the performance of interns who do not have a degree?

My own feelings concerning these questions are as follows:

(a) Since the intern program is the only comprehensive formal training program the Agency has at the technician level, on-board applicants have tried to become interns for a variety of reasons, such as getting popular training courses, satisfying a desire for diversification, escaping from an unchallenging or dead-end position, becoming certified in the shortest possible time, etc. In short, the intern program has been viewed as the solution to a number of problems technicians have. I do not think that it is reasonable to expect to satisfy the needs of the veteran and the new employee through one program; Agency and employee needs would be better served by differentiating levels of training. As mentioned previously, I think every new employee should be given introductory level training in several fields. Those selected for the intern program would then already have some of the courses required of most interns, and the level of training provided through the intern program could be raised to that of an intermediate level training program. This might also alleviate the problem some panels currently face of interns who have completed the program but who can not be certified because they can not pass the PQE. While some Panels are searching for the course or the type of assignment needed to correct this problem, I think the answer is that the intern should dig deeper into the field.

(b) There are currently varying, even conflicting, schools of thought on who should be considered "overqualified" for an intern program. Some panels seem to exclude the candidates with the best potential for success. For instance, a college recruit coming into the Agency with a master's degree in data systems is automatically certified, and therefore is not considered for the data systems intern program, while a recruit with a degree in English may be accepted. This means that the data systems

DOCID: 4009707

major does not get the benefit of the variety of operational tours and training courses that his new colleague does. Similarly, the college graduate linguist who converts from the military is likely to be considered overqualified for the language intern program, while the girl from Sunnyvale Academy is readily taken in. (However, the military convertee could apply for the SR program and, until very recently, probably would have been accepted.)

(c) Since the study that was done on the intern program last year did not indicate that the performance of hires who went directly into the program was superior to that of on-board interns, I would advocate further research before re-imposing the requirement that all interns must have a degree. For some fields a degree is more relevant than prior cryptologic experience, but for other fields the reverse is true. I am concerned that a blanket requirement for a degree will eliminate some good candidates for the program. In fact, the program initially did have a requirement for a degree but it was removed several years ago because of a number of high quality on-board applicants who did not have a degree.

To summarize: Given the goals that have been set for the intern program, I would establish the following entry requirements: (1) a score of 5 or above in the applicable CQB category, (2) grades of B or better in course work at the National Cryptologic School, (3) performance at or above the "strong" level during an initial 12 to 18 months' assignment in operational work. I would put the people thus selected into a two-year program, beginning with broad exposure to a particular field and becoming increasingly specialized as the intern progressed. At the end of the two years the interns would be returned to operational work, with the understanding that at a later time--perhaps a minimum of three years later--their records and those of other qualified employees would be reviewed, and that at that time, depending on the size and future needs of their career fields, some of them would be invited back for 12 to 18 months of additional training--either advanced technical courses or management training.

(Next issue: Motivation and Morale)

(UNCLASSIFIED)

NEWS FROM THE SCHOOL

EO 1.4.(c)
P.L. 86-36

AGENCY RESUMES HIRING OF LIC'S

In recent years most new NSA employees have had to be fully cleared before being hired, but employees who came in in the middle 60's will remember the initials L.I.C, which stood for "Limited Interim Clearance," and for an arrangement under which new hires not yet fully cleared were brought into the Agency and put on the payroll while awaiting final sanction. This arrangement is now being reactivated, and several hundred recruits in critical skill areas (primarily language, certain fields of engineering, and mathematics) will be hired under it.

The School, which is tasked with keeping them usefully occupied while awaiting final clearance, has worked out a course of training which will give the new hires a good background in cryptologic and intelligence work. The first phase is expected to last about 9½ weeks. Some of the material studied will consist of standard School courses, such as MP-060 (Survey of EDP), TA-100 (Basic Traffic Analysis), and CA-105 (Introduction to Manual and Machine Cryptosystems), for which the the students will receive Agency credit and which will count toward eventual certification. By the end of the course, says [redacted] Chief of E33 and Project Officer for the program, "the LIC's should have a pretty good idea of what the Agency and the intelligence community are all about."

NCS OFFERS COURSE IN "SIGINT APPRECIATION"

Over 300 DIA intelligence analysts will be attending a special course at NCS this fiscal year to learn more about SIGINT processes and analytic techniques.

It all began when Dr. Hall, Assistant Secretary of Defense for Intelligence, looked over the post-mortem reports of the USIB Intelligence Committee [redacted] He felt that DIA analysts needed to be "cross-trained thoroughly in the use of SIGINT sources so that they /could/ understand its capabilities and become familiar with the methods of SIGINT analysis and with the modes and highly specialized terminology of SIGINT reporting."

To meet this need the National Cryptologic School has organized a one-week course, SIGINT Exploitation for User-Agency Analysts (CYZ-600) to be presented once a month at FANX II for about 35 persons. (Please note that enrollment is limited to non-NSA personnel).

P.L. 86-36

~~(CONFIDENTIAL/HVCCO)~~

DOCID: 4009707

COMING EVENTS

nsa computer & information sciences institute

Dr. HARLAN MILLS of IBM
an authority on Structural Programming & Software Engineering will address CISI on
Thursday, 17 Oct 74 Ø93Ø
in the NSA Auditorium

Dr. EUGENE BOLD, P13D
will address CISI SIG/IPS
Wed 3Ø Oct 74 Ø93Ø
on DATA STANDARDS.

CRYPTO-LINGUISTIC ASSOCIATION

will present

Mr. CLIFFORD B. GROCE
Deputy Program Manager, VOA
speaking about
THE VOICE OF AMERICA
&
Dr. ROBERT J. HERMANN, DDR
discussing R&D and Its Impact on Language Processing in the Future
&
Brigadier JOHN H. TILTMAN
who will recount SOME MEMORABLE CRYPTOLINGUISTIC EXPERIENCES

Dates to be announced

The CRYPTO-MATHEMATICS INSTITUTE
announces

Dr. PHILLIP CHASE, R1
SPEAKING ABOUT
SUBSEQUENCES
Thursday, 7 Nov 74 Ø93Ø
AND
Mr. CHARLES BOSTICK
speaking on a classified topic
Thursday, 5 Dec 74 Ø93Ø
BOTH OF THESE LECTURES WILL BE GIVEN IN THE NSA AUDITORIUM

The INTERNATIONAL AFFAIRS INSTITUTE
Speakers:

Tuesday **29 Oct** 1330 hrs
Ambassador ARMIN MEYER
Former Ambassador to Lebanon, Iran, and (most recently) Japan
TOPIC:
US-Japanese Relations

rsday **5 Dec** 1330 hrs
Dr. ROBERT SLIGHTON
The National Intelligence Officer for Economics
pic:
Economic Intelligence
IN THE NSA AUDITORIUM

The COMMUNICATIONS ANALYSIS ASSOCIATION
is considering a "partially subsidized" LUNCHEON soon.
WATCH FOR ANNOUNCEMENTS!

und don't forget das Oktoberfest
12,13,14 October
Rear NSA Parking Lot

DOCID: 4009707

EO 1.4.(c)
P.L. 86-36

THE [redacted] EXERCISE

A CASE STUDY IN SPECIAL RESEARCH ANALYSIS

by VERA R. FILBY E12

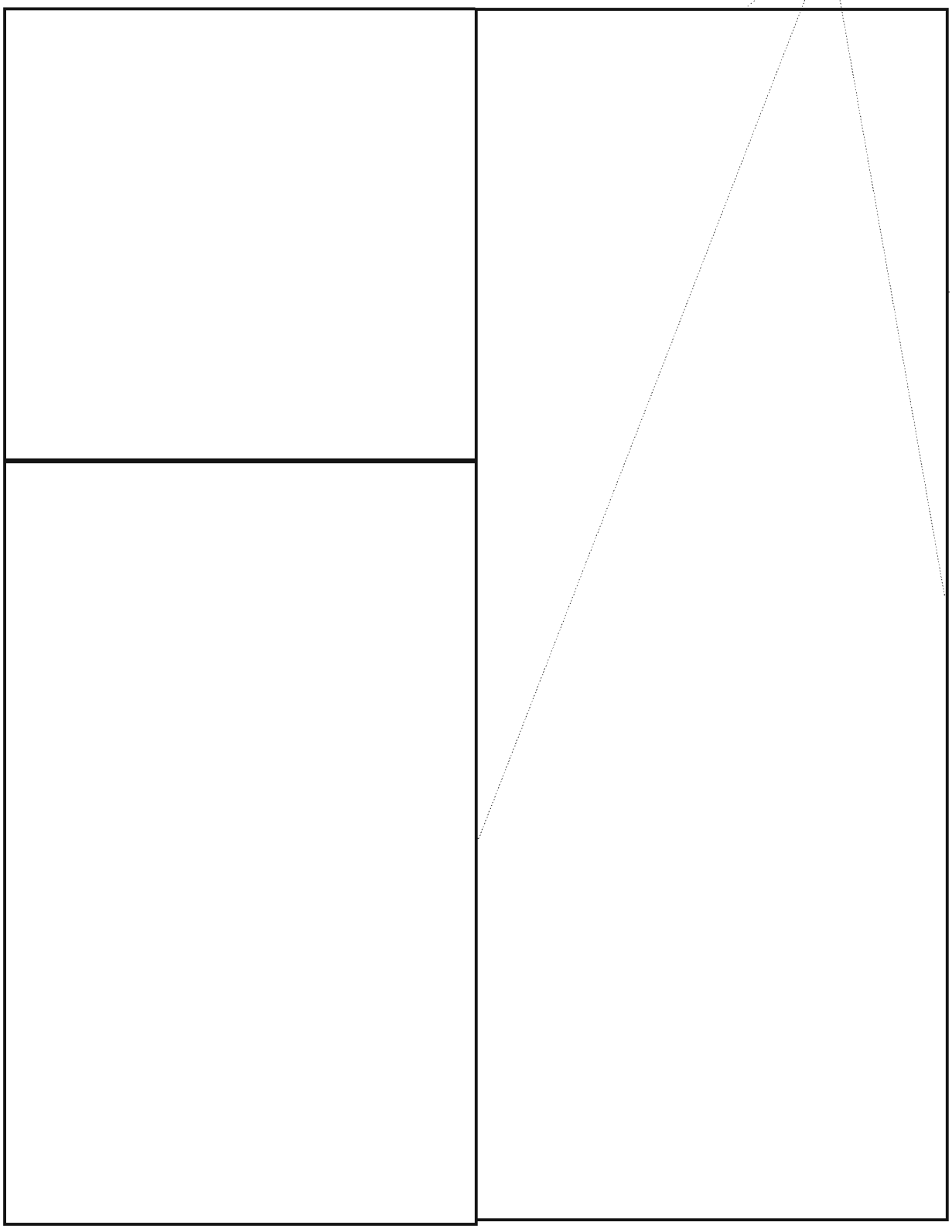
This article is adapted from a report-writing exercise formerly used in the SIGINT reporting course. It is presented here as a case study in COMINT analysis, research, and reporting, not only for SRAs but also--and even more--for the purpose of showing readers not well acquainted with the SRA field some of its variety and complexity, its frustrations and rewards. The message around which it centers and all the research data are authentic. (Except in the message itself, Cyrillic letters have been transliterated into English letters for the purpose of this article.) Some Agency organizational elements and procedures have changed since this was written, but the essentials of special research, analysis, and reporting remain the same, and the "case" described is not at all untypical.

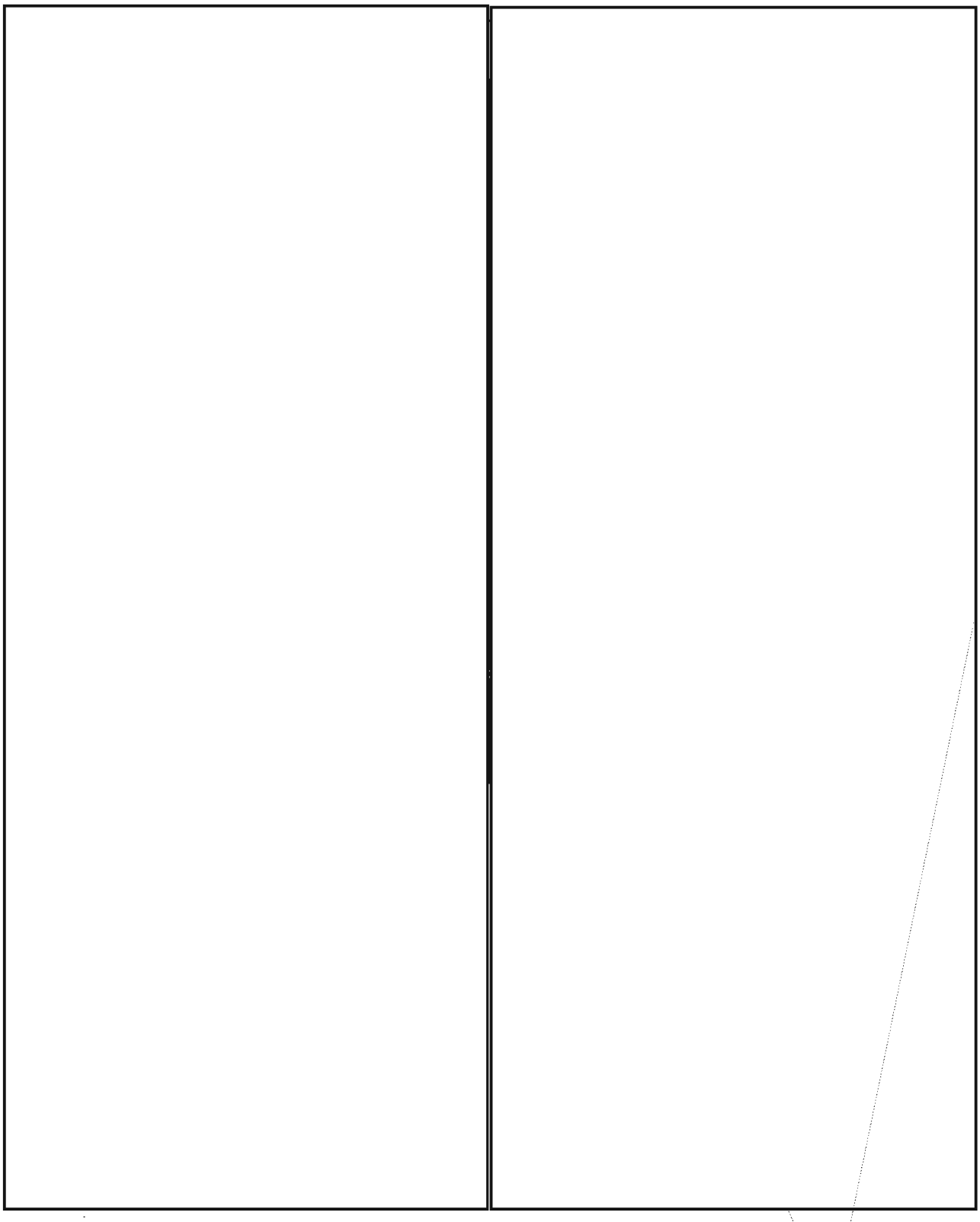
Here, then, is a day (and then another) in the life of an SRA.

[redacted]

DOCID: 4009707

EO 1.4.(c)
P.L. 86-36





EO 1.4.(c)
P.L. 86-36

DOCID: 4009707

EO 1.4.(c)
P.L. 86-36

[redacted]

~~(TOP SECRET UMBRA)~~

Subject: SRA SYMPOSIUM
To: Mr. [redacted] c/o Cryptolog P.L. 86-36

I highly endorse your proposal on page 20 of the first issue of Cryptolog to hold a two-day or two-and-a-half day seminar for Special Research Analysts. Almost every professional community, including its subspecialists, needs this sort of thing to heighten professional awareness and to promote the (cryptologic) commonweal. I would be willing to present a short paper on techniques of tactical SIGINT reporting and integrated intelligence support in the tactical situation or a short paper on how to report when you have a reportable item at a collection site but no authorized reporting vehicle into which the substance will "legally" fit.

[redacted]

EO 1.4.(c)
P.L. 86-36

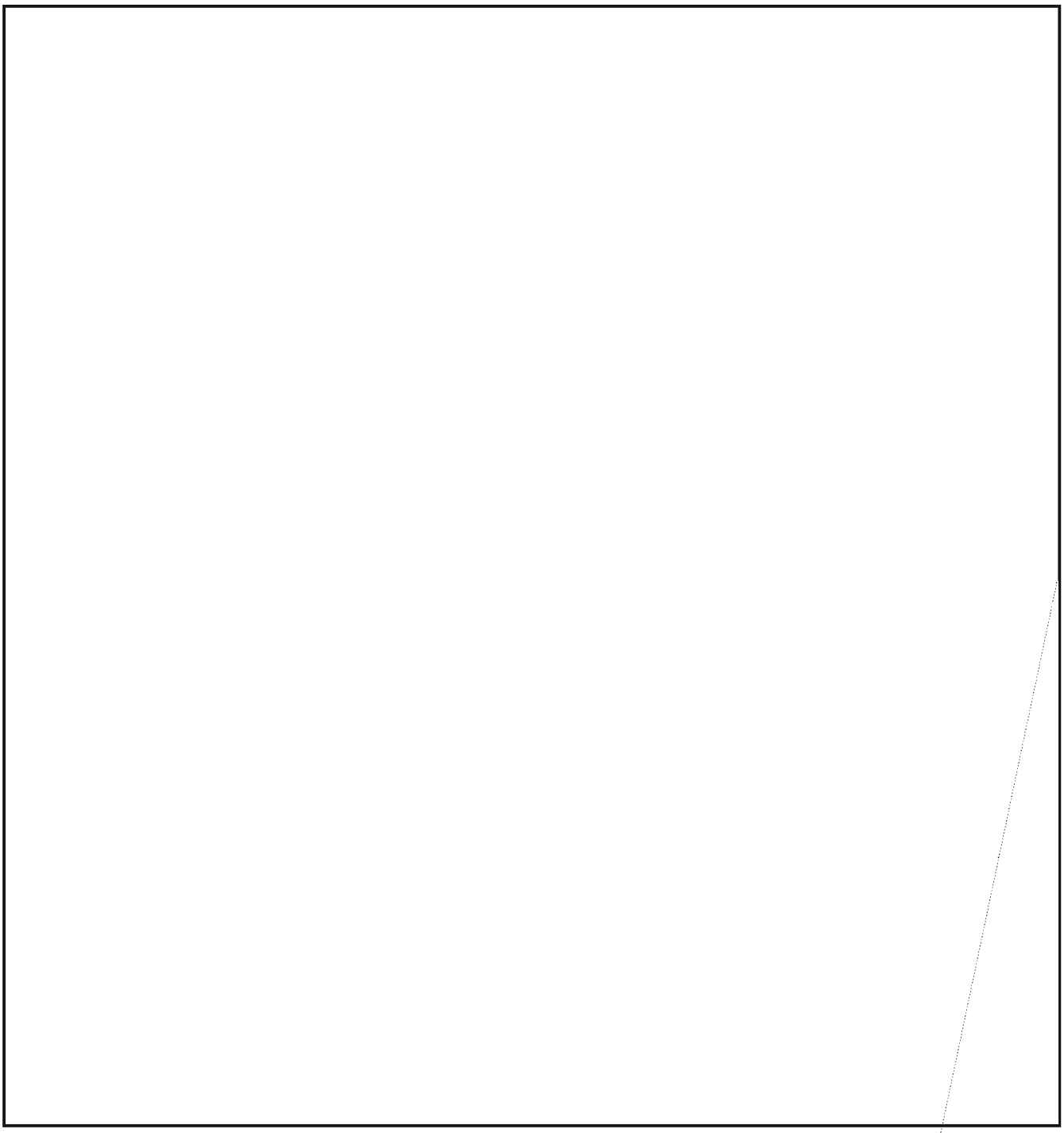
/s/ [redacted] P.L. 86-36
SIGINT Directives Staff

DOCID: 4009707

OCTOBER OVERLAP

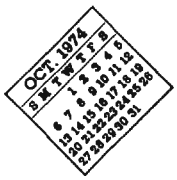
by [redacted]

P.L. 86-36

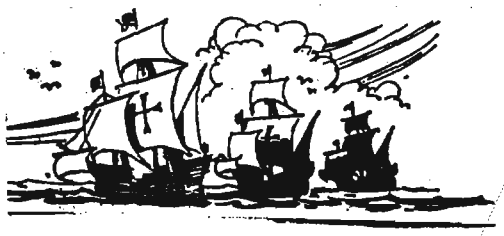


EO 1.4.(c)
P.L. 86-36

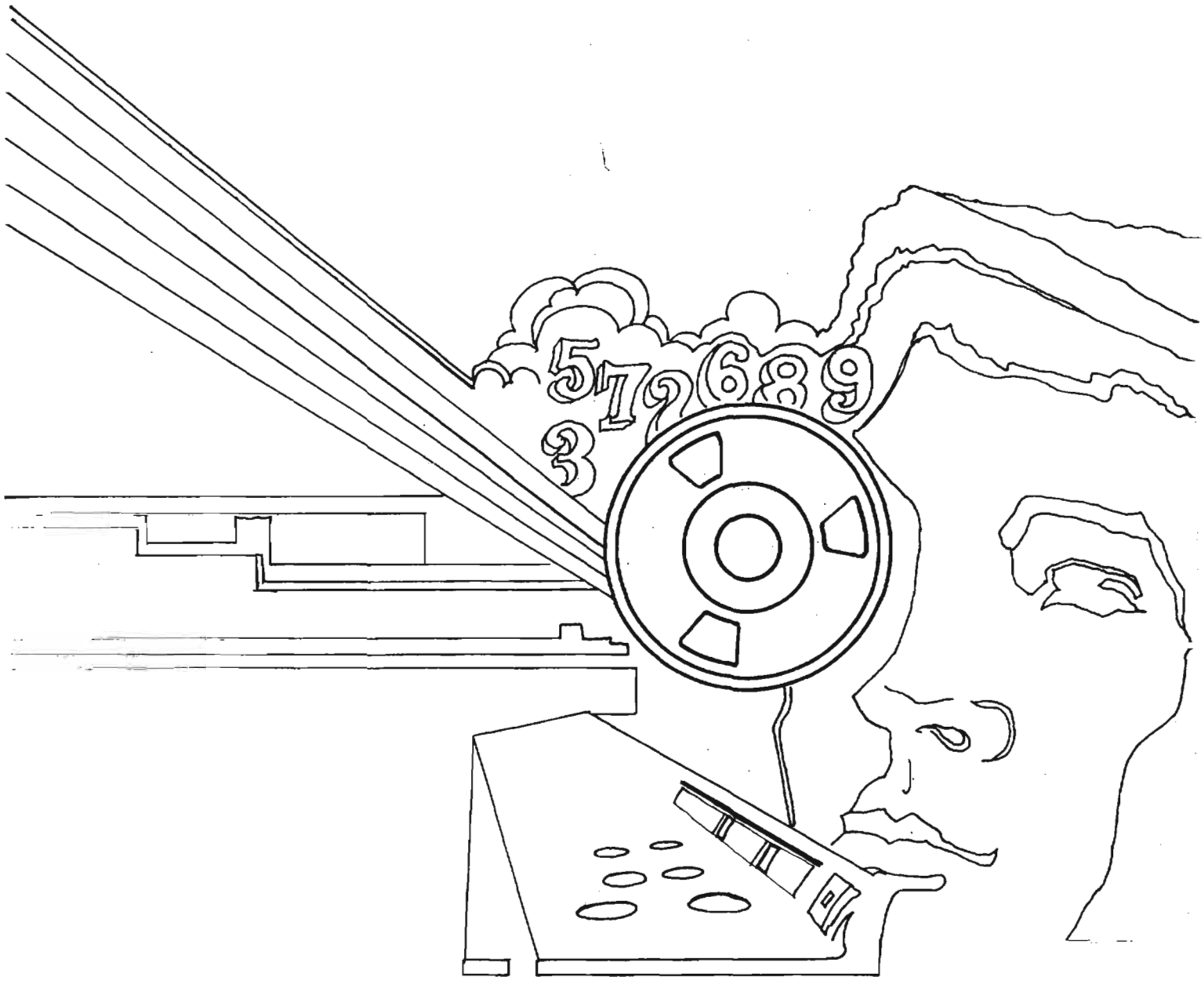
DOCID: 4009707



(Answers next month)



EO 1.4.(c)
P.L. 86-36


5 7 2 6 8 9
3

DOCID: 4009705

[redacted] ~~TOP SECRET~~ [redacted]

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

SEPTEMBER 1974

EO 1.4.(c)
P.L. 86-36

P.L. 86-36

[redacted]....Derek K. Craig..... 1
CRYPTANALYSIS AND CODE RECOVERY.....Marjorie Mountjoy..... 5
GARY'S COLORS.....Caterino G. Garofalo.. 8
PROJECT CARRIAGE.....James B. Webster.....10
SECRETS OF THE ALTARS.....[redacted].....10
SOME THOUGHTS ON LEXICOGRAPHY.....Stuart H. Buck.....11
LANGUAGE IN THE NEWS.....14
A LONG HARD LOOK AT THE INTERN PROGRAM..Anne Exinterne.....16
DEP'T OF GOLDEN OLDIES: KING EUSYB.....[redacted].....19
CONTRIBUTIONS SOLICITED.....21

~~Classified by DIRNSA (NSAM 123-2)~~
~~Exempt from GDS, EO 11652, Cat. 2.~~
~~Declas Date Cannot Be Determined~~

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR case # 54778

DOCID: 4009705

[redacted] TOP SECRET

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL.I, NO. 2 SEPTEMBER 1974

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief ..... Doris Miller (5642s)
Collection..... [redacted] (4410s)
Cryptanalysis..... [redacted] (3215s)
Language..... [redacted] (5236s)
Machine Support..... [redacted] (3321s)
Special Research..... Vera R. Filby (7119s)
Traffic Analysis..... William J. Jackson, Jr. (3369s)

Art Editor..... [redacted]

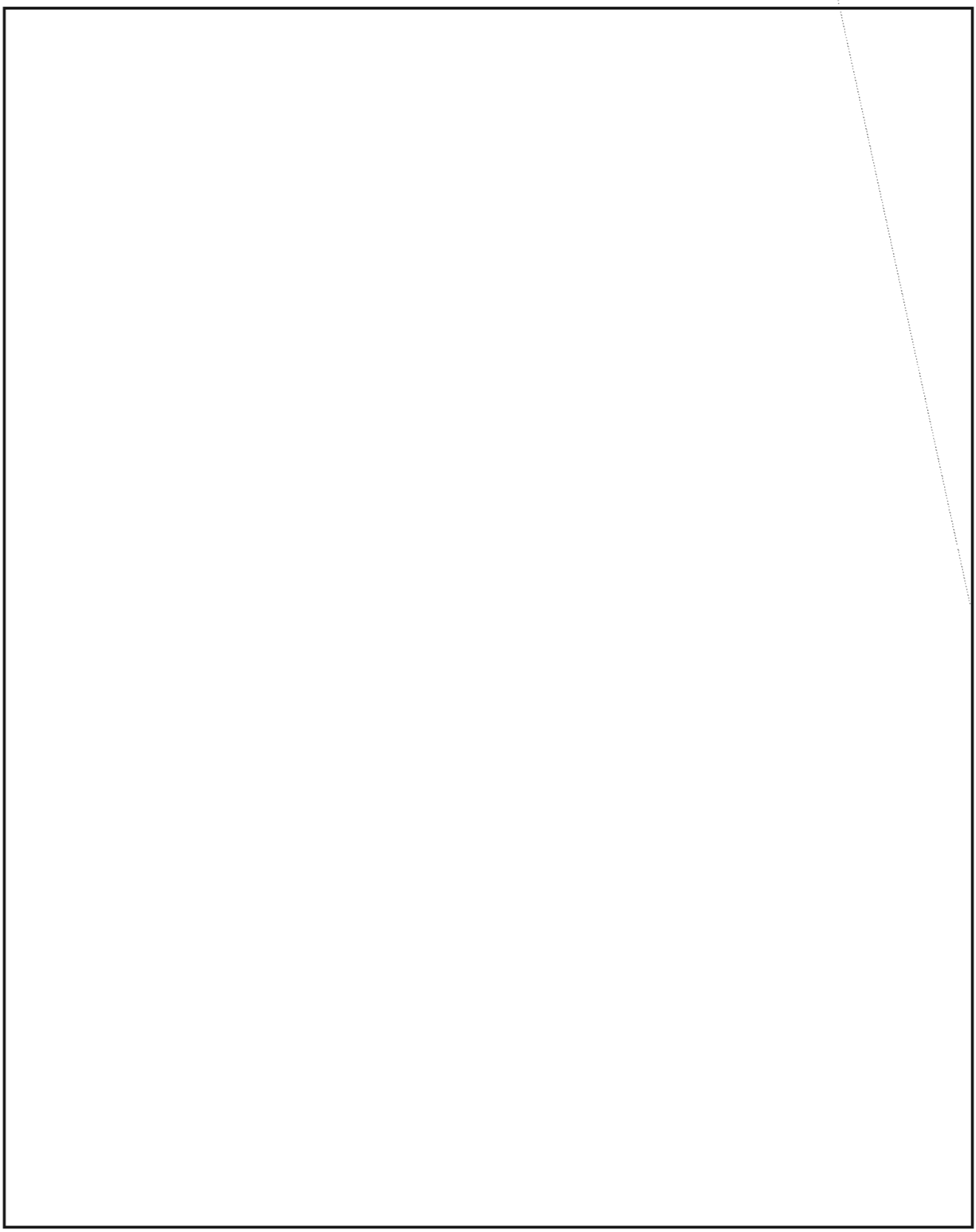
P.L. 86-36

* * * * *

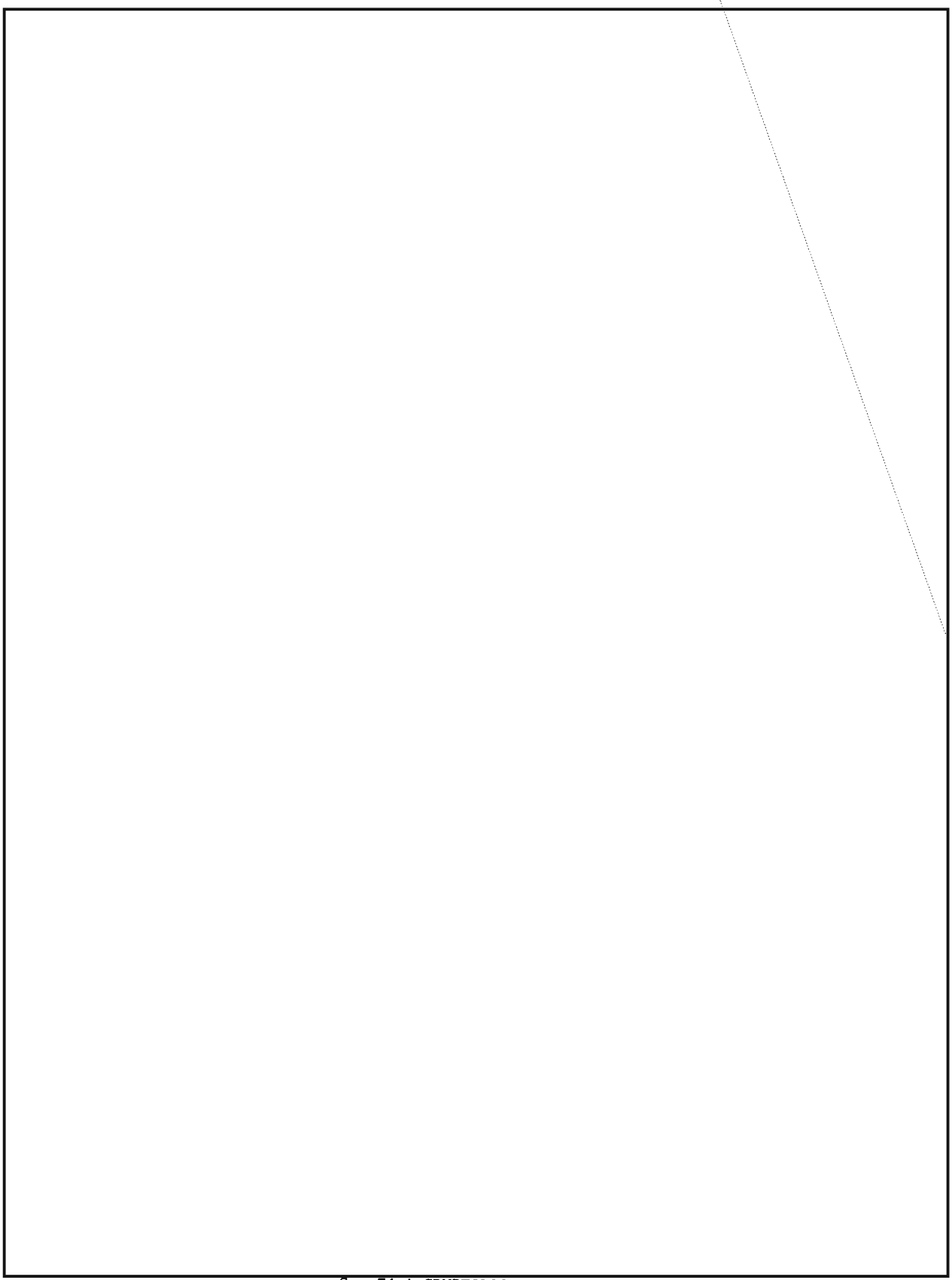
TOP SECRET

EO 1.4.(c)
P.L. 86-36

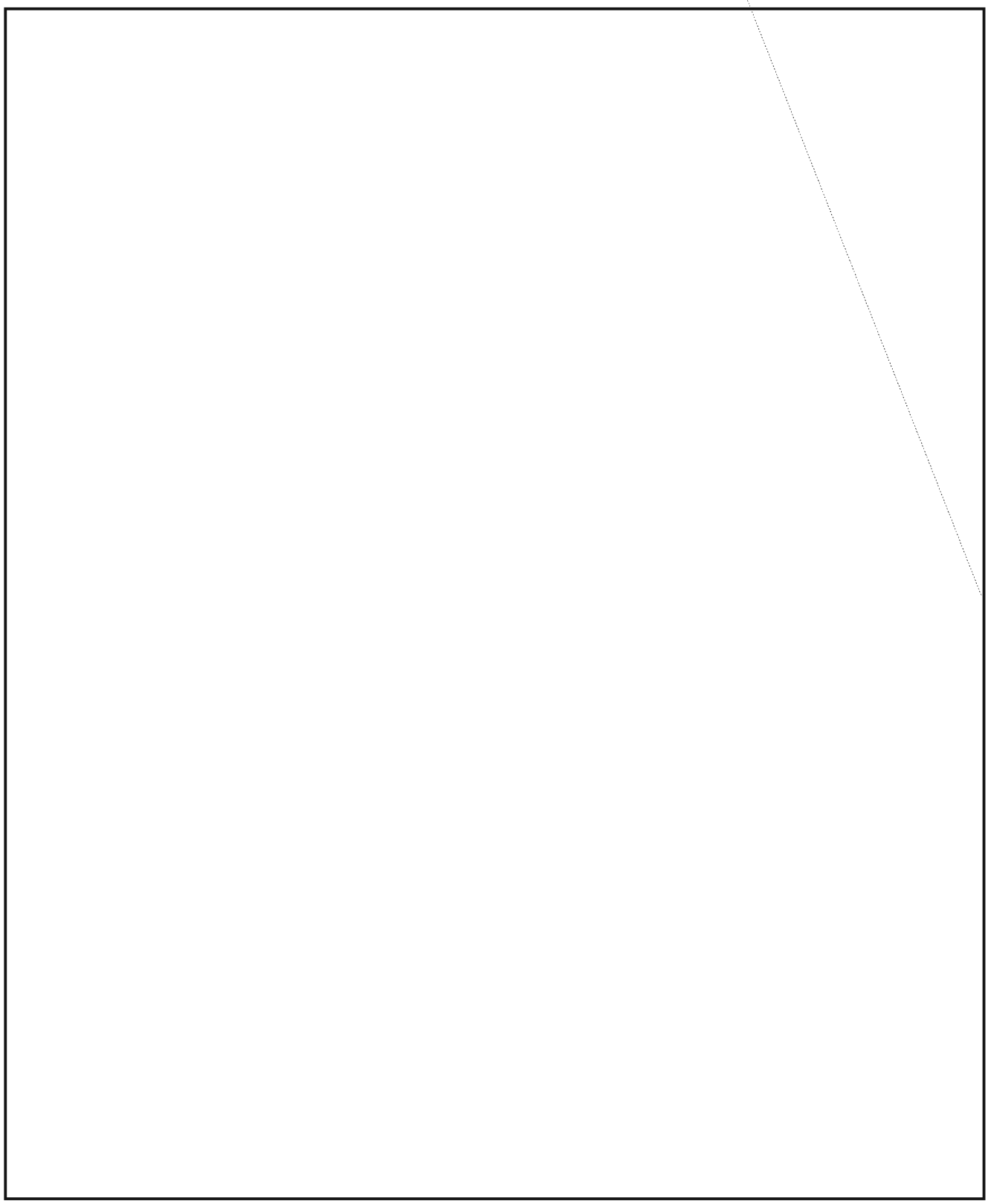
~~TOP SECRET UMBRA~~



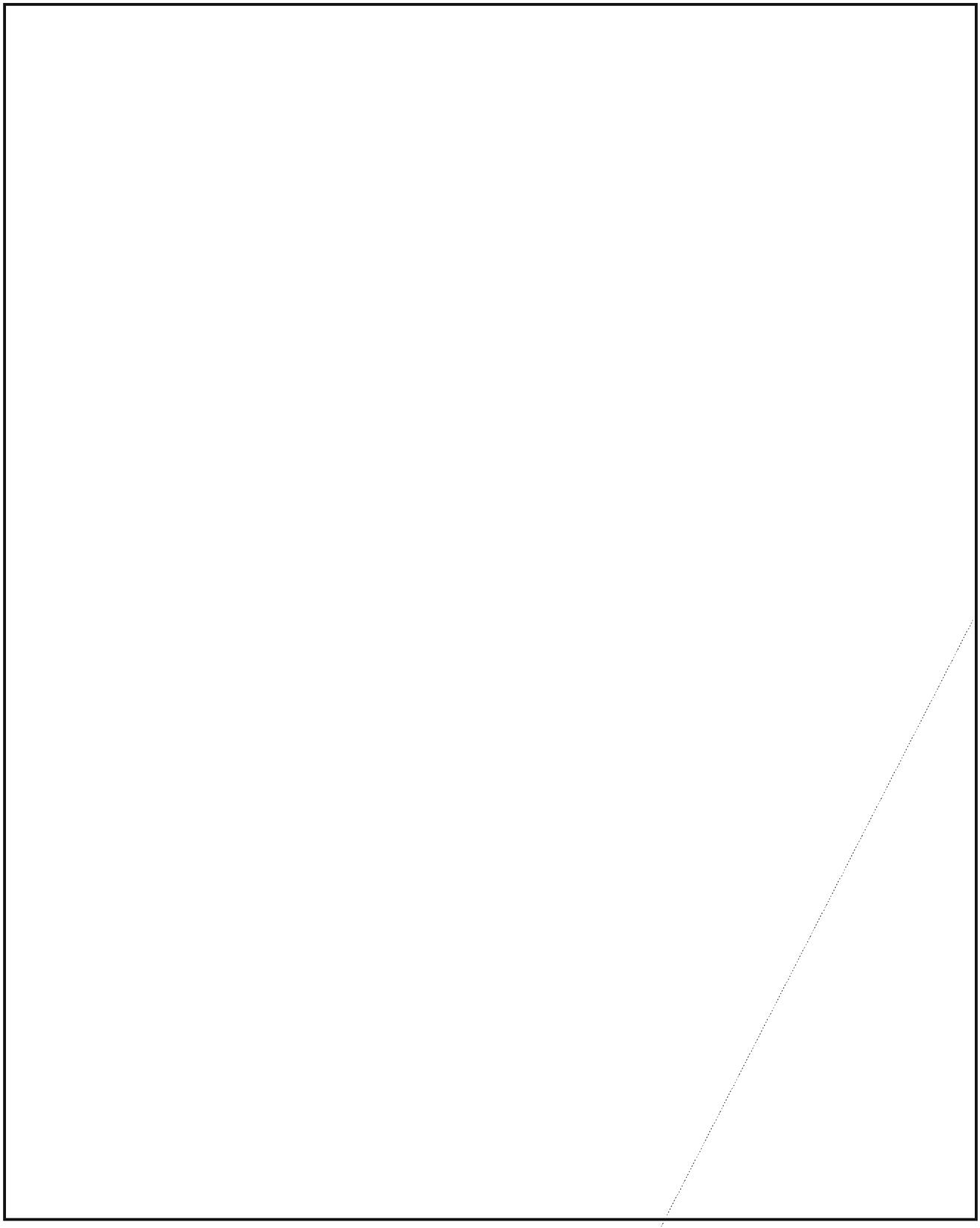
EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36



~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

EO 1.4.(c)
P.L. 86-36

DOCID: 4009705

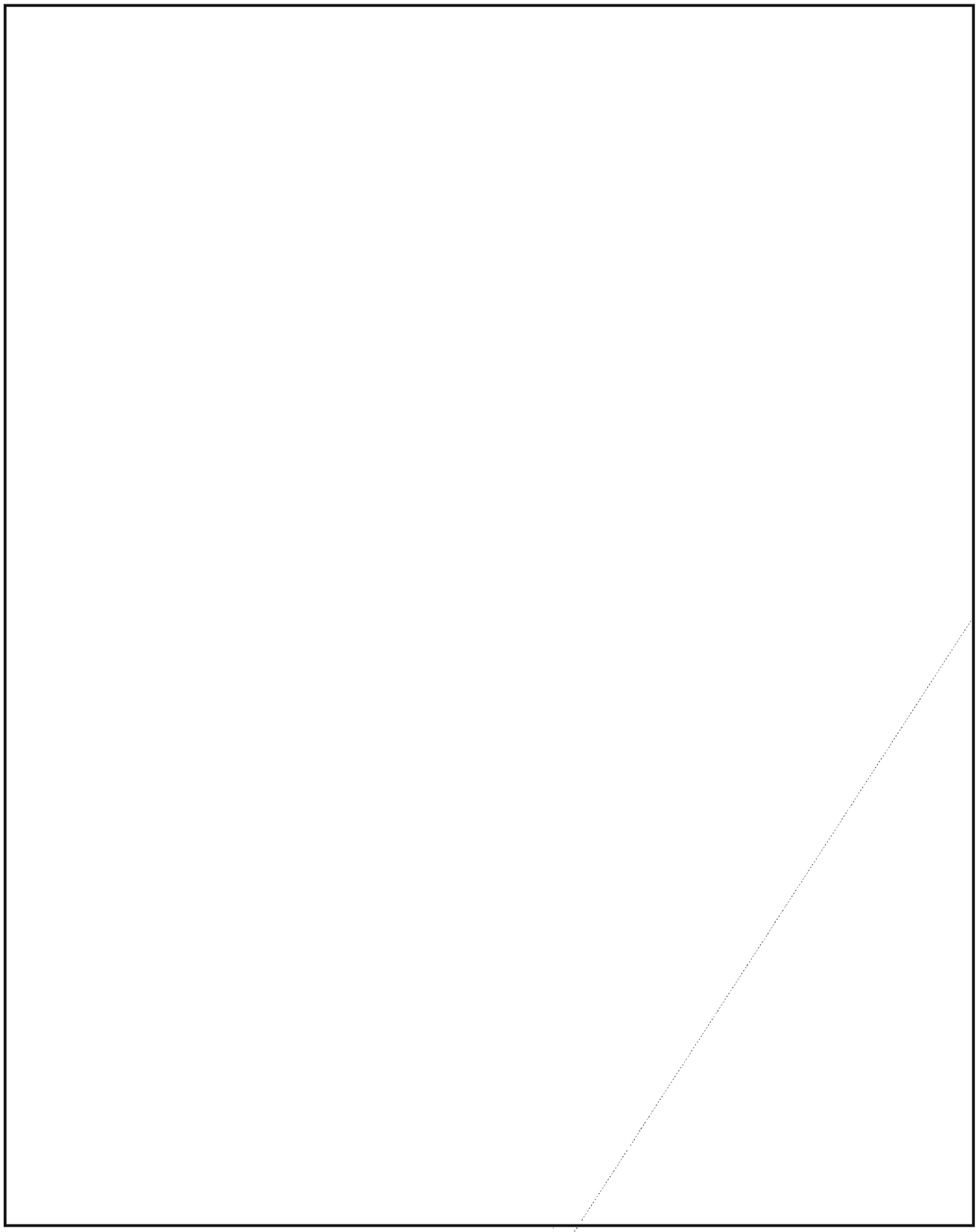
~~SECRET~~

CRYPTANALYSIS & CODE RECOVERY

by MARJORIE MOUNTJOY

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

P.L. 86-36

~~SECRET~~

[redacted]

[redacted]

~~(SECRET/HVCCO)~~

AS WE GO TO PRESS...

(A Note from the Collection Editor)

In a previous issue we explained that the raw material for analysis in NSA is not brought by the tooth fairy but is collected by units and people in the field. We are probably about to be given a graphic demonstration of how important those resources are.

[redacted]

* * *

[redacted]

[redacted]

~~(SECRET/HVCCO)~~

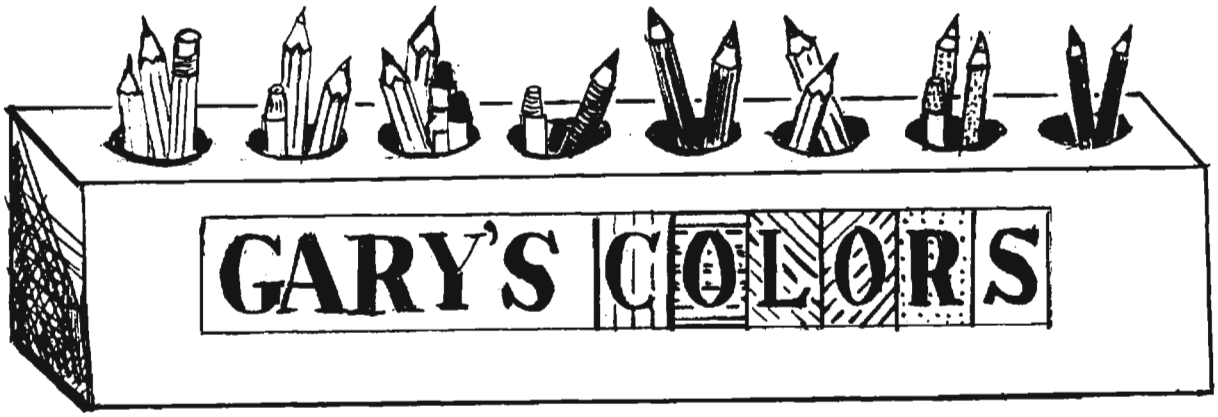
~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

DOCID: 4009705



by Caterino G. Garofalo, P14

Frequently, studies in crypto-traffic analysis require differentiation in the quality of the data being researched. The use of a color scheme in recording the data facilitates such differentiation. I have developed and make use of one which is simple in nature and which my experience has demonstrated to be highly practical. The system uses the colors described below; they were chosen with specific purposes in mind. They permit the visual display of six different qualitative levels, which are also described below.

The colors:

Black - the black carbon #2 pencil has been found to be the best choice for normal usage, suitable both for erasure and longevity.

Green - is the weakest, that is, the lightest density. All of the other colors in the system superimpose on green quite readily.

Red and Blue - are of equal boldness; either can be easily superimposed on both black and green.

Purple - a bolder color which can also be produced by superimposition of red on blue or blue on red.

Brown - is considered to be the boldest of all the colors and the most exclusive and conclusive.

I have found that colored pencils manufactured by different commercial firms vary considerably in hardness, density, and shade. It is desirable, therefore, having started with a particular brand, to continue with it and not intermix brands; this will ensure that distinctiveness and clarity are maintained. Also, once a color scheme is established for a given problem, maintenance of color discipline is mandatory in order to achieve unambiguous continuity of understanding of problem details regardless of changes of the personnel involved in the analytic effort.

The meanings of the colors in my system are as follows:

Color	Qualitative Level	Significance
Brown	5	The ultimate in degree of trueness; not to be questioned. May also represent captured or compromised information or its equivalent.
Purple	4	High in degree of reliability; may be used as a substitute or companion for brown where special conditions of clarity or distinction are vital to the problem. Primarily useful as a final and ordered value enjoying the same general stature as brown.
Blue	3	A relative base value having a significant bearing on the state of recovery.
Red	2	A base of lesser value or no relativeness (completely arbitrary); a necessary first step.
Black	1	To record or log information as it appears in its earliest or original form.
Green	0	Reserved for suspected garbles and for projected or expected but unobserved values (not proven but highly suspected as being correct). Used to alter a meaning or information without obliterating the original (black) form.

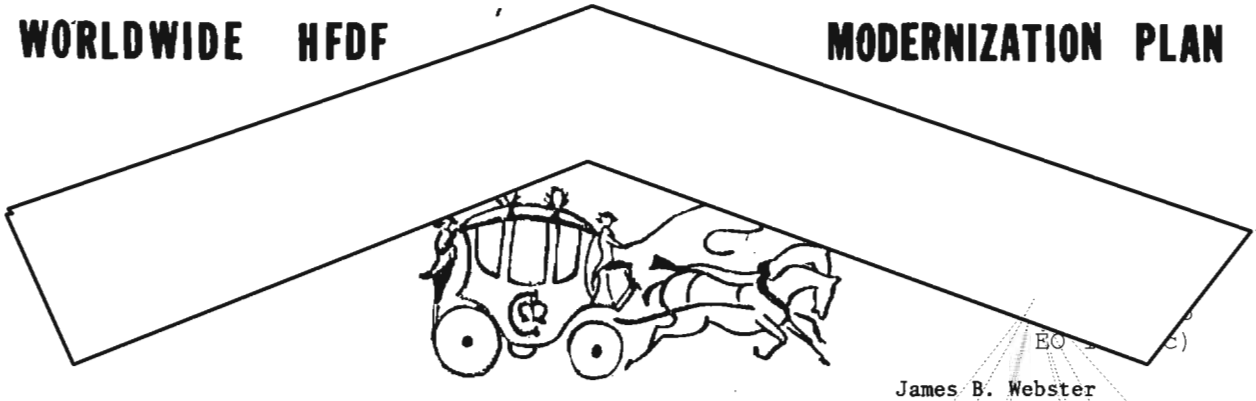
(UNCLASSIFIED)

This article originally appeared under the title "Simplicity in Color" in the October 1971 issue of COMMAND.

DOCID: 4009705

~~SECRET~~

WORLDWIDE HFDF MODERNIZATION PLAN



P.L. 86-36
EO 1.4.(c)

EO 1.4.(c)

James B. Webster

Reprinted by kind permission of the FIELD INFORMATION LETTER

Since the mid 1960's with the advent of the large Circular Disposed Antenna Array (CDAA) sites there has been a continued DOD effort to effect the consolidation and standardization of the US HFDF System. There is an inherent difficulty in consolidating these efforts,

These overall goals of DOD are being realized with the development of . Two programs, are the primary programs which will bring about this interoperable system.

Project is the overall plan to up-grade, modernize and integrate the existing worldwide HFDF facilities. It encompasses a number of the separate projects for improving individual facilities, specific service-upgrade programs and selected actions designed to integrate specific geographic networks. The primary goal of Project is to build an integrated national system to provide for the most modern, accurate and responsive HFDF system possible.

Project will also result in considerable manpower savings and some of these savings have been included in the fiscal planning for fiscal year 1977.

Project includes the following programs:

1. is the outgrowth of the U.S. Army and the U.S. Air Force Resource Change Proposals (RCP) designed to modernize and consolidate their respective HFDF systems.

The plan has a number of operational advantages in addition to manpower savings.

In addition, a common basis for training, procurement and maintenance is provided to the two services.

3. the U.S. Navy's project to modernize the Navy system. It includes automation of many functions now performed manually, thus resulting in extensive

EO 1.4.(c)
P.L. 86-36

P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

~~SECRET~~

P.L. 86-36

DOCID: 4009705

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

manpower savings. This is the largest of the projects [redacted] and is still in the design phase so that details will have to await a future publication.

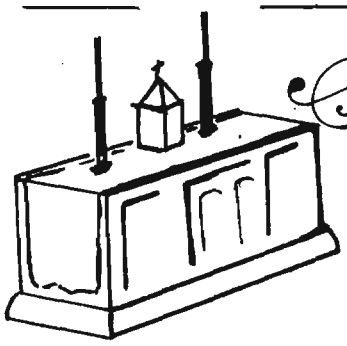
[redacted]

The current plans are for completion of [redacted] in 1980 when [redacted] will be completed. The other projects are scheduled for earlier completion. P.L. 86-36
EO 1.4.(c)

[redacted] is in the beginning stages of development. It presents many engineering and management challenges. As we proceed with its implementation, we will no doubt encounter many obstacles in engineering and operating this system. We feel certain, however, that [redacted] will go a long way toward meeting user requirements for increased numbers and accuracy of target locations.

~~(SECRET)~~

EO 1.4.(c)
EO 1.4.(d)



Secrets of the Altars: THE MOUSTIER CRYPTOGRAMS

[redacted]

Engraved in the stone fronts of two altars in a church in western Belgium are the Moustier Cryptograms--20 short lines of alphabetical text which no one has yet deciphered. Why are they of interest to Cryptolog? The answer to that question lies in an intriguing story that began in the first half of the last century and most recently included a request for help addressed to the Director, National Security Agency.

Professor Jean Connart, who is engaged in writing a history of the town of Moustier, has been trying since 1961 to discover the meaning of the texts. He has sought help from scholars, historians, archeologists, and military cryptologists--Belgian, French, Russian, German, American. All have been intrigued, but none has discovered the key to the cryptograms. The altar inscriptions still hold their secrets.

Early last year, Professor Connart obtained NSA's address from our embassy in Belgium and dispatched to the Director a plea for help. He enclosed photographs and a sketch of the inscriptions (reproduced at the end of this article) together with a number of substitutions he had tried and copies of responses to his similar pleas to others for expert help.

From those who have attempted to solve the puzzle come the following comments:

1. The texts contain a secret message (names of families, benefactors, etc.)

2. There are numerous digraphs (dipthongs) and doubled letters, perhaps represented by the "Greek" letters. (Disputed)

3. The job of the decrypter is to solve a substitution with multiple equivalents for some characters.

4. The underlying language may be Latin, French, Flemish, Spanish, or perhaps even English or German.

Professor Connart included some of his own notes on the history of the region, and these notes may have a bearing on the solution. According to parish records, the church at Moustier was in such dilapidated condition about 1836 that repairs were needed to prevent total ruin of the building. In addition, the winds of November 1836 had taken off part of the roof. In June 1838, some work was undertaken "in accordance with the plans of Philibert Pluvinage and Pierre Joseph Lemaitre. *A stonemason (un tailleur de pierre) received board and lodging for 18 days.*" (Italics Prof. Connart's)

(Continued on page 20)

P.L. 86-36

DOCID: 4009705

LEXICOGRAPHIC CORNER

Some Thoughts on Lexicography

by Stuart H. Buck

Glancing through the latest bulletin of the Mongolia Society, my eye caught the following statement by John Krueger, professor of Altaic studies at Indiana University:

"The worst possible way to make a dictionary, and horribile dictu, the way that nearly all seem to be made, is to make a grand compilation of all existing dictionaries, possibly abridging slightly and adding a few examples. The obvious and ideal way, seldom followed, is to begin with a set of texts, draw from them only the words used in those texts, and create a dictionary out of the actual recorded usage of the literature (or in the case of a spoken dialect, from the noted speech of the speakers). The latter and better course is self-evidently vastly more difficult and time-consuming." [1]

These are the words of a purist. I must admit, however, that they really shook me up---not because I object, in principle, to definitions based on the personal experience and judgment of the lexicographer, but because Professor Krueger's "ideal" seems to me impractical, if not impossible to achieve (at least in a general dictionary). Now I have known John Krueger for almost twenty years, and I have the highest regard for his scholarship. I know also what he was driving at: the habit of so-called "circularity" among compilers of dictionaries, resulting in the perpetuation of ancient errors. Certainly this is a detestable practice, to be avoided if humanly possible. But where does one start? If Professor Krueger is so distrustful of others, where does he expect his lexicographer to acquire the knowledge of a foreign language which will be expert enough to enable him to read through both ancient and modern texts and to select from them the precise meaning of each word? When not reading, he is advised to glean terms from native speakers, presumably in the course of free conversations in their own language. Again, how does he acquire that skill? A modest amount of faith in someone else's judgment seems called for.

Part of the trouble, it seems to me, stems from confusing the role of the compiler of a general, or comprehensive, dictionary with the task of providing suitable "vocabulary lists" for a specific set of texts. Normally, this is the sort of information that the author of a reader provides in his glossary at the end of the book. To expect the lexicographer to wade, by himself, through all the published literature in a particular foreign language must assume that he would have the life expectancy of a Methuselah. Even then he would never quite catch up with the flood of new expressions appearing in the daily press. No, it is just plain unrealistic to expect the lexicographer to "go it alone!"

To be sure, it is flattering to view one's own products as truly independent, free of the slightest taint of plagiarism (that ugly word!). How nice

it would be if we could all operate in an ideal laboratory situation, with all the reference works we would like and quick access to native scholars (who are also bilingual)! All those knotty problems would fall like tenpins. Unfortunately, life is not like that---at least at NSA.

On TV we see the masked surgeon, garbed in his green gown and cap, working away in a germ-free room. There is a muttered command, a gloved hand is thrust out, and just the right instrument plops into it. Everything sterile, efficient, scientific, and prompt. Then we turn to old "Doc" in Gunsmoke, where someone is always getting shot up. No green gown here. The rule is very simple: The bullet has to come out! And Doc does it, rubbing his nose before and after the event. Somehow, his "patients" seem to survive.

Don't get me wrong. I'm not arguing for sloppiness--in lexicography or anything else. I'm merely saying that when there is a job of lexicography to be undertaken at NSA, we can either do it, honestly, as best we can or "leave the bullet in" and suffer the consequences. I heartily agree with John Krueger that there are good and bad ways to compile a dictionary, but I do not share his distaste for the eclectic method. The main thing here is to know your sources. Before you start harvesting words and examples from other dictionaries, find out all you can about each compiler---his background, purpose, method of operating, and reputation among his peers. Distinguish the sturdy oaks from the spindly saplings. I remember one work in particular that impressed me when I was compiling my Tibetan-English dictionary.(2) It was a massive tome, representing almost 50 years of careful research by several generations of conscientious French missionaries in the field.(3) These men were no dilettantes; they were dedicated to the task of spreading the gospel, and the Tibetan language was their means of doing this. Thus, their original word list was constantly tested, retested, corrected, and updated until they were finally satisfied that it was good enough to publish. One would be foolish indeed to ignore such a goldmine of information. The Chinese communists, who conquered Tibet, are also dedicated to a cause. They, too, are obsessed with getting a message across. Moreover, they have the enormous advantage of being on the spot, in control of the educational system. For anyone interested in understanding current Tibetan publications, the necessary clues are to be found in Chinese cribs---or in the special glossaries that accompany translations of Marxist texts. One could spend a lifetime plowing through the Kanjur and Tanjur (i.e., the sacred literature of Old Tibet) and end up incapable of reading editorials---or even telegrams---in this new, ersatz Tibetan.

On the other hand, the lexicographer is bound to run into dictionaries, glossaries, or private files of dubious value. Again, the tipoff is to know something about the author. Was he a "language bum," making quick trips in and out of one language after another? Or was he only interested in one subject: e.g., mathematics, zoology, botany, religion, entomology, ichthyology, folklore, etc.? Where did he get his information? By asking "informants" whose knowledge of English was minimal or who were so anxious to please that they would agree immediately with all his conclusions? I know of one lexicographer who regarded camel drivers as a prime source of information. Well, if camel drivers are anything like truck drivers, I wouldn't put it past them to take a malicious delight in pulling the leg of an inquisitive foreigner.

Now let me get one thing straight: I am unalterably opposed to the notion of a general dictionary as a "dumping ground" for every card file, glossary, or dictionary in sight. I believe that lexicography is primarily a process of

selecting or rejecting information contained in all available lexicographical sources, plus the author's own experience in the language. At this point I agree completely with Professor Krueger that the lexicographer should read extensively in the target language, selecting words, phrases, and examples of usage as he goes along, with special care taken to record the precise source of everything extracted. If challenged, he should be able to say, "That's where I got it. You take a look and tell me what you think!"

It pains me to bring this up, but I think it not unreasonable to assume that the lexicographer is well enough versed in the other language to check his own ideas in native dictionaries. It is one thing to base everything on what a lot of foreigners have said that a particular word means. It might be quite revealing to discover how natives define the same term in their own tongue.

Above all, it is imperative for the lexicographer to know exactly what he is trying to do. Don't leap on your horse and ride off in all directions. Ask yourself, "Why am I compiling this dictionary?" "Who is going to use it---and for what purpose?" "Will it meet the specific needs of NSA linguists?" "Is this the most practical format to follow in order to achieve my stated aim?" Are you trying to please some entrenched clique or other because you are afraid of hostile criticism? If so, you had better forget the whole thing because you are bound to be clobbered by someone---and perhaps unfairly. Life is like that!

You can take your lumps if you believe in what you are doing and give it your very best effort. Remember that you will never have enough time to do as good a job as you would like. Inevitably, your published dictionary will contain mistakes, but don't be dismayed. There will be plenty of kindly souls around to point them out to you. If it turns out that you are wrong, admit it---and thank the person who spotted the error. Also, make sure that an errata list is distributed to all users of the dictionary, under your name. This is vitally important because I insist that the lexicographer must stand back of his product, personally. He can select useful information from any source, but he must form a value judgment on each item selected---and answer for it. This does not guarantee that he will be infallible, but it will keep him honest.

I hope that no one gets the impression that I think that a large, general dictionary should be compiled by one person, single-handed. That is almost too much to expect of mere mortals. The eclectic method, which I support, does not require that all contributors be dead. Considering the magnitude of the task, a joint effort is highly desirable---so long as someone assumes responsibility for the overall product. Also, there is no great virtue in trying to do everything by hand. Make an imaginative use of the computer. Think of it, however, not as an insatiable monster requiring constant feeding, but as a faithful servant who will save you an enormous amount of labor.

(1) The Mongolia Society Bulletin, Vol. XII, Nos. 1-2, 1973, page 53.
(2) Buck, Stuart H., Tibetan-English Dictionary with Supplement, the Catholic University of America Press, Washington, D.C., 1969.
(3) Les Missionnaires Catholique du Thibet, Dictionnaire Thibétain-Latin-Français, Hongkong, 1899.

UNCLASSIFIED

DOCID: 4009705

LANGUAGE IN THE NEWS

by P16

P.L. 86-36

It's quite possible that some of our readers have missed the following items. CRYPTOLOG accordingly relays them as a public service to NSA linguists.

AFRIKAANS: The Union of South Africa recently banned its first Afrikaans book. Government censors had previously banned many books in English but never had occasion to suppress works in Afrikaans, usually because people who wrote in that Dutch-related language stuck to traditional themes or topics approved by the government. However, Andre Brink recently wrote a book called KENNIS VAN DIE AAND (Knowledge of the Night) about a black actor's love for a white girl, his attempts to establish a theater with a message for black people, his torture at the hands of security police, and his conviction for murder. Some people describe the book as "trash" and "evil" while others compare it to Solzhenitsyn's exposes of Stalinist repression. Brink is working on an English translation so you may soon have a chance to judge for yourself.

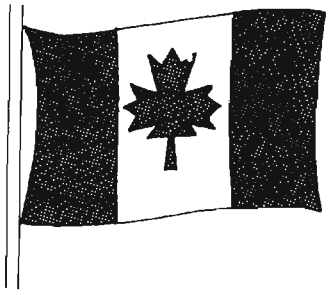
AMERICAN INDIAN LANGUAGES: The Wisconsin Native American Languages Project is an undertaking funded by the Great Lakes Inter-Tribal Council, Inc., to involve speakers of Wisconsin Indian languages (Ojibwa, Potawatomi, Menomini, and Oneida) in the application of linguistics to the analysis, study, and teaching of native American languages.

ARABIC: Is becoming one of the official languages of the United Nations (along with Chinese, English, French, Russian, & Spanish) because several Arab states agreed to meet the entire cost of expenses entailed in installing additional sound booths in all conference rooms and channels for interpreters and the hiring of additional personnel -- $8,300,000 for the next three years.

CHINESE: The government of Hong Kong recently passed a bill making Cantonese Chinese an official language of the Crown Colony, alongside English. Now leaders are busy trying to draw up programs to improve the standards of the language spoken and to get the government to use simple Chinese in its communications with the public (avoiding esoteric and outmoded terms). It has also been suggested that Mandarin should be declared equal in status with Cantonese.

官話

FRENCH: The government of Quebec, after years of controversy and debate, finally proclaimed French the official language of the province. Of Canada's 22 million people, 6 million speak French (5 million in Quebec and the rest in the other 9 provinces). Despite government emphasis that Quebec's 13% English-speaking minority's rights would be respected, many people worried about having their children forced into French-speaking schools. The matter became an issue in last July's election, which bilingual Pierre Eliot Trudeau won.

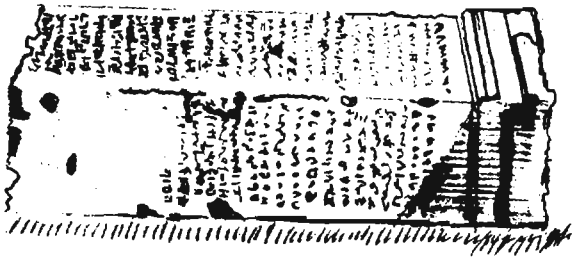


DOCID: 4009705

The French-speaking people of Switzerland's Jura region, after 159 years of trying, finally won a battle for separation from the predominantly German-speaking canton of Bern. The Jura, along the northern border with France, had been attached to the canton of Bern in 1815, but by a surprisingly close vote (36,802 to 34,057) the Jurassiens voted in favor of making Jura Switzerland's 23d canton and the sixth with a French majority. The capital of the new canton will be Delemont.

HEBREW: Many of the babies born in Israel during and right after the October 1973 war were given names connected with the war fronts and Yom Kippur, the day on which hostilities began. Thus, there will be a new crop of Israelis bearing names such as Golan, Golana, Sinai, Sinaya, and Miah (from the initials of the phrase MILCHEMET YOM HADIN, War of the Day of Judgment). Since the cease-fire brought about by the shuttle diplomacy of the US Secretary of State, a number of newborn Israeli baby boys have been named Henry Kissinger Cohen, Henry Kissinger Goldberg, etc.

LYCIAN: An archeological team recently unearthed a 4-foot, 4-faced limestone tablet in southern Turkey with inscriptions in Lycian, Aramaic, and Greek. Scientists have compared the find to the Rosetta Stone because with it they may be able to unlock the mysteries of Lycian, an Indo-European language spoken in southwestern Asia Minor back in the 5th and 4th centuries BC.

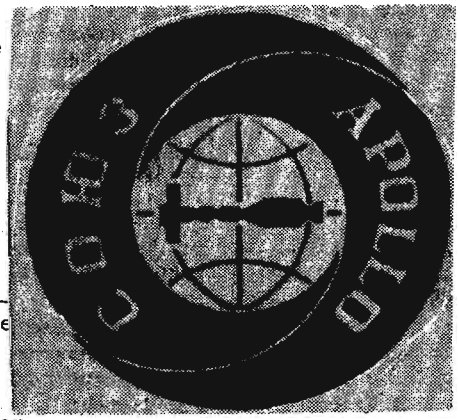


POLISH: When Archbishop Agostino Casaroli, Vatican Secretary of State, went to Warsaw to confer with the Polish Foreign Minister, it led to speculation that diplomatic relations may soon be resumed. The Archbishop even spoke some Polish while there. "Let God guard Poland and lead it to great and happy goals," he said, adding "NIECH ZYJE POLSKA!" ("Long live Poland!")

SPANISH: Mexico City's mayor thought "it was getting so one couldn't tell whether one was in Mexico or Manhattan" so he banned English-language commercial signs in an area visited largely by American tourists. The mayor might have experienced the same disorientation of locale had he toured Manhattan's Spanish-speaking upper East Side.

SPANISH AND PORTUGUESE: The Library of Congress recently issued a document entitled Latin America, Spain and Portugal: An Annotated Bibliography of Paperback Books, a list of 1,512 inexpensive paperbacks currently available. It supersedes an earlier (1967) bibliography that was restricted to Latin American works and includes travel guides, grammars, readers, dictionaries, and textbooks (Spanish & Portuguese). The cost is a mere 75¢ and you can order it from the Superintendent of Documents, Washington, DC, 20402.

RUSSIAN: The emblem chosen for the patch to be worn by the astronauts participating in the joint US-Soviet space mission in 1975 will include Cyrillic lettering. The Russian word SOYUZ (union, unity) will appear on it, along with the English word APOLLO. The mission names will encircle a drawing of the two spacecraft docked together above the world.



SWAHILI: Kajiga Balibutu, a priest in the African country of Zaire (formerly the Belgian Congo), recently completed and published a 700-page Swahili dictionary. Unfortunately, the report from Azap (the Zairese news agency) didn't specify whether the work was a bilingual dictionary or was entirely in Swahili, but our guess is the latter.

DOCID: 4009705

A LONG HARD LOOK AT THE Intern Program

by 'Anne Exinterne'

In 1965 NSA started an Intern Program designed, according to the Personnel Management Manual, "to provide the quantity and quality of professional personnel required to perform effectively the professional work functions of the Agency." The PPM further states:

> "An intern program provides the mechanism through which an annual input of pre-professional personnel with appropriate qualifications will be broadly trained in line with current and projected needs of the Agency as well as the participants' immediate and long-range career goals. The goal of each intern program is to assure that high-quality pre-professionals are carefully selected, initially trained, and given a proper variety of job assignments to prepare them for filling professional positions in a particular career field."

In view of the budget cuts that the Agency has taken in recent years and the resultant restrictions in hiring, a Special Task Force was appointed last year to study the intern program and to recommend whether it should or should not be continued. While I would not disagree with their recommendations that it should be continued, I would recommend certain changes on the basis of my experience as an intern and graduate.

Promulgation of Program Philosophy

I do not believe that many of the interns or line supervisors are aware of the intern program philosophy as it is stated in the PMM. In fact, I had never read that description before I began this paper, and I doubt that the recruiters who interviewed me and some of my contemporaries had read it.

The version that we heard went something like this: "Most of the Agency's top managers will be eligible for retirement in the early 70's. The Intern Program was created when the Agency realized that bright young people would be needed to fill the gaps left by these retirements."

Now, not even in our naive and brash youth did many of us imagine that managers from Dr. Tordella on down would anoint us to be their successors, but it did seem that we were going to be groomed for great things; and some of the first interns accordingly dubbed themselves "FSG's": "Future Super-Grades."

It was not too long, however, before hints of reality began to creep into this rose-colored picture. For one thing, if this was to be a management-training program, where were the management courses? Most panels do not require any management courses; some include one; and none, so far as I know, make an attempt to include on-the-job training in management. For another thing, while the panels have often referred to interns as a "select" group, as does the PMM description, their sheer numbers discount claims of much selectivity: to date, over fifteen hundred interns have entered the program.

I concluded some time ago that the real purpose of the program was to train new hires of average or slightly above-average potential to be competent technically in one of the Agency's career fields. I say "average or slightly above" because the admission requirements of most of the panels require a Staten score of 5 in the appropriate CQB (Career Qualification Battery) category. Such a score indicates what the Personal Management Manual describes as "average test performance" and would place that person in the middle of a bell-curve distribution of test scores. (As a predictor of success in that field, it indicates that the person has approximately a 55 percent chance of performing above the average for a total test group composed of all NSA employees and applicants.) If I had a lot of faith in CQB scores as predictors of success and did view the intern program as a highly selective one, I would require a Staten of 7 in the appropriate category, indicating that the candidate's performance was "distinctly above average" and that he had scored better than 84 percent of the people taking the test.

It seems that the PMM statement about the program's supplying input to career fields "based on current and projected needs" was not taken very seriously by the panels or by the operational elements. If it had been, would the Agency now be faced with the current skill imbalance? Some of the operational elements tended to use the intern program as a "billet savings bank" which could be added to or taken from as other needs dictated. Since then, direct control over those billets has been taken from them. Unfortunately, however, it appears that panels are still being encouraged to supply graduates for fields currently over strength. The Study Group which reviewed the program last year recommended that "interns currently in the program /who are/ training for skills that are in excess in the new TD be immediately evalu-

DOCID: 4009705

ated by ADPS for redirection to other career fields where vacancies exist." Instead of redirecting interns in such programs, M3 is continuing to recruit new hires for overstrength fields, on the theory that "every field needs new blood." How will these new hires react to the knowledge that they are being trained for a field in which the Agency already has a surplus of personnel and that they may be without a billet when they graduate, or that after spending three years in training for one field they may be asked to retrain in another?

After nine years of program operation, it is time to make sure that recruiters, supervisors, interns and panel members have a common and realistic picture of the program philosophy.

Recruitment

If I were recruiting for NSA I would, first of all, recruit high school graduates for many of the jobs now identified for college graduates. There are many jobs at NSA which involve very routine procedures, and in the past there has been a tendency to use college graduates for some of these jobs. The philosophy behind this may have been that they would be more alert to new techniques that could be used, but I suspect it was more likely the result of the now-fading obsession with hiring college graduates for all jobs. But just as the outside world has come to appreciate the importance of the trade and technical school graduate, the Agency shows signs of beginning to appreciate the high school graduate. It is time to take a close look at some of our jobs and determine exactly how complex the duties are and what type of educational background really is needed.

As far as college graduates are concerned, where there are people already trained on the outside, I would hire those people rather than trying to create a data systems analyst out of a psychology major, and I would not try to fashion an Arabic linguist out of an English major until I had checked to see if some of the linguists that Uncle Sam had trained and then turned loose were interested in Agency employment. Nor would I hire a person because he had a specific skill and then give him an option to use or not to use that skill. A friend of mine scored straight 7's on a scale of 9 on the Russian test, but when she came on board she was given a choice of several internships and selected Data Systems; a military convertee who had been trained in two scarce-skill languages at Uncle Sam's expense entered the Special Research Program. I don't mean to imply that if you are hired in one field you should be required to spend the next 30 years in that field, but I think you should at least be initially assigned to a position that makes use of your background.

(A note on military personnel who wish to convert: I have known a number of such people who had a sincere interest in converting but were reluctant to try because of the polygraph. Since the polygraph is forbidding even to people like me who were raised in a rather protected pre-drug, pre-coed-dorm environment, and have backgrounds that could probably be checked out in an afternoon, it is not surprising that men and women who have been in the military and who have not been in such a protected environment should have considerably more qualms about it. Other than drugs and sex, a major problem seems to concern the discussion of classified material. Although supergrades can be heard discussing such material in the halls--and if the tables at the "602" could talk, KGB agents would probably feel guilty about collecting their checks--civilians, with but rare exceptions, do not have to face the polygraph again. However, the enlisted man who wants to convert knows that he will be asked something to the effect, "Did you ever divulge classified information?" While he knows that he has not divulged it to unauthorized persons, he also knows that his mind will go back to conversations in the NCO club in Turkey or the NSA cafeteria that M5 would not have endorsed, and suspects that he will react to the question. I think that M5 must be realistic in dealing with such people, as compared with college hires who have only been exposed to classified material via James Bond. Perhaps they are realistic--but the potential convertees do not know that, so some elect not even to try to convert.)

Related subject: I suspect that the testing battery and other screening devices used by M may be producing a population that is too homogeneous. Well-rounded people are good company, but people with a bias in one direction often provide the spark that "all round good fellows" cannot. Does it really matter if a superb linguist almost did not graduate because of trouble with math? Or that a computer whiz would never pass a Dale Carnegie course? Or that a first-rate signals analyst has problems with grammar and a girl in every port?

Admittedly we cannot have thousands of brilliant but querulous technicians, but there must be a middle ground, and this is where personality and aptitude tests could be put to better use. It would be worthwhile, for instance, to give the Minnesota Multiphasic Personality Inventory, the Kuder Occupational Preference Test, and others, to a hundred outstanding crypt- analysts, traffic analysts, linguists, etc.; there is a very good chance that personality patterns associated each profession would emerge. The Agency relies heavily on aptitude tests, but the fact that a person scored well on the language aptitude test does not necessarily mean that he will be a good transcriber--that he has the temperament that will enable him to sit at a position eight hours a day with earphones on.

DOCID: 4009705

Such tests would be especially helpful in evaluting liberal arts graduates. I am told that in the early years of the program about one college recruit in five expressed an interest in personnel work -- usually because he was disenchanted with his assigned field. Naturally Personnel cannot absorb all those interested. I do not think this disenchantment with the technical side of NSA is unusual or surprising considering the number of liberal arts graduates with no directly related skills who are recruited. Many of the people who came in with me had majored in English, History, Political Science, Psychology and Sociology, and had a bent of mind that is not needed or even useful here. To me and my friends, for instance, numbers that show attrition rates by college major would be fascinating, whereas numbers that show a station's frequency usage for the month would not. It is true that we can cultivate an interest in this, just as we can learn to take frequency counts, but the traffic analyst or the cryptanalyst needs a special insight or interest that we do not have, and the Agency would be better off training someone whose natural bent is in that direction.

The recruiter who interviewed me made a rather feeble attempt to see if I had the type of personality required for CA work by asking if I liked crossword puzzles. "Sure!" was my enthusiastic reply. Much later, when I really thought about that question and understood why it was asked, I realized that I hadn't worked a crossword puzzle since the eighth grade, but I wasn't consciously lying when I gave that answer; I think you will find that a recent college graduate who is jobless has an open-minded interest in almost anything that seems to interest the interviewer.

If he had asked, "When was the last time you worked a crossword puzzle from start to finish?" and "Have you ever tried to figure out what was wrong with the family radio when it didn't work?" he might have gotten a closer indication of where I would--and more important --where I would not fit in at NSA. The Agency could devise a preference test to determine what interests applicants have that might suggest an adaptability for NSA professions (e.g., "Rank the following subjects in the order in which you would prefer to take them: Translation, Math, English, Philosophy, Psychology, Programming, Music, Sociology").

It would also be helpful to ask the potential employees what they think they might be doing at NSA, based on knowledge of the Agency they have acquired through open-source publications, etc. Like many recruits I had a mistaken notion of what I might do at the Agency. I thought I would probably be researching and preparing biographies on foreign personalities. After hearing my idea (had he asked) the recruiter probably would have been wise to refer me to CIA.

In some ways the recent budget cuts almost have a bright side so far as recruiting is concerned. The Agency no longer needs droves of new employees. As result there is no reason why an applicant should be hired who is not exactly the type of person we want and need. The number of college seniors taking the Professional Qualification Test, the Agency's first screening tool, was still high the last time I heard, the job market is tight, and NSA offers a good starting salary, so there is no reason why we should settle for second choices.

(Next issue: Selection and Orientation)

(UNCLASSIFIED)

* * * * * * * *

AN EDITORIAL NOTE:

We in NSA have had too little discussion--in print--of controversial issues, and it is easy to see why. In the world at large the writer on serious questions works with considerable freedom. Subject only to his conscience and the demands of truth, he can hew to the line and let the chips fall where they may. In NSA, however, we are a closed community; the "line" runs close to home, and the chips inevitably fall on our colleagues, our chiefs, ourselves.

This is a great inhibitor of comment and correction. If it were only possible (we have all thought at some time) to discuss the problem apart from the people! But even if I am willing to take the consequences of my words, and the icy wind that may thereafter blow from the front office, it will look as if I'm getting at Phil or Liz, and I don't want that at all.

To alleviate this situation, CRYPTOLOG invites informed and thoughtful discussions of current issues, with or without an author's pseudonym. (As explained on page 21, and as required by all serious publications, the writer must identify himself to the editor, but may request anonymity in print.)

So give your country the benefit of your views!

DOCID: 4009705

Department of Golden Oldies

King Eusyb & Queen Deodi

(c. 1961) [redacted] P.L. 86-36

Once upon a time there was a rich and generous king named Eusyb, who dwelt in a tower of purest ivory. He had one weakness--an inordinate craving for rich pastries of all sorts, but especially for dark brown devil's-food cake with thick fudge frosting, which he demanded every Friday morning promptly at 0830 hours (with occasional samples on other days); and he insisted that some always be available in the event that unexpected visitors should call.

Queen Deodi handled the funds, and she was very frugal. The royal baker, Durensi, found it most difficult to stay within the budget because of King Eusyb's weakness. He sent his assistants to faraway lands to obtain the exotic materials needed for these confections, and some of them were so closely held by their owners that they could not be purchased at any price. But Durensi and his assistants were faithful servants and they frequently obtained the needed goodies by stealth. The scarcest commodity was cocoa, which was needed to produce King Eusyb's favorite, that dark brown devil's food cake. Unfortunately, the entire world's production was controlled by the wicked King of the North, Ivan the Awful, who jealously guarded his shipments, and disguised the cocoa beans in every possible way. He went to such lengths that Durensi and his men would sometimes find a single bean hidden in a whole wagonload of garbage.

So Durensi's assistants started intercepting all the garbage shipments they could find and sending them home to their own land to be sifted through; and all went well until Deodi got wind of the project. She was very wroth, and told poor Durensi that he must not waste his funds in this way or she would reduce his budget. Durensi explained that he was only searching for cocoa beans to prepare King Eusyb's favorite dish, and the Queen finally relented. However, she told Durensi that he must not keep so much garbage in the royal castle, and that his assistants must sift it as close as possible to the point of intercept, sending home only the goodies which they found.

Durensi complied, but he was sorely troubled. He had spent a long time and had invested much money in equipment and training; now he was fearful lest he lose technical continuity, forget how to sort garbage, and lose the assistants he had trained to run the complicated sifters, sorters, slicers, dicers and ricers. He explained the predicament to his staff, who made the following recommendations: (1) Move the bakery farther away from Deodi's chambers, (2) use some of the garbage which had been closely associated with cocoa beans as a cocoa substitute when there was not enough of the real thing available, (3) convince the Queen that the men in faraway places did not have the equipment or the technical ability to extract the goodies from the garbage, and (4) demonstrate to King Eusyb that, by noting the type and quantity of garbage collected, the time and place of collection, the direction of travel and mode of transportation, it would be possible to keep tabs on the disposition of King Ivan's cocoa caravans.

Durensi was persuasive, and before long all these things were done. A new bakery was erected, far from Deodi's chambers, hidden in the wilderness where only the most loyal and dedicated assistants were willing to travel. Fresh garbage began to arrive and soon the vast storage and processing areas were full to overflowing.

But Deodi became very upset as Durensi hired more and more assistants. She suspected that much of the sifting was not producing any goodies, and was being done only to keep the helpers on the payroll. So Durensi hit upon another scheme: he would get a superduper sifter/sorter/slicer/dicer/ricer which would sift, sort, slice, dice, and rice a hundred times as much, automatically, as all his manual sifters, sorters, etc., were capable of doing. This would not only produce more cocoa beans, it would reduce the tremendous backlog of garbage and prevent its building up in the future.

King Eusyb, with visions of devil's-food cake with thick fudge frosting dancing in his head, heartily endorsed the plan. Deodi, too, was delighted, seeing not only an opportunity to get rid of the accumulated garbage but also to reduce the number of manual sifter, sorters, slicers, dicers, and ricers in the bakery. But just when it seemed that Durensi's troubles were over, he suddenly found himself worse off than ever. Queen Deodi told him that he could not hire and train people to operate the new

DOCID: 4009705

equipment because he already had more assistants than he really needed. At the same time King Eusyb would tolerate no lag in the production of devil's-food cake.

More garbage kept flowing in. In desperation Durensi took some of his more experienced workers off their jobs to train on the new equipment. It was not enough. The new equipment required more and more workers as it approached the operational stage. This cut deeper and deeper into current production, and the garbage collected faster than ever. One day Durensi and all of his helpers were smothered under an avalanche of garbage.

Not long afterward, unexpected visitors arrived at the castle. They were King Ivan the Awful and his warriors. Just as they approached, Queen Deodi was murmuring comfortably to her husband, "You know, dear, our budget has certainly stretched a lot further since we got rid of Durensi and his smelly crew."

(UNCLASSIFIED)

Secrets of the Altars

(from p. 10)

In spite of these repairs, the church was (c.1840?) in such poor condition that part of it collapsed when the roof was raised. The contractors had to rebuild the choir and the side chapels (where the altars are) from the ground up.

There is a published report (Moulart, *Basecles; Esquisse religieuse)* that the ancient altar of St. Martin was sold or offered for sale at Basecles in 1843. Basecles, a Belgian town near the French border, contains the Church of St. Martin which dates from 1779 and is considered the best product of the Tournai School. Does the Moustier St. Martin's altar come from Basecles? Were both it and the Virgin's altar constructed in 1843? Or does only the stone-cutting date from that time? Answers to these questions could have a bearing on the date of the Moustier cryptograms and their underlying message.

Like to try your hand at this puzzle? Send your proposed solution to the Editor who will pass it on to the Oglethorpe Team which handles such problems for the Agency. Cryptolog hopes to publish in a future issue an article about the workings of that group, which some of us have heard of and some have not.

Meanwhile, here are the inscriptions. Good Luck!

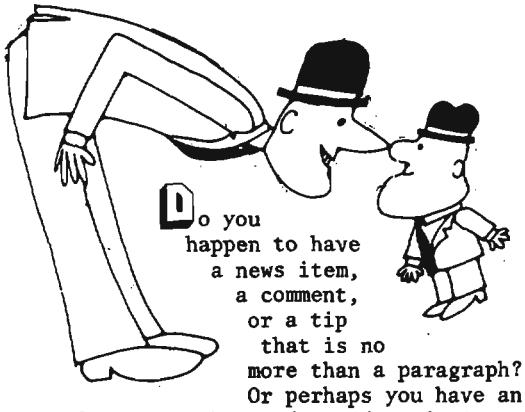
(UNCLASSIFIED)

St. Martin's Altar

The Virgin's Altar

DOCID: 4009705

Contributions Solicited

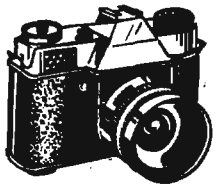


Do you happen to have a news item, a comment, or a tip that is no more than a paragraph? Or perhaps you have an article of several thousands words...? Long or short, if it has something worthwhile to say, we'll print it. (For your interest and guidance, one page of typescript, double-spaced, makes about one column in CRYPTOLOG.)

First-person articles or stories about your own experiences are welcome, so long as they relate to our work. (See "Busman's Holiday" in the August issue.)

Want anonymity? A thoughtful piece on a subject of interest to many readers will be considered for anonymous publication, if the writer requests it. (The writer must, however, identify himself to the editor in an accompanying note or by a personal call.) Needless to say, personal or trivial complaints will not be considered.

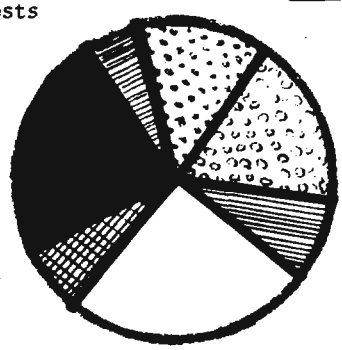
Photographic illustrations can be reproduced, at the same quality as those in the NSA Newsletter.



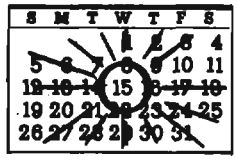
Sensitive materials? No. We'll go all the way to Top Secret Codeword, but we have to draw the line at compartmented or otherwise exlusive sources.

Your contribution does not have to be typed; we'll give preference to content over form, every time. (Though, especially in the case of a long piece, the editorial eye will appreciate any effort you can make in that direction--garbles and strikeovers freely forgiven.)

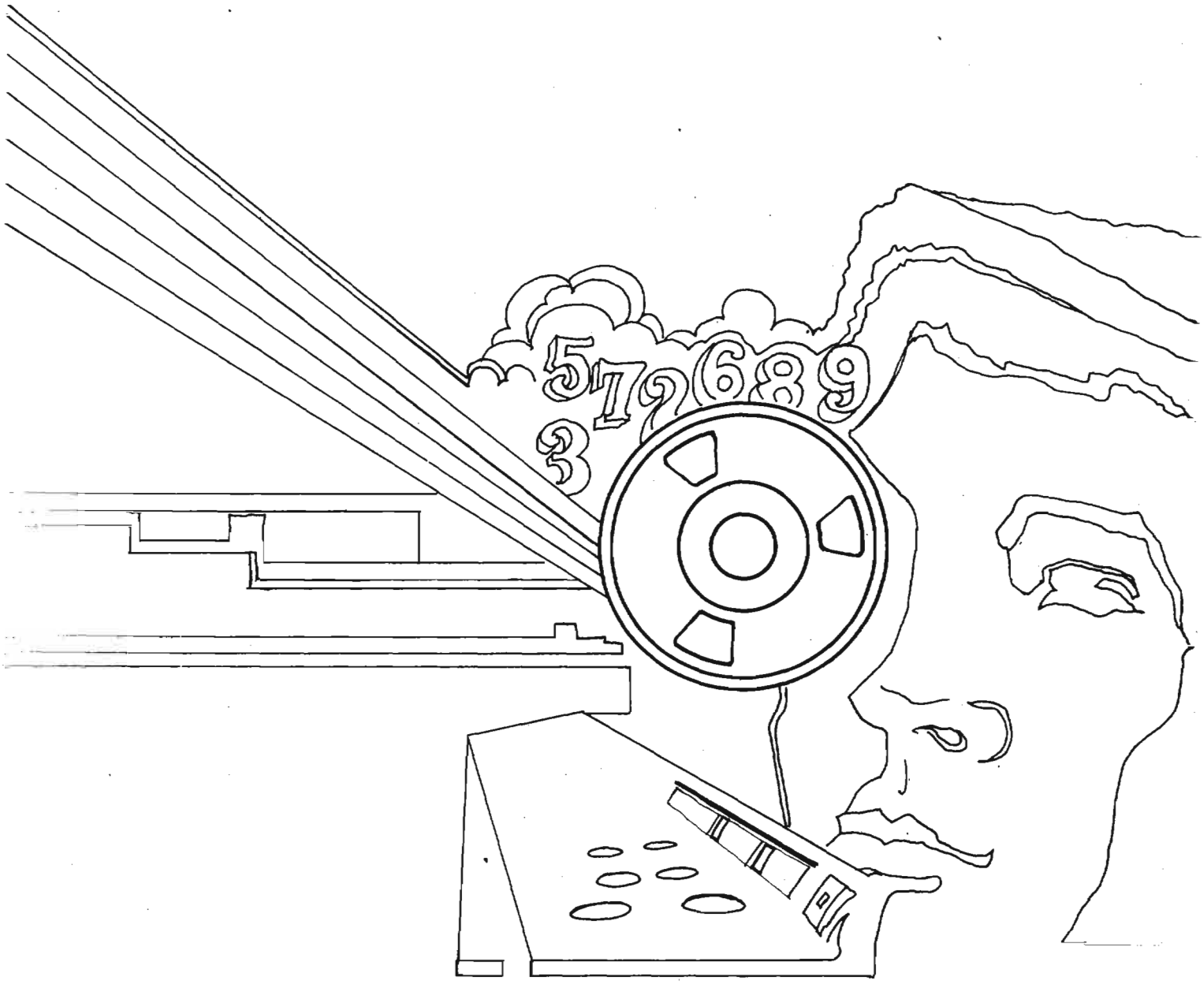
Something missing? If you feel that your work or your interests are not being well represented in CRYPTOLOG, it's probably because you and your friends are not contributing. The editors earnestly want to cover the whole territory, but articles don't grow on trees, y'know! Somebody (who knows the subject matter) has to write them.



Need assistance? You may have an idea, or some notes, or even a half-finished paper that you feel has possibilities but you don't quite know what to do with. A call to the appropriate departmental editor will get you a "story conference" and possibly inspire you to finish it up and get it into print.



Our deadline is theoretically the middle of the month (the 15th of August, for publication in October, and so on), but don't let that stop you if something good comes along on the 16th. And anyhow, this is a monthly publication; if you miss this month's deadline you'll be just in time for next month's CRYPTOLOG. See you!


5726893

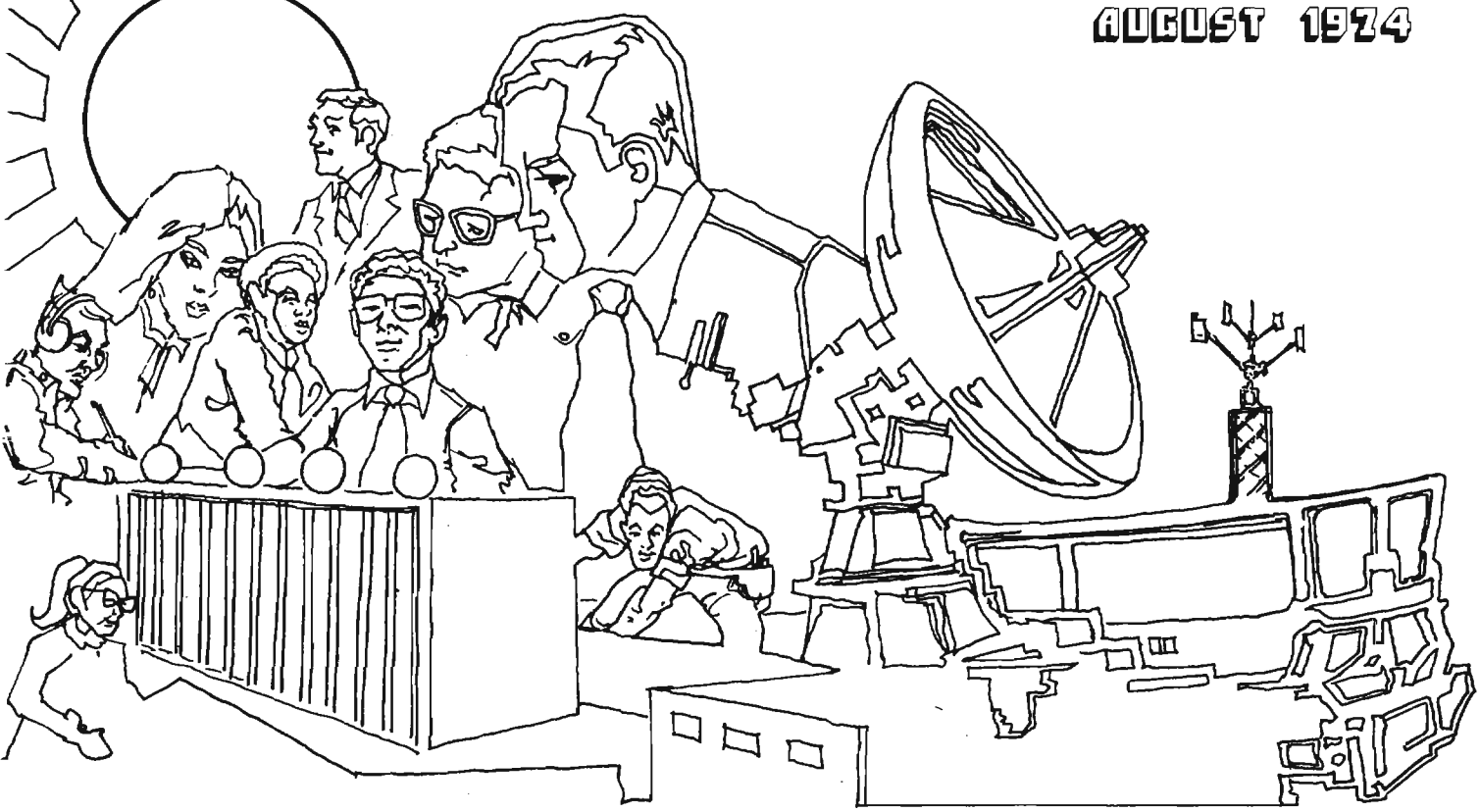
DOCID: 4009704

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

VOLUME I NUMBER I
AUGUST 1974



A LETTER OF INTRODUCTION.....General Wolff..... 1
WHAT IS A COLLECTOR?..... [redacted] 2
THE TEXTA DATA BASE.....William J. Jackson..... 4
WHAT SHOULD YOU EXPECT FROM CRYPTANALYSTS?..... [redacted] 5
A SPOT BY ANY OTHER NAME.....Vera R. Filby..... 7
THE NEW TRAFFIC ANALYSIS GLOSSARY..... 8
THE LANGUAGE OF "BEISBOL"... [redacted] & R. Santiago-Ortiz.....11
RIGHT-TO-LEFT TEXT SORTS ARE NOT IMPOSSIBLE..... [redacted] 14
SELF-PACED INSTRUCTION: THE FUTURE IS NOW... [redacted] 15
A SHORT DIRECTORY OF CAREER PANELS.....17
BUSMAN'S HOLIDAY.....Barbara Dudley.....18
DEPARTMENT OF GOLDEN OLDIES..... [redacted] 20
CALLING ALL SRA'S: REPORTING SYMPOSIUM?..... [redacted] 20
PRIZES AND HONORS FROM THE LEARNED ORGANIZATIONS.....21

~~Classified by DIRNSA (NSAM 123-2)~~
~~Exempt from GDS, EO 11652, Cat. 2~~
~~Declas Date Cannot Be Determined~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

P.L. 86-36

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

DOCID: 4009704

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL.I, NO.1 AUGUST 1974

PUBLISHER WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief ..... Doris Miller (5642s)
Collection..... [redacted] (4410s)
Cryptanalysis..... [redacted] (3215s)
Language..... [redacted] (5236s)
Machine Support..... [redacted] (3321s)
Special Research..... Vera R. Filby (7119s)
Traffic Analysis..... William J. Jackson, Jr. (3369s)

Art Editor..... [redacted]

P.L. 86-36

* * * * *

~~TOP SECRET~~

DOCID: 4009704

~~CONFIDENTIAL~~

A LETTER OF INTRODUCTION

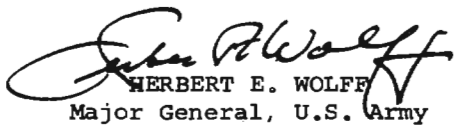
This is CRYPTOLOG -- a new vehicle for the interchange of ideas on technical subjects in Operations.

Operations is a large organization; the skills and talents on which we depend are many, our workings widely scattered and often sequestered in compartments. These conditions argue for special efforts to keep us in touch with each other and with new problems as they arise and new solutions as they are developed.

In the past this need has been partially met by a number of small specialized magazines, some keyed to a given sector of Operations (as Dragonseeds to B Group, Keyword to G) and some to subject matter (as QRL to language and Command to traffic analysis and special research). Not all areas and disciplines were thus represented, however, and distribution of the existing vehicles was limited.

It is to improve this situation that CRYPTOLOG, combining the resources of the above-mentioned vehicles, has been established. I count on it to provide all the good effects of its predecessor publications, plus additional ones. As a monthly it can be more responsive than the quarterlies and bi-monthlies it replaces. Because it is Operations-wide it can embrace all our disciplines and address all our people. Its classification, up to and including Top Secret Codeword, permits discussion of very specific subjects in the cryptologic sphere, and its level of informal exchange invites short articles and letters on any subject.

To be successful, CRYPTOLOG must reflect current operational topics in a way that interests you and others. I hope that you will want to read it and will help to write it.



HERBERT E. WOLFF
Major General, U.S. Army
Deputy Director, Operations
NSA, CSS

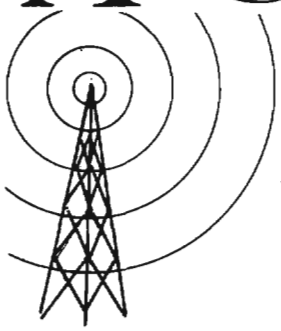
~~CONFIDENTIAL~~

DOCID: 4009704

WHAT IS A COLLECTOR?

by [redacted]

P.L. 86-36



If you have looked at the masthead of this magazine you will have seen that the various members of the editorial board represent different disciplines. When seen in life, nobody has trouble distinguishing among these disciplines: everyone knows that traffic analysts are clear-eyed, clean-limbed people who draw meticulously neat--if arcane--squares and circles on paper, and that cryppies are two-headed people who tend to twitch. The machine people are those pale ones who inhabit, like troglodytes, the bowels of the basement. Collectors are--uh--aren't they the can-clangers who come around three times a week with a truck?

Collectors are a strange breed. Outside of the National Security Agency and a few other agencies with which we deal it would be a hopeless undertaking to try to explain them. It will not be easy explaining them to people who should know.

Personnel assigned to NSA in billets identified with a Career Occupational Specialty Code in the 1600 series are collectors. That is one way to identify them, but not a very effective way. Agency employees don't have their COSC's stamped on their foreheads. Let's look at this another way. What do collectors do? Well, you know those pieces of traffic that traffic analysts analyze? They were collected by collectors. In fact, a number of collectors working in concert got the analyst his piece of traffic.

Somebody downtown decided that we could not go another minute without finding out what the Zendian Army's 279th Underground Balloon Battalion was up to. Then somebody important in NSA, in V5 as a matter of fact, agreed that this was a valid requirement, translated this demand into NSA-ese and tasked one of (presumably the appropriate) elements in DDO. (When translated, the task becomes, "Find out what the 279th Underground Balloon Battalion of the Zendian Army is up to." Actually, by this time it will be known as the 279th UBB, and as it is a pronounceable acronym, it will be pronounced.[1] The neophyte who has to ask "What's UBB?" may receive a polite if patronizing explanation. More likely, however, the response will be, "Not much, what's ubb with you?")

Enter the first collector, the collection manager in the office of primary concern--in this case, whichever office is responsible for Zendia. He will say something like, "Gee whiz![2] I already have 47 cases on each position I own and the bottom 45 in the priorder don't get heard now!" (The cases are listed in priority order, and having too many cases on too few positions is a chronic problem.) To assign this new task in such a way that it may have a chance of being heard, he may take his entire mission apart, shuffle it around and rewrite every assignment. He has a good idea of what may be heard where, what kind of equipment he needs to do which jobs at which sites, what book of rules he has to consult to render a simple requirement incomprehensible to anybody who doesn't own a copy of the same book of rules, and what he has available to do the job with. Additionally, it serves him well to know what other managers have and what they need, in case a trade is necessary. Finally, he has to know where he can get help if he has to have it in order to satisfy the requirement.

After the details are worked out and the task is converted to a Collection Control Message (CONMSG) or a Signals Collection Objectives List (SCOL) or whatever happens to be currently fashionable, it goes to the site or sites where the actual collection will take place. Another collector receives the task and tries to translate it back to English. His title may vary from station to station, service to service, but his function is to manage the collection resources at his station. He is intimately aware of the capabilities in his station, he knows what talent is available, what conditions his resources are in, where he can cram the mission in--specific instructions from the manager at NSA notwithstanding--and, often, what rules he has to break or instructions he has to ignore in order to get the job done. (Incidentally, we at Fort Meade have absolutely no idea that he is breaking rules or ignoring instructions in order to get the traffic to us--as long as he gets it to us.)

DOCID: 4009704

Now the mission is in the hands of the operator. His is the real collection function. He finds the signal that the Zendian UBB 279 is using to convey whatever it is they are conveying, he records in some way the signal itself and information about it. That is, if it is a Morse signal, he copies what the Zendians are saying to each other. When the signal is weak and atmospheric conditions are not conducive to facile copying, the Morse operator sometimes mutters "Tut!" or even "Darn!"

In addition to copying the signal, he records on his logs such information as the frequency it is operating on, the time it is active and other ancillary information from which predictions may be made about future activity.

If the signal is non-Morse the operator must determine what the nature of it is and manipulate machinery to copy it, but the principle is the same.

The collectors in all of the steps, from the operator on the position to the exalted manager in his luxurious Fort Meade office, must also know something about the other disciplines in order to do their jobs effectively. They ought to know what kind of information is important to the traffic analyst, in order to be alert for that kind of information when it appears. They have to be aware that indicators for the cryptanalysts may appear in traffic and that it is important to collect them--and helpful, sometimes, to highlight them.[3] The collectors at the management levels have to be familiar with the needs and wants of the other disciplines in order to meet them or to anticipate them when writing and assigning tasks. They should also constantly remain aware that every collection success creates a processing problem. Hence the collector must be aware of and should be sympathetic to the problems of the other disciplines.

This is a vastly oversimplified account. This writer is a collector, and at one time or another each of those activities was his job. This article has not gone into any of the details of a collector's job. [redacted] It was intentionally designed to be a brief introduction to a relatively little-known discipline, but one without which the other disciplines would have no reason to exist.

P.L. 86-36
EO 1.4.(c)

Another motive for this article was to throw down a gage. Many readers are going to say, "I could write rings around this guy." Anyone who can, ought to. Even if you can't write rings around this guy, you probably have something to contribute. Write an article on some aspect of Collection, or tell us about an experience you have had as a collector or with collectors, and whip it on the editors.

* * * * * * *

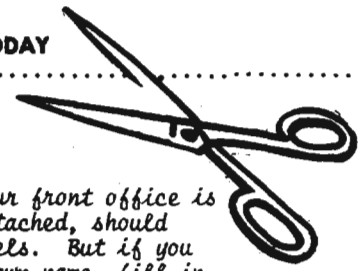
1. Acronyms don't have to be pronounceable to be pronounced. Take, for example, "Discus" satellites (DSCS), "Flare-9" antennas (AN/FLR-9) and "Angry-9" radios (AN/GRC-9).

2. Collectors are often given to strong language. Some expletives used in this article have been modified to protect more sensitive personnel.

3. Some Morse operators are instructed, for example, that unless the preamble and first five groups of text are copied, the rest of the message is not even worth taking.

~~(CONFIDENTIAL)~~

CLIP OUT AND MAIL TODAY



SUBSCRIPTION COUPON

If our circulation department is doing its stuff and your front office is doing its stuff, a copy of CRYPTOLOG, with buck-slip attached, should reach you every month through your organizational channels. But if you would like to have a copy mailed direct to you in your own name, fill in this coupon--or any old slip of paper--put it in a shotgun envelope and send it to CRYPTOLOG, P1.

(Name) _____

(Organization) _____ *(Secure telephone)* _____

DOCID: 4009704

TDB — THE TEXTA DATA BASE

by William J. Jackson, P14

TEXTA means Technical Extracts of Traffic Analysis. A system of recording and maintaining a data base of technical information on communications targets, it was instituted in 1946 by agreement among NSA,

[redacted]

In recognition of the problems arising from the variety of TEXTA-related systems, Major General Herbert E. Wolff, Deputy Director, Operations, NSA/CSS, has directed that a worldwide common TEXTA data base, to be known as the TDB, be established, to comprise one technical file which will embrace both TEXTA and specialized files, meet field needs, simplify feedback operations, and be compatible with the activities of collaborating centers. He has designated P1 as overall management authority for the development and initiation of the TDB; Mr. William Lutwiniak, Chief P1, has named Mr. C. G. Garofalo, Chief P14, as the project manager. Assisting Mr. Garofalo are sub-project managers named by Operations Groups A, B, C, G, V, and W. This committee is meeting periodically to develop and establish the TDB. Members are ascertaining the ideal data base requirements of each using organization, identifying common elements in these requirements, and determining what additional elements might be needed. Considered in the planning is the rectifying of factors which caused the variety of TEXTA-related systems to come into existence.

[redacted]

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

will be involved in the final stages of the development of the TDB. Upon agreement of all concerned, an ideal TDB format will be developed, after which C Group will be requested to devise and establish flexible machine processing systems to handle all present and anticipated TDB requirements. Following initial implementation, V3 will assume operational control of the system.

~~(SECRET HVCCO)~~

==========

Our thanks to the unknown person who coined the name CRYPTOLOG--which we found in a list of suggestions left over from the naming of SPECTRUM. In addition to being unique (we must assume) in all the world, it is most appropriate to our purpose, which is to serve as an informal running record of events and issues in cryptology and its associated fields.

DOCID: 4009704

WHAT SHOULD YOU EXPECT?

or The Analysis of Cryptanalysts

BY [redacted] P.L. 86-36

You are a manager among whose newly acquired responsibilities is the production of intelligence information from encrypted messages of a SIGINT target. Your personal background is firmly in traffic analysis and reporting, and you have always felt that cryptanalysis was an esoteric art that an outsider could not really appreciate. Now you must sit in judgment of people and operations in that "foreign" field. What should you expect of a crypt effort? More pertinently, what should you expect of the cryppies involved in it? If your deputy is an experienced, professional cryptanalyst, you have some breathing space, but the responsibility is still yours. Here are some thoughts from one professional cryptanalyst and erstwhile manager which may help.

The good crypt effort, whether manned by one or one hundred people, is marked by a "professional" outlook. Webster's defines professional as, among other things, "manifesting fine artistry or workmanship based on sound knowledge and conscientiousness." The definition covers the product, the methods used to produce it, and the fundamental principles from which those methods proceed. Principles and methods imply order, and the good crypt effort is orderly. That is not to say the desks and papers are neat; it is to say there is intellectual order in the attack on the target problem. For the members of the group characteristically use the scientific method of systematic pursuit of knowledge, yet--and we might consider the "fine artistry" part of the definition--they are flexible enough to allow for and to profit from the intuitive leaps that sometimes bring solutions. The lucky guess, the shot in the dark have their place, closely tied to the "surprise" and "rational behaviour" I. J. Good speaks of in the introduction to his Standard Reagents and Diagnostician's Dictionary.

Another professional attribute of both the crypt group and its members is thoroughness. Whether its mission is initial diagnosis of a large or small body of encrypted messages or the exploitation of traffic in solved systems or both, the crypt effort covers all aspects of the problem according to a reasoned plan established in the light of all the information, all the material, and all the resources available for the job.

As with other scientific professions, the good crypt effort is well documented. The Technical SIGINT Report, the SIGINT Support Report, The Technical Journal article, the Informal Technical Notes, the Technical Support Letters all put pertinent information on the record and invite evaluation and response from other members of the profession. Producing one's own publications and profiting from those of others are indispensable to complete, professional cryptanalytic operations.

Now that we agree on the characteristics of a good crypt effort, you as the manager still have to measure yours against the standard. Even without more than a superficial knowledge of the ins and outs of crypt, you can gauge your group's status with some reliability. Consider the characteristics. Is there a long-term goal? Are there intermediate stages along the way? Do the members of the group know what they are? Does the group as a whole agree on a single goal or a single set of goals? Can the group leader describe these goals to you so that you can understand them? Do the group and its members know how they will try to get to the goal? Again, can the leader explain the routes or methods to you so that you can understand? Have they alternative methods in reserve in case the first ones don't work? Is there contingency planning? Does the group consider the whole problem or only that portion that comes readily to hand? All these points have to do with order and method; they presuppose knowledge and skills belonging to the profession of cryptanalysis.

The second characteristic, thoroughness, applies to the order and method; it also applies to the execution of the chosen methods of getting to the end result which lies somewhere along the path of diagnosis, solution, exploitation. Does the group collect all the available traffic? All the pertinent traffic analysis information? Collateral? Does it study all the material and information gathered? Does it know or find out or write or request and use appropriate computer programs? Does it consult experts in the field? Does it study reports on what has been done in the past against the same target? Against the same type of cryptosystem?

DOCID: 4009704

It comes last in the list of characteristics and it all too often comes last to mind if it surfaces at all--documentation. Yet it is an integral part of the professional and scientific effort in cryptanalysis as in any other technical discipline. You, the manager, should expect that the procedures and results will be put on the record. Does at least the group leader keep a technical diary? Does your group report in writing? Does it publish technical reports? Does it think that only successes are reportable? Does it report, for the record, procedures developed or adapted, with information on the material the procedures were applied to, and the outcome of the application, failure or success, in whole or in part? Are the reports well written? Can you understand them or at least grasp the essentials of what was done and why? Do the reports published by your crypt group provoke questions, suggestions, refutations, visits, or telephone calls from other cryptanalysts or other crypt organizations?

Having looked at the effort, let's consider the individual. The same features that mark the good crypt effort mark the activities of the good cryptanalyst. Only the scale is smaller, and the personal attributes of the individuals vary from one to another. Aside from the specific training and experience one would need for your problem, there are some generalities about the "professional" cryptanalyst (not necessarily so certified by the Career Panel).

Mature, responsible, self-reliant, forward-looking, optimistic--all the trite laudatory adjectives--mark the good analyst. Add common sense and sound pragmatic judgment and a willingness to share knowledge with others, and you come closer to the ideal. He may be a "loner" by inclination and may be more valuable to the effort working that way, but he always knows how his problem dovetails with other problems or with other facets of the same problem. He knows and subscribes to the set goals of the group and, indeed, of the Agency.

The good cryptanalyst keeps up with developments. He reads technical publications, participates in professional assemblies and conferences; he seeks advanced training to sharpen crypt skills and to increase his knowledge of related fields. He talks to other analysts and learns from those he talks to. He finds out what is going on in related fields. He does not retire to his own snug corner and let the rest of the SIGINT world pass by.

The good cryptanalyst is intellectually alive. He keeps learning and keeps trying to relate what he learns to the problem he is dealing with. He can tell you what he is doing and why, and he wants to. He keeps on working and never completely abandons hope of eventual success, but he knows when the law of diminishing returns becomes operative and is willing to call a halt. He documents what he has done and what he thinks ought to be done if the propitious time ever arrives. He prepares for the future--his own and the problem's.

To judge the cryptanalyst and his work, the non-cryptanalyst manager should look for knowledge and commitment to goals, both organizational and personal; for thoroughness; for documentation of work and outcome; for order in materials and methods. The questions to ask are really the same as for judging the whole effort. In addition, look for initiative, imagination, innovation, and enthusiasm tempered by practical good judgment about potential results. Beware the pitfall of judging the capability and performance of the individual primarily on the basis of the number of systems solved or messages read--there are all kinds of systems and all kinds of messages.

The documentation of the crypt effort of whatever size can give you insight into both the group's and the individual's operations. Technical reports, published and unpublished, formal or informal, can help you evaluate the effort, its directions, and its prospects as well as its people. Good documentation shows that the cryptanalyst is looking beyond his own desk--to other SIGINT fields and to the future.

To judge crypt documentation, read the reports. Do they cover the whole problem or, if they cover only part of it, do they describe how the part fits into the whole? Do they fit in with what you know from other sources? Are they written while the information is still fresh in the author's mind? Are they convincing? Do you understand at least the general outline of the problem, the work, and the results? In other words, are reports written? Are they well written? Will they be useful for the next crypt attack on the same problem or on similar problems of the same or another target now or in the future?

The cryppie knows he has reached a solution when the system "reads." You, the manager, have no such definite measure in evaluating a crypt effort. Perhaps these few ideas can provide a starting point to help you arrive at a reliable judgment about this part of your responsibilities.

~~(CONFIDENTIAL HVCCO)~~

DOCID: 4009704

EO 1.4.(c)
P.L. 86-36

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

A SPOT BY ANY OTHER NAME

by VERA R. FILBY, E12

When things or situations or the contexts in which they exist change but our words for them do not, it may be some time before we perceive the disparity between our understanding of the words and the reality they represent. Such a disparity appears to be affecting names for certain SIGINT reporting vehicles.

Take the term electrigram. The word was invented in the mid-1960's to distinguish between reports of current events issued electrically soon after the events happened or could be recognized, and routine, recurring reports, such as daily and other summaries, which were issued electrically. Instructions celebrated the newness of the term by showing it in caps: ELECTRIGRAM. It soon acquired the nickname E-GRAM and eventually tended to lose its majuscule status. It was defined as "a vehicle for publishing information that does not meet the criteria for SPOT Reporting....but which is of significance and/or urgency requiring electrical dissemination."

Distribution instructions brought out a further distinction in that electrigrams, unlike spots, were not

Thus the meaning of the term was clearly defined, and it made sense in the context of SIGINT reporting--until a year or two ago. But changes resulting from, among other things, automation, security, and economy, have altered the context situation. Now, for example, many reports are issued electrically which formerly would have been issued in hard copy only. These may be reports of information a week, a month, or six months or more old, information not exploitable when current, or not useful or recognized as useful at the time, or of limited priority but still reportable. The question now arises: When such a report is issued, is it an electrigram?

The problem is not as trivial as it may seem. People need to understand what words mean, and there must be common understanding of terms and their significance between writer and reader, because that means common understanding between analyst/reporter and user.

Consider the spot report. Some reporting units and some instructions have set time limits of 30 minutes or even 15 minutes from time of recognition of spot information to time of release. But urgent and important information may be quite complex. It may require extensive processing and analysis. If it takes a day, or two, or more, for processing, coordination, and release, but must go to a spot distribution because of content, is it still a spot? Instructions define spot report information as "highly significant, perishable SIGINT" and require that spot reports be labeled as such. They also require a precedence of PRIORITY or higher. But current telecommunications system regulations call for a maximum handling time for PRIORITY precedence of three hours; so what is the point of a 30-minute reporting requirement? At present (Spring 1974), with the degree of automation achieved over the past two years, average system handling time for PRIORITY is about seven minutes, but actual delivery time for both ROUTINE and PRIORITY is about two and a half hours, for IMMEDIATE about one hour, and for FLASH about 10 to 15 minutes.

Sometimes a brief summary of complicated facts can be issued as a spot with the details in a follow-up, and this may be a useful device for getting out urgent but complex information. It is less useful for information less urgent but still requiring spot distribution, since it means that readers must refer to two documents instead of one to get the story.

Because of distribution requirements, there has been a tendency lately to put a SPOT REPORT label on items which do not meet the definition of "spot" as urgent and perishable but may even be wrap-ups or periodic summaries of a continuing situation. A puzzled user who was asked recently about a rather relaxed reaction to information in a spot report responded plaintively, "But we don't know what a spot report is!"

Is it any wonder?

And so a process of rethinking and redefining is now under way. Would you like to help? Any ideas? Try defining:

An electrigram is.....

A spot report is.....

~~(CONFIDENTIAL/HVCCO)~~

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4009704

THE NEW TRAFFIC ANALYSIS GLOSSARY by P14

"Glossary" is defined as a collection of terms limited to a special area of knowledge; it derives from the Latin glossa, which refers to an unusual word requiring explanation. Since the SIGINT business includes several such areas, each of which makes use of many such words, and since its successful pursuit depends on the ability of its organizational elements to intercommunicate with precise understanding of meaning, SIGINT glossaries are a definite and practical necessity. Nevertheless, only during the past year has there been a formally directed PROD effort, under USSID 412, to develop and publish a complete, authoritative, and official glossary for each of the special technical fields peculiar to SIGINT, coordinated with and agreed upon by all using operational elements and, in some instances, second parties. Earlier, some glossaries, both specialized and general, had been published, but, with one exception, without having undergone a rigorous developmental treatment throughout Operations and without having acquired second-party agreement. These included a general glossary prepared by the U.S. Army Security Agency in 1947, a traffic analysis glossary published by NSA in 1954 (NSA Interim Report #168-54), a glossary contained in the Radio Traffic Analysis Manuals of 1955 and 1964, and, in three editions, the Basic Cryptologic Glossary, the latest dated June 1971. The exception referred to above is the Combined Glossary of Traffic Analysis Terminology, published in January 1958 by NSA, which was thoroughly coordinated throughout PROD and with second parties (the latter indicated by the term "Combined").

After the Combined Glossary was issued, a decision was made that no further glossaries would be published by PROD--that hereafter they would be the responsibility of the then Office of Training. As one result, PROD personnel who had been concerned with the Combined Glossary and who had intended to keep it updated were discouraged from so doing. Finally, in 1964 the Office of Training published an all-inclusive glossary, called the Basic Cryptologic Glossary. It included some terms used in traffic analytics, but it did not adequately or accurately fulfill PROD needs--many TA terms were omitted and some were changed from the 1958 Combined Glossary without proper coordination either with NSA elements which were operationally concerned or with second parties. Also, the Combined Glossary contained Codeword information, while the Basic Cryptologic Glossary was limited to Confidential material. Thus, two glossaries containing differing terminology and spelling were extant, leading the British to comment that "only NSA could afford the luxury of two glossaries," and, along with most of the knowledgeable NSA traffic analysts, to continue to use the Combined Glossary while ignoring the 1964 publication, at least with regard to TA terms. Later editions of the Basic Cryptologic Glossary evidenced no significant improvement as far as TA was concerned, as there was little input from and no formal coordination with NSA operational personnel and second parties.

In recognition of the somewhat confused glossary situation and the need for the development of definitive and authoritative terminology, not only for traffic analysis but for the other SIGINT disciplines, USSID 412, SIGINT Terminology, was promulgated, on 1 February 1973. This USSID established the program for standardizing terminology used throughout the U.S. SIGINT System to direct, manage, and support SIGINT operations. As part of the program, terminology panels are authorized to be established to develop standard definitions for terms required in the specialized areas of SIGINT operation. The USSID also designates the NSA Data Standards Center (NDSC) as having overall responsibility for the issuance of the respective glossaries, and makes it responsible for maintaining a complete SIGINT Terminology Data Base and for making the base, in the form of machine printouts,

DOCID: 4009704

P.L. 86-36

available to authorized users, principally the terminology panels.

Under the authority of USSID 412, and with operational terms of reference agreed upon between P14 (Traffic Analysis) and P13 (in which the NDSC is located), the Traffic Analysis Terminology Panel (TATP) has been established to develop the Traffic Analysis Glossary. Under the chairmanship of Mrs. Gloria Chiles, of P14, the TATP consists of representatives of A, B, C, G, W, E, and P14, appointed by the chiefs of those organizations. Three senior cryptologists, Messrs. C. G. Garofalo, Chief P14, Robert [redacted] Chief P13D, and Donald Borrmann, D/Chief V, act as advisors to the TATP.

As the initial step in the development of the TA Glossary, the NDSC made available to the TATP the printout of a terminology data base consisting of thirteen technical glossaries containing a total of 4,641 unique items presumed to have a possible relationship to traffic analytics. (The TATP found that many of these items had a variety of definitions, some as many as thirteen--a different one in each of the contributing glossaries.) The first task of the TATP was to sift through the list of terms to identify those which could be of concern to the field of traffic analytics and which therefore would warrant further consideration. (This process, although at first glance a simple one, was complicated by the overlapping and intimate relationship of traffic analysis and other special fields, such as cryptanalysis, collection, signal analysis, data systems, etc. The difficulty apparently arises from a lack of precise definition of the field of traffic analytics - this problem is being studied by the TATP.) In addition to using this list, the TATP selected potential terms for study from a variety of operational publications, such as TECHINS, USSID's, working aids, Technical SIGINT Reports, etc. The sifting and selection process resulted in the TATP designating about 1500 terms for detailed study and possible inclusion in the TA Glossary; this study is now in progress. The terms have been grouped into two general divisions-one by subject matter and the other, those terms that remain, alphabetically. In addition, each term has been categorized as follows:

Category 1: terms of primary concern in traffic analytics, which will be defined and included in the Glossary.

Category 2: terms of secondary concern in traffic analytics, which will be included in the Glossary but defined by other panels.

Category 3: terms determined to be of no concern in traffic analytics, which will not be included in the Glossary.

Category 4: terms to be included in the Glossary as cross references.

Subject-matter groupings consist of terms relating to a particular area of study in traffic analytics, such as callsigns, addresses, procedure, etc. Considering related terms together results both in finding and devising new terms and in eliminating some that are duplicative or unnecessary. For example, in the address grouping, 182 terms were considered and eventually reduced to less that 100. Also, in this group, a new term was created--"coverterm"--as a generic term which includes "covername," "covernumber," and "coverword." Consolidation of terms was also effected--e.g., "weather station identifier" becomes the generic term, and "indicative," "station identifier" and "station number" are cross-referenced to the generic term by the statement "same as weather station identifier." Correspondingly, included in the definition for the generic term is the statement "synonymous with indicative, station identifier, and station number."

In its operation, the TATP establishes an agenda consisting of a list of terms to be discussed at each weekly meeting. In preparation for the meeting the panel members research assigned terms by examining technical documents and dictionaries, determining their use in operational elements, reviewing previous definitions, obtaining opinions from senior analysts, etc. Thus prepared, the panel members in open discussion at the weekly meetings attempt to arrive at a standard definition for each term. At the time of this writing, the TATP has established definitions for terms beginning with A through H, as well as for the subject-matter groupings for addresses and for communications structure and operations.

When the definitions for all terms have been completed by the TATP they will be arranged in prescribed draft format as Annex D to USSID 412, which will be forwarded by P1 to USSID representatives in the operational elements for concurrence and distribution requirements. Concurrently, the draft, which is scheduled for completion in December 1974, will be coordinated by P14 with second parties through the existing TEXTA Working Party, of which Mr. C. G. Garofalo, Chief P14, is chairman. After completion of coordination and any required substantive revisions by the TATP, a final draft will be prepared by the NDSC for final coordination by P13 with the SCA's and second parties and eventual reproduction and distribution. Although the Glossary will be part of USSID 412 for record purposes, it is planned that it will be issued as a separate document physically, principally for ease of reference and to facilitiate distribution and use by second parties.

Publication and use of this Glossary, and eventually of those in the other specialized fields, should make for a clearer understanding in SIGINT matters among all those concerned, and thus improve the effectiveness and efficiency of their efforts.

~~(SECRET HVCCO)~~

PUZZLE 1

As if the SIGINT business weren't puzzle enough, some people like to make up their own riddles and inflict them on their friends. A simple form of puzzle (which also makes a great game for children on long trips) is the stinky-pinky, in which the answer must be given in a pair of rhyming words of a stated number of syllables. In the list below, for example, all-out offensive breaks out to large charge, carefree captain to chipper skipper, and so on. While you are waiting for that call to be returned, try your hand at these.

1 syllable:	All-out offensive
	Intoxicated agent
	Blue dossier
	Taped speech
	Polished Pole
2 syllables:	Carefree captain
	Corrugated film
	Smaller soldier
	Facsimile messages
	Beatnik codebreaker
	Error in an epitaph
	30-year cryptanalyst
	Poor intercept
3 syllables:	Evil emissary
	Searching examination
	Sadat loses cool!
	Cleverer calculator
	Future goal
4 syllables:	Deserted city
	German swimmer
	Chic Japanese
5 syllables:	Polysyllabic ragamuffin
	Central American underground

DOCID: 4009704

UNCLASSIFIED

THE LANGUAGE OF BEISBOL IN EVERYDAY TALK

by [redacted] P16
& Ramón Santiago-Ortiz, G643

P.L. 86-36

WHEN we say that baseball is an "American" game, the reference is usually to the United States, but the sport is played and loved in Latin America as well. It has even affected their language and terms that originated on the diamond are now a part of everyday conversation in Spanish as they are in English—-compare "he's 'way off base," or "What's the pitch?" or "I really struck out on that deal!" An article in the Cuban magazine BOHEMIA collected about 35 such expressions. We have arranged them alphabetically, run the original BOHEMIA entries (as in the original, without written accents, in full capitals, etc), and supplied a rather free English translation.

The English words in parentheses on the Spanish side were in the original. The English words in square brackets are more-or-less literal translations of the capitalized Spanish (the baseball term); the remainder of the English entry consists of comment and explanation of the Spanish, rather than being just a translation of it.

AL BAO (bound).– Que nos llega fácilmente: sin problemas, a las manos.

[on the rebound, on the bounce] no sweat!, very easy, like taking candy from a baby.

¡AZUCAR!– (así bautizó el estrai un narrador deportivo).– Sublimación del piropo.

[sugar; a term invented by a sportscaster to refer to a strike] the highest form of compliment. (A whole article could be written about that word PIROPO, which is usually restricted to complimentary remarks made to and about pretty girls. Note also that word ESTRAI, strike, which we'll see again in ME TIENEN DOS ESTRAI Y PELEADO CON EL AMPAYA later in this article.)

BOTO LA PELOTA.–(jonrón).–Hizo algo en grande; óptimo o pésimo.

[he knocked the ball out of sight for a home run] He went all the way; whatever he did (good or bad), he did it in a big way; no halfway measures with him!

CERO CARRERA, CERO HIT, CERO ERROR.–Nada de nada, no de esa obediente materia prima ("pues de ella fue la humanidad creada") sino la equivalente a una cifra cero sin orillas. El elocuentísimo "nico..."

[no hits, no runs, no errors] a real nothing, a total nonentity. (Sometimes the word HIT is spelled JIT.)

COGIENDO ROLE (rolling).–Rascabucheando, viviendo un cuadro.

[catching a rolling ball, fielding a grounder] Sponging off others, freeloading.

COMO TIENE EL BRAZO.
COMO TIRAE EL BRAZO.–(Que tira a la base certera y fuertemente).–Que está acertando, que está entrándole como el cernicero a la res.

[What an arm he has! (referring to a player who throws the bases accurately and with force)] He's an expert; he really knows what he's doing; he really does a good job. (The two Spanish expressions are equivalent.)

DE BATE EMERGENTE.–Suplenteando. Ayuda temporal.

[pinch hitter] filling in, plugging the gap.

DE PITCHER TAPON.–Idem.

[emergency relief pitcher] same as the previous entry: filling in, plugging the gap.

UNCLASSIFIED

DOCID: 4009704

ES CUARTO BATE EN CUALQUIER NOVENA.—Bueno a todo. Eficiente a cualquier nivel.

[he can bat fourth on any team. (Assuming that the first three men have gotten on base, the fourth man at bat—usually called "the cleanup hitter"— is expected to get a hit and score one or more of them.)] you can depend on him to do a good job; he's tops; "Old Faithful."

ES UN CARGABATES.—Un cachanachán, un hala-levas, un traca**, un perrillo faldero. En fin: una guasasa.

[he's a bat boy] he's not important, no big thing; just a lackey; low man on the totem pole. (Most of the Spanish terms used in this definition are not in standard bilingual dictionaries and are worthy of note. Unfortunately, there was an imperfection on the page at the end of the word that begins with TRACA.)

ESPERATE, QUE ESTOY AL BATE AHORA.—Llegó mi chance, mi turno, mi oportunidad.

[Wait a minute! I'm coming up to bat now] Now it's my turn; I finally got my chance! (Not quite equivalent to the English proverb "Every dog has his day," but pretty close to it.)

ESTA EN EL NOVENO INNING.—Se está acabando, falta poco para finalizar.

[We're in the ninth inning] Time is running out, not much time left; it's now or never; it's the eleventh hour.

ESTA EN 3 Y 2.—(alternativa definitoria: o le pasan un estrai y lo ponen fuera, o le pasan una bola y toma la base). —O se salva, o se hunde. Lo toma o lo deja.

[the count is 3 and 2 (it's now or never: either they'll throw him a strike and put him out or they'll give him a ball and put him on base).] The moment of truth has arrived. It's time to fish or cut bait. You have to make a decision now. (Compare ME TIENEN EN 2 ESTRAI, etc, below.)

ESTA FUERA DE JUEGO.—Perdió la puntería por falta de ejercicio, no tiene su habitual acierto.

[he's not in condition to play, out of shape] he missed the shot because he's out of practice; he's over the hill.

ESTA FUERA DEL JUEGO.—No lo llevan. Lo han desco-desconocido.

[he's not in the game] They don't even have down (on the roster); they've forgotten about him. He's a has-been.

ESTA FUERA DE SEÑA.
NO LO COGIO LA SEÑA.—No entendió, no captó lo que insinuaron. Desubicado, fuera-de-onda.

[he missed the sign; he didn't catch the sign] He didn't understand, didn't take the hint. He's not with it, in a world of his own, not tuned in to our frequency.

ESTA GUAI (wild).—La otra cara de la moneda con respecto a la expresión VIENE POR LA GOMA.

[he (the pitcher) is wild] He's not doing his job properly, he's messing things up.

ESTA JUGANDO AL DURO.—Que no afloja, que sigue los principios.

[he's playing it tight] He's not slackening up, taking shortcuts; he's following the rules, doing things according to the book.

ESTA JUGANDO AL FLOJO.—Lo contrario de la expresión anterior. Cubaneo.

[he's playing it loose] The opposite of the previous entry: He doesn't always finish what he starts.

ESTE ES OUT POR REGLA.—Sin remedio su asunto o su mal. Fracaso inevitable. Infeliz. Sin iniciativa.

[According to the rules, that's an out] There's no cure for what he has. The poor guy! He never had a chance!

ESTE ES QUIEN MANICHEA.—(de manager, director de equipo).—El que manda y también el que maneja la cosa como la de gana.

[he's the guy who manages the team] He's the one who gives the orders; he's the boss.

JUEGA TODAS LAS POSICIONES.—Superindividualista. El universal inútil hombre-orquesta.

[he plays all the positions (on the team)] Jack-of-all-trades, master of none; in a class by himself. (The Spanish uses a lovely expression: the universally useless one-man band.)

LO COGIERON FUERA DE BASE¡—Lo sorprendieron, lo pillaron, atrapado en un mal paso.

[They caught him off base.] They caught him napping, pulled the rug out from under him. They caught him (in a lie or in the act of wrongdoing).

LO DEJO CON EL BATE AL HOMBRO.—No le permitió actuar.

[He left him standing there with his bat on his shoulder] He wouldn't let the poor guy do anything; he stopped him from acting, put up roadblocks in front of him.

MANICHE DE GLORIETA.—Que critica por fuera, desde una posición cómoda, sin riesgos; pero cuando está en el agua se olvida de nadar.

[grandstand manager, manager in the bleachers] Guy who stays on the side and criticizes; a "sidewalk supervisor" or "Monday morning quarterback."

DOCID: 4009704

ME TIENEN EN 2 ESTRAI Y PELEADO CON EL AMPAYA (umpire).—Sin salvación. Agonizando.

[they've got two strikes on me and I'm quarreling with the umpire] a desperate situation; between the devil and the deep blue sea. The best I can get out of this situation is the worst.

NO LO VIO PASAR.—(la bola).—No se enteró, está como la cherna en tarima: con los ojos abiertos pero sin ver.

[he didn't even see it (the ball) go by] he wasn't paying attention; "Eyes have they but they see not"" (The Spanish has a picturesque description: Like a fish in the market, with its eyes open but not seeing anything.)

NO ME PONGAS LA DE TRAPO.
NO ME PONGAS LA PODRIDA.—(En beisbol se usa pelota de "poli," que es relativamente pesada y resistente).—No me hagas la cosa imposible. No me vengas con engañifas.

[Don't throw me the ball made of rags. Don't throw the rotten (ball) at me.] Just give me the real stuff, no tricks! Don't try to cheat me!

NO SE VA CON BOLAS MALAS.—No se le puede engañar. Se lo sabe todo.

[he won't swing at bad pitches] It's not easy to pull the wool over his eyes; he wasn't born yesterday; he knows what the score is.

NO TE LANCES, QUE TE PONEN OUT.—No te atreves, que fracasas.

[Don't try to steal a base 'cause you might get put out] Don't take too many chances because you're bound to fail if you do; look before you leap; play it safe.

SE LA DEJA EN LA MANO A CUALQUIERA.—Incumplidor, falto de palabra. Dejar embarcado.

SANTIAGO "CHANGA" MEDEROS

[Let somebody else catch the ball] he loves to pass the buck; he's irresponsible.

SI ME LA PASA, SE LA BATEO.—Si me alude, replico en tiempo y forma.

[If the ball comes by me, I'll bat it] If the remarks apply to me, I'll answer them duly and properly. If he provokes me, I'll get him.

TAI (time).—Tiempo, espera, tregua.

[Time!] Time out! Let's take a break!

TIENE MAS CURVAS QUE CHANGA MEDEROS.—Referido a mujer bien dotada en su diseño anatómico según el patrón criollo.

[She has more curves than Changa Mederos (a famous contemporary Cuban baseball pitcher)] Used in speaking of an especially curvaceous, well endowed woman.

VIENE POR LA GOMA (pitchea con control).—Acertado, que está planteando las cosas oportuna y certeramente.

[he throws right to the plate, he reall has control when he pitches] he figures things out correctly; he always has the situation well in hand; he's very direct and accurate in his judgments, a no-nonsense type of person.

The Spanish-language article concludes "Y... VAMOS A SUSPENDER EL JUEGO POR LLUVIA" (Let's call the game off on account of rain—an expression used to cut off a gabby person's drawn-out narration) because there are many, many more baseball terms used in everyday Cuban conversation. That also seems like a pretty appropriate way to end this English version.

Puzzle #2

In what Agency publication would you find the following?

1. x f x a y d a s h x j x u d i t h x o x ' x c o n n e l l
2. x j x o h n s o n x c x h e s t e r f i e l d x e x
3. x o x c h s x c x a r l x j x
4. x o x x h x a r a x d x e n n i s
5. x s x t o n e x s x i n c l a i r e x m x c x k x e e

ANSWER ON PAGE 18

DOCID: 4009704

Right-to-Left Text Sorts Are Not Impossible

by

[redacted]

P16

P.L. 86-36

Have you ever been faced with a pressing need for a list of data sorted in a particular way and been unable to get it? Perhaps this list of data so urgently needed contained elements of variable length such as plaintext words, and the sort sequence desired was not the "standard" left-to-right ordering of data. Does that sound familiar? I have heard of instances wherein a right-to-left word sort of data was needed--plaintext or decrypted message endings, etc.--but the computer support personnel assigned weren't sufficiently experienced in using sort routines to provide them in the form needed.

The problem at first glance seems to be that most computers only compare strings of data in a left-to-right direction. But upon closer scrutiny we see that a left-to-right comparison of the words within the data strings is what we want. The real problem is that we have to use sort routines designed for comparing fixed-length sort fields to sort variable-length data elements (words) appearing at variable positions within the data stream. For the novice programmer this may be such a formidable task that he may convince himself, and you, that it cannot be done, and leave you to waste many frustrating hours using an analytic tool that is not what you really need.

One simple solution to this problem is to generate a special fixed-length "sort key" for each data record that is to be sorted. This can be done by allocating a data field equal to a fixed maximum-word-size times the number of words wide the data is to be sorted. Sufficient textual words are then isolated, padded with blanks, and loaded in left-to-right, major-to-minor sort order into this key field. Each of these special sort keys is then either appended to the record from which it was derived or "tagged" with the location of the record from which it was derived, for use in a "tag sort" routine. After normal sorting using this special sort key, the original record is printed unaltered for the user.

As an example of how this is done, assume we have the following message endings, and the sort desired is on the last five words, with major sort on the last word and minor sort on each succeeding one to the left for up to five words:

```
001 STOP COLONEL JOHN BROWN COMMANDING
002 RETURN AT ONCE STOP BROWN
003 REPLY AT ONCE STOP BROWN
004 STOP LT. GEN. BROWN COMMANDING
```

The sort key generated would be:

COMMANDING	BROWN	JOHN	COLONEL	STOP	001
BROWN	STOP	ONCE	AT	RETURN	002
BROWN	STOP	ONCE	AT	REPLY	003
COMMANDING	BROWN	GEN.	LT.	STOP	004

The sequence listed after sorting would then be:

```
003 .....REPLY AT ONCE STOP BROWN
002 ....RETURN AT ONCE STOP BROWN
004 ....STOP LT. GEN. BROWN COMMANDING
001 STOP COLONEL JOHN BROWN COMMANDING
```

Once this basic strategy is adopted, the multitude of methods for scanning the text for word separators and moving single words into fixed-length fields to generate a sort key is limited only by the characteristics of the particular programming language being used and the ingenuity of the programmer involved. Generating this sort-key is not a trivial matter, especially using certain programming languages, but don't let anyone convince you that it is "impossible."

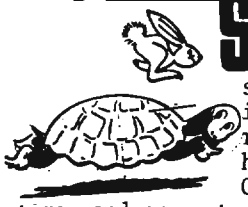
(UNCLASSIFIED)

DOCID: 4009704

SELF-PACED INSTRUCTION: "The Future is NOW!"

by [redacted] E13

P.L. 86-36



Self-paced instruction (SPI--sometimes called programmed instruction, self study, correspondence study, and so on) has been used at the National Cryptologic School for some time, and present planning calls for the amount of such instruction to increase greatly during the next few years. Unfortunately, few people are familiar with SPI in its new and improved form. This article presents the answers to some basic questions on the subject.

What is SPI?

SPI, as used by the National Cryptologic School, means a set of ordered instructional lessons to be mastered by the student. These lessons will combine written material with various kinds of media: tapes, slides, filmstrips, videotapes, and computer programs. Courses will be conducted in learning centers both at Fort Meade and at Friendship.

When you enroll in an SPI course you receive Lesson One which, like every other lesson in the course, starts with a list of terminal objectives telling you exactly what you are expected to learn during the lesson, the conditions under which you are to learn, and the standards you are expected to meet. In other words, you are shown the test before you start the lesson. If you wonder why we do it this way, the answer is simple: controlled studies show that students learn better knowing the objectives, as opposed to the old-fashioned method of keeping them a secret until the end of the lesson.

After reading the terminal objectives, you start to study the material. The lesson is broken down into several sections. Each section concludes with questions and exercises for you to do so that you may immediately practice what you have learned. You proceed through the lesson at your own pace. Don't worry if you get stuck at some point, a qualified instructor will be present at all times to answer any questions you may have. When you feel you have mastered the material, that is, met the terminal objectives you read at the start of the lesson, you ask for the test on that lesson. The test checks to see whether you have indeed achieved those objectives.

If you pass the test you go on to the next lesson; if not, you go over your mistakes with the instructor and do whatever remedial work he suggests. Then when you feel you are ready, you retake the test. If you pass this time, your record shows only that you have successfully completed that lesson, and you now proceed to the next. When you have completed all the packages, you take a final test for the course, and you're done.

What is SPI not?

There are some common misconceptions about SPI. The most common is that you receive a course, are sent to a dark corner and told to remain there until you have completed it. Actually, the course will be conducted in a learning center, an area consisting of individual study areas called "carrels," where you sit while you study your text, listen to a tape, view slides, etc. The learning center is designed to be conducive to study and to make you feel comfortable. You will not be alone; other students will probably be using the learning center while you are there, and of course the instructor will be there to help you as required. You don't even have to work alone. If you are part of a small group which wishes to proceed at a common pace, that's fine. Some people learn more quickly by themselves, others prefer to be part of a group. So work alone or together--the choice is yours.

A second misconception is that you can study whatever you want. While some SPI courses offered at universities give students great latitude in choice of subject matter, ours in NCS will not. They will consist of a set of lessons which must be completed in a specified order. Therefore if you enroll in a course you must complete the specified program in order to get credit for it.

And a third is that SPI is a free ride for instructors. Certainly SPI frees me, as an instructor, from lecturing; but whereas in conventional teaching I conduct all my students

through a course at the same pace, and can predict from experience many of the questions that will arise and get ready for them, in SPI each student may be at a different point in the course, and even in different courses. I'm going to have to be on my toes to handle every question that pops up.

What's in it for students?

I've already mentioned some points, but they are worth repeating. The most important is self-pacing. You're no longer locked into a fixed pace; go faster or slower, work alone or in a group, work when you want and for as long as you want, work at Fort Meade or Friendship: it's your choice. No longer will sick leave or annual leave conflict with your study. We hope eventually to have each lesson available in several different media so you can have your choice in that, too. You want to read today, but listen or watch tomorrow? SPI offers the possibility of fulfilling all choices.

Another important advantage is that you always know where you stand. In conventional courses the test usually comes too late to help. You just get a bad grade and forge ahead without any remedial work on your weaknesses. This doesn't help you, but you are kept "on schedule." With SPI and its many checks and tests--which are often self-administered--your weak areas are spotted immediately and you do remedial work to correct your deficiencies at once. Only then do you proceed to new material.

Have you ever been in a course and found some point which struck your fancy so that you wanted to follow it up? This is often impossible in conventional courses, but it is still another advantage of SPI. Follow it as far and as long as you want. Your instructor will help and encourage you. That's his job.

Have you ever been withdrawn from a course because of operational necessity? How about not being able even to enroll because the office can't spare you full-time, or even half-time? But you might have had two or three hours available each day and with SPI you could still have taken the course during those hours. Remember, you set the pace. Afraid the course will now take forever? Forget it. For most people those hour lectures become 15-20 minutes in SPI. In summary, there is just greater flexibility for you, me, and the boss.

What's in it for the instructor?

Conventional teaching forces me, the instructor, to spend many hours preparing and delivering lectures. It does not give me the opportunity to do the things studies have proved I do best: for example, diagnose your difficulties, interact with you when you need help, inspire and motivate, encourage creativity and self-direction. With SPI I have more time for these tasks. As a matter of fact, these four actions describe my job in SPI.

Another advantage is interaction with the course material. Lectures are one-way streets; I am the only active participant. Except for asking questions, you remain pretty passive. SPI forces you to interact. This is good, because studies show you learn better when you do. And if you are learning more efficiently, I'm happier.

Finally, as an instructor, I will have the time to develop the advanced and specialized courses which are needed to meet the ever-changing technology of today.

What's in it for supervisors?

Yes, there are advantages for you supervisors as well. You no longer have to give up your personnel to a rigid class schedule. You can let them take an SPI course for a few hours a day--at your convenience. Even better, you can expect them to finish the courses faster. Studies have shown that most students work more quickly with SPI than in classroom courses. A further economy is in travel time; SPI courses are to be offered at both Fort Meade and FANX. And whereas the fixed time limit of classroom teaching sometimes forces the instructor to delete material ordinarily presented, SPI courses are of standard quality and every student is given the same material.

SPI allows the Cryptologic School to help with the training of new personnel. For example a new worker in your office is unfamiliar with your type of operational problem. Perhaps Lessons X, Y, and Z of Course 000 could give him valuable background. Send him to us, we'll let him do Lessons X,Y, and Z. He won't get credit for the course, but this brief training may make him immediately valuable on the job. And don't forget that experienced workers also might benefit from a quick refresher on some aspect of a new problem.

Remember, we are not interested in training for the sake of training; we want what you want: to increase the efficiency of employees for their jobs.

What's in it for the Agency?

So far I've pointed out advantages SPI has for the student, the instructor, and the supervisor. If these advantages are real, the Agency will gain happier and more efficient employees; but more than that, it will have better trained personnel. A well-written SPI course is expected to be superior to its conventional counterpart, if only because the burden of learning is placed where it belongs: on the student. The inherent flexibility of SPI will allow more timely training for new office personnel or for that new problem which suddenly crops up.

Finally, in terms of work hours lost to training, SPI courses will be much cheaper, and that is a big plus these days.

Conclusion

Does all this mean you have heard your last lecture? No, not at all. Writing SPI courses takes time and is therefore expensive. Therefore only those courses which are taught many times a year are candidates for conversion, because they become cheaper over the long run with self-pacing. I am talking, therefore, only about introductory or survey and basic courses. Advanced courses will continue to be offered conventionally. It is simply a matter of economics. However, SPI will release some instructors to develop and teach new advanced level courses which are needed.

So if you sign up for a course in the near future and find out that it's to be offered in SPI, please don't panic. As the old saying goes: Try it, you'll like it.

(UNCLASSIFIED)

A Short Directory of Career Panels

		(Appointment expires)
H113	COMMUNICATIONS SECURITY	
	Chairman: Mr. Ryon A. Page (S4, 2365s, 8151b)	Jun 76
	Executive: Mr. [redacted] (H113, 2308s, 6804b)	Dec 74
H112	COMPUTER SYSTEMS	
	Chairman: Mr. Robert L. Hagedorn (C4, 3829s, 7980b)	May 75
	Executive: Mr. Richard L. Wille (H112, 3421s, 7041b)	Oct 75
H111	CRYPTANALYSIS	
	Chairman: Miss [redacted] (A509, 8311s, 6674b)	Jul 76
	Executive: Mr. [redacted] (H111, 3868s, 6629b)	Jun 75
H125	EDUCATION AND TRAINING	
	Chairman: Mr. Mark T. Pattie, Jr. (E3, 8041s, 6417b)	Jan 77
	Executive: Mr. [redacted] (E1, 8957s, 6234b)	Jan 75
H120	ENGINEERING AND PHYSICAL SCIENCE	
	Chairman: Mr. William H. Gossard (R13, 3031s, 7159b)	Jul 75
	Executive: Mr. [redacted] (H120, 4924s, 7410b)	Jun 75
H127	INDUSTRIAL PRODUCTION	
	Chairman: Mr. [redacted] (S3, 2387s, 8133b)	Feb 77
	Executive: Mr. [redacted] (S321, 2191s, 6919b)	Sep 76
H114	LANGUAGE	
	Chairman: Dr. [redacted] (P16, 3957s, 7319b)	Dec 76
	Executive: Mr. [redacted] (H114, 4866s, 6468b)	Dec 74
H124	LOGISTICS	
	Chairman: Mr. [redacted] (L52, 3703s, 6757b)	Aug 75
	Executive: Mr. [redacted] (L11, 3281s, 7097b)	Sep 75

P.L. 86-36

UNCLASSIFIED

H121 MATHEMATICS

Chairman: Mr. [redacted] (R1, 3661s, 7815b) Apr 77
Executive: Mr. [redacted] (H121, 3957s, 7391b) Jul 75

H122 PERSONNEL

Chairman: Mr. [redacted] (M3, 3393s, 7487b) Mar 76
Executive: Mr. [redacted] (M09, 5901s, 6583b) Jan 76

H126 RESOURCES MANAGEMENT

Chairman: Mr. [redacted] (P, 5835s, 6521b) Jun 76
Executive: Mr. [redacted] (H126, 3775s, 7642b) Sep 74

H123 SECURITY

Chairman: Mr. [redacted] (M5, 3472s, 7531b) Jul 76
Executive: Mr. [redacted] (M55, 3602s, 6701b) Jun 76

H116 SIGNALS ANALYSIS

Chairman: Mr. [redacted] (W1, 5188s, 7438b) Jun 74
Executive: Mr. [redacted] (H116, 5188s, 7438b) Jan 75

P.L. 86-36

H117 SIGNALS COLLECTION

Chairman: Mr. William Hunt (K1, 3871s, 7193b) Feb 75
Executive: Mr. [redacted] (H117, 4578s, 7911b) Feb 77

H118 SPECIAL RESEARCH

Chairman: Mr. [redacted] (A8, 3493s, 7397b) Aug 76
Executive: Cdr. [redacted] (H118, 5287s, 6498b) Feb 76

H119 TELECOMMUNICATIONS

Chairman: Mr. [redacted] (T2, 3788s, 7044b) Jan 77
Executive: Mr. Robert Poisal (H119, 4463s, 6468b) Jun 75

H115 TRAFFIC ANALYSIS

Chairman: Mr. [redacted] (R22, 3651s, 6429b) Aug 75
Executive: Mr. [redacted] (H115, 4325s, 7667b) May 77

--- TECHNICAL WRITING

Senior Advisor: Mr. [redacted] (R4109, 4860s, 7091b) Apr 74

--- EDITING/WRITING AND HISTORIAN

Senior Advisor: Mr. [redacted] (E51, 8297s, 6656b) Indef.

(UNCLASSIFIED)

Answer to Puzzle 2: *In the January 1974 Telephone Directory, on pages 26, 44, 65 and 85.*

DOCID: 4009704

NICE BUSMAN'S HOLIDAY FOR ONE NSA EMPLOYEE

BARBARA P. DUDLEY, G5

The Seventh World Congress of Translators was held in Nice from 4 to 9 May 1974, and after spending a few days in Paris (during which, among other things, I toured the Foreign Ministry, I attended the Congress as an independent observer. I estimated the total attendance as 250 to 300. The overall fee--including all the sessions, an excursion to Monte Carlo, and the gala dinner--was about $32, which I consider to be quite reasonable.

At the Congress it was interesting to compare the reports handed out by various national translators' organizations. While they all stressed the need for effective cooperation among translators to improve their lot, the American Translators' Association has been working to improve the standards of translators and translation, as well as to establish university-level accreditation programs and translator training; the French organization has been concentrating its efforts on the broadening of copyright laws to protect translators' rights; the Slovak association has been busy organizing translation activities and the criticism of translation. All stressed the need to maintain ties with other national and international associations of translators and interpreters. I have the reports from the United States, France, Great Britain, Canada, Belgium, Sweden, Yugoslavia, Czechoslovakia, and Hungary, and will gladly make copies for anyone interested in them.

I attended sessions covering the link between literary and scientific translation, translation terminology and documentation in international organizations, translation and computer techniques, and the translator's status. The papers that I found interesting were A Contrastive Analysis of Scientific and of Literary Translations by Janko Golias of Ljubljana (who stressed at the outset that he was not a member of the 60-man Yugoslav delegation), Terminology Bank and Translation by Robert Dubuc of the Terminology Bank of the University of Montreal (TERMIUM), and Data Processing at the Translator's Service by Frederick Krollman of the West German Federal Bureau of Languages. The TERMIUM paper was of especial interest to me, and I hope that there will be an opportunity to visit the Terminology Bank "in depth" during the next Congress, which will be held in Montreal in 1977.

The most important action taken by the Congress was the recommendation of a format for the exchange of bilingual terminological information, with blocks for Semantic Unit, Source(s), and Definition(s) or Significant Context(s) in both the source and target language, plus blocks for Field(s) of Application and Author of Information Unit. /Editor's note: NSA linguists might like to compare this format with NSA Form M2424--see QRL, August 1973, page 23--or the CAMINO card./

While the formal part of the Congress was valuable and stimulating, the most interesting aspect for me was the great variety of people, a feeling which crystallized at the Gala, where the impressions came so thick and fast that I couldn't possibly recall all of them. Most of the men wore somber business suits but the women were dazzling in every kind of fancy attire and coiffure. I told the head of the European Communities' terminology committee that this was the first international gathering that I had ever attended, and that I would give anything to have it all recorded on sound-and-color film. He gallantly said, "You are an excellent observer, Madame"--I suppose that everything I was thinking about everyone could be read on my non-poker face.

My greatest thrill at the Congress came at the end of the dinner, when I summoned up courage enough to approach the eminent lexicographer Paul (le Petit and le Grand) Robert for his autograph. He is most gracious and looks as you'd expect "Monsieur Robert" to look: jovial, genial, of ruddy complexion, and apparently good for at least three more editions of his famous dictionary.

I was so impressed with the Seventh World Congress of Translators that I am already making plans to tour Quebec province in 1977 and will arrange to be in Montreal when the Eighth World Congress is in session.

Will there be any other NSA people there?

(UNCLASSIFIED)

DOCID: 4009704

DEPT. OF GOLDEN OLDIES

THE MANAGEMENT SURVEY OF THE PHILHARMONIC

These excerpts from a "management survey" of the --------- Philharmonic Orchestra by the distinguished firm of Mc------ and ------ may strike a responsive chord in the souls of all those who have been, are being, or are about to be surveyed.

"...For considerable periods the four oboe players have nothing to do. Their number should be reduced and the work spread more evenly over the whole of the concert thus eliminating peaks of activity.

"All the 12 first violins were playing identical notes. This is unnecessary duplication. The staff of this section should be drastically cut. If a large volume of sound is required, it could be obtained by means of electronic amplifier apparatus.

"Much effort was absorbed in the playing of semi-quavers. This seems an excessive refinement. It is recommended that all notes be rounded up to the nearest quaver. If this were done, it would be possible to use trainees and lower grade operatives more extensively. There seems to be too much repetition of some musical passages. Scores should be drastically pruned. No useful purpose is served by repeating on the horns a passage which has already been played on the strings. It is estimated that if all redundant passages were eliminated, the whole concert time of the two hours could be reduced to 20 minutes and there would be no need for an intermission.

"The conductor agrees generally with these recommendations, but expresses the opinion that there might be some falling off in attendance. In that unlikely event it should be possible to close sections of the auditorium entirely, with a consequent saving of overhead expense, lighting, salaries for ushers, etc."

(From Hospitals, March 1954, author unknown.)

Calling all SRAs!! Reporting Symposium?

TO : ALL SPECIAL RESEARCH ANALYSTS
FROM : [redacted] P.L. 86-36

SUBJECT: SYMPOSIUM ON REPORTING

I propose the holding of a two-day Symposium on Reporting as a means of supporting and encouraging continued emphasis on professional and uniform standards of reporting at the National Security Agency.

The Symposium would include major addresses by selected report editors from production elements, members of the reporting training faculty, and editors of Agency periodicals such as the Technical Journal and the Cryptologic Spectrum. Special Research analysts would be encouraged to submit papers on trends, developments, and techniques of reporting, and the best of their efforts would be presented at the sessions. A written report of the proceedings would be published and distributed to all Special Research analysts.

If successful, the Symposium might be repeated annually.

Is there any support for this proposal? Any suggestions for the agenda? Any offers of papers or assistance?

Please address your replies to me, [redacted] *care of Cryptolog.* P.L. 86-36

(UNCLASSIFIED)

Answers to Puzzle 1:

1 syllable: large charge, high spy, vile file, reel spiel, suave Slav. 2 syllables: chipper skipper, groovy movie, lighter fighter, graphic traffic, hippy crippy, marble garble, cipher lifter, sloppy copy. 3 syllables: sinister minister, quizzical physical, Egyptian convict-tion, astuter computer, prospective objective. 4 syllables: unpopulous metropolis (;), Bavarian aquarian, ornamental Oriental. 5 syllables: sequipedalian tatterdemalion, Panamanian subterranean. OK, now it's your turn.

DOCID: 4009704

★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ from the ★ ★ ★ ★ ★ ★ PRIZES & HONORS learned SPRING 1974 organizations

The Crypto-Mathematics Institute awarded prizes for the following papers:

First: [redacted] EO 1.4.(c) P.L. 86-36

P.L. 86-36 [redacted]

Second: [redacted]

Third: [redacted]," [redacted] EO 1.4.(c) P.L. 86-36

The first and third papers appeared in a Special Edition of the NSA Technical Journal (Special Fast Fourier Transform Issue II) in August 1973. The second was published as R111/MATH/09/74, in March 1974.

The Cryptolinguistic Association awarded prizes for the following papers:

First: "Can We Lick the Voice Problem?" [redacted] Technical Journal, Summer, 1972.

Second: "The Role of [redacted] Carrier Telephony in Soviet WWII Strategic Communications," (to be published in the Technical Journal, Summer, 1974). P.L. 86-36

Third: [redacted] [redacted] QRL (Quarterly Review for Linguists), August 1973.

EO 1.4.(c) P.L. 86-36

The Association presented the second annual Jaffe Award for linguistic accomplishment to Norman Wild "for his lifetime of continuing achievement and his permanent contributions in the field of language."

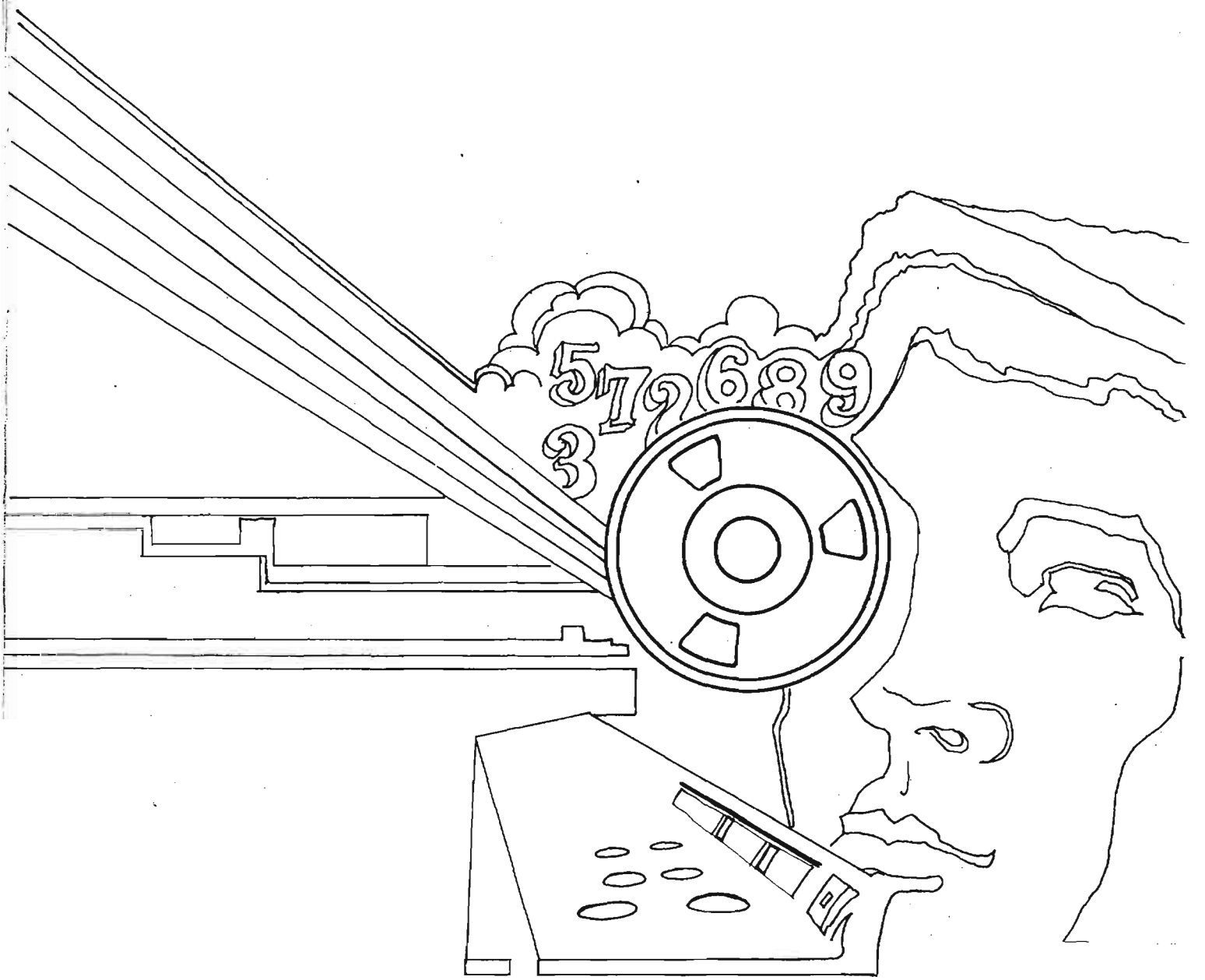
The Computer and Information Sciences Institute did not hold an essay contest this year, but replaced it with a Spring Conference "to promote professional writing and to provide a forum" for topics of current interest. Fourteen papers, chosen from those submitted, were presented at the Conference and have now been published in the Proceedings of the CISI Spring Conference, 21-24 May 1974. They are:

"Thoughts About System and Program Design" .....
"An Introduction to Structured Programming" .....
"Tools and Techniques in Optimization Efforts" .....
"The Insatiable Appetite of the Analyst" .....
"Large Scale File Processing--POGOL" .....
"An Interactive Display Position for the Morse Operator" .....
"A Graphics Protocol for Network Applications" .....
"The ARPANET, the COINS Network, and the Future" .....
[redacted] .....
"OMNIBUS Computer Network Communications Protocols" .....
"Minicomputers for Process Control" .....
"A Mini-Computer Speech Synthesizer" .....
"A 'Mini' Revolution in Field Processing and Reporting" .....
"A Generalized Character Input/Output System" .....

[redacted] P.L. 86-36

EO 1.4.(c) P.L. 86-36

~~(CONFIDENTIAL HVCCO)~~


5 7 2 6 8 9
3